CYBERCONTAINMENT 5
- ETERNAL_HELL -
THE WILD SPRING OF 2017

PART 2: CYBER BOOGALOO

Arch0nte – 05/2020

TABLE OF CONTENTS

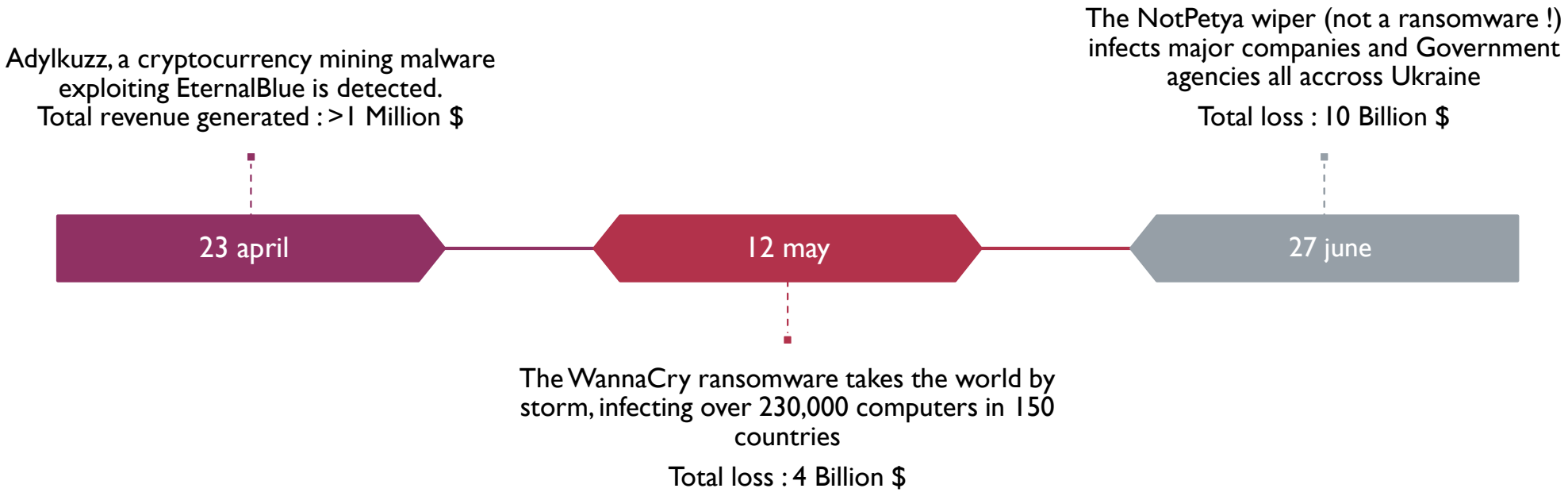
INTRODUCTION AND CONTEXT : APRIL 14TH

SPRING 2017, HOW EVENTS UNFOLDED ON APRIL 14TH 2017

- A hacker group called The Shadow Brokers decided to publish cybersecurity exploit tools stolen from the NSA [1] for free on the internet. At the time of the hack, the NSA warned several companies of the existence of these vulnerabilities and most had already been patched by the time the tools were published.
- Given that in a previous post, they pretended that they got these tools from "Equation Group" a notorious hacker group responsible for Stuxnet and reportedly VERY close to US intelligence services, this could be considered an additional reason to link EG to US intelligence.

- So, what consequences did these vulnerabilities have ?

SPRING 2017, HOW EVENTS UNFOLDED IN THE FOLLOWING 2 MONTHS



In the span of 45 days, the damage inflicted by WannaCry and NotPetya is equal to the annual GDP of a country like Nicaragua.

APRIL 23RD, ADYLKUZZ : SMALL GAME HUNTER

ADYLKUZZ : CRYPTOCURRENCY MINING

- First of all, what did that malware do ?
  Well, it installed a hidden program on your computer that would use your computer's power to make complex calculations for the benefit of the hacker (by mining cryptocurrency). Thus, it will slow down your computer but apart from that, you won't see any noticeable change !
- This is called cryptojacking [2] and allows the criminal to turn a very small profit per computer infected. But when deployed on hundreds of thousands of unsuspecting computers, it could generate quite a huge sum of money !

ADYLKUZZ : CRYPTOCURRENCY MINING

- Adylkuzz is notorious because it was the first malware discovered to exploit a vulnerability disclosed by The Shadow Brokers (EternalBlue [3 – shameless self-promotion]). It infected tens of thousand of computers and generated more than a million dollar.

- It is characteristic of small, petty crime on the Internet, targeting any and every one it could find.

MAY 12TH, WANNACRY : THE UNPOLISHED GAME CHANGER

WANNACRY : YOUR MONEY OR YOUR BUSINESSES LIFE !

- WannaCry was a ransomware, a malware that ciphered the infected devices hard drives, making them unreadable and only promising to unlock your device if you paid a certain amount in cryptocurrency to the hacker.

- This was the screen that showed up on your computer once you had been infected by WannaCry. It mainly targeted companies in Russia, Europe and the US.

- The hackers extorted about 130k US$ [4] before the attack was stopped. Note that we may never know if the hackers actually gave the payers the decryption key.

WANNACRY : YOUR MONEY OR YOUR BUSINESSES LIFE !

- The current Microsoft Windows version at the time **had been patched already against EternalBlue** (the main vulnerability used by WannaCry). But a lot of companies either used outdated Windows OS or just didn't install the security patches.

