Infocyte

CASE STUDY / BANKING & FINANCIAL

Infocyte HUNT

Top-tier banking and financial institution uses Infocyte HUNT for compromise assessment in acquisition due dilligence.

THE CUSTOMER

The acquirer is a major banking and financial institution based in the US and managing over a trillion dollars in assets. This institution engages in multiple mergers and acquisitions transactions throughout the year.

In this case, the acquiree is a 50-employee wealth management firm located in the US and serving high net worth clients, managing over a billion dollars in assets.

Using Infocyte HUNT, the institution ran a comprehensive compromise assessment on the acquiree's network to quickly and conclusively assess the security posture of the acquiree and determine if there are any potential cyber risks — prior to proceeding with the acquisition.

BACKGROUND

Mergers and acquisitions (M&A) can be high-risk operations in which it's difficult to determine what the buyer is adopting. In this case, the acquirer was purchasing a business whose primary value was in the form of private customer data and intellectual property (e.g. trading algorithms). The need to measure information risk and verify the confidentiality of this information was a must-have for completing a successful acquisition.

Traditionally, M&A due diligence utilizes questionnaires, representations, and warranties from the acquiree to measure risk. However, considering the average security breach can go undetected for more than six months, and given the reduced regulatory requirements and resources of the acquiree (compared to the acquirer) it became more important to independently verify the secure state of these systems.

After being briefed on Infocyte's tools and technology, the lead IT Risk Manager involved in the transactions asked our team to perform an Infocyte HUNT Compromise Assessment during the due diligence phase.

OUR SOLUTION

Far better than traditional network risk assessment services, an Infocyte HUNT Compromise Assessment is independent and conslusive, and verifies whether a network has been breached or not and if it can be breached. Our CA seeks to discover adversaries or malicious software currently in the environment and/or any post-breach activity.

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.

Our solution brings together proprietary and third party threat intelligence, multiple advanced threat detection engines, and automated static and dynamic malware analysis which enables the operator to find all known (and unknown) variants of malware – including advanced threats capable of bypassing the world's best defensive tools.

INDUSTRY

Banking & Financial

CHALLENGE

As part of their M&A due diligence our customer needed to verify the health of the aquiree's IT systems, data, and network. Additionally, our customer needed to determine if the acquiree's network had been breached, was currently breached, or if it posed any risk of being breached in its current state.

SOLUTION

An Infocyte HUNT Compromise Assessment

RESULTS

- Five days to scan, analyze, and report on 54 workstations and servers active on the network
- Found several machines not using corporate standard antivirus software
- Confirmed the acquiree had strong technical controls, good security hygiene practices, and IT policies in place to protect their network and systems
- Conclusively determined the compromised state of the acquiree's network and established confidence that the acquiree's data and systems were clean, and the M&A transaction could proceed

THE PROCESS

The acquiree provided Infocyte consultants with a Virtual Private Network connection and an Active Directory service account with local administrator access to each host (workstations and servers) throughout the network.

Infocyte HUNT was loaded on a virtual machine to remotely scan the environment. Infocyte enumerated and mapped 54 workstations and servers currently active on the network. These systems were then deep-scanned by deploying a dissolvable agent to collect a forensic snapshot of each system.

Several primary scans took place to maximize coverage of active systems as the network had many transient laptops. Suspicious executables and artifacts were collected for deeper analysis as needed. Scans concluded at the end of day three, successfully inspecting 88% of all assets.

A malware analysis and threat intelligence expert was on-hand to help identify and correlate suspicious findings to organized threat groups, corporate espionage, and/or insider threats.

THE RESULTS

Our assessment provided a clean bill of health and showed that the acquiree had strong technical controls, regular security hygiene (e.g. nightly reboots) and IT policies in place to protect the network. As a result, Infocyte HUNT found surprisingly few unwanted programs and no nuisances (like adware and browser toolbars) which are common on any network, even when serious threats are absent.

Infocyte HUNT also reported several (30) instances of legitimate Remote Access Tools active on the network – a remote support suite called "Saazod" by Zenith Infotech used by support technicians to remotely control computers. This program was confirmed authorized, but needs to be controlled to minimize attack surface and risk of insider misuse.

Finally, the customer used Trend Micro Worry-Free Business Security (WFBS) suite as their managed anti-virus solution, but during the CA we discovered it was not installed on all systems. A few outliers had consumer versions of anti-malware which, being unmanaged, would not report to network administrators had there been an attack.

The entire Compromise Assessment lasted five days from the initial engagement to the final report. Infocyte was able to verify the integrity and confidentiality of the information systems to the acquirer at an unprecedented level compared to traditional due diligence methods.

THE CONCLUSION

Without Infocyte's compromise assessment using Infocyte HUNT, the acquirer would have taken on unknown risk which could have had significant repercussions had the network had an undetected or unreported security breach.

As a result of the comprehensive Compromise Assessment using Infocyte HUNT technology, the acquirer was able to continue into the next phase of consolidating networks and finalizing the transaction with confidence.

Infocyte HUNT:
Compromise Assessment

KEY FINDINGS

- Systems: Multiple (30) workstations and servers
- Detection: Legitimate, but potentially unauthorized remote access tools
- Indicators: Running processes (no stealth)
- Description: Saazod is used by foreign support technicians to remotely control another computer across the internet. This attack vector can be misused and exploited if not controlled properly.

Infocyte

3801 N. Capital of Texas Hwy.
Suite D-120
Austin, TX 78746

(844) 463-6298
sales@infocyte.com
www.infocyte.com