HORNETSECURITY

INFOPAPER:
EMOTET - THE MOST DANGEROUS MALWARE IN THE WORLD

Content

Introduction

++++ Massive increase of Emotet activity ++++

++++ Emotet: Total IT damage at the Berlin Court of Appeal ++++

++++ Emotet still has countries under control ++++

The name „Emotet“ repeatedly appears in the news in connection with extremely serious hacker attacks on companies, administrations, hospitals and universities. In 2019, the BSI called the malware the most dangerous malware in the world, because the malware has caused damage amounting in millions. **What makes Emotet so threatening, and how you can protect yourself against it? Hornetsecurity will give you their expert explanation below.**

HORNETSECURITY

What is Emotet?

Emotet **first appeared as a banking Trojan in 2014.** The attack was aimed at intercepting online access data of German and Austrian bank customers. Meanwhile, Emotet is able to reload and execute a variety of other modules with other malicious functions. Emotet strikes **primarily via spam emails** and effects private users as well as companies, hospitals, government institutions and critical infrastructures.

It adapts and automates methods of highly professional Advanced Persistent Threat attacks. **Cyber criminals proceed very purposefully** and with great effort in order to remain capable of acting in the infected system for as long as possible.

One aspect makes Emotet particularly dangerous: Since the end of 2018, the malware has been able to read contact relationships and email content from the mailboxes of infected systems using so-called Outlook harvesting in order to launch further attacks on this basis. The spread is thus extremely rapid. Other recipients will then receive equally authentic-looking emails from people with whom they were recently in contact. Malicious file attachments or URLs contained in the message are opened carelessly.

In addition to this spam module, Emotet can also load a worm module, which allows it to spread independently in the company network. This allows it to **spread to other computers without requiring users to click and activate an attachment.** In this context, Emotet also undertakes brute force attacks with the aim of hacking passwords. This can have serious consequences. Once the computer is infected, Emotet downloads additional malware via C&C servers, depending on the target. There is a risk of data theft, loss of control over systems, failure of the entire IT infrastructure and restrictions on critical business processes. In extreme cases, an entire company's networks must be rebuilt after infection. **The damages often amount to millions in losses.**

Master of disguise: Why is Emotet so difficult to fight?

Emotet is not easy to identify and intercept, because it deceives traditional antivirus products: **as a polymorphic virus.** The code changes slightly with each new retrieval to avoid detection by signature-based virus scanners. In addition, the virus detects when it is running in a virtual machine. As soon as a sandbox environment is registered, the **program falls into a kind-of stand-by mode and does not perform** any malicious actions during that moment.

A dangerous alliance: Emotet, TrickBot and the ransomware Ryuk

As mentioned earlier, Emotet loads additional malware after a successful infection. A particularly dangerous alliance is created when used in **conjunction with TrickBot and Ryuk:** disguised in a Word document, Emotet penetrates and spies on a corporate network when the file is executed. As a „door opener", it reloads the banking Trojan TrickBot, which among other things copies account access data. It passes this information on to the ransomware Ryuk, which is the last to be loaded. **Ryuk now encrypts all files in the system that TrickBot and Emotet have previously classified as sensitive** or important.

A dangerous alliance: Emotet, TrickBot and the ransomware Ryuk

The sneaky thing about Ryuk is that in addition to encrypting important data, it **also deletes all existing backup copies of that data at the same time,** making recovery much more difficult. According to the experts at Hornetsecurity, a new trend in the development of blackmailing software is emerging with this deletion function. In addition, the amount requested is based on the value that TrickBot could provide as the company's current financial availability. **The attack is extremely targeted and mainly affects companies** that are able to pay large sums of money in order to regain access to their data. Ryuk first appeared in August 2018, and has since generated several million dollars. It is still unclear which hacker group is behind it.

How to protect yourself?

To effectively protect yourself from Emotet, you need to focus on the main entrance point of the malware: email communication. **Hornetsecurity Advanced Threat Protection easily detects Emotet and Ryuk** in emails and quarantines both malware programs. The first instance of analysis identifies the Emotet Trojan. The subsequent Trojans Ryuk and TrickBot can be unmasked using the dynamic behavior analysis in the ATP sandbox. **Emails containing the perfidious malware are not delivered to the recipients.**

Basic security-relevant behavior

Since Emotet often **hides in Microsoft Office files** and needs macros to install malware, it makes sense not to allow them. They are also not needed in private and most business areas. However, if you cannot do without them, it is possible to allow only signed macros.

Deployed **security updates must be installed immediately** for operating systems, anti-virus programs, web browsers, email clients and office programs.

Regular data backups are recommended.

Vigilance is paramount: Even with supposedly known senders, one should be careful with file attachments of emails, especially with Office documents and contained links. In case of doubt, it is advisable to make direct contact with the sender of a suspicious email and check the credibility of the content.

Accesses to the **company's own network should be continuously monitored.** In this way it can be determined in a timely manner whether an Emotet-infection has occurred.

Checklist: What must happen in the case of an Emotet infection?

If the security measures taken have failed and an infection occurs, the following steps must be taken immediately:

To prevent further spread, the **company IT and the environment must be informed** about the infection as quickly as possible. Mail contacts are particularly at risk of becoming infected as well.

Emotet C&C IPs must be blocked immediately. As a result, the malware will not receive any new commands and cannot download any more modules.

The malware makes profound security changes to the infected system, and is not easily removed from computers. It is therefore essential to **reinstall the affected IT components.**

All previously used **passwords should be exchanged,** as attackers are likely to have tapped them and thus gain access to further sensitive areas.

It is necessary to **question existing security concepts and identify entry points** in order to better protect oneself from new attacks.

- ☑ **Inform company IT and the environment**
- ☑ **Block Emotet C&C IPs**
- ☑ **Reinstall affected IT components**
- ☑ **Change previously used passwords**
- ☑ **Question security concepts**
- ☑ **Identify entry points**