CCDCOE
NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia

News

30 June 2017

NotPetya and WannaCry Call for a Joint Response from International Community

The global outbreak of NotPetya malware on 27 June 2017 hitting multiple organisations in Ukraine, Europe, US and possibly Russia can most likely be attributed to a state actor, concluded a group of NATO CCD COE researchers Bernhards Blumbergs, Tomáš Minárik, LTC Kris van der Meij and Lauri Lindström. Analysis of both recent large-scale campaigns WannaCry and NotPetya raises questions about possible response options of affected states and the international community.

According to Bernhards Blumbergs, researcher at the NATO CCD COE Technology Branch, NotPetya authors have acknowledged the drawbacks and mistakes of recent WannaCry ransomware. "In the case of NotPetya, significant improvements have been made to create a new breed of ultimate threat. Among all new features, the malware has been more professionally developed in contrast with sloppy WannaCry, and instead of scanning the whole Internet it is more targeted and searches for new hosts to infect deeper on local computer networks once initial breach has occurred," said Blumbergs.

NotPetya malware was spread via drive-by exploit kits, e-mails with malicious attachments, embedded URI links, and compromised software update services (i.e. MeDoc accounting software update) to gain initial access to the host. Once the foothold has been established, the malware will extract plain-text credentials from the computer memory, use PsExec and WMIC tools for remote command execution, and employ leaked NSA exploits from Shadow Brokers, such as ETERNALBLUE exploit (MS17-010), to spread to other hosts on local network and escalate privileges. While Microsoft has released emergency patches for its operating systems, starting with Windows XP, unfortunately they have not been applied everywhere.

After seizing full control over its victim, NotPetya will trigger a reboot. Upon computer restart, encryption of file allocation tables is being carried out resembling a regular MS Windows utility performing system integrity checks. Malware will then request 300 USD worth of Bitcoins to provide a decryption key. Primary defence is ensured by having updated and patched systems, and browsing the Internet or working with e-mails with reasonable caution. However, in case of suspected infection, if computer unexpectedly reboots, it is suggested to unplug it from power or remove its battery and seek expert help to recover files from hard drive.

According to Tallinn Manual Countermeasures Require Attribution

In the case of the current campaign, international law analysis is similar to WannaCry campaign, with the caveat that accurate attribution is much more difficult. Nevertheless, NotPetya was probably launched by a state actor or a non-state actor with support or approval from a state. Other options are unlikely. The operation was not too complex, but still complex and expensive enough to have been prepared and executed by unaffiliated hackers for the sake of practice. Cyber criminals are not behind this either, as the method for collecting the ransom was so poorly designed that the ransom would probably not even cover the cost of the operation.

NATO's Secretary General reaffirmed on 28 June that a cyber operation with consequences comparable to an armed attack can trigger Article 5 of the North Atlantic Treaty and responses might be with military means. However, there are no reports of such effects, so according to Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, self-defence or collective defence of victim states are not available options.

"If the operation could be linked to an ongoing international armed conflict, then law of armed conflict would apply, at least to the extent that injury or physical damage was caused by it, and with respect to possible direct participation in hostilities by civilian hackers, but so far there are reports of neither," said Tomáš Minárik, researcher at NATO CCD COE Law Branch.

"There is a lack of a clear coercive element with respect to any government in the campaign, so prohibited intervention does not come into play. As important government systems have been targeted, then in case the operation is attributed to a state this could count as a violation of sovereignty. Consequently, this could be an internationally wrongful act, which might give the targeted states several options to

respond with countermeasures," adds Minárik. A countermeasure is a state response that would otherwise be unlawful but for the fact that the state is responding to an internationally wrongful act attributable to another state. A countermeasure could be, for example, a cyber operation sabotaging the offending state's government IT systems, but it does not necessarily have to be conducted by cyber means. In any case, the effects of a countermeasure must not amount to a use of force or affect third countries.

EU drafted this month a framework for a joint EU diplomatic response to malicious cyber activities which will make full use of measures within the Common Foreign and Security Policy.

Recent Campaigns Call for a Joint Response

As the extortion of money seems to be just a negligently prepared cover according to various news then the question about the motivation behind NotPetya attack should be looked from other perspectives. Even though the same vulnerability was used by WannaCry, the actors behind these two similar attacks are likely not the same. In both cases a possible financial gain for attackers has been more than modest. However, an effect was achieved, a large-scale successful disruptive attack almost globally, is almost identical in both cases.

