opentext™ | Cybersecurity

2023 NASTIEST MALWARE

Five years of malware intel

We've seen a steady increase in the number and sophistication of malware attacks over the five years we've made this list. As malware gets nastier, our security methods and tools must evolve to keep up.

Nastiest, most costly, dangerous threats in **2023:**

Cl0p

(AKA TA505)

- Ransomware-as-a-service (RaaS) with double extortion leaks sites
- Delivered via phishing emails from botnets—also available for hire
- Exploited MoveIT platform, hitting 3 of the top 4 accounting firms

BLACK CAT

(AKA ALPHV)

- Easily customizable RaaS built on Rust programming language
- Believed to be the successor to the REvil ransomware group (#1 in 2021)
- Made headlines in Sep. 2023 for taking down MGM Casino resorts

AKIRA

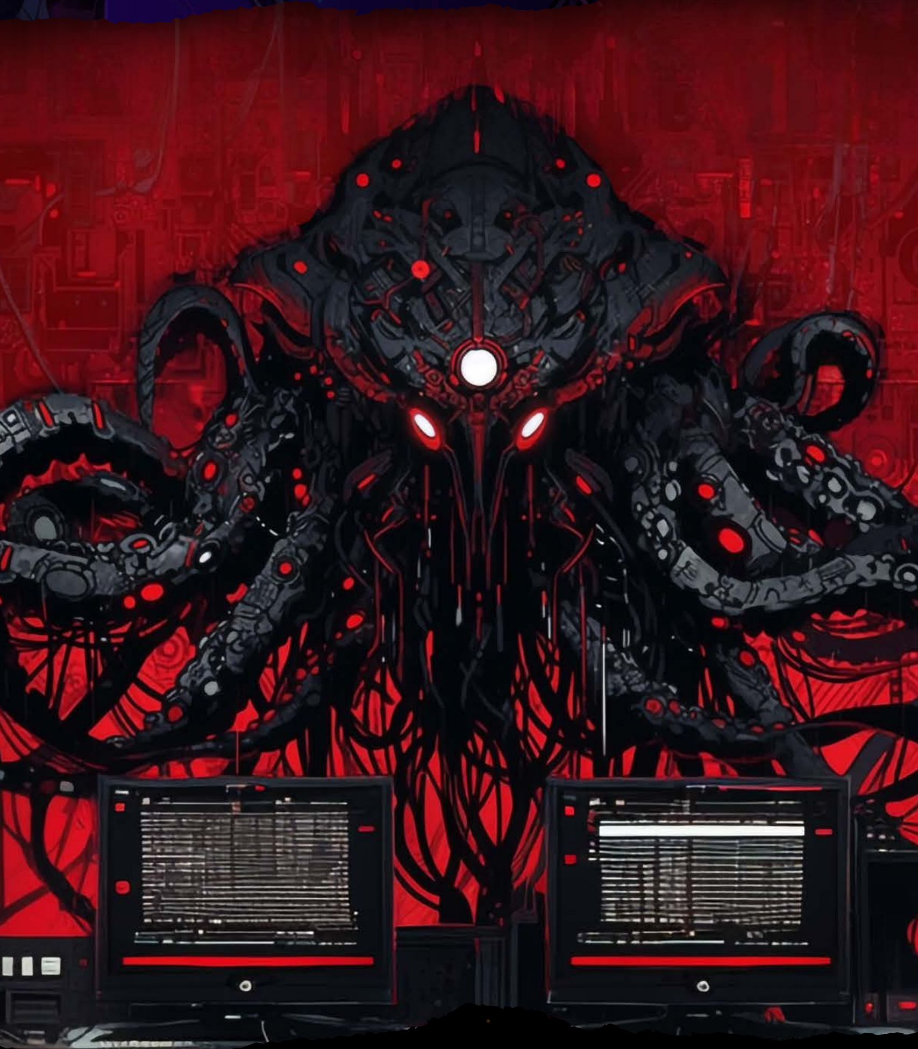
- New RaaS platform—targets small to medium-sized businesses
- Believed to be the successor to the Conti ransomware group
- Uses web-based terminal emulator for a retro 80s look

Royal

- Uses partial encryption to evade detection and changes file extension to ".royal"
- Believed to be the successor to the Ryuk ransomware group
- Targets IT, finance, materials, healthcare, and government

LOCKBIT 3.0

- Third epoch is more modular and evasive than previous versions
- Pioneered triple extortion (leak site & DDOS) and offers extensive bug bounties
- Targets small- to medium-sized businesses



BLACK BASTA

- Steals sensitive data via phishing or vulnerabilities for initial infection vector
- Spreads laterally with white hat pen-testing tools
- Targets many different types of industries indiscriminately

GHASTLY GOINGS-ON

Learn about the latest tactics from this year's nastiest malware.

If it talks like a duck, it's probably qakbot

Qakbot/Pinkslip bot/Qbot has been especially active this year.

Did someone order Doordash?

Delivery methods pivoted to OneNote files and shortcuts .lnk to deliver payloads.

They're getting smarter

Chat GPT and similar LLMs have likely made phishing and malware lures more sophisticated.

It's not safe to talk here

A data breach at Discord leaked the data of 750k users—now we're seeing malware specifically targeting Discord and its users.

MOBILE MENTIONS

This year we're highlighting some of the nastiest mobile malware.

GravityRAT

- New Android malware targeting WhatsApp backups
- Steals messages, contacts, and other data from devices
- Uses two-factor authentication codes to control WhatsApp accounts

FakeCalls

- Android Trojan targeting South Korean banks
- Can mimic 20+ financial applications and imitate phone conversations with employees
- Extracts private data from devices.

Breaking Bad

- Legitimate app secretly recording users' screens and exfiltrating data
- Available on Google Play, has over 100,000 downloads
- Collects sensitive data such as passwords and credit card numbers

SURVIVAL TIPS FROM OUR USERS

Businesses:

- Lock down Remote Desktop Protocols (RDP).
- Educate end users.
- Patch or die!
- Install reputable cybersecurity software—layered security plan.
- Set up a strong backup and disaster recovery plan.

Individual users:

- Develop a healthy dose of suspicion toward messages.
- Protect your devices with antivirus and VPN.
- Keep your antivirus software and other apps up to date.
- Use a secure cloud backup.
- Create strong, unique passwords (and don't share them).
- Use passphrases to increase password characters and defend against brute force.
- Don't enable macros if a downloaded file asks you to.

Get more intel

This infographic is just a taste of our thorough report on the **nastiest malware** of **2023.** Check out **our post** for more details and survival tips.

opentext™ | Cybersecurity