accelerite

SENTIENT

Case Study

An American Bank’s readiness against WannaCry

Modus Operandi of an online ransomware attack

On May 12, 2017, the world woke up to one of the most widespread cyber-attacks of recent times called WanaCryptor Ransomware (popularly known as WannaCry). The attack had a broad reach affecting large corporations, technology giants, financial institutions, hospitals, banks, and individuals. Unidentified hackers encrypted data of around 300,000 machines across 150 countries, effectively locking the machines down and rendering them useless. The perpetrators demanded a ransom of approximately $300 worth in bitcoins from each victim within a short period of time to “rescue” them from the logjam. Even though the attack lasted for only a few days, the reported financial losses went to the tune of $4 billion. In the wake of the attack, many companies had to take immediate action to safeguard themselves, foremost of which was to assess which devices are potential targets and need to be taken off the network.

The IT team at a large American bank, started getting calls from leaders and business heads across multiple divisions and departments asking for their readiness against the WannaCry attack. Since the bank had almost all their banking facilities online, the bank was highly vulnerable to such an attack, and a hijack on their systems could bring their operations to a grinding halt. To add to the pressure, the head of IT was required to present to the board what the company’s exposure was to WannaCry. That meant finding out possibly compromised devices, devices that had the potential to be compromised, create a mitigation plan and present all of this to a non-technical, high-powered audience. The bank faced a number of issues in trying to address a problem of this magnitude.

Challenges

- The IT department knew that presence of deprecated SMBv1 and SMBv2 made machines running Windows OS susceptible to the WannaCry attack. However, it was no easy task to find out which of the 10s of thousands of PCs and servers had these attributes. This would easily be days to weeks’ worth of investigation – time they did not have.
- The banks large, distributed footprint made that problem harder still – the devices were in the headquarters, regional offices, branch offices and with field personnel.
- Even if the devices were to be found, how would they disable these devices, especially if large number of them were involved? Time was of the essence.

Sentient to the rescue

The bank had only recently deployed Accelerite Sentient in their enterprise, and they had access to Sentient as one of the tools in their considerable arsenal of software products. Sentient is an integrated and highly scalable solution that addresses three major pain points most IT and security organizations struggle with – visibility of what is present and happening on all endpoints in their networks, being alerted to anomalous events, and the ability to take remedial action on the devices – at scale and in real time.

109131 device(s) found out of 109131 applicable device(s)

109131 scanned in 19.973 seconds

With Sentient, the bank was able to achieve the following:

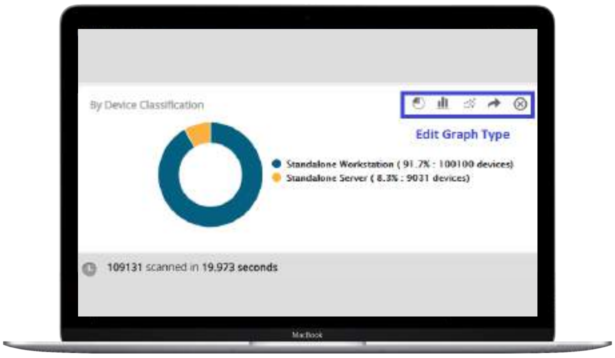
- Quickly create a script and distribute to all endpoints to check for possible vulnerabilities that included:
    - Endpoints running SMBv1 or SMBv2 protocols
    - Monitor inbound SMB activity or machines listening on TCP port 445 or 135, especially if they are open on the Firewall
    - Accessibility of many remote locations acting as kill-switch for the WannaCry worm
    - Endpoints having WannaCry worm module running as mssecsvc2.0 service
    - Endpoints that attempted connection to certain well-known websites
    - Check for any instances of files with extensions, .wnry, .wcry, .wncry, .wncryt
- With Sentient Endpoint Management, they were already well protected by way of patching. They were quickly able to identify 3 devices out of the many 10s of thousands that were potentially vulnerable. This was real time data that the head of IT took to the board.
- Using Sentient's capabilities, they were also able to rapidly remediate those 3 devices and prevent any vectors from spreading to the rest of the network.

Sentient Benefits

Sentient provided the capability to tackle an unforeseen attack like WannaCry using ready-to-fire commands on endpoints, and the ability to deploy and run custom scripts immediately

Sentient's completely web-based interface enabled the bank to run simplified natural language queries to detect any anomaly or deviation in its enterprise systems, saving hugely on time and costs

Sentient supports custom patching on select set of endpoints for emergency deployment and categorized patch upgrade, which was very useful in this case for the bank


By Device Classification
Edit Graph Type
● Standalone Workstation (91.7% : 100100 devices)
● Standalone Server (8.3% : 9031 devices)
MacBook

109131 scanned in 19.973 seconds

Sentient provided a flexible "query chaining" functionality that allowed response teams to quickly build complex search and remediation logic from granular building blocks, which could be rapidly tested and deployed

The IT team was able to create detailed status reports on deployment status, compliance metrics and several other reports for a detailed presentation to the board

Sentient empowered the bank's IT team to implement tighter endpoint management through a precise and real-time endpoint state ("Installed", "Running", "Updated") of the programs, applications, antiviruses etc. across all the endpoints

About Sentient

Accelerite Sentient pulls together real-time information from enterprise endpoints for IT administrators to quickly identify critical security threats and vulnerabilities, and address compliance and configuration issues in their endpoint network within minutes. Sentient allows administrators to proactively query the current status and existence/non-existence of configurations and files from the point of view of actively unearthing issues in real-time. It classifies and presents the information gathered in visual format with drilldown information and makes it easy for IT to locate problem areas in their network of endpoints quickly. The search queries in Sentient are in freeform text format, which enables IT to easily query their endpoints using natural language phrases.

About Accelerite

Accelerite is a Silicon Valley based company delivering secure business-critical infrastructure software for Global 1000 enterprises. Accelerite's product suite includes hybrid cloud infrastructure, endpoint security, big data analytics, and the Internet of Things.

To know more about Accelerite Sentient visit: http://www.accelerite.com/sentient