Sigurnosne prijetnje na Internetu

Ucjenjivački softver

Lovre Ninčević, 18.12.2024.

Pregled predavanja

- Pitanja za ispite
- Motivacija
- Ucjenjivački softver
- Ransomware-as-a-Service (RaaS)
- WannaCry
- Zaključak
- Literatura
- Dodatna literatura

Pitanja za ispite

- Objasni što je ucjenjivački softver i kako funkcionira
- Navedi dionike u procesu plaćanja otkupnine
- Navedi korake šifriranja podataka WannaCry ucjenjivačkog softvera
- Ukratko opiši kako funkcionira EternalBlue eksploit
- Kako funkcionira “killswitch” za WannaCry

Motivacija

- Napadači zarađuju veliku količinu novca od žrtava ransomware-a koji plaćaju otkupninu kako bi povratili pristup svojim podacima.
- Rast Ransomware-as-a-Service (RaaS) poslovnog modela
- Složenost i sofisticiranost napada

Ucjenjivački softver

- Tip zlućudnog softvera koji korisniku onemogućuje pristup uređaju i podacima na njemu, tipično šifrirajući ih
- Traži se otkupnina za povrat podataka, najčešće u kriptovalutama

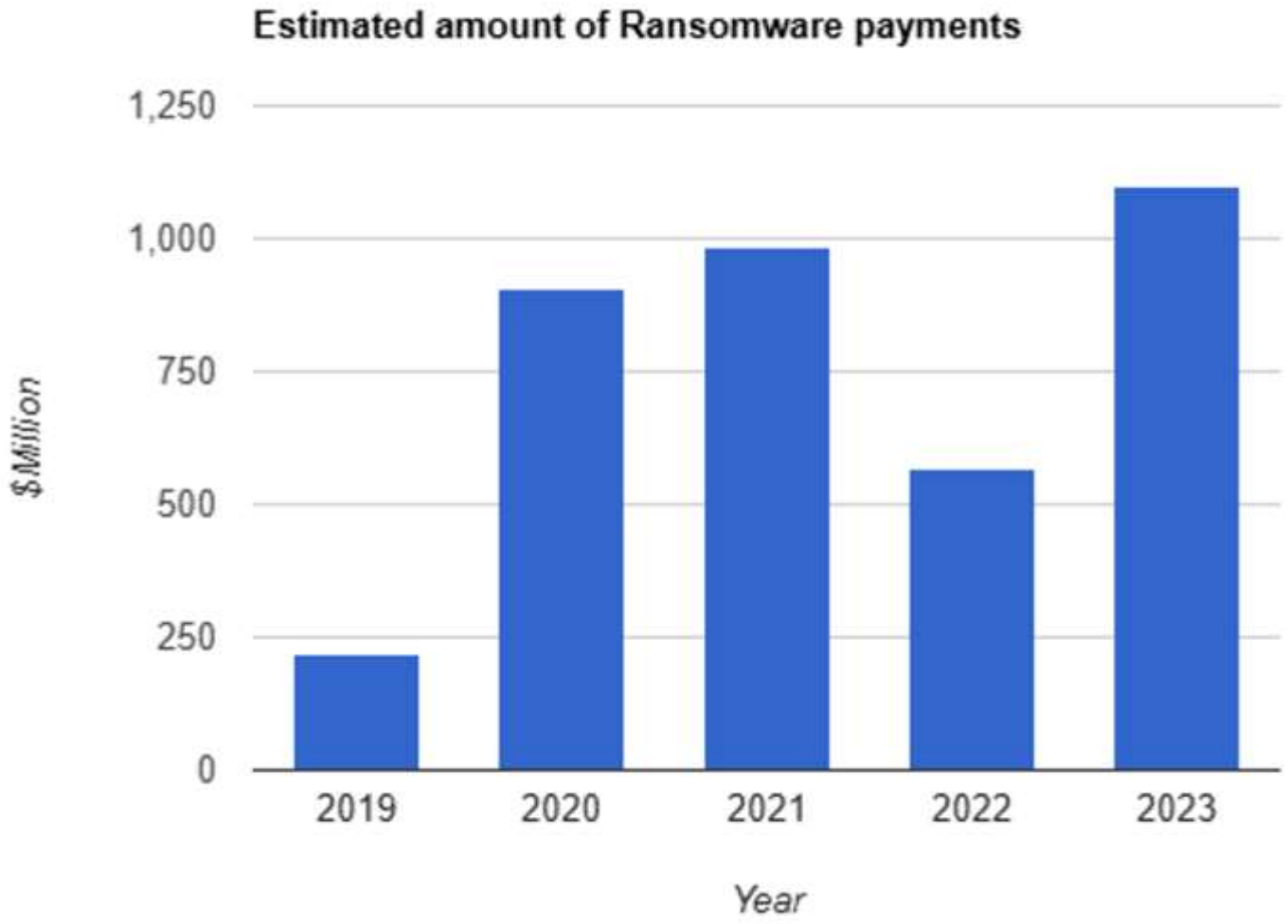
Koraci ucjenjivačkog softvera

- Access (hrv. pristup)
  - Napadač dobiva pristup računalu ili mreži
  - Postavlja softver za šifriranje
- Activation (hrv. aktivacija)
  - Napadač pokreće softver za šifriranje
  - Uređaj se zaključava, pristup podacima onemogućen
- Ransom demand (hrv. traženje otkupnine)
  - Napadač ostavlja poruku o procesu plaćanja otkupnine

Ransomware-as-a-Service (RaaS)

- Podskupina Crime-as-a-Service (CaaS) modela
- Poslovni model u kojem vlasnici ucjenjivačkog softvera iznajmljuju svoj softver kibernetičkim kriminalcima za izvršavanje napada
- Uzajamni profit programera ucjenjivačkog softvera i kibernetičkih kriminalaca koji ga koriste

