Russian wipers in the cyberwar against Ukraine Alexander Adamov NioGuard Security Lab

Published: 2022-10-24 · Archived: 2026-04-05 14:10:25 UTC

Presented at the VB2022 conference in Prague, 28 - 30 September, 2022. ↓ Slides: https://www.virusbulletin.com/uploads... ↓ Paper: https://www.virusbulletin.com/uploads... → Details: https://www.virusbulletin.com/confere... ✪ PRESENTED BY ✪ • Alexander Adamov (NioGuard Security Lab) ✪ ABSTRACT ✪ The story of Russian wipers used in Ukraine began in 2015 when the APT28 group (Russian GRU) attacked the Ukrainian power grid with the BlackEnergy backdoor and KillDisk wiper to take down the SCADA servers in the power distribution centres. Thus, the attackers left 230,000 residents in Western Ukraine without electricity for six hours. Two years later, in June 2017, the same APT28 group ran a supply-chain attack delivered through another wiper, called NotPetya, which was a patched version of the Petya ransomware but without the ability to decrypt MFT. This year we've been seeing an unprecedented chain of Russian cyberattacks against Ukrainian government organizations and critical infrastructure using a variety of different wipers that have nothing in common. It all started with the WhisperGate operation, discovered by Microsoft on 13 January 2022, against Ukrainian financial and government institutions where a rather complex wiper was used that rewrote not only the MBR but also part of the data on all hard disks while being in boot mode. The day before the Russian army invaded Ukraine (23 February 2022), the HermeticWiper malware was used in an attack against at least five government organizations in Ukraine. The wiper used legitimate drivers from the EaseUS Partition Master software to get direct access to disk partitions. The next day (24 February 2022), researchers from ESET detected another wiper, which they called IsaacWiper. Later, on 14 March 2022, ESET discovered one more basic wiper, CaddyWiper, which simply fills the first 1920 bytes of disks with zeros, making a target system unbootable. In April, CERT-UA reported a new attack against the Ukrainian power grid with a new version of the Industroyer malware used previously in 2016 by the Russian Sandworm group and an encoded version of the already known CaddyWiper that was launched and decoded using a patched version of the remote IDA debugger server 'win32_remote.exe' known to all reverse engineers. The attackers established a foothold in February 2022 and planned to take down the energy systems on the evening of Friday 8 April 2022. The last attack may show that the Russian GRU (APT28, Sandworm) does not have enough resources to develop a new cyberweapon and switched to the malware reuse practice or "malware recycling". Moreover, this tactic has already been seen in 2017, when the Russian APT28 group was using clones of open-source or stolen ransomware such as XData (originally AES-NI ransomware, whose source code had been stolen), PsCrypt (Globe), WannaCry.NET (similarly to WannaCry, the EternalBlue exploit was used in the .NET version of the ransomware), NotPetya (Petya's binary was patched to irreversibly destroy an MFT) in the supply-chain attack via the compromised MEDoc software. In the talk, we'll run through the techniques that were used to deliver and execute the wipers as well as their destructive payloads and indicators that can be useful for attribution.
