Ransomware-as-Service (RaaS)

Si funksionon dhe si të mbrohemi?

"Një masë e vogël parandalimi vlen më shumë se një përpjekje e madhe për të riparuar dëmet." - Benjamin Franklin

AUTORITETI KOMBËTAR PËR SIGURINË KIBERNETIKE

aksk.gov.al

ÇFARË ËSHTË AKSK?

Autoriteti Kombëtar për Sigurinë Kibernetike

është institucioni përgjegjës për sigurinë kibernetike në Shqipëri, i ngarkuar për mbrojtjen e infrastrukturave kritike dhe të rëndesishme nga sulmet kibernetike. Ai luan një rol kyç në forcimin e mbrojtjes digjitale të vendit dhe koordinimin e përgjigjes ndaj incidenteve kibernetike.

🔹 Roli kryesor:

✅ Monitorimi & përgjigjja ndaj incidenteve

✅ Parandalimi i kërcënimeve kibernetike

✅ Hartimi i politikave & rregulloreve mbi sigurinë kibernetike

✅ Bashkëpunimi me partnerë ndërkombëtarë

✅ Ndërgjegjësimi & edukimi për sigurinë kibernetike, etj

⚠️AKSK funksionon si CERT* Kombëtar, duke siguruar mbrojtje proaktive ndaj kërcënimeve dixhitale në Shqipëri.

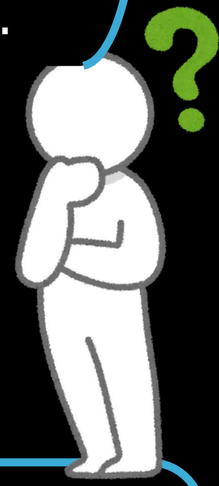
🔹 AKSK është një pikë kyçe në ekosistemin e sigurisë kibernetike, duke punuar vazhdimisht për të rritur rezistencën ndaj kërcënimeve dixhitale dhe për të ndihmuar në krijimin e një hapësire kibernetike më të sigurt për të gjithë.

***Computer Emergency Response Team (CERT)**

PSE DUHET TA NDJEK UNË KËTË WEBINAR?

- Nëse je një përdorues
  - Mëso si të mbrohesh nga ransomware dhe të shmangësh mashtrimet kibernetike.
  - Zbulo praktikat më të mira për sigurinë e të dhënave të tua personale dhe profesionale.
  - Kupto pse sulmet si Ransomware-as-a-Service (RaaS) po bëhen gjithnjë e më të zakonshme.

- Nëse je një ekspert IT/Cybersecurity
  - Zbulo taktikat më të fundit që përdorin grupet ransomware dhe si funksionon ekosistemi Ransomware-as-a-Service (RaaS).
  - Mëso teknikat më efektive për zbulimin, parandalimin dhe përgjigjen ndaj sulmeve ransomware.
  - Analizo raste reale të sulmeve dhe mëso strategji praktike për mbrojtjen e infrastrukturave kritike.



Gjithmonë mendo si një përdorues për të kuptuar rreziqet dhe si një ekspert për t'i parandaluar ato!

PËRMBAJTJA

Çfarë do të trajtojmë në këtë webinar?

- Çfarë është ransomware dhe si funksionon?
- Ransomware në histori: Si ka evoluar ky kërcënim?
- Pasojat financiare dhe impakti në shërbime kritike
- Grupet më famëkeqe të ransomware-it dhe taktikat e tyre
- Ransomware-as-a-Service (RaaS): Po sikur ransomware të përdoret si shërbim?
- Tendencat e reja në ransomware dhe sulmet e automatizuara
- Simulimi i një sulmi ransomware – Si duket një kompromet im real?
- Ransomware teknikisht: Si funksionon në detaje?
- Si të mbrohemi? Strategji dhe praktika më të mira për parandalim
- Përmbledhje
- Pyetje dhe regjistrimi për certifikate

RANSOMWARE – Kur të dhënat e tua s'janë më të tuat!

Ransomware është një lloj malware-i që bllokon të dhënat e viktimës përmes enkriptimit dhe kërkon shpërblim për dekriptimin e tyre.

Kërcënimi ka evoluar dhe sot godet individë, biznese dhe institucione qeveritare në shkallë globale.

Si funksionon ransomware?

Infektimi – Pajisja e viktimës kompromethohet përmes email-eve phishing, faqeve të infektuara, shfrytëzimit të dobësive të sistemeve ose skedarëve keqdashës.

