# HISTORIA I DOKŁADNY OPIS WYBRANEGO ATAKU

Karkulowski Tomasz 163105

# AGENDA

- Jak rozumiemy pojęcie cyberatak ?
- Historia ataków NotPetya
- Co to jest Wiper (malware) ?
- Przebieg ataku
- Jak się zabezpieczyć przed cyberatakiem ?
- Ciekawostki


# JAK ROZUMIEMY POJĘCIE CYBERATAK ?

Są to działania przeprowadzone za pomocą komputera przy użyciu złośliwego oprogramowania (ang. malware) w celu kradzieży różnych kont do portali społecznościowych, bankowych, wykradania informacji niejawnych do szantażu ofiary i żądania wykupu w postaci kryptowaluty (zazwyczaj jest to BTC – bitcoin), zniszczenia/usunięcia danych lub ich szyfrowanie na komputerze użytkownika poszkodowanego.


# JAK ROZUMIEMY POJĘCIE CYBERATAK ?

Najpopularniejsze techniki przeprowadzenia cyberataku:

- szkodliwe oprogramowanie (malware)
- oprogramowanie szantażujące (ransomware)
- wyłudzanie informacji (phishing)
- MitM (Man in the Middle)
- DDoS (Distributed Denial of Service) – rozproszona odmowa usługi
- SQL injection (wstrzyknięcie złośliwego kodu do bazy SQL)
- „wykorzystanie luki zabezpieczeń w dniu zerowym”

# HISTORIA ATAKÓW NOTPETYA

Atak NotPetya – seria cyberataków przeprowadzonych w czerwcu 2017 roku, który udawał ransomware, a tak naprawdę okazał się wiperem. Głównym celem ataku miała być Ukraina, ale przez przypadek rozpowszechnił się na cały świat. Ucierpiały przez to firmy tj. koncern farmaceutyczny Merck, spółka FedEx, TNT Express, francuska firma budowlana Saint-Gobain, producent żywności Modelez, Reckitt Benckiser, rosyjska spółka naftowa Rosnieft.

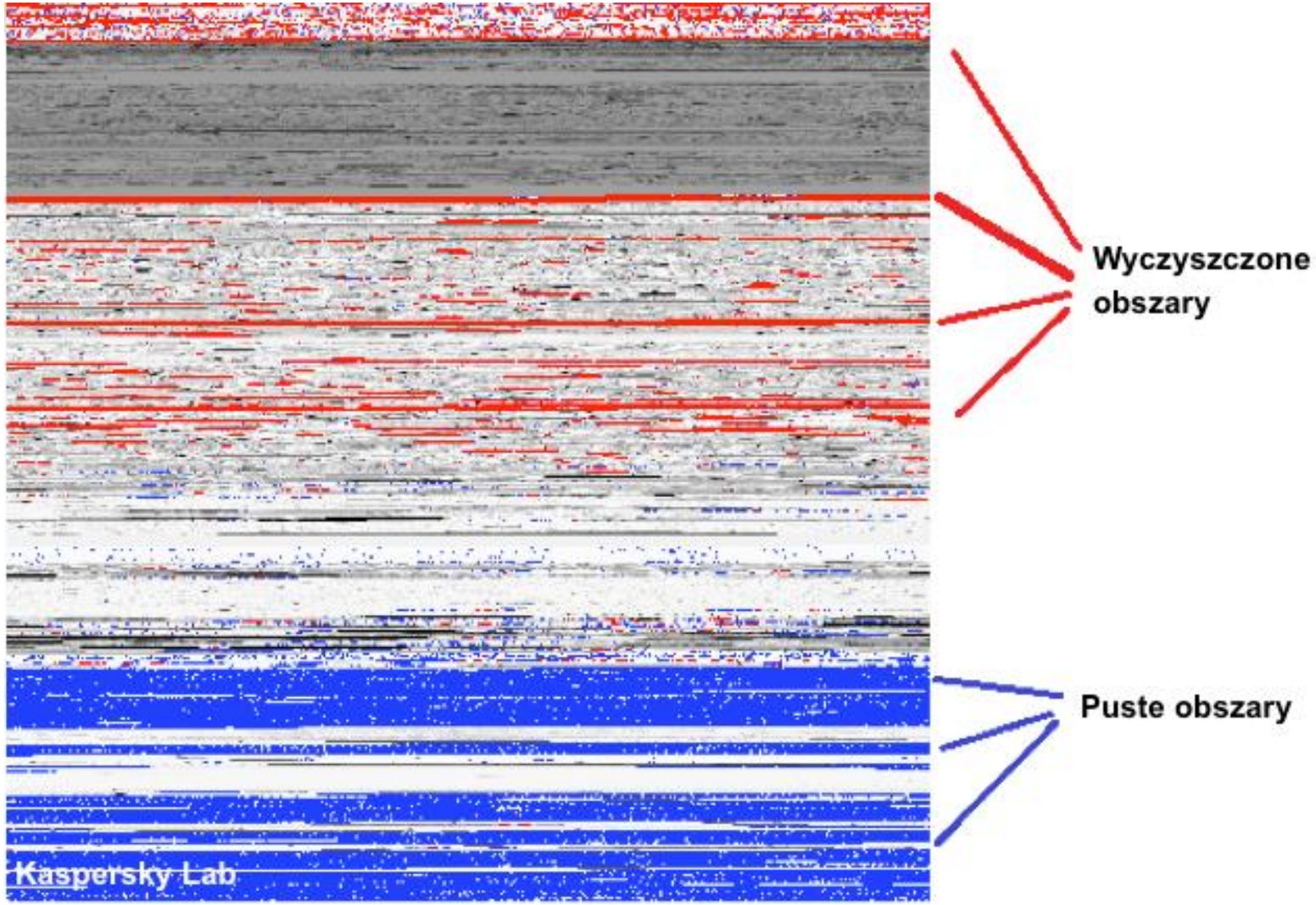
Skład wipera NotPetya:

