Phobos - Cyber Threat Intelligence

April 2024

Author(s): Nkata Sekonya, Daryl Nyawasha

April 2, 2024

Cybercom (part of the Cyanre Family of Companies) has collected, reviewed, and analyzed tactics, techniques, and procedures (TTP) gathered from internal incident response cases and open-source threat intelligence. Through the examination of the datasets on hand, it was possible to document consistent TTPs associated with the threat actors behind the Phobos Ransomware, hereafter referred to as the Phobos ransomware operators.

The associated research output can be utilized to refine detection capabilities and raise expertise among internal security operation teams and incident responders who may encounter variants of the Phobos Ransomware .

1 Summary

This advisory provides an overview of the Tactics, Techniques, and Procedures (TTPs) with the MITRE ATT&CK® framework [1] employed in cyber intrusions involving the deployment of the Phobos ransomware. The research findings can be effectively utilized to refine detection capabilities and elevate the expertise of internal security operations teams and incident responders. This is particularly beneficial since ransomware operators often maintain consistent TTPs, repeating the same processes.

The Phobos ransomware exhibits similarities with variants belonging to the Dharma (CrySiS) ransomware family, as the TTPs observed in cyber intrusions where Phobos ransomware was deployed are consistent with those seen in deployments of the Dharma ransomware.

[1] https://attack.mitre.org/

As highlighted by BlackBerry Research & Intelligence Team, Phobos predominantly targets small to medium-sized organizations across various industries. Noteworthy is the operators' tendency to demand lower ransom payments compared to other ransomware families. This advisory aims to equip organizations with valuable insights to fortify their defenses against the distinctive characteristics associated with Phobos ransomware incidents.

Modus Operandi

The Phobos ransomware operators gain access to victim systems by compromising Remote Desktop Protocol (RDP) credentials, obtained through either brute-force attacks or purchases on cybercriminal forums. Utilizing a combination of publicly available and custom-developed tools, they disable host-based security systems to operate undetected.

After establishing a foothold, the operators employ network scanning utilities to identify high-value systems and potential lateral movement pathways. Mimikatz [2] is used for extracting credentials, enabling remote desktop connections to extend their activities within the compromised environment. Ultimately, the operators deploy Phobos ransomware, leading to ransom notes guiding victims on file recovery steps. Below is an indication of the TTPs with the MITRE ATT&CK® framework that the opertors employ.

