REPORT

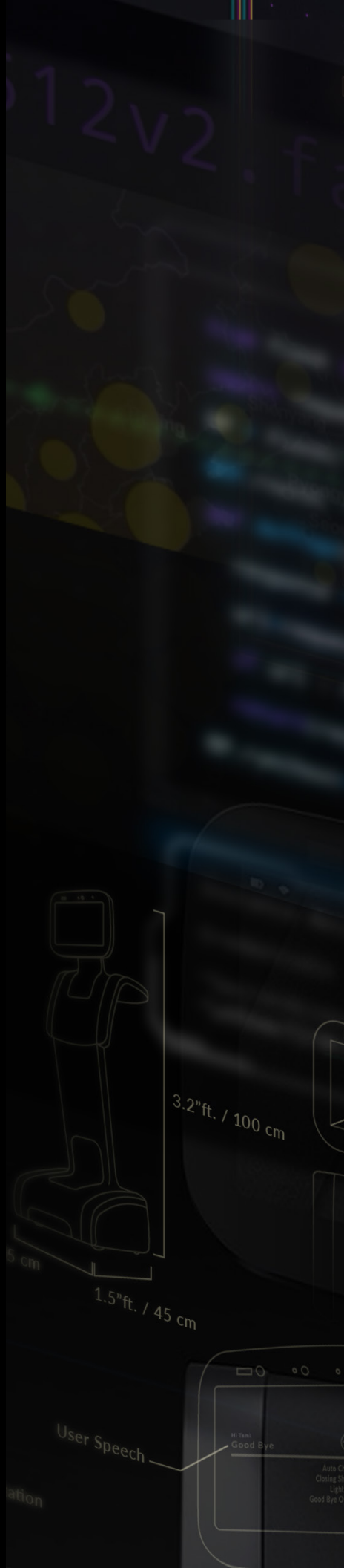
McAfee

MCAFEE LABS THREAT REPORT

04.21

TABLE OF CONTENTS

3 LETTER FROM OUR CHIEF SCIENTIST
4 MCAFEE COVID-19 RELATED MALICIOUS FILE DASHBOARD
5 INTRODUCTION
6 THREATS TO SECTORS AND VECTORS
7 PUBLICLY DISCLOSED SECURITY INCIDENTS BY CONTINENT
8 PUBLICLY DISCLOSED SECURITY INCIDENTS BY COUNTRY
9 PUBLICLY DISCLOSED SECURITY INCIDENTS BY INDUSTRY
10 PUBLICLY DISCLOSED SECURITY INCIDENTS BY VECTORS
11 CLOUD INCIDENTS BY COUNTRY OF ORIGIN
12 MALWARE THREATS STATISTICS
17 SUNBURST MALWARE AND SOLARWINDS SUPPLY CHAIN COMPROMISE
18 TOP MITRE ATT&CK TECHNIQUES APT/CRIME
21 TOP RANSOMWARE FAMILIES AND TECHNIQUES
21 TOP FAMILIES, MITRE ATT&CK TECHNIQUES, AND PRIMARY SECTORS
21 TOP MITRE ATT&CK TECHNIQUES
23 RESOURCES
23 MCAFEE LABS AND RESEARCHERS ON TWITTER
24 ABOUT MCAFEE
24 ABOUT MCAFEE LABS AND ADVANCED THREAT RESEARCH



This latest report incorporates not only the malware zoo, but new analysis for what is being detected in the wild. We've also added statistics detailing the top MITRE ATT&CK techniques observed in Q4 2020 from Criminal/APT groups.

LETTER FROM OUR CHIEF SCIENTIST

Welcome to our latest McAfee Labs® Threat Report and our coverage of the end of a tumultuous 2020. While you'll notice a new, enhanced digital presentation showcasing our review of notable threats, this report also includes many new McAfee insights into the threat landscape.

Historically our reports detailed the volume of key threats, such as "what is in the malware zoo." The introduction of MVISION Insights in 2020 has since made it possible to track the prevalence of campaigns (and their associated IoCs) and determine the in-field detections. This latest report incorporates not only the malware zoo, but new analysis for what is being detected in the wild. We have also added statistics detailing the top MITRE ATT&CK techniques observed in Q4 2020 from Criminal/APT groups.

These new, insightful additions really make for a bumper report! The analysis does not end there, however. The end of Q4 2020 saw the revelation about the SolarWinds breach, and the consequences associated with the compromised organizations. The focus of the narrative within this report will detail the findings of the SUNBURST malware which of course continues to dominate the headlines in Q1 2021.

In addition to these timely threat campaigns, the pandemic continued to have its effects on the threatscape. McAfee's global network of more than a billion sensors registered a 605% increase in total Q2 COVID-19-themed threat detections. As you can track on our McAfee COVID-19 Threats Dashboard, pandemic-related campaigns continued to increase in Q3 and Q4 of 2020.

We hope you enjoy this new McAfee Labs threat report presentation and find our new data valuable.

—Raj Samani
McAfee Fellow, Chief Scientist

Twitter @Raj_Samani

WRITING AND RESEARCH

Christiaan Beek
Eoin Carroll
Mo Cashman
Sandeep Chandana
John Fokker
Melissa Gaffney
Steve Grobman
Tracy Holden
Tim Hux
Douglas McKee
Lee Munson
Chris Palm
Tim Polzer
Thomas Roccia
Raj Samani
Craig Schmugar

MCAFEE COVID-19 RELATED MALICIOUS FILE DASHBOARD

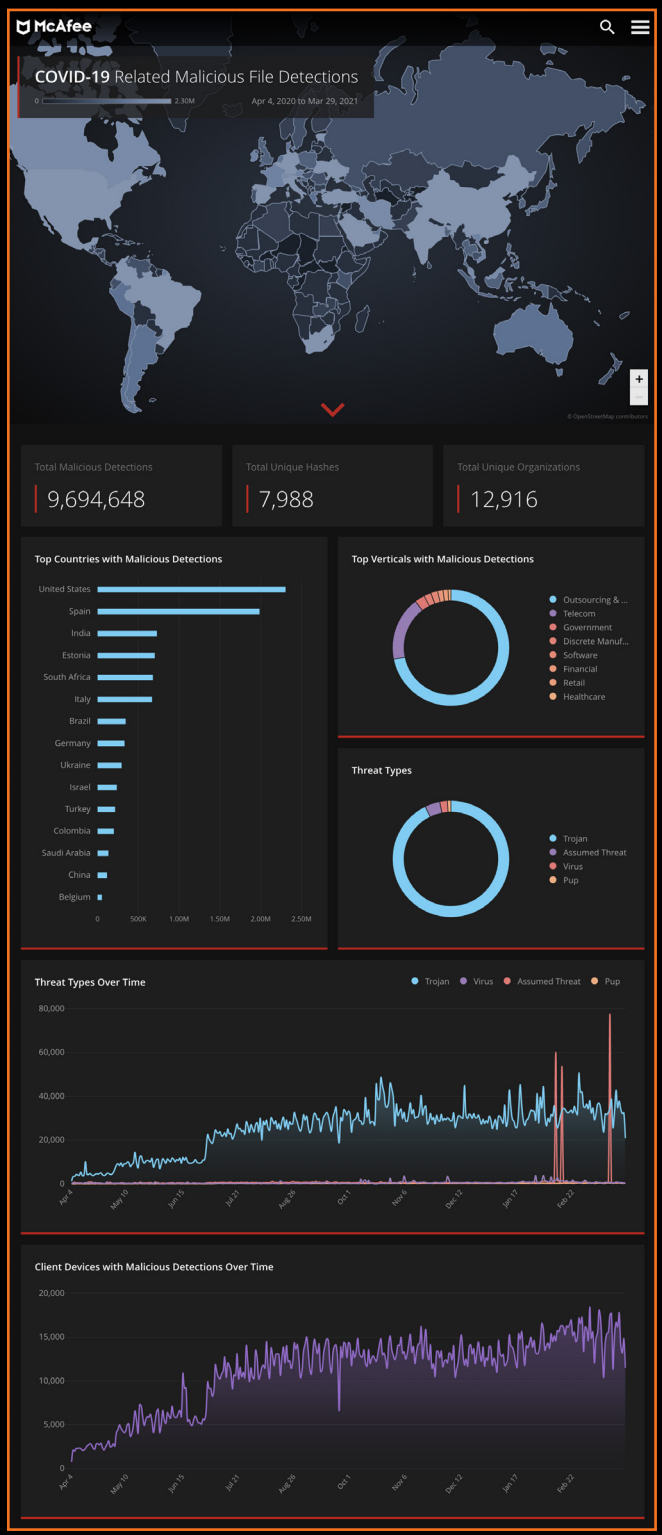


FIGURE 1. WEAPONIZING THE CHALLENGES OF LIVING AND WORKING AMIDST A PANDEMIC REMAINED A POPULAR THREAT TACTIC FOR BAD ACTORS AS 2020 CAME TO A CLOSE. MCAFEE'S GLOBAL NETWORK OF MORE THAN A BILLION SENSORS REGISTERED COVID-19-THEMED THREAT DETECTIONS TOTALING 445,922 IN Q2 2020 (605% INCREASE), 1,071,257 IN Q3 2020 (240% INCREASE), AND 1,224,628 IN Q4 2020 (114% INCREASE).

