MAR-10320115-1.v1 - TEARDROP | CISA

Published: 2021-04-15 · Archived: 2026-04-05 19:34:02 UTC

body#cma-body { font-family: Franklin Gothic Medium, Franklin Gothic, ITC Franklin Gothic, Arial, sans-serif; font-size: 15px; } table#cma-table { width: 900px; margin: 2px; table-layout: fixed; border-collapse: collapse; } div#cma-exercise { width: 900px; height: 30px; text-align: center; line-height: 30px; font-weight: bold; font-size: 18px; } div.cma-header { text-align: center; margin-bottom: 40px; } div.cma-footer { text-align: center; margin-top: 20px; } h2.cma-tlp { background-color: #000; color: #ffffff; width: 180px; height: 30px; text-align: center; line-height: 30px; font-weight: bold; font-size: 18px; float: right; } span.cma-fouo { line-height: 30px; font-weight: bold; font-size: 16px; } h3.cma-section-title { font-size: 18px; font-weight: bold; padding: 0 10px; margin-top: 10px; } h4.cma-object-title { font-size: 16px; font-weight: bold; margin-left: 20px; } h5.cma-data-title { padding: 3px 0 3px 10px; margin: 10px 0 0 20px; background-color: #e7eef4; font-size: 15px; } p.cma-text { margin: 5px 0 0 25px !important; word-wrap: break-word !important; } div.cma-section { border-bottom: 5px solid #aaa; margin: 5px 0; padding-bottom: 10px; } div.cma-avoid-page-break { page-break-inside: avoid; } div#cma-summary { page-break-after: always; } div#cma-faq { page-break-after: always; } table.cma-content { border-collapse: collapse; margin-left: 20px; } table.cma-hashes { table-layout: fixed; width: 880px; } table.cma-hashes td{ width: 780px; word-wrap: break-word; } .cma-left th { text-align: right; vertical-align: top; padding: 3px 8px 3px 20px; background-color: #f0f0f0; border-right: 1px solid #aaa; } .cma-left td { padding-left: 8px; } .cma-color-title th, .cma-color-list th, .cma-color-title-only th { text-align: left; padding: 3px 0 3px 20px; background-color: #f0f0f0; } .cma-color-title td, .cma-color-list td, .cma-color-title-only td { padding: 3px 20px; } .cma-color-title tr:nth-child(odd) { background-color: #f0f0f0; } .cma-color-list tr:nth-child(even) { background-color: #f0f0f0; } td.cma-relationship { max-width: 310px; word-wrap: break-word; } ul.cma-ul { margin: 5px 0 10px 0; } ul.cma-ul li { line-height: 20px; margin-bottom: 5px; word-wrap: break-word; } #cma-survey { font-weight: bold; font-style: italic; } div.cma-banner-container { position: relative; text-align: center; color: white; } img.cma-banner { max-width: 900px; height: auto; } img.cma-nccic-logo { max-height: 60px; width: auto; float: left; margin-top: -15px; } div.cma-report-name { position: absolute; bottom: 32px; left: 12px; font-size: 20px; } div.cma-report-number { position: absolute; bottom: 70px; right: 100px; font-size: 18px; } div.cma-report-date { position: absolute; bottom: 32px; right: 100px; font-size: 18px; } img.cma-thumbnail { max-height: 100px; width: auto; vertical-align: top; } img.cma-screenshot { margin: 10px 0 0 25px; max-width: 800px; height: auto; vertical-align: top; border: 1px solid #000; } div.cma-screenshot-text { margin: 10px 0 0 25px; } .cma-break-word { word-wrap: break-word; } .cma-tag { border-radius: 5px; padding: 1px 10px; margin-right: 10px; } .cma-tag-info { background: #f0f0f0; } .cma-tag-warning { background: #ffdead; }

Notification

Summary

Description

This report provides detailed analysis of malicious artifacts associated with a sophisticated supply chain compromise of Solar Winds Orion network management software, identified by the security company FireEye as TEARDROP.

