LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS
HHS CYBERSECURITY PROGRAM
OFFICE OF INFORMATION SECURITY

HC3: Analyst Note

July 7, 2021 TLP: White Report: 202107071200

Overview of Phobos Ransomware

Executive Summary

Phobos ransomware first surfaced in late 2017 with many researchers quickly discovering links between Phobos and the Dharma and CrySiS ransomware variants. The Phobos ransomware operators are known to primarily target small- to medium-sized businesses (including healthcare entities such as hospitals) and typically demand lower ransom amounts compared to other ransomware families. Phobos proved to be one of the most prevalent ransomware families throughout 2019 and 2020. The capabilities of Phobos ransomware continue to evolve, with new variants making the ransomware more difficult to detect, identified as recently as April 2021. Basic mitigations include securing Remote Desktop Protocol (RDP), strong password and account lockout policies, enforcing multi-factor authentication, enforcing virtual private networks, disaster recovery strategies, and keeping software updated.

Report

At its inception in 2017, Phobos was being distributed by the Dharma ransomware operators. Phobos likely served as an insurance policy for malicious campaigns, providing affiliates with a second option for conducting attacks should Dharma end up being decrypted, according to ZDNet. In 2019, researchers at Malwarebytes concluded that there were significant similarities between Phobos and Dharma ransomware, suggesting the same developers were responsible for their creation. Phobos also contains elements of CrySiS ransomware (which is also related to Dharma) with anti-virus software often detecting Phobos as CrySiS. Phobos has served as the foundation for later variants, including Eking, discovered in October 2020, and Fair, detected in March 2021. In this most recent variant, developers added new fileless and evasive techniques.

Given the considerable effort by the ransomware developers to add new defense evasion capabilities and footprint reduction in the recent Fair variant of Phobos ransomware, researchers suggest that the operators behind Phobos are likely more focused on cyber espionage while attempting to increase their foothold in enterprise businesses. In one case, the threat actors maintained persistence in a company's network for eight months while remaining undetected. One of the more significant recent updates to Phobos ransomware is a lower scope of encryption in which the Phobos developers removed the UAC requirement to maintain medium integrity. This means no encryption of privileged folders, which leads to a lower footprint. While there are fewer files to encrypt, Phobos's developers did not want to compromise on files with open handles, which most likely will have a significant impact on the victims. Additionally, in December 2020, researchers discovered a variant of Agent Tesla (aka Negasteal) that used the paste site "hastebin[.]com" for the fileless delivery of the CrySiS ransomware. CrySiS and Dharma are both known to be related to Phobos ransomware. There is also a clear indication that Phobos ransomware targets servers versus workstations as some of the malware's commands are only relevant to servers.

Like Dharma, Phobos ransom notes do not demand a specific amount, but rather instruct victims to email the Ransomware as a Service operators to discuss pricing. Sources differ on the average ransomware payment for Phobos, with Coveware placing it at approximately $38,100 as of May 2021, Unit 42 identifying it as $13,955 in 2020, and Advanced Intelligence claiming the average ransom is between $5,000 and $6,000 in Bitcoin. Advanced Intelligence also reports that the ransom amount is increased by $3,000 if the initial ransom demand is ignored. Additionally the average amount of time from reporting to full data recovery of a Phobos Ransomware incident was 16 days compared to an average of 19 days for all ransomware variants, according to Coveware. The recovery period is usually quicker since most victims have small networks with just a few endpoints.

Common infection vectors for Phobos ransomware include distribution from malicious attachments via phishing, open and poorly secured Remote Desktop Protocol (RDP) connections, brute force techniques to obtain RDP credentials, leveraging stolen or illegally purchased RDP credentials, common security misconfigurations, and via insecure connections on ports 338 and 3389, which are legitimate protocols used to access servers remotely.

Palo Alto Networks has observed Phobos ransomware attacks on victims in various industries including healthcare, with the threat actors mainly targeting small- to medium-sized businesses. In September 2019, an attack by the Dharma/CrySiS ransomware on a hospital in Texas resulted in the encryption of many of the hospital's records containing patient information and medical data. In June 2019, at least four hospitals in Romania were hit by ransomware in attacks the Romanian Intelligence Service said it suspected were launched by Chinese hackers. A further investigation carried out by specialists from CERT-RO, Cyberint, and Bitdefender indicated that the hospitals were attacked with Maoloa and Phobos ransomware.