#Hackerat shfrytëzojne çdo metodë apo pakujdesi për të infektuar viktimën#

Ekzekutimi dhe përhapja – Pasi aktivizohet, ransomware përhapet në sistemin e viktimës dhe në disa raste kërkon të infektojë edhe pajisje të tjera në rrjet.

Enkriptimi i të dhënave – Malware skanon diskun lokal, pajisjet e lidhura (USB, NAS), dhe ndonjëherë rrjetin për skedarë të rëndësishëm (dokumenta, foto, databaza, backups etj). Përdor algoritme të forta enkriptimi (AES-256, RSA-2048 etj).

Kërkesa për shpërblim – Ransomware vendos një ransom note ku informon viktimën për enkriptimin dhe kërkon pagesë në kriptomonedha për çelësin e dekriptimit.

Presioni psikologjik dhe shantazhi (Double & Triple Extortion)

- Double Extortion – Sulmuesit jo vetëm që enkriptojnë të dhënat, por edhe i eksfiltrojnë dhe kërcënojnë me publikimin e tyre në dark web nëse pagesa nuk kryhet.
- Triple Extortion – Përveç publikimit të të dhënave, sulmuesit kryejnë DDoS ndaj sistemit të viktimës ose kontaktojnë klientët e saj për të rritur presionin.

Pagesa dhe rezultati (Opsionale) – Nëse viktima paguan:

- Nuk ka garanci që do të marrë çelësin e dekriptimit.
- Disa grupe ofrojnë çelësin, por të dhënat mbeten të dëmtuara ose vetëm një pjesë e tyre rikuperohet.
- Pagesa i inkurajon sulmuesit të sulmojnë përsëri viktimën ose të shesin të dhënat e saj.

"UPSS... ICLICKED"

Visit our Blog:

Tor Browser Links:
http://ransomxifxwc5eteopdobynonjctkxxvap77yqifu2emfbecgbqdw6qd.onion/

Links for normal browser:
http://ransomxifxwc5eteopdobynonjctkxxvap77yqifu2emfbecgbqdw6qd.onion.ly/

>>> Your data is stolen and encrypted.

- If you don't pay the ransom, the data will be published on our TOR darknet sites. Keep in mind that once your data appears on our leak site, it could be bought by your competitors at any second, so don't hesitate for a long time. The sooner you pay the ransom, the sooner your company will be safe.

>>> If you have an external or cloud backup; what happens if you don’t agree with us?

- All countries have their own PDPL (Personal Data Protection Law) regulations. In the event that you do not agree with us, information pertaining to your companies and the data of your company’s customers will be published on the internet, and the respective country’s personal data usage authority will be informed. Moreover, confidential data related to your company will be shared with potential competitors through email and social media. You can be sure that you will incur damages far exceeding the amount we are requesting from you should you decide not to agree with us.

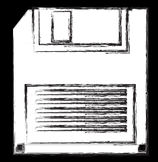
>>> Don't go to the police or the FBI for help and don't tell anyone that we attacked you.

- Seeking their help will only make the situation worse,They will try to prevent you from negotiating with us, because the negotiations will make them look incompetent,After the incident report is handed over to the government department, you will be fined <This will be a huge amount,Read more about the GDRP legislation:https://en.wikipedia.org/wiki/General_Data_Protection_Regulation>,The government uses your fine to reward them.And you will not get anything, and except you and your company, the rest of the people will forget what happened!!!!!

LockBit Petya RansomHub
WannaCry CONT REvil

RANSOMWARE NË HISTORI – SI KA EVOLUAR KY KËRCËNIM?

- SHUMË PREJNESH NUK E PËLQEJMË HISTORINË...POR HAKERAT PO!



1989 – AIDS Trojan

"Ransomware në disketë? Po, dikush mendoi se ishte një ide e mirë!"

2013 – CryptoLocker

"Hej, çfarë janë këto Bitcoin dhe pse duhet t'i blej?"

2017 – WannaCry

"Një gabim i vogël i Microsoft? Sulm global. Mësimi i ditës: Përditëso sistemin!"

RANSOMWARE NË HISTORI – SI KA EVOLUAR KY KËRCËNIM?

● SHUMË PREJNESH NUK E PËLQEJMË HISTORINË...POR HAKERAT PO! ●

2019 – RaaS (Ransomware-as-a-Service) ☠

"Po sikur ransomware të kishte support si Netflix? Tani mund ta marrësh me abonim!"

