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)

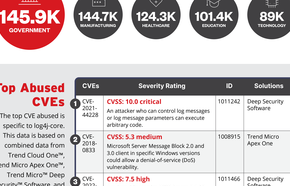
35.2B
Risky Cloud Access

18.5B
Risky Website Access

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

Top 3 Countries

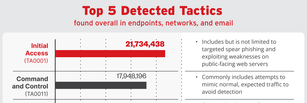
with risk events, malware detection, and malicious URL access



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

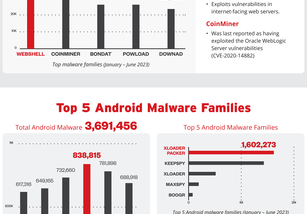
exploited in the wild

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



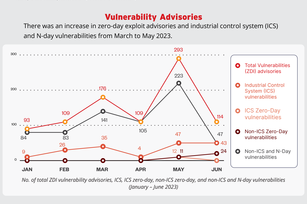
- Includes but is not limited to targeted spear phishing and exploiting weaknesses on public-facing web servers
- Commonly includes attempts to mimic normal, expected traffic to avoid detection
- Can involve the use of remote access tools or legitimate credentials with native network and operating system 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)

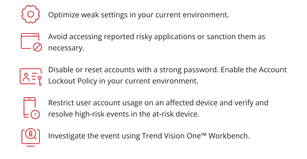
Detections from February to April show a shift in focus from Persistence to Defense Evasion and Impact tactics.



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