Oct 15 2023

NETMANAGEIT

Intelligence Report

#StopRansomware: AvosLocker Ransomware (Update)

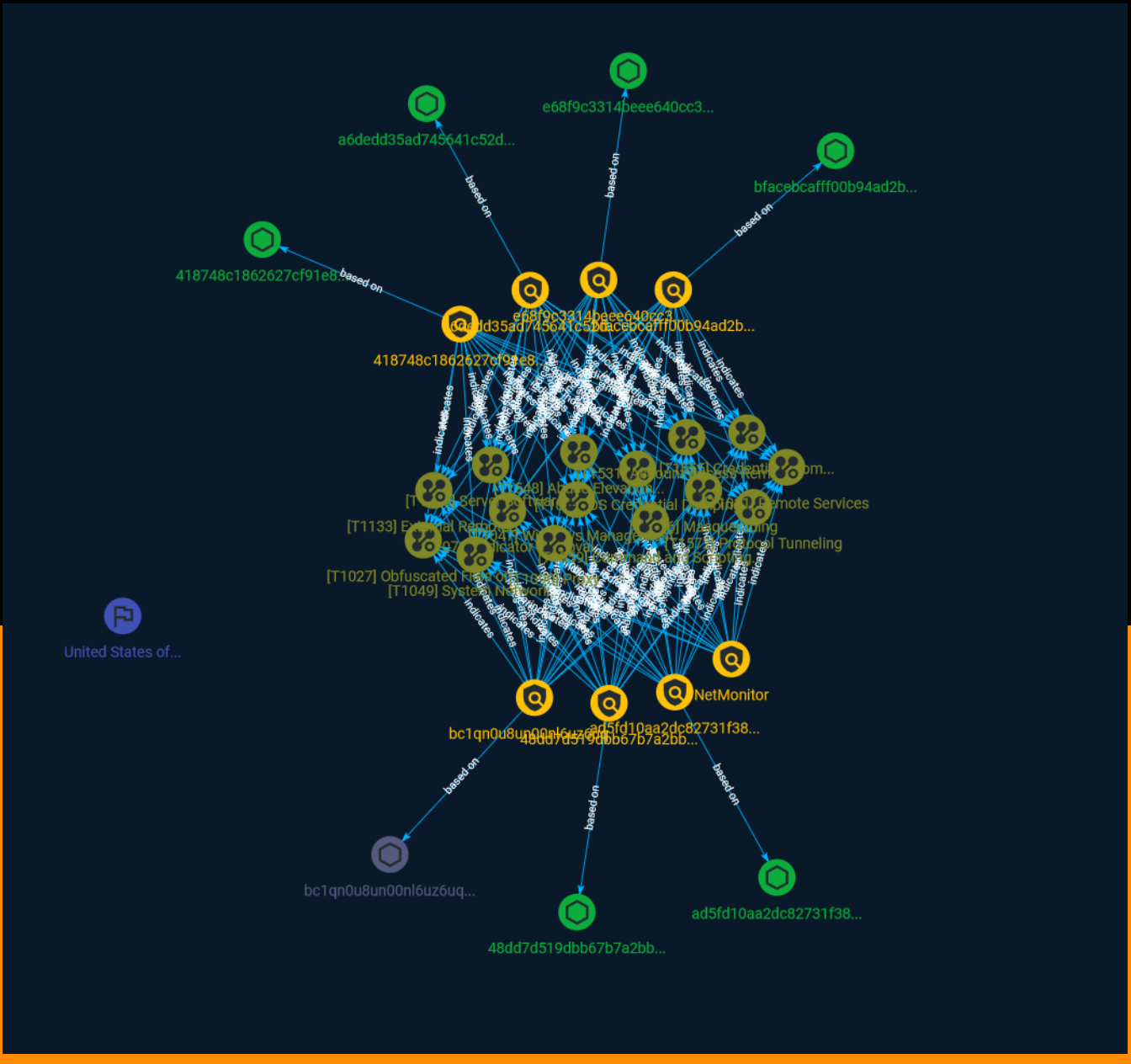

Table of contents

Overview

Entities

Observables

External References

Overview

Description

The Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) are releasing this joint Cybersecurity Advisory (CSA) to disseminate known IOCs, TTPs, and detection methods associated with the AvosLocker variant identified through FBI investigations as recently as May 2023. AvosLocker operates under a ransomware-as-a-service (RaaS) model. AvosLocker affiliates have compromised organizations across multiple critical infrastructure sectors in the United States, affecting Windows, Linux, and VMware ESXi environments. AvosLocker affiliates compromise organizations' networks by using legitimate software and open-source remote system administration tools. AvosLocker affiliates then use exfiltration-based data extortion tactics with threats of leaking and/or publishing stolen data.

