Привредна комора
Републике Српске

Cyber Threat Intelligence семинар

Свијет сајбер безбједности послије 23.фебруара

20.09.2022. у 11:00
сала ”Сутјеска”

Циљеви семинара

24. фебруара 2022. ескалација украјинске кризе довела је до глобалног хибридног рата са пратећим сајбер ратом. Ефекти сајбер рата директно су утицали на еволуцију сајбер пријетњи уз истовремену деградацију капацитета комерцијалних система заштите.

Од 24. фебруара 2022. детектована је појава: 264 фамилије нових малвера, 535 нових варијанти постојећих фамилија малвера, преко 38 000 рањивости IT система те еволуција свих врста криминалних сервиса.

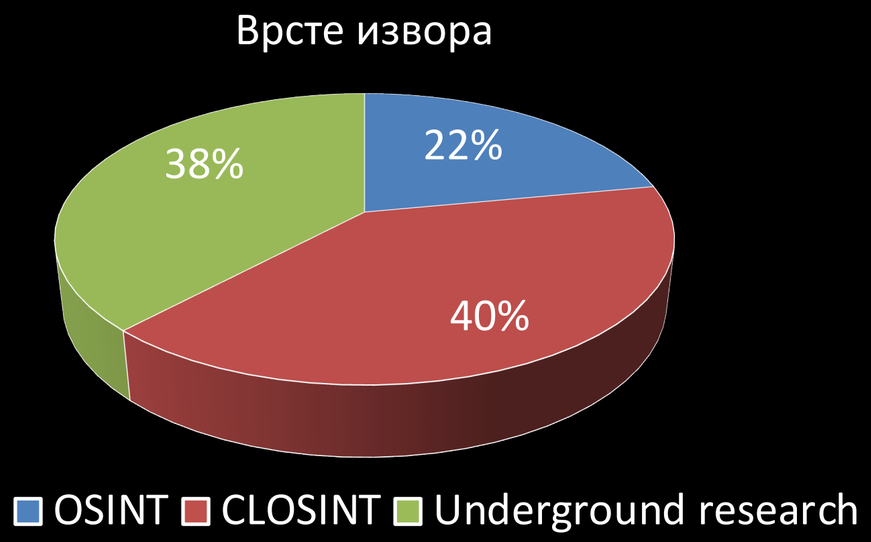
Циљеви семинара:

- презентација еволуције пријетњи
- разматрање трендова (ре)дизајна корпоративне сајбер безбједности
- разматрање развоја секторске сајбер безбједности

Особености CTI

Семинар је заснован на циљаним 7-мјесечним CTI анализама:

- ✓ Malware Intelligence: *више од 400 фамилија малвера*
- ✓ Vulnerability Intelligence: *више од 200 експлоита*
- ✓ Credential Intelligence: *900 GB података*
- ✓ Adversary Intelligence: *активности 140 група*



Теме семинара

1. IT технологије у служби хибридног рата

Кроз тему се излаже улога IT технологија у пропагандном и психолошком рату, те као средство прикупљања финансијских средстава у украјинској кризи.

2. Еволуција превара

Украјинска криза је постала генератор различитих врста превара. У теми се обрађују детектоване врсте превара.

3. Сајбер рат

Кроз тему се обрађују особености напада на објекте (државне институције, сектори енергетике, финансија, телекомуникација, транспорта), актери сајбер рата, идентификоване технике и малвери за шпијунажу и деструкцију.

4. Посљедице сајбер рата

Сајбер рат је довео до интеграције подземља сајбер криминала, кризе међународне сарадње и фрагментације (слабљења) индустрије сајбер безбједности. Кроз тему се анализирају процеси са примјерима и утицајем на регион централног Балкана.

Теме семинара

5. Еволуција криминалних сервиса

Темом се дају преглед и трендови криминалних сервиса: DDOS, Dark Market-и, MaS (Malware as a Service) са тежиштем на RaS (Ransomware as a Service). У разради RaS анализира се примјер рансомвер напада на Владу Црне Горе, те активних рансомвер малициозних софтвера.

6. Еволуција малвера

Темом се даје преглед нових фамилија малициозних софтвера из следећих категорија: Mobile malware, RAT, Banking trojan, Information-stealer, Loader, Botnet, Worm, Point of sale (POS) malware, ATM malware, Internet of things malware, DOS malware, Proxy malware, Destructive malware..

7. Еволуција рањивости

Vulnerability Intelligence и Vulnerability Management данас представљају једну од централних тачки сајбер безбједности институција и компанија. Тема обрађује значај и особености рањивости IT система. У разради се анализира контекст Log4Shell (CVE-2021-44228), реакција индустрије сајбер безбједности, те дају прегледи из подземља сајбер криминала.

Тематске дискусије

Редизајн корпоративне сајбер безбједности фин сектора

- Од пасивне до активне одбране: концепти и трендови
- Сајбер осигурања: изазови и рјешења
- Дистрибутивни anti-fraud национални системи

Развој секторске сајбер безбједности

Развој система секторске сајбер безбједности као одговор на проблем фрагментације индустрије сајбер безбједности

Материјали

Учесницима семинара ће бити подијељене:

1. листе сумњивих домена који се могу довести у везу са преварама.
2. threat hunting скрипте (Yara rules) за анализиране малициозне софтвере
3. CTI извјештаји за институције/корпорације.

CTI извјештаји укључују резултате претраге дигиталних актива компанија-институција у подземљу сајбер криминала, Darkweb маркетима, domain intelligence, OSINT/SOCMINT.