heimdall

security research

A DIVISION OF ISH

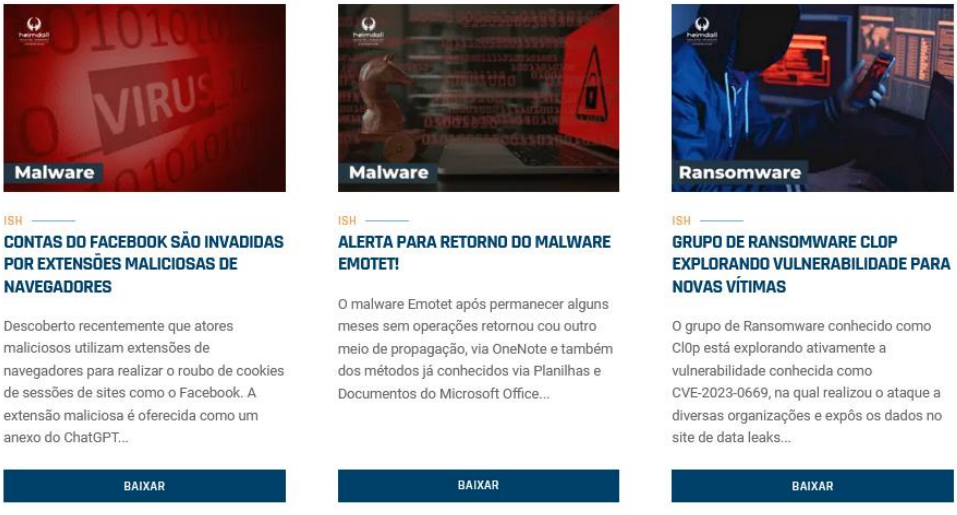
Novos grupos de *ransomwares* identificados

Receba alertas e informações sobre segurança cibernética e ameaças rapidamente, por meio do nosso Twitter.

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



Sumário

Lista de Figuras

1 INTRODUÇÃO

Novos grupos de *ransomwares* surgiram entre os meses de abril a junho, contabilizando aproximadamente 13 (treze) grupos com operações distintas. Tais grupos apresentam-se como *Ransomware-as-a-Service* (RaaS) e possuem *sites* de vazamento de dados (*data leak*) hospedados na rede Tor, atuando de forma a realizar a dupla extorsão de suas vítimas, sendo por meio de criptografia e exfiltração de dados.

O time de inteligência da ISH, Heimdall, realizou a elaboração de boletins segregados acerca dos *ransomwares* que serão mencionados neste boletim, bem como identificou sua operação, principais indicadores de comprometimentos (IoCs) e demais detalhes.

Os boletins se encontram no portal de boletins de segurança, disponíveis em: https://www.ish.com.br/boletins-de-seguranca/

Figura 1 – Aba de boletins de segurança publicados pela Heimdall.

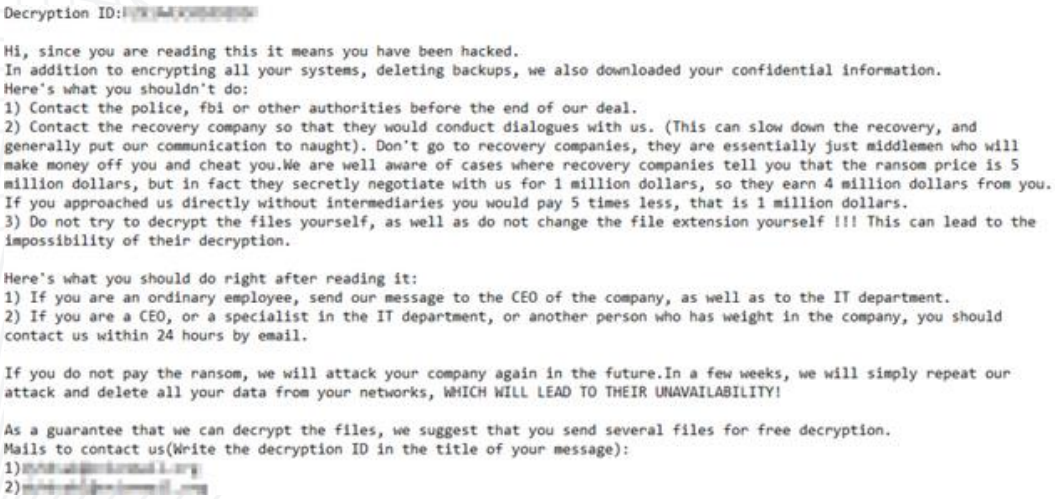
2 *RANSOMWARES* IDENTIFICADOS

Como forma de apresentar os grupos identificados, iremos, de forma breve, apresentar o resumo da ameaça e características.

- ***Ransomware* Rorschach**

Este *ransomware* foi identificado e apelidado como **Rorschach**, havendo comportamento único pois não havia indicações de atribuições a qualquer outra variante conhecida de *ransomwares*, bem como não havia marca ou métodos específicos conhecidos de grupos *ransomwares*.

A identificação do *ransomware* foi realizada pela CheckPoint, que o descreveu em sua análise como tendo comportamento de criptografia mais rápido do que outras cepas de *ransomwares* conhecidas.



