Symantec
A Division of Broadcom

Threat Alert

TLP: Amber

Monster Ransomware: Indicators of compromise

Attackers deploying wide range of password-harvesting tools.

Actor:
Hyadina

Actor Aliases:
N/A

Target Geographies:
All

Target Sectors:
All

Attack Motivation:
Ransomware

Overview

Attacks involving the emergent Monster ransomware have continued into November 2022. In recent attacks investigated by Symantec, the attackers made heavy use of dual-use tools, including multiple network-scanning and credential-dumping tools.

One hallmark of recent attacks has been the installation of a password protected self-extracting archive (file name: mim.exe) containing the Mimikatz credential-dumping tool and a large number of password-harvesting tools developed by NirSoft.

Monster first appeared in March 2022 and operates as a ransomware-as-a-service. The payload's functionality was recently documented by BlackBerry.

Tools Used:

AnyDesk: A legitimate remote desktop application. It and similar tools are often used by attackers to obtain remote access to computers on a network.

BulletsPassView: Password recovery tool that retrieves passwords stored behind the bullets in the standard password text-box in Windows and Internet Explorer. Developed by NirSoft.

ChromePass: Password recovery tool for the Google Chrome browser. Developed by NirSoft.

DialupPass: Password recovery tool that reveals all passwords stored in dial-up entries of Windows. Developed by NirSoft.

IEPassView: Password recovery tool for the Internet Explorer browser. Developed by NirSoft.

KPortScan 3.0: Publicly available port scanning tool.

MailPassView: Password recovery tool for multiple email clients. Developed by NirSoft

Mimikatz: Publicly available credential dumping tool.

NetScan: SoftPerfect Network Scanner (netscan.exe), a publicly available tool used for discovery of host names and network services.

NetRouteView: Network Route Utility for Windows. Developed by NirSoft.

NetworkPasswordRecovery: Password recovery tool for network share passwords stored by Windows. Developed by NirSoft

OperaPassView: Password recovery tool for the Opera browser. Developed by NirSoft.

PasswordFox: Password recovery tool for the Firefox browser. Developed by NirSoft.

Process Hacker: Publicly available administration tool.

ProtectedStoragePassView: Password recovery tool for passwords stored inside Windows Protected Storage. Developed by NirSoft.

PstPassword: Password recovery tool for Microsoft Outlook .pst files. Developed by NirSoft.

RemoteDesktopPassView: Password recovery tool for Microsoft Remote Desktop Connection. Developed by NirSoft.

RouterPassView: Password recovery tool for router configuration files. Developed by NirSoft.

SniffPass: Password recovery tool that captures passwords passing through a network adapter. Developed by NirSoft.

VNCPassView: Password recovery tool for passwords stored by VNC. Developed by NirSoft.

WebBrowserPassView: Password recovery tool for the Internet Explorer, Firefox, Chrome, and Opera browsers. Developed by NirSoft.

WirelessKeyView: Password recovery tool for all WEP/WPA wireless keys stored on a computer. Developed by NirSoft.

Indicators of Compromise

SOC analysts should review this alert and hunt on their network for associated indicators of compromise (IOCs). Their presence may indicate a ransomware attack in preparation. If an IOC is malicious and the file available to us, Symantec Endpoint products will detect and block that file. If you discover any other unknown or unavailable files while hunting, you can submit them to Symantec for analysis.

Symantec products will detect and alert against the behaviors and techniques detailed in this alert. For guidance on how to search for IOCs using Symantec's EDR, read this guide for the Cloud solution or this guide for the On-Prem solution.

SHA256 file hashes:

52b8e94a73231d197f492b5e6cb88d42ff393c667e93f92d9b4219e19ceb2bed - AnyDesk

b556d90b30f217d5ef20ebe3f15cce6382c4199e900b5ad2262a751909da1b34 - BrowserPassView

e71cda5e7c018f18aefcdfbce171cfeee7b8d556e5036d8b8f0864efc5f2156b - BulletsPassView

c4304f7bb6ef66c0676c6b94d25d3f15404883baa773e94f325d8126908e1677 - ChromePass

598555a7e053c7456ee8a06a892309386e69d473c73284de9bbc0ba73b17e70a - DialupPass

dbe98193aced7285a01c18b7da8e4540fb4e5b0625debcfbabcab7ea90f5685d - IEPassView

22a44425290a7c566fc1cdb2e1bf0e60a3920e540b2307716c26b2559220d7b7 - KPortScan 3.0 port scanning tool