Confidence

This value represents the confidence in the correctness of the data contained within this report.

15 / 100

Content

N/A

Attack-Pattern

Name
OS Credential Dumping
ID
T1003
Description
Adversaries may attempt to dump credentials to obtain account login and credential material, normally in the form of a hash or a clear text password, from the operating system and software. Credentials can then be used to perform [Lateral Movement](https://attack.mitre.org/tactics/TA0008) and access restricted information. Several of the tools mentioned in associated sub-techniques may be used by both adversaries and professional security testers. Additional custom tools likely exist as well.
Name
Windows Management Instrumentation
ID
T1047
Description
Adversaries may abuse Windows Management Instrumentation (WMI) to execute malicious commands and payloads. WMI is an administration feature that provides a uniform

environment to access Windows system components. The WMI service enables both local and remote access, though the latter is facilitated by [Remote Services](https://attack.mitre.org/techniques/T1021) such as [Distributed Component Object Model](https://attack.mitre.org/techniques/T1021/003) (DCOM) and [Windows Remote Management](https://attack.mitre.org/techniques/T1021/006) (WinRM).(Citation: MSDN WMI) Remote WMI over DCOM operates using port 135, whereas WMI over WinRM operates over port 5985 when using HTTP and 5986 for HTTPS.(Citation: MSDN WMI)(Citation: FireEye WMI 2015) An adversary can use WMI to interact with local and remote systems and use it as a means to execute various behaviors, such as gathering information for Discovery as well as remote Execution of files as part of Lateral Movement. (Citation: FireEye WMI SANS 2015) (Citation: FireEye WMI 2015)

Name

Abuse Elevation Control Mechanism

ID

T1548

Description

Adversaries may circumvent mechanisms designed to control elevate privileges to gain higher-level permissions. Most modern systems contain native elevation control mechanisms that are intended to limit privileges that a user can perform on a machine. Authorization has to be granted to specific users in order to perform tasks that can be considered of higher risk. An adversary can perform several methods to take advantage of built-in control mechanisms in order to escalate privileges on a system.

Name

Masquerading

ID

T1036

Description

Adversaries may attempt to manipulate features of their artifacts to make them appear legitimate or benign to users and/or security tools. Masquerading occurs when the name or location of an object, legitimate or malicious, is manipulated or abused for the sake of evading defenses and observation. This may include manipulating file metadata, tricking users into misidentifying the file type, and giving legitimate task or service names. Renaming abusable system utilities to evade security monitoring is also a form of [Masquerading](https://attack.mitre.org/techniques/T1036).(Citation: LOLBAS Main Site)

Name

Indicator Removal

ID

T1070

Description

Adversaries may delete or modify artifacts generated within systems to remove evidence of their presence or hinder defenses. Various artifacts may be created by an adversary or something that can be attributed to an adversary's actions. Typically these artifacts are used as defensive indicators related to monitored events, such as strings from downloaded files, logs that are generated from user actions, and other data analyzed by defenders. Location, format, and type of artifact (such as command or login history) are often specific to each platform. Removal of these indicators may interfere with event collection, reporting, or other processes used to detect intrusion activity. This may compromise the integrity of security solutions by causing notable events to go unreported. This activity may also impede forensic analysis and incident response, due to lack of sufficient data to determine what occurred.

Name

Credentials from Password Stores

ID

T1555

Description

Adversaries may search for common password storage locations to obtain user credentials. Passwords are stored in several places on a system, depending on the operating system or application holding the credentials. There are also specific applications that store passwords to make it easier for users manage and maintain. Once credentials are obtained, they can be used to perform lateral movement and access restricted information.

Name

Proxy

ID

T1090

Description

Adversaries may use a connection proxy to direct network traffic between systems or act as an intermediary for network communications to a command and control server to avoid direct connections to their infrastructure. Many tools exist that enable traffic redirection through proxies or port redirection, including [HTRAN](https://attack.mitre.org/software/S0040), ZXProxy, and ZXPortMap. (Citation: Trend Micro APT Attack Tools) Adversaries use these types of proxies to manage command and control communications, reduce the number of simultaneous outbound network connections, provide resiliency in the face of connection loss, or to ride over existing trusted communications paths between victims to avoid suspicion. Adversaries may chain together multiple proxies to further disguise the source of malicious traffic. Adversaries can also take advantage of routing schemes in Content Delivery Networks (CDNs) to proxy command and control traffic.

