REPUBLIKA E SHQIPËRISË
AUTORITETI KOMBËTAR PËR SIGURINË KIBERNETIKE
DREJTORIA E ANALIZËS SË SIGURISË KIBERNETIKE

Analizë teknike për skedarin keqdashës
RaLord-0xb

Versioni: 1.0
Datë: 13/01/2026

PËRMBAJTJA

Ky raport ka kufizime dhe duhet interpretuar me kujdes!

Disa nga këto kufizime përfshijnë:

Faza e parë:
Burimet e informacionit: Raporti është bazuar në informacionet të vendosura në dispozicion në momentin e përgatitjes së tij. Ndërkohë, disa aspekte mund të jenë të ndryshme nga zhvillimet aktuale.

Faza e dytë:
Detajet e analizës: Për shkak të kufizimeve burimore, disa aspekte të skedarit keqdashës mund të mos jenë analizuar thellësisht. Çdo informacion shtesë i panjohur mund të reflektojë në ndryshime të raportit.

Faza e tretë:
Siguria e informacionit: Për të mbrojtur burimet dhe informacionet konfidenciale, disa detaje mund të jenë të zbutura ose jo të përfshira në raport. Ky vendim është marrë për të mbajtur integritetin dhe sigurinë e të dhënave të përdorura.

AKSK rezervon të drejtën për të ndryshuar, përditësuar, ose ndryshuar çfarëdo pjesë të këtij raporti pa lajmërim paraprak.

Ky raport nuk është një dokument përfundimtar.
Gjetjet e raportit bazohen në informacionin e disponueshëm gjatë kohës së hetimit dhe analizës. Nuk ka garanci në lidhje me ndryshime të mundshme apo përditësime të informacioneve të raportuara gjatë periudhës në vijim. Autorët e raportit nuk marrin përgjegjësi për përdorimin e gabuar ose pasojat e ndonjë vendimmarrjeje të bazuar në këtë raport.

Informacione Teknike

Është evidentuar qarkullimi i një fushate sulmesh kibernetike duke përdorur Ransomware nga grupi **NOVA Ransomware Group**, ku vërehen teknika dhe taktika të reja. Ky grup u shfaq për herë të parë në vitin 2024 dhe aktiviteti i tyre tregon një metodë sulmesh të fokusuara. Grupi kombinon enkriptimin e sistemeve me vjedhjen e të dhënave sensitive, duke përdorur kërcënime se do të ekspozojë këto të dhëna duke rritur dhe forcuar kërkesat për pagesë. Nga një këndvështrim operacional, Nova favorizon efikasitetin mbi inovacionin, duke përdorur teknika të vendosura siç janë çaktivizimi i kopjeve rezervë, ndalimi i shërbimeve të sigurisë dhe shfrytëzimi i mjeteve legjitime administrative për të lëvizur në rrjetet e kompromentuara. Megjithëse ende me profil të ulët, **Nova** paraqet se si aktorët e rinj të ransomware-ve mund të shkaktojnë shpejt sulme kibernetike domethënëse duke shfrytëzuar dobësitë e njohura në mbrojtjet e infrastrukturave të informacionit.

Analiza e skedarit RaLord-0xb

Skedari RaLord-0xb është një skedar i ekzekutueshëm në sistemet operative Windows dhe është i krijuar me gjuhën e programimit RUST.

