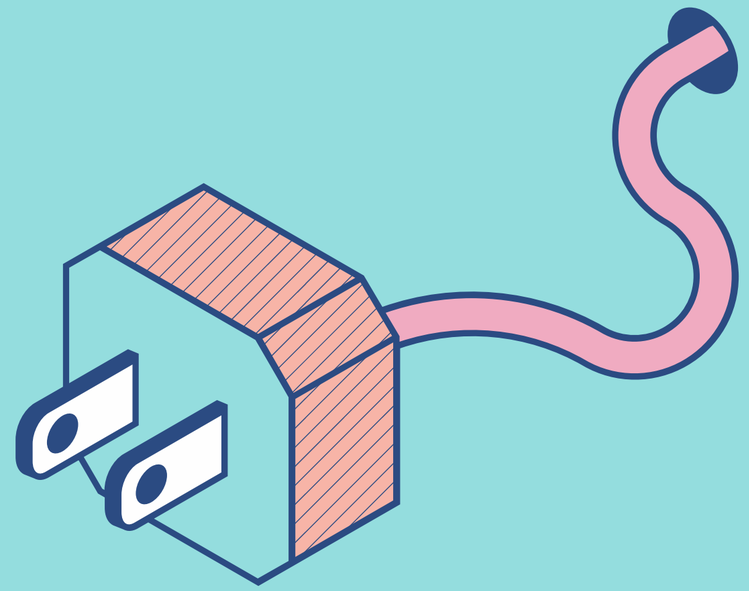
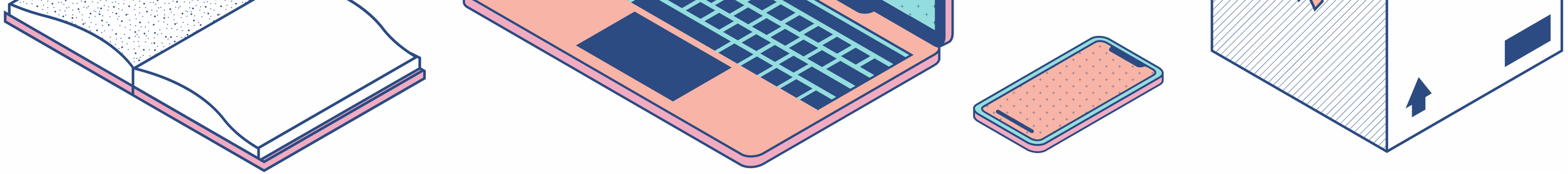
Mbrojtja ndaj sulmeve Ransomware

AUTORITETI KOMBËTAR PËR CERTIFIKIMIN ELEKTRONIK DHE SIGURINË KIBERNETIKE

Çfarë është një sulm ransomware?

Ransomware është një lloj sulmi malware, nëpërmjet të cilit sulmuesi bllokon të dhënat e viktimës, skedarët e rëndësishëm dhe më pas kërkon një pagesë për të zhbllokuar dhe dekriptuar të dhënat.
Ky lloj sulmi shfrytëzon vulnerabilitete të sistemit, të rrjetit dhe të softuerit për të infektuar pajisje të ndryshme si kompjuter, printer, telefon etj





Shembuj të sulmit ransomware

- **WannaCry -**ransomware që shfrytëzon një dobësi në protokollin Windows SMB dhe ka mekanizëm vetëpërhapjeje, që e lejon të infektojë sisteme të tjera.

- **Cerber-** është ransomware-as-a-service (RaaS), qëndron i fshehur ndërsa është duke enkriptuar skedarët dhe përpiqet të parandalojë funksionimin e antivirusit dhe funksionet e tjera të sigurisë së Windows.

- **Locky-** përhapet nëpërmjet emaileve phishing duke inkurajuar përdoruesin të hapë një skedar Microsoft Office Word/Excel me përmbajtje keqdashëse, ose një skedar ZIP që instalon malware.

- **Cryptolocker-** Zakonisht infekton kompjuterët përmes emaileve, faqeve për shkëmbimin e dokumentave (*filesharing*) dhe shkarkimeve në faqe jo-zyrtare.

- **NotPetya and Petya - Petya** infekton dhe enkripton të gjithë hard drive-n e pajisjes, duke aksesuar Master File Table (MFT). Ky sulm e bën të gjithë diskun të paaksesueshëm, edhe pse skedarët nuk enkriptohen. **Notpetya** përhapet duke shfrytëzuar vulnerabilitetet EternalBlue dhe EternalRomance të protokollit SMB të Windows.

- **Ryuk**-infekton pajisjet nëpërmjet emaileve phishing ose shkarkimeve nga faqe jo-zyrtare. Ai aktivizon një virus trojan në pajisjen e viktimës dhe krijon një lidhje të vazhdueshme rrjeti. Pasi sulmuesit të kenë instaluar trojanin në sa më shumë sisteme të jetë e mundur, enkriptohen skedarët.