TEARDROP is a loader designed to decrypt and execute an embedded payload on the target system. The payload has been identified as the Cobalt Strike Beacon Implant (Version 4) and provides a remote operator command and control capabilities over a victim system through an encrypted network tunnel. The capabilities include the ability to rapidly exfiltrate data, log keystrokes, take screenshots, and deploy additional payloads.

For a downloadable copy of IOCs, see: MAR-10320115-1.v1.stix.

Submitted Files (2)

1817a5bf9c01035bcf8a975c9f1d94b0ce7f6a200339485d8f93859f8f6d730c (1817a5bf9c01035bcf8a975c9f1d94...)

b820e8a2057112d0ed73bd7995201dbed79a79e13c79d4bdad81a22f12387e07 (b820e8a2057112d0ed73bd7995201d...)

Domains (2)

ervsystem.com

infinitysoftwares.com

Findings

1817a5bf9c01035bcf8a975c9f1d94b0ce7f6a200339485d8f93859f8f6d730c

Tags

backdoordroppertrojan

Details

Name	1817a5bf9c01035bcf8a975c9f1d94b0ce7f6a200339485d8f93859f8f6d730c
Size	321024 bytes
Type	PE32+ executable (DLL) (GUI) x86-64 (stripped to external PDB), for MS Windows
MD5	35abfb98dac5bf48f7ac0e67afc9bdb7
SHA1	9185029c2630b220a74620c8f3d04886a457e1cf
SHA256	1817a5bf9c01035bcf8a975c9f1d94b0ce7f6a200339485d8f93859f8f6d730c
SHA512	93f1336e3bc7ac01561f0ad7ce5fec7ae078e55db0f5b0cf0663cb5dbbe2acb08f27490da179e27579debc04843bf02f047456c516bf0345ba827
ssdeep	6144:NQGxkGwaxIOkqNQI7LI8L/pOXlZg2gv+rtcOHNManxm2wf:NtxpgyNQIo8LePWOHWgTa
Entropy	7.922861

Antivirus

BitDefender	Generic.Teardrop.1.244AC43A
Clamav	Win.Dropper.Teardrop-9808996-3
Emsisoft	Generic.Teardrop.1.244AC43A (B)
Lavasoft	Generic.Teardrop.1.244AC43A
Microsoft Security Essentials	Trojan:Win64/Cobaltstrike.RN!dha
Symantec	Backdoor.Teardrop

