



RELATÓRIO DE PESQUISAS

RALord:

Novo grupo de Ransomware-as-a-Service

Acesse a nossa nova comunidade através do WhatsApp!

Heimdall Security Research



Acesse boletins diários sobre agentes de ameaças, *malwares*, indicadores de comprometimentos, TTPs e outras informações no *site* da ISH.

Boletins de Segurança – Heimdall

 Malware	 Malware	 Ransomware
ISH CONTAS DO FACEBOOK SÃO INVADIDAS POR EXTENSÕES MALICIOSAS DE NAVEGADORES Descoberto recentemente que atores maliciosos utilizam extensões de navegadores para realizar o roubo de cookies de sessões de sites como o Facebook. A extensão maliciosa é oferecida como um anexo do ChatGPT...	ISH ALERTA PARA RETORNO DO MALWARE EMOTET! O malware Emotet após permanecer alguns meses sem operações retornou com outro meio de propagação, via OneNote e também dos métodos já conhecidos via Planilhas e Documentos do Microsoft Office...	ISH GRUPO DE RANSOMWARE CLOP EXPLORANDO VULNERABILIDADE PARA NOVAS VÍTIMAS O grupo de Ransomware conhecido como ClOp está explorando ativamente a vulnerabilidade conhecida como CVE-2023-0669, na qual realizou o ataque a diversas organizações e expôs os dados no site de data leaks...
BAIXAR	BAIXAR	BAIXAR

SUMÁRIO

1	Sumário executivo	6
2	Estratégico	6
2.1	Introdução sobre a nova ameaça	6
2.2	Segmento de mercado e Países afetados	6
3	Tático	8
3.1	Operação da ameaça	8
3.2	Atividades e recrutamento de afiliados	8
3.3	Modelo de negócio - RALord	15
4	Análise das capacidades do RALord ransomware	16
4.1	Identificação de Linguagem Utilizada e Strings em Texto Puro	17
4.2	Engenharia reversa do RALord Ransomware	18
4.2.1	Diretório alvo da criptografia	18
4.2.2	Processo de configuração customizado de criptografia	19
4.2.3	Lista de extensões de arquivos a serem criptografados	23
4.2.4	Direcionamento de vítimas ou Bugs?	24
5	Atribuição e similaridades	26
6	MITRE ATT&CK – TTPs	27
7	Recomendações	28
8	Conclusão de pesquisa	30
9	Operacional	31
9.1.1	Engenharia de Detecção	31
10	Malware Behavior Catalog (MBC)	32
11	Indicadores de Comprometimento	33
12	Referências	34
13	Autores	34

LISTA DE TABELAS

Tabela 1 - Extensões de arquivos para criptografar.	23
Tabela 2 - Amostras do Funksec que deram match com a assinatura criada por nossa equipe.	26
Tabela 3 – Tabela MITRE ATT&CK.	27
Tabela 4 – Tabela Malware Behavior Catalog.	32
Tabela 5 - Indicadores de Comprometimento do RALord Ransomware.....	33
Tabela 6 - Data Leak Site Principal do RALord.	33
Tabela 7 - Backup I do Data Leak Site.	33
Tabela 8 - Backup II do Data Leak Site.	33
Tabela 9 - Método de comunicação com operadores do RALord.....	33

LISTA DE FIGURAS

<i>Figura 1 – Segmentos afetados pelo RALord Ransomware.</i>	<i>6</i>
<i>Figura 2 – Países afetados pelo RALord Ransomware.</i>	<i>7</i>
<i>Figura 3 – Atividades do RALord desde seu surgimento.</i>	<i>8</i>
<i>Figura 4 – Leak Site do RALord.</i>	<i>9</i>
<i>Figura 5 – Exemplo de vazamento no Leak Site do RALord.</i>	<i>10</i>
<i>Figura 6 – Discurso de identidade do RALord.</i>	<i>11</i>
<i>Figura 7 - Guia de como se afiliar ao RALord.</i>	<i>12</i>
<i>Figura 8 - Métodos de contato com o grupo.</i>	<i>13</i>
<i>Figura 9 - Guia de compra de criptomoedas.</i>	<i>14</i>
<i>Figura 10 - Continuação do guia de compra de criptomoedas.</i>	<i>14</i>
<i>Figura 11 - Modelo de execução de campanha do RALord.</i>	<i>15</i>
<i>Figura 12 - Fluxo geral de execução do RALord.</i>	<i>16</i>
<i>Figura 13 - Identificação de tamanho e de linguagem de programação.</i>	<i>17</i>
<i>Figura 14 - Identificação de Strings em texto puro e de usuário de desenvolvimento.</i>	<i>18</i>
<i>Figura 15 - Identifica diretório atual do prompt.</i>	<i>18</i>
<i>Figura 16 - Identificação de arquivos do sistema.</i>	<i>18</i>
<i>Figura 17 - Chave inicial aleatória de 24-byte.</i>	<i>19</i>
<i>Figura 18 - Coleta de Hash BCrypt e conteúdo do README para Key Wrapping.</i>	<i>20</i>
<i>Figura 19 - Chacha20 Quarter Round.</i>	<i>21</i>
<i>Figura 20 - ChaCha20 RFC Quarter Round.</i>	<i>22</i>
<i>Figura 21 - Lista de extensões.</i>	<i>23</i>
<i>Figura 22 - Importação de APIs do VCRUNTIME140.dll.</i>	<i>24</i>
<i>Figura 23 - Crash de execução por conta da dependência do VCRUNTIME140.dll.</i>	<i>24</i>
<i>Figura 24 - Criptografia da própria Nota de Ransomware.</i>	<i>25</i>
<i>Figura 25 - Match de padrão de código com amostras do Funksec Ransomware.</i>	<i>26</i>

1 SUMÁRIO EXECUTIVO

Este relatório de segurança, desenvolvido pela equipe de inteligência do **Purple Team da ISH Tecnologia**, tem como objetivo proporcionar uma compreensão aprofundada e um dimensionamento preciso das ameaças cibernéticas identificadas. O documento está estruturado em três níveis de abordagem: **Estratégico**, **Tático** e **Operacional**, garantindo uma visão completa e integrada das ameaças e ações recomendadas.

2 ESTRATÉGICO

2.1 INTRODUÇÃO SOBRE A NOVA AMEAÇA

O cenário de ransomware manteve-se ativo em 2024 e se estendeu para este ano de 2025, com diversos grupos realizando ataques a uma ampla gama de organizações, setores e com surgimento de novos grupos. Nesse contexto, um dos mais recentes temos o **RALord**. Pensando em trazer informações relevante sobre esta nova ameaça o time **CTI-Purple Team da ISH tecnologia** realizou uma análise detalhada do mesmo, as quais serão descritas logo abaixo.

2.2 SEGMENTO DE MERCADO E PAÍSES AFETADOS

Os segmentos de mercado e países potencialmente afetados por essa ameaça até o momento, incluem:

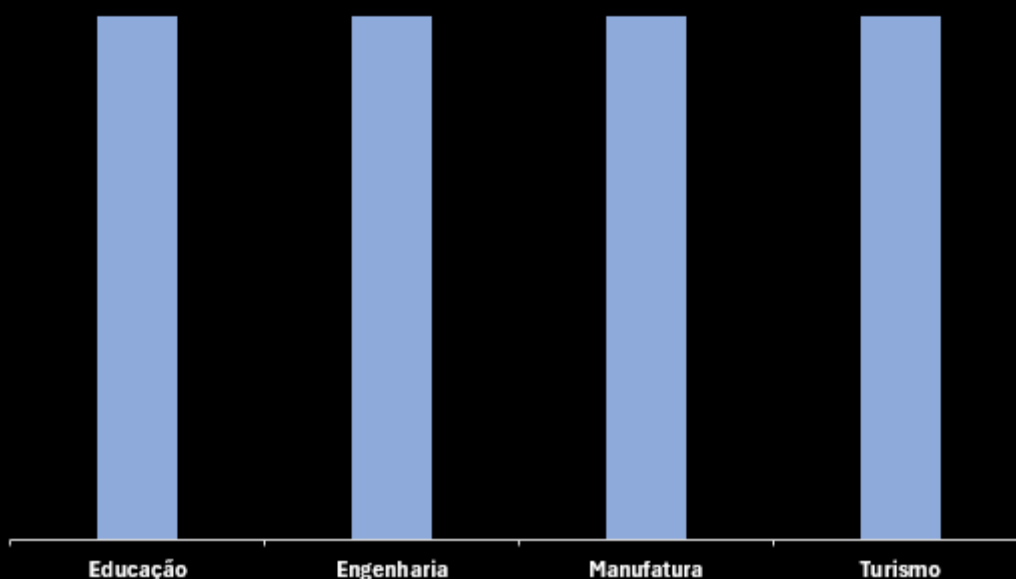


Figura 1 – Segmentos afetados pelo RALord Ransomware.

