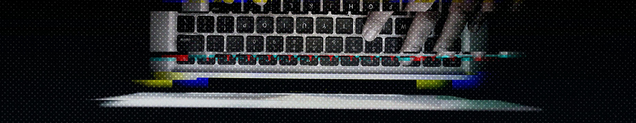


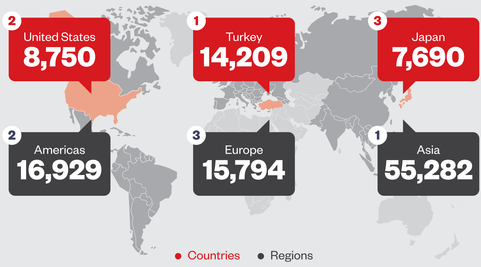
STEPPING AHEAD OF RISK

TREND MICRO 2023 MIDYEAR CYBERSECURITY THREAT REPORT

RANSOMWARE THREATS

Top 3 Countries and Regions

by detected ransomware attacks

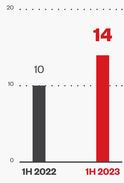


Top 3 Industries and Segments

by detected ransomware attacks

New Ransomware Families

found in the first half of 2023



Newly detected ransomware families

Mimic ransomware

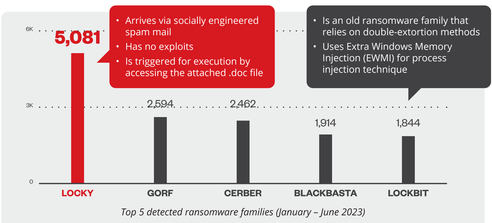
- Targets Russian- and English-speaking users.
- Abuses APIs of Everything, a Windows file name search engine, to query target files to encrypt.
- Has code similar to the 2022 Conti ransomware.

DarkBit ransomware

- Targets educational institutions in Israel.
- Is written in Go programming language, which simplifies the process of supporting various operating systems.
- Employs AES-256 encryption, which can affect a wide range of file types.
- Accepts command-line arguments and can be run autonomously.

Top 5 Ransomware Families

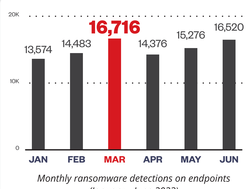
detected in the first half of 2023



Top 5 detected ransomware families (January – June 2023)

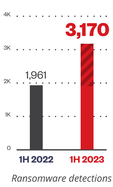
Ransomware Detections

Total Ransomware Detections **90,945**



Monthly ransomware detections on endpoints (January – June 2023)

Most Increased Detection by Operating System



Ransomware detections on Linux

Linux variants remain a staple for new ransomware families with over 62% more ransomware detections in the first half of 2023 compared to the first half of 2022.

Ransomware families that target Linux include RTM Locker, BlackSuit, Akira, and Trigona

Notable Insights

In addition to Go and Rust, threat actors now also use the new compiling ransomware programming language NIM to avoid detection and make analysis harder, as observed in the BazarLoader and DarkPower ransomware.

We observed an increase in new arrival and execution methods that help ransomware actors avoid detection and increase success:

- Bring-your-own-vulnerable-driver (BYOVD) attacks, specifically involving AuKill, SpyBoy, and BlackCat
- Zero-day exploit attacks: Nokoyawa and BlackBasta abused CVE-2023-28252, and Clop abused vulnerabilities in 3CX, GoAnywhere, MOVEit, and PaperCut

Threat actors continue to use leaked source code as the basis for the new ransomware variants. The LockBit ransomware used Bl00dy and BabLock source code, Babuk used Cylance and RA Group, and both ransomware families used Buhti.

While WannaCry remains detected in our telemetry, the ransomware family's infections have been classified as dormant and very low risk. A kill switch was activated when an odd domain was registered by security researcher Marcus Hutchins. As long as the sinkholed domain is up and running, WannaCry will not encrypt files.

Trend Research

TREND MICRO

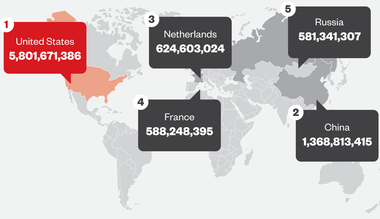
STEPPING AHEAD OF RISK

TREND MICRO 2023 MIDYEAR CYBERSECURITY THREAT REPORT

CLOUD AND ENTERPRISE

Top 5 Countries

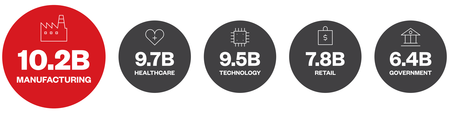
with detected email threats



Top 5 Industries

affected by risk events

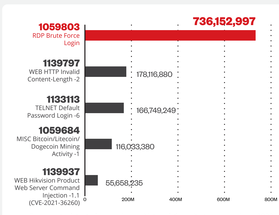
The manufacturing industry had the most risk event detections based on our attack surface risk management (ASRM) data.



