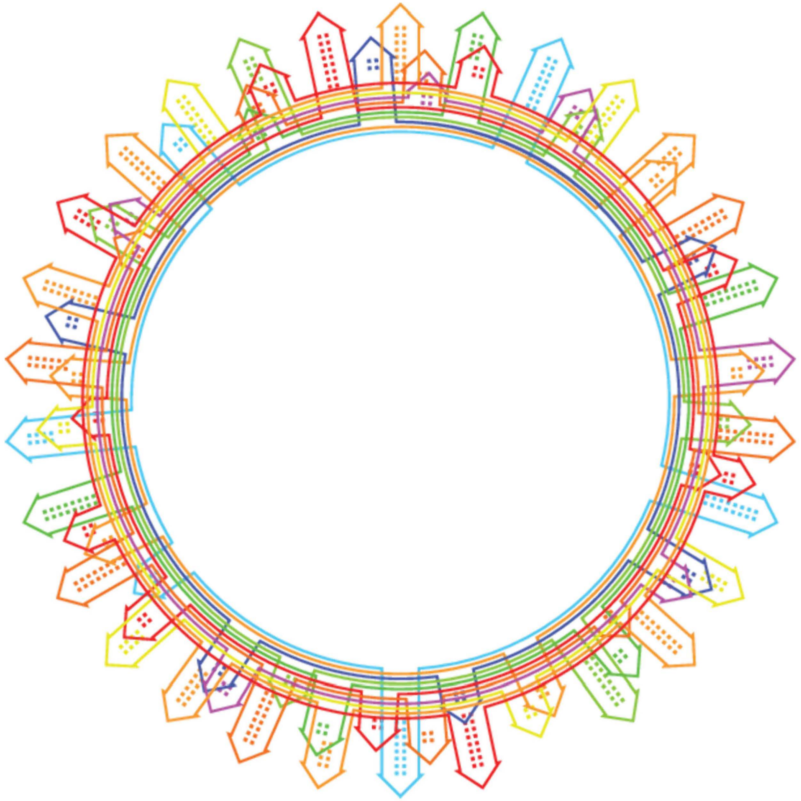
Deloitte.



Project Lurus

Executive Summary

January 22, 2020

Executive Summary

On December 7, 2019, the City of Pensacola experienced a ransomware attack (the "Incident") that impacted the City of Pensacola's Information Technology environment.

The City of Pensacola engaged Deloitte & Touche LLP ("Deloitte & Touche") to assist with the investigation of the Incident, and to determine, to the extent possible, the initial compromise vector, the extent of the attack, and what internal data was exposed or stolen by the attackers. We were also asked to provide security observations and recommendations with the intent of improving the overall security of the environment and mitigating the risk of further cyber attacks.

Objectives	Findings
Determine initial attack vector	The initial attack vector was very likely two systems with RDP (Remote Desktop Protocol) exposed to the internet. Once compromised, this allowed full access to the internal environment due to lax firewall rules between the DMZ[1] and the internal network.
Determine overall extent of the attack	We confirmed ransomware activity on at least 27 systems, but it is possible that additional systems were impacted by the ransomware. The attacker also claimed to have exfiltrated approx. 32GB of data. We were able to confirm approximately 6GB of compressed data had left the environment.
Determine what internal data was exposed or stolen	The attacker claimed to have exfiltrated approx. 32GB of data. We were able to confirm approximately 6GB of compressed data had left the environment. We also confirmed that the attacker had full access to internal systems, and had knowledge of the primary network shares containing a variety of internal data. No evidence was available to allow confirmation of whether the attacker directly or indirectly accessed confidential client data due to inadvertent evidence destruction during the recovery efforts.

