Feb 05 2024

NETMANAGEIT

Intelligence Report

Distribution of Zephyr CoinMiner Using Autoit

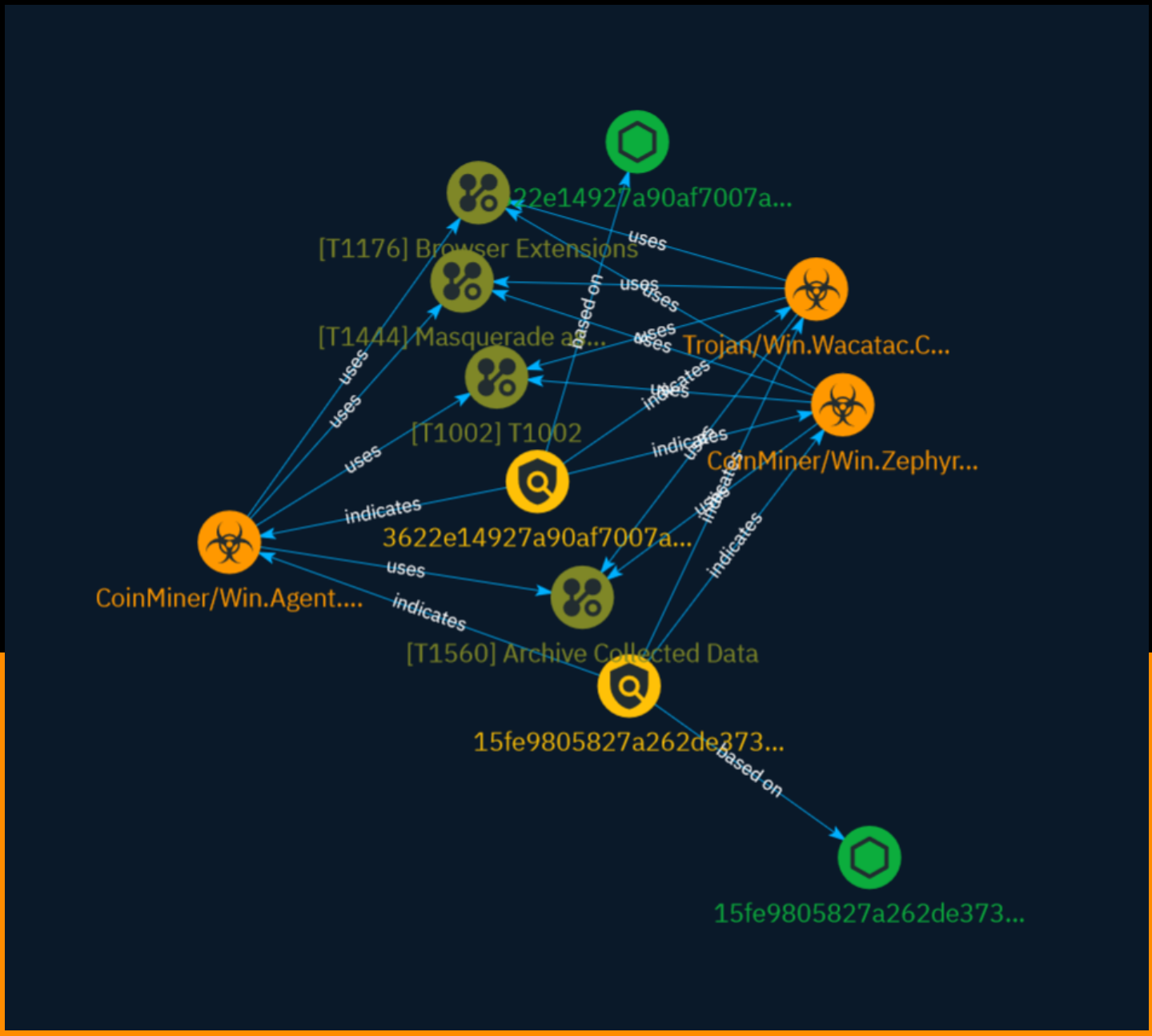

Table of contents

Overview

Entities

Observables

External References

Overview

Description

A CoinMiner that mines Zephyr, the crytocurrency, is being distributed with Autoit, a popular tool for detecting and detecting cyber-thieves.

