DETECTION AND RESPONSE GAME

INITIAL ACCESS

DETECTION AND RESPONSE GAME

INITIAL ACCESS

DETECTION AND RESPONSE GAME

PRIVILEGE ESCALATION

DETECTION AND RESPONSE GAME

DEFENSE EVASION

DETECTION AND RESPONSE GAME

DISCOVERY

DETECTION AND RESPONSE GAME

LATERAL MOVEMENT

DETECTION AND RESPONSE GAME

COMMAND AND CONTROL

DETECTION AND RESPONSE GAME

IMPACT

SPEARPHISHING

Ryuk send a spear phishing email leading to a Bazar Loader malware executable.

- From SendGrid email marketing platform
- Decoy google preview page
- Certificate signing to evad anti-virus
- Downloads encrypted BazarBackdoor

BAZAR

Ryuk uses Bazar a malware downloader and backdoor to deploy additional malware, including ransomware and to steal sensitive data.

- Relies on user execution
- Injects malicious code into cmd, explorer, and svchost
- Creates autorun entries
- Download and execute the BazarBackdoor and Cobalt Strike beacons

CVE-2020-1472

Ryuk establishes a vulnerable Netlogon secure channel connection to a domain controller, using the Netlogon Remote Protocol to reset the credentials on the domain controllers.

- Unauthenticated attacker requires MS-NRPC and a TCP Connection to the DC
- Takes advantage of incorrect AES mode

RUNDLL32

Ryuk abuses rundll32.exe to proxy execution malicious code on the Domain Controller.

- Signed Binary Proxy Execution
- May avoid triggering security tools because of allowlists or false positives from normal operations

ACTIVE DIRECTORY

Ryuk used cmd, Powersell and ADFind to collect information about the Activ Directory Evironment.

- Host names
- Operating systems
- Last logon dates
- Domain Trusts
- Domain Admins
- User- und Computernames

REMOTE SERVICES

Ryuk used a valid domain administrator account to log into a service specifically designed to accept remote connections, such as telnet, SSH, and VNC to transfer data undetected.

- An executable was transferred to the DC via SMB
- RDP was used to distribute a ransomware payload enterprise wide

BAZARBACKDOOR & COBALT STRIKE

Ryuk used Bazarbackdoor and Cobalt Strike to exfiltrate network data to several domains and to control the network.

- Report_Print.exe
- 3.137.182.114:443
- cstr3.com
- servisses.exe
- 88.119.171.94:443

RYUK EXECUTABLE

Ryuk executes Ransomware - a type of malware that encrypts files of the victim and restores access in exchange for a ransom payment

- Lowest observed ransom was for 1.7 BTC and the highest was for 99 BTC