McAfee Sees COVID-19-Themed Threats and PowerShell Malware Surge in Q2 2020

November 5, 2020

Key Findings

- McAfee sees COVID-19-themed cyber-attack detections increase by 605% in Q2 2020
- McAfee saw PowerShell malware surge 117% due to proliferation of malicious Donoff documents
- Attacks on cloud services users reached nearly 7.5 million
- New malware samples grow 11.5% in Q2 2020; averaging 419 new threats per minute
- New Coimmining malware increases 25% with adoption of new Coimmining applications
- New Linux malware increases 22% due to Gafgyt and Mirai Internet of Things activity
- Mobile malware grows 15% driven by Android Mobby Adware surge
- Publicly disclosed security incidents rose 22%; incidents targeting technology industry increase 91%

SAN JOSE, Calif.--(BUSINESS WIRE)--Nov. 5, 2020-- McAfee Corp. (Nasdaq: MCFE), the device-to-cloud cybersecurity company, today released its McAfee Labs Threats Report: November 2020, examining cybercriminal activity related to malware and the evolution of cyber threats in Q2 2020. During this period, McAfee saw an average of 419 new threats per minute as overall new malware samples grew by 11.5%. A significant proliferation in malicious Donoff Microsoft Office documents attacks propelled new PowerShell malware up 117%, and the global impact of COVID-19 prompted cybercriminals to adjust their cybercrime campaigns to lure victims with pandemic themes and exploit the realities of a workforce working from home.

“The second quarter of 2020 saw continued developments in innovative threat categories such as PowerShell malware and the quick adaptation by cybercriminals to target organizations working from remote environments,” said Raj Samani, McAfee fellow and chief scientist. “What began as a trickle of phishing campaigns and the occasional malicious app quickly turned into a deluge of malicious URLs, attacks on cloud users and capable threat actors leveraging the world’s thirst for more information on COVID-19 as an entry mechanism into systems across the globe.”

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.

COVID-19-Themed Threat Campaigns

After a first quarter that saw the world plunge into pandemic, the second quarter saw enterprises continue to adapt to unprecedented numbers of employees working from home and the cybersecurity challenges this new normal demands. In response, McAfee launched the McAfee COVID-19 Threats Dashboard to help CISOs and security teams understand how bad actors have retargeted increasingly sophisticated techniques toward businesses, governments, schools, and a workforce coping with COVID-19 restrictions and the potential vulnerabilities of remote device and bandwidth security. Over the course of Q2, McAfee’s global network of over a billion sensors observed a 605% increase in COVID-19-related attack detections compared to Q1.

Donoff & PowerShell Malware

Donoff Microsoft Office documents act as TrojanDownloaders by leveraging the Windows Command shell to launch PowerShell and proceed to download and execute malicious files. Donoff played a critical role in driving the 689% surge in PowerShell malware in Q1 2020. In Q2, the acceleration of Donoff-related malware growth slowed but remained robust, driving up PowerShell malware by 117% and helping to drive a 103% increase in overall new Microsoft Office malware. This activity should be viewed within the context of the overall continued growth trend in PowerShell threats. In 2019, total samples of PowerShell malware grew 1,902%.

Attacks on Cloud Users

McAfee observed nearly 7.5 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 second 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.

Q2 2020 Threat Activity

- **Malware overall.** McAfee Labs observed 419 new threats per minute in Q2 2020, an increase of almost 12% over the previous quarter. Ransomware growth remained steady compared to the first quarter of 2020.
- **Coimminer malware.** After growing 26% in Q1, new Coimmining malware increased 25% over the previous quarter sustained by the popularity of new Coimmining applications.
- **Mobile malware.** After a 71% increase in new mobile malware samples in Q1, Q2 saw the category slow 15% despite a surge in Android Mobby Adware.
- **Internet of Things.** New IoT malware increased only 7% in Q2, but the space saw significant activity by Gafgyt and Mirai threats, both of which drove growth in new Linux malware by 22% during the period.
- **Regional cyber activity.** McAfee counted 561 publicly disclosed security incidents in the second quarter of 2020, an increase of 22% from Q1. Disclosed incidents targeting North America decreased 30% over the previous quarter. These incidents decreased 47% in the United States, but increased 25% in Canada and 29% in the United Kingdom.
- **Attack vector.** Overall, Malware led among reported attack vectors accounting for 35% of publicly reported incidents in Q2. Account Hijacking and Targeted Attacks accounted for 17% and 9% respectively.
- **Sector activity.** Disclosed incidents detected in the second quarter of 2020 targeting Science and Technology increased 91% over the previous quarter. Incidents in Manufacturing increased 10%, but Public Sector events decreased by 14%.

**Resources:**
- McAfee Labs Threats Report: November 2020
- 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](http://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/20201104005812/en/)

McAfee
Chris Palm
media@mcafee.com

Source: McAfee