IcedID Stealer Man-in-the-browser Banking Trojan

blog.cyberint.com/icedid-stealer-man-in-the-browser-banking-trojan

December 2, 2020

Executive Summary

IcedID stealer (Also known as BokBot) was first discovered at the end of 2017, believed to be a resurgence of the NeverQuest banking Trojan. It is a modular banking trojan that uses man-in-the-browser (MitB) attacks to steal banking credentials, payment card information and other financial data.

The stealer possesses relatively sophisticated functionality and capabilities such as web injects, a large remote access trojan (RAT) arsenal and a VNC module for remote control. Additionally, the use of steganography to hide configuration data along with anti-VM detection and anti-debugging techniques complicate detection and analysis.

IcedID's typical range of targets includes the customers of banks and telecommunications organizations worldwide leading to impacts including brand abuse, funds theft and customer data breaches.

Cyberint have recently observed an ongoing campaign targeting users in the APAC region with an apparent focus on the Philippines and Japan.

The IcedID stealer is traditionally delivered by a malspam lure, with Microsoft Word attachments weaponized with malicious Macros, based on Emotet.

While the majority of recently detected lure documents were written in English and targeted a wide range of users, localized campaigns have also been reported. One such recent example targeted users located in Japan with lure documents in Japanese, likely indicating that the threat actor behind this threat is relatively sophisticated and may focus on specific geographies as potential targets, adjusting their arsenal accordingly.

Whilst it is not possible to attribute IcedID to a specific group, past indications suggest a potential link to the following threat actors:

- Lunar Spider
- TA2101

Delivery

As a generic malspam campaign that utilizes Emotet as the delivery mechanism, the lures are comprised from a generic subject (quotation/request/Document/report) being sent to the targeted user.

The email contains an attached ZIP folder protected by a password provided within the email body. At the next stage, once the user extracts the document file from the ZIP folder, they will be requested to 'Enable Content' (Figure 1) within Microsoft Word, leading to malicious Macro code being executed whilst decoy content (Figure 2) is displayed.

