R

Ramnit Malware: File Infection, Banking Theft, Removal, and Recovery

Ramnit evolved from a Windows file-infecting worm into a banking Trojan and botnet. Learn how it spreads, why widespread infection often requires a rebuild, and which accounts to secure.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
5 min

CONTENTS

In this guide

01 How Ramnit evolved
02 What Ramnit can infect or collect
03 Signs of a Ramnit infection
04 Immediate response
05 Removal versus rebuild
06 Account and network recovery
07 Prevention
08 Frequently asked questions
09 References

Ramnit is a Windows malware family that began as a file-infecting virus and worm around 2010 and evolved into a modular botnet and banking Trojan. It can infect executable and other files, spread through removable drives, steal browser and FTP credentials, provide remote access, and download additional components.

A confirmed Ramnit infection is more serious than a single removable Trojan file: infected applications can multiply across the device, and stolen credentials remain at risk even after the malware is removed.

01 How Ramnit evolved

Stage	Main capabilities	Defensive implication
Early file infector and worm	Infected Windows executables, HTML, and some Office files; copied itself to removable drives.	Many local files and external media may need inspection or replacement.
Botnet and banking Trojan	Added command-and-control, browser injection, credential and cookie theft, downloads, screenshots, and remote-control functions.	Removal must be followed by account recovery and network scoping.
Later variants and campaigns	Capabilities and infection methods varied; not every sample retained every original file-infection feature.	Use the exact detection and behavior rather than assuming one fixed feature list.

In 2015, an international operation coordinated by Europol targeted Ramnit infrastructure associated with millions of infected computers. A takedown reduces active infrastructure at a point in time; it does not make old infected files safe or prevent later operators and variants from appearing.

02 What Ramnit can infect or collect

- Windows executable files such as EXE, DLL, and SCR files in variants with file-infection capability;

- HTML files by appending script code;
- some Microsoft Office documents through malicious macro content;
- removable and mapped drives using copies and, in older environments, AutoRun-related mechanisms;
- browser cookies, web sessions, and banking or other login data;
- stored credentials from FTP and file-transfer applications;
- system information requested by command-and-control components.

Ramnit can also inject code into legitimate processes, weaken security settings, terminate security tools, receive instructions, and install other malware. The exact behavior depends on the variant and downloaded modules.

03 Signs of a Ramnit infection

- A security product reports Ramnit in several legitimate-looking executables rather than one downloaded file.
- The number of infected files grows between scans.
- HTML or Office files change unexpectedly or trigger new script and macro alerts.
- Unknown executables and AutoRun artifacts appear on USB or network drives.
- Security services, Windows Update, firewall settings, or user-account controls are disabled.
- Browsers or system processes make unexplained outbound connections or contain injected code.
- Bank, email, FTP, or other accounts show unfamiliar access after use on the device.

One generic or machine-learning alert can be a false positive. Preserve the full detection name, paths, hashes, and scan log. A pattern across multiple changed host files, persistence, and network activity is much stronger evidence.

04 Immediate response

1. **Isolate the device.** Disconnect networks and remove external storage so the infection cannot spread or continue communicating.
2. **Stop using it for accounts.** Do not log into banking, email, password managers, or administrative services from the suspected system.
3. **Preserve evidence.** Save alert details and, for an organization, involve incident response before deleting files or reimaging.
4. **Identify connected media and shares.** List USB drives, external disks, mapped drives, shared folders, and backup destinations accessed by the computer.
5. **Scan from a trusted environment.** Use current vendor-supported offline or recovery media because active malware may interfere with security tools.

05 Removal versus rebuild

Finding	Recommended direction
Downloaded file was blocked before execution and no other artifacts exist	Quarantine it, run full and offline scans, and verify that it never launched.
A small, known set of data files is detected but the host shows no execution	Keep the files quarantined and validate with the security vendor; do not open them while investigating.
Multiple executables or system files are infected	Prefer a full reimage from trusted media. Disinfection can leave damaged or missed host files.
Security controls were disabled, credentials were stolen, or a backdoor ran	Treat the system as fully compromised, rebuild it, rotate credentials, and investigate other systems.

Do not restore application executables from a backup that may have been connected during the infection. Reinstall software from original trusted packages. Restore documents from a backup created before the incident and scan them in a controlled environment.

06 Account and network recovery

1. From a known-clean device, change passwords used on the infected computer.
2. Prioritize email, banking, password managers, remote access, FTP, cloud, and administrator accounts.
3. Revoke active sessions, browser tokens, application passwords, and remembered devices; enable MFA.
4. Contact financial providers about suspicious access or transactions.
5. Search other endpoints for Ramnit detections, infected files, removable-media exposure, unusual authentication, and related command-and-control.
6. Monitor for recurrence after rebuilt systems return to service.

07 Prevention

- Keep Windows, browsers, Office, and security software supported and updated.
- Block untrusted macros, scripts, and executables from email and downloads.
- Disable AutoRun where it is not needed and scan removable media before use.
- Use application control and restrict write access to shared software locations.
- Segment user networks and limit administrative and file-share credentials.
- Maintain offline, versioned backups and test restoration without carrying executable files forward.

08 Frequently asked questions

Does downloading a Ramnit-infected file infect the computer?

Not necessarily. It normally must execute or be opened by a vulnerable or script-capable application. Do not test it; quarantine it and verify with full and offline scans.

Can antivirus repair every infected file?

No. Some known variants can be disinfected, but host files may be damaged or the full set may be unknown. Reinstalling from trusted media is more reliable after widespread infection.

Can Ramnit spread to a USB drive?

Yes, documented variants copied themselves to removable drives. Isolate and scan every drive connected to a confirmed infected system before using it elsewhere.

09 References

- Microsoft Security Intelligence: Win32/Ramnit
- Europol: Ramnit botnet operation
- Malwarebytes: Ramnit file-infector detection and aftermath

NEED MORE HELP?

We are here when the guide is not enough.

Visit the Gridinsoft Support Center for current product guidance or submit a support request with the details of your case.

Open this guide online at support.gridinsoft.com