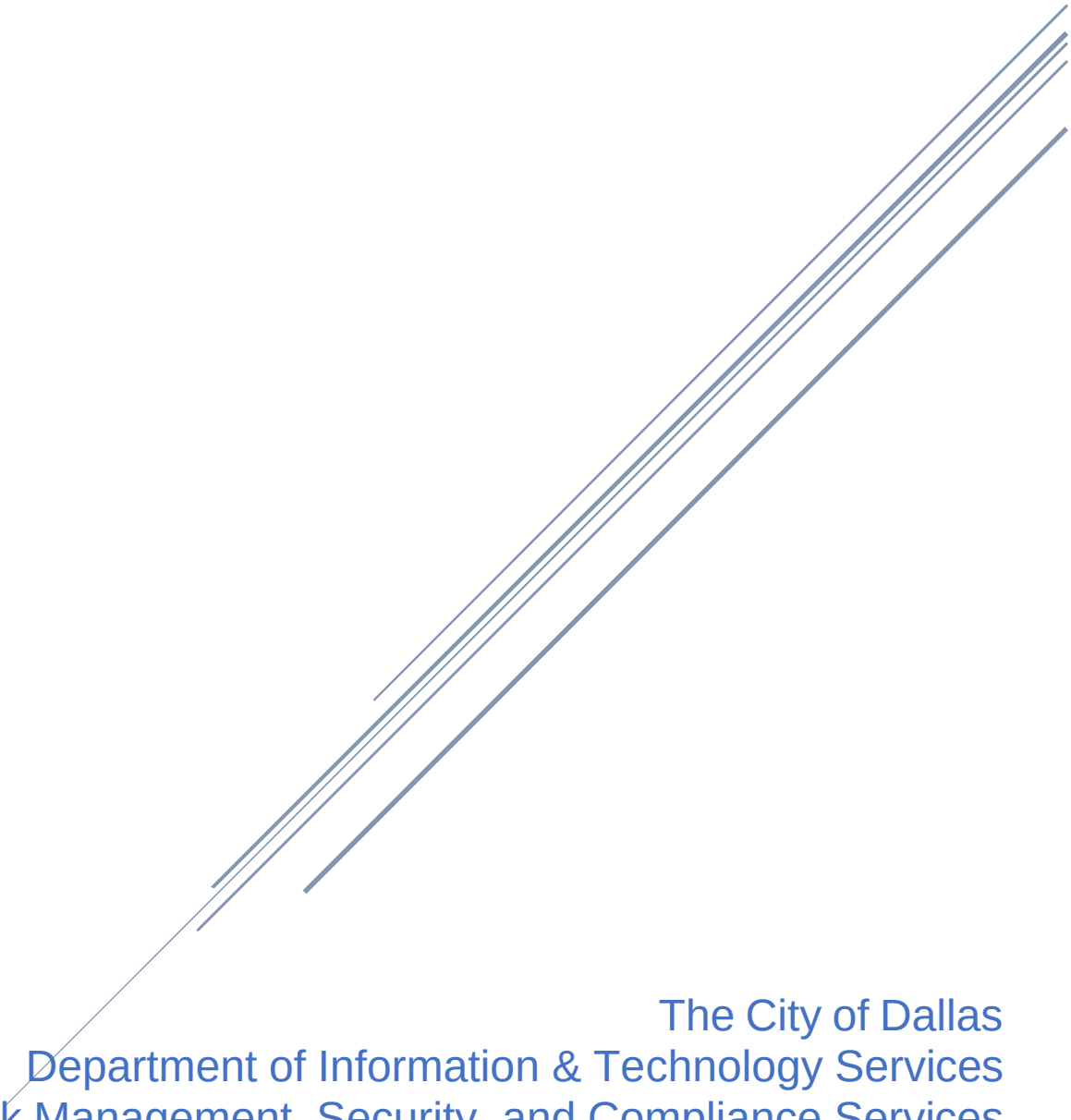
THE CITY OF DALLAS RANSOMWARE INCIDENT: MAY 2023

Incident Remediation Efforts and Resolution



The City of Dallas
Department of Information & Technology Services
ITS Risk Management, Security, and Compliance Services
September 20, 2023

Document Revision

Item	Change Description	Version	Date	Document State
1	Final Draft Document	1.0	08/30/2023	FINAL
2	Final Document	1.0	9/20/2023	FINAL

The City of Dallas Ransomware Incident: May 2023 Acknowledgements

The Chief Financial Officer of the City of Dallas and the Director of the Department of Information and Technology Services (ITS) acknowledge and thank the ITS Risk Management, Security, and Compliance Division for the efforts in capturing, analyzing, and reporting on information and events related to the City of Dallas 2023 Ransomware Incident: May 2023 – Incident Remediation Efforts and Resolution. Without their assistance, expertise, and background in information and cyber security matters, the City would not have as deep of an understanding as to the causes and effects related to this cyberattack upon City computing and communications resources.

General Source Information Acknowledgements

The City of Dallas acknowledges and thanks the many information sources that contributed to the construction of this document. Some source information was obtained through Gartner and Forrester research services. The City acknowledges and thanks those organizations for the guidance and assistance their individual contracted services provide the City. Some source information was also gathered from the elements of the United States Federal Government including but not limited to The National Institute of Standards and Technology (NIST), The Department of Homeland Security (DHS), The Department of Justice (DOJ), and others. The City acknowledges and thanks those organizations for the guidance and assistance for their services and standards provided to the City.

Since this document is not an academic paper, detailed citations are not used. This document will generally cite the sources of information used in the construction of this report using a bracketing artifice. The artifice used is square brackets with indication of the source within the square brackets. The following is an illustration of a citation used in this document: [Source], and [Source1, Source2].

Executive Summary

Purpose

This document provides an After-Action Report (AAR) to the Mayor, City Council, and City Executive Leadership pertaining to the ransomware incident initiated against the City of Dallas on the morning of Wednesday, May 03, 2023.

The purpose of an After-Action Report (AAR) is to analyze the management or response to an incident, exercise, or event by identifying strengths to be maintained and built upon, as well as identifying potential areas of improvement. [UH]

Context

The City of Dallas is a municipal corporation of the State of Texas. As the third largest Texas municipality, the hub of the fourth largest metropolitan area of the United States, and the ninth largest city within the United States, the City of Dallas is a logical choice for bad actors wishing to initiate and prosecute an Information Security (InfoSec) attack.

The City of Dallas is comprised of over 40 different departments, multiple offices, and several boards that support the many different missions assigned to it. Each department, office, and board effectively manages its own activities in support of the assigned missions. This diversity of approaches provides diversity in approach but also introduces a certain lack of organizational cohesion.

The City of Dallas operates over 860+ computer-based applications in support of approximately 100 technology and business services supporting City and City department missions. These applications and services are generally managed and operated by approximately 200 information technology (IT) professionals working within the City's Department of Information & Technology Services (ITS).

Royal Hacker Group and Initial Surveillance

Cyber criminals and hackers have found computer-based crime to be a viable and lucrative activity for financial and political gain. Over the past few decades, various hacker groups have banded and disbanded. In September 2022, a hacker group known as Royal came to the attention of law enforcement and cybersecurity officials.

Royal is identified as an amalgam of non-state actors believed to be composed of some very experienced cyber operators. Many Royal operators are believed to have previously belonged to other infamous cybercriminal groups including Conti Team One. [HHS]

In its short period of existence, Royal has successfully crippled – if not shut down – a shockingly large number of commercial, healthcare, and governmental entities. In the year 2022, ransomware victimized over 70 percent of organizations, marking a surge compared to the preceding five years and establishing the highest recorded proportion to date. This enduring

upward trajectory corresponds with the increasing profitability of ransomware for malicious actors. The incidence of ransomware exhibited a noteworthy annual growth rate of 13% during 2022, surpassing the cumulative increase of the preceding five years. Furthermore, the number of public ransomware victims escalated by 38% when compared to the initial quarter of 2023 and demonstrated an astounding 100% surge from the second quarter of 2022. This denotes a substantial 75 percent upswing in the mean count of monthly attacks in the United States between the initial and latter halves of the preceding 12-month period.

Royal began its cyber-attack surveillance and date exfiltration activities at the City of Dallas beginning in early April 2023. A review of system log data by both City and external cybersecurity experts identified the Royal group as having infiltrated the City and beginning its surveillance operations on April 7, 2023. Royal's initial access utilized the basic service domain service account, connecting to a server. Royal was then able to traverse the internal City infrastructure during the surveillance period using legitimate 3rd party remote management tools.

Using the City service account credentials, Royal performed reconnaissance activities in the City's IT infrastructure during the period of April 7, 2023, through May 4, 2023. During this time, Royal performed data exfiltration and ransomware delivery preparation activities. The data exfiltration activities performed during the surveillance period resulted in data leakages totaling an estimated 1.169 TB at a time prior to May 03, 2023.

During the surveillance period, Royal performed several actions to inject command and control software and established command-and-control beacons. The command-and-control beacons allowed Royal to prepare the City's network resources for the May 03, 2023, ransomware encryption attack.

Royal Ransomware Incident

Early on the morning of Wednesday, May 03, 2023, Royal began its ransomware attack on the City of Dallas. Using its previously deployed beacons, Royal began moving through the City's network and encrypting an apparently prioritized list of servers using legitimate Microsoft system administrative tools.

City attack mitigation efforts began immediately upon the detection of Royal's ransomware attack. To thwart Royal and slow its progress, City Server Support and Security teams began taking high-priority services and service supporting servers offline. As this was done, City service restoration identification activities began. Though service restoration could not begin until Royal was effectively removed from the City's network, service restoration teams needed to begin acquiring resources for service restoration efforts. For certain services such as Public Safety Computer-Aided Dispatch, those service restoration efforts began almost immediately.

Early in the attack, both internal and external cybersecurity, as well as external vendor support team professionals were called upon to assist the City in mitigating Royal and to recover its services. The Federal Law Enforcement was engaged and informed of the attack to provide guidance for future evidence needs. The external cybersecurity professionals provided expertise to identify, thwart, and remove Royal from the City's network while evidence was preserved and to Federal Law Enforcement of the Royal activities for possible future criminal prosecution efforts.

Notification of Information Disclosure

As obligated under State law, the City of Dallas provided notice to the State of Texas Office of the Attorney General (TxOAG). The City reported to the TxOAG that personal information of 26,212 Texas residents and a total of 30,253 individuals was potentially exposed due to the attack. The City reference to the City's notice was first published to the OAG's website on August 07, 2023. The OAG's website indicated that personal information such as names, addresses, social security information, health information, health insurance information, and other such information was exposed by Royal.

As required under federal law, and using different metrics for inclusion of individuals, the Department of Health and Human Services (HHS) was notified that the Sensitive Personal information (SPI) and Protected Health Information (PHI) of 30,253 individuals was potentially exposed by the activities of Royal. The breach submission date was recorded by HHS as of August 03, 2023.

Direct Costs of Ransomware Incident

To date, The Dallas City Council has approved a budget of $8.5 million in computer-based interdiction, mitigation, recovery, and restoration efforts directly tied to the Royal ransomware attack. This sum includes external cybersecurity professional services, identify theft and fraud protection services, and providers offering breach notification services to business partners and individuals that experienced data exposure due to the attack.

External cybersecurity professional services provided the City assistance that complemented the services provided by the City's external legal services team and that provided by federal, state, and local law enforcement agencies. The external cybersecurity professional services provided an alternative and experienced view to Royal, their activities, and relevant remediation approaches to reduce or remove damage caused by Royal. These efforts are largely complete, but an estimated final cost is to be provided by the end of 2023.

The breach notification service providers have provided data breach notifications to current, retired, and prior City personnel as well as their documented dependents when such information was exposed. The breach notification letters also offer complimentary two-year memberships in an identity protection program designed to deter individual identity theft or fraud. The cost for the first round of notifications will be provided by the end of 2023. Additional cost for this activity will be incurred as a second round of notifications is expected to occur in the fourth quarter of 2023 as additional individuals are identified. The second round of notifications is expected due to the City's detailed ongoing review of possible breached information.

To date, the City has dedicated a total of 39,590 hours towards the comprehensive remediation effort, of which ITS methodically documented 14,158 hours. Collaboratively, the City received support from external partners and contractors, who contributed an additional 1671 hours. These efforts encompassed various tasks such as the extraction of Mobile Dispatch Computer (MDC) and desktop units from fire and substations, the meticulous reconfiguration of compromised devices, the thorough reconstruction of technological infrastructure, and the ongoing vigilant

oversight of City technology environments as defined by the City's comprehensive security landscape.

As noted above, the City's current approved budget for the remediation of the Royal ransomware event is presently set to not exceed $8.5 million, The Dallas City Council was supportive and understanding in providing this initial budget amount as they understood that the attack response was ongoing and could extend significantly past the initial time and budget estimates.

City leadership is managing costs across both internal and external resources to ensure that Royal is removed from City computer and network resources. Presently, cost estimates are aligning with the initial budget approval from the Dallas City Council. The final cost analysis has not been completed at this time. The final forensic cost examination will be provided at a later date.

Section I – Royal Ransomware Incident – May 2023

This section of the document describes the ransomware incident on the City of Dallas initially identified on May 03, 2023. The incident on the City was claimed by the Royal Hacker Group and attributed by the United States Federal Bureau of Investigation (FBI) to that same group.

Royal Hacker Group

The threat actor group behind Royal ransomware first appeared in January 2022, pulling together actors previously associated with Roy/Zeon, Conti and TrickBot malware. Originally known as "Zeon" before renaming themselves "Royal" in September 2022, they are not considered a ransomware-as-a-service (RaaS) operation because their coding/infrastructure are private and not made available to outside actors [Kroll]. Backed by threat actors from Conti, Royal ransomware became one of the most prolific ransomware groups within three months of its founding. [TrendMicro]

Royal ransomware has been involved in high-profile attacks against critical infrastructure, especially healthcare since it was first observed in September 2022. Bucking the popular trend of hiring affiliates to promote their threat as a service, Royal ransomware operates as a private group made up of former members of Conti. [PA Unit42]

Since the start of 2023, Royal has escalated their attacks to focus on top tier corporations for larger ransoms. Their ransoms reportedly range from $250,000 to over $2 million. Although known for using the double extortion method of both encrypting and exfiltrating data, as of this writing the group does not have a data leak site where they publish the names of their victims. [Kroll]

Royal generally attempts to compromise victims through a BATLOADER infection, which threat actors usually spread through search engine optimization (SEO) poisoning. This infection involves dropping a Cobalt Strike Beacon as a precursor to the ransomware execution. [PA Unit42]

Royal ransomware made the rounds in researcher circles on social media in September 2022 after a cybersecurity news site published an article reporting how threat actors behind the ransomware group were targeting multiple corporations using targeted callback phishing techniques. [TrendMicro]

In its early campaigns, Royal deployed BlackCat's (another hacker group) encryptor, but later shifted to its own which dropped ransom notes like Conti's (a hacker group preceding the formation of Royal). After rebranding from Zeon to Royal, they began using the latter in its ransom notes generated by its own encryptor. [TrendMicro]

Malware

Malware, also known as malicious software or malicious code, refers to a program that is covertly inserted into another program with the intent to destroy data, run destructive or intrusive programs, or otherwise compromise the confidentiality, integrity, or availability of the victim's data, applications, or operating system. Malware is the most common external threat to most hosts, causing widespread damage and disruption and necessitating extensive recovery efforts within most organizations. [NIST 800-83r1]

End Point Response

Endpoint Detection and Response (EDR), also referred to as endpoint detection and threat response (EDTR), is an endpoint security solution that continuously monitors end-user devices to detect and respond to cyber threats like ransomware and malware. [CrowdStrike]

EDR security solutions record the activities and events taking place on endpoints and all workloads, providing security teams with the visibility they need to uncover incidents that would otherwise remain invisible. An EDR solution needs to provide continuous and comprehensive visibility into what is happening on endpoints in real time. [CrowdStrike]

An EDR tool should offer advanced threat detection, investigation, and response capabilities — including incident data search and investigation alert triage, suspicious activity validation, threat hunting, and malicious activity detection and containment. [CrowdStrike]

Introduction

Early on the morning of Wednesday, May 03, 2023, the City of Dallas was directly challenged by unknown third-party aggressors which had infiltrated the City's production computing and communications environments. The aggressors, self-identified in a text file – and corroborated by the Federal Authorities– as Royal, used the organizational information it had gathered through its previous surveillance efforts to launch a ransomware attack against the City, its personnel, and various residents.

Between April 7, 2023, and May 3, 2023, Royal initiated cyber-attack operations against the City of Dallas. The initial entry point was established through the utilization of service account which connected to a server. Leveraging this initial access, the threat actor cleverly navigated the internal infrastructure of the City by exploiting legitimate third-party remote management utilities.

Prior to May 3rd Ransomware deployment the Royal group constructed what are typically known as "Beacons" using remote management utilities and legitimate pen-testing technologies to traverse the City's internal network. These actions provided staging for Royal to exfiltrate an estimated 1.169 TB of data through the initial impacted server. In addition to data exfiltration, the

Threat Actor's credential harvesting techniques. This provided a list of users, accounts, and devices.

At 2:04 AM CST on May 3, 2023, the Threat Actor deployed the ransomware onto the systems within the Dallas environment. This process of malware execution persisted until May 4, 2023, at 5:58 AM CST, marked by the final observed instance of the Royal ransomware file. Subsequent to this occurrence, no further indications of Threat Actor activities identified.

Incident Response Plan

At 8:30 AM May 3, 2023, ITS reviewed and enacted the Incident Response Plan (IRP) enabling the incident response processes for a Ransomware event. These processes included communication directives to the Mayor, City Council, and City Manager's office. The plan provides detailed steps for detecting, containing, eradicating, and recovering from the ransomware incidents. It encompasses some technical measures, while also addressing legal and regulatory considerations, public relations, and stakeholder notifications.