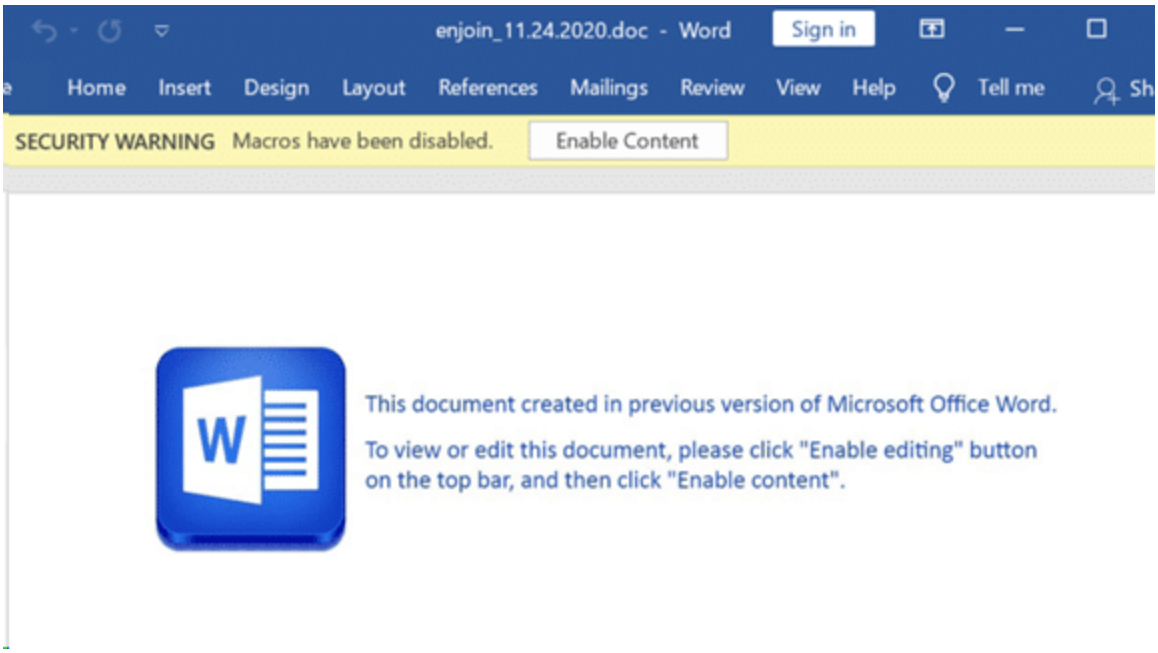


Figure 1 – Prompt to relax security controls

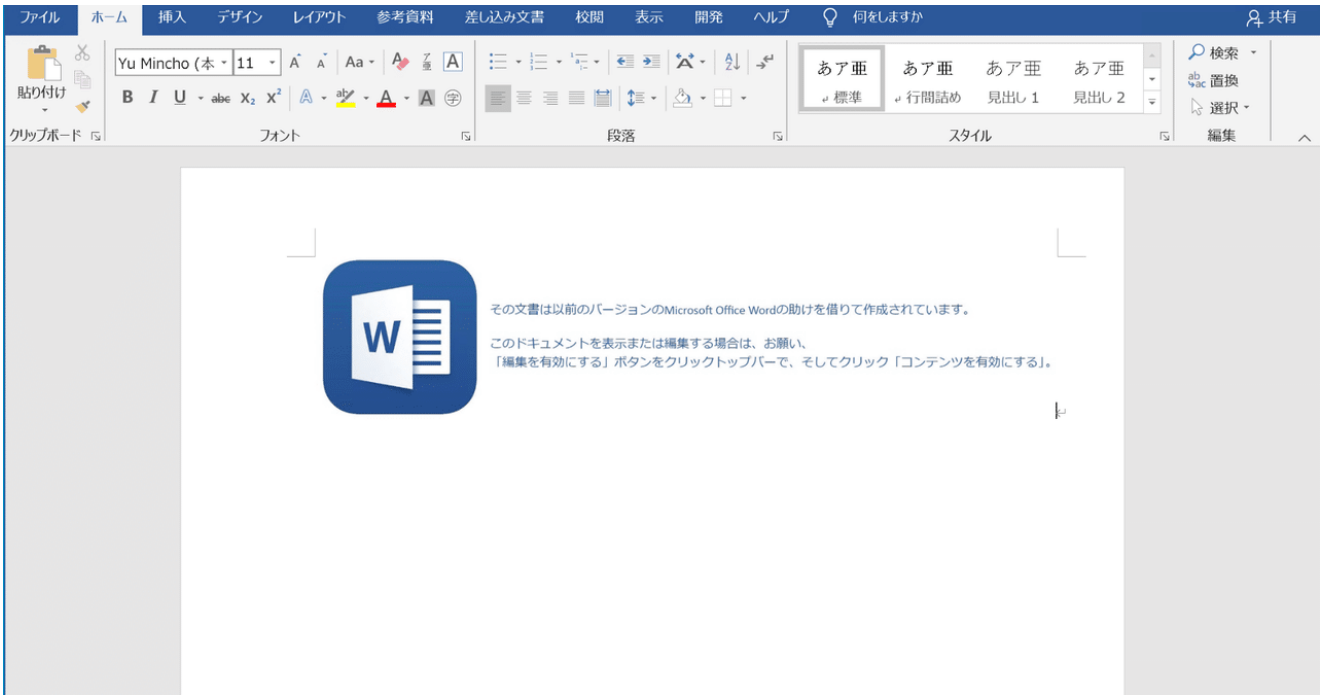
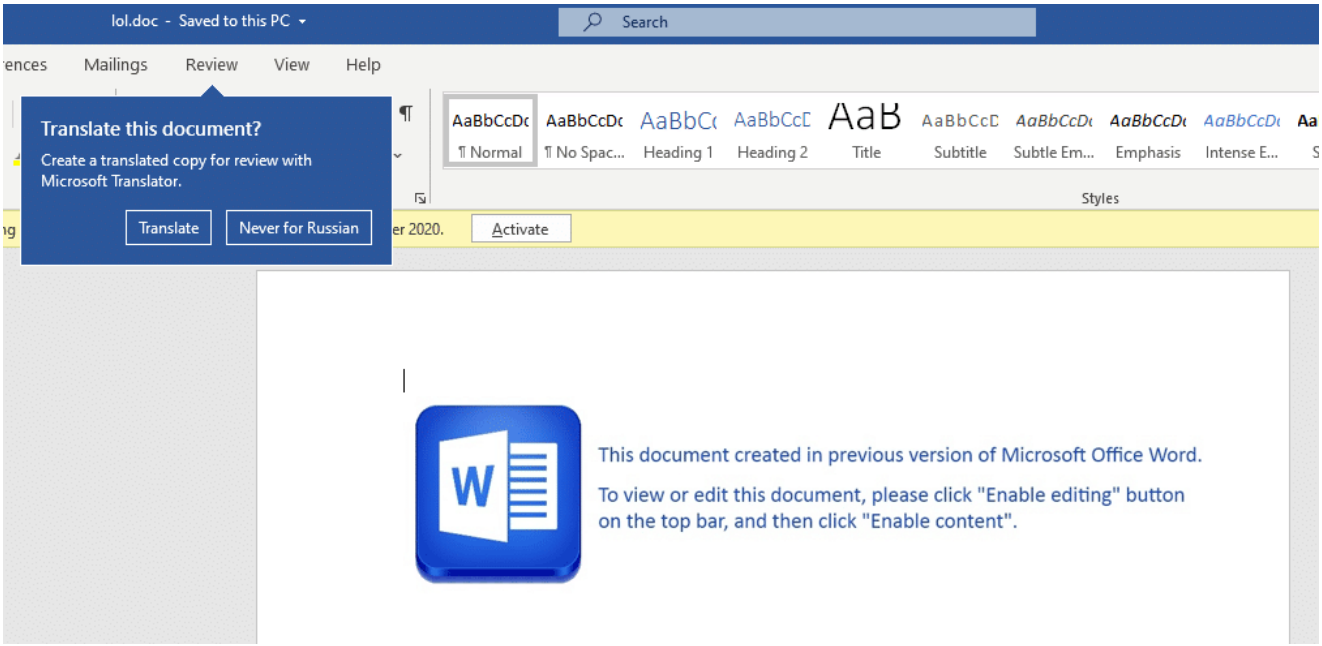
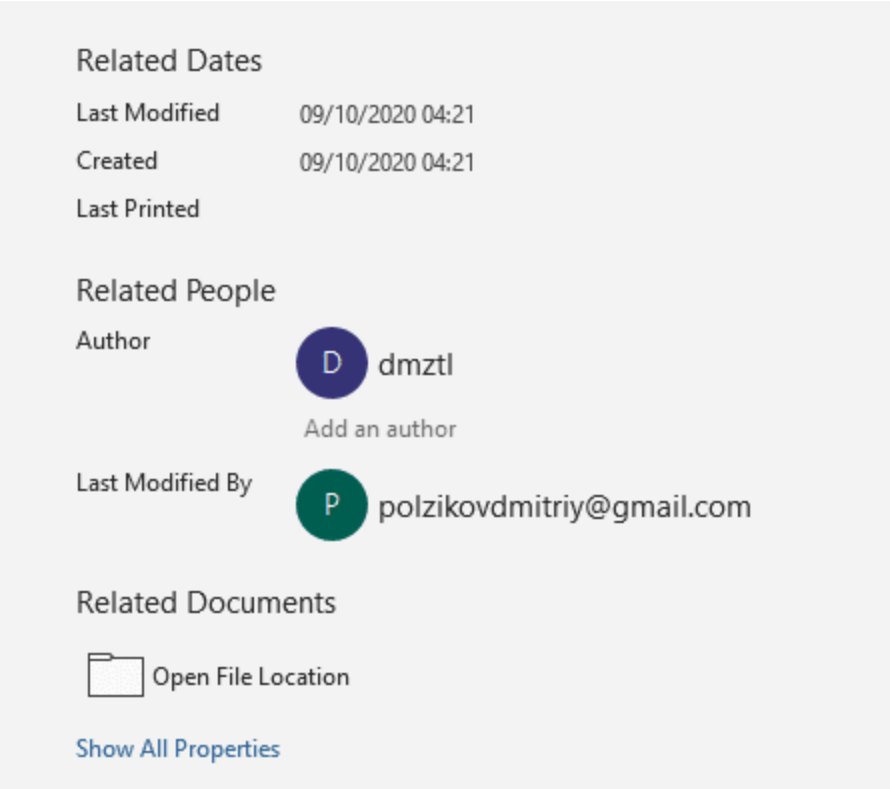


Figure 2 – Decoy document content



Document metadata detected as Russian



Threat actor email address, used for the file creation

Once executed, the macro will write a variety of files to the drive, used for the download and decryption of the latest IcedID trojan, including an up-to-date configuration file containing a list of target bank and telecommunication organizations. In some cases, this was observed as a DLL file, where in others it was a steganographically obfuscated PNG file (Figure 3).