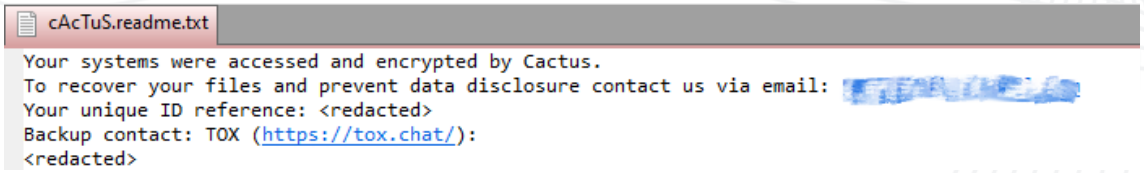
```
Decryption ID:[redacted]

Hi, since you are reading this it means you have been hacked.
In addition to encrypting all your systems, deleting backups, we also downloaded your confidential information.
Here's what you shouldn't do:
1) Contact the police, fbi or other authorities before the end of our deal.
2) Contact the recovery company so that they would conduct dialogues with us. (This can slow down the recovery, and
generally put our communication to naught). Don't go to recovery companies, they are essentially just middlemen who will
make money off you and cheat you.We are well aware of cases where recovery companies tell you that the ransom price is 5
million dollars, but in fact they secretly negotiate with us for 1 million dollars, so they earn 4 million dollars from you.
If you approached us directly without intermediaries you would pay 5 times less, that is 1 million dollars.
3) Do not try to decrypt the files yourself, as well as do not change the file extension yourself !!! This can lead to the
impossibility of their decryption.

Here's what you should do right after reading it:
1) If you are an ordinary employee, send our message to the CEO of the company, as well as to the IT department.
2) If you are a CEO, or a specialist in the IT department, or another person who has weight in the company, you should
contact us within 24 hours by email.

If you do not pay the ransom, we will attack your company again in the future.In a few weeks, we will simply repeat our
attack and delete all your data from your networks, WHICH WILL LEAD TO THEIR UNAVAILABILITY!

As a guarantee that we can decrypt the files, we suggest that you send several files for free decryption.
Mails to contact us(Write the decryption ID in the title of your message):
1)[redacted]
2)[redacted]
```

Figura 2 – Nota de resgate do ransomware Rorschach.

- ***Ransomware* Cactus**

Este *ransomware* foi identificado atuando desde março de 2023, adotando o nome de Cactus. Segundo pesquisadores, foi verificado que o Cactus realizava a exploração de vulnerabilidades em produtos de VPN da Fortinet.

O *ransomware* atua de forma similar a outros grupos de *ransomwares*, adotando as mesmas TTPs.



cAcTuS.readme.txt

```
Your systems were accessed and encrypted by Cactus.
To recover your files and prevent data disclosure contact us via email: [redacted]
Your unique ID reference: <redacted>
Backup contact: TOX (https://tox.chat/):
<redacted>
```

Figura 3 – Nota de resgate do ransomware *Cactus*

- ***Ransomware* Akira**

Este *ransomware* foi identificado em operação desde março de 2023, contabilizando mais de dezesseis organizações vítimas. O referido *ransomware* atua de forma similar a outros grupos de *ransomware* já mapeados.