2023-2024 – Triple Extortion

"Jo vetëm që të enkriptojmë, por i nxjerrim të dhënat në dark web dhe të bëjmë DDoS për më shumë stres!"

💡 PSE DUHETTË NA INTERESOJË HISTORIA?

SEPSE RANSOMWARE PO BËHET GJITHNJË E MË INTELIGJENT, DHE NE DUHET TË JEMI NJË HAP PARA TIJ!

■ Përgjigja është e thjeshtë: PARA dhe DËMTIM!

Kërkesat për shpërblim:

- Mesatarisht $5.2 milionë për sulm në 2024
- Pagesa më e lartë: $75 milionë (Mars 2024)

Pagesat e shpërblimeve:

- $1.25 miliardë në 2023 → $814 milionë në 2024 (-35%)
- Ndërsa disa kompani refuzojnë të paguajnë, të tjerat nuk kanë zgjidhje tjetër!

Numri i sulmeve:

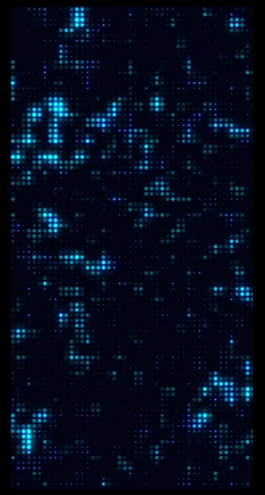
- 5,243 sulme në 2024 (15% më shumë se në 2023)

⚠ Sa më shumë të paguajnë viktimat, aq më shumë fuqizohen hakerat!

PASOJAT FINANCIARE DHE IMPAKTI NË SHËRBIME KRITIKE

Infrastruktura kritike: Rrjeti i energjisë, uji dhe transporti ndërpriten, duke ndikuar miliona njerëz.

Sektori publik: Qeveritë dhe institucionet publike goditen, duke kompromentuar të dhëna të ndjeshme.



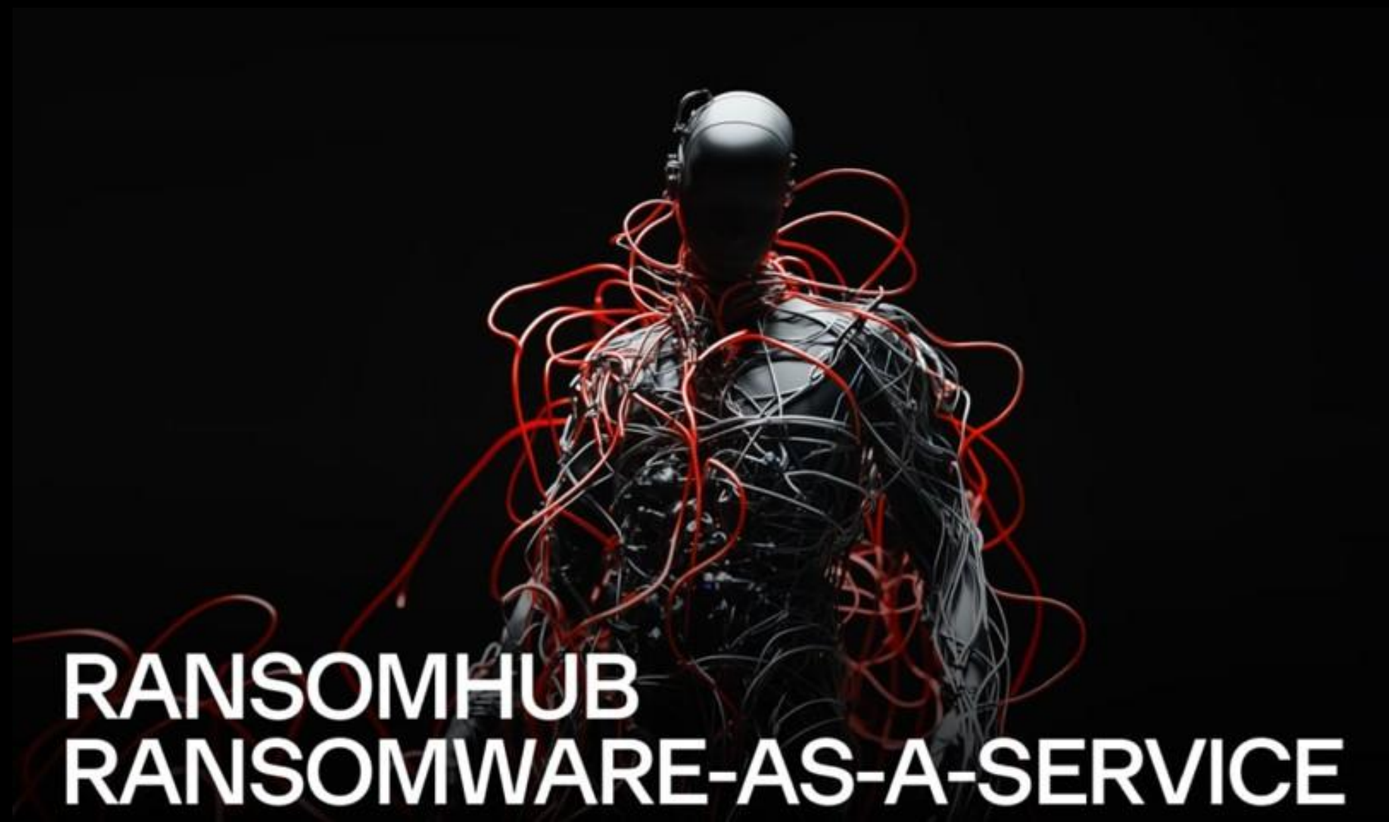
Sektori shëndetësor: Spitale dhe institucione shëndetësore ndalojnë operacionet për shkak të sulmeve ransomware.

