Exchange Servers Speared in IcedID Phishing Campaign

By Elizabeth Montalbano

Published: 2022-03-29 · Archived: 2026-04-10 03:17:39 UTC

The ever-evolving malware shows off new tactics that use email thread hijacking and other obfuscation techniques to provide advanced evasion techniques.

The ever-evolving banking trojan IcedID is back again with a phishing campaign that uses previously compromised Microsoft Exchange servers to send emails that appear to come from legitimate accounts. Attackers also are using stealthy new payload-delivery tactics to spread the modular malware.

Researchers from Intezer earlier this month uncovered the campaign, which employs thread hijacking to send malicious messages from stolen Exchange accounts, thus adding an extra level of evasion to the campaign's malicious intent, wrote researchers Joakim Kennedy and Ryan Robinson in a blog post published Monday.

The actors behind IcedID – as well as other spearphishers – have previously used phishing emails that "reuse previously stolen emails to make the lure more convincing," researchers wrote. However, this time the threat has evolved in a couple of key ways that make it even more dangerous to targets, which include organizations within energy, healthcare, law and pharmaceutical sectors, researchers noted.

Not only is the threat actor now using compromised Microsoft Exchange servers to send the phishing emails from the account that they stole from, but the delivery of the malicious payload also has shifted in a way that can execute malware without the user even knowing, researchers said.

"The payload has also moved away from using office documents to the use of ISO files with a Windows LNK file and a DLL file," researchers wrote. "The use of ISO files allows the threat actor to bypass the Mark-of-the-Web controls, resulting in execution of the malware without warning to the user."

Previously the infection chain most commonly associated with IcedID phishing campaigns has been an email with an attached password-protected ZIP archive that contains a macro-enabled Office document, which executes the IcedID installer.

Breakdown of the Attack Chain

The new campaign starts with a phishing email that includes a message about an important document and includes a password-protected ZIP archive file attached, the password for which is included in the email body.

The email seems extra convincing to users because it uses what's called "thread hijacking," in which attackers use a portion of a previous thread from a legitimate email found in the inbox of the stolen account.

"By using this approach, the email appears more legitimate and is transported through the normal channels which can also include security products," researchers wrote.

The majority of the originating Exchange servers that researchers observed in the campaign appear to be unpatched and publicly exposed, "making the ProxyShell vector a good theory," they wrote. ProxyShell is a remote-code execution (RCE) bug discovered in Exchange Servers last year that has since been patched but has been throttled by attackers.

Once unzipped, the attached file includes a single "ISO" file with the same file name as the ZIP archive that was created not that long before the email was sent. That ISO file includes two files: a LNK file named "document" and a DLL file named "main," also prepared relatively recently and potentially used in previous phishing email, researchers said.

When a user double clicks the LNK file, it uses "regsvr32" to execute the DLL file, which allows for proxy execution of malicious code in main.dll for defense evasion, they wrote in the post. The DLL file is a loader for the IcedID payload.

The loader will locate the encrypted payload, which is stored in the resource section of the binary, through the technique API hashing. The resulting hash is then compared with a hardcoded hash, locating the call for FindResourceA, which is dynamically called to fetch the encrypted payload, researchers wrote.

The ultimate step in the attack chain is that the IcedID "Gziploader" payload is decoded and placed in memory and then executed. The GZiploader fingerprints the machine and sends a beacon to the command-and-control (C2) server – located at yourgroceries[.]top. – with information about the infected host, which then can be used for further nefarious activity.

Evolution of a Threat

Researchers at IBM first discovered IcedID back in 2017 as a trojan targeting banks, payment card providers, mobile services providers, payroll, web mail and e-commerce sites.

The malware has evolved over the years and already has a storied history of clever obfuscation. For example, it resurfaced during the COVID-19 campaign with new functionality that uses steganography – the practice of hiding code within images to stealthily infect victims – as well as other enhancements.

The new campaign is evidence of its further evolution and could signify that IcedID is indeed becoming, as many fear, the new Emotet – a modular threat that began as a trojan but steadily evolved into one of the most dangerous malwares ever seen.

"This attack shows how much effort attackers put in all the time to evade detection and why defense in depth is necessary," observed Saumitra Das, CTO and co-founder at security firm Blue Hexagon, in an email to Threatpost.

This time and effort, in turn, shows a level of sophistication on the part of those behind IcedID in that they have thorough knowledge of contemporary email protections and are continuously adding new tactics as security also grows and evolves, he said.

“Many email security systems use reputation of senders to block malicious email without being able to assess the email itself,” Das noted. “Here, they used compromised Exchange servers to make it through.”

The group’s use of obfuscated file formats to deliver malware, as well as the final payload’s delivery over the network, also demonstrate that the threat actors know how to evade signature and sandboxes, he added.

“These attacks often go much deeper than simply stealing data,” concurred Chris Clements, vice president of solutions architecture at security firm Cerberus Sentinel**,** in an email to Threatpost. “The cybercriminals take the time to read through the mailboxes to understand the inter-organization relationships and operating procedures.

“To protect themselves from similar attacks, it’s critical that organizations ensure that they apply security patches promptly and thoroughly in their environment,” he added. However, what is historically true for patching remains true now: that it’s “a task that’s easier said than done,” Clemens acknowledged.

“It really takes a cultural approach to cybersecurity to plan for failures in defenses like patch management,” he said.

Moving to the cloud? Discover emerging cloud-security threats along with solid advice for how to defend your assets with our FREE downloadable eBook, “Cloud Security: The Forecast for 2022.” We explore organizations’ top risks and challenges, best practices for defense, and advice for security success in such a dynamic computing environment, including handy checklists.
