

## **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

This submission included one unique file. This file has been identified as a variant of the malware known as ICONICSTEALER. This variant of malware was utilized in the supply chain attack on the commercial software 3CXDesktopApp. The primary purpose of this malware is to steal sensitive data from a victim user's web browser, and make it available for exfiltration by a separate malicious component.

### Submitted Files (1)

 $e2ef455e92b3cb5a4c0f3093191d0bfb4fe3ff961e2a403feaa26060a298c70f \ (infostealer.dll)$ 

### **Findings**

### e2ef455e92b3cb5a4c0f3093191d0bfb4fe3ff961e2a403feaa26060a298c70f

Tags	
backdoor	information-stealer trojan
Details	
Name	ofostealer.dll
Size	186167 bytes
Туре	E32+ executable (DLL) (GUI) x86-64, for MS Windows
MD5	9f452576b2430814821da0223a535c8
SHA1	ad1120d91b812acafef7175f949dd1b09c6c21a
SHA256	2ef455e92b3cb5a4c0f3093191d0bfb4fe3ff961e2a403feaa26060a298c70f
SHA512	099c4f970b04400b1b9db283ba60850e806217a3fbceba8bac5168621ad1994cf2c5a77e4ff7639c1660eba79504a5d 684e0c7e3e746d3c8fe60111f436428
ssdeep	4576:qxvjY/8tWCp4I1+HufhT3cimlXiOHhMdR03ZCNgqI0XK:8WCKI1zT3cimlXichMXwCrI
Entropy	.476725
Antivirus	
	AhnLab Infostealer/Win.Agent
	Antiy Trojan/Win64.NukeSped



```
Avira
                         TR/NukeSped.grojn
           Bitdefender
                         Gen: Variant. Supply Chain Agent. 8
              Emsisoft
                         Gen: Variant. Supply Chain Agent. 8 (B)
                 ESET
                         Win64/NukeSped.OX trojan
                         Trojan (005a1eee1)
                    K7
          Trend Micro
                         TrojanS.82E50547
                         TrojanS.82E50547
Trend Micro HouseCall
         VirusBlokAda
                         Trojan.Win64.SamScissors
```

#### **YARA Rules**

```
• rule CISA 10435108 01 : trojan backdoor steals authentication credentials
   meta:
      Author = "CISA Code & Media Analysis"
      Incident = "10435108"
      Date = "2023-04-12"
     Last Modified = "20230412 1700"
     Actor = "n/a"
     Family = "3CXDESKTOPAPP"
      Capabilities = "steals-authentication-credentials"
     Malware Type = "trojan backdoor"
      Tool Type = "n/a"
      Description = "Detects 3CXDesktopApp InfoStealer samples"
      SHA256 1 = "e2ef455e92b3cb5a4c0f3093191d0bfb4fe3ff961e2a403feaa26060a298c70f"
   strings:
      $s0 = { 53 00 45 00 4c 00 45 00 43 00 54 00 20 00 75 00 }
      $s1 = { 72 00 6c 00 2c 00 20 00 74 00 69 00 74 00 6c 00 }
      $s2 = { 65 00 20 00 46 00 52 00 4f 00 4d 00 20 00 6d }
      $s3 = { 6f 00 7a 00 5f 00 70 00 6c 00 61 00 63 00 65 00 }
      $s4 = { 4d 00 6f 00 7a 00 69 00 6c 00 6c 00 61 00 5c 00 }
      $s5 = { 46 00 69 00 72 00 65 00 66 00 6f 00 78 00 5c }
      $s6 = { 33 00 43 00 58 00 44 00 65 00 73 00 6b 00 74 00 6f 00 70 }
   condition:
      all of them
 }
```

#### ssdeep Matches

No matches found.

### **Description**

This file is a 64-bit Windows DLL (Dynamic-link Library). Analysis indicates this application was part of a supply chain attack against the commercial application 3CXDesktopApp. This malicious DLL was included within an installer for the 3CXDesktopApp. The primary purpose of this DLL is to steal information from various web browsers employed by a victim user. This malware is being referred to in open source as ICONICSTEALER. During runtime the application first attempts to read a file named "\\3CXDesktopApp\\config.json". Additionally, the malware attempts to collect the victim system's hostname, domain name, and OS version (Figure 1).

