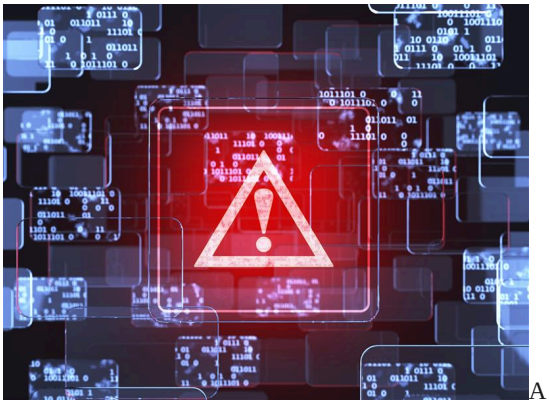
Emotet Now Spreads via Wi-Fi

Archived: 2026-04-05 22:32:22 UTC



A new strain of Emotet was found spreading through wireless internet connections, deviating from the email spam campaigns that the malware commonly utilizes as a means of propagation. According to researchers from Binary Defense, this new loader type takes advantage of the wlanAPI interface to spread from an infected device to an unsecure Wi-Fi network.

How Emotet spreads via Wi-Fi

Emotet can now hop from infected devices and servers to Wi-Fi networks. These networks can then go on to infect other devices, possibly causing a never-ending loop of infection. Based on the analysis by Binary Defense, below is the method used by this strain to infect other devices:

- First, Emotet infects a host (computers or other devices). The malware then downloads and executes the Wi-Fi spreader module.
- The Wi-Fi spreader module then enumerates all Wi-Fi devices enabled on the host. This module then comes up with the list of reachable Wi-Fi networks.
- The module then launches brute-force attacks on each of the enumerated Wi-Fi networks. To do this, it uses its two internal lists of easy-to-guess passwords. It wasn't indicated where these lists came from.
- If this attack succeeds, it then launches a second brute-force attack to guess the log-in credentials of computers and servers connected to the compromised Wi-Fi network.
- If this second attack succeeds, the cycle goes back to step 1 for another round of infection.

Records of an executable file used in the attacks had the timestamp of April 16, 2018, suggesting that Emotet's capability to propagate via Wi-Fi may have been left undetected for almost 2 years.

The Trend Micro detections for the threat are Worm.Win32.EMOTET.AA and TrojanSpy.Win32.EMOTET.TIABOFHL.

Securing Wi-Fi devices

Securing Wi-Fi devices is crucial in thwarting threats. One simple way to do this is having secure passwords. For users, it can be difficult to remember complex passwords, not to mention typing these take long, pushing many people to choose easy-to-guess passwords such as "abc123" and "qwerty". Some don't even change the default passwords at all. However, doing this for Wi-Fi devices (and for any device, for that matter) is like giving threat actors a free pass to home and even work networks.

Apart from ensuring strong passwords are used across devices and networks, enterprises can protect Wi-Fi devices further by ensuring that encryption is enabled. System administrators should also closely monitor networks to spot signs of

suspicious activities.

As most strains of Emotet still propagate through spam campaigns, employees should remain on the lookout for socially engineered emails that Emotet and other malware families can use as entry points.

Because the Emotet strain affects endpoints, servers, and networks, the necessity of employing a multilayered securityproducts is highlighted. Protect gateways, endpoints, networks, and servers while having centralized visibility and control.

For specialized protection, Trend Micro™ Network Defenseproducts, powered by XGen™ security, protects against known, unknown, and undisclosed vulnerabilities in the network. It can detect and respond to targeted attacks, whether the threat moves laterally, inbound, or outbound.

The Trend Micro Deep Discovery™ solution delivers detection, in-depth analysis, and proactive response to attacks. It has a layer for email inspectionproducts that can secure enterprises through the detection of malicious attachments and URLs. It can detect remote scripts, even those that are not downloaded on endpoints. The Trend Micro Deep Discovery Inspectorproducts solution protects customers from Emotet via this DDI rule:

- 4320 - EMOTET - HTTP (Request) – Variant 6
- 4345 - EMOTET - HTTP (Request) – Variant 7

SHA-1	Trend Micro Predictive Machine Learning Detection	Trend Micro Pattern Detection
a9c13d03e2f056d233ed7b7c97a6dc2b1ec70a50	Troj.Win32.TRX.XXPE50FFF033	Worm.Win32.EMOTET.AA
1e7c5ada1ac91990b20215397cb9ce9fd66528dd	N/A	TrojanSpy.Win32.EMOTET.TIABOFH
a97fbd3a89ba663ab9eb3488ff47665b21d17107	N/A	Worm.Win32.EMOTET.AA

HIDE

Like it? Add this infographic to your site:
1. Click on the box below. 2. Press Ctrl+A to select all. 3. Press Ctrl+C to copy. 4. Paste the code into your page (Ctrl+V).

Image will appear the same size as you see above.

We Recommend

-
-
-
-
-
  - The Industrialization of Botnets: Automation and Scale as a New Threat Infrastructurenews article
  - Complexity and Visibility Gaps in Power Automatenews article
-
  - Cracking the Isolation: Novel Docker Desktop VM Escape Techniques Under WSL2news article
  - Azure Control Plane Threat Detection With TrendAI Vision One™news article
-
  - The AI-fication of Cyberthreats: Trend Micro Security Predictions for 2026predictions
  - Ransomware Spotlight: DragonForcenews article
-
  - Stay Ahead of AI Threats: Secure LLM Applications With Trend Vision Onenews article
  - The Road to Agentic AI: Navigating Architecture, Threats, and Solutionsnews article

---