YARA Rules

- ```
  rule CISA_10320115_01 : TEARDROP trojan backdoor
  {
    meta:
      Author = "CISA Code & Media Analysis"
      Incident = "10320115"
      Date = "2020-12-31"
      Last_Modified = "20201231_1800"
      Actor = "n/a"
      Category = "Trojan Backdoor"
      Family = "TEARDROP"
      Description = "Detects variants of TEARDROP malware"
      MD5_1 = "f612bce839d855bbff98214a197489f7"
      SHA256_1 = "dc20f4e50784533d7d10925e4b056f589cc73c139e97f40c0b7969728a28125c"
      MD5_2 = "91e47c7bc9a7809e6b1560e34f2d6d7e"
      SHA256_2 = "b37007db21a7f969d2c838f3bbbeb78a7402d66735bb5845ef31df9048cc33f0"
      MD5_3 = "91e47c7bc9a7809e6b1560e34f2d6d7e"
      SHA256_3 = "1817a5bf9c01035bcf8a975c9f1d94b0ce7f6a200339485d8f93859f8f6d730c"
    strings:
      $s0 = { 65 23 FB 7F 20 AA EB 0C B8 16 F6 BC 2F 4D D4 C4 39 97 C7 23 9F 3E 5C DE }
      $s1 = { 5C E6 06 63 FA DE 44 C0 D4 67 95 28 12 47 C5 B5 EF 24 BC E4 }
      $s2 = { 9E 96 BA 1B FB 7F 19 5A 8C 06 AB FA 43 3B F0 83 9E 54 0B 02 }
      $s3 = { C2 7E 93 FC 02 B9 C6 DE 2B AF C6 C2 BE 2C 88 02 B4 1D 03 F5 }
      $s4 = { 48 B8 53 4F 46 54 57 41 52 45 C7 44 24 60 66 74 5C 43 C6 44 24 66 00 48 89 44 24 50 48 B8 5C 4D
  69 63 72 6F 73 6F }
  ```
  ```

$s5 = { 48 83 F8 FF 48 8D }
$s6 = { 8B 0A 48 83 C2 04 8D 81 FF FE FE FE F7 D1 21 C8 25 80 80 80 80 }
$s7 = { 5B 5E 5F 5D 41 5C 41 }
$s8 = { 4E 00 65 00 74 00 77 00 6F 00 72 00 6B 00 20 00 53 00 65 00 74 00 75 00 70 00 20 00 53 00 65 00 72 00 76 00 69 00 63 00 65 }
$s9 = { 64 6C 6C 00 4E 65 74 53 65 74 75 70 53 65 72 76 69 63 65 4D 61 69 6E }
$s10 = { 41 31 C0 45 88 04 0A 48 83 C1 01 45 89 C8 41 39 CB 7F }
condition:
($s0 or $s1 or $s2 or $s3) or ($s4 and $s5 and $s6 and $s7 and $s8 and $s9 and $s10)
}

- rule FireEye_20_00025665_01 : TEARDROP APT dropper
{
meta:
Author = "FireEye"
Date = "2020-12-13"
Last_Modified = "20201213_1916"
Actor = "n/a"
Category = "Hacktool"
Family = "TEARDROP"
Description = "This rule looks for portions of the TEARDROP backdoor that are vital to how it functions. TEARDROP is a memory only dropper that can read files and registry keys, XOR decode an embedded payload, and load the payload into memory. TEARDROP persists as a Windows service and has been observed dropping Cobalt Strike BEACON into memory."
MD5_1 = ""
SHA256_1 = ""
strings:
$sb1 = { C7 44 24 ?? 80 00 00 00 [0-64] BA 00 00 00 80 [0-32] 48 8D 0D [4-32] FF 15 [4] 48 83 F8 FF [2-64] 41 B8 40 00 00 00 [0-64] FF 15 [4-5] 85 C0 7? ?? 80 3D [4] FF }
$sb2 = { 80 3D [4] D8 [2-32] 41 B8 04 00 00 00 [0-32] C7 44 24 ?? 4A 46 49 46 [0-32] E8 [4-5] 85 C0 [2-32] C6 05 [4] 6A C6 05 [4] 70 C6 05 [4] 65 C6 05 [4] 67 }
$sb3 = { BA [4] 48 89 ?? E8 [4] 41 B8 [4] 48 89 ?? 48 89 ?? E8 [4] 85 C0 7? [1-32] 8B 44 24 ?? 48 8B ?? 24 [1-16] 48 01 C8 [0-32] FF D0 }
condition:
all of them
}
- rule FireEye_20_00025665_02 : TEARDROP APT dropper
{
meta:
Author = "FireEye"
Date = "2020-12-13"
Last_Modified = "20201213_1916"
Actor = "n/a"
Category = "Hacktool"
Family = "TEARDROP"
