



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



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...

BAIXAR



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...

BAIXAR



ISH
GRUPO DE RANSOMWARE CLOP EXPLORANDO VULNERABILIDADE PARA NOVAS VITIMAS

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

Sumário

1	Introdução.....	6
2	<i>Ransomwares</i> identificados.....	7
3	Dados estatísticos	18
4	GTI – Global Threat Intelligence.....	19
5	Recomendações.....	20
6	Referências.....	21

Lista de Figuras

Figura 1 – Aba de boletins de segurança publicados pela Heimdall.....	6
Figura 2 – Nota de resgate do ransomware Rorschach.	7
Figura 3 – Nota de resgate do ransomware Cactus	7
Figura 4 – Nota de resgate do ransomware Akira.....	8
Figura 5 – Nota de resgate do ransomware Rancoz.	9
Figura 6 – Nota de resgate do ransomware CryptNet.	10
Figura 7 – Nota de resgate do ransomware Darkrace.	11
Figura 8 – Nota de resgate do ransomware MalasLocker.	12
Figura 9 – Nota de resgate do ransomware 8Base.	13
Figura 10 – Nota de resgate do ransomware BlackSuit.....	14
Figura 11 – Nota de resgate do ransomware Rhysida.....	15
Figura 12 – Nota de resgate do ransomware NoEscape.	16
Figura 13 – Nota de resgate do ransomware RA Group.	17
Figura 14 – Número de IoCs gerais tratados.....	19
Figura 15 – Números de IoCs MISP de acordo com cada categoria.	19

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.

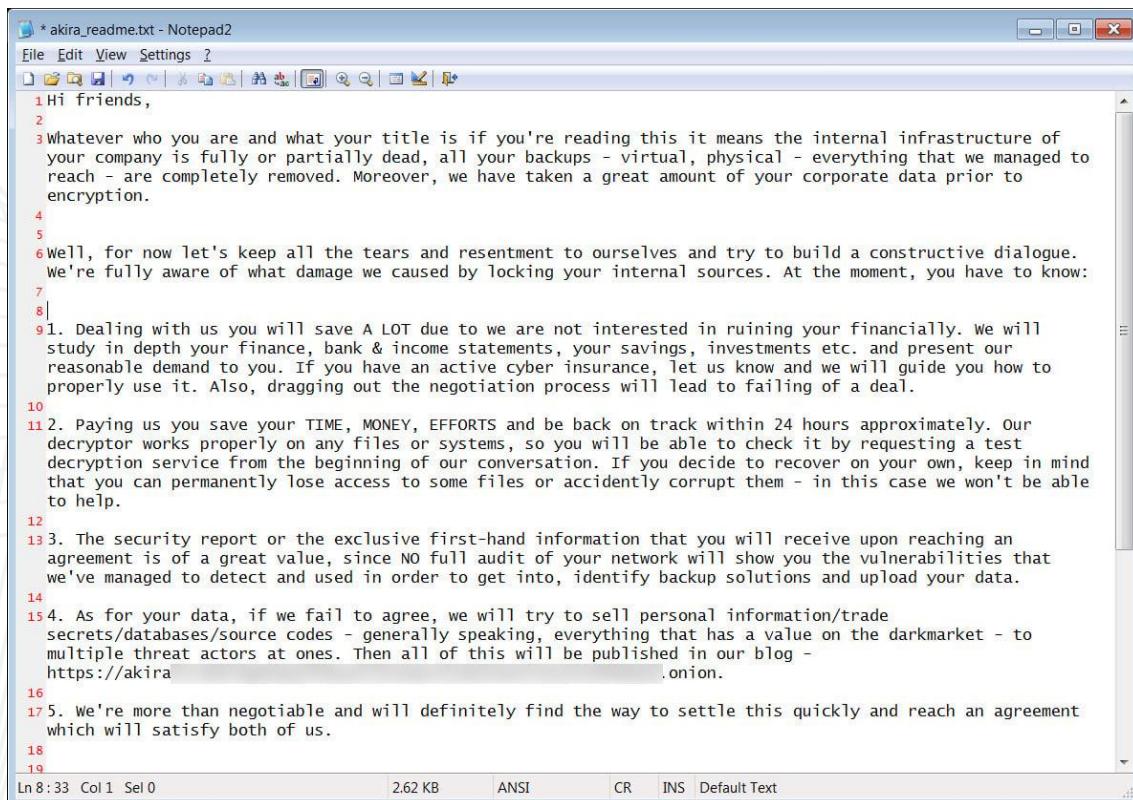
cAcTuS.readme.txt

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.