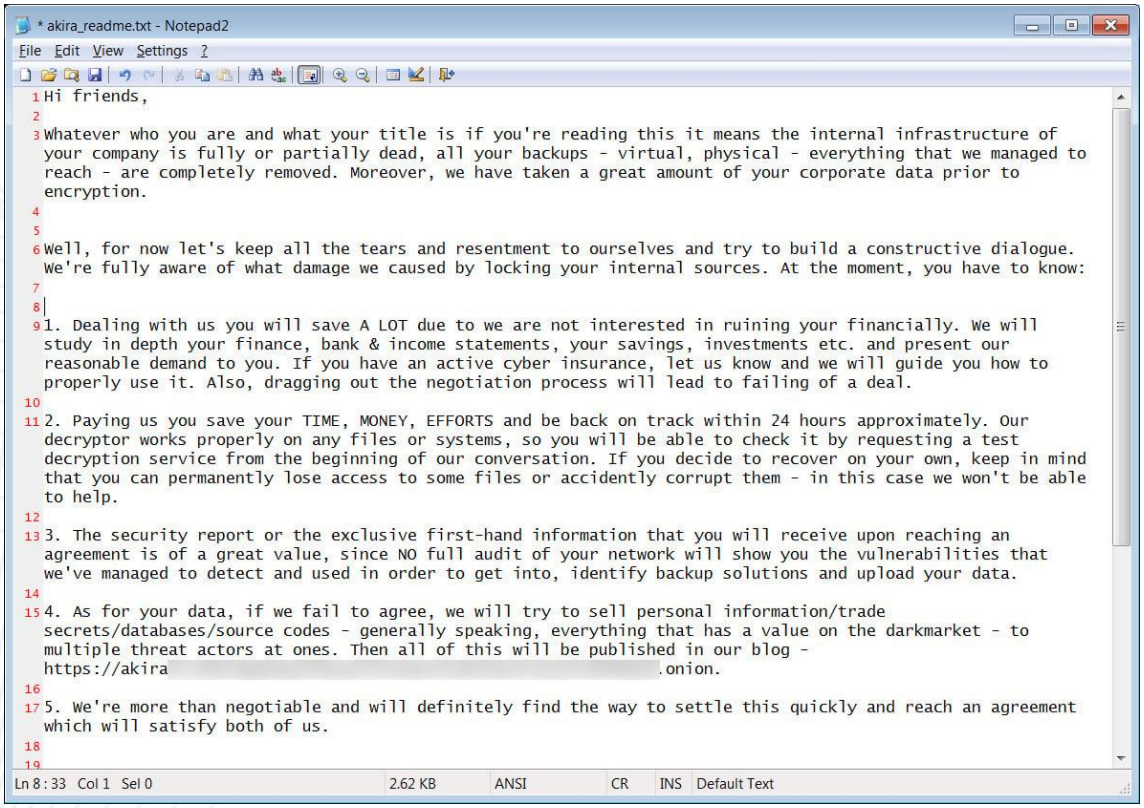


Figura 4 – Nota de resgate do ransomware Akira.

- ***Ransomware* Rancoz**

Este *ransomware* foi identificado em maio de 2023, e durante sua análise foi verificado que possui semelhanças com o código fonte do *ransomware* Vice Society.

Além da semelhança, foi possível verificar que ele atua de forma semelhante aos demais grupos de *ransomwares* existentes, criptografando e exfiltrando arquivos para pagamentos de resgates.

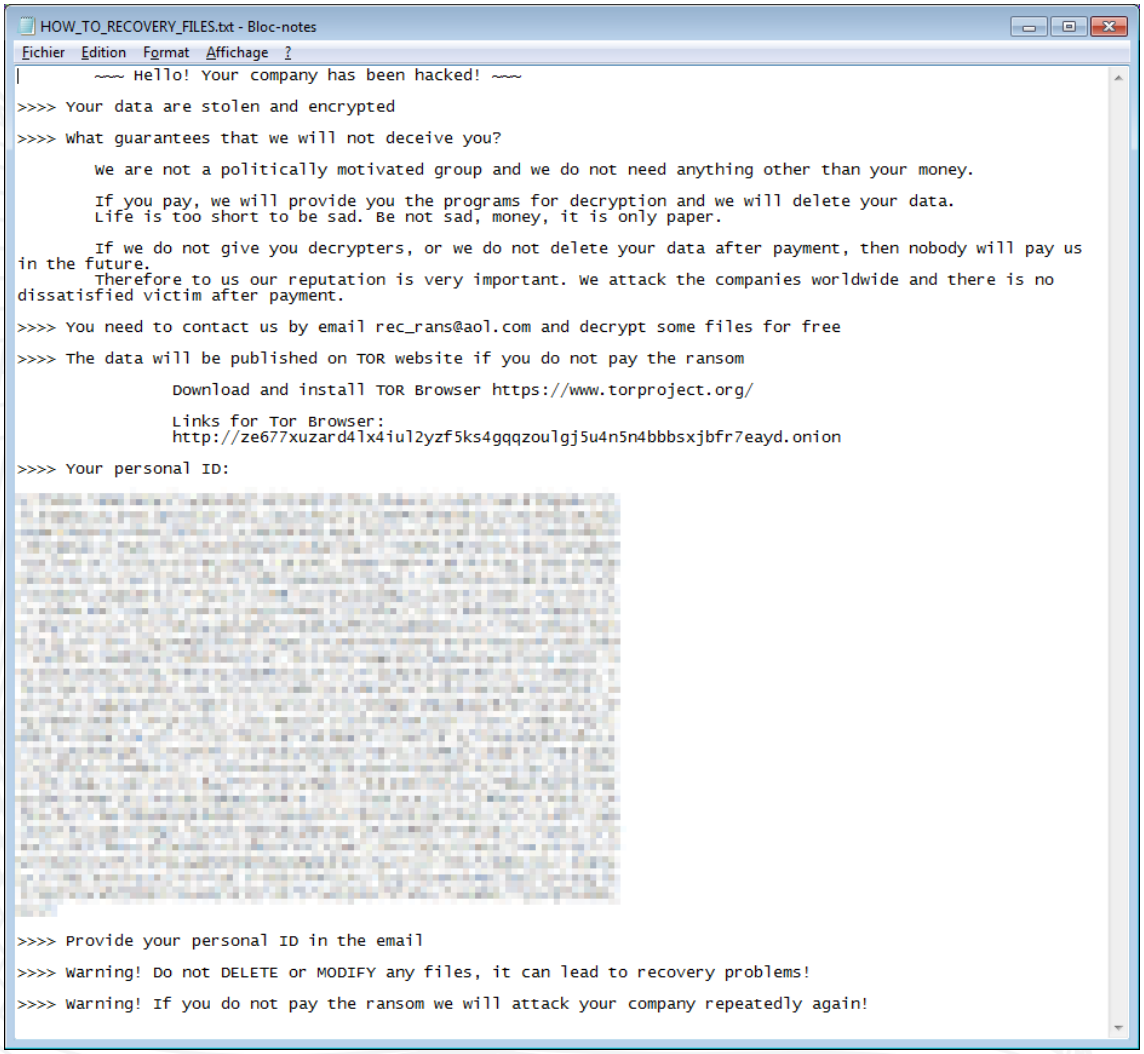


Figura 5 – Nota de resgate do ransomware Rancoz.