LETTER FROM OUR CHIEF SCIENTIST

INTRODUCTION

THREATS TO SECTORS AND VECTORS

MALWARE THREATS STATISTICS

SUNBURST MALWARE AND SOLARWINDS SUPPLY CHAIN COMPROMISE

TOP MITRE ATT&CK TECHNIQUES APT/CRIME

RESOURCES

ABOUT MCAFEE

ABOUT MCAFEE LABS AND ADVANCED THREAT RESEARCH

INTRODUCTION

In this report, McAfee® Labs examines the threats that emerged in the third and fourth quarters of 2020. Our Advanced Threat Research team has aggressively tracked, identified, and researched the cause and effects of the prevalent and news-making campaigns threatening enterprises in the second half of 2020.

The world—and enterprises—adjusted amidst pandemic restrictions and sustained remote challenges, while security threats continued to evolve in complexity and increase in volume. 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. Prominent campaigns such as SUNBURST and new ransomware tactics left SOCs no time to rest.

As your enterprise meets new challenges in 2021, it remains imperative that workforces—both on-site and remote—be alert to potential threats emerging from seemingly routine communications. Remind and test your workforce's resistance against clicking unverified links and engaging external email attachments. As this report confirms, ransomware and malware targeting vulnerabilities in work-related apps and work processes were active in the last half of 2020 and remain dangerous threats capable of taking over networks and data, while costing millions in assets and recovery costs.

McAfee researchers remain vigilant against new tactics and continuing techniques and focused on the race to thwart threats against our customers and security community. McAfee stands apart in the security industry utilizing one billion global sensors to provide timely intelligence and powerful insight toward defending your business, protecting your assets and helping your workforce remain productive even in a pandemic.

Visit the McAfee Threat Center to tap into industry-leading research and security guidance against the latest and most impactful evolving threats identified by our threat team.

LETTER FROM OUR CHIEF SCIENTIST

INTRODUCTION

THREATS TO SECTORS AND VECTORS

MALWARE THREATS STATISTICS

SUNBURST MALWARE AND SOLARWINDS SUPPLY CHAIN COMPROMISE

TOP MITRE ATT&CK TECHNIQUES APT/CRIME

RESOURCES

ABOUT MCAFEE

ABOUT MCAFEE LABS AND ADVANCED THREAT RESEARCH

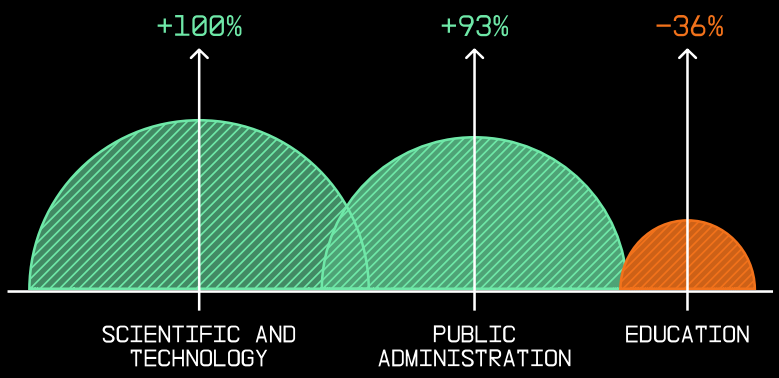
THREATS TO SECTORS AND VECTORS

The volume of malware threats observed by McAfee Labs averaged 588 threats per minute, an increase of 169 threats per minute (40%) in the third quarter of 2020. The fourth quarter volume averaged 648 threats per minute, an increase of 60 threats per minute (10%).

Notable Sector increases and decreases from Q3 to Q4 2020 include:

- Scientific and Technology +100%
- Public Administration +93%
- Education -36%

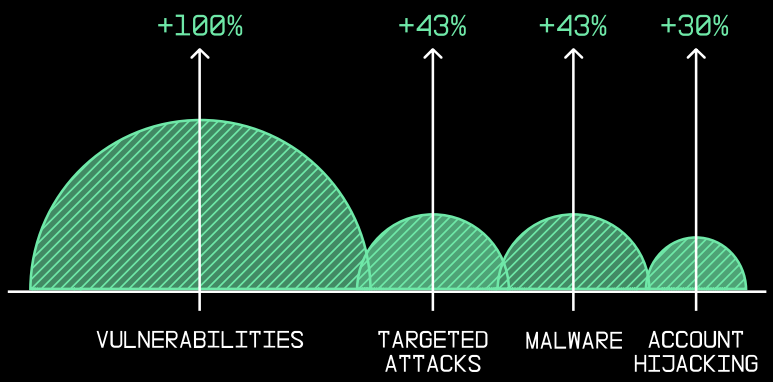
NOTABLE SECTOR INCREASES AND DECREASES FROM Q3 TO Q4 2020:



Notable Vector increases from Q3 to Q4 2020 include:

- Vulnerabilities +100%
- Malware +43%
- Targeted Attacks +43%
- Account Hijacking +30%

NOTABLE VECTOR INCREASES FROM Q3 TO Q4 2020:



LETTER FROM OUR CHIEF SCIENTIST

INTRODUCTION

THREATS TO SECTORS AND VECTORS

MALWARE THREATS STATISTICS

SUNBURST MALWARE AND SOLARWINDS SUPPLY CHAIN COMPROMISE

TOP MITRE ATT&CK TECHNIQUES APT/CRIME

RESOURCES

ABOUT MCAFEE

ABOUT MCAFEE LABS AND ADVANCED THREAT RESEARCH

PUBLICLY DISCLOSED SECURITY INCIDENTS BY CONTINENT

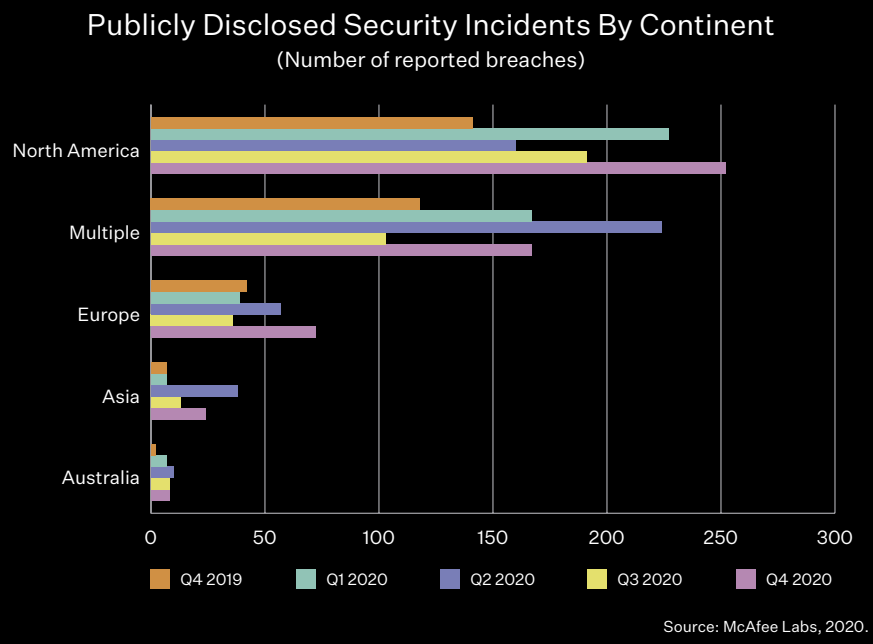


FIGURE 2. PUBLICLY DISCLOSED INCIDENTS SURGED 100% IN EUROPE FROM Q3 TO Q4 2020. INCIDENTS IN ASIA INCREASED 84%. INCIDENTS IN NORTH AMERICA ROSE 36%.

