Jan 25 2024

NETMANAGEIT

Intelligence Report

JAVA-Based Sophisticated Stealer Using Discord Bot as EventListener

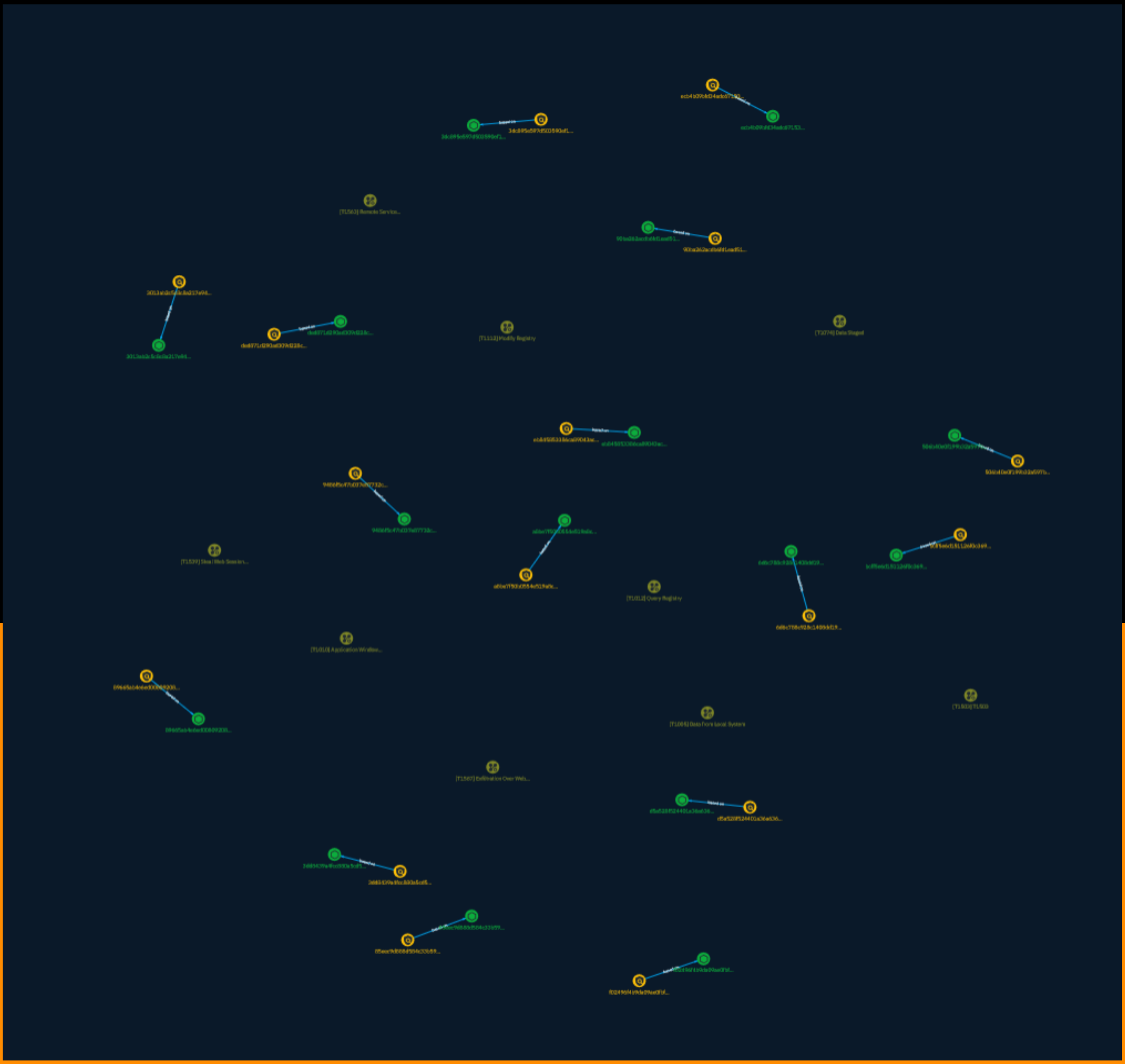

Table of contents

Overview

Entities

Observables

External References

Overview

Description

In mid-November 2023, Trellix Advanced Research Center team members observed a Java-based stealer being spread through cracked software zip files using JDABuilder Classes to create an instance of the EventListener to easily register. The Stealer uses Discord bot channel as an EventListener.

