Threat Thursday: Who’s Afraid of Phobos Ransomware?

blogs.blackberry.com/en/2021/09/threat-thursday-phobos-ransomware

Phobos is an older ransomware family that targets small to medium organizations in a wide range of industries, including healthcare. Attackers usually demand much lower ransom amounts than other ransomware families, which may appear more affordable to victims and increase the likelihood of payment. Ransomware incident response company Coveware reports that the average Phobos payment amount in July 2021 was approximately $54,700.

Phobos attacks have two main infection vectors: email phishing campaigns with malicious attachments, or gaining access to the system over Remote Desktop Protocol (RDP). Attackers obtain RDP credentials by a variety of different methods. They can conduct brute force attacks, leverage stolen credentials purchased from darknet marketplaces, or they can identify open, poorly configured, or vulnerable connections that can be exploited. After gaining a foothold in the environment, the threat actor will attempt to move laterally via RDP.

Phobos actors are known to prefer targeting servers rather than end user computers when deploying their ransomware attack.

Operating System

Windows	MacOS	Linux	Android
Yes	No	No	No

Risk & Impact

Impact	Medium
Risk	Medium

Introduction

The name Phobos is likely inspired by the Greek god who was believed to be the personification of fear and panic. Phobos ransomware is closely related to the CrySIS and Dharma malware families.

CrySIS was first discovered in 2016, but it gained a new level of popularity among threat actors when the original author released its source code that same year. After its decryption keys were leaked, the malware was rebranded as Dharma.

Dharma operates under a Ransomware-as-a-Service (RaaS) model and is sold by multiple independent actors. Phobos appeared in the threat landscape late in 2018 as a successor to Dharma, after decryption tools and keys became available for the Dharma family.

Dharma and Phobos share code similarities and nearly identical ransom notes. The main difference between the two is how they encrypt files during an attack. Currently there is no decryption tool available for Phobos.

Phobos is simplistic in design, which makes it popular with threat actors of varying technical abilities.

Technical Analysis

The sample reviewed for this report is a Windows® 32-bit executable developed in Microsoft® Visual C++, with a compile date of March 1, 2021.

The binary contains no embedded file information to indicate or conceal its origin or purpose; it doesn't try to masquerade as a legitimate file. It is also not packed or encrypted when compiled. Malware authors frequently use these techniques to help conceal a file's true functionality from security products, or to hinder analysis by researchers. But this is not the case with Phobos, and statically analyzing the file gives some insight to its malicious intent.

This threat is able to fingerprint a target system, list processes, manipulate files, interact with services, and modify registry keys. It can also spread via network connections, and it has the potential for backdoor activity.

In an effort to add some complexity to the malware, some of the strings within the file have been obfuscated. This conceals some of the file's malicious attributes. The executable will de-obfuscate the strings during runtime as and when they are needed.

The ransomware does not attempt to bypass User Access Control, and when executed the potential victim receives a pop-up message:

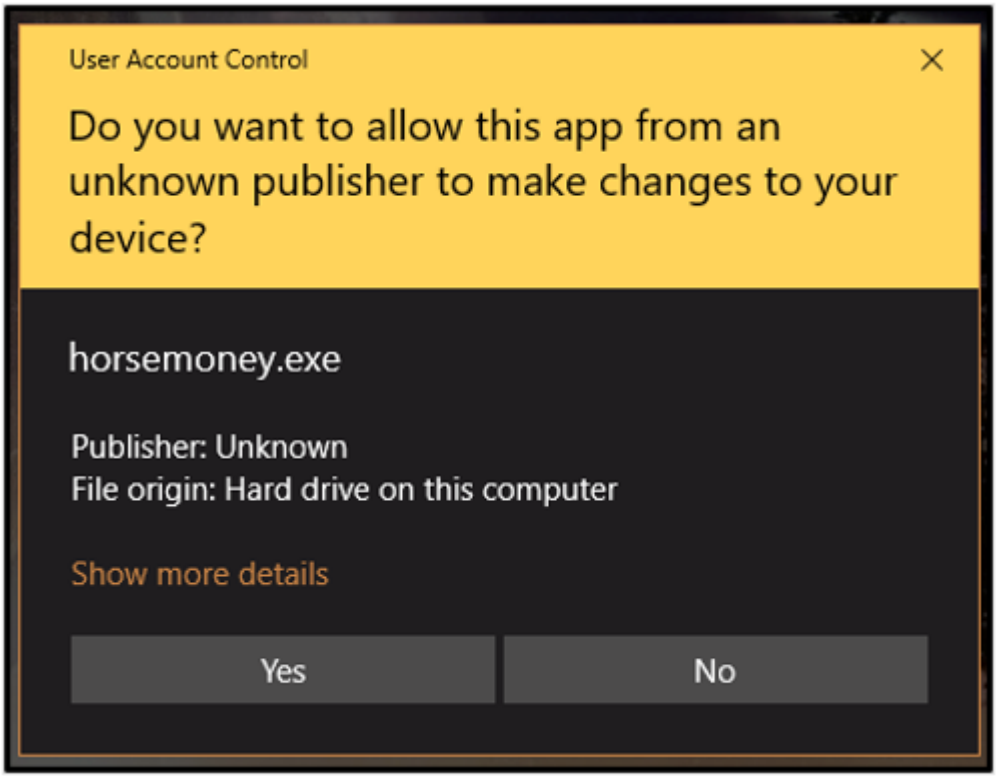

Figure 1: User Access Control warning

If the binary is allowed to run, the malware launches another instance of itself with elevated privileges.

To achieve persistence on the target, the malicious file creates a copy of itself under the StartUp folder found under both the victim's AppData directory and in ProgramData. The sample also creates autorun registry keys pointing to these binaries when logging into the device.

Phobos invokes the Windows command prompt to conduct some tasks before beginning its encryption routine. The threat uses several native Windows command line tools to impede easy restoration of the system. Shadow copies that hold backup copies and system snapshots are deleted by the following commands:

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

The backup catalog is also deleted with the command “wbadmin delete catalog -quiet.” This backup catalog stores details about the backup itself, such as which volumes are included and where the restore file can be found.

Bcdedit is executed to change settings for Windows’ startup repair feature, by setting it to disable recovery and to ignore failures:

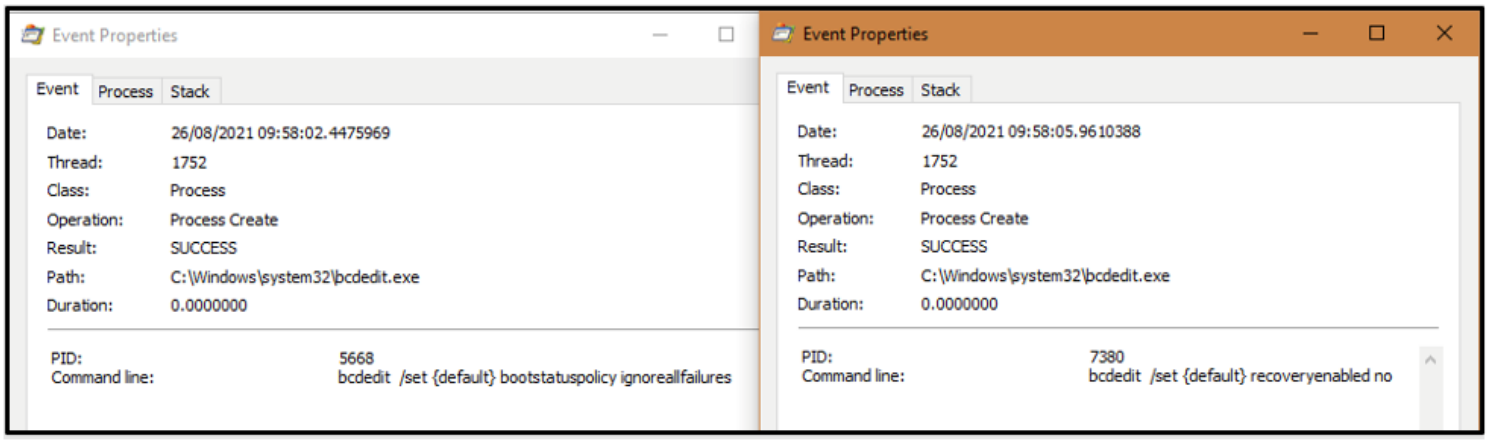

Figure 2: Disabling Windows' startup repair feature

The local system Firewall is disabled via netsh:

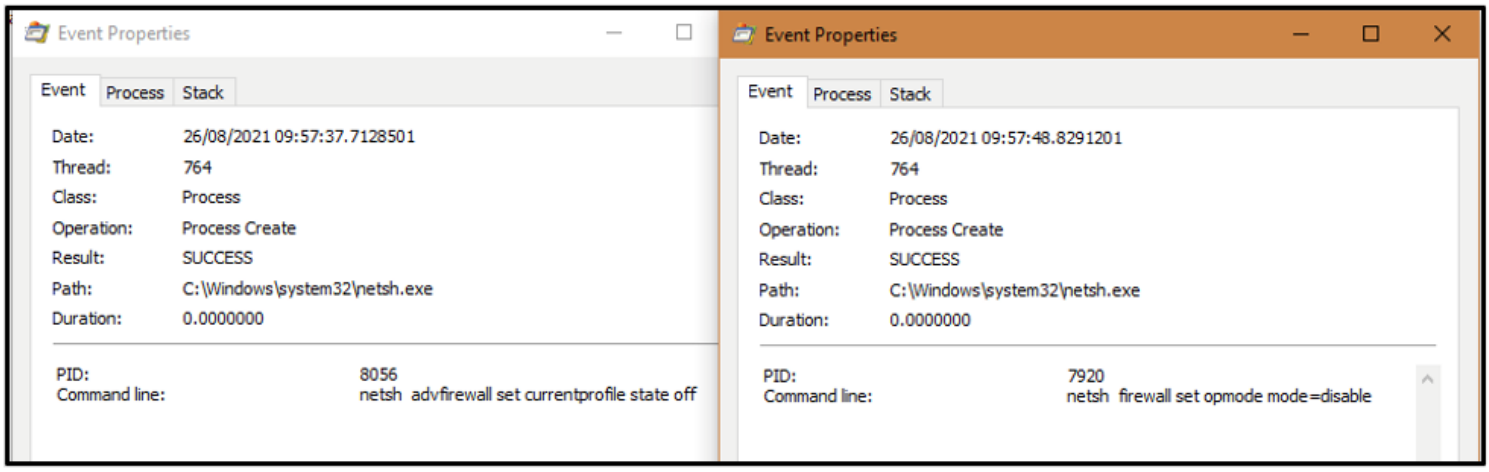

Figure 3: Disabling the firewall

Phobos uses AES with a 256-bit key to encrypt local files as well as those found on network drives. The symmetric block cipher does not require an Internet connection to encrypt an infected system, which can be useful when targeting internal assets. The malware encrypts a wide range of filetypes, though it bypasses essential files belonging to the operating system.

As seen in the image below, the encrypted files are renamed with a unique victim ID and a version ID appended to the original file name. This variant also adds the extension “.HORSEMONEY”.

