MS-ISAC®
Multi-State Information
Sharing & Analysis Center®

Security Primer
September 2019 • SP2019-0961

IcedID

Overview

IcedID, also known as BokBot, is a modular banking trojan that targets user financial information and is capable of acting as a dropper for other malware. It uses a man-in-the-browser attack to steal financial information, including login credentials for online banking sessions. Once it successfully completes its initial attack, it uses the stolen information to take over banking accounts and automate fraudulent transactions. IcedID is primarily dropped as a secondary payload from other malware, most notably Emotet, in addition to its own malspam campaigns. IcedID uses multiple injection methods to evade antivirus and other malware detection methods, such as injecting itself into operating system (OS) memory and regular processes. The malware authors are known to update IcedID to increase persistence and evade new detection efforts.

Main Module

Following the initial infection, IcedID bypasses antivirus and establishes persistence through process-hollowing. The malware hooks several Application Programming Interface (API) functions, such as "ntdll!ZwCreateUserProcess" and "ntdll!RtlExitUserProcess". Once it executes, the malware removes the hooking code and creates a service host process, "svchost.exe." This allows IcedID to write itself into two Dynamic Link Libraries (DLL), the "KERNEL32.DLL" and "SHLWAPI.DLL." Once "svchost.exe" is created, it writes the payload into the "%ProgramData%" or "%AppData%" folder, depending on the victim's account privileges. Additionally, a scheduled task is created, which allows the malware to execute its binary every time the system reboots. Lastly, IcedID creates three additional "svchost.exe" subprocesses to hold its shellcode.

The malware then waits for the system to reboot before initiating its main module. These steps ensure IcedID's malicious processes successfully run and appear to be legitimate processes on the OS every time the system reboots. IcedID is capable of propagating throughout the network, allowing it to monitor all activity on the infected system, exfiltrate data, and conduct a man-in-the-browser attack. In specific, the man-in-the-browser attack is made up of three steps:

- Web-injection
- Proxy Setup
- Redirection

IcedID waits for the user to open a web browser, such as Firefox, Google Chrome, or Internet Explorer. When a browser is launched, IcedID identifies the type of browser and injects shellcode into the application. To further evade detection and security applications, it also allocates memory to the target process and injects its shellcode. After the injection of its shellcode, IcedID applies a patch to the "NtWaitForSingleObject" function, which modifies the browser’s protection status. This browser injection process is perpetually repeated when another browser application is opened. The web-injection attack allows the malware to see the victim's activity, interfere with the browser's behavior, and silently collect associated information.

One browser function IcedID hooks, is "Ws2_32:connect." This function redirects traffic to an IcedID proxy server. The proxy server redirection is set up via creating an additional malicious "svchost.exe." The additional "svchost.exe" is used to create instructions for setting the IP address with a new port number. The proxy server then begins receiving all browsing traffic. This proxy is established to monitor browsing traffic to identify specific information, such as login credentials, banking information, and payment card details. Upon identification, this data is exfiltrated from the victim's network to the attacker's Command and Control (C2) server.

A key web-injection is the malware's recent use of an Automatic Transaction System (ATS) Engine. This is a control panel based in the web browser that works directly from the injection server. The use of this commercial injection panel gives IcedID additional flexibility when stealing data, creating fraudulent transactions, and updating the injection process, as it does not rely on commands from the C2 server.

After a proxy is established, the malware monitors traffic and begins preparing to redirect traffic. IcedID uses malicious websites that masquerade as legitimate major banking and financial institutions. These fake websites are hosted on the cyber threat actor's (CTA) server and are used to socially engineer victims into providing login credentials and bank account access. This is accomplished through the proxy server, which generates a SSL certificate and then inserts it into the certificate store via the "CertCreateSelfSignCertificate" function. In addition, IcedID hooks the Boolean function to validate the certificate's chain of trust, which is then used to authenticate the forged certificate.

All user traffic is intercepted at the proxy. The proxy redirects the victim to the malicious mirrored websites which then forwards login credentials and associated information to the actual website. Using this method, IcedID successfully circumvents multi-factor authentication (MFA). For example, when a victim enters the MFA code from an email or text message into the malicious website, it is immediately captured, redirected, and used on the real banking login page.

Command and Control Communication

IcedID communicates with its C2 server using Hypertext Transfer Protocol Secure (HTTPS) via its proxy. IcedID downloads files to the infected client as well as exfiltrates information back to the C2 server. Traffic from the infected system to the C2 server contains unique client IDs about the infected host along with other exfiltrated data. These unique IDs are used to identify the individual client through a bot, project, or campaign ID, which helps the malware operator determine the malware's stage of infection. The malware's IDs are hashed for verification when communicating with the C2 server.

Obfuscation and Encryption

IcedID uses four different obfuscation methods to make code analysis difficult. Its DAT files are encrypted at rest, with decryption occurring on an as needed basis. It uses the unique client ID and specific file IDs to create the encryption key. Secondly, IcedID uses string obfuscation to encode significant strings with a XOR cipher via a shifting key algorithm. Additionally, IcedID uses signature verification when the binary or the C2 URLs require updating. Lastly, the malware is polymorphic, which makes detection and analysis more difficult. The binary code of the ".text" section of the malware is modified every time it is installed on a system. After modification, the virtual size is updated and a new checksum is generated for verification.

