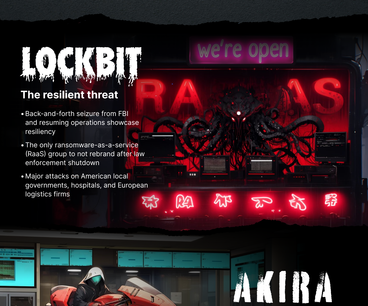
opentext™ Cybersecurity

2024 NASTIEST MALWARE

Top 6 Nastiest Malware of 2024

This year in cybersecurity shows digital threats evolving rapidly alongside AI. Our annual Nastiest Malware report highlights six notorious ransomware and malware groups that have caused significant disruptions across multiple sectors.



LOCKBIT

The resilient threat

- Back-and-forth seizure from FBI and resuming operations showcase resiliency
- The only ransomware-as-a-service (RaaS) group to not rebrand after law enforcement shutdown
- Major attacks on American local governments, hospitals, and European logistics firms

AKIRA

The healthcare menace

- Impacted over 250 organizations since showing up last year with over $50M in payments
- Encrypted patient data and threatened to release sensitive medical records
- Deployed a Linux variant targeting VMware ESXi virtual machines with great success

RANSOMHUB

The high-profile attacker

- Attacked Planned Parenthood and exfiltrated sensitive patient data
- Demonstrated a willingness to target organizations with significant social impact
- Believed to be the successor to the Black Cat (ALPHV) group

Dark Angels

The whaling experts

- Record breaking $75M ransom payment from a Fortune 50 company
- Stole proprietary information and threatened to leak sensitive content
- Typically steal vast amounts of data—more than 10TB

REDLINE

The credential thief

- Stole over 170M passwords in a six-month period
- Harvests user credentials, credit card details, and crypto wallets
- Attacked global retailer Target and stole 70M user accounts and 40M credit cards

Play Ransomware

The versatile threat

- Uses intermittent encryption to evade detection
- Exploits FortiOS vulnerabilities and exposed Remote Desktop Protocol (RDP) servers for initial access
- Focuses on IT services to orchestrate significant vendor or third-party attacks

GHASTLY GOINGS-ON

How are these cybercriminals evolving? A few trends we've noticed include:

AI-driven phishing and social engineering

AI and machine learning makes phishing emails more personal, convincing, and harder to detect.

Targeting critical infrastructure

Cybercriminals are attacking utilities and healthcare sectors, raising concerns about national security and public safety.

Fileless malware

There has been an increase in sophisticated, complex, and persistent kill chains, which are difficult to detect.

New malware language

Malware written in Golang continues to trend in both scale and complexity.

SURVIVAL TIPS

Protect your organization and yourself with these helpful survival tips:

Businesses

- Lock down RDP—this infiltration tactic has been around for a while, but it's still one of the top infection vectors.
- Enhance employee training: Go beyond basic awareness. Implement regular, interactive cybersecurity simulations and scenario-based training.
- PATCH OR DIE!
- Implement an in-depth, multi-layered security and defense posture.
- Adopt a comprehensive back-up strategy: Implement the 3-2-1 back-up rule with immutable backups to protect against ransomware attacks.
- Develop and test incident response plans: Create, regularly update, and practice cybersecurity incident response plans.

Individual users

- Use password managers: Employ a reputable password manager to create and store strong, unique passwords for all accounts—consider passphrases.
- Enable multi-factor authentication (MFA): Activate MFA on all accounts that offer it, preferably using authenticator apps or hardware keys.
- Keep software updated: Enable automatic updates for your operating system, applications, and security software.
- Be cautious with smart devices: Secure your IoT devices by changing default passwords and keeping firmware updated.
- Practice safe social media: Be cautious about the personal information you share on social media platforms.
- Use virtual private networks (VPNs): Employ a reliable VPN service, especially when using public Wi-Fi networks.

GET THE FULL NASTIEST MALWARE OF 2024 REPORT

Want more insights about threats and tips about how to protect against them?

Learn more