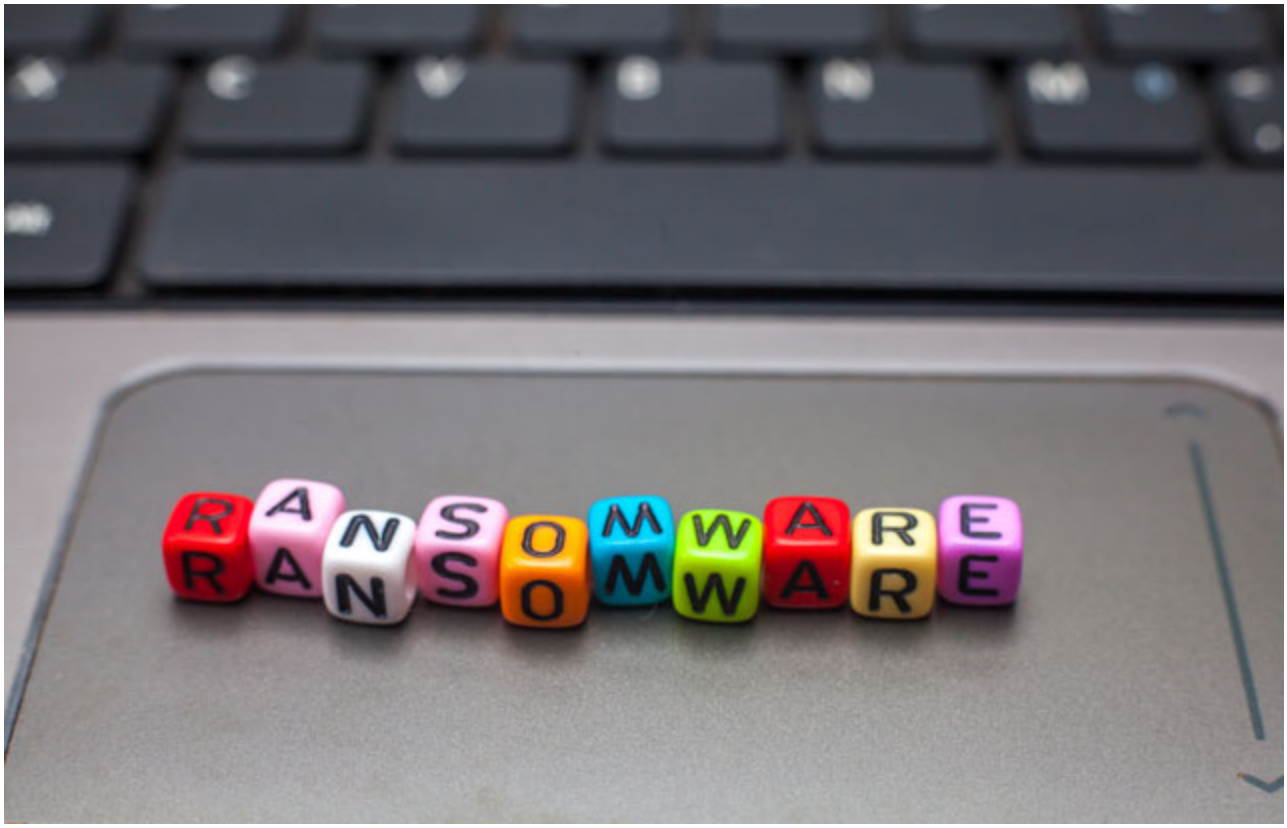
XData ransomware making rounds amid global WannaCryptor scare

welivesecurity.com/2017/05/23/xdata-ransomware-making-rounds-amid-global-wannacryptor-scare/

May 23, 2017



A week after the global outbreak of WannaCryptor, also known as WannaCry, another ransomware, known as XData, has been making rounds.

