Trellix

# THE THREAT REPORT

Summer 2022

Presented by Trellix Threat Labs

# TABLE OF CONTENTS


3 LETTER FROM OUR LEAD SCIENTIST

5 EVOLUTION OF RUSSIAN CYBERCRIME

7 METHODOLOGY

7 RANSOMWARE STATISTICS: Q1 2022

11 CRITICAL FLAWS IN BUILDING ACCESS CONTROL SYSTEMS

13 PREVALENT THREAT STATISTICS: Q1 2022

14 CALL TO ACTION: CONNECTED HEALTHCARE CYBERSECURITY

15 LIVING OFF THE LAND: Q1 2022

17 NATION-STATE STATISTICS: Q1 2022

18 EMAIL SECURITY TRENDS: Q1 2022

20 THREATS TO COUNTRIES CONTINENTS, SECTORS, AND VECTORS: Q1 2022

20 BUG REPORT

22 EPPS SCORE

23 WRITING AND RESEARCH

23 RESOURCES

The first quarter of 2022 in cybersecurity was more about evolution than revolution. The techniques and prevalence of ransomware attacks advanced while Russian cyberattacks continued a slow-building evolution fed by the continuing conflict in Ukraine. Our latest Trellix Threat Report includes our findings from Q1 2022 and other vital research including the evolution of Russian cybercrime, ransomware in the United States, and email security trends. We also share our team's recent research into vulnerabilities found in building access control systems, and risks unique to connected healthcare.

## LETTER FROM OUR LEAD SCIENTIST

Welcome to our latest threat report.

When we started the journey with Trellix, we knew merging two major backends would give us a tremendous cyberthreat perspective of what's happening in the world. This edition includes a new category providing our readers more insights into what kind of threats are being observed from an email perspective.

We enjoyed seeing so many of you at RSA where we released and presented several pieces of our research ranging from an overview of attacks observed in the Ukraine to vulnerabilities we discovered in medical devices and building access control technology. This report highlights this research and other prevalent threats and attacks observed in the wild as well as and our data and findings from the first quarter of 2022.


LETTER FROM OUR LEAD SCIENTIST

EVOLUTION OF RUSSIAN CYBERCRIME

METHODOLOGY

RANSOMWARE STATISTICS: Q1 2022

CRITICAL FLAWS IN BUILDING ACCESS CONTROL SYSTEMS

PREVALENT THREAT STATISTICS: Q1 2022

CALL TO ACTION: CONNECTED HEALTHCARE CYBERSECURITY

LIVING OFF THE LAND: Q1 2022

NATION-STATE STATISTICS: Q1 2022

EMAIL SECURITY TRENDS: Q1 2022

THREATS TO COUNTRIES, CONTINENTS, SECTORS, AND VECTORS: Q1 2022

BUG REPORT

EPPS SCORE

WRITING AND RESEARCH

RESOURCES

When we're at Black Hat, DEFCON, RSA, and other conferences, we appreciate the kind words and feedback we receive for our threat report. Don't be a stranger between conferences and always feel free to reach out to us on our socials if you have a suggestion or missed information.

Until next time, please check out our Trellix Threat Labs blog page featuring our latest threat content, videos, and research.

— *Christiaan Beek*
Lead Scientist

Twitter @ChristiaanBeek


LETTER FROM OUR LEAD SCIENTIST

EVOLUTION OF RUSSIAN CYBERCRIME

METHODOLOGY

RANSOMWARE STATISTICS: Q1 2022

CRITICAL FLAWS IN BUILDING ACCESS CONTROL SYSTEMS

PREVALENT THREAT STATISTICS: Q1 2022

CALL TO ACTION: CONNECTED HEALTHCARE CYBERSECURITY

LIVING OFF THE LAND: Q1 2022

NATION-STATE STATISTICS: Q1 2022

EMAIL SECURITY TRENDS: Q1 2022

THREATS TO COUNTRIES, CONTINENTS, SECTORS, AND VECTORS: Q1 2022

BUG REPORT

EPPS SCORE

WRITING AND RESEARCH

RESOURCES

## THE EVOLUTION OF RUSSIAN CYBERCRIME

Per public attribution, Russian cybercriminal groups have always been active. Their tactics, techniques, and procedures (TTPs) have not significantly evolved over time, although some changes have been observed. Lately, the threat landscape has changed, as multiple domains have partially merged. This trend was already on-going, but the increased digital activity further accelerated and exposed said trend.

Trellix has historically had a significant customer base in Ukraine and when the cyberattacks targeting the country intensified, we coordinated closely with government and industry partners to provide greater visibility into the evolving threat landscape. We have been eager to support the region against malicious cyber activity and have been able to go beyond sharing knowledge to also provide a wide range of security appliances at no cost in the affected region (our special thanks go out to our partners at Mandiant in getting some of the appliances deployed at those organizations who needed protection the most).

To support our customers and the people of Ukraine, Trellix Threat Labs coordinated with multiple government institutions to provide them with the necessary telemetry insights, intelligence briefings and analysis of the malware tools used by Russian actors. A large portion of Trellix's efforts were performed in discretion as protection of our customers is our highest priority. In coordination with RSA, our Trellix Threat Labs team released our research (Growling Bears Make Thunderous Noise) on the Russian cybercriminal evolutions over time, the impact of a (cyber) war, and observed organization and activity.