- The malware had a blatant design flaw : a hardcoded **kill switch** which rendered the worm inert if he managed to connect to a given website (certainly designed to prevent undesired infections on the hackers intranet). Thus, simply creating the said web site sufficed to stop all new infections. This was discovered and done less than 48h after the first infections. This combined to WannaKey [5], a French developed tool which allowed to decrypt your filesystem if your computer had not been rebooted, helped limit the damage.

WANNACRY : YOUR MONEY OR YOUR BUSINESSES LIFE !

- Even with a quick stop to the contamination and the quick solution to decipher devices (both of which were due to blatant design issues in the malware), the damage amounted to more than 4 Billion $ worldwide making it, at the time, the most damaging cyber attack ever.

- The worm targeted mostly western companies and is strongly suspected to have been built in North Korea [6].
  As you can imagine, even though at first sight, both malwares seem to have the sole goal of making money, this kind of malware is widely different from miners like Adylkuzz.
  Here, we have a rogue state, ransoming money from companies and destroying millions of $ worth of equipment.

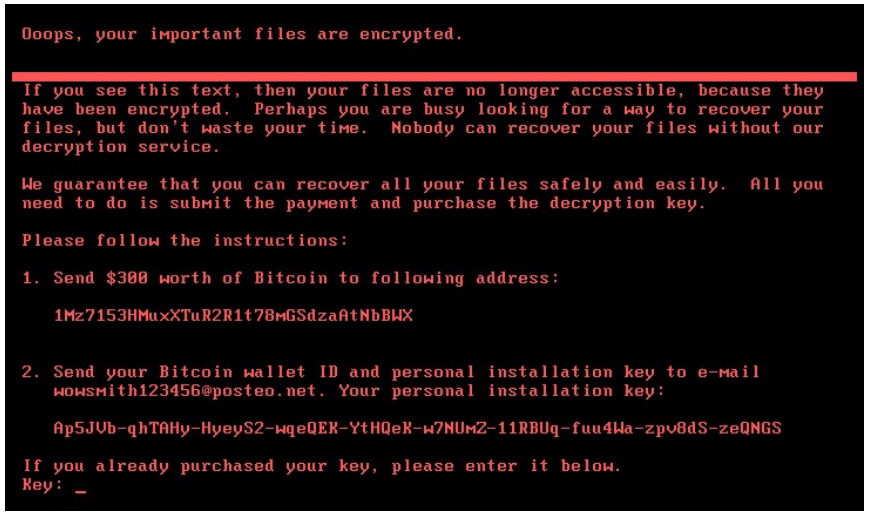
JUNE 27TH, NOTPETYA : RANSOMWARE 2 RUSSIAN BOOGALOO

NOTPETYA : WHY YOU SHOULD'NT TRUST HACKERS (DUH !)

- NotPetya was a "ransomware", which used two exploits published by The Shadow Brokers (EternalBlue and EternalRomance).

- This was the screen that showed up on your computer once you had been infected by NotPetya

- This time, the hackers had specific targets : Ukraine (and some western companies).



NOTPETYA : WHY YOU SHOULD'NT TRUST HACKERS (DUH !)

- So, what's so different about this ransomware ?
  Welp, to start, it is not a ransomware. It's actually a wiper, which, as the name implies, wipes your data. So it is of absolutely no use to pay the ransom, your data is already long gone.

- It's also far better coded than WannaCry, with no global kill switch and obviously no way to retrieve the key (since it does not exist).

- But who would make a sneaky cyber weapon targeting Ukraine on its Constitution Day, with the goal to do maximum damage and disruption ?

WANNACRY : YOUR MONEY OR YOUR BUSINESSES LIFE !

- Even with security patched deployed for months, and the most damaging cyberattack ever (up to this point) just 40 days ago, an ***undisclosed*** state actor managed to cause more than 10 Billion $ worth of damage in just two days.

- Once again, WannaCry and NotPetya might look similar on the outside but both their structure, the goal for which they were created and their targets are widely different !
  Here, we have a cyber weapon directly targeting a state for political reasons with the goal to cause maximum damage. Welcome to the new age of covert operations, billions of dollars at the whim of a keyboard !

CONCLUSION

CONCLUSION : THE FULL HOUSE OF MALWARES

- These two months are extremely interesting because, through these three malwares, we get a preview of just how diverse the threats on the Internet can be :
  - From a miner, which tries to infect any computer to create money for the hacker (a "petty" crime)
  - With the sloppily-designed ransomware, targeting anyone it can reach, but aiming at companies
  - To the highly efficient state-sponsored cyber-weapon targeted at an other state

BIBLIOGRAPHY

- https://en.wikipedia.org/wiki/2017_cyberattacks_on_Ukraine
- [1] : https://steemit.com/shadowbrokers/@theshadowbrokers/lost-in-translation
- [2] : https://www.malwarebytes.com/cryptojacking/
- [3] : https://github.com/Arch0nte/Blog_containment/blob/master/Cyberconfinement%204%20-%20EternalHell%201%20-%20EternalBlue.pdf
- [4] : https://qz.com/982993/watch-as-these-bitcoin-wallets-receive-ransomware-payments-from-the-ongoing-cyberattack/
- [5] : https://github.com/aguinet/wannakey
- [6] : https://www.theguardian.com/technology/2017/may/15/wannacry-ransomware-north-korea-lazarus-group

- If you have any questions : archonte@hackademint.org