New Banking Trojan IcedID Discovered by IBM X-Force Research

securityintelligence.com/new-banking-trojan-icedid-discovered-by-ibm-x-force-research/

November 13, 2017

Home / Banking & Finance

New Banking Trojan IcedID Discovered by IBM X-Force Research

Banking & Finance November 13, 2017

By Limor Kessem co-authored by Maor Wiesen , Tal Darsan , Tomer Agayev 7 min read

IBM X-Force research follows developments in the financial cybercrime arena to map the events and trends that shape the threat landscape for organizations and consumers alike. After a year that has been very active in terms of banking malware, point-of-sale (POS) malware and rampant ransomware attacks, the X-Force team identified a new banking Trojan active in the wild dubbed IcedID.

Read the white paper: How digital banking is transforming fraud detection

IcedID Emerges

According to X-Force research, the new banking Trojan emerged in the wild in September 2017, when its first test campaigns were launched. Our researchers noted that IcedID has a modular malicious code with modern banking Trojan capabilities comparable to malware such as the Zeus Trojan.

At this time, the malware targets banks, payment card providers, mobile services providers, payroll, webmail and e-commerce sites in the U.S. Two major banks in the U.K. are also on the target list the malware fetches.

IcedID does not seem to have borrowed code from other Trojans, but it implements comparable features that allow it to perform advanced browser manipulation tactics. Although IcedID's capabilities are already up to par with those of other banking Trojans such as Zeus, Gozi and Dridex, our researchers believe it will see further updates in the coming weeks.

Served by Emotet

X-Force's analysis of IcedID's delivery method suggests that its operators are not new to the cybercrime arena, opting to infect users via the Emotet Trojan. X-Force research believes that a threat actor or a small cybergang has been operating Emotet as a distribution operation for banking Trojans and other malware codes this year. Emotet's most prominent attack zone is the U.S. To a lesser extent, it also targets users in the U.K. and other parts of the world.

Emotet has been one of the notable malware distribution methods in 2017, serving elite cybercrime groups from Eastern Europe, such as those operating QakBot and Dridex. It has now added IcedID as a new payload drop.

Emotet emerged in 2014 after a leak of the original source code of the Bugat Trojan. It was originally a banking Trojan that preceded Dridex. As such, it is designed to amass and maintain botnets. Emotet persists on the machine and then fetches additional components such as a spamming module, a network worm module, and password and data stealers for Microsoft Outlook email and browser activity.

Emotet itself comes via malspam, usually inside rigged productivity files that contain malicious macros. Once Emotet infects the endpoint, it becomes a silent resident and is operated to serve malware from other cybercriminal groups.

IcedID's TTPs

When it comes to tactics, techniques and procedures (TTPs), IcedID has a few tricks up its sleeve.

Aside from the more common Trojan features, IcedID can propagate over a network. It monitors the victim's online activity by setting up a local proxy for traffic tunneling, which is a concept reminiscent of the GootKit Trojan. Its attack tactics include both webinjection attacks and sophisticated redirection attacks similar to the scheme used by Dridex and TrickBot.

Network Propagation

IcedID's operators probably plan on targeting businesses because they added a network propagation module to the malware from the get-go. IcedID possesses the ability to move to other endpoints, and X-Force researchers also observed it infecting terminal servers. Terminal servers typically provide terminals, such as endpoints, printers and shared network devices, with a common connection point to a local area network (LAN) or a wide area network (WAN), which suggests that IcedID has already been targeting employee email to land on organizational endpoints.

Figure 1: IcedID's network propagation functions, viewed on IDA-Pro

To find other users to infect, IcedID queries the lightweight directory access protocol (LDAP).

Figure 2: IcedID queries the LDAP for more users on the network

IcedID's financial fraud TTPs include two attack modes: webinjection attacks and redirection attacks.

To begin, the malware downloads a configuration file from the Trojan's command-and-control (C&C) server when the user opens the internet browser. The configuration includes targets for which a webinjection attack will be activated — mostly banks and other targets that were fitted with redirection attacks, such as payment cards and webmail sites.

Technical Details

X-Force researchers ran a dynamic analysis on IcedID samples. At this time, the malware deploys on endpoints running various versions of the Windows operating system. It does not appear to possess any advanced anti-virtual machine (VM) or anti-research techniques, aside from the following:

- It requires a reboot to complete full deployment, possibly to evade sandboxes that do not emulate rebooting.
- It communicates via secure sockets layer (SSL) to add a layer of security to the communications and to bypass automated scans by intrusion detection systems.

That being said, X-Force researchers assert that anti-forensic features could be added to this Trojan over time.

Payload Deployment

IcedID is deployed to target endpoints using the Emotet Trojan as a dropper. After a reboot, the payload is written to the Windows %LocalAppData% folder with a value generated per some parameters from the operating system. That value is used both in the deployment path and the RunKey value for the file.

The full convention for the value is: %LOCALAPPDATA%\[a-z]{9}\[a-z]{9}.exe.