Description = "This rule is intended match specific sequences of opcode found within TEARDROP, including those that decode the embedded payload. TEARDROP is a memory only dropper that can read files and registry keys, XOR decode an embedded payload, and load the payload into memory. TEARDROP persists as a Windows service and has been observed dropping Cobalt Strike BEACON into memory."
MD5_1 = ""
SHA256_1 = ""
strings:
$loc_4218FE24A5 = { 48 89 C8 45 0F B6 4C 0A 30 }
$loc_4218FE36CA = { 48 C1 E0 04 83 C3 01 48 01 E8 8B 48 28 8B 50 30 44 8B 40 2C 48 01 F1 4C 01 FA }
$loc_4218FE2747 = { C6 05 ?? ?? ?? ?? 6A C6 05 ?? ?? ?? ?? 70 C6 05 ?? ?? ?? ?? 65 C6 05 ?? ?? ?? ?? 67 }
$loc_5551D725A0 = { 48 89 C8 45 0F B6 4C 0A 30 48 89 CE 44 89 CF 48 F7 E3 48 C1 EA 05 48 8D 04 92 48 8D 04 42 48 C1 E0 04 48 29 C6 }
$loc_5551D726F6 = { 53 4F 46 54 57 41 52 45 ?? ?? ?? ?? 66 74 5C 43 ?? ?? ?? ?? 00 }
condition:
(uint16(0) == 0x5A4D and uint32(uint32(0x3C)) == 0x00004550) and any of them
}

ssdeep Matches

No matches found.

PE Metadata

Compile Date	2018-12-09 10:37:58-05:00
Import Hash	0a331624686ac9055694d7ddd9c0815d
Company Name	None
File Description	Network Setup Service
Internal Name	None
Legal Copyright	© Microsoft Corporation. All rights reserved.
Original Filename	NETSETUPSVC.DLL
Product Name	Microsoft® Windows® Operating System
Product Version	10.0.14393.0

PE Sections

MD5	Name	Raw Size	Entropy
d990149684ac611b98b9d389766a7e17	header	1024	2.584189
5fbd9948fd72f083803635022111fd99	.text	23552	6.358535
122bd1d155ed0c51226ea0b38872e13d	.data	286720	7.998098
9d8aead5ec18fa55740a34a7eaa3c2bb	.rdata	1536	3.673323
7b5aab64a2810cf05bd80323f8aa17d4	.pdata	1536	3.660221
8b15f6849b0bf0f60bd81b23988f5ca7	.xdata	1024	2.883941
d41d8cd98f00b204e9800998ecf8427e	.bss	0	0.000000
091c8665b4cd95cc583105c223f156aa	.edata	512	0.967748
c94c470079ed994735caebed176cd925	.idata	2560	4.429320
c806ece4d1aa4e25beb529c6e7dc947d	.CRT	512	0.253231
9f168cc07fa95e573b1f74a2e4614f79	.tls	512	0.331828
5b06dd2d5de3cb635e5e15313a541789	.rsrc	1024	2.933337
99450283e3e0c313f697d0165f585598	.reloc	512	1.239038

Relationships

1817a5bf9c...	Connected_To	ervsystem.com

Description

This file is a malicious 64-bit DLL, identified as a variant of the TEARDROP loader. The malware attempts to read the first 64-bytes of a file named "festive_computer.jpg" (Figure 1). It does not utilize the data it reads from this file and it will continue executing even if this file is not present on the target system.

After attempting to read the file "festive_computer.jpg," it will decrypt and execute an embedded code buffer using an XOR based stream cipher (Figure 2). Below is the key utilized by the cipher algorithm to decrypt the embedded code buffer:

—Begin Cipher Key—
C27E93FC02B9C6DE2BAFC6C2BE2C8802B41D03F53365B25AEE1A67D0E9525171F5F7149045E5D1F672176CA686C3C7A0D34E5FF1FBCBF6
—End Cipher Key—

The embedded code buffer has been identified as the Cobalt Strike Beacon (version 4) Remote Access Tool (RAT).
Displayed below is the embedded Beacon configuration data:

—Begin Cobalt Beacon Configuration Data—
Port - 443
SleepTime - 7200000
MaxGetSize - 1399696