Confidence

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

15 / 100

Content

N/A

Indicator

Name
3622e14927a90af7007ae998f647f11813f0dfb49eda36f5e8a9cab14c5961b4
Description
Themida_2xx SHA256 of 6647cd9d0ab63506c230fbce8019d0b8
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '3622e14927a90af7007ae998f647f11813f0dfb49eda36f5e8a9cab14c5961b4']
Name
15fe9805827a262de3738dad2c1f8e2dbcdf43e13e42e558e63e3a1c169cbef1
Description
Nullsoft_NSIS SHA256 of 2b7931a70748c38c8046dea9dc708379
Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '15fe9805827a262de3738dad2c1f8e2dbcdf43e13e42e558e63e3a1c169cbef1']

Name

3622e14927a90af7007ae998f647f11813f0dfb49eda36f5e8a9cab14c5961b4

Description

Themida_2xx SHA256 of 6647cd9d0ab63506c230fbce8019d0b8

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '3622e14927a90af7007ae998f647f11813f0dfb49eda36f5e8a9cab14c5961b4']

Name

15fe9805827a262de3738dad2c1f8e2dbcdf43e13e42e558e63e3a1c169cbef1

Description

Nullsoft_NSIS SHA256 of 2b7931a70748c38c8046dea9dc708379

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '15fe9805827a262de3738dad2c1f8e2dbcdf43e13e42e558e63e3a1c169cbef1']

Malware

Name
CoinMiner/Win.Zephyr.C5575600
Name
CoinMiner/Win.Agent.R631683
Name
Trojan/Win.Wacatac.C5571541
Name
CoinMiner/Win.Zephyr.C5575600
Name
CoinMiner/Win.Agent.R631683
Name
Trojan/Win.Wacatac.C5571541

Attack-Pattern

Name

Masquerade as Legitimate Application

ID

T1444

Description

An adversary could distribute developed malware by masquerading the malware as a legitimate application. This can be done in two different ways: by embedding the malware in a legitimate application, or by pretending to be a legitimate application. Embedding the malware in a legitimate application is done by downloading the application, disassembling it, adding the malicious code, and then re-assembling it.(Citation: Zhou) The app would appear to be the original app, but would contain additional malicious functionality. The adversary could then publish the malicious application to app stores or use another delivery method. Pretending to be a legitimate application relies heavily on lack of scrutinization by the user. Typically, a malicious app pretending to be a legitimate one will have many similar details as the legitimate one, such as name, icon, and description. (Citation: Palo Alto HenBox) Malicious applications may also masquerade as legitimate applications when requesting access to the accessibility service in order to appear as legitimate to the user, increasing the likelihood that the access will be granted.

Name

T1002

ID

T1002

Name

Archive Collected Data

ID

T1560

Description

An adversary may compress and/or encrypt data that is collected prior to exfiltration. Compressing the data can help to obfuscate the collected data and minimize the amount of data sent over the network. Encryption can be used to hide information that is being exfiltrated from detection or make exfiltration less conspicuous upon inspection by a defender. Both compression and encryption are done prior to exfiltration, and can be performed using a utility, 3rd party library, or custom method.

Name

Browser Extensions

ID

T1176

Description

Adversaries may abuse Internet browser extensions to establish persistent access to victim systems. Browser extensions or plugins are small programs that can add functionality and customize aspects of Internet browsers. They can be installed directly or through a browser's app store and generally have access and permissions to everything that the browser can access.(Citation: Wikipedia Browser Extension)(Citation: Chrome Extensions Definition) Malicious extensions can be installed into a browser through malicious app store downloads masquerading as legitimate extensions, through social engineering, or by an adversary that has already compromised a system. Security can be limited on browser app stores so it may not be difficult for malicious extensions to defeat automated

scanners.(Citation: Malicious Chrome Extension Numbers) Depending on the browser, adversaries may also manipulate an extension's update url to install updates from an adversary controlled server or manipulate the mobile configuration file to silently install additional extensions. Previous to macOS 11, adversaries could silently install browser extensions via the command line using the `profiles` tool to install malicious `.mobileconfig` files. In macOS 11+, the use of the `profiles` tool can no longer install configuration profiles, however `.mobileconfig` files can be planted and installed with user interaction.(Citation: xorrior chrome extensions macOS) Once the extension is installed, it can browse to websites in the background, steal all information that a user enters into a browser (including credentials), and be used as an installer for a RAT for persistence. (Citation: Chrome Extension Crypto Miner)(Citation: ICEBRG Chrome Extensions)(Citation: Banker Google Chrome Extension Steals Creds)(Citation: Catch All Chrome Extension) There have also been instances of botnets using a persistent backdoor through malicious Chrome extensions.(Citation: Stantinko Botnet) There have also been similar examples of extensions being used for command & control.(Citation: Chrome Extension C2 Malware)

