Jul 11 2024

NETMANAGEIT

Intelligence Report

Ransomware: Activity Levels Remain High Despite Disruption

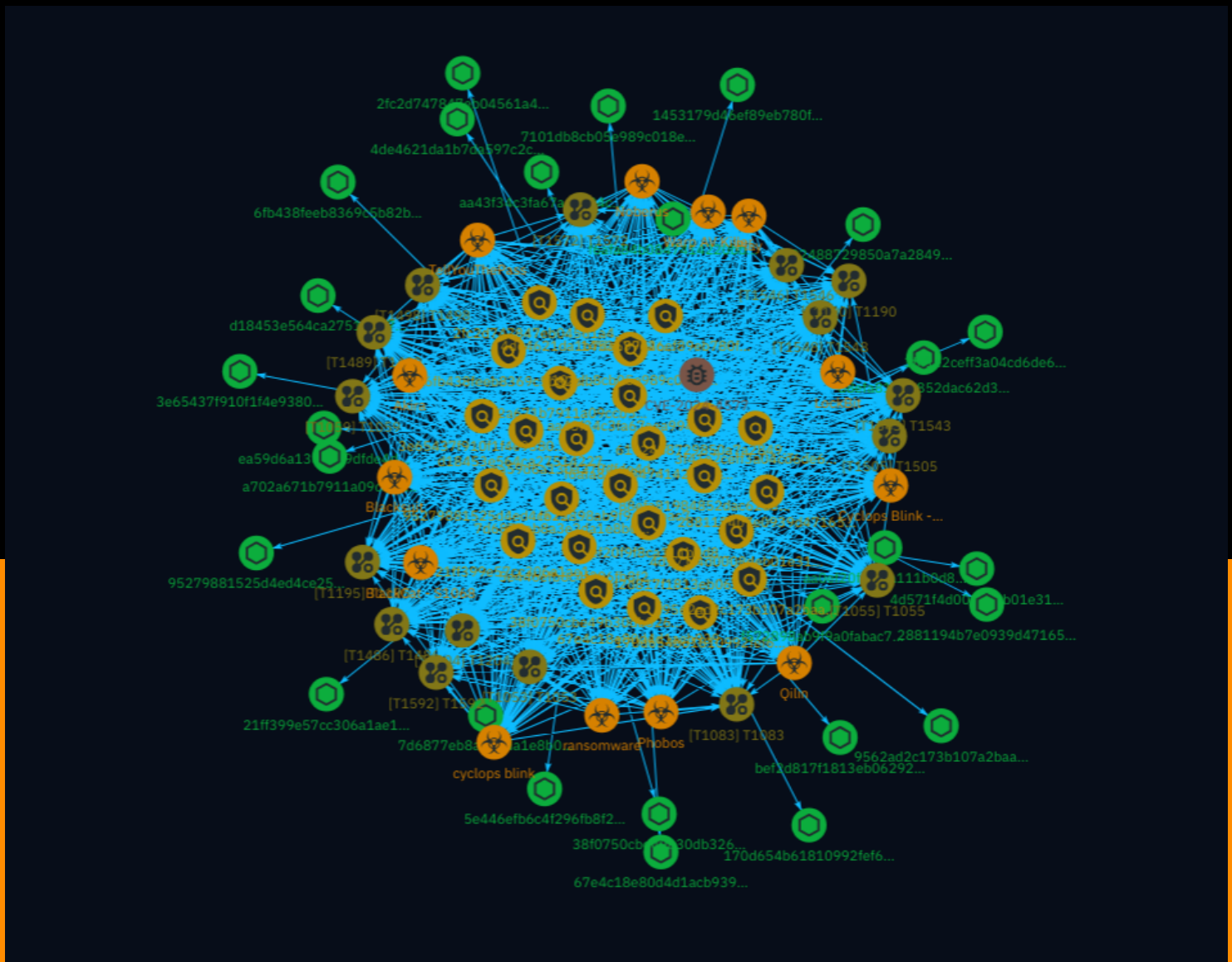

Table of contents

Overview

- Description 4
- Confidence 4
- Content 5

Entities

- Attack-Pattern 6
- Indicator 18
- Malware 29
- indicates 32
- uses 34

Observables

- StixFile 35

External References

- External References 37

Overview

Description

While overall activity levels dipped slightly in the first quarter of 2024, the number of claimed attacks remained high, with LockBit accounting for over 20%. The report explores the changing tactics employed by ransomware actors, including the exploitation of vulnerabilities, the use of Bring-Your-Own-Vulnerable-Driver techniques, and the return of the Clop ransomware by the Snakefly group.

