Feb 18 2024

NETMANAGEIT

Intelligence Report

TicTacToe Dropper

Table of contents

Overview

- Description 4
- Confidence 4
- Content 5

Entities

- Indicator 6
- Malware 11
- Attack-Pattern 14

Observables

- Url 17
- StixFile 18
- IPv4-Addr 19

External References

- External References 20

Overview

Description

Analysis of malware samples identified a grouping of malware droppers used to deliver various final-stage payloads in 2023. The droppers employ multiple stages of obfuscated payloads loaded reflectively. Final payloads include info-stealers and remote access trojans. Dropper exhibits anomalous behaviors like multi-stage extraction and reflective loading detectable by EDR.

Confidence

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

15 / 100

Content

N/A

Indicator

Name

http://64.227.48.212/project/five/fre.php

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': 'N/A', 'timestamp': None, 'iso': None} - **IPQS: Domain:** 64.227.48.212 - **IPQS: IP Address:** 127.0.0.1

Pattern Type

stix

Pattern

[url:value = 'http://64.227.48.212/project/five/fre.php']

Name

a5a5b60edcbbb203cb1965b1d544b74c47284e015ffd50312de0a251141bfbd7

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a5a5b60edcbbb203cb1965b1d544b74c47284e015ffd50312de0a251141bfbd7']

Name

69dfa8c16879ab1c6c3bb738619dabe9660f2376cb15051ce55e465680e4f67f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '69dfa8c16879ab1c6c3bb738619dabe9660f2376cb15051ce55e465680e4f67f']

Name

3af5c0843b016faa6129e40b696565d4117b48fd6750164ac4a0f307ef3d6a36

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '3af5c0843b016faa6129e40b696565d4117b48fd6750164ac4a0f307ef3d6a36']

Name

349fada4859b8ffa4c690af723daa16669d6fa2b9f5ec51111adee2e8cb63748

Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '349fada4859b8ffa4c690af723daa16669d6fa2b9f5ec51111adee2e8cb63748']
Name
0239bc35516d6d3680c64f7a5a5a40801c7b0ea4db8a80718e4774687c565af3
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '0239bc35516d6d3680c64f7a5a5a40801c7b0ea4db8a80718e4774687c565af3']
Name
8fe52481cdabec8900f78cab1d673dbb1bde3366d9347a89c2ea8e2e74ab01b4
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '8fe52481cdabec8900f78cab1d673dbb1bde3366d9347a89c2ea8e2e74ab01b4']

Name

64.227.48.212

Description

- **Zip Code:** N/A - **ISP:** Digital Ocean - **ASN:** 14061 - **Organization:** Digital Ocean - **Is Crawler:** False - **Timezone:** America/Los_Angeles - **Mobile:** False - **Host:** 64.227.48.212 - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** True - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** US - **Region:** California - **City:** Santa Clara - **Latitude:** 37.34 - **Longitude:** -121.98

Pattern Type

stix

Pattern

[ipv4-addr:value = '64.227.48.212']

Name

http://171.22.30.147/tony/five/fre.php

Description

Loki Password Stealer (PWS) botnet C2 (confidence level: 75%)

Pattern Type

stix

Pattern

[url:value = 'http://171.22.30.147/tony/five/fre.php']

Name

171.22.30.147

Description

Agent Tesla payload delivery server (confidence level: 50%)

Pattern Type

stix

Pattern

[ipv4-addr:value = '171.22.30.147']

Malware

Name
Upatre
Name
ANDROMEDA - S1074
Name
Taskun
Name
Lokibot - S0447
Name
Sabsik
Name
RemLoader
Name
SnakeLogger

Name
Leonem

Name
ANDROMEDA

Description
[ANDROMEDA](https://attack.mitre.org/software/S1074) is commodity malware that was widespread in the early 2010's and continues to be observed in infections across a wide variety of industries. During the 2022 [C0026](https://attack.mitre.org/campaigns/C0026) campaign, threat actors re-registered expired [ANDROMEDA](https://attack.mitre.org/software/S1074) C2 domains to spread malware to select targets in Ukraine.(Citation: Mandiant Suspected Turla Campaign February 2023)