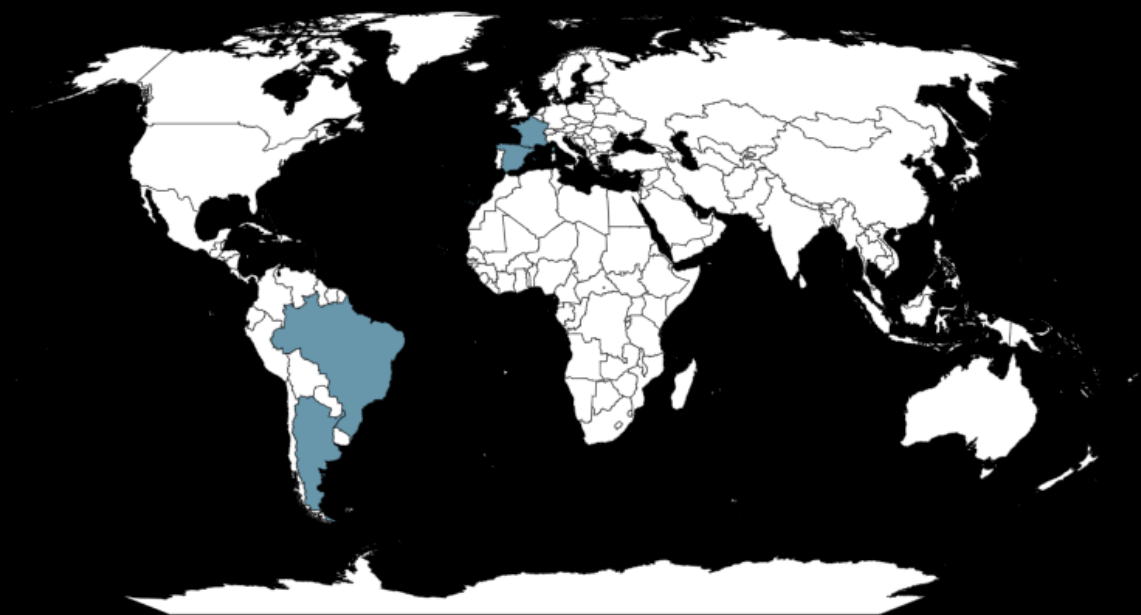


Figura 2 – Países afetados pelo RALord Ransomware.

O grupo emergiu recentemente, com seus primeiros incidentes reportados impactando os setores de Educação, Engenharia, Manufatura e Turismo, em países como França, Argentina e Brasil, entre outros. Uma característica distintiva é a abordagem mais "amigável" adotada em seu Data Leak Site (DLS), onde os setores das vítimas são explicitamente destacados — uma possível estratégia para aumentar a pressão sobre organizações semelhantes e ampliar o impacto da ameaça.

Essa tática de exposição setorial está alinhada com práticas comuns entre grupos Ransomware-as-a-Service (RaaS), no contexto da dupla extorsão. As vítimas iniciais evidenciam não apenas a diversidade de setores-alvo, mas também a abrangência geográfica do grupo, com foco particular em países da **América Latina**. Embora ainda não seja possível determinar se a concentração de vítimas na LATAM é intencional ou apenas coincidente, o cenário serve como um importante alerta para a região no que diz respeito à evolução da ameaça.

3 TÁTICO

3.1 OPERAÇÃO DA AMEAÇA

Abaixo é possível observar que as atividades do **RALord** foram de fato iniciadas ano em (*Março de 2025*), o que nos permite realizar um acompanhamento em tempo real, com o objetivo de identificar as tendências e as evoluções do grupo desde seu nascimento.

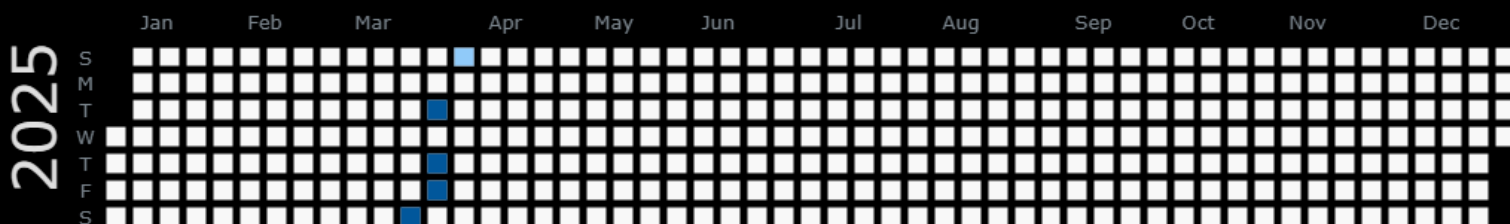


Figura 3 – Atividades do RALord desde seu surgimento.

Os vetores de ataque priorizados pelo RALord incluem o direcionamento a produtos de segurança de rede como *Fortinet*, *SonicWall* e *Cisco*, possivelmente com a exploração de vulnerabilidades via Brute-Force e *exploits* de CVEs. Essa estratégia indica uma busca por meio de acessos iniciais comuns em infraestruturas corporativas, visando obter acesso inicial através de falhas de segurança em dispositivos perimetrais, serviços de autenticação e aplicações web vulneráveis. A infraestrutura online do **RALord** inclui *Data Leak Sites* acessíveis via domínios **TOR**, como é comum para todos os grupos de RaaS. O nome de usuário do administrador do grupo, "**ForLord**", o que é relevante para o rastreamento de suas atividades em diferentes plataformas e para a identificação de possíveis conexões com outros atores ou grupos.

3.2 ATIVIDADES E RECRUTAMENTO DE AFILIADOS

A atividade de recrutamento do grupo RALord foi identificada a partir de 19 de março de 2025, em fóruns comumente utilizado por atores maliciosos. Um requisito técnico para afiliados é a capacidade de codificar o *encryptor* utilizando **Python** e **Rust**, indicando uma preferência por linguagens que oferecem versatilidade (*Python*) e potencial para otimização de performance e evasão (*Rust*). Essa exigência sugere um grupo com um certo nível de sofisticação técnica ou a ambição de desenvolver ferramentas robustas e multiplataforma. Um ponto intrigante é a possível ligação do RALord com o grupo RA World, por conta da semelhança do nome, e porque recentemente o RA World encerrou suas atividades. O RA World utilizava o serviço *Go File Storage* para hospedar amostras de malware, e uma amostra do RA World apresentou uma correspondência de código de **25%** com o ransomware **FunkSec**, que também se encontra offline. Essa correlação sugere uma possível reutilização de código, compartilhamento de

recursos ou até mesmo uma reestruturação de grupos, onde indivíduos ou partes de um grupo anterior ressurgem sob uma nova identidade.

Como descrito no próprio *DLS* o **RALord** segue o modelo já consolidado de **RaaS**, uma abordagem permite que afiliados possam utilizar-se de sua infraestrutura e malwares. Abaixo, podemos observar o **Data Leak Site** do RALord, no qual expõe as vítimas infectadas durante suas operações, e onde é efetivado o ato de dupla extorsão.

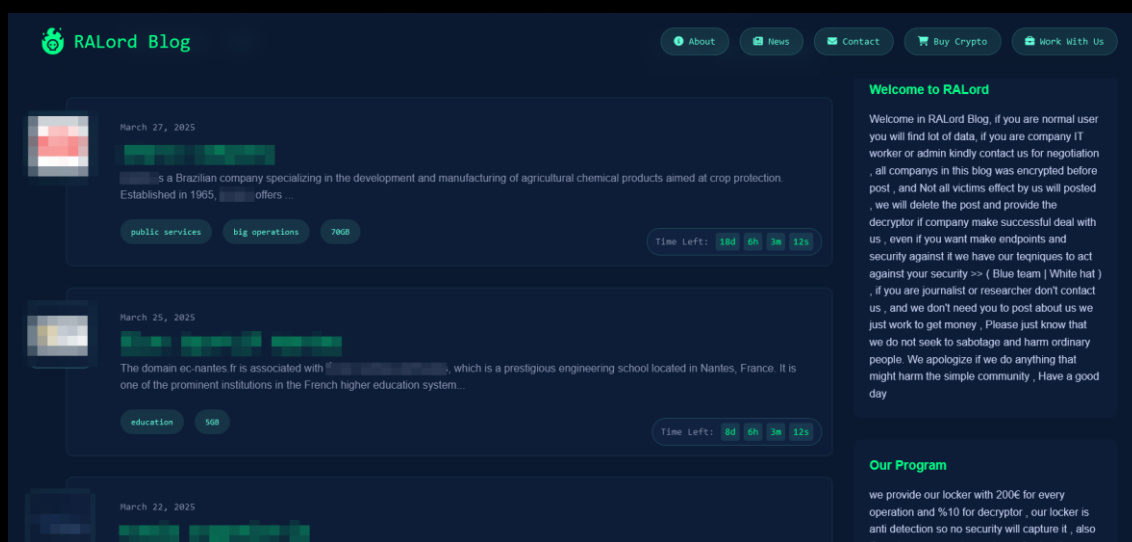
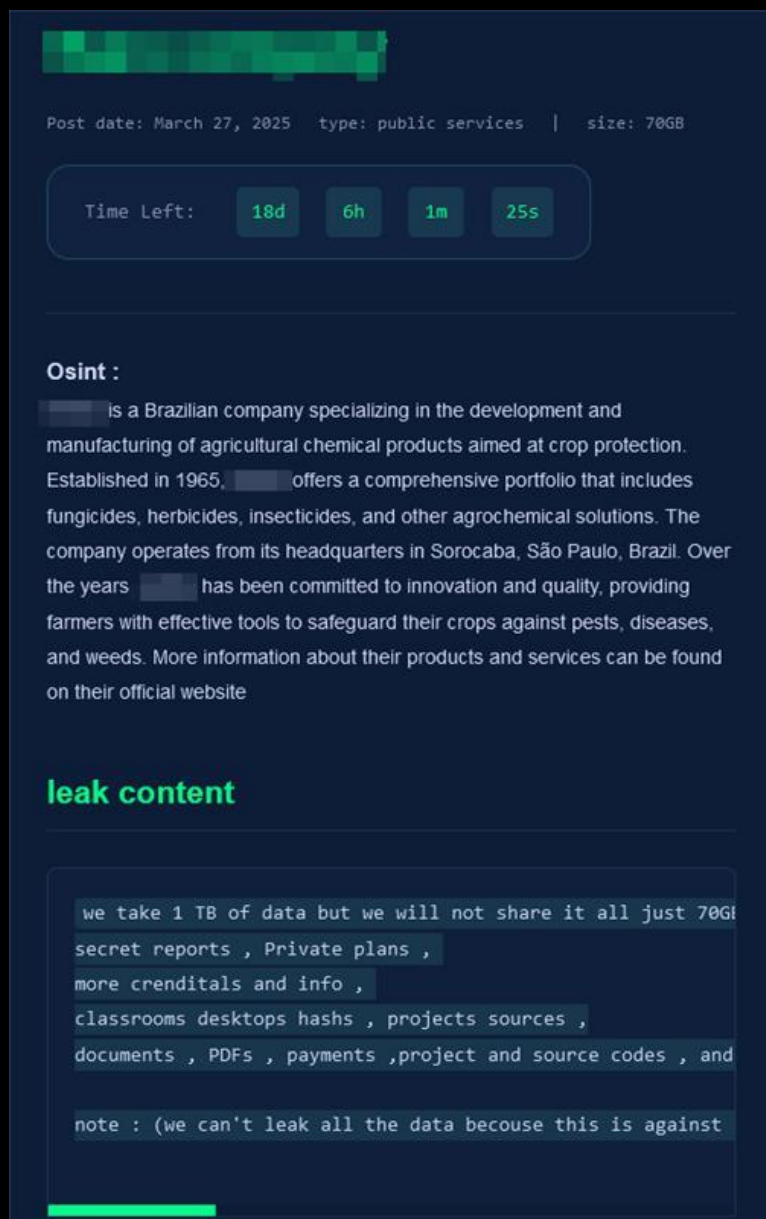


