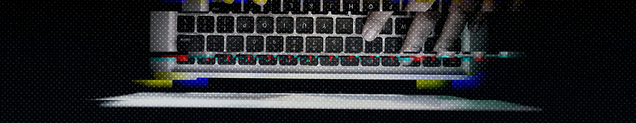


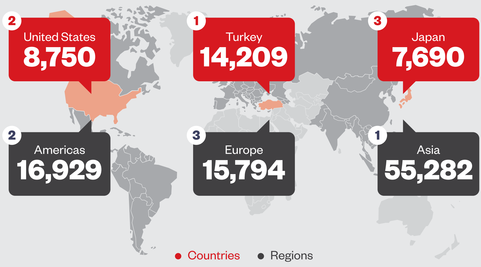
STEPPING AHEAD OF RISK

TREND MICRO 2023 MIDYEAR CYBERSECURITY THREAT REPORT

RANSOMWARE THREATS

Top 3 Countries and Regions

by detected ransomware attacks

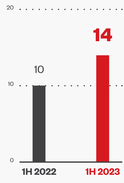


Top 3 Industries and Segments

by detected ransomware attacks

New Ransomware Families

found in the first half of 2023



Newly detected ransomware families

Mimic ransomware

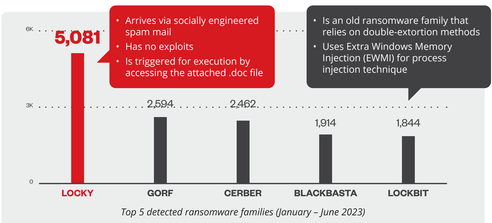
- Targets Russian- and English-speaking users.
- Abuses APIs of Everything, a Windows file name search engine, to query target files to encrypt.
- Has code similar to the 2022 Conti ransomware.

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

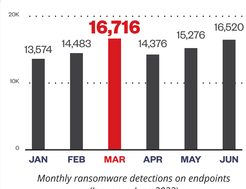
detected in the first half of 2023



Top 5 detected ransomware families (January – June 2023)

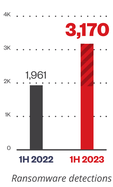
Ransomware Detections

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