ANALYSIS REPORT

10445155.r1.v1 NUMBER

Malware Analysis Report

2023-06-08 DATE

Notification

This report is provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained herein. The DHS does not endorse any commercial product or service referenced in this bulletin or otherwise.

This document is marked TLP:CLEAR--Recipients may share this information without restriction. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction. For more information on the Traffic Light Protocol (TLP), see http://www.cisa.gov/tlp.

Summary

Description

CISA received one Windows Portable Executable (PE) file for analysis. The file is a variant of TrueBot malware. It is designed to collect system information and report it to a command-and-control (C2). The bot is also capable of downloading and executing additional payloads.

Submitted Files (1)

7d75244449fb5c25d8f196a43a6eb9e453652b2185392376e7d44c21bd8431e7 (3LXJyAv6Gf.exe)

Domains (2)

dremmfyttrred[.]com

droogggdhfhf[.]com

Findings

7d75244449fb5c25d8f196a43a6eb9e453652b2185392376e7d44c21bd8431e7

Tags

trojan

Details

Name	3LXJyAv6Gf.exe
Size	1200732656 bytes
Type	PE32+ executable (GUI) x86-64, for MS Windows
MD5	5588286a702e0c36c8318be0b164fa8c
SHA1	5449f3f141958de2d1140bc8323f5ac95c203287
SHA256	7d75244449fb5c25d8f196a43a6eb9e453652b2185392376e7d44c21bd8431e7
SHA512	105e72e1f1e3af8942e0e77e1294f74cd0518f7d601e4e2f20f7ed9db3cd1c67739c31e085e028eafe0394af74b2fbeb6ffbffb67d7731023a04c53a6784924e
ssdeep	25165824:d1AuQ/FFyK8db8kdjeyPpiMh5gbiwcfYjh+dkfaeLq4H/LLhtf:Q/FoK8rteknh54ZcfvdkfpnLhtf
Entropy	7.999996

Antivirus

ESET	a variant of Win64/Agent.BVF trojan

YARA Rules

```
rule CISA_10445155_01 : TRUEBOT downloader
{
    meta:
        Author = "CISA Code & Media Analysis"
        Incident = "10445155"
        Date = "2023-05-17"
        Last_Modified = "20230523_1500"
        Actor = "n/a"
        Family = "TRUEBOT"
        Capabilities = "n/a"
        Malware_Type = "downloader"
        Tool_Type = "n/a"
        Description = "Detects TRUEBOT downloader samples"
        SHA256 = "7d75244449fb5c25d8f196a43a6eb9e453652b2185392376e7d44c21bd8431e7"
    strings:
        $s1 = { 64 72 65 6d 6d 66 79 74 74 72 72 65 64 2e 63 6f 6d }
        $s2 = { 4e 73 75 32 4f 64 69 77 6f 64 4f 73 32 }
        $s3 = { 59 69 50 75 6d 79 62 6f 73 61 57 69 57 65 78 79 }
        $s4 = { 72 65 70 6f 74 73 5f 65 72 72 6f 72 2e 74 78 74 }
        $s5 = { 4c 6b 6a 64 73 6c 66 6a 33 32 6f 69 6a 72 66 65 77 67 77 2e 6d 70 34 }
        $s6 = { 54 00 72 00 69 00 67 00 67 00 65 00 72 00 31 00 32 }
        $s7 = { 54 00 55 00 72 00 66 00 57 00 65 00 73 00 54 00 69 00 66 00 73 00 66 }
    condition:
        5 of them
}
```

ssdeep Matches

No matches found.

Relationships

7d75244449...	Connected_To	dremmfyttrred[.]com
7d75244449...	Connected_To	droogggdhfhf[.]com

Description

This artifact is a variant of the TrueBot downloader. The file is padded with over one gigabyte (Gb) of junk code, designed to hinder analysis. When the bot is executed on the system, it will check the current Operating System (OS) version (RtlGetVersion) and the processor architecture (GetNativeSystemInfo). From this information the bot will create a unique ID for the compromised system. It will store the ID in C:\ProgramData as a randomly named 13 character file with a .JSONIP extension, e.g. 'IgtyXEQuCEvAM.JSONIP'.

The malware proceeds to enumerate all running processes on the system. The bot configuration contains a list of common Windows processes that are excluded from its list. The remaining process names are concatenated into a base64 encoded string. The malware specifically looks for the presence of the following disassembly and debugging tools:

—Begin Disassembly & Debugging Tools—
IDA Pro
Process Monitor
ProcessHacker
Process Explorer
CFF Explorer
Resource Hacker
Cheatengine-x86_64
OllyDbg
Radare2

X64dbg
WinDbg
Zeta Debugger
Rock Debugger
Obsidian debugger
—End Disassembly & Debugging Tools—

The presence of these tools does not change the execution of the malware. They are also concatenated into a base64 encoded string and sent along with the system information.

