CASE STUDY

Threat Dissection: Anatomy of an Emotet Outbreak

Threat Type:
Banking Trojan

Functionality:
Downloader or dropper of other banking Trojans

First Discovered:
2014

Infection Mechanism:
malspam (Javascript, Word Docs) or EternalBlue vulnerability that downloads and executes payload

Traditional Detection Challenges:
Emotet has several methods for maintaining persistence, including auto-start registry keys and services, and it uses modular Dynamic Link Libraries (DLLs) to continuously evolve. Due to Emotet's polymorphic and modular nature, it can evade typical signature-based detection.

Containment and Remediation Challenges:
Due to Emotet's ability to move laterally, administrator's are required to follow a strict policy of isolating infected endpoints from the network, patching, disabling Administrative Shares, and ultimately removing the Trojan before reconnecting to the network. If these steps are not followed, Emotet will re-infect cleaned machines with infected peers. In addition, Emotet's capabilities have evolved to become VM-aware generating false indicators if run in a virtual environment in addition to spam avoidance and automated security program removal.

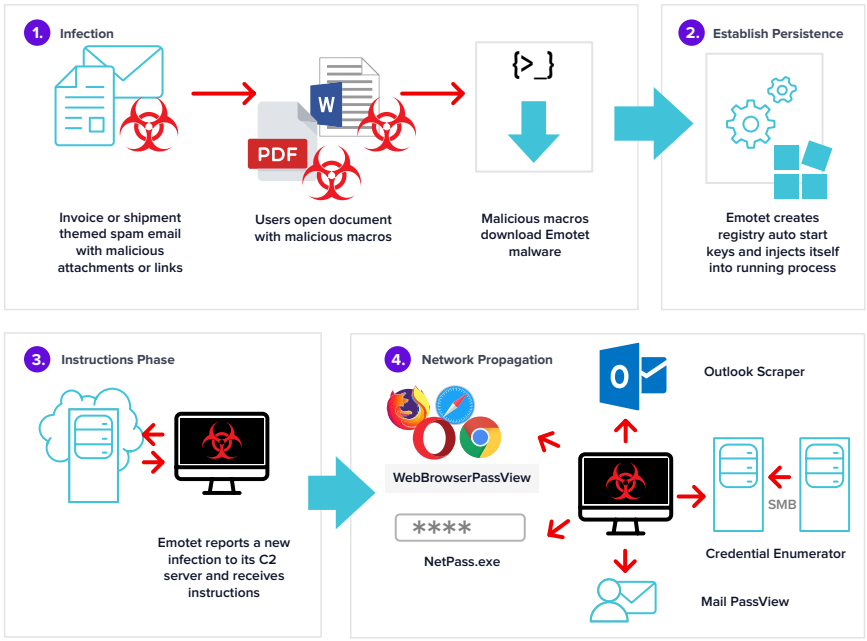
Potential Effects:

- Temporary or permanent loss of sensitive or proprietary information
- Disruption to regular operations
- Financial losses incurred to restore systems and files
- Potential harm to an organization's reputation
- Loads other malware

Background: How Does Emotet work?

Emotet is a modular Trojan, allowing its creators/operators to easily change out components and functionality. By employing frequent updates, Emotet stays one step ahead of signature-based anti-virus products. Emotet emails are designed to mimic legitimate emails coming from known users to trick recipients into clicking on the malicious files that emulate shipping notifications or "past due" invoices. Once downloaded, Emotet establishes persistence and attempts to propagate the local networks through incorporated spreader modules.

Process



Due to the characteristics and attack lifecycle of this type of malware it is increasingly difficult to rely on traditional measures and detection methods based on endpoint protection platforms. Traditional AV solutions that rely on signature-based detection with non-customizable heuristics are very limited in their ability to detect and prevent emerging threats. Detection of emerging threats rely on unfiltered data that can be processed for specific behavioral characteristics. MITRE ATT&CK is a great framework to leverage for creating detectors that are not specific to a malware variant. The tactics and techniques can be associated with specific samples but at a higher level can be used to share commonalities and detection criteria between strains. The key to preventing Emotet type malware families requires a defense in depth strategy focused on controlling code execution that can occur on your endpoints.