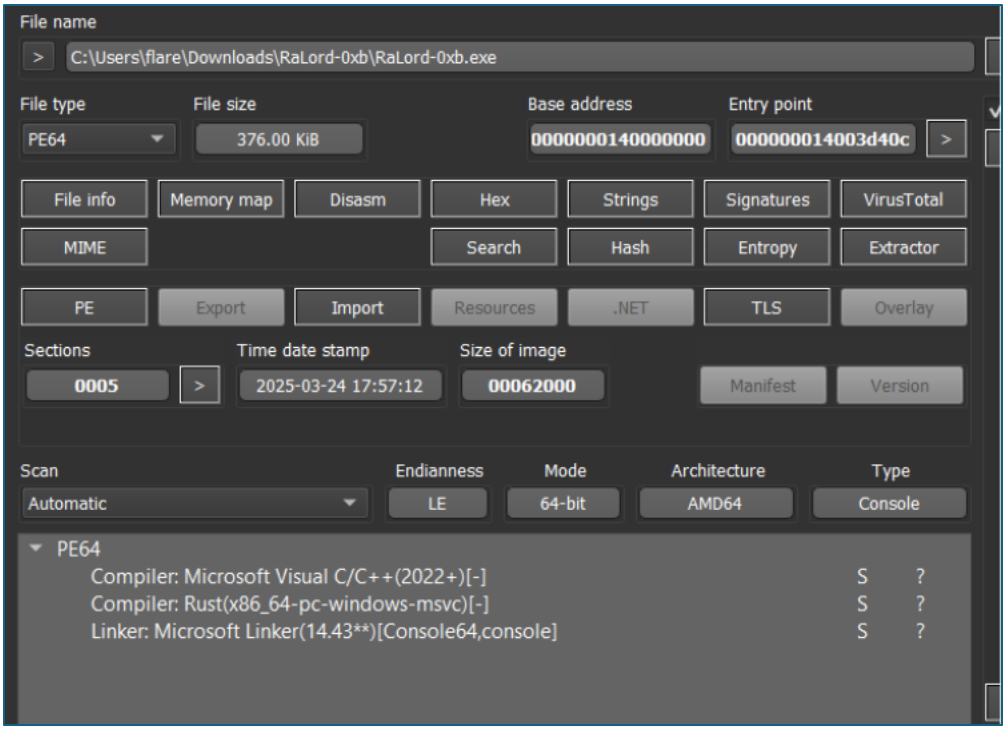

Figura 1. Gjuha e programimit RUST.

Nga analiza e strings evidentohet se ky skedar nis skanimin e direktorive të sistemit operativ dhe nis enkriptimin e tyre, kjo në bazë të të drejtave që ky skedar ekzekutohet.

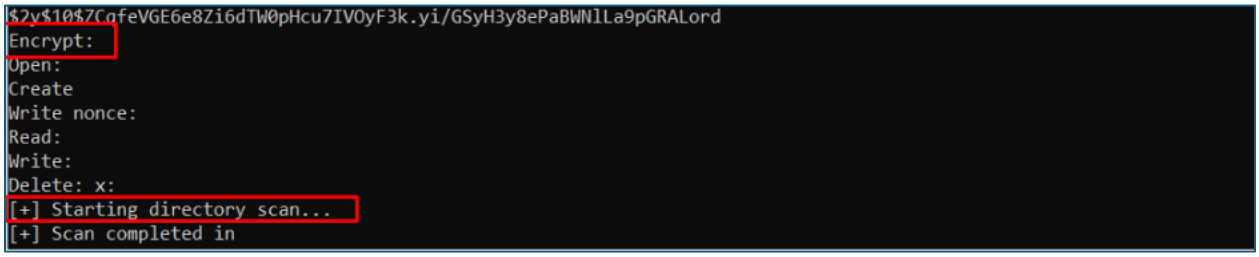

Figura 2. Strings të skedarit.

Evidentohet dhe në momentin që këtë skedar tentojm ta ekzekutojmë nëpërmjet **CMD** dhe çfarë ndodh është pikërisht skanimi(***enumeration***) i direktorive dhe më pas nis procesi i enkriptimit.

```
C:\Users\flare\Downloads\RaLord-0xb>RaLord-0xb.exe
[+] Starting directory scan...
[!] Retry 1/3: C:\Users\flare\Downloads\RaLord-0xb\RaLord-0xb.exe - Delete: Access is denied. (os error 5)
[!] Retry 2/3: C:\Users\flare\Downloads\RaLord-0xb\RaLord-0xb.exe - Delete: Access is denied. (os error 5)
[!] Retry 3/3: C:\Users\flare\Downloads\RaLord-0xb\RaLord-0xb.exe - Delete: Access is denied. (os error 5)
[!] Failed: C:\Users\flare\Downloads\RaLord-0xb\RaLord-0xb.exe - Delete: Access is denied. (os error 5)
[+] Scan completed in 7.07s
^C
FLARE-VM Mon 01/12/2026  8:48:46.15
```

Figura 3. Ekzekutim nga cmd.