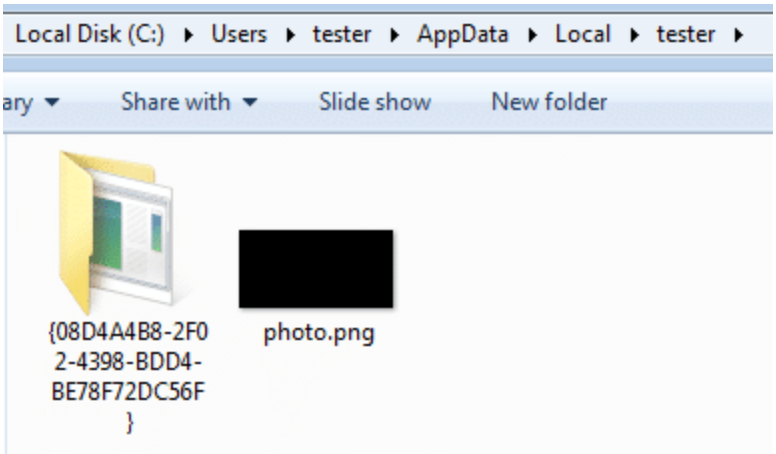


Figure 3 – PNG Configuration Payload

Although surfaced in 2017, many iterations of this trojan have been well-investigated by numerous security researchers globally, but for the past year (circa January 2020), several new techniques were added in order to detect and evade sandboxes, and to generally hide the execution process taking place.

It was also noticed that the malware creates a new folder with a random name, where it saves a downloaded configuration in encrypted form (Figure 4).

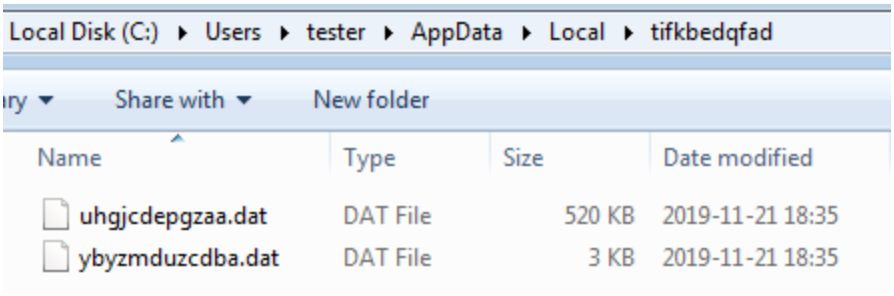


Figure 4 – Download directory

Inside the %TEMP% folder, it drops some non-malicious helper elements: sqlite32.dll (that will be used for reading SQLite browser databases found in web browsers), and a certificate that will be used for intercepting traffic (Figure 5).

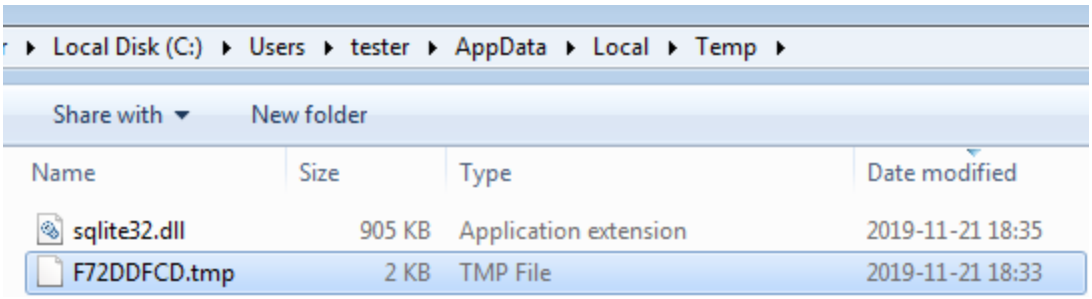


Figure 5 – Temp directory

Infection

Once infected, the IcedID trojan, known as a banking Trojan, steals data related to banking transactions by injecting implants into browsers, API hooks and a ‘Man-in-the-Browser’ (MitB)[1] attack to manipulate visited webpages.