Areas of Strength

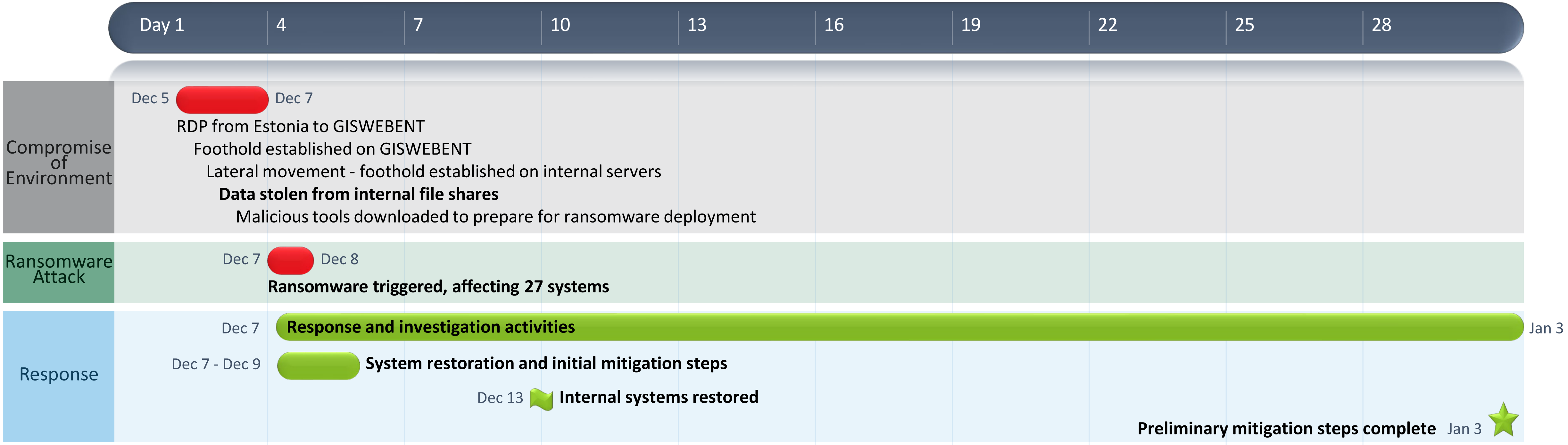
- **Backups -** Backups for major systems were readily available promptly following the attack
- **Proactive Communication -** City of Pensacola proactively communicated with the public, rather than failing to acknowledge the attack
- **Proactive Protection -** Out of an abundance of caution, the City of Pensacola chose to provide identity theft services to clients to protect them in the event of a potential damage as a result of the attack

Opportunities for Improvement

- **Staffing -** Consider dedicated security staff
- **Incident Response Plan -** Consider developing a more robust Incident Response plan
- **Security Assessments -** Consider conducting regular assessments of the security posture of the City and addressing issues as they are discovered

[1] DMZ, or "Demilitarized Zone" is a separate subnet within an environment. Systems inside the DMZ are generally exposed and available to the outside world (the internet) and as a result are more at risk than standard systems. Access between the DMZ and the internal environment is restricted to mitigate the risk to the entire environment should a successful compromise of a DMZ system occur.

Timeline of attack



Compromise of Environment

Dec 5 Dec 7

RDP from Estonia to GISWEBENT

Foothold established on GISWEBENT

Lateral movement - foothold established on internal servers

Data stolen from internal file shares

Malicious tools downloaded to prepare for ransomware deployment

Ransomware Attack

Dec 7 Dec 8

Ransomware triggered, affecting 27 systems

Response

Dec 7 **Response and investigation activities** Jan 3

Dec 7 - Dec 9 **System restoration and initial mitigation steps**

Dec 13 **Internal systems restored**

Preliminary mitigation steps complete Jan 3

Important Points

- The attacker connected to an internet facing system with Remote Desktop Protocol (RDP) open to the internet
- The attacker found data on one or more internal file shares, and exfiltrated a subset of those files
    - The attacker claims to have exfiltrated a total of 32 Gb of data from the City of Pensacola internal network
- The attacker then distributed and executed ransomware on 27 systems
- Shortly after being alerted, City of Pensacola IT personnel began restoration of affected systems and took initial steps to mitigate further damage to the environment
- Although it is clear that the attacker had potential access to database systems containing City of Pensacola client data, no evidence was found that indicates that data was actually accessed by the attackers