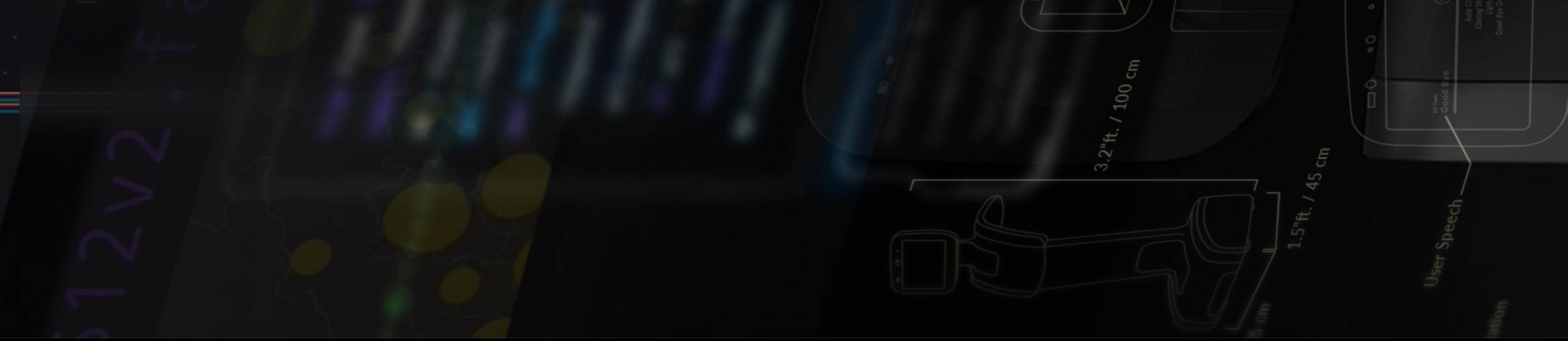
REPORT

McAfee™

# ADVANCED THREAT RESEARCH REPORT

OCT.2021


3.2”ft. / 100 cm
1.5”ft. / 45 cm
User Speech

## چکیده مدیریتی

به شماره جدید گزارش McAfee Enterprise Advanced Threat Research خوش آمدید.

در این گزارش میزان فراوانی تهدیدات سایبری و اهداف آنها در ماه‌های اخیر مورد بررسی قرار گرفته است.

در حالی به ماه‌های پایانی سال ۲۰۲۱ نزدیک می‌شویم که مهاجمان با تهدیدات و تاکتیک‌های جدید و دائما در حال تکامل خود صنایع مختلف را هدف قرار می‌دهند.

حملات باج‌افزاری همچنان در حال گسترش هستند و کسب‌وکار آنها با میلیون‌ها دلار اخاذی از شرکت‌های بزرگ تا کوچک هر روز پررونق‌تر از قبل می‌شود.

در اواسط سال ۲۰۲۱ که DarkSide و REvil پس از حملاتی پرسروصدا فعالیت خود را متوقف کردند، BlackMatter خیلی زود توانست تا جای خالی آنها را پر کند. بر اساس شواهد موجود برخی منابع معتقدند که BlackMatter نسخه جدیدی از DarkSide است؛ اگر چه این موضوع از سوی گردانندگان BlackMatter رد شده است.

باج‌افزار قدیمی دیگر که نگارش متفاوتی از آن در ماه‌های اخیر منتشر شد LockBit 2.0 است. LockBit 2.0 نگارشی به‌روز شده از نسخه ۲۰۲۰ باج‌افزار LockBit است که با قابلیت‌های جدید قادر به اجرا امور مخربی از جمله رمزگذاری دستگاه‌ها در سطح دامنه و سرقت داده‌ها است.

سه‌ماهه دوم ۲۰۲۱ دوره‌ای پرتلاطم برای حملات باج‌افزاری به برخی سازمان‌ها و شرکت‌های مطرح بود. در پی اختلالات و بحران‌های ناشی از حمله گردانندگان باج‌افزار DarkSide به خط لوله شرکت کولونیال، تأثیرات مخرب و بالقوه فاجعه‌بار حملات باج‌افزاری بیش از هر زمانی روشن شد. فشارهای سیاسی پس از آن و تلاش‌های نهادهای امنیتی، موجب توقف فعالیت DarkSide شد. چندین گروه دیگر از گردانندگان تهدیدات سایبری نیز اعلام کردند تا برای در امان ماندن از چنین فشارهایی، از حمله به برخی حوزه‌های خاص خودداری خواهند کرد. اندکی بعد، دو تالار گفتگوی اینترنتی معروف هکرها به نام‌های XSS و Exploit، تبلیغات باج‌افزاری را در سایت خود ممنوع کردند. برای سالها این تالارها، بهشتی امن برای تبهکاران سایبری و گردانندگان باج‌افزاری برای فروش خدمات RaaS، تبادل اطلاعات سرقت‌شده و بسیاری امور مخرب دیگر بود. به نظر می‌رسد که این اقدام مدیران XSS و Exploit تلاشی برای بقای این تالارهای گفتگو در برابر فشارهای دولتی و نهادهای قانونی بوده که بر اثر حملات گسترده باج‌افزاری ماه‌های گذشته تشدید شده است. با این حال همان‌طور که در این گزارش خواهید خواند همچنان تالارهای متعددی هستند که گردانندگان باج‌افزار بی‌محابا در آنها جولان می‌دهند.