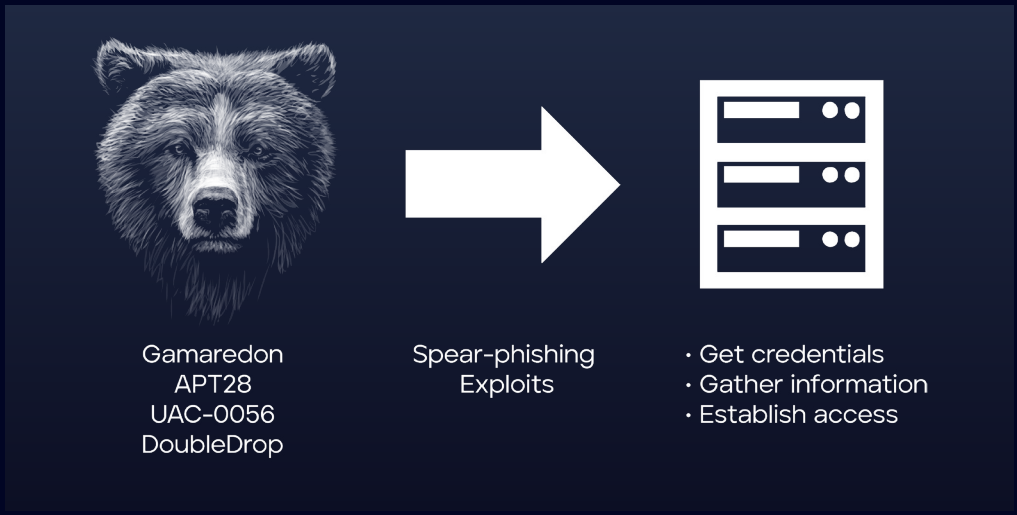



Figure 1: Initial attack techniques used by observed groups

LETTER FROM OUR LEAD SCIENTIST

EVOLUTION OF RUSSIAN CYBERCRIME

METHODOLOGY

RANSOMWARE STATISTICS: Q1 2022

CRITICAL FLAWS IN BUILDING ACCESS CONTROL SYSTEMS

PREVALENT THREAT STATISTICS: Q1 2022

CALL TO ACTION: CONNECTED HEALTHCARE CYBERSECURITY

LIVING OFF THE LAND: Q1 2022

NATION-STATE STATISTICS: Q1 2022

EMAIL SECURITY TRENDS: Q1 2022

THREATS TO COUNTRIES, CONTINENTS, SECTORS, AND VECTORS: Q1 2022

BUG REPORT

EPPS SCORE

WRITING AND RESEARCH

RESOURCES

The report includes detailed research not only on the impact of post-Russian invasion cyberwar, but also on many cyber groups and campaigns associated with the conflict:

- Phishing the Ukrainian Ministry of Defense
- Gamaredon
- Wipers
- Targeted exchange servers
- UAC-0056
- APT28
- DoubleDrop

Read more on the evolution of Russian cybercrime in the full report.

## METHODOLOGY

Trellix's backend systems are providing telemetry that we use as input for our quarterly threat reports. We combine our telemetry with open-source intelligence around threats and our own investigations into prevalent threats like ransomware, nation-state activity, etc.

When we talk about telemetry, we talk about detections, not infections. A detection is recorded when a file, URL, IP address or other indicator is detected by one of our products and reported back to us.

Privacy of our customers is key. It also is important when it comes down to telemetry and mapping that out to the sectors and countries of our customers. Client-base per country differs and number could be showcasing increases while we have to look deeper into the data to explain. An example: The Telecom sector often scores high in our data. It doesn't necessarily mean this sector is highly targeted. The Telecom sector contains ISP providers as well that own IP-address spaces that can be bought by companies. What does that mean? Submissions from the IP-address space of the ISP are showing up as Telecom detections but could be from ISP clients that are in a different sector operating.


LETTER FROM OUR LEAD SCIENTIST

EVOLUTION OF RUSSIAN CYBERCRIME

METHODOLOGY

RANSOMWARE STATISTICS: Q1 2022

CRITICAL FLAWS IN BUILDING ACCESS CONTROL SYSTEMS

PREVALENT THREAT STATISTICS: Q1 2022

CALL TO ACTION: CONNECTED HEALTHCARE CYBERSECURITY

LIVING OFF THE LAND: Q1 2022

NATION-STATE STATISTICS: Q1 2022

EMAIL SECURITY TRENDS: Q1 2022

THREATS TO COUNTRIES, CONTINENTS, SECTORS, AND VECTORS: Q1 2022

BUG REPORT

EPPS SCORE

WRITING AND RESEARCH

RESOURCES

## U.S. RANSOMWARE: Q1 2022

In the beginning of 2022, we were optimistic when news came out that the Russian FSB had arrested several members of the REvil ransomware gang in Russia. Based on our analysis these affiliates played a minor role within the crime group, nevertheless, we were hopeful that this fragile hint of cooperation would lead to more arrests in Russia.

With the Russian invasion of Ukraine at the end of January 2022, we now know that this was wishful thinking. The war became a catalyst for cybercriminals to split up. Historically, politics were often set aside by cybercriminals, and we suspected we may see RU and UA ransomware criminals working together for financial gain.

The choosing of sides became most evident with Conti ransomware gang when they publicly expressed their support for the Russian administration and their actions.

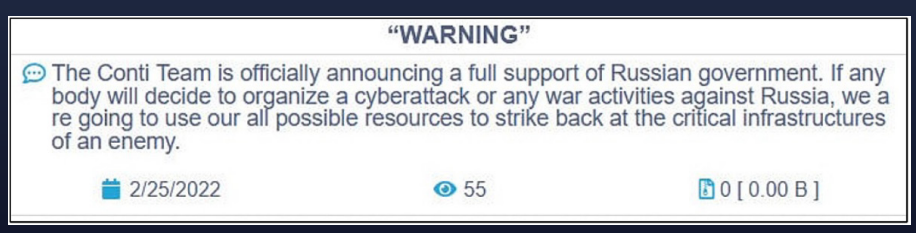



Figure 2: Conti expressing their support to the Russian administration

This public statement did not go unnoticed and within a few days an anonymous researcher using the twitter handle @contileaks began publishing Conti's internal communications online. The chats spanned across several years and consisted of thousands of messages that we dubbed this the "Panama Papers of Ransomware."

Trellix has examined the leaked chats extensively and published a very extensive blog that is well worth the read. Highlights we found in the chats included their public statement supporting the Russian administration and a possible close relationship between the Conti leadership and the Russian intelligence services. These ties support the findings from the report; "In the Crosshairs: Organizations and Nation-State Cyber Threats" which we published earlier this year in collaboration with CSIS. One of the key findings of the report was that the line between state and non-state actors continues to blur.