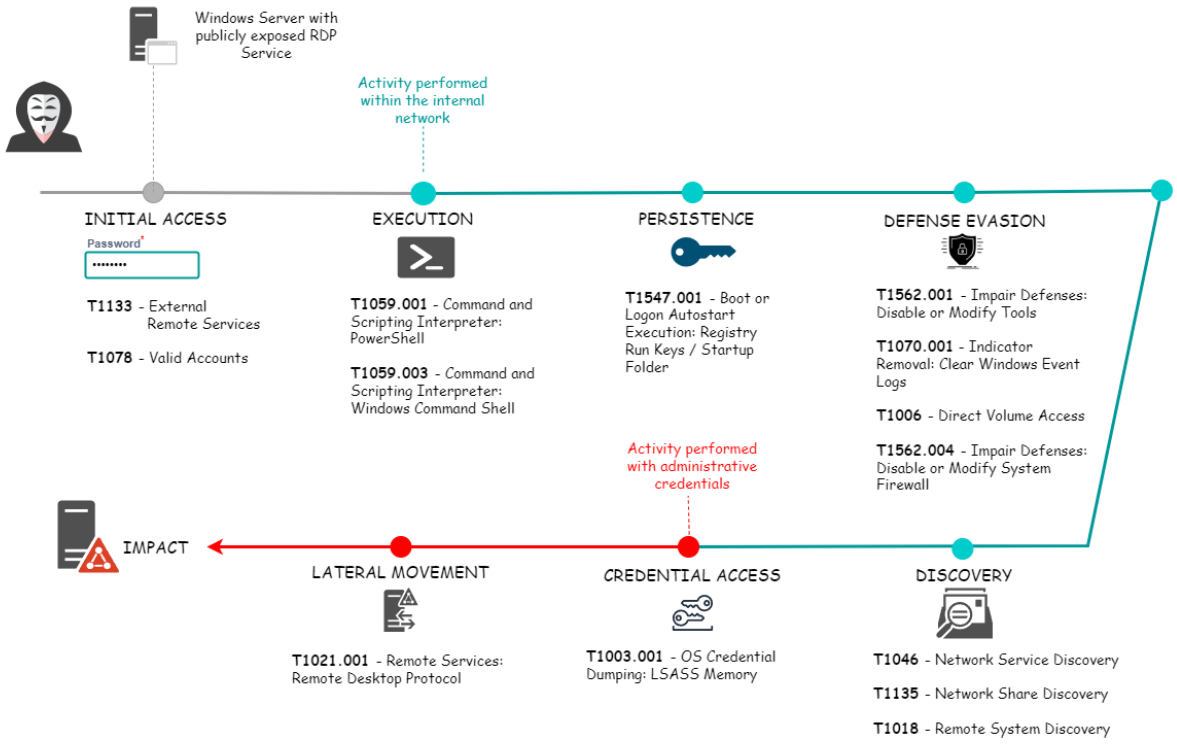
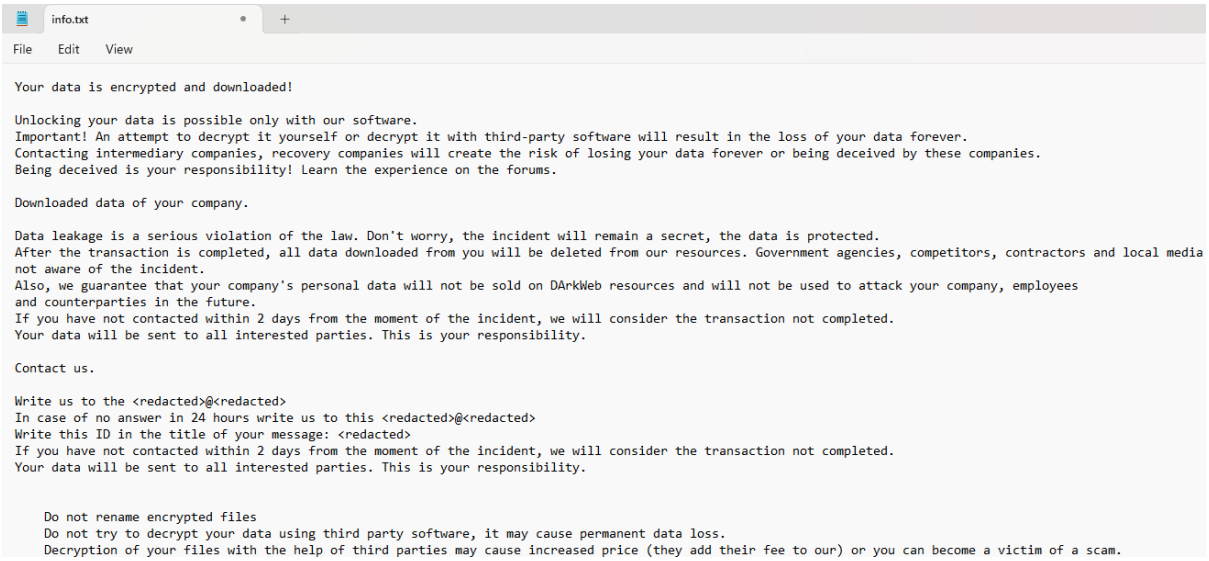


Figure 1: Phobos Ransomware Operator

At this point, the threat actors engage in extortion, placing organizations that lack effective recovery policies at risk of losing access to their data unless the ransom is paid. Organizations are advised to review the recommendations section to explore measures that can be taken to safeguard against this threat actor group.

[2] https://www.sentinelone.com/cybersecurity-101/mimikatz/

The ransomware creates two distinct types of ransom notes; one in `.txt` format and another in `.hta` format conatining the content below:


info.txt

File Edit View

Your data is encrypted and downloaded!

Unlocking your data is possible only with our software.
Important! An attempt to decrypt it yourself or decrypt it with third-party software will result in the loss of your data forever.
Contacting intermediary companies, recovery companies will create the risk of losing your data forever or being deceived by these companies.
Being deceived is your responsibility! Learn the experience on the forums.

Downloaded data of your company.

Data leakage is a serious violation of the law. Don't worry, the incident will remain a secret, the data is protected.
After the transaction is completed, all data downloaded from you will be deleted from our resources. Government agencies, competitors, contractors and local media not aware of the incident.
Also, we guarantee that your company's personal data will not be sold on DArkWeb resources and will not be used to attack your company, employees and counterparties in the future.
If you have not contacted within 2 days from the moment of the incident, we will consider the transaction not completed.
Your data will be sent to all interested parties. This is your responsibility.

Contact us.

Write us to the <redacted>@<redacted>
In case of no answer in 24 hours write us to this <redacted>@<redacted>
Write this ID in the title of your message: <redacted>
If you have not contacted within 2 days from the moment of the incident, we will consider the transaction not completed.
Your data will be sent to all interested parties. This is your responsibility.

