opentext™ Cybersecurity

2025 NASTIEST MALWARE

Top 6 nastiest malware of 2025

This year, ransomware evolved into AI-powered, identity-focused warfare. Our annual Nastiest Malware report highlights six notorious threat groups that have dominated 2025 through unprecedented sophistication and devastating business disruption.

QILIN

The Volume Leader

- Dominated 2025 as one of the most active ransomware groups with sustained high-tempo campaigns
- Revolutionary "Call Lawyer" feature provided legal counsel to affiliates during negotiations
- North Korean state adoption (Moonstone Sleet) signaled nation-state ransomware evolution
- Aggressively targeted healthcare, government, and critical infrastructure sectors

AKIRA

The Strategic Survivor

- Maintained consistent operations by not targeting hospitals and critical infrastructure
- Strategic pivot attracted skilled affiliates seeking lower-risk, high-value business targets
- Exploited SonicWall SSL VPN vulnerabilities in major July-August 2025 attack surge
- Professional RaaS model with generous profit-sharing kept affiliates loyal model, avoids attracting law enforcement.

SCATTERED SPIDER (UNC3944)

The Master Manipulator

- Arrests in UK and US (September 2025) revealed teenage operators behind massive extortion operations
- Lightning-fast attacks accessed domain admin in under 40 minutes
- Coordinated "wave" campaigns systematically targeted retail, insurance, and aviation sectors
- Advanced deepfake technology and helpdesk impersonation reached new sophistication levels

PLAY RANSOMWARE

The Supply Chain Specialist

- FBI reported victim count reached 900+ organizations by May 2025
- Used intermittent encryption strategy to evade detection while maximizing operational impact
- Professional victim communications, including phone threats and formal ransom demands
- Systematically targeted IT service providers for devastating supply-chain amplification targeting, quiet consistency.

SHINY-HUNTERS

The Data Extortion Specialists

- High-profile 2025 breaches: Google, Workday, Kering luxury brands, major financial institutions
- French law enforcement arrests in June 2025 disrupted core operations but group persists
- Strategic months-long delays before extortion maximized psychological and financial leverage
- Partnerships with Scattered Spider created hybrid threat collectives

LUMMA STEALER

The Phoenix Infostealer

- Rapid resurrection after Microsoft-led takedown seized thousands of malicious domains in May 2025
- Evolved distribution through GitHub repositories disguised as game cheats and software cracks
- Foundation technology enabled many ransomware attacks through credential theft
- New covert channels (Telegram, Steam, Cloudflare proxies) demonstrated remarkable resilience rapid variant evolution.

GHASTLY GOINGS-ON

2025's most sinister cyber trends

AI-powered social engineering

Deepfake voice calls and AI-generated phishing emails have reached near-perfect authenticity, with dramatic increases in vishing attacks directly linked to AI capabilities.

Identity-based attack revolution

The battlefield has shifted from network perimeters to identity systems, with stolen credentials now matching vulnerability exploitation as primary entry vectors.

Lightning-speed attack timelines

Average "breakout time" has collapsed dramatically, with fastest observed lateral movement occurring in under one minute, putting extreme pressure on detection capabilities.

Third-wave extortion tactics

Beyond encryption and data theft, attackers now deliberately sabotage business operations through DDoS attacks, customer harassment, and false regulatory complaints in most major incidents.

Malware-as-a-Service explosion

MaaS platforms democratized sophisticated attacks, with global malware attacks increasing substantially as technical barriers disappeared for entry-level cybercriminals.

SURVIVAL TIPS

How to stay out of the crosshairs

For businesses

- **Patch or Perish:** Prioritize internet-facing systems, VPNs, and edge security devices which represent the majority of initial access vectors.
- **Identity-first security:** Implement zero-trust architecture with MFA everywhere, especially for privileged accounts and SaaS applications.
- **AI-ready employee training:** Deploy deepfake detection training and real-time vishing simulations to combat AI-powered social engineering.
- **Incident response evolution:** Develop playbooks assuming extremely rapid breakout times with legal counsel integration for ransom payment decisions.
- **Immutable backup strategy:** Follow 3-2-1 rule with air-gapped, immutable copies to counter third-wave extortion tactics targeting recovery systems.

For individuals

- **Password manager mandatory:** Use enterprise-grade password managers with passphrase generation for all accounts.
- **Deepfake awareness:** Verify unusual requests through alternative communication channels, especially financial or access-related demands.
- **MFA everywhere:** Enable hardware-based authentication where possible, avoiding SMS-based systems vulnerable to SIM swapping.
- **Social media discipline:** Limit oversharing of personal information that enables AI-powered personalized attacks.
- **Software vigilance:** Keep all systems updated and avoid downloading software from unofficial sources or social media promotions.

STAY AHEAD OF 2025'S NASTIEST MALWARE.

Contact us