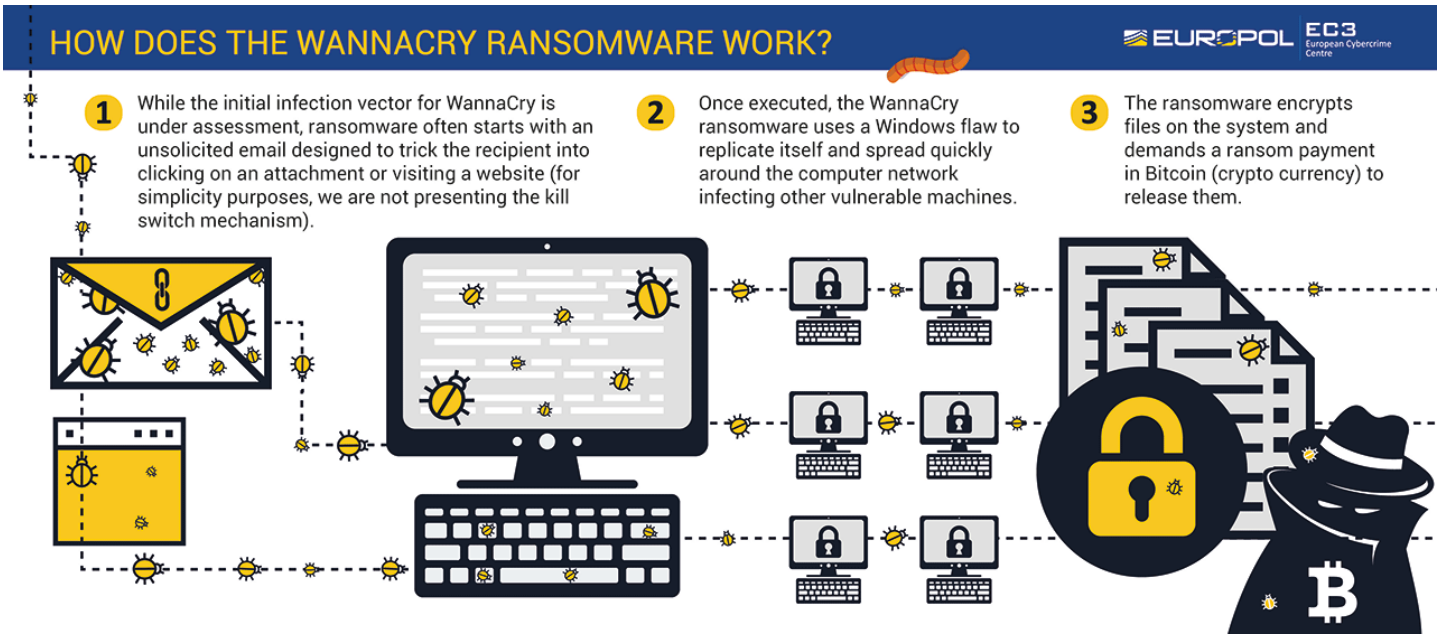
WANNACRY RANSOMWARE



The European Cybercrime Centre (EC3) at Europol is working closely with cybercrime units in affected countries and with key industry partners to provide operational support and to coordinate international efforts to mitigate the threat and help victims. The recent attack is at an unprecedented level and requires a complex international investigation to respond effectively and identify the culprits. The Joint Cybercrime Action Taskforce (J-CAT) at EC3 - a unique operational team of international cyber investigators, specially designed to assist in such cross-border cases, is playing an important role in supporting the investigation.

WHAT IS IT?

Ransomware is malware that prevents or limits users from accessing their systems or devices, demanding they pay a ransom, using certain online payment methods and by a set deadline, in order to regain control of their data.

Crypto ransomware is a type of malware that encrypts user data and demands a ransom (usually payable with Bitcoin cryptocurrency) in order to decrypt the data. WannaCry is a crypto ransomware variant which has massively spread around the world since 12 May 2017. It is also known as WannaCrypt, WanaCrypt0r, WRrypt, and WCRY.

Since its detection, businesses, organisations and individual users across Europe and beyond have been greatly affected.

WHY IS IT CAUSING SO MANY PROBLEMS FOR ORGANISATIONS?

WannaCry is a dangerous combination of two malicious software components:

1. A **worm** that has the ability to spread itself within networks without user interaction
2. A **ransomware variant** that encrypts user files and then asks for money in order to decrypt the files.

HOW DOES WANNACRY SPREAD?

At the moment, the initial attack vector is being assessed. It appears that the infection vector relies on the remote exploitation of a known Microsoft Windows vulnerability in the Server Message Block (SMB) protocol (SMB is a Microsoft Windows protocol for file-sharing over a network). Once a system becomes infected, the ransomware propagates through the network, infecting other vulnerable devices, without the need for any user involvement.

WHICH VERSIONS OF WINDOWS ARE VULNERABLE?

The exploit works on versions of Windows that have not been updated since 14 March 2017 onwards, especially those platforms that are in custom support only, including Windows XP, Windows 8, and Windows Server 2003, among others.

CAN YOU RECOVER THE ENCRYPTED FILES?

Decryption of WannaCry encrypted files is currently not possible.