Figura 4 – Leak Site do RALord.

No *DLS* contém um contador regressivo de tempo, que aplica uma sensação de urgência para as vítimas, indicando que o grupo não contém apenas os dados já vazados, mas na verdade, contém muito mais que poderá ser integralmente publicado se a vítima não efetuar o pagamento.



The screenshot shows a dark-themed web interface. At the top, there is a blurred header area. Below it, a status bar displays "Post date: March 27, 2025", "type: public services", and "size: 70GB". A prominent countdown timer is centered, showing "Time Left:" followed by four buttons: "18d", "6h", "1m", and "25s". Below the timer, a section titled "Osint :" contains a paragraph of text about a Brazilian agricultural chemical company. Further down, a section titled "leak content" in red text is followed by a text box containing a list of leaked data types: "we take 1 TB of data but we will not share it all just 70GB", "secret reports , Private plans ,", "more credentials and info ,", "classrooms desktops hashes , projects sources ,", "documents , PDFs , payments ,project and source codes , and", and a note: "note : (we can't leak all the data because this is against".

Post date: March 27, 2025 type: public services | size: 70GB

Time Left: 18d 6h 1m 25s

Osint :

██████████ is a Brazilian company specializing in the development and manufacturing of agricultural chemical products aimed at crop protection. Established in 1965, ██████████ offers a comprehensive portfolio that includes fungicides, herbicides, insecticides, and other agrochemical solutions. The company operates from its headquarters in Sorocaba, São Paulo, Brazil. Over the years ██████████ has been committed to innovation and quality, providing farmers with effective tools to safeguard their crops against pests, diseases, and weeds. More information about their products and services can be found on their official website

leak content

we take 1 TB of data but we will not share it all just 70GB
secret reports , Private plans ,
more credentials and info ,
classrooms desktops hashes , projects sources ,
documents , PDFs , payments ,project and source codes , and
note : (we can't leak all the data because this is against

Figura 5 – Exemplo de vazamento no Leak Site do RALord.

Apesar dos crimes cometidos pelo grupo **RALord** e seus afiliados, o grupo se autodenomina como **Bug Bounties** (escreveram erroneamente ‘*BugBountys*’, o que pode indicar que inglês de fato não é sua língua materna), e apesar da péssima habilidade em escrita, o grupo define uma posição ofensiva em relação à *Pesquisadores e Jornalistas*, além de atacar fabricantes de *Softwares de Proteção a Endpoints*, informando que eles não podem ajudar suas vítimas. Em seu discurso, eles também informam que não são novos no mercado de *RaaS*, o que nos permite afirmar a suposta ligação deste novo grupo, com os citados anteriormente.

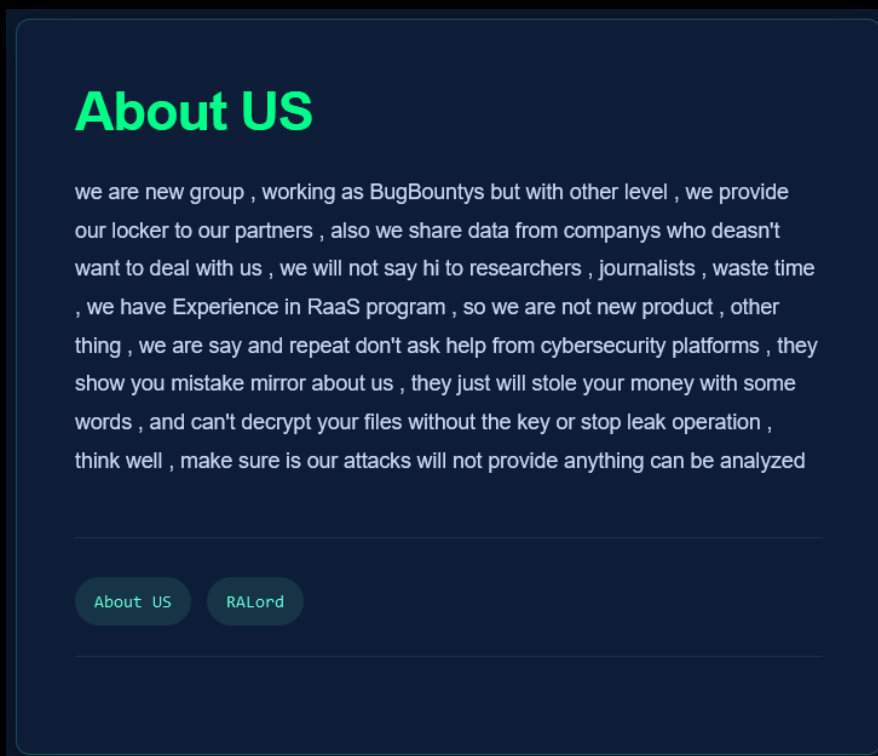


Figura 6 – Discurso de identidade do RALord.

No DLS também há um guia de como se afiliar ao grupo, de como a operação será conduzida, e de como o dinheiro será dividido. É interessante notar, que o **RALord** é quem trás para si a responsabilidade de efetuar o ataque a partir do momento em que o *Afiliado* tem acesso à rede interna da vítima em potencial.



how to work with us ?

our RaaS rules:

- 1 the data you will extract will be posted in our BLOG and we are who will encrypt
- 2 we will take 15% from decryption deal
- 3 our program is target the advanced peoples in cybersecurity

providers and partners types :

- 1 access providers for our personal use
- 2 Data buyers
- 3 Ads in other Onion platforms

the price of service and operation Requirements:

- 1 the price is 200€ for every encrypt operation , decryptor cost 10% from deal
- 1 Make sure you have access to desktop systems or ESXI with admin or user (IT , workers, accountant etc)
- 2 the attack will be from our side , mean we are who will enter and do the operation for you
- 3 if you want post data in our Blog you need to add another 20€

Work with us RALord

Figura 7 - Guia de como se afiliar ao RALord.

Também possível observar os métodos de contatos, que são do mesmo padrão através de chat **qTOX**.

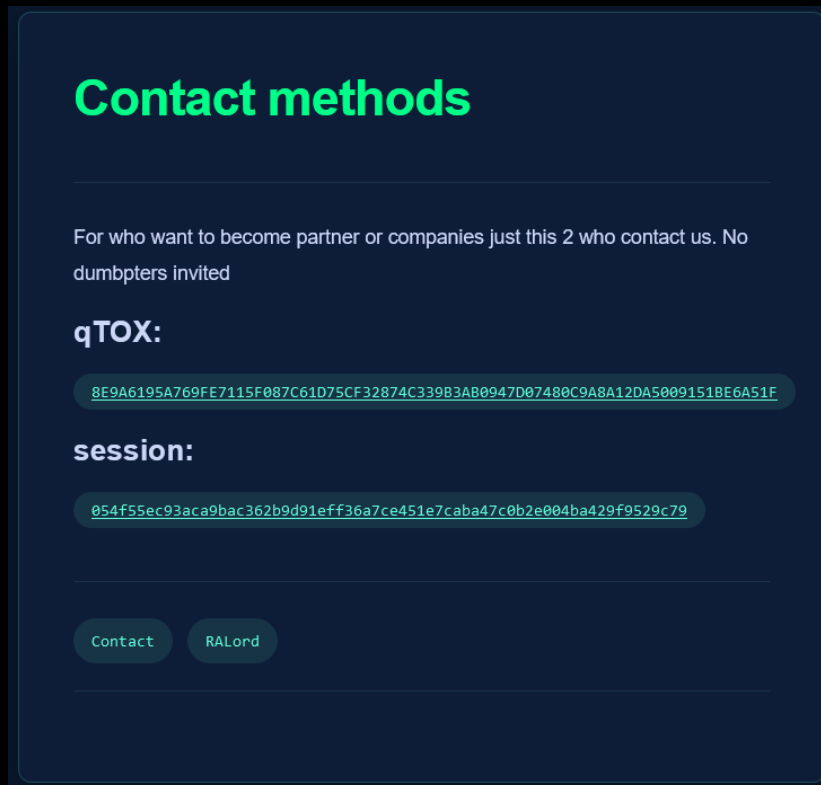


Figura 8 - Métodos de contato com o grupo.