Intrusion and Incident Timeline

Intrusion(s) Timeline:

The following table provides further details pertaining to timelines and system recovery efforts:

Intrusion or Recovery Action/Activity	Approximate Date
Likely entry into network	April 07, 2023
Intrusion Surveillance Phase	April 07 – May 03, 2023
Account Credentials First Obtained	April 07 – May 03, 2023
Attack Beacons Installed	April 07 – May 03, 2023
Identification of Possible Attack	May 03, 2023, at 2:54 am
Security Team Begins Analysis	May 03, 2023, at 2:54 am
Likely Lateral Movement through Network Begins	May 03, 2023, at 2:54 am
Attack Mitigation Procedures Initiated	May 03, 2023, at 5:00 am
Bridge Call Opened	May 03, 2023, at 5:23 am
Sanitation Servers Identified as affected	May 03, 2023, at 5:32 am
Set of Servers Identified as Infected	May 03, 2023, at 6:00 am
Team expanded to include additional IT disciplines	May 03, 2023, at 7:00 am
Disaster Recovery Manager Notified of Ongoing Incident	May 03, 2023, at 7:46 am
Citywide Announcement of Widespread Service Outage Made to City Staff	May 03, 2023, at 8:05 am
IT Executive Leadership Notified of Ongoing Incident (CIO, CFO)	May 03, 2023, at 8:22 am
Incident Response Plan (IRP) Initiated	May 03, 2023, at 8:30 am
Communication to Federal Authorities	May 03, 2023, at 8:30 am
City's Office of the City Attorney (CAO) and Office of Emergency Management (OEM) Notified of Ongoing Incident	May 03, 2023, at 8:30 am

Intrusion or Recovery Action/Activity	Approximate Date
Preservation of Evidence Procedures Initiated	May 03, 2023, at 8:31 am
Notification to City Mayor and Council of Ongoing Incident	May 03, 2023, at 9:05 am
Preservation and Restoration of Public Safety CAD Services Set as a Priority	May 03, 2023, at 9:35 am
Infected Server Inventory Tracking Initiated	May 03, 2023, at 9:44 am
Content of Royal README.txt Message Shared with Incident Team	May 03, 2023, at 9:45 am
Critical Public Safety Servers Infected	May 03, 2023, at 11:10 am
Begin Disconnecting Servers	May 03, 2023, at 11:00 am
Rebuild of CAD Servers Begin	May 03, 2023, at 12:00 pm
News Outlets Announce the Attack to the Public	May 03, 2023, at 12:30 pm
New Servers Become Infected	May 03, 2023, at 1:22 pm
Infected Databases Identified	May 03, 2023, at 1:30 pm
Print Servers Are Disconnected	May 03, 2023, at 2:11 pm
Initial Analysis Determines 173 Servers Are Impacted	May 03, 2023, at 2:15 pm
Multiple Domains Impacted	May 03, 2023, at 2:15 pm
Assessment that Multiple Departments Impacted	May 03, 2023, at 2:15 pm
Server Reinfection Confirmed	May 03, 2023, at 5:00 pm
Additional Blocks by CrowdStrike	May 03, 2023, at 5:30 pm
Confirmation of a Development Services server infected	May 03, 2023, at 6:00 pm
Confirmed Database GIS Servers Infected	May 03, 2023, at 6:09 pm
Malware Execution Extinguished by the City	May 04, 2023, at 5:58 am
Incident Support Team (IST) Activation	May 08, 2023, at 9:00 am
Incident Support Team (IST) De-activation	June 09, 2023, at 5:00 pm

Recovery Efforts

The ITS Operational team initiated restorative actions promptly after the acknowledged occurrence of malware affecting the technological framework, crucial to the operational vitality of the City and essential for resident services. This encompassed pivotal constituents, such as technology infrastructure components and systems deemed mission critical, including Computer Aided Dispatch (CAD), 311 Services, GIS services, and City-facing communication websites, were evaluated in terms of the extent of their influence and ranked for the sequence of reinstatement. To assist in this effort, the Incident Support Team (IST) was activated to provide the responding teams with information pertinent to the recovery and restoration of specific services.

The ITS team expeditiously initiated 24/7-hour around the clock rotating scheduled with efforts for an immediate trajectory of recuperation and reconstruction, constrained within the parameters of virtualized infrastructure environments. However, these endeavors necessitated a temporary pause due to the incomplete neutralization of the malicious executable's through EDR and its ability to propagate throughout the network ecosystem. ITS instituted a temporary hold, redirecting their efforts toward eradicating the executable in question. This included implementing

security protocols aimed at eliminating remote management technologies and introducing security policies to prevent reinfection.

After confirming the efficacy of these measures through assessment against the existing IT security technologies and visibility, the restorative endeavors refocused on reinstating the mission-critical and essential infrastructural technologies necessary for application support. These restorative tasks were organized into distinct workstreams, each assigned to specialized teams dedicated to the recovery initiative. The 24/7 approach allowed for a targeted allocation of resources based on specific requirements. The teams were structured into segments comprising server/system recovery, asset retrieval, adherence to the DOD 5220.22 M standards for complete device purging to eliminate malware, and the subsequent reimagining of affected systems.

Through a collaborative and cooperative effort involving the City and external vendors, essential functionality was restored to critical systems. These systems included Computer Aided Dispatch (CAD), which regained basic functionality through a manual dispatch process, City Websites, and the Development Services Permitting System. This restoration was achieved by the conclusion of May 8, 2023. Following this initial phase of recovery, on May 11, 2023, the CAD dispatch system transitioned back to full automation for dispatch operations. Additionally, regular services such as water billing to residents, regional wants and warrants processing, and the utilization of services critical for City payment and financial processing resumed operations.

In the final analysis, it was ascertained that the event led to the impairment of 230 servers, necessitating comprehensive endeavors for their complete restoration and recovery through available backups. Among these affected servers, the City successfully retired more than 100 surplus servers hosting outdated applications, unsupported operating systems, or deemed non-essential for crucial municipal services. The cumulative count of 1,398 endpoint devices went through reconstruction directly due to the effects of the Royal ransomware infection.

Major Affected Services and Supporting Applications

The following is a table of known services and supporting applications that were affected by ransomware operations performed by the Royal Hacker Group against the City of Dallas:

Service/Application	Brief Service Description	Affected City Department
GIS	Enterprise Geographic Information System	DWU, Dallas Police, Dallas Fire-Rescue, Other
Fusion Center	Dallas Police multi-source intelligence fusion solution	Dallas Police
Computer-Aided Dispatch (CAD)	Emergency Services Computer-Aided Dispatch Service	Dallas Police, Dallas Fire-Rescue, Dallas EMS, Dallas Marshals
Report Management Service/Code Compliance Management System	DPD-Web Report Management System (RMS) and Code Compliance Management System (CCMS)	Dallas Police, Code Compliance Services

Service/Application	Brief Service Description	Affected City Departments
Public Safety File Shares	Remote data stores (server-based, cloud-based) for individual and group use	Dallas Police
Surveillance Cameras Management System	Street cameras used for Police surveillance of a venue (e.g., Fair Park) or of a location (e.g., Starlight program)	Dallas Police
Animal Management Services	Animal and animal support monitoring, system management solution	Dallas Animal Shelter
Building Permitting System	Building Inspection plan and permitting management solution	Development Services
Secure File Transfer Service	Secure file transfer protocol server physically present within the City Data Center	Information & Technology Services (ITS), all other City departments
Library Management Service	Dallas Library book, media, and artifact management solution	Dallas Library
Warrants Management Service	Court ordered warrant management solution	Dallas Police, Dallas Marshals, Dallas Municipal Courts, other local agencies interoperating with City warrant resources.
Remote Water Meter Reading Service	Remote water meter reading technology supporting Dallas Water Utilities billing and operations divisions	Dallas Water Utilities
Payment Card Acceptance Solution	Payment card acceptance services supporting Dallas Water Utilities Billing solution operations.	Dallas Water Utilities, other departments using ePay for payment acceptance.
Public Safety Mobile Data Computer Services	Mobile Data Computer (MDC) predominately used by polices, fire, Emergency Medical Services (EMS), and emergency services for remote digital communications between deployed assets and between deployed assets and City Computer-Aided Dispatch Services.	Dallas Police, Dallas Fire-Rescue, Dallas EMS, Dallas Emergency Services, and other City departments and agencies using Mobile Data Computer for the capture and presentation of service information.
Alerting Service	Fire Station Alerting solutions designed to reduce response times and improve first responders' quality of life.	Dallas Fire-Rescue
Secure Print Services	Citywide secure print services used to monitor and manage print of secure documents at designated print stations.	All departments.
Fax Services	These applications and systems securely transmit paperless, digital faxes. This digital faxing solution greatly reduces the faxing costs by connecting to onsite analog or	All departments.

Service/Application	Brief Service Description	Affected City Departments
	digital telephony, voice-over-IP or the cloud.	

Systems and Services Restoration May 09, 2023, through June 13, 2023

The following chart represents the systems and services restoration checklist that was leveraged during the recovery efforts. Green – indicates completed, tested, and returned to production, Yellow – indicates Completed and in testing, White – indicates staged and currently being built.

Date Restored	Restoration Phase	Color Status	Application/Service
5/5/2023	Phase 1	Green	Computer Aided Dispatch
5/8/2023			Incident Support Team Activated
5/9/2023	Phase 1	Green	Financial Server
5/9/2023	Phase 1	Green	City Website
5/9/2023	Phase 1	Green	Development Service System
5/10/2023	Phase 1	Green	Police/Fire Automated Dispatch
5/11/2023	Phase 2	Green	City Controller System
5/11/2023	Phase 1	Green	Payment Card Acceptance Solution
5/11/2023	Phase 2	Green	Warrants Management Service
5/11/2023	Phase 1	Green	Cyber Security Server
5/11/2023	Phase 1	Green	Remote Meter Reading Service
5/12/2023	Phase 1	Green	Records Management System
5/15/2023	Phase 2	Green	Dallas Police Crime System
5/15/2023	Phase 2	Green	Code Management Service
5/15/2023	Phase 1	Green	Field Base Reporting Service
5/15/2023	Phase 1	Green	Citizen Request Management Service
5/16/2023	Phase 3	Green	Dallas Police Crimes Server
5/16/2023	Phase 2	Green	Animal Management Service
5/16/2023	Phase 3	Green	Financial Management Service
5/16/2023	Phase 2	Green	Dallas Fire Rescue System
5/17/2023	Phase 4	Green	Application and Data Workflow Orchestration
5/17/2023	Phase 2	Green	City Secretary System
5/17/2023	Phase 2	Green	Sanitation System
5/19/2023	Phase 4	Yellow	Virtual Viewer
5/22/2023	Phase 5	Green	Dallas Police Narcotic System
5/22/2023	Phase 4	Green	Dallas Fire Rescue Incident System
5/22/2023	Phase 4	Green	City Attorney System
5/22/2023	Phase 5	Green	Evidence Management Service
5/22/2023	Phase 5	Green	Dallas Police Safety Servers
5/22/2023	Phase 2	Green	Dallas Fire Rescue Safety Servers

Date Restored	Restoration Phase	Color Status	Application/Service
5/22/2023	Phase 5	Green	Dallas Police System
5/22/2023	Phase 4	Green	Virtual Viewer Service
5/23/2023	Phase 4	Green	Print Server
5/24/2023	Phase 2	Green	Financial Service Reporting Service
5/24/2023	Phase 5	Green	Merchant Accounting Software
5/25/2023	Phase 4	Green	Life Event Certificate Management Service
5/25/2023	Phase 4	Green	GIS Water Server
5/26/2023	Phase 1	Green	Court Management System
5/26/2023	Phase 3	Green	Dallas Police Enhanced Neighborhood System
5/30/2023	Phase 5	Green	Payment Management System
5/30/2023	Phase 5	Green	Dallas Police Specialized Server
5/30/2023	Phase 3	Green	Dallas Police Impound System
5/30/2023	Phase 3	Green	Internal Workflow Management Service
5/31/2023	Phase 5	Green	Vital Statistics
6/2/2023	Phase 3	Green	Court Docket Management System
6/2/2023	Phase 5	Green	Dallas Fire Specialized Server
6/2/2023	Phase 4	Green	Dallas Police Warrants System
6/6/2023	Phase 6	Green	Employee Management System
6/6/2023	Phase 6	Green	Survey Management Service
6/8/2023	Phase 5	Green	Dallas Police Traffic Data System
6/8/2023	Phase 5	Green	Vehicle Management Safety Report System
6/13/2023	Phase 6	Green	Back-Up Site Servers
6/13/2023	Phase 6	Green	Dallas Water Billing Payment File Service
6/13/2023	Phase 6	Green	Street Maintenance and Repair Management Service
6/13/2023	Phase 6	White	Financial Services Management Service
6/13/2023	Phase 4	Yellow	File Share Resources
6/13/2023	Phase 6	Green	GED Testing Management Service
6/13/2023	Phase 3	Yellow	Dallas Fire Rescue Personnel Server
6/13/2023	Phase 3	White	Library System
6/13/2023	Phase 2	Yellow	Library Resource Reservation Service
6/13/2023	Phase 4	Yellow	Building Services Server
6/13/2023	Phase 6	Yellow	Library Resource Reservation Service
6/13/2023	Phase 2	Yellow	Library Resource Management Service
6/13/2023	Phase 5	Yellow	Dallas Fire Rescue Case Entry System
6/13/2023	Phase 5	White	Public Safety Back-up Site Server
6/13/2023	Phase 6	Yellow	Security Gate Server
6/13/2023	Phase 4	Yellow	Stormwater Management Service
6/13/2023	Phase 6	Yellow	Development Services System
6/13/2023	Phase 6	Green	Waste Management Server

Section II – Operational Risk Factors Conducive to the Incident

This section of the document details internal and external risk factors conducive to the Royal Ransomware incident upon The City of Dallas. The Royal Ransomware incident upon the City began early on the morning of Wednesday, May 03, 2023.

City Under Constant Cyber Attack

The City of Dallas rejects millions of questionable inbound Internet network connection requests monthly. These requests are for a variety of reasons; many having legitimate reasons with most generally considered to be malicious in nature. The City is a large municipality and may be considered a potential target by cybercriminals because most municipalities fail to adequately secure its network resources. Additionally, the City manages, operates, and maintains several critical infrastructure targets that are appealing to cybercriminals (e.g., potable water, storm water management, flood water management, airports, aviation management systems, first-responder communications networks, emergency management operations, street management systems [e.g., streetlights, traffic lights])

The City of Dallas attempts to manage access to its network resources (e.g., servers, routers, load balancers) using the latest-generation firewall technology. Physical firewall devices and appliances are deployed, managed, and operated at Dallas City Hall. The City uses core firewalls for enterprise network operation and for security purposes. Perimeter firewalls are managed and operated in support of public internet access. Despite the use of latest-generation technology, the City is subject to 24/7 intrusion attempts requiring the City to use a multitude of security technologies both hardware and software based to ensure that only authorized traffic may access and enter the City's network.

The City is a Conglomeration of Missions

The City of Dallas is comprised of over 40 different departments, multiple offices, and several boards that support the many different missions assigned to it. Each department, office, and board effectively manage its own activities in support of assigned missions. This diversity of approaches provides diversity in approach but also introduces a certain lack of organizational cohesion.

A recent City organization chart identified eight high level portfolios individually managed by Deputy City Managers and Assistant City Managers. These portfolios included Housing & Homeless Solution; Public Safety; Economic Development; Workforce, Education, & Equity; Transportation & Infrastructure; Quality of Life, Art & Culture; Environment & Sustainability; and Government Performance & Financial Management. The missions and mission objectives of each of these portfolios is as diverse as the next.

As stated previously, this creates a sizable attack surface for the data City departments utilize. Departments and residents rely daily use of Critical Infrastructure, Payment Cards, Health Care, and resident's personal information to maintain continuity.

Technical Debt

The need to maintain current systems technical debt represents the compromises and suboptimal solutions that can emerge during the development and maintenance of software systems, is normal and unavoidable. [Gartner] ITS has recognized the presence of technical debt in its Technology Accountability Report (TAR) and initiated the modernization process. There is a clear requirement for the City to persist in these endeavors. These compromises may pose challenges for securing the environment. While they may provide short-term benefits, they can lead to risk. In terms of cybersecurity, technical debt can potentially aid the success of cyber events by virtue of inadequate built-in security measures in newer systems and unremedied vulnerabilities.

Vulnerabilities

Correspondingly, for all organizations, vulnerabilities and remote technology management is key to reducing risk in the City. Vulnerabilities may emerge during the development processes, making them universal targets for hackers who continually search for such weaknesses to exploit them for their own purposes. Effective patch management, involving the routine application of software and system updates to address known vulnerabilities and enhance software security, is paramount in safeguarding against ransomware attacks. Protocols are susceptible due to their less modern architectures and security standards, which often lack modern encryption, authentication mechanisms, and defenses against evolving cyber threats. These protocols frequently persist with unresolved vulnerabilities, leaving them exposed to exploitation by malicious actors. [CISA]

All organizations need to reduce risk of entry points for attackers to infiltrate systems and spread ransomware throughout networks. The absence of contemporary security features, coupled with attackers' ability to exploit these vulnerabilities through specialized techniques, heightens the risk of successful cyber intrusions. [FBI] After threat actors successfully achieves code execution on a device or gains network access, they can proceed to deploy ransomware. It's worth noting that these infection methods have likely maintained their popularity due to the surge in remote work and schooling since 2020, [CISA]

Section III – Factors Directly Mitigating the Impact of the Incident

This section of the document details internal and external factors believed to have directly mitigated the Royal Ransomware incident upon the City of Dallas. The Royal Ransomware incident upon the City has been identified as beginning early on the morning of Wednesday, May 03, 2023.