در بخشی از این گزارش، متداول‌ترین تاکتیک‌ها و تکنیک‌های MITRE ATT&CK که در سه‌ماهه دوم سال ۲۰۲۱ توسط گروه‌های مختلف از مهاجمان استفاده شدند نیز به تفصیل مورد بررسی قرار گرفته است.

این گزارش، منبعی باارزش در مطالعات و تحقیقات در حوزه تهدیدات سایبری است. آمار و اطلاعات ارائه شده در این گزارش، بر پایه شبکه جهانی McAfee Enterprise متشکل از بیش از یک میلیارد حسگر (Sensor) و بررسی‌ها و رصدهای مستمر متخصصان این شرکت است.

*گروه تحقیق و توسعه*
*شرکت مهندسی شبکه گستر - اولین شرکت فعال در حوزه ضدویروس در ایران*
*www.shabakeh.net*

We’ve shifted new focus to prevalence. In other words, the team is now paying attention to how often do we see the threat in the globe, and more importantly who does it target?

## LETTER FROM OUR CHIEF SCIENTIST

Welcome to a NEW Threat Report, and a NEW Company.

So much has changed since our last threat report. We learned that despite a rebrand the DarkSide ransomware group did not walk away and thought we would miss the (alleged) connection to BlackMatter! Not only that but our recent findings into infusion pumps demonstrates the importance of security research (more on this later in the report!).

As for the team and I, we made our move to McAfee Enterprise, a newly dedicated Enterprise Cybersecurity company, which means we will no longer publish our work under McAfee Labs. But don’t worry, you can still find us on our new McAfee Enterprise ATR Twitter feed: @McAfee_ATR.

Of course, the changes are more substantial than a simple Twitter feed, and some of these are reflected in our new threat report. We’ve shifted focus to prevalence. In other words, the team is now paying attention to how often do we see the threat around the globe, and more importantly who does it target? These findings are backed up with additional analysis, which will be detailed in the report to incorporate active research against threat actors, as well as the vulnerabilities they are currently exploiting now and potentially in the future.

We hope you enjoy this new format and welcome your feedback about what you loved and were less enthusiastic about. More importantly, what would you like to see in the future?

Please do keep in touch.

*—Raj Samani*

*McAfee Enterprise Chief Scientist and Fellow*

Twitter @Raj_Samani

## WRITING AND RESEARCH

Christiaan Beek
Ashley Dolezal
John Fokker
Melissa Gaffney
Tracy Holden
Tim Hux
Phillippe Laulheret
Douglas McKee
Lee Munson
Chris Palm
Tim Polzer
Steve Povolny
Raj Samani
Pankaj Solanki
Leandro Velasco

## RANSOMWARE

### RANSOMWARE'S INCREASING PREVALENCE

As 2021 progressed through its second quarter and into the third, cyber criminals introduced new—and updated—threats and tactics in campaigns targeting prominent sectors. Ransomware campaigns maintained their prevalence while evolving their business models to extract valuable data and millions in ransoms from enterprises big and small.

DarkSide's highly publicized attack on Colonial Pipeline's gas distribution dominated cybersecurity headlines in May. MVISION Insights quickly identified DarkSide's early prevalence of targets within the United States, primarily Legal Services, Wholesale and Manufacturing, Oil, Gas, and Chemical sectors.

Shutting down a major U.S. gas supply chain grabbed the attention of public officials and Security Operations Centers but equally concerning were other ransomware groups operating similar affiliate models. Ryuk, REvil, Babuk, and Cuba ransomware actively deployed business models supporting others' involvement to exploit common entry vectors and similar tools. These, and other groups and their affiliates, exploit common entry vectors and, in many cases, the tools we see being used to move within an environment are the same. Not long after DarkSide's attack, the REvil gang stole the spotlight using a Sodinokibi payload in its ransomware attack on Kaseya, a global IT infrastructure provider. REvil/Sodinokibi topped our list of ransomware detections in Q2 of 2021.