C:\Users\User\AppData\Local**ewonliarl****ewonliarl**.exe
HKCU\Software\Microsoft\Windows\CurrentVersion\Run**ewonliarl**

The malware sets its persistence mechanism by creating a RunKey in the registry to ensure its survival after system reboot events.

Next, IcedID writes an RSA crypto key to the system into the AppData folder. The malware may write to this RSA key during the deployment routine, which could be linked to the fact that web traffic is tunneled through IcedID's process even as it channels SSL traffic. X-Force is still investigating the exact use of the RSA key.

The temp file is written according to the following convention: %TEMP%\[A-F0-9]{8}.tmp.

```
C:\Users\User\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-2137145731-
2486784493-1554833299-1000\fdbe618fb7eb861d65554863fc5da9a0_883f9a43-a12c-
410f-b47d-bb7275830b53
C:\Users\User\AppData\Local\Temp\CACCEF19.tmp
```

IcedID's process continues to run, which is rather uncommon for malware. This could mean that some parts of the code are still being fixed and that this issue will change in the next update.

The deployment process ends here and the dropper continues to run under the Explorer process until the next reboot of that endpoint. Upon the reboot event, the payload is executed and the IcedID Trojan becomes resident on the endpoint. At this point, the malware's components are in place to begin redirecting the victim's internet traffic through a local proxy that it controls.

Tunneling the Victim's Web Traffic

IcedID sets up a local proxy to listen and intercept communications from the victim's endpoint and redirects all internet traffic through it in two hops. First, the traffic is transferred to the localhost (127.0.0.1) via port 49157, which is part of the dynamic/private TCP/IP ports. Second, the malware's malicious process listens on that port and exfiltrates relevant communications to its C&C server.

Triggering the Redirection to a Bank Site Replica

Although it has only recently been launched, IcedID already uses redirection attacks. The redirection scheme IcedID uses is not a simple handover to another website with a different URL. Rather, it is designed to appear as seamless as possible to the victim. These tactics include displaying the legitimate bank's URL in the address bar and the bank's correct SSL certificate, which is made possible by keeping a live connection with the actual bank's site.

IcedID's redirection scheme is implemented through its configuration file. The malware listens for the target URL from the list and, once it encounters a trigger, executes a designated webinjection. The webinjection sends the victim to a fake bank site set up in advance to match the one originally requested.

The victim is fooled into submitting his or her credentials on the fake page replica, which unknowingly sends him or her to the attacker's server. From that point on, the attacker controls the session the victim goes through, which typically includes social engineering to trick the victim into divulging transaction authorization elements.

Malware Communications

IcedID's communications take place over encrypted SSL. During a campaign analyzed in late October, the malware communicated with four different C&C servers.

A schematic view of IcedID's infection and communication infrastructure is shown below.

Figure 3: IcedID's infection and communication infrastructure

To report new infections to the botnet, IcedID sends an encoded message with the bot ID and basic system information:

 *Figure 4: IcedID's C&C communication*

Parts of the decoded message shows the following details being sent to the C&C:

- B = Bot ID
- K = Computer Name
- L = Workgroup
- M = OS version

Remote Inject Panel

To orchestrate webinjection attacks for each targeted bank site, IcedID's operators have a dedicated, web-based remote panel accessible with a username and password combination.

Webinjection panels are typically commercial offerings criminals buy in underground markets. It is possible that IcedID's uses a commercial panel or that IcedID itself is commercial malware. However, at this time there is no indication that IcedID is being sold in the underground or Dark Web marketplaces.

Figure 5: IcedID's remote webinject panel login page

The panel communicates back to a server based on the OpenResty web platform. According to its official website, OpenResty is designed to help developers easily build scalable web applications, web services and dynamic web gateways.

A New Player in the Cybercrime Arena?

IcedID is a newly identified threat in the financial cybercrime arena. While it is still early to tell how it will fare, its current capabilities, distribution choices and targets point to a group that is no stranger to this domain.

IBM X-Force research continues to follow and post updates on IcedID on X-Force Exchange. To learn more about mitigating financial threats such as IcedID, please visit IBM Security Trusteer products page.

Indicators of Compromise

IBM X-Force analyzed the following dropper MD5s for this research.

- 38921f28bb74fea2cab6e70039ee65f3
- 6899d3b51430679254635d78357c087e
- c01dcdba9223d037eb8bf0944f1c1c9e
- d982c6de627441765c89da5cfeb04d6f
- de4ef2e24306b35d29891b45c1e3fbfd

Browser Patching

IBM X-Force analyzed the following hooks for this research.

Internet Explorer:

- Connect
- CreateProcessInternalW
- CertGetCertificateChain
- CertVerifyCertificateChainPolicy

FireFox:

nss3.dll!SSL_AuthCertificateHook

Other hooks:

- CreateProcessInternalW
- CreateSemaphoreA

For IP addresses and URLs from our investigation, please check reports in the IcedID collection on X-Force Exchange.

Limor Kessem
Executive Security Advisor, IBM

Limor Kessem is an Executive Security Advisor at IBM Security. She is a widely sought-after security expert, speaker and author and a strong advocate for wom...


IBM Security