LETTER FROM OUR LEAD SCIENTIST
EVOLUTION OF RUSSIAN CYBERCRIME
METHODOLOGY
RANSOMWARE STATISTICS: Q1 2022
CRITICAL FLAWS IN BUILDING ACCESS CONTROL SYSTEMS
PREVALENT THREAT STATISTICS: Q1 2022
CALL TO ACTION: CONNECTED HEALTHCARE CYBERSECURITY
LIVING OFF THE LAND: Q1 2022
NATION-STATE STATISTICS: Q1 2022
EMAIL SECURITY TRENDS: Q1 2022
THREATS TO COUNTRIES, CONTINENTS, SECTORS, AND VECTORS: Q1 2022
BUG REPORT
EPPS SCORE
WRITING AND RESEARCH
RESOURCES

Initially we expected this communication breach to have a severe impact on the ransomware gang's operation. However, it seemed that they were doubling down and continued their attacks, to a point that they brought a complete nation, Costa Rica, to a state of emergency. At the end of Q2 2022, we observed Conti-related infrastructure being dismantled. However, this isn't exactly a reason to celebrate. Given the fact no senior members of this crime group have been arrested, and their connections to the Russian intelligence agencies, we should consider we might be witnessing the formation of a hybrid group, one that can attack targets chosen by the government, but maintaining the plausible deniability of a crime group after financial gain. The ransomware might have a dual purpose, on the one hand being disruptive in nature and on the other hand serving as a distraction for a data exfiltration operation.

Therefore, we highly urge every organization to take close note of ransomware TTPs especially if you have already determined RU state-sponsored groups to be your most likely threat.

Innovation-wise, we are observing more ransomware groups building lockers targeting ESXi systems, seemingly realizing virtualization services play an important role in an organization. This trend has been ongoing for quite some time, but with varied success leading to corrupted VMs due to faulty lockers and or decryptors.

Is it all bad news? Not necessarily. The Q1 2022 statistics from ransomware incident-response company Coveware do show a strong decline in the amount of cases in which victims were forced to pay the ransom amount to the attackers. This gives us hope, because not paying is still the best way to disrupt the criminal business model.

### U.S. RANSOMWARE SECTORS Q1 2022

Business Services accounted for 64% of total ransomware detections among the top 10 sectors in the United States in Q1 2022. Non-profits ranked a distant second among ransomware detections.

64%


LETTER FROM OUR LEAD SCIENTIST

EVOLUTION OF RUSSIAN CYBERCRIME

METHODOLOGY

RANSOMWARE STATISTICS: Q1 2022

CRITICAL FLAWS IN BUILDING ACCESS CONTROL SYSTEMS

PREVALENT THREAT STATISTICS: Q1 2022

CALL TO ACTION: CONNECTED HEALTHCARE CYBERSECURITY

LIVING OFF THE LAND: Q1 2022

NATION-STATE STATISTICS: Q1 2022

EMAIL SECURITY TRENDS: Q1 2022

THREATS TO COUNTRIES, CONTINENTS, SECTORS, AND VECTORS: Q1 2022

BUG REPORT

EPPS SCORE

WRITING AND RESEARCH

RESOURCES

## TOOLS USED IN U.S. RANSOMWARE CAMPAIGNS Q1 2022

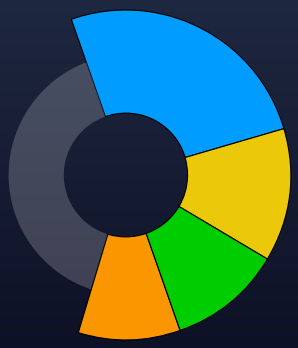
# 32%

Cobalt Strike was the malware tool used in 32% of top-10 U.S. ransomware queries in Q1 2022, reaching a prevalence equal to the next-most prevalent RCLONE (12%), BloodHound (10%), and Bazar Loader (10%) combined.

## U.S. RANSOMWARE FAMILIES Q1 2022

Lockbit was the most prevalent of ransomware families, used in 26% of top-10 queries in the U.S. in Q1 2022, ahead of Conti (13%), BlackCat (11%), and Ryuk (10%).

- Lockbit
- Blackcat
- Conti
- Ryuk



## MOST DETECTED U.S. RANSOMWARE CAMPAIGNS Q1 2022

| Connecting Vatet, PyXie, and Defray 777 | Ryuk | Lockbit | Agrius launching disruptive attacks on Israeli Targets | Conti |
|---|---|---|---|---|
| 17% | 14% | 13% | 9% | 8% |

## MOST DETECTED U.S. RANSOMWARE MITRE ATTACK PATTERNS Q1 2022

| | | |
|---|---|---|
| 1. | Data Encrypted for Impact | 14% |
| 2. | File and Directory Discovery | 12% |
| 3. | Process Discovery | 11% |
| 4. | System Information Discovery | 10% |
| 5. | PowerShell | 10% |

## TOOLS USED IN U.S. RANSOMWARE CAMPAIGNS Q1 2022

| | | |
|---|---|---|
| 1. | Cmd | 14% |
| 2. | Mimikatz | 14% |
| 3. | PsExec | 13% |
| 4. | AdFind | 11% |
| 5. | Ping.exe | 11% |


LETTER FROM OUR LEAD SCIENTIST

EVOLUTION OF RUSSIAN CYBERCRIME

METHODOLOGY

RANSOMWARE STATISTICS: Q1 2022

CRITICAL FLAWS IN BUILDING ACCESS CONTROL SYSTEMS

PREVALENT THREAT STATISTICS: Q1 2022

CALL TO ACTION: CONNECTED HEALTHCARE CYBERSECURITY

LIVING OFF THE LAND: Q1 2022

NATION-STATE STATISTICS: Q1 2022

EMAIL SECURITY TRENDS: Q1 2022

THREATS TO COUNTRIES, CONTINENTS, SECTORS, AND VECTORS: Q1 2022

BUG REPORT

EPPS SCORE

WRITING AND RESEARCH

RESOURCES

## GLOBAL RANSOMWARE: Q1 2022

### MOST REPORTED RANSOMWARE GLOBAL CUSTOMER SECTORS Q1 2022

- Telecom
- Business Services
- Media & Communications
- Finance
- Transportation & Shipping

**53%**

Telecom led the global customer sector ransomware category with 53% of detections among top-10 sectors for the second consecutive quarter.

### RANSOMWARE FAMILY DETECTIONS Q4 2021 TO Q1 2022

▼ **44%** Lockbit ▼ **37%** Conti ▼ **55%** Cuba

Ransomware Family detections were down in Q1 of 2022. Lockbit accounted for 20% of top-10 ransomware tool queries, followed by Conti (17%), and Cuba (14%) in Q4 of 2021. However, queries of all three Q4 category prevalence leaders – Lockbit (-44%), Conti (-37%), and Cuba (-55%) – decreased in Q1 of 2022 when compared to Q1 of 2022.

