ANALYSIS REPORT

10448362.c1.v1 NUMBER

Malware Analysis Report

2024-02-02 DATE

Notification

Summary

Description

CISA received three files for analysis obtained from a critical infrastructure compromised by the People's Republic of China (PRC) state-sponsored cyber group known as Volt Typhoon.

The submitted files enable discovery and command-and-control (C2): (1) An open source Fast Reverse Proxy Client (FRPC) tool used to open a reverse proxy between the compromised system and a Volt Typhoon C2 server; (2) a Fast Reverse Proxy (FRP) that can be used to reveal servers situated behind a network firewall or obscured through Network Address Translation (NAT); and (3) a publicly available port scanner called ScanLine.

For more information on Volt Typhoon see, joint Cybersecurity Advisory PRC State-Sponsored Actors Compromise, and Maintain Persistent Access to, U.S. Critical Infrastructure. For more information on PRC state-sponsored malicious cyber activity, see CISA's China Cyber Threat Overview and Advisories, webpage.

Submitted Files (3)

99b80c5ac352081a64129772ed5e1543d94cad708ba2adc46dc4ab7a0bd563f1 (SMSvcService.exe)

eaef901b31b5835035b75302f94fee27288ce46971c6db6221ecbea9ba7ff9d0 (eaef901b31b5835035b75302f94fee...)

edc0c63065e88ec96197c8d7a40662a15a812a9583dc6c82b18ecd7e43b13b70 (BrightmetricAgent.exe)

IPs (2)

203[.]95[.]8[.]98

203[.]95[.]9[.]54

Findings

edc0c63065e88ec96197c8d7a40662a15a812a9583dc6c82b18ecd7e43b13b70

Tags

obfuscated proxy trojan utility

Details

Name	BrightmetricAgent.exe
Size	2840064 bytes
Type	PE32+ executable (console) x86-64 (stripped to external PDB), for MS Windows

MD5	fd41134e8ead1c18ccad27c62a260aa6
SHA1	04423659f175a6878b26ac7d6b6e47c6fd9194d1
SHA256	edc0c63065e88ec96197c8d7a40662a15a812a9583dc6c82b18ecd7e43b13b70
SHA512	df55591e730884470afba688e17c83fafb157ecf94c9f10a20e21f229434ea58b59f8eb771f8f9e29993f43f4969fe66dd913128822b534c9b1a677453dbb93c
ssdeep	49152:99z0w/qP1dKPzeietmd64H9QaIG0aYkn0GzkWVlSaJUET6qyxASu0szP7hn+S6wB:v0R9dKSiekd68ZIQ0obVI9UG6qyuhF6
Entropy	7.999902

Antivirus

Adaware	Generic.Trojan.Volt.Marte.A.05F91E9C
Antiy	GrayWare/Win32.Kryptik.ffp
Bitdefender	Generic.Trojan.Volt.Marte.A.05F91E9C
Emsisoft	Generic.Trojan.Volt.Marte.A.05F91E9C (B)
ESET	a variant of WinGo/HackTool.Agent.Y trojan
IKARUS	Trojan.WinGo.Rozena
Microsoft Defender	Malware
Sophos	App/FRProxy-F
Varist	W64/Agent.FXW.gen!Eldorado

YARA Rules

No matches found.

ssdeep Matches

No matches found.

Relationships

edc0c63065...	Connected_To	203[.]95[.]8[.]98

Description

This artifact is a cross platform full featured FRP that is written in GO language (Golang) and packed using Ultimate Packer for Executables (UPX). This utility can be used to locate servers behind a network firewall or obscured through NAT. It includes the KCP (no acronym) network protocol that allows for error-checked and anonymous delivery of data streams using the User Datagram Protocol (UDP) with packet level encryption support.

The program contains two different multiplexer libraries that can bi-directionally stream data over a NAT'd network. It also contains a command line interface (CLI) library that can leverage command shells such as PowerShell, Windows Management Instrumentation (WMI), and Z Shell (zsh). In addition, the utility features a unique capability that detects if the utility is executed from the command line or by double-clicking.

By default it is configured to connect to the Internet Protocol (IP) address, 203[.]95[.]8[.]98 on Transmission Control Protocol (TCP) port 1080. It must receive a specially formed packet from the command-and-control (C2) for the utility to deploy on the system.

