Feb 15 2024

NETMANAGEIT

Intelligence Report

TinyTurla Next Generation - Turla APT spies on Polish NGOs

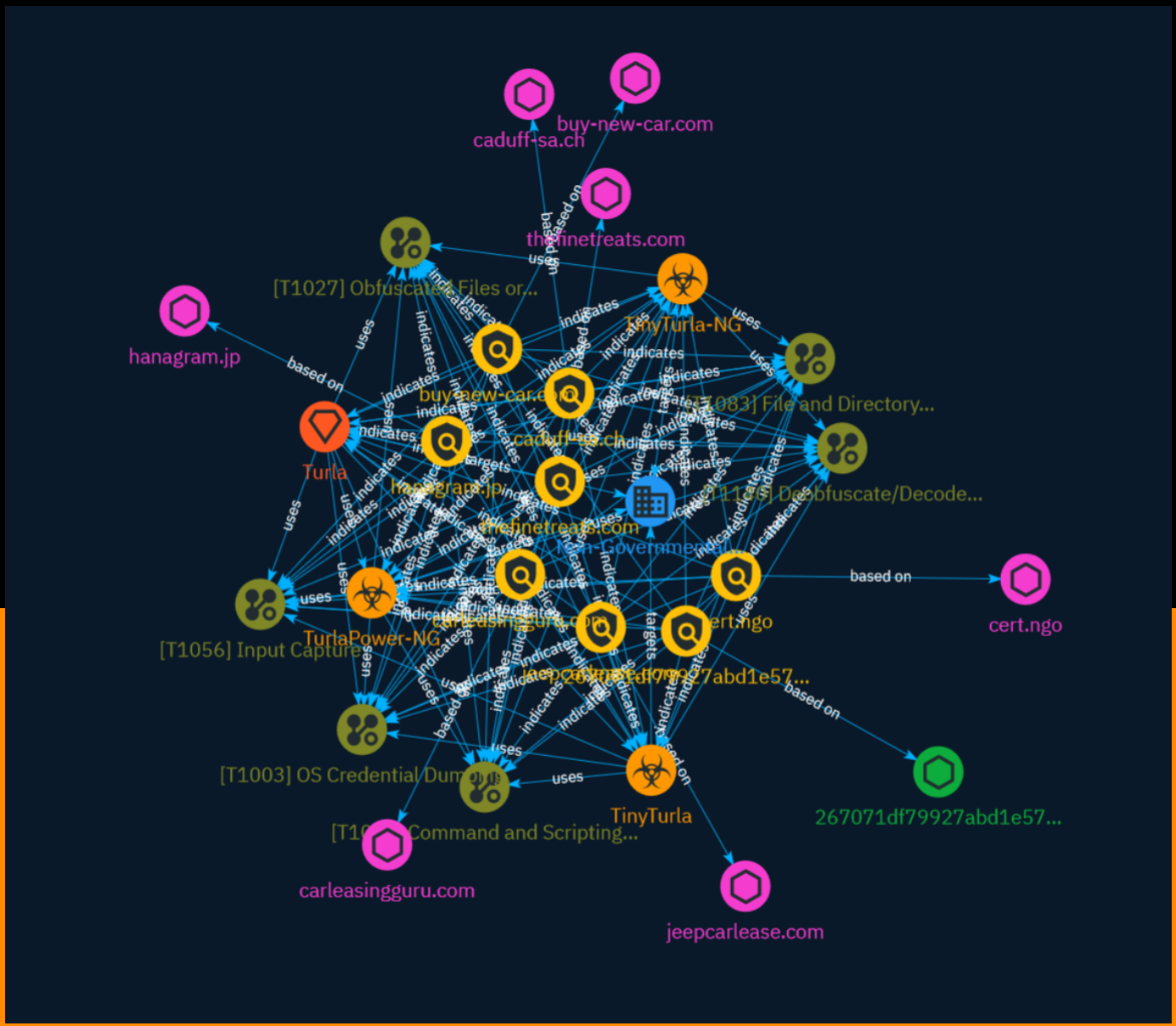

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Cisco Talos has identified a new backdoor authored and operated by the Turla APT group, a Russian cyber espionage threat actor. This backdoor, called TinyTurla-NG, is similar to Turla's previous implant TinyTurla in coding style and functionality. TinyTurla-NG was seen targeting a Polish non-governmental organization working on improving Polish democracy and supporting Ukraine. The backdoor deployed PowerShell scripts called TurlaPower-NG to exfiltrate key material used to secure password databases, indicating an effort to steal login credentials.