Introduction

This section of the After-Action Report (AAR) introduces and describes those factors that had directly impact upon ransomware incident mitigation.

Though interdiction, mitigation, and restoration of services was an “All Hands!” 24/7 effort, there were instances where the actions, activities, and ownership of just a few prevented the City Production computing and communications infrastructure from being dramatically damaged by Royal.

The City has developed and maintains a dynamic five-year strategic cyber security plan. The strategies identified in the plan rest upon a set of guiding principles, objectives, and priorities for cybersecurity that should benefit the City of Dallas’ over the coming three-to-five-year period. These principles, objectives, and priorities are selected from research and guidance from governmental authorities such as MITRE and the National Institute of Standards and Technology (NIST). It is believed that the use of this foundation will provide the City with the ability to appropriately select, deploy, manage, and operate cyber security technologies to effectively address, manage, and mitigate City IT vulnerabilities and threats.

The size and scope of the cybersecurity program has been increased to achieve the City’s strategic goals, including such efforts as improved public safety, critical infrastructure, and smarter cities. In addition to the important projects and security systems that will carry over from the last year’s improvements, new initiatives will be undertaken over the next three to five years to address emerging threats. This is to expand focus on identifying, protecting, detecting, responding, and recovering activities for the City of Dallas.

A threat environment can be managed and mitigated through identification, development, and use of appropriate cyber security initiatives. The City’s cyber security strategic plan identifies several sets of goals and addresses the City’s threat environment through use of appropriate cyber security initiatives supported by relevant investments in cyber security technology selected to protect the City’s information resources and assets.

The program roadmap, objectives, and intended outcomes have been identified and assessed by mature NIST functional families. This framework facilitates the monitoring and evaluation of the City’s efforts to implement cyber security controls and reduce risk.

Since 2019 the City of Dallas has evaluated the maturity of its Cybersecurity program. The evaluation utilizes NIST’s Common Security Framework (CSF) along with the application of the Capability Maturity Model Integration (CMMI) framework. This periodic evaluation provides the

City's Cybersecurity program with a direct view into essential areas of program operation and gives insight into five functional areas of cybersecurity (Identify, Protect, Detect, Respond, Recover) through inspection of City cyber security performance with 22 categories and 98 subcategories of management and control.

The City's Cybersecurity program is evaluated from Policy, Practice and/or Technology perspectives. These various perspectives assist City leadership in determining where investments should be made to continuously improve the City's ability to respond to and recover from any cyber security event.

Increased City InfoSec Investment

The City of Dallas has continuously augmented its commitment to Information Security (InfoSec) tools and solutions since the year 2019. These investments have bolstered and expanded the stratified strategy employed for cyber and information security. In 2019, the expenditure on IT security accounted for approximately 2.5% of the total IT budget. In contrast, as indicated by the projected budget for the 2023-24 fiscal period, a recommendation from the City Manager, coupled with the City Council's endorsement, is poised to elevate this allocation to nearly 10%. This substantial augmentation has enabled the City to curtail risk exposure and enhance the resilience of its technological infrastructure.

Despite the notable increase in overall expenditure, the maturation of the IT Operational program necessitated a comprehensive strategy and implementation methodology capable of accommodating the intricacies inherent to each supplemental IT security technology demand. The encumbrance of technological debt and the unwarranted intricacy inherent legacy networks introduce difficulties in adequately fortifying the network. Acknowledging the imperatives of the threat landscape becomes apparent that entities must empower all facets of a framework through meticulous planning, thereby safeguarding the infrastructure while simultaneously preparing for the expeditious execution of response and recovery measures.

Periodic Federal Agency Security Assessments

At intervals, the City of Dallas enters into arrangements with the United States Department of Homeland Security (DHS) to evaluate the security status of municipal information resources, including but not limited to its network and computer-based services. As recently as February 2023, the City finalized a fortnight-long collaboration with the Cybersecurity and Infrastructure Security Agency (CISA) to conduct a Security Penetration Test, commonly denoted as a "Red Team exercise." This evaluation comprehensively examined the City's infrastructure from both external and internal vantage points. These collaborative undertakings have yielded substantial insights into the cybersecurity posture; pinpointing areas necessitating enhancement and remediation.

Zero Trust Technologies

The City's stratified strategy for cybersecurity and information security is synergistically reinforced by a Security Program that actively involves City personnel, facilitating secure autonomous work practices. Over the course of the previous five years, the City has implemented the subsequent security governance, cyber, and information security technologies in harmony with numerous cybersecurity directives at the Federal level. Concurrently, IT has introduced and administers zero-trust network technologies to enhance resource access and management within the network. A substantial proportion of these technologies harness Artificial Intelligence-driven systems to aid in detecting and mitigating conceivable threats.

1. System backups – following events in 2021 comprehensive and precisely coordinated data safeguarding structure, seamlessly integrating automated regular backups, encrypted storage spread across redundant locations, versioning functionalities, offline storage mechanisms, expedient recovery protocols, regular testing procedures, sustained historical data retention, lucid documentation, and strategic alignment with business continuity requisites. This all-encompassing methodology guarantees the conservation, integrity, and swift restoration of vital information and system recovery.

2. Identity and Access Management platforms – the City has deployed and operates a cloud-based identity and access management platform. Such platforms allow the City to centralize, manage, and secure user authentication into City applications/solutions to over 200 applications. The platform provides multifactor authentication to assist in only allowing authorized personnel to access and use City applications/systems.
3. Real-time Threat Detection – the City has deployed and operates real-time thread detection solutions. Using network detection and response technologies, the City can identify and respond to security incidents as they are happening. The technologies use "cloud-scale machine learning" (ML) algorithms and rule-based techniques to detect behaviors, anomalies, and software vulnerabilities to provide security recommendations to City staff.

4. Network Behavior Analysis - The City has deployed and operates technologies built upon machine learning technologies that allow the City to identify if malevolent traffic flow within City networks. If such behavior is identified, the technologies can rapidly slow or remove such traffic from City networks.

5. Security Information and Event Management (SIEM) – The City has deployed and operates security information and event management technologies that allows the City to have real-time visibility into network and server events. The City has also engaged a managed security service provider (MSSP) to assist it in the monitoring and management of the large volumes of data captured by its security information and event management solutions.

6. FAIR Risk Assessments – The Factor Analysis of Information Risk (FAIR) is a taxonomy of the factors that contribute to risk and how they affect each other. FAIR is primarily concerned with determining accurate probabilities for two risk components of data loss events: frequency and magnitude. FAIR complements other risk methodologies by providing a way to produce consistent, defensible belief statements about risk.

7. HIPAA Risk Assessment – HIPAA risk assessments are a method to identify areas where an organization's protected health information (PHI) could be at risk. Factors considered in a HIPAA breach risk assessment include the nature and extent of breached PHI, the types of identifiers and the likelihood of re-identification, the unauthorized person who accessed or used the breached PHI, whether PHI was actually acquired or viewed, and the extent to which the risk to PHI is present.

8. NIST 800-171 Data Confidentiality Assessments – The NIST 800-171 standard establishes the base level of security required of computing systems that use or store confidential unclassified information (CUI). All organizations that access U.S. government date must comply with NIST standards. As this is a given, an 800-171 risk assessment can identify if an organization adequately safeguards information in a compliant manner relative to the current version of NIST 800-171.

9. Recovery Planning – Recovery Planning aligns with the City's primary cybersecurity goals, to identify and become proactive toward potential recovery efforts. The City plans to improve the maturity of its risk management processes and procedures. These processes and procedures will include identification of any potential deficiencies within recovery planning. Continued efforts to include many tabletop exercises and technical testing of planned recovery effort will contribute to a more resilient recovery when needed.

10. Privacy Risk Management – Privacy Risk Management describes a method for managing the risks that the processing of personal data can generate to individuals. In data privacy risk management, the impacted asset would be personal data, and its classification level. Privacy risk assessment is a process for identifying and evaluating privacy risks, which organizations can use to build customer trust by developing more effective solutions to protecting individuals' privacy when designing or deploying systems, products, and services that process data. This process assists the City to bring privacy into parity with their broader portfolio of enterprise risks.

11. Governance, Risk, and Compliance (GRC) – Governance, Risk, and Compliance (GRC) is a structured way to align IT with business goals while managing risks and meeting all industry and government regulations. It includes tools and processes to unify an organization's governance and risk management with its technological innovation and adoption. Companies use GRC to achieve organizational goals reliably, remove uncertainty, and meet compliance requirements.

12. Security Operations Center (SOC) – The City's Security Operations Center is where security technologies are applied and used to identify remediation challenges to the security of City information resources. The City's SOC provides visibility into distinct security challenges and coordinates the remediation efforts to reduce or eliminate those security challenges.

13. Business Impact Analysis (BIA) – A Business Impact Analysis (BIA) attempts to predict the consequences of disruptions to business function processes due to loss of information

technology. The BIA attempts to gather information needed to develop recovery strategies. When developing a BIA, potential loss scenario should be identified using a risk assessment methodology.

14. Periodic Disaster Recovery Tabletop Exercises –Tabletop exercises are discussion-based group sessions where team members meet to discuss their assigned roles and responsibilities in the event an organizational disaster is declared. A facilitator guides participants through discussions of one or more potential scenarios so that participants can visualize how they would respond to the scenario. An additional discussion is held after the scenario has been resolved to identify lessons learned and to discuss the possibilities of better scenario responses. These exercises are held on a periodic basis.
15. Configuration Management Database (CMDB) – The City is in the middle of assessment and implementation to track and better identify assets and their current configurations. This deployment operates a cloud-based Configuration Management Database (CMDB) used to store deployment and usage information about software and hardware assets. Including both, software asset management solution that allows the City to identify, define, track, and manage the City's 860+ software assets and hardware asset management solution.
16. Vulnerability Management Solutions – The City has deployed and operates various vulnerability management technologies and solutions to identify and remediate both known and potential vulnerabilities associated with City hardware and software resources. The management of vulnerabilities allows the City to identify, define, prioritize, and remediate according to the City's perception of possible threats to its vulnerability pool.
17. Microsegmentation – The City has deployed a network management technology that allows the City to manage relatively small segments of its network separately than other segments of its network. This technology allows the City to attribute special network characteristics to unique portions of its network relative to other small segments and to the overall network as a whole.
18. Crisis Communications – The City has begun implementing ITS Crisis communication technologies to allow ITS to better report and communicate within the department and City staff. These technologies will be leveraged for both the internal response as well as recovery.

The City of Dallas plans to acquire, deploy, manage, and operate the following cybersecurity technologies over the coming five-year period:

1. Security Orchestration, Automation and Response (SOAR) – Security Orchestration, Automation and Response is a group of cybersecurity technologies that allow organizations to respond to some incidents automatically. It collects inputs monitored by a security operations team and helps define, prioritize, and drive standardized incident response activities.

2. Application Performance Management – The City has deployed and operates application performance management technologies that allows the City to monitor and manage the availability of software applications. The goal of such technology is to ensure appropriate levels of application services are provided to the City.

3. Network Performance Management – The City has deployed and operates network performance management technologies that allow the City to monitor and manage the service capacity of its various networks. The technologies allow the City to determine in advance if any service capacity challenges may present themselves to City staff during the performance of their duties.

4. Industrial Control Systems Cybersecurity – The City has deployed and operates intrusion detection and intrusion protection systems in support of City Industrial Control Systems (ICS). These systems assure the secure operation of industrial control network components and emerging Internet of Things (IoT) control points. This technology may be used to protect City operated critical infrastructure such as aviation environment assets, streets management technology (e.g., smart street lighting, traffic light systems).

The City's current IT security program played a pivotal role in effectively mitigating the threat of ransomware attacks by employing a multifaceted and proactive approach. First, the program emphasizes robust cybersecurity measures across various layers of the organization's infrastructure. It involves the implementation of advanced intrusion detection systems, firewalls, and network segmentation to isolate critical systems from potential threats.

Secondly, a focus on comprehensive user education and awareness. By consistently training employees and IT teams about the risks associated with ransomware, the program empowers them to recognize and respond to the event quickly and with purpose to remediation. This heightened awareness enhances the City's ability to prevent ransomware from gaining more paralyzing foothold for a lengthy timeframe. Moreover, employees are educated on the importance of regular data backups and secure data storage practices, ensuring that critical information can be restored in the event of an attack, thus reducing the likelihood of succumbing to ransomware extortion.

In essence, a diligent IT security program combines advanced technological safeguards limit the impact for ransomware and assist in expediting the recovery. This approach not only prevents initial infection but also facilitates swift detection and response, minimizing the potential impact and disruption caused by ransomware attacks.

Section IV – Findings

This section of the document describes findings pursuant to the Royal Ransomware incident upon the City of Dallas. The Royal Ransomware incident has been identified as beginning early on the morning of Wednesday, May 03, 2023.

The following findings were the result of the City's engagement of the Royal Hacker Group beginning the morning of Wednesday, May 03, 2023.

Competent Incident Response Plans

The City of Dallas has managed and maintained Security Incident Response Plans for quite some time. Since 2019, the Department of Information and Technology Services (ITS) and its predecessor, the Department of Communications and Information Services (CIS) has engaged cybersecurity experts and federal agencies to assist in developing, managing, and maintaining current, relevant Incident Response Plans (IRP). The plans considered security incidents from a variety of sources and perspectives and identified approaches to remediating and resolving security incidents in a manner consistent with City goals and objectives for information resource management.

Security Incident Staff Periodically Exercised

The City of Dallas understands that plans without preparation are generally unproductive. To adequately prepare incident response staff for a variety of possible security incidents, the City periodically performs tabletop exercises, functional testing, and continuous updates to the Incident Response Plan. These exercises are performed to expose City staff to various attack vectors and possible attack interdiction techniques before they are needed to defend City information assets and resources. It is believed that the periodic tabletop exercises facilitated the prompt attention to the Royal ransomware attack and assisted staff coordinate during the actual threat to the City.

Identification

For 2023, the typical overall mean time to identify a data breach is 204 days [IBM]. This has been consistent over the past several years. Cybercriminals have become increasingly sophisticated in their methods of infiltrating systems and stealing sensitive information. This sophistication can contribute to the prolonged period it takes to detect these breaches, as attackers exploit vulnerabilities and use advanced techniques to avoid detection. The City's commitment to a cybersecurity program can directly attribute to the mean time of 27 days to identification, equating to a more "smash and grab approach".

Aggressive Incident Response

The City's response to Royal's ransomware incident of May 03, 2023, was considered both internally and externally as quite aggressive. Though there was an initial delay to identifying and

understanding that an attack against the City was underway, City leadership was able to turn a large number of resources toward the challenge in a very short period of time. As the timeline table displayed in Section II above indicates, Organizations typically require an average of 73 days to contain breaches in 2023, while requiring just 70 days on average in 2022 [IBM]. The City was effective at containing the issue in 1 day.

Vigorous measures were undertaken to ensure an uninterrupted round-the-clock commitment to the restoration of mission critical services for City critical infrastructure, public communications and essential services. The celerity of service restoration was of paramount importance. Both technology vendors and the cybersecurity experts contracted by the City expressed their commendation for the City's endeavors to prevent and eliminate unauthorized access by Royal to City information assets. Additionally, the City's protocols for service restoration also garnered appreciation.

Prompt Application and Service Restoration the recovery endeavor successfully attained a restoration rate exceeding 90 percent within an 18-day period. Through their concerted endeavors, methodical planning, and prompt execution, essential systems were successfully rehabilitated, thereby enabling the significant reinstatement of crucial services. It is important to note that this swift advancement was achieved despite the necessity to rebuild over 230 servers and 1,168 workstations. This rapid progress unarguably attests to the tenacity and resourcefulness of the recovery teams, underscoring their steadfast dedication to expeditiously surmount challenges and restore a state of normalcy.

Substantial Cybersecurity Investments Made in Advance of Incident

The City of Dallas understood that the information and cyber-security landscapes were quickly changing and began adopting and deploying risk-driven security technology in 2019. These investments correlated to the NIST Cybersecurity Framework (CSF) first published in 2014 and revised in 2018. The investments correlated to the five functional areas of the CSF: Identify, Protect, Detect, Respond, and Recover.

Relevant investments were made in technology areas such as Identity and Access Management (IAM), End-Point Detection and Response, Managed Detection and Response (EDR/MDR), Network-Centric Threat Detection and Response (NDR). The City’s financial dedication to cybersecurity growth from $3.4 million in 2019 to $7.8 million in 2023 with an additional $ 8.5 million for the event, is a direct contribution to protection of the resident’s data and assets. In addition, City staff dedicated to cybersecurity has grown from 18 full time resources in 2020 to 35 resources to manage security, compliance, and risk.

Section V –Recommendations

This section of the document describes recommendations to City management and operation teams in the context of the Royal Ransomware incident upon the City of Dallas. The Royal Ransomware incident upon the City has been identified as beginning early on the morning of Wednesday, May 03, 2023.

Perform a Cybersecurity Program Review

The City of Dallas has an active Cybersecurity Program. This program involves various security initiatives and involves City personnel from various departments and personnel levels. The consultants recommended that the program review focus on the identification of current state program gaps. The recommended review should include an in-depth analysis of people, processes, and technologies to gain an understanding of breakdowns in capabilities against real-world techniques used by attackers. The recommendation that the output of the review be used to develop and implement a threat-centric and risk-based cybersecurity program.

Privacy/Security Risk Assessment (Long-Term)

ITS Risk Management and Privacy teams shall conduct departmental Privacy and Security Risk Assessments. This Assessment is imperative to systematically identify, evaluate, and mitigate potential risks associated with the collection, processing, and storage of personal and sensitive information. By assessing the department's data management practices, technical safeguards, and compliance with relevant regulations. The Assessment provides a robust foundation for implementing tailored security measures. The outcomes of this Assessment will enable the organization to proactively address vulnerabilities, educate City employees, protect against data breaches, and ensure compliance with legal and regulatory obligations. Furthermore, the Assessment's insights will facilitate informed decision-making, allocate resources judiciously, and establish a defensible position against potential legal liabilities stemming from data privacy and security breaches.