Teknikat e Shpërndarjes së Ransomware

1

EMAILE PHISHING

Duke klikuar një link në email, i cili të ridrejton në një faqe të infektuar

2

BASHKËNGJITJET NË EMAIL

shkarkimi i një ose disa dokumenteve në email me përmbajtje keqdashëse

3

RRJETET SOCIALE

klikimi i një linku keqdashës në rrjetet sociale, si Facebook, Twitter etj

4

PROGRAMET E INFEKTUARA

Instalimi i një aplikacioni ose programi që përmban kod keqdashës

5

VETËPËRHAPJA

Përhapja e kodit keqdashës në pajisje të tjera përmes rrjetit dhe pajisjeve të USB

Si funksionon Ransomware?

1.**Infektimi**—Ransomware shkarkohet dhe instalohet në mënyrë të fshehtë në pajisje.

2.**Ekzekutimi -** Ransomware skanon vendndodhjet e skedarëve të ndryshëm , duke përfshirë skedarët e ruajtur lokalisht . Disa sulme ransomware gjithashtu fshijnë ose enkriptojnë çdo skedar dhe dosje backup.

3. **Enkriptimi**—kryhet një shkëmbim çelësash me Serverin C2 (*Command & Control)*, duke përdorur çelësin e enkriptimit për të enkriptuar të gjithë skedarët.

4. **Njoftimi i përdoruesit -** lajmërohet përdoruesi për infektimin e pajisjes së tij, nëpërmjet një shënimi me udhëzimet që duhen kryer dhe pagesën e shpërblimit për rikthimin e skedarëve.

5. **Pastrimi**- në këtë fazë Ransomware zakonisht përfundon ekzekutimin dhe fshihet vetë nga pajisja, duke lënë vetëm skedarët me udhëzime për të kryer pagesën e kërkuar nga viktima.

6. **Pagesa-** Viktima klikon një link, i cili përmban udhëzime sesi mund të kryhet pagesa e kërkuar.

7.**Dekriptimi-** Pasi viktima të paguajë shpërblimin e kërkuar drejt adresës së sulmuesit, e cila zakonisht kërkohet në Bitcoin, viktima mund të marrë çelësin e dekriptimit. Megjithatë, nuk ka asnjë garanci që çelësi i dekriptimit do të dorëzohet siç është premtuar.

Mbrojtja ndaj sulmit Ransomware

1.Mbrojtja "Endpoint"

Platformat moderne Endpoint ofrojnë antiviruse të gjeneratave të reja, të cilët sigurojnë mbrojtje kundër sulmeve ransomware

---

2. Backup i të dhënave

Bëni backup rregullisht të dhënat në një hard disk të jashtëm, duke përdorur rregullin 3-2-1 (krijoni tre kopje rezervë në dy media të ndryshme, ku njëra kopje rezervë të ruhet në një vend të veçantë). Nëse është e mundur, shkëputni hard diskun nga pajisja për të parandaluar enkriptimin e të dhënave, të cilat janë bërë backup.

3.Menaxhimi i patche-ve

Mbani të përditësuar sistemin operativ të pajisjes suaj dhe aplikacionet e instaluara, si dhe instaloni patch-e sigurie. Kryeni skanimet e nevojshme për të identifikuar vulnerabilitete dhe për t'i korrigjuar ato sa më shpejt.

Si të mbroheni nga Ransomware

Disa hapa për të zbutur kërcënimin e ransomware

Izolimi – identifikoni pajisjet e infektuara dhe shkëputini nga rrjeti për të parandaluar enkriptimin.

Hetimi – kontrolloni se cilat backup janë të disponueshme për të dhënat e enkriptuara. Kontrolloni se me çfarë lloji të ransomware jeni sulmuar dhe nëse ka dekriptues të disponueshëm.

Rikuperimi- nëse nuk ka mjete dekriptuese, rikuperoni të dhënat që keni ruajtur gjatë procesit të backup. Në shumicën e shteteve, autoritetet ligjzbatuese nuk rekomandojnë pagesën e *ransom*. Përdorni praktika të standardizuara dhe miratuara për të fshirë dhe rikthyer në funksion sistemet e prekura.

Identifikimi – identifikoni shkaqet e infektimit të sistemeve të brendshme dhe si të parandalohet përsëritja. Identifikoni dobësitë kryesore ose praktikat e mungesës së sigurisë që i lejuan sulmuesit të hynin dhe korrigjojini ato.

Vlerësimi – pasi të jetë zgjidhur sulmi, është e rëndësishme të vlerësohet ajo që ka ndodhur dhe mësimet e nxjerra. Si u ekzekutua me sukses ransomware? Cilat dobësi e bënë të mundur depërtimin? etj