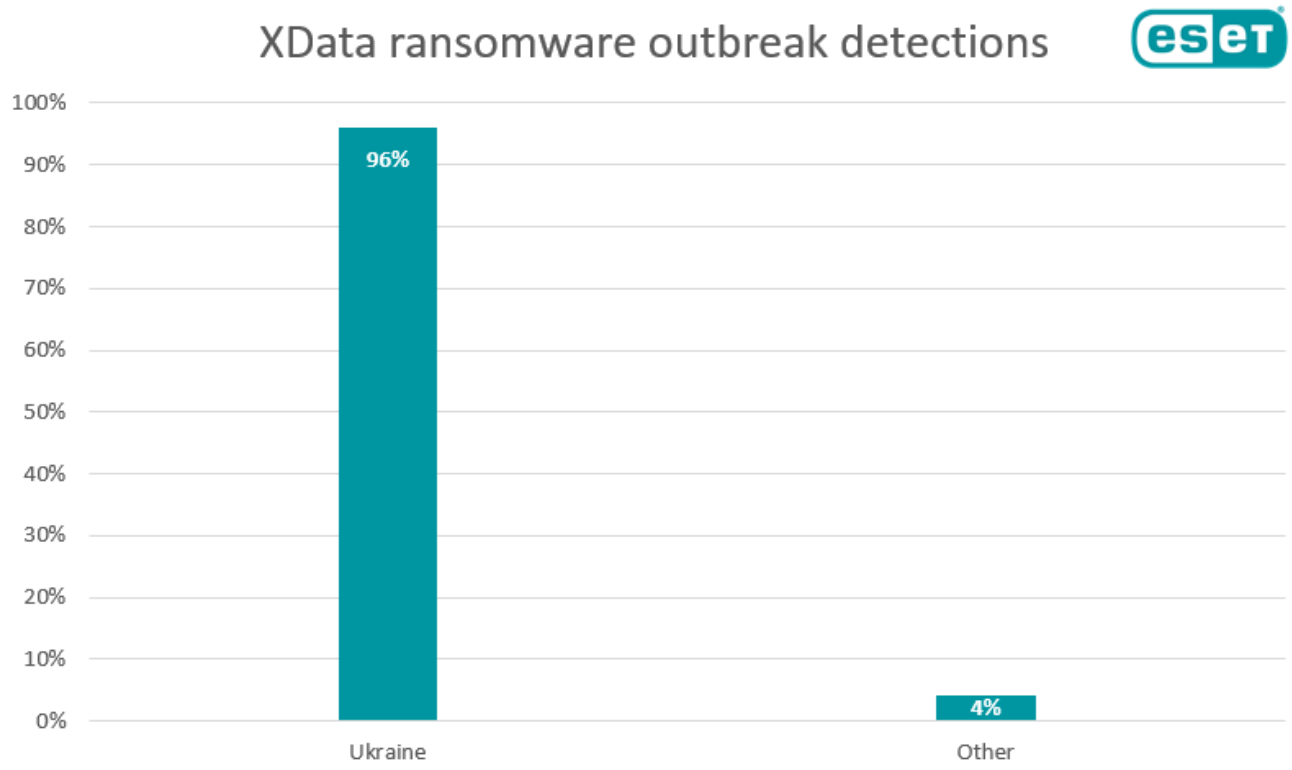
Anton Cherepanov
23 May 2017 - 06:00PM

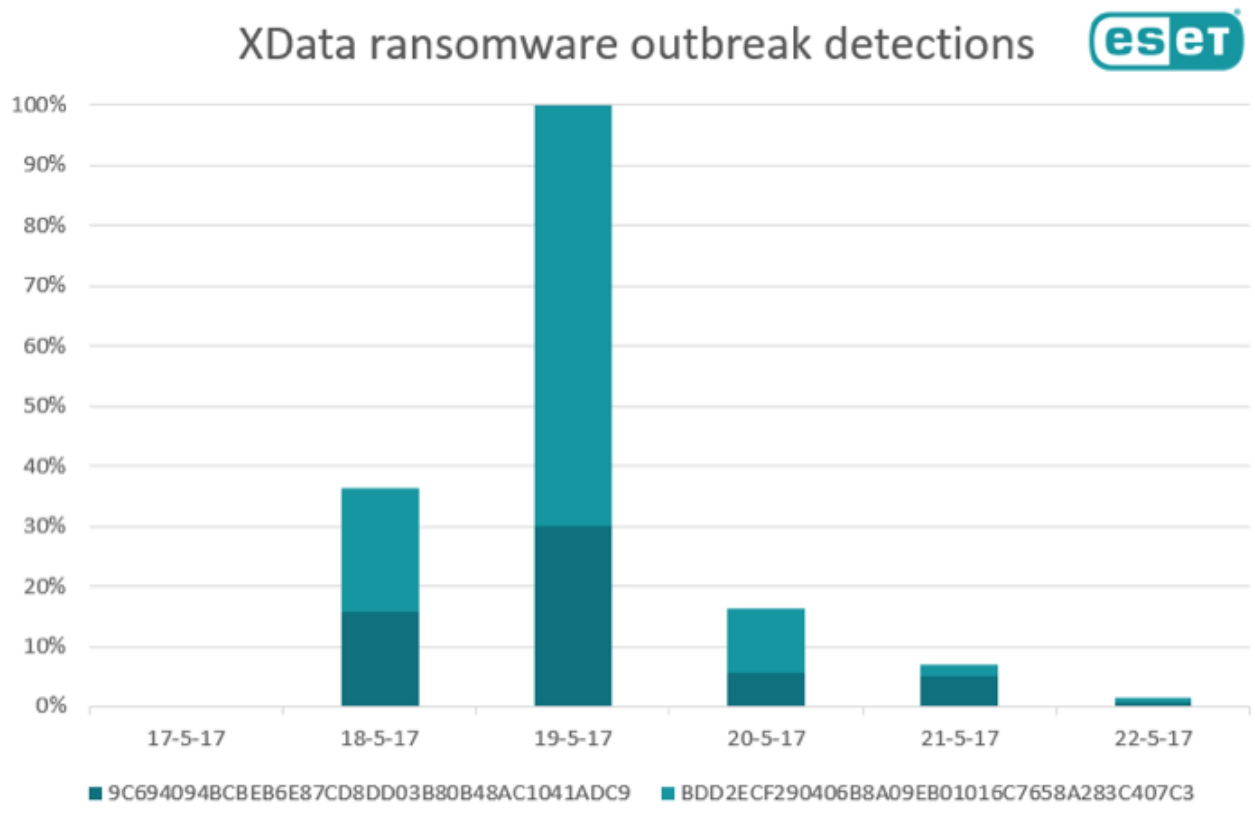
A week after the global outbreak of WannaCryptor, also known as WannaCry, another ransomware, known as XData, has been making rounds.

A week after the global outbreak of WannaCryptor, also known as WannaCry, another ransomware variant has been making the rounds.

Detected by ESET as Win32/Filecoder.AESNI.C, and also known as XData ransomware, the threat has been most prevalent in Ukraine, with 96% of the total detections between May 17th and May 22th, and peaking on Friday, May 19th. ESET has protected its customers against this threat since May 18th.

However, we've been tracking the malware since December 8th, 2016, when the version Win32/Filecoder.AESNI.A first appeared. For the AESNI.A variant, some of the decryption keys have been recently published on a BleepingComputer.com forum.