Improve Data Backup and Restoration Processes

Application, service backup, and restoration processes are not always emphasized as a component of information resource deployment into the City's production environments. This lack of emphasis causes applications and services to be introduced into City production environments without appropriately tailored backup, recovery, or restoration processes and procedures; instead relying upon generic approaches to these application and service activities. It is recommended that all applications and services be required to have appropriately tailored backup, recovery, or restoration processes and procedures defined before an application or service can be introduced into a City production environment.

Harden Network and Compute Assets

Information Technology asset resources (e.g., servers) are not consistently managed and operated in a hardened state. Resource hardening is a set of processes or procedures that attempts to protect IT resources against cyberattacks by reducing its attack surface.

Reduce, Eliminate and Manage Technical Debt

Many City applications and services are not operating the most current versions of the underlying software. Several significant applications and services are operating on software versions that are no longer supported by software manufacturers and vendors. This condition causes a mismatch between the City's ability to deliver technical services in support of City and individual department business missions and cybersecurity best practices to discourage or defeat potential Threat Actor intrusions. It is recommended that City leadership participate in ongoing prioritization of technical services so that technical debt is eliminated or focused to low priority City applications and services.

Update to the Incident Response Plan

The City's incident response plan shall continuously be reviewed because of this or any event and as technology evolves. The Plan serves as a pivotal framework guiding an organization's approach to identifying, assessing, and mitigating security incidents. However, after major incidents, lessons learned become important to understand what worked and what did not according to the plan. This allows ITS to incorporate current threat intelligence, advanced mitigation strategies, and industry best practices. The updates are imperative to ensure the Plan's continued relevance and effectiveness in addressing emerging cyber threats. By continuously maintaining the Plan the City is allowed to improve not only its ability to safeguard sensitive information but also demonstrates a proactive commitment to mitigating legal and financial risks associated with potential security breaches and recovery efforts.

Comprehensive Plan of Actions and Milestones (POAM)

These recommendations shall be consolidated into a comprehensive Plan of Actions and Milestones (POAM) to track remediation. This strategic document serves as a roadmap for implementing the identified security and privacy measures in a structured and organized manner. Each recommendation will be assigned a specific action to be undertaken, accompanied by a corresponding milestone, which outlines a target completion date or timeframe. The POAM will outline the responsible individuals or teams accountable for executing each action item and will delineate the required resources, budget, and dependencies for successful implementation. Additionally, the POAM will provide a mechanism for ongoing tracking, monitoring, and reporting of progress toward achieving the established milestones.

Section VI – Appendices

This section of the document provides appendices of information relevant to the Royal Ransomware incident upon the City of Dallas. The Royal Ransomware incident upon the City has been identified as beginning early on the morning of Wednesday, May 03, 2023.

Appendix A – Glossary

This section of the document provides a glossary of terms used within this document.

Term	Definition
AAR	After-Action Report
CIO	Chief Information Officer / Director of ITS
CISO	Chief Information Security Officer
CTO	Chief Technology Officer
CIS	Department of Communications and Information Technology (a forerunner to ITS)
CISA	Cybersecurity & Infrastructure Security Agency
ITS	Department of Information & Technology Services
MITRE	MITRE Corporation
NIST	National Institute of Standards and Technology
Targeted Risk Assessment (TRA)	An assessment of risk targeted to a specific activity dependent upon the vulnerabilities, threats, and impact caused by a successful impact of a threat through exploitation of identified vulnerabilities.
TxOAG	The State of Texas Office of the Attorney General

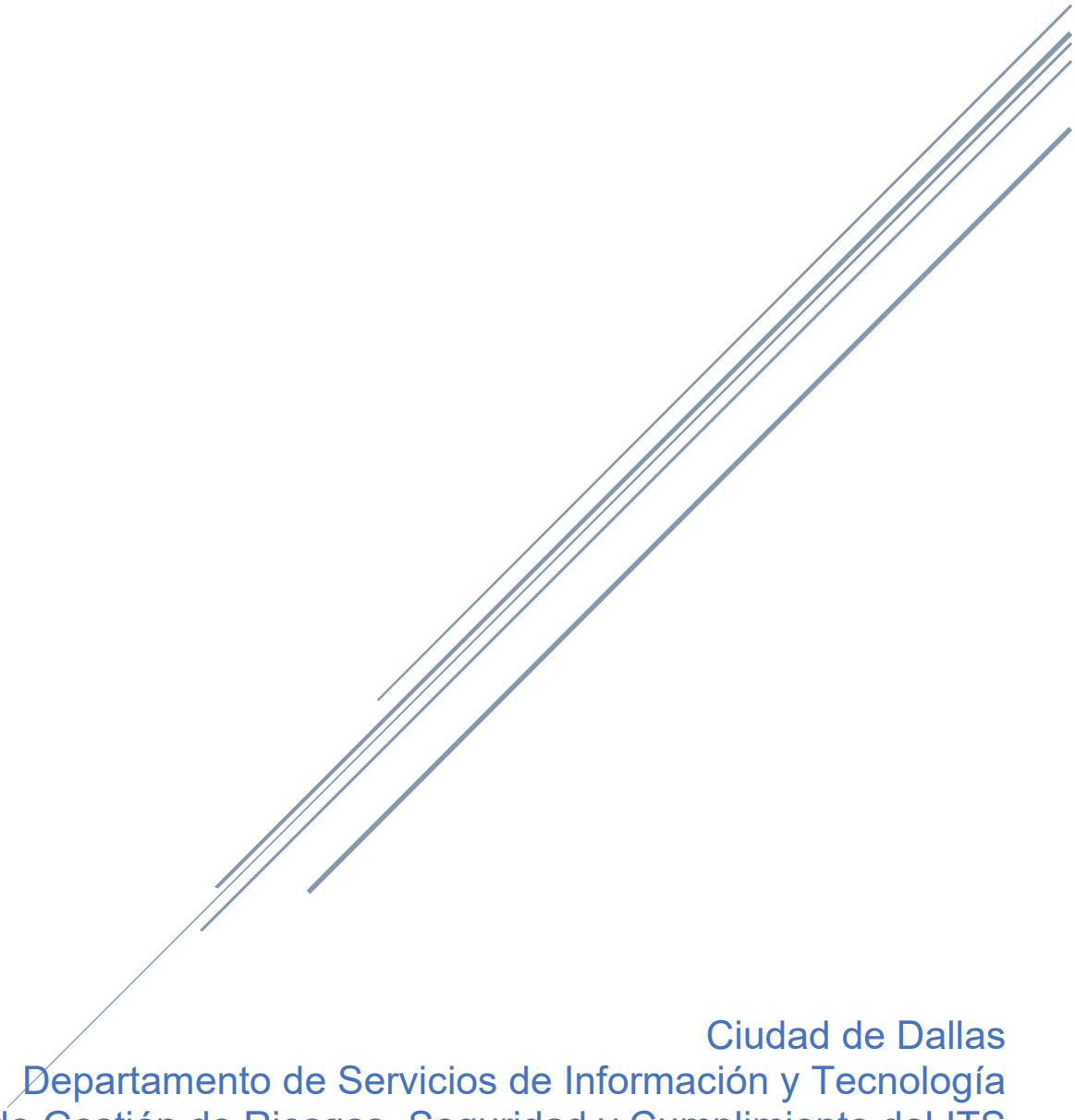
Appendix B – Information Sources

This section of the document provides a listing of informational sources used in the development of this document.

Identifier/Tag	Information Source
AWS	Amazon Web Services
CrowdStrike	CrowdStrike
Forrester	Forrester
Fortra	Fortra
Gartner	Gartner
HHS	US Department of Health and Human Services
IBM	IBM Corporation
ITIL2	Information Technology Infrastructure Library, Version 2, 2004
ITIL3	Information Technology Infrastructure Library, Version 3, 2007
ITIL4	Information Technology Infrastructure Library, Version 4, 2019
MITRE	MITRE Corporation
NIST	National Institute of Standards and Technology
OpenAI	The Open AI Foundation
PA Unit42	Palo Alto Unit 42
UH	University of Houston

INCIDENTE DE CIBERSECUESTRO DE DATOS EN LA CIUDAD DE DALLAS: MAYO 2023

Esfuerzos de Remediación y Resolución del Incidente



Ciudad de Dallas
Departamento de Servicios de Información y Tecnología
Servicios de Gestión de Riesgos, Seguridad y Cumplimiento del ITS
06 de septiembre de 2023

Revisión de Documentos

Asunto	Cambiar Descripción	Versión	Fecha	Estado del Documento
1	Borrador Final del Documento	1.0	30/08/2023	FINAL
2	Documento Final	1.0	01/09/2023	FINAL

Incidente de Cibersecuestro de Datos en la Ciudad de Dallas: Agradecimientos, mayo de 2023

El director financiero de la Ciudad de Dallas y el director del Departamento de Servicios de Información y Tecnología (ITS, por sus siglas en inglés) reconocen y agradecen a la División de Gestión de Riesgos, Seguridad y Cumplimiento del ITS los esfuerzos realizados en la recopilación, análisis y elaboración de informes sobre la información y los eventos relacionados con el Incidente de Cibersecuestro de Datos en la Ciudad de Dallas de 2023: Mayo de 2023 – Esfuerzos de Remediación y Resolución del Incidente. Sin su asistencia, experiencia y conocimientos en asuntos de información y ciberseguridad, la Ciudad no tendría un conocimiento tan profundo de las causas y efectos relacionados con este ataque cibernético a los recursos informáticos y de comunicaciones de la Ciudad.

Agradecimientos en relación con las Fuentes Generales de Información

La Ciudad de Dallas reconoce y agradece las numerosas fuentes de información que han contribuido a la elaboración de este documento. Algunas fuentes de información se obtuvieron a través de los servicios de investigación de Gartner y Forrester. La Ciudad reconoce y agradece a estas organizaciones la orientación y asistencia que sus servicios individuales contratados proporcionan a la Ciudad. También se recopiló alguna fuente de información de sectores del Gobierno Federal de los Estados Unidos, incluyendo, pero no limitándose a, el Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés), el Departamento de Seguridad Nacional (DHS, por sus siglas en inglés), el Departamento de Justicia (DOJ, por sus siglas en inglés) y otros. La Ciudad reconoce y agradece a esas organizaciones por la orientación y asistencia por sus servicios y estándares brindados a la Ciudad.

Dado que este documento no es un trabajo académico, no se utilizan citas detalladas. En general, este documento citará las fuentes de información utilizadas en la elaboración de este informe utilizando un artificio de corchetes. El artificio utilizado son los corchetes con indicación de la fuente entre corchetes. A continuación, se ilustra una cita utilizada en este documento: [Fuente] y [Fuente1, Fuente2].

Resumen Ejecutivo

Propósito

Este documento proporciona un Informe Posterior a la Acción (AAR, por sus siglas en inglés) para el alcalde, el Concejo de la Ciudad y el personal directivo de la Ciudad en relación con el incidente de cibersecuestro de datos iniciado contra la Ciudad de Dallas en la mañana del miércoles, 3 de mayo de 2023.

El propósito de un Informe Posterior a la Acción (AAR) es analizar la gestión o la respuesta a un incidente, ejercicio o evento mediante la identificación de los puntos fuertes que se deben mantener y aprovechar, así como la identificación de posibles áreas de mejora. [UH]

Contexto

La Ciudad de Dallas es una corporación municipal del Estado de Texas. Como el tercer municipio más grande de Texas, el centro de la cuarta área metropolitana más grande de los Estados Unidos y la novena ciudad más grande dentro de los Estados Unidos, la Ciudad de Dallas es una opción lógica para los malos actores que desean iniciar y procesar un ataque de Seguridad de la Información (InfoSec).

La Ciudad de Dallas se compone de más de 40 departamentos diferentes, múltiples oficinas y varias juntas que apoyan las diferentes misiones que se le han asignado. Cada departamento, oficina y junta gestiona eficazmente sus propias actividades en respaldo de las misiones asignadas. Esta diversidad de enfoques proporciona diversidad de enfoques, pero también introduce una cierta falta de cohesión organizacional.

La Ciudad de Dallas opera más de 860 aplicaciones informáticas que respaldan aproximadamente 100 servicios tecnológicos y comerciales que respaldan las misiones de la Ciudad y los departamentos de la Ciudad. Estas aplicaciones y servicios generalmente son gestionados y operados por aproximadamente 200 profesionales de tecnología de la información (IT, por sus siglas en inglés) que trabajan dentro del Departamento de Servicios de Información y Tecnología de la Ciudad (ITS, por sus siglas en inglés).

Grupo de Piratas Informáticos Royal y Vigilancia Inicial

Los ciberdelincuentes y los piratas informáticos han descubierto que los delitos informáticos son una actividad viable y lucrativa para obtener beneficios económicos y políticos. En las últimas décadas, varios grupos de piratas informáticos se han agrupado y disuelto. En septiembre de 2022, un grupo de piratas informáticos conocido como Royal llamó la atención de los oficiales policiales y de ciberseguridad.

Se cree que Royal es una amalgama de actores no estatales compuesta por algunos operadores cibernéticos muy experimentados. Se cree que muchos operadores de Royal pertenecieron con anterioridad a otros grupos infames de cibercriminales, incluyendo Conti Team One. [HHS]

En su corta existencia, Royal ha conseguido paralizar –cuando no cerrar– un número asombrosamente elevado de entidades comerciales, de salud y gubernamentales. En 2022, el cibersecuestro de datos afectó a más del 70 por ciento de las organizaciones, lo que marcó un aumento en comparación con los cinco años previos y estableció la proporción más elevada registrada hasta la fecha. Esta persistente trayectoria ascendente se corresponde con la creciente rentabilidad del cibersecuestro de datos para los actores maliciosos. La incidencia del cibersecuestro de datos demostró una notable tasa de crecimiento anual del 13% durante 2022, superando el aumento acumulado de los cinco años previos. Además, el número de víctimas públicas del cibersecuestro de datos aumentó un 38% en comparación con el trimestre inicial de 2023 y demostró un sorprendente aumento del 100% con respecto al segundo trimestre de 2022. Esto denota un aumento sustancial del 75% en el recuento medio de ataques mensuales en los Estados Unidos entre la primera y la última mitad del periodo de 12 meses anterior.

Royal comenzó sus actividades de vigilancia de ciberataques y exfiltración de datos en la Ciudad de Dallas a comienzos de abril de 2023. Una revisión de los datos de registro del sistema por parte de expertos en ciberseguridad externos y de la Ciudad identificó que el grupo Royal se había infiltrado en la Ciudad y había comenzado sus operaciones de vigilancia el 7 de abril de 2023. El acceso inicial de Royal utilizó la cuenta de servicio de dominio de servicio básico y se conectó a un servidor. Luego, Royal pudo atravesar la infraestructura interna de la Ciudad durante el período de vigilancia utilizando herramientas legítimas de gestión remota de terceros.

Utilizando las credenciales de la cuenta de servicio de la Ciudad, Royal realizó actividades de reconocimiento en la infraestructura de IT de la Ciudad durante el período del 7 de abril de 2023 al 4 de mayo de 2023. Durante este tiempo, Royal realizó actividades de preparación de exfiltración de datos y distribución del programa para el cibersecuestro de datos. Las actividades de exfiltración de datos realizadas durante el período de vigilancia dieron lugar a filtraciones de datos por un total estimado de 1.169 TB en un momento previo al 3 de mayo de 2023.

Durante el período de vigilancia, Royal realizó varias acciones para introducir un programa informático de comando y control y estableció balizas de comando y control. Las balizas de comando y control permitieron a Royal preparar los recursos de red de la Ciudad para el ataque de cifrado para el cibersecuestro de datos del 3 de mayo de 2023.

Incidente de Cibersecuestro de Datos de Royal

A primera hora del miércoles, 3 de mayo de 2023, Royal comenzó su ataque de cibersecuestro de datos en la Ciudad de Dallas. Utilizando sus balizas previamente implementadas, Royal comenzó a moverse a través de la red de la Ciudad y a cifrar una lista aparentemente priorizada de servidores utilizando herramientas administrativas legítimas del sistema Microsoft.

Los esfuerzos de mitigación del ataque de la Ciudad comenzaron inmediatamente luego de la detección del ataque de cibersecuestro de datos de Royal. Para frustrar a Royal y ralentizar su progreso, los equipos de seguridad y soporte del Servidor de la Ciudad comenzaron a desconectar los servicios de alta prioridad y los servidores de soporte de servicios. Una vez hecho esto, comenzaron las actividades de identificación de restauración del servicio de la Ciudad. Aunque la restauración del servicio no podría comenzar hasta que Royal fuera efectivamente eliminado de la red de la Ciudad, los equipos de restauración del servicio necesitaban comenzar a adquirir recursos para los esfuerzos de restauración del servicio. Para

ciertos servicios, como el Despacho Asistido por Computadora de Seguridad Pública, esos esfuerzos de restauración del servicio comenzaron casi de inmediato.

En las primeras fases del ataque, se pidió a los profesionales del equipo tanto interno como externo de ciberseguridad, así como a los proveedores externos que ayudaran a la Ciudad a mitigar a Royal y recuperar sus servicios. Las autoridades federales participaron y fueron informadas sobre el ataque para brindar orientación para futuras necesidades de evidencia. Los profesionales externos de ciberseguridad brindaron experiencia para identificar, frustrar y eliminar a Royal de la red de la Ciudad mientras se preservaban las pruebas y las actividades de Royal para las autoridades federales para posibles acciones penales futuras.