### MOST REPORTED RANSOMWARE MITRE-ATT&CK TECHNIQUES Q1 2022

1. Data Encrypted for Impact
2. File and Directory Discovery
3. PowerShell
4. Process Discovery
5. System Information Discovery

### MALWARE USED IN GLOBAL RANSOMWARE CAMPAIGNS IN Q1 2022 QUERIES

| | | |
|---|---|---|
| 1. | Cobalt Stike | 30% |
| 2. | Bazar Loader | 15% |
| 3. | RCLONE | 10% |
| 4. | BloodHound | 9% |
| 5. | TrickBot | 7% |


LETTER FROM OUR LEAD SCIENTIST

EVOLUTION OF RUSSIAN CYBERCRIME

METHODOLOGY

RANSOMWARE STATISTICS: Q1 2022

CRITICAL FLAWS IN BUILDING ACCESS CONTROL SYSTEMS

PREVALENT THREAT STATISTICS: Q1 2022

CALL TO ACTION: CONNECTED HEALTHCARE CYBERSECURITY

LIVING OFF THE LAND: Q1 2022

NATION-STATE STATISTICS: Q1 2022

EMAIL SECURITY TRENDS: Q1 2022

THREATS TO COUNTRIES, CONTINENTS, SECTORS, AND VECTORS: Q1 2022

BUG REPORT

EPPS SCORE

WRITING AND RESEARCH

RESOURCES

## TRELLIX RESEARCHERS UNCOVER CRITICAL FLAWS IN BUILDING ACCESS CONTROL SYSTEM

Critical infrastructure continues to represent one of the most enticing targets for criminals, worldwide. This industry is plagued by legacy systems and riddled with trivial hardware and software flaws, configuration issues, and exceptionally sluggish update cycles. Yet, behind this façade, are many of the most essential systems we rely on, from fuel pipelines to water treatment, energy grids to building automation, defense systems and much more.

One often-overlooked area of industrial control systems is access control, part of the building automation framework. Access control systems are commonplace, de facto solutions which provide automation and remote management for card readers and entry/exit points to secure locations.

According to a study done by IBM in 2021, the average cost of a physical security compromise is 3.54 million dollars and takes an average of 223 days to identify a breach. The stakes are high for organizations that rely on access control systems to ensure the security and safety of facilities.

Trellix Labs recently unveiled breaking research into one such system, a ubiquitous access control panel by HID Mercury. Numerous OEM vendors rely on Mercury boards and firmware to implement their access control solutions. Our team shared our findings at Hardwear.io in Santa Clara on June 9, 2022 and will be featured at BlackHat this summer as well. Their findings highlighted four zero-day vulnerabilities and four previously patched vulnerabilities, never published as CVEs, with the top two leading to remote code execution and arbitrary reboot, completely unauthenticated. This means attackers on a building network could remotely lock and unlock doors, and avoid detection via the management software. The researchers prepared a blog highlighting the findings and will release a multi-part technical deep dive coinciding with BlackHat. Furthermore, they filmed a demonstration video of the attack, using two of the vulnerabilities to compromise a production cloned access control system in their lab.

Watch Our Demonstration Video


LETTER FROM OUR LEAD SCIENTIST

EVOLUTION OF RUSSIAN CYBERCRIME

METHODOLOGY

RANSOMWARE STATISTICS: Q1 2022

CRITICAL FLAWS IN BUILDING ACCESS CONTROL SYSTEMS

PREVALENT THREAT STATISTICS: Q1 2022

CALL TO ACTION: CONNECTED HEALTHCARE CYBERSECURITY

LIVING OFF THE LAND: Q1 2022

NATION-STATE STATISTICS: Q1 2022

EMAIL SECURITY TRENDS: Q1 2022

THREATS TO COUNTRIES, CONTINENTS, SECTORS, AND VECTORS: Q1 2022

BUG REPORT

EPPS SCORE

WRITING AND RESEARCH

RESOURCES

## Vulnerability Findings

| CVE | Detail Summary | Mercury Firmware Version | CVSS Score |
|---|---|---|---|
| CVE-2022-31479 | Unauthenticated command injection | <=1.291 | Base 9.0, Overall 8.1 |
| CVE-2022-31480 | Unauthenticated denial-of-service | <=1.291 | Base 7.5, Overall 6.7 |
| CVE-2022-31481 | Unauthenticated remote code execution | <=1.291 | Base 10.0, Overall 9.0 |
| CVE-2022-31486 | Authenticated command injection | <=1.291 (no patch) | Base 8.8, Overall 8.2 |
| CVE-2022-31482 | Unauthenticated denial-of-service | <=1.265 | Base 7.5, Overall 6.7 |
| CVE-2022-31483 | Authenticated arbitrary file write | <=1.265 | Base 9.1, Overall 8.2 |
| CVE-2022-31484 | Unauthenticated user modification | <=1.265 | Base 7.5, Overall 6.7 |
| CVE-2022-31485 | Unauthenticated information spoofing | <=1.265 | Base 5.3, Overall 4.8 |

Table 1: CVE Filings for Mercury Access Control Vulnerabilities

## Security Updates

Carrier has released a new advisory on its product security page with specifics of the flaws and recommended mitigations and firmware updates. Applying vendor patches should be the first course of action, whenever possible.


LETTER FROM OUR LEAD SCIENTIST

EVOLUTION OF RUSSIAN CYBERCRIME

METHODOLOGY

RANSOMWARE STATISTICS: Q1 2022

CRITICAL FLAWS IN BUILDING ACCESS CONTROL SYSTEMS

PREVALENT THREAT STATISTICS: Q1 2022

CALL TO ACTION: CONNECTED HEALTHCARE CYBERSECURITY

LIVING OFF THE LAND: Q1 2022

NATION-STATE STATISTICS: Q1 2022

EMAIL SECURITY TRENDS: Q1 2022

THREATS TO COUNTRIES, CONTINENTS, SECTORS, AND VECTORS: Q1 2022

BUG REPORT

EPPS SCORE

WRITING AND RESEARCH

RESOURCES

## PREVALENT THREAT STATISTICS

Our team tracked threat categories in the first quarter of 2022. The research reflects percentages of detections in the type of prevalent Malware families observed, associated Client Countries, Enterprise Customer Sectors, and MITRE ATT&CK techniques.