Do not rename encrypted files
Do not try to decrypt your data using third party software, it may cause permanent data loss.
Decryption of your files with the help of third parties may cause increased price (they add their fee to our) or you can become a victim of a scam.

Figure 2: Ransomware Note (info.txt)

2 Technical Details

The Phobos ransomware represents a strain within the `Dharma (CrySiS)` ransomware family. Operators behind Phobos consistently employ techniques reminiscent of those used by Dharma operators. In this section, we delineate these techniques and align them with the MITRE ATT&CK® Framework Version 13. Organizations are strongly advised to leverage this mapping to evaluate the effectiveness of their existing security controls in detecting the threat actor activity described below.

The provided table correlates the observed TTPs with the MITRE ATT&CK® framework. Organizations can utilize this reference to assess the effectiveness of their existing security measures in identifying and mitigating such activities. In cases where deficiencies are identified, organizations should consider implementing additional security controls. The recommendations section offers guidance on enhancing security measures.

Tactic	ID	Technique(s)
Initial Access	T1133 T1078	External Remote Services, Valid Accounts
Execution	T1059.001 T1059.003	Command and Scripting Interpreter: PowerShell Command and Scripting Interpreter: Windows Command Shell
Persistence	T1547.001	Boot or Logon Autostart Execution: Registry Keys / Startup Folder

Tactic	ID	Technique(s)
Defense Evasion	T1562.001 T1070.001 T1006 T1562.004	Impair Defenses: Disable or Modify Tools Indicator Removal: Clear Windows Event Logs Direct Volume Access Impair Defenses: Disable or Modify System Firewall
Discovery	T1046 T1135 T1018	Network Service Discovery Network Share Discovery Remote System Discovery
Credential Access	T1003.001	OS Credential Dumping: LSASS Memory
Lateral Movement	T1021.001	Remote Services: Remote Desktop Protocol
Impact	T1486	Data Encrypted for Impact

Table 1: Phobos Ransomware MITRE tactics and techniques

2.1 Initial Access

The Phobos ransomware operators gain access to the victim network through compromised Remote Desktop Protocol (RDP) credentials. These credentials are obtained through either brute-force attacks on RDP servers exposed to the public [T1133 - External Remote Services] or by leveraging initial access brokers [T1078 - Valid Accounts].

Mitigation

T1133 - External Remote Services

[M1035 - Limit Access to Resource Over Network] should be implemented to restrict remote access services from being publicly exposed, such a solution would require the client to be on a Virtual Private Netork (VPN), or restricted to predefined source IP address. Furthermore, [M1032 - Multi-factor Authentication] should be leveraged to limit an adversary's ability to utilize compromised credentials without an additional form of authentication.

2.2 Execution

In multiple incidents investigated by Cybercom, the operators of the Phobos ransomware were discovered using PowerShell ([T1059.001 - Command and Scripting Interpreter: PowerShell] and [T1059.003 - Command and Scripting Interpreter: Windows Command Shell]) to retrieve batch scripts from a deceitful news site (`https://ccbs[.]news`). Despite masquerading as a news platform, this website serves as a covert facade of a news forum with the header below.

Самые важные новости Кавказа и каспийско-черноморского региона

Translated "The most important news of the Caucasus and the Caspian-Black Sea region"

https://ccbs[.]news

The platform covers geopolitical advancements within the Caspian, Caucasus, and Black Sea region, thereby earning its designation as **CCBS**.

