Case Study

RYUK vs GAMAYAN

On the day UHS was hit with the first stages of a $6M attack, all seemed well, but unbeknownst to senior management and IT staff, a type of malware, known as Bazaar, was loaded and executed by a remote attacker. The malware was delivered by email; the email was from known spam sources which had been creeping up in volume over the month of September. From the initial execution of the payload, Bazar injected into various processes including explorer.exe and svchost.exe, as well as spawning cmd.exe processes. The initial activity was all about reconnaissance; the attackers used built-in Windows utilities and a 3rd party tool to gather information.

After the initial discovery phase, the malware stayed relatively quiet until the second round of discovery the following day. The same tools were employed in the second round of discovery, plus Rubeus. This time the discovery logs were exfiltrated via FTP to a server hosted in Russia. Next, the threat actor began to move laterally.

It took a few attempts, using various methods to transfer Cobalt Strike beacons over SMB to move around the environment. From here forward, the threat actors relied on a Cobalt Strike beacon running on a domain controller as their main operations point.

After picking the most reliable method to move through the environment, the threat actor then proceeded to establish beacons across the enterprise. In preparation for their final objectives, they used PowerShell to disable Windows Defender in the environment.

The server utilized for backups in the domain was targeted first for encryption, with some further preparation completed on the host. However, once the Ryuk ransom executable was transferred over SMB from their domain controller (DC) pivot, it only took one minute to execute it.

The threat actors requested 600+ bitcoins, which have a market value of 6+ million USD.

At this point, Ryuk was transferred to the rest of the hosts in the environment via SMB and executed through an RDP connection from the pivot domain controller. In total, the campaign lasted 29 hours from initial execution to domain-wide ransomware. If a defender missed the first day of recon, they would have had a little over 3 hours to respond before being ransomed.

The organisation missed 28 opportunities to detect and respond to the attack in order to prevent it. Gamayan would have caught all of them.

RYUK TIMELINE

- **Day 1**
  - 16:37 Bazar Malware Executed (Remote IP)
  - 16:48 Domain discovery commands
  - 17:06 Registry discovery commands
  - 17:28 More domain discovery and network checks to domain controllers
  - 17:41 AdFind used to map active directory
- **Day 2**
  - 18:49 checks again for domain trusts and AdFind using Bazar (FTP exfiltration to remote IP)
  - 20:12 First lateral movement attempt with WMIC (SMB transfer, Multiple payloads tried)
  - 20:23 P64.exe Cobalt Strike beacon run on beachhead host (Remote IP)
  - 21:04 Second P64.exe Cobalt Strike beacon dropped on beachhead host (New remote IP)
  - 21:09 Next lateral movement attempt via a service and PowerShell (First Successful Lateral Movement)
  - 21:10-22:06 Continual lateral movement using Cobalt Strike beacons via SMB across the environment
  - 21:43 Windows Defender begins to be disabled using Powershell commands
  - 21:45 First RYUK ransomware executable transferred to the backup system (Ryuk Executed)
  - 21:50-22:10 RYUK ransomware deployed enterprise-wide (Transferred via SMB, executed RDP commands)

ALL TEXT MARKED IN RED ARE ‘INDICATORS OF COMPROMISE’ THAT GAMAYAN WOULD HAVE DETECTED AND ENABLED REAL-TIME INCIDENT RESPONSE HANDLING.

Initial Access

Initial delivery was via **1) known spam emails with a link** to the malware which connected to **2) a new remote address**.

GAMAYAN'S RESPONSE
Downloading and executing code from a remote IP is easily detected and prevented with Gamayan. AI email WatchGuard would have used sandboxed execution on the de-militarised zone (DMZ) based hosts to extract IOCs and monitor activity that the file may or may not generate, from remote connections to spawning new processes. Only safe binaries are forwarded to users, suspected files are quarantined for manual tier-1 analyst review. Every organisation should be able to detect remote IP addresses executing code on systems and should have the ability to execute files to check their behaviour before being sent to users. With Gamayan, most dangerous file types can be permanently blocked completely.

Execution

3) Service execution was used several times to run scripts and executables during lateral movement. **4) WMI was used** as well in an attempt to **5) execute DLLs laterally** in addition to **6) process injection**.

GAMAYAN'S RESPONSE
Gamayan monitors every process, including new thread spawns and commands that are executed. This is instantly logged and flagged to the security team. With GAMAYAN'S kernel extension, Gamayan sees the command execute before it returns anything to the attacker - meaning we can block that command, kill their process or activate aggressive firewall rules.

Defence Evasion

7) Windows Defender was disabled with a Windows **8) Powershell obfuscated command**.

GAMAYAN'S RESPONSE
Gamayan monitors PowerShell execution and can instantly reactivate defences like Windows Defender. In addition, Gamayan can disable this ability to disable firewalls with PowerShell and much more.