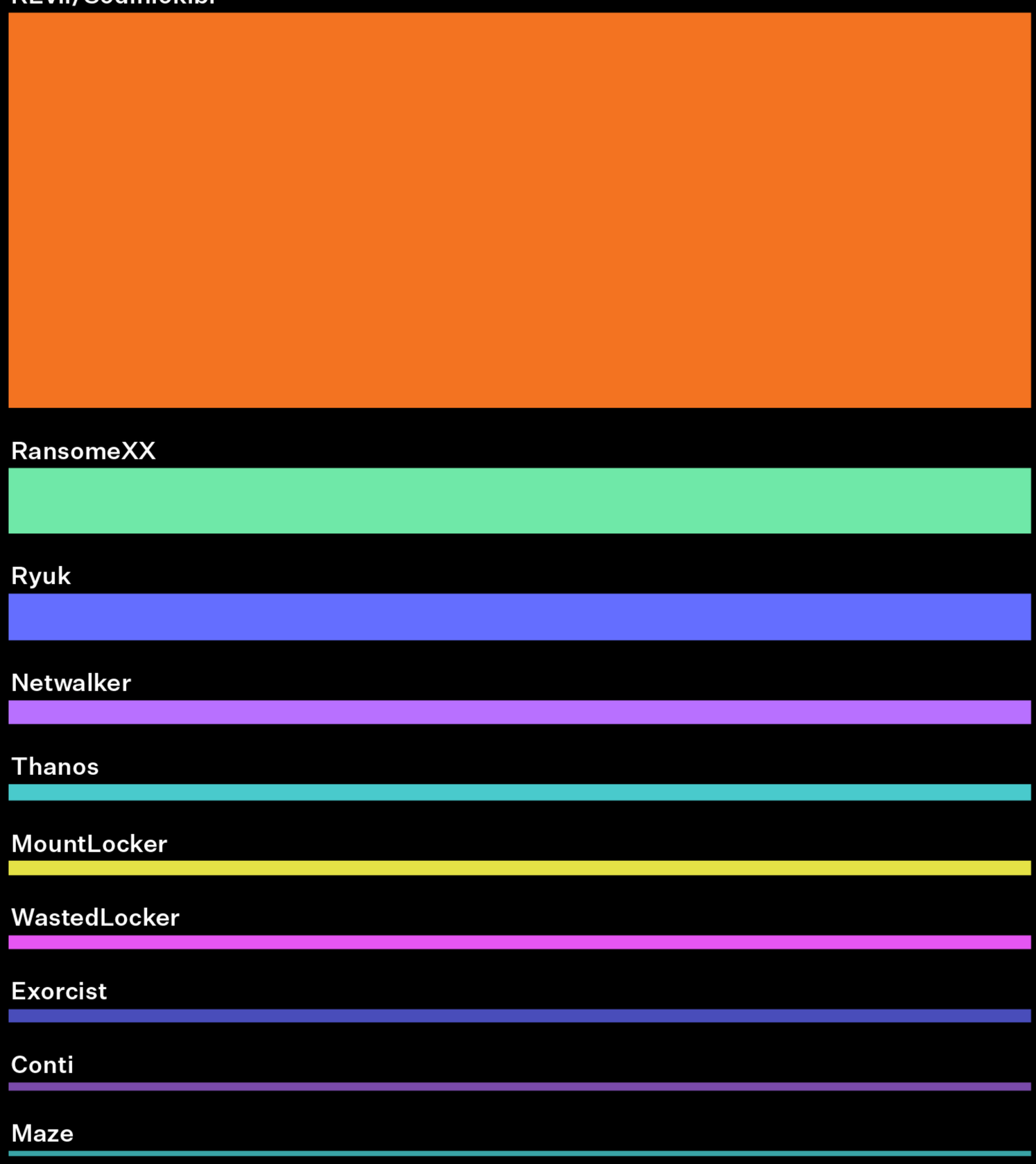



FIGURE 1. REVIL/SODINOKIBI TOPPED OUR RANSOMWARE DETECTIONS IN Q2 OF 2021, ACCOUNTING FOR 73% OF OUR TOP-10 RANSOMWARE DETECTIONS.

While DarkSide and REvil stepped back into the shadows after their high-profile attacks, an heir to DarkSide emerged in July. BlackMatter Ransomware surfaced primarily in Italy, India, Luxembourg, Belgium, the United States, Brazil, Thailand, the United Kingdom, Finland, and Ireland as a Ransomware-as-a-Service affiliate program incorporating elements from DarkSide, REvil, and Lockbit Ransomware. Based on the code similarity of the binary and their resemblance of their public page to DarkSide, it is common consensus that BlackMatter Ransomware is most likely a continuation of DarkSide Ransomware—which BlackMatter has denied.

Another “old” ransomware with a twist was discovered in mid-2021. LockBit 2.0 Ransomware is an updated version of 2020’s LockBit with new features that automatically encrypt devices across the domain, exfiltrates data and accesses systems over RDP, as well as the ability to recruit new affiliates from inside a target enterprise.

Ransomware developers introduced new campaigns as well. The Hive ransomware family was first observed in June of 2021 with prevalence in India, Belgium, Italy, the United States, Turkey, Thailand, Mexico, Germany, Colombia, and Ukraine, operating as a Ransomware-as-a-Service written in Go language compromising healthcare and critical infrastructure organizations.