Name

Server Software Component

ID

T1505

Description

Adversaries may abuse legitimate extensible development features of servers to establish persistent access to systems. Enterprise server applications may include features that allow developers to write and install software or scripts to extend the functionality of the main application. Adversaries may install malicious components to extend and abuse server applications.(Citation: volexity_0day_sophos_FW)

Name

Protocol Tunneling

ID

T1572

Description

Adversaries may tunnel network communications to and from a victim system within a separate protocol to avoid detection/network filtering and/or enable access to otherwise unreachable systems. Tunneling involves explicitly encapsulating a protocol within another. This behavior may conceal malicious traffic by blending in with existing traffic and/or provide an outer layer of encryption (similar to a VPN). Tunneling could also enable routing of network packets that would otherwise not reach their intended destination, such as SMB, RDP, or other traffic that would be filtered by network appliances or not routed over the Internet. There are various means to encapsulate a protocol within another protocol. For example, adversaries may perform SSH tunneling (also known as SSH port forwarding), which involves forwarding arbitrary data over an encrypted SSH tunnel. (Citation: SSH Tunneling) [Protocol Tunneling](https://attack.mitre.org/techniques/T1572) may also be abused by adversaries during [Dynamic Resolution](https://attack.mitre.org/techniques/T1568). Known as DNS over HTTPS (DoH), queries to resolve C2 infrastructure may be encapsulated within encrypted HTTPS packets.(Citation: BleepingComp Godlua JUL19) Adversaries may also leverage [Protocol Tunneling](https://attack.mitre.org/techniques/T1572) in conjunction with [Proxy](https://attack.mitre.org/techniques/T1090) and/or [Protocol Impersonation](https://attack.mitre.org/techniques/T1001/003) to further conceal C2 communications and infrastructure.

Name

Obfuscated Files or Information

ID

T1027

Description

Adversaries may attempt to make an executable or file difficult to discover or analyze by encrypting, encoding, or otherwise obfuscating its contents on the system or in transit. This is common behavior that can be used across different platforms and the network to evade defenses. Payloads may be compressed, archived, or encrypted in order to avoid detection. These payloads may be used during Initial Access or later to mitigate detection. Sometimes a user's action may be required to open and [Deobfuscate/Decode Files or Information](https://attack.mitre.org/techniques/T1140) for [User Execution](https://attack.mitre.org/techniques/T1204). The user may also be required to input a password to open a password protected compressed/encrypted file that was provided by the adversary. (Citation: Volexity PowerDuke November 2016) Adversaries may also use compressed or archived scripts, such as JavaScript. Portions of files can also be encoded to hide the plain-text strings that would otherwise help defenders with discovery. (Citation: Linux/Cdorked.A We Live Security Analysis) Payloads may also be split into separate, seemingly benign files that only reveal malicious functionality when reassembled. (Citation: Carbon Black Obfuscation Sept 2016) Adversaries may also abuse [Command Obfuscation](https://attack.mitre.org/techniques/T1027/010) to obscure commands executed from payloads or directly via [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059). Environment variables, aliases, characters, and other platform/language specific semantics can be used to evade signature based detections and application control mechanisms. (Citation: FireEye Obfuscation June 2017) (Citation: FireEye Revoke-Obfuscation July 2017)(Citation: PaloAlto EncodedCommand March 2017)

Name

Account Access Removal

ID

T1531

Description

Adversaries may interrupt availability of system and network resources by inhibiting access to accounts utilized by legitimate users. Accounts may be deleted, locked, or manipulated (ex: changed credentials) to remove access to accounts. Adversaries may also subsequently log off and/or perform a [System Shutdown/Reboot](https://attack.mitre.org/techniques/T1529) to set malicious changes into place.(Citation: CarbonBlack LockerGoga 2019)(Citation: Unit42 LockerGoga 2019) In Windows, [Net](https://attack.mitre.org/software/S0039) utility, `Set-LocalUser` and `Set-ADAccountPassword` [PowerShell](https://attack.mitre.org/techniques/T1059/001) cmdlets may be used by adversaries to modify user accounts. In Linux, the `passwd` utility may be used to change passwords. Accounts could also be disabled by Group Policy. Adversaries who use ransomware or similar attacks may first perform this and other Impact behaviors, such as [Data Destruction](https://attack.mitre.org/techniques/T1485) and [Defacement](https://attack.mitre.org/techniques/T1491), in order to impede incident response/recovery before completing the [Data Encrypted for Impact](https://attack.mitre.org/techniques/T1486) objective.

