Who is behind Petna?

gdatasoftware.com/blog/2017/07/29859-who-is-behind-petna

The news talk about a cyber attack when reporting about Petna and WannaCry. This implies purposeful activities aiming at causing damage. On the other hand, cyber-criminals who are in the blackmailing business with ransomware are mainly interested in making easy money. They failed both with WannaCry and even more with Petna. This leaves some open questions.

From Petya via GoldenEye to Petna

When Petya spread for the first time in March 2016, the ransomware stood out by in terms of efficiency, the new technical approach and the well-designed phishing campaign. Emails with typical job applications written in flawless German point to a file in Dropbox. If you download and open it, the first sectors of the harddrive will be overwritten. After a reboot the Master File Tabel (MFT) is encrypted: the files are still on the harddrive, but the system cannot access them. The technical sophistication consists in the few hundred bytes of code written to the first sectors of the harddrive, which manage the whole logic of decryption and system recovery. It even contained the infamous "skull" screen.

Petya had a few drawbacks. First and foremost, it needs admin privileges. That's why Petya after a short while got a companion: Mischa. Mischa only needed user rights and was a classic file encrypting ransomware. The combination of both circulated in May 2016 and were merged with slight changes under the new name of GoldenEye in December 2016. Again, it used a phishing scam based on job applications in perfect language, some of which were actually referring to real, existing job offers. The payment of the ransom was automated with a TOR hidden service. Both Petya and GoldenEye were very effective ransomware campaigns, and as such were quite profitable. Then it became silent around the actors behind of GoldenEye, who were acting under the name of Janus.

A now, half a year later, a ransomware has been spreading that also triggers a reboot, and encrypts the Master File Table. The evident similarity to Petya caused many researchers to name the new threat "Petya", too. But first doubts emerged soon, which are reflected in names like NotPetya, Nyetya, or Petna.

How much Petya is in Petna?

It soon turned out that Petya's code for encrypting the MFT is almost a complete copy of the original Petya-code from the GoldenEye version. It utilizes Salsa20 for encryption and the implementation is done in a way, that decryption is not possible. There were only small

changes: The original key of Petya was replaced by anonther one, which is constructed from random numbers. Not even the authors of Petna know this key. I.e. decryption of the data is not possible by any stretch of the imagination.

And that's already the end of similarities. The two other components of GoldenEye - the dropper for the encryption component, and the user-mode ransomware Mischa - are completely rewritten. This might have been a usual maintenance of the software. GoldenEye also had major modifications in relation to the original Petya especially in these two components. But it may also be the case that someone reused the code of GoldenEye's Petya. All it needs is an infected machine, and a hex editor. The malicious code is available in the first sectors of the harddrive. The changes mentioned above do not need a recompilation and hence not the original source code.

More interesting than the similarities are the differences. It starts with the infection method. Petya and GoldenEye were using phishing mails addressed to German human resource managers. And now Petna is infecting systems with drive-by-infections on websites in a waterhole attack? Or even more outlying it abuses the update mechanism of a financilal software called MEDoc which is popular in Ukrainian enterprises. It is not very likely that Janus is suddenly changing an established strategy. After months of silence they announced to participate in the search for the decryption key. Obviously there is another group behind this. There are some clues that the Telebots group has relations to Petna.

Few similarities to WannaCry

The last big wave of ransomware WannaCry is slowly fading out, and there are some parallels with Petna. Petna uses the same vulnerability from the NSA leaks: EternalBlue. But Petna does not propagate over the internet. It only spreads in local networks. Petna also has some additional characteristics. EternalBlue is combined with another vulnerability from the NSA leaks: EternalRomance. In addition Petna identifies domain controllers and runs special searches in order to locate other machines on the network. It also spreads by using the WMI administration console, and by probing admin$ shares with passwords and starting the infection with the tool psexec. WannaCry lacks all of these additional propagation vectors.

It is also exceptional that Petna is deleting USN journals and certain Event-Logs of infected computers. This is where Windows is logging the system's activities. By deleting these entries Petna impedes the analysis of affected systems, and - even more important - evades detection by logfile analysis as it is used in Security Information and Event Management (SIEM) systems, which are often used in huge enterprises. Thus the malware specialists in the Security Operation Centers (SOC) might notice the malicious activities too late.

What the intention of Petna's creators?

By addressing human resource managers, Petya was sort of targeting enterprises. Petna is obviously aiming at major companies in a certain region. A tax and accounting software that is frequently used in Ukraine is part of the initial infection vector, it only spreads in local networks, and it hides from detection methods, which are only used in large enterprises. Looking at the list of victims this worked out well: oil production, banks, cash desks, production lines, logistics, etc. were shut down. PCs of private users are not affected.

There are several ransomware families, which are specialised on enterprises or at least identify that they are running in a company network. This usually implies higher ransom. 4-figure sums are quite common, but it could also be a 5-figure or a 6-figure digit. Petna is asking a ransom of 300 USD in BitCoins. This is the lower end for private users. This small price strongly indicates that this ransomware was not about making money. This conclusion is is supported by the sloppy implementation of the payment process. It is based on a single email address from a German provider. The email address was blocked promptly. So victims who paid could no longer send the notification. As Petna is not able to decrypt the files anyway, there is no point in paying. The associated BitCoin account is currently holding about 4 BTC which is a little bit more than 10,000 USD. Given the current exchange rate this means that there were 29 victims who paid the ransom (with 46 transactions). From a financial point of view Petna is a flop.

Cyber attacks

Maybe money was not the primary motivation for Petna. Come to think of it, why is someone putting so much effort into intruding the networks of large Ukranian and worldwide enterprises, and the lets it all down with a poorly implemented payment system? On a second thought, it appears that it might be an act of targeted sabotage. But then, the fact that Petna spread so widely is not typical for a targeted attack. It could have been contained better to remain under the radar. It might have been a test run 'gone wild'. This is further backed by the fact that no updated versions were used after the first wave.

An international law enforcement team is trying to find out where the attacks were originating. It is too early to say whether there are nation states involved. But NATO is making clear that it is considering "cyber" as a military domain , and that attacks in this domain may trigger Article 5, assuming that reliable attribution is possible with. It is currently not known who is behind the current attacks.

Lessons learned

Some companies were hit very hard. The trouble that logistics giant Maersk was affected, too, shows how much an entire business area is reliant on a working computer infrastructure. Petna and WannaCry also showed, that in many enterprises or at least areas of enterprises the protection measures are suitable to prevent and block the attack or at least deal with it swiftly. Petna also demonstrated that there are other areas where protection is not yet

sufficient. It is necessary for companies to improve the protection of these areas and that there is homework to be done. The protection methods are as individual as companies are. When in doubt, companies should ask advice from security experts (e.g. G DATA Advanced Analytics). If Petna was indeed a test run, then its evaluation is now in progress and the lessons learned will be considered in the next round. There is not much time left to safeguard your IT.