Emotet Prevention Using eSentire MDR for Endpoint

An endpoint protection platforms main job is to stop malicious code execution. Initial droppers are the main way that threat actors get initial code execution within an environment. Controlled execution within an environment is a key way to limit the susceptibility of malicious content being introduced. Initial droppers are most often delivered in the following file formats:

- HTML / HTA
- EXE / DLL / MSI
- VBA / VBS / VBE
- JS
- Macros (DOCM, XLSM, POTX)
- PDF
- ZIP / 7ZIP / RAR
- PS
- SCT

Understanding how code execution is utilized for malicious staging allows the eSentire team to create a prevention strategy. The power of customizable behavioral rules allows for granular control of whitelists for business operations while restricting unapproved execution of potential threats. Script interpreters have been abused heavily in the past few years due to the ease of execution and lack of prevention from traditional signature-based tools. Ensuring an organization controls script interpreter execution is key to having a mature endpoint security strategy.

Emotet Detection Using eSentire MDR for Endpoint

Where prevention fails eSentire MDR for Endpoint gets full visibility into everything that is happening on the endpoint. The key advantage the eSentire SOC benefits from is raw unfiltered data. The ability to consume a detailed record of every file event, process command-line event, process event, process use of network, etc is extremely valuable to identify emerging threats. The eSentire MDR for Endpoint service extends the built-in capability of endpoint detection and response (EDR) for detection via customizable behavioral detectors and threat feeds. Behavioral rules that monitor for suspicious activity mapped to MITRE ATT&CK allow for identification of malicious content within a customer's environment. In addition to the behavioral detectors, consuming all this raw data into a data analysis pipeline allows eSentire to create global detectors at scale. Crunching very large data sets and contextual events is the perfect fit for a machine learning model. There are limitations on what an analyst can do within the confines of an EDR query language and dashboard. The eSentire MDR for Endpoint service has the capability of detecting malicious activity that EDR platforms cannot do out of box due to our threat analytics pipeline.

Emotet Containment Using eSentire MDR for Endpoint

The eSentire SOC primarily detects and stops Emotet attacks using Managed Detection and Response (MDR) capabilities. In one incident, an Emotet infection was able to rapidly spread laterally across a client's network, but eSentire's Security Analysts were able to discover and stop the attack. The client had eSentire's MDR for Endpoint service, as well as an antivirus (AV) solution in place. However, due to Emotet's rapid evolution and polymorphing capabilities, the AV solution did not detect or prevent Emotet's lateral movements.

Ground Zero

The incident involved a network in which several hosts were out of scope for the client's endpoint monitoring. Over a 12-hour period, the out-of-scope machines kept infecting machines in scope, allowing some insight into how Emotet spreads internally.

At ground zero, the outbreak was observed spreading to eight hosts from a single source (Figure 1, orange). A few hours later, another source was observed infecting four more machines with a new variant of Emotet (Figure 1, blue) followed by the original source re-infecting the same four with the new variant. Several hours later, a third variant was observed spreading to 24 hosts (Figure 1, red).

Figure 1: Emotet outbreak infecting clusters of hosts. Three different Emotet variants were spotted (denoted by distinct colors) across the twelve hour span.

After collecting all discoverable telemetry, it was discovered that more machines were infected. Twelve in the first cluster, seven in the second cluster, and 25 in the final cluster. In total, nearly forty infected machines were observed within, or peripheral to, endpoint scope by the end of the 12-hour period.

Spreading Mechanism

During the investigation, eSentire discovered that lateral outbreak occurred five times in three distinct clusters (Figure 2). For a given cluster, the spread across hosts was rapid. For example, in the first cluster at 12:30 AM, ten machines were infected within 12 seconds with the first two machines being infected within the first second (Figure 2, inset).