As observed (Figure 6) in the memory of an infected host, the svchost process contains strings that reveal the configuration of these ‘web-injects’, that being modular HTML and JavaScript code elements that are injected into the webpage of a targeted brand to steal data.

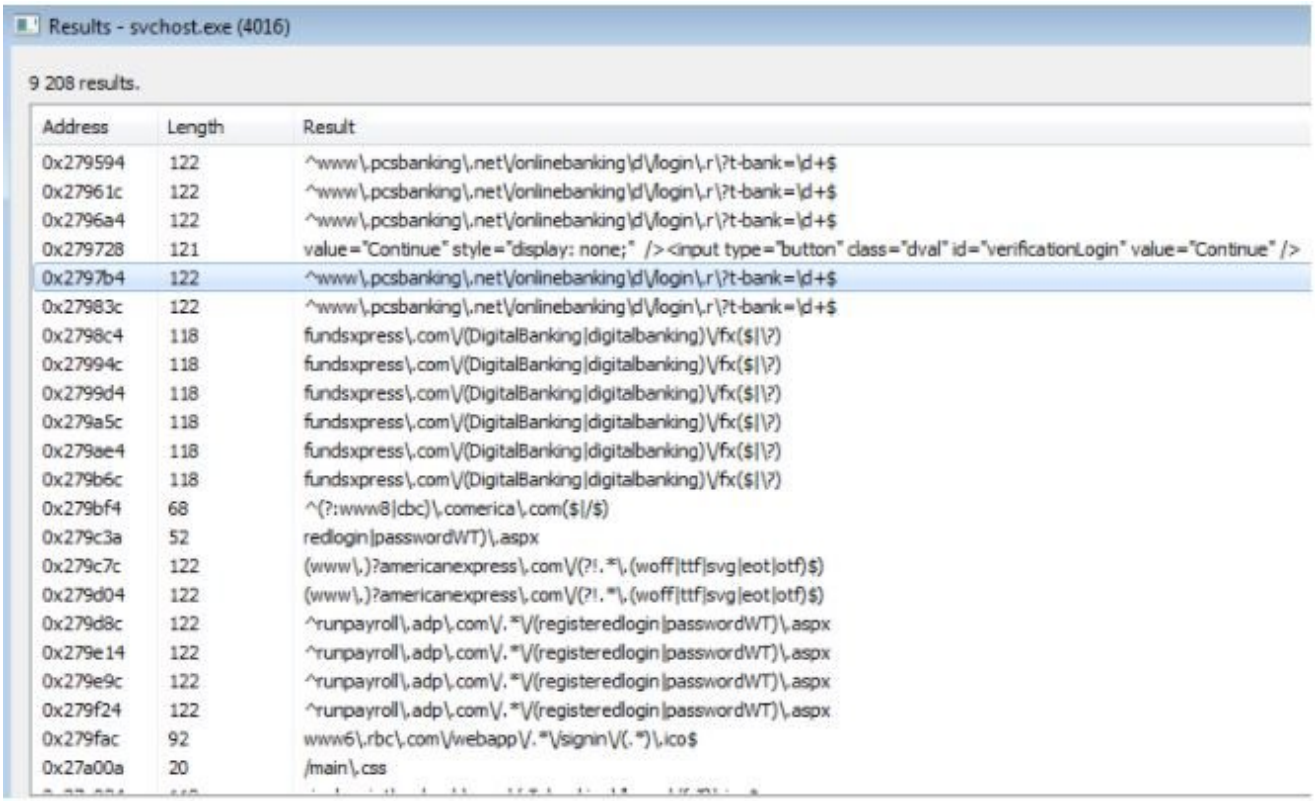


Figure 6 – Web-inject strings found in memory

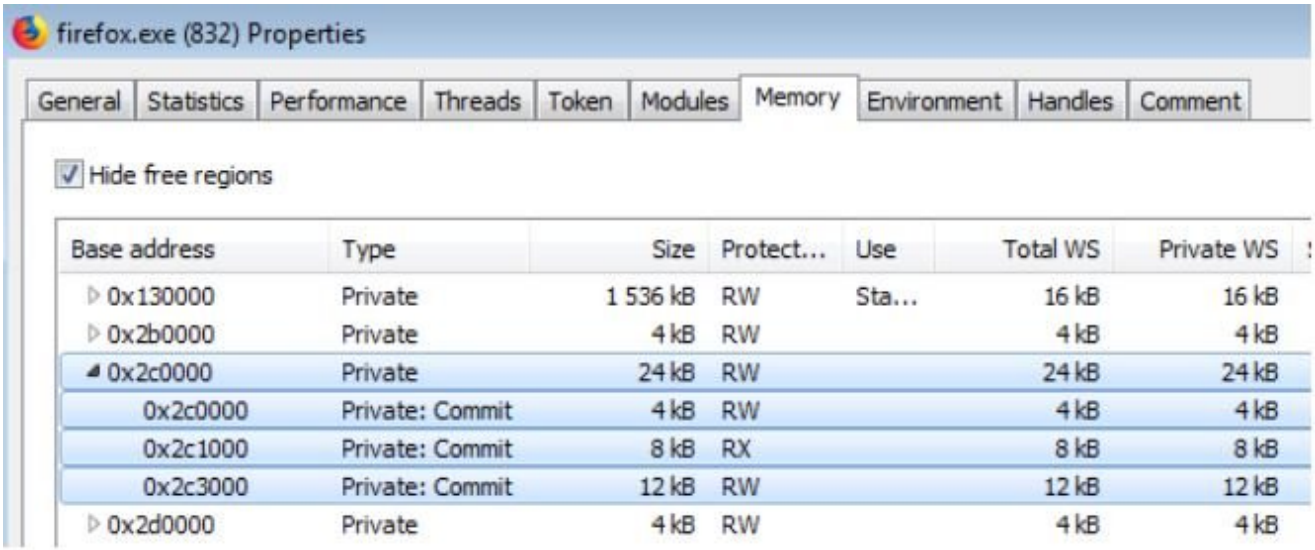


Figure 7 – Mozilla Firefox Web-inject

Figure 8 – Injected code snippet executed on the client side (Example code available via GitHub[2])

The core bot that runs inside the memory of the svchost process observes other processes running on the system and injects implants into browsers, for example as seen in Mozilla Firefox (Figure 7).

The IcedID module running inside the browser's memory is responsible for applying the web-injects and installing malicious JavaScript into targeted webpages causing them to be executed on the client side (Figure 8).

C2

The hooked scripts, loaded from modified browser DLLs, communicate with the main bot process residing inside the svchost process. The main bot coordinates the work of all the injected components and exfiltrates stolen data to the C2 server.