💡 **Hakerat nuk duan vetëm para – ata synojnë të krijojnë kaos dhe panik!**

- **Cilët janë kriminelët kibernetikë që po sundojnë botën e ransomware-ë?**
- **Të dhëna bazuar në sulmet më të raportuara në 2024**

RansomHub – "Mbreti i shantazhit në 2024"

- Nr. 1 për postime të të dhënave të vjedhura – 631 raste të raportuara.
- Metoda kryesore: Double extortion – Enkriptojnë skedarët dhe publikojnë të dhënat nëse viktima nuk paguan.
- Viktimat kryesore: Sektori publik, Sektori shëndetësor dhe koorporatat.



- **Cilët janë kriminelët kibernetikë që po sundojnë botën e ransomware-ë?**
- **Të dhëna bazuar në sulmet më të raportuara në 2024**

LockBit – "Veterani i ransomware-it"

Idyti më aktiv në 2024 – 585 raste të publikuara në leak sites.

- Përdorues i modelit Ransomware-as-a-Service (RaaS), duke lejuar kriminelët të përdorin mjetet e tij kundrejt një përqindjeje të fitimeve.
- Taktikat:

✅ Sulme të shpejta duke përdorur mjete të automatizuara.
✅ Përdorimi i dobësive zero-day për të depërtuar në rrjete.
✅ Kërcënimi për publikim të të dhënave për të rritur presionin mbi viktimat.

- **Cilët janë kriminelët kibernetikë që po sundojnë botën e ransomware-ë?**
- **Të dhëna bazuar në sulmet më të raportuara në 2024**

Play – "Loja e vërtetë fillon pas enkriptimit"

- 350 sulme të raportuara në 2024.
- Taktikat kryesore:

✅ Përhapja me RDP* Brute Force dhe phishing emails.
✅ Fshirja e log-ve të sistemit për të fshehur gjurmët.
✅ Shënjestrimi i kompanive të mëdha me dobësi të njohura.

***RDP - Remote Desktop Protocol**

- **Cilët janë kriminelët kibernetikë që po sundojnë botën e ransomware-ë?**
- **Të dhëna bazuar në sulmet më të raportuara në 2024**

Akira – "Një emër i ri me taktikë të vjetër"