Emotet has previously been reported as spreading through Server Message Block (SMB), using the EternalBlue exploit and administrative shares [1]. In this incident, the spread was facilitated through administrative shares, using a privileged account or legitimate credentials. It is not known how the credentials might have been obtained since the Emotet outbreak originated from machines outside of the eSentire MDR for Endpoint monitoring scope. Common credential harvesting methods include local extraction, bruteforce, phishing, and the acquisition of credentials from previous breaches and dumps.

Administrative shares are created automatically by default on most Windows machines, including servers. Once an attacker has escalated privilege to an administrative account, they will typically have access to these default administrative shares. Disabling the shares requires modification of the AutoShareWks parameter in the windows registry keys [2].

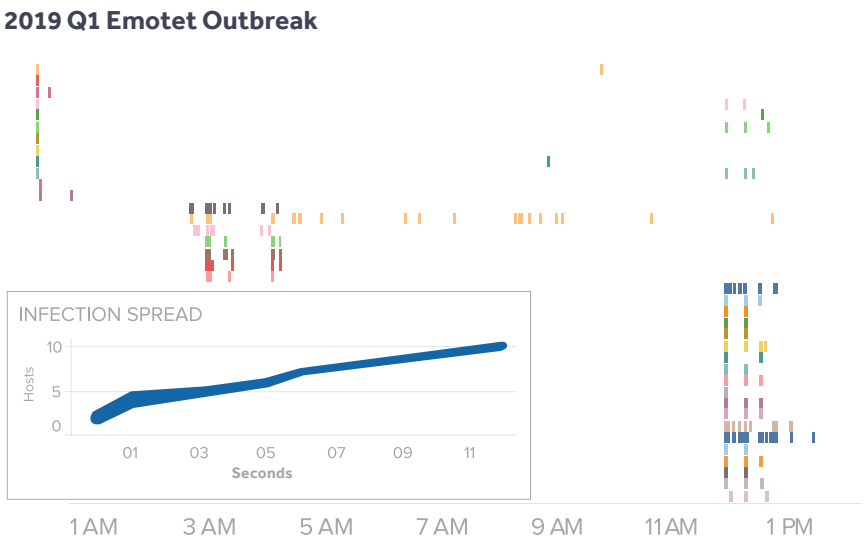


Figure 2: A time course of outbreaks across hosts on the victim's network. Inset: spread time in the first cluster of infections.

Continuing The Fight Against Emotet

eSentire Security Analysts were able to stop the attack by isolating the infected machines as they were detected using eSentire MDR for Endpoint. As Emotet continues to evolve, so do eSentire's detection capabilities. Synthesizing and analyzing data from across a wide range of sources throughout the network and systems makes it very difficult for adversaries to hide. Combining machine learning with human expertise and applying it to eSentire's MDR capabilities, our SOC analysts are empowered to disrupt and contain threats like Emotet every day.

Additional Reading

The Evolution of Emotet: From Banking Trojan to Threat Distributor - Symantec Blog
https://www.symantec.com/blogs/threat-intelligence/evolution-emotet-trojan-distributor

Emotet: The Tricky Trojan that 'Git Clones' - Check Point Research
https://research.checkpoint.com/emotet-tricky-trojan-git-clones/

Malware Team Up: Malspam Pushing Emotet + Trickbot – Unit42, PaloAlto Networks
https://unit42.paloaltonetworks.com/unit42-malware-team-malspam-pushing-emotet-trickbot/

A One-two Punch of Emotet, TrickBot, & Ryuk Stealing and Ransoming Data – Cybereason
https://www.cybereason.com/blog/one-two-punch-emotet-trickbot-and-ryuk-steal-then-ransom-data

The Unholy Alliance of Emotet, TrickBot and the Ryuk Ransomware – Decipher
https://duo.com/decipher/the-unholy-alliance-of-emotet-trickbot-and-the-ryuk-ransomware

References

[1] *https://www.us-cert.gov/ncas/alerts/TA18-201A*

[2] *https://ibm.co/2Xw7pcu*

Reach out to learn more.

Get Started

If you're experiencing a security incident or breach contact us  **1-866-579-2200**

eSentire