Confidence

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

15 / 100

Content

N/A

Indicator

Name
thefinetreats.com
Pattern Type
stix
Pattern
[domain-name:value = 'thefinetreats.com']
Name
jeepcarlease.com
Pattern Type
stix
Pattern
[domain-name:value = 'jeepcarlease.com']
Name
hanagram.jp

Pattern Type
stix
Pattern
[domain-name:value = 'hanagram.jp']
Name
cert.ngo
Pattern Type
stix
Pattern
[domain-name:value = 'cert.ngo']
Name
carleasingguru.com
Pattern Type
stix
Pattern
[domain-name:value = 'carleasingguru.com']
Name
caduff-sa.ch

Pattern Type
stix
Pattern
[domain-name:value = 'caduff-sa.ch']
Name
267071df79927abd1e57f57106924dd8a68e1c4ed74e7b69403cdcdf6e6a453b
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '267071df79927abd1e57f57106924dd8a68e1c4ed74e7b69403cdcdf6e6a453b']
Name
buy-new-car.com
Pattern Type
stix
Pattern
[domain-name:value = 'buy-new-car.com']

Malware

Name
TurlaPower-NG
Name
TinyTurla-NG
Name
TinyTurla
Description
[TinyTurla](https://attack.mitre.org/software/S0668) is a backdoor that has been used by [Turla](https://attack.mitre.org/groups/G0010) against targets in the US, Germany, and Afghanistan since at least 2020.(Citation: Talos TinyTurla September 2021)

Intrusion-Set

Name
Turla

Description
[Turla](https://attack.mitre.org/groups/G0010) is a cyber espionage threat group that has been attributed to Russia's Federal Security Service (FSB). They have compromised victims in over 50 countries since at least 2004, spanning a range of industries including government, embassies, military, education, research and pharmaceutical companies. [Turla](https://attack.mitre.org/groups/G0010) is known for conducting watering hole and spearphishing campaigns, and leveraging in-house tools and malware, such as [Uroburos](https://attack.mitre.org/software/S0022).(Citation: Kaspersky Turla)(Citation: ESET Gazer Aug 2017)(Citation: CrowdStrike VENOMOUS BEAR)(Citation: ESET Turla Mosquito Jan 2018)(Citation: Joint Cybersecurity Advisory AA23-129A Snake Malware May 2023)

Attack-Pattern

Name
Input Capture
ID
T1056
Description
Adversaries may use methods of capturing user input to obtain credentials or collect information. During normal system usage, users often provide credentials to various different locations, such as login pages/portals or system dialog boxes. Input capture mechanisms may be transparent to the user (e.g. [Credential API Hooking](https://attack.mitre.org/techniques/T1056/004)) or rely on deceiving the user into providing input into what they believe to be a genuine service (e.g. [Web Portal Capture](https://attack.mitre.org/techniques/T1056/003)).
Name
File and Directory Discovery
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)

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

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

Deobfuscate/Decode Files or Information

ID

T1140

Description

Adversaries may use [Obfuscated Files or Information](https://attack.mitre.org/techniques/T1027) to hide artifacts of an intrusion from analysis. They may require separate mechanisms to decode or deobfuscate that information depending on how they intend to use it. Methods for doing that include built-in functionality of malware or by using utilities present on the system. One such example is the use of [certutil](https://attack.mitre.org/software/S0160) to decode a remote access tool portable executable file that has been hidden inside a certificate file.(Citation: Malwarebytes Targeted Attack against Saudi Arabia) Another example is using the Windows `copy /b` command to reassemble binary fragments into a malicious payload.(Citation: Carbon Black Obfuscation Sept 2016) Sometimes a user's action may be required to open it for deobfuscation or decryption as part of [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)

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.

Domain-Name

Value
thefinetreats.com
jeepcarlease.com
hanagram.jp
cert.ngo
carleasingguru.com
caduff-sa.ch
buy-new-car.com

StixFile

Value
267071df79927abd1e57f57106924dd8a68e1c4ed74e7b69403cdcdf6e6a453b

External References

- https://blog.talosintelligence.com/tinyturla-next-generation/
- https://otx.alienvault.com/pulse/65ce2367ea7518a38c69ed4d