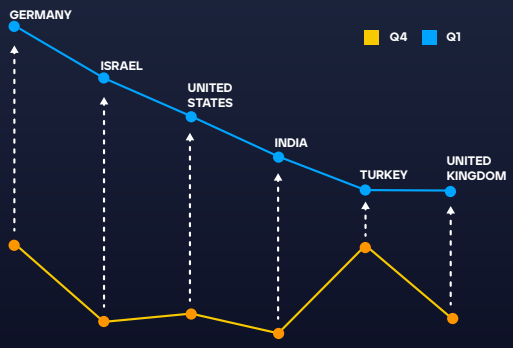
### MALWARE FAMILIES Q1 2022

**23%**

Phorpiex was the most prevalent Tool Malware Family queried in Q1 of 2022

- Phorpiex
- Electron Bot
- RedLine Stealer
- Agent Tesla
- Remcos RAT

### MALWARE CLIENT COUNTRY DETECTIONS Q1 2022




### MOST REPORTED MITRE ATT&CK TECHNIQUES Q1 2022

1. Ingress Tool Transfer
2. Obfuscated Files or Information
3. Web Protocols
4. Deobfuscate/Decode Files or Information
5. Modify Registry

### MALWARE SECTORS Q1 2022 DETECTIONS Q1 2022

- Telecom
- Business Services
- Media & Communications
- Finance
- Transportation & Shipping


LETTER FROM OUR LEAD SCIENTIST

EVOLUTION OF RUSSIAN CYBERCRIME

METHODOLOGY

RANSOMWARE STATISTICS: Q1 2022

CRITICAL FLAWS IN BUILDING ACCESS CONTROL SYSTEMS

PREVALENT THREAT STATISTICS: Q1 2022

CALL TO ACTION: CONNECTED HEALTHCARE CYBERSECURITY

LIVING OFF THE LAND: Q1 2022

NATION-STATE STATISTICS: Q1 2022

EMAIL SECURITY TRENDS: Q1 2022

THREATS TO COUNTRIES, CONTINENTS, SECTORS, AND VECTORS: Q1 2022

BUG REPORT

EPPS SCORE

WRITING AND RESEARCH

RESOURCES

## CALL TO ACTION: CONNECTED HEALTHCARE CYBERSECURITY

The medical industry is at unique risk of attack due to the numerous purpose-built devices used, such as anesthesia machines, IV pumps, point of care systems, MRI machines, and numerous others. Many of these devices are not found in other industries nor the average household. Their lack of ubiquity creates a false sense of security and reduced scrutiny from the security research industry.

Medical devices and software are falling short in fundamental security practices such as handling credentials and are ripe with RCE vulnerabilities. This is enticing to cybercriminals and we must be on our guard to prevent further attacks as it won't be an ignored attack surface forever. All stakeholders must acknowledge that the large selection of authentication vulnerabilities indicates the medical space needs more research, both internally and externally, to harden these devices. It's not simply management systems and other web-based applications we need to focus on, but any network connected medical device needs to be accessed. Currently it doesn't appear that these devices are being targeted by malicious actors but this doesn't mean we can relax. There have been plenty of RCE vulnerabilities to choose from and public exploit code for re-use. While attackers are using other methods to attack hospitals and clinics they will search for easier access when those methods run dry. Society as whole cannot allow medical devices and software to continue to be a weak point for attackers to exploit and therefore should encourage both internal and external security testing across developers and researchers alike.

You can read the details of our research in our recent Connected Healthcare: A Cybersecurity Battlefield We Must Win blog. Using public data such as CVE databases we analyzed the current state of the attack surface in the medical space and evaluated active threats and distribution of discovered vulnerabilities. We believe that more partnerships between medical device vendors, medical care facilities and security researchers in junction with increased security testing is warranted to prevent a growing attack surface from becoming even more attractive to malicious actors.


LETTER FROM OUR LEAD SCIENTIST

EVOLUTION OF RUSSIAN CYBERCRIME

METHODOLOGY

RANSOMWARE STATISTICS: Q1 2022

CRITICAL FLAWS IN BUILDING ACCESS CONTROL SYSTEMS

PREVALENT THREAT STATISTICS: Q1 2022

CALL TO ACTION: CONNECTED HEALTHCARE CYBERSECURITY

LIVING OFF THE LAND: Q1 2022

NATION-STATE STATISTICS: Q1 2022

EMAIL SECURITY TRENDS: Q1 2022

THREATS TO COUNTRIES, CONTINENTS, SECTORS, AND VECTORS: Q1 2022

BUG REPORT

EPPS SCORE

WRITING AND RESEARCH

RESOURCES

## LIVING OFF THE LAND

We track threat actors, tactics techniques and procedures as well as malware being used. We have also identified and reported quarterly regarding non-malicious and often necessary default binaries that can and often are abused to conduct various phases in an attack. While it remains necessary to know the custom and commodity malware, as well as living of the land TTP's to defend against, it is also necessary to know the enemy and identify objectives. Diving a little deeper into the LoLBins the question remains who is using these our tools against us and why? Do they not have the ability to write custom malware that may accomplish the objective at hand? Or is it simply a tool of convenience and an attempt to stay unseen? After all threat actors are often employed much like everyone else, they have meetings with their overlords, they have daily, quarterly, and yearly goals, work on sprints and earn a paycheck.

If we are going to honor our mission "To Deliver Living Security Everywhere" we must equip ourselves, our customers and our colleagues who are in the day-to-day fight to protect our critical information, infrastructures, and assets from those who seek to profit from the exploitation of vulnerabilities and theft of intellectual and organizational data.

What binaries have we seen being abused and who have we identified abusing them in Q1 2022?