Confidence

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

15 / 100

Content

N/A

Attack-Pattern

Name
Query Registry
ID
T1012
Description
Adversaries may interact with the Windows Registry to gather information about the system, configuration, and installed software. The Registry contains a significant amount of information about the operating system, configuration, software, and security.(Citation: Wikipedia Windows Registry) Information can easily be queried using the [Reg](https://attack.mitre.org/software/S0075) utility, though other means to access the Registry exist. Some of the information may help adversaries to further their operation within a network. Adversaries may use the information from [Query Registry](https://attack.mitre.org/techniques/T1012) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions.
Name
Application Window Discovery
ID
T1010

Description

Adversaries may attempt to get a listing of open application windows. Window listings could convey information about how the system is used.(Citation: Prevailion DarkWatchman 2021) For example, information about application windows could be used identify potential data to collect as well as identifying security tooling ([Security Software Discovery](https://attack.mitre.org/techniques/T1518/001)) to evade.(Citation: ESET Grandoreiro April 2020) Adversaries typically abuse system features for this type of enumeration. For example, they may gather information through native system features such as [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059) commands and [Native API](https://attack.mitre.org/techniques/T1106) functions.

Name

Modify Registry

ID

T1112

Description

Adversaries may interact with the Windows Registry to hide configuration information within Registry keys, remove information as part of cleaning up, or as part of other techniques to aid in persistence and execution. Access to specific areas of the Registry depends on account permissions, some requiring administrator-level access. The built-in Windows command-line utility [Reg](https://attack.mitre.org/software/S0075) may be used for local or remote Registry modification. (Citation: Microsoft Reg) Other tools may also be used, such as a remote access tool, which may contain functionality to interact with the Registry through the Windows API. Registry modifications may also include actions to hide keys, such as prepending key names with a null character, which will cause an error and/or be ignored when read via [Reg](https://attack.mitre.org/software/S0075) or other utilities using the Win32 API. (Citation: Microsoft Reghide NOV 2006) Adversaries may abuse these pseudo-hidden keys to conceal payloads/commands used to maintain persistence. (Citation: TrendMicro POWELIKS AUG 2014) (Citation: SpectorOps Hiding Reg Jul 2017) The Registry of a remote system may be modified to aid in execution of files as part of lateral movement. It requires the remote Registry service to be running on the target system. (Citation: Microsoft Remote) Often [Valid Accounts](https://attack.mitre.org/techniques/

T1078) are required, along with access to the remote system's [SMB/Windows Admin Shares](https://attack.mitre.org/techniques/T1021/002) for RPC communication.

Name

Data from Local System

ID

T1005

Description

Adversaries may search local system sources, such as file systems and configuration files or local databases, to find files of interest and sensitive data prior to Exfiltration. Adversaries may do this using a [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059), such as [cmd](https://attack.mitre.org/software/S0106) as well as a [Network Device CLI](https://attack.mitre.org/techniques/T1059/008), which have functionality to interact with the file system to gather information.(Citation: show_run_config_cmd_cisco) Adversaries may also use [Automated Collection](https://attack.mitre.org/techniques/T1119) on the local system.

Name

Steal Web Session Cookie

ID

T1539

Description

An adversary may steal web application or service session cookies and use them to gain access to web applications or Internet services as an authenticated user without needing credentials. Web applications and services often use session cookies as an authentication token after a user has authenticated to a website. Cookies are often valid for an extended period of time, even if the web application is not actively used. Cookies can be found on disk, in the process memory of the browser, and in network traffic to remote systems.

