2024-03-11

HUNTER

EMERGING THREATS

PHOBOS RANSOMWARE

The Phobos Ransomware variant has been active since May of 2019, targeting a variety of entities that include governments, emergency services, critical infrastructure, education and public healthcare. Operating under a RaaS (Ransomware-as-a-Service) model, this ransomware variant has been responsible for the extortion of millions of dollars from victims targeted. Since it was first observed, there have been multiple variants that spun from Phobos; Eking, Eight, Elbie, Devos, Faust, and Backmydata - with Cisco Talos relaying in 2023, that the actors utilizing 8Base ransomware were exploiting a variant of Phobos in their attacks. Known for implementing a variety of initial access vectors, such as phishing campaigns to deliver payloads like SmokeLoader (used to deliver payloads) and exploiting exposed Remote Desktop Protocol (RDP) services through brute-force attacks - eventually leading to the encryption of files below a file size threshold (1.5MB) and partially encrypting any that are above that in order to shorten the time it takes for the encryption stage to complete. On February 2024, CISA, FBI and MS-ISAC released an advisory on Phobos Ransomware as part of an effort against Ransomware variants and to better equip organizations that may be susceptible to infection. Due to the multiple variants that are by-product(s) of Phobos Ransomware, and the very recent advisory from government entities; it is pertinent that an organization understands and prepares for this threat in order to safeguard assets.

CYBORG SECURITY

THREAT SUMMARY

The Phobos Ransomware variant has been active since May of 2019, targeting a variety of entities that include governments, emergency services, critical infrastructure, education and public healthcare. Operating under a RaaS (Ransomware-as-a-Service) model, this ransomware variant has been responsible for the extortion of millions of dollars from victims targeted. Since it was first observed, there have been multiple variants that spun from Phobos; Eking, Eight, Elbie, Devos, Faust, and Backmydata - with Cisco Talos relaying in 2023, that the actors utilizing 8Base ransomware were exploiting a variant of Phobos in their attacks. Known for implementing a variety of initial access vectors, such as phishing campaigns to deliver payloads like SmokeLoader (used to deliver payloads) and exploiting exposed Remote Desktop Protocol (RDP) services through brute-force attacks - eventually leading to the encryption of files below a file size threshold (1.5MB) and partially encrypting any that are above that in order to shorten the time it takes for the encryption stage to complete. On February 2024, CISA, FBI and MS-ISAC released an advisory on Phobos Ransomware as part of an effort against Ransomware variants and to better equip organizations that may be susceptible to infection. Due to the multiple variants that are by-product(s) of Phobos Ransomware, and the very recent advisory from government entities; it is pertinent that an organization understands and prepares for this threat in order to safeguard assets.

SYNOPSIS

Phobos Ransomware operates under a RaaS model, meaning the possibility of widespread distribution is high - this can be exemplified with observed connection(s) to multiple variants like Eking, Eight, Elbie, Devos, Faust, and Backmydata. The variant employs TTPs (Tactics, Techniques, and Procedures) that begin with phishing attacks that are used to deliver payloads via droppers like SmokeLoader (backdoor trojan) embedded in malicious attachments - additionally, initial access has been achieved by exploiting exposed RDP services via brute-force attacks.

After initial access is obtained, actors abuse legitimate executables such as lsass.exe or cmd.exe to deploy additional payloads with elevated privileges; as well as to abuse typically harmless windows functionalities. Phobos capabilities also include the usage of a three phase process to decrypt the ransomware payload via SmokeLoader. The first phase has been observed to manipulate VirtualAlloc or VirtualProtect API functions to reveal where the the next stage of decryption will be, or the entry point. The following stage includes the calling of this entry point to a memory container (during this time it produces requests to legitimate websites in an attempt to hide behind the activity produced). Then the third and final stage is when the unpacked binary is pulled from the memory and the payload is delivered.

Discovery takes place when Phobos enumerates connected storage devices, and processes - and is also capable of scanning for network shares. In order to evade detection, the variant abuses process injection techniques, and makes modifications to the system's security/firewall configurations. Abusing startup folders and Run Registry keys to maintain persistence has been observed, as well as the disabling of system recovery and backup options (i.e. shadow copies). It is also important to note that Credential dumping and active directory enumeration has been observed via tools such as Bloodhound and Mimikatz - as well as instances of UAC bypass discovered by Talos researchers, occurring with the exploitation of a vulnerability in the .Net Profiler DLL loading process.

Subsequently, Phobos actors use WinSCP and/or Mega.io for file exfiltration before the encryption of data across local and network drives begins. The encryption of files below a file size threshold (1.5MB) and the partial encryption of any that are above that in file size has been observed to shorten the time it takes for the encryption stage to reach completion. As typical with other ransomware variants, a ransom note is produced on the victim's system - extorting the victim in order to receive decryption keys.

HUNT PACKAGES

AUTORUN OR ASEP REGISTRY KEY MODIFICATION
https://hunter.cyborgsecurity.io/research/hunt-package/8289e2ad-bc74-4ae3-bfaa-cdeb4335135c

WINDOWS MANAGEMENT INSTRUMENTATION (WMI) CALL TO DELETE SHADOWCOPY VIA WMIC COMMAND
https://hunter.cyborgsecurity.io/research/hunt-package/f047c78d-d761-4e34-b4fd-fc1902e4f8b1

DELETE SYSTEM CATALOG
https://hunter.cyborgsecurity.io/research/hunt-package/a92f18ea-a1fd-45c9-a6fa-4e9169aca14a

FILE CREATED IN STARTUP FOLDER
https://hunter.cyborgsecurity.io/research/hunt-package/8fedb48c-396b-4cd5-9483-69d7fc3eecee

SHADOW COPIES DELETION USING OPERATING SYSTEMS UTILITIES
https://hunter.cyborgsecurity.io/research/hunt-package/2e3e9910-70c1-4822-804a-ee9919b0c419

RELATED LINKS
Sign up for free HUNTER access
Phobos Ransomware Emerging Threat Collection

MITRE CONTEXT

- Tactic Names:
  - Persistence
  - Privilege Escalation
  - Execution
  - Impact
- Technique Names:
  - Registry Run Keys / Startup Folder
  - Windows Management Instrumentation
  - Inhibit System Recovery
- Threat Names:
  - Phobos Ransomware

REFERENCES

1. https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-060a
2. https://www.malwarebytes.com/blog/news/2019/07/a-deep-dive-into-phobos-ransomware
3. https://blog.talosintelligence.com/deep-dive-into-phobos-ransomware/
4. https://thehackernews.com/2024/03/phobos-ransomware-aggressively.html#:~:text=%22Structured%20as%20a%20ransomware%2Das,dollars%2C%22%20the%20government%20said.