Confidence

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

100 / 100

Content

N/A

Attack-Pattern

Name
T1548
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.(Citation: TechNet How UAC Works)(Citation: sudo man page 2018) An adversary can perform several methods to take advantage of built-in control mechanisms in order to escalate privileges on a system.(Citation: OSX Keydnap malware) (Citation: Fortinet Fareit)
Name
T1498
ID
T1498
Description

Adversaries may perform Network Denial of Service (DoS) attacks to degrade or block the availability of targeted resources to users. Network DoS can be performed by exhausting the network bandwidth services rely on. Example resources include specific websites, email services, DNS, and web-based applications. Adversaries have been observed conducting network DoS attacks for political purposes(Citation: FireEye OpPoisonedHandover February 2016) and to support other malicious activities, including distraction(Citation: FSISAC FraudNetDoS September 2012), hacktivism, and extortion. (Citation: Symantec DDoS October 2014) A Network DoS will occur when the bandwidth capacity of the network connection to a system is exhausted due to the volume of malicious traffic directed at the resource or the network connections and network devices the resource relies on. For example, an adversary may send 10Gbps of traffic to a server that is hosted by a network with a 1Gbps connection to the internet. This traffic can be generated by a single system or multiple systems spread across the internet, which is commonly referred to as a distributed DoS (DDoS). To perform Network DoS attacks several aspects apply to multiple methods, including IP address spoofing, and botnets.
Adversaries may use the original IP address of an attacking system, or spoof the source IP address to make the attack traffic more difficult to trace back to the attacking system or to enable reflection. This can increase the difficulty defenders have in defending against the attack by reducing or eliminating the effectiveness of filtering by the source address on network defense devices. For DoS attacks targeting the hosting system directly, see [Endpoint Denial of Service](https://attack.mitre.org/techniques/T1499).

Name

T1489

ID

T1489

Description

Adversaries may stop or disable services on a system to render those services unavailable to legitimate users. Stopping critical services or processes can inhibit or stop response to an incident or aid in the adversary's overall objectives to cause damage to the environment.(Citation: Talos Olympic Destroyer 2018)(Citation: Novetta Blockbuster) Adversaries may accomplish this by disabling individual services of high importance to an organization, such as `MSExchangeIS`, which will make Exchange content inaccessible (Citation: Novetta Blockbuster). In some cases, adversaries may stop or disable many or all services to render systems unusable.(Citation: Talos Olympic Destroyer 2018) Services or

processes may not allow for modification of their data stores while running. Adversaries may stop services or processes in order to conduct [Data Destruction](https://attack.mitre.org/techniques/T1485) or [Data Encrypted for Impact](https://attack.mitre.org/techniques/T1486) on the data stores of services like Exchange and SQL Server.(Citation: SecureWorks WannaCry Analysis)

Name

T1055

ID

T1055

Description

Adversaries may inject code into processes in order to evade process-based defenses as well as possibly elevate privileges. Process injection is a method of executing arbitrary code in the address space of a separate live process. Running code in the context of another process may allow access to the process's memory, system/network resources, and possibly elevated privileges. Execution via process injection may also evade detection from security products since the execution is masked under a legitimate process. There are many different ways to inject code into a process, many of which abuse legitimate functionalities. These implementations exist for every major OS but are typically platform specific. More sophisticated samples may perform multiple process injections to segment modules and further evade detection, utilizing named pipes or other inter-process communication (IPC) mechanisms as a communication channel.

Name

T1053

ID

T1053

Description

Adversaries may abuse task scheduling functionality to facilitate initial or recurring execution of malicious code. Utilities exist within all major operating systems to schedule programs or scripts to be executed at a specified date and time. A task can also be scheduled on a remote system, provided the proper authentication is met (ex: RPC and file and printer sharing in Windows environments). Scheduling a task on a remote system typically may require being a member of an admin or otherwise privileged group on the remote system.(Citation: TechNet Task Scheduler Security) Adversaries may use task scheduling to execute programs at system startup or on a scheduled basis for persistence. These mechanisms can also be abused to run a process under the context of a specified account (such as one with elevated permissions/privileges). Similar to [System Binary Proxy Execution](https://attack.mitre.org/techniques/T1218), adversaries have also abused task scheduling to potentially mask one-time execution under a trusted system process. (Citation: ProofPoint Serpent)

