Continued Emotet Attacks Highlight 2023 Malware Dangers

In January 2021 the FBI partnered with global law enforcement agencies and private companies to take down the Emotet malware. However, just eleven months later Emotet attacks began again. This destructive malware family continues to evolve, emphasizing the need for organizations to prioritize cyber security in the new year.

The Botnet that Refuses to Die

Emotet first emerged in 2014 as a simple banking trojan. Since then, it has evolved into one of the most dangerous botnet operations in the threat landscape. Two years ago, a combined effort of law enforcement and cyber security experts from around the world celebrated its demise. But Emotet re-appeared after months, stronger than ever.

Emotet attacks use phishing campaigns to trick organizations into infecting themselves with malicious software. Typically, the phishing emails include attached Microsoft files that contain dangerous macros. When executed, the macros spread the Emotet infection throughout a network of connected devices, creating a robot network or “botnet.”

Attackers can then control the botnet remotely. For instance, they may use the infected devices to launch a distributed denial of service (DDoS) attack. Botnets can also be used to generate fake website traffic, mine cryptocurrency and steal information. And criminals may rent a botnet to other bad actors as part of a malware-as-a-service scheme.

In the latest versions of Emotet, phishing emails include Excel templates with instructions on bypassing Microsoft's Protected View. The malicious code inserted by infected files has also evolved to make it more difficult to detect.

Steps to Mitigate the Danger of Emotet Attacks

Organizations should take deliberate steps to reduce the risk of a successful attack. For instance, since Emotet typically uses macros in attached Microsoft Office files, companies should consider disabling macros unless they are signed.

Additionally, Emotet and other malware families commonly use email as a delivery device. Consequently, organizations should periodically review and update their email filters. And they should conduct regular security awareness training and phishing simulations. End users may prove the most important defense.

Continuous monitoring of network activity will also prove critical to catching infections early. With automated 24x7 monitoring, organizations can spot and address potential issues before they cause damage.

Emotet Attacks Just One Part of an Active Threat Landscape

While Emotet poses significant danger, it represents just one of the cyber security threats facing organizations in 2023. For instance, security experts warn of the following:

- Increased professionalization of cyber crime – Like Emotet, other known strands of malware indicate that malware-as-a-service and ransomware-as-a-service are becoming more prevalent. This means that even relatively unsophisticated criminals can have access to very sophisticated technology, including machine learning and AI.
- Intensified supply chain attacks – Rather than simply attacking large targets, criminals focus on SMBs and managed service providers in the supply chain. By compromising a single vendor, for instance, they can gain access to multiple customers.

- More business email compromise (BEC) attacks – While not a new threat by any means, BEC continues to provide the easiest way for attackers to gain access. Training users to recognize and avoid BEC attacks will prove more critical than ever.

- Transition from traditional ransomware to double extortion ransomware – As organizations implement better security and backup strategies, attackers have begun to change tactics. Instead of focusing on data encryption, they now more often emphasize data theft, threatening to leak or sell sensitive data.

Additional factors complicate the cyber security landscape. With tensions increasing both abroad and at home, cyber crime has become a weapon of war. For instance, wiperware attacks have increased dramatically since war erupted in the Ukraine. Also, the explosion of connected devices, combined with continued remote work, drastically expands the attack surface.

Strengthen Cyber Defenses with Expert Help

Organizations cannot afford to leave critical digital assets under-protected. At the same time, the economic downturn and the cyber security skills gap make it difficult for companies to mount an effective defense. Partnering with cyber security experts can help.

eMazzanti provides a full range of cyber security services, from risk assessments and penetration testing to continuous monitoring and email defense. Our consultants will work with your organization to tailor a security strategy to your needs and budget.