Name

Command and Scripting Interpreter

ID

T1059

Description

Adversaries may abuse command and script interpreters to execute commands, scripts, or binaries. These interfaces and languages provide ways of interacting with computer systems and are a common feature across many different platforms. Most systems come with some built-in command-line interface and scripting capabilities, for example, macOS and Linux distributions include some flavor of [Unix Shell](https://attack.mitre.org/techniques/T1059/004) while Windows installations include the [Windows Command Shell](https://attack.mitre.org/techniques/T1059/003) and [PowerShell](https://attack.mitre.org/techniques/T1059/001). There are also cross-platform interpreters such as [Python](https://attack.mitre.org/techniques/T1059/006), as well as those commonly associated

with client applications such as [JavaScript](https://attack.mitre.org/techniques/T1059/007) and [Visual Basic](https://attack.mitre.org/techniques/T1059/005). Adversaries may abuse these technologies in various ways as a means of executing arbitrary commands. Commands and scripts can be embedded in [Initial Access](https://attack.mitre.org/tactics/TA0001) payloads delivered to victims as lure documents or as secondary payloads downloaded from an existing C2. Adversaries may also execute commands through interactive terminals/shells, as well as utilize various [Remote Services](https://attack.mitre.org/techniques/T1021) in order to achieve remote Execution. (Citation: Powershell Remote Commands)(Citation: Cisco IOS Software Integrity Assurance - Command History)(Citation: Remote Shell Execution in Python)

Name

External Remote Services

ID

T1133

Description

Adversaries may leverage external-facing remote services to initially access and/or persist within a network. Remote services such as VPNs, Citrix, and other access mechanisms allow users to connect to internal enterprise network resources from external locations. There are often remote service gateways that manage connections and credential authentication for these services. Services such as [Windows Remote Management](https://attack.mitre.org/techniques/T1021/006) and [VNC](https://attack.mitre.org/techniques/T1021/005) can also be used externally.(Citation: MacOS VNC software for Remote Desktop) Access to [Valid Accounts](https://attack.mitre.org/techniques/T1078) to use the service is often a requirement, which could be obtained through credential pharming or by obtaining the credentials from users after compromising the enterprise network.(Citation: Volexity Virtual Private Keylogging) Access to remote services may be used as a redundant or persistent access mechanism during an operation. Access may also be gained through an exposed service that doesn't require authentication. In containerized environments, this may include an exposed Docker API, Kubernetes API server, kubelet, or web application such as the Kubernetes dashboard.(Citation: Trend Micro Exposed Docker Server)(Citation: Unit 42 Hildegard Malware)

Name

Remote Services

ID

T1021

Description

Adversaries may use [Valid Accounts](https://attack.mitre.org/techniques/T1078) to log into a service that accepts remote connections, such as telnet, SSH, and VNC. The adversary may then perform actions as the logged-on user. In an enterprise environment, servers and workstations can be organized into domains. Domains provide centralized identity management, allowing users to login using one set of credentials across the entire network. If an adversary is able to obtain a set of valid domain credentials, they could login to many different machines using remote access protocols such as secure shell (SSH) or remote desktop protocol (RDP).(Citation: SSH Secure Shell)(Citation: TechNet Remote Desktop Services) They could also login to accessible SaaS or IaaS services, such as those that federate their identities to the domain. Legitimate applications (such as [Software Deployment Tools](https://attack.mitre.org/techniques/T1072) and other administrative programs) may utilize [Remote Services](https://attack.mitre.org/techniques/T1021) to access remote hosts. For example, Apple Remote Desktop (ARD) on macOS is native software used for remote management. ARD leverages a blend of protocols, including [VNC](https://attack.mitre.org/techniques/T1021/005) to send the screen and control buffers and [SSH](https://attack.mitre.org/techniques/T1021/004) for secure file transfer. (Citation: Remote Management MDM macOS)(Citation: Kickstart Apple Remote Desktop commands)(Citation: Apple Remote Desktop Admin Guide 3.3) Adversaries can abuse applications such as ARD to gain remote code execution and perform lateral movement. In versions of macOS prior to 10.14, an adversary can escalate an SSH session to an ARD session which enables an adversary to accept TCC (Transparency, Consent, and Control) prompts without user interaction and gain access to data.(Citation: FireEye 2019 Apple Remote Desktop)(Citation: Lockboxx ARD 2019)(Citation: Kickstart Apple Remote Desktop commands)

