# CaddyWiper

Threat: **Wiper**

Author: **Jeffrey Farnan** Date Originally Published: **June 29th, 2022**

## 1. SUMMARY


- CaddyWiper is a new wiper malware first discovered on March 14, 2022 in Ukraine. This wiper malware is specifically designed to damage targeted systems by erasing user data, programs, hard drives, and in some cases, partition information. As Russia's invasion of Ukraine continues, Threat Actors are infiltrating specific networks of organizations deemed high value before unleashing the wiper. Wipers are not focused on theft or financial gain but rather they erase everything in their path for purely destructive purposes.


## 2. MALWARE FAMILY

- **Type** = Wiper.
- The name "Wiper" comes from a single piece of malware which appeared back in 2012, but it has come to be associated with a whole class of malware intended to erase (wipe) the hard drive of the computer it infects, maliciously deleting data and programs. Wiper malware can be defined as malicious software that tries to destroy data and are now included as part of large-scale cyberattacks**.**

## 3. MALWARE CHARATERISTICS

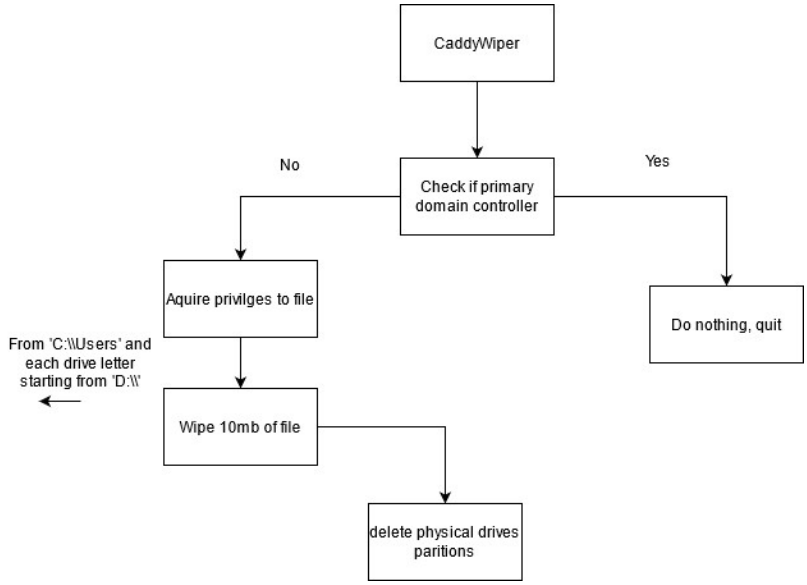
- **Suspected country of origin** = Russia.
- **First seen date/period** = March 14, 2022.
- **Still active** = Yes.
- **Last submitted sample as of writing this article** = May 25, 2022.

## 4. MALWARE HISTORY

- Wipers have been in existence since 2012 some of the first cases found were shutting down computer systems in Iran.
- In 2014 a wiper made major news when it lead to a massive data destruction against Sony Pictures who was planning to release a movie about the North Korean leader, this attack is believed to have come from North Korea.
- CaddyWiper is the third wiper malware to hit Ukraine since February 23$^{rd}$ but bears no major code similarities to either of the other two called HermeticWiper and IsaacWiper.

## 5. MALWARE DESCRIPTION

- CaddyWiper's primary purpose is to destroy user data and partition information for each available disk. The malware overwrites the main drive and any attached drives with null bytes which would corrupt them and destroy any stored data. It is smaller (compiled size of 9KB) than previous wipers attacks found in Ukraine and has less complex capabilities than the others.
- The different stages of the CaddyWiper execution flow:




  - When CaddyWiper is executed it first checks if the computer is a domain controller (DC). A domain controller is a server that responds to authentication requests and verifies users on a computer network. If the machine is a domain controller it does nothing, stops execution, allowing the attackers to keep their access inside the organization while still disturbing operations.
  - If the machine is not a domain controller the malware attempts to acquire admin privileges to gain access to the system files and folders.
  - It starts wiping files at "C:\\Users" so as not to break the operating system before the wiping process completes.
  - When this stage is complete, the malware will attempt to access drives attached to the target system form "D:\\" to "Z:\\".
  - If the malware was run with admin privileges it deletes the partition of the physical drive to absolutely wreak the operating system.

- The creators of CaddyWiper were extremely careful to destroy absolutely every single piece of data which could be used to trace any incidents in which it was involved.
- CaddyWiper has been used in much larger cyberattacks recently used in combination with Industroyer2 malware which can take down electric grids. The Industroyer2 malware is designed to disrupt the working processes of Industrial control systems (ICS), it is modular malware with its many components each designed for a specific purpose. CaddyWiper is the wiper component of this cyberattack used to make the system unbootable and also leave no trace of the larger cyberattack.

## 6. POTENTIAL CUSTOMER DEFENSE

- CaddyWiper is mostly used in cyberattacks against targeted companies with the aim of disrupting operations, destroying evidence or just to cause havoc to the companies. Hackers would usually have gained access to the company's network and taken anything of value before CaddyWipper would be deployed.
- Purely defensive measures will not prevent a wiper attack. There are measures that will at least increase your odds of not being caught by this malware. Some recommendations include:
    - Maintain up-to-date antivirus software.
    - Keep operating system patches up-to-date.
    - Enable a personal firewall on workstations and configured to deny unsolicited connection requests.
    - Regularly back up all important data, preferably offsite.
    - Harden all information systems to the greatest extent possible.
    - Recovery, response and business continuity plans should be tested and continuously tightened.
    - User and network segmentation and overlapping anti-malware solutions.

**Research Sources:**


- https://blog.morphisec.com/caddywiper-analysis-new-malware-attacking-ukraine
- https://resources.infosecinstitute.com/topic/malware-spotlight-what-are-wipers/
- https://www.cisa.gov/uscert/ncas/analysis-reports/ar22-115c
- https://www.welivesecurity.com/2022/03/15/caddywiper-new-wiper-malware-discovered-ukraine/
- https://blog.talosintelligence.com/2022/03/threat-advisory-caddywiper.html
- https://www.zdnet.com/article/caddywiper-more-destructive-wiper-malware-strikes-ukrainian-targets/
- https://www.bleepingcomputer.com/news/security/new-caddywiper-data-wiping-malware-hits-ukrainian-networks/