Additionally, other applications on the targets machine might store sensitive authentication cookies in memory (e.g. apps which authenticate to cloud services). Session cookies can be used to bypasses some multi-factor authentication protocols.(Citation: Pass The Cookie) There are several examples of malware targeting cookies from web browsers on the local system.(Citation: Kaspersky TajMahal April 2019)(Citation: Unit 42 Mac Crypto Cookies January 2019) There are also open source frameworks such as `Evilginx2` and `Muraena` that can gather session cookies through a malicious proxy (ex: [Adversary-in-the-Middle](https://attack.mitre.org/techniques/T1557)) that can be set up by an adversary and used in phishing campaigns.(Citation: Github evilginx2)(Citation: GitHub Mauraena) After an adversary acquires a valid cookie, they can then perform a [Web Session Cookie](https://attack.mitre.org/techniques/T1550/004) technique to login to the corresponding web application.

Name

Data Staged

ID

T1074

Description

Adversaries may stage collected data in a central location or directory prior to Exfiltration. Data may be kept in separate files or combined into one file through techniques such as [Archive Collected Data](https://attack.mitre.org/techniques/T1560). Interactive command shells may be used, and common functionality within [cmd](https://attack.mitre.org/software/S0106) and bash may be used to copy data into a staging location.(Citation: PWC Cloud Hopper April 2017) In cloud environments, adversaries may stage data within a particular instance or virtual machine before exfiltration. An adversary may [Create Cloud Instance](https://attack.mitre.org/techniques/T1578/002) and stage data in that instance.(Citation: Mandiant M-Trends 2020) Adversaries may choose to stage data from a victim network in a centralized location prior to Exfiltration to minimize the number of connections made to their C2 server and better evade detection.

Name

Exfiltration Over Web Service

ID

T1567

Description

Adversaries may use an existing, legitimate external Web service to exfiltrate data rather than their primary command and control channel. Popular Web services acting as an exfiltration mechanism may give a significant amount of cover due to the likelihood that hosts within a network are already communicating with them prior to compromise. Firewall rules may also already exist to permit traffic to these services. Web service providers also commonly use SSL/TLS encryption, giving adversaries an added level of protection.

Name

Remote Service Session Hijacking

ID

T1563

Description

Adversaries may take control of preexisting sessions with remote services to move laterally in an environment. Users may use valid credentials to log into a service specifically designed to accept remote connections, such as telnet, SSH, and RDP. When a user logs into a service, a session will be established that will allow them to maintain a continuous interaction with that service. Adversaries may commandeer these sessions to carry out actions on remote systems. [Remote Service Session Hijacking](https://attack.mitre.org/techniques/T1563) differs from use of [Remote Services](https://attack.mitre.org/techniques/T1021) because it hijacks an existing session rather than creating a new session using [Valid Accounts](https://attack.mitre.org/techniques/T1078).(Citation: RDP Hijacking Medium)(Citation: Breach Post-mortem SSH Hijack)

Name

T1503

ID
T1503

Indicator

Name
eb845853386ca89043ac04ec399e5111a906fd2bcde24ab02494eb035fdd1224
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'eb845853386ca89043ac04ec399e5111a906fd2bcde24ab02494eb035fdd1224']
Name
90ba262acdb6fd1ead5167a7347a1d66ee0075c24ed18d5b4cb07933a4c42805
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '90ba262acdb6fd1ead5167a7347a1d66ee0075c24ed18d5b4cb07933a4c42805']
Name

a8be7f50b0554e519a8c98ec39d2ba76e0655da133c8795a41d36dc29d9c7433

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a8be7f50b0554e519a8c98ec39d2ba76e0655da133c8795a41d36dc29d9c7433']

Name

3013ab2c5c8c8a217e9484f6a46fbacacbce92475dbe7f8d5e3f04d23974de83

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '3013ab2c5c8c8a217e9484f6a46fbacacbce92475dbe7f8d5e3f04d23974de83']

Name

d5a528f524401a36a6366619f3b2d83efed740801128f527e9dce80e68060922

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'd5a528f524401a36a6366619f3b2d83efed740801128f527e9dce80e68060922']

Name

89665ab4e6ed00809208a4656bc38da81831fd4b8044d7039e5542fe47b81d0e

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'89665ab4e6ed00809208a4656bc38da81831fd4b8044d7039e5542fe47b81d0e']

Name

3dc895e597d503590ef117dd942709a180392c9522c704901e272113bea8310f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'3dc895e597d503590ef117dd942709a180392c9522c704901e272113bea8310f']