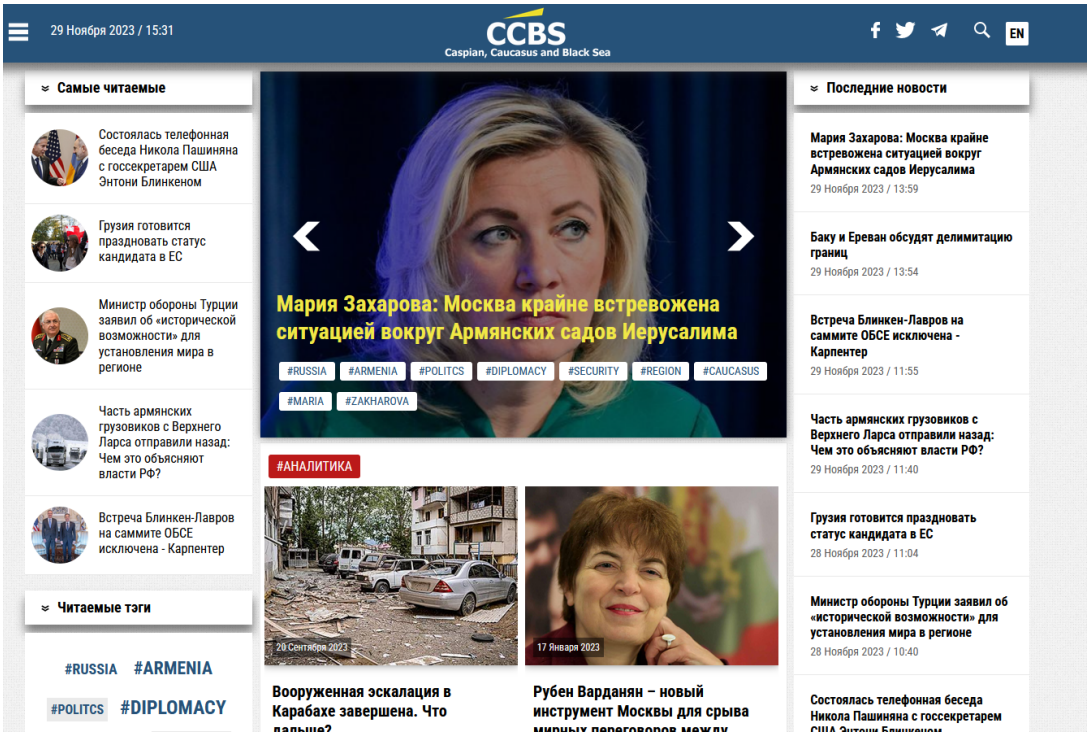


Figure 3: https://ccbs[.]news

The website offers comprehensive coverage of geopolitical developments across the transcontinental expanse from the Black Sea to the Caspian Sea. Encompassing nations like Russia, Georgia, Azerbaijan, Armenia, Turkey, and Iran (in the Caucasus region), it provides in-depth insights into this pivotal area's dynamics.

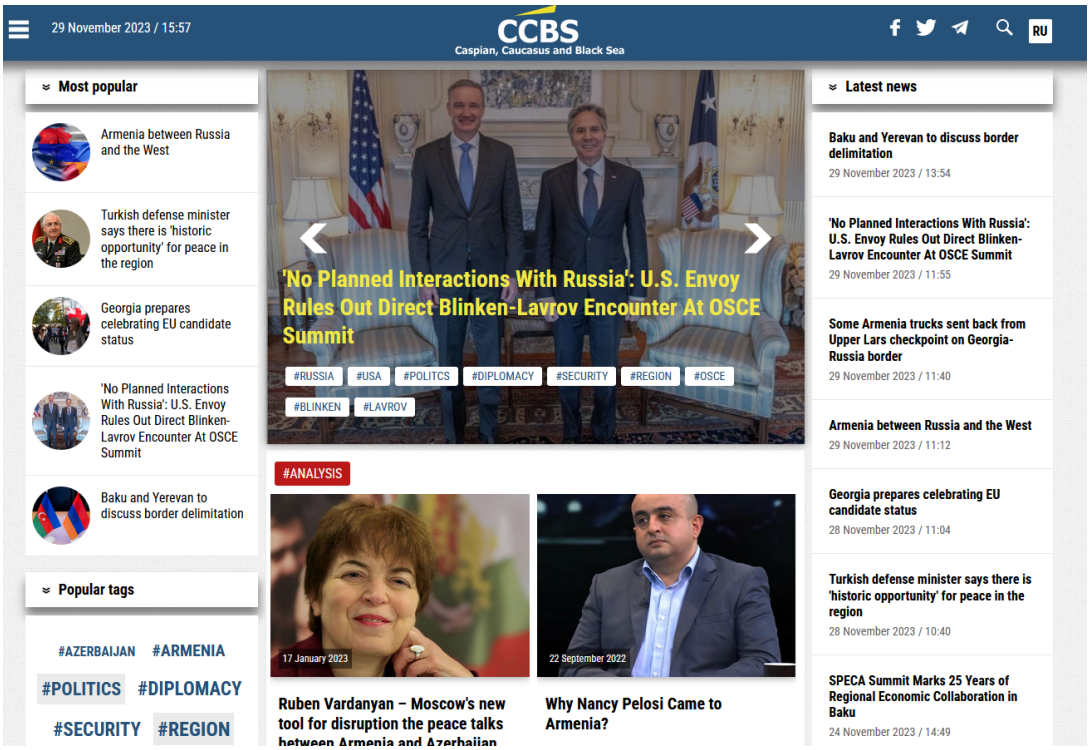


Figure 4: https://ccbs[.]news (Translated)

2.3 Persistence

Upon execution, Phobos ransomware initiates persistence mechanisms by creating entries in the registry's run keys and startup folders [T1547.001 - Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder]. The registry entries ensure that the ransomware will encrypt any new files added to the system whenever a user logs in or the system is booted.