- ***Ransomware* CrypNet**

Esta operação de *ransomware* foi iniciada em abril de 2023, sendo ofertado em fóruns clandestinos como *Ransomware-as-a-Service* (RaaS), atuando de forma similar aos demais *ransomwares* do mercado.

A característica deste *ransomware* é a similaridades em suas funções com o código-fonte dos *ransomwares* Chaos e Yashma.

```
*** CRYPTNET RANSOMWARE ***

--- What happened? ---

All of your files are encrypted and stolen. Stolen data will be published soon
on our tor website. There is no way to recover your data and prevent data leakage without
us
Decryption is not possible without private key. Don't waste your and our time to recover
your files.
It is impossible without our help

--- How to recover files & prevent leakage? ---

To make sure that we REALLY CAN recover your data - we offer FREE DECRYPTION for warranty.
We promise that you can recover all your files safely and prevent data leakage. We can do
it!

--- Contact Us---

Download Tor Browser - https://www.torproject.org/download/ and install it
Open website: http://cryptr[redacted]
Enter DECRYPTION ID: [DECRYPTION ID]
```

Figura 6 – Nota de resgate do ransomware CryptNet.

- ***Ransomware* Darkrace**

Outra operação de *ransomware* iniciou-se em maio de 2023, desta vez denominado Darkrace, na qual a equipe da ISH realizou a análise e pode constatar que o *ransomware* atua de forma similar à demais operações, possuindo também um *site* de publicação de dados.

A sua nota de resgate é observada uma certa similaridade com a nota de resgate do *ransomware* LockBit3.0, o qual teve seu compilador vazado em setembro de 2020.

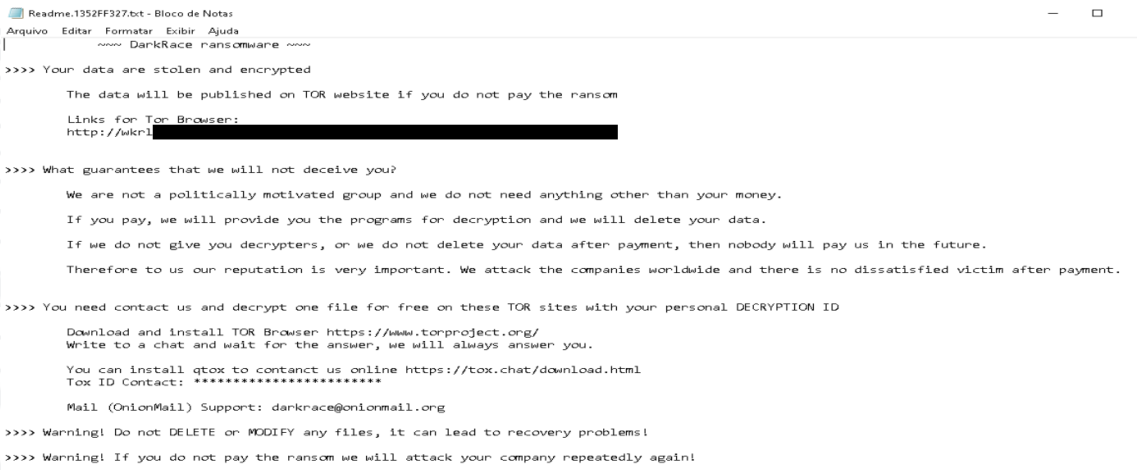


Figura 7 – Nota de resgate do ransomware Darkrace.

- ***Ransomware* MalasLocker**

Esta operação de *ransomware* foi observada em junho de 2023, conhecida como Malaslocker.

A característica deste grupo de *ransomwares* é que o pagamento do resgate dos arquivos criptografados deve ser realizado como doação para caridades sem fins lucrativos. Uma vez que a doação é aprovada pelos operadores, o descriptografador é liberado para a organização vítima.