Chainalysis analiza



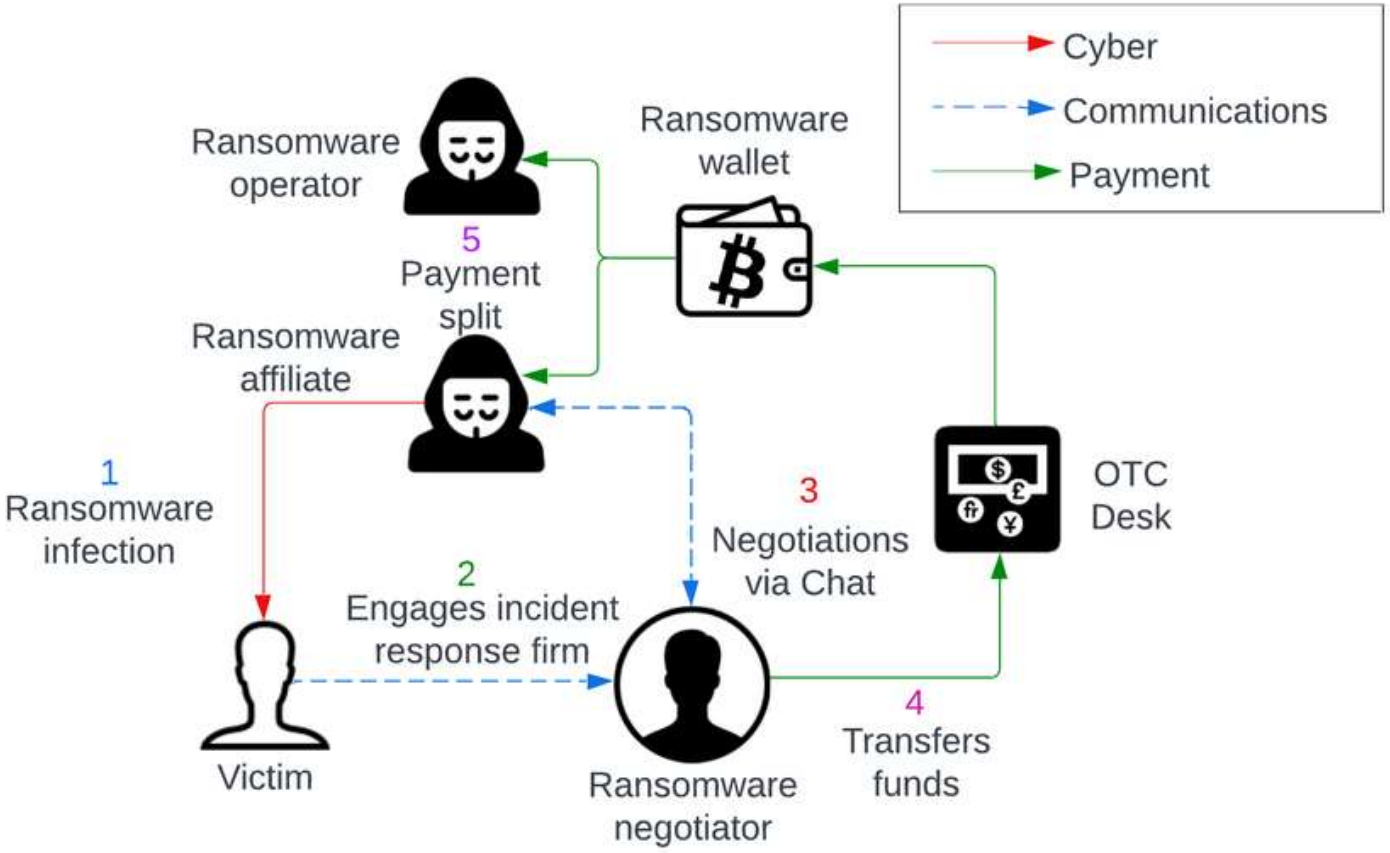
Proces plaćanja otkupnine - Dionici

- Ransomware operator (hrv. vlasnik ucjenjivačkog koda)
- Ransomware affiliate (hrv. suradnik)
- Victim (hrv. žrtva)
- Ransomware negotiator (hrv. pregovarač)

Proces plaćanja otkupnine - koraci

1. Ransomware affiliate zarazu žrtvu ucjenjivačkim softverom
2. Žrtva izvrši analizu incidenta
3. Negotiator stupi u kontakt s napadačem i pregovara o otkupnini
4. Žrtva izvrši uplatu
5. Podjela zarade između operatora i affiliate-a

Proces plaćanja otkupnine - Ilustracija



WannaCry

- Pojavio se 2017.
- Jedan od najraširenijih ransomware napada
- Ponašao se kao crv (samoreplicirajući)
- Iskorištavao ranjivost na Windows SMB uslugama (EternalBlue)
- Otkupnina u BTC


Wana Decrypt0r 2.0
Ooops, your files have been encrypted!
English
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37
Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin
ACCEPTED HERE
Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Copy
Check Payment
Decrypt