203[.]95[.]8[.]98

Tags

proxy

Ports

- 1080 TCP

Whois

Domain Name: pdsguam.biz
Registry Domain ID: D15926452-BIZ
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: whois.godaddy.com

Updated Date: 2023-06-15T04:28:19Z
Creation Date: 2007-01-10T00:40:37Z
Registry Expiry Date: 2024-01-09T23:59:59Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1.4806242505
Registrant Organization: Domains By Proxy, LLC
Registrant State/Province: Arizona
Registrant Country: US
Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
Admin Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
Tech Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
Name Server: ns.pdsguam.biz
Name Server: ns2.pdsguam.biz
DNSSEC: unsigned

Relationships

203[.]95[.]8[.]98	Connected_From	edc0c63065e88ec96197c8d7a40662a15a81 2a9583dc6c82b18ecd7e43b13b70

Description

BrightmetricAgent.exe (edc0c63065...) attempts to connect to this IP address. The IP address hosts a proxy server.

---

eaef901b31b5835035b75302f94fee27288ce46971c6db6221ecbea9ba7ff9d0

Tags

pup trojan

Details

Name	eaef901b31b5835035b75302f94fee27288ce46971c6db6221ecbea9ba7ff9d0
Size	20480 bytes
Type	PE32 executable (console) Intel 80386, for MS Windows, UPX compressed
MD5	3a97d9b6f17754dcd38ca7fc89caab04
SHA1	ffb1d8ea3039d3d5eb7196d27f5450cac0ea4f34
SHA256	eaef901b31b5835035b75302f94fee27288ce46971c6db6221ecbea9ba7ff9d0
SHA512	d99941e4445efed5d4e407f91a9e5bba08d1be3f0dab065d1bfb4e70ab48d6526a730233d6889ba58de449f622e6a14e99dab853d40fc30a508627fd2735c973
ssdeep	384:ahXoLj9Zez0Bm4SUZa8WLLXyjSL2RtfAwj/yneIMUogQ:ahXoLhZez0m4SIabLLCmL2Rvj/yeIEg
Entropy	7.297754

Antivirus

AhnLab	Unwanted/Win32.Foundstone
Antiy	HackTool[NetTool]/Win32.Portscan
ClamAV	Win.Trojan.Scanline-1
Comodo	ApplicUnwnt
Cylance	Malware
Filseclab	Hacktool.ScanLine.a.fsff
IKARUS	Virtool
Microsoft Defender	Malware
NANOAV	Riskware.Win32.ScanLine.dhhus
Quick Heal	Trojan.Win32

Scrutiny	Malware
Sophos	App/ScanLn-A
VirusBlokAda	Trojan.Genome.fl
Zillya!	Tool.Portscan.Win32.77

YARA Rules

No matches found.

ssdeep Matches

No matches found.

Description

This artifact is a command-line port scanning utility from Foundstone, Inc. called ScanLine, which is packed using UPX. It is used to scan for open UDP and TCP ports, grab banners from open ports, resolve IP addresses to host names, and bind to specified ports and IP addresses.