No *DLS* do **RALord**, também há uma seção de [Guia de Compras de Criptomoedas](#).

Secure Cryptocurrency Purchasing Guide

Step-by-Step Guide to Acquiring Cryptocurrency:

- 1 Select a reputable exchange platform (recommended below)
- 2 Complete KYC verification for higher limits
- 3 Enable 2FA security on your account

Verified Exchange Platforms:

Binance	Supported: BTC, ETH, XMR
Kraken	Supported: BTC, LTC, ZEC
LocalMonero	Anonymous Options
coinbase	Supported: BTC, ETH, XMR
Blockchain	Supported: BTC, ETH, XMR

Figura 9 - Guia de compra de criptomoedas.

Accepted Payment Methods:

Cryptocurrency

BTC, XMR, LTC
Min: 0.01 BTC
Confirmation: 3 blocks

Bank Transfer

SEPA/Wire Transfer
1-3 Business Days
Fee: 1.5%

Escrow Service

Secure Transactions
2/3 Multisig
0.5% Service Fee

[buy crypto lessons](#) [RALord](#)

Figura 10 - Continuação do guia de compra de criptomoedas.

3.3 MODELO DE NEGÓCIO - RALORD

Como na seção anterior, o modelo *RaaS* é mantido pelo **RALord**, mas com uma ênfase no fato de quem irá conduzir a implantação do Ransomware nos sistemas das vítimas, sendo os próprios operadores do **Grupo RALord**.

Isso nos permite supor que o grupo de fato está interessado em que a campanha seja executada da forma correta, e que os afiliados não tenham o controle sobre as amostras do *Ransomware* e de outras possíveis *toolkits*. Apesar de ser uma tática interessante, isso nos permitirá (se de fato este planejamento prosseguir) observar uma *Kill Chain* sólida dos operadores ao decorrer que os incidentes forem acontecendo.



Figura 11 - Modelo de execução de campanha do RALord.

4 ANÁLISE DAS CAPACIDADES DO RALORD RANSOMWARE

Nesta seção iremos nos aprofundar nas principais características do RALord ransomware, o que e como ele implementa determinada capacidade, com o objetivo de obter inteligência deste novo ransomware, a fim de que possamos ter uma rastreabilidade de sua evolução, ao longo do tempo. Abaixo, podemos observar o seu fluxo macro da execução.

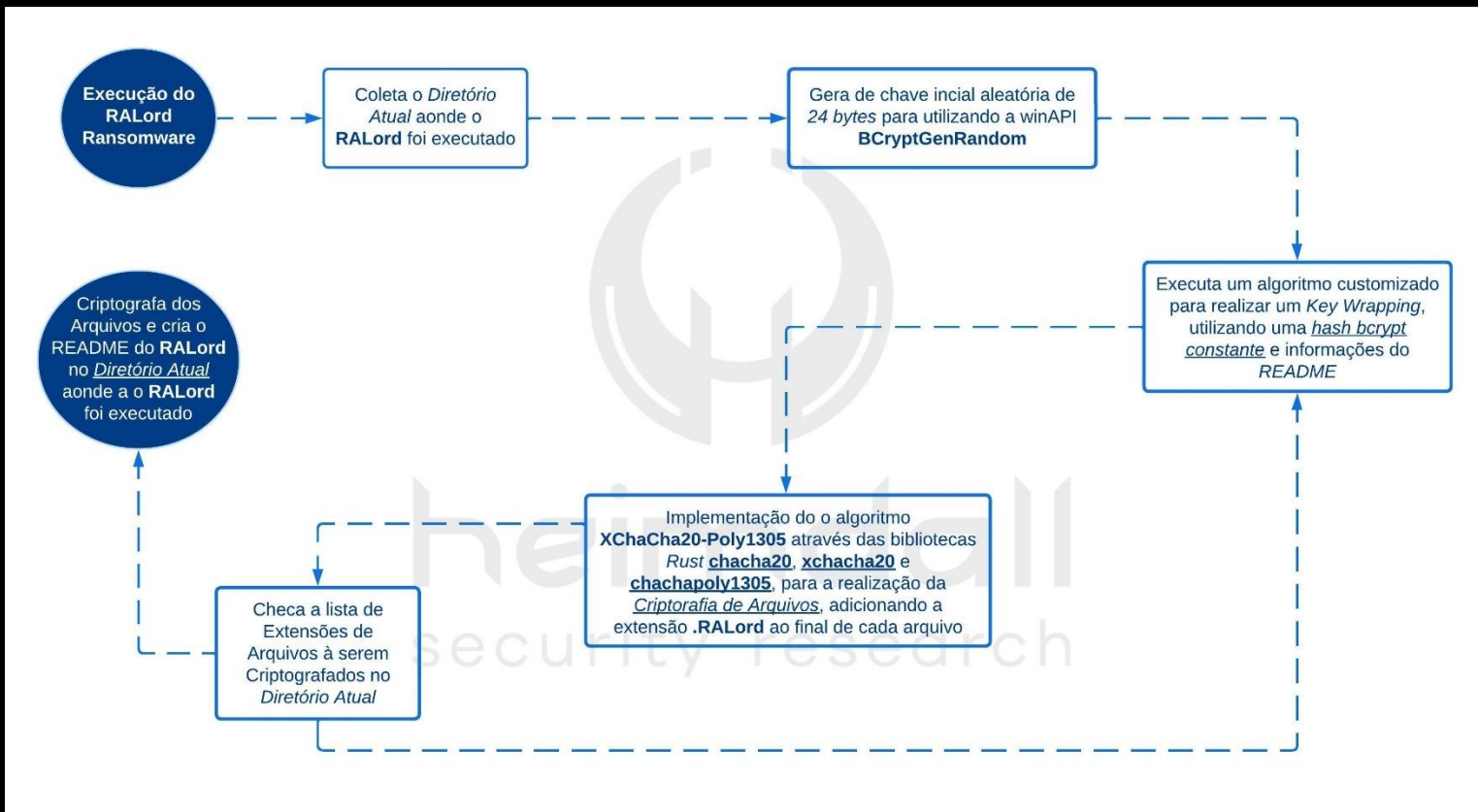


Figura 12 - Fluxo geral de execução do RALord.

4.1 IDENTIFICAÇÃO DE LINGUAGEM UTILIZADA E STRINGS EM TEXTO PURO

Nos últimos anos, tem havido um aumento notável na criação de *malware* utilizando linguagens de programação modernas como **Rust**, *Golang* e *Nim*. Dentre estas, o *Rust* tem ganhado particular atenção por parte de desenvolvedores de *ransomware* devido à dificuldade adicional que impõe à engenharia reversa, pelo fato da maioria dos malwares serem desenvolvidos em **C/C++** ou **.NET**.

Como já citado neste relatório, este é o caso do novo ransomware **RALord**, que é desenvolvido em **Rust**, como é possível observar pelo grande tamanho do binário na imagem abaixo.

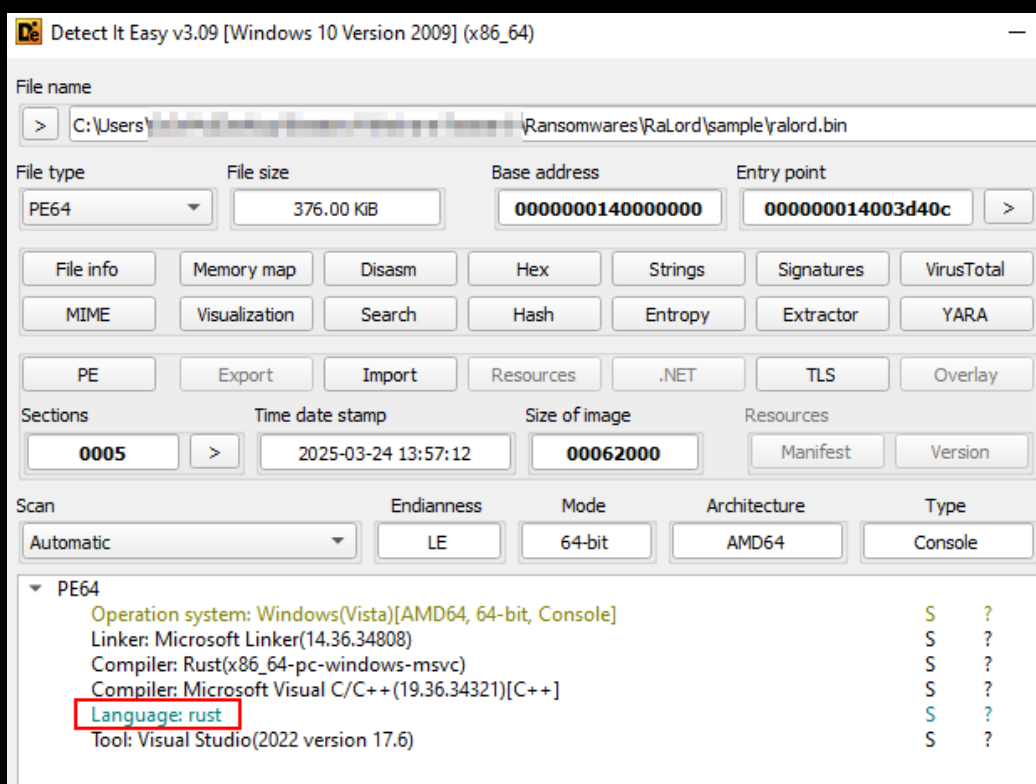


Figura 13 - Identificação de tamanho e de linguagem de programação.