The malicious application next attempts to steal sensitive information from the victim user's web browser. Specifically it will target the Chrome, Edge, Brave, or Firefox browsers (Figure 2). It uses an embedded SQLITE library to query the browser databases for sensitive information (Figure 3). Analysis indicates the data stolen from the web browsers will be websites recently visited including sensitive parameters passed to the sites. These parameters could include sensitive information including login credentials or credit card numbers.

No exfiltration capability was discovered within this malicious application, indicating it works with another malicious component to exfiltrate collected data.



#### **Screenshots**

```
edx, [r9+1Ah]
          lea
                                           ; csidl
          call
                     cs:
          lea
                     r8, Source
                                               \\3CXDesktopApp\\config.json
                     edx, 105h ; SizeInwords
rcx, [rbp+510h+Destination]; Destination
         mov
lea
          call
                                           · "rb
          lea
                     r8, Mode
                     [rsp+610h+Stream], rsi
rdx, [rbp+510h+Destination]; FileName
          mov
lea
          lea
                     rcx, [rsp+610h+Stream] ; Stream
          call
                     rcx, [rsp+610h+Stream] ; Stream rbx, OFFFFFFFFFFFFFFFF
          mov
          mov
                                           ; READONG.CONFIG.JSON
                   rcx, rcx ; loc_1800D30DF
starts at 1800D2F1C
          test
         iz
🔟 🚄
loc_1800D2F97:
                         GSHandlerCheck
     unwind { //
mov
lea
           [rsp+610h+var_28], r12
r8d, [rbx+3] ; Origin
edx, edx ; Offset
xor
           [rsp+610h+var_30], r15
fseek ; FSEEK.FOR.APPEND
call
mov
call
           rcx, [rsp+610h+Stream]; Stream
           rcx, [rsp+610h+Stream]; Stream
                            ; Origin
; Offset
xor
           r8d, r8d
           edx, edx
r15d, eax
xor
mov
call
           edx, [r15+1] ; uBytes
ecx, [rbx+41h] ; uFlags
lea
lea
call
           r9, [rsp+610h+Stream]; Stream edx, [rbx+2]; ElementSize rcx, rax; Buffer
mov
lea
mov
           r8d, r15d
r12, rax
                                 ; ElementCount
mov
call
mov
call
           rcx, [rsp+610h+Stream]; Stream
test
           short loc_1800D304F
```

Figure 1 - This screenshot illustrates this malware attempting to access the file \\3CXDesktopApp\\config.json.

```
org 180113000h
       dq offset aAppdataLocalGo ; "AppData\\Local\\Google\\Chrome\\User Da"...
dq offset aAppdataLocalMi ; "AppData\\Local\\Microsoft\\Edge\\User D"...
dq offset aAppdataLocalBr ; "AppData\\Local\\BraveSoftware\\Brave-Br"...
dq offset aAppdataRoaming ; "AppData\\Roaming\\Mozilla\\Firefox\\Pro"...
       dq offset aAppdataRoaming ; "AppDa
dq offset aHistory ; "History
                                                                  "History
       dq offset aHistory
       dq offset aHistory
dq offset aPlacesSqlite;
                                                                   "places.sqlite"
                                                              ; DATA XREF: CHROME_FINDFIRSTFILE_FINDNEXTFILE+24+o ; "Chrome"
       dq offset aChrome
                                                                   "Edge"
       dq offset aEdge
                                                                  "Brave"
"Firefox"
       dq offset aBrave
dq offset aFirefox
       dq offset aSelectUrlTitle
       ; DATA XREF: SELECT URLS FROM TITLES SQL_QUERIES+CDto
; "SELECT url, title FROM urls ORDER BY id"...
dq offset aSelectUrlTitle; "SELECT url, title FROM urls ORDER BY id"...
dq offset aSelectUrlTitle; "SELECT url, title FROM urls ORDER BY id"...
dq offset aSelectUrlTitle; "SELECT url, title FROM urls ORDER BY id"...
dq offset aSelectUrlTitle_0; "SELECT url, title FROM moz_places ORDER"...
okie da ZB992DDFA232h
                                                               : DATA XREF: sub 1800011E0+Btr
```

