PUBLIC TRANSPORTATION CASE STUDY

Mass Transit Agency Hunts Down Cybersecurity Threats with Infocyte

ORGANIZATION

A mass transit agency serving a metropolitan area and surrounding municipalities.

INDUSTRY

Public Transportation

CHALLENGE

In the face of increasing cyber risks to public infrastructure from hackers, this mass transit agency took steps to understand their current security posture and assess the need for more advanced security measures and investments.

SOLUTION

A Compromise Assessment using Infocyte HUNT™

RESULTS

- Five days to scan, analyze and reports on 950 workstations and servers active on the network.
- Despite having an enterprise-grade antivirus solution and network-based threat detection capabilities, the system was infected with multiple pieces of malware
- Identified five variants of known-bad malware and backdoors, plus another 15 instances of potentially unwanted programs (nuisance-ware) across 25 systems.
- Suspicious code found in active memory of one system which did not trigger an alert on any antivirus or Threat Intel sources.
- Multiple instances of legitimate but unauthorized Remote Access Tools, which can be used maliciously by attackers and insiders alike, were found.

The Organization

A mass transit agency serving a metropolitan area and surrounding municipalities with a fleet of 500+ buses and streetcars, 2,000 employees, serving daily ridership of over 150,000 people.

The Growing Cyber Challenge

Cybersecurity is a top concern for public transit managers as their services become increasingly dependent on networked information technology. Transit IT infrastructure is a series of complex, interconnected control, management and communication systems. These systems are vulnerable to cyberattack which could disrupt operations or cause financial damage.

Given these increasing cyber risks, this mass transit agency took steps to understand their current security posture and assess the need for more advanced security measures and investments. To begin, the Board of Directors asked Infocyte to perform a “Compromise Assessment” of their primary IT infrastructure to analyze their systems to determine if any existing threats had made it past their current security controls.

Conducting a Compromise Assessment with Infocyte HUNT

A new addition to the various network risk assessment services that are available, the Compromise Assessment is a breach discovery service that independently verifies whether a network has been breached or not. The assessment seeks to discover adversaries or malicious software currently in the environment or any activity in the recent past.

According to various industry reports, the average security breach goes undetected for more than six months before found. Many targeted attacks can remain hidden for years as they use tools and techniques tuned to bypass an organization’s particular security stack.

As an independent assessment which does not rely on existing security infrastructure, Infocyte’s Compromise Assessment answers the growing need for confidence and confidentiality in the enterprise and critical infrastructure.

The assessment leverages Infocyte HUNT™ malware hunting software built to conduct a compromise assessment effectively and rapidly. Infocyte HUNT enables a security practitioner to scan and validate the integrity of each device to include determining what is running on them and any indication that the system has been manipulated or infected by malware or an unauthorized party.

The solution brings together proprietary and third party threat intelligence, multiple advanced threat detection engines, and automated static and dynamic malware analysis to enable the operator to find all known and unknown variants of malware.

The Process

Infocyte sent an analyst armed with a laptop and Infocyte HUNT software on-site for two days. Network credentials in the form of an Active Directory service account were provisioned to give Infocyte HUNT local administrator access to each host (workstations and servers) throughout the network.

Within an hour, Infocyte HUNT enumerated and mapped 950 workstations and servers active on the network. These systems were then scanned by deploying a temporary dissolvable agent to collect a snapshot of each system. Primary scans took place during the first day and second day at various times to maximize coverage of active systems.

Scans concluded at the end of day two, successfully examining 85% of all assets registered in Active Directory. The balance were identified as off network or unpowered laptops, backup or previously decommissioned systems.

The Results

Despite having an enterprise-grade antivirus solution and network-based threat detection capabilities, Infocyte HUNT found that their system was infected with multiple pieces of malware, some going back two years and exposing the mass transit agency to critical risk.

Within the first day of scans Infocyte HUNT identified five variants of known-bad malware and backdoors, plus another 15 instances of potentially unwanted programs (nuisance-ware) across 25 systems. Suspicious code was also found in the active memory of one system which did not trigger an alert on any antivirus or Threat Intel sources. The suspicious code was automatically extracted by Infocyte and submitted to Infocyte's cloud for static analysis and sandbox detonation. Analysis of the results identified the code as a component of the Alureon Data Exfiltration Trojan. Further evidence collected from the system showed it had been active as far back as December 2013 - undetected for two years. Fortunately the malware's botnet controller was decommissioned sometime in the past and did not present an immediate threat to the mass transit agency.

In addition, multiple instances (8) of legitimate but unauthorized Remote Access Tools, which can be used maliciously by attackers and insiders alike, were found. Findings also included active Cygwin SSH Daemon, WinVNC, UltraVNC, TightVNC, and RealVNC servers. VNC programs are graphical desktop sharing apps used to remotely control another computer across the internet. It is recommended such programs be highly controlled in enterprise environments to reduce the external threat surface and risk of insider misuse.

Conclusion

Our national security depends on an open, reliable and secure transportation system and failure to protect these systems may result in significant and adverse safety, security and business implications for both the organization and the public it serves. Without a compromise assessment, the mass transit agency's security problems would have continued to go undetected and it would have been difficult to provide tangible evidence to warrant increasing their security posture. As a result of the assessment, they are pursuing increased budget and petitioning the US Department of Transportation (USDOT) and Department of Homeland Security (DHS) for federal funds to better secure municipal and regional transportation networks nationwide.

Infocyte HUNT
Compromise Assessment

MAJOR FINDINGS:

Detection: Alureon Data Exfiltration Trojan (memory-resident only)

Alureon (also known as TDSS) is a "bootkit" created to steal data by intercepting a system's network traffic and searching for: banking usernames and passwords, credit card data, PayPal information, social security numbers, and other sensitive user data.

Detection: Fake Antivirus Trojan

Fake Antivirus trojans present themselves as anti-virus in order to infiltrate a system and set up a backdoor to the network.

Detection: Memory-resident Backdoor/Trojan

Fake Antivirus Trojans present themselves as anti-virus in order to infiltrate a system and set up a backdoor to the network.

Detection: Legitimate but potentially unauthorized Remote Access Tools: Cygwin SSH Daemon, WinVNC, UltraVNC, TightVNC, and RealVNC servers

VNC programs are graphical desktop sharing apps used to remotely control another computer across the internet.

Infocyte™

CORPORATE HEADQUARTERS

110 E. Houston St. Floor 7
San Antonio, TX 78205
+ 1.844.INFOCYTE (844.463.6298)
sales@infocyte.com

www.infocyte.com
@InfocyteInc