Microsoft Exchange targeted for IcedID reply-chain hijacking attacks

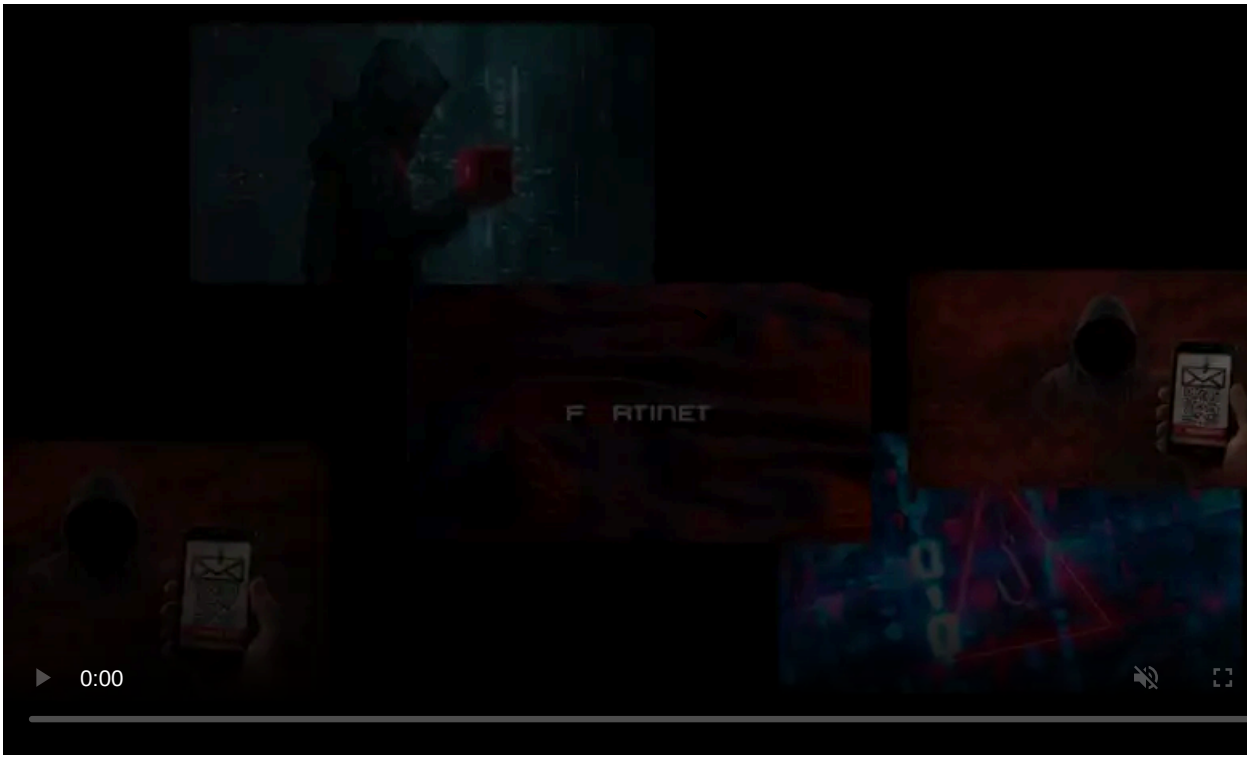
By Bill Toulas

Published: 2022-03-28 · Archived: 2026-04-06 01:35:01 UTC

The distribution of the IcedID malware has seen a spike recently due to a new campaign that hijacks existing email conversation threads and injects malicious payloads that are hard to spot.

IcedID is a modular banking trojan first spotted back in 2017, used mainly to deploy second-stage malware such as other loaders or ransomware.

Its operators are believed to be initial access brokers who compromise networks and then sell the access to other cybercriminals.


F RTINET
0:00

The ongoing IcedID campaign was discovered this month by researchers at Intezer, who have shared their findings with Bleeping Computer prior to publication.

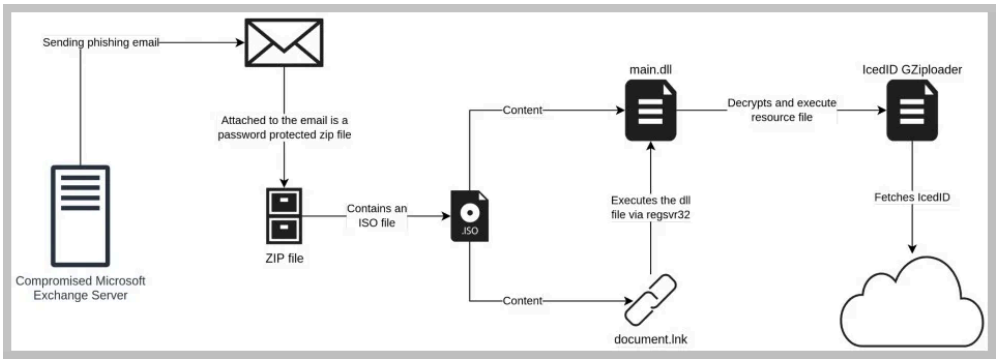
How the attack works

The primary method of the conversation hijacking attack is to assume control of a key email account participating in a discussion with the target, and then send a phishing message crafted to appear as a continuation of the thread.