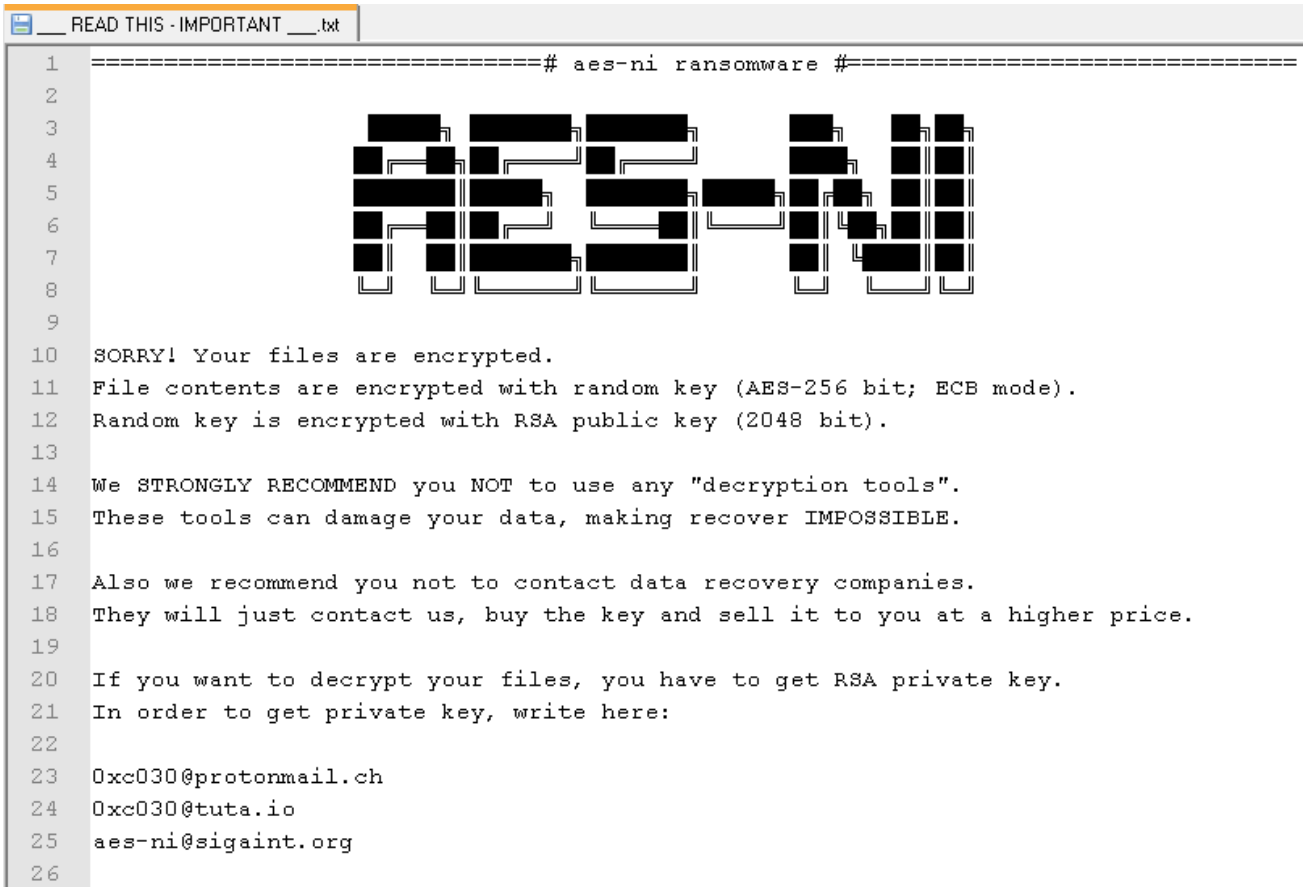


Based on ESET's research, the ransomware appears to have been distributed through a Ukrainian document automation system widely used in accounting. Since the infection ratio is still low, a probable distribution scenario involves some kind of social engineering – e.g. connected to a malicious software update – however, it is still early to tell with absolute certainty.

Once it infects a computer, the main file drops a legitimate system utility – SysInternals PsExec – and then executes the dropped ransomware sample (Win32/Filecoder.AESNI.C.).

If executed with admin privileges, the ransomware can infect an entire network. To do so, it uses the Mimikatz tool to extract admin credentials and then uses them to run a copy of itself on all computers in the internal network.

If you're interested in why the threat is called AESNI, it is derived from the ransom note dropped by one of its previous variants:



Moreover, there is also a functionality behind the name – the ransomware checks whether the affected machine supports Advanced Encryption Standard Instruction Set, aka AES-NI. If that's the case, it uses it to encrypt victims' data faster thanks to hardware acceleration.

How to stay safe

Particularly in this case, separating admin and user accounts would prevent much of the damage, as the XData ransomware misuses admin passwords if run on accounts with admin privileges. Without admin privileges, XData is only able to infect one computer instead of the whole network.

In general, here's what you can do to protect yourself against most ransomware:

- Use a reliable security solution that utilizes multiple layers to protect you from similar threats in the future.
- Make sure to update and patch your operating system regularly.
- Keep backups of your files on a remote hard disk or location that will not be hit in case of a network infection.
- Never click on attachments and links in suspicious or unexpected emails.

23 May 2017 - 06:00PM

Sign up to receive an email update whenever a new article is published in our Ukraine Crisis – Digital Security Resource Center

Newsletter

Discussion