Name
agenttesla

Name
Remcos

Name
Lokibot

Description
[Lokibot](https://attack.mitre.org/software/S0447) is a widely distributed information stealer that was first reported in 2015. It is designed to steal sensitive information such as usernames, passwords, cryptocurrency wallets, and other credentials. [Lokibot](https://attack.mitre.org/software/S0447) can also create a backdoor into infected systems to allow

an attacker to install additional payloads.(Citation: Infoblox Lokibot January 2019)(Citation: Morphisec Lokibot April 2020)(Citation: CISA Lokibot September 2020)

Attack-Pattern

Name

Mark-of-the-Web Bypass

ID

T1553.005

Description

Adversaries may abuse specific file formats to subvert Mark-of-the-Web (MOTW) controls. In Windows, when files are downloaded from the Internet, they are tagged with a hidden NTFS Alternate Data Stream (ADS) named `Zone.Identifier` with a specific value known as the MOTW.(Citation: Microsoft Zone.Identifier 2020) Files that are tagged with MOTW are protected and cannot perform certain actions. For example, starting in MS Office 10, if a MS Office file has the MOTW, it will open in Protected View. Executables tagged with the MOTW will be processed by Windows Defender SmartScreen that compares files with an allowlist of well-known executables. If the file is not known/trusted, SmartScreen will prevent the execution and warn the user not to run it.(Citation: Beek Use of VHD Dec 2020)(Citation: Outflank MotW 2020)(Citation: Intezer Russian APT Dec 2020) Adversaries may abuse container files such as compressed/archive (.arj, .gzip) and/or disk image (.iso, .vhd) file formats to deliver malicious payloads that may not be tagged with MOTW. Container files downloaded from the Internet will be marked with MOTW but the files within may not inherit the MOTW after the container files are extracted and/or mounted. MOTW is a NTFS feature and many container files do not support NTFS alternative data streams. After a container file is extracted and/or mounted, the files contained within them may be treated as local files on disk and run without protections.(Citation: Beek Use of VHD Dec 2020) (Citation: Outflank MotW 2020)

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

Spearphishing Attachment

ID

T1566.001

Description

Adversaries may send spearphishing emails with a malicious attachment in an attempt to gain access to victim systems. Spearphishing attachment is a specific variant of spearphishing. Spearphishing attachment is different from other forms of spearphishing in that it employs the use of malware attached to an email. All forms of spearphishing are electronically delivered social engineering targeted at a specific individual, company, or industry. In this scenario, adversaries attach a file to the spearphishing email and usually rely upon [User Execution](https://attack.mitre.org/techniques/T1204) to gain execution. Spearphishing may also involve social engineering techniques, such as posing as a trusted

source. There are many options for the attachment such as Microsoft Office documents, executables, PDFs, or archived files. Upon opening the attachment (and potentially clicking past protections), the adversary's payload exploits a vulnerability or directly executes on the user's system. The text of the spearphishing email usually tries to give a plausible reason why the file should be opened, and may explain how to bypass system protections in order to do so. The email may also contain instructions on how to decrypt an attachment, such as a zip file password, in order to evade email boundary defenses. Adversaries frequently manipulate file extensions and icons in order to make attached executables appear to be document files, or files exploiting one application appear to be a file for a different one.

Url

Value
http://64.227.48.212/project/five/fre.php
http://171.22.30.147/tony/five/fre.php

StixFile

Value
a5a5b60edcbbb203cb1965b1d544b74c47284e015ffd50312de0a251141bfbd7
69dfa8c16879ab1c6c3bb738619dabe9660f2376cb15051ce55e465680e4f67f
3af5c0843b016faa6129e40b696565d4117b48fd6750164ac4a0f307ef3d6a36
349fada4859b8ffa4c690af723daa16669d6fa2b9f5ec51111adee2e8cb63748
0239bc35516d6d3680c64f7a5a5a40801c7b0ea4db8a80718e4774687c565af3
8fe52481cdabec8900f78cab1d673dbb1bde3366d9347a89c2ea8e2e74ab01b4

IPv4-Addr

Value
64.227.48.212
171.22.30.147

External References

- https://www.fortinet.com/blog/threat-research/tictactoe-dropper
- https://otx.alienvault.com/pulse/65cf3c3e8a27ffb8384ffad6