### WINDOWS BINARIES Q1 2022

| | | |
|---|---|---|
| 1. | Windows Command Shell/CMD | 41.90% |
| 2. | PowerShell | 37.14% |
| 3. | WMI/WMIC | 21.43% |
| 4. | Schtasks | 19.05% |
| 5. | Rundll32 | 14.29% |

### ADMINISTRATIVE TOOLS Q1 2022

| | | |
|---|---|---|
| 1. | Remote Access Tools | 20.48% |
| 2. | File Transfer | 6.19% |
| 3. | Network Discovery | 6.19% |
| 4. | Archive Utilities | 5.71% |
| 5. | Remote Program Execution | 4.29% |


LETTER FROM OUR LEAD SCIENTIST

EVOLUTION OF RUSSIAN CYBERCRIME

METHODOLOGY

RANSOMWARE STATISTICS: Q1 2022

CRITICAL FLAWS IN BUILDING ACCESS CONTROL SYSTEMS

PREVALENT THREAT STATISTICS: Q1 2022

CALL TO ACTION: CONNECTED HEALTHCARE CYBERSECURITY

LIVING OFF THE LAND: Q1 2022

NATION-STATE STATISTICS: Q1 2022

EMAIL SECURITY TRENDS: Q1 2022

THREATS TO COUNTRIES, CONTINENTS, SECTORS, AND VECTORS: Q1 2022

BUG REPORT

EPPS SCORE

WRITING AND RESEARCH

RESOURCES

## THREAT ACTORS ABUSING WINDOWS BINARIES AND ADMINISTRATIVE TOOLS Q1 2022

Throughout events in Q1 of 2022, our analysis attributed the following threat groups as the top abusers of legitimate Windows Binaries and Administrative Tools:

| | | |
|---|---|---|
| 1. | APT41 | 39% |
| 2. | Gamaredon Group | 39% |
| 3. | APT35 | 33% |
| 4. | Winnti Group | 33% |
| 5. | MuddyWater | 24% |

## RANSOMWARE ABUSING WINDOWS BINARIES AND ADMINISTRATIVE TOOLS Q1 2022

Additionally, through our tracking and analysis, we identified the following ransomware families that abused legitimate Windows Binaries and Administrative Tools prior to deployment of a ransomware payload:

| | | |
|---|---|---|
| 1. | BlackCat | 29.63% |
| 2. | LockBit | 16.67% |
| 3. | Midas | 16.67% |
| 4. | BlackByte | 14.81% |
| 5. | Hermetic Ransom | 14.81% |

## NATION-STATE STATISTICS: Q1 2022

Our team tracks and monitors Nation-State campaigns and associated indicators and techniques. Our research reflects Threat Actors, Tools, Client Countries, Customer Sectors, and MITRE ATT&CK Techniques from Q1 of 2022. All of the data around these events, including indicators, YARA rules, and detection logic are available in Insights.

### TOP 5 MOST ACTIVE APT GROUPS Q1 2022

**15%**

APT 36 was the most active APT group accounting for 15% of the detections in Q1 of 2022.

- APT36
- APT27
- APT29
- APT28
- IndigoZebra

LETTER FROM OUR LEAD SCIENTIST

EVOLUTION OF RUSSIAN CYBERCRIME

METHODOLOGY

RANSOMWARE STATISTICS: Q1 2022

CRITICAL FLAWS IN BUILDING ACCESS CONTROL SYSTEMS

PREVALENT THREAT STATISTICS: Q1 2022

CALL TO ACTION: CONNECTED HEALTHCARE CYBERSECURITY

LIVING OFF THE LAND: Q1 2022

NATION-STATE STATISTICS: Q1 2022

EMAIL SECURITY TRENDS: Q1 2022

THREATS TO COUNTRIES, CONTINENTS, SECTORS, AND VECTORS: Q1 2022

BUG REPORT

EPPS SCORE

WRITING AND RESEARCH

RESOURCES

## NATION-STATE CLIENT COUNTRIES Q1 2022

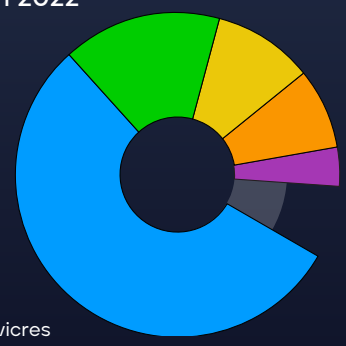
**31%**

Nation-State activity in Turkey accounted for 31% of top 10 detections among client countries in Q1 2022, followed by Israel (18%), United Kingdom (11%), Mexico 10%), and the United States (8%).

## MOST REPORTED MITRE ATT&CK PATTERNS Q1 2022

1. Obfuscated Files or Information
2. Deobfuscate/Decode Files or Information
3. Spearphishing Attachment
4. System Information Discovery
5. Web Protocols

## NATION-STATE SECTORS Q1 2022



- Telecom
- Business Servicres
- Media & Communications
- Finance
- Transportation & Shipping

## MALWARE USED IN NATION-STATE CAMPAIGNS Q1 2022

**22%** Cobalt Strike ranked highest (22%) among top-10 malware used in Q1 2022 APT campaigns.

| Cobalt Strike | njRAT | PlugX | PoisonIvy | Crimson RAT |
|---|---|---|---|---|
| 22% | 10% | 10% | 8% | 8% |


LETTER FROM OUR LEAD SCIENTIST

EVOLUTION OF RUSSIAN CYBERCRIME

METHODOLOGY

RANSOMWARE STATISTICS: Q1 2022

CRITICAL FLAWS IN BUILDING ACCESS CONTROL SYSTEMS

PREVALENT THREAT STATISTICS: Q1 2022

CALL TO ACTION: CONNECTED HEALTHCARE CYBERSECURITY

LIVING OFF THE LAND: Q1 2022

NATION-STATE STATISTICS: Q1 2022

EMAIL SECURITY TRENDS: Q1 2022

THREATS TO COUNTRIES, CONTINENTS, SECTORS, AND VECTORS: Q1 2022

BUG REPORT

EPPS SCORE

WRITING AND RESEARCH

RESOURCES

## EMAIL SECURITY TRENDS: Q1 2022

Email telemetry analysis from the first quarter of 2022 revealed phishing URLs and malicious document trends in email security.

Most of the malicious emails detected contained a phishing URL used to either steal credentials or lure the victims to download malware. Next in popularity we identified emails with malicious documents such as Microsoft Office files or PDFs attached. These documents contain macros that work as downloaders or exploits that result in the attacker gaining control of the victim system. Lastly, we encounter several emails with malicious executables like infostealers or trojans attached.