Name

T1505

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

T1204

ID

T1204

Description

An adversary may rely upon specific actions by a user in order to gain execution. Users may be subjected to social engineering to get them to execute malicious code by, for example, opening a malicious document file or link. These user actions will typically be observed as follow-on behavior from forms of [Phishing](https://attack.mitre.org/techniques/T1566). While [User Execution](https://attack.mitre.org/techniques/T1204) frequently occurs shortly after Initial Access it may occur at other phases of an intrusion, such as when an adversary places a file in a shared directory or on a user's desktop hoping that a user will click on it. This activity may also be seen shortly after [Internal Spearphishing](https://attack.mitre.org/techniques/T1534). Adversaries may also deceive users into performing actions such as enabling [Remote Access Software](https://attack.mitre.org/techniques/T1219), allowing direct control of the system to the adversary; running malicious JavaScript in their browser, allowing adversaries to [Steal Web Session Cookie](https://attack.mitre.org/techniques/T1539)s; or downloading and executing malware for [User Execution](https://attack.mitre.org/techniques/T1204).(Citation: Talos Roblox Scam 2023)(Citation: Krebs Discord Bookmarks 2023) For example, tech support scams can be facilitated through [Phishing](https://attack.mitre.org/techniques/T1566), vishing, or various forms of user interaction. Adversaries can use a combination of these methods, such as spoofing and promoting toll-free numbers or call centers that are used to direct victims to malicious websites, to deliver and execute payloads containing malware or [Remote Access Software](https://attack.mitre.org/techniques/T1219).(Citation: Telephone Attack Delivery)

Name

T1486

ID

T1486

Description

Adversaries may encrypt data on target systems or on large numbers of systems in a network to interrupt availability to system and network resources. They can attempt to render stored data inaccessible by encrypting files or data on local and remote drives and withholding access to a decryption key. This may be done in order to extract monetary compensation from a victim in exchange for decryption or a decryption key (ransomware) or to render data permanently inaccessible in cases where the key is not saved or

transmitted.(Citation: US-CERT Ransomware 2016)(Citation: FireEye WannaCry 2017)(Citation: US-CERT NotPetya 2017)(Citation: US-CERT SamSam 2018) In the case of ransomware, it is typical that common user files like Office documents, PDFs, images, videos, audio, text, and source code files will be encrypted (and often renamed and/or tagged with specific file markers). Adversaries may need to first employ other behaviors, such as [File and Directory Permissions Modification](https://attack.mitre.org/techniques/T1222) or [System Shutdown/Reboot](https://attack.mitre.org/techniques/T1529), in order to unlock and/or gain access to manipulate these files.(Citation: CarbonBlack Conti July 2020) In some cases, adversaries may encrypt critical system files, disk partitions, and the MBR.(Citation: US-CERT NotPetya 2017) To maximize impact on the target organization, malware designed for encrypting data may have worm-like features to propagate across a network by leveraging other attack techniques like [Valid Accounts](https://attack.mitre.org/techniques/T1078), [OS Credential Dumping](https://attack.mitre.org/techniques/T1003), and [SMB/Windows Admin Shares](https://attack.mitre.org/techniques/T1021/002).(Citation: FireEye WannaCry 2017)(Citation: US-CERT NotPetya 2017) Encryption malware may also leverage [Internal Defacement](https://attack.mitre.org/techniques/T1491/001), such as changing victim wallpapers, or otherwise intimidate victims by sending ransom notes or other messages to connected printers (known as "print bombing").(Citation: NHS Digital Egregor Nov 2020) In cloud environments, storage objects within compromised accounts may also be encrypted.(Citation: Rhino S3 Ransomware Part 1)

Name

T1572

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

T1543

ID

T1543

Description

Adversaries may create or modify system-level processes to repeatedly execute malicious payloads as part of persistence. When operating systems boot up, they can start processes that perform background system functions. On Windows and Linux, these system processes are referred to as services.(Citation: TechNet Services) On macOS, launchd processes known as [Launch Daemon](https://attack.mitre.org/techniques/T1543/004) and [Launch Agent](https://attack.mitre.org/techniques/T1543/001) are run to finish system initialization and load user specific parameters.(Citation: AppleDocs Launch Agent Daemons) Adversaries may install new services, daemons, or agents that can be configured to execute at startup or a repeatable interval in order to establish persistence. Similarly, adversaries may modify existing services, daemons, or agents to achieve the same effect. Services, daemons, or agents may be created with administrator privileges but executed under root/SYSTEM privileges. Adversaries may leverage this functionality to create or modify system processes in order to escalate privileges.(Citation: OSX Malware Detection)

