


TrickBot's AnchorDNS is Now Upgraded to AnchorMail

 cyware.com/news/trickbots-anchordns-is-now-upgraded-to-anchormail-a21f5490/



Researchers have discovered a new and improved version of the AnchorDNS backdoor. The backdoor is used by the TrickBot group and employed in recent attacks deploying the Conti ransomware.

The newly upgraded backdoor

The recent discovery of AnchorMail (aka Delegatz) during ransomware attacks spotlights TrickBot's devotion to upgrading its malware.

- The newly upgraded backdoor variant uses an email-based C2 server, with which it communicates using SMTP and IMAP protocols over TLS.
- Post-execution, AnchorMail creates a scheduled task for persistence that runs every 10 minutes.
- It collects basic system info, registers with its C2, and enters a loop of checking for and executing acquired commands.

Similarities with AnchorDNS

Except for the overhauled C2 communication mechanism, AnchorMail's behavior aligns with its predecessor AnchorDNS.

- The command structure is very similar to that of AnchorDNS and both versions accept the same set of command codes that provides different options for running commands and payloads obtained from the C2.
- AnchorMail is written in C++ and targets only Windows systems. However, as AnchorDNS is ported to Linux, there is a high chance that there will be a Linux-variant of AnchorMail.

Conclusion

TrickBot is one of the most prolific threat actors and is known for upgrading its malware from time to time. Thus, experts recommend having good detection, monitoring, and response solutions, and robust internal SOC processes. Further, it is recommended to train employees to spot phishing emails.

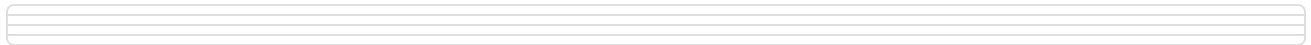
[TrickBot Anchor DNS](#)

[AnchorMail](#)

[Linux](#)

[AnchorDNS Backdoor](#)

[TrickBot](#)



TM



Publisher

Cyware
