Feb 09 2024

NETMANAGEIT

Intelligence Report

Spyware isn't going anywhere, and neither are its tactics

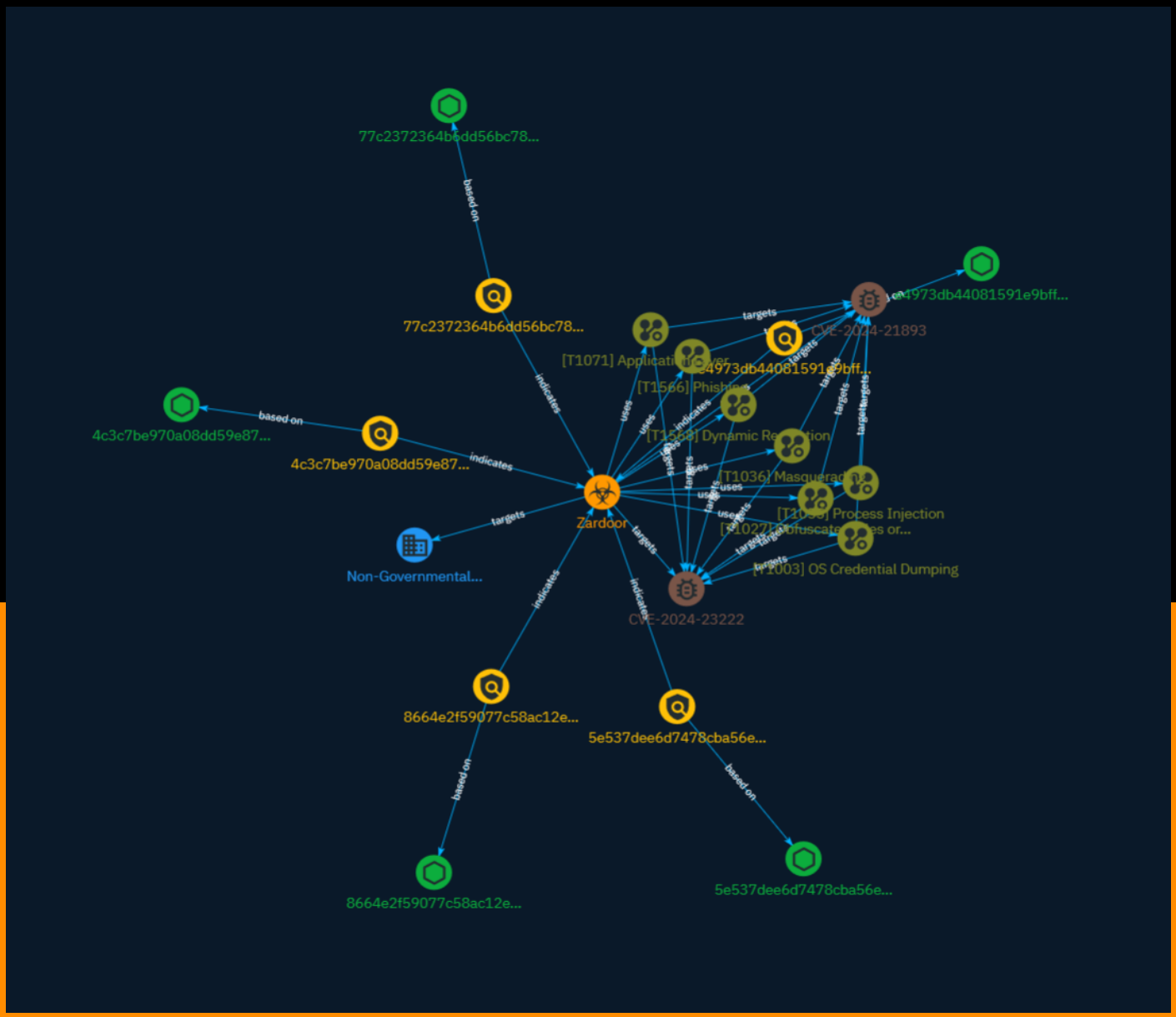

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Recent public and private efforts aim to curb spyware use, but its tendrils remain deep. Spyware can track targets and steal personal data. Private companies sell it regardless of motive. The US and allies want to limit spyware globally but current efforts seem aspirational. However, the US did restrict visas for spyware misuse. Many agree more action is needed. Spyware is embedded in ads, apps and the internet. To curb spyware, info sharing and detection is key. Talos found a new backdoor, Zardoor, used since 2021 in an espionage campaign. It evaded detection and exfiltrated data from a charity. More victims may exist. Talos released protections against it.