LETTER FROM OUR CHIEF SCIENTIST

INTRODUCTION

THREATS TO SECTORS AND VECTORS

MALWARE THREATS STATISTICS

SUNBURST MALWARE AND SOLARWINDS SUPPLY CHAIN COMPROMISE

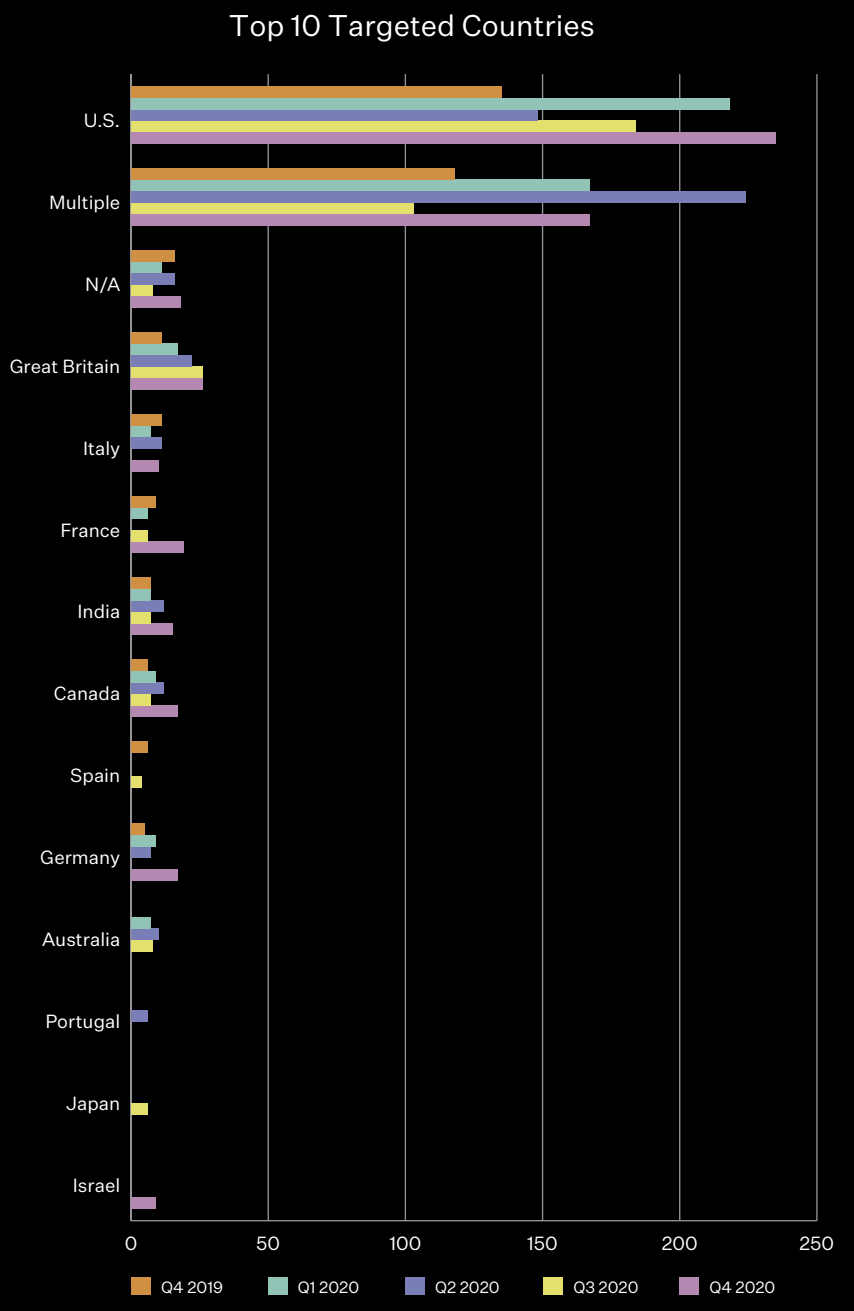
TOP MITRE ATT&CK TECHNIQUES APT/CRIME

RESOURCES

ABOUT MCAFEE

ABOUT MCAFEE LABS AND ADVANCED THREAT RESEARCH

PUBLICLY DISCLOSED SECURITY INCIDENTS BY COUNTRY



Source: McAfee Labs, 2020.

FIGURE 3. NOTABLE INCREASES FROM Q3 TO Q4 2020 INCLUDE CANADA (142%). INCIDENTS IN THE UNITED STATES ROSE 27%. INCIDENTS IN THE U.S. COMPRISED 47% OF INCIDENTS OBSERVED IN THE TOP 10 COUNTRIES.

LETTER FROM OUR CHIEF SCIENTIST

INTRODUCTION

THREATS TO SECTORS AND VECTORS

MALWARE THREATS STATISTICS

SUNBURST MALWARE AND SOLARWINDS SUPPLY CHAIN COMPROMISE

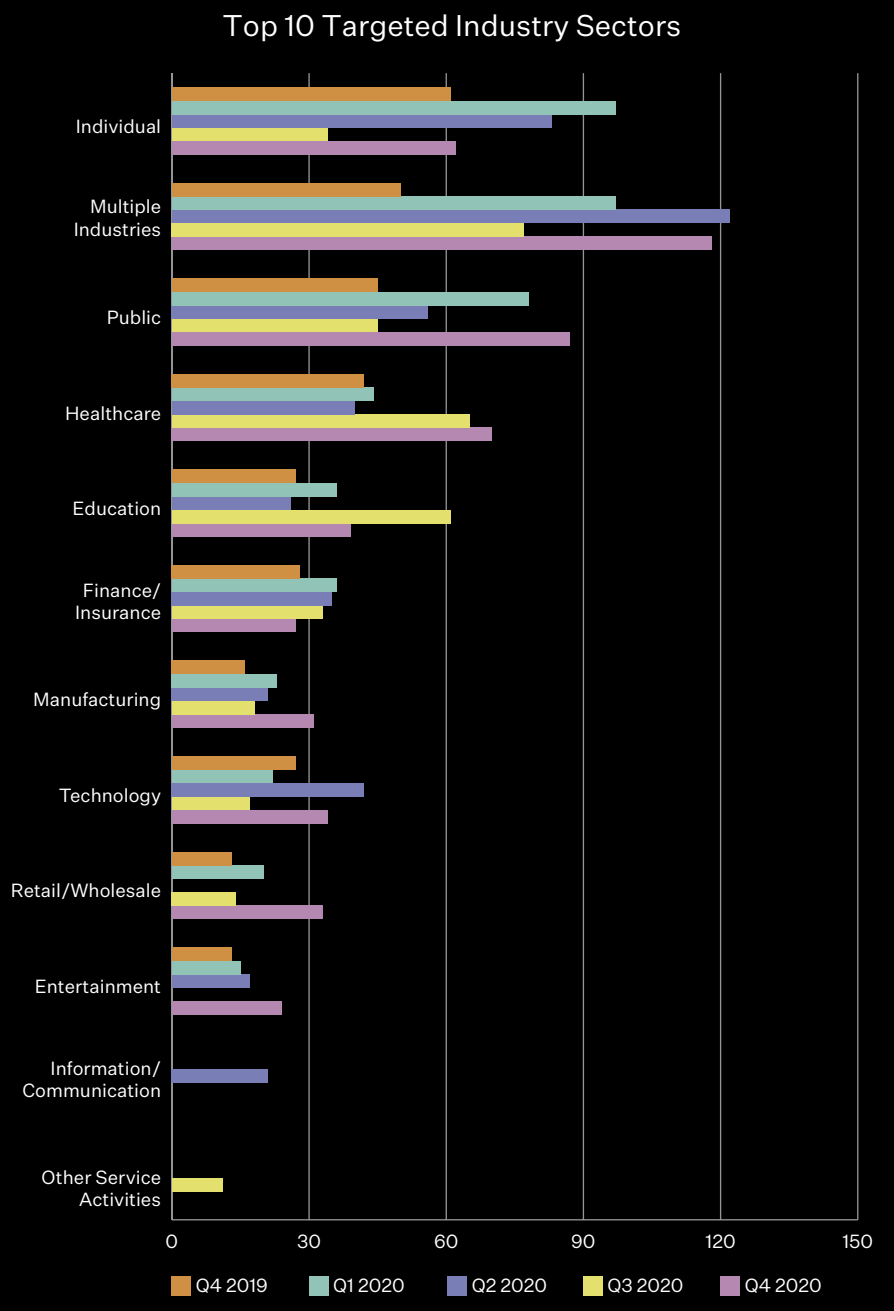
TOP MITRE ATT&CK TECHNIQUES APT/CRIME

RESOURCES

ABOUT MCAFEE

ABOUT MCAFEE LABS AND ADVANCED THREAT RESEARCH

PUBLICLY DISCLOSED SECURITY INCIDENTS BY INDUSTRY



Source: McAfee Labs, 2020.

FIGURE 4. DISCLOSED INCIDENTS TARGETING TECHNOLOGY INCREASED 100% FROM Q3 TO Q4 2020. INCIDENTS TARGETING THE PUBLIC SECTOR SURGED 93%.

LETTER FROM OUR CHIEF SCIENTIST

INTRODUCTION

THREATS TO SECTORS AND VECTORS

MALWARE THREATS STATISTICS

SUNBURST MALWARE AND SOLARWINDS SUPPLY CHAIN COMPROMISE

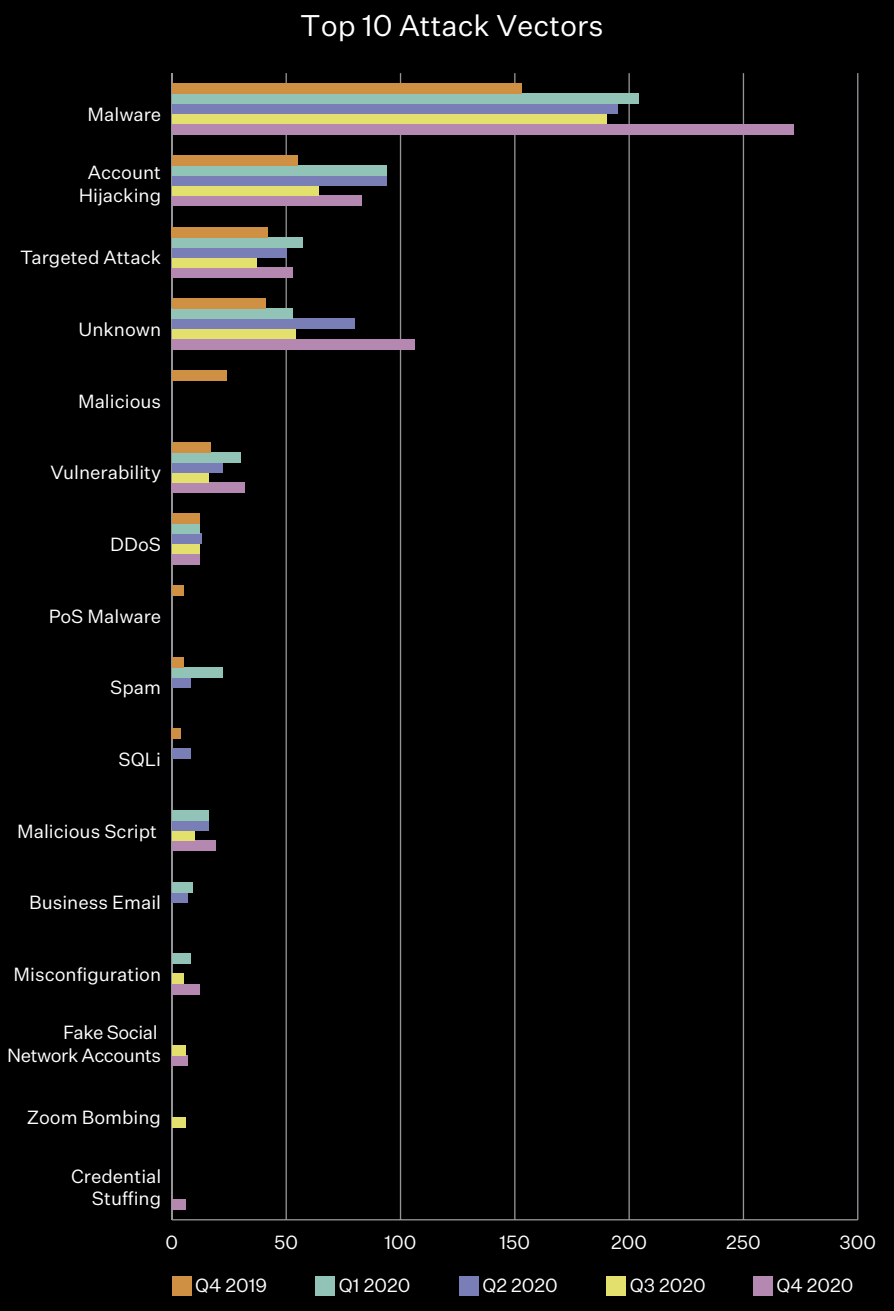
TOP MITRE ATT&CK TECHNIQUES APT/CRIME

RESOURCES

ABOUT MCAFEE

ABOUT MCAFEE LABS AND ADVANCED THREAT RESEARCH

PUBLICLY DISCLOSED SECURITY INCIDENTS BY VECTORS



Source: McAfee Labs, 2020.

FIGURE 5. NEW VULNERABILITIES VECTORS SURGED 100% FROM Q3 TO Q4 2020. NEW MALWARE AND TARGETED ATTACKS EACH ROSE 43%. ACCOUNT HIJACKING INCREASED 30%.

LETTER FROM OUR CHIEF SCIENTIST

INTRODUCTION

THREATS TO SECTORS AND VECTORS

MALWARE THREATS STATISTICS

SUNBURST MALWARE AND SOLARWINDS SUPPLY CHAIN COMPROMISE

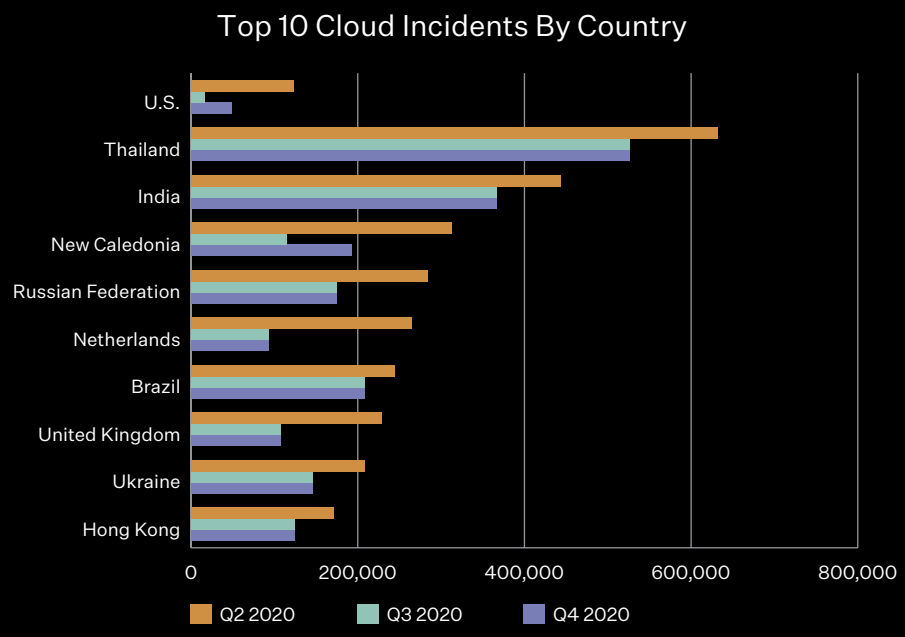
TOP MITRE ATT&CK TECHNIQUES APT/CRIME

RESOURCES

ABOUT MCAFEE

ABOUT MCAFEE LABS AND ADVANCED THREAT RESEARCH

CLOUD INCIDENTS BY COUNTRY OF ORIGIN



Source: McAfee Labs, 2020.

FIGURE 6. MCAFEE OBSERVED APPROXIMATELY 3.1 MILLION EXTERNAL ATTACKS ON CLOUD ACCOUNTS, AGGREGATING AND ANONYMIZING CLOUD USAGE DATA FROM MORE THAN 30 MILLION MCAFEE MVISION CLOUD USERS WORLDWIDE DURING Q4 OF 2020. THIS DATA SET REPRESENTS COMPANIES IN FINANCIAL SERVICES, HEALTHCARE, PUBLIC SECTOR, EDUCATION, RETAIL, TECHNOLOGY, MANUFACTURING, ENERGY, UTILITIES, LEGAL, REAL ESTATE, TRANSPORTATION, AND BUSINESS SERVICES.

LETTER FROM OUR CHIEF SCIENTIST

INTRODUCTION

THREATS TO SECTORS AND VECTORS

MALWARE THREATS STATISTICS

SUNBURST MALWARE AND SOLARWINDS SUPPLY CHAIN COMPROMISE

TOP MITRE ATT&CK TECHNIQUES APT/CRIME

RESOURCES

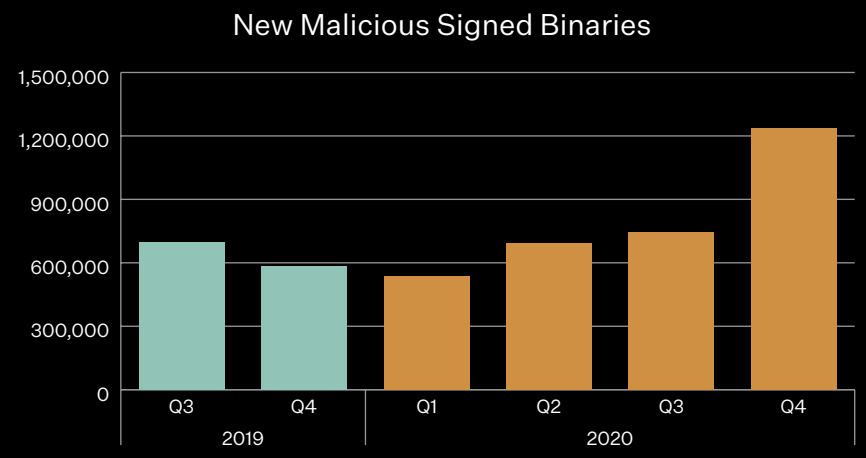
ABOUT MCAFEE

ABOUT MCAFEE LABS AND ADVANCED THREAT RESEARCH

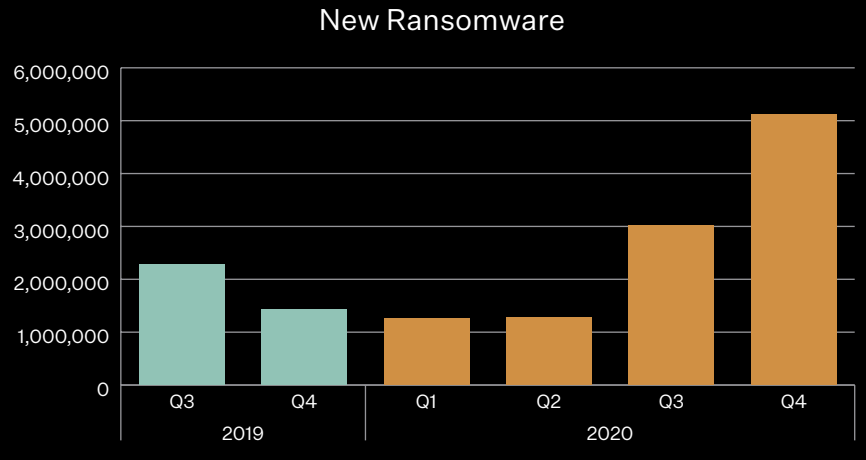
MALWARE THREATS STATISTICS

The third and fourth quarters of 2020 saw significant increase in several threat categories:

- Powershell threats grew 208% from Q3 to Q4, also pushed by Donoff
- MacOS malware exploded in Q3 420%(?) due to EvilQuest ransomware, but came back to normal levels in Q4
- Office malware surged 199% from Q3 to Q4
- Mobile malware grew 118% from Q3 to Q4 driven by SMS Reg
- New Ransomware, driven by Cryptodefense, grew in volume 69% from Q3 to Q4
- New Linux malware increased 6% from Q3 to Q4
- Coin Miner malware decreased 35% in Q4
- Slight decreases in iOS, IoT, and JavaScript were observed



Source: McAfee Labs, 2020.



