Ukrainian Man Arrested, Charged in NotPetya Distribution

By Tom Spring

Published: 2017-08-11 · Archived: 2026-04-05 17:00:04 UTC

Ukranian police arrested a suspect alleged to have distributed the NotPetya/ExPetr malware that ultimately infected 400 computers.

The Cyber Police of Ukraine arrested a suspect they allege distributed the destructive NotPetya/ExPetr malware resulting in the infection of 400 computers.

NotPetya/ExPetr was the malware behind a massive global cyberattack that took place earlier this year. It infected computers worldwide with wiper malware disguised as a ransomware attack; the bulk of infections were in the Ukraine.

The unidentified Ukrainian man, 51, was arrested earlier this week at his home in Nikopol.

Police allege the man uploaded a video to a file exchange service that contained instructions on how to run the malware, and shared links to the video on a personal blog and social media. Links from the video pointed to downloads of the Petya.A malware, said police. In all, authorities said, 400 victims followed the link and downloaded the malware to their computers and became infected. Victims were unaware of what exactly they were downloading at the time, according to a translation of the Cyber Police of Ukraine's report of the arrest.

This summer's outbreak was a wiper attack that sabotaged PCs globally, overwriting their Master Boot Record forever. It's important to note the suspect was not accused of creating Petya.A.

NotPetya/ExPetr spread using the leaked NSA EternalBlue and EternalRomance exploits, infecting machines that still had not applied the MS17-010 Microsoft update that patches a handful of SMBv1 vulnerabilities targeted by the exploit.

The malware initially impacted critical industries and services in Ukraine, Russia and then throughout Europe, including the radiation monitoring station for the crippled Chernobyl nuclear power plant and pharmaceutical giant Merck and Co.'s MSD operation in the United Kingdom.

In June, the Ukraine's Cyber Police said the initial infection vector was via an update mechanism for Ukrainian financial software provider MEDoc. Cisco, Kaspersky Lab and Microsoft also implicated the company, saying that its software update system had been compromised and was serving up the ransomware in phony updates.

Interestingly, during the police seizure of the suspect's computers, it found a list of companies that it claimed used the Petya malware to purposely sabotage their own computers to hide incriminating information. "They specifically infected their own computers to cover up (unspecified) illegal activities and evade the payment of fines to the government," according to a translation of the report.

Authorities said the suspect is being charged under criminal proceedings tied to “unauthorized interference with the work of computers,” according to a translation of the post.
