

This year in cybersecurity shows digital threats evolving rapidly alongside Al. Our annual Nastiest Malware report highlights six

Top 6 Nastiest Malware of 2024

notorious ransomware and malware groups that have caused significant disruptions across multiple sectors.

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





threatened to release sensitive medical records

since showing up last year with

over \$50M in payments

Encrypted patient data and

- Deployed a Linux variant targeting VMware ESXi virtual machines with great success

Demonstrated a willingness to target organizations with significant social impact Believed to be the successor to the Black Cat (ALPHV) group

RANSOMHUB

The high-profile attacker

 Attacked Planned Parenthood and exfiltrated sensitive patient data

1

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

Dark

Angels

The whaling experts

Play

REDLINE

The credential thief

Stole over 170M passwords

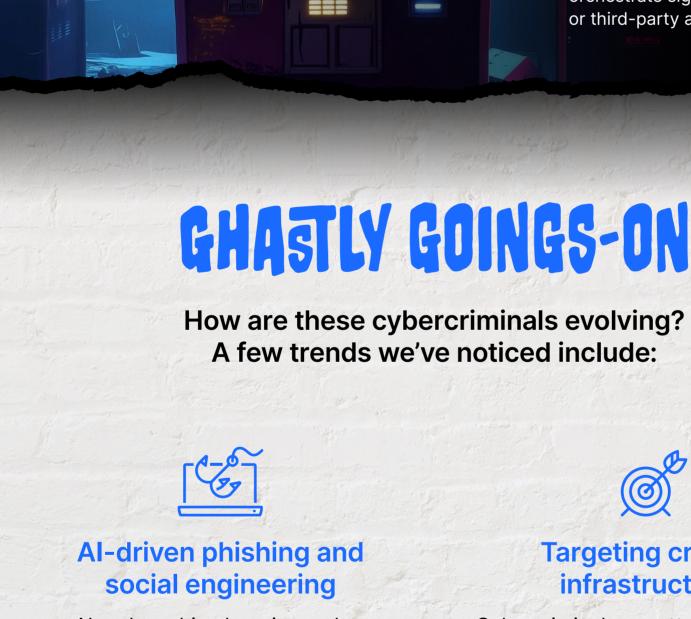
Harvests user credentials,

 Attacked global retailer Target and stole 70M user accounts

credit card details, and crypto wallets

in a six-month period

and 40M credit cards



or third-party attacks

orchestrate significant vendor

Ransomware

The versatile threat

Uses intermittent encryption

 Exploits FortiOS vulnerabilities and exposed Remote Desktop

Protocol (RDP) servers for

Focuses on IT services to

to evade detection

initial access

infrastructure Al and machine learning makes Cybercriminals are attacking utilities phishing emails more personal, and healthcare sectors, raising concerns



convincing, and harder to detect.

Fileless malware

There has been an increase in

sophisticated, complex, and persistent

kill chains, which are difficult to detect.

Protect your organization and yourself with these helpful survival tips:

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.

Lock down RDP—this infiltration tactic has

 Implement an in-depth, multi-layered security and defense posture. Adopt a comprehensive back-up strategy:

Businesses

PATCH OR DIE!

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.

Targeting critical about national security and public safety.

SURVIVAL TIPS

New malware language

Malware written in Golang continues

to trend in both scale and complexity.

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

passwords and keeping firmware updated.

your IoT devices by changing default

 Practice safe social media: Be cautious about the personal information you share on social media platforms.

Use virtual private networks (VPNs):

when using public Wi-Fi networks.

Employ a reliable VPN service, especially

GET THE FUL

NASTIEST MALWARE OF 2024 REPORT Want more insights about threats and tips

Learn more

about how to protect against them?