NASTIEST MALWARE 2020

Each year, threat research experts comb through data to identify the nastiest malware they've seen throughout the year. Phishing and RDP (Remote Desktop Port) attacks continue to be major threats, particularly with more people working from home due to the COVID-19 pandemic. Additionally, many types of malware are now designed to join forces to maximize danger.

Here are this year's wicked winners and how they work together.

Emotet

- #1 malicious spam botnet
- Heavily used and "friends" with most malware
- Responsible for the most ransomware
- Creates backdoor for info stealers and others

TrickBot

- Banking and info-stealing Trojan and backdoor
- Spreads laterally and listens for domain credentials so attackers can disable protections and perform recon
- Eventually leads to ransomware like Ryuk

Dridex

- Banking and info-stealing Trojan and backdoor
- Spreads laterally and listens for domain credentials
- Eventually leads to ransomware like BitPaymer/DoppelPaymer

QakBot

- Possibly the oldest info-stealing Trojan still getting updates today
- May be delivered by its own malspam
- Favors ProLock ransomware (not featured here)

Ransomware as a Service (RaaS)

These for-hire ransomware payloads are often distributed via malicious spam emails and RDP attacks with brute-forced, easily guessed or previously phished/stolen credentials.

Valak

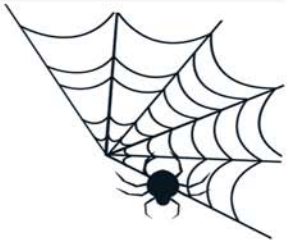
- Banking and info-stealing Trojan and backdoor
- Spreads laterally and listens for domain credentials so attackers can disable protections and perform recon
- Eventually leads to ransomware like Ryuk

Sodinokibi/REvil/GandCrab

- Banking and info-stealing Trojan and backdoor
- Spreads laterally and listens for domain credentials so attackers can disable protections and perform recon
- Eventually leads to ransomware like Ryuk

CrySIS/Dharma/Phobos

- Banking and info-stealing Trojan and backdoor
- Spreads laterally and listens for domain credentials so attackers can disable protections and perform recon
- Eventually leads to ransomware like Ryuk



Ursnif

- Info-stealing Trojan that's almost as old as QakBot
- Often associated with IcedID

IcedID

- Upgraded Trojan with steganographic payloads
- Often dropped by TrickBot and Ursnif
- Typically results in Maze ransomware

Conti / Ryuk

- #1 ransomware according to victim reports to the FBI
- TrickBot's favorite ransomware
- Will leak or auction off your data if you don't pay the ransom

Maze

- Goes after the largest targets for juicy payouts
- Also uses malspam and RDP as attack vectors
- Believed to have "pioneered" the data leak/auction site phenomenon

BitPaymer / DoppelPaymer

- Highly successful ransomware
- Also uses a data leak/auction site if you don't pay the ransom

HOW TO STAY SAFE

Since modern cyberattacks use multiple attack vectors and tactics to ensure success, you need a multi-layered protection strategy.

Here are some tips from our experts.

BUSINESSES

Lock down RDP.
Use RDP solutions that encrypt the data and use multi-factor authentication to increase security when remoting into other machines.

Educate end users about phishing.
Many attack scenarios could be prevented with stronger phishing/spam awareness among end users. Run regular cybersecurity awareness training and phishing simulations with actionable feedback. Also, make sure employees know when and how to report a suspicious message.

Install reputable cybersecurity software.
Choose a solution that uses real-time, global threat intelligence and machine learning to stop threats. Look for protection with multi-layered shielding to detect and prevent attacks at numerous different attack stages.

Set up a strong backup and disaster recovery plan.
Particularly with a mostly or entirely remote workforce, businesses can't afford not to have a strong backup. Test backups regularly and set alerts so admins can easily see if something's amiss.

computer dimensions

520.210.0909
computerdimensions.net

INDIVIDUALS

Develop a healthy dose of suspicion toward messages.
Don't click on links or attachments in emails. Be suspicious of any emails, texts, phone calls, or social media messages that ask for personal info.

Protect your devices with antivirus and a VPN.
Be sure to secure not just computers, but smartphones and tablets, too. And when you ditch an old device, be sure to wipe it first.

Keep your antivirus software and other apps up to date.
Hackers can use outdated software and operating systems to get malware into your system and steal from you. Do your updates.

Use a secure cloud backup.
We recommend using both an online backup that stores your data in an encrypted format, and also a physical backup drive that you unplug when not in use.

Create strong, unique passwords (and don't share them.)
You can use a password manager to help you create and store good passwords. That way, you don't have to remember them all or write them down.

If a file you downloaded asks you to enable macros, DON'T DO IT.
This is a strong telltale sign that the file is infected with malicious code. Even though macros have legitimate uses, they are extremely rare in a normal home user context.