- Exploit EternalBlue
- Mimikatz
- MEDoc

# CO TO JEST WIPER (MALWARE)?

Wiper (z ang. tłumaczenia „wycieraczka”) to złośliwe oprogramowanie, którego celem było wyczyszczenie dysku twardego zainfekowanego komputera. Na początku jest przeszukiwanie plików, które Wiper może pliki wyczyścić. Następnie wprowadzana jest usługa „RAHDAUD64”, która jest usuwana przed czyszczeniem dysku, a następnie wprowadzane i nadpisywane w niej losowe dane. Ostatnim krokiem usługa zastępuje nazwy plików na pliki tymczasowe. Dla przykładu: „~DF24.tmp”.

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| accdb | cdx | dmp | H | js | PNF | Rom | tif | wmdb |
| acl | cfg | doc | Hlp | json | png | Rpt | tiff | wmv |
| acm | chk | docx | HPI | lnk | pps | Rsp | tlb | xdr |
| amr | com | dot | Htm | log | ppt | Sam | tmp | xls |
| apln | cpl | drv | Html | lst | pptx | Scp | tsp | xlsx |
| asp | cpx | dwg | Hxx | m4a | pro | Scr | txt | xml |
| avi | dat | eml | Ico | mid | psd | Sdb | vbs | xsd |
| ax | db | exe | Inc | nls | rar | Sig | wab | zip |
| bak | dbf | ext | Ini | one | rar | Sql | wab~ | |
| bin | dbx | fdb | Jar | pdf | rdf | sqlite | wav | |
| bmp | dll | gif | Jpg | pip | resources | theme | wma | |


Wyczyszczone obszary
Puste obszary
Kaspersky Lab

# SKŁAD WIPERA NOTPETYA

Exploit EternalBlue

- exploit
- Opracowane przez NSA (amerykańską agencję bezpieczeństwa)
- wykorzystywał lukę do zdalnego wykonania kodu w protokole SMBv1
- użycie backdoora

Mimikatz

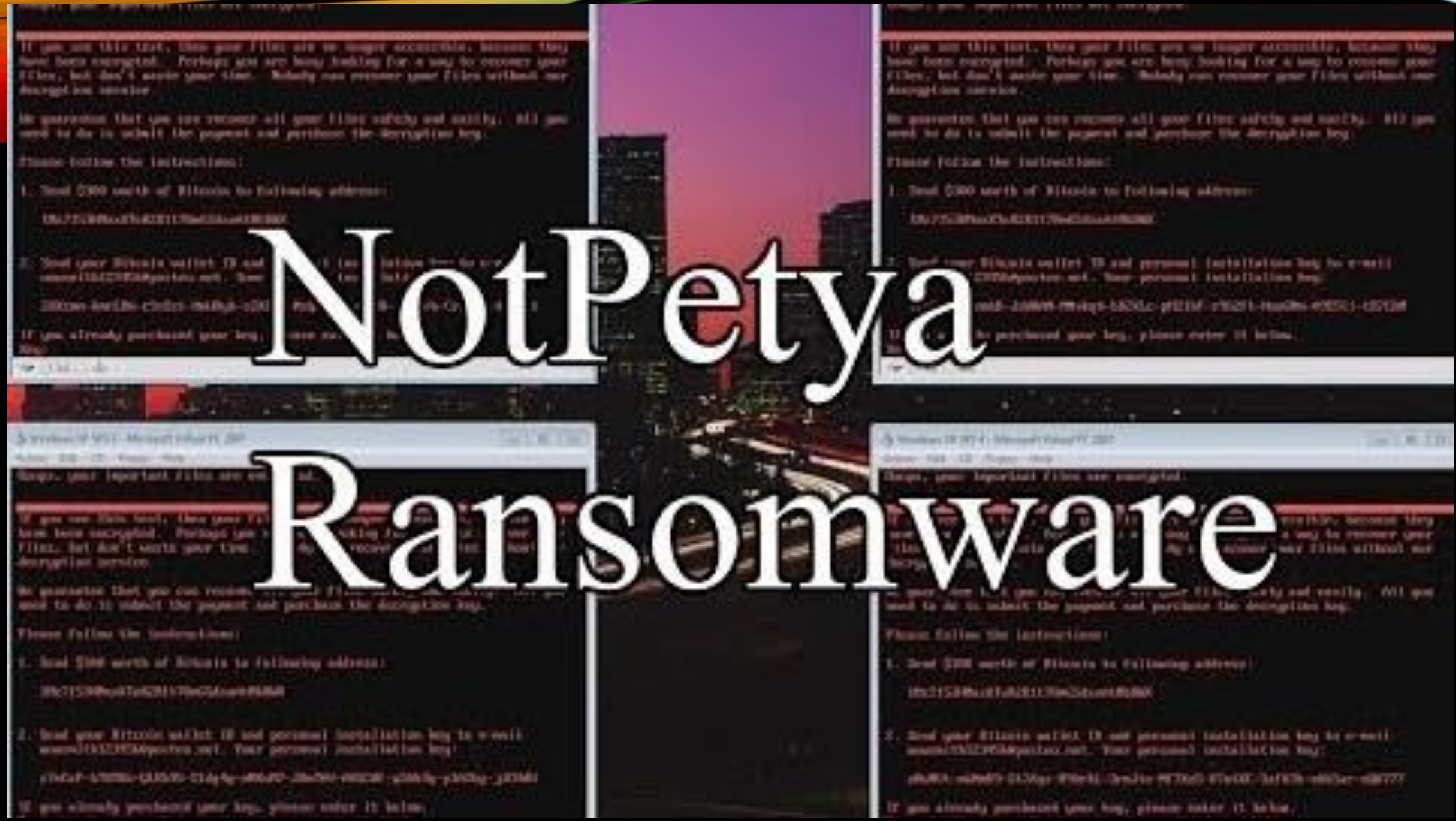
- zbiera i wykorzystuje poświadczenia w OS Windows
- wykrada dane