Duke analizuar skedarin evidentojmë funksionin **FUN_140007e90** i cili ka rolin kryesor në thirrjen e kodit keqdashës. Kjo gjë evidentohet në pjesën e kodit ku pret parametrin **param_1**. Nga analiza statike vlera e **param_1** është pikërisht **param_1 = &LAB_140006230**. Pra për të parë kodin, duhet të kontrollojmë një ***label*** me vlerën **LAB_140006230.**

```
void FUN_140007e90(undefined *param_1)

{
  (*(code *)param_1)();
  return;
}
```

Figura 4. Thirrja e kodit.

Në emërtimin e përmendur, duket pjesa e kodit të skedarit keqdashës nga ku evidentohet dhe **ransom-note** hardcoded në skedar. Po në këtë funksion evidentohen dhe **strings** të përmendur më lart:

"[+] Starting directory scan..."
"[+] Scan completed in ..."
"[!] Error creating README: ..."
Funksioni i cili bën enkriptimin nis me funksionin **FUN_14000c8e0.**

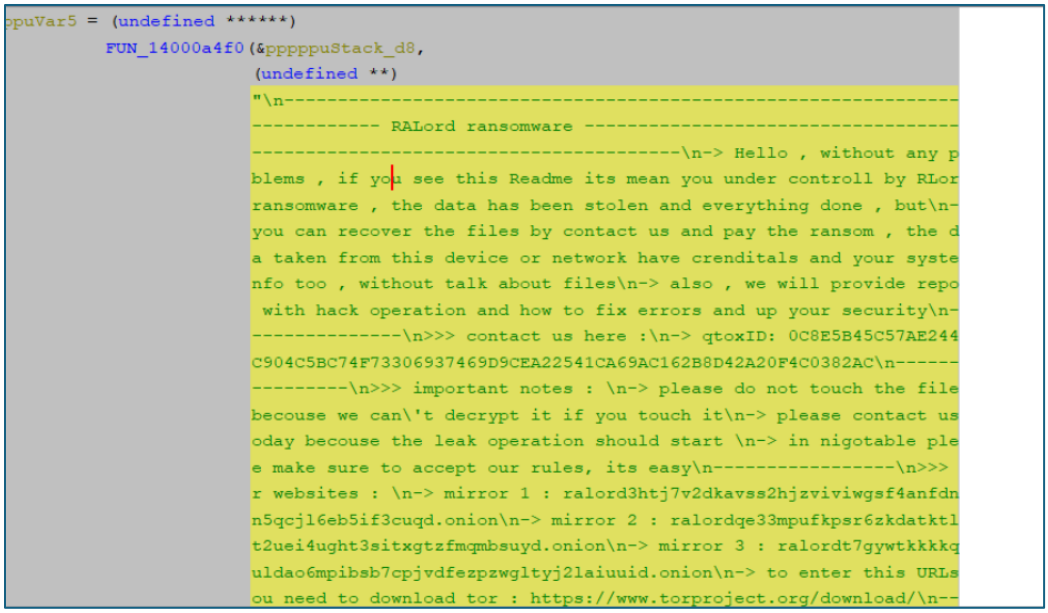

Figura 5. Ransomware note i skedarit.

FUN_14000c8e0 është pika ku nis përpunimi real i një skedari. Por algoritmi i enkriptimit vetë nuk është i shkruar direkt në këtë pjesë kodi. Kopjon të dhënat e skedarit në një buffer privat gjë e cila evidentohet si më poshtë. Më pas përgatit **metadata** / **nonce** / **IV** (përgatit header kriptografik ose strukturë ndihmëse për enkriptim).

