# MAR-10435108-1.v1 ICONICSTEALER | CISA

Published: 2023-04-20 · Archived: 2026-04-05 17:38:50 UTC

## Notification



## 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.

Download the PDF version of this report:

#### Submitted Files (1)

e2ef455e92b3cb5a4c0f3093191d0bfb4fe3ff961e2a403feaa26060a298c70f (infostealer.dll)

## Findings

#### e2ef455e92b3cb5a4c0f3093191d0bfb4fe3ff961e2a403feaa26060a298c70f

#### Tags

backdoor information-stealer trojan

#### Details

| | |
|---|---|
| **Name** | infostealer.dll |
| **Size** | 1186167 bytes |
| **Type** | PE32+ executable (DLL) (GUI) x86-64, for MS Windows |
| **MD5** | c9f452576b2430814821da0223a535c8 |
| **SHA1** | cad1120d91b812acafef7175f949dd1b09c6c21a |
| **SHA256** | e2ef455e92b3cb5a4c0f3093191d0bfb4fe3ff961e2a403feaa26060a298c70f |
| **SHA512** | 9099c4f970b04400b1b9db283ba60850e806217a3fbceba8bac5168621ad1994cf2c5a77e4ff7639c1660eba79504a5de684e0c7e3e746d3 |
| **ssdeep** | 24576:qxvjY/8tWCp4I1+HufhT3cimlXiOHhMdR03ZCNgqI0XK:8WCKI1zT3cimlXichMXwCrI |
| **Entropy** | 6.476725 |

#### Antivirus

| | |
|---|---|
| **AhnLab** | Infostealer/Win.Agent |
| **Antiy** | Trojan/Win64.NukeSped |
| **Avira** | TR/NukeSped.grojn |

| | |
|---|---|
| **Bitdefender** | Gen:Variant.SupplyChainAgent.8 |
| **Emsisoft** | Gen:Variant.SupplyChainAgent.8 (B) |
| **ESET** | Win64/NukeSped.OX trojan |
| **K7** | Trojan ( 005a1eee1 ) |
| **Trend Micro** | TrojanS.82E50547 |
| **Trend Micro HouseCall** | TrojanS.82E50547 |
| **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