Our team takes a deeper dive into ransomware including an unexpected reaction among underground forums, targeted sectors and the delta between open-source intelligence and telemetry.

## THRIVING RANSOMWARE EXPELLED FROM UNDERGROUND FORUMS

The second quarter of 2021 was a vibrant quarter for ransomware earning its place as a high-profile cyber agenda item for the U.S. administration, but things have also shifted in the historically safe cybercriminal underground forums.

The impact of a ransomware attack became very clear when the Colonial Pipeline was forced to shut down by a DarkSide ransomware attack. This abrupt halt in the supply chain affected much of the eastern U.S., creating a frantic consumer run on fuel. The attack and resulting consumer and economic impact showed the true lethality of ransomware and grabbed the full attention of security authorities.

The political response to the impact of the Colonial Pipeline attack caused the DarkSide ransomware group to abruptly halt its operation. Several additional threat groups announced they would vet future targets and exclude certain sectors.

A week later, two of the most influential underground forums, XSS and Exploit, announced a ban on ransomware advertisements. For years, these same forums provided a safe haven for cybercrime and the ransomware boom that sparked a lively trade in breached networks, Stealer logs, and Crypter services among others. Considering that many of the threat actors behind the major ransomware families are career criminals and often have a close relationship with forum administrators and moderators, we believe that this gesture was done to save the existence of the forums.

Even though the ransomware associated online personas were banned, our team has observed that the threat actors are still active on several forums under different other personas.

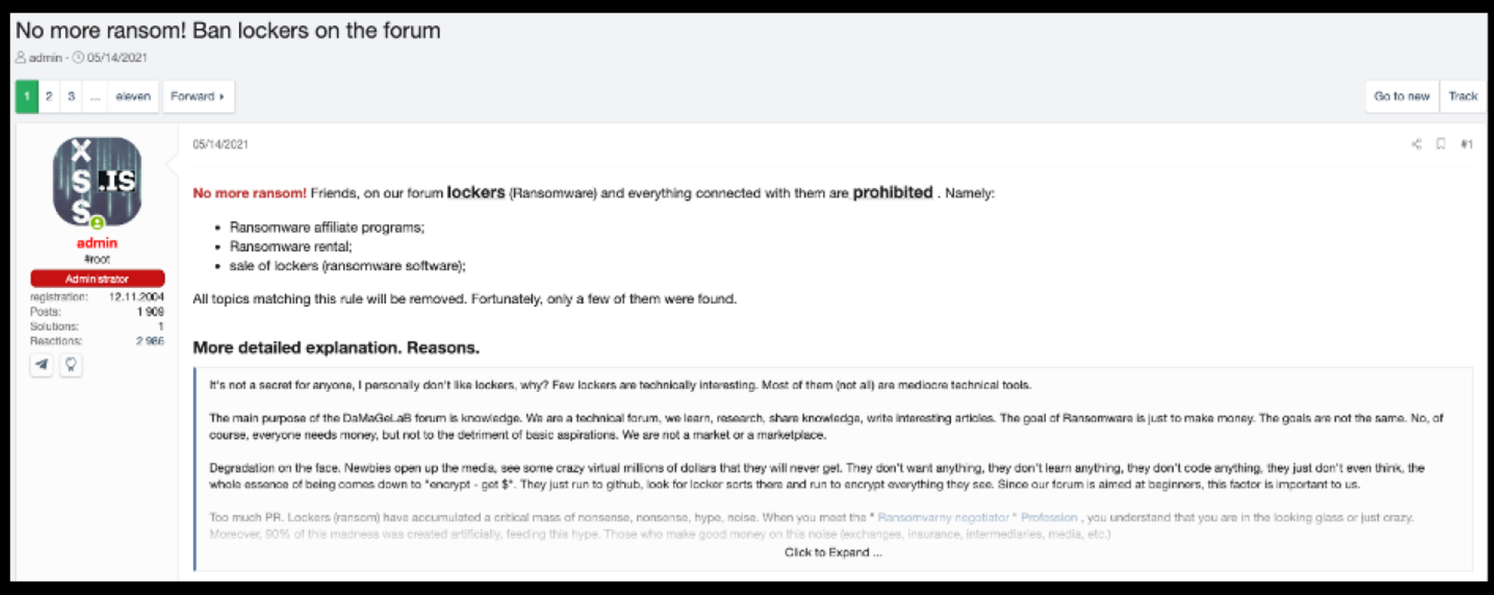



FIGURE 2. THE ADMIN OF XSS CALLING FOR THE BAN ON RANSOMWARE

During this period, the Babuk ransomware group was going through their own issues, one of which, a defect *nix ESXi locker, we have described extensively in our blog.

Ultimately the Babuk team's internal struggles led to a separation and the start of a new forum dedicated to ransomware known as RAMP, where many of ransomware-focused cyber criminals now gather to do business and share TTPs. Despite the ban on some of the larger cybercriminal forums, ransomware has shown no indication of slowing down and still must be considered as one of the most impactful cyberthreats any size organization can face.

