

**INITIAL ACCESS**



**DEFENSE EVASION**



**PRIVILEGE ESCALATION**



**INITIAL ACCESS**



**INITIAL ACCESS**



**INITIAL ACCESS**



**INITIAL ACCESS**



**INITIAL ACCESS**



**COMMAND AND CONTROL**



**LATERAL MOVEMENT**



**DISCOVERY**



**IMPACT**

**RUNDLL32**

The 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

**BAZAR**

Ryuk uses Bazar. a downloader and backdoor malware 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 in the environment

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

**SPEARPHISHING**

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

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



**INITIAL ACCESS**



**INITIAL ACCESS**



**INITIAL ACCESS**



**INITIAL ACCESS**

**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

**RUNDLL32**

The hacker uses traffic mirroring to exfiltrate data over an already compromised network.

MITIGATION

Encrypt sensitive information

DETECTION

Monitor network traffic for uncommon data flows

**TRAFFIC DUPLICATION**

The hacker uses traffic mirroring to exfiltrate data over an already compromised network.

MITIGATION

Encrypt sensitive information

DETECTION

Monitor network traffic for uncommon data flows

**TRAFFIC DUPLICATION**

The hacker uses traffic mirroring to exfiltrate data over an already compromised network.

MITIGATION

Encrypt sensitive information

DETECTION

Monitor network traffic for uncommon data flows