Name

T1190

ID

T1190

Description

Adversaries may attempt to exploit a weakness in an Internet-facing host or system to initially access a network. The weakness in the system can be a software bug, a temporary glitch, or a misconfiguration. Exploited applications are often websites/web servers, but can also include databases (like SQL), standard services (like SMB or SSH), network device administration and management protocols (like SNMP and Smart Install), and any other system with Internet accessible open sockets.(Citation: NVD CVE-2016-6662)(Citation: CIS Multiple SMB Vulnerabilities)(Citation: US-CERT TA18-106A Network Infrastructure Devices 2018)(Citation: Cisco Blog Legacy Device Attacks)(Citation: NVD CVE-2014-7169) Depending on the flaw being exploited this may also involve [Exploitation for Defense Evasion](https://attack.mitre.org/techniques/T1211) or [Exploitation for Client Execution](https://attack.mitre.org/techniques/T1203). If an application is hosted on cloud-based infrastructure and/or is containerized, then exploiting it may lead to compromise of the underlying instance or container. This can allow an adversary a path to access the cloud or container APIs, exploit container host access via [Escape to Host](https://attack.mitre.org/techniques/T1611), or take advantage of weak identity and access management policies. Adversaries may also exploit edge network infrastructure and related appliances, specifically targeting devices that do not support robust host-based defenses.(Citation: Mandiant Fortinet Zero Day)(Citation: Wired Russia Cyberwar) For websites and databases, the OWASP top 10 and CWE top 25 highlight the most common web-based vulnerabilities. (Citation: OWASP Top 10)(Citation: CWE top 25)

Name

T1592

ID

T1592

Description

Adversaries may gather information about the victim's hosts that can be used during targeting. Information about hosts may include a variety of details, including administrative data (ex: name, assigned IP, functionality, etc.) as well as specifics regarding its configuration (ex: operating system, language, etc.). Adversaries may gather this

information in various ways, such as direct collection actions via [Active Scanning](https://attack.mitre.org/techniques/T1595) or [Phishing for Information](https://attack.mitre.org/techniques/T1598). Adversaries may also compromise sites then include malicious content designed to collect host information from visitors.(Citation: ATT ScanBox) Information about hosts may also be exposed to adversaries via online or other accessible data sets (ex: [Social Media](https://attack.mitre.org/techniques/T1593/001) or [Search Victim-Owned Websites](https://attack.mitre.org/techniques/T1594)). Gathering this information may reveal opportunities for other forms of reconnaissance (ex: [Search Open Websites/Domains](https://attack.mitre.org/techniques/T1593) or [Search Open Technical Databases](https://attack.mitre.org/techniques/T1596)), establishing operational resources (ex: [Develop Capabilities](https://attack.mitre.org/techniques/T1587) or [Obtain Capabilities](https://attack.mitre.org/techniques/T1588)), and/or initial access (ex: [Supply Chain Compromise](https://attack.mitre.org/techniques/T1195) or [External Remote Services](https://attack.mitre.org/techniques/T1133)).

Name

T1546

ID

T1546

Description

Adversaries may establish persistence and/or elevate privileges using system mechanisms that trigger execution based on specific events. Various operating systems have means to monitor and subscribe to events such as logons or other user activity such as running specific applications/binaries. Cloud environments may also support various functions and services that monitor and can be invoked in response to specific cloud events. (Citation: Backdooring an AWS account)(Citation: Varonis Power Automate Data Exfiltration) (Citation: Microsoft DART Case Report 001) Adversaries may abuse these mechanisms as a means of maintaining persistent access to a victim via repeatedly executing malicious code. After gaining access to a victim system, adversaries may create/modify event triggers to point to malicious content that will be executed whenever the event trigger is invoked. (Citation: FireEye WMI 2015)(Citation: Malware Persistence on OS X)(Citation: amnesia malware) Since the execution can be proxied by an account with higher permissions, such as SYSTEM or service accounts, an adversary may be able to abuse these triggered execution mechanisms to escalate their privileges.

