NETWORKWORLD Reprint

THE CONNECTED ENTERPRISE = DECEMBER 19, 2016

SECURITY TESTS

Review: Threat hunting turns the tables on attackers

BY JOHN BREEDEN II, NETWORK WORLD

Credit: Thinkstock

Unlike the more traditional model of a lone hunter stalking their prey, Infocyte HUNT has added vast amounts of automation to the point where an entire network can be hunted in about a day. It's more like hunting from a helicopter with a machine gun.

Founded by former Air Force officers in 2014, HUNT was designed to replace the sometimes months-long, labor intensive hunting process that some government agencies were using at the time. HUNT is completely centered on network endpoints and has no need for additional sensors. The main console, which is traditionally installed as a virtual machine, but is lightweight enough to exist on a laptop, sends out agents to all endpoints. However, the agents only exist for about 90 seconds on each endpoint and are dissolved afterwards. HUNT works natively with Linux and Windows endpoints plus most payment processing terminals. A Mac version is in the works.

Pushing out an agent takes up about 1 megabyte of network bandwidth while the return response is about 1.2 megs. The software defaults to sending out 60 at a time, and agents are smart enough to wait if the network is too busy, sending their report back when traffic clears. Using this method, HUNT is able to scan about 25,000 endpoints a day if the network is that large. Our test network had a modest 50 clients, so the total process took about a minute.

The main console controls the agent deployment and response process as well as the reporting dashboards, but heavy lifting is done in the Infocyte cloud. That includes hash and DNS lookups as well as comparing results with outside threat feeds and even sandboxing. Government agencies or companies that prefer to keep everything inside their networks can opt for a much larger on-premises configuration. In addition to the lookups, unknown executables can be submitted to Infocyte for analysis, where the staff maintains a threat lab to help identify zero-day type attacks. Human operators need to choose to submit those for analysis help, so again, data will only leave a network if it's authorized to do so.

To begin our investigation, we first had the console send out the dissolvable endpoints to our network. A report quickly came back because our test network was so small. From there, we could see that several endpoints could not be scanned. One of those had recently changed its login credentials. We could then log into it by hand and make sure it got the agent from the HUNT console. Another was disconnected from the network, so there was nothing we could do about that other than setting HUNT to catch it when it was back online. A couple of clients were VR machines that had been decommissioned but whose images remained in Active Directory. Those could be eliminated from future consideration.

The default scan looks at everything within the detection capabilities of HUNT including processes, modules, drivers, memory scanning, account information, network connections and hooks. Scans can also be tailored to specific items. If you are explicitly hunting malware disguised as a driver for example, you could just run that part of the scan. However, because the dissolvable agents are so quick, you don't really save too much time paring them down, so the full scan is probably best most of the time.

With active endpoint scanning, HUNT could almost be deployed as a more traditional security tool, especially for organizations that have not invested heavily in endpoint protection. However, while HUNT can find traditional threats, its value as a threat hunting tool is that it is designed to catch advanced malware that would otherwise avoid detection.

As an example, in our testing we found an instance where Firefox.exe was listed as probably bad on one client machine. This

was quite puzzling so we dove into that part of the report, which was easy to do using a good graphical interface. Drilling down to the first level, we found that everything with Firefox seemed fine. HUNT runs all endpoint programs through 21 anti-virus programs and provides a report back on their findings. In this case, all of them said that the file was fine, although HUNT was still not convinced. Drilling down further, the hash for the Firefox file was correct, so it was the actual Firefox program provided by the company.

We started to think that HUNT was providing us with a false positive, until we went a little deeper. It turns out that a module installed inside that version of Firefox turned out to be a bitcoin miner. HUNT not only caught this during the sandboxing process, but also allowed us to see every module that was part of the core program. That enabled us to identify a threat that would have escaped almost every other type of endpoint protection.

Another strength of HUNT is its ability to do true memory mapping, so malware that only exists within memory, even if it uses stealth technology or tries to stay under the radar, is quickly identified. We found a memory injection type of attack against Explorer on another machine. HUNT can take all types of memory code and convert it into executable files which can then have their characteristics checked in a safe environment. We have not previously seen this type of mapping process that allowed HUNT to drill so far down, and so accurately, into the system memory of connected endpoints.

Finally, HUNT is able to see if any type of malware or malicious process is using hooks to divert programs or users away from their intended destinations. On our test system, there was a program that was supposed to point to a specific place inside system memory, only a hook was being used to read from a different place each time the function call was made. That is a pretty subtle type of vulnerability that could be stealthily exploited by attackers without triggering too much attention. But HUNT found it and gave a detailed report about what was happening.

Once a scan is complete, a report with multiple levels can be generated. For the analysts, very detailed descriptions of all threats, where they reside and what they are attempting to accomplish is available. And for the C-suite, HUNT provides a really nice top-level overview of everything that is wrong or compromised within a network.

On the flip side, a HUNT report could also certify that a network is completely clean and uncompromised, something very few other programs are willing to do. A clean report shows everything that HUNT did and checked, and explains why it is so confident that no APT or other breaches exist. That should help executives sleep a little better at night.

Pricing for HUNT starts at $6,000 for 100 endpoint licenses with volume discounts available. Because of the way the scanning engine works with dissolvable agents, its scalability is practically unlimited. And with a constant rate of about 25,000 endpoints scanned per day, it's easy to figure out how long a scan will take based on network size.

Infocyte's HUNT would be a good program for organizations that are just starting to upgrade their cybersecurity defenses, particularly protecting endpoints. But it would also be a perfect check for organizations that have invested huge amounts of money in robust defenses. HUNT could check those cybersecurity programs and either point out any holes that still exist, or certify that those defenses are working perfectly.

© Copyright 2016 by Network World, Inc., Southborough, MA 01772-9108 • Posted from NetworkWorld.com • Trademark is owned by International Data Group, Inc.
#C59859 Managed by The YGS Group, 800.290.5460. For more information visit www.theYGSgroup.com.

Infocyte®

www.infocyte.com
sales@infocyte.com