Network Propagation

IcedID seeks to propagate throughout a network using a brute force dictionary attack against user accounts it finds through querying the Lightweight Directory Access Protocol (LDAP). In addition to IcedID's own propagation method, it will leverage Emotet's existing network access if Emotet is present on the system. Using these methods, it seeks to move from the original host to other endpoints and terminal servers. These servers service various endpoints, such as workstations, printers, and other shared network devices.

Recommendations

The MS-ISAC recommends organizations adhere to the following general best practices, to limit the effect of IcedID.

- Perform regular anti-malware scans of systems to ensure that known malicious files are promptly detected and mitigated. Ensure that antivirus applications are kept up-to-date with the latest definitions.
- Ensure that antivirus software is both deployed and centrally monitored across all endpoints.
- Apply appropriate patches and updates immediately after appropriate testing.
- Enable multi-factor authentication, where possible.
- Implement application whitelisting to prevent unknown programs from executing on servers. Additionally, this will restrict web browsing activities by attackers if they use an unapproved browser.
- The organization's application whitelisting software must ensure that only authorized, digitally signed scripts (*.ps1, *.py, macros, etc.) are allowed to run on a system.
- Disable macros in your environment. If disabling macros completely is not possible, create an Organizational Unit (OU) in Active Directory (AD) for those users who need macros enabled.
- Implement filters at the email gateway to filter out emails with known malspam indicators, such as known malicious subject lines, and block suspicious IP addresses at the firewall.
- Mark external emails with a banner denoting it is from an external source. This will assist users in detecting spoofed emails.
- To lower the chance of spoofed or modified emails from valid domains, implement Domain-based Message Authentication, Reporting and Conformance (DMARC) policy and verification, starting by implementing the Sender Policy Framework (SPF) and the Domain Keys Identified Mail (DKIM) standards.
- If you do not have a policy regarding suspicious emails, consider creating one and specifying that all suspicious emails should be reported to the security and/or IT departments.
- Provide social engineering and phishing training to employees. Urge them to not open suspicious emails, click on links contained in such emails, post sensitive information online, and to never provide usernames, passwords and/or personal information to any unsolicited request. Teach users to hover over a link with their mouse to verify the destination prior to clicking on the link.
- Create backups of systems on a regular basis and store those backups on a separate out-of-band
- Use Group Policy to set a Windows Firewall rule to restrict inbound SMB communication between client systems. If using an alternative host-based intrusion prevention system (HIPS), consider implementing custom modifications for the control of client-to-client SMB communication. At a minimum create a Group Policy Object that restricts inbound SMB connections to clients originating from clients.
- Adhere to the principle of least privilege, ensuring that users have the minimum level of access required to accomplish their duties. Limit administrative credentials to designated administrators.

- Adhere to best practices, such as those described in the CIS Controls, which are part of the CIS SecureSuite.

If a user opened a malicious email or an infection is believed to exist, we recommend running an antivirus scan on the system and take action based on the results to isolate the infected computer. If multiple machines are infected:

- Use Group Policy to set a Windows Firewall rule to restrict inbound SMB communication between client systems. If using an alternative host-based intrusion.
- Identify, shutdown, and take the infected machines off the network.
- Apply host-based isolation via Windows Firewall Group Policy Objects (GPOs), HIDS/NIDS products, a Private Virtual Local Area Network (pVLAN), or similar means to help mitigate propagation.
- Start with remediation of multi-homed systems (EX: Domain Controller, File Server) as these can communicate across VLANs and can be a potential means for spreading malware.
- Create clean Virtual Local Area Networks (VLANs) that do not have access to infected VLANs. After the systems have been reimaged or restored from a known good backup, place them on the clean VLAN.
- Do not login to infected systems with domain or shared local administrator accounts. This is the best remediation strategy since IcedID has several ways of gaining access to credentials.
- As IcedID is known for scraping credentials, it is recommended that a network-wide password reset take place. This is best done after the systems have been cleaned and moved to the new VLAN. This is recommended so new passwords are not scraped by the malware.
- As IcedID scrapes banking and other credentials, consider password resets for other applications that may have had stored credentials on the compromised machine(s).
- If needed, take the network offline to perform identification, prevent reinfections, and stop the spread of the malware
- If needed, disable Internet access at the affected site to help minimize the extent of exfiltration of credentials associated with external, third-party resources.
- Determine the infection vector (patient zero) to determine the root cause of the incident. An IcedID infection could indicate that there is an active Emotet, or other infection, on the network and vice versa. These infections are similar and have the same remediation steps. The MS-ISAC CERT can assist with forensics of the machine(s) suspected of being patient zero.

The *MS-ISAC* is the focal point for cyber threat prevention, protection, response, and recovery for the nation's state, local, tribal, and territorial (SLTT) governments. More information about this topic, as well as 24x7 cybersecurity assistance is available at 866-787-4722, *SOC@cisecurity.org*. The MS-ISAC is interested in your comments - an anonymous feedback *survey* is available.