Name

T1059

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

T1195

ID

T1195

Description

Adversaries may manipulate products or product delivery mechanisms prior to receipt by a final consumer for the purpose of data or system compromise. Supply chain compromise can take place at any stage of the supply chain including: * Manipulation of development tools * Manipulation of a development environment * Manipulation of source code repositories (public or private) * Manipulation of source code in open-source dependencies * Manipulation of software update/distribution mechanisms * Compromised/infected system images (multiple cases of removable media infected at the factory)(Citation: IBM Storwize)(Citation: Schneider Electric USB Malware) * Replacement of legitimate software with modified versions * Sales of modified/counterfeit products to legitimate distributors * Shipment interdiction While supply chain compromise can impact any component of hardware or software, adversaries looking to gain execution have often focused on malicious additions to legitimate software in software distribution or update channels.(Citation: Avast CCleaner3 2018)(Citation: Microsoft Dofoil 2018)(Citation: Command Five SK 2011) Targeting may be specific to a desired victim set or malicious software may be distributed to a broad set of consumers but only move on to additional tactics on specific victims.(Citation: Symantec Elderwood Sept 2012)(Citation: Avast CCleaner3 2018)(Citation: Command Five SK 2011) Popular open source projects that are used as dependencies in many applications may also be targeted as a means to add malicious code to users of the dependency.(Citation: Trendmicro NPM Compromise)

Name

T1083

ID

T1083

Description

Adversaries may enumerate files and directories or may search in specific locations of a host or network share for certain information within a file system. Adversaries may use the information from [File and Directory Discovery](https://attack.mitre.org/techniques/T1083) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions. Many command shell utilities can be used to obtain this information. Examples include `dir`, `tree`, `ls`, `find`, and `locate`.(Citation: Windows Commands JPCERT) Custom tools may also be used to gather file and directory information and interact with the [Native API](https://

attack.mitre.org/techniques/T1106). Adversaries may also leverage a [Network Device CLI] (https://attack.mitre.org/techniques/T1059/008) on network devices to gather file and directory information (e.g. `dir`, `show flash`, and/or `nvram`).(Citation: US-CERT-TA18-106A) Some files and directories may require elevated or specific user permissions to access.

Indicator

Name

aa0ef20f9f8ca111b0d8a550daf6651f5b0557f0acb0a26545755c5a02263a9b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'aa0ef20f9f8ca111b0d8a550daf6651f5b0557f0acb0a26545755c5a02263a9b']

Name

38f0750cbe49b30db326b53b9f752b66c4f5e23cc3bbbd6d1844e2878a19b9a7

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '38f0750cbe49b30db326b53b9f752b66c4f5e23cc3bbbd6d1844e2878a19b9a7']

Name

3f41e2ceff3a04cd6de6aadce7e7b7c8584940e4320a7db55dd712debb061510

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '3f41e2ceff3a04cd6de6aadce7e7b7c8584940e4320a7db55dd712debb061510']

Name

170d654b61810992fef6f18dbce5b4c7f5762cf36c9b41c36a14c9f6609f6e7d

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '170d654b61810992fef6f18dbce5b4c7f5762cf36c9b41c36a14c9f6609f6e7d']

Name

f572898ab9f9a0fabac77d5d388680f84f85f9eb2c01b4e5de426430c6b5008f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f572898ab9f9a0fabac77d5d388680f84f85f9eb2c01b4e5de426430c6b5008f']

Name

7101db8cb05e989c018ebc5df47819029cd76c4093b22c4582288795e46f6689

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '7101db8cb05e989c018ebc5df47819029cd76c4093b22c4582288795e46f6689']

Name

21ff399e57cc306a1ae1daab6009ea40c8aa96c39296d0f8781626de6bd19256

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '21ff399e57cc306a1ae1daab6009ea40c8aa96c39296d0f8781626de6bd19256']

Name

4d571f4d0008deb01e3144e0e3d5f882c5422acfcb4dd260082852a822d8d2fb

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '4d571f4d0008deb01e3144e0e3d5f882c5422acfcb4dd260082852a822d8d2fb']

Name

9562ad2c173b107a2baa7a4986825b52e881a935deb4356bf8b80b1ec6d41c53

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9562ad2c173b107a2baa7a4986825b52e881a935deb4356bf8b80b1ec6d41c53']