_Src = *(void **)(param_2 + 0x18);
sVar1 = *(size_t *)(param_2 + 0x20);

```
  local_30 = 0xfffffffffffffffe;
  _Src = *(void **)(param_2 + 0x18);
  sVar1 = *(size_t *)(param_2 + 0x20);
  local_128 = 0;
  local_118 = 0x8000000000000000;
  uStack_100 = uStack_100 & 0xffffffffffffff00;
  local_48 = param_2;
  if ((longlong)sVar1 < 0) {
    lVar5 = 0;
LAB_14000caec:
    local_32 = 1;
    FUN_140041323(lVar5,sVar1,&PTR_s_C:\Users\scorp\.rustup\toolchain_140044a88);
                    /* WARNING: Does not return */
```

Figura 6. Kopjimi i të dhënave të skedarit në buffer.

Funksion shumë i rëndësishëm është funksioni **FUN_14002cd60**. Këtu krijon një **thread** të ri dhe i jep atij një funksion për t'u ekzekutuar. **LAB_14002cf00** është **entry-point** i thread dhe aty nis zinxhiri ku do nisi dhe enkriptimi.

```
undefined8 FUN_14002cd60(SIZE_T param_1,undefined8 param_2,undefined8 param_3)

{
  LPVOID pvVar1;
  undefined8 *puVar2;
  code *pcVar3;
  undefined8 *lpParameter;
  HANDLE pvVar4;
  undefined8 uVar5;

  lpParameter = (undefined8 *)thunk_FUN_140029330(0x10,8);
  if (lpParameter != (undefined8 *)0x0) {
    *lpParameter = param_2;
    lpParameter[1] = param_3;
    uVar5 = 0;
    pvVar4 = CreateThread((LPSECURITY_ATTRIBUTES)0x0,param_1,(LPTHREAD_START_ROUTINE)&LAB_14002c...
    0,
                          lpParameter,0x10000,(LPDWORD)0x0);
    if (pvVar4 == (HANDLE)0x0) {
      pvVar1 = (LPVOID)*lpParameter;
```

Figura 7. Krijimi i thread.

Në këtë fazë ndiqen funksionet njëri pas tjetrit në mënyrë që të arrijm në funksionin final ku shfaqet dhe algoritmi i përdorur për enkriptim.

```
undefined8 UndefinedFunction_14002cf00(undefined8 *param_1)

{
  LPVOID pvVar1;
  ULONG UStack_24;
  longlong lStack_20;
  undefined8 uStack_18;

  uStack_18 = 0xfffffffffffffffe;
  UStack_24 = 0x5000;
  SetThreadStackGuarantee(&UStack_24);
  pvVar1 = (LPVOID)*param_1;
  lStack_20 = param_1[1];
  (**(code **)(lStack_20 + 0x18))();
  if (*(longlong *)(lStack_20 + 8) != 0) {
    thunk_FUN_140029390(pvVar1,*(longlong *)(lStack_20 + 8),*(ulonglong *)(lStack_20 + 0x10));
  }
  thunk_FUN_140029390(param_1,0x10,8);
  return 0;
}
```

Figura 8. Thirrja e kodit kryesor.

Duke kërkuar adresën e saktë evidentohet parametri e **lStack_20** dhe duke bërë një llogaritje *qword* në **PTR_FUN_140045848 + 0x18 = 0x140011790; 0x0000000140011790** është adresa e saktë gjë e cila paraqitet dhe me foton më poshtë.

Figura 9. Adresa e përllogaritur.

Duke ndjekur funksionet hap pas hapi, funksioni ku ndodh enkriptimi është funksioni **FUN_140004760**.

- Hap file-in (Read / Open)
- Krijon buffer 0x100000 (1 MB):
- **local_140 = malloc(0x100000);**
- **Loop kryesor (file processing loop).**

Konkretisht në këtë pjesë kodi funksioni **FUN_140013dd0** thërret funksionin më kryesor **FUN_14001b630** ku është e gjithë llogjika e enkriptimit.