## RANSOMWARE TARGET SECTORS: THE DELTA OF DATA BETWEEN OPEN-SOURCE INTELLIGENCE AND TELEMETRY

Many ransomware crews have portals in which they announce the victims they have breached and samples of data they have gathered, to force the victims to pay the ransom, otherwise their data will be leaked and, in some cases, sold. Leak sites are showcases of failed negotiations and do not reflect the full extent of attacks executed by the ransomware crews, however insights into reported sectors and geo's are interesting data to observe.

Our team monitors many of those pages and gathers the ransomware family name, maps victim to sector and country. Gathering this data and compile, we observe the following ransomware families targeting the below top 10 sectors in the United States:

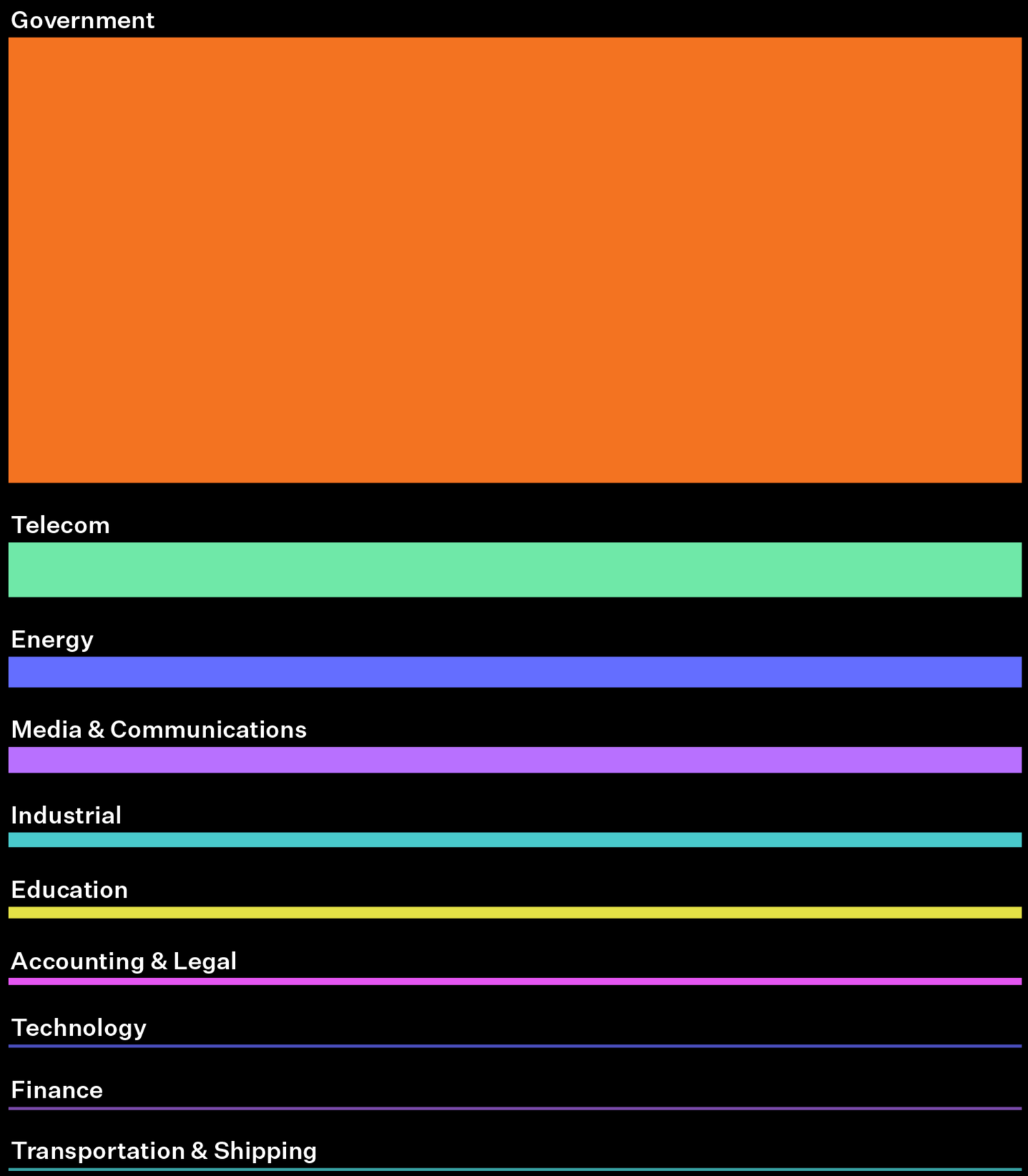



FIGURE 3. GOVERNMENT WAS THE SECTOR MOST TARGETED BY RANSOMWARE IN Q2 OF 2021, FOLLOWED BY TELECOM, ENERGY, AND MEDIA & COMMUNICATIONS.