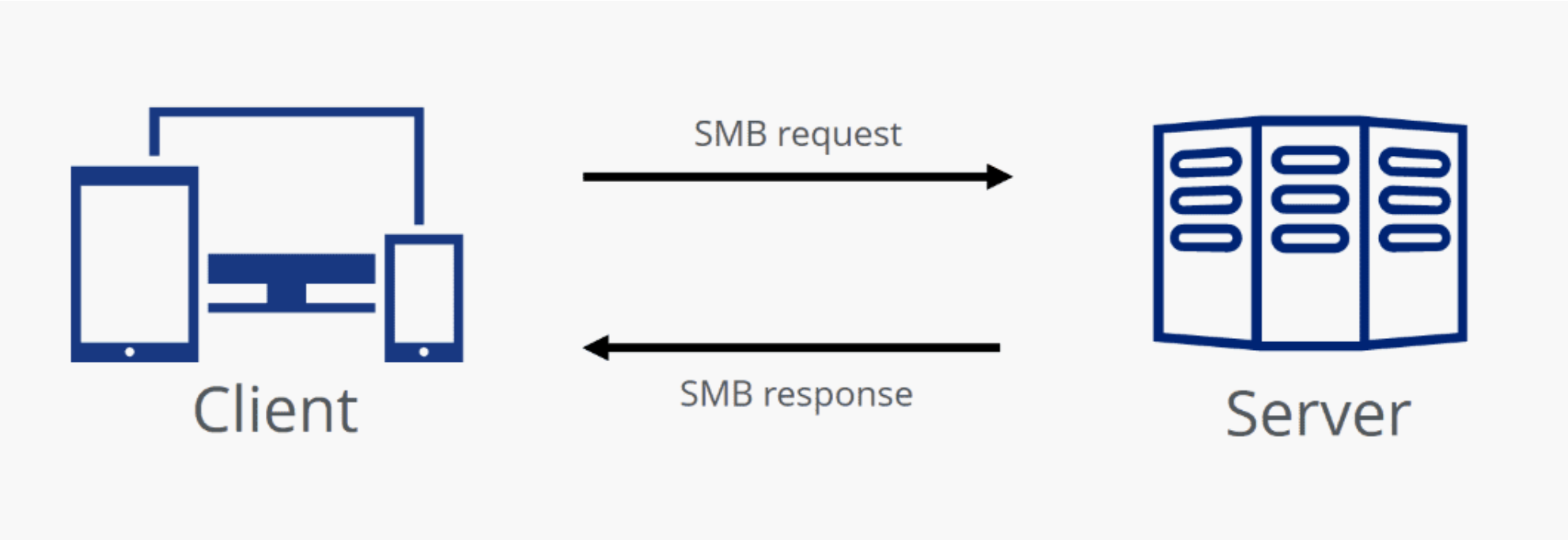
WannaCry – Koraci šifriranja datoteka

- Generiranje AES ključa za svaku datoteku
- Korištenje AES ključa za šifriranje datoteke
- Šifriranje AES ključa javnim RSA ključem (hardkodiran u samom WannaCry kodu)
- Čekanje otkupnine

WannaCry – Koraci dešifriranja datoteka

- Dostavljanje RSA privatnog ključa žrtvi nakon plaćene otkupnine
- Dešifriranje AES ključa s RSA privatnim ključem
- Dešifriranje datoteke s AES ključem

SMB (Server Message Block)



EternalBlue

- Iskorištava buffer overflow ranjivost na SMBv1
- SMB buffer prima samo određen broj bajtova, ako se pošalje više od očekivanog, višak se piše u susjednu memoriju i izvršava
- Izvršava se sa sistemskim ovlastima
- Nakon infekcije, služi za daljnju propagaciju

DoublePulsar

- Backdoor koji omogućava udaljen pristup zaraženom računalu (perzistentnost)
- Ima sistemske privilegije
- Čeka naredbe od napadača i dobavlja WannaCry ucjenjivački kod