```
Jitter                          - 18
MaxDNS                          - 255
C2Server                        - ervsystem.com/2019/Two-Man-Point-The-Brands/
UserAgent                       - Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR
3.5.30729; rv:11.0) like Gecko
HttpPostUri                     - /2019/Users-Case-Documentation-And-Yourselt/
Malleable_C2_Instructions       - Remove 38 bytes from the end
                                Remove 1554 bytes from the beginning
                                Base64 decode
HttpGet_Metadata                - Referer: https://yahoo.com/
                                Host: ervsystem.com
                                Accept: */*
                                Accept-Language: en-US
                                Accept-Encoding: gzip, deflate
                                Connection: close
                                PHPSESSID=
                                Cookie
HttpPost_Metadata               - Referer: https://yahoo.com/
                                Host: ervsystem.com
                                Accept: */*
                                Accept-Language: en-US
                                Connection: close
                                name="uploaded_1";filename="04373.avi"
Content-Type: text/plain

                                p
SpawnTo                         - b'\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00'
PipeName                        -
DNS_Idle                        - 9.9.9.9
DNS_Sleep                       - 0
SSH_Host                        - Not Found
SSH_Port                        - Not Found
SSH_Username                    - Not Found
SSH_Password_Plaintext          - Not Found
SSH_Password_Pubkey             - Not Found
HttpGet_Verb                    - GET
HttpPost_Verb                   - POST
HttpPostChunk                   - 0
Spawnto_x86                     - %windir%\syswow64\msiexec.exe
Spawnto_x64                     - %windir%\sysnative\print.exe
CryptoScheme                    - 0
Proxy_Config                    - Not Found
Proxy_User                      - Not Found
Proxy_Password                  - Not Found
Proxy_Behavior                  - Use IE settings
Watermark                       - 892810033
bStageCleanup                   - True
bCFGCaution                     - False
KillDate                        - 0
bProcInject_StartRWX            - False
bProcInject_UseRWX              - False
bProcInject_MinAllocSize        - 7281
ProcInject_PrependAppend_x86    - b'\x90'
                                Empty
ProcInject_PrependAppend_x64    - b'\x90\x90\x90'
                                Empty
ProcInject_Execute              - ntdll:RtlUserThreadStart
                                CreateThread
                                NtQueueApcThread
                                SetThreadContext
ProcInject_AllocationMethod     - NtMapViewOfSection
bUsesCookies                    - True
HostHeader                      -
—End Cobalt Beacon Configuration Data—
```

Screenshots

Figure 1 - Screenshot of the code structure that tries to read "festive_computer.jpg" from disk.