Name

System Network Connections Discovery

ID

T1049

Description

Adversaries may attempt to get a listing of network connections to or from the compromised system they are currently accessing or from remote systems by querying for information over the network. An adversary who gains access to a system that is part of a cloud-based environment may map out Virtual Private Clouds or Virtual Networks in order to determine what systems and services are connected. The actions performed are likely the same types of discovery techniques depending on the operating system, but the resulting information may include details about the networked cloud environment relevant to the adversary's goals. Cloud providers may have different ways in which their virtual networks operate.(Citation: Amazon AWS VPC Guide)(Citation: Microsoft Azure Virtual Network Overview)(Citation: Google VPC Overview) Similarly, adversaries who gain access to network devices may also perform similar discovery activities to gather information about connected systems and services. Utilities and commands that acquire this information include [netstat](https://attack.mitre.org/software/S0104), "net use," and "net session" with [Net](https://attack.mitre.org/software/S0039). In Mac and Linux, [netstat](https://attack.mitre.org/software/S0104) and `lsof` can be used to list current connections. `who -a` and `w` can be used to show which users are currently logged in, similar to "net session". Additionally, built-in features native to network devices and [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) may be used (e.g. `show ip sockets`, `show tcp brief`).(Citation: US-CERT-TA18-106A)

Indicator

Name

NetMonitor

Description

NetMonitor Yara rule to detect NetMonitor.exe

Pattern Type

yara

Pattern

rule NetMonitor { meta: author = "FBI" source = "FBI" sharing = "TLP:CLEAR" status = "RELEASED" description = "Yara rule to detect NetMonitor.exe" category = "MALWARE" creation_date = "2023-05-05" strings: $rc4key = {11 4b 8c dd 65 74 22 c3} $op0 = {c6 [3] 00 00 05 c6 [3] 00 00 07 83 [3] 00 00 05 0f 85 [4] 83 [3] 00 00 01 75 ?? 8b [2] 4c 8d [2] 4c 8d [3] 00 00 48 8d [3] 00 00 48 8d [3] 00 00 48 89 [3] 48 89 ?? e8} condition: uint16(0) == 0x5A4D and filesize < 50000 and any of them }

Name

bc1qn0u8un00nl6uz6uqrw7p50rg86gjrx492jkwfn

Pattern Type

stix

Pattern

[cryptocurrency-wallet:value = 'bc1qn0u8un00nl6uz6uqrw7p50rg86gjrx492jkwfn']

Name

e68f9c3314beee640cc32f08a8532aa8dcda613543c54a83680c21d7cd49ca0f

Description

Win.Trojan.CobaltStrike-7917400-0

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'e68f9c3314beee640cc32f08a8532aa8dcda613543c54a83680c21d7cd49ca0f']

Name

ad5fd10aa2dc82731f3885553763dfd4548651ef3e28c69f77ad035166d63db7

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ad5fd10aa2dc82731f3885553763dfd4548651ef3e28c69f77ad035166d63db7']

Name

418748c1862627cf91e829c64df9440d19f67f8a7628471d4b3a6cc5696944dd

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '418748c1862627cf91e829c64df9440d19f67f8a7628471d4b3a6cc5696944dd']

Name

bfacebcafff00b94ad2bff96b718a416c353a4ae223aa47d4202cdbc31e09c92

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'bfacebcafff00b94ad2bff96b718a416c353a4ae223aa47d4202cdbc31e09c92']

Name

48dd7d519dbb67b7a2bb2747729fc46e5832c30cafe15f76c1dbe3a249e5e731

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '48dd7d519dbb67b7a2bb2747729fc46e5832c30cafe15f76c1dbe3a249e5e731']

Name

a6dedd35ad745641c52d6a9f8da1fb09101d152f01b4b0e85a64d21c2a0845ee

Description

ConventionEngine_Anomaly_MultiPDB_Double

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a6dedd35ad745641c52d6a9f8da1fb09101d152f01b4b0e85a64d21c2a0845ee']

Country

Name
United States of America

Cryptocurrency-Wallet

Value
bc1qn0u8un00nl6uz6uqrw7p50rg86gjrx492jkwfn

StixFile

Value
48dd7d519dbb67b7a2bb2747729fc46e5832c30cafe15f76c1dbe3a249e5e731
e68f9c3314beee640cc32f08a8532aa8dcda613543c54a83680c21d7cd49ca0f
418748c1862627cf91e829c64df9440d19f67f8a7628471d4b3a6cc5696944dd
a6dedd35ad745641c52d6a9f8da1fb09101d152f01b4b0e85a64d21c2a0845ee
ad5fd10aa2dc82731f3885553763dfd4548651ef3e28c69f77ad035166d63db7
bfacebcafff00b94ad2bff96b718a416c353a4ae223aa47d4202cdbc31e09c92

External References

- https://otx.alienvault.com/pulse/6526fdf7bc7addfd7d0d9baa
- https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-284a