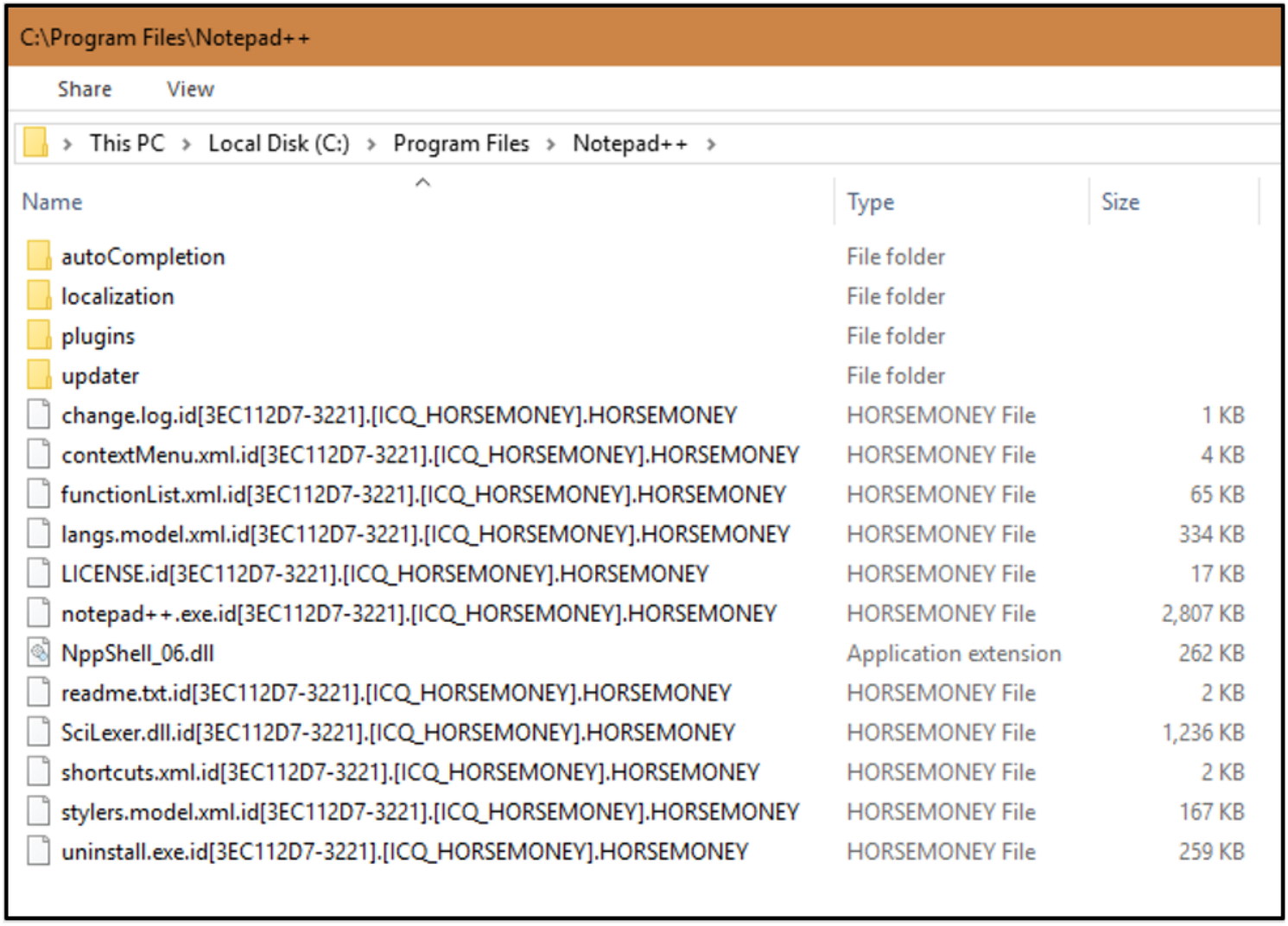

Figure 4: Local files renamed following encryption

Phobos ransomware drops two versions of its ransom note: One is a text file, and one is a HTML application file. With this variant of Phobos, the text file is named “info.txt,” but it contains no text. The HTML file is named “info.hta,” which is run by the Windows native mshta.exe application.

