# Trendet Kryesore të Sigurisë Kibernetike në 2025

# Hyrja

- Në vitin 2025, vëllimi i të dhënave të gjeneruara në përditshmëri  globalisht pritet të arrijë mbi 180 zettabytes, krahasuar me 147 zettabytes të gjeneruara në vitin 2024.
- Administratat shtetërore janë ndër sektorët më të synuar nga sulmet kibernetike për shkak të ndjeshmërisë së të dhënave që mbajnë.
- Dëmet globale nga sulmet kibernetike në vitin 2024 ishin rreth 10 Trilion dollarë.
    - Dëmet e shkaktuara në Europë nga sulmet kibernetike , sektori shtetëror, në vitin 2024 ishin rreth 1.5 Bilion dollar.

**Të dhënat përmbajnë informacion të ndjeshëm mbi qytetarët, bizneset dhe infrastrukturat kritike.**

# Trendet Kryesore të Sulmeve Kibernetike në 2025

- **Kërcënime të sponsorizuara nga shteti - APT**
- **Ransomware**
  - **Double Extortion**
  - **RaaS (Ransomware-as-a-Service)**
- **Sulmet e Inxhinierisë Sociale dhe Phishing**
  - Taktika të tilla si **Whaling** (targetimi i drejtuesve të lartë), **Spear Phishing** (targetimi i personalizuar), **Smishing** (përmes SMS-ve), dhe **Vishing** (telefonata të manipuluara).
  - **Deep Fake** (AI Tool)
- **Sulmet DDoS (Distributed Denial of Service)**
- **Sulmet në Zinxhirin e Furnizimit (Supply Chain Attacks)**
- **Sulmet që Targetojnë Pajisjet IoT**
- **Kërcënimet e Gjeneruara nga Inteligjenca Artificiale**

# Rast Studimor I – Social Engineering & Impersonation

**Periudha:** Janar 2025

**Sulmuesit:** Grupet ruse STAC5777 (Storm-1811) dhe STAC5143 (mendohet të ketë lidhje me FIN7)

**Përmbledhje:** Sulmuesit shfrytëzuan Microsoft Teams për të hyrë në infrastrukturë.

**Metodologjia e Sulmit:**

- **Bombardimi me Email-e:** mbingarkimi i punonjësme me një numër të madh email-esh të padëshiruara, deri në 3,000 në një orë.

Qëllimi: krijimi i konfuzionit dhe urgjencës.

- **Impersonifikimi në Microsoft Teams:** impersonimi i stafit të IT (help desk) të Microsoft Teams.

Ata shfrytëzuan cilësimet e paracaktuara të platformës, të cilat lejojnë komunikimin e përdoruesve të jashtëm me punonjësit e brendshëm, dhe kontaktuan viktimat duke pretenduar se do të zgjidhnin problemin e spam-it.

- **Fitimi i Aksesit (remote access):** kërkuan qasje remote në kompjuterët e viktimave, ndarjes së ekranit në Teams (screen share) ose Microsoft Quick Assist.

Pasi morën aksesin, ata instaluan ransomware, duke enkriptuar të dhënat dhe kërkuar pagesë për dekriptimin.

