Security Newsletter

19 October 2019

Subscribe to this newsletter

German authorities raid FinFisher office

German authorities have raided the offices of FinFisher, a German software company that makes surveillance tools, accused in the past of providing software to oppressive regimes.

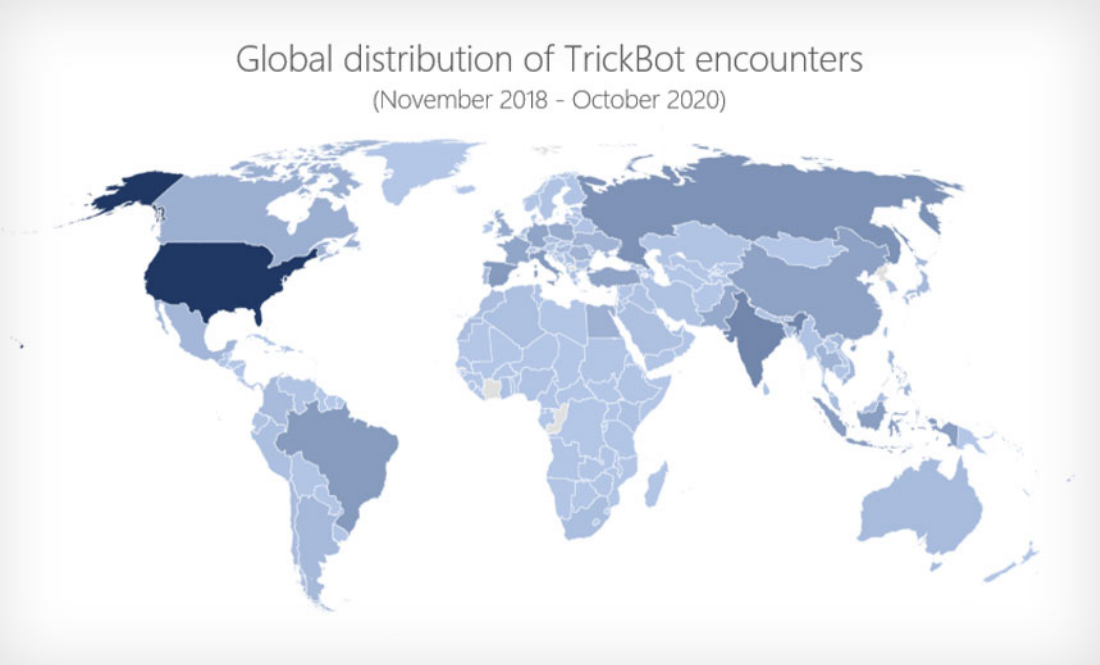
The signatories argued that FinFisher's malware had been installed on the devices of activists, political dissidents, and regular citizens in countries with oppressive regimes, countries to which FinFisher would have been prohibited from selling its software.

The company's products are usually detected as malware by most antivirus products, including major products like Windows Defender. FinFisher surveillance tools are available for Windows, iOS, and Android. In the past, cyber-security firms have spotted FinFisher infections in more than 20 countries. FinFisher markets its tools as meant for law enforcement investigations and intelligence agencies. Known customers include the German federal police and Berlin police. However, the company's tools have also been found on the devices of government critics and journalists in countries like Ethiopia, Bahrain, Egypt, and Turkey — countries where surveillance tools exports are prohibited.

Read More on BleepingComputers

Even More on TheHackerNews

Microsoft, Others Dismantle Trickbot Botnet, Will Takedown Impact Be Temporary?



Microsoft collaborated with cybersecurity companies and government agencies to take down the million-device Trickbot botnet in an effort to help protect the Nov. 3 U.S. election and stop the global spread of ransomware and other malware. The botnet has been used to distribute a variety of malicious code, including the Ryuk ransomware variant, which the U.S. government has cited as a potential threat vector against the election. Microsoft says the malicious operators behind Trickbot will immediately attempt to recover.

Burt notes Microsoft was able to determine how the Trickbot botnet operated - including the infrastructure the malware used to communicate with and control victim computers, the way infected computers talk with each other and the botnet's mechanisms to evade detection and attempts to disrupt its operation. Microsoft's Digital Crimes Unit used a new legal weapon against Trickbot. "Our case includes copyright claims against Trickbot's malicious use of our software code. This approach is an important development in our efforts to stop the spread of malware, allowing us to take civil action to protect customers in the large number of countries around the world that have these laws in place," Burt says.

Despite the takedown of the Trickbot botnet by Microsoft and others Monday, the malware is still functioning, and its operators retain the tools needed to rebuild their malicious network, some cybersecurity experts say. So, the impact, while significant, could prove to be temporary. Microsoft has used the U.S. court system to disrupt many illegal activities in the last year, including a move in March to disrupt the Necurs botnet.

Read More on BankInfoSecurity

Even More on BleepingComputers

More #News

- Facebook launches bug bounty 'loyalty program'
- Document-signing service Docsketch discloses security breach
- Largest cruise line operator Carnival confirms ransomware data theft
- Video Conference Firm Targeted for Payment Card Skimming
- Software AG IT giant hit with $23 million ransom by Clop ransomware
- 'Network access' sold on hacker forums estimated at $500,000 in September 2020
- International law firm Seyfarth discloses ransomware attack
- Morgan Stanley Fined $60 Million for Data Protection Mishaps
- Microsoft Warns Android Users About A New Ransomware
- Card details for 3 million Dickey's customers posted on carding forum
- Barnes & Noble hit by cyberattack that exposed customer data
- Preparing for Better Payment Card Security With PCI DSS 4.0
- Criminals Still Going Crazy for Cryptocurrency
- Google Warns of Zero-Click Bluetooth Flaws in Linux-based Devices

#Patch Time!

- Microsoft Patch Tuesday, October 2020 Edition
- Adobe patches Magento bugs that lead to code execution, customer list tampering
- 55 New Security Flaws Reported in Apple Software and Services
- Foxit Patches Code Execution Vulnerabilities in PDF Software
- Remotely Exploitable DoS Vulnerabilities Found in Allen-Bradley Adapter
- 800,000 SonicWall VPNs vulnerable to new remote code execution bug
- SAP Patches Critical Vulnerability in CA Introscope Enterprise Manager
- Adobe Patches Critical Code Execution Vulnerability in Flash Player

#Tech and #Tools

- Announcing HashiCorp Boundary - Open source secure remote access solution
- Don't Copy Paste Into A Shell
- Introducing WARP for Desktop and Cloudflare for Teams
- Developing Burp Suite Extensions - Free training
- The Difficulties of Tracking Running Processes on Linux
- Dockerfile Security Best Practices
- Microsoft Rolling out OS-wide Endpoint DLP feature
- Microsoft Zero Trust Deployment Center
- RVA mapped to the mitre ATT&CK framework infographic
- Honeytokens using Azure keyvaults
- Burp Multiplayer - Sync's in-scope requests/responses, comments, and highlights in realtime.
- OSCD Sprint #2: Simulation, Detection & Response
- Moneta - Windows Usermode live memory analysis tool

Kingred Group is growing, so does the Group Security team! We're looking for new talented professionals to come join us:

- You like to break things, then explain how to fix it? Be part of our Cyber Security team
- You prefer the blue team side? Check out our Security analyst position
- Interested in Governance, Risk and Compliance? Apply for our Information Security Specialist role

Kindred is one of the largest online gambling companies in the world with over 24 million customers across 100 markets. You can find all our open vacancies on our career page.

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 over 24 million customers across 100 markets. 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 as an innovation driven company that builds on trust.

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