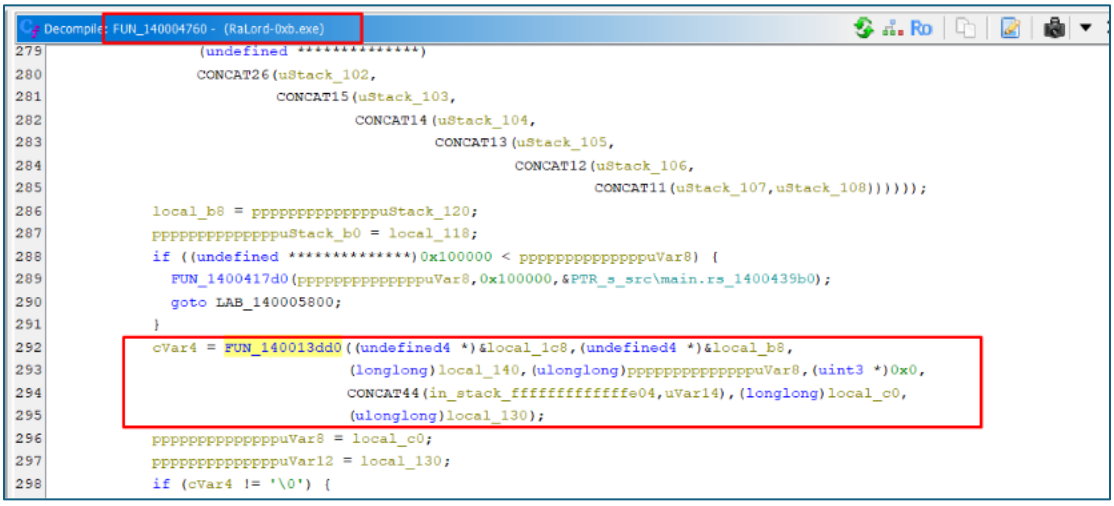

Figura 10. Thirrja e funksionit enkriptues.

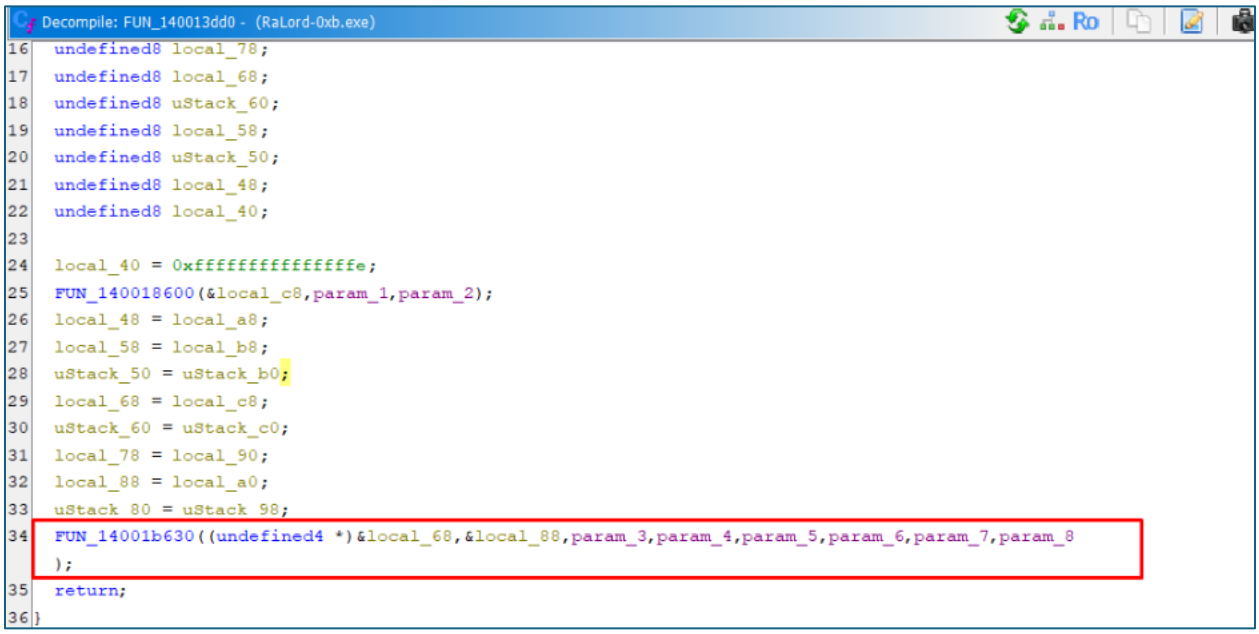

Figura 11. Funksioni me kryesor ku ndodh enkriptimi në të vërtetë.