It was found that this functionality and persistence is established directly through the ransomware upon execution.

Mitigation

T1547.001 - Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	Mitigating the persistence techniques associated with Boot or Logon Autostart Execution, specifically through Registry Run Keys and Startup Folder manipulation, poses a challenge for preventive controls. This difficulty arises due to the reliance on exploiting inherent system features, making it resistant to straightforward mitigation measures.

2.4 Defense Evasion

The operators behind Phobos ransomware employ `Process Hacker` to disable antivirus tools, as documented in [T1562.001 - Impair Defenses: Disable or Modify Tools]. Previous incidents reveal the operators' use of batch scripts to clear log files [T1070.001 - Indicator Removal: Clear Windows Event Logs].

Furthermore, the operators have been observed utilizing `IObit Unlocker`, a tool designed to unlock files in use by the operating system or other programs [T1006 - Direct Volume Access]. This enables the threat actors to manipulate files—copy, rename, delete, or move—circumventing Windows file access controls.

The ransomware, during execution, displays defense evasion capabilities by disabling the system firewall [T1562.004 - Impair Defenses: Disable or Modify System Firewall].

Mitigation

T1562.001 - Impair Defenses: Disable or Modify Tools	[M1038 - Execution Prevention] and application control should be diligently implemented, particularly in relation to the execution of tools outside the organization's security policies, such as those intended for rootkit removal, that adversaries may exploit to compromise system defenses. It is crucial to enforce the usage of only approved security applications on enterprise systems. Additionally, consider leveraging [M1022 - Restrict File and Directory Permissions] to establish and maintain appropriate process and file permissions, thus thwarting adversaries' attempts to disable or interfere with services.
T1070.001 - Indicator Removal: Clear Windows Event Logs	[M1029 - Remote Data Storage] should be implemented to facilitate the automatic forwarding of events to a log server or data repository. This mitigates the risk of adversaries locating and manipulating data.

T1006 - Direct Volume Access	[M1040 - Behavior Prevention on Endpoint] is a valuable mitigation strategy provided by specific security solutions.
T1562.004 - Impair Defenses: Disable or Modify System Firewall	Regularly [M1047 - Audit] account role permissions to confirm that only authorized users and roles possess the capability to modify system firewalls. Establish and maintain appropriate process and file permissions to prevent adversaries from tampering with or disabling firewall settings with non-administrative accounts.

2.5 Discovery

Upon establishing a foothold in the compromised environment, the operators engage in network discovery activities to enhance their understanding of the victim's network. Investigation evidence indicates the utilization of tools such as Advanced IP Scanner and NS v.2.exe for this purpose.

These network scanning utilities empower the operators to extract information about systems within the environment, identify network shares, pinpoint high-value systems, and identify potential pathways for lateral movement [T1046 - Network Service Discovery], [T1135 - Network Share Discovery], and [T1018 - Remote System Discovery].

Mitigation

T1046 - Network Service Discovery	[M1042 - Disable or Remove Feature or Program] provides an effective strategy to safeguard against the discovery and potential exploitation by ensuring the closure of unnecessary ports and services. Given that a significant aspect of discovery involves identifying and exploiting exposed services, the most robust defense lies in exposing only the essential and securing the exposed elements. Moreover, leveraging [M1031 - Network Intrusion Prevention (NIPS)] to detect and prevent remote service scans within the environment. Additionally, implementing [M1030 - Network Segmentation] can further enhance security by protecting critical servers and devices.
T1135 - Network Share Discovery	[M1028 - Operating System Configuration] can be leveraged to enable the Windows Group Policy below, to limit users who can enumerate network shares: `Do Not Allow Anonymous Enumeration of SAM Accounts and Shares`
T1018 - Remote System Discovery	Mitigating this type of attack technique proves challenging with preventive controls as it relies on the exploitation of inherent system features, making straightforward prevention difficult.

2.6 Credential Access

The Phobos ransomware operators use valid accounts for lateral movement through the network. To acquire these credentials, the operators utilize Mimikatz [T1003.001 - OS Credential Dumping: LSASS Memory]. Mimikatz is a program used to extract plaintexts passwords, password hashes and kerberos tickets from memory.

The operators of the ransomware family from which Phobos originated, Dharma ransomware, have been observed in the past using an attack path similar to the one detailed in this report, as detailed by a Zscaler ThreatLabZ report. Additionally, they employed NirSoft CredentialsFileView, a program designed to decrypt and display passwords and other data stored within Windows Credentials files.