In order to properly hide and encrypt its communication processes, all C2 communications are made over HTTPS using the trojan's own certificate (Figure 9).

Recommendations

- Notify customer care of the ongoing threat in case of funds loss.
- Cyberint recommends that customers educate their end-users and always check for unusual browser behaviors that may lead to account compromise or funds theft.
- Phishing awareness to the end-users is advised.
- Usage of a modern, updated AV solution is advised.
- MFA should be enabled on all of the end-user accounts.

Indicators Of Compromise

Targeted Brands/Organizations

Based on strings extracted from IcedID samples, the following brands and/or organizations appear to be targeted:

- `Amazon.com`
- `American Express`
- `AT&T`
- `Bank Of America`
- `Capital One`
- `Chase`
- `CIBC`
- `Comerica`
- `Dell`
- `Discover`
- `Dollar Bank`

- `eBay`
- `Erie Bank`
- `E-Trade`
- `Frost Bank`
- `Halifax UK`
- `Hancock Bank`
- `Huntington Bank`
- `J.P. Morgan`
- `Lloyds Bank`
- `M&T bank`
- `Centennial Bank`
- `PNC`
- `RBC`
- `Charles Schwab`
- `SunTrust Bank`
- `Synovus`
- `T-Mobile`
- `Union Bank`
- `USAA`
- `US Bank`
- `Verizon Wireless`
- `Wells Fargo`

IcedID Samples

The following SHA256 hashes relate to recently observed IcedID malware samples:

- `00ec5cc40b91832adc257b43cb28f2fe0734c6e1761ae5020bd8178116ed005c`
- `02c2cace0eab2cb902cf567be3524616db1747abd79c3417d3762452c604ab85`
- `08cc79fac123eefee7e05e3568a0aa6d219e43d22b0679ea5d7a3ffaf4337403`
- `08d1f171b424a35c7aeebb55da2077078f62fae847616a4f8c80f3e3e11d6573`
- `10164d00c17bacb88eca79a8a836176ac49bfb7547ed90efcb86d19cdfda9dcb`
- `12b73194a373f12d89a83152bd56ee02054dd20030cb6b421b7e79e70e1d2484`
- `17f2d25fcba0ad909c0561179407b4bb37917b643b2c181dcdcb4c3cec743a5c`
- `213347251fc9f4b6812547ecfef2b3783789067ccffee1521eb88c36003a742e`
- `36d5d2317b7172e45229c24b2870bd827a8bdc7204fe2cd70aedb74c81e75126`
- `3df7246090c8b2a9c9d19d68ca4bd2908247494a8badea39c00e3f20d60dfcae`
- `3eace4aacf5dc5dc624ab72cf84b7c0f476ee0ff0de267d0976e25d2eee9f5d9`
- `3f1b388938f1e6c6920e54639b8a3dafa9e381f3ef45e855123941e83bad64c7`
- `3f8bc3cde5654bd8ac467a2efd1f926808c5915a6fd3e3f1d32edd13eaf3f1b1`
- `4e7b3116a6589afe645b3e42e0ee9d0fa9c41c7847bca52e1be85ccd1058556b`
- `550e7c5e79a0455d26f02e84921b7c40645d0b361c1e09e1b00bc79a930b2e85`
- `56de520fa4445ccabe60373b039299f5709f291ff594482c92670d1eb8b911f6`

- 6297e0fa6229c7f329f66227656bbf99d1329aaa48341c2f750c78f1937ac952
- 65ca5c2ea9b9eb4d10ab9d91e3928bdff5f27883a5a4c85a4e0871b56ab3533f
- 6a6243c111cbf9a94177835ab02a8378497ed18b5ba1d6fdceb03e9410e08cec
- 6bae8f2c4c1b730825cc5e9ce7bae35039eb08833b7310bf4f444d2524b1601f
- 6df240658329d6c21a7d6669c47ad824cb0d8af76cca197da2d919f27fc4b70e
- 6eb53a11d07dd708ecb63b036145e7e942a61eb693cc3353c612569121b4a110
- 732a12f4a7b85176abfc17c142e83761d7a957672852af0d9069a9bc47defeb1
- 75509601134e810e7ae3dc36e8b9abff1025c0a0dada3b21ead7e24fd5f3ce2c
- 79957427faa2eed376f597aba9eb43fe9789e715833026fefd50458c73ee32b4
- 7a1a59257242c047bb2864abb448e00cfc8b2d281faab4bbfd3ce790c9c27400
- 7a371fcda4e07d7d7e516eed24c84908a601041bc00bb8736680d0b2349e3dec
- 7d6cdbaac836d0c95876c7c669687c933d3097477680864d9d4d6b7fb0c08345
- 7df70a77a6d20050c3d38bc30a2ccfeef4523f811c128717dbfd82325b50bbc8
- 7f19267b62de5efe0bbcd716c9f481e108fb60f4d35435595ae27489d08f7e0d
- 7fde0ff1061d3d15fe584f6ea186e1a23b9ce07123ff9dd70f71fcb51c099369
- 8be1e875a92483a1301d9144b5cd8897951ccb3ca811c99f10e51fff67552166
- 8c7dc92c6019d80364cda2d6ce19b157ac77b013731415d825b1a30f93c6d56d
- 9bb46cd5d1047a3694b3a3862c7ec16d0c3e7838d91c1361760f92958897be5c
- a4f88c40f615a527c16159d41c2798ff452c17a394e96d3b028516c46f88462f
- a7d8b3ab991c3be2e0f60fd748be9b55072f65b4cc0a36dc0d3c470ac3ea33b2
- b559a7560009ca33ad205d32122cb67538dd392ea4a4f5feffa521288810e5bd
- b8a1f0962411b5e5b5bc5e2c77b56c5a2f0fdfc5fe3c3a5857466fbfe9ac66bd
- b9d50f2ddfaa200c7c4695a9eb59c81347b52d53383534997c8b318b75be07d1
- ba92631f803bed252ce1839612315ab40653b2eff3e5f12edc38e4a66e004ccb
- baf2c1ade873167029a7ebc83ba56dca256ca91bd527a451ddde2efa3e3b6ddb
- c6019a1c6d66bc6aae0b6c1502ff241dd9cd00b60ef5e45b2dbd38571f40fb1f
- c6ea88ec4f01251649010e4a364374c90fc9f5bb6c22f1368ee5f222ea5e9b60
- c7bb632d52a485b9a2be160b2f8fa29abb3cd840ef0e7747f5d509846dcbf38b
- ca6738bd50f5eb9a4559f58d5c5ee6e8045a30fd306c110d760dcc325c9aacff
- cab24ced596b142b9bb38e691addea16c72b40d4b5f96865a25052ff11aeb6e0
- cdba1a0f75ecbeda42243f44cd8ac9b9fcd90e9213d8b4f8280e90b956635030
- ce36a13c5f837b9a1658ea5d77f1114b16ce4dada582e47d646321e5dd7cb0c1
- d35d93cbf992171905ec9c00f6c821850d3d1335c591df86f2dd3966d25f8ba0
- d5baabfe5ca28dd041bea2504807dbcdb1ff91b5c8f7e74c16e56f5b810ea3b5
- d9c7e8813b3d6c361e655a90c76b713bc90865819394df52e38e6012e48836b8
- e77c51ee76cde36adf1ad4a2461a3d29e6964aa13fde870c4e6fad041cebbec8
- eb1c15124298fa388784f270ceb0e6176dac3e65ad81f2e6951b1c4ce9381ea3
- f540a652469981b7a0ba4337c228712888e1d9cf75a00ce17c3fd3775c9b2781
- f6cba12a315620b39f172e496ade5dd6048cc09a6e454f9209284c73ffd055e2
- f8ed31cb2708b5230a3ce326153dbe0a1821161ef5e8b4d9e4df1edcd536db3e
- fc9565534d447bb7d5498aec1dcf1e0b933a7a717c159690529ba3b5ad7c9922

