Microsoft: Emotet Took Down a Network by Overheating All Computers

bleepingcomputer.com/news/security/microsoft-emotet-took-down-a-network-by-overheating-all-computers/

Sergiu Gatlan

By
Sergiu Gatlan

- April 3, 2020
- 03:25 PM
- 1

Microsoft says that an Emotet infection was able to take down an organization's entire network by maxing out CPUs on Windows devices and bringing its Internet connection down to a crawl after one employee was tricked to open a phishing email attachment.

"After a phishing email delivered Emotet, a polymorphic virus that propagates via network shares and legacy protocols, the virus shut down the organization's core services," DART said.

"The virus avoided detection by antivirus solutions through regular updates from an attacker-controlled command-and-control (C2) infrastructure, and spread through the company's systems, causing network outages and shutting down essential services for nearly a week."

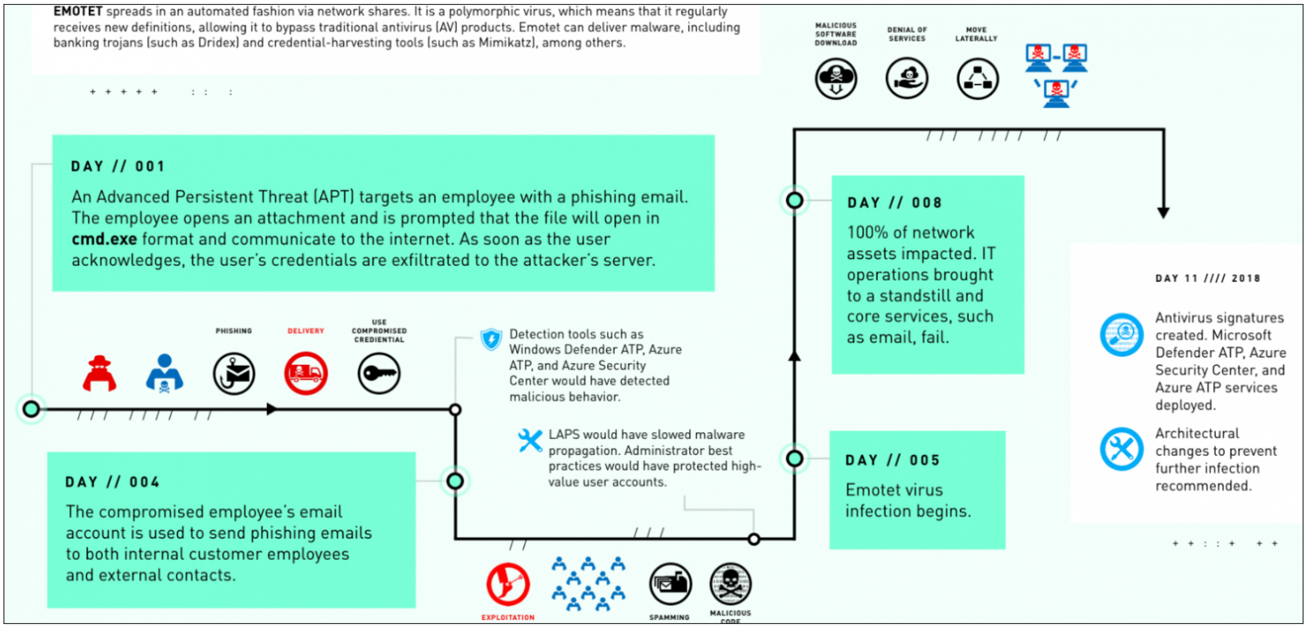
All systems down within a week

The Emotet payload was delivered and executed on the systems of Fabrikam — a fake name Microsoft gave the victim in their case study — five days after the employee's user credentials were exfiltrated to the attacker's command and control (C&C) server.

Before this, the threat actors used the stolen credentials to deliver phishing emails to other Fabrikam employees, as well as to their external contacts, with more and more systems getting infected and downloading additional malware payloads.

The malware further spread through the network without raising any red flags by stealing admin account credentials authenticating itself on new systems, later used as stepping stones to compromise other devices.

Within 8 days since that first booby-trapped attachment was opened, Fabrikam's entire network was brought to its knees despite the IT department's efforts, with PCs overheating, freezing, and rebooting because of blue screens, and Internet connections slowing down to a crawl because of Emotet devouring all the bandwidth.



EMOTET spreads in an automated fashion via network shares. It is a polymorphic virus, which means that it regularly receives new definitions, allowing it to bypass traditional antivirus (AV) products. Emotet can deliver malware, including banking trojans (such as Dridex) and credential-harvesting tools (such as Mimikatz), among others.