Mitigation

T1003.001 - OS Credential Dumping: LSASS Memory

[M1043 - Credential Access Protection] can be used since Microsoft introduced enhanced security measures known as Credential Guard to safeguard Local Security Authority (LSA) secrets, mitigating the risk of credential theft through methods like credential dumping. However, it is not enabled by default and necessitates specific hardware and firmware prerequisites. It's important to note that while Credential Guard provides a substantial layer of protection, it does not cover all potential avenues of credential dumping.

Additionally, to enhance endpoint security and thwart credential theft, consider implementing [M1040 - Behavior Prevention on Endpoint]. This can be achieved by enabling Attack Surface Reduction (ASR) rules, specifically targeting LSASS to bolster protection against credential-stealing techniques.

2.7 Lateral Movement

With the compromised credentials at their disposal, the operators conduct lateral movement by establishing remote desktop connections to access other systems within the environment [T1021.001 - Remote Services: Remote Desktop Protocol].

Mitigation

T1021.001 - Remote Services: Remote Desktop Protocol

[M1032 - Multi-factor Authentication] should be configured for remote logins, as this adds an extra layer of security by requiring users to verify their identity through multiple means, such as passwords and one-time codes.

2.8 Impact

In executing their operational activities, the operators initiate the deployment of the Phobos ransomware through malicious tool designed to encrypt files on the victim's systems, as detailed in [T1486 - Data Encrypted for Impact].

The encrypted files are appended with an extension that takes the form:
`"<original name>.id[<victim ID>-<version ID>][<attacker e-mail>].<extension>"`

Before commencing the encryption process, the Phobos ransomware employs preemptive measures to obstruct system recovery. These preventive actions are achieved through specific commands, demonstrating distinct behavioral characteristics that contribute to the ransomware's efficacy in limiting attempts to restore the compromised systems. Below is an indication of the behaviour utilized to obstruct system recovery:

- **Deletion of Volume Shadow Copies (VSS) on the Windows System**

  Volume Shadow Copies are a built-in feature in Windows that allows users to create backups of files and system states. By deleting these copies, malware prevents users from restoring their files to a previous, unaffected state. This is especially crucial for ransomware, which aims to encrypt files and demand payment for their release. If victims can easily restore their files from backups, the ransomware attack loses its leverage.

  - `vssadmin delete shadows /all /quiet`
  - `wmic shadowcopy delete`

- **Prevention of Recovery Mode system boot**

  Recovery or Safe Mode is often used by users and system administrators to troubleshoot and remediate issues, including dealing with malware infections. By preventing the system from booting into recovery mode, the malware hinders attempts to identify and remove it from the system.

  - `bcdedit /set default bootstatuspolicy ignoreallfailures`
  - `bcdedit /set default recoveryenabled no`

- **Deletion of the Catalog of Backups on the Windows System**

  By deleting the catalog of backups, the malware erases the reference points that the operating system uses to identify and access backup copies of files and the system state. This makes it difficult for users and administrators to restore the system to a previous, clean state.

  - `wbadmin delete catalog -quiet`

- **Disabling of the Windows Firewall**

  Ransomware seeks to spread to other systems within the network. Disabling the firewall makes it easier for the malware to propagate by removing a barrier that might otherwise block its attempts to move laterally across the network.

  - `netsh advfirewall set currentprofile state off`
  - `netsh firewall set opmode mode=disable`

- **Establishment of Persistence Mechanisms**
  - `SOFTWARE\Microsoft\Windows\CurrentVersion\Run`
  - `.\Users\<User>\AppData\Roaming\Microsoft\Windows\Start Menu \Programs\Startup`
  - `.\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp`

3 Indicators of Compromise

Cybercom successfully retrieved the tools employed in an incident where the Phobos ransomware was deployed. This recovery has granted valuable insights into the objectives of the threat actors and the functionality of malicious scripts.

The following comprises a list of Indicators of Compromise (IoC) file names along with their corresponding hashes. This compilation serves as a resource to enhance detection capabilities within security monitoring solutions.