### Exploits

When we focus on the exploits used, we realize that most of them come packed as malicious RTF files, MS Office documents with weaponized OLE objects, or PDFs infected with Adobe Reader exploits or malicious JS scripts. In the following figure we can see that the top three file formats are the windows rtf, followed by the latest office format and finally we have the legacy role office formats.

| RTF | 50.76% |
|---|---|
| CVE-2017-11882 | 15.7% |
| CVE-2012-0158 | 12.84% |
| CVE-2017-0199 | 11.94% |
| CVE-2014-1761 | 5.8% |
| CVE-2017-8759 | 4.41% |

| OFFICE | 31.25% |
|---|---|
| CVE-2017-11882 | 23.84% |
| CVE-2017-0199 | 3.05% |
| CVE-2017-8570 | 1.7% |

| OLE | 17.99% |
|---|---|
| CVE-2017-11882 | 12.74% |
| CVE-2012-0158 | 4.16% |


LETTER FROM OUR LEAD SCIENTIST

EVOLUTION OF RUSSIAN CYBERCRIME

METHODOLOGY

RANSOMWARE STATISTICS: Q1 2022

CRITICAL FLAWS IN BUILDING ACCESS CONTROL SYSTEMS

PREVALENT THREAT STATISTICS: Q1 2022

CALL TO ACTION: CONNECTED HEALTHCARE CYBERSECURITY

LIVING OFF THE LAND: Q1 2022

NATION-STATE STATISTICS: Q1 2022

EMAIL SECURITY TRENDS: Q1 2022

THREATS TO COUNTRIES, CONTINENTS, SECTORS, AND VECTORS: Q1 2022

BUG REPORT

EPPS SCORE

WRITING AND RESEARCH

RESOURCES

## THREATS TO COUNTRIES, CONTINENTS, SECTORS, AND VECTORS: Q1 2022

Notable country and continent increases of open-sourced publicly reported incidents in the first quarter of 2022 include:

### ATTACK VECTORS Q1 2022

- Malware
- Unknown
- Account Takeover
- Targeted Takeover
- Vulnerability

**490%**

Russia recorded the highest increase of incidents reported from Q4 2021 to Q1 2022.

**35%**

The United States experienced the most reported incidents in Q1 2022.

### ATTACK SECTORS Q1 2022

- Multiple Industries
- Healthcare
- Public
- Individuals
- Financial

LETTER FROM OUR LEAD SCIENTIST

EVOLUTION OF RUSSIAN CYBERCRIME

METHODOLOGY

RANSOMWARE STATISTICS: Q1 2022

CRITICAL FLAWS IN BUILDING ACCESS CONTROL SYSTEMS

PREVALENT THREAT STATISTICS: Q1 2022

CALL TO ACTION: CONNECTED HEALTHCARE CYBERSECURITY

LIVING OFF THE LAND: Q1 2022

NATION-STATE STATISTICS: Q1 2022

EMAIL SECURITY TRENDS: Q1 2022

THREATS TO COUNTRIES, CONTINENTS, SECTORS, AND VECTORS: Q1 2022

BUG REPORT

EPPS SCORE

WRITING AND RESEARCH

RESOURCES

## BUG REPORT

### If Bugs were a Band, Here's Their Greatest Hits

Any music nerd worth their salt will tell you digging into a new artist is best done not by Googling their hit singles, but by digesting them album by album – each release promising to bring something novel, worthwhile, and self-contained. For the rockstars at Trellix Threat Labs , this might mean tuning in to our monthly Bug Report, where we highlight the most impactful vulnerabilities each month based on qualitative analysis and decades of collective industry experience – not just CVSS scores. We realize, however, that not everyone has the time to sit down with a nice drink, put on their coziest bathrobe, and listen to an entire discography. For those wishing to dip their toes, consider this the Bug Report's Greatest Hits of 2022. And if you like what you hear, be sure to check out our other work – we treat our groupies right.

### Crème de la Crème

Truthfully, the bugs that make the cut each month are already standouts in their own right among the dozens competing for the ever-scarce attention span of Twitter, so selecting a handful of winners from these is no small feat. Our greatest tool in this endeavor is the benefit of hindsight. In other words, we want to pick out the classics from the one-hit wonders – which vulns have demonstrated an impact, or we anticipate will demonstrate an impact, well beyond their respective months of infamy?

The first that comes to mind is CVE-2022-0847, AKA "Dirty Pipe." Although perhaps not as sexy as some 9.8 RCEs, this Linux kernel bug went beyond a simple escalation of privilege and allowed unfettered write access to any file, a concerning state of affairs for an environment where everything is a file. The nail in the coffin, however, is that unless you're a masochist running a bleeding-edge distro like Arch, kernel updates are not standard fare for devices running Linux, meaning vulnerable devices are likely to stay that way for a good while. Add the incredibly simple PoC and evidence of in-the-wild exploitation to the mix, and you've got a bug that's guaranteed to go double platinum.


LETTER FROM OUR LEAD SCIENTIST

EVOLUTION OF RUSSIAN CYBERCRIME

METHODOLOGY

RANSOMWARE STATISTICS: Q1 2022

CRITICAL FLAWS IN BUILDING ACCESS CONTROL SYSTEMS

PREVALENT THREAT STATISTICS: Q1 2022

CALL TO ACTION: CONNECTED HEALTHCARE CYBERSECURITY

LIVING OFF THE LAND: Q1 2022

NATION-STATE STATISTICS: Q1 2022

EMAIL SECURITY TRENDS: Q1 2022

THREATS TO COUNTRIES, CONTINENTS, SECTORS, AND VECTORS: Q1 2022

BUG REPORT

EPPS SCORE

WRITING AND RESEARCH

RESOURCES

Another standout comes to us courtesy of our April issue, and not just because I happened to author that one: CVE-2022-22965 AKA "Spring4Shell." In case the name didn't give it away, the InfoSec community immediately saw its similarities to 2021's biggest vuln (likely in part due to collective PTSD) and the moniker, while clunky, stuck. Instead of targeting a popular open-source Java logging library, however, this one targeted a popular open-source Java framework known as Spring. Like a cash-grab sequel to a popular movie with no ideas of its own, Spring4Shell also went through a life cycle of less-than-perfect patches and also saw in-the-wild exploitation within 48 hours of public disclosure. If nothing else, this further solidifies Log4Shell's importance, as its cheap knockoff is a strong contender for top vuln of 2022 thus far.

## Hidden Gems

Although a Greatest Hits album can serve as an efficient highlight reel for an artist, it is inevitable that some hidden gems will slip through the cracks. For Microsoft, one such surprise hit was CVE-2022-30190 AKA "Follina," an RCE-capable (with minimal user interaction) bug in the Microsoft Support Diagnostic Tool (MSDT). If you want to lose any remaining faith in humanity, we highly advise you take a look at the disclosure timeline for this bug. The issue, albeit utilizing a different attack vector, was disclosed to Microsoft several times as early as March, and Microsoft was provided with evidence of in-the-wild exploitation as early as April, only for Microsoft to dismiss it outright or silently patch the highlighted attack vector and not the root cause each time. It wasn't until May 30th that Microsoft finally issued a CVE and mitigation advisory for the core MSDT bug, resulting in it being left out of our May Bug Report.

