Pnyetya: Yet Another Ransomware Outbreak

By thaddeus t. grugq

Published: 2017-07-04 · Archived: 2026-04-05 17:13:40 UTC

Hiding the small movement inside the big movement

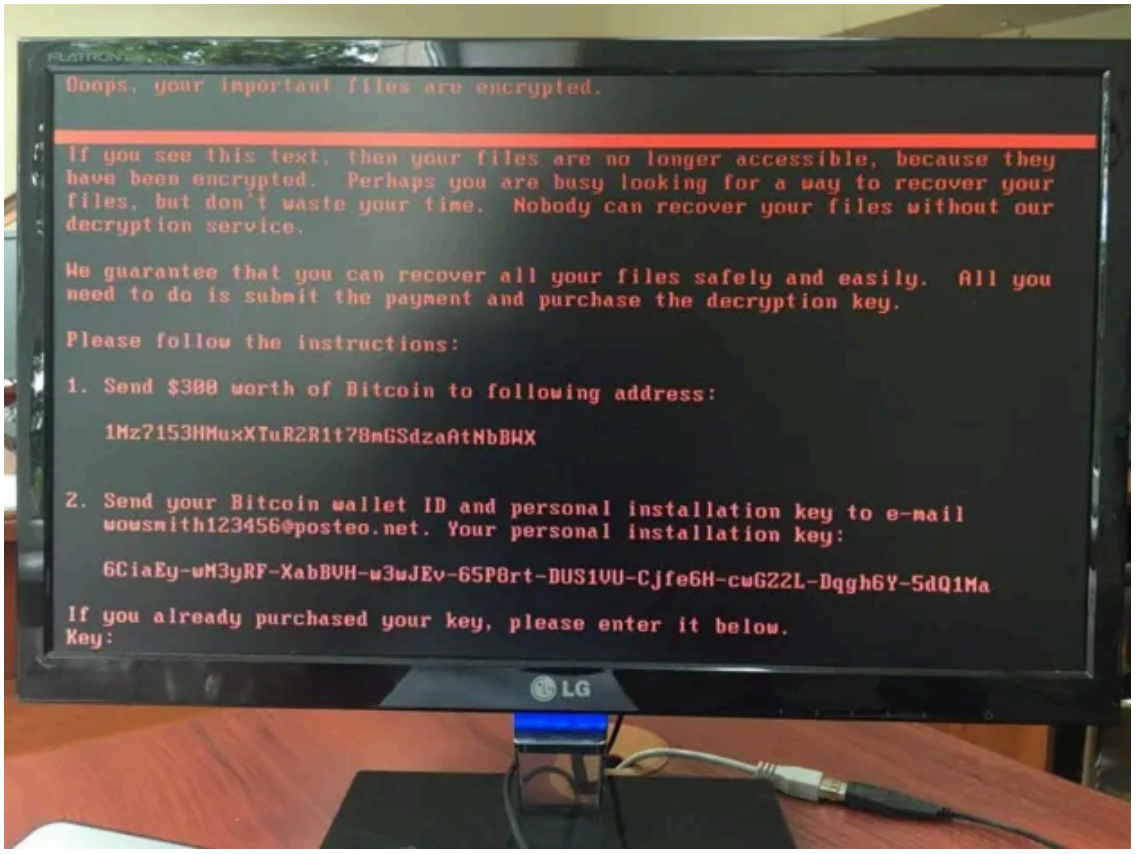
Today saw a massive outbreak of not-really ransomware that has caused significant damage to both Ukrainian targets and strategic global logistics companies. The worm uses three different infection vectors:

- ETERNALBLUE
- Harvested password hashes
- psexec

The code is well written, obfuscated to protect against AV detection using at least two techniques:

- Fake Microsoft signature (apparently fools some AV)
- XOR encrypted shellcode payload (to bypass signature checks)

Although the worm is camouflaged to look like the infamous Petya ransomware, it has an extremely poor payment pipeline. There is a single hardcoded BTC wallet and the instructions require sending an email with a large amount of complex strings (something that a novice computer victim is unlikely to get right.)



Predictably, within hours the email address had been disabled by the service provider. If this well engineered and highly crafted worm was meant to generate revenue, this payment pipeline was possibly the worst of all options (short of “send a personal cheque to: Petya Payments, PO Box …”)

Get thaddeus t. grugq’s stories in your inbox

Join Medium for free to get updates from this writer.

Remember me for faster sign in

The superficial resemblance to Petya is only skin deep. Although there is significant code sharing, the real Petya was a criminal enterprise for making money. This is definitely not designed to make money. This is designed to spread fast and cause damage, with a plausibly deniable cover of “ransomware.”

Update: congratulations, it’s a wiper!

Research by Kaspersky has revealed that the pseudo-ransomware is in fact a wiper, with no potential for successfully recovering from an attack. The key material displayed as “installation ID” – necessary for decryption in real ransomware – is just random data. There is no possible way to recover the encrypted files as the key is not preserved and given to the user to request a decryption key.

There are at least three issues (post MBR sector corruption, random garbage installation ID, buggy encryption code) that indicate successful decryption of an infected computer was not a developer priority compared with fast and thorough propagation.

> Once is an accident. Twice is a coincidence. Three times is an enemy action.— Goldfinger, by Ian Fleming

This was a straight forward cyber attack with a target space of basically every company that does business in Ukraine.

Worth mentioning that whomever developed Pnyetya had source code to Petya. **UPDATE** nope, that is incorrect.