Durante nossa análise não foi identificado qualquer tentativa de ofuscar as strings do RALord ransomware, o que nos permite identificar facilmente a nota de ransomware, e o 'nome do usuário' que desenvolveu esta amostra.

```
PS C:\Users\scorp\Desktop\Research\Malware Research\Ransomwares\RALord\sample> strings.exe -n 100 .\ralord.bin
C:\Users\scorp\.rustup\toolchains\stable-x86_64-pc-windows-msvc\lib\rustlib\src\rust\library\core\src\iter\traits\iterator.rs
C:\Users\scorp\.cargo\registry\src\index.crates.io-6f17d22bba15001f\rayon-core-1.12.1\src\registry.rs
called `Result::unwrap()` on an `Err` value: C:\Users\scorp\.cargo\registry\src\index.crates.io-6f17d22bba15001f\rayon-core-1.12.1\src\latch.rs
C:\Users\scorp\.rustup\toolchains\stable-x86_64-pc-windows-msvc\lib\rustlib\src\rust\library\std\src\path.rs
C:\Users\scorp\.rustup\toolchains\stable-x86_64-pc-windows-msvc\lib\rustlib\src\rust\library\alloc\src\slice.rs
----- RALord ransomware -----
-> Hello , without any problems , if you see this Readme its mean you under controll by RALord ransomware , the data has
been stolen and everything done , but
-> you can recover the files by contact us and pay the ransom , the data taken from this device or network have credita
ls and your systeminfo too , without talk about files
----- RALord ransomware -----
C:\Users\scorp\.cargo\registry\src\index.crates.io-6f17d22bba15001f\rayon-core-1.12.1\src\high_level\hltimes.rs
```

Figura 14 - Identificação de Strings em texto puro e de usuário de desenvolvimento.

4.2 ENGENHARIA REVERSA DO RALORD RANSOMWARE

Apesar do **RALord** não implementar nenhuma capacidade além da criptografia dos arquivos e escrita do arquivo **README** no sistema, identificamos métodos customizados no processo de criptografia, além de um comportamento não comum e possíveis alvos (ou simplesmente um *bug*).

4.2.1 Diretório alvo da criptografia

Diferentemente dos demais ransomwares, o **RALord** não criptografa todo o disco raiz por padrão, em contrapartida, criptografa de maneira recursiva apenas o diretório no qual o operador se encontra no momento da execução do ransomware. Portanto, se o prompt de comando do operador, estiver no *Desktop* do usuário atual, o **RALord** irá criptografar de maneira recursiva o diretório de *Desktop*.

Essa capacidade é implementada através da implementação de uma função que coleta o caminho completo do diretório atual.

```
ptr_CurrentDirectory = GetCurrentDirectoryW((DWORD)uVar6,lpBuffer);
if ((ptr_CurrentDirectory == 0) && (error_return = GetLastError(), error_return != 0)) {
```

Figura 15 - Identifica diretório atual do prompt.

Após coletar o diretório atual, o ransomware passa a coletar o nome de cada arquivo existente no diretório retornado anteriormente.

```
ralord_get_file_fullpath(&local_b8,&lpFindFileData,\"x01\");
memset(&lpFindFileData,0,0x250);
file_handler = FindFirstFileExW(fullpath_filename,FindExInfoBasic,&lpFindFileData,FindExSearchNameMatch,(LPVOID)0x0,0);
```

Figura 16 - Identificação de arquivos do sistema.

4.2.2 Processo de configuração customizado de criptografia

Diferentemente de outros ransomwares que utilizam *winAPIs* em todo o processo de criptografia, ou, que utilizam uma combinação de *winAPIs* em conjunto com uma implementação manual de um algoritmo de criptografia conhecido, o RALord ransomware emprega o seguinte esquema híbrido robusto:

- Geração de uma chave simétrica forte aleatoriamente, utilizando a *winAPI* **BCryptGenRandom**.
- Proteção dessa chave usando um algoritmo customizado, que recebe como entrada uma constante diferente para cada campanha (através de uma constante *hash bcrypt*), provavelmente com o objetivo de implementar um *key wrapping*.
- Por fim implementa o algoritmo **XChaCha20-Poly1305** para criptografar os arquivos, garantindo *nonces* únicos para cada um.

Abaixo, podemos observar a primeira fase do processo de criptografia, que é a geração da chave inicial, na qual será aplicado o *key wrapping* para proteger a chave.

```
ralord_bcrypt_key_gen(PUCHAR pbBuffer,ulonglong cbBuffer)

{
    BOOLEAN BVar1;
    NTSTATUS ntstatus;
    ulonglong ptr_cbBuffer;

    if (cbBuffer != 0) {
        do {
            ptr_cbBuffer = 0xffffffff;
            if (cbBuffer < 0xffffffff) {
                ptr_cbBuffer = cbBuffer;
            }
            ntstatus = BCryptGenRandom((BCRYPT_ALG_HANDLE)0x0,pbBuffer,(ULONG)ptr_cbBuffer,BCRYPT_USE_SYSTEM_PREFERRED_RNG);
            if ((0xbfffffff < (uint)ntstatus) && (BVar1 = SystemFunction036(pbBuffer,(ULONG)ptr_cbBuffer), BVar1 == '\0')) {
                return ntstatus & 0x7fffffff;
            }
            pbBuffer = pbBuffer + ptr_cbBuffer;
            cbBuffer = cbBuffer - ptr_cbBuffer;
        } while (cbBuffer != 0);
    }
    return 0;
}
```

Figura 17 - Chave inicial aleatória de 24-byte.

Em sequência, o ransomware implementa uma função que recebe uma hash bcrypt, provavelmente única para cada campanha do RALord, em união com determinado conteúdo parcial do **README**, para a execução do *Key Wrapping*, através de um algoritmo customizado.

```
memalloc_memcpy((size_t *)&buffer,"$2y$10$ZCqfeVGE6e8Zi6dTW0pHcu7IV0yF3k.yi/GSyH3y8ePaBWNlLa9pG",0x3c);
uStack_d0 = CONCAT44(uStack_10c,uStack_110);
local_d8 = local_118;
bcrypt_hash_const = (undefined *****)buffer;
pppppppppppppuStack_e0 = ppppppppppppppuStack_120;
memalloc_memcpy((size_t *)&buffer,partial_readme_content,0x18);
uStack_150 = CONCAT44(uStack_10c,uStack_110);
local_158 = local_118;
key_wrapping_output = buffer;
pppppppppppppuStack_160 = ppppppppppppppuStack_120;
uVar14 = 0x20;
ralord_wrapping_key_alg((ulonglong *)&buffer,(longlong)&bcrypt_hash_const,(longlong)&key_wrapping_output,0xf,0x400,0x20);
```

Figura 18 - Coleta de Hash BCrypt e conteúdo do README para Key Wrapping.

Este algoritmo recebe como argumento o ponteiro da constante **hash bcrypt** identificada como:

\$2y\$10\$ZCqfeVGE6e8Zi6dTW0pHcu7IV0yF3k.yi/GSyH3y8e PaBWNlLa9pG, que é utilizada juntamente com o conteúdo parcial do **README** no processo de *Key Wrapping* da chave assimétrica aleatória criada anteriormente, para a campanha referente a esta amostra, através de um algoritmo customizado. Abaixo podemos observar, o fluxo do código de execução do *key wrapping*.

Após a configuração do processo de criptografia, o ransomware de fato implementa o algoritmo **XChaCha20-Poly1305**, através da importação de bibliotecas do Rust identificadas facilmente através do *Disassembler*, ou por ferramentas simples como **strings.exe**, pelo fato das *strings* estarem em texto puro.

Porém, um dos indicadores que adiciona precisão adicional à detecção das *strings* em texto puro, é a identificação da implementação da função de geração dos **Blocos Keystream**, que contém a implementação do **Quarter Round Rotate Left de 32-bits (ROTL32)** que contém as constantes características desta fase de configuração do **ChaCha20**, que são:

- Primeiro round implementando um **ROTL32** de 16;
- Segundo round implementando um **ROTL32** de 12;
- Terceiro round implementando um **ROTL32** de 8;
- Quarto round implementando um **ROTL32** de 7.

Abaixo podemos observar esta implementação no código do **RALord**.

```
/* Implementação da Quarter Round do ChaCha20

    ROTL32 */
uVar25 = uVar20 << 16 | uVar20 >> 0x10;
uVar20 = uVar17 << 16 | uVar17 >> 0x10;
uVar28 = uVar27 << 16 | uVar27 >> 0x10;
uVar30 = uVar29 << 16 | uVar29 >> 0x10;
uVar26 = uVar26 + uVar25;
uVar23 = uVar23 + uVar20;
uVar15 = uVar15 + uVar28;
uVar19 = uVar19 + uVar30;
uVar14 = uVar14 ^ uVar26;
uVar16 = uVar16 ^ uVar23;
uVar11 = uVar11 ^ uVar15;
uVar24 = uVar24 ^ uVar19;

/* ROTL32 */
uVar27 = uVar14 << 12 | uVar14 >> 0x14;
uVar16 = uVar16 << 12 | uVar16 >> 0x14;
uVar14 = uVar11 << 12 | uVar11 >> 0x14;
uVar17 = uVar24 << 12 | uVar24 >> 0x14;
uVar13 = uVar13 + uVar27;
uVar21 = uVar21 + uVar16;
uVar22 = uVar22 + uVar14;
uVar31 = uVar31 + uVar17;
uVar25 = uVar25 ^ uVar13;
uVar20 = uVar20 ^ uVar21;
uVar28 = uVar28 ^ uVar22;
uVar30 = uVar30 ^ uVar31;

/* ROTL32 */
uVar25 = uVar25 << 8 | uVar25 >> 0x18;
uVar29 = uVar20 << 8 | uVar20 >> 0x18;
uVar11 = uVar28 << 8 | uVar28 >> 0x18;
uVar28 = uVar30 << 8 | uVar30 >> 0x18;
uVar26 = uVar26 + uVar25;
uVar23 = uVar23 + uVar29;
uVar15 = uVar15 + uVar11;
uVar19 = uVar19 + uVar28;
uVar27 = uVar27 ^ uVar26;
uVar16 = uVar16 ^ uVar23;
uVar14 = uVar14 ^ uVar15;
uVar17 = uVar17 ^ uVar19;

/* ROTL32 */
uVar20 = uVar27 << 7 | uVar27 >> 0x19;
uVar24 = uVar16 << 7 | uVar16 >> 0x19;
uVar30 = uVar14 << 7 | uVar14 >> 0x19;
uVar14 = uVar17 << 7 | uVar17 >> 0x19;
```

Figura 19 - Chacha20 Quarter Round.