Name

67e4c18e80d4d1acb9395f4a1fe9c2a75d95fcccdb33bcdd5259ba6f47e60e57

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '67e4c18e80d4d1acb9395f4a1fe9c2a75d95fcccdb33bcdd5259ba6f47e60e57']

Name

2881194b7e0939d47165c894c891737d8c189ee8fb4720e814a4bcdd804d00d1

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2881194b7e0939d47165c894c891737d8c189ee8fb4720e814a4bcdd804d00d1']

Name

7d6877eb8a3e2da1e8b06e2ed41604c6c3d5ced8293f7cc7e760ba972303bd0e

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '7d6877eb8a3e2da1e8b06e2ed41604c6c3d5ced8293f7cc7e760ba972303bd0e']

Name

5e446efb6c4f296fb8f25ef7a1a0a482f51dc475bd5ef3e89be9d43782a9f60f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '5e446efb6c4f296fb8f25ef7a1a0a482f51dc475bd5ef3e89be9d43782a9f60f']

Name

3e65437f910f1f4e93809b81c19942ef74aa250ae228caca0b278fc523ad47c5

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '3e65437f910f1f4e93809b81c19942ef74aa250ae228caca0b278fc523ad47c5']

Name

6192488729850a7a28498f233346e856b0097e4b3160baa641f8cf9571b56da8

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6192488729850a7a28498f233346e856b0097e4b3160baa641f8cf9571b56da8']

Name

6fb438feeb8369c5b82bfaa77144a641f7645c321f0b24dd97cfe2687b1ebd44

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6fb438feeb8369c5b82bfaa77144a641f7645c321f0b24dd97cfe2687b1ebd44']

Name

95279881525d4ed4ce25777bb967ab87659e7f72235b76f9530456b48a00bac3

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '95279881525d4ed4ce25777bb967ab87659e7f72235b76f9530456b48a00bac3']

Name

4de4621da1b7da597c2c8def4c08b8d405672dadb9c70d7dffd647c8d6abd394

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '4de4621da1b7da597c2c8def4c08b8d405672dadb9c70d7dffd647c8d6abd394']

Name

aa43f34c3fa67aea994c1babeb71b46c7b24eccaa0455ae21aa561e251e7cc4d

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'aa43f34c3fa67aea994c1babeb71b46c7b24eccaa0455ae21aa561e251e7cc4d']

Name

bef2d817f1813eb0629222112fd3721865a2a4eb1f4d51ad1f09fd807d4380ab

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'bef2d817f1813eb0629222112fd3721865a2a4eb1f4d51ad1f09fd807d4380ab']

Name

ea59d6a130a279dfde4df53640bd720419c7b5d9711a21a78af9453b1b3b5805

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ea59d6a130a279dfde4df53640bd720419c7b5d9711a21a78af9453b1b3b5805']

Name

f6afa84b0847414220bb15517b8b5e2c505b64b53efbba73b753379c66ac5017

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f6afa84b0847414220bb15517b8b5e2c505b64b53efbba73b753379c66ac5017']

Name

88efa81984852dac62d325f2091a09de1e6423a711d7913aeac103c50664cf84

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '88efa81984852dac62d325f2091a09de1e6423a711d7913aeac103c50664cf84']

Name

d18453e564ca27514227478f225d85811fe15d08aa5fb1f613022c43155c5c54

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd18453e564ca27514227478f225d85811fe15d08aa5fb1f613022c43155c5c54']

Name

1453179d46ef89eb780f8b82632f352017a3586e8d49fc3f087f633f7bebbf0a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1453179d46ef89eb780f8b82632f352017a3586e8d49fc3f087f633f7bebbf0a']

Name

a702a671b7911a09ccb5b4f42923e8b301e0bbb851443dd52622022959a3055a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a702a671b7911a09ccb5b4f42923e8b301e0bbb851443dd52622022959a3055a']

Name

2fc2d747847eb04561a435e65954f0103101e2190458eb3c125deda49326c597

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2fc2d747847eb04561a435e65954f0103101e2190458eb3c125deda49326c597']

Malware

Name
LockBit
Name
Warp AV Killer
Name
Phobos
Name
BlackCat - S1068
Name
Akira
Description
[Akira](https://attack.mitre.org/software/S1129) ransomware, written in C++, is most prominently (but not exclusively) associated with the a ransomware-as-a-service entity [Akira](https://attack.mitre.org/groups/G1024).(Citation: Kersten Akira 2023)
Name