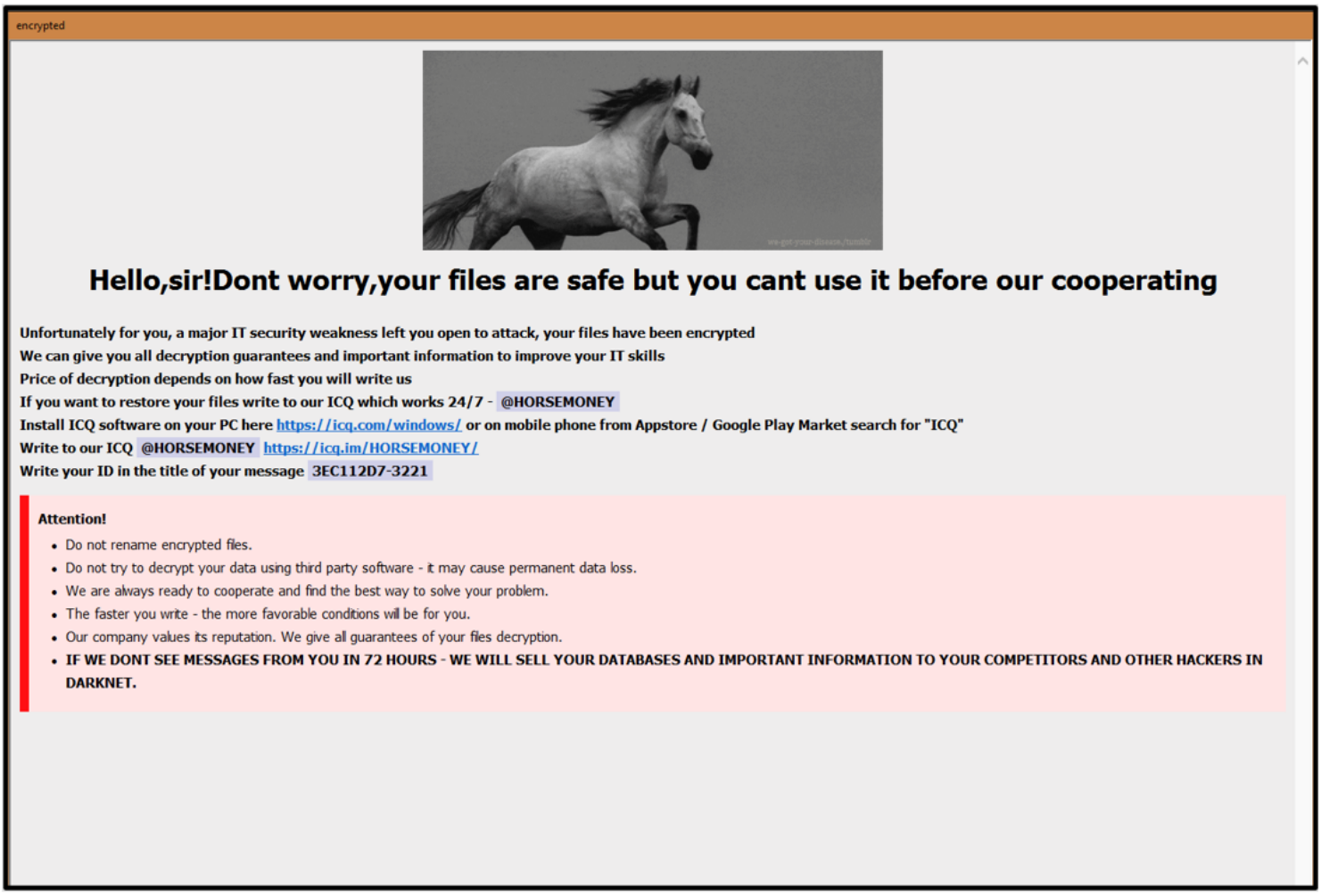

Figure 5: Phobos HORSEMONEY ransom note

The attackers do not define a ransom amount or provide details of a cryptocurrency wallet for payment. Instead, they request the victim to contact them directly through ICQ.

The ransom threatens that, “IF WE DONT (sic) SEE MESSAGES FROM YOU IN 72 HOURS - WE WILL SELL YOUR DATABASES AND IMPORTANT INFORMATION TO YOUR COMPETITORS AND OTHER HACKERS IN DARKNET.”

During analysis, we found no evidence of data being compressed and exfiltrated.

Despite the threats in the ransom note, Phobos does not currently employ the technique of double extortion. There have been no reports yet of any underground leak site disclosing confidential information belonging to its targets. This threat is likely included to manipulate the victim, playing on the fears created by other high-profile ransomware attacks that have occurred this year.

YARA Rule

The following YARA rule was authored by the BlackBerry Research & Intelligence Team to catch the threat described in this document:

```
import "pe"

rule Mal_Win_Ransom_Phobos{

meta:
description = "Phobos Ransomware August 2021"
author = "BlackBerry Threat Research Team"
date = "2021-08"

strings:
$s1 = {5c005c003f005c0055004e0043005c005c005c0020002d007300}
$s2 = {5c005c003f005c0058003a00}
$s3 = "WinHttpConnect" ascii
$s4 = "FindFirstFileW" ascii
$s5 = "FindNextFileW" ascii
$s6 = "Process32FirstW" ascii

condition:
all of them and
pe.is_32bit() and
filesize < 70KB and
pe.imports("MPR.dll") and
pe.imports("WINHTTP.dll") and
pe.imphash() == "16807f046780c6a0b6d02a2f1cc9a6f6" and
pe.number_of_signatures == 0 and
pe.number_of_sections == 5
}
```

Indicators of Compromise (IoCs)

Processes Created:

- horsemoney.exe > "%WinDir%\system32\cmd.exe"
- cmd.exe > "vssadmin delete shadows /all /quiet"
- cmd.exe > "netsh advfirewall set currentprofile state off"
- cmd.exe > "netsh firewall set opmode mode=disable"
- cmd.exe > "wmic shadowcopy delete"
- cmd.exe > "bcdedit /set {default} bootstatuspolicy ignoreallfailures"
- cmd.exe > "bcdedit /set {default} recoveryenabled no"
- cmd.exe > "wbadmin delete catalog -quiet"

Files Dropped:

- %LocalAppData%\horsemoney.exe
- %AppData%\Microsoft\Windows\Start Menu\Programs\Startup\horsemoney.exe
- %AllUsersProfile%\Microsoft\Windows\Start Menu\Programs\StartUp\horsemoney.exe

AutoRun Registry Key:

- HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Windows\CurrentVersion\Run\horsemoney
- HKEY_CURRENT_USER\SOFTWARE\WOW6432Node\Windows\CurrentVersion\Run\horsemoney

Encrypted Files:

<filename>.id[alpha-numeric_id].[alpha-numeric_id].HORSEMONEY

Ransom Note:

info.hta

URL to contact attackers:

https://icq[.]im/HORSEMONEY/

For more information about Phobos ransomware, check out our new demo video blog, Blackberry Prevents: Phobos Ransomware.