DAY // 001

An Advanced Persistent Threat (APT) targets an employee with a phishing email. The employee opens an attachment and is prompted that the file will open in **cmd.exe** format and communicate to the internet. As soon as the user acknowledges, the user's credentials are exfiltrated to the attacker's server.

Detection tools such as Windows Defender ATP, Azure ATP, and Azure Security Center would have detected malicious behavior.

LAPS would have slowed malware propagation. Administrator best practices would have protected high-value user accounts.

DAY // 004

The compromised employee's email account is used to send phishing emails to both internal customer employees and external contacts.

DAY // 005

Emotet virus infection begins.

DAY // 008

100% of network assets impacted. IT operations brought to a standstill and core services, such as email, fail.

DAY 11 //// 2018

Antivirus signatures created. Microsoft Defender ATP, Azure Security Center, and Azure ATP services deployed.

Architectural changes to prevent further infection recommended.

Emotet attack flow (*Microsoft DART*)

"When the last of their machines overheated, Fabrikam knew the problem had officially spun out of control. 'We want to stop this hemorrhaging,' an official would later say," DART's case study report reads.

"He'd been told the organization had an extensive system to prevent cyberattacks, but this new virus evaded all their firewalls and antivirus software. Now, as they watched their computers blue-screen one by one, they didn't have any idea what to do next."

Based on what the official said following the incident, although not officially confirmed, the attack described by Microsoft's Detection and Response Team (DART) matches a malware attack that impacted the city of Allentown, Pennsylvania in February 2018, as ZDNet first noticed.

At the time, Mayor Ed Pawlowski said that the city had to pay nearly $1 million to Microsoft to clean out their systems, with an initial $185,000 emergency-response fee to contain the malware and up to $900,000 in additional recovery costs, as first reported by The Morning

Call.

Emotet infection aftermath and containment procedures

"Officials announced that the virus threatened all of Fabrikam’s systems, even its 185-surveillance camera network," DART's report says.

"Its finance department couldn’t complete any external banking transactions, and partner organizations couldn’t access any databases controlled by Fabrikam. It was chaos.

"They couldn’t tell whether an external cyberattack from a hacker caused the shutdown or if they were dealing with an internal virus. It would have helped if they could have even accessed their network accounts.

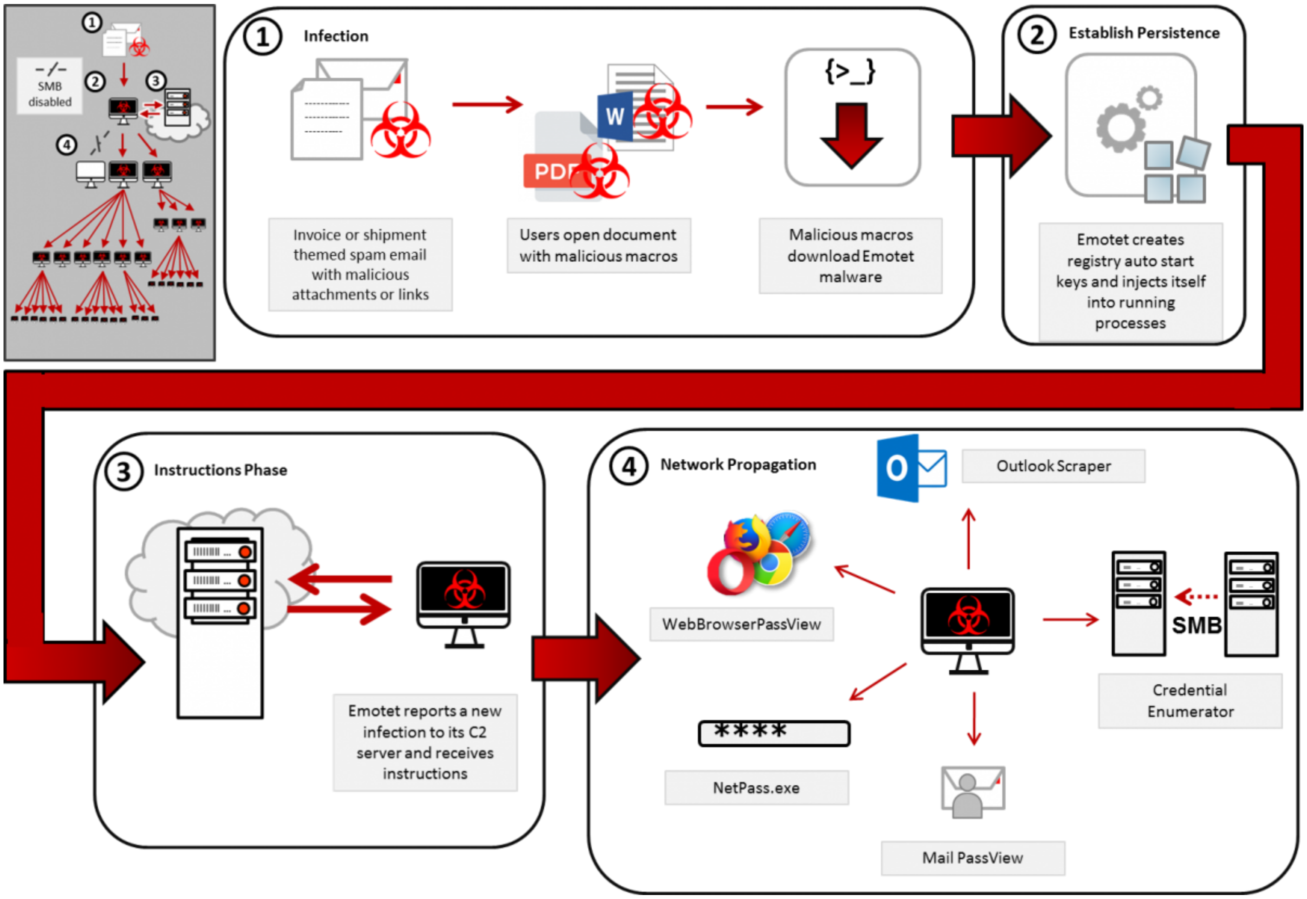
"Emotet consumed the network’s bandwidth until using it for anything became practically impossible. Even emails couldn’t wriggle through."