Your options to recover affected files:

- Restoring from backups
- In some cases, files may be recovered without backups:
  - From Shadow Copies (if enabled)
  - Using an undelete tool.
  - The partial solution developed by Benjamin Delpy, Matt Suiche and Adrien Guinet has been tested by EC3 and found to recover data encrypted by WannaCry in some circumstances. Infected victims are advised not to reboot their machines and to try it by following the instructions: WannaCry — Decrypting files with WanaKiwi + Demos

In any case, **do not pay the ransom**. Paying does not guarantee that your problem will be solved and that you will be able to access your files again. In addition, you will be supporting the cybercriminals' business and the financing of their illegal activities.

REPORTING

If you have fallen victim of the WannaCry ransomware, please report it to the competent authorities in your country. Reporting mechanisms vary from one country to another. More information on official reporting channels in the EU Member States is available here. Alternatively, you are strongly encouraged to go to your local police station to make an official report.

IF YOU ARE A VICTIM OR HAVE REASON TO BELIEVE THAT YOU COULD BE A VICTIM:

This link provides some practical advice on how to contain the propagation of this type of ransomware: https://www.ncsc.gov.uk/guidance/ransomware-latest-ncsc-guidance
The most important step involves patching the Microsoft vulnerability (MS17-010):
https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

A patch for legacy platforms is available here:
https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks

In instances where it is not possible to install the patch, managing the vulnerability becomes key. One way of doing this is to disable the SMBv1 (Server Message Block) protocol:
https://support.microsoft.com/en-us/help/2696547_
and/or block SMBv1 ports on network devices [UDP 137, 138 and TCP 139, 445].

Another step would be to update endpoint security and AV solutions with the relevant hashes of the ransomware (e.g. via VirusTotal).

If these steps are not possible, not starting up and/or shutting down vulnerable systems can also prevent the propagation of this threat.

IF YOU HAVE NOT BEEN INFECTED:

Apply the following recommendations as soon as possible:

1. Back-up and protect your systems and files
2. Update your antivirus signature database to the latest version. Antivirus firms are now detecting all the current variations of the ransomware.
3. CCN-CERT (Spanish CERT) has developed a Vaccine, which prevents WannaCry from executing and encrypting a system if the system gets infected by WannaCry afterwards. Users can use this tool as an added layer of security in addition to the rest of the recommendations and not instead of them.

HOW TO PREVENT A RANSOMWARE ATTACK?

1. **Back-up! Back-up! Back-up!** Have a backup and recovery system in place so a ransomware infection cannot destroy your personal data forever. It is advisable to create at least two back-up copies on a regular basis: one to be stored in the cloud (remember to use a service that makes an automatic backup of your files) and one stored locally (portable hard drive, thumb drive, etc.). Disconnect these when you are done and store them separately from your computer. Your back-up copies will also come in handy should you accidentally delete a critical file or experience a hard drive failure.
2. **Use robust antivirus software** to protect your system from ransomware. Always use the latest virus definition/database and do not switch off the 'heuristic' functions as these help the solution to catch samples of ransomware (and other type of malware) that have not yet been formally detected.
3. **Keep all the software on your computer up to date.** When your operating system (OS) or applications release a new version, install it. If the software that you use offers the option of automatic updating, enable it.
4. **Trust no one. Literally.** Any account can be compromised and malicious links can be sent from the accounts of friends on social media, colleagues, or an online gaming partner. Never open attachments in emails from someone you don't know. Similarly, don't open attachments in emails from somebody you know but from whom you would not expect to receive such a message. Cybercriminals often distribute fake email messages that look very much like email notifications from an online store, a bank, the police, a court or a tax collection agency, luring recipients into clicking on a malicious link and releasing the malware into their system. If in doubt, call the sender at a trusted phone number to confirm the legitimacy of the message received.
5. **Enable the 'Show file extensions' option in the Windows settings on your computer.** This will make it much easier to spot potentially malicious files. Stay away from file extensions like '.exe', '.com', '.vbs' or '.scr'. Cybercriminals can use several extensions to disguise a malicious file as a video, photo, or document (like hot-chics.avi.exe or report.doc.scr).
6. If you discover a rogue or unknown process on your machine, **immediately disconnect it from the internet or other network connections (such as home Wi-Fi)** — this will prevent the infection from spreading.

For further information, download our tips and advice infographic.

Law enforcement and IT security companies have joined forces to disrupt cybercriminal businesses

with ransomware connections.

The No More Ransom portal is an initiative by the National High Tech Crime Unit of the Netherlands' Police, Europol's European Cybercrime Centre and two cyber security companies – Kaspersky Lab and Intel Security. The goal is to help victims of ransomware retrieve their encrypted data without having to pay the criminals. More than 80 partners from the public and private sectors all over the world have joined the project since its launch in July 2016.

As it is much easier to avoid the threat, rather than fight it once infected, the project also aims to educate users on how ransomware works and what countermeasures can be taken to effectively prevent infection.

CRIME AREAS: Cybercrime
TARGET GROUPS: General Public • Law Enforcement • Academia • Professor • Students • Researcher • Press/Journalists • Other

---

Source URL: https://www.europol.europa.eu/wannacry-ransomware#comment-0