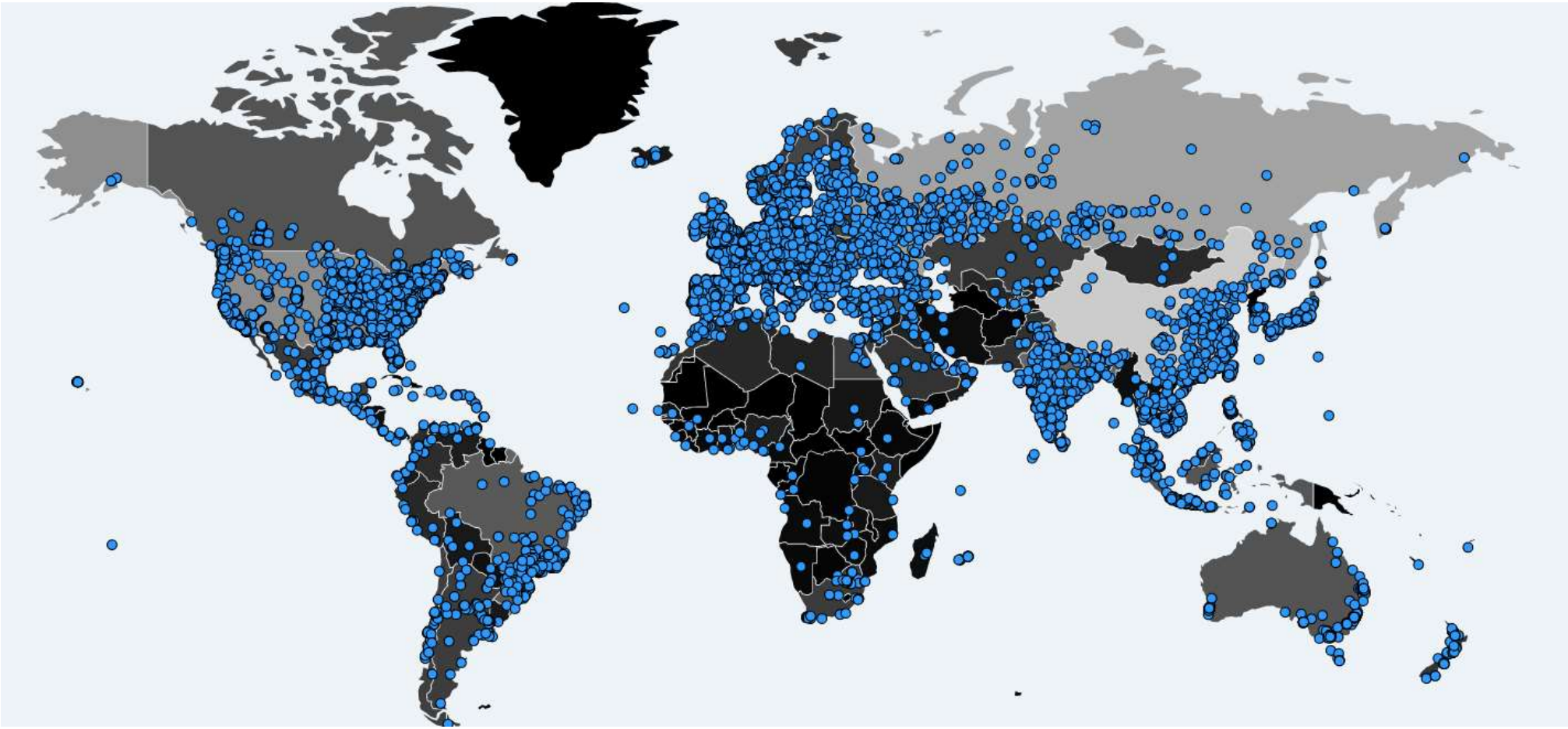
WannaCry - Rezime

- Iskorištavanje EternalBlue ranjivosti za postavljanje DoublePulsar backdoor-a
- DoublePulsar skida WannaCry ucjenjivački softver
- Skeniranje mreže i propagacija na ostale uređaje ranjive na EternalBlue
- Pokretanje WannaCry ucjenjivačkog softvera

WannaCry – “Killswitch”

- Prije postupka šifriranja podataka, WannaCry se pokušava spojiti na neregistriranu domenu
- Šifriranje podataka samo ako je spajanje na domenu neuspješno
- Svrha ove funkcionalnosti nije poznata
- Ključan za sprječavanje daljnje propagacije

WannaCry - Rasprostranjenost



WannaCry - Posljedice

- Zarada od $140,000 u BTC
- 200,000 do 300,000 zaraženih uređaja (projicirano nekoliko milijuna uređaja da nije bio aktiviran “killswitch”)
- Tko je odgovoran? Sjeverna Koreja?

Zaključak

- Uz rast popularnosti RaaS poslovnog modela, raste i broj napada ucjenjivačkog softvera
- Napadi su vrlo sofisticirani i zahtijevaju ogromno znanje i angažman od strane napadača
- Nemojte zanemariti sigurnost!!!

Literatura

- Cable, Jack, Ian W. Gray, and Damon McCoy. "Showing the Receipts: Understanding the Modern Ransomware Ecosystem." arXiv preprint arXiv:2408.15420 (2024).
- https://www.kaspersky.com/resource-center/threats/ransomware-wannacry - Opis WannaCry ucjenjivačkog softvera na stranici Kaspersky
- https://www.microsoft.com/en-us/security/business/security-101/what-is-ransomware - Definicija ucjenjivačkog softvera sa službene Microsoft stranice
- https://www.sentinelone.com/blog/eternalblue-nsa-developed-exploit-just-wont-die/ - Blog o funkcioniranju EternalBlue-a sa stranice Sentinelone
- https://www.chainalysis.com/ - Službena Chainalysis stranica

Dodatna literatura

- Matthijsse, Sifra R., M. Susanne van ‘t Hoff-de Goede, and E. Rutger Leukfeldt. "Your files have been encrypted: A crime script analysis of ransomware attacks." Trends in Organized Crime (2023): 1-27.
- Kshetri, Nir, and Jeffrey Voas. "Do crypto-currencies fuel ransomware?." IT professional 19.5 (2017): 11-15.

Hvala!