Command & Control Infrastructure

The following command and control (C2) IP addresses have recently been observed as IcedID infrastructure:

- `149.154.64.179`
- `178.250.156.74`
- `178.250.157.144`
- `185.219.43.85`
- `185.98.87.6`
- `193.109.79.219`
- `193.201.126.18`
- `194.61.2.224`
- `45.12.4.206`
- `45.128.206.80`
- `45.129.237.168`
- `45.150.64.102`
- `45.150.64.57`
- `45.8.124.36`
- `45.89.67.169`
- `5.253.61.235`
- `62.109.14.179`
- `80.85.158.53`
- `83.166.242.27`
- `93.189.41.223`

References

[1] https://blog.malwarebytes.com/threat-analysis/2019/12/new-version-of-icedid-trojan-uses-steganographic-payloads/

MITRE ATT&CK

The following techniques have been observed in recent IcedID campaigns:

Technique	Tactic
T1027 – Obfuscated Files or Information	Defense Evasion
T1027.002 – Software Packing	Defense Evasion
T1027.003 – Steganography	Defense Evasion
T1047 – Windows Management Instrumentation	Execution
T1053.005 – Scheduled Task/Job: Scheduled Task	Execution, Persistence, Privilege Escalation

T1059.005 – Command and Scripting Interpreter: Visual Basic	Execution
T1069 – Permission Groups Discovery	Discovery
T1071.001 – Application Layer Protocol: Web Protocols	Command & Control
T1082 – System Information Discovery	Discovery
T1087.002 – Account Discovery: Domain Account	Discovery
T1105 – Ingress Tool Transfer	Command & Control
T1106 – Native API	Execution
T1137.001 – Office Application Startup: Office Template Macros	Persistence
T1185 – Man in the Browser	Collection
T1204.002 – User Execution: Malicious File	Execution
T1218.007 – Signed Binary Proxy Execution: Msiexec	Defense Evasion
T1529 – System Shutdown/Reboot	Impact
T1547.001 – Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	Persistence, Privilege Escalation
T1553.002 – Subvert Trust Controls: Code Signing	Defense Evasion
T1555.003 – Credentials from Password Stores: Credentials from Web Browsers	Credential Access
T1573.002 – Encrypted Channel: Asymmetric Cryptography	Initial Access