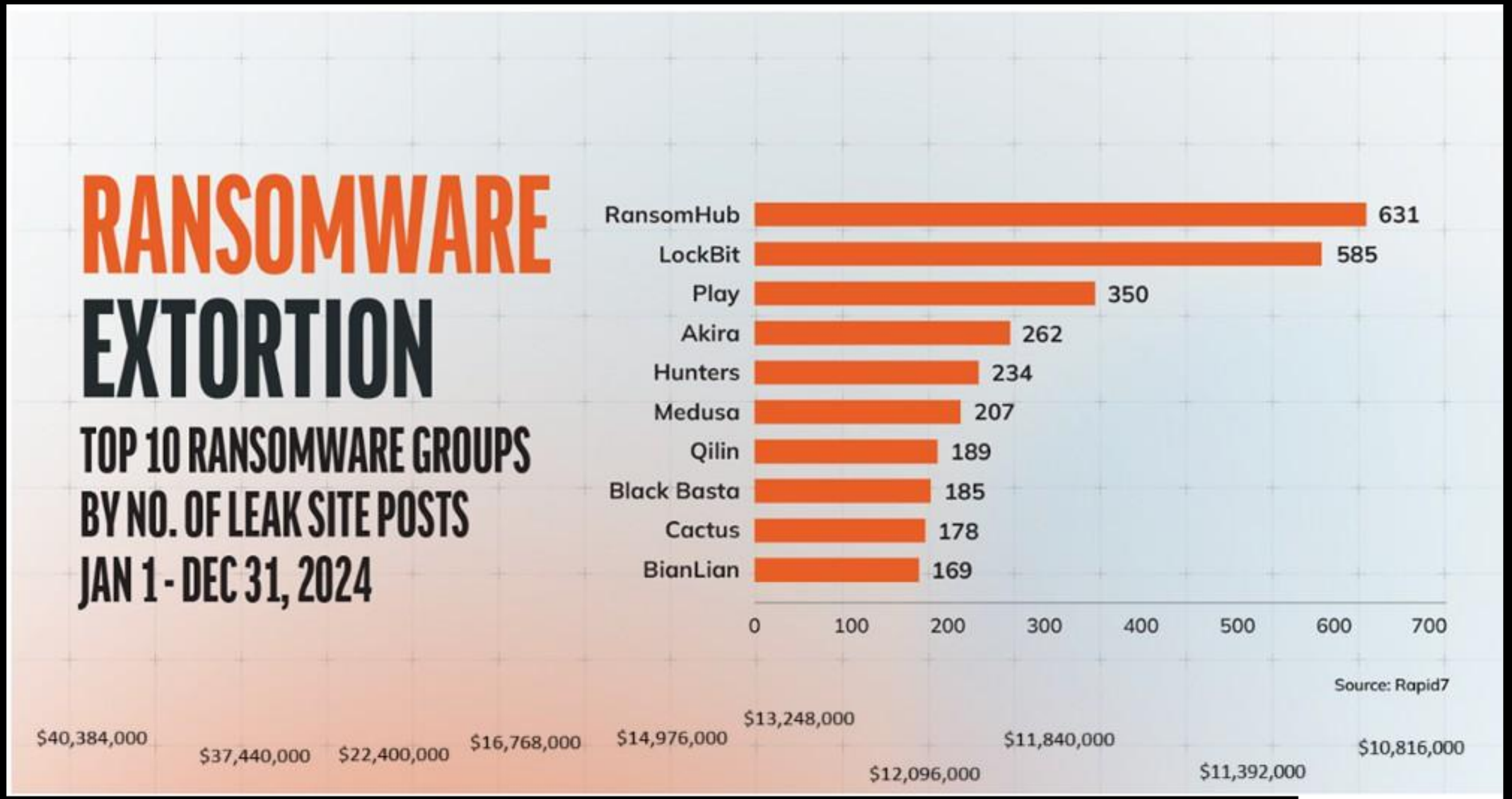
- 262 raste të raportuara në 2024.
- Kë sulmon?

✅ Biznese të vogla dhe të mesme që nuk kanë politika të forta sigurie.

✅ Kërkon shuma të mëdha shpërblimi, duke synuar pagesa të shpejta.

GRUPET MË FAMËKEQE TË RANSOMWARE-IT DHE TAKTIKAT E TYRE

- Cilët janë kriminelët kibernetikë që po sundojnë botën e ransomware-it?
- Të dhëna bazuar në sulmet më të raportuara në 2024



Ransomware nuk është më vetëm për hakerat –

tashmë është një shërbim i aksesueshëm për këdo që dëshiron të bëhet pjesë e botës së krimit kibernetik!

Nëse nuk jemi të kujdesshëm, mund të bëhemi viktima të këtij modeli biznesi të errët!

ÇFARË ËSHTË RAAS?