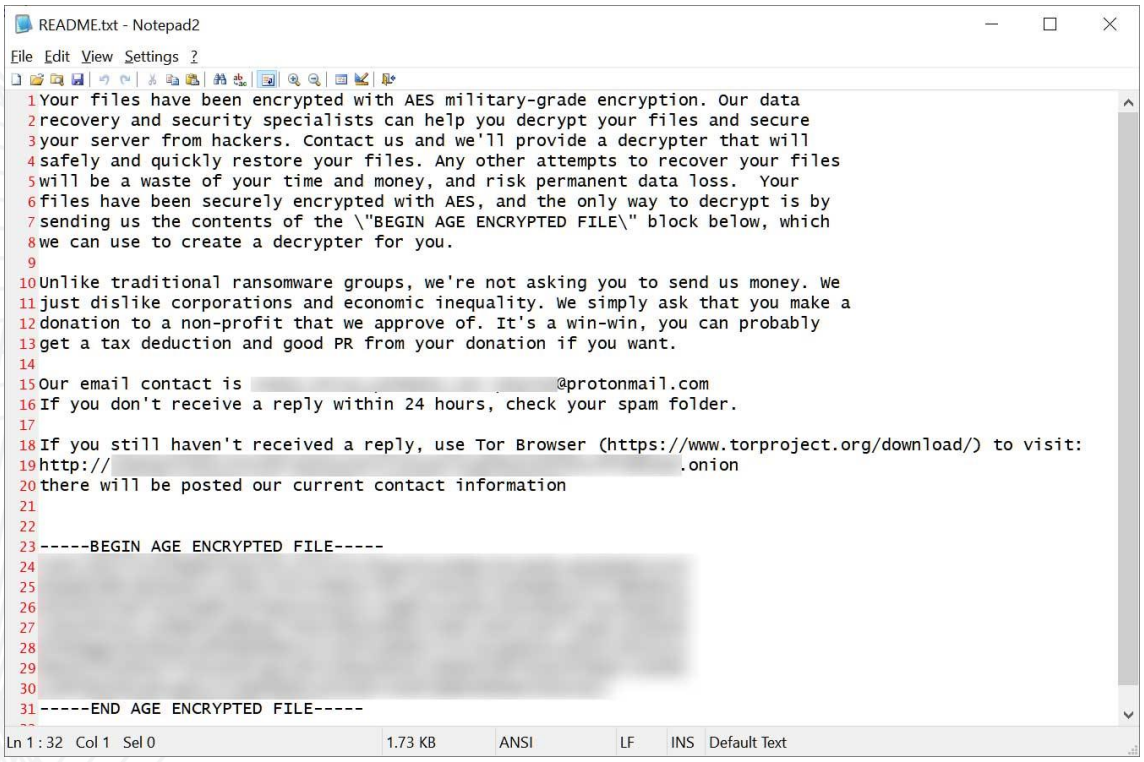


Figura 8 – Nota de resgate do ransomware MalasLocker.

- ***Ransomware* 8base**

Outra grande operação foi o *ransomware* 8base, identificado em junho. A referida operação já teria prejudicado diversas empresas brasileiras, possuindo a forma de operação idêntica aos demais grupos de *ransomwares*.

Até o momento da elaboração do presente alerta, não havia amostras disponíveis para serem analisadas e que estejam disponíveis em fontes abertas.

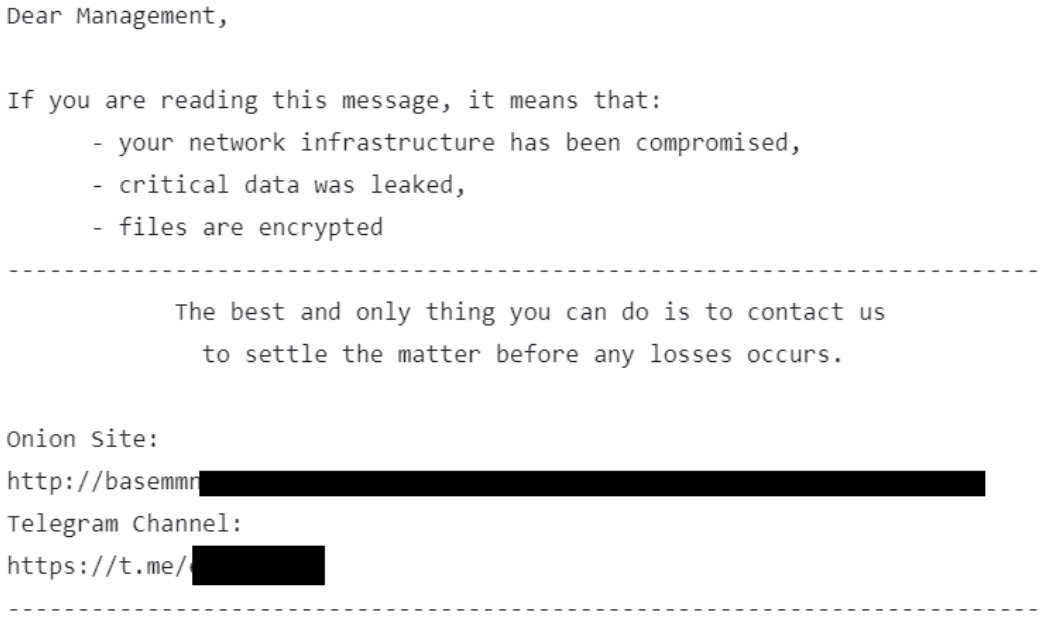
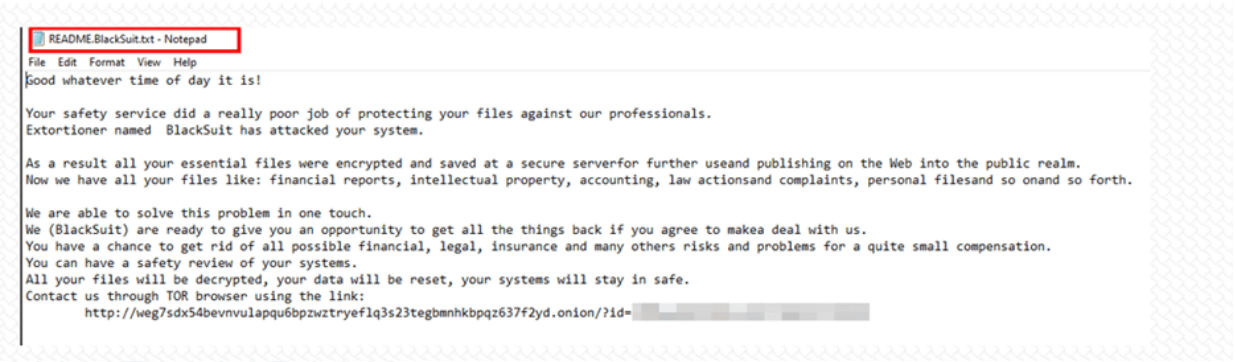


Figura 9 – Nota de resgate do ransomware 8Base.