Logo mais, podemos observar a [RFC do ChaCha20](#), que nos permite estabelecer uma precisão em nossa afirmação, referente ao uso deste algoritmo de criptografia. Através da identificação da geração dos **Blocos de Keystream** através de um **Quarter Round**.

The elements in this vector or matrix are 32-bit unsigned integers.

The algorithm name is "ChaCha". "ChaCha20" is a specific instance where 20 "rounds" (or 80 quarter rounds -- see [Section 2.1](#)) are used. Other variations are defined, with 8 or 12 rounds, but in this document we only describe the 20-round ChaCha, so the names "ChaCha" and "ChaCha20" will be used interchangeably.

2. The Algorithms

The subsections below describe the algorithms used and the AEAD construction.

2.1. The ChaCha Quarter Round

The basic operation of the ChaCha algorithm is the quarter round. It operates on four 32-bit unsigned integers, denoted *a*, *b*, *c*, and *d*. The operation is as follows (in C-like notation):

1. *a* += *b*; *d* ^= *a*; *d* <<= 16;
2. *c* += *d*; *b* ^= *c*; *b* <<= 12;
3. *a* += *b*; *d* ^= *a*; *d* <<= 8;
4. *c* += *d*; *b* ^= *c*; *b* <<= 7;

Figura 20 - ChaCha20 RFC Quarter Round.

Esta correlação entre o código encontrado no RALord e a *RFC*, nos permite dar uma maior precisão a informação de que este ransomware utiliza o algoritmo **ChaCha20** para a criptografia de arquivos.

4.2.3 Lista de extensões de arquivos a serem criptografados

O RALord implementa uma lista [hardcoded](#) de extensões de arquivos a serem criptografados, conforme podemos observar de maneira parcial, na imagem abaixo.

```

file_extensions_to_encrypt_140042fa8

140042fa8 74 78 74      file_ext...
        63 73 76
        64 6f 63 ...
140042fa8 74 78 74      char[3]    "txt"

140042fab 63 73 76      char[3]    "csv"
140042fae 64 6f 63 78    char[4]    "docx"
140042fb2 78 6c 73 78    char[4]    "xlsx"
140042fb6 70 64 66      char[3]    "pdf"
140042fb9 6a 73 6f 6e    char[4]    "json"
140042fbd 78 6d 6c      char[3]    "xml"
140042fc0 73 71 6c      char[3]    "sql"
140042fc3 6c 6f 67      char[3]    "log"
140042fc6 68 74 6d 6c    char[4]    "html"
140042fca 63 73 73      char[3]    "css"
140042fcd 6a 73 70      char[3]    "jsp"
140042fd0 68 70        char[2]    "hp"
140042fd2 70 79        char[2]    "py"
140042fd4 6a 61 76 61    char[4]    "java"
140042fd8 63 63 70      char[3]    "ccp"
140042fdb 70 73 68      char[3]    "psh"
140042fde 62 61 74      char[3]    "bat"
140042fel 69 6e 69      char[3]    "ini"
140042fe4 79 61 6d 6c    char[4]    "yaml"
140042fe8 6d 64        char[2]    "md"
140042fea 72 74 66      char[3]    "rtf"

```

Figura 21 - Lista de extensões.

Abaixo, podemos observar todas as extensões que serão criptografadas durante a execução do ransomware.

Extensões de Arquivos para Criptografar

txt, csv, docx, xlsx, pdf, json, xml, sql, log, html, css, js, php, py, java, c, cpp, sh, bat, ini, yaml, md, rtf, ts, jsx, tsx, pptx, odt, ods, odp, msg, eml, apk, ipa, exe, dll, dmg, iso, vmdk, vhd, tgz, 7z, zip, tar, rar, bak, db, mdb, sqlite, hdf5, parquet, avro, etl, pfx, cer, pem, csr, key, pgp, kdbx, gpg, tar.gz, xz, dbf, tiff, raw, ai, psd, indd, eps, svg, dwg, dxf, fla, flv, mov, mp4, avi, mkv, mp3, wav, flac, aac, ogg, wma, webm, m3u, cue, midi, ps, tex, bib, chm, epub, azw3, fb2, djvu, opf, xps, jar, war, ear, pdb, msi, deb, rpm, vcs, git, svn, nfs, bin, bkp, lst, dat, png

Tabela 1 - Extensões de arquivos para criptografar.

4.2.4 Direcionamento de vítimas ou Bugs?

Durante a análise foi identificada algumas características, que implicam na necessidade de um ambiente específico. Me refiro a presença de importações de APIs da DLL **VCRUNTIME140.DLL**, que causam crash na execução do ransomware, caso o sistema da vítima não tenha os pacotes necessários do Microsoft Visual C++ Redistributable, que normalmente está instalado em ambientes que contém um ambiente de desenvolvimento, ou que contém softwares legados que necessitam destas bibliotecas para o seu bom funcionamento.

```

LAB_14000470d                                XREF[1]: 1400046fb(j)
14000470d 4a 3b 3c 33    CMP     RDI,qword ptr [RBX + R14*0x1]=>DAT_140043120    = 0000000000000003h
140004711 75 ed        JNZ     LAB_140004700
140004713 4a 8b 4c      MOV     param_1=>file_extensions_to_encrypt_140042fa8,... = 140042fa8
33 f8
140004718 48 89 f2      MOV     param_2,RSI
14000471b 49 89 f8      MOV     R8,RDI
14000471e e8 55 96      CALL    VCRUNTIME140.DLL::memcmp                                     int memcmp(void * _Buf1, void * ...
  
```

Dependência que causa erro em sua execução, caso não exista a biblioteca VCRUNTIME140.dll

Figura 22 - Importação de APIs do VCRUNTIME140.dll.

Ao tentar executar o RALord em um dispositivo **Windows 10** padrão, a sua execução apresentou um *crash*, informando que não foi possível encontrar no sistema o **VCRUNTIME140.DLL**.

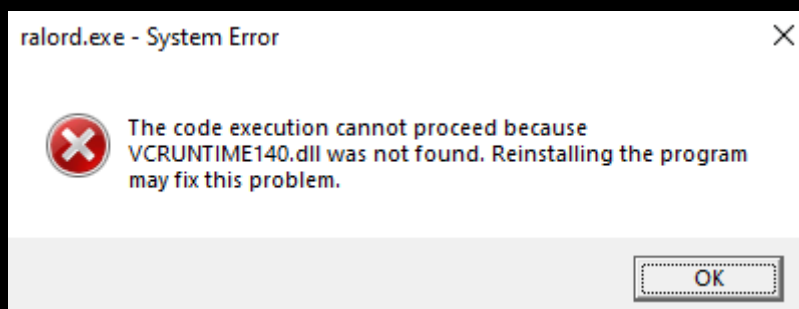
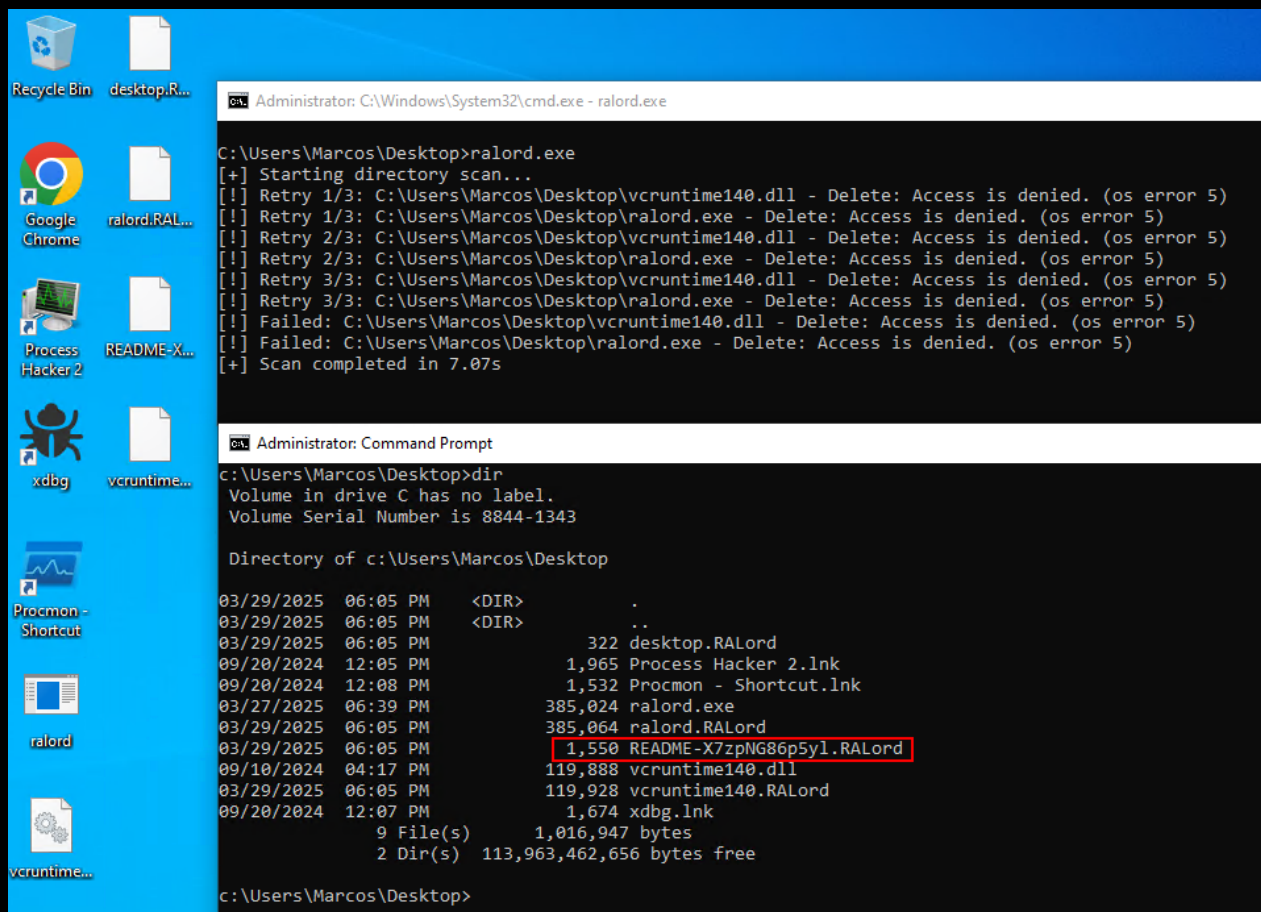