Table 2: Indicators of Compromise

#	File Names	SHA1
1	0.start.bat	b0c66d13e1eba2418c0d7cadc05dce0f475e9ec4
2	1.Automim.bat	c9a428aac16caeeac31818cdbc21d8c79df05da5
3	2.LaZagne_AIO.bat	160b4ea9dddc370d3fd45a6c482065d11d762bad
4	2.LaZagne_x86.bat	a4a21425e11ec31c199e95b775c5c01674b193be
5	3.Install_MimPassHunter.bat	422b7cf9729a24f1ecdf11663c9226064cc93550
6	3.UnInstall_MimPassHunter.bat	e89e560a4c9b60ad590026e20d67ef8407c66fb1
7	3.ViewPassKiwiSSP.bat	aa1df75428cb85399f64123f8136eafba127b4c4
8	3.ViewPassMimiLsa.bat	c0082c4e1a03030c8dbf8a2652df8c18f98ab16c
9	4.NirSOFT_x64v0.1.cmd	41fc40141bfa353f0c80f9af5ff5a9c73f1e34f0
10	auth.bat	2ce0b26ffa9a47595e79b69e8057bdd79e57ef5d
11	BulletsPassView.exe	08edc669c2a5408cdbc3968fc4ac0a2f23ed69ba
12	BulletsPassView64.exe	22544df33b80b9da3f91946cacb706805a5a992d
13	ChromePass.exe	a1be5f0c625a5da20d79b282d349c2c455c0e757
14	cmd_pass.exe	709e904b1c10289c406ed881007f896c7cb63877
15	coba.bat	d46c2ca57806c65e1c17e3287762e19c87205a21
16	CredentialsFileView.exe	fb7494e393557694af906c73658ed23137502ba7
17	CredentialsFileView64.exe	c300545976d9a91d1080de05c9bb6aa51599e4fb
18	DataProtectionDecryptor.exe	bc5440fff60f8c974a2ac0dcd53a61da61e9e17e
19	DataProtectionDecryptor64.exe	c41e0a60bcdd5afd410c141bb3dd3dea9f8313c5
20	DefenderControl2.exe	5da4de1dbba55774891497297396fd2e5c306cf5
21	defoff.bat	0ff136d72647e50ec60fbdb1a44ec8f36d1a851d
22	Dialupass.exe	bd48322845f8930e58e038dfd4e1e243e80a6b76

Table 2: Indicators of Compromise

#	File Names	SHA1
23	empv.exe	172b4e31ed15d1275ac07f3acbf499daf9a055d7
24	EncryptedRegView.exe	50fd38867cf5d0fd29efd7d42e61e26709d0f76d
25	EncryptedRegView64.exe	c8ce2908e4c9f3ad93bfa630fc34e440868f5aa7
26	ExtPassword.exe	f479b5859833b19aa4f5354ff0243ac91fb77a5d
27	finder.vbs	49c8a3e0246e0e65ed31b0379fab830a4d881b8f
28	fndr.vbs	411075ee805770e3f1e8297a64d4e87cfbf2bda6
29	iepv.exe	7e0e6900f4528e7dacb65ab1b1c107425d2a321b
30	ipall.bat	2f5991e67615763865b7e4c4c9558eb447ed7c0d
31	ipinfo.bat	723baea0983b283eebd8331025a52eb13d5daaa7
32	ipwho.bat	52f7e3437d83e964cb2fcc1175fad0611a12e26c
33	lazagne.bat	ea8c7ef120df284e35c7326272667aac233dcab7
34	lazagne.exe	fa2f281fd4009100b2293e120997bfd7feb10c16
35	laZagne_x86.exe	e94ab2b39f152bcae8261613796f98355e258262
36	lod.bat	fe89267c08b6277ee6a2407c4fa35a204ca0cc4f
37	logdel3.bat	2ea01333b3064cb767fd387c3cc00410af22d91a
38	LSADowngrade%28hunter%29.vbs	611c2e0080583a3371d2b23c6d74df520e7789d9
39	LSASecretsView.exe	5646008cf4bf805847e26804a280a05883b5c4c9
40	LSASecretsView64.exe	a531f4a0861afe5d8a37d129808bd6fb9cc4cfc8
41	mailpv.exe	5a451dab3c943dbe8eaff99b1a4ba5861bd190da
42	mimikatz.exe	250875212d58e1d4169b7e7d0cd236d1a19a4b9a
43	mimon.bat	ce705296e218387daec0337c2d2cd44842a1590a
44	mspass.exe	4a3418d78d8fe36b39d1ee5435796369b88a8762
45	netpass.exe	17a513dfad8f9c1ae7a612e0a7c18f64811b929d
46	netpass64.exe	7ab128659ad586761ea68009d59a1ccf1547a039
47	netscan.exe	52332ce16ee0c393b8eea6e71863ad41e3caeafd
48	newnewuser.bat	1b65d347bea374bb9915c445382ae696ba4064d4
49	newuser.bat	fcdff444af14366b4a5c31de580ac38b1e2edda4
50	openrdp.bat	ac0dce3b0f5b8d187a2e3f29efc358538fd4aa45
51	OperaPassView.exe	cab798294be00a94ba8ebf9ccb7443e837835d05