- ***Ransomware* BlackSuit**

Esta operação de *ransomware* foi identificada por meio da Unit42 da Palo Alto Networks, descrevendo ainda em seu relatório que este *ransomware* compartilhava semelhanças com o código-fonte da variante do Linux com o *ransomware* Royal.

Atua de forma semelhante aos demais grupos de *ransomwares*, realizando a criptografia e exfiltração dos dados.


README.BlackSuit.txt - Notepad

File Edit Format View Help

Good whatever time of day it is!

Your safety service did a really poor job of protecting your files against our professionals.
Extortioner named BlackSuit has attacked your system.

As a result all your essential files were encrypted and saved at a secure serverfor further useand publishing on the Web into the public realm.
Now we have all your files like: financial reports, intellectual property, accounting, law actionsand complaints, personal filesand so onand so forth.

We are able to solve this problem in one touch.
We (BlackSuit) are ready to give you an opportunity to get all the things back if you agree to makea deal with us.
You have a chance to get rid of all possible financial, legal, insurance and many others risks and problems for a quite small compensation.
You can have a safety review of your systems.
All your files will be decrypted, your data will be reset, your systems will stay in safe.
Contact us through TOR browser using the link:
http://weg7sdx54bevnvulapqu6bpzwztryeflq3s23tegbmnhkbpqz637f2yd.onion/?id=

Figura 10 – Nota de resgate do ransomware BlackSuit.

- ***Ransomware* Rhysida**

Esta operação de *ransomware* foi identificada em maio de 2023, utilizando o nome de *ransomware* Rhysida, que atua de forma idêntica aos demais grupos de *ransomware*.

A característica observada deste grupo é o despejo de uma nota de resgate em formato PDF, semelhante ao *ransomware* Dark Power analisado pela ISH.

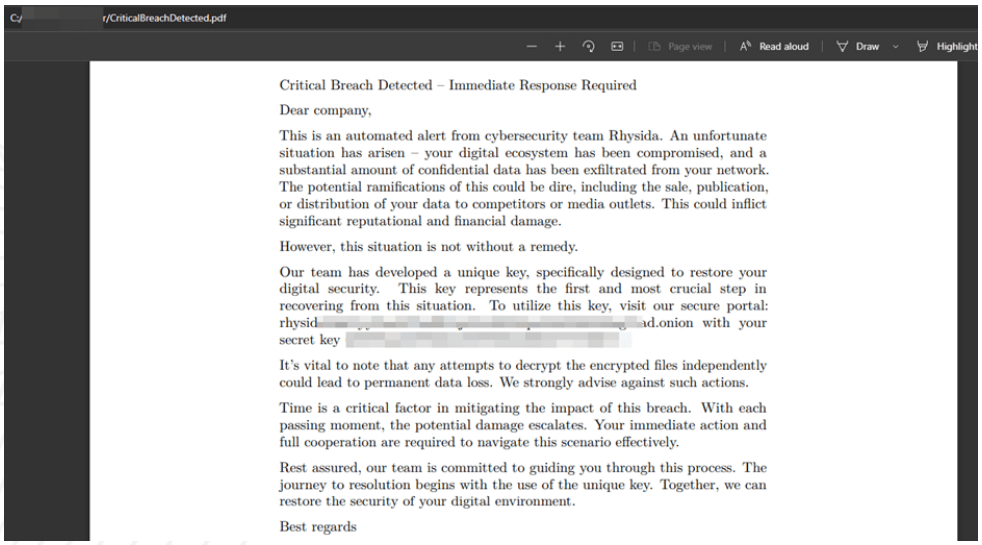


Figura 11 – Nota de resgate do ransomware Rhysida.

- ***Ransomware* NoEscape**

Atuando me maneira semelhante a um *ransomware-as-a-Service* (RaaS), adotou o nome de *ransomware* NoEscape, sendo identificado em maio de 2023 em um fórum clandestino.

Foi verificado que uma amostra teria sido identificada pela Trend Micro em meados de março de 2023, através de despejo de outro *malware* por meio de visita a *sites* infectados, cujo acesso teria sido realizado por um usuário.