Figure 2 - This screenshot illustrates web browsers targeted by this malware, known as ICONICSTEALER.



```
xor
lea
             edx, edx
            rcx, [rsp+8F8h+FileName] r8d, 208h
mov
call
             sub_1800D45C0
xor
lea
             edx, edx
            rcx, [rsp+8F8h+Buffer]
r8d, 208h
sub_1800D45C0
r12, cs:180000000h
mov
call
lea
mov
lea
            r9, [r15+r12+113000h]
r8, [rsp+8F8h+var_678]
rdx, aSS_4 ; "%s\
lea
            rcx, [rsp+8F8h+FileName]; Buffer
sub_1800D2DC0
lea
call
            rdx, [rsp+8F8h+FindFileData]; lpFindFileData
rcx, [rsp+8F8h+FileName]; lpFileName
cs:FindFirstFileW; START.ENUMERATING.FOLDER
lea
lea
call
mov
cmp
jz
             rax, OFFFFFFFFFFFFFFF loc 1800D3390
         4
          loc_1800D32D3:
          lea
                      rdx, asc_1800EE8A4
                      rcx, [rsp+8F8h+FindFileData.cFileName] ; String1
          lea
          call
          test
                      eax, eax
loc_1800D3371
         jг
           <mark>■</mark> 🕍 🗷
lea
                        rdx, asc 1800EE8A8 ;
                        rcx, [rsp+8F8h+FindFileData.cFileName] ; String1
            lea
           call
                        eax, eax
short loc_1800D3371
           test
           jz
          u 🚾 🖼
test
                      byte ptr [rsp+8F8h+FindFileData.dwFileAttributes], 10h
short loc_1800D3371
              MOV
                           rax. [r15+r12+113020h1
```

**Figure 3** - This screenshot illustrates the malware beginning to search through folders of various web browsers looking for the database files. The database files will be queried with an embedded SQLITE library looking for sensitive information.

```
r8d, 208h
qword ptr [rbp+410h+UrlComponents.dwExtraInfoLength], rax
xmmword ptr [rsp+510h+UrlComponents.dwScructSize], xmm0
xmmword ptr [rsp+510h+UrlComponents.dwSchemeLength], xmm0
xmmword ptr [rsp+510h+UrlComponents.dwHostNameLength], xmm0
xmmword ptr [rsp+510h+UrlComponents.dwUserNameLength], xmm0
xmmword ptr [rbp+410h+UrlComponents.dwPasswordLength], xmm0
xmmword ptr [rbp+410h+UrlComponents.dwUrlPathLength], xmm0
xmmword ptr [rsp+510h+UrlComponents.dwPasswordLength], xmm0
xmmword ptr [rbp+410h+UrlComponents.dwPasswordLength], xmm0
xmmword ptr
mov
mov
movups
movups
 movups
movups
movups
movups
call
  lea
                                                  rcx, [rbp+410h+NewFileName]; Buffer
sub_1800D2DC0
  call
xor
                                                                                                                                                        ; bFailIfExists
                                                    r8d, r8d
                                                 rdx, [rbp+410h+NewFileName]; lpNewFileName rcx, rdi ; lpExistingFileName cs:CopyFileW ; MAKE.BACKUP.OF.CHROME.FILES rdx, [rsp+510h+var_4D8]
 mov
call
lea
                                                  rcx, [rbp+410h+NewFileName]
sub_1800CB440
lea
call
test
                                                  eax, eax
loc_1800D35ED
 jnz
                                                                       lea
                                                                                                                          rdx, off_180113060 ; "SELECT url, title FROM urls ORDER BY id"...
rax, OFFFFFFFFFFFFFF
                                                                        mov
mov
                                                                                                                           rdx, [rdx+rbx*8] ; SQL.QUERY
                                                                                                                                                              i 🚾
                                                                                                                                                               loc 1800D34B0:
                                                                                                                                                                                                                  [rdx+rax*2+2], r12w
                                                                                                                                                             cmp
lea
                                                                                                                                                                                                                 rax, [rax+1]
short loc_1800D34B0
                                                                                                                                                             jnz
```



**Figure 4 -** This screenshot indicates the malware "backs up" the web browser databases before querying them for sensitive information. It may do this to prevent accidental corruption of the databases, or to prevent the browser from crashing if the user is currently browsing the web.

#### 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)



**TLP: CLEAR** 

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 <a href="https://www.cisa.gov">www.cisa.gov</a>.