Top 5 Risk Events

detected on secured routers

Top risk events in our Home Network Security involved initial access through credentials and a vulnerability caused by an error in processing HTTP packets that results in a heap buffer overflow.



Top events detected in our Home Network Security (January – June 2023)

Brute Force Login

- Might be RDP via port 3389, FTP via port 21, or SSH via port 22 to repeatedly attempt logging in to target hosts using a dictionary of common usernames and passwords.

WEB HTTP Invalid Content-Length -2

- Is caused by an error in processing HTTP packets containing negative Content-Length header field values that results in a heap buffer overflow.

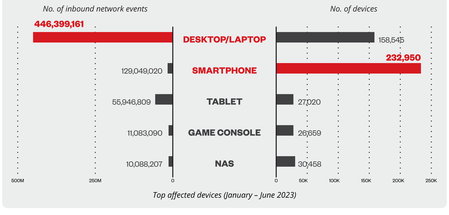
TELNET Default Password Login -6

- Detects when a user within the network uses the default password to log in.

Top 5 Devices

affected by inbound attacks

Desktops and laptops recorded the most inbound attack detections based on our Home Network Security data.

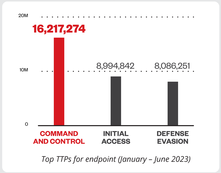


Top affected devices (January – June 2023)

Top Tactics, Techniques, and Procedures (TTPs)

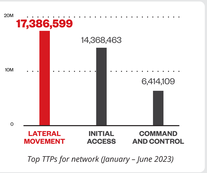
used against endpoints and networks

Endpoint



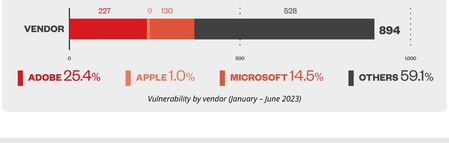
Top TTPs for endpoint (January – June 2023)

Network



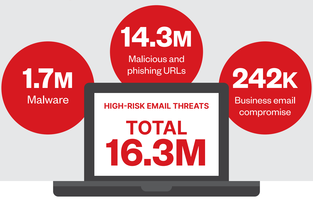
Top TTPs for network (January – June 2023)

Vendor Vulnerability Count



Vulnerability by vendor (January – June 2023)

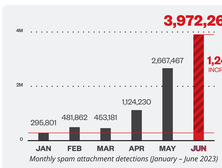
High-Risk Email Threats



Spam Attachments

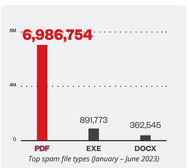
Spam attachments peaked in June at 3.9 million detections, a whopping 1,242% increase from the beginning of the year. PDFs are the most used spam attachment file type.

Total Spam Attachments **8,994,806**



Monthly spam attachment detections (January – June 2023)

File Types



Top spam file types (January – June 2023)

STEPPING AHEAD OF RISK

TREND MICRO 2023 MIDYEAR CYBERSECURITY THREAT REPORT

RISK LANDSCAPE

Top Risk Events

detected via Trend Micro Attack Surface Risk Management (ASRM)

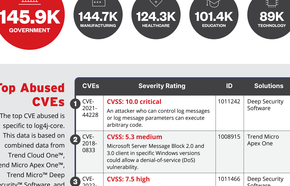
35.2B
Risky Cloud Access

18.5B
Risky Website Access

The top two risk events detected via ASRM involve risky cloud applications and accessing risky websites.

Top 3 Countries

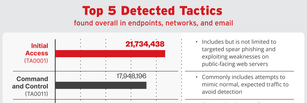
with risk events, malware detection, and malicious URL access



Top 5 Industries

affected by malware campaigns

In the first half of 2023, malware campaigns targeted government organizations the most with 145,912 detections.



Top Abused CVEs

The top CVE abused is specific to log4j-core. This data is based on combined data from Trend Cloud One™, Trend Micro Apex One™, Trend Micro™ Deep Security™ Software, and Trend Micro™ TippingPoint™.