The screenshot shows a Windows-style window titled "akira_readme.txt - Notepad2". The text content is a ransom note from the Akira ransomware group:

```
1 Hi friends,
2
3 Whatever who you are and what your title is if you're reading this it means the internal infrastructure of
your company is fully or partially dead, all your backups - virtual, physical - everything that we managed to
reach - are completely removed. Moreover, we have taken a great amount of your corporate data prior to
encryption.
4
5 Well, for now let's keep all the tears and resentment to ourselves and try to build a constructive dialogue.
We're fully aware of what damage we caused by locking your internal sources. At the moment, you have to know:
6
7
8|
9 1. Dealing with us you will save A LOT due to we are not interested in ruining your financially. We will
study in depth your finance, bank & income statements, your savings, investments etc. and present our
reasonable demand to you. If you have an active cyber insurance, let us know and we will guide you how to
properly use it. Also, dragging out the negotiation process will lead to failing of a deal.
10
11 2. Paying us you save your TIME, MONEY, EFFORTS and be back on track within 24 hours approximately. Our
decryptor works properly on any files or systems, so you will be able to check it by requesting a test
decryption service from the beginning of our conversation. If you decide to recover on your own, keep in mind
that you can permanently lose access to some files or accidentally corrupt them - in this case we won't be able
to help.
12
13 3. The security report or the exclusive first-hand information that you will receive upon reaching an
agreement is of a great value, since NO full audit of your network will show you the vulnerabilities that
we've managed to detect and used in order to get into, identify backup solutions and upload your data.
14
15 4. As for your data, if we fail to agree, we will try to sell personal information/trade
secrets/databases/source codes - generally speaking, everything that has a value on the darkmarket - to
multiple threat actors at ones. Then all of this will be published in our blog -
https://akira.onion.
16
17 5. We're more than negotiable and will definitely find the way to settle this quickly and reach an agreement
which will satisfy both of us.
18
19
```

At the bottom of the window, status bar text includes: Ln 8:33 Col 1 Sel 0, 2.62 KB, ANSI, CR, INS, Default Text.

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.

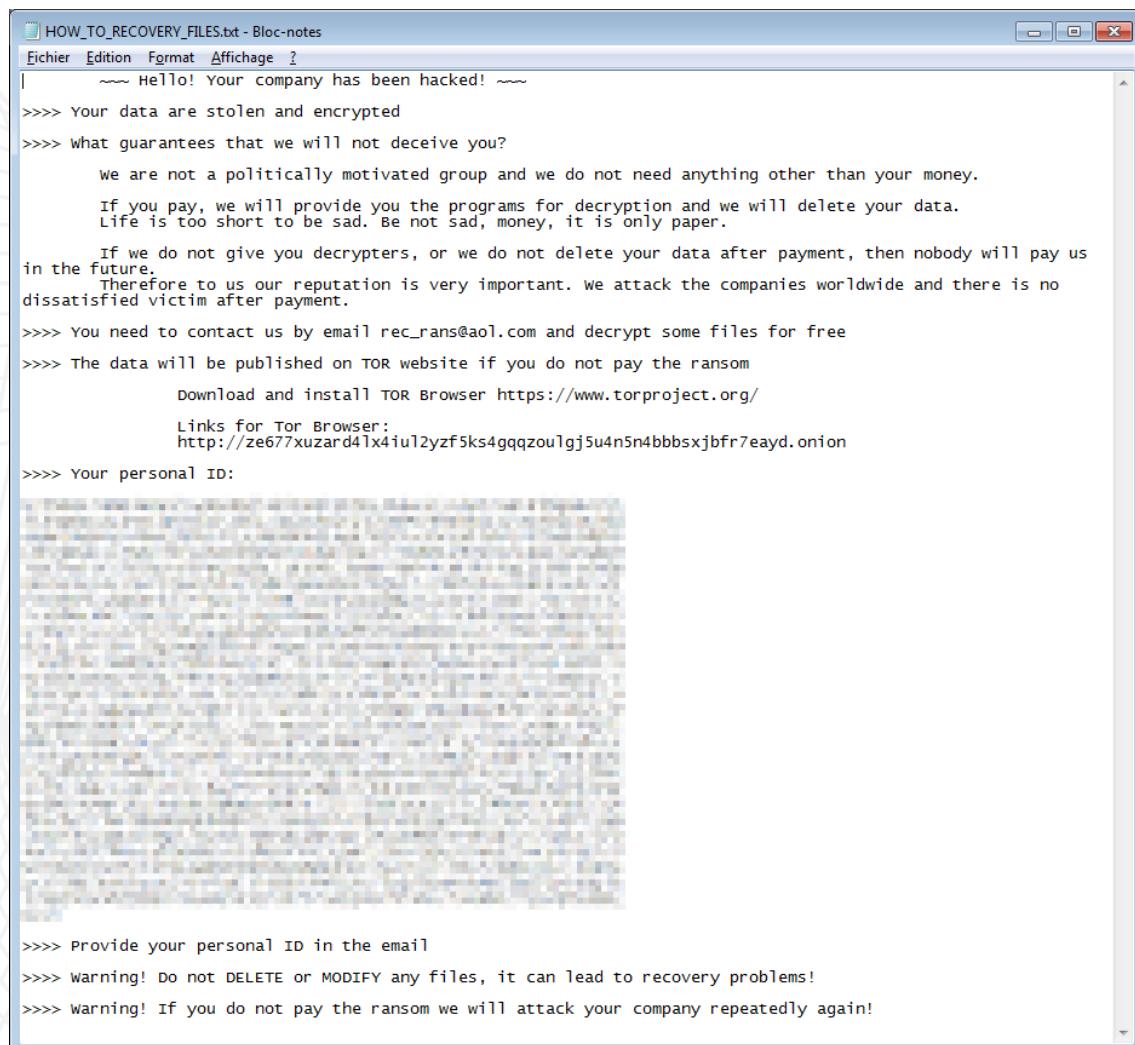


Figura 5 – Nota de resgate do ransomware Rancoz.

- **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\[REDACTED\]](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.