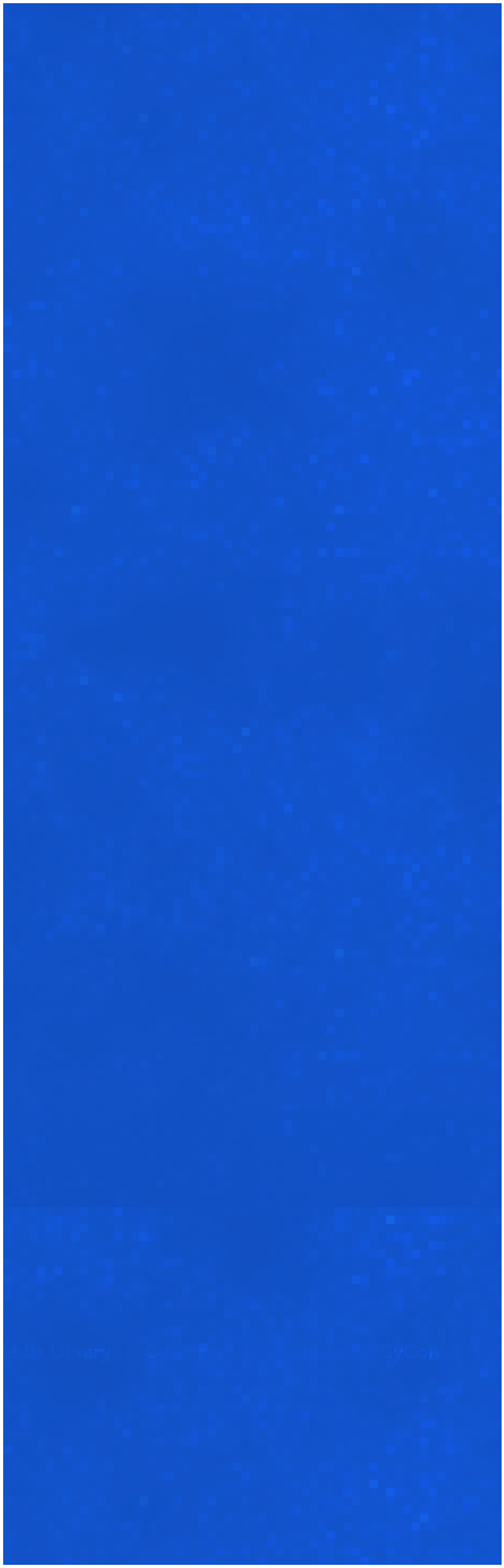
"NotPetya is a sign that after WannaCry, yet another actor has exploited vulnerability exposed by the Shadow Brokers. Furthermore, it seems likely that the more sophisticated and expensive NotPetya campaign is a declaration of power - demonstration of the acquired disruptive capability and readiness to use it," concluded Lauri Lindström, researcher at NATO CCD COE Strategy Branch.

We should also keep in mind that ransomware type of malware is highly visible for the end user while most of the other type of malicious software tries to remain as invisible as possible. NotPetya-like visible campaigns are great reminder that there is probably invisible malicious software operating in our networks that we know nothing about and there are no "silver bullets" - even big organizations can, and will, be hit when targeted.

WannaCry and NotPetya raise again the question about the possible response options of the international community. The number of affected countries shows that attackers are not intimidated by a possible global level investigation in response to their attacks. This might be an opportunity for victim nations to demonstrate the contrary by launching a special joint investigation.

Significant Facts on NotPetya Campaign

- The ransom collection part of the operation was botched. Only one address for sending the bitcoins was provided by the attackers, meaning that they were unable to distinguish who paid the ransom and should be sent the decryption key. The attackers had provided an email address to the victims where they had been supposed to send the proof of payment (wowsmith123456@posteo.net); however, this address was promptly blocked by the provider. Most reports conclude that the ransom demand was only a ruse, and that the real aim of the operation was causing economic losses, sowing chaos, or perhaps testing attack capabilities or showing own power.
- The malware was 'likely very cheap to deploy', Volodymyr Tsap, a Ukrainian cyber security specialist claimed. He estimated the costs to 100.000 USD, which is not beyond the means of criminal organisations and non-state actors; however, this can also be a ruse by a more powerful organisation, like a state actor.
- The malware was not too resilient and could easily be stopped by a simple kill switch, which takes advantage of the fact that the malware is looking for its own filename in c:\windows, called perfc. Once the file is there, the malware stops operating. This shows that the attackers wanted to be able to control the spreading of the malware and the damage caused. This could support the theory that the attackers wanted to be able to target the malware more precisely.
- After the first infection, the malware only spreads through internal networks. This would imply that NotPetya was designed to avoid the snowball effect of spreading through the Internet, as opposed to the WannaCry malware. This also supports the theory that the malware was to be used in a more targeted fashion.
- The malware uses known vulnerabilities leaked from the NSA. A malware using one or more zero-day vulnerabilities would have wreaked much more havoc on networks worldwide. Without them, the spreading is more limited, but the public debate about states hoarding vulnerabilities might be revived, which might have been one of the motives.
- Most infections were reported from Ukraine, although the malware is reported from more than 60 countries. Rosneft, a Russian state-controlled company, was also targeted; however, the infection was remarkably well-contained and it likely caused very little damage. Nevertheless, the global economic losses caused by the operation could well be in billions of USD, judging by the losses from the earlier WannaCry campaign.
- Malware analysis supports the theory that main purpose of the malware was to be destructive because key used for encrypting the hard disk was discarded.



For further insight, please also learn about the analysis of WannaCry campaign by CCDCOE researchers.