Notificación de Divulgación de Información

De conformidad con la legislación Estatal, la Ciudad de Dallas notificó a la Oficina del Fiscal General del Estado de Texas (TxOAG, por sus siglas en inglés). La Ciudad informó a la TxOAG que información personal de 26,212 residentes de Texas y un total de 30,253 personas quedó potencialmente expuesta debido al ataque. La referencia de la Ciudad al aviso de la Ciudad se publicó por primera vez en el sitio web de la OAG el 7 de agosto de 2023. El sitio web de la OAG indicó que Royal expuso información personal como nombres, direcciones, información de seguridad social, información de salud, información de seguro de salud, y otra información similar.

Tal y como exige la ley federal, y utilizando diferentes parámetros para la inclusión de personas, se notificó al Departamento de Salud y Servicios Humanos (HHS, por sus siglas en inglés) que la Información Personal Confidencial (SPI, por sus siglas en inglés) e Información de Salud Protegida (PHI, por sus siglas en inglés) de 30,253 personas quedaron potencialmente expuestas por las actividades de Royal. La fecha de presentación de la filtración fue registrada por el HHS el 3 de agosto de 2023.

Costos Directos del Incidente de Cibersecuestro de Datos

Hasta la fecha, el Concejo de la Ciudad de Dallas ha aprobado un presupuesto de $8.5 millones en esfuerzos de interdicción, mitigación, recuperación y restauración basados en computadora directamente relacionados con el ataque de cibersecuestro de datos de Royal. Esta suma incluye servicios profesionales externos de ciberseguridad, servicios de protección contra robo de identidad y fraude, y proveedores que ofrecen servicios de notificación de filtraciones a socios comerciales e individuos que experimentaron exposición de datos debido al ataque.

Los servicios profesionales externos de ciberseguridad brindaron a la Ciudad asistencia que complementó los servicios brindados por el equipo de servicios legales externos de la Ciudad y los brindados por las agencias policiales federales, estatales y locales. Los servicios profesionales externos de ciberseguridad brindaron una perspectiva alternativa y experimentada de Royal, sus actividades y enfoques de remediación relevantes para reducir o eliminar el daño causado por Royal. Estos esfuerzos están en gran medida completos, pero se proporcionará un costo final estimado a fines de 2023.

Los proveedores de servicios de notificación de filtraciones han proporcionado notificaciones de filtración de datos al personal actual, jubilado y previo de la Ciudad, así como a sus dependientes

documentados cuando dicha información fue expuesta. Las cartas de notificación de filtración también ofrecen membresías gratuitas de dos años en un programa de protección de identidad diseñado para disuadir el fraude o el robo de identidad individual. El costo de la primera fase de notificaciones se proporcionará a fines de 2023. Se incurrirá en costos adicionales para esta actividad, ya que se espera que se realice una segunda fase de notificaciones en el cuarto trimestre de 2023, a medida que se identifiquen personas adicionales. Se espera la segunda fase de notificaciones debido a la revisión detallada y continua por parte de la Ciudad de la posible información vulnerada.

Hasta la fecha, la Ciudad ha dedicado un total de 39,590 horas al esfuerzo integral de remediación, de las cuales el ITS documentó metódicamente 14,158 horas. De manera colaborativa, la Ciudad recibió apoyo de socios y contratistas externos, quienes contribuyeron con 1671 horas adicionales. Estos esfuerzos abarcaron diversas tareas, como la extracción de Computadoras de Despacho Móviles (MDC, por sus siglas en inglés) y unidades de escritorio del Departamento de Bomberos y subestaciones, la reconfiguración meticulosa de dispositivos comprometidos, la reconstrucción exhaustiva de la infraestructura tecnológica y la supervisión atenta y continua de los entornos tecnológicos de la Ciudad, tal como se define en el panorama de seguridad integral de la Ciudad.

Como se ha indicado previamente, el presupuesto actual aprobado por la Ciudad para la remediación del evento de cibersecuestro de datos de Royal no excederá los $8.5 millones. El Concejo de la Ciudad de Dallas apoyó y comprendió al proporcionar esta suma presupuestaria inicial, ya que comprendieron que la respuesta al ataque estaba en curso y podría extenderse significativamente más allá de las estimaciones iniciales de tiempo y presupuesto.

El personal directivo de la Ciudad está gestionando los costos de los recursos internos y externos para garantizar que Royal sea eliminado de los recursos informáticos y de la red de la Ciudad. Actualmente, las estimaciones de costos se están alineando con la aprobación del presupuesto inicial por parte del Concejo de la Ciudad de Dallas. El análisis de costos final no se ha completado en este momento. El examen final de costos periciales se realizará en una fecha posterior.

Sección I – Incidente de Cibersecuestro de Datos de Royal – Mayo de 2023

Esta sección del documento describe el incidente de cibersecuestro de datos en la Ciudad de Dallas inicialmente identificado el 3 de mayo de 2023. El incidente en la Ciudad fue reivindicado por el Grupo de Piratas Informáticos Royal y atribuido por la Buró Federal de Investigaciones (FBI, por sus siglas en inglés) de los Estados Unidos a ese mismo grupo.

Grupo de Piratas Informáticos Royal

El grupo de actores amenazantes detrás del cibersecuestro de datos de Royal apareció por primera vez en enero de 2022, reuniendo a actores previamente asociados con el programa malicioso Roy/Zeon, Conti y TrickBot. Originalmente conocidos como “Zeon” antes de rebautizarse como “Royal” en septiembre de 2022, no se consideran una operación de cibersecuestro de datos como servicio (RaaS, por sus siglas en inglés) porque su codificación/infraestructura es privada y no está disponible para actores externos [Kroll]. Respaldado por actores amenazantes de Conti, el cibersecuestro de datos de Royal se convirtió en uno de los grupos de cibersecuestro de datos más prolíficos a los tres meses de su fundación. [TrendMicro]

El cibersecuestro de datos de Royal ha estado involucrado en ataques de alto perfil contra infraestructura crítica, especialmente atención médica, desde que se observó por primera vez en septiembre de 2022. Contradiciendo la tendencia popular de contratar afiliados para promover su amenaza como un servicio, el cibersecuestro de datos de Royal opera como un grupo privado formado por antiguos miembros de Conti. [PA Unit42]

Desde principios de 2023, Royal ha intensificado sus ataques para enfocarse en corporaciones de primer nivel para obtener rescates mayores. Según se informa, sus rescates oscilan entre $250,000 y más de $2 millones. Aunque es conocido por utilizar el método de doble extorsión de cifrar y exfiltrar datos, al momento de elaborar este documento el grupo no tiene un sitio de filtración de datos donde publiquen los nombres de sus víctimas. [Kroll]

Royal generalmente intenta comprometer a las víctimas a través de una infección BATLOADER, que los actores amenazantes suelen propagar infectando la Optimización del Motor de Búsqueda (SEO, por sus siglas en inglés). Esta infección implica colocar una Baliza de Cobalt Strike como precursor de la ejecución del cibersecuestro de datos. [PA Unit42]

El cibersecuestro de datos de Royal se difundió en los círculos de investigadores de las redes sociales en septiembre de 2022 luego de que un sitio de noticias sobre ciberseguridad publicara un artículo en el que informaba cómo los actores amenazantes detrás del grupo de cibersecuestro de datos se dirigían a múltiples corporaciones utilizando técnicas de fraude electrónico con devolución de llamadas selectivas. [TrendMicro]

En sus primeras campañas, Royal implementó el cifrado de BlackCat (otro grupo de piratas informáticos), pero luego cambió a uno propio que arrojaba notas de rescate como el de Conti (un grupo de piratas informáticos que precedió a la formación de Royal). Luego de cambiar de nombre de Zeon a Royal, comenzaron a utilizar este último en sus notas de rescate generadas por su propio cifrado. [TrendMicro]

Programa Malicioso

El programa malicioso, también conocido como programa informático malicioso o código malicioso, se refiere a un programa que se inserta de forma encubierta en otro programa con la intención de destruir datos, ejecutar programas destructivos o intrusivos, o comprometer de otro modo la confidencialidad, integridad o disponibilidad de los datos, aplicaciones o sistema operativo de la víctima. Un programa malicioso es la amenaza externa más común para la mayoría de los servidores, causa daños e interrupciones generalizados y requiere grandes esfuerzos de recuperación dentro de la mayoría de las organizaciones. [NIST 800-83r1]

Respuesta de Puntos Finales

Detección y Respuesta de Puntos Finales (EDR, por sus siglas en inglés), también conocida como detección de puntos finales y respuesta a amenazas (EDTR, por sus siglas en inglés), es una solución de seguridad de puntos finales que monitorea continuamente los dispositivos de los usuarios finales para detectar y responder a amenazas cibernéticas como cibersecuestro de datos y programas maliciosos. [CrowdStrike]

Las soluciones de seguridad de EDR registran las actividades y eventos que tienen lugar en los puntos finales y todas las cargas de trabajo, brindando a los equipos de seguridad la visibilidad que necesitan para descubrir incidentes que de otro modo permanecerían invisibles. Una solución EDR debe proporcionar una visibilidad continua y completa de lo que sucede en los puntos finales en tiempo real. [CrowdStrike]

Una herramienta EDR debe ofrecer capacidades avanzadas de detección, investigación y respuesta a amenazas, incluyendo la búsqueda de datos de incidentes y la clasificación de alertas de investigación, validación de actividades sospechosas, búsqueda de amenazas y detección y contención de actividades maliciosas. [CrowdStrike]

Introducción

A primera hora de la mañana del miércoles, 3 de mayo de 2023, la Ciudad de Dallas fue atacada directamente por agresores desconocidos que se habían infiltrado en los entornos informáticos y de comunicaciones de producción de la Ciudad. Los agresores, autoidentificados en un archivo de texto (y corroborado por las autoridades federales) como Royal, utilizaron la información organizacional que habían recopilado a través de sus esfuerzos de vigilancia previos para lanzar un ataque de cibersecuestro de datos contra la Ciudad, su personal y varios residentes.

Entre el 7 de abril de 2023 y el 3 de mayo de 2023, Royal inició operaciones de ciberataque contra la Ciudad de Dallas. El punto de entrada inicial se estableció mediante la utilización de una cuenta de servicio que se conectaba a un servidor. Aprovechando este acceso inicial, el actor amenazante navegó hábilmente por la infraestructura interna de la Ciudad explotando utilidades legítimas de gestión remota de terceros.

Antes de la implementación del cibersecuestro de datos el 3 de mayo, el grupo Royal construyó lo que normalmente se conoce como "Balizas" utilizando utilidades de gestión remota y tecnologías legítimas de prueba de penetración para atravesar la red interna de la Ciudad. Estas acciones sirvieron de escenario para que Royal filtrara un estimado de 1.169 TB de datos a través del servidor afectado inicialmente. Además de la exfiltración de datos, las técnicas de recolección de credenciales del actor amenazante. Esto proporcionó una lista de usuarios, cuentas y dispositivos.

A las 2:04 AM CST del 3 de mayo de 2023, el actor amenazante implementó el cibersecuestro de datos en los sistemas dentro del entorno de Dallas. Este proceso de ejecución del programa maligno persistió hasta el 4 de mayo de 2023 a las 5:58 AM CST, marcado por la última instancia observada del archivo del cibersecuestro de datos de Royal. Luego de este suceso, no se identificaron más indicios de actividades del actor amenazante.

Plan de Respuesta al Incidente

A las 8:30 AM del 3 de mayo de 2023, ITS revisó y promulgó el Plan de Respuesta al Incidente (IRP, por sus siglas en inglés) que permite los procesos de respuesta a incidentes para un evento de cibersecuestro de datos. Estos procesos incluyeron directivas de comunicación para el alcalde, el Concejo de la Ciudad y la Oficina del Administrador de la Ciudad. El plan proporciona pasos detallados para detectar, contener, erradicar y recuperarse de los incidentes de cibersecuestro de datos. Abarca algunas medidas técnicas, a la vez que aborda consideraciones legales y regulatorias, relaciones públicas y notificaciones a las partes interesadas.

Cronología de la Intrusión e Incidente

Cronograma de Intrusiones:

La siguiente tabla proporciona más detalles relacionados con las fechas y los esfuerzos de recuperación del sistema:

Acción/Actividad de Intrusión o Recuperación	Fecha Aproximada
Probable entrada en la red	07 de abril de 2023
Fase de Vigilancia de Intrusiones	07 de abril – 03 de mayo de 2023
Credenciales de Cuenta Obtenidas por Primera Vez	07 de abril – 03 de mayo de 2023
Balizas de Ataque Instaladas	07 de abril – 03 de mayo de 2023
Identificación de Posible Ataque	03 de mayo de 2023, a las 2:54 am
Equipo de Seguridad Comienza el Análisis	03 de mayo de 2023, a las 2:54 am
Comienza el Movimiento Lateral Probable a Través de la Red	03 de mayo de 2023, a las 2:54 am
Procedimientos de Mitigación de Ataques Iniciados	03 de mayo de 2023, a las 5:00 am
Puente de Llamadas Abierto	03 de mayo de 2023 a las 5:23 am
Servidores de Aseo y Recolección de Basura Identificados como afectados	03 de mayo de 2023, a las 5:32 am
Conjunto de Servidores Identificados como Infectados	03 de mayo de 2023, a las 6:00 am
Equipo ampliado para incluir disciplinas de IT adicionales	03 de mayo de 2023, a las 7:00 am

Acción/Actividad de Intrusión o Recuperación	Fecha Aproximada
Se Notifica al Administrador de Recuperación ante Desastres sobre un Incidente en Curso	3 de mayo de 2023 a las 07:46 am
Se envía anuncio al Personal de la Ciudad sobre la Interrupción Generalizada del Servicio	3 de mayo de 2023, a las 8:05 am
Personal Directivo de IT Notificado sobre un Incidente en Curso (CIO, CFO, por sus siglas en inglés)	3 de mayo de 2023 a las 8:22 am
Plan de Respuesta al Incidente (IRP) Iniciado	3 de mayo de 2023, a las 8:30 am
Comunicación a las Autoridades Federales	3 de mayo de 2023, a las 8:30 am
Se notifica a la Oficina del Abogado de la Ciudad (CAO) y a la Oficina de Manejo de Emergencias (OEM) de la Ciudad sobre el incidente en curso	3 de mayo de 2023, a las 8:30 am
Procedimientos de Preservación de Pruebas Iniciados	3 de mayo de 2023 a las 8:31 am
Notificación al Alcalde de la Ciudad y al Concejo sobre el Incidente en Curso	3 de mayo de 2023, a las 9:05 am
Preservación y Restauración de los Servicios CAD de Seguridad Pública Establecidos como Prioridad	3 de mayo de 2023, a las 9:35 am
Seguimiento del Inventario del Servidor Infectado Iniciado	3 de mayo de 2023, a las 9:44 am
Contenido del mensaje README.txt de Royal compartido con el Equipo del Incidente	3 de mayo de 2023, a las 9:45 am
Servidores Críticos de Seguridad Pública Infectados	3 de mayo de 2023, a las 11:10 am
Se Comienza a Desconectar Servidores	3 de mayo de 2023, a las 11:00 am
Se Comienza la Reconstrucción de los Servidores CAD	3 de mayo de 2023, a las 12:00 pm
Medios de Comunicación Anuncian el Ataque al Público	3 de mayo de 2023, a las 12:30 pm
Nuevos Servidores se Infectan	3 de mayo de 2023, a las 1:22 pm
Bases de Datos Infectadas Identificadas	3 de mayo de 2023, a las 1:30 pm
Los Servidores de Impresión están Desconectados	3 de mayo de 2023, a las 2:11 pm
Análisis Inicial Determina que 173 Servidores Están Afectados	3 de mayo de 2023, a las 2:15 pm
Múltiples Dominios Afectados	3 de mayo de 2023, a las 2:15 pm
Evaluación de que Varios Departamentos fueron Impactados	3 de mayo de 2023, a las 2:15 pm
Reinfección del Servidor Confirmada	3 de mayo de 2023, a las 5:00 pm
Bloques Adicionales de CrowdStrike	3 de mayo de 2023, a las 5:30 pm
Confirmación de un Servidor de Servicios de Desarrollo Infectado	3 de mayo de 2023, a las 6:00 pm
Confirmación de Servidores GIS de Bases de Datos Infectados	3 de mayo de 2023, a las 6:09 pm
Ejecución de Programa Malicioso Extinguida por la Ciudad	4 de mayo de 2023, a las 5:58 am
Activación del Equipo de Soporte de Incidentes (IST, por sus siglas en inglés)	8 mayo 2023, a las 9:00 am
Desactivación del Equipo de Soporte de Incidentes (IST)	9 de junio de 2023, a las 5:00 pm

Esfuerzos de Recuperación

El equipo operativo de ITS inició acciones de restauración inmediatamente luego de la aparición reconocida del programa malicioso que afectaba el marco tecnológico, crucial para la vitalidad operativa de la Ciudad y fundamental para los servicios a los residentes. Esto abarcó componentes fundamentales, como los componentes de infraestructura tecnológica y los sistemas considerados de misión crítica, incluyendo el Despacho Asistido por Computadora

(CAD), los Servicios 311, los servicios GIS y los sitios web de comunicación orientados a la Ciudad, que se clasificaron según la secuencia de restablecimiento. Para ayudar en este esfuerzo, se activó el Equipo de Soporte de Incidentes (IST) para proporcionar a los equipos de respuesta información pertinente para la recuperación y restauración de servicios específicos.

El equipo de ITS inició rápidamente una rotación de 24 horas al día, los 7 días de la semana, con esfuerzos para una trayectoria inmediata de recuperación y reconstrucción, limitada dentro de los parámetros de los entornos de infraestructura virtualizados. Sin embargo, estos esfuerzos necesitaron una pausa temporal debido a la neutralización incompleta del ejecutable malicioso a través de EDR y su capacidad de propagarse por todo el ecosistema de la red. ITS instituyó una pausa temporal, redirigiendo sus esfuerzos hacia la erradicación del ejecutable en cuestión. Esto incluyó la implementación de protocolos de seguridad destinados a eliminar las tecnologías de gestión remota y la introducción de políticas de seguridad para evitar la reinfección.