Nëse analizojmë funksionin më kryesor **FUN_14001b630** ku kemi enkriptimin e skedarëve kupojmë se kemi të bëjmë me **ChaCha20** për enkriptim + **Poly1305** për autentikim **(MAC).**

- Blloqe **64 byte (0x40)** e cila është tipike e **ChaCha20**

if (local_148 < 0x40) { ... }
local_148 = local_148 - 0x40;
lVar20 = local_140 + 0x40;
lVar24 = lVar24 + 0x40;

- **XOR keystream me plaintext**

***_Dst = *_Dst ^ *puVar1;**
_Dst[1] = _Dst[1] ^ uVar25;

- **Counter rritet për çdo bllok**

FUN_140017000(local_128, iVar29, (uint *)&local_188, 0x40);
iVar29 = block counter

- Gjeneron keystream për çdo block

ChaCha20 counter-based keystream

- **Poly1305 MAC në fund (16 byte TAG)**

if (param_8 < param_4 + 0x10) return error;
FUN_140018e30((longlong)local_d8, ..., 0x10);

- **+0x10 = 16 byte tag**
- **Kontroll autentikimi**

Poly1305 = 16-byte MAC

Indikatorët e Komprometimit

456B9ADAABAE9F3DCE2207AA71410987F0A571CD8C11F2E7B41468501A863606	**RaLord-0xb.exe**
794807D348783FDA909C94D28458A7325D2C57644DF17289729BC8158BB4B3AA	**RaLord-0xb.zip**
a9f701ff27899e33e6948a9d63b02d58e53d95ff54dfdf70f4ce0a5b4faaf9ef	**README-XeBY311RpMRQ.txt**

Rekomandime

Autoriteti Kombëtar për Sigurinë Kibernetike rekomandon:

- Bllokimin e menjëhershëm të Indikatorëve të Kompromentimit, të përmendura më sipër në pajisjet tuaja mbrojtëse.
- Analizimin e vazhdueshëm të logeve që vijnë nga SIEM (Security information and Event Management).
- Trajnimin e stafit jo-teknik rreth sulmeve "Phishing" si dhe mënyrat e shmangies së infektimit prej tyre.
- Instalimin e pajisjeve të perimetrit të rrjetit që bëjnë analizë të thellë të trafikut duke u mbështetur jo vetëm në rregullat e listave të aksesit por edhe në sjelljen e tij (Firewall-et NextGen).
- Sistemet e evidentuara të segmentohen në VLAN-e të ndryshme, duke aplikuar "Access control list për të gjithë perimetrin e rrjetit", webserviset duhet të jenë të ndarë nga Databaza e tyre, Active Directory duhet të jetë në një VLAN të ndarë.
- Aplikimin dhe përdorimin e teknikës LAPS për sistemet Microsoft, për menagjimin e fjalëkalimeve të Administratorëve Lokal.
- Të aplikohen filtra të trafikut në rastin e aksesimit në distancë të hosteve (punonjësve/palë të treta/klientë).
- Të implementohen zgjidhje që kryen filtrimin, monitorimin dhe bllokimin e trafikut keqdashës ndërmjet aplikacioneve Web dhe internetit, Web Application Firewall (WAF).
- Të kryhen analiza të trafikut në nivel sjellje "behaviour" për pajisjet fundore, aplikimi i zgjidhjeve EDR, XDR. Kjo sjell analizën e skedarëve keqdashës jo vetëm në nivel signature por dhe në nivel behaviour.
- Të projektohet zgjidhja për menaxhimin e aksesit të përdoruesve "Identity Access Management" për të kontrolluar identitetin dhe privilegjet e përdoruesve në kohë reale sipas parimit "zero-trust".