Our telemetry point of view, gathered from U.S. sensors, mapped ransomware activity observed and against the Open-Source Intelligence (OSINT) reported sectors:

| Telemetry Reported Sectors | OSINT Reported Sectors |
|---|---|
| Government | Manufacturing |
| Finance | Retail |
| Education | Healthcare |
| Telecom | Construction |
| Energy | Transportation |
| Media | Education |
| Industrial | Business |
| Real-Estate | Legal |
| Legal | Finance |
| Tech | IT |

TABLE 1. THE MORE DISTANCE BETWEEN THE TWO SECTORS, THE BETTER THEY ARE PROTECTED; THE CLOSER THE DISTANCE, THE MORE THE SECTOR NEEDS TO PAY ATTENTION TO THE RISK OF RANSOMWARE.

What does the difference mean? What is the delta? From our telemetry perspective, we observe ransomware activity that has been detected and blocked in the sector where we have customers. Identifying Government as the No. 1 targeted sector in our telemetry reveals the many attempts targeted toward this sector, that are NOT successful. In the OSINT-reported sectors, we observe that sectors requiring high demands on IT service capabilities to support critical business services are high on the target list of ransomware crews.

## MITRE ATT&CK PATTERNS/TECHNIQUES USED BY RANSOMWARE FAMILIES: Q2 2021

### ATTACK PATTERN/TECHNIQUE

1. Data Encrypted for Impact
2. File and Directory Discovery
3. Obfuscated Files or Information
4. Process Injection
5. Deobfuscate/Decode Files or Information
6. Process Discovery
7. Inhibit System Recovery
8. PowerShell
9. System Information Discovery
10. Modify Registry

TABLE 2. DATA ENCRYPTED FOR IMPACT WAS THE MOST DETECTED ATTACK PATTERN IN Q2 2021.

## B BRAUN: UNCOVERING VULNERABILITIES IN GLOBALLY USED INFUSION PUMP

The medical industry is faced with unique security challenges. Potential attacks on medical centers could amount to an even bigger threat than a system-wide ransomware assault. Our team, in partnership with Culinda, discovered a set of vulnerabilities in B. Braun Infusomat Space Large Pump and the B. Braun SpaceStation.

Our research led us to discover five previously unreported vulnerabilities in the medical system which include:

1. CVE-2021-33886: Use of Externally-Controlled Format String (CVSS 7.7)
2. CVE-2021-33885: Insufficient Verification of Data Authenticity (CVSS 9.7)
3. CVE-2021-33882: Missing Authentication for Critical Function (CVSS 8.2)
4. CVE-2021-33883: Cleartext Transmission of Sensitive Information (CVSS 7.1)
5. CVE-2021-33884: Unrestricted Upload of File with Dangerous Type (CVSS 5.8)

Together, these vulnerabilities could be used by a malicious actor to modify a pump's configuration while the pump is in standby mode, resulting in an unexpected dose of medication being delivered to a patient on its next use—all with zero authentication.

Shortly after our team reported our initial findings to B. Braun, the company responded and worked with our team to adopt the mitigations we outlined in our disclosure report.

These findings present an overview and some technical detail of the most critical attack chain along with addressing unique challenges faced by the medical industry. For a brief summary, please see our blog.

# CLOUD THREATS

## CLOUD THREAT PREVALENCE

The challenges of shifting cloud security to accommodate a more flexible pandemic workforce while still maintaining and even increasing workloads presented cybercriminals even more potential exploits and targets in Q2 of 2021.

Our team's cloud threat research found that Financial Services faced the greatest challenge against cloud threat campaigns in Q2 of 2021.

### MOST COMMON CLOUD THREATS Q2 2021

1. Excessive Usage From Anomalous Location
2. Insider Data Exfiltration
3. Privilege Access Misuse
4. High Risk Data Exfiltration
5. Privilege Access Exfiltration
6. Land Expand Exfiltration
7. Suspicious Superhuman
8. Data Exfiltration by Privileged User

TABLE 3. **EXCESSIVE USAGE FROM ANOMALOUS LOCATION** DEFINITION: THE USER HAS ACCESSED OR DOWNLOADED A VERY LARGE VOLUME OF DATA WITHIN A SHORT SPAN OF TIME. THIS IS SEVERE BECAUSE 1) ENTERPRISE USERS HAVE PREVIOUSLY NEVER ACCESSED SUCH A LARGE VOLUME, AND 2) DATA VOLUME IS HIGH EVEN WHEN REFERENCED TO A LARGE POOL OF USERS. **EXCESSIVE USAGE FROM ANOMALOUS LOCATION** THREATS RANKED HIGHEST AMONG GLOBAL CLOUD THREATS, FOLLOWED BY **INSIDER DATA EXFILTRATION** AND **PRIVILEGE ACCESS MISUSE**. **EXCESSIVE USAGE FROM ANOMALOUS LOCATION** COMPOSED 62% OF THREATS RECORDED.