Una vez confirmada la eficacia de estas medidas mediante la evaluación de las tecnologías de seguridad de IT existentes y la visibilidad, los esfuerzos de restauración se reorientaron en restablecer las tecnologías de infraestructura fundamentales y de misión crítica necesarias para el soporte de aplicaciones. Estas tareas de restauración se organizaron en distintos flujos de trabajo, cada uno asignado a equipos especializados dedicados a la iniciativa de recuperación. El enfoque de 24 horas al día, 7 días a la semana permitió una asignación específica de recursos basada en requisitos específicos. Los equipos se estructuraron en segmentos que comprendían recuperación de servidores/sistemas, recuperación de activos, cumplimiento de los estándares DOD 5220.22 M para la purga completa de dispositivos para eliminar el programa malicioso y la posterior reinvención de los sistemas afectados.

Mediante un esfuerzo de colaboración y cooperación en el que participó la Ciudad y proveedores externos, se restauró la funcionalidad fundamental a los sistemas críticos. Estos sistemas incluían el Despacho Asistido por Computadora (CAD) que recuperó la funcionalidad básica a través de un proceso de despacho manual, los sitios web de la Ciudad y el Sistema de Permisos de Servicios de Desarrollo. Esta restauración se logró a finales del 8 de mayo de 2023. Luego de esta fase inicial de recuperación, el 11 de mayo de 2023, el sistema de despacho CAD volvió a la automatización total para las operaciones de despacho. Además, los servicios regulares, como la facturación del agua a los residentes, el procesamiento de solicitudes y órdenes regionales, y la utilización de servicios críticos para el pago de la Ciudad y el procesamiento financiero, reanudaron sus operaciones.

Al final se pudo constatar que el evento provocó el deterioro de 230 servidores, siendo necesario realizar esfuerzos integrales para su completa restauración y recuperación mediante los respaldos disponibles. Entre estos servidores afectados, la Ciudad retiró con éxito más de 100 servidores excedentes que alojaban aplicaciones obsoletas, sistemas operativos sin soporte o que se consideraban no fundamentales para los servicios municipales cruciales. El recuento acumulado de 1,398 dispositivos terminales pasó por reconstrucción directamente debido a los efectos de la infección del programa de cibersecuestro de datos de Royal.

Principales Servicios Afectados y Aplicaciones de Soporte

La siguiente es una tabla de servicios conocidos y aplicaciones de soporte que se vieron afectados por las operaciones de cibersecuestro de datos realizadas por el Grupo de Piratas Informáticos Royal contra la Ciudad de Dallas:

Servicio/Aplicación	Breve Descripción del Servicio	Departamentos de la Ciudad Afectados
GIS	Sistema de Información Geográfica Empresarial	DWU, Policía de Dallas, Bomberos de Dallas, Otros
Centro de Fusión	Solución de fusión de inteligencia de fuentes múltiples de la Policía de Dallas	Policía de Dallas
Despacho Asistido por Computadora (CAD)	Servicios de Emergencia de Servicio de Despacho Asistido por Computadora	Policía de Dallas, Bomberos de Dallas, EMS de Dallas, Alguaciles de Dallas
Servicio de Gestión de Informes/Sistema de Gestión de Cumplimiento del Código	DPD-Web Sistema de Gestión de Informes (RMS, por sus siglas en inglés) y Sistema de Gestión de Cumplimiento del Código (CCMS, por sus siglas en inglés)	Policía de Dallas, Servicios de Cumplimiento del Código
Archivos Compartidos de Seguridad Pública	Almacenes de datos remotos (basados en servidor, basados en la nube) para uso individual y grupal	Policía de Dallas
Sistema de Gestión de Cámaras de Vigilancia	Cámaras en calles utilizadas para la vigilancia policial de un sitio (por ejemplo, Fair Park) o de una ubicación (por ejemplo, el programa Starlight)	Policía de Dallas
Servicios de Gestión de Animales	Monitoreo de animales y soporte animal, solución de gestión de sistemas.	Refugio de Animales de Dallas
Sistema de Permisos de Construcción	Plan de inspección de edificios y solución de gestión de permisos.	Servicios de Desarrollo
Servicio de Transferencia Segura de Archivos	Servidor de protocolo de transferencia de archivos seguro físicamente presente dentro del Centro de Datos de la Ciudad	Servicios de Información y Tecnología (ITS), todos los demás departamentos de la Ciudad
Servicio de Gestión de Biblioteca	Solución de gestión de libros, medios y artefactos de la Biblioteca de Dallas	Biblioteca de Dallas
Servicio de Gestión de Órdenes Judiciales	Solución de gestión de órdenes judiciales ordenada por el tribunal	Policía de Dallas, Alguaciles de Dallas, Tribunales Municipales de Dallas y otras agencias locales que interoperan con los recursos de órdenes de la Ciudad
Servicio de Lectura Remota de Medidores de Agua	Tecnología de lectura remota de medidores de agua que respalda las divisiones de operaciones y	Servicios de Agua de Dallas

Servicio/Aplicación	Breve Descripción del Servicio	Departamentos de la Ciudad Afectados
	facturación de los Servicios de Agua de Dallas	
Solución de Aceptación de Tarjetas de Pago	Servicios de aceptación de tarjetas de pago que respaldan las operaciones de la solución de facturación de los Servicios de Agua de Dallas	Servicios de Agua de Dallas y otros departamentos que utilizan ePay para aceptar pagos
Servicios Informáticos de Datos Móviles de Seguridad Pública	Computadora de datos móviles (MDC) utilizada predominantemente por policías, bomberos, servicios médicos de emergencia (EMS) y servicios de emergencia para comunicaciones digitales remotas entre activos desplegados y servicios de despacho asistidos por computadora de la Ciudad.	Policía de Dallas, Bomberos de Dallas, Servicio de Emergencias Médicas de Dallas, Servicios de Emergencia de Dallas y otros departamentos y agencias de la Ciudad que utilizan computadoras de datos móviles para recopilar y presentar información de servicio
Servicio de Alerta	Soluciones de alerta para estaciones de bomberos diseñadas para reducir los tiempos de respuesta y mejorar la calidad de vida de los socorristas.	Bomberos de Dallas
Servicios de Impresión Segura	Servicios de impresión segura en toda la Ciudad utilizados para monitorear y gestionar la impresión de documentos seguros en estaciones de impresión designadas.	Todos los departamentos
Servicios de Fax	Estas aplicaciones y sistemas transmiten de forma segura faxes digitales sin papel. Esta solución de fax digital reduce en gran medida los costos de envío de fax al conectarse a telefonía analógica o digital en el sitio, voz sobre IP o la nube.	Todos los departamentos

Restauración de Sistemas y Servicios del 9 de mayo de 2023 al 13 de junio de 2023

El siguiente cuadro representa la lista de verificación de restauración de sistemas y servicios que se aprovechó durante los esfuerzos de recuperación. Verde: indica completado, probado y devuelto a producción, Amarillo: indica completado y en prueba, Blanco: indica en etapa de preparación y en construcción actualmente.

Fecha de Restauración	Fase de Restauración	Estado del Color	Aplicación/Servicio
5/5/2023	Fase 1	Verde	Despacho Asistido por Computadora
8/5/2023			Equipo de Soporte de Incidentes Activado
9/5/2023	Fase 1	Verde	Servidor Financiero
9/5/2023	Fase 1	Verde	Sitio Web de la Ciudad
9/5/2023	Fase 1	Verde	Sistema de Servicios de Desarrollo
10/5/2023	Fase 1	Verde	Despacho Automatizado de Policía/Bomberos
11/5/2023	Fase 2	Verde	Sistema de Control de la Ciudad
11/5/2023	Fase 1	Verde	Solución de Aceptación de Tarjetas de Pago
11/5/2023	Fase 2	Verde	Servicio de Gestión de Órdenes Judiciales
11/5/2023	Fase 1	Verde	Servidor de Ciberseguridad
11/5/2023	Fase 1	Verde	Servicio de Lectura Remota De Medidores
12/5/2023	Fase 1	Verde	Sistema de Gestión De Registros
15/5/2023	Fase 2	Verde	Sistema de Delitos de la Policía de Dallas
15/5/2023	Fase 2	Verde	Servicio de Gestión del Código
15/5/2023	Fase 1	Verde	Servicio de Informes de Base de Campo
15/5/2023	Fase 1	Verde	Servicio de Gestión de Solicitudes Ciudadanas
16/5/2023	Fase 3	Verde	Servidor de Delitos de la Policía de Dallas
16/5/2023	Fase 2	Verde	Servicio de Gestión de Animales
16/5/2023	Fase 3	Verde	Servicio de Gestión Financiera
16/5/2023	Fase 2	Verde	Sistema de Bomberos de Dallas
17/5/2023	Fase 4	Verde	Orquestación del Flujo de Trabajo de Datos y Aplicaciones
17/5/2023	Fase 2	Verde	Sistema del Secretario de la Ciudad
17/5/2023	Fase 2	Verde	Sistema de Aseo y Recolección de Basura
19/5/2023	Fase 4	Amarillo	Visor Virtual
22/5/2023	Fase 5	Verde	Sistema de Narcóticos de la Policía de Dallas
22/5/2023	Fase 4	Verde	Sistema de Incidentes de Bomberos de Dallas
22/5/2023	Fase 4	Verde	Sistema del Abogado de la Ciudad
22/5/2023	Fase 5	Verde	Servicio de Gestión de Pruebas
22/5/2023	Fase 5	Verde	Servidores de Seguridad de la Policía de Dallas
22/5/2023	Fase 2	Verde	Servidores de Seguridad de Bomberos de Dallas
22/5/2023	Fase 5	Verde	Sistema de Policía de Dallas
22/5/2023	Fase 4	Verde	Servicio de Visor Virtual
23/5/2023	Fase 4	Verde	Servidor de Impresión
24/5/2023	Fase 2	Verde	Servicio de Informes de Servicios Financieros
24/5/2023	Fase 5	Verde	Programa Informático de Contabilidad Mercantil
25/5/2023	Fase 4	Verde	Servicio de Gestión de Certificados de Eventos de Vida
25/5/2023	Fase 4	Verde	Servidor de Agua de GIS
26/5/2023	Fase 1	Verde	Sistema de Gestión de Tribunales
26/5/2023	Fase 3	Verde	Sistema Vecinal Mejorado de la Policía de Dallas
30/5/2023	Fase 5	Verde	Sistema de Gestión de Pagos

Fecha de Restauración	Fase de Restauración	Estado del Color	Aplicación/Servicio
30/5/2023	Fase 5	Verde	Servidor Especializado de la Policía de Dallas
30/5/2023	Fase 3	Verde	Sistema de Incautaciones de la Policía de Dallas
30/5/2023	Fase 3	Verde	Servicio de Gestión de Flujo de Trabajo Interno
31/5/2023	Fase 5	Verde	Estadísticas Vitales
2/6/2023	Fase 3	Verde	Sistema de Gestión de Expedientes Judiciales
2/6/2023	Fase 5	Verde	Servidor Especializado de Bomberos de Dallas
2/6/2023	Fase 4	Verde	Sistema de Órdenes Judiciales de la Policía de Dallas
6/6/2023	Fase 6	Verde	Sistema de Gestión de Empleados
6/6/2023	Fase 6	Verde	Servicio de Gestión de Encuestas
8/6/2023	Fase 5	Verde	Sistema de Datos de Tránsito de la Policía de Dallas
8/6/2023	Fase 5	Verde	Sistema de Informes de Seguridad de Gestión de Vehículos
13/6/2023	Fase 6	Verde	Servidores de Sitios de Respaldo
13/6/2023	Fase 6	Verde	Servicio de Archivo de Pago de Facturación de Agua de Dallas
13/6/2023	Fase 6	Verde	Servicio de Gestión de Mantenimiento y Reparación de Calles
13/6/2023	Fase 6	Blanco	Servicio de Gestión de Servicios Financieros
13/6/2023	Fase 4	Amarillo	Recursos para Compartir Archivos
13/6/2023	Fase 6	Verde	Servicio de Gestión de Exámenes de GED
13/6/2023	Fase 3	Amarillo	Servidor del Personal de Bomberos de Dallas
13/6/2023	Fase 3	Blanco	Sistema de la Biblioteca
13/6/2023	Fase 2	Amarillo	Servicio de Reserva de Recursos Bibliotecarios
13/6/2023	Fase 4	Amarillo	Servidor de Servicios de Construcción
13/6/2023	Fase 6	Amarillo	Servicio de Reserva de Recursos Bibliotecarios
13/6/2023	Fase 2	Amarillo	Servicio de Gestión de Recursos Bibliotecarios
13/6/2023	Fase 5	Amarillo	Sistema de Entrada de Casos de Bomberos de Dallas
13/6/2023	Fase 5	Blanco	Servidor de Sitios de Respaldo de Seguridad Pública
13/6/2023	Fase 6	Amarillo	Servidor de Puerta de Seguridad
13/6/2023	Fase 4	Amarillo	Servicio de Gestión de Aguas Pluviales
13/6/2023	Fase 6	Amarillo	Sistema de Servicios de Desarrollo
13/6/2023	Fase 6	Verde	Servidor de Gestión de Residuos

Sección II –Factores de Riesgo Operativo que Propiciaron el Incidente

Esta sección del documento detalla los factores de riesgo internos y externos que propiciaron el Incidente de Cibersecuestro de Datos de Royal en la Ciudad de Dallas. El Incidente de Cibersecuestro de Datos de Royal en la Ciudad comenzó a primera hora de la mañana del miércoles, 03 de mayo de 2023.

Ciudad Bajo Constante Ataque Cibernético

La Ciudad de Dallas rechaza mensualmente millones de solicitudes entrantes de conexión a la red de internet dudosas. Estas solicitudes se deben a diversas razones; muchas de ellas tienen motivos legítimos y la mayoría generalmente se consideran de naturaleza maliciosa. La Ciudad es un municipio grande y los ciberdelincuentes pueden considerarla un posible objetivo porque la mayoría de los municipios no protegen adecuadamente sus recursos de red. Además, la Ciudad gestiona, opera y mantiene varios objetivos de infraestructura crítica que resultan atractivos para los ciberdelincuentes (por ejemplo, agua potable, gestión de aguas pluviales, gestión de aguas de inundación, aeropuertos, sistemas de gestión de la aviación, redes de comunicaciones de primeros auxilios, operaciones de gestión de emergencias, sistemas de gestión de calles [por ejemplo, iluminación, semáforos]).

La Ciudad de Dallas intenta gestionar el acceso a los recursos de su red (por ejemplo, servidores, enrutadores, equilibradores de carga) utilizando la tecnología de cortafuego de última generación. Los aparatos y dispositivos de cortafuego físicos se implementan, administran y operan en la Alcaldía de Dallas. La Ciudad utiliza cortafuegos centrales para el funcionamiento de la red empresarial y con fines de seguridad. Los cortafuegos perimetrales se gestionan y operan para respaldar el acceso público a internet. A pesar del uso de tecnología de última generación, la Ciudad está sujeta a intentos de intrusión las 24 horas del día, los 7 días de la semana, lo que requiere que la Ciudad utilice varias tecnologías de seguridad basadas tanto en *hardware* como en programas informáticos para garantizar que solo el tránsito autorizado pueda acceder e ingresar a la red de la Ciudad.

La Ciudad es un Conglomerado de Misiones

La Ciudad de Dallas está compuesta por más de 40 departamentos diferentes, múltiples oficinas y varias juntas que apoyan las diferentes misiones que se le asignan. Cada departamento, oficina y junta gestiona eficazmente sus propias actividades en apoyo de las misiones asignadas. Esta diversidad de enfoques proporciona diversidad de enfoques, pero también introduce una cierta falta de cohesión organizacional.

Un organigrama de la Ciudad reciente identificó ocho carteras de alto nivel gestionadas individualmente por administradores adjuntos y administradores asistentes de la Ciudad. Estas carteras incluían Vivienda y Soluciones para Personas Sin Hogar; Seguridad Pública; Desarrollo Económico; Fuerza de Trabajo, Educación y Equidad; Transporte e Infraestructura; Calidad de Vida, Arte y Cultura; Medio Ambiente y Sustentabilidad; y Desempeño Gubernamental y Gestión Financiera. Las misiones y los objetivos de misión de cada una de estas carteras son tan diversos como los siguientes.

Como se indicó previamente, esto crea una superficie de ataque considerable para los datos que utilizan los departamentos de la Ciudad. Los departamentos y los residentes dependen del uso diario de la infraestructura crítica, las tarjetas de pago, la atención médica y la información personal de los residentes para mantener la continuidad.

Deuda Técnica

La necesidad de mantener la deuda técnica de los sistemas actuales representa los compromisos y soluciones subóptimas que pueden surgir durante el desarrollo y mantenimiento de los sistemas de programas informáticos, es normal e inevitable. [Gartner] ITS ha reconocido la presencia de deuda técnica en su Informe de Responsabilidad Tecnológica (TAR, por sus siglas en inglés) e inició el proceso de modernización. Existe un requisito claro para que la Ciudad persista en estos esfuerzos. Estos compromisos pueden plantear desafíos para proteger el ambiente. Si bien pueden proporcionar beneficios a corto plazo, pueden generar riesgos. En términos de ciberseguridad, la deuda técnica puede contribuir posiblemente al éxito de los eventos cibernéticos en virtud de medidas de seguridad integradas inadecuadas en los sistemas más nuevos y vulnerabilidades no remediadas.