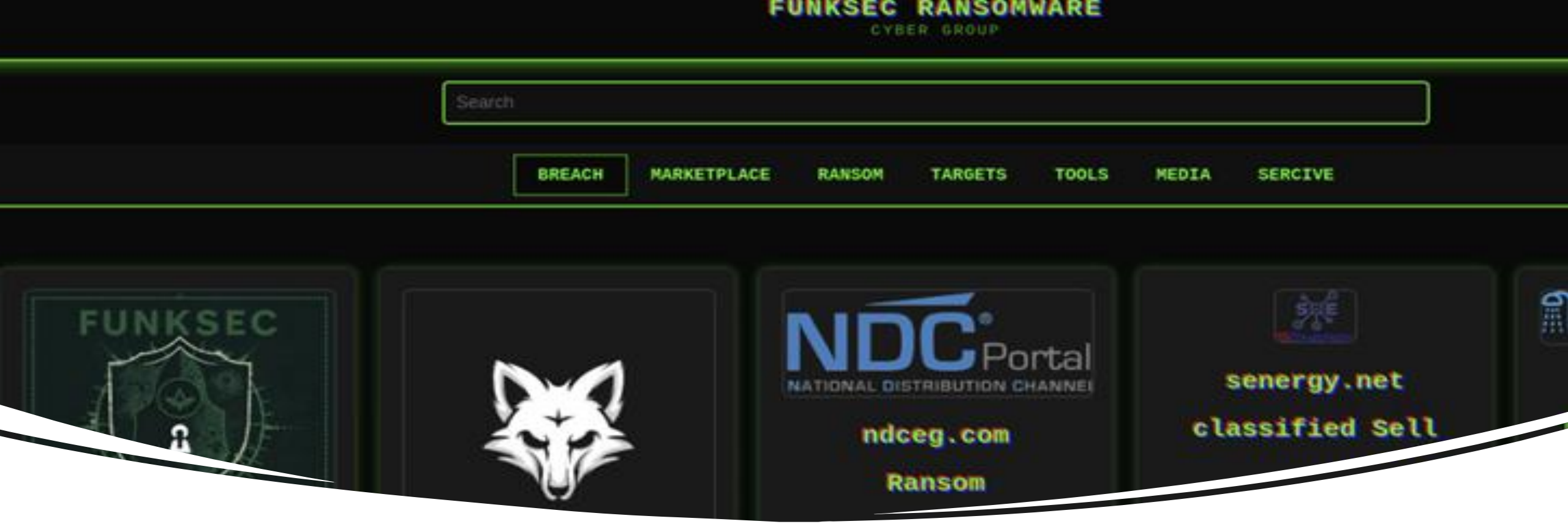
# Rast Studimor I – Social Engineering & Impersonation

**Pikat Kyce**

- **Nivel të lartë planifikimi dhe realizimi**, duke kombinuar social engineering me impersonation dhe dobësitë e infrastrukturës.
- Duke u hequr si persona të besueshëm të brendshëm(**impersonation i suportit të Microsoft Teams**), sulmuesit manipuluan punonjësit për t'u dhënë akses në kompjuterat e tyre.
- **Shfrytëzuan cilësimet e paracaktuara** (default) të Microsoft Teams që lejojnë komunikim të jashtëm.

**Rekomandime**

- **Për përdoruesit:** Trajnime për rritjen e ndërgjegjësimit mbi sigurinë kibernetike dhe udhëzime se kujt duhet t'i drejtohen në raste të tilla (SOC/IT) si edhe verifikimin e kërkesave të dyshimta nga help desk.
- **Përmirësimi i Infrastrukturës:** mos lihen konfigurimet default të aplikacionit Teams, të ndalohet komunikimi me palë të treta jashtë kompanisë si edhe të kufizohet aksesi remote i kompjuterave vetëm për një grup të caktuar (p.sh. Help Desk), pajisja me email gateway dhe automatizime.