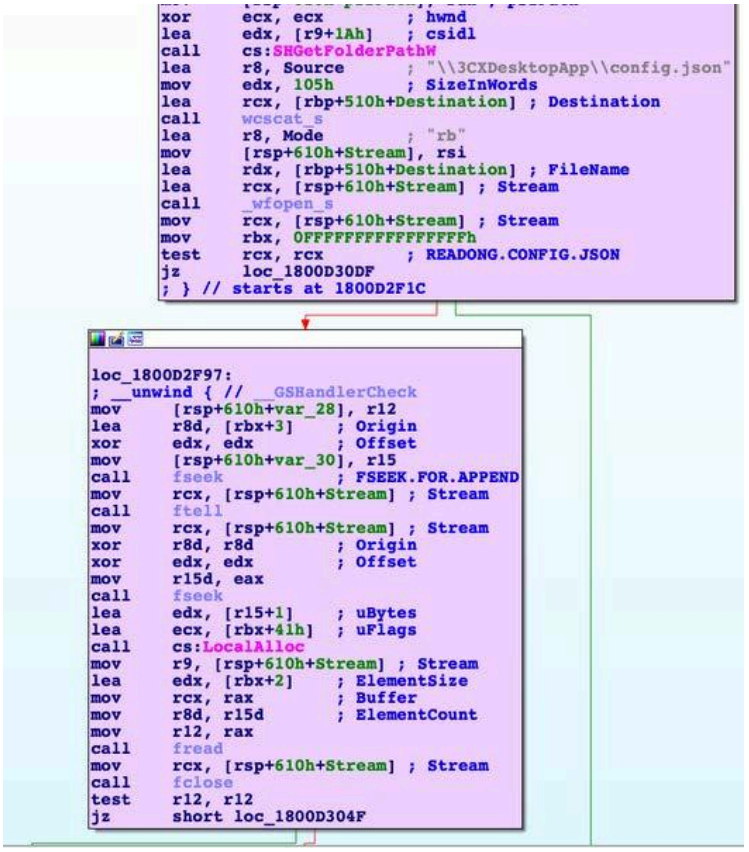


**Figure 1 -** This screenshot illustrates this malware attempting to access the file \\3CXDesktopApp\\config.json.


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

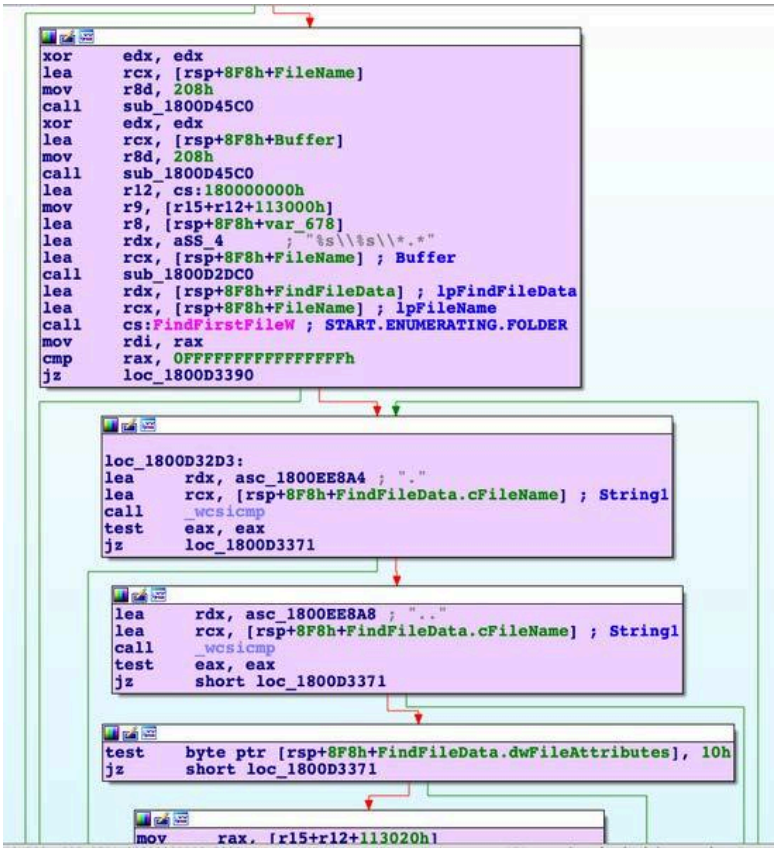


**Figure 3 -** This screenshot illustrates the malware beginning to search through folders of various web browsers looking for the database files. The database files will be queried with an embedded SQLITE library looking for sensitive information.

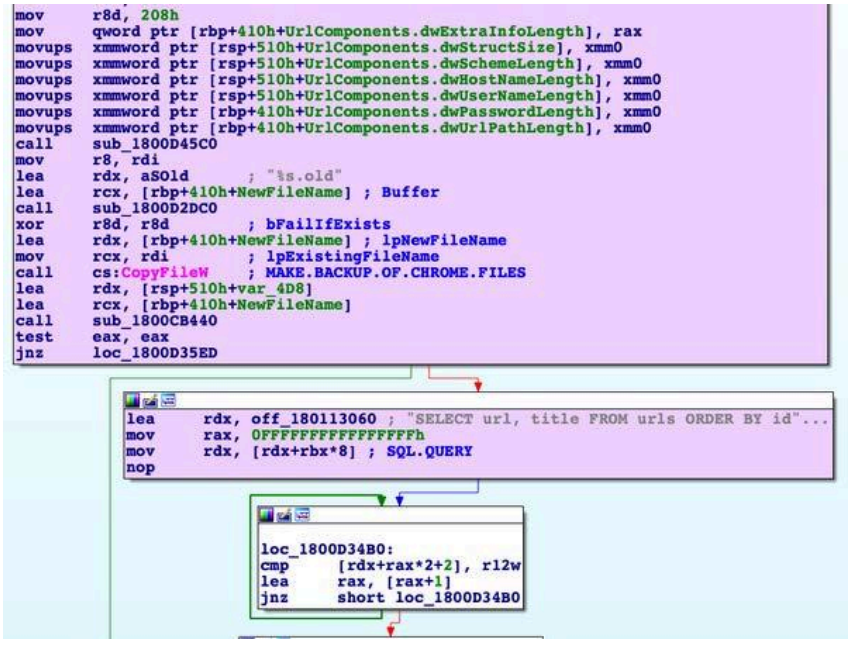


**Figure 4 -** This screenshot indicates the malware "backs up" the web browser databases before querying them for sensitive information. It may do this to prevent accidental corruption of the databases, or to prevent the browser from crashing if the user is currently browsing the web.

### 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

- 1-844-Say-CISA
- CISA Central✉ (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 MAR?** A Malware Analysis Report (MAR) is intended to provide organizations with more detailed malware analysis acquired via manual reverse engineering. To request additional analysis, please contact CISA and provide information regarding the level of desired analysis.

**Can I edit this document?** This document is not to be edited in any way by recipients. All comments or questions related to this document should be directed to the CISA at 1-844-Say-CISA or CISA Central✉.

**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.

This product is provided subject to this Notification and this Privacy & Use policy.

### ACKNOWLEDGEMENTS

SentinelOne contributed to this report.

---