### GLOBAL TARGETED CLOUD VERTICAL Q2 2021

#### ENTERPRISE

1. Financial Services
2. Healthcare
3. Manufacturing
4. Retail
5. Professional Services
6. Travel & Hospitality
7. Software & Internet
8. Technology
9. Computers & Electronics
10. Non-Profit Organization

TABLE 4. **FINANCIAL SERVICES** WERE TARGETED MOST AMONG REPORTED CLOUD INCIDENTS, FOLLOWED BY **HEALTHCARE**, **MANUFACTURING**, **RETAIL**, AND **PROFESSIONAL SERVICES**. CLOUD INCIDENTS TARGETING THE **FINANCIAL SERVICES** ACCOUNTED FOR 33% OF THE TOP 10 INDUSTRIES REPORTED, FOLLOWED BY **HEALTHCARE** AND **MANUFACTURING** (8%).

VERTICAL TOTAL CLOUD INCIDENTS GLOBAL & U.S. Q2 2021

| GLOBAL CLOUD VERTICAL | COUNTRY |
|---|---|
| 1. Financial Services | U.S. |
| 2. Financial Services | Singapore |
| 3. Healthcare | U.S. |
| 4. Retail | U.S. |
| 5. Professional Services | U.S. |
| 6. Financial Services | China |
| 7. Manufacturing | U.S. |
| 8. Financial Services | France |
| 9. Retail | Canada |
| 10. Financial Services | Australia |

TABLE 5. **FINANCIAL SERVICES** WERE GLOBALLY TARGETED IN 50% OF THE TOP 10 CLOUD INCIDENTS OF Q2 2021 INCLUDING INCIDENTS IN THE **UNITED STATES**, **SINGAPORE**, **CHINA**, **FRANCE**, **CANADA**, AND **AUSTRALIA**. CLOUD INCIDENTS TARGETING VERTICALS IN THE **UNITED STATES** ACCOUNTED FOR 34% OF INCIDENTS RECORDED IN THE TOP 10 COUNTRIES.

UNITED STATES CLOUD VERTICAL

1. Financial Services
2. Healthcare
3. Retail
4. Professional Services
5. Manufacturing
6. Media & Entertainment
7. Travel & Hospitality
8. Government
9. Software & Internet
10. Educational Services

TABLE 6. **FINANCIAL SERVICES** WERE THE TOP TARGET OF CLOUD THREAT INCIDENTS IN THE U.S. IN Q2 OF 2021. INCIDENTS TARGETING **FINANCIAL SERVICES** REPRESENTED 29% OF TOTAL CLOUD INCIDENTS AMONG TOP 10 SECTORS.

### VERTICAL CLOUD INCIDENTS BY COUNTRY: Q2 2021

| COUNTRY |
| --- |
| 1. United States |
| 2. India |
| 3. Australia |
| 4. Canada |
| 5. Brazil |
| 6. Japan |
| 7. Mexico |
| 8. Great Britain |
| 9. Singapore |
| 10. Germany |

TABLE 7. THE MOST CLOUD INCIDENTS TARGETING COUNTRIES WERE REPORTED IN THE UNITED STATES FOLLOWED BY INDIA, AUSTRALIA, CANADA, AND BRAZIL. CLOUD INCIDENTS TARGETING THE UNITED STATES ACCOUNTED FOR 52% OF INCIDENTS RECORDED IN THE TOP 10 COUNTRIES.



## THREATS TO COUNTRIES, CONTINENTS, SECTORS AND VECTORS

### COUNTRIES & CONTINENTS: Q2 2021

Notable country and continent increases of publicly reported incidents in the second quarter of 2021 include:

- The **United States** experienced the most reported incidents in Q2 2021.
- **Europe** saw the largest increases in reported incidents in Q2 with 52%.

### ATTACK SECTORS: Q2 2021

Notable increases of publicly reported incidents against sectors in the second quarter of 2021 include:

- Multiple Industries were targeted most often.
- Notable sector increases include **Public** (64%) and **Entertainment** (60%).

### ATTACK VECTORS: Q2 2021

Notable increases of publicly reported incidents against vectors in the second quarter of 2021 include:

- **Malware** was the technique used most often in reported incidents in Q2 2021.
- **Spam** showed the highest increase of reported incidents—250%—from Q1 to Q2 2021, followed by **Malicious Script** with 125% and **Malware** with 47%.