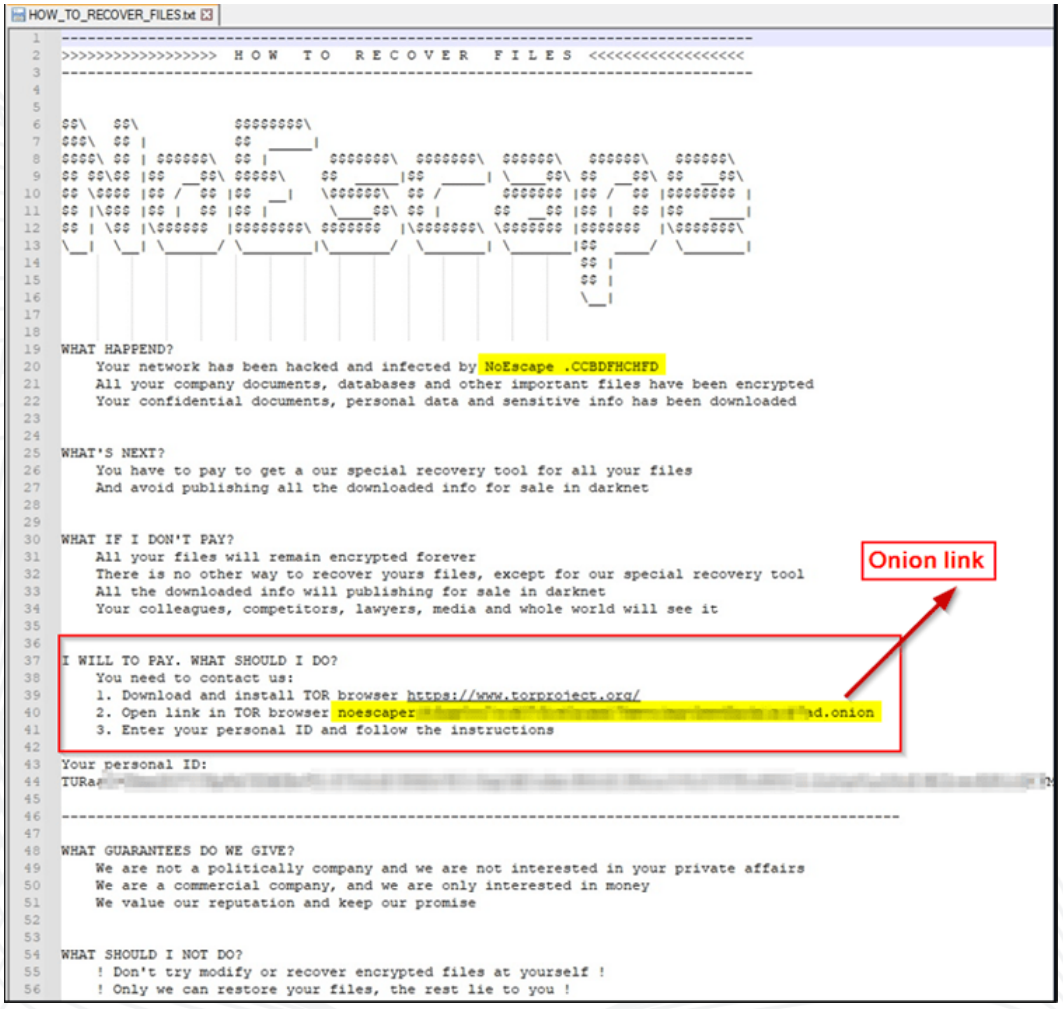
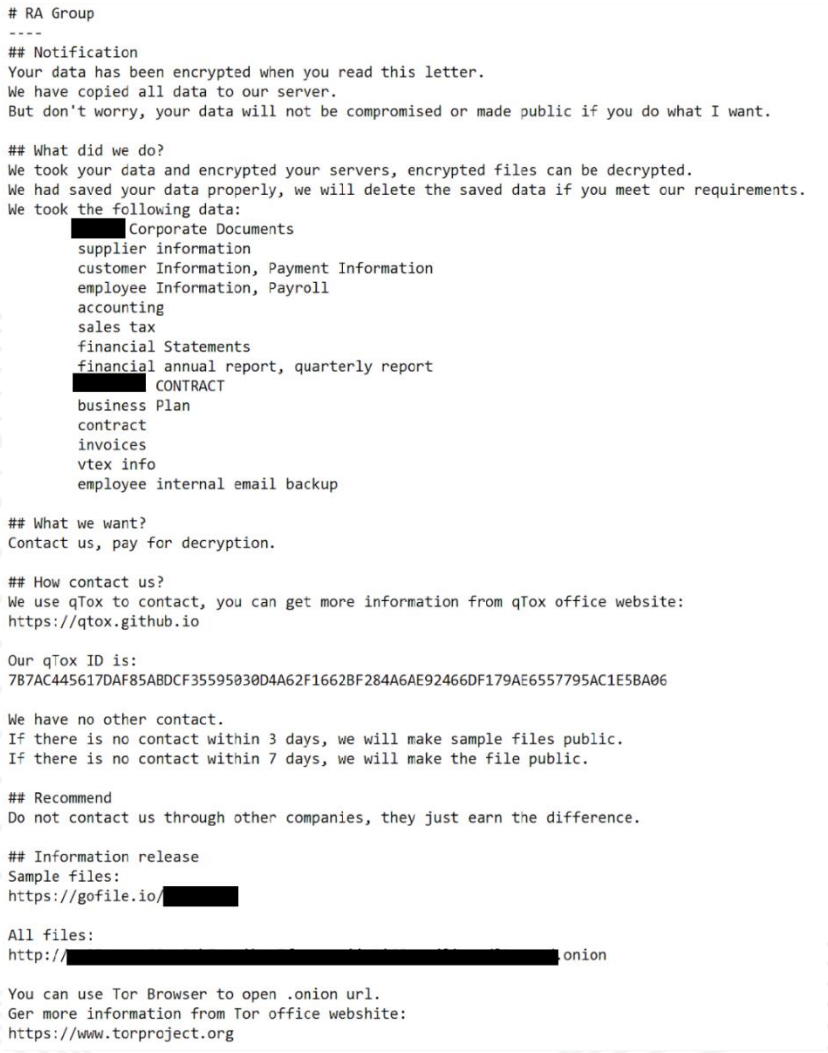


Figura 12 – Nota de resgate do ransomware NoEscape.