Screenshots

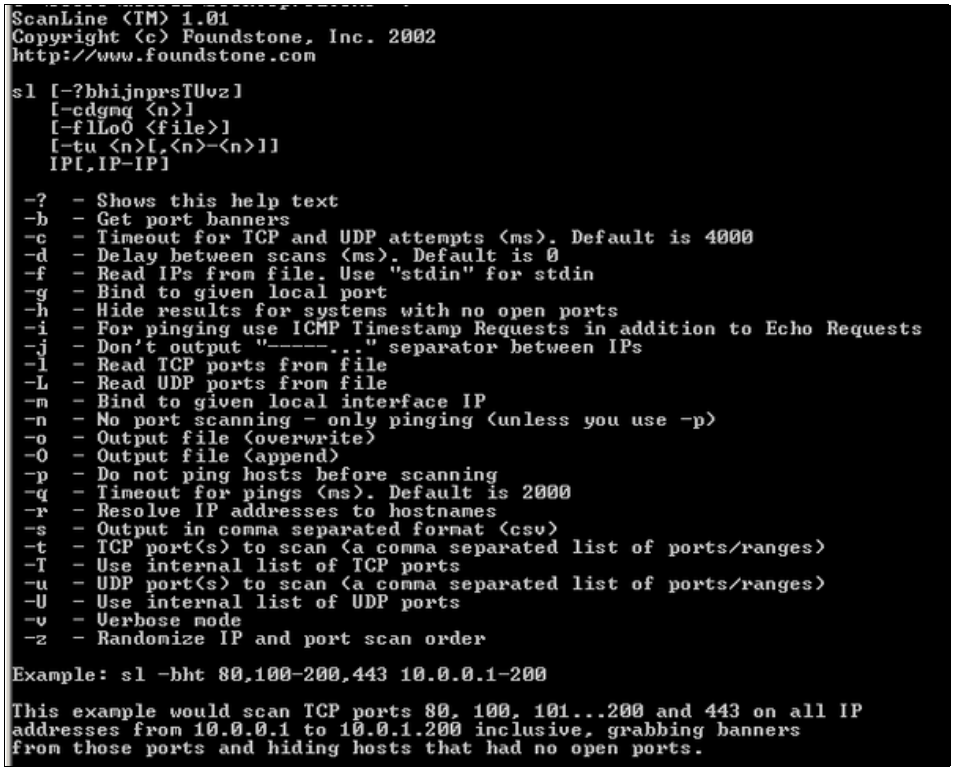

Figure 1 - Usage and syntax for the ScanLine utility.

99b80c5ac352081a64129772ed5e1543d94cad708ba2adc46dc4ab7a0bd563f1

Tags

obfuscated proxy trojan

Details

Name	SMSvcService.exe
Size	3712512 bytes
Type	PE32+ executable (console) x86-64 (stripped to external PDB), for MS Windows
MD5	b1de37bf229890ac181bdef1ad8ee0c2
SHA1	ffdb3cc7ab5b01d276d23ac930eb21ffe3202d11

SHA256	99b80c5ac352081a64129772ed5e1543d94cad708ba2adc46dc4ab7a0bd563f1
SHA512	e41df636a36ac0cce38e7db5c2ce4d04a1a7f9bc274bdf808912d14067dc1ef478268035521d0d4b7bcf96facce7f515560b38a7ebe47995d861b9c482e07e25
ssdeep	98304:z2eyMq4PuR5d7wgdo0OFfnFJkEUCGdaQLhpYYEfRTl6sysy:ryxzbdo0ifnoEOdz9pY7j5
Entropy	7.890436

Antivirus

Adaware	Generic.Trojan.Volt.Marte.A.105C517F
AhnLab	HackTool/Win.Frpc
Antiy	GrayWare/Win32.Kryptik.ffp
Bitdefender	Generic.Trojan.Volt.Marte.A.105C517F
Emsisoft	Generic.Trojan.Volt.Marte.A.105C517F (B)
ESET	a variant of WinGo/Riskware.Frp.U application
IKARUS	Trojan.WinGo.Shellcoderunner
Microsoft Defender	Malware
Sophos	App/FRProxy-F
Varist	W64/Agent.FXW.gen!Eldorado

YARA Rules

No matches found.

ssdeep Matches

No matches found.

PE Metadata

Compile Date	1970-01-01 00:00:00+00:00
Import Hash	6ed4f5f04d62b18d96b26d6db7c18840

PE Sections

MD5	Name	Raw Size	Entropy
7f8e8722da728b6e834260b5a314cbac	header	512	2.499747
d41d8cd98f00b204e9800998ecf8427e	UPX0	0	0.000000
f9943591918adeeeee7da80e4d985a49	UPX1	3711488	7.890727
5c0061445ac2f8e6cadf694e54146914	UPX2	512	1.371914

Relationships

99b80c5ac3...	Connected_To	203[.]95[.]9[.]54

Description

This artifact is a 64-bit Windows executable file that is packed using UPX. This packed file contains a compiled version of an open-source tool published on GitHub called "FRPC". The "FRPC" is a command-line tool written in Golang that is designed to open a reverse proxy between the compromised system and the TA's C2 server.

When the "FRPC" is installed and executed on the compromised system, it attempts to establish a connection with the Fast Reverse Proxy Server (FRPS) using the reverse proxy method to allow the TA to control the compromised system. This "FRPC" application supports encryption, compression, and allows easy token authentication. It also supports the protocols below:

–Begin protocols–
Transmission Control Protocol (TCP)
User Datagram Protocol (UDP)
An alternative Hypertext Transfer Protocol (HTTP)
An alternative Hypertext Transfer Protocol Secure (HTTPS)
–End protocols–

Displayed below is the "FRPC" tool configuration that contains the network communication method, the remote "FRPS" server's public