CVE-2022-22954 and CVE-2022-22960, on the other hand, slipped through the cracks as a result of us misjudging their severity, resulting in them not making the cut for our April Bug Report although they probably should have. While the former is a true RCE and the latter is a privilege escalation vulnerability, we mention them together because they both affect a sizable fraction of VMware's suite of widely used enterprise software. Additionally, these two vulns have been utilized, sometimes in combination, in numerous exploitation campaigns conducted by APT groups, according to a recent CISA advisory. Having received IOCs from multiple large corporations, federal agencies were mandated to either patch or take offline all impacted software by May 5th, less than a month from the vulnerability's public disclosure. Unfortunately, this is where the musician analogy completely falls apart, as I'm going to have to agree with the feds on this one.


LETTER FROM OUR LEAD SCIENTIST

EVOLUTION OF RUSSIAN CYBERCRIME

METHODOLOGY

RANSOMWARE STATISTICS: Q1 2022

CRITICAL FLAWS IN BUILDING ACCESS CONTROL SYSTEMS

PREVALENT THREAT STATISTICS: Q1 2022

CALL TO ACTION: CONNECTED HEALTHCARE CYBERSECURITY

LIVING OFF THE LAND: Q1 2022

NATION-STATE STATISTICS: Q1 2022

EMAIL SECURITY TRENDS: Q1 2022

THREATS TO COUNTRIES, CONTINENTS, SECTORS, AND VECTORS: Q1 2022

BUG REPORT

EPPS SCORE

WRITING AND RESEARCH

RESOURCES

### Zooming Out

With the benefit of hindsight, what's the lesson learned, both for us and our ~~groupies~~ readers? Well, I think the biggest blind spot demonstrated in our evaluation of the severity of these vulnerabilities was attempting to judge them in a vacuum based largely on the technical merit of the vulnerability alone. In actuality, the deciding factors for which vulnerabilities proved most impactful in 2022 were their utilization in campaigns and the ubiquity of the platforms they affected. This does, however, grant us further confidence in our approach of looking beyond the CVSS score, as this contextual insight is often poorly represented in a numerical score alone.

## EPPS SCORE

With the amount of released CVE's, the suggested updates/patches, it is hard to determine which ones to prioritize. Within Trellix we have embraced the 'Exploit Prediction Scoring System' (EPSS). The mission of this model is what is the likekood/probability of the vulnerability being exploited. Several features/telemetry are put into a model that than will calculate the score of that CVE. The output of the model will be a score will be a probability score between 0 and 1 (0 and 100%). The higher the score, the greater the probability that a vulnerability will be exploited. For the first quarter of 2022, the following CVEs ranked as a top 10:

### CVE Number

CVE-2022-0543

CVE-2022-24734

CVE-2022-0441

CVE-2022-21371

CVE-2022-21907

CVE-2022-24112

CVE-2022-20699

CVE-2022-0824

CVE-2021-22947

CVE-2022-24862


LETTER FROM OUR LEAD SCIENTIST

EVOLUTION OF RUSSIAN CYBERCRIME

METHODOLOGY

RANSOMWARE STATISTICS: Q1 2022

CRITICAL FLAWS IN BUILDING ACCESS CONTROL SYSTEMS

PREVALENT THREAT STATISTICS: Q1 2022

CALL TO ACTION: CONNECTED HEALTHCARE CYBERSECURITY

LIVING OFF THE LAND: Q1 2022

NATION-STATE STATISTICS: Q1 2022

EMAIL SECURITY TRENDS: Q1 2022

THREATS TO COUNTRIES, CONTINENTS, SECTORS, AND VECTORS: Q1 2022

BUG REPORT

EPPS SCORE

WRITING AND RESEARCH

RESOURCES

## WRITING AND RESEARCH

Alfred Alvarado
Christiaan Beek
Mark Bereza
John Fokker
Charles McFarland
Doug McKee
Tim Polzer
Steve Povolny
Sam Quinn
Leandro Velasco

## RESOURCES

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

Threat Center – Today's most impactful threats identified by our team.

### TWITTER

Trellix Threat Labs
Christiaan Beek
John Fokker
Douglas McKee
Steve Povolny

### DOWNLOAD PDF

View Threat Report Archives

## ABOUT TRELLIX

Trellix is a global company redefining the future of cybersecurity and soulful work. The company's open and native extended detection and response (XDR) platform helps organizations confronted by today's most advanced threats gain confidence in the protection and resilience of their operations. Trellix, along with an extensive partner ecosystem, accelerates technology innovation through machine learning and automation to empower over 40,000 business and government customers with living security. More at https://trellix.com.

Trellix Threat Labs

Subscribe to Receive Our Threat Information

This document and the information contained herein describes computer security research for educational purposes only and the convenience of Trellix customers. Trellix conducts research in accordance with its Vulnerability Reasonable Disclosure Policy | Trellix. Any attempt to recreate part or all of the activities described is solely at the user's risk, and neither Trellix nor its affiliates will bear any responsibility or liability.

LETTER FROM OUR LEAD SCIENTIST
EVOLUTION OF RUSSIAN CYBERCRIME
METHODOLOGY
RANSOMWARE STATISTICS: Q1 2022
CRITICAL FLAWS IN BUILDING ACCESS CONTROL SYSTEMS
PREVALENT THREAT STATISTICS: Q1 2022
CALL TO ACTION: CONNECTED HEALTHCARE CYBERSECURITY
LIVING OFF THE LAND: Q1 2022
NATION-STATE STATISTICS: Q1 2022
EMAIL SECURITY TRENDS: Q1 2022
THREATS TO COUNTRIES, CONTINENTS, SECTORS, AND VECTORS: Q1 2022
BUG REPORT
WRITING AND RESEARCH
RESOURCES

Visit Trellix.com to learn more.

Trellix

About Trellix

Trellix is a global company redefining the future of cybersecurity. The company's open and native extended detection and response (XDR) platform helps organizations confronted by today's most advanced threats gain confidence in the protection and resilience of their operations. Trellix's security experts, along with an extensive partner ecosystem, accelerate technology innovation through machine learning and automation to empower over 40,000 business and government customers.

Copyright © 2022 Musarubra US LLC

072022-05