Next, the malware will collect the ComputerName and Domain name of the system. All of the collected information and the unique ID is sent to a hard-coded Uniform Resource Locator (URL) in a POST request using a unique User-agent string:

—Begin POST Request—
POST
dremmfyttrred[.]com/dns.php
Content-type: application/x-www-form-urlencoded
Mozilla/112.0 (compatible; MSIE 11.0; Windows NT 10.00)
—End POST Request—

The malware uses a second obfuscated domain to accept commands and receive additional payloads. The configuration contains two base64 encoded strings that the malware will decode and run through a string operation to generate a unique hexadecimal string. The hexadecimal string is decoded using the embedded RC4 key 'YiPumybosaWiWexy'. The following URL was decoded from the strings:

—Begin Decoded URL—
droogggdhfhf[.]com/gate.php
—End Decoded URL—

---

dremmfyttrred[.]com

Tags

command-and-control

HTTP Sessions

- POST
  dremmfyttrred[.]com/dns.php
  Content-type: application/x-www-form-urlencoded
  Mozilla/112.0 (compatible; MSIE 11.0; Windows NT 10.00)

Relationships

dremmfyttrred[.]com	Connected_From	7d75244449fb5c25d8f196a43a6eb9e453652b 2185392376e7d44c21bd8431e7

Description

3LXJyA6Gf.exe attempts to send the collected system information to this domain.

---

droogggdhfhf[.]com

Tags

command-and-control

Relationships

droogggdhfhf[.]com	Connected_From	7d75244449fb5c25d8f196a43a6eb9e453652b 2185392376e7d44c21bd8431e7

Description

3LXJyA6Gf.exe receives commands and payloads from this domain.

Relationship Summary

7d75244449...	Connected_To	dremmfyttrred[.]com
7d75244449...	Connected_To	droogggdhfhf[.]com
dremmfyttrred[.]com	Connected_From	7d75244449fb5c25d8f196a43a6eb9e453652b2185392376e7d44c21bd8431e7
droogggdhfhf[.]com	Connected_From	7d75244449fb5c25d8f196a43a6eb9e453652b2185392376e7d44c21bd8431e7

Recommendations

CISA recommends that users and administrators consider using the following best practices to strengthen the security posture of their organization's systems. Any configuration changes should be reviewed by system owners and administrators prior to implementation to avoid unwanted impacts.

- Maintain up-to-date antivirus signatures and engines.
- Keep operating system patches up-to-date.
- Disable File and Printer sharing services. If these services are required, use strong passwords or Active Directory authentication.
- Restrict users' ability (permissions) to install and run unwanted software applications. Do not add users to the local administrators group unless required.
- Enforce a strong password policy and implement regular password changes.
- Exercise caution when opening e-mail attachments even if the attachment is expected and the sender appears to be known.
- Enable a personal firewall on agency workstations, configured to deny unsolicited connection requests.
- Disable unnecessary services on agency workstations and servers.
- Scan for and remove suspicious e-mail attachments; ensure the scanned attachment is its "true file type" (i.e., the extension matches the file header).
- Monitor users' web browsing habits; restrict access to sites with unfavorable content.
- Exercise caution when using removable media (e.g., USB thumb drives, external drives, CDs, etc.).
- Scan all software downloaded from the Internet prior to executing.
- Maintain situational awareness of the latest threats and implement appropriate Access Control Lists (ACLs).

Additional information on malware incident prevention and handling can be found in National Institute of Standards and Technology (NIST) Special Publication 800-83, **"Guide to Malware Incident Prevention & Handling for Desktops and Laptops".**

Contact Information

- 1-888-282-0870
- CISA Service Desk (UNCLASS)
- CISA SIPR (SIPRNET)
- CISA IC (JWICS)

CISA continuously strives to improve its products and services. You can help by answering a very short series of questions about this product at the following URL: https://us-cert.cisa.gov/forms/feedback/

Document FAQ

What is a MIFR? A Malware Initial Findings Report (MIFR) is intended to provide organizations with malware analysis in a timely manner. In most instances this report will provide initial indicators for computer and network defense. To request additional analysis, please contact CISA and provide information regarding the level of desired analysis.

What is a MAR? A Malware Analysis Report (MAR) is intended to provide organizations with more detailed malware analysis acquired via manual reverse engineering. To request additional analysis, please contact CISA and provide information regarding

the level of desired analysis.

Can I edit this document? This document is not to be edited in any way by recipients. All comments or questions related to this document should be directed to the CISA at 1-888-282-0870 or CISA Service Desk.

Can I submit malware to CISA? Malware samples can be submitted via three methods:

- Web: https://malware.us-cert.gov
- E-Mail: submit@malware.us-cert.gov
- FTP: ftp.malware.us-cert.gov (anonymous)

CISA encourages you to report any suspicious activity, including cybersecurity incidents, possible malicious code, software vulnerabilities, and phishing-related scams. Reporting forms can be found on CISA's homepage at www.cisa.gov.

TLP: CLEAR