# Rast Studimor II – Ransomware

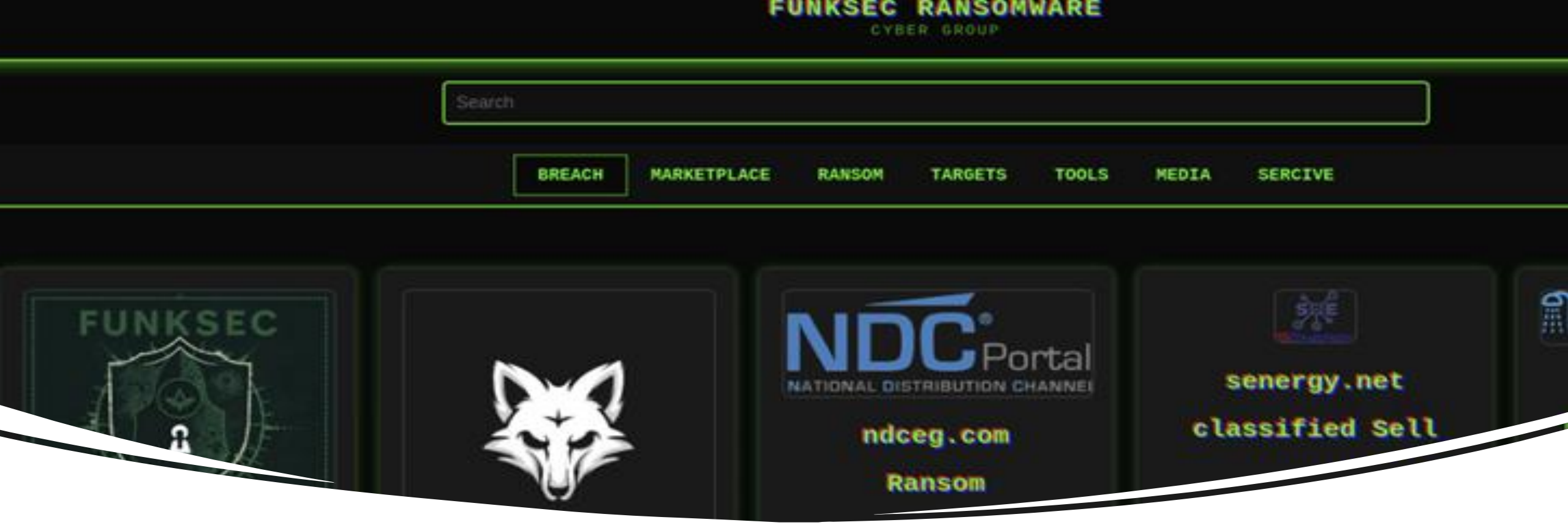
**Periudha:** Dhjetor 2024

**Sulmuesit:** FunkSec

**Përmbledhje:** Sulmuesit shfrytëzuan inteligjencën artificiale për realizimin e double extorsion në organizata të ndryshme.

**Metodologjia e Sulmit:**

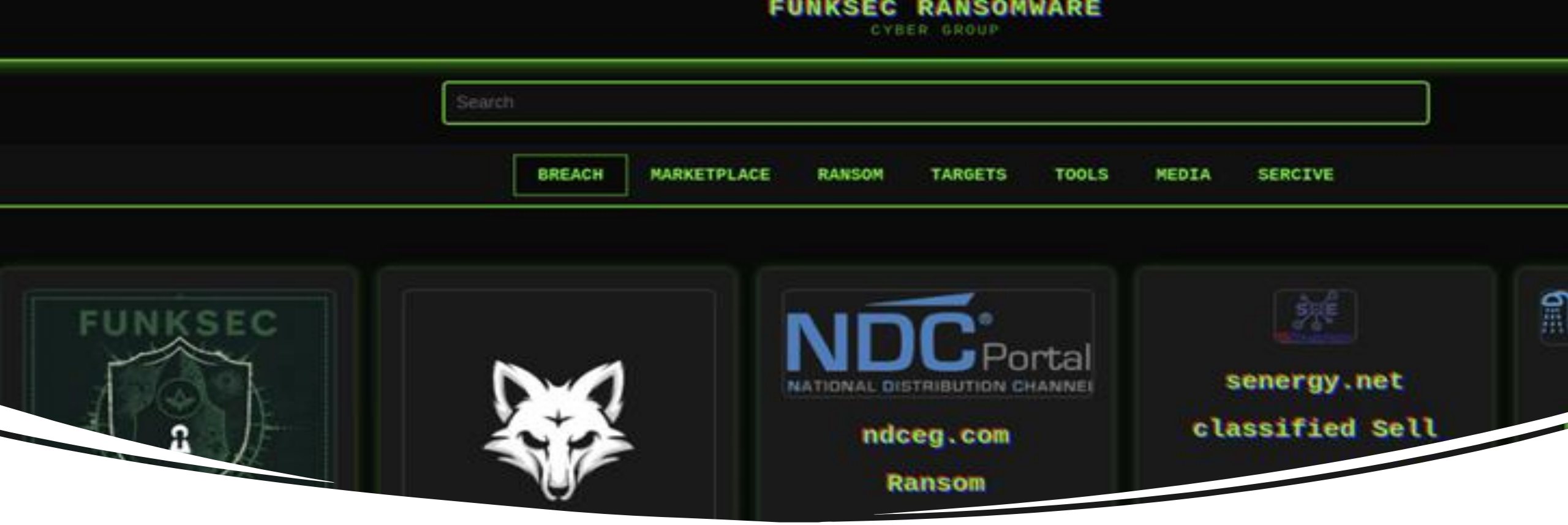
- **Përdorimi i Inteligjencës Artificiale** (AI) për të automatizuar dhe optimizuar procesin e sulmeve, duke krijuar një metodë më të fuqishme dhe më të vështirë për t'u zbuluar.
- **Double Extortion:** Eksfiltrim të dhënash, enkriptim i tyre, ramsome që organizata duhet të pagujë, si edhe shitja e të dhënat e vjedhura për fitim të mëtejshëm.
- Nga sulmi u afektuan mbi **85 viktima në mbarë botën**, duke përfshirë organizata të sektorëve të ndryshëm si **financiar, shëndetësor dhe edukativ.**




