Share

ESET researchers spot an updated version of the malware loader used in the Industroyer2 and CaddyWiper attacks

Sandworm, the APT group behind some of the world's most disruptive cyberattacks, continues to update its arsenal for campaigns targeting Ukraine.

The ESET research team has now spotted an updated version of the ArguePatch malware loader that was used in the Industroyer2 attack against a Ukrainian energy provider and in multiple attacks involving data wiping malware called CaddyWiper.

The new variant of ArguePatch — named so by the Computer Emergency Response Team of Ukraine (CERT-UA) and detected by ESET products as Win32/Agent.AEGY — now includes a feature to execute the next stage of an attack at a specified time. This bypasses the need for setting up a scheduled task in Windows and is likely intended to help the attackers stay under the radar.

#BREAKING #Sandworm continues attacks in Ukraine 🇺🇦. #ESETresearch found an evolution of a malware loader used during the #Industroyer2 attacks. This updated piece of the puzzle is malware @_CERT_UA calls #ArguePatch. ArguePatch was used to launch #CaddyWiper. #WarInUkraine 1/6 pic.twitter.com/y3muhtjps6

— ESET research (@ESETresearch) May 20, 2022

Another difference between the two otherwise highly similar variants is that the new iteration uses an official ESET executable to hide ArguePatch, with the digital signature removed and code overwritten. The Industroyer2 attack, meanwhile, leveraged a patched version of HexRays IDA Pro's remote debug server.

The latest find builds on a string of discoveries that ESET researchers have made since just before Russia's invasion of Ukraine. On February 23rd, ESET's telemetry picked up HermeticWiper on the networks of a number of high-profile Ukrainian organizations. The campaigns also leveraged HermeticWizard, a custom worm used for propagating HermeticWiper inside local networks, and HermeticRansom, which acted as decoy ransomware. The next day, a second destructive attack against a Ukrainian governmental network started, this time deploying IsaacWiper.

In the middle of March, ESET uncovered CaddyWiper on several dozen systems in a limited number of Ukrainian organizations. Importantly, ESET's collaboration with CERT-UA led to the discovery of a planned attack involving Industroyer2, which was intended to be unleashed on a Ukrainian power company in April.

IoCs for the new ArguePatch variant: Filename: eset_ssl_filtered_cert_importer.exe SHA-1 hash: 796362BD0304E305AD120576B6A8FB6721108752 ESET detection name: Win32/Agent.AEGY

Further resources: ESET Research webinar: How APT groups have turned Ukraine into a cyber-battlefield ESET Research podcast: Ukraine's past and present cyberwar

For any inquiries about our research published on WeLiveSecurity, please contact us at threatintel@eset.com. ESET Research now also offers private APT intelligence reports and data feeds. For any inquiries about this service, visit the ESET Threat Intelligence page.

Editor 20 May 2022 - 07:01PM