McAfee Sees COVID-19-Themed Threats and Powershell Malware Continue to Surge

April 13, 2021

Key Findings

- McAfee sees COVID-19-themed cyber-attack detections increase by 114% in Q4 2020
- Powershell threats grow 208% driven by Donoff malware
- New malware samples grow 10%; averaging 648 new threats per minute
- New ransomware increases 69%; Mobile malware grows 118%
- McAfee observes 3.1 million external attacks on cloud user accounts
- The Eternal Blue exploit was the most prominent vulnerability exploited in Q4
- Leading MITRE ATT&CK techniques included System Information Discovery, Obfuscated Files, Process Injection and Exploits of Public Facing Applications

SAN JOSE, Calif.--(BUSINESS WIRE)--Apr. 13, 2021-- McAfee Corp. (Nasdaq: MCFE), the device-to-cloud cybersecurity company, today released its McAfee Threats Report: April 2021, examining cybercriminal activity related to malware and the evolution of cyber threats in the third and fourth quarters of 2020. In Q4, McAfee Labs observed an average of 648 threats per minute, an increase of 60 threats per minute (10%) over Q3. The two quarters also saw COVID-19-related cyber-attack detections increase by 240% in Q3 and 114% in Q4, while Powershell threats again surged 208% due to continued increases in Donoff malware activity.

“The world—and enterprises—adjusted amidst pandemic restrictions and sustained remote work challenges, while security threats continued to evolve in complexity and increase in volume,” said Raj Samani, McAfee fellow and chief scientist. “Though a large percentage of employees grew more proficient and productive in working remotely, enterprises endured more opportunistic COVID-19 related campaigns among a new cast of bad-actor schemes. Furthermore, ransomware and malware targeting vulnerabilities in work-related apps and processes were active and remain dangerous threats capable of taking over networks and data, while costing millions in assets and recovery costs.”

Each quarter, McAfee assesses the state of the cyber threat landscape based on in-depth research, investigative analysis, and threat data gathered by the McAfee Global Threat Intelligence cloud from over a billion sensors across multiple threat vectors around the world. The introduction of MVISION Insights in 2020 has made it possible for McAfee to track the prevalence of campaigns, their associated IoCs, and determine the in-field detections. This month’s report is the first to feature statistics such as the top MITRE ATT&CK techniques observed in Q4 among criminal and APT groups, while sharing observations on the SUNBURST malware that rocked the cybersecurity world at the end of 2020.

COVID-19-Themed Threats

As organizations the world over adapted to unprecedented numbers of employees working from home, cybercriminals worked feverishly to launch COVID-19-themed attacks on a workforce coping with pandemic restrictions and the potential vulnerabilities of remote device and bandwidth security. As the pandemic began to surge around the world, McAfee saw a 605% increase in Q2 2020. These attacks again increased by 240% in Q3 and 114% in Q4.

Malware Threats

In Q3 2020, McAfee Labs observed an average of 588 threats per minute, an increase of 169 threats per minute (40%). By the fourth quarter, this average rose to 648 threats per minute, an increase of 60 threats per minute (10%).

- **Powershell** threats grew 208% in Q4 driven largely by Donoff malware. McAfee observed numerous Powershell attacks utilizing Process Injection to insert code into legitimate running processes as a privilege escalation technique.
- **Mobile malware** grew 118% in Q4 in part due to a surge in SMS Reg samples. The HiddenAds, Clicker, MoqHao, HiddenApp, Dropper and FakeApp strains were the most detected mobile malware families.
- **Ransomware** grew in volume 69% from Q3 to Q4 driven by Cryptodefense. REvil, Thanos, Ryuk, RansomeXX and Maze groups topped the overall list of ransomware families.
- **MacOS malware** exploded in Q3 420% due to EvilQuest ransomware but then slowed towards the end of the year.

Victims, Vectors & Vulnerabilities

Publicly Reported Incidents. McAfee tracked a 100% increase in publicly reported cyber incidents targeting the technology sector during the fourth quarter of 2020. Reported incidents in the public sector grew by 93% over the same period.

Attack Vectors. Malware was the most reported cause of security incidents in Q4 followed by account hijackings, targeted attacks and vulnerabilities. Incidents related to new vulnerabilities surged 100% in Q4, malware and targeted attacks each rose 43%, and account hijackings increased 30%.

Vulnerabilities Exploited. Among the campaigns McAfee monitored and investigated, the Eternal Blue exploit was the most prominent in Q4 2020.

MITRE ATT&CK Techniques

The top MITRE ATT&CK techniques observed by McAfee in Q3 and Q4 included System Information Discovery, Obfuscated Files or Information, File and Directory Discovery, Data Encryption for Impact, Stop Services, Process Injection, Process Discovery, Masquerading Techniques, and Exploits of

Public Facing Applications.

- **System Information Discovery** was one of the more notable MITRE techniques in the campaigns McAfee observed in Q4 2020. The malware in these campaigns contained functionality that gathered the OS version, hardware configuration and hostname from a victim's machine and communicated back to the threat actor.
- **Obfuscated Files or Information** was the second most observed technique for Q4. One noteworthy example was threat actor group APT28's use of virtual hard drive (VHD) files to package and obfuscate their malicious payloads to bypass security technology.
- **Process Injection.** McAfee observed this privilege escalation technique among several malware families and threat groups, including Powershell threats, RAT tools such as Remcos, ransomware groups such as REvil, and multiple state-sponsored APT groups.
- **Exploits of Public Facing Applications.** The fourth quarter saw an uptick in the use of this technique as multiple reports from CISA, NSA warned that industry that state sponsored threat actors are actively leveraging several vulnerabilities in public facing applications such as remote management and VPN software. Beyond sophisticated nation-state actors, McAfee also observed ransomware groups leveraging this initial access tactic.

Attacks on Cloud Users

McAfee observed nearly 3.1 million external attacks on cloud user accounts. This is based on the aggregation and anonymization of cloud usage data from more than 30 million McAfee MVISION cloud users worldwide during the fourth quarter of 2020. This data set represents companies in all major industries across the globe, including financial services, healthcare, public sector, education, retail, technology, manufacturing, energy, utilities, legal, real estate, transportation, and business services.

Resources:

- **McAfee Threats Report: April 2021**
- **MVISION Insights Public View**
- **McAfee Threat Center**
- **McAfee COVID-19 Threats Dashboard**

About McAfee Labs and Advanced Threat Research

McAfee Labs and McAfee Advanced Threat Research are a leading source for threat research, threat intelligence, and cybersecurity thought leadership. With data from over a billion sensors across key threats vectors—file, web, message, and network— McAfee Labs and McAfee Advanced Threat Research deliver real-time threat intelligence, critical analysis, and expert thinking to improve protection and reduce risks.

About McAfee

McAfee Corp. (Nasdaq: MCFE) is the device-to-cloud cybersecurity company. Inspired by the power of working together, McAfee creates consumer and business solutions that make our world a safer place. www.mcafee.com

McAfee® and the McAfee logo are trademarks of McAfee, LLC or its subsidiaries in the United States and other countries. Other marks and brands may be claimed as the property of others.

View source version on businesswire.com: https://www.businesswire.com/news/home/20210412005896/en/

McAfee
Chris Palm
media@mcafee.com

Source: McAfee