Quick Note:
So far the host has enumerated other hosts and the network, it has connected to a remote IP and executed code, in addition, it has disabled the firewall. **These actions should be triggering the alarms of any enterprise security team whose job is it to monitor a network like this.**

Discovery

Day 1

9) AdFind, a third party script and the attackers' custom script were dropped and run minutes after Document-Preview.exe was executed. The batch file output information into text files. **10) Nltest was used to check for Domain trusts, Net was used to show Domain Admins** and Ping was used to test if systems were up in the environment.

GAMAYAN'S RESPONSE
To Gamayan, this activity is like a 747 jet taking off. It is noticed, it is stopped. With the context of previous actions, we can be sure we are not dealing with a regular user.

Quick Note:
There is no reason this attack should have been able to carry on to day 2. Enough activity took place by now to fully defend all systems. Real-time intelligence allows Gamayan to restore systems and defend before Day 2 where the ransomware is deployed.

Day 2

11) Afind was run again, and then the threat actor attempted to Kerberoast using Rubeus. After **12) a few false starts during lateral movement failures**, the threat actors performed some **13) additional local system recon**. **14) WMI was used to check for the current AntiVirus on numerous systems**.

GAMAYAN'S RESPONSE
Gamayan instantly detects failed commands, a huge red flag, one that should always be examined in detail. In addition, commands that output to CSV and do this level of enumeration are loud; there is no reason this should go undetected and not be stopped in real-time. With Gamayan, this can be automated, done manually or a hybrid approach taken. Kerberoasting is easily detected.

Quick Note:
This stage was very noisy and surprising that it went undetected.

Lateral Movement

On day 1 the threat actors **15) checked a domain controller for MS17-010** before continuing with more discovery. The system was not vulnerable to MS17-010. Lateral movement began around 28 hours after initial entry, **16) using SMB to drop a Cobalt Strike beacon on a domain controller**. From there, the threat actor used WMIC to execute the beacon.

This **17) payload did not appear to run successfully**, as shortly after the threat actors dropped **18) an additional payload** on the beachhead host, and then **19) executed a service on the DC**, after no command and control traffic was apparent.

At this point, **20) C2 connections appear on the domain controller**. **21) Backup systems were targeted for lateral movement using the SMB exe** executed around one hour after the first lateral movement execution from the beachhead host. The threat actor was **22) having issues running beacons on numerous systems**, and on at least one of the systems, **23) they mounted the drive remotely.**

GAMAYAN'S RESPONSE
Gamayan monitors all host activity, like new processes, file writes, file reads and checks all network traffic, from files to host-based threat intelligence. All remote connections and failed payloads are instantly flagged and activate Gamayan defence features. Gamayan easily detects the attacker checking for MS17-010.

Quick Note:
MS17-010 is an old SMB exploit, if exploitation is attempted, this should always trigger alarms internally. One should also ask why is a backup server laterally moving through the network via SMB?

Exfiltration

24) Domain discovery (AdFind and Rubeus outputs) **25) exfiltrated by vsftpd**.

GAMAYAN'S RESPONSE
Gamayan monitors all network ingress and egress in real-time. Exfiltration via FTP is extremely easy to detect, and stop. In addition, such aggressive domain discovery linked to linked activity is a strong indicator of compromise.

Impact

26) SMB was used to transfer the Ryuk executables. Then, **27) RDP connections were made from the first compromised DC**, and then, ransomware executed throughout the environment, starting with the Backup servers. **28) On the backup server, prior to execution, the threat actors pulled up the wbadmin msc console**. The threat actors asked for more than $6 million.

Summary

This attack could have been detected and stopped at every stage, in fact, UHS had at least 28 opportunities to stop it. In some cases, each stage had multiple commands or failures that technically would count as yet another opportunity to detect and defend. The success of RYUK is due to UHS's lack of defence in depth applied to the organisation's operations, lack of monitoring and lack of detection and response capabilities.

Detecting RYUK

Gamayan rules robustly detect the most important activities. This is achieved with our software-based endpoint agent - no hardware or special equipment required.

- ET INFO Observed DNS Query for EmerDNS_TLD (.bazar)
- ETPRO POLICY Possibly Suspicious example.com SSL Cert
- ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex/Trickbot CnC)
- ETPRO TROJAN Observed Malicious SSL Cert (Cobalt Strike CnC)
- Feodo Tracker: potential TrickBot CNC Traffic_detected
- ET NETBIOS DCERPC SVCCTL - Remote Service Control Manager Access
- ET POLICY SMB2 NT Create AndX Request For a DLL File - Possible Lateral Movement
- ET POLICY SMB2 NT Create AndX Request For an Executable File
- ET POLICY SMB2 NT Create AndX Request For an Executable File In a Temp Directory
- ET POLICY RunDll Request Over SMB - Likely Lateral Movement
- GPL NETBIOS SMB-DS IPC$ share access
- ET CNC Feodo Tracker Reported CnC Server TCP group 15
- ET EXPLOIT Possible ETERNALBLUE Probe MS17-010 (Generic Flags)
- ET EXPLOIT Possible ETERNALBLUE Probe MS17-010 (MSF style)
- ET POLICY Command Shell Activity Over SMB - Possible Lateral Movement