Emotet Attack took down an Organization's Network by overheating all the Computers and bringing its Internet Access Down.

Microsoft shared details of the Emotet attack suffered by an organization named Fabrikam in the Microsoft's Detection and Response Team (DART) Case Report 002, where Fabrikam is a fake name the IT giant gave the victim.

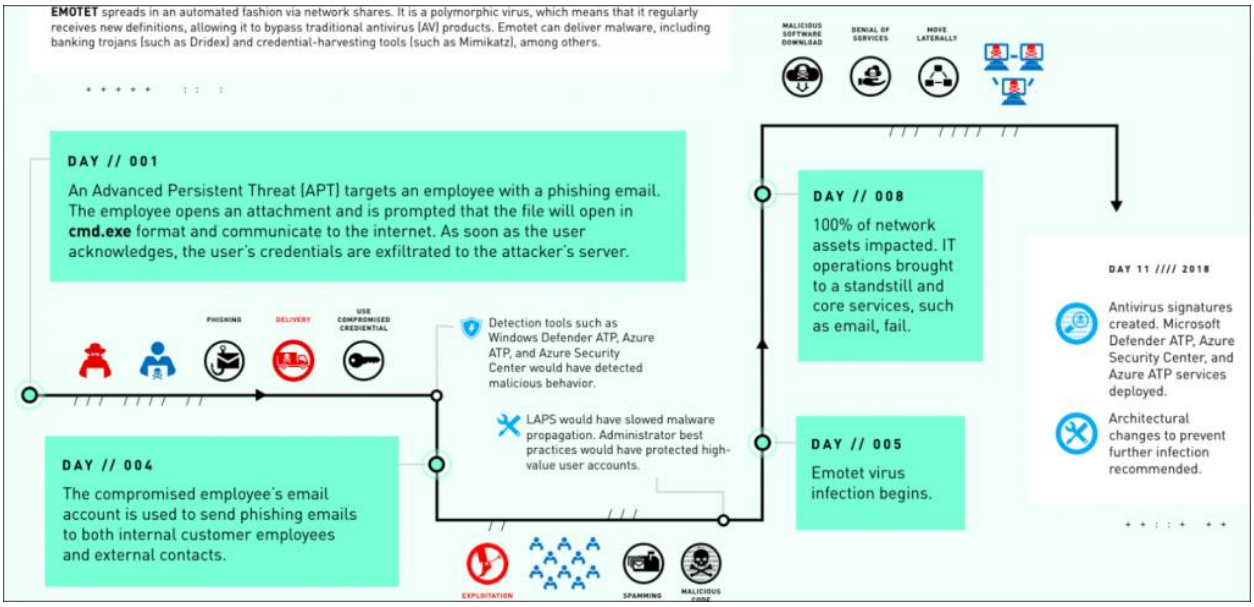
The attack described by Microsoft begun with a phishing message that was opened by an internal employee, the malware infected its systems and made lateral movements infected other systems in the same network.

The virus halted core services by saturating the CPU usage on Windows devices.

"We are glad to share the DART Case Report 002: Full Operational Shutdown. In the report 002, we cover an actual incident response engagement where a polymorphic malware spread through the entire network of an organization," reads the Microsoft DART announcement. (Currently is not available but you can view the copy cache). "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. 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."

Attackers stole the employee's user credentials and five days later used them to deliver and execute the Emotet payload. Threat actors also used these credentials to send phishing emails to other Fabrikam employees and to their external contacts in the attempt to infect the largest number of systems as possible.

Microsoft's DART was involved in the incident response activities eight days after the first device on Fabrikam's network compromised.



The malware made lateral movements by stealing admin account credentials, and in just eight days after the initial infection, the Fabrikam's entire network was shut down.

The internal staff was not able to restore the internal systems that were overheating, experts observed the machines freezing and rebooting, while Internet connections were slightly slowing down.

"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," states DART case study report.

"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."

Media speculate that the attack described in the DART report is the one that hit the city of Allentown, Pennsylvania in February 2018.

At the time, the city paid nearly $1 million to Microsoft to clean out their systems, with an initial $185,000 emergency-response fee stop malware from spreading and up to $900,000 in recovery operations.

The incident also affected the surveillance camera network of the company along with the finance department.

“Emotet consumed the network’s bandwidth until using it for anything became practically impossible. Even emails couldn’t wriggle through,” continues the report.

Microsoft experts successfully contained the Emotet infection and eradicated the malware from the infected network, and then it deployed Microsoft Defender ATP and Azure ATP trials to detect and remove the malicious code.

The Emotet banking trojan has been active at least since 2014, the botnet is operated by a threat actor tracked as TA542.

In 2019, security experts have not detected any activity associated with Emotet since early April, when researchers at Trend Micro have uncovered a malware campaign distributing a new Emotet Trojan variant that compromises devices and uses them as Proxy C2 servers.

Emotet re-appeared on the threat landscape in August 2019, with an active spam distribution campaign. At the time, Malwarebytes observed the Trojan started pumping out spam, spam messages initially targeted users in Germany, Poland and Italy, and the US. The campaign continues targeting users in Austria, Switzerland, Spain, the United Kingdom, and the United States.

https://securityaffairs.co/wordpress/101031/hacking/emotet-attack-microsoft-customer.html?web_view=true