080c6108c3bd0f8a43d5647db36dc434032842339f0ba38ad1ff62f72999c4e5 - KPortScan 3.0 port scanning tool

16c6af4ae2d8ca8e7a3f2051b913fa1cb7e1fbd0110b0736614a1e02bbbbceaf - MailPassView

31eb1de7e840a342fd468e558e5ab627bcb4c542a8fe01aec4d5ba01d539a0fc - Mimikatz

df1f007f8a0a7bd2921fda692aac5a98257abab4b6d04eeab331dc90511a1108 - Monster ransomware

390aefbba503ba2f1c5eb52a5b3675d32063a7df7c867f5420b140acceddd677 - Monster ransomware

86965d6a0076d71b4c841cacd72b9199732b9b50c1104875d57e727b4971a788 - Monster ransomware

c08b6f2f62fec4b765a156e03a6fe06f4142fd0341c98be9810e14d4f75979bf - Monster ransomware

c867d85196b0663f6a3568893be8e0d8489b9e5b71a93293e2d204e7b31dfe6a - Monster ransomware

91041b616969e1526ee6dce23f8d18afdd353786ac6afa0b6611903263ee6f63 - NetRouteView

6a87226ed5cca8e072507d6c24289c57757dd96177f329a00b00e40427a1d473 - NetworkPasswordRecovery

8e4b218bdbd8e098fff749fe5e5bbf00275d21f398b34216a573224e192094b8 - OperaPassView

7fee96ae0ed1972a80abbd4529dc81ec033083857455bbf3c803c4f47e1ac31c - PasswordFox

6bc073fbbd99be360298d37cf9e037825a44ad7284e3f7eb26b022aeed8ffedc - Process Hacker

bd2c2cf0631d881ed382817afcce2b093f4e412ffb170a719e2762f250abfea4 - Process Hacker

64788b6f74875aed53ca80669b06f407e132d7be49586925dbb3dcde56cbca9c - ProtectedStoragePassView

5e85446910e732111ca9ac90f9ed8b1dee13c3314d2c5117dcf672994ce73bd6 - PstPassword

205818e10c13d2e51b4c0196ca30111276ca1107fc8e25a0992fe67879eab964 - RemoteDesktopPassView

ae474417854ac1b6190e15cc514728433a26cc815fdc6d12150ef55e92d643ea - RouterPassView

930d287d45df81e40b64a40b8cd166d7300d4ad2ce873ae340352cca2e797c18 - Archive of Mimikatz and NirSoft Tools

c92580318be4effdb37aa67145748826f6a9e285bc2426410dc280e61e3c7620 - SniffPass

66c488c1c9916603fc6d7ec00470d30e6f5e3597ad9f8e5ce96a8af7566f6d89 - SoftPerfect Network Scanner

816d7616238958dfe0bb811a063eb3102efd82eff14408f5cab4cb5258bfd019 - VNCPassView

48b77c1efbc3197128391a35d0e1ed0b5cc3a05b96dd12c98ac73ffc6a886fc8 - WirelessKeyView

File names:

anydesk-4.2.2.exe

bulletspassview64.exe

chromepass.exe

csbswuee.exe

dialupass.exe

encrypter.exe

foonaloj.exe

iepv.exe

kportscan 3.0.exe

kportscan3.exe

lsass.exe

mailpv.exe

mim.exe

mimik.exe

nasp.exe

netpass64.exe

netrouteview.exe

operapassview.exe

passwordfox64.exe

processhacker.exe

pspv.exe

pstpassword.exe

rdpv.exe

routerpassview.exe

sniffpass64.exe

txfknwmb.exe

vncpassview.exe

webbrowserpassview.exe

wirelesskeyview64.exe

Ransomware execution commands & associated process lineage(s):

encrypter.exe /v+

^

encrypter.exe <- CSIDL_SYSTEM\cmd.exe <- CSIDL_WINDOWS\explorer.exe

encrypter.exe <- CSIDL_SYSTEM\cmd.exe <- CSIDL_WINDOWS\explorer.exe <- CSIDL_SYSTEM\winlogon.exe

encrypter.exe <- CSIDL_SYSTEM\cmd.exe <- CSIDL_WINDOWS\explorer.exe <- CSIDL_SYSTEM\userinit.exe <- CSIDL_SYSTEM\winlogon.exe <- CSIDL_SYSTEM\smss.exe <- CSIDL_SYSTEM\smss.exe

“CSIDL_COMMON_APPDATA\installed updates.\{d450a8a1-9568-45c7-9c0e-b4f9fb4537bd}\csbswuee.exe" "/v+"

^

csbswuee.exe <- CSIDL_PROFILE\downloads\encrypter.exe <- CSIDL_SYSTEM\cmd.exe <- CSIDL_WINDOWS\explorer.exe

"CSIDL_COMMON_APPDATA\installed updates.\{d450a8a1-9568-45c7-9c0e-b4f9fb4537bd}\foonaloj.exe" "/v+"

^

foonaloj.exe <- CSIDL_PROFILE\music\encrypter.exe <- CSIDL_SYSTEM\cmd.exe <- CSIDL_WINDOWS\explorer.exe <- CSIDL_SYSTEM\userinit.exe <- CSIDL_SYSTEM\winlogon.exe <- CSIDL_SYSTEM\smss.exe <- CSIDL_SYSTEM\smss.exe

"CSIDL_COMMON_APPDATA\installed updates.\{d450a8a1-9568-45c7-9c0e-b4f9fb4537bd}\txfknwmb.exe" "/v+"

^

txfknwmb.exe <- CSIDL_PROFILE\downloads\encrypter.exe <- CSIDL_SYSTEM\cmd.exe <- CSIDL_WINDOWS\explorer.exe <- CSIDL_SYSTEM\winlogon.exe

NetScan commands & associated process lineage(s):

"CSIDL_PROFILE\downloads\nasp.exe"

"CSIDL_PROFILE\music\nasp.exe"

^

nasp.exe <- CSIDL_WINDOWS\explorer.exe <- CSIDL_SYSTEM\userinit.exe <- CSIDL_SYSTEM\winlogon.exe <- CSIDL_SYSTEM\smss.exe <- CSIDL_SYSTEM\smss.exe

KPortScan commands & associated process lineage(s):

"CSIDL_PROFILE\downloads\kportscan 3.0.exe"

^

kportscan 3.0.exe <- CSIDL_WINDOWS\explorer.exe

"CSIDL_PROFILE\downloads\kportscan 3.0\kportscan3.exe"

^

kportscan3.exe <- CSIDL_WINDOWS\explorer.exe

AnyDesk commands & associated process lineage(s):

"CSIDL_PROFILE\downloads\anydesk-4.2.2.exe" --local-service

^

anydesk-4.2.2.exe <- CSIDL_PROFILE\downloads\anydesk-4.2.2.exe <- CSIDL_WINDOWS\explorer.exe

Process Hacker commands & associated process lineage(s):

"CSIDL_PROFILE\downloads\x64\processhacker.exe"

^

processhacker.exe <- CSIDL_WINDOWS\explorer.exe <- CSIDL_SYSTEM\winlogon.exe

Self-Extracting Archive containing Mimikatz and Nirsoft Tools - commands & associated process lineage(s):

"CSIDL_PROFILE\music\mim.exe"

^

mim.exe <- CSIDL_WINDOWS\explorer.exe <- CSIDL_SYSTEM\userinit.exe <- CSIDL_SYSTEM\winlogon.exe <- CSIDL_SYSTEM\smss.exe <- CSIDL_SYSTEM\smss.exe

Nirsoft Tools - commands & associated process lineage(s):

.\Pass\BulletsPassView64.exe

.\Pass\ChromePass.exe

.\Pass\Dialupass.exe

.\Pass\NetRouteView.exe

.\Pass\OperaPassView.exe

.\Pass\PasswordFox64.exe

.\Pass\PstPassword.exe

.\Pass\RouterPassView.exe

.\Pass\SniffPass64.exe

.\Pass\VNCPassView.exe

.\Pass\WebBrowserPassView.exe

.\Pass\SniffPass64.exe

.\Pass\VNCPassView.exe

.\Pass\WebBrowserPassView.exe

.\Pass\WirelessKeyView64.exe

.\Pass\iepv.exe

.\Pass\mailpv.exe

.\Pass\mspass.exe

.\Pass\netpass64.exe

.\Pass\pspv.exe

.\Pass\rdpv.exe

^

CSIDL_SYSTEM\cmd.exe <- CSIDL_WINDOWS\explorer.exe <- CSIDL_SYSTEM\userinit.exe <- CSIDL_SYSTEM\winlogon.exe <- CSIDL_SYSTEM\smss.exe <- CSIDL_SYSTEM\smss.exe