Si një abonim për ransomware – Kriminelët kibernetikë(hakerat) mund të blejnë ransomware ose të abonohen për të përdorur këtë shërbim.

abonim

Hakerat nuk kanë nevojë të krijojnë ransomware-in vetë – Mjafton të paguajnë zhvilluesit e malware-it dhe të fillojnë sulmet.

qera

Model biznesi për kriminelët – Zhvilluesi i RaaS merr një përqindje nga fitimet e sulmeve të kryera nga “klientët” e tij.

biznes

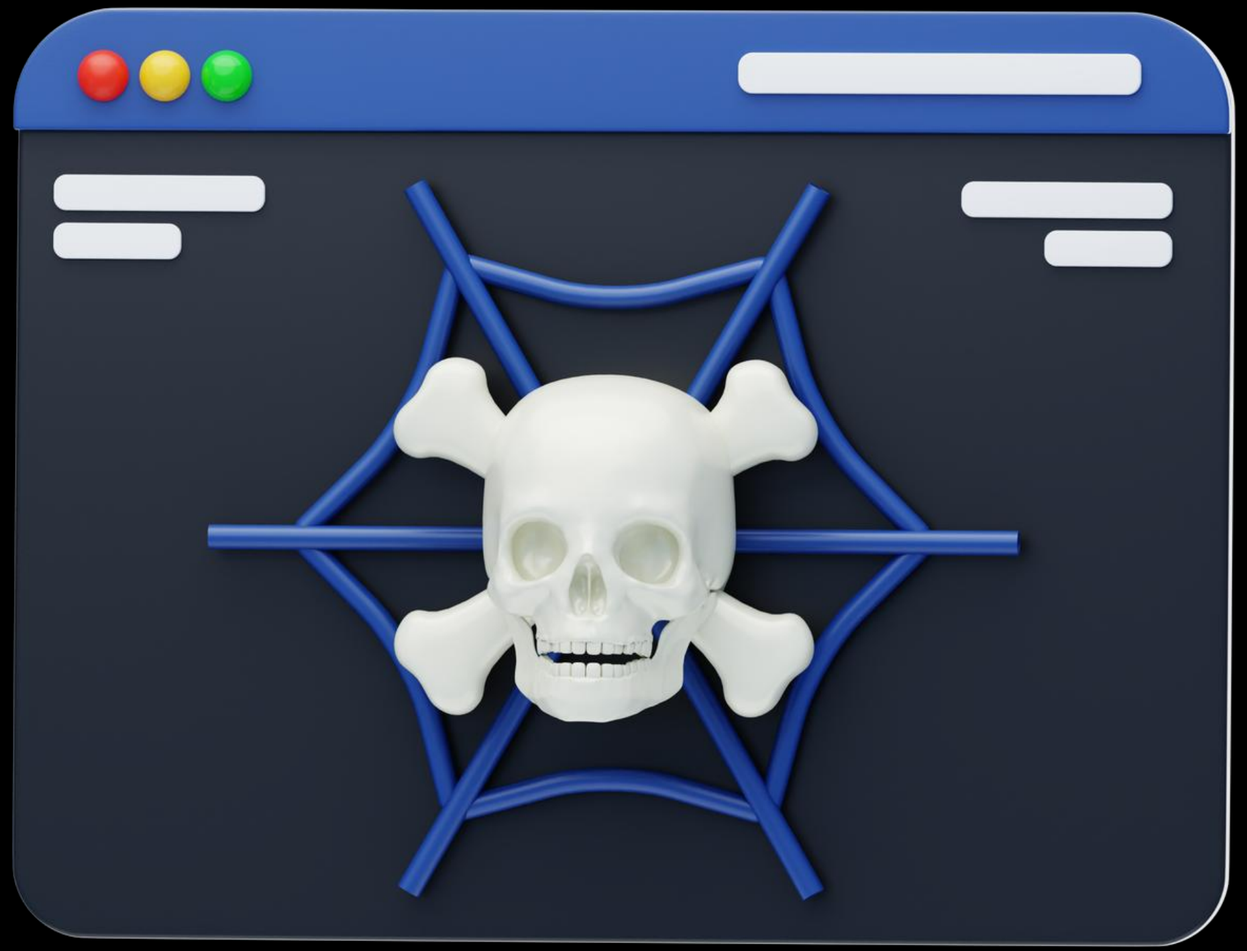
SI FUNKSIONON RAAS?

Zhvilluesit e ransomware-it krijojnë malware dhe e vendosin në dark web.

"Klientët" blejnë ose marrin me qira ransomware-in në këmbim të një tarife ose përqindjeje nga fitimet.

Ata përdorin ransomware-in për të sulmuar viktima nëpërmjet phishing, dobësive të sistemeve ose teknikave të tjera.

Fitimet ndahen mes zhvilluesve dhe ekzekutuesve të sulmeve.



Pse RaaS është kaq i rrezikshëm?

✅ E bën ransomware-in të aksesueshëm për këdo, madje edhe për njerëzit pa aftësi teknike.

