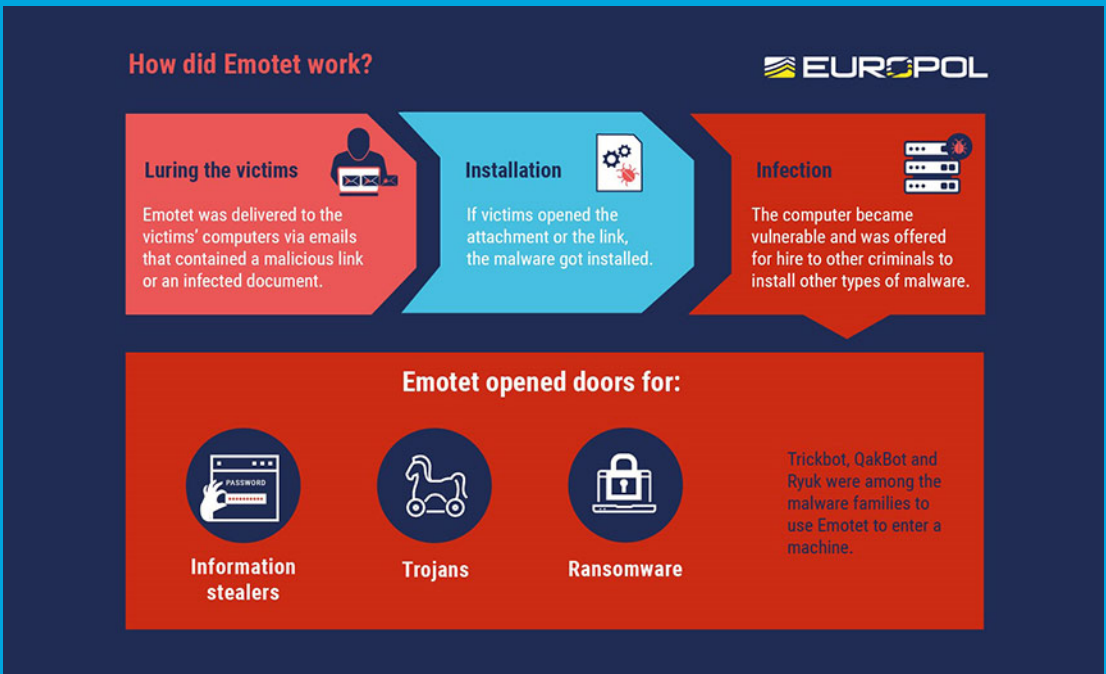
kindred

Security Newsletter

1 February 2021

Subscribe to this newsletter

European Authorities Disrupt Emotet — World's Most Dangerous Malware. Emotet will uninstall itself on March 25th



Law enforcement agencies from as many as eight countries dismantled the infrastructure of Emotet, a notorious email-based Windows malware behind several botnet-driven spam campaigns and ransomware attacks over the past decade.

Emotet establishes a backdoor onto Windows computer systems via automated phishing emails that distribute Word documents compromised with malware. Subjects of emails and documents in Emotet campaigns are regularly altered to provide the best chance of luring victims into opening emails and installing malware regular themes include invoices, shipping notices and information about COVID-19. Those behind the Emotet lease their army of infected

machines out to other cyber criminals as a gateway for additional malware attacks, including remote access tools (RATs) and ransomware.

"The infrastructure that was used by Emotet involved several hundreds of servers located across the world, all of these having different functionalities in order to manage the computers of the infected victims, to spread to new ones, to serve other criminal groups and to ultimately make the network more resilient against takedown attempts," Europol says.

The disruption effort will pose serious short-term problems for the Emotet gang, but the group is likely to eventually reemerge, says Jason Meurer, who's a senior research engineer at Cofense. Indeed, other hacking groups operating malicious services have proven to be all too resilient despite law enforcement efforts to shutter their operations. In October 2020, for example, Microsoft and federal agencies disrupted the Trickbot operation. Within several weeks, however, the gang behind Trickbot was able to start rebuilding its network. Even if that happens, however, experts say the operation has been dealt a serious blow. "The effort is a shining example of what needs to be done in order to have any real impact on these organized cybercrime groups," Intel 471 says. "The difference between disruption and takedown boils down to criminals being put in handcuffs. It's the pinnacle of a takedown operation and the only way to have a long-term impact on the health and safety of the internet."

Read More on TheHackerNews

Even More on BankInfoSecurity

Authorities plan to mass-uninstall Emotet from infected hosts on March 25, 2021

Bad actors launched an unprecedented wave of DDoS attacks in 2020

For many enterprises, 2020 was a tough year for cyberattacks, with dozens suffering from devastating DDoS attacks due to the newfound reliance on digital tools, according to a new report from cybersecurity firm Akamai. In its report, the company found that it had more customers attacked in November 2020 than any prior month going back to 2016. The company had more customers attacked over 50Gbps in August 2020 than any month before, another record that dates back to 2016.

"In fact, across all attacks, 7 of the 11 industries we track saw more attacks in 2020 than any year to date. Think about that. This was led by huge jumps in Business Services (960%), Education (180%), Financial Services (190%), Retail & Consumer Goods (445%), and Software & Tech (196%)," the report said. The report cites a number of record-breaking attacks, including a 1.44 Tbps attack against a major bank in Europe as well as an 809 Mpps attack on an internet hosting provider. According to the study's findings, some of the largest DDoS extortion campaigns took place in 2020 and the numbers only continued to grow throughout the year.

When researchers mapped it out, the timing of the increases in attacks coincides perfectly with the start of the COVID-19 pandemic, particularly in Europe and the US. All signs point to continued DDoS attack growth. Not one of the indicators we track is flat or trending down," Emmons said.

Read More on TechRepublic

Report from Akamai

More #News

More #News

- New Attack Could Let Remote Hackers Target Devices On Internal Networks
- Citrix's $2.3 million settlement offer for employees impacted by data breach approved
- Authorities Seize Dark-Web Site Linked to the Netwalker Ransomware
- New cybercrime tool can build phishing pages in real-time
- Top Cyber Attacks of 2020
- Privacy budgets soared in 2020, doubling to an average of $2.4 million
- Pen Testing By Numbers: Tracking Pen Testing Trends and Challenges
- Another ransomware now uses DDoS attacks to force victims to pay
- Expert: Manpower is a huge cybersecurity issue in 2021
- Google researcher discovers new iOS security system
- 5 identity priorities for 2021—strengthening security for the hybrid work era and beyond
- Reported US Data Breaches Declined by 19% in 2020 - Switching focus to Ransomware

#Breach Log

- Australian Financial Regulator Hit by Data Breach
- cut2
- Stack Overflow Shares Technical Details on 2019 Hack
- Mimecast links security breach to SolarWinds hackers
- Dutch COVID-19 patient data sold on the criminal underground
- Illinois Court Exposes More Than 323,000 Sensitive Records
- Hacker leaks data of 2.28 million dating site users
- SonicWall says it was hacked using zero-days in its own products
- Bonobos clothing store suffers a data breach, hacker leaks 70GB database

#Patch Time!

- Apple critical patches fix in-the-wild iPhone exploits – update now!
- Fully-Functional Exploit Released Online for SAP Solution Manager Flaw
- Researchers: Beware of 10-Year-Old Linux Vulnerability

#Tech and #Tools

- A Red Team Guide for a Hardware Penetration Test
- Anticipate cyber-threats with PatrOwl, manage them with TheHive
- How to detect sudo's CVE-2021-3156 using Falco
- Azure Key Vault Certificates with Let's Encrypt as the Issuer CA
- No, java is not a secure programming language
- Twenty-three SUNBURST Targets Identified
- Cyber Threats and NATO 2030: Horizon Scanning and Analysis
- Security Overview of AWS Lambda
- Red Team Notes 2.0
- Prevent Legitimate Windows Executables To Be Used To Gain Initial Foothold In Your

Infrastructure

This content was created by Kindred Group Security. Please share if you enjoyed!

Kindred Group in brief

Kindred is one of the largest online gambling companies in the world with a diverse team of 1,600 people serving over 26 million customers across Europe, Australia and the US. We offer pre-game and live Sports betting, Poker, Casino and Games through 11 brands across our markets. We are committed to offer our customers the best deal and user experience possible, while ensuring a safe and fair gambling environment. Kindred is a pioneer in the online gambling industry and is an innovation driven company that builds on trust.

You can access the previous newsletters at https://news.infosecgur.us