Infocyte

CASE STUDY / OIL AND GAS

Infocyte HUNT

Infocyte HUNT used to detect custom malware that successfully bypassed EDR defenses.

THE CUSTOMER

A midstream natural gas transportation and distribution company providing gas to light and heavy industries, petrochemical facilities, desalination, power, refinery, steel and cement plants. The customer operates an extensive network of gas pipelines, compressors and supply stations.

The customer made significant capital and operational investments into defensive solutions to protect their IT assets and corporate data. These investments included EDR, network monitoring, next-generation firewalls, stateful packet inspection, and more.

The customer chose to use Infocyte HUNT to run a comprehensive compromise assessment on their entire estate in order to validate the strength of their existing defenses.

THE PROCESS

The scope of work was carried out jointly by the customer and Infocyte Inc. The decision was made to scan all 800 endpoints within the estate to ensure complete visibility. The customer took responsibility for scanning endpoints using Infocyte HUNT, and Infocyte was responsible for analysis.

The customer prepared their environment per the requirements provided by Infocyte and provided a dedicated server for baseline analysis results, which will expedite future compromise assessments.

The installation of Infocyte HUNT was completed in under 20 minutes, and the first endpoint sweep was completed in under one hour. A small percentage (<10%) of estate endpoints were not discoverable or scannable on the first sweep, largely due to being offline. In subsequent sweeps over the course of 2 days, the majority of these were scanned. Those that remained outliers were manually scanned and the data imported into Infocyte HUNT for analysis.

THE DISCOVERY

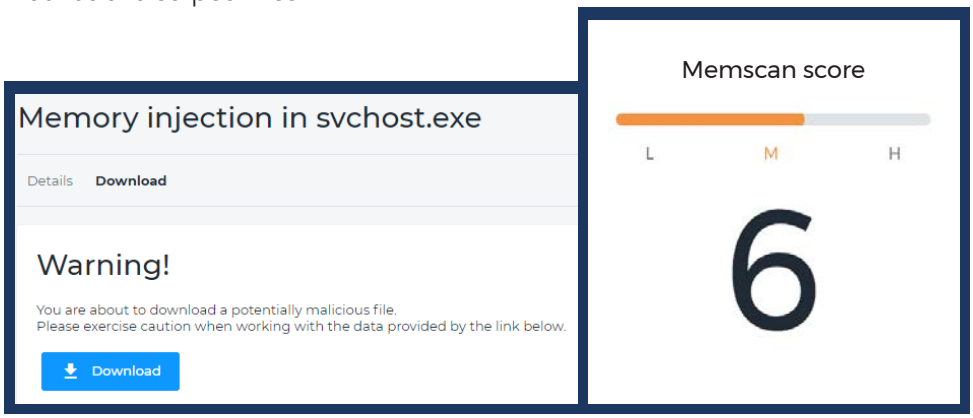
Infocyte led an analytic review process on the third day of the engagement, and within 30 minutes an unknown piece of software was discovered injected into a system process.

The compromised endpoint runs software that is responsible for tracking the volume of product distributed through the customer's network of gas pipelines. The customer considers this data to be proprietary intellectual property.

The unmapped memory was provided to the client in a PE format for downstream incident response efforts that included reverse engineering activities.

The customer's reverse engineer determined that the program in question was indeed malware which had been tailored specifically to attack the enterprise and had successfully bypassed the customer's network and endpoint defenses – including its EDR solution.

A review of the detected malware further determined that the malware relied on alternate channels for persistence; while the EDR solution did record some events, they did not trigger alerts because they were filtered out as a false-positives.



Infocyte HUNT:
Compromise Assessment

SUMMARY

- Scope:
  Oil and Gas operational and critical infrastructure
- Term of engagement:
  5 days
- Date of engagement:
  December 2017
- Resources to deliver:
  1 person
- Machines scanned: 800 endpoints

KEY FINDINGS

- Tailored Malware
- Failure of EDR defences

ANCILLARY FINDINGS

- Adware
- Generally unwanted software

THE RESULTS

The client was able to validate the effectiveness of their existing defences and discovered that malware still poses an ongoing threat. This result has been useful in securing further modernization funding required to not only defend the estate but also ensure that existing defences are not already breached.

The malware in question was ultimately confirmed to be tailored specifically to exploit the customer's environment. While attribution was not possible, it is strongly believed to have been created and controlled by a hostile state.

The malware was ultimately purged from the environment within hours of discovery, but it also underscored the need for a new class of control: the ability to define and manage dwell time.

The customer has moved to budget and procure enterprise licenses of Infocyte HUNT to allow them the ability to discover malware within 24 hours of first execution, should it manage to breach all existing defences in future.

- Efficacy of defenses was validated and forward planning improved
- Re-allocation of budget to allow funding for modernization
- Custom malware isolated and purged from estate within hours
- Customer recognized the need to control dwell time, and moved to procure enterprise licenses

THE CONCLUSION

Infocyte HUNT allowed the early discovery of tailored malware, before any data was lost or exfiltrated from the estate. Given that the nature of the data met the threshold of national security concerns, an ROI was demonstrated with a single discovery. The customer is so convinced of the value of controlling dwell time that they are moving to procure this capability to run scans independently on a daily basis - providing a safety net for when existing defences fail.

Infocyte HUNT is the only solution in the market that allows for rapid and automated memory analysis and high frequency scans to validate that enterprises are in fact malware free.

"We saw measurable value in layering Infocyte on top of our EDR deployment. Infocyte HUNT offers insight into memory resident threats - coupled with the visibility EDR provides of event driven data from processes, the file system, the registry and more, makes a great combination."

- Senior Engineer, Information Communications Technology Security, ONG customer

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