Name

3dd8439a4fcc880a5cd5df005e15638be298993c141c200e47c769ef2e3ca1f4

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'3dd8439a4fcc880a5cd5df005e15638be298993c141c200e47c769ef2e3ca1f4']

Name

9486f5c47b037e87732c0c7d7d686334d7c3761133735f8b6d65b3aa479ec113

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'9486f5c47b037e87732c0c7d7d686334d7c3761133735f8b6d65b3aa479ec113']

Name

506b40e0f199b32a597bb44aa90343cc14830796f2bf3fd7c3fa281a52ce27c9

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'506b40e0f199b32a597bb44aa90343cc14830796f2bf3fd7c3fa281a52ce27c9']

Name

85eec9d888d584c33b597d6e40f1a74b4d00db9838d681339b845bb87c14cd10

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '85eec9d888d584c33b597d6e40f1a74b4d00db9838d681339b845bb87c14cd10']

Name

ecb4b09bfd34adc671537c98d1b1cd6f662e66077904db0da9f88e2054ef9edd

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ecb4b09bfd34adc671537c98d1b1cd6f662e66077904db0da9f88e2054ef9edd']

Name

6d6c788c928c1408dd19de83b6dd1a12092c96b179fc17a66414886cf8d1daf0

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6d6c788c928c1408dd19de83b6dd1a12092c96b179fc17a66414886cf8d1daf0']

Name

ded871d290ad309d228c00107d87e88dfadbc9d682ff3e04d9fb63f2c34aa256

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ded871d290ad309d228c00107d87e88dfadbc9d682ff3e04d9fb63f2c34aa256']

Name

bcff5e6d151126f0c3691b8c0fc46fb4e586ee5559068ac3acc2bd478c1c9ca1

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'bcff5e6d151126f0c3691b8c0fc46fb4e586ee5559068ac3acc2bd478c1c9ca1']

Name

f02496f4b9da09ae0fbf1b59fbdc4b2193cc9e03134ee4c5e71141bb618fdd0c

Pattern Type

stix
Pattern
[file:hashes.'SHA-256' = 'f02496f4b9da09ae0fbf1b59fbdc4b2193cc9e03134ee4c5e71141bb618fdd0c']

StixFile

Value
d5a528f524401a36a6366619f3b2d83efed740801128f527e9dce80e68060922
ded871d290ad309d228c00107d87e88dfadbc9d682ff3e04d9fb63f2c34aa256
85eec9d888d584c33b597d6e40f1a74b4d00db9838d681339b845bb87c14cd10
3dc895e597d503590ef117dd942709a180392c9522c704901e272113bea8310f
506b40e0f199b32a597bb44aa90343cc14830796f2bf3fd7c3fa281a52ce27c9
89665ab4e6ed00809208a4656bc38da81831fd4b8044d7039e5542fe47b81d0e
6d6c788c928c1408dd19de83b6dd1a12092c96b179fc17a66414886cf8d1daf0
9486f5c47b037e87732c0c7d7d686334d7c3761133735f8b6d65b3aa479ec113
3013ab2c5c8c8a217e9484f6a46fbacacbce92475dbe7f8d5e3f04d23974de83
ecb4b09bfd34adc671537c98d1b1cd6f662e66077904db0da9f88e2054ef9edd
bcff5e6d151126f0c3691b8c0fc46fb4e586ee5559068ac3acc2bd478c1c9ca1
90ba262acdb6fd1ead5167a7347a1d66ee0075c24ed18d5b4cb07933a4c42805
eb845853386ca89043ac04ec399e5111a906fd2bcde24ab02494eb035fdd1224

3dd8439a4fcc880a5cd5df005e15638be298993c141c200e47c769ef2e3ca1f4
a8be7f50b0554e519a8c98ec39d2ba76e0655da133c8795a41d36dc29d9c7433
f02496f4b9da09ae0fbf1b59fbdc4b2193cc9e03134ee4c5e71141bb618fdd0c

External References

- https://otx.alienvault.com/pulse/65b15516bfe5a5cc02280ba2
- https://www.trellix.com/about/newsroom/stories/research/java-based-sophisticated-stealer-using-discord-bot-as-eventlistener/