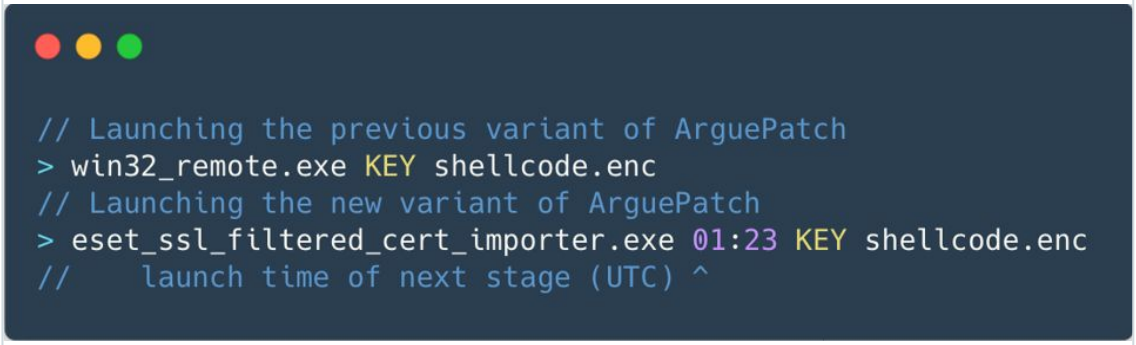
← **Thread**

**ESET research**
@ESETresearch

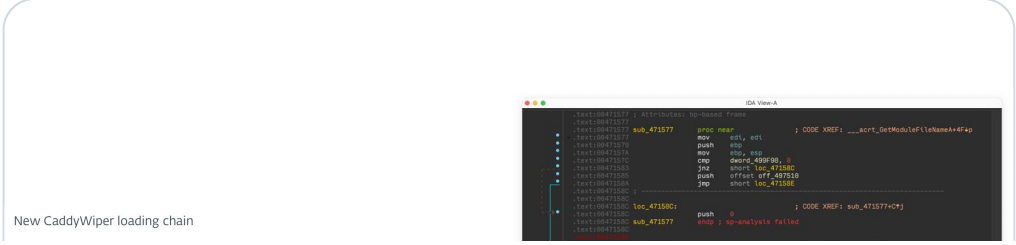
#BREAKING #Sandworm continues attacks in Ukraine 🇺🇦. #ESETresearch found an evolution of a malware loader used during the #Industroyer2 attacks. This updated piece of the puzzle is malware @_CERT_UA calls #ArguePatch. ArguePatch was used to launch #CaddyWiper. #WarInUkraine 1/6



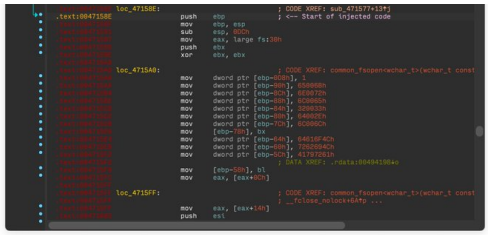

8:08 AM · May 20, 2022 · Twitter Web App

**35** Retweets **2** Quote Tweets **51** Likes

**ESET research** @ESETresearch · 1h
Replying to @ESETresearch
The #Industroyer2 attacks used a patched version of @HexRaysSA IDA Pro's remote debug server (win32_remote.exe). It was modified to include code to decrypt and run #CaddyWiper from an external file. 2/6



In the network of the energy provider, attackers deployed a new version of CaddyWiper that uses a new loader, named ARGUEPATCH by CERT-UA. ARGUEPATCH is a patched version of a legitimate component of Hex-Rays IDA Pro software, specifically the remote IDA debugger server `win32_remote.exe`. IDA Pro is not intended to be used in an ICS environment, as its main purpose is for software reverse-engineering including malware analysis. We don't know why attackers chose to trojanize this piece of software; it might be a troll towards defenders.

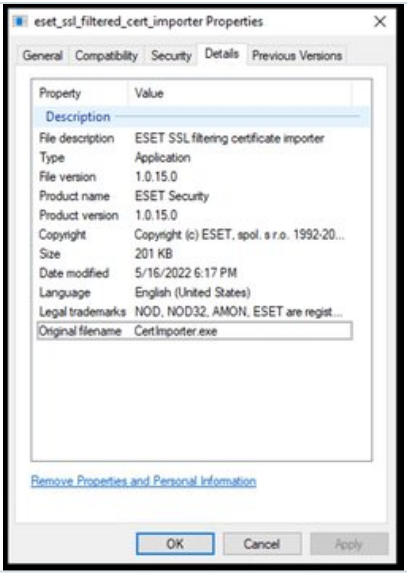


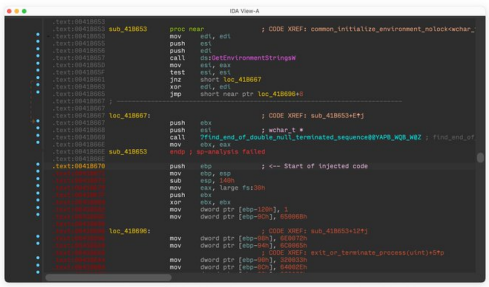
1 2 5

---

**ESET research** @ESETresearch · 1h

This time, #Sandworm chose an official @ESET executable to hide #ArguePatch. It was stripped of its digital signature and code was overwritten in a function called during the MSVC runtime initialization. 3/6



1 1 8

---

**ESET research** @ESETresearch · 1h

The added code is very similar in both cases, but it now includes a feature to launch the next stage at a particular time. This makes #ArguePatch a timed bomb when started. 4/6

```
// Launching the previous variant of ArguePatch
> win32_remote.exe KEY shellcode.enc
// Launching the new variant of ArguePatch
> eset_ssl_filtered_cert_importer.exe 01:23 KEY shellcode.enc
//    launch time of next stage (UTC) ^
```

1 6

**ESET research** @ESETresearch · 1h

This replaces the need to setup a Windows scheduled task for future detonation. This is perhaps a way to evade detections using known TTPs. 5/6

2 7

**ESET research** @ESETresearch · 1h

IoC:
eset_ssl_filtered_cert_importer.exe
SHA-1: 796362BD0304E305AD120576B6A8FB6721108752
ESET detection name: Win32/Agent.AEGY trojan #ESETresearch
6/6

1 7