Microsoft's DART — a remote team and one that would deal with the attack on site — was called in eight days after the first device on Fabrikam's network was compromised.

DART contained the Emotet infection using asset controls and buffer zones designed to isolate assets with admin privileges.

They eventually were able to completely eradicate the Emotet infection after uploading new antivirus signatures and deploying Microsoft Defender ATP and Azure ATP trials to detect and remove the malware.

Microsoft recommends using email filtering tools to automatically detect and stop phishing emails that spread the Emotet infection, as well as the adoption of multi-factor authentication (MFA) to stop the attackers from taking advantage of stolen credentials.


1
SMB disabled
2
3
4
1 Infection
Invoice or shipment themed spam email with malicious attachments or links
W
PDF
Users open document with malicious macros
{>_}
Malicious macros download Emotet malware
2 Establish Persistence
Emotet creates registry auto start keys and injects itself into running processes
3 Instructions Phase
Emotet reports a new infection to its C2 server and receives instructions
4 Network Propagation
O
Outlook Scraper
WebBrowserPassView
SMB
Credential Enumerator
****
NetPass.exe
Mail PassView

Emotet infection chain (*CISA*)

Emotet infections can lead to severe outcomes

Emotet, originally spotted as a banking Trojan in 2014, has evolved into a malware loader used by threat actors to install other malware families including but not limited to the Trickbot banking Trojan (a known vector used in the delivery of Ryuk ransomware payloads).

Emotet was recently upgraded with a Wi-Fi worm module designed to help it spread to new victims via nearby insecure wireless networks.

Recently, in January 2020, the Cybersecurity and Infrastructure Security Agency (CISA) warned government and private organizations, as well as home users, of increasing activity around targeted Emotet attacks.

In November 2019, the Australian Signals Directorate's Australian Cyber Security Centre (ACSC) also warned of the dangers behind Emotet attacks, saying at the time that the malware "provides an attacker with a foothold in a network from which additional attacks can be performed, often leading to further compromise through the deployment of ransomware."

Emotet ranked first in a 'Top 10 most prevalent threats' ranking published by interactive malware analysis platform Any.Run at the end of December 2019, with triple the number of sample uploads submitted for analysis when compared to the next malware in the top, the Agent Tesla info-stealer.

CISA provides general best practices to limit the effect of Emotet attacks and to contain network infections within an Emotet Malware alert published two years ago and updated earlier this year.

Related Articles:

Microsoft: Sysrv botnet targets Windows, Linux servers with new exploits

Historic Hotel Stay, Complementary Emotet Exposure included

EmoCheck now detects new 64-bit versions of Emotet malware

Emotet botnet switches to 64-bit modules, increases activity

Emotet malware infects users again after fixing broken installer

- Emotet
- Malware
- Microsoft

Sergiu Gatlan

Sergiu Gatlan is a reporter who covered cybersecurity, technology, Apple, Google, and a few other topics at Softpedia for more than a decade. Email or Twitter DMs for tips.

- Previous Article
- Next Article

Comments

NoneRain - 2 years ago

Emotet never ceases to evolve D:

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: