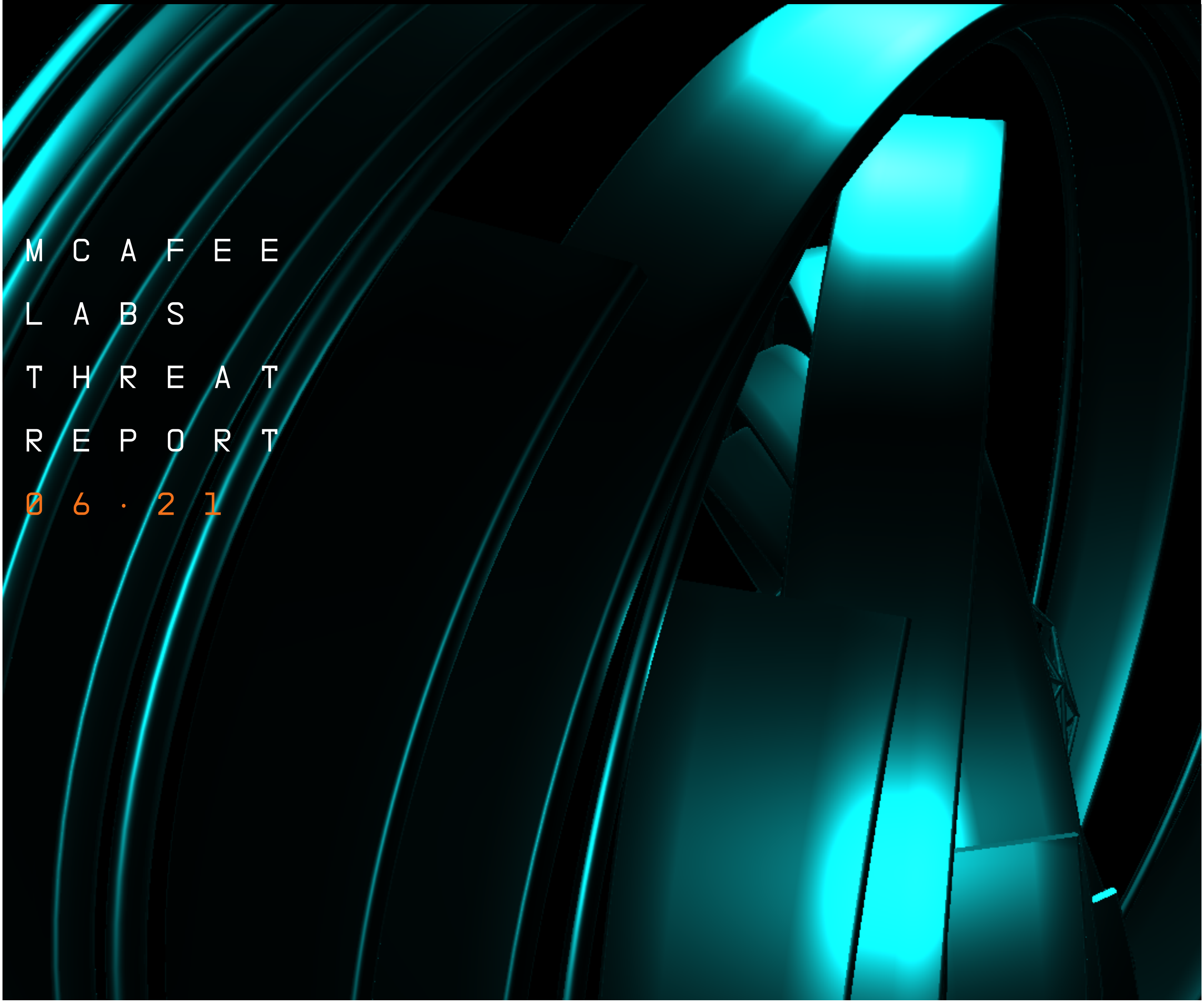


MCAFEE LABS THREAT REPORT

06·21

WRITING & RESEARCH

JUMP TO SECTION

COPIED LINK TO CLIPBOARD.

and of course can be tracked within our MVISION Insights preview dashboard.

This dashboard shows that—beyond the headlines—many more countries have experienced such attacks. What it will not show is that victims are paying the ransoms, and criminals are introducing more Ransomware-as-a-Service (RaaS) schemes as a result. With the five-year anniversary of the launch of the No More Ransom initiative now upon us it's fair to say that we need more global initiatives to help combat this threat.

We hope you enjoy this Threats Report, please stay safe.

—Raj Samani
McAfee Fellow, Chief Scientist

Twitter @Raj_Samani

# RANSOMWARE: FROM BABUK TO DARKSIDE AND BEYOND

While the DarkSide Ransomware-as-a-Service (RaaS) attack on Colonial Pipeline held recent headlines hostage in Q2 2021, the ransomware activity story actually went deeper in the first quarter of the year.

Babuk, Conti, Ryuk, and REvil, preceded DarkSide in establishing 2021 ransomware trends.

We observed that "smaller" ransomware campaigns decreased in Q1 while the Ransomware-as-a-Service campaigns targeted and breached larger organizations and companies. The number of Q1 samples dropped as

more attackers shifted from mass-spread campaigns, toward fewer, but more lucrative targets. Most of these larger, targeted victims received a custom created variant of the ransomware family at a low volume.

Here's a breakdown of McAfee Labs Ransomware research and findings from Q1 of 2021:

DAILY, WEEKLY, MONTHLY RANSOMWARE

COPIED LINK TO CLIPBOARD.

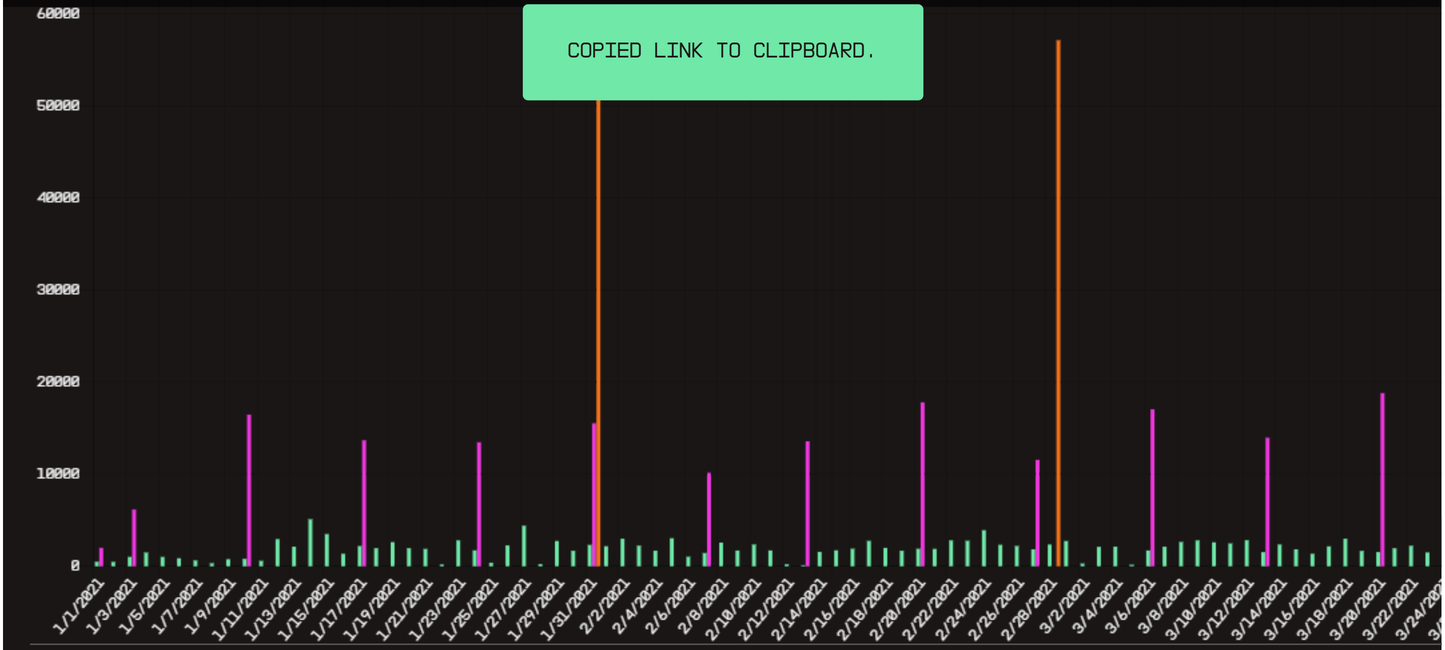
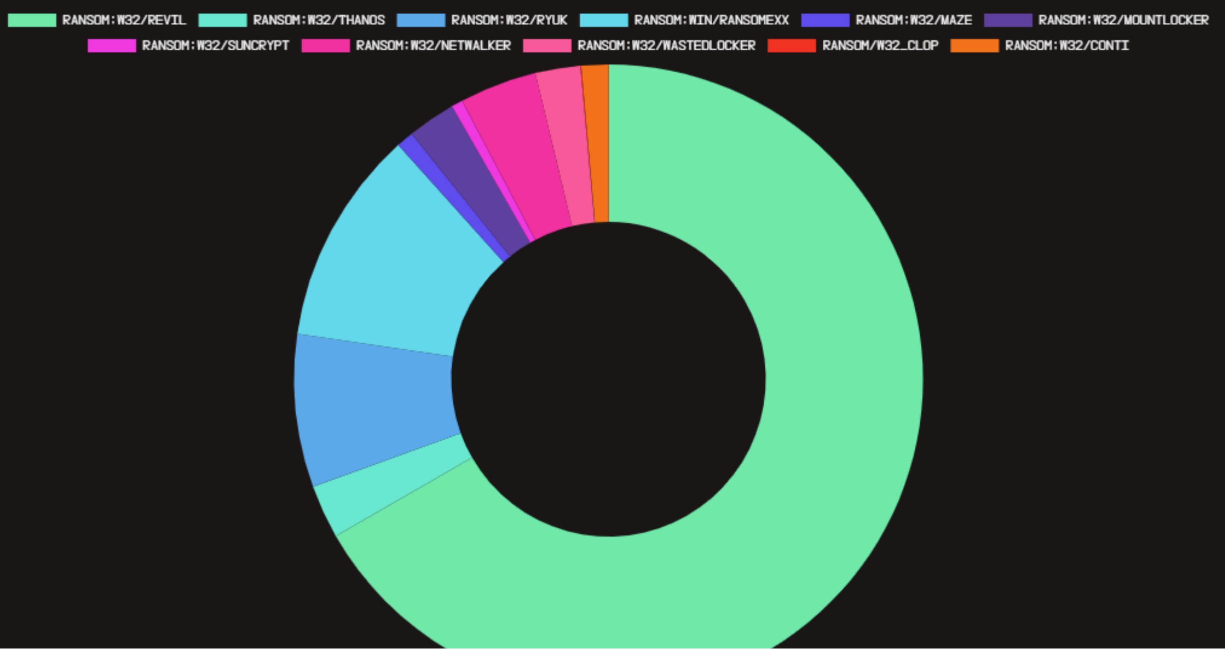


FIGURE 01. A SNAPSHOT OF RANSOMWARE DETECTED AMONG MCAFEE CLIENTS IN Q1 2021 INCLUDES A DAILY HIGH OF 5,634 DETECTIONS ON MARCH 25 AND AN AVERAGE OF 2,417 DETECTIONS PER DAY DURING THE LAST WEEK OF MARCH. THE MOST RANSOMWARE DETECTIONS (18,833) IN Q1 2021 WERE RECORDED IN THE WEEK OF 3/21-3/27. ACCORDING TO THE MONTHLY CHART,THE GREATEST NUMBER OF Q1 RANSOMWARE DETECTIONS WERE RECORDED IN MARCH.

TOP RANSOMWARE FAMILIES AND TECHNIQUES



COPIED LINK TO CLIPBOARD.

FIGURE 02. RANSOMWARE-RELATED MALWARE FAMILIES EVALENCE OF REVIL, RANSOMEXX, AND RYUK PRIOR TO DARKSIDE'S HEADLINEGRABBING HACK OF COLONIAL

UNIQUE RANSOMWARE FAMILIES

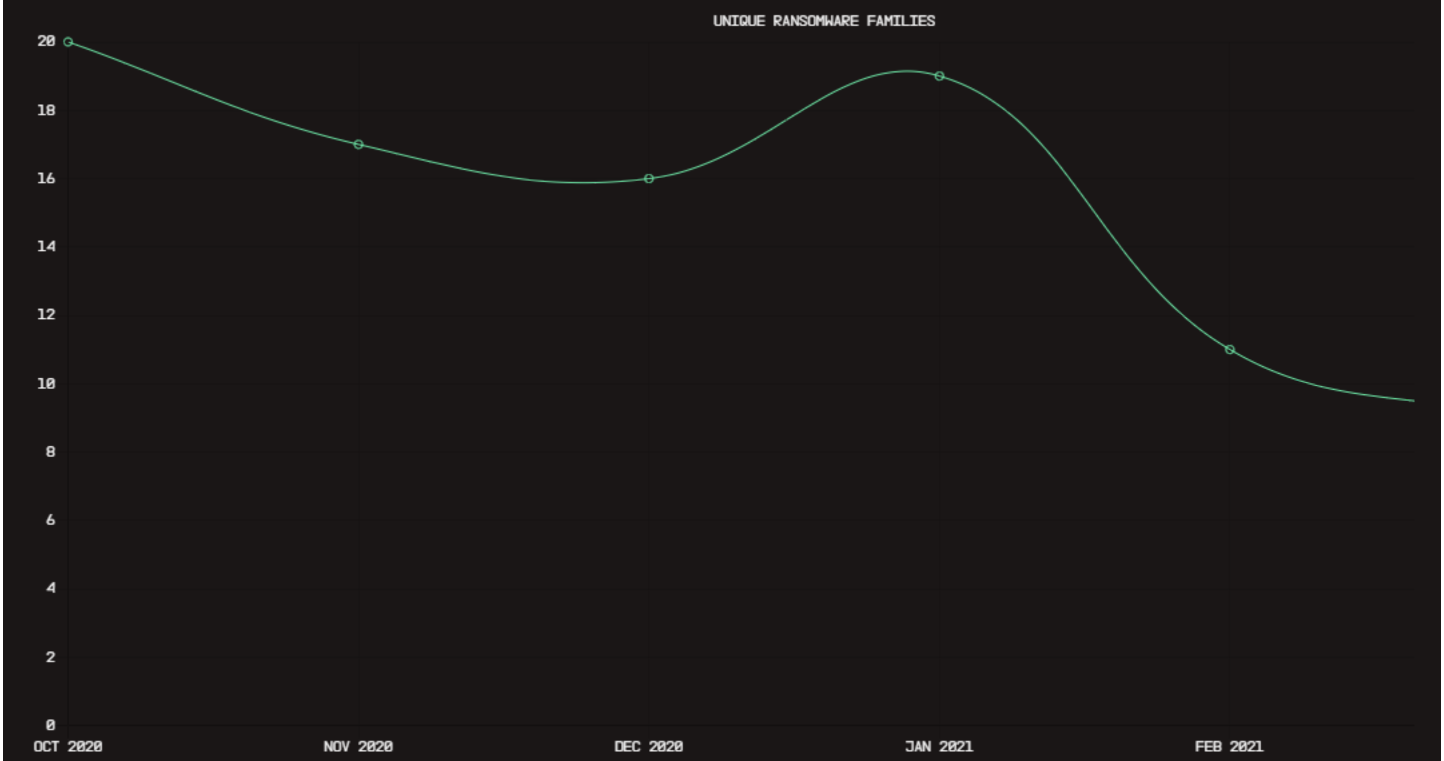


FIGURE 03. THE AMOUNT OF UNIQUE RANSOMWARE FAMILIES DECREASED FROM 19 IN JANUARY 2021 TO 9 IN MARCH 2021, FOLLOWING THE Q1 TREND OF FEWER CAMPAIGNS TARGETING LARGER ORGANIZATIONS AND BUSINESSES WITH POTENTIALLY MORE LUCRATIVE RANSOMS.

RANSOMWARE COVERAGE AND PROTECTION

When it comes to the actual ransomware binary, we strongly advise updating and upgrading your endpoint protection, as well as enabling options like tamper protection and rollback. Please read our blog on how to best configure ENS 10.7 to protect against ransomware for more details.

McAfee is a proud partner of the Ransomware Task Force, which released a details on how ransomware attacks are occurring and countermeasures that should be taken. As many of us have published, presented on, and released research upon, it is time to act.

# MCAFEE GLOBAL THREAT INTELLIGENCE (GTI)

Based on activity from millions of sensors world-wide and an extensive research team, McAfee Labs publishes timely, relevant threat activity via McAfee Global Threat Intelligence (GTI). This always-on, cloudbased threat intelligence service enables accurate protection against known and fast-emerging threats by providing threat determination and contextual reputation metrics. McAfee GTI integrates directly with our security products, protecting against emerging threats to reduce operational efforts and time between detection and containment.

Here are notable statistics from Q1 2021

Here are notable statistics from Q1 2021.

COPIED LINK TO CLIPBOARD.

FILE BY COUNTRY CHARTS

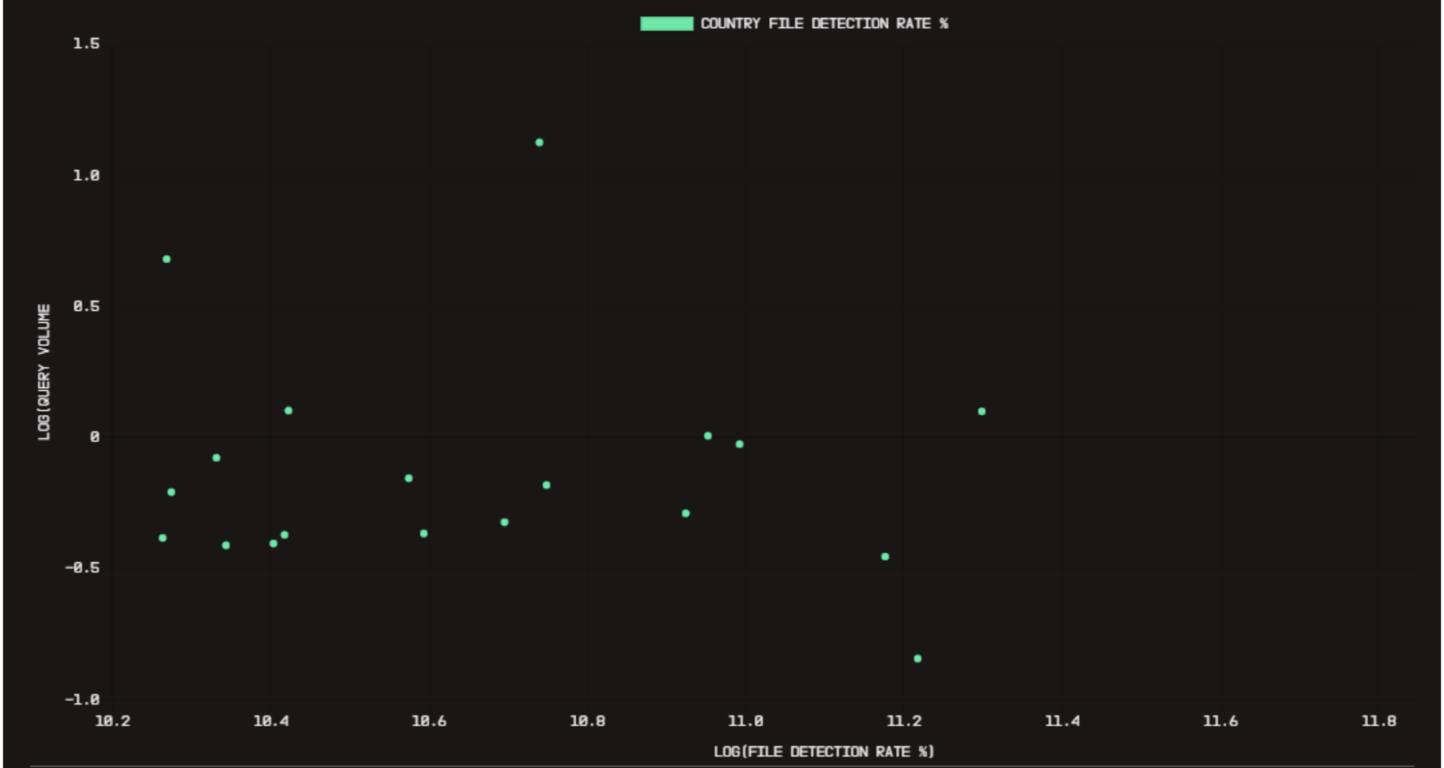


FIGURE 04. IN Q1 2021, THE UNITED STATES HAD THE HIGHEST QUERY VOLUME OF 775 BILLION QUERIES WITH A LOW DETECTION RATE OF 0.31%. OF THE 55 BILLION GTI QUERIES IN RUSSIA, MALWARE WAS DETECTED 13.38% OF THE TIME, RESULTING IN RUSSIAN CUSTOMERS EXPERIENCING THE HIGHEST DETECTION RATE OF MALWARE AMONG THE TOP 20 COUNTRIES. TURKEY HAD THE BIGGEST CHANGE FROM THE PREVIOUS QUARTER WITH A REDUCTION IN DETECTION RATE FROM 9.76% TO 4.8% AND A QUERY VOLUME OF 19 BILLION. JAPAN HAD THE LOWEST DETECTION RATE OF THE COUNTRIES IN THE TOP 20 WHICH WAS 0.14% AND A HIGH NUMBER OF QUERIES WITH 165 BILLION. CHINA HAD A DETECTION RATE OF 1.26% AND THE SECOND HIGHEST QUERY VOLUME OF 199 BILLION.

QUERIES AND DETECTIONS

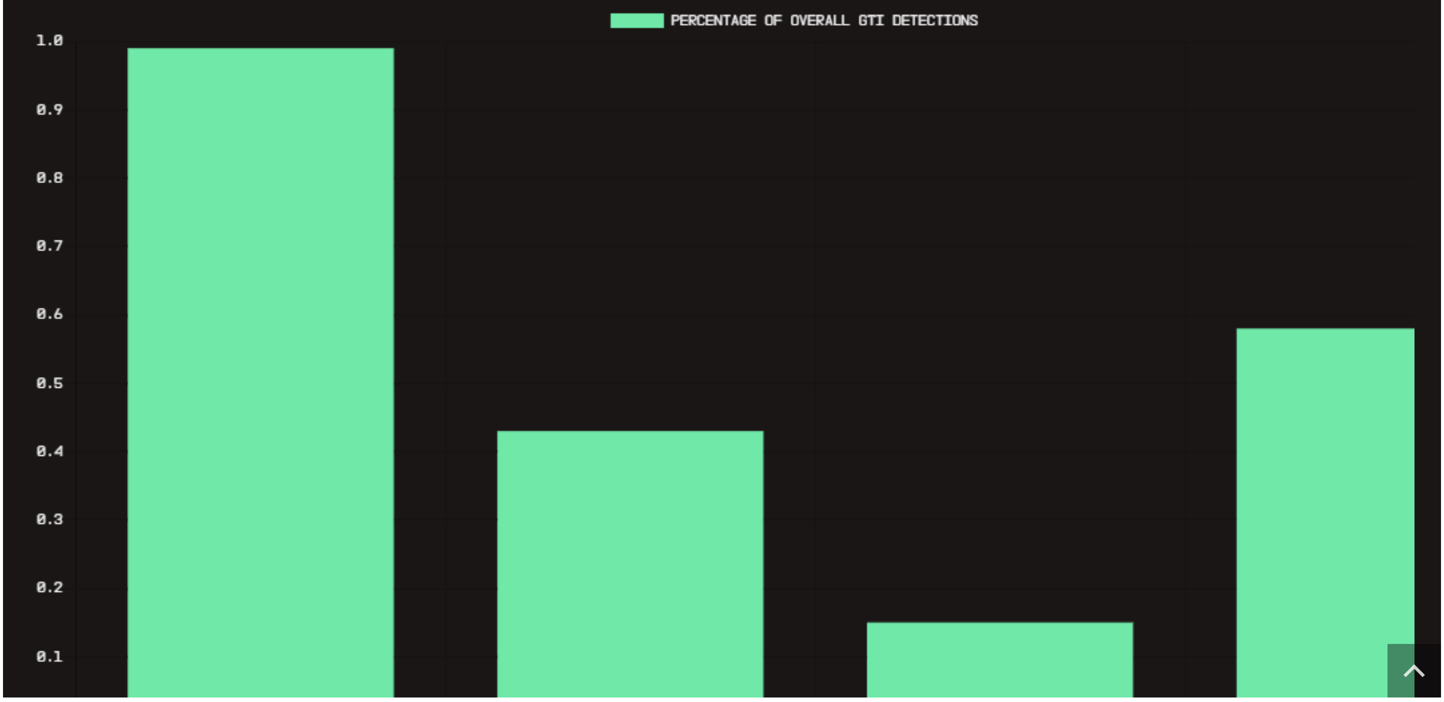


FIGURE 05. IN Q1 2021, THE DAILY AVERAGE OF FIL ETECTION RATE) WHICH INCREASED FROM 243 MILLION (1.03%) IN Q4 2020. IN Q1, THE DAILY AV N DETECTIONS (0.15 % DETECTION RATE) WHICH DECREASED FROM 35 MILLION (0.21%) IN Q4. THE DA WAS 79 MILLION DETECTIONS (0.43% DETECTION RATE) WHICH INCREASED FROM 63 MILLION (0.34%) I

COPIED LINK TO CLIPBOARD.

# THREATS TO SECTORS AND VECTORS

The volume of malware threats observed by McAfee Labs averaged 688 threats per minute, an increase of 40 threats per minute (3%) in the first quarter of 2021.

Notable Sector increases and decreases from Q4 2020 to Q1 2021 include:

- Technology 54%
- Education 46%
- Finance/Insurance 41%
- Wholesale & Retail -76%
- Public Administration -39%

PUBLICLY DISCLOSED SECURITY INCIDENTS

VIEW BY

COUNTRY CONTINENT INDUSTRY VECTOR

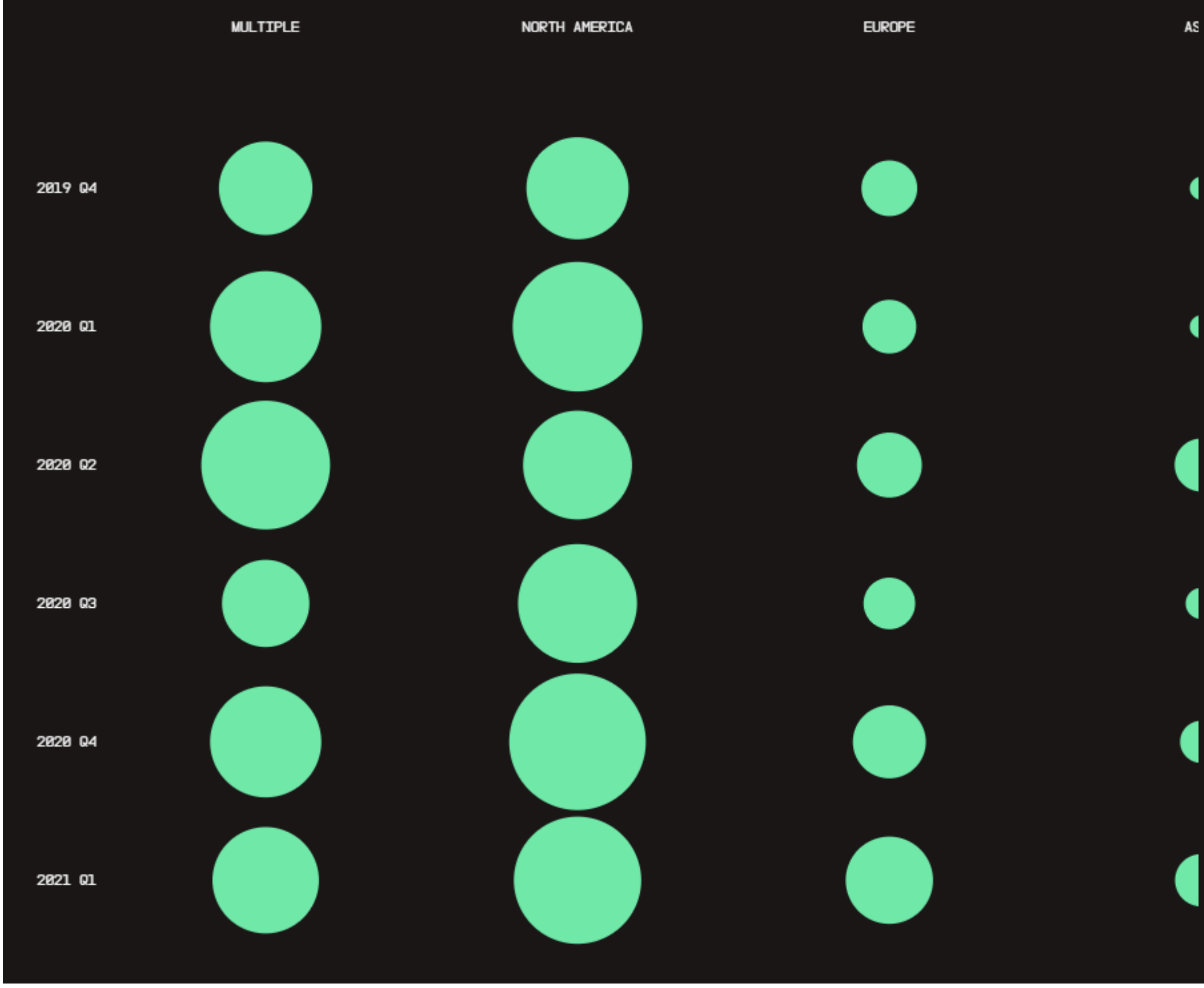


FIGURE 02. PUBLICLY DISCLOSED INCIDENTS SURGED 54% IN ASIA FROM Q4 2020 TO Q1 2021. INCIDENTS INCREASED IN ASIA (54%) AND EUROPE (43%) WHILE DECREASING 1

COPIED LINK TO CLIPBOARD.

# MALWARE THREATS STATISTICS

The first quarter of 2021 saw notable increases in several threat categories:

- Coin Miner malware increased 117% primarily due to growth in 64-bit coin miner applications
- Internet of Things (IoT) surged 55% due to Mirai
- Linux rose 38% along with the increase in Mirai

The first quarter of 2021 also was notable for decreases in several threat categories:

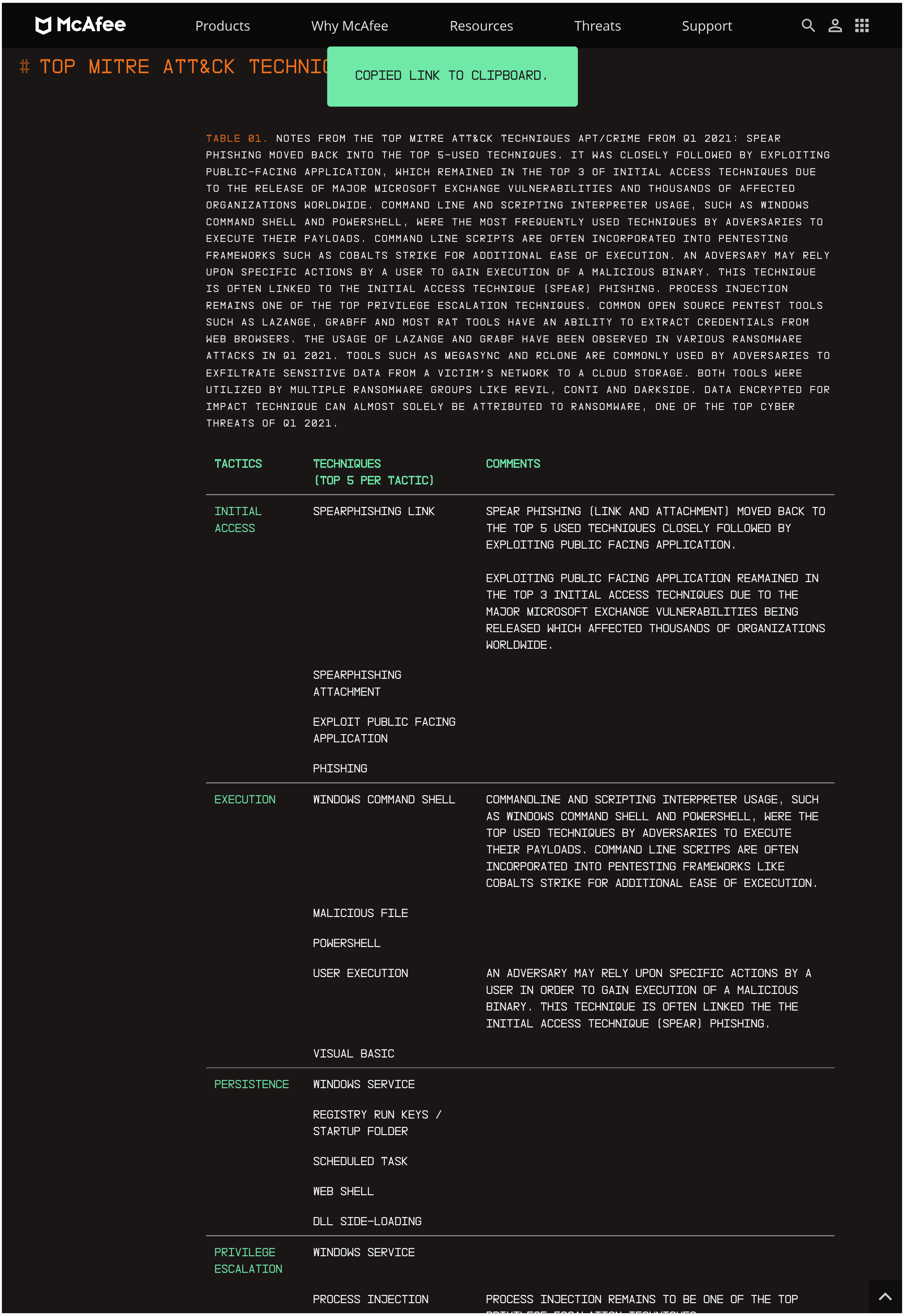
- New PowerShell was down 89% due to the drop in Donoff
- New Office malware decreased 87% also due to the drop in Donoff
- MacOS decreased 70% due to the drop in EvilQuest
- Ransomware fell 50% due to the drop in Cryptodefense

NEW MALWARE THREATS

VIEW

■ STACKED

FIGURE 10. WHILE UNIQUE RANSOMWARE DETECTED IN Q1 2021 DECREASED 50% COMPARED TO Q4 2020 DETECTIONS—IN PART FOLLOWING A DROP IN CRYPTODEFENSE—RANSOMWARE REMAINED A MOST SERIOUS THREAT AGAINST LARGER ORGANIZATIONS AND BUSINESSES IN Q1 AND Q2 2021.



# TOP MITRE ATT&CK TECHNI

COPIED LINK TO CLIPBOARD.

TABLE 01. NOTES FROM THE TOP MITRE ATT&CK TECHNIQUES APT/CRIME FROM Q1 2021: SPEAR PHISHING MOVED BACK INTO THE TOP 5-USED TECHNIQUES. IT WAS CLOSELY FOLLOWED BY EXPLOITING PUBLIC-FACING APPLICATION, WHICH REMAINED IN THE TOP 3 OF INITIAL ACCESS TECHNIQUES DUE TO THE RELEASE OF MAJOR MICROSOFT EXCHANGE VULNERABILITIES AND THOUSANDS OF AFFECTED ORGANIZATIONS WORLDWIDE. COMMAND LINE AND SCRIPTING INTERPRETER USAGE, SUCH AS WINDOWS COMMAND SHELL AND POWERSHELL, WERE THE MOST FREQUENTLY USED TECHNIQUES BY ADVERSARIES TO EXECUTE THEIR PAYLOADS. COMMAND LINE SCRIPTS ARE OFTEN INCORPORATED INTO PENTESTING FRAMEWORKS SUCH AS COBALTS STRIKE FOR ADDITIONAL EASE OF EXECUTION. AN ADVERSARY MAY RELY UPON SPECIFIC ACTIONS BY A USER TO GAIN EXECUTION OF A MALICIOUS BINARY. THIS TECHNIQUE IS OFTEN LINKED TO THE INITIAL ACCESS TECHNIQUE (SPEAR) PHISHING. PROCESS INJECTION REMAINS ONE OF THE TOP PRIVILEGE ESCALATION TECHNIQUES. COMMON OPEN SOURCE PENTEST TOOLS SUCH AS LAZANGE, GRABFF AND MOST RAT TOOLS HAVE AN ABILITY TO EXTRACT CREDENTIALS FROM WEB BROWSERS. THE USAGE OF LAZANGE AND GRABF HAVE BEEN OBSERVED IN VARIOUS RANSOMWARE ATTACKS IN Q1 2021. TOOLS SUCH AS MEGASYNC AND RCLONE ARE COMMONLY USED BY ADVERSARIES TO EXFILTRATE SENSITIVE DATA FROM A VICTIM'S NETWORK TO A CLOUD STORAGE. BOTH TOOLS WERE UTILIZED BY MULTIPLE RANSOMWARE GROUPS LIKE REVIL, CONTI AND DARKSIDE. DATA ENCRYPTED FOR IMPACT TECHNIQUE CAN ALMOST SOLELY BE ATTRIBUTED TO RANSOMWARE, ONE OF THE TOP CYBER THREATS OF Q1 2021.

TACTICS	TECHNIQUES (TOP 5 PER TACTIC)	COMMENTS
INITIAL ACCESS	SPEARPHISHING LINK	SPEAR PHISHING (LINK AND ATTACHMENT) MOVED BACK TO THE TOP 5 USED TECHNIQUES CLOSELY FOLLOWED BY EXPLOITING PUBLIC FACING APPLICATION. EXPLOITING PUBLIC FACING APPLICATION REAMAINED IN THE TOP 3 INITIAL ACCESS TECHNIQUES DUE TO THE MAJOR MICROSOFT EXCHANGE VULNERABILITIES BEING RELEASED WHICH AFFECTED THOUSANDS OF ORGANIZATIONS WORLDWIDE.
	SPEARPHISHING ATTACHMENT	
	EXPLOIT PUBLIC FACING APPLICATION	
	PHISHING	
EXECUTION	WINDOWS COMMAND SHELL	COMMANDLINE AND SCRIPTING INTERPRETER USAGE, SUCH AS WINDOWS COMMAND SHELL AND POWERSHELL, WERE THE TOP USED TECHNIQUES BY ADVERSARIES TO EXECUTE THEIR PAYLOADS. COMMAND LINE SCRITPS ARE OFTEN INCORPORATED INTO PENTESTING FRAMEWORKS LIKE COBALTS STRIKE FOR ADDITIONAL EASE OF EXCECUTION.
	MALICIOUS FILE	
	POWERSHELL	
	USER EXECUTION	AN ADVERSARY MAY RELY UPON SPECIFIC ACTIONS BY A USER IN ORDER TO GAIN EXECUTION OF A MALICIOUS BINARY. THIS TECHNIQUE IS OFTEN LINKED THE THE INITIAL ACCESS TECHNIQUE (SPEAR) PHISHING.
	VISUAL BASIC	
PERSISTENCE	WINDOWS SERVICE	
	REGISTRY RUN KEYS / STARTUP FOLDER	
	SCHEDULED TASK	
	WEB SHELL	
	DLL SIDE-LOADING	
PRIVILEGE ESCALATION	WINDOWS SERVICE	
	PROCESS INJECTION	PROCESS INJECTION REMAINS TO BE ONE OF THE TOP

COPIED LINK TO CLIPBOARD.

TACTICS	TECHNIQUES	COMMENTS
	(REGISTRY RUN KEYS)/ ST	PRIVILEGE ESCALATION TECHNIQUES.
	SC	
	PROCESS HOLLOWING	
DEFENSE EVASION	DEOBFUSCATE/DECODE FILES OR INFORMATION	
	OBFUSCATED FILES OR INFORMATION	
	SOFTWARE PACKING	
	PROCESS INJECTION	
	FILE DELETION	
	MODIFY REGISTRY	
CREDENTIAL ACCESS	KEYLOGGING	
	CREDENTIALS FROM WEB BROWSERS	COMMON OPENSOURCE PENTEST TOOLS LIKE LAZANGE, GRABFF AND MOST RAT TOOLS HAVE AN ABILITY TO EXTRACT CREDENTIALS FROM WEB BROWSERS. THE USAGE OF LAZANGE AND GRABFF HAVE BEEN OBESERVED IN VARIOUS RANSOMWARE ATTACKS IN Q1 2021.
	BRUTE FORCE	
	OS CREDENTIAL DUMPING	
	CREDENTIALS FROM PASSWORD STORES	
DISCOVERY	SYSTEM INFORMATION DISCOVERY	
	FILE AND DIRECTORY DISCOVERY	
	PROCESS DISCOVERY	
	SYSTEM NETWORK CONFIGURATION DISCOVERY	
	SYSTEM OWNER/USER DISCOVERY	
LATERAL MOVEMENT	REMOTE FILE COPY	
	REMOTE DESKTOP PROTOCOL	
	SMB/WINDOWS ADMIN SHARES	
	EXPLOITATION OF REMOTE SERVICES	
	SSH	
COLLECTION	DATA FROM LOCAL SYSTEM	
	SCREEN CAPTURE	
	KEYLOGGING	
	ARCHIVE COLLECTED DATA	
	CLIPBOARD DATA	
COMMAND AND CONTROL	WEB PROTOCOLS	
	INGRESS TOOL TRANSFER	

TACTICS	TECHNIQUES (TOP 5 PER TACTIC)	COMMENTS
	STANDARD ENCODING	
	SYMMETRIC CRYPTOGRAPHY	
	AP PR	
EXFILTRATION	EXFILTRATION OVER COMMAND AND CONTROL CHANNEL	
	EXFILTRATION OVER ALTERNATIVE PROTOCOL	
	AUTOMATED EXFILTRATION	
	EXFILTRATION OVER UNENCRYPTED/OBFUSCATION NON-C2 PROTOCOL	
	EXFILTRATION TO CLOUD STORAGE	TOOLS LIKE MEGASYNC AND RCLONE ARE COMMONLY USED BY ADVERSARIES TO EXFILTRATE SENSITIVE DATA FROM A VICTIM'S NETWORK TO A CLOUD STORAGE. BOTH TOOLS WERE UTILIZED BY MULTIPLE RANSOMWARE GROUPS LIKE REVIL, CONTI, DARKSIDE.
IMPACT	DATA ENCRYPTED FOR IMPACT	
	RESOURCE HIJACKING SERVICE	
	SYSTEM SHUTDOWN/REBOOT	
	DIRECT NETWORK FLOOD	

COPIED LINK TO CLIPBOARD.

DOWNLOAD PDF

READ ARCHIVED REPORTS

McAfee™

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.

COPIED LINK TO CLIPBOARD.

TWITTER

McAfee Labs

Raj Samani

Christiaan Beek

John Fokker

Steve Povolny

Eoin Carroll

Thomas Roccia

Douglas McKee

CREDITS

Design & Code
Patrick Altair McDonald

Interactive Graphs
Kenneth Ormandy

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,

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.

MCAFEE LABS AND ADVANCED THREAT RESEARCH

SUBSCRIBE TO RECEIVE OUR THREAT INFORMATION.

COPIED LINK TO CLIPBOARD.

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.

New to McAfee?

What Is MVISION?
Cloud Security Products
Endpoint Protection Products
Explore Products
Explore Services
Skyhigh
Skyhigh Networks

Resources

Enterprise Support
Product Downloads
Product Documentation
Shop Online
Renew Products
Partner Portal Login
Free Trials
Free Tools

Connect with Us

Contact Us
Find a Partner
Partners
MPOWER
Events
Webinars

About McAfee

About Us
Latest News
Diversity & Inclusion
Investors
Careers
Blogs

United States / English
Privacy | Legal | Terms of Service | Site Map |

COPIED LINK TO CLIPBOARD.