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:

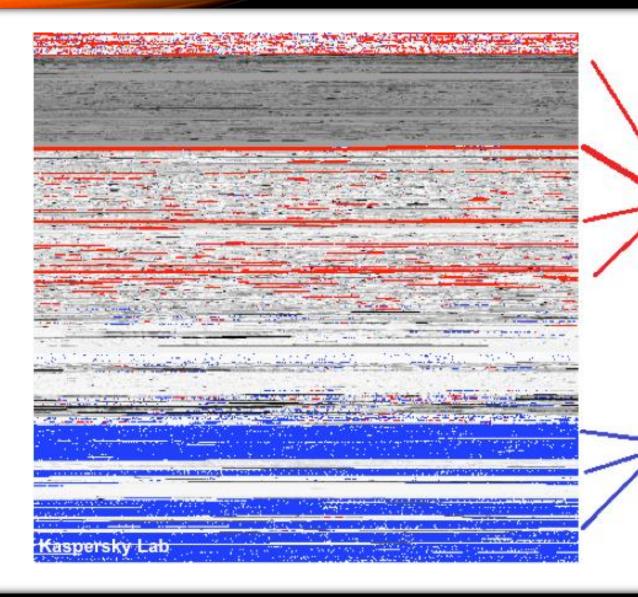
- Exploit EternalBlue
- Mimikatz
- MEDoc



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	Н	js	PNF	Rom	tif	wmdb
acl	cfg	doc	Hlp	json	png	Rpt	tiff	wmv
acm	chk	docx	HPI	Ink	pps	Rsp	tlb	xdr
amr	com	dot	Htm	log	ppt	Sam	tmp	xls
apln	cpl	drv	Html	lst	pptx	Scp	tsp	xlsx
asp	срх	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

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

- 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.



If jum on this that, then your filet of an image exempths, become they have been energeted. Perhaps and are bony hadden for a way to decome your files, but they's never your time. But of our present your files without my bearing the name of the without my bearing time assents.

the guarantees that use you recover will gove filling sufficing and satisfy. All monored to do in school the pageons and partitions the Serrogition beg.

Principle Footiow the Instructions:

1. Seed \$300 could of \$14color to finitening atterner

THE PERSON NAMED IN COLUMN 2 I

Soud upor Bitcoin wallet ID and concellative appropriate set. New INCommental civilia methyl-siki

If you already preclaims gover beg-

IotPetv

If you see this test, then your files are an imager accumible, between they have been excepted. Perhaps you are been booking for a long to recome governless, but don't paster your time. But also recomer your files without one damage in marries.

He prevented that one two recover all good filter safeing and matths. Bill you need to do to sainth the paperat and perchang the decryption boy.

Plante Forton the Instructions:

1. Send \$300 and third Blikestar to feel towing addresses

THE PERSON NAMED IN COLUMN TWO IS NOT THE OWNER, THE PERSON NAMED IN COLUMN TWO IS NOT THE OWNER, THE PERSON NAMED IN COLUMN TWO IS NOT THE OWNER, THE PERSON NAMED IN COLUMN TWO IS NOT THE OWNER, THE PERSON NAMED IN COLUMN TWO IS NOT THE OWNER, THE PERSON NAMED IN COLUMN TWO IS NOT THE OWNER, THE PERSON NAMED IN COLUMN TWO IS NOT THE OWNER, THE PERSON NAMED IN COLUMN TWO IS NOT THE OWNER, THE PERSON NAMED IN COLUMN TWO IS NOT THE OWNER, THE PERSON NAMED IN COLUMN TWO IS NOT THE OWNER, THE PERSON NAMED IN COLUMN TWO IS NOT THE OWNER, THE PERSON NAMED IN COLUMN TWO IS NOT THE OWNER, THE OW

Total tour Silectic seller ID and proposal included his to contil

mid-16804 (Write-1820), pt210 -p1221 Hunder eXEXT-18704

s perchant good larg, planes states 14 believ.

Samuel Vol. Money rough St.

O CONTRACT

Street, tent laportant fillin are or

If you can find tone, then your Fihouse here concepted. Portland your FIRE, but don't worth your than a description persons. danson

to do it which the papers and parties the deputies has

Flower Palling the Southwestings;

1. head 5000 worth of Mitcoln to Intinaing address:

BICTISS BROKETURES INTO CLASS BLANK

 Send your Rittolic wallet IV and present inequilitation log to wow it was with the large transfer and the person of the large log to the large.

CHEST - STORM - CLASS - CLASS - MARY - Jackey - MARY - SANS - - SANS - - SANS - - SANS - SANS - SANS

If you alonely perchapte their key, please enter it below.

Property and a property of the second

THE RESERVE THE PARTY OF THE PA

Wall

a way to recover year a way to recover year account may filled willbook our

med to do to make the payment and paycher the description key.

Phonon Sallies the Lastone Linear

L. Sent SHE meetle of Stickets to Pullberry address.

MICHSTRAGE LABOUR TWO SEARCH ROBOT

 Seed upon filling pariet IR and present touts liking any by a cell pages or high pariety part. Your proposed particles for that

MARK HARD DAME PROVIDENCE PRODUCTION AND AND ADDRESS OF THE PARTY.

If you already procleme town boy, please taker it he has

KTO BYŁ NAJWIĘKSZYM OSKARŻONYM W TYM CYBERATAKU ?





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-atakihakerskie-i-wycieki-danych-ostatnich-lat/4gyhpcs
- https://securelist.pl/blog/7131,co_to_jest_wiper_i_skad_cale_zamieszanie_wo kol_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 ©