Mitigations

Malwarebytes recommends that both consumers and IT administrators take the following actions to secure and mitigate against Phobos ransomware attacks:

- Set your RDP server, which is built in the Windows OS, to deny public IPs access to TCP ports 3389 and 338, the default ports Windows Remote Desktop listens to. If you or your organizations have no need for RDP, better to disable the service altogether. Critical systems or systems with sensitive information should not have RDP enabled.
- Along with RDP port blocking, Malwarebytes also suggests the blocking of TCP port 445, the default port a Server Message Block (SMB) uses to communicate in a Windows-based LAN at the network perimeter. Note that you or your organization may have to do in-depth testing to see how your system and/or programs are impacted by this block. As a rule of thumb, block all unused ports.
- Allow RDP access to IP addresses that are under you or your organization's control.
- Enable the logging of RDP access attempts and review them regularly to detect instances of potential intrusion.
- Enforce the use of strong passwords and account lockout policies for Active Directory domains and local Windows accounts.
- Enforce multi-factor authentication (MFA) to RDP and local account logons whenever possible.
- Enforce the use of a virtual private networks if your organization allows employees to work remotely.
- Come up with and implement a sound backup strategy.
- Maintain an inventory of running services and applications on your system and review it regularly. For critical systems, it's best to have an active monitoring and alerting scheme in place.
- Have a disaster recovery scheme in place in case of a successful breach via RDP happens.
- Keep all your software, including OS and anti-malware, up to date.

Additionally, CISA recently released a new module in its Cyber Security Evaluation Tool (CSET): the Ransomware Readiness Assessment (RRA). CSET is a desktop software tool that guides network defenders through a step-by-step process to evaluate their cybersecurity practices on their networks. CSET—applicable to both information technology (IT) and industrial control system (ICS) networks—enables users to perform a comprehensive evaluation of their cybersecurity posture using many recognized government and industry standards and recommendations. CISA strongly encourages all organizations to take the CSET Ransomware Readiness Assessment, available at: https://github.com/cisagov/cset/.

Furthermore, the following indicators of compromise (IOCs) associated with Phobos ransomware were gathered by HC3 from various sources. The Description column includes a brief description of the IOC with the corresponding malware detection rate on VirusTotal (VT). The second column denotes the type of IOC and the third column provides the indicator of compromise. Lastly, the fourth column lists the date that each corresponding IOC was first seen or submitted to VirusTotal for analysis. It is important to note that this is by no means a comprehensive list of indicators. Some historical IOCs published by McAfee in August 2020 can be found here for reference: https://kc.mcafee.com/corporate/index?page=content&id=KB93202