Source: McAfee Labs, 2020.

LETTER FROM OUR CHIEF SCIENTIST

INTRODUCTION

THREATS TO SECTORS AND VECTORS

MALWARE THREATS STATISTICS

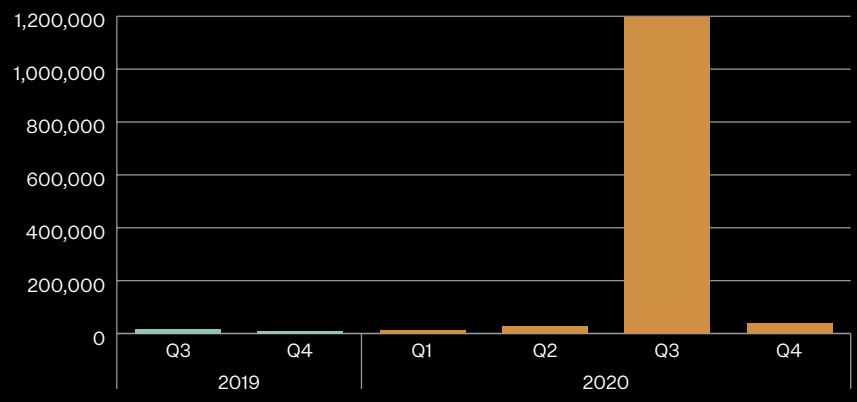
SUNBURST MALWARE AND SOLARWINDS SUPPLY CHAIN COMPROMISE

TOP MITRE ATT&CK TECHNIQUES APT/CRIME

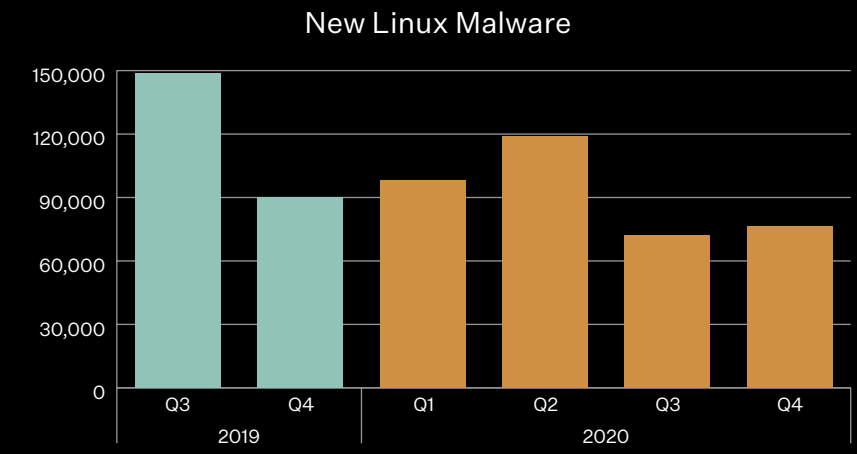
RESOURCES

ABOUT MCAFEE

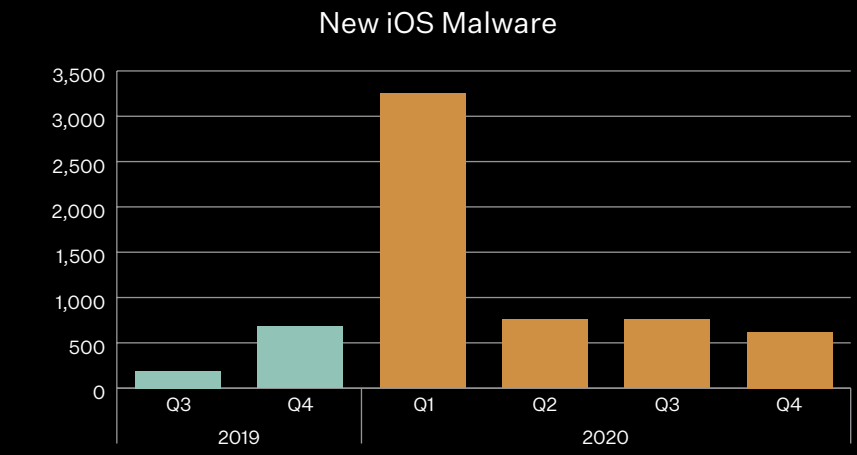
ABOUT MCAFEE LABS AND ADVANCED THREAT RESEARCH



Source: McAfee Labs, 2020.



Source: McAfee Labs, 2020.



Source: McAfee Labs, 2020.

LETTER FROM OUR CHIEF SCIENTIST

INTRODUCTION

THREATS TO SECTORS AND VECTORS

MALWARE THREATS STATISTICS

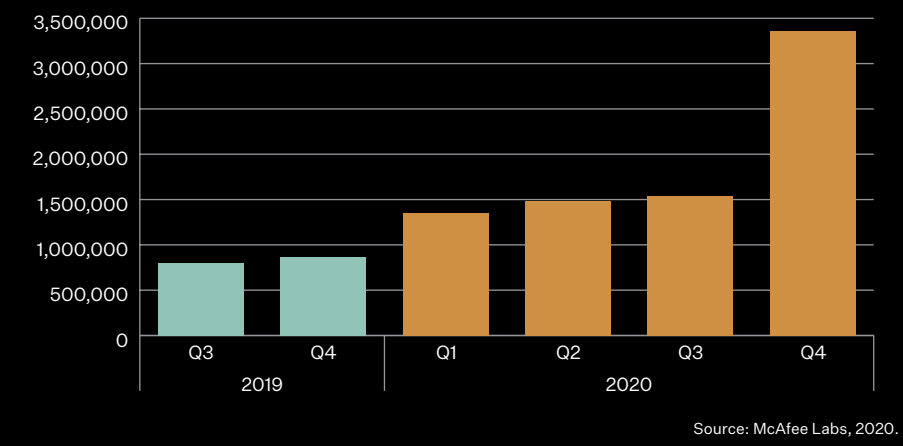
SUNBURST MALWARE AND SOLARWINDS SUPPLY CHAIN COMPROMISE

TOP MITRE ATT&CK TECHNIQUES APT/CRIME

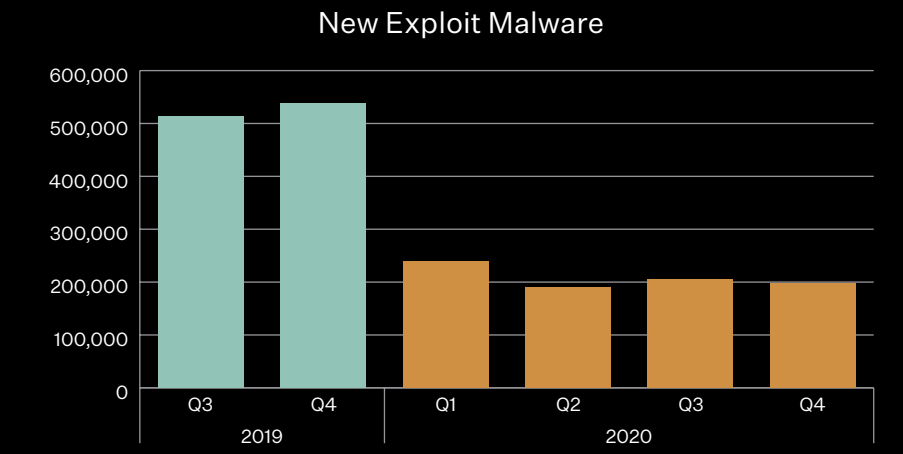
RESOURCES

ABOUT MCAFEE

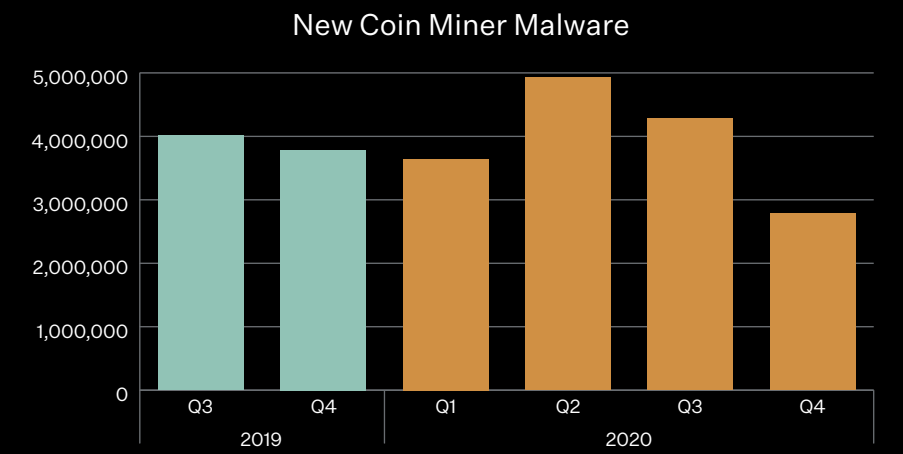
ABOUT MCAFEE LABS AND ADVANCED THREAT RESEARCH



Source: McAfee Labs, 2020.