Vulnerabilidades

En consecuencia, para todas las organizaciones, las vulnerabilidades y la gestión remota de la tecnología son clave para reducir el riesgo en la Ciudad. Pueden surgir vulnerabilidades durante los procesos de desarrollo, lo que los convierte en objetivos universales para los piratas informáticos que buscan continuamente dichas debilidades para explotarlas para sus propios fines. La gestión eficaz de parches, que implica la aplicación rutinaria de actualizaciones de programas informáticos y sistemas para abordar vulnerabilidades conocidas y mejorar la seguridad de los programas informáticos, es esencial para protegerse contra ataques de cibersecuestro de datos. Los protocolos son susceptibles debido a sus arquitecturas y estándares de seguridad menos modernos, que a menudo carecen de cifrado, mecanismos de autenticación y defensas modernos contra las amenazas cibernéticas en evolución. Estos protocolos frecuentemente persisten con vulnerabilidades no resueltas, dejándolos expuestos a la explotación por parte de actores maliciosos. [CISA]

Todas las organizaciones deben reducir el riesgo de puntos de entrada para que los atacantes se infiltren en los sistemas y propaguen programas de cibersecuestro de datos a través de las redes. La ausencia de características de seguridad contemporáneas, junto con la capacidad de los atacantes para explotar estas vulnerabilidades mediante técnicas especializadas, aumenta el riesgo de que se produzcan intrusiones cibernéticas exitosas. [FBI] Luego de que los actores maliciosos logran ejecutar con éxito el código en un dispositivo u obtienen acceso a la red, pueden implementar programas de cibersecuestro de datos. Vale la pena señalar que es probable que estos métodos de infección hayan mantenido su popularidad debido al aumento del trabajo y la educación remotos desde 2020. [CISA]

Sección III – Factores que Mitigaron Directamente el Impacto del Incidente

Esta sección del documento detalla los factores internos y externos que se cree que mitigaron directamente el Incidente de Cibersecuestro de Datos de Royal en la Ciudad de Dallas. Se ha identificado que el Incidente de Cibersecuestro de Datos de Royal en la Ciudad comenzó a primera hora en la mañana del miércoles, 3 de mayo de 2023.

Introducción

Esta sección del Informe Posterior a la Acción (AAR, por sus siglas en inglés) presenta y describe aquellos factores que tuvieron un impacto directo en la mitigación del Incidente de Cibersecuestro de Datos.

Aunque la interdicción, mitigación y restauración de servicios fue un esfuerzo de "¡Todos!" 24 horas al día, 7 días a la semana, hubo casos en los que las acciones, actividades e iniciativa de unos pocos impidieron que Royal dañara dramáticamente la infraestructura informática y de comunicaciones de Producción de la Ciudad.

La Ciudad ha desarrollado y mantiene un plan estratégico dinámico de ciberseguridad de cinco años. Las estrategias identificadas en el plan se basan en un conjunto de principios rectores, objetivos y prioridades para la ciberseguridad que deberían beneficiar a la Ciudad de Dallas durante el próximo período de tres a cinco años. Estos principios, objetivos y prioridades se seleccionan a partir de investigaciones y orientación de autoridades gubernamentales como MITRE y el Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés). Se cree que el uso de esta base brindará a la Ciudad la capacidad de seleccionar, implementar, gestionar y operar de manera adecuada tecnologías de ciberseguridad para abordar, gestionar y mitigar de manera efectiva las vulnerabilidades y amenazas de IT de la Ciudad.

El tamaño y el alcance del programa de ciberseguridad se han incrementado para lograr los objetivos estratégicos de la Ciudad, incluyendo esfuerzos como mejorar la seguridad pública, infraestructura crítica y ciudades más inteligentes. Además de los importantes proyectos y sistemas de seguridad que se arrastrarán de las mejoras del año pasado, en los próximos tres a cinco años se emprenderán nuevas iniciativas para hacer frente a las amenazas emergentes. Se trata de ampliar el enfoque de las actividades de identificación, protección, detección, respuesta y recuperación de la Ciudad de Dallas.

Un entorno de amenazas puede gestionarse y mitigarse mediante la identificación, el desarrollo y el uso de iniciativas de ciberseguridad adecuadas. El plan estratégico de ciberseguridad de la Ciudad identifica varios conjuntos de objetivos y aborda el entorno de amenazas de la Ciudad mediante el uso de iniciativas de ciberseguridad apropiadas respaldadas por inversiones relevantes en tecnología de ciberseguridad seleccionadas para proteger los recursos y activos de información de la Ciudad.

La hoja de ruta del programa, los objetivos y los resultados previstos han sido identificados y evaluados por grupos funcionales maduros del NIST. Este marco facilita la supervisión y

evaluación de los esfuerzos de la Ciudad para implementar controles de seguridad cibernética y reducir el riesgo.

Desde 2019, la Ciudad de Dallas ha evaluado la madurez de su programa de Ciberseguridad. La evaluación utiliza el Marco Común de Seguridad (CSF, por sus siglas en inglés) del NIST junto con la aplicación del marco de Integración del Modelo de Madurez de Capacidades (CMMI, por sus siglas en inglés). Esta evaluación periódica proporciona al programa de ciberseguridad de la Ciudad una perspectiva directa de las áreas fundamentales del funcionamiento del programa y da una idea de las cinco áreas funcionales de la ciberseguridad (Identificar, Proteger, Detectar, Responder, Recuperar) a través de la inspección del rendimiento de la ciberseguridad de la Ciudad con 22 categorías y 98 subcategorías de gestión y control.

El programa de ciberseguridad de la Ciudad se evalúa desde perspectivas de política, práctica y/o tecnología. Estas diversas perspectivas ayudan al personal directivo de la Ciudad a determinar dónde se deben realizar inversiones para mejorar continuamente la capacidad de la Ciudad para responder y recuperarse de cualquier evento de ciberseguridad.

Mayor Inversión de la Ciudad en InfoSec

La Ciudad de Dallas ha aumentado continuamente su compromiso con las herramientas y soluciones de Seguridad de la Información (InfoSec) desde el año 2019. Estas inversiones han reforzado y ampliado la estrategia estratificada empleada para la ciberseguridad y la seguridad de la información. En 2019, el gasto en seguridad informática representó aproximadamente el 2.5% del presupuesto total de IT. En cambio, tal y como indica el presupuesto previsto para el periodo fiscal 2023-24, una recomendación del administrador de la Ciudad, unida al respaldo del Concejo de la Ciudad, está llamada a elevar esta asignación hasta casi el 10%. Este aumento sustancial ha permitido a la Ciudad reducir la exposición al riesgo y mejorar la resistencia de su infraestructura tecnológica.

A pesar del notable aumento del gasto global, la maduración del programa operativo de IT requería una estrategia global y una metodología de aplicación capaz de albergar las complejidades inherentes a cada demanda suplementaria de tecnología de seguridad de IT. El peso de la deuda tecnológica y la complejidad injustificada inherente a las redes heredadas introducen dificultades al momento de fortificar adecuadamente la red. Reconocer los imperativos del panorama de amenazas hace evidente que las entidades deben potenciar todas las facetas de un marco mediante una planificación meticulosa, salvaguardando así la infraestructura y preparándose simultáneamente para la ejecución expeditiva de medidas de respuesta y recuperación.

Evaluaciones Periódicas de Seguridad de Agencias Federales

Cada cierto tiempo, la Ciudad de Dallas establece acuerdos con el Departamento de Seguridad Nacional de Estados Unidos (DHS) para evaluar el estado de seguridad de los recursos de información municipales, incluyendo, pero no limitándose a, su red y sus servicios informáticos. Recientemente, en febrero de 2023, la Ciudad finalizó una colaboración de quince días con la Agencia de Ciberseguridad y Seguridad de Infraestructuras (CISA) para llevar a cabo una Prueba

de Penetración de Seguridad, comúnmente denominada "ejercicio de Equipo Rojo". Esta evaluación examinó exhaustivamente la infraestructura de la Ciudad desde perspectivas tanto externas como internas. Estas iniciativas de colaboración han aportado información sustancial sobre la situación de la ciberseguridad, indicando las áreas que necesitan mejoras y soluciones.

Tecnologías de Confianza Cero

La estrategia estratificada de la Ciudad para la ciberseguridad y la seguridad de la información se ve reforzada sinérgicamente por un Programa de Seguridad que implica activamente al personal de la Ciudad, facilitando prácticas de trabajo autónomas seguras. En el transcurso de los cinco años previos, la Ciudad ha implantado las subsiguientes tecnologías de gobernanza de la seguridad, ciberseguridad y seguridad de la información en armonía con numerosas directivas de ciberseguridad a nivel federal. A la vez, IT ha introducido y gestiona tecnologías de red de confianza cero para mejorar el acceso a los recursos y la gestión dentro de la red. Una parte sustancial de estas tecnologías aprovecha los sistemas basados en Inteligencia Artificial para ayudar a detectar y mitigar las amenazas concebibles.

1. Copias de seguridad del sistema: luego de los eventos de 2021, estructura de protección de datos integral y coordinada con precisión, que integra perfectamente copias de seguridad periódicas automatizadas, almacenamiento cifrado distribuido en ubicaciones redundantes, funcionalidades de control de versiones, mecanismos de almacenamiento fuera de línea, protocolos de recuperación oportunos, procedimientos de prueba regulares, retención sostenida de datos históricos, documentación clara y alineación estratégica con los requisitos de continuidad del negocio. Esta metodología integral garantiza la conservación, integridad y rápida restauración de información vital y recuperación del sistema.

2. Plataformas de Gestión de Acceso e Identidad: la Ciudad ha implementado y opera una plataforma de gestión de acceso e identidad basada en la nube. Dichas plataformas permiten a la Ciudad centralizar, gestionar y asegurar la autenticación de usuarios en aplicaciones/soluciones de la Ciudad para más de 200 aplicaciones. La plataforma proporciona autenticación de varios factores para ayudar a que solo el personal autorizado acceda y utilice las aplicaciones/sistemas de la Ciudad.

3. Detección de Amenazas en Tiempo Real: la Ciudad ha implementado y opera soluciones de detección de amenazas en tiempo real. Gracias a las tecnologías de detección y respuesta de redes, la Ciudad puede identificar y responder a los incidentes de seguridad en el momento en que se producen. Estas tecnologías utilizan “algoritmos de aprendizaje automático” (ML, por sus siglas en inglés) a escala de la nube y técnicas basadas en normas para detectar comportamientos, anomalías y vulnerabilidades de programas informáticos con el fin de ofrecer recomendaciones de seguridad al personal de la Ciudad.

4. Análisis del Comportamiento de la Red: la Ciudad ha implementado y opera tecnologías basadas en tecnologías de aprendizaje automático que le permiten a la Ciudad identificar si hay un flujo de tráfico malintencionado dentro de las redes de la Ciudad. Si se identifica

tal comportamiento, las tecnologías pueden ralentizar o eliminar rápidamente dicho tráfico de las redes de la Ciudad.

5. Gestión de Eventos e Información de Seguridad (SIEM, por sus siglas en inglés): la Ciudad ha implementado y opera tecnologías de gestión de eventos e información de seguridad que le permiten a la Ciudad tener visibilidad en tiempo real de los eventos de la red y del servidor. La Ciudad también ha contratado a un proveedor de servicios de seguridad gestionados (MSSP, por sus siglas en inglés) para que le ayude en el seguimiento y la gestión de los grandes volúmenes de datos recopilados por sus soluciones de gestión de eventos e información de seguridad.

6. Evaluaciones de Riesgo FAIR: el Análisis Factorial de Riesgo de la Información (FAIR, por sus siglas en inglés) es una taxonomía de los factores que contribuyen al riesgo y cómo se afectan entre sí. FAIR se ocupa principalmente de determinar probabilidades precisas para dos componentes de riesgo de eventos de pérdida de datos: frecuencia y magnitud. FAIR complementa otras metodologías de riesgo al proporcionar una manera de producir declaraciones de creencias consistentes y defendibles sobre el riesgo.

7. Evaluación de Riesgos HIPAA: las evaluaciones de riesgos HIPAA son un método para identificar áreas donde la información de salud protegida (PHI) de una organización podría estar en riesgo. Los factores considerados en una evaluación de riesgo de filtración de HIPAA incluyen la naturaleza y el alcance de la PHI vulnerada, los tipos de identificadores y la probabilidad de reidentificación, la persona no autorizada que accedió o utilizó la PHI vulnerada, si la PHI fue realmente adquirida o vista, y hasta qué punto está presente el riesgo para la PHI.

8. Evaluaciones de Confidencialidad de Datos NIST 800-171: el estándar NIST 800-171 establece el nivel básico de seguridad requerido para los sistemas informáticos que utilizan o almacenan información confidencial no clasificada (CUI, por sus siglas en inglés). Todas las organizaciones que acceden a la información del gobierno de EE. UU. deben cumplir con los estándares NIST. Como esto es un hecho, una evaluación de riesgos 800-171 puede identificar si una organización protege adecuadamente la información de manera compatible con la versión actual de NIST 800-171.

9. Planificación de Recuperación: La Planificación de la Recuperación se alinea con las principales metas de ciberseguridad de la Ciudad, para identificar y ser proactivos hacia potenciales esfuerzos de recuperación. La Ciudad tiene previsto mejorar la madurez de sus procesos y procedimientos de gestión de riesgos. Estos procesos y procedimientos incluirán la identificación de cualquier posible deficiencia en la planificación de la recuperación. Los esfuerzos continuos para incluir muchos ejercicios de simulación y pruebas técnicas de los esfuerzos de recuperación planificados contribuirán a una recuperación más resiliente cuando sea necesario.

10. Gestión de Riesgos de la Privacidad: La Gestión de Riesgo de la Privacidad describe un método para gestionar los riesgos que el tratamiento de datos personales puede generar para las personas. En la gestión del riesgo para la privacidad de los datos, el activo afectado serían los datos personales y su nivel de clasificación. La evaluación del riesgo

de la privacidad es un proceso para identificar y evaluar los riesgos para la privacidad, que las organizaciones pueden utilizar para fomentar la confianza de los clientes mediante el desarrollo de soluciones más eficaces para proteger la privacidad de las personas al momento de diseñar o implantar sistemas, productos y servicios que procesen datos. Este proceso ayuda a la Ciudad a equiparar la privacidad con su cartera más amplia de riesgos empresariales.

11. Gobernanza, Riesgo y Cumplimiento (GRC, por sus siglas en inglés): Gobernanza, Riesgo y Cumplimiento (GRC) es una forma estructurada de alinear la IT con las metas comerciales mientras se gestionan los riesgos y se cumplen todas las regulaciones gubernamentales y de la industria. Incluye herramientas y procesos para unificar la gobernanza y la gestión de riesgos de una organización con su innovación y adopción tecnológica. Las empresas utilizan GRC para alcanzar las metas organizacionales de manera fiable, eliminar la incertidumbre y cumplir con los requisitos de cumplimiento.

12. Centro de Operaciones de Seguridad (SOC, por sus siglas en inglés): el Centro de Operaciones de Seguridad de la Ciudad es donde se aplican y utilizan tecnologías de seguridad para identificar desafíos de remediación para la seguridad de los recursos de información de la Ciudad. El SOC de la Ciudad brinda visibilidad sobre los distintos desafíos de seguridad y coordina los esfuerzos de remediación para reducir o eliminar esos desafíos de seguridad.

13. Análisis de impacto empresarial (BIA, por sus siglas en inglés): un análisis de impacto empresarial (BIA) intenta predecir las consecuencias de las interrupciones en los procesos de funciones empresariales debido a la pérdida de tecnología de la información. El BIA intenta recopilar la información necesaria para desarrollar estrategias de recuperación. Al desarrollar un BIA, se debe identificar el escenario de posible pérdida utilizando una metodología de evaluación de riesgos.

14. Ejercicios Teóricos Periódicos de Recuperación ante Desastres: los ejercicios teóricos son sesiones grupales basadas en debates en las que los miembros del equipo se reúnen para discutir las funciones y responsabilidades asignadas en caso de que se declare un desastre organizacional. Un facilitador guía a los participantes a través de discusiones sobre uno o más escenarios potenciales para que los participantes puedan visualizar cómo responderían al escenario. Se lleva a cabo una discusión adicional luego de que se haya resuelto el escenario para identificar las lecciones aprendidas y discutir las posibilidades de mejores respuestas al escenario. Estos ejercicios se realizan periódicamente.

15. Base de Datos de Gestión de Configuración (CMDB, por sus siglas en inglés): la Ciudad se encuentra en medio de la evaluación e implementación para rastrear e identificar mejor los activos y sus configuraciones actuales. Esta implementación opera una base de datos de gestión de configuración (CMDB) basada en la nube que se utiliza para almacenar información de implementación y uso sobre activos de programas informáticos y *hardware*. Incluyendo ambas, una solución de gestión de activos de programas informáticos que permite a la Ciudad identificar, definir, rastrear y gestionar más de 860

activos de programas informáticos y soluciones de gestión de activos de *hardware* de la Ciudad.

16. Soluciones de Gestión de Vulnerabilidades: la Ciudad ha implementado y opera varias tecnologías y soluciones de gestión de vulnerabilidades para identificar y remediar vulnerabilidades conocidas y potenciales asociadas con los recursos de *hardware* y programas informáticos de la Ciudad. La gestión de vulnerabilidades permite a la Ciudad identificar, definir, priorizar y remediar de acuerdo con la percepción de la Ciudad de posibles amenazas a su grupo de vulnerabilidades.

17. Microsegmentación: la Ciudad ha implementado una tecnología de gestión de red que le permite gestionar segmentos relativamente pequeños de su red por separado de otros segmentos de su red. Esta tecnología permite a la Ciudad atribuir características especiales de la red a porciones únicas de su red en relación con otros segmentos pequeños y con la red general en su conjunto.

18. Comunicaciones de Crisis: la Ciudad ha comenzado a implementar tecnologías de comunicación de crisis de ITS para permitir que ITS informe y se comunique mejor dentro del departamento y el personal de la ciudad. Estas tecnologías se aprovecharán tanto para la respuesta interna como para la recuperación.