Figura 23 - Crash de execução por conta da dependência do VCRUNTIME140.dll.

Esta dependência pode ser facilmente resolvida, através de uma simples configuração no IDE do *Visual Studio*. Isso pode nos indicar o direcionamento para o tipo de vítima que o RALord direciona suas campanhas, ou, uma desatenção durante a compilação do ransomware.

Outro *bug* interessante, é a presença da extensão txt na lista de extensões de arquivos a serem criptografados, causando a criptografia da própria Nota de Ransomware. Apesar da extensão dos arquivos criptografados deixarem claro por qual ransomware o seu sistema foi infectado, se o objetivo era deixar a **Nota de Ransomware** não acessível à vítima, bastava não criar ela no sistema. Isso nos dá mais certeza, de que foi mais uma desatenção durante o processo de desenvolvimento do ransomware.



```
Administrator: C:\Windows\System32\cmd.exe - ralord.exe

C:\Users\Marcos\Desktop>ralord.exe
[+] Starting directory scan...
[!] Retry 1/3: C:\Users\Marcos\Desktop\vcruntime140.dll - Delete: Access is denied. (os error 5)
[!] Retry 1/3: C:\Users\Marcos\Desktop\ralord.exe - Delete: Access is denied. (os error 5)
[!] Retry 2/3: C:\Users\Marcos\Desktop\vcruntime140.dll - Delete: Access is denied. (os error 5)
[!] Retry 2/3: C:\Users\Marcos\Desktop\ralord.exe - Delete: Access is denied. (os error 5)
[!] Retry 3/3: C:\Users\Marcos\Desktop\vcruntime140.dll - Delete: Access is denied. (os error 5)
[!] Retry 3/3: C:\Users\Marcos\Desktop\ralord.exe - Delete: Access is denied. (os error 5)
[!] Failed: C:\Users\Marcos\Desktop\vcruntime140.dll - Delete: Access is denied. (os error 5)
[!] Failed: C:\Users\Marcos\Desktop\ralord.exe - Delete: Access is denied. (os error 5)
[+] Scan completed in 7.07s

Administrator: Command Prompt

C:\Users\Marcos\Desktop>dir
Volume in drive C has no label.
Volume Serial Number is 8844-1343

Directory of c:\Users\Marcos\Desktop

03/29/2025  06:05 PM    <DIR>          .
03/29/2025  06:05 PM    <DIR>          ..
03/29/2025  06:05 PM                322 desktop.RALord
09/20/2024  12:05 PM            1,965 Process Hacker 2.lnk
09/20/2024  12:08 PM            1,532 Procmon - Shortcut.lnk
03/27/2025  06:39 PM           385,024 ralord.exe
03/29/2025  06:05 PM           385,064 ralord.RALord
03/29/2025  06:05 PM           1,550 README-X7zpNG86p5y1.RALord
09/10/2024  04:17 PM           119,888 vcruntime140.dll
03/29/2025  06:05 PM           119,928 vcruntime140.RALord
09/20/2024  12:07 PM            1,674 xdbg.lnk
          9 File(s)        1,016,947 bytes
          2 Dir(s)      113,963,462,656 bytes free

C:\Users\Marcos\Desktop>
```

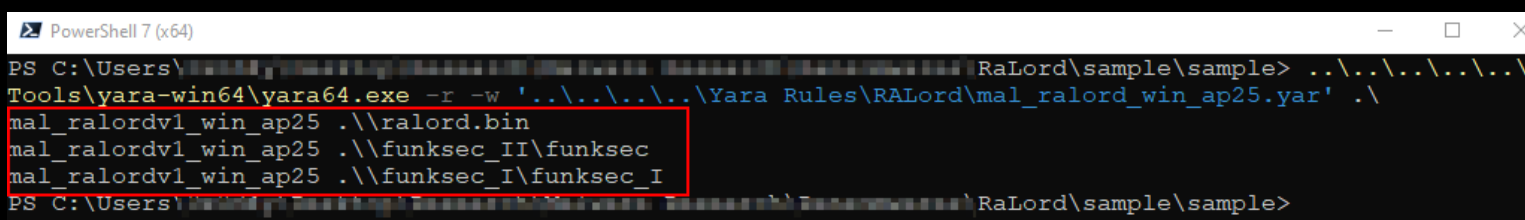
Figura 24 - Criptografia da própria Nota de Ransomware.

5 ATRIBUIÇÃO E SIMILARIDADES

Durante o processo de validação da regra de detecção produzida com a inteligência coletada através desta pesquisa, fomos capazes de identificar que os padrões de código do RALord em conjunto com determinadas strings, deram match com amostras recentes do Funksec. São eles:

- Padrão de Código do Algoritmo de **Key Wrapping**;
- Padrão de Código do Algoritmo de **Quarter Round** do ChaCha20;
- *Strings* referentes à linguagem de programação **Rust**;
- E etc.

Abaixo, podemos observar o match com duas amostras coletadas.



```

PS C:\Users\...RaLord\sample\sample> ..\..\..\..\..\Tools\yara-win64\yara64.exe -r -w '..\..\..\..\..\Yara Rules\RALord\mal_ralord_win_ap25.yar' .\mal_ralordv1_win_ap25 .\\ralord.bin
mal_ralordv1_win_ap25 .\\funksec_II\\funksec
mal_ralordv1_win_ap25 .\\funksec_I\\funksec_I
PS C:\Users\...RaLord\sample\sample>
  
```

Figura 25 - Match de padrão de código com amostras do Funksec Ransomware.

E a seguir podemos observar uma lista de amostras das últimas **12 semanas**, que deram match com os padrões descritos na regra Yara.

Hashes de artefatos similares ao RALord	
Funksec	c233aec7917cf34294c19dd60ff79a6e0fac5ed6f0cb57af98013c08201a7a1c
Funksec	89b9f7499d59d0d308f5ad02cd6fddd55b368190c37f6c5413c4cfd343eeff3
Funksec	e622f3b743c7fc0a011b07a2e656aa2b5e50a4876721bcf1f405d582ca4cda22
Funksec	00acf5d0db7ef50140dae7a3482d9db80704ec98670bd1607e76c99382a4888c
Funksec	dd15ce869aa79884753e3baad19b0437075202be86268b84f3ec2303e1ecd966
Funksec	20ed21bfdb7aa970b12e7368eba8e26a711752f1cc5416b6fd6629d0e2a44e5d
Funksec	dcf536edd67a98868759f4e72bcbd1f4404c70048a2a3257e77d8af06cb036ac
Funksec	5226ea8e0f516565ba825a1bbed10020982c16414750237068b602c5b4ac6abd

Tabela 2 - Amostras do Funksec que deram match com a assinatura criada por nossa equipe.

Isto nos permite compreender, que os grupos **Funksec** e **RALord** implementaram as mesmas capacidades de criptografia, além da escolha do **Rust** como linguagem de desenvolvimento do Ransomware, o que nos permite supor uma certa colaboração entre os grupos, principalmente porque o Rust não é uma linguagem muito comum no desenvolvimento de malware.

6 MITRE ATT&CK – TTPs

Este tópico apresenta as Táticas, Técnicas e Procedimentos (TTPs) identificados nesta ameaça, conforme o framework **MITRE ATT&CK**, oferecendo uma visão tática detalhada sobre o comportamento do adversário. O objetivo é permitir o mapeamento das técnicas utilizadas pelos atacantes, facilitando a implementação de contramedidas eficazes e o aprimoramento das defesas de segurança.

Tática	Técnica	Detalhes
Discovery	T1083 File and Directory Discovery	O RALord Ransomware implementa um loop por meio de WinAPIs, que realiza o processo de coleta de cada arquivo de maneira recursiva no diretório atual, para realizar o processo de criptografia. O RALord coleta a informações, de qual é o diretório atual do prompt no qual foi executado, para que todas as funcionalidades do RALord sejam apenas aplicadas à aquele diretório.
Impact	T1486 Data Encrypted for Impact	O RALord Ransomware implementa o ChaCha20 como algoritmo, com o objetivo de criptografar todos os arquivos do sistema, a fim de solicitar um resgate, para a recuperação dos arquivos.