	CVEs	Severity Rating	ID	Solutions
1	CVE-2021-44228	**CVSS: 10.0 critical** An attacker who can control log messages or log message parameters can execute arbitrary code.	1011242	Deep Security Software
2	CVE-2018-0833	**CVSS: 5.3 medium** Microsoft Server Message Block 2.0 and 3.0 client in specific Windows versions could allow a denial-of-service (DoS) vulnerability.	1008915	Trend Micro Apex One
3	CVE-2022-30521	**CVSS: 7.5 high** A vulnerable Apache HTTP Server 2.4.53 could allow excessively large memory allocations and trigger an abort.	1011466	Deep Security Software

Top Riskiest CVEs

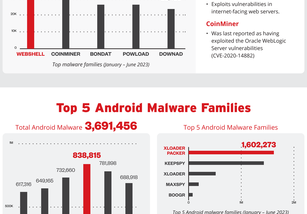
exploited in the wild

The top five riskiest CVEs exploited in the wild and detected by our ASRM telemetry show vulnerabilities in Windows operating systems.

	CVEs	Severity Rating
1	CVE-2023-28252	**CVSS: 7.8 high** Windows Common Log File System Driver Elevation of Privilege Vulnerability
2	CVE-2023-24880	**CVSS: 4.4 medium** Windows SmartScreen Security Feature Bypass Vulnerability
3	CVE-2023-21823	**CVSS: 7.8 high** Windows Graphics Component Remote Code Execution Vulnerability
4	CVE-2023-23376	**CVSS: 7.8 high** Windows Common Log File System Driver Elevation of Privilege Vulnerability
5	CVE-2023-21674	**CVSS: 8.8 high** Windows Advanced Local Procedure Call (ALPC) Elevation of Privilege Vulnerability

Top 5 Detected Tactics

found overall in endpoints, networks, and email



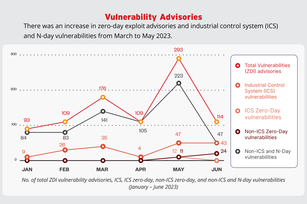
- Includes but is not limited to targeted spear phishing and exploiting weaknesses on public-facing web servers
- Commonly includes attempts to mimic normal, expected traffic to avoid detection
- Can involve the use of remote access tools or legitimate credentials with native network and operating system tools
- Uninstalls or disables security software, or obfuscates and encrypts data and scripts
- Involves abusing trusted processes to hide the presence of malware
- Pertains to techniques to gain knowledge about the system and internal network
- Involves the use of native operating system tools for gathering information and exploring what can be controlled

Top tactics in total detection count each month (January – April 2023)

Top Tracked Trends

of detected tactics, techniques, and procedures (TTPs)

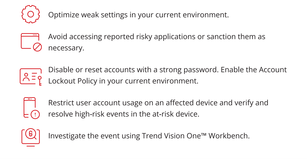
Detections from February to April show a shift in focus from Persistence to Defense Evasion and Impact tactics.



Overall trend in TTPs by number of customers hit each month (December 2022 – April 2023)

Top Malware Families

Three malware families maintained prolificacy in the first half of 2022 and 2023.



Top malware families (January – June 2023)

Webshell
- Had the most malware detections in the first half of 2022 and maintained this top spot in the first half of 2023.
- Exploits vulnerabilities in internet-facing web servers.

CoinMiner
- Was last reported as having exploited the Oracle WebLogic Server vulnerabilities (CVE-2020-14882).

Top 5 Android Malware Families

Total Android Malware **3,691,456**

Monthly Android malware detections (January – June 2023)

Top 5 Android Malware Families

Top 5 Android malware families (January – June 2023)

A new trojan malware family made it to the top five in the first half of 2023.

Boogr is a new trojan malware family first reported in May 2023. This piece of malware is capable of:
- Downloading malicious files
- Sending text messages

It was last reported as having exploited the Oracle WebLogic Server vulnerabilities (CVE-2020-14882).

Vulnerabilities

944 1H 2022

894 1H 2023

There are 50 fewer zero-day vulnerability advisories in the first half of this year compared to last year.

No. of vulnerability advisories (1H 2022 vs. 1H 2023)

Vulnerability Advisories

There was an increase in zero-day exploit advisories and industrial control system (ICS) and N-day vulnerabilities from March to May 2023.