Figure 2 - Screenshot of TEARDROP using an algorithm to decrypt the embedded code buffer which contains the Cobalt Strike Beacon remote access tool (RAT).

ervsystem.com

Tags

command-and-control

URLs

- ervsystem.com/2019/Two-Man-Point-The-Brands/

Ports

- 443 TCP

Whois

Domain Name: ERVSYSTEM.COM
Registry Domain ID: 2222911627_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.epik.com
Registrar URL: http://www.epik.com
Updated Date: 2020-09-04T23:23:29Z
Creation Date: 2018-02-04T08:45:05Z
Registrar Registration Expiration Date: 2022-02-04T08:45:05Z
Registrar: Epik, Inc.
Registrar IANA ID: 617
Registrar Abuse Contact Email: abuse@epik.com
Registrar Abuse Contact Phone: +1.4253668810
Reseller:
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: Privacy Administrator
Registrant Organization: Anonymize, Inc.
Registrant Street: 704 228th Ave NE
Registrant City: Sammamish
Registrant State/Province: WA
Registrant Postal Code: 98074
Registrant Country: US
Registrant Phone: +1.4253668810
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: ervsystem.com@anonymize.com
Registry Admin ID:
Admin Name: Privacy Administrator
Admin Organization: Anonymize, Inc.
Admin Street: 704 228th Ave NE
Admin City: Sammamish
Admin State/Province: WA
Admin Postal Code: 98074
Admin Country: US
Admin Phone: +1.4253668810
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: ervsystem.com@anonymize.com
Registry Tech ID:
Tech Name: Privacy Administrator
Tech Organization: Anonymize, Inc.
Tech Street: 704 228th Ave NE

Tech City: Sammamish
Tech State/Province: WA
Tech Postal Code: 98074
Tech Country: US
Tech Phone: +1.4253668810
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: ervsystem.com@anonymize.com
Name Server: NS3.EPIK.COM
Name Server: NS4.EPIK.COM
DNSSEC: signedDelegation
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/

Relationships

ervsystem.com	Connected_From	1817a5bf9c01035bcf8a975c9f1d94b0ce7f6a200339485d8f93859f8f6d730c

Description

This domain is the command and control (C2) for the sample "1817a5bf9c01035bcf8a975c9f1d94b0ce7f6a200339485d8f93859f8f6d730c."

b820e8a2057112d0ed73bd7995201dbed79a79e13c79d4bdad81a22f12387e07

Tags

backdoortrojan

Details

Name	b820e8a2057112d0ed73bd7995201dbed79a79e13c79d4bdad81a22f12387e07
Size	530432 bytes
Type	PE32+ executable (DLL) (GUI) x86-64 (stripped to external PDB), for MS Windows
MD5	bd842c41b4c1b3c2deb475d7a3876599
SHA1	f7e61eb028b399b74c73883a2fccedbe56ecea2e
SHA256	b820e8a2057112d0ed73bd7995201dbed79a79e13c79d4bdad81a22f12387e07
SHA512	110a10662342b0d5716c3307c51fa8a591bf621049d8d291aa44f8ab864ab07506465175033461929 2e9362136e328c14dd637033c244d4255
ssdeep	12288:NMINVoXxVuxcowWRjZ9dpOLg8UU8YhUhKEcBvg+:2rxIwU19eL4oUAEun
Entropy	7.533146

Antivirus

BitDefender	Trojan.Teardrop.C
ESET	a variant of Generik.NFGRBKQ trojan
Emsisoft	Trojan.Teardrop.C (B)
Lavasoft	Trojan.Teardrop.C
Microsoft Security Essentials	Trojan:Win64/Cobaltstrike.RN!dha
Symantec	Backdoor.Teardrop

YARA Rules

- rule FireEye_20_00025665_02 : TEARDROP APT dropper
  {
    meta:
      Author = "FireEye"
      Date = "2020-12-13"