Name

Masquerade as Legitimate Application

ID

T1444

Description

An adversary could distribute developed malware by masquerading the malware as a legitimate application. This can be done in two different ways: by embedding the malware in a legitimate application, or by pretending to be a legitimate application. Embedding the malware in a legitimate application is done by downloading the application, disassembling it, adding the malicious code, and then re-assembling it.(Citation: Zhou) The app would appear to be the original app, but would contain additional malicious functionality. The adversary could then publish the malicious application to app stores or use another delivery method. Pretending to be a legitimate application relies heavily on lack of scrutinization by the user. Typically, a malicious app pretending to be a legitimate one will have many similar details as the legitimate one, such as name, icon, and description. (Citation: Palo Alto HenBox) Malicious applications may also masquerade as legitimate applications when requesting access to the accessibility service in order to appear as legitimate to the user, increasing the likelihood that the access will be granted.

Name

T1002

ID

T1002

Name

Archive Collected Data

ID

T1560

Description

An adversary may compress and/or encrypt data that is collected prior to exfiltration. Compressing the data can help to obfuscate the collected data and minimize the amount of data sent over the network. Encryption can be used to hide information that is being exfiltrated from detection or make exfiltration less conspicuous upon inspection by a defender. Both compression and encryption are done prior to exfiltration, and can be performed using a utility, 3rd party library, or custom method.

Name

Browser Extensions

ID

T1176

Description

Adversaries may abuse Internet browser extensions to establish persistent access to victim systems. Browser extensions or plugins are small programs that can add functionality and customize aspects of Internet browsers. They can be installed directly or through a browser's app store and generally have access and permissions to everything that the browser can access.(Citation: Wikipedia Browser Extension)(Citation: Chrome Extensions Definition) Malicious extensions can be installed into a browser through malicious app store downloads masquerading as legitimate extensions, through social engineering, or by an adversary that has already compromised a system. Security can be limited on browser app stores so it may not be difficult for malicious extensions to defeat automated scanners.(Citation: Malicious Chrome Extension Numbers) Depending on the browser, adversaries may also manipulate an extension's update url to install updates from an adversary controlled server or manipulate the mobile configuration file to silently install additional extensions. Previous to macOS 11, adversaries could silently install browser extensions via the command line using the `profiles` tool to install malicious `.mobileconfig` files. In macOS 11+, the use of the `profiles` tool can no longer install configuration profiles, however `.mobileconfig` files can be planted and installed with user interaction.(Citation: xorrior chrome extensions macOS) Once the extension is installed, it can browse to websites in the background, steal all information that a user enters into a browser (including credentials), and be used as an installer for a RAT for persistence. (Citation: Chrome Extension Crypto Miner)(Citation: ICEBRG Chrome Extensions)(Citation: Banker Google Chrome Extension Steals Creds)(Citation: Catch All Chrome Extension) There have also been instances of botnets using a persistent backdoor through malicious Chrome extensions.(Citation: Stantinko Botnet) There have also been similar examples of extensions being used for command & control.(Citation: Chrome Extension C2 Malware)

StixFile

Value
3622e14927a90af7007ae998f647f11813f0dfb49eda36f5e8a9cab14c5961b4
15fe9805827a262de3738dad2c1f8e2dbcdf43e13e42e558e63e3a1c169cbef1
3622e14927a90af7007ae998f647f11813f0dfb49eda36f5e8a9cab14c5961b4
15fe9805827a262de3738dad2c1f8e2dbcdf43e13e42e558e63e3a1c169cbef1

External References

- https://asec.ahnlab.com/en/61164/
- https://otx.alienvault.com/pulse/65c0f246bb1492cec382cf73