# Rast Studimor II – Ransomware

**Pikat Kyce**

- **Përdorimi i AI:** Automatikon dhe optimizon sulmet, përfshirë enkriptimin dhe përdorimin e mjeteve të avancuara.
- Mënyrat e Hyrjes (**Initial Access**):Phishing, Shfrytëzimi i Vulnerabiliteteve, Brute Force dhe Credential Stuffing, RDP (Remote Desktop Protocol), Social Engineering dhe Impersonation
- **Data Leak Site** për centralizimin e sulmeve: ransomware, shpërndarjen e të dhënave të vjedhura, RaaS, tools i përdorur për DDoS..
- Viktimat Kryesore: SHBA, India, Brazili.




# Rast Studimor II – Ransomware

**Rekomandime**

- **Për përdoruesit:** Ofrimi i trajnimeve të rregullta për rritjen e ndërgjegjësimit mbi sigurinë dhe higjenën kibernetike.
- **Përmirësimi i Infrastrukturës**: Sigurimi i **përditësimeve** të rregullta të softuerëve, implementimi i **MFA**, përdorimi i **email gateway** të avancuar për email-et, realizimi i a**uditimeve të sigurisë dhe testimeve** të vazhdueshme të infrastrukturës (pentesting). Gjithashtu, zbatimi i praktikave më të mira për krijimin e **fjalëkalimeve të forta** ose përdorimi i metodave **passwordless**, monitorimi i trafikut të dyshimtë, implementimi i qasjes "**least-privilege**", përdorimi i **softuerëve për kontrollin e aplikacioneve** dhe krijimi i politikave për kufizimin e aksesit me RDP vetëm për një grup të caktuar punonjësish.

# Masat që Duhet të Ndërmerren

- Përmirësimi i sistemeve të mbrojtjes përmes implementimit të teknologjive të avancuara.
- Zbatimi i zgjidhjeve të bazuara në Inteligjencë Artificiale për përmirësimin e mbrojtjes.
- Zbatimi i Qasjes "Zero Trust"  dhe "Least Priviledge".
- Sigurimi i përputhshmërisë me standardet e sigurisë dhe praktikave më të mira të industrisë.
- Kryerja e testimeve të rregullta të sistemeve për të siguruar qëndrueshmëri dhe mbrojtje.
- Kryerja e vlerësimeve të vazhdueshme të sigurisë.
- Krijimi i një plani për menaxhimin e incidenteve të sigurisë.
- Përgatitja dhe trajnimet e punonjësve për ndërgjegjësimin mbi rreziqet e mundshme.
- Përditësimi i vazhdueshëm me lajmet dhe kërcënimet e reja të sigurisë kibernetike.