Source: McAfee Labs, 2020.



Source: McAfee Labs, 2020.

LETTER FROM OUR CHIEF SCIENTIST

INTRODUCTION

THREATS TO SECTORS AND VECTORS

MALWARE THREATS STATISTICS

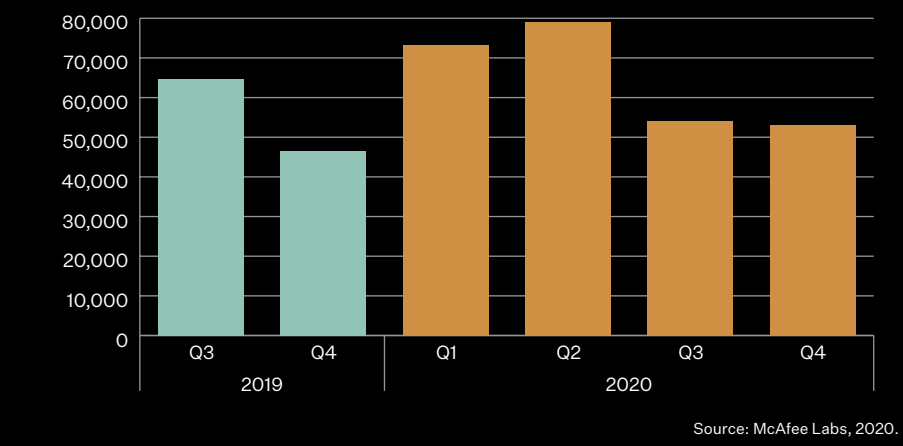
SUNBURST MALWARE AND SOLARWINDS SUPPLY CHAIN COMPROMISE

TOP MITRE ATT&CK TECHNIQUES APT/CRIME

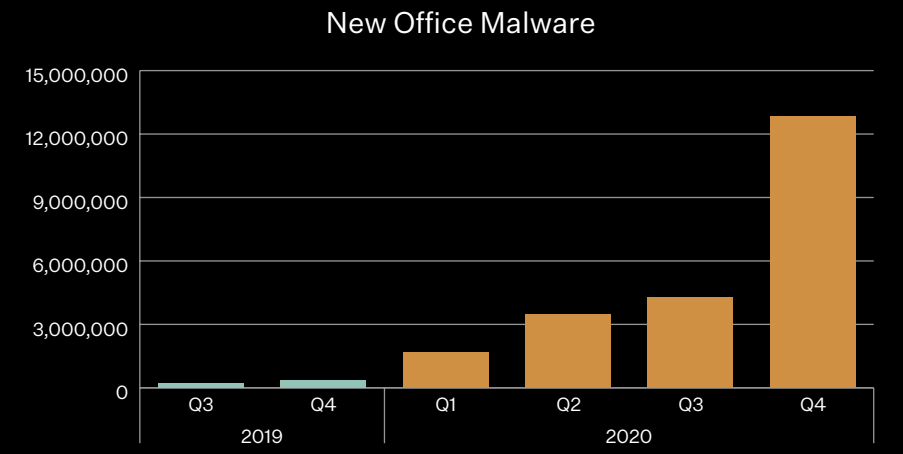
RESOURCES

ABOUT MCAFEE

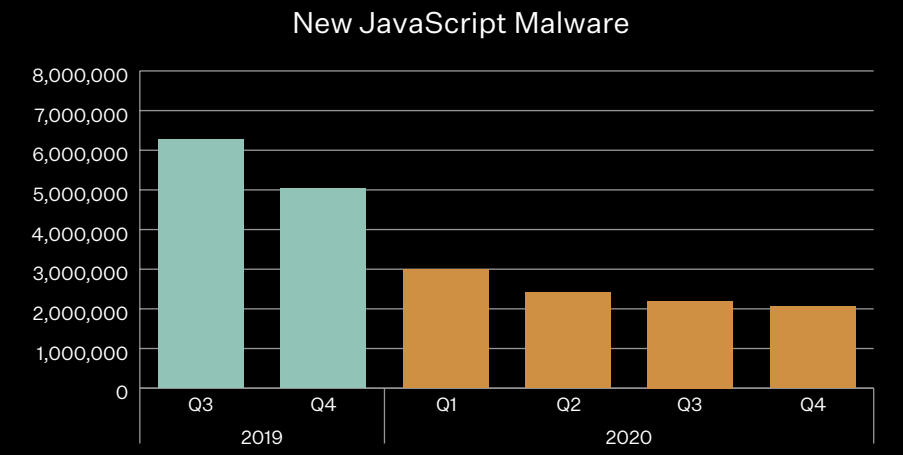
ABOUT MCAFEE LABS AND ADVANCED THREAT RESEARCH



Source: McAfee Labs, 2020.



Source: McAfee Labs, 2020.



Source: McAfee Labs, 2020.

LETTER FROM OUR CHIEF SCIENTIST

INTRODUCTION

THREATS TO SECTORS AND VECTORS

MALWARE THREATS STATISTICS

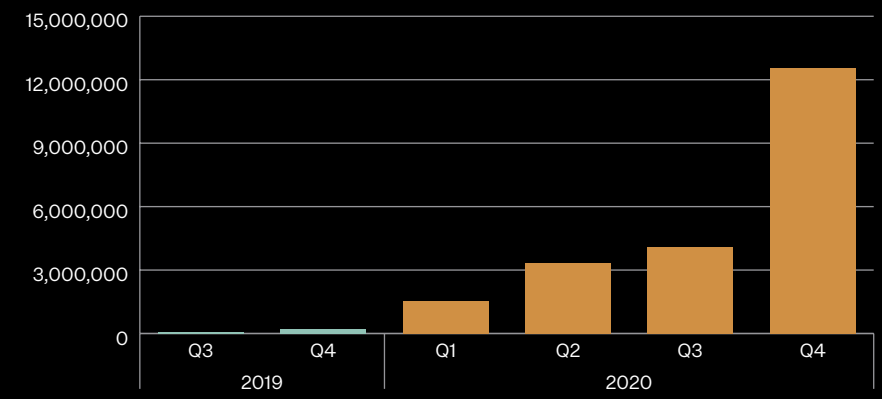
SUNBURST MALWARE AND SOLARWINDS SUPPLY CHAIN COMPROMISE

TOP MITRE ATT&CK TECHNIQUES APT/CRIME

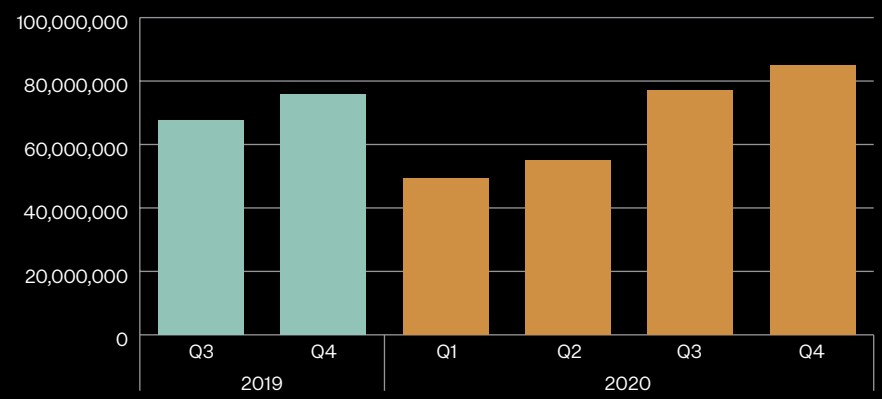
RESOURCES

ABOUT MCAFEE

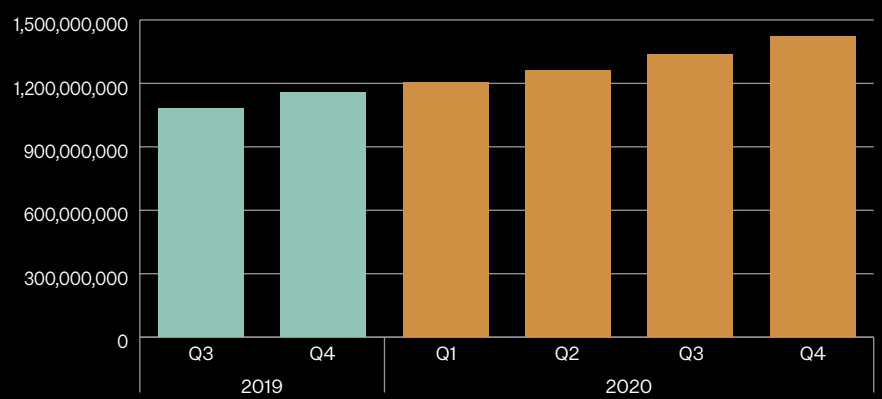
ABOUT MCAFEE LABS AND ADVANCED THREAT RESEARCH



Source: McAfee Labs, 2020.



Source: McAfee Labs, 2020.



Source: McAfee Labs, 2020.