Internet Protocol (IP) address and port numbers:

```
–Begin configuration–
[common]
  server_addr = 192.168.18.111
  server_port = 8081
  server_addrs = 203[.]95[.]9[.]54,203[.]95[.]9[.]54,203[.]95[.]9[.]54
  server_ports = 8443,8443,8443
  token = 1kyRdFmuk0i25JbCJmtift1c9VA05VBS
  protocol = tcp
  tls_enable = true
  disable_custom_tls_first_byte = true
  log_level = debug

  [plugin_socks5]
  type = tcp
  remote_port = 1080
  plugin = socks5
  use_encryption = true
  use_compression = true
–End configuration–
```

Displayed below are the command-line usages and flags of the "FRPC" tool:

```
–Begin usages and flags–

Usage:
frpc [flags]
frpc [command]

Available Commands:
help        Help about any command
tcp         Run frpc with a single tcp proxy
udp         Run frpc with a single udp proxy
verify      Verify that the configures is valid

Flags:
-c, –config string config file of frpc (default "./frpc.ini")
-h, –help           help for frpc
-v, –version        version of frpc

Use "frpc [command] –help" for more information about a command.

_____
Run frpc with a single tcp proxy

Usage:
frpc tcp [flags]

Flags:
    –disable_log_color    disable log color in console
-h, –help                 help for tcp
-i, –local_ip string      local ip (default "127.0.0.1")
-l, –local_port int       local port
    –log_file string      console or file path (default "console")
    –log_level string     log level (default "info")
    –log_max_days int     log file reversed days (default 3)
-p, –protocol string      tcp or kcp or websocket (default "tcp")
-n, –proxy_name string    proxy name
-r, –remote_port int      remote port
-s, –server_addr string frp server's address (default "127.0.0.1:7000")
    –tls_enable           enable frpc tls
-t, –token string         auth token
    –uc                   use compression
```

```
    --ue               use encryption
-u, --user string      user

Global Flags:
-c, --config string config file of frpc (default "./frpc.ini")
-v, --version        version of frpc

_____________________________________________________________
Run frpc with a single udp proxy

Usage:
frpc udp [flags]

Flags:
    --disable_log_color    disable log color in console
-h, --help                 help for udp
-i, --local_ip string      local ip (default "127.0.0.1")
-l, --local_port int       local port
    --log_file string      console or file path (default "console")
    --log_level string     log level (default "info")
    --log_max_days int     log file reversed days (default 3)
-p, --protocol string      tcp or kcp or websocket (default "tcp")
-n, --proxy_name string    proxy name
-r, --remote_port int      remote port
-s, --server_addr string frp server's address (default "127.0.0.1:7000")
    --tls_enable         enable frpc tls
-t, --token string         auth token
    --uc               use compression
    --ue               use encryption
-u, --user string      user

Global Flags:
-c, --config string config file of frpc (default "./frpc.ini")
-v, --version        version of frpc
_____________________________________________________________
Verify that the configures is valid

Usage:
frpc verify [flags]

Flags:
-h, --help help for verify

Global Flags:
-c, --config string config file of frpc (default "./frpc.ini")
-v, --version        version of frpc

--End usages and flags--
```

203[.]95[.]9[.]54

Ports

- 8443 TCP

Whois

```
Domain Name: pdsguam.biz
Registry Domain ID: D15926452-BIZ
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: whois.godaddy.com
Updated Date: 2023-01-15T17:08:00Z
Creation Date: 2007-01-10T00:40:37Z
Registry Expiry Date: 2024-01-09T23:59:59Z
```

Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1.4806242505
Registrant Organization: Domains By Proxy, LLC
Registrant State/Province: Arizona
Registrant Country: US
Name Server: ns.pdsguam.biz
Name Server: ns2.pdsguam.biz
DNSSEC: unsigned

Relationships		
203[.]95[.]9[.]54	Connected_From	99b80c5ac352081a64129772ed5e1543d94c ad708ba2adc46dc4ab7a0bd563f1

Description

The IP address used to establish a connection with the remote FRPS.

Relationship Summary

edc0c63065...	Connected_To	203[.]95[.]8[.]98
203[.]95[.]8[.]98	Connected_From	edc0c63065e88ec96197c8d7a40662a15a81 2a9583dc6c82b18ecd7e43b13b70
99b80c5ac3...	Connected_To	203[.]95[.]9[.]54
203[.]95[.]9[.]54	Connected_From	99b80c5ac352081a64129772ed5e1543d94c ad708ba2adc46dc4ab7a0bd563f1

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