✅ Shton numrin e sulmeve, pasi më shumë njerëz mund ta përdorin këtë shërbim.

✅ Evoluon vazhdimisht, duke i bërë mbrojtjet tradicionale më të vështira.

✅ Ofrohet mbështetje teknike për hakerat.

SIMULIM

A jeni gati për një simulim Ransomware?

📢 KUJDES

"Ky është një simulim edukativ për të demonstruar sesi funksionojnë sulmet ransomware. Ky test kryhet në një mjedis të izoluar (sandbox) dhe NUK duhet të përsëritet jashtë rrethanave të kontrolluara. Ky nuk është një promovim i teknikave të paligjshme, por një mënyrë për të ndërgjegjësuar dhe mbrojtur organizatat nga kërcënimet kibernetike."

SIMULIM

📢 KUJDES

"Ky është një simulim edukativ për të demonstruar sesi funksionojnë sulmet ransomware. Ky test kryhet në një mjedis të izoluar (sandbox) dhe NUK duhet të përsëritet jashtë rrethanave të kontrolluara. Ky nuk është një promovim i teknikave të paligjshme, por një mënyrë për të ndërgjegjësuar dhe mbrojtur organizatat nga kërcënimet kibernetike."

AKSESIMI FILLESTAR – SI HYJNË SULMUESIT?

Hakerat përdorin metoda të ndryshme për të futur malware-in në sistemin e viktimës:

1. Phishing emails – Email me bashkëngjitje të infektuara (.docm, .xlsm, .exe, etj).
2. Exploit kits – Shfrytëzimi i dobësive të softuereve (p.sh., EternalBlue për WannaCry).
3. RDP Brute Force – Hyrje në sistem përmes fjalëkalimeve të dobëta.
4. Malvertising – Reklama të infektuara që instalojnë malware në sfond. Ose software piratë i mundësojnë hakerave të marrin akses në kompjuterat e viktimave

Për të mësuar më shumë rreth sulmeve kibernetike dhe analizave teknike, shiko raportet e AKSK:

- **Raportet e incidenteve kibernetike – AKSK**

EKZEKUTIMI – ÇFARË NDODH PASI RANSOMWARE INFEKTON SISTEMIN?

1. Kopjon veten në sistem dhe në rrjet për të siguruar qëndrim afatgjatë.
2. Çaktivizon antivirusin dhe mbrojtjet për të shmangur zbulimin.
3. Skanon dhe liston skedarët e vlefshëm për enkriptim (dokumente, imazhe, databaza, etj).
4. Fshin shadow copies dhe çaktivizon recovery mode për të ndaluar rikuperimin.

Për të mësuar më shumë rreth sulmeve kibernetike dhe analizave teknike, shiko raportet e AKSK:

- **Raportet e incidenteve kibernetike – AKSK**

RAAS & BUILDER RANSOMWARE – SI KRIJOHEN RANSOMWARE MODERNË?

1

Së pari, hyjnë në sistemin e viktimës përmes phishing, RDP ose shfrytëzimeve.

2

Pasi kanë akses, ata përdorin një "Builder" për të krijuar një ransomware të personalizuar sipas infrastrukturës së viktimës.

3

Kjo i ndihmon të shmangin zbulimin, pasi ransomware-i nuk ka një hash fiks dhe nuk njihet nga antivirusët.

4

Ransomware Builder mund të krijojë një decryptor të personalizuar që jepet vetëm pasi viktima kryen pagesën!

Shëmbuj të grupeve që përdorin këtë metodë: LockBit, BlackCat, RansomHub, Conti, etj.

Për të mësuar më shumë rreth sulmeve kibernetike dhe analizave teknike, shiko raportet e AKSK:

- **Raportet e incidenteve kibernetike – AKSK**

ENKRIPTIMI – SI BLLOKOHEN TË DHËNAT?

Ransomware përdor algoritme të forta enkriptimi për të bërë skedarët të papërdorshëm:

1

AES-256 + RSA-2048 – Kombinon enkriptim simetrik dhe asimetrik për siguri maksimale.

2

Çelësi i enkriptimit ruhet në serverin e sulmuesit, duke e bërë rikuperimin të pamundur pa pagesë.

3

Double encryption – Disa ransomware përdorin dy nivele enkriptimi për të vështirësuar dekriptimin.

Për të mësuar më shumë rreth sulmeve kibernetike dhe analizave teknike, shiko raportet e AKSK:

- **Raportet e incidenteve kibernetike – AKSK**

REKOMANDIME

Rekomandime për individët/Përdoruesit

- Kujdes me email-et dhe phishing!