```
        Last_Modified = "20201213_1916"
        Actor = "n/a"
        Category = "Hacktool"
        Family = "TEARDROP"
        Description = "This rule is intended match specific sequences of opcode found within TEARDROP, including
    those that decode the embedded payload. TEARDROP is a memory only dropper that can read files and registry
    keys, XOR decode an embedded payload, and load the payload into memory. TEARDROP persists as a Windows
    service and has been observed dropping Cobalt Strike BEACON into memory."
        MD5_1 = ""
        SHA256_1 = ""
      strings:
        $loc_4218FE24A5 = { 48 89 C8 45 0F B6 4C 0A 30 }
        $loc_4218FE36CA = { 48 C1 E0 04 83 C3 01 48 01 E8 8B 48 28 8B 50 30 44 8B 40 2C 48 01 F1 4C 01 FA }
        $loc_4218FE2747 = { C6 05 ?? ?? ?? ?? 6A C6 05 ?? ?? ?? ?? 70 C6 05 ?? ?? ?? ?? 65 C6 05 ?? ?? ?? ?? 67 }
        $loc_5551D725A0 = { 48 89 C8 45 0F B6 4C 0A 30 48 89 CE 44 89 CF 48 F7 E3 48 C1 EA 05 48 8D 04 92 48
    8D 04 42 48 C1 E0 04 48 29 C6 }
        $loc_5551D726F6 = { 53 4F 46 54 57 41 52 45 ?? ?? ?? ?? 66 74 5C 43 ?? ?? ?? ?? 00 }
      condition:
        (uint16(0) == 0x5A4D and uint32(uint32(0x3C)) == 0x00004550) and any of them
    }
```

ssdeep Matches

No matches found.

PE Metadata

Compile Date	2018-03-09 23:23:43-05:00
Import Hash	3417123af2f473f771d46841bfce6d48
Company Name	None
File Description	GetText: library and tools for native language support
Internal Name	None
Legal Copyright	© 2015 Free Software Foundation <www.fsf.org>
Original Filename	libintl3.dll
Product Name	libintl3.dll
Product Version	0.14.4.1952

PE Sections

MD5	Name	Raw Size	Entropy
1ae8ec5795f9a3cad5d54e569634d668	header	1024	2.703747
989e04fb5dc1eb83a3055a3fea30fb7a	.text	209408	6.327319
d2bcd776a8ca1ed76feb8344d0739f1a	.data	286720	7.998501
fdbd0954169972c21876938dbd536da3	.rdata	1536	3.636101
7eddb104f4aad897faffc33762e896cf	.pdata	7680	5.364572
8232395ce211b61e4df169c38afdb7f6	.xdata	3072	1.658757
d41d8cd98f00b204e9800998ecf8427e	.bss	0	0.000000
add3d2ca7de32da5c3a5d2718129d600	.edata	15872	5.809199
8e6af2ae43eb16502507eeb8c7c03aa5	.idata	2560	3.983544
768bf26d947f32101953daeeea4a19b1	.CRT	512	0.238291
60227c557d35a7f2cf79a13c284b1dab	.tls	512	0.335735
2d007e3e5c7f7423ed5c43b129f03f34	.rsrc	1024	2.956911

MD5	Name	Raw Size	Entropy
ddbe94bbe8aeacf9cb120fe816659354	.reloc	512	1.215071

Relationships

b820e8a205...	Connected_To	infinitysoftwares.com

Description

This file is a malicious 64-bit DLL, identified as a variant of the TEARDROP loader. During runtime, the malicious application decodes and executes an embedded code buffer using an XOR based stream cipher. Displayed below is the key utilized by the cipher algorithm to decrypt the embedded code buffer:

—Begin XOR Cipher Key—
AFAFD51031EE936AFC50B611CDC70E7E62A7BAFCA72B43DB0023915BBBBAC016A5331CB28EE6E3DF0804B24004D219EE7ED24C7B41D9
—End XOR Cipher Key—

The embedded code buffer contains the malicious identified as Cobalt Strike Beacon (version 4) RAT. Displayed below is the embedded Beacon configuration data:

—Begin Cobalt Beacon Configuration Data—
BeaconType - HTTPS
Port - 443
SleepTime - 14400000
MaxGetSize - 1049217
Jitter - 23
MaxDNS - 255
C2Server - infinitysoftwares.com,/files/information_055.pdf
UserAgent - Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/81.0.4044.92 Safari/537.36
HttpPostUri - /wp-admin/new_file.php
Malleable_C2_Instructions - Remove 313 bytes from the end
Remove 324 bytes from the beginning
XOR mask w/ random key
HttpGet_Metadata - Referer: https://twitter.com/
Host: infinitysoftwares.com
Accept: */*
Accept-Language: en-US
Accept-Encoding: gzip, deflate
Connection: close
PHPSESSID=
Cookie
HttpPost_Metadata - Host: infinitysoftwares.com
Accept: */*
Accept-Language: en-US
Connection: close
name="uploaded_1";filename="33139.pdf"
Content-Type: text/plain

r
SpawnTo - b'\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00'