# Rëndësia e Trajnimit të Punonjësve

- **88% e Sulmeve Kibernetike** ndodhin për shkak të gabimeve njerëzore. Trajnimi është kyçi për të reduktuar këtë rrezik.
- **Rritja e Ndërgjegjësimit**: Punonjësit e trajnuar janë më të vetëdijshëm për rreziqet dhe mund të shmangin gabimet kritike.
- **Si mund të trajnohen punonjësit?**
  - **Simulime reale të sulmeve** për të praktikuar reagimet në situata të vërteta.
  - **Workshope mbi praktikat më të mira** për të forcuar njohuritë e sigurisë.
  - **Kurse online të personalizuara** që lejojnë përvetësimin e njohurive në mënyrë fleksibël

## Agjensia Kombëtare  e Sigurisë Kibernetike

- Monitoron dhe mbikëqyr incidentet e sigurisë kibernetike ndaj CII-ve.
- Përgjegjës për kategorizimin dhe prioritizimin e incidenteve bazuar në natyrën dhe impaktin e tyre, sipas rregullores të kategorizimit të incidenteve
- Siguron mbështetje dhe koordinim në përgjigjen ndaj incidenteve kibernetike.

## Infrastrukturat e Rëndësishme dhe Kritike

- Raportojnë çdo incident të rëndësishëm kibernetik në afat të përcaktuar sipas ligjit dhe akteve nënligjore.
- Kategorizimi i incidenteve bëhet sipas 12 kategorive të rregullores për kategorizimin e incidenteve. (brenda 4 orëve, vendosja në dispozicion kopjen e logeve)
- Incidentet  e rëndësishme raportohen brenda 72 orëve nga identifikimi, vleresimin fillestar me përditësime periodike për sulmet më të sofistikuara.
- Raportimi bëhet përmes platformës online, emailit ose telefonit, duke përdorur formatin zyrtar të raportimit të incidentit.

# Rregullore

- Rregullore për Procedurat e Menaxhimit të Incidenteve të Sigurisë Kibernetike, Kundërmasat dhe Playbooks (Miratuar me Urdhër Nr.1089, datë 18.12.2024)
- Rregullore për Mënyrat dhe Afatet e Ruajtjes së Log-eve të Incidenteve të Sigurisë Kibernetike (Miratuar me Urdhër Nr.408, datë 07.11.2024)
- Rregullore për Kategorizimin e Incidenteve të Sigurisë Kibernetike (Miratuar me Urdhër Nr.299, datë 21.08.2024)
- Rregullore mbi Mënyrën e Dokumentimit dhe Implementimit të Masave të Sigurisë në Infrastrukturat Kritike dhe të Rëndësishme të Informacionit (Miratuar me Urdhër Nr. 97, datë 05.03.2024)
- Rregullore mbi Përmbajtjen dhe Mënyrën e Dokumentimit të Masave të Sigurisë (Versioni 2.0) (Ndryshuar me Urdhër Nr.148, datë 20.07.2023)
- Rregullore për Kategoritë e Incidenteve Kibernetike si dhe Formatin e Elementët e Raportit (Miratuar me urdhër nr.62, datë 10.09.2018)
- Rregullore e Brendshme

# FALEMINDERIT!

https://forms.office.com/e/5keB0D0K97?origin=lprLink

# Referenca


- https://cybernews.com/security/russian-hackers-ransomware-microsoft-teams-sophos/
- https://www.techradar.com/pro/security/microsoft-teams-abused-in-russian-email-bombing-ransomware-campaign
- https://www.itpro.com/security/cyber-attacks/hackers-are-using-microsoft-teams-to-conduct-email-bombing-attacks
- https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/ai-powered-cyberattacks/
- https://thehackernews.com/2025/01/ai-driven-ransomware-funksec-targets-85.html?utm_source=chatgpt.com
- https://www.bing.com/search?q=2025+threat+lanscape+cyber+threats+2025+&qs=n&form=QBRE&sp=-1&ghc=1&lq=0&pq=2025+threat+lanscape+cyber+threats+2025&sc=4-39&sk=&cvid=73F7ED8547984AD38D40A19E4062A610&ghsh=0&ghacc=0&ghpl=