La Ciudad de Dallas planea adquirir, implementar, gestionar y operar las siguientes tecnologías de ciberseguridad durante el próximo período de cinco años:

1. Orquestación, Automatización y Respuesta de Seguridad (SOAR, por sus siglas en inglés): la orquestación, automatización y respuesta de seguridad es un grupo de tecnologías de ciberseguridad que permiten a las organizaciones responder a algunos incidentes automáticamente. Recopila información supervisada por un equipo de operaciones de seguridad y ayuda a definir, priorizar e impulsar actividades estandarizadas de respuesta a incidentes.

2. Gestión del Rendimiento de las Aplicaciones: la Ciudad ha implementado y opera tecnologías de gestión del rendimiento de las aplicaciones que le permiten monitorear y gestionar la disponibilidad de las aplicaciones de programas informáticos. La meta de dicha tecnología es garantizar que se proporcionen a la Ciudad niveles apropiados de servicios de aplicaciones.

3. Gestión del Rendimiento de la Red: la ciudad ha implementado y opera tecnologías de gestión del rendimiento de la red que le permiten monitorear y gestionar la capacidad de servicio de sus diversas redes. Las tecnologías permiten a la Ciudad determinar de antemano si algún desafío en la capacidad del servicio puede presentarse al personal de la Ciudad durante el desempeño de sus funciones.

4. Ciberseguridad de los Sistemas de Control Industrial: la Ciudad ha implementado y opera sistemas de detección y protección de intrusiones en apoyo de los sistemas de control industrial de la ciudad (ICS, por sus siglas en inglés). Estos sistemas garantizan el

funcionamiento seguro de los componentes de la red de control industrial y los puntos de control emergentes de Internet de las Cosas (IoT, por sus siglas en inglés). Esta tecnología se puede utilizar para proteger la infraestructura crítica operada por la Ciudad, como los activos ambientales de la aviación, la tecnología de gestión de calles (por ejemplo, alumbrado público inteligente, sistemas de semáforos).

El actual programa de seguridad de IT de la Ciudad tuvo una función fundamental en la mitigación efectiva de la amenaza de ataques de cibersecuestro de datos mediante el empleo de un enfoque multifacético y proactivo. En primer lugar, el programa enfatiza medidas sólidas de ciberseguridad en varias capas de la infraestructura de la organización. Implica la implementación de sistemas avanzados de detección de intrusos, cortafuegos y segmentación de redes para aislar los sistemas críticos de posibles amenazas.

En segundo lugar, un enfoque en la educación y concientización integral de los usuarios. Al capacitar sistemáticamente a los empleados y a los equipos de IT sobre los riesgos asociados al cibersecuestro de datos, el programa les capacita para reconocer y responder al suceso con rapidez y con el propósito de remediarlo. Esta mayor concienciación mejora la capacidad de la Ciudad para evitar que el cibersecuestro de datos se convierta en una amenaza paralizante durante mucho tiempo. Además, se educa a los empleados sobre la importancia de las copias de seguridad periódicas y las prácticas seguras de almacenamiento de datos, lo que garantiza que la información crítica pueda restaurarse en caso de ataque, reduciendo así la probabilidad de sucumbir a la extorsión relacionada al cibersecuestro de datos.

En esencia, un programa de seguridad informática diligente que combine salvaguardas tecnológicas avanzadas limita el impacto del cibersecuestro de datos y ayuda a acelerar la recuperación. Este enfoque no sólo previene la infección inicial, sino que también facilita una rápida detección y respuesta, minimizando el posible impacto y la interrupción causada por los ataques de cibersecuestro de datos.

Sección IV – Resultados

Esta sección del documento describe los resultados derivados del Incidente de Cibersecuestro de Datos Royal en la Ciudad de Dallas. Se ha identificado que el Incidente de Cibersecuestro de Datos Royal comenzó a primera hora en la mañana del miércoles, 3 de mayo de 2023.

Los siguientes hallazgos fueron el resultado del enfrentamiento de la Ciudad con el Grupo de Piratas Informáticos Royal a partir de la mañana del miércoles, 3 de mayo de 2023.

Planes de Respuesta Competentes a Incidentes

La Ciudad de Dallas ha gestionado y mantenido Planes de Respuesta a Incidentes de Seguridad durante bastante tiempo. Desde 2019, el Departamento de Servicios de Información y Tecnología (ITS) y su predecesor, el Departamento de Comunicaciones y Servicios de Información (CIS, por sus siglas en inglés) han contratado a expertos en ciberseguridad y agencias federales para ayudar a desarrollar, gestionar y mantener Planes de Respuesta a Incidentes (IRP) actuales y relevantes. Los planes consideraron incidentes de seguridad de una variedad de fuentes y perspectivas e identificaron enfoques para remediar y resolver incidentes de seguridad de una manera consistente con las metas y objetivos de la Ciudad para la gestión de recursos de información.

Personal de Incidentes de Seguridad Realiza Ejercicios Periódicamente

La Ciudad de Dallas comprende que los planes sin preparación generalmente son improductivos. Para preparar adecuadamente al personal de respuesta a incidentes para una variedad de posibles incidentes de seguridad, la Ciudad realiza periódicamente ejercicios teóricos, pruebas funcionales y actualizaciones continuas al Plan de Respuesta a Incidentes. Estos ejercicios se realizan para exponer al personal de la Ciudad a diversos vectores de ataque y posibles técnicas de interdicción de ataques antes de que sean necesarios para defender los activos y recursos de información de la Ciudad. Se cree que los ejercicios teóricos periódicos facilitaron la atención inmediata al ataque de cibersecuestro de datos de Royal y ayudaron al personal a coordinar durante la amenaza real a la Ciudad.

Identificación

Para 2023, el tiempo medio general típico para identificar una fuga de datos es de 204 días [IBM]. Esto ha sido constante en los últimos años. Los ciberdelincuentes se han vuelto cada vez más sofisticados en sus métodos para infiltrarse en los sistemas y robar información confidencial. Esta sofisticación puede contribuir al prolongado periodo que se tarda en detectar estas filtraciones, ya que los atacantes explotan las vulnerabilidades y utilizan técnicas avanzadas para evitar ser detectados. El compromiso de la Ciudad con un programa de ciberseguridad puede atribuirse directamente al tiempo medio de 27 días para la identificación, lo que equivale a un enfoque mucho más "relámpago".

Respuesta Dinámica al Incidente

La respuesta de la Ciudad al Incidente de Cibersecuestro de Datos de Royal del 3 de mayo de 2023 se consideró, tanto interna como externamente, como bastante agresiva. Aunque hubo un retraso inicial para identificar y comprender que se estaba produciendo un ataque contra la Ciudad, el personal directivo de la Ciudad pudo destinar una gran cantidad de recursos hacia el desafío en un período de tiempo muy corto. Como indica la tabla de fechas que se muestra en la Sección II, las organizaciones generalmente requieren un promedio de 73 días para contener las filtraciones de datos en 2023, mientras que solo requerían 70 días en promedio en 2022 [IBM]. La Ciudad logró contener el problema en 1 día.

Se tomaron medidas vigorosas para garantizar un compromiso ininterrumpido las 24 horas del día para restaurar los servicios de misión crítica para la infraestructura crítica, las comunicaciones públicas y los servicios fundamentales de la Ciudad. La prontitud del restablecimiento del servicio fue de suma importancia. Tanto los proveedores de tecnología como los expertos en ciberseguridad contratados por la Ciudad expresaron su elogio por los esfuerzos de la Ciudad para prevenir y eliminar el acceso no autorizado por parte de Royal a los activos de información de la Ciudad. Además, los protocolos de la Ciudad para el restablecimiento del servicio también obtuvieron reconocimiento.

Rápida Aplicación y Restauración del Servicio: el esfuerzo de recuperación logró con éxito una tasa de restauración superior al 90 por ciento en un período de 18 días. Gracias a sus esfuerzos concertados, planificación metódica y pronta ejecución, se rehabilitaron con éxito sistemas fundamentales, permitiendo así el restablecimiento significativo de servicios críticos. Es importante señalar que este rápido avance se logró a pesar de la necesidad de reconstruir más de 230 servidores y 1,168 estaciones de trabajo. Este rápido progreso es una prueba indiscutible de la tenacidad y el ingenio de los equipos de recuperación, lo que subraya su firme dedicación para superar rápidamente los desafíos y restablecer un estado de normalidad.

Inversiones Sustanciales en Ciberseguridad Realizadas Antes del Incidente

La Ciudad de Dallas comprendió que los panoramas de la información y la ciberseguridad estaban cambiando rápidamente y comenzó a adoptar e implementar tecnología de seguridad basada en riesgos en 2019. Estas inversiones se correlacionaron con el Marco de Ciberseguridad (CSF, por sus siglas en inglés) del NIST publicado por primera vez en 2014 y actualizado en 2018. Estas inversiones están relacionadas con las cinco áreas funcionales del MCA: Identificar, Proteger, Detectar, Responder y Recuperar.

Se realizaron inversiones relevantes en áreas tecnológicas como Gestión de Identidad y Acceso (IAM, por sus siglas en inglés), Detección y Respuesta de Punto Final, Detección y Respuesta Gestionadas (EDR/MDR, por sus siglas en inglés), Detección y Respuesta a Amenazas Enfocadas en la Red (NDR, por sus siglas en inglés). La dedicación financiera de la Ciudad al crecimiento de la ciberseguridad de $3.4 millones en 2019 a $7.8 millones en 2023 con $8.5 millones adicionales para el evento, es una contribución directa a la protección de los datos de los residentes y los activos. Además, el personal de la Ciudad dedicado a la ciberseguridad ha aumentado de 18 recursos de tiempo completo en 2020 a 35 recursos para gestionar la seguridad, el cumplimiento y el riesgo.

Sección V –Recomendaciones

Esta sección del documento describe recomendaciones para los equipos de operación y gestión de la Ciudad en el contexto del Incidente de Cibersecuestro de Datos de Royal en la Ciudad de Dallas. Se ha identificado que el Incidente de Cibersecuestro de Datos de Royal en la Ciudad comenzó a primera hora en la mañana del miércoles, 3 de mayo de 2023.

Realizar una Revisión del Programa de Ciberseguridad

La Ciudad de Dallas cuenta con un Programa de Ciberseguridad activo. Este programa incluye varias iniciativas de seguridad e involucra a personal de la Ciudad de varios departamentos y niveles de personal. Los consultores recomendaron que la revisión del programa se enfocara en la identificación de las carencias actuales del programa. La revisión recomendada debería incluir un análisis en profundidad de las personas, los procesos y las tecnologías para comprender los fallos en las capacidades frente a las técnicas del mundo real utilizadas por los atacantes. La recomendación de que los resultados de la revisión se utilicen para desarrollar e implantar un programa de ciberseguridad enfocado en las amenazas y basado en los riesgos.

Evaluación de Riesgos de Privacidad/Seguridad (A Largo Plazo)

Los equipos de privacidad y gestión de riesgos de ITS deberán realizar evaluaciones de riesgos de seguridad y privacidad departamentales. Esta evaluación es imperativa para identificar, evaluar y mitigar sistemáticamente los posibles riesgos asociados con la recopilación, el procesamiento y el almacenamiento de información personal y confidencial. Evaluando las prácticas de gestión de datos del departamento, las salvaguardias técnicas y el cumplimiento de las regulaciones pertinentes. La evaluación proporciona una base sólida para implementar medidas de seguridad personalizadas. Los resultados de esta evaluación permitirán a la organización abordar de manera proactiva las vulnerabilidades, educar a los empleados de la Ciudad, protegerse contra fuga de datos y garantizar el cumplimiento de las obligaciones legales y normativas. Además, los conocimientos de la Evaluación facilitarán la toma de decisiones informadas, asignarán recursos con prudencia y establecerán una posición defendible contra posibles responsabilidades legales derivadas de infracciones de seguridad y privacidad de datos.

Mejorar los Procesos de Copia de Seguridad y Restauración de Datos

No siempre se hace hincapié en los procesos de copia de seguridad y restauración de aplicaciones y servicios como componente del despliegue de recursos de información en los entornos de producción de la Ciudad. Esta falta de énfasis hace que las aplicaciones y los servicios se introduzcan en los entornos de producción de la Ciudad sin procesos y procedimientos de copia de seguridad, recuperación o restauración debidamente adaptados; en su lugar, se confía en enfoques genéricos para estas actividades de aplicaciones y servicios. Se recomienda exigir que todas las aplicaciones y servicios cuenten con procesos y procedimientos de copia de seguridad, recuperación o restauración debidamente adaptados y definidos antes de que una aplicación o servicio pueda introducirse en un entorno de producción de la Ciudad.

Reforzar la Red y los Activos Informáticos

Los recursos de activos de tecnología de la información (por ejemplo, servidores) no se gestionan ni operan de manera consistente en un estado reforzado. El reforzamiento de recursos es un conjunto de procesos o procedimientos que intenta proteger los recursos de IT contra ciberataques reduciendo su superficie de ataque.

Reducir, Eliminar y Gestionar la Deuda Técnica

Muchas aplicaciones y servicios de la Ciudad no funcionan con las versiones más actuales de los programas informáticos subyacentes. Varias aplicaciones y servicios importantes funcionan en versiones de programas informáticos que ya no cuentan con el respaldo de los fabricantes y proveedores. Esta condición provoca un desajuste entre la capacidad de la Ciudad para brindar servicios técnicos en apoyo de las misiones comerciales de la Ciudad y de los departamentos individuales y las mejores prácticas de ciberseguridad para desalentar o derrotar posibles intrusiones de actores amenazantes. Se recomienda que los líderes de la Ciudad participen en la priorización continua de los servicios técnicos para que la deuda técnica se elimine o se enfoque en aplicaciones y servicios de la Ciudad de baja prioridad.

Actualización del Plan de Respuesta al Incidente

El Plan de Respuesta al Incidente de la Ciudad será revisado continuamente a causa de éste o de cualquier acontecimiento y a medida que evoluciona la tecnología. El Plan sirve como marco fundamental que guía el enfoque de una organización para identificar, evaluar y mitigar incidentes de seguridad. Sin embargo, luego de incidentes importantes, las lecciones aprendidas se vuelven importantes para comprender qué funcionó y qué no según el plan. Esto permite a ITS incorporar inteligencia actual sobre amenazas, estrategias de mitigación avanzadas y mejores prácticas de la industria. Las actualizaciones son imperativas para garantizar la relevancia y eficacia continuas del Plan para abordar las amenazas cibernéticas emergentes. Al mantener continuamente el Plan, la Ciudad puede mejorar no solo su capacidad para salvaguardar información confidencial, sino que también demuestra un compromiso proactivo para mitigar los riesgos legales y financieros asociados con posibles infracciones de seguridad y esfuerzos de recuperación.

Plan Integral de Acciones y Objetivos (POAM, por sus siglas en inglés)

Las recomendaciones deben ser incorporadas sistemáticamente en un Plan Integral de Acciones y Objetivos (POAM, por sus siglas en inglés) para rastrear las remediaciones. Este documento estratégico sirve como hoja de ruta para implementar las medidas de seguridad y privacidad identificadas de manera estructurada y organizada. A cada recomendación se le asignará una acción específica a llevar a cabo, acompañada de un hito correspondiente, que describe una fecha o cronograma objetivo de finalización. El POAM describirá las personas o equipos responsables de ejecutar cada elemento de acción y delineará los recursos, el presupuesto y las dependencias necesarios para una implementación exitosa. Además, el POAM proporcionará un mecanismo para el seguimiento, monitoreo y presentación de informes continuos del progreso hacia el logro de los objetivos establecidos.

Sección VI – Apéndices

Esta sección del documento proporciona apéndices de información relevante al Incidente de Cibersecuestro de Datos de Royal en la Ciudad de Dallas. Se ha identificado que el Incidente de Cibersecuestro de Datos de Royal en la Ciudad comenzó a primera hora en la mañana del miércoles, 3 de mayo de 2023.

Apéndice A – Glosario

Esta sección del documento proporciona un glosario de términos utilizados en este documento.

Término	Definición
AAR	Informe Posterior a la Acción
CIO	Director de Información/Director de ITS
CISO	Director de Seguridad de la Información
CTO	Director de Tecnología
CIS	Departamento de Comunicaciones y Tecnología de la Información (precursor de ITS)
CISA	Agencia de Seguridad de Infraestructura y Ciberseguridad
ITS	Departamento de Servicios de Información y Tecnología
MITRE	Corporación MITRE
NIST	Instituto Nacional de Estándares y Tecnología
Evaluación de Riesgos Dirigida (TRA, por sus siglas en inglés)	Una evaluación del riesgo dirigida a una actividad específica que depende de las vulnerabilidades, las amenazas y el impacto causado por el impacto exitoso de una amenaza mediante la explotación de las vulnerabilidades identificadas.
TxOAG	La Oficina del Fiscal General del Estado de Texas

Apéndice B – Fuentes de Información

Esta sección del documento proporciona una lista de fuentes de información utilizadas en el desarrollo de este documento.

Identificador/Etiqueta	Fuente de Información
AWS	Servicios Web de Amazon
CrowdStrike	CrowdStrike
Forrester	Forrester
Fortra	Fortra
Gartner	Gartner
HHS	Departamento de Salud y Servicios Humanos de EE. UU.
IBM	Corporación IBM
ITIL2	Biblioteca de Infraestructura de Tecnología de la Información, Versión 2, 2004
ITIL3	Biblioteca de Infraestructura de Tecnología de la Información, Versión 3, 2007
ITIL4	Biblioteca de Infraestructura de Tecnología de la Información, Versión 4, 2019
MITRE	Corporación MITRE
NIST	Instituto Nacional de Estándares y Tecnología
OpenAI	The Open AI Foundation
PA Unit42	Palo Alto Unit 42
UH	Universidad de Houston