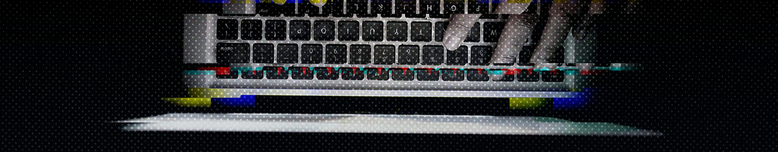
No. of total ZDI vulnerability advisories, ICS, ICS zero-day, non-ICS zero-day, and non-ICS and N-day vulnerabilities (January – June 2023)

Top Recommendations to Lower Risk

- Apply the latest patch or upgrade your operating system or application version.
- Apply prevention rules from Trend Micro products to protect vulnerabilities from being exploited.
- Optimize weak settings in your current environment.
- Avoid accessing reported risky applications or sanction them as necessary.
- Disable or reset accounts with a strong password. Enable the Account Lockout Policy in your current environment.
- Restrict user account usage on an affected device and verify and resolve high-risk events in the at-risk device.
- Investigate the event using Trend Vision One™ Workbench.

Trend Research

TREND MICRO

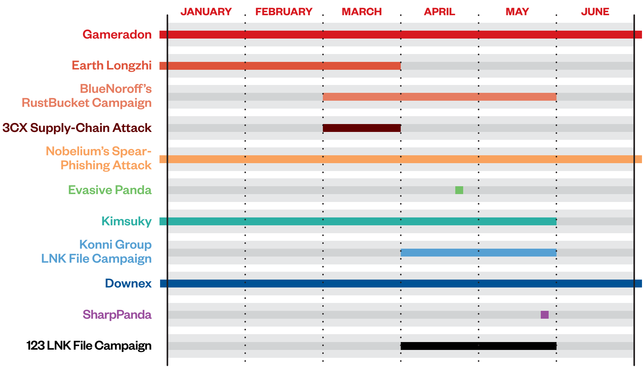


STEPPING AHEAD OF RISK

TREND MICRO 2023 MIDYEAR CYBERSECURITY THREAT REPORT

APT CAMPAIGNS

APT Campaigns



Timeline of APT campaign attacks (January – June 2023)

Notable Insights

Gameradon

2020 - present

- Targets government organizations in Ukraine
- Is delivered by spear-phishing emails, typically by attaching Word files that trigger remote template injection and execute a malicious macro
- Is possibly a general intelligence operation against Ukraine

Bluenoroff's RustBucket Campaign

March - May 2023

- Targets crypto assets and blockchain-related organizations
- Possibly aimed to obtain funds for weapons development (based on a report by the Panel of Experts of the UN Security Council Sanctions Committee)

NOBELIUM's Spear-Phishing Attack

January 2022 - present

- Targets diplomatic agencies
- Sent spear-phishing emails to diplomats and impersonated embassies in European countries
- Attached a PDF file or had an email body that contained an embedded link to the next stage payload source
- Possibly aimed at finding information on the diplomatic policies of each target country

Kimsuky

2013 - May 2023

- Targets security, diplomacy, defense, and Korean-language support groups
- Is delivered in a phishing email with a .doc and a .chm file infecting the device with a piece of malware that harvests credentials
- Collects intelligence from diplomatic, security, and national defense organizations

Downex

2022 - present

- Targets diplomatic missions and organizations in Afghanistan, Germany, and Mongolia
- Is delivered by executing a disguised .exe file that itself executes a .hta file and attempts to obtain and execute the next stage payload from the command-and-control (C&C) server
- Is possibly a general intelligence operation against the Central Asian region

Earth Longhzhi

December 2022 - March 2023

- Targets government, healthcare, technology, and manufacturing organizations
- Abuses a Windows Defender executable to perform DLL sideloading
- Disables security products by "stack rumbling" via Image File Execution Options

3CX Supply-Chain Attack

March 2023

- Targets cryptocurrency companies and users
- Uses an MSI package compromised with trojanized DLLs and a malicious macOS DYLIB
- Steals information, such as browser data and history, and launches additional attacks if the victim organization is valuable

Evasive Panda

April 26, 2023

- Targets China-affiliated individuals and individuals affiliated with NGOs in Hong Kong, Macau, and Nigeria
- Is distributed via software updates for legitimate applications
- Reportedly used backdoor MgBot

Konni Group LNK File Campaign

April - May 2023

- Targets Korean-language businesses
- Uses LNK files and tax-related decoy files in its attacks
- Is possibly motivated by monetary goals

SharpPanda

May 28, 2023

- Targets government agencies in Europe, United States, and Asia
- Is distributed by a decoy file that is a malware executable via the RoyalRoad exploit
- Is possibly a general intelligence operation against the Central Asian region

Group 123 LNK File Campaign

April - May 2023

- Targets individuals assumed to have expertise in the Democratic People's Republic of Korea (DPRK)
- Uses LNK files that infect victims with ROKRAT in its attacks