- ***Ransomware* RA Group**

O *ransomware* RA Group foi identificado em uma operação desde meados de abril de 2023, e possui similaridade bem próxima com o código-fonte vazado do *ransomwares*Babuk.

Esta operação de *ransomware* atua de forma semelhante aos demais, por meio de criptografia e exfiltração de dados.



```
# RA Group
---
## Notification
Your data has been encrypted when you read this letter.
We have copied all data to our server.
But don't worry, your data will not be compromised or made public if you do what I want.

## What did we do?
We took your data and encrypted your servers, encrypted files can be decrypted.
We had saved your data properly, we will delete the saved data if you meet our requirements.
We took the following data:
        [redacted] Corporate Documents
        supplier information
        customer Information, Payment Information
        employee Information, Payroll
        accounting
        sales tax
        financial Statements
        financial annual report, quarterly report
        [redacted] CONTRACT
        business Plan
        contract
        invoices
        vtex info
        employee internal email backup

## What we want?
Contact us, pay for decryption.

## How contact us?
We use qTox to contact, you can get more information from qTox office website:
https://qtox.github.io

Our qTox ID is:
7B7AC445617DAF85ABDCF35595030D4A62F1662BF284A6AE92466DF179AE6557795AC1E5BA06

We have no other contact.
If there is no contact within 3 days, we will make sample files public.
If there is no contact within 7 days, we will make the file public.

## Recommend
Do not contact us through other companies, they just earn the difference.

## Information release
Sample files:
https://gofile.io/[redacted]

All files:
http://[redacted].onion

You can use Tor Browser to open .onion url.
Ger more information from Tor office webshite:
https://www.torproject.org
```

Figura 13 - Nota de resgate do ransomware RA Group.

3 DADOS ESTATÍSTICOS

De acordo com o monitoramento da ISH, acerca de ataques de *ransomware*, foi possível verificar que aproximadamente mais de **1.800 organizações foram vítimas de *ransomwares* em 2023**.

Vale salientar que o número pode ser muito maior, visto que grupos de *ransomwares* surgem quase que diariamente ou, muitos dos grupos não realizam a publicação do nome da organização em seu *site* de *data leak* (vazamento).

Apenas em **junho**, foi realizada a publicação e divulgação por parte de grupos de *ransomwares* de mais de **180 vítimas**.

4 GTI – Global Threat Intelligence

A ISH Tecnologia, por meio do GTI (*Global Threat Intelligence*) coleta, trata e compartilha alguns dos principais Indicadores de Comprometimentos localizados e analisados pela equipe de Inteligência de Ameaças, focalizando em entregar tais dados para identificação ou facilitação de tratamento de incidentes de segurança cibernético

Foi coletada e tratada a quantia de **110.783 (cento e onze mil setecentos e oitenta e três)** Indicadores de Comprometimento de artefatos maliciosos nos últimos **90 dias**, sendo classificados como ***ransomware***, havendo indicadores de comprometimentos como *hashes*, domínios e endereços IP.

Figura 14 – Número de IoCs gerais tratados.

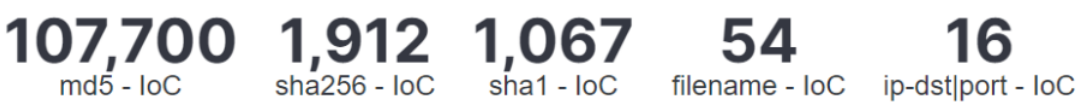


Figura 15 – Números de IoCs MISP de acordo com cada categoria.

5 RECOMENDAÇÕES

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

- **Realização de *backups* regulares:** armazene cópias de segurança de todos os dados importantes em um local seguro e desconectado.
- **Realização de atualizações de *softwares*:** mantenha todos os *softwares* de ativos atualizados, incluindo sistemas operacionais e aplicativos.
- **Utilização de proteção de rede**, como *firewalls*, antivírus e outras medidas de segurança para proteger sua rede.
- **Realização do trabalho de conscientização** com os colaboradores, ensinando aos mesmos a reconhecer e evitar ameaças, como *phishing* e/ou clicar em *links* maliciosos.
- **Monitoração regular da sua rede e sistemas** para identificar e responder rapidamente a qualquer atividade suspeita.
- **Criação e aplicação de um plano de resposta de incidentes**, sendo que em caso de ataques de *ransomware* poderão ser utilizados e conterão informações como questões relacionadas a *backups* e recuperação de sistema.

6 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**

heimdall
security research

A DIVISION OF ISH