Infocyte

CASE STUDY / FINANCIAL

Infocyte HUNT

Infocyte MSSP partner uses HUNT to identify malware, ransomware, adware, and more on payment gateways prior to activation.

THE CUSTOMER

The bank is a major regional financial institution that suffered a significant undisclosed data breach. Specifically, the bank had been the target of unknown/zero-day malware which was discovered accidentally, following the notice of abnormal network communications.

A third party was contracted to conduct Incident Response work, upon the completion of which the bank sought to validate that no further malware was residing undetected on its critical infrastructure with the help of an independent MSSP.

THE PARTNER

A large, award-winning multinational systems integrator servicing customers from small businesses to large enterprises. The MSSP arm is a security practice that combines consulting, design, products and services to provide end-to-end solutions to deliver highly resilient and secure infrastructure. The partner has designed, integrated, and implemented some of the most secure networks in the region.

The Partner was contracted by the Customer to deliver managed security services in the form of a Compromise Assessment on the critical infrastructure of the bank.

THE PROCESS

The scope of work included a full compromise assessment, completed on endpoints that the bank considered or identified as critical assets, across the bank's entire network of critical assets and endpoints.

The MSSP partner provided the environmental and system requirements necessary for optimal functioning of Infocyte HUNT to the customer. These requirements mirrored the bank's existing enterprise management tools' protocols and settings, resulting in minimal customer effort to prep the environment. Further, HUNT was able to perform all scans without impacting the bank's productivity and resulted in zero downtime.

The Infocyte HUNT server was installed into the customer environment in less than ten minutes, with the first active scans completing within twenty minutes of the start of the engagement. It is worth noting that a small number of the endpoints in scope (fewer than ten) were not connected to the network; these endpoints were scanned offline and the results were imported into HUNT to complete the full scope of work.

The full engagement was completed in four days, and included multiple scans of the endpoints in scope. The secondary and tertiary scans were completed by the end of day two, while the analysis and report creation were finalized and delivered at the end of day four.

THE DISCOVERY

Within minutes of the first completed scans, the partner found a 5.3MB executable injected into the LSASS process with read, write, and execute privileges. Local Security Authority Subsystem Service (LSASS) is a process in Microsoft Windows operating systems that is responsible for enforcing security policy on the system.

The injected memory was unmapped into a native PE file structure and submitted to HUNT's AI-powered Incyte engine for static, heuristic, and IOC analysis. This data was later enhanced with supplemental information from other feeds in our file intelligence services.

The injected memory in question was assessed and given a threat score of 10 using our scoring system because it was identified as malware based on signatures of three AV vendors.

Today, this same sample would be confirmed as malware by over thirty different AV vendors.

Infocyte HUNT:
Compromise Assessment

SUMMARY

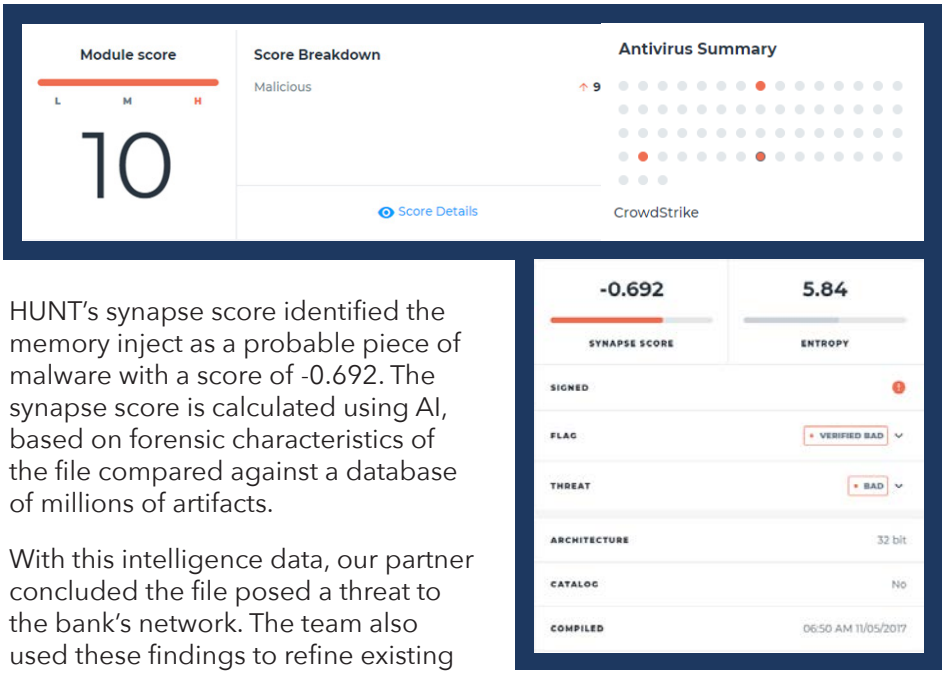
- Scope:
  Critical banking infrastructure
- Term of engagement:
  4 days
- Date of engagement:
  February 2018
- Resources to deliver:
  1 person
- Scan type:
  Critical assets/endpoints
- First results in less than 20 minutes

KEY FINDINGS

- Wannacry ransomware
- Adware

ANCILLARY FINDINGS

- Unauthorized Remote Access Tools
- Unauthorized File Sharing Tools
- Disabled A/V
- Abuse of Administrative Accounts
- Hackware
- Riskware
- Generally unwanted software



HUNT results—scores, score breakdown, AV summary, and entropy.

HUNT's synapse score identified the memory inject as a probable piece of malware with a score of -0.692. The synapse score is calculated using AI, based on forensic characteristics of the file compared against a database of millions of artifacts.

With this intelligence data, our partner concluded the file posed a threat to the bank's network. The team also used these findings to refine existing tools and policies, strengthening the bank's overall security posture.

THE RESULTS

- Ransomware was removed from the payment gateway before it had an opportunity to activate
- The same ransomware HUNT found was also detected on another enterprise endpoint
- The gateway and secondary endpoint were rescanned to validate remediation, before concluding the engagement
- Had the ransomware activated, the cost to the bank would have been in the tens of thousands of dollars – per hour; redundancies were non-functional at the time

THE CONCLUSION

Infocyte HUNT allowed the MSSP partner to successfully protect the bank from the inevitable activation of the ransomware found. Over the course of the assessment, other significant insights were made and recommendations suggested. Operational concerns had led to an erosion of defensive measures, placing the bank at an unnecessary risk. Some defenses were also quite dated and required modernization.

These conclusions offered value to both the customer and the partner, validating the consultancy work delivered by the partner and resulting in a stronger defensive cybersecurity posture for the bank and its network.

"Infocyte HUNT allowed us to deliver a full compromise assessment and consulting for our customer, in record time without business interruption.

Deploying Infocyte HUNT was a simple, seamless, 10-min process. Our customer was thrilled with the concrete results provided and elimination of threats, including finding ransomware waiting to strike on critical banking infrastructure.

Our partnership with Infocyte allows us to deliver instant, tangible value through our security services practice."

- President Security Business, MSSP Partner

Infocyte

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

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

TRY HUNT FOR FREE »

Discover why Infocyte HUNT has been recognized as a top threat hunting solution by industry leaders.

try.infocyte.com