Tabela 3 – Tabela MITRE ATT&CK.

7 RECOMENDAÇÕES

Além dos indicadores de comprometimento elencados abaixo pela ISH, poderão ser adotadas medidas visando a mitigação da infecção do referido *malware*, como por exemplo:

Mantenha sistemas e softwares atualizados

- Garanta que todos os sistemas operacionais, aplicativos e softwares de segurança estejam atualizados com os patches mais recentes. Isso corrige vulnerabilidades que podem ser exploradas por atacantes.

Implemente soluções de segurança confiáveis

- Utilize ferramentas de segurança robustas, como antivírus e firewalls, para detectar e bloquear ameaças potenciais.

Realize backups regulares

- Mantenha backups atualizados e armazenados em locais seguros, preferencialmente offline ou em ambientes isolados, para garantir a recuperação de dados sem necessidade de pagar resgates.

Eduque e treine funcionários

- Promova treinamentos regulares sobre segurança cibernética para que os colaboradores reconheçam e evitem e-mails de phishing e outras tentativas de ataque.

Restrinja privilégios de acesso

- Adote o princípio do menor privilégio, garantindo que usuários tenham apenas as permissões necessárias para suas funções, limitando o potencial de movimentação lateral de atacantes na rede.

Monitore e analise atividades da rede

- Implemente ferramentas de monitoramento para identificar atividades suspeitas ou não autorizadas, permitindo respostas rápidas a possíveis incidentes.

Desenvolva um plano de resposta a incidentes

- Estabeleça e teste regularmente um plano de resposta a incidentes específico para ataques de ransomware, assegurando que sua equipe saiba como agir rapidamente para conter ameaças e restaurar operações.

Utilize autenticação Multifator (MFA)

- Implemente MFA para adicionar uma camada extra de segurança, dificultando o acesso não autorizado, mesmo que credenciais sejam comprometidas.

Desative serviços e protocolos não utilizados

- Reduza a superfície de ataque desativando serviços e protocolos desnecessários que podem ser explorados por cibercriminosos.

Realize avaliações de vulnerabilidades

- Conduza avaliações regulares para identificar e corrigir pontos fracos em sua infraestrutura de TI antes que sejam explorados.

8 CONCLUSÃO DE PESQUISA

Ao finalizarmos a análise desta primeira versão do **RALord**, nós fomos capazes de perceber que com o objetivo de otimizar tempo, o grupo escolheu uma linguagem de programação moderna e de alto nível, com o propósito de agilizar o início das operações. Isso se reflete em *bugs* no funcionamento do ransomware. O grupo se dedicou em implementar uma forma segura de criptografia, mas, com algumas falhas em sua execução, como no processo de criptografia de arquivos que resulta na criptografia da própria **Nota de Ransomware**.

Através da produção de inteligência, fomos capazes de identificar similaridades de código entre o **RALord** e o **Funksec** ransomware, o que nos permite fazer algumas suposições:

- Uma possível colaboração entre grupos, como já houve no passado.
- Reutilização de código entre um mesmo desenvolvedor com especialidade em **Rust**.
- Com o objetivo de otimizar o tempo para o início das operações do grupo, o **RALord** decidiu implementar as mesmas capacidades de criptografia do **Funksec**.

A equipe de pesquisa **Heimdall** da **ISH Tecnologia**, continuará monitorando a evolução deste grupo ao longo do tempo, com o objetivo de rastrear suas atividades e trazer visibilidade e poder de detecção para nossos clientes!

9 OPERACIONAL

9.1.1 Engenharia de Detecção

Tendo compreendido as principais capacidades do **RALord Ransomware**, fomos capazes de construir uma regra Yara, com o propósito de detectarmos a presença das amostras, e para monitorarmos a evolução do RALord Ransomware ao longo do tempo.

```
rule mal_ralordv1_win_ap25 {
    meta:
        description = "Detecta amostras da v1 do RALord Ransowmare."
        author = "Ícaro César"
        date = "2025-04-01"
        score = 100
        md5 = "BE15F62D14D1CBE2AECCE8396F4C6289"
        malpedia_family = "win.ralord"

    strings:
        $code_pattern_quarterround = { 4? 31 ?? 48 8b ?? ?? ?? 4?
31 ?? 48 8b ?? ?? ?? 31 e8 4? 31 ?? 41 c1 ?? 0c c1 ?? 0c c1 ?? 0c
48 89 c2 c1 ?? 0c }

        $code_pattern_custom_alg = { 0f 57 ?? 0f 10 ?? c5 ?? ?? ??
?? 0f 57 ?? 0f 10 ?? c5 ?? ?? ?? ?? 0f 57 ?? 0f 10 ?? c5 ?? ?? ??
?? 0f 57 ?? 0f 11 ?? c5 ?? ?? ?? ?? 0f 11 ?? c5 ?? ?? ?? ?? 0f 11
?? c5 ?? ?? ?? ?? 0f 11 ?? c5 ?? ?? ?? ?? 48 83 c0 08 48 3d 8? }

        $ralord_str_I = "chacha" wide ascii
        $ralord_str_II = "scorp" wide ascii
        $ralord_str_III = "RALord" wide ascii
        $ralord_str_IV = "onion" wide ascii
        $ralord_str_V = "/rust" wide ascii
        $ralord_str_VI = "BCryptGenRandom" wide ascii

    condition:
        uint16(0) == 0x5a4d and
        all of ($code_pattern_*) and
        4 of ($ralord_str_*)
}
```

10 MALWARE BEHAVIOR CATALOG (MBC)

Com o objetivo de documentar o comportamento evolutivo do RALord Ransomware, através do [Malware Behavior Catalog \(MBC\)](#), segue abaixo uma tabela de referência das técnicas identificadas durante nossa análise.

Tática	Técnica	Detalhes
Discovery	File and Directory Discovery	O RALord Ransomware implementa um loop por meio de WinAPIs, que realiza o processo de coleta de cada arquivo de maneira recursiva no no diretório atual, para realizar o processo de criptografia. O RALord coleta a informações, de qual é o diretório atual do <i>prompt</i> no qual foi executado, para que todas as funcionalidades do RALord sejam apenas aplicadas à aquele diretório.
File System	Create/Write/Delete File	Pela característica de Ransomware, o RALord implementa diversos loops, no qual ele cria as <i>Notas de Ransomware</i> , Criptografa os Arquivos, e altera a extensão para .RALord .
Process	Create Thread	Para que não a amostra fique ocupada com apenas uma atividade, o RALord implementa <i>Threads</i> que executam atividades de criptografia.
Impact	Data Encrypted for Impact	Por sua natureza, o RALord criptografa os dados para pedir resgate posteriormente.

Tabela 4 – Tabela Malware Behavior Catalog.

11 INDICADORES DE COMPROMETIMENTO

A ISH Tecnologia realiza o tratamento de diversos indicadores de compromissos coletados por meio de fontes abertas, fechadas e também de análises realizadas pela equipe de segurança *Heimdall*. Diante disto, abaixo listamos todos os Indicadores de Comprometimento (IoCs) relacionadas a análise do(s) artefato(s) deste relatório.

Indicadores do artefato	
md5:	be15f62d14d1cbe2aecce8396f4c6289
sha1:	e9cced71d31937d75edac3fcee1d21e46cd5351
sha256:	456b9adaabae9f3dce2207aa71410987f0a571cd8c11f2e7b41468501a863606
File name:	RaLord-0xb.exe

Tabela 5 - Indicadores de Comprometimento do RALord Ransomware.

Indicadores de URL, IPs e Domínios

Indicadores do artefato	
TOR Link:	ralordqe33mpufkpsr6zkdatktlu3t2uei4ught3sitxgtzfmqmbusuyd[.]onion
Tipo:	Data Leak Site
Descrição:	Site de Vazamento de Dados do RALord

Tabela 6 - Data Leak Site Principal do RALord.

TOR Link:	ralord3htj7v2dkavss2hjzviviwgsf4anfndnihn5qcjl6eb5if3cuqd[.]onion
Tipo:	Data Leak Site
Descrição:	Site de Vazamento de Dados do RALord

Tabela 7 - Backup I do Data Leak Site.

Indicadores do artefato	
TOR Link:	ralordt7gywtkkkkq2suldao6mpibsb7cpjvdfezpzwgltyj2laiuuid[.]onion
Tipo:	Data Leak Site
Descrição:	Site de Vazamento de Dados do RALord

Tabela 8 - Backup II do Data Leak Site.

Indicadores do artefato	
qTOX Chat:	8E9A6195A769FE7115F087C61D75CF32874C339B3AB0947D07480C9A8A12D A5009151BE6A51F 0C8E5B45C57AE244E9C904C5BC74F73306937469D9CEA22541CA69AC162B 8D42A20F4C0382AC
Sessão	054f55ec93aca9bac362b9d91eff36a7ce451e7caba47c0b2e004ba429f9529c7 9
Tipo:	Chat via TOX
Descrição:	Chat exclusivo com os operadores do RALord

Tabela 9 - Método de comunicação com operadores do RALord.

12 REFERÊNCIAS

- Heimdall *by* ISH Tecnologia
- Purple Team *by* ISH Tecnologia
- [MITRE ATT&CK](#)
- [Ransomware.live](#)

13 AUTORES

- Ícaro César – Malware Researcher
- Ismael Rocha – Threat Intelligence Specialist



heimdall
security research

A DIVISION OF ISH