Indicators of Compromise

Description (VT Score)	Type	Indicator of Compromise (IOC)	First Seen/ First Submission to VT
Lookfornewitguy (new Phobos variant) (56/70 on VT)	MD5	792b27b961ee8ae67855b952859053c7	4/26/2021
PowerShell script (12/58 on VT)	MD5	86e50a7bd09c2a5fc2eac716c29ea6c7	3/12/2021
Ransomware (fileless) (61/70 on VT)	MD5	6ad6c98f75c3133b94026c2fdd06a6f1	1/15/2021
Ransomware (on disk) (53/70 on VT)	MD5	d62a9ae1380402cc467cced405ba4aa0	3/8/2021
Loader (hollower) (10/86 on VT)	MD5	840d99c89f366505d06259a89273f8b1	4/17/2021
Executable (57/70 on VT)	MD5	4f25e57d4f754f0cea4f30d9da4156fd	6/25/2021
Sample (57/70 on VT)	MD5	373a7a21c65d50861b0f7fa81d998165	6/26/2021
GZIP (40/60 on VT)	MD5	90bfa1d3b743c1546a053a206e49cac6	6/28/2021
Win32 EXE (59/70 on VT)	MD5	4942b6f7a7b009cf5bb1ef7d31270b98	6/26/2021
Win32 EXE (53/69 on VT)	MD5	733035ba7c294dd365d2a9601b900b4a	6/13/2021
Win32 EXE (46/69 on VT)	MD5	471cb7869b9c4078717156e809e24001	6/14/2021
.eight (Phobos) (53/69 on VT)	MD5	719000d0db27119867daf91dd1e8a20b	6/13/2021
.help (Phobos) (53/69 on VT)	MD5	2ec9ad510241a00a53f3090af9899250	3/2/2021
Contact email addresses provided in ransom notes	Email address	cadillac.407[@]aol.com, OttoZimmerman[@]protonmail.ch, ofizducwe111988[@]aol.com, FobosAmerika[@]protonmail.ch, posiccimen1982[@]aol.com, kipp.swindlehurst[@]aol.com, lachneyorlachb[@]aol.com, abbott_wearing[@]aol.com, decryptyourfiles[@]firemail.cc, 1decryption1[@]protonmail.com	5/12/2021
Serving IP for hxxps://paste[.]ee/r/1q1gD	IPv4	104.26.5[.]223	4/2/2021
Serving IP for hxxps://paste[.]ee/r/OwAyf	IPv4	104.26.4[.]223	3/30/2021
Ransomware (fileless) (12/86 on VT)	URL	hxxps://paste[.]ee/r/1q1gD	4/2/2021
Loader (hollower) (10/86 on VT)	URL	hxxps://paste[.]ee/r/OwAyf	3/30/2021
Outgoing link for hxxps://paste[.]ee/r/OwAyf	URL	hxxps://www.patreon[.]com/ccatss	3/30/2021

Analyst Comment

Recent efforts by the ransomware developers to evade detection, coupled with the ransomware operators' targeting of small- to medium-sized businesses, make this a serious cyber threat to take into consideration, especially for healthcare entities with legacy systems that support critical, 24/7 operations.

The Phobos ransomware uses AES encryption and adds several extensions to infected files. Phobos is known to encrypt files with at least 53 different extensions identified to date. Some recently observed extensions include Eight, Eking, and Help. It is highly likely that Phobos ransomware will continue to develop new variants with novel file extensions for encryption.

References

Camacho, Matt. "Negasteal Uses Hastebin for Fileless Delivery of Crysis Ransomware," Trend Micro. December 18, 2020. https://www.trendmicro.com/vinfo/my/security/news/cybercrime-and-digital-threats/negasteal-uses-hastebin-for-fileless-delivery-of-crysis-ransomware

Coveware. "Phobos Ransomware Recovery, Payment & Decryption Statistics," Coveware. Accessed June 30, 2021. https://www.coveware.com/phobos-ransomware-payment

Coveware. "Phobos Ransomware, A Combo of CrySiS and Dharma," Coveware. January 18, 2019. https://www.coveware.com/blog/phobos-ransomware-distributed-dharma-crew

Deep Instinct. "The Hasty Agent: Agent Tesla Attack Uses Hastebin," Deep Instinct. October 29, 2020. https://www.deepinstinct.com/2020/10/29/the-hasty-agent-agent-tesla-attack-uses-hastebin/

Dnwls07219. "Social media post by @fbgwls245: New Variant #Phobos #Ransomware," Twitter. September 29, 2020. https://twitter.com/fbgwls245/status/1310891675724570624

Emsisoft Malware Lab. "Ransomware statistics for 2020: Year in summary," Emsisoft. March 19, 2021. https://blog.emsisoft.com/en/38259/ransomware-statistics-for-2020-year-in-summary/

GoldSparrow. "Phobos Ransomware," EnigmaSoft. April 2019. https://www.enigmasoftware.com/phobosransomware-removal/

Gorelik, Michael. "The 'Fair' Upgrade Variant of Phobos Ransomware," Morphisec. April 2, 2021. https://blog.morphisec.com/the-fair-upgrade-variant-of-phobos-ransomware

Gillespie, Michael. "Social media post by @demonslay335," Twitter. January 8, 2019. https://twitter.com/demonslay335/status/1082699473950834688

Hasherezade. "A deep dive into Phobos ransomware," Malwarebytes. July 24, 2019. https://blog.malwarebytes.com/threat-analysis/2019/07/a-deep-dive-into-phobos-ransomware/