Confidence

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

15 / 100

Content

N/A

Indicator

Name
e4973db44081591e9bff5117946defbef6041397e56164f485cf8ec57b1d8934
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'e4973db44081591e9bff5117946defbef6041397e56164f485cf8ec57b1d8934']
Name
8664e2f59077c58ac12e747da09d2810fd5ca611f56c0c900578bf750cab56b7
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '8664e2f59077c58ac12e747da09d2810fd5ca611f56c0c900578bf750cab56b7']
Name

77c2372364b6dd56bc787fda46e6f4240aaa0353ead1e3071224d454038a545e

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '77c2372364b6dd56bc787fda46e6f4240aaa0353ead1e3071224d454038a545e']

Name

5e537dee6d7478cba56ebbcc7a695cae2609010a897d766ff578a4260c2ac9cf

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '5e537dee6d7478cba56ebbcc7a695cae2609010a897d766ff578a4260c2ac9cf']

Name

4c3c7be970a08dd59e87de24590b938045f14e693a43a83b81ce8531127eb440

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '4c3c7be970a08dd59e87de24590b938045f14e693a43a83b81ce8531127eb440']

Name

e4973db44081591e9bff5117946defbef6041397e56164f485cf8ec57b1d8934

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'e4973db44081591e9bff5117946defbef6041397e56164f485cf8ec57b1d8934']

Name

8664e2f59077c58ac12e747da09d2810fd5ca611f56c0c900578bf750cab56b7

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '8664e2f59077c58ac12e747da09d2810fd5ca611f56c0c900578bf750cab56b7']

Name

77c2372364b6dd56bc787fda46e6f4240aaa0353ead1e3071224d454038a545e

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '77c2372364b6dd56bc787fda46e6f4240aaa0353ead1e3071224d454038a545e']

Name

5e537dee6d7478cba56ebbcc7a695cae2609010a897d766ff578a4260c2ac9cf

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '5e537dee6d7478cba56ebbcc7a695cae2609010a897d766ff578a4260c2ac9cf']

Name

4c3c7be970a08dd59e87de24590b938045f14e693a43a83b81ce8531127eb440

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '4c3c7be970a08dd59e87de24590b938045f14e693a43a83b81ce8531127eb440']

Malware

Name
Zardoor

Name
Zardoor

Vulnerability

Name

CVE-2024-21893

Description

Ivanti Connect Secure (ICS, formerly known as Pulse Connect Secure), Ivanti Policy Secure, and Ivanti Neurons contain a server-side request forgery (SSRF) vulnerability in the SAML component that allows an attacker to access certain restricted resources without authentication.

Name

CVE-2024-23222

Description

Apple iOS, iPadOS, macOS, tvOS, and Safari WebKit contain a type confusion vulnerability that leads to code execution when processing maliciously crafted web content.

Name

CVE-2024-21893

Description

Ivanti Connect Secure (ICS, formerly known as Pulse Connect Secure), Ivanti Policy Secure, and Ivanti Neurons contain a server-side request forgery (SSRF) vulnerability in the SAML

component that allows an attacker to access certain restricted resources without authentication.

Name

CVE-2024-23222

Description

Apple iOS, iPadOS, macOS, tvOS, and Safari WebKit contain a type confusion vulnerability that leads to code execution when processing maliciously crafted web content.

Attack-Pattern

Name
Dynamic Resolution
ID
T1568
Description
Adversaries may dynamically establish connections to command and control infrastructure to evade common detections and remediations. This may be achieved by using malware that shares a common algorithm with the infrastructure the adversary uses to receive the malware's communications. These calculations can be used to dynamically adjust parameters such as the domain name, IP address, or port number the malware uses for command and control. Adversaries may use dynamic resolution for the purpose of [Fallback Channels](https://attack.mitre.org/techniques/T1008). When contact is lost with the primary command and control server malware may employ dynamic resolution as a means to reestablishing command and control.(Citation: Talos CCleanup 2017)(Citation: FireEye POSHSPY April 2017)(Citation: ESET Sednit 2017 Activity)
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

Phishing

ID

T1566

Description

Adversaries may send phishing messages to gain access to victim systems. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass malware spam campaigns. Adversaries may send victims emails containing malicious attachments or links, typically to execute malicious code on victim

systems. Phishing may also be conducted via third-party services, like social media platforms. Phishing may also involve social engineering techniques, such as posing as a trusted source, as well as evasive techniques such as removing or manipulating emails or metadata/headers from compromised accounts being abused to send messages (e.g., [Email Hiding Rules](https://attack.mitre.org/techniques/T1564/008)).(Citation: Microsoft OAuth Spam 2022)(Citation: Palo Alto Unit 42 VBA Infostealer 2014) Another way to accomplish this is by forging or spoofing(Citation: Proofpoint-spoof) the identity of the sender which can be used to fool both the human recipient as well as automated security tools.(Citation: cyberproof-double-bounce) Victims may also receive phishing messages that instruct them to call a phone number where they are directed to visit a malicious URL, download malware,(Citation: sygnia Luna Month)(Citation: CISA Remote Monitoring and Management Software) or install adversary-accessible remote management tools onto their computer (i.e., [User Execution](https://attack.mitre.org/techniques/T1204)).(Citation: Unit42 Luna Moth)

Name

Process Injection

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

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) Masquerading may also include the use of [Proxy](https://attack.mitre.org/techniques/T1090) or VPNs to disguise IP addresses, which can allow adversaries to blend in with normal network traffic and bypass conditional access policies or anti-abuse protections.