Qilin

Name

Noberus

Description

[BlackCat](https://attack.mitre.org/software/S1068) is ransomware written in Rust that has been offered via the Ransomware-as-a-Service (RaaS) model. First observed November 2021, [BlackCat](https://attack.mitre.org/software/S1068) has been used to target multiple sectors and organizations in various countries and regions in Africa, the Americas, Asia, Australia, and Europe.(Citation: Microsoft BlackCat Jun 2022)(Citation: Sophos BlackCat Jul 2022)(Citation: ACSC BlackCat Apr 2022)

Name

ransomware

Name

Cyclops Blink - S0687

Name

Play

Name

cyclops blink

Description

[Cyclops Blink](https://attack.mitre.org/software/S0687) is a modular malware that has been used in widespread campaigns by [Sandworm Team](https://attack.mitre.org/groups/G0034) since at least 2019 to target Small/Home Office (SOHO) network devices, including

WatchGuard and Asus.(Citation: NCSC Cyclops Blink February 2022)(Citation: NCSC CISA Cyclops Blink Advisory February 2022)(Citation: Trend Micro Cyclops Blink March 2022)

Name
Blacksuit

Name
TellYouThePass

indicates

Name
Name
Name
Name
Name
Name
Name
Name
Name
Name

Name
Name
Name
Name
Name
Name
Name

uses

Name

StixFile

Value
2881194b7e0939d47165c894c891737d8c189ee8fb4720e814a4bcdd804d00d1
9562ad2c173b107a2baa7a4986825b52e881a935deb4356bf8b80b1ec6d41c53
a702a671b7911a09ccb5b4f42923e8b301e0bbb851443dd52622022959a3055a
2fc2d747847eb04561a435e65954f0103101e2190458eb3c125deda49326c597
7d6877eb8a3e2da1e8b06e2ed41604c6c3d5ced8293f7cc7e760ba972303bd0e
3f41e2ceff3a04cd6de6aadce7e7b7c8584940e4320a7db55dd712debb061510
aa43f34c3fa67aea994c1babeb71b46c7b24eccaa0455ae21aa561e251e7cc4d
1453179d46ef89eb780f8b82632f352017a3586e8d49fc3f087f633f7bebbf0a
88efa81984852dac62d325f2091a09de1e6423a711d7913aeac103c50664cf84
95279881525d4ed4ce25777bb967ab87659e7f72235b76f9530456b48a00bac3
4d571f4d0008deb01e3144e0e3d5f882c5422acfcb4dd260082852a822d8d2fb
3e65437f910f1f4e93809b81c19942ef74aa250ae228caca0b278fc523ad47c5
6fb438feeb8369c5b82bfaa77144a641f7645c321f0b24dd97cfe2687b1ebd44

6192488729850a7a28498f233346e856b0097e4b3160baa641f8cf9571b56da8

f6afa84b0847414220bb15517b8b5e2c505b64b53efbba73b753379c66ac5017

67e4c18e80d4d1acb9395f4a1fe9c2a75d95fcccdb33bcdd5259ba6f47e60e57

4de4621da1b7da597c2c8def4c08b8d405672dadb9c70d7dffd647c8d6abd394

170d654b61810992fef6f18dbce5b4c7f5762cf36c9b41c36a14c9f6609f6e7d

aa0ef20f9f8ca111b0d8a550daf6651f5b0557f0acb0a26545755c5a02263a9b

5e446efb6c4f296fb8f25ef7a1a0a482f51dc475bd5ef3e89be9d43782a9f60f

7101db8cb05e989c018ebc5df47819029cd76c4093b22c4582288795e46f6689

21ff399e57cc306a1ae1daab6009ea40c8aa96c39296d0f8781626de6bd19256

d18453e564ca27514227478f225d85811fe15d08aa5fb1f613022c43155c5c54

f572898ab9f9a0fabac77d5d388680f84f85f9eb2c01b4e5de426430c6b5008f

38f0750cbe49b30db326b53b9f752b66c4f5e23cc3bbbd6d1844e2878a19b9a7

bef2d817f1813eb0629222112fd3721865a2a4eb1f4d51ad1f09fd807d4380ab

ea59d6a130a279dfde4df53640bd720419c7b5d9711a21a78af9453b1b3b5805

External References

- https://symantec-enterprise-blogs.security.com/threat-intelligence/ransomware-q2-2024
- https://otx.alienvault.com/pulse/668fd8ec788983816343aa3a