As such, when the target receives a reply message with an attachment named and presented as something relevant to the previous discussion, the chances of suspecting fraud are reduced to a minimum.

Intezer explains that there are clues pointing to threat actors targeting vulnerable Microsoft Exchange servers to steal the credentials, as many of the compromised endpoints they found are public-facing and unpatched.

Additionally in this campaign, the analysts have seen malicious emails sent from internal Exchange servers, using local IP addresses within a more trustworthy domain, and hence unlikely to be marked as suspicious.



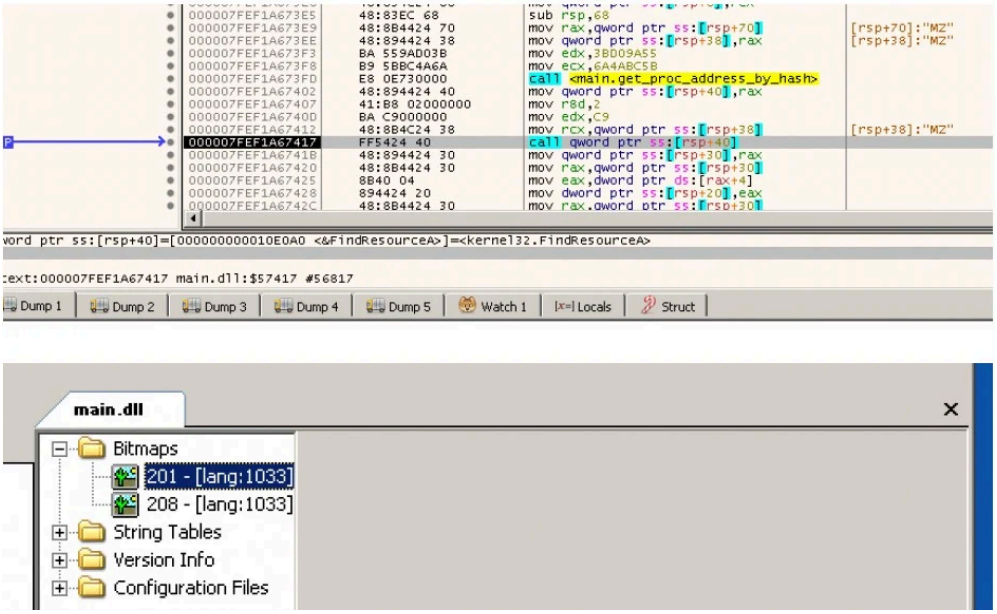
IcedID latest infection chain *(Interzer)*

The email attachment sent to targets is a ZIP archive containing an ISO file, which, in turn, encloses an LNK and a DLL file. If the victim double clicks the "document.lnk", the DLL launches to set up the IcedID loader.

The IcedID GZiploader is stored in an encrypted form in the resource section of the binary, and after decoding, it's placed in memory and executed.

The host is then fingerprinted and the basic system information is sent to the C2 (yourgroceries[.]top) via an HTTP GET request.

Finally, the C2 responds by sending a payload to the infected machine, although that step was not performed during Intezer's analysis.



Dynamically called function that fetches the payload *(Interzer)*

Ties to November 2021 campaign

While Intezer's report focuses on current and ongoing activity, it is unclear when this campaign started. It is possible that it started five months ago.

In November 2021, a Trend Micro report described a wave of attacks using ProxyShell and ProxyLogon vulnerabilities in exposed Microsoft Exchange servers to hijack internal email reply-chains and spread malware-laced documents.

The actors behind that campaign were believed to be 'TR', known to work with a plethora of malware, including Qbot, IcedID, and SquirrelWaffle.

All three malware pieces have been previously involved in email thread hijacking to deliver malicious payloads [1, 2, 3, 4].

Intezer puts threat group TA551 in the spotlight this time due to the use of regsvr32.exe for the DDL's binary proxy execution and password-protected ZIP files.

The link between those two threat groups is unclear, though, but it's not improbable that there's some overlap or even underlying connection there.

Update your Exchange servers

We're approaching the one-year mark since Microsoft published fixes for the ProxyLogon and ProxyShell vulnerabilities, so applying the latest security updates is well overdue.

Not doing so leaves your Exchange servers, company, and employees prey to phishing actors, cyber-espionage, and ransomware infections.