McAfee, "MVISION Insights: Phobos Ransomware," McAfee Knowledge Center. August 4,2020. https://kc.mcafee.com/corporate/index?page=content&id=KB93202

Osborne, Charlie. "Texas hospital becomes victim of Dharma ransomware," ZDNet. November 19, 2018. https://www.zdnet.com/article/texas-hospital-becomes-victim-of-ransomware-patient-data-potentially-leaked/
Palmer, Danny. "New Phobos ransomware exploits weak security to hit targets around the world," ZDNet. January 21, 2019. https://www.zdnet.com/article/new-phobos-ransomware-exploits-weak-security-to-hit-targets-around-the-

world/

Petcu, Alina Georgiana. "Phobos Ransomware: Everything You Need to Know and More," Heimdal Security. December 17, 2020. https://heimdalsecurity.com/blog/phobos-ransomware/

Postelnicu, Leontina. "Ransomware hits Romanian hospitals, disrupts operations," Healthcare IT News. June 27, 2019. https://www.healthcareitnews.com/news/emea/ransomware-hits-romanian-hospitals-disrupts-operations

Rauluar, "Phobos Ransomware (<ID>-<id***>.[<email>].phobos, .Adame, .help) Support," December 20, 2018 https://www.bleepingcomputer.com/forums/t/688649/phobos-ransomware-id-idemailphobos-adame-help-support/

RedBeardIOCs. "Phobos Ransomware IOCs," Twitter. https://twitter.com/RedBeardIOCs

Schwartz, Mathew J. "Ransomware Attacks: STOP, Dharma, Phobos Dominate," Bank Info Security. October 16, 2019. https://www.bankinfosecurity.com/ransomware-attacks-stop-dharma-phobos-dominate-a-13259

Sullivan, Bridgit. "Inside "Phobos" Ransomware: "Dharma" Past & Underground," Advanced Intelligence. August 11, 2020. https://www.advanced-intel.com/post/inside-phobos-ransomware-dharma-past-underground

Tetra Defense, "Phobos Ransomware: What To Do If You're Infected," Tetra Defense. Accessed July 1, 2021. https://www.tetradefense.com/incident-response-services/phobos-ransomware-what-to-do-if-youre-infected/

Toulas, Bill. "The ‘Phobos’ Ransomware Is Getting a Stealth-Boosting Upgrade," Technadu. April 3, 2021. https://www.technadu.com/phobos-ransomware-getting-stealth-boosting-upgrade/261640/

Umawing, Jovi. "Threat spotlight: Phobos ransomware lives up to its name," Malwarebytes. August 10, 2020. https://blog.malwarebytes.com/threat-spotlight/2020/01/threat-spotlight-phobos-ransomware-lives-up-to-its-name/

Unit 42. "Ransomware Threat Assessments: A Companion to the 2021 Unit 42 Ransomware Threat Report," Palo Alto Networks. March 17, 2021. https://unit42.paloaltonetworks.com/ransomware-threat-assessments/5/

VirusTotal, "Submission for '62d67fe5548da330b0074f8fd162833e2675f8973899ae5778c10ef33a3f06af'," VirusTotal. July 25, 2020. https://www.virustotal.com/gui/file/62d67fe5548da330b0074f8fd162833e2675f8973899ae5778c10ef33a3f06af/detection

Zhang, Xiaopeng. "Deep Analysis – The EKING Variant of Phobos Ransomware," Fortinet. October 13, 2020. https://www.fortinet.com/blog/threat-research/deep-analysis-the-eking-variant-of-phobos-ransomware

Zhang, Xiaopeng. “[AVAR 2020] Pay or Lose Your Critical Data - Deep Analysis of A Variant of Phobos Ransomware,” FortiGuard Labs. December 3, 2020. https://www.fortiguard.com/events/3760/avar-2020-pay-or-lose-your-critical-data-deep-analysis-of-a-variant-of-phobos-ransomware

We want to know how satisfied you are with our products. Your answers will be anonymous, and we will use the responses to improve all our future updates, features, and new products. Share Your Feedback