## TOP MITRE ATT&CK TECHNIQUES Q2 2021

| Tactics | Techniques (Top 5 per Tactic) | Comments |
|---|---|---|
| Initial Access | Spearphishing Attachment | Spear Phishing (Link and Attachment) is sharing the top 3 Initial Access Techniques with Exploiting Public facing Application. |
| | Exploit Public-Facing Application | |
| | Spearphishing Link | |
| | Valid Accounts | |
| | External Remote Services | |
| Execution | Windows Command Shell | This Quarter we have observed several attacks making use of PowerShell or the Windows Command shell to execute either malware in memory or to make use of dual-use/non-Malicous tools to aid their network exploitation attempts. Command line scripts are often incorporated into Pentesting frameworks like Cobalts Strike for additional ease of excecution. |
| | PowerShell | |
| | Malicious File | |
| | Windows Management Instrumentation | |
| | Shared Modules | |
| Persistence | Registry Run Keys/ Startup Folder | |
| | Scheduled Task | |
| | Windows Service | |
| | Valid Accounts | |
| | DLL Side-Loading | |
| Privilege Escalation | Registry Run Keys/ Startup Folder | |
| | Process Injection | Process injection remains to be one of the top Privilege Escalation techniques. |
| | Scheduled Task | |
| | Windows Service | |
| | Portable Executable Injection | |
| Defense Evasion | Deobfuscate/Decode Files or Information | |
| | Obfuscated Files or Information | |
| | Modify Registry | |
| | System Checks | |
| | File Deletion | |

| Tactics | Techniques (Top 5 per Tactic) | Comments |
|---|---|---|
| Credential Access | Keylogging | Keylogging and gathering credentials from web browsers are common functionalities of most Remote Access Trojans (RATs). |
| | Credentials from Web Browsers | |
| | OS Credential Dumping | This technique is the core functionality of the credential harvesting tool Mimikatz, which ATR has observed in many of the analyzed Campaigns in Q2. |
| | Input Capture | |
| | LSASS Memory | |
| Discovery | System Information Discovery | |
| | File and Directory Discovery | |
| | Process Discovery | |
| | System Checks | |
| | Query Registry | |
| Lateral Movement | Remote Desktop Protocol | |
| | Exploitation of Remote Services | |
| | Remote File Copy | |
| | SMB/Windows Admin Shares | |
| | SSH | |
| Collection | Screen Capture | Several campaigns involving Remote Administration Trojan (RAT) took place in Q2. Screen capture was a technique deployed by many of the RAT malware variants. |
| | Keylogging | |
| | Data from Local System | |
| | Clipboard Data | |
| | Archive Collected Data | |
| Command and Control | Web Protocols | |
| | Ingress Tool Transfer | |
| | Non-Standard Port | |
| | Web Service | |
| | Non-Application Layer Protocol | |

| Tactics | Techniques (Top 5 per Tactic) | Comments |
|---|---|---|
| Exfiltration | Exfiltration Over Command and Control Channel | |
| | Exfiltration Over Alternative Protocol | |
| | Exfiltration to Cloud Storage | Ransomware Threat actors continued to exfiltrate victim data to different cloud storage providers. Mostly done by the use of commercial like RClone and MegaSync. |
| | Automated Exfiltration | |
| | Exfiltration Over Unencrypted/ Obfuscation Non-C2 Protocol | |
| Impact | Data Encrypted for Impact | Encrypting data for impact is yet again the most technique across the campaigns and threats examined by ATR. During this quarter several Ransomware families have launched a Linux based locker that targets ESXi servers, increasing the use of this technique even more. |
| | Inhibit System Recovery | Inhibit system recovery is a technique often used by ransomware gangs before they deliver the final payload. By deleting the Volume Shadow Copies, they make it harder for victims to recover from the attack. |
| | Resource Hijacking | |
| | Service Stop | |
| | System Shutdown/ Reboot | |

TABLE 8. NOTES FROM THE TOP MITRE ATT&CK TECHNIQUES APT/CRIME FROM Q2 2021.

## HOW TO DEFEND AGAINST THESE THREATS

In the second quarter of 2021 we saw, and commented on, many different types of threats. Fortunately, we also have the advice and products to keep you and/or your organization protected, for instance:

Learn how configuring ENS 10.7, tamper protection, and Rollback can protect against Cuba ransomware, or dive into our detailed blog written with defenders in mind.

Brush up on how you can block all those annoying popups from your browser and how our customers are protected from malicious sites via Web Advisor and Web Control.

Read how scammers impersonate Windows Defender to push malicious Windows apps, along with our safety tips for dealing with that. Customers will be pleased to know that Real Protect Cloud proactively protects them via machine learning while Web Advisor and Web Control customers are protected from known malicious sites.

Learn the best practices for securing and monitoring your network against one of the more notorious ransomwares seen this quarter, DarkSide. Additionally, this blog also offers a wealth of information on coverage and protection, covering EPP, MVISION Insights, EDR, and ENS.

Finally, find out why virtual machines are so valuable to cybercriminals and why affected VMware users should patch immediately. For those who cannot install patches straight away we offer practical tips and a reminder that our Network Security Platform offers signatures for the CVEs in question.

## RESOURCES

To keep track of the latest threats and research, see our team's resources:

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.

## TWITTER

Raj Samani

Christiaan Beek

John Fokker

Steve Povolny

Douglas McKee

شبکه گستر

خدمات اطلاع رسانی و آگاه‌سازی

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