MEDoc

- pobranie uaktualnienia z serwera upd.me-doc.ua (wykorzystanie backdoora)
- szyfrowanie MFT i wyświetlenie żądania okupu

# PRZEBIEG ATAKU

1. Za pomocą oprogramowania do księgowości o nazwie MEDoc użytkownik pobierał aktualizację z serwera upd.me-doc.ua, gdzie hakerzy wcześniej wykorzystali backdoor oprogramowania do zainfekowania wielu komputerów.
2. Szkodliwe oprogramowanie atakuje główny rekord rozruchowy systemu, szyfrując MFT (Master File Table).
3. Wyświetla komunikat o wymogu zapłacenia w postaci kryptowaluty za zaszyfrowanie pliki tak samo jak w wirusie Petya.
4. Mimo zapłaconego okupu pliki dalej nie zostaną odszyfrowane, ponieważ wiper wymazał/usunął zawartość dysku lub zastąpił je losowymi danymi.


NotPetya
Ransomware

# KTO BYŁ NAJWIĘKSZYM OSKARŻONYM W TYM CYBERATAKU ?


NYPD

# JAK SIĘ ZABEZPIECZYĆ PRZED CYBERATAKIEM ?

- nie otwierać i nie pobierać bezmyślnie plików wykonywalnych (.exe) lub skryptów (.sh) z nieznanego źródła
- nie łączyć się z sieciami publicznymi za pomocą wi-fi
- wchodzić wyłącznie na te strony internetowe, które są w pełni bezpieczne (nie ma podejrzeń o prób phishingu lub skryptów do kopania kryptowalut)
- posiadać bardzo mocne hasło do różnych kont oraz używać menadżera haseł
- używać dwuetapowej weryfikacji !!!
- zacząć naukę Linuxa i go używać codziennie 🐧
- antywirusy są ok, ale najlepszym jest reakcja użytkownika

# CIEKAWOSTKI

- https://securitycenter.sonicwall.com/m/page/worldwide-attacks
- https://www.virustotal.com/gui/home/upload
- http://www.artur.pl/muzeum.html
- https://www.darknet.org.uk
- https://haveibeenpwned.com

# ŹRÓDŁA


- https://blog.specfile.pl/co-to-sa-te-cyberataki/
- https://www.komputerswiat.pl/artykuly/redakcyjne/najwieksze-ataki-hakerskie-i-wycieki-danych-ostatnich-lat/4qyhpcs
- https://securelist.pl/blog/7131,co_to_jest_wiper_i_skad_cale_zamieszanie_wokol_niego.html
- https://pl.wikipedia.org/wiki/Atak_NotPetya
- https://pl.wikipedia.org/wiki/Master_File_Table
- https://en.wikipedia.org/wiki/Wiper_(malware)
- https://zaufanatrzeciastrona.pl/post/komputery-zaatakowane-przez-notpetya-mogly-byc-zainfekowane-co-najmniej-od-kwietnia/

# DZIĘKUJĘ ZA UWAGĘ ☺