Name

Application Layer Protocol

ID

T1071

Description

Adversaries may communicate using OSI application layer protocols to avoid detection/network filtering by blending in with existing traffic. Commands to the remote system, and often the results of those commands, will be embedded within the protocol traffic between the client and server. Adversaries may utilize many different protocols, including those used for web browsing, transferring files, electronic mail, or DNS. For connections that occur internally within an enclave (such as those between a proxy or pivot node and other nodes), commonly used protocols are SMB, SSH, or RDP.

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

Dynamic Resolution

ID

T1568

Description

Adversaries may dynamically establish connections to command and control infrastructure to evade common detections and remediations. This may be achieved by using malware that shares a common algorithm with the infrastructure the adversary uses to receive the malware's communications. These calculations can be used to dynamically adjust parameters such as the domain name, IP address, or port number the malware uses for command and control. Adversaries may use dynamic resolution for the purpose of [Fallback Channels](https://attack.mitre.org/techniques/T1008). When contact is lost with the primary command and control server malware may employ dynamic resolution as a means to reestablishing command and control.(Citation: Talos CCleanup 2017)(Citation: FireEye POSHSPY April 2017)(Citation: ESET Sednit 2017 Activity)

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

Phishing

ID

T1566

Description

Adversaries may send phishing messages to gain access to victim systems. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass malware spam campaigns. Adversaries may send victims emails containing malicious attachments or links, typically to execute malicious code on victim systems. Phishing may also be conducted via third-party services, like social media platforms. Phishing may also involve social engineering techniques, such as posing as a trusted source, as well as evasive techniques such as removing or manipulating emails or metadata/headers from compromised accounts being abused to send messages (e.g., [Email Hiding Rules](https://attack.mitre.org/techniques/T1564/008)).(Citation: Microsoft OAuth Spam 2022)(Citation: Palo Alto Unit 42 VBA Infostealer 2014) Another way to accomplish this is by forging or spoofing(Citation: Proofpoint-spoof) the identity of the sender which can be used to fool both the human recipient as well as automated security tools.(Citation: cyberproof-double-bounce) Victims may also receive phishing messages that instruct them to call a phone number where they are directed to visit a malicious URL, download malware,(Citation: sygnia Luna Month)(Citation: CISA Remote Monitoring and Management Software) or install adversary-accessible remote management tools onto their computer (i.e., [User Execution](https://attack.mitre.org/techniques/T1204)).(Citation: Unit42 Luna Moth)

Name

Process Injection

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

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) Masquerading may also include the use of [Proxy](https://attack.mitre.org/techniques/T1090) or VPNs to disguise IP addresses, which can allow adversaries to blend in with normal network traffic and bypass conditional access policies or anti-abuse protections.

Name

Application Layer Protocol

ID

T1071

Description

Adversaries may communicate using OSI application layer protocols to avoid detection/network filtering by blending in with existing traffic. Commands to the remote system, and often the results of those commands, will be embedded within the protocol traffic between the client and server. Adversaries may utilize many different protocols, including those used for web browsing, transferring files, electronic mail, or DNS. For connections that occur internally within an enclave (such as those between a proxy or pivot node and other nodes), commonly used protocols are SMB, SSH, or RDP.

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.

Sector

Name
Non-Governmental Organizations (NGOs)
Description
A legally constituted non-commercial organization created by natural or legal persons with no participation or representation of any government.
Name
Non-Governmental Organizations (NGOs)
Description
A legally constituted non-commercial organization created by natural or legal persons with no participation or representation of any government.

StixFile

Value
e4973db44081591e9bff5117946defbef6041397e56164f485cf8ec57b1d8934
8664e2f59077c58ac12e747da09d2810fd5ca611f56c0c900578bf750cab56b7
77c2372364b6dd56bc787fda46e6f4240aaa0353ead1e3071224d454038a545e
5e537dee6d7478cba56ebbcc7a695cae2609010a897d766ff578a4260c2ac9cf
4c3c7be970a08dd59e87de24590b938045f14e693a43a83b81ce8531127eb440
e4973db44081591e9bff5117946defbef6041397e56164f485cf8ec57b1d8934
8664e2f59077c58ac12e747da09d2810fd5ca611f56c0c900578bf750cab56b7
77c2372364b6dd56bc787fda46e6f4240aaa0353ead1e3071224d454038a545e
5e537dee6d7478cba56ebbcc7a695cae2609010a897d766ff578a4260c2ac9cf
4c3c7be970a08dd59e87de24590b938045f14e693a43a83b81ce8531127eb440

External References

- https://blog.talosintelligence.com/threat-source-newsletter-feb-8-2024/
- https://otx.alienvault.com/pulse/65c540e800692ac0e30ffec2