PipeName -
DNS_Idle - 208.67.220.220
DNS_Sleep - 0
SSH_Host - Not Found
SSH_Port - Not Found
SSH_Username - Not Found
SSH_Password_Plaintext - Not Found
SSH_Password_Pubkey - Not Found
HttpGet_Verb - GET
HttpPost_Verb - POST
HttpPostChunk - 0
Spawnto_x86 - %windir%\syswow64\print.exe
Spawnto_x64 - %windir%\sysnative\msiexec.exe

CryptoScheme - 0
Proxy_Config - Not Found
Proxy_User - Not Found
Proxy_Password - Not Found
Proxy_Behavior - Use IE settings
Watermark - 943010104
bStageCleanup - True
bCFGCaution - False
KillDate - 0
bProcInject_StartRWX - False
bProcInject_UseRWX - False
bProcInject_MinAllocSize - 8493
ProcInject_PrependAppend_x86 - b'\x90\x90'
Empty
ProcInject_PrependAppend_x64 - b'\x0f\x1f\x00'
Empty
ProcInject_Execute - ntdll:RtlUserThreadStart
CreateThread
NtQueueApcThread
SetThreadContext
ProcInject_AllocationMethod - NtMapViewOfSection
bUsesCookies - True
HostHeader -
—End Cobalt Beacon Configuration Data—

Screenshots

Figure 3 - Screenshot of the XOR based cipher utilized by this TEARDROP variant to decode an embedded Cobalt Strike Beacon payload.

infinitysoftwares.com

Tags

command-and-control

URLs

- infinitysoftwares.com/files/information_055.pdf

Ports

- 443 TCP

Whois

Domain Name: infinitysoftwares.com
Registry Domain ID: 2356151174_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.namesilo.com
Registrar URL: https://www.namesilo.com/
Updated Date: 2021-01-01T07:00:00Z
Creation Date: 2019-01-28T07:00:00Z
Registrar Registration Expiration Date: 2021-01-28T07:00:00Z
Registrar: NameSilo, LLC
Registrar IANA ID: 1479
Registrar Abuse Contact Email: abuse@namesilo.com
Registrar Abuse Contact Phone: +1.4805240066
Domain Status: clientTransferProhibited https://www.icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: Domain Administrator
Registrant Organization: See PrivacyGuardian.org
Registrant Street: 1928 E. Highland Ave. Ste F104 PMB# 255
Registrant City: Phoenix
Registrant State/Province: AZ
Registrant Postal Code: 85016
Registrant Country: US

Registrant Phone: +1.3478717726
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: pw-531dcecd9bbebe6f78f00ff61cc84da6@privacyguardian.org
Registry Admin ID:
Admin Name: Domain Administrator
Admin Organization: See PrivacyGuardian.org
Admin Street: 1928 E. Highland Ave. Ste F104 PMB# 255
Admin City: Phoenix
Admin State/Province: AZ
Admin Postal Code: 85016
Admin Country: US
Admin Phone: +1.3478717726
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: pw-531dcecd9bbebe6f78f00ff61cc84da6@privacyguardian.org
Registry Tech ID:
Tech Name: Domain Administrator
Tech Organization: See PrivacyGuardian.org
Tech Street: 1928 E. Highland Ave. Ste F104 PMB# 255
Tech City: Phoenix
Tech State/Province: AZ
Tech Postal Code: 85016
Tech Country: US
Tech Phone: +1.3478717726
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: pw-531dcecd9bbebe6f78f00ff61cc84da6@privacyguardian.org
Name Server: NS1.DNSOWL.COM
Name Server: NS2.DNSOWL.COM
Name Server: NS3.DNSOWL.COM
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/

Relationships

infinitysoftwares.com	Connected_From	b820e8a2057112d0ed73bd7995201dbed79a79e13c79d4bdad81a22f12387e07

Description

This domain is the C2 for the sample "b820e8a2057112d0ed73bd7995201dbed79a79e13c79d4bdad81a22f12387e07."

Relationship Summary

1817a5bf9c...	Connected_To	ervsystem.com
ervsystem.com	Connected_From	1817a5bf9c01035bcf8a975c9f1d94b0ce7f6a200339485d8f93859f8f6d730c
b820e8a205...	Connected_To	infinitysoftwares.com
infinitysoftwares.com	Connected_From	b820e8a2057112d0ed73bd7995201dbed79a79e13c79d4bdad81a22f12387e07

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

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 1-844-Say-CISA or SayCISA@cisa.dhs.gov.

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.

February 8, 2021: Initial Version|April 15, 2021: Updated with Attribution Statement

---