Table 2: Indicators of Compromise

#	File Names	SHA1
52	PasswordFox.exe	863d6cd47276b38b21f835938067aee48bd6ad43
53	PasswordFox64.exe	9605ad4adc7de7f53fa7d99e6f32082da90831a1
54	PortScanner.exe	233d8dcf8c3178b15af449fc83e1313116bd92b2
55	PPLKiller.exe	1f2f9c60e0fbb3bf134b5d65a067d1aeef22c1f5
56	PPLKillerx86.exe	c240391eda5dee822ae4662d69cc98dffa725ada
57	processhacker-2.39-setup.exe	162b08b0b11827cc024e6b2eed5887ec86339baa
58	PsExec.exe	e50d9e3bd91908e13a26b3e23edeaf577fb3a095
59	psNET.bat	8003bcb91775386084dcedeca3e1ea68d50888c3
60	pspv.exe	836cb49c8d08d5e305ab8976f653b97f1edba245
61	PstPassword.exe	28ae5dc662dcb251cc67ebc5841df02f3b4bd875
62	rdp.exe	641b7cf77286bd86eb144147bbf073bbd2c9c261
63	rdproute_in.bat	4cced1a24c9a5ef87804c6c20473ecf76ce32ca3
64	rdproute_out.bat	ef302b349ffefd705459f3dd7df0756c25dab9ef
65	rdpv.exe	9f7835b3cdc7cbc641904b1923d7de4a72b3c437
66	removesophos.bat	0bb064941a782913fa392c359584554374262cb6
67	RouterPassView.exe	243e85a669b79c0ae4297663497796aa7d7116dd
68	RTCore64.sys	f6f11ad2cd2b0cf95ed42324876bee1d83e01775
69	sd.exe	2cb4b4fb1ec8305ef03e1802f56be22b12379a0c
70	SniffPass.exe	3bd9fd175a098192a48d6257fded4fc5064fd5c2
71	SniffPass64.exe	6638e718501de489649a5a3a7fcd62a92fd7cdc1
72	start.bat	9d6fa6437ba3705721c7cd32c994fd64c89b0488
73	SuppTrendMICRO.BAT	fc111ca712e1a87bc726e2c5ce97c4e66748d474
74	turnoff.bat	22776dd3929dabff5565f7c8bfb4acdb650a41c3
75	Twin-Del.vbs	8d9a50eb761bb3a97776353952ebac76cac99dcd
76	Twin-SessionRDP.vbs	fcfadcd6b014d1a434c971ffe357e3e7cea45808
77	uninstallSophos.bat	d859c1aaa0f62c0d9eb6a2418e6355c9764eb088
78	VaultPasswordView.exe	a9cabbf3b28ba897c6f5dea331046f33de823922
79	VaultPasswordView64.exe	62b69689fdc026c524d12fd7a11a09b0bfcffba7
80	VNCPassView.exe	32e24780735a0148c3cc4ce7dda30ed9365397a9

Table 2: Indicators of Compromise

#	File Names	SHA1
81	vncroute.bat	b5124120d470555fd2d82eb0720f1c3eb4477742
82	wallfnd.vbs	b9a236db8906565701c9375ff25df272ce1a160b
83	WebBrowserPassView.exe	6c9f9c26d829b048f4d4be18055ebfe27bb2e74d
84	winservice.exe	6d390038003c298c7ab8f2cbe35a50b07e096554
85	WirelessKeyView.exe	b4dfbae3ec429b966cf689e7b3448f0d431318fb
86	WirelessKeyView64.exe	c191fde066fdf577c81e8bb7f1971040cd124715
87	zam.bat	636bff4cc869f303588728c99531c0a911012836

4 Disclaimer

Cybercom is not responsible for damages that might arise from the misuse of the information contained within this report.

Cybercom does not give legal advice or legal opinions, but does provide reference to legal aspects which might pertain to the allegations and actions. Our findings should be discussed with your legal advisor before formulating any formal legal opinions.

Although the work performed incorporates Cybercom's understanding of the law as it stands, we do not express a legal opinion on any issue, but merely state the facts as they have come to our attention. It should be noted that we are not legal experts and any comment on matters of law should be directed to your legal counsel or attorneys.

Cybercom does not provide any warranties of any kind regarding any information contained within. In no event shall Cybercom or its contractors or subcontractors be liable for any damages, including but not limited to, direct, indirect, special, or consequential damages and including damages based on any negligence of Cybercom or its contractors or subcontractors, arising out of, resulting from, or in any way connected with this report, whether based on warranty, contract, or otherwise, whether loss or injury was sustained from, or arose out of the results of, or reliance upon the report.