✅ Mos kliko linke apo bashkëngjitje të dyshimta – Phishing është një nga metodat kryesore të infektimit.

✅ Kontrollo gjithmonë adresën e dërguesit dhe nëse ke dyshime, verifiko përmes një burimi zyrtar.

- Përdor fjalëkalime të forta dhe autentikim me shumë faktorë (MFA)

✅ Kurrë mos përdor të njëjtin fjalëkalim për shërbime të ndryshme.

✅ Aktivizo 2FA/MFA për llogaritë e rëndësishme (email, bankë, shërbime cloud).

- Siguro të dhënat dhe pajisjet e tua

✅ Kryej backup të rregullt në një pajisje të jashtme ose në cloud të sigurt.

✅ Përdor një antivirus të përditësuar dhe sigurohu që sistemet të jenë të përditësuara.

✅ Mos përdor software të piratuar – shpesh përmbajnë malware të fshehur.

- Kujdes me lidhjet në internet

✅ Mos vendos pajisjet personale dhe të punës në të njëjtin rrjet – izolo të dhënat e rëndësishme.

REKOMANDIME

Rekomandime për profesionistët e IT dhe Cybersecurity

- Implemento strategjinë "Zero Trust"

✅ Asnjë pajisje apo përdorues nuk duhet të ketë akses të plotë pa verifikim.

✅ Kufizo privilegjet sipas principit të nevojës minimale (least privilege).

- Segmentimi i rrjetit dhe mbrojtja nga përhapja laterale

✅ Përdor VLAN dhe firewall për të izoluar sistemet kritike.

✅ Blloko protokollet e pasigurta si SMBv1, RDP pa VPN, dhe Telnet.

✅ Aktivizo Egress Filtering për të parandaluar komunikimin me C2 servers.

- Mbrojtja ndaj ransomware për sistemet dhe backup-et

✅ Implemento Immutable Backups që nuk mund të ndryshohen nga ransomware.

✅ Përdor EDR/XDR (Endpoint Detection and Response) për monitorim të avancuar.

✅ Përdor Threat Intelligence Feeds për të zbuluar IOCs (Indicators of Compromise) në rrjet.

Rekomandime për profesionistët e IT dhe Cybersecurity

- Menaxhimi i aksesit dhe monitorimi i sjelljeve anormale

✅ Aktivizo logim dhe auditim të sistemeve për të zbuluar sjellje të dyshimta.

✅ Përdor SIEM (Security Information and Event Management) për të analizuar aktivitetin në kohë reale.

- Përdorimi i sandbox dhe mjediseve të izoluara për testim

✅ Mos hap dokumente të panjohura në sistemin kryesor! Përdor sandbox si Any.Run, FLARE VM ose Cuckoo Sandbox.

✅ Nëse teston malware për qëllime edukative, përdor një makinë virtuale të izoluar me snapshot të ruajtur.

PËRMBLEDHJE

Autoriteti Kombëtar për Sigurinë Kibernetike

- Ransomware është një industri kriminale miliardë-dollarëshe!

✅ Si funksionon? – Infekton përmes phishing, RDP, exploit kits, enkripton të dhënat dhe kërkon pagesë.

✅ RaaS – Kriminelët krijojnë ransomware sipas nevojës dhe ofrojnë decryptor pas pagesës.

✅ Grupet më të rrezikshme – LockBit, RansomHub, BlackCat, Cl0p përdorin double/triple extortion.

✅ Si të mbrohemi?

- Individët – Kujdes me phishing, aktivizoni MFA, bëni backup.
- IT & Cybersecurity – Zero Trust, Immutable Backups, SIEM/XDR monitoring.

✅ Nëse ndodh një sulm? Mos paguaj menjëherë! Izolo sistemin dhe raportoje te autoritetet përgjegjëse.

Mëso më shumë nga raportet e AKSK → Raportet e AKSK

Parandalimi është arma më e fortë kundër ransomware-it!

www.aksk.gov.al

Pyetje?

Webinaret mund të jenë të mërzitshëm... por ransomware-i nuk është!

Për më tepër :

www.facebook.com/aksk.gov.al

www.instagram.com/aksk.gov.al

www.linkedin.com/aksk.gov.al

Pak kohë për plotësimin e formës

www.aksk.gov.al

Faleminderit

Mos harroni: Më mirë të parandalosh sesa të paguash!