Note: Originally this assessment rested on analysis by

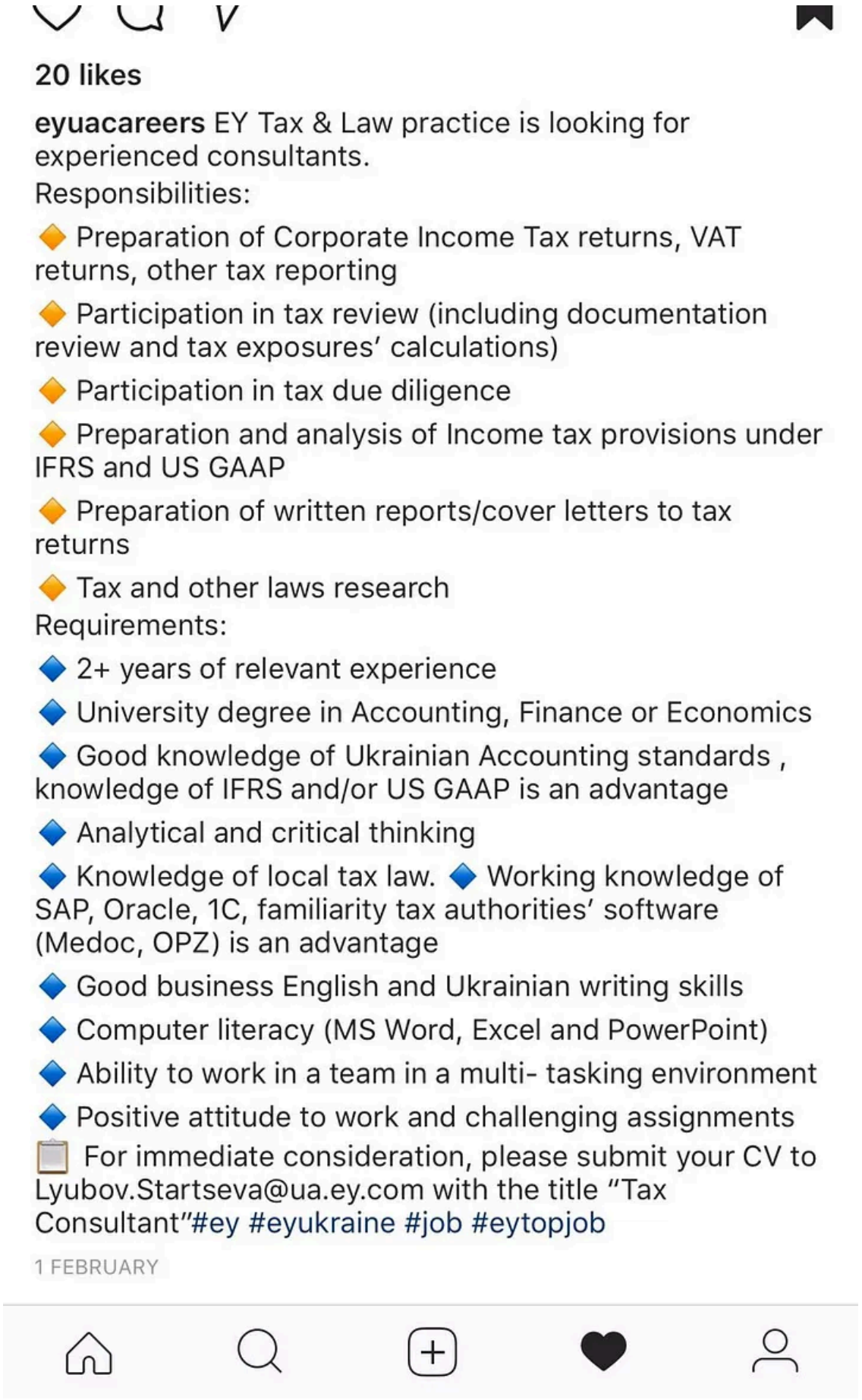
regarding the cavalier attitude Pnyetya has towards preserving the sectors after the MBR. However, more recent analysis suggests that this failure to preserve those sectors would not impact the integrity of the system. The foundations for the wiper assessment has thus been moved from “doesn’t preserve post-MBR sectors” to the far more damning “decryption key is random garbage.”

Patient Zero

Interestingly, it seems that Maersk was also using MeDoc:

In fact, everyone that does business requiring them to pay taxes in Ukraine has to use MeDoc (one of only two approved accounting software packages.) So an attack launched from MeDoc would hit not only Ukraine’s government but many foreign investors and companies.

Press enter or click to view image in full size



E&Y job posting for Ukraine accountant

The MeDoc infection vector has been confirmed by the Ukrainian police.

The immaculate infection

Rosneft, a Russian state controlled company (that does not use MeDoc), was also hit by the worm. They managed to escape practically unscathed, evading all the lateral traversal mechanisms of the worm and simply switching to their backup system. Fortunately, all this without even an interruption to their operations.

Although there has been talk that the Russian oil sector was also hit, their infinitely superior cybersecurity skills meant that they suffered no downtime or outages. Curious that they were so poorly protected they got infected — especially since they aren't connected to MeDoc (the initial infection vector) — however they were so well protected they were able to remediate the infection (which didn't spread… although it can take out 5000 computers in less than 10 minutes.) It's a miracle!

Update:

False alarm. Seems unrelated.

In other news

Combined arms cyber operations?

Does a bear shit in Ukraine?

It doesn't take a weatherman to know which way the wind blows.

Support more analysis like this.

Thanks to @marasawr for discussion and analysis.