LETTER FROM OUR CHIEF SCIENTIST

INTRODUCTION

THREATS TO SECTORS AND VECTORS

MALWARE THREATS STATISTICS

SUNBURST MALWARE AND SOLARWINDS SUPPLY CHAIN COMPROMISE

TOP MITRE ATT&CK TECHNIQUES APT/CRIME

RESOURCES

ABOUT MCAFEE

ABOUT MCAFEE LABS AND ADVANCED THREAT RESEARCH

SUNBURST MALWARE AND SOLARWINDS SUPPLY CHAIN COMPROMISE

In Q4 of 2020, FireEye disclosed that threat actors compromised SolarWinds's Orion IT monitoring and management software with a trojanized version of SolarWinds.Orion.Core.BusinessLayer.dll. The trojanized file delivers the SUNBURST malware through a backdoor as part of a digitally signed Windows Installer Patch. Use of a Compromised Software Supply Chain (T1195.002) as an Initial Access technique is particularly critical as it can go undetected for a long period. FireEye released countermeasures that can identify the SUNBURST malware.

McAfee reported on SUNBURST in this blog and additional analysis into the backdoor and continues to track the campaign as SolarWinds Chain Attack Multiple Global Victims with SUNBURST Backdoor through MVISION Insights. McAfee senior vice president and chief technology officer Steve Grobman detailed the game-changing impact of SolarWinds-SUNBURST. Customers can view the public version of MVISION Insights for the latest attack details, prevalence, techniques used and indicators of compromise.

FIGURE 7. MVISION INSIGHTS PROVIDES THE INDICATORS USED BY SUNBURST. THE INDICATORS WILL CONTINUE TO UPDATE BASED ON AUTOMATED COLLECTION AND HUMAN ANALYSIS. YOU CAN USE THE INDICATORS TO HUNT ON YOUR NETWORK.

LETTER FROM OUR CHIEF SCIENTIST

INTRODUCTION

THREATS TO SECTORS AND VECTORS

MALWARE THREATS STATISTICS

SUNBURST MALWARE AND SOLARWINDS SUPPLY CHAIN COMPROMISE

TOP MITRE ATT&CK TECHNIQUES APT/CRIME

RESOURCES

ABOUT MCAFEE

ABOUT MCAFEE LABS AND ADVANCED THREAT RESEARCH

TOP MITRE ATT&CK TECHNIQUES APT/CRIME

Tactics	Techniques (Top 5 per Tactic)	Comments
Initial Acess	Exploit public facing application	Uptick in the useage of this technique in Q4. Multiple reports from CISA, NSA warming the industry that State sponsered Threat actors are actively leveraging several CVE's related to public facing applications suchs as popular Remote management and VPN software. McAfee has observed that besides state sponsored groups, the ransomware groups were leveraging this initail access tactic.
	Replication through removable Media	
	Valid accounts	
	Drive-by-Comprimise	
	Phishing	
Execution	User execution	
	Command -line Interface	
	Scripting	
	Windows Management Instrumentation	
	Scheduled Task	
Persistence	Scheduled Task	
	Registry Run Keys / Startup Folder	
	DLL Side-loading	
	Valid accounts	
	Startup Items	
Privilege Escalation	Process Injection	Process injection remains to be one of the top Privilege Escalation techniques, we have observed the usage of this technique by several Malware families and threat groups, ranging from Rat tools like Remcos, Ransomware groups like REvil and mulitple State Sponsored APT groups. We have obsvered several attacks involving PowerShell injecting code into another running process.
	Scheduled Task	
	Registry Run Keys / Startup Folder	
	DLL- Side loading	
	Exploitation for Privilege Escalation	

LETTER FROM OUR CHIEF SCIENTIST

INTRODUCTION

THREATS TO SECTORS AND VECTORS

MALWARE THREATS STATISTICS

SUNBURST MALWARE AND SOLARWINDS SUPPLY CHAIN COMPROMISE

TOP MITRE ATT&CK TECHNIQUES APT/CRIME

RESOURCES

ABOUT MCAFEE

ABOUT MCAFEE LABS AND ADVANCED THREAT RESEARCH

Tactics	Techniques (Top 5 per Tactic)	Comments
Defense Evasion	Obfuscated Files or information	"This is the second most observed technique for Q4 2020. This technique is synonymous for the Cat and Mouse game played between malware and security software. Attackers constantly think of new ways to avoid being detected. One of the noteworthy methods we have observed in Q4 was by the threat actor group APT28 who used VHD files (or virtual Hard drives) to package and obfuscate their malicious payload."
	Deobfuscate/Decode Files or Information	
	Masquerading	
	Modify Registry	
	Process Injection	
Credential Access	Input Capture	
	Credential Capture	
	Keylogging	
	Brute Force	
	Steal Web Session Cookie	
Discovery	System Information Discovery	System Information Discovery was the most used MITRE technique of the Campaigns we observed in Q4 2020. The malware in these campaigns contained functionalities that gathered the OS version, hardware configuration and hostname from a victims machine and eventually communicated back to the Threat actor.
	File and Directory Discovery	
	Process Discovery	
	Query Registry	
	System Owner/User Discovery	
Lateral Movement	Remote File Copy	
	Exploitation of Remote Services	
	Replication Through Removable Media	
	Logon Scripts	
	Remote Services	
Collection	Data from Local System	
	Screen Capture	
	Automated Collection	
	Input Capture	
	Data Staged	

LETTER FROM OUR CHIEF SCIENTIST

INTRODUCTION

THREATS TO SECTORS AND VECTORS

MALWARE THREATS STATISTICS

SUNBURST MALWARE AND SOLARWINDS SUPPLY CHAIN COMPROMISE

TOP MITRE ATT&CK TECHNIQUES APT/CRIME

RESOURCES

ABOUT MCAFEE

ABOUT MCAFEE LABS AND ADVANCED THREAT RESEARCH

Tactics	Techniques (Top 5 per Tactic)	Comments
Command and Control	Standard Application Layer Protocol	
	Remote File Copy	
	Commonly used Port	
	Web Service	
	Connection Proxy	
Exfiltration	Exfiltration Over Command and Control Channel	
	Automated Exfiltration	
	Exfiltration Over Alternative Protocol	
	Exfiltration to Cloud Storage	
	Scheduled Transfer	
Impact	Resource Hijacking	This technique is often used by Crypto currency mining malware, where a systems resources are being abused to mine crypto currency.
	Data Encrypted for impact	Data encrypted for impact technique can almost solely be attributed by Ransomware. Which remains a top cyber threat, also in Q4 of 2020.
	System Shutdown/ Reboot	
	Firmware corruption	
	Inhibit System Recovery	

TABLE 1. EXPLOIT PUBLIC-FACING APPLICATION; MCAFEE LABS OBSERVED UPTICK IN THE EXPLOIT OF PUBLIC-FACING APPLICATIONS. MULTIPLE REPORTS FROM CISA, NSA WARNED THE INDUSTRY THAT STATE-SPONSORED THREAT ACTORS WERE ACTIVELY LEVERAGING SEVERAL CVES RELATED TO PUBLIC-FACING APPLICATIONS SUCH AS POPULAR REMOTE MANAGEMENT AND VPN SOFTWARE. MCAFEE OBSERVED RANSOMWARE GROUPS – IN ADDITION TO STATE-SPONSORED GROUPS – LEVERAGING THIS INITIAL ACCESS TACTIC. PROCESS INJECTION: MCAFEE LABS HAS ALSO OBSERVED SEVERAL MALWARE FAMILIES AND THREAT GROUPS USING THIS TECHNIQUE. THESE HAVE RANGED FROM RAT TOOLS SUCH AS REMCOS, RANSOMWARE GROUPS SUCH AS REVIL AND MULTIPLE STATE-SPONSORED APT GROUPS. MCAFEE LABS HAS ALSO OBSERVED SEVERAL ATTACKS INVOLVING POWERSHELL.

LETTER FROM OUR CHIEF SCIENTIST

INTRODUCTION

THREATS TO SECTORS AND VECTORS

MALWARE THREATS STATISTICS

SUNBURST MALWARE AND SOLARWINDS SUPPLY CHAIN COMPROMISE

TOP MITRE ATT&CK TECHNIQUES APT/CRIME

RESOURCES

ABOUT MCAFEE

ABOUT MCAFEE LABS AND ADVANCED THREAT RESEARCH

TOP RANSOMWARE FAMILIES AND TECHNIQUES

McAfee observed a 69% increase in new ransomware from Q3 to Q4 of 2020, with Cryptodefense playing a factor in the surge. Data gathered by the McAfee Advanced Threat Research team include:

TOP FAMILIES, MITRE ATT&CK TECHNIQUES, AND PRIMARY SECTORS

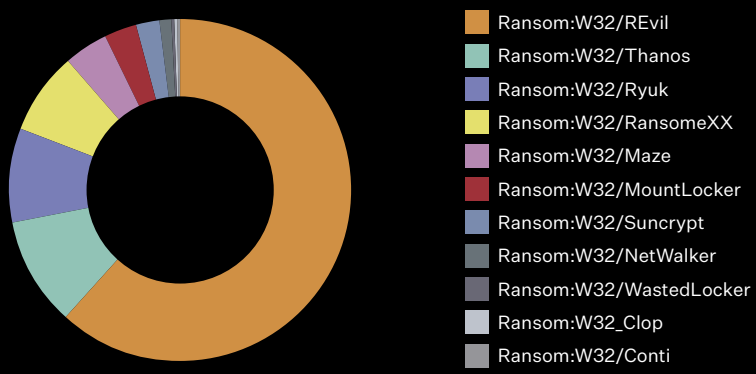
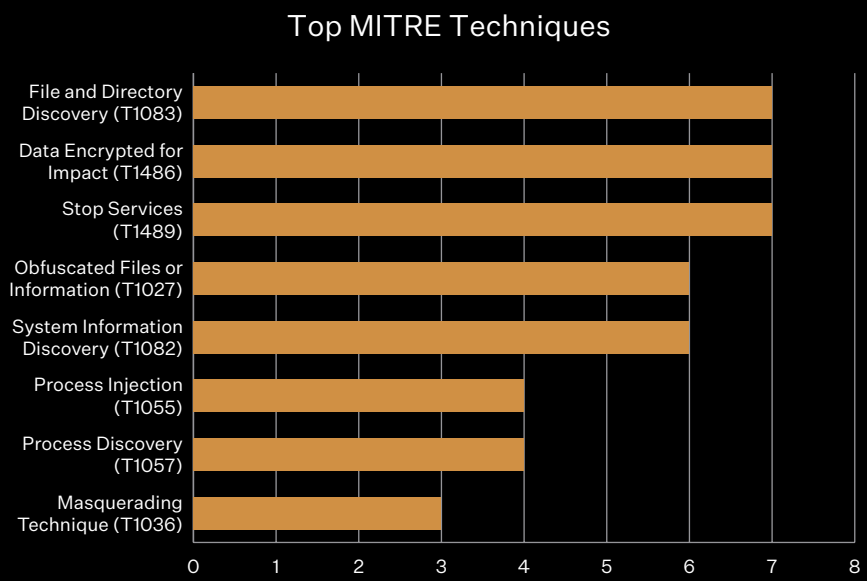


FIGURE 8. THE LIST OF RANSOMWARE FAMILIES OBSERVED IS TOPPED BY REVIL, THANOS, RYUK, RANSOMEXX, AND MAZE

TOP MITRE ATT&CK TECHNIQUES



Source: McAfee Labs, 2020.

FIGURE 9. TOP MITRE ATT&CK TECHNIQUES OBSERVED INCLUDE FILE & DIRECTORY DISCOVERY (T1083), DATA ENCRYPTED FOR IMPACT (T1486), STOP SERVICES (T1489), OBFUSCATED FILES OR INFORMATION (T1027), AND SYSTEM INFORMATION DISCOVERY (T1082)

LETTER FROM OUR CHIEF SCIENTIST
INTRODUCTION
THREATS TO SECTORS AND VECTORS
MALWARE THREATS STATISTICS
SUNBURST MALWARE AND SOLARWINDS SUPPLY CHAIN COMPROMISE
TOP MITRE ATT&CK TECHNIQUES APT/CRIME
RESOURCES
ABOUT MCAFEE
ABOUT MCAFEE LABS AND ADVANCED THREAT RESEARCH

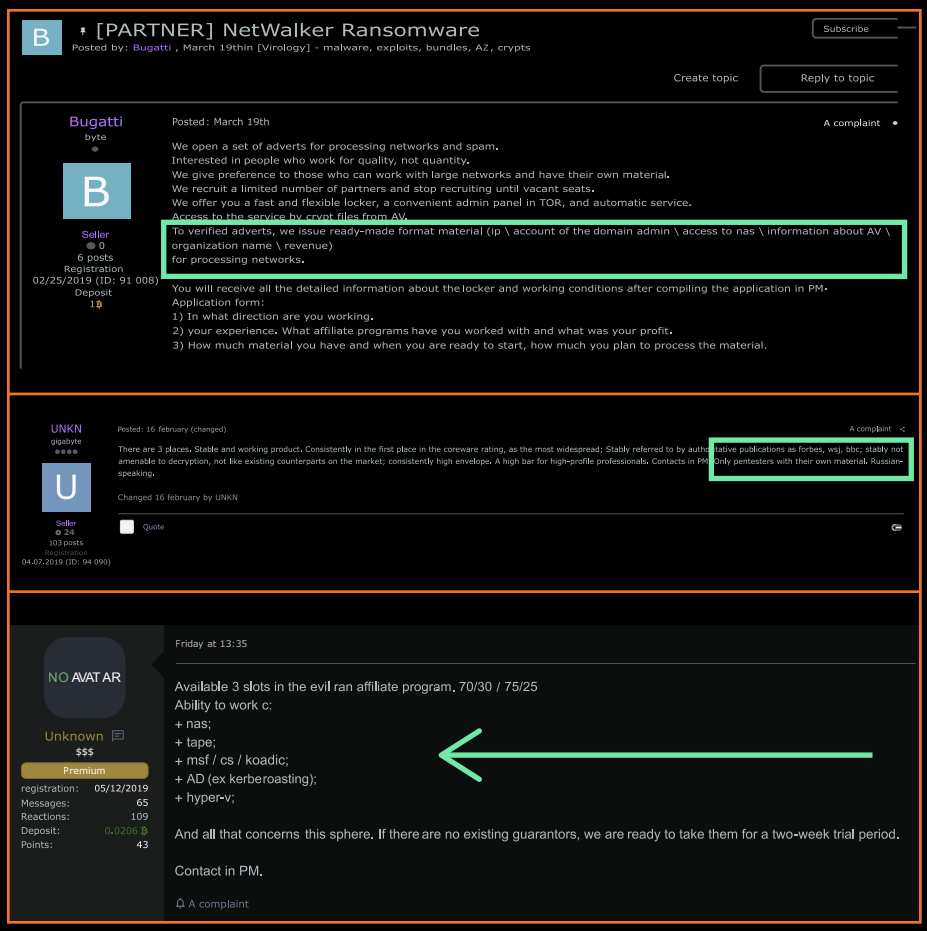


FIGURE 10. THIS IS AN EXAMPLE OF HOW RANSOMWARE GROUPS ARE RECRUITING FOR OTHER TEAMS OR PEN-TESTERS TO GET ACCESS TO CORPORATE NETWORKS. RANSOMWARE GROUPS ARE NO LONGER RELYING ON SPRAY-AND-PAY ATTACKS BUT RATHER SEEKING ACCESS TO HIGH-VALUE TARGETS TO STEAL THEIR INFORMATION BEFORE INFECTING WITH IN THE RANSOMWARE. MORE RANSOMWARE GROUPS ARE LOOKING FOR BAD ACTORS WITH EXPERTISE IN BACKUPS/ESX SERVER.

In Q4 2020, McAfee joined Microsoft and 17 other security firms, tech companies and non-profits to form a new Ransomware Task Force (RTF) to focus on stopping the rising threat of ransomware.

LETTER FROM OUR CHIEF SCIENTIST

INTRODUCTION

THREATS TO SECTORS AND VECTORS

MALWARE THREATS STATISTICS

SUNBURST MALWARE AND SOLARWINDS SUPPLY CHAIN COMPROMISE

TOP MITRE ATT&CK TECHNIQUES APT/CRIME

RESOURCES

ABOUT MCAFEE

ABOUT MCAFEE LABS AND ADVANCED THREAT RESEARCH

RESOURCES

To keep track of the latest threats and research, see these McAfee resources:

McAfee COVID-19 Dashboard—Updated COVID-19 related malicious file detections including countries, verticals, and threat types.

MVISION Insights Preview Dashboard—Explore a preview of the only proactive solution to stay ahead of emerging threats.

McAfee Threat Center—Today's most impactful threats have been identified by our threat research team.

MCAFEE LABS AND RESEARCHERS ON TWITTER

McAfee Labs

Raj Samani

Christiaan Beek

John Fokker

Steve Povolny

Eoin Carroll

Thomas Roccia

Douglas McKee

LETTER FROM OUR CHIEF SCIENTIST

INTRODUCTION

THREATS TO SECTORS AND VECTORS

MALWARE THREATS STATISTICS

SUNBURST MALWARE AND SOLARWINDS SUPPLY CHAIN COMPROMISE

TOP MITRE ATT&CK TECHNIQUES APT/CRIME

RESOURCES

ABOUT MCAFEE

ABOUT MCAFEE LABS AND ADVANCED THREAT RESEARCH

ABOUT MCAFEE

McAfee is the device-to-cloud cybersecurity company. Inspired by the power of working together, McAfee creates business and consumer solutions that make our world a safer place. By building solutions that work with other companies' products, McAfee helps businesses orchestrate cyber environments that are truly integrated, where protection, detection and correction of threats happen simultaneously and collaboratively. By protecting consumers across all their devices, McAfee secures their digital lifestyle at home and away. By working with other security players, McAfee is leading the effort to unite against cybercriminals for the benefit of all.

www.mcafee.com

ABOUT MCAFEE LABS AND ADVANCED THREAT RESEARCH

McAfee Labs, led by McAfee Advanced Threat Research, is one of the world's leading sources for threat research, threat intelligence, and cybersecurity thought leadership. With data from millions of 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.

www.mcafee.com/enterprise/en-us/threat-center/mcafee-labs.html

Subscribe to receive our Threat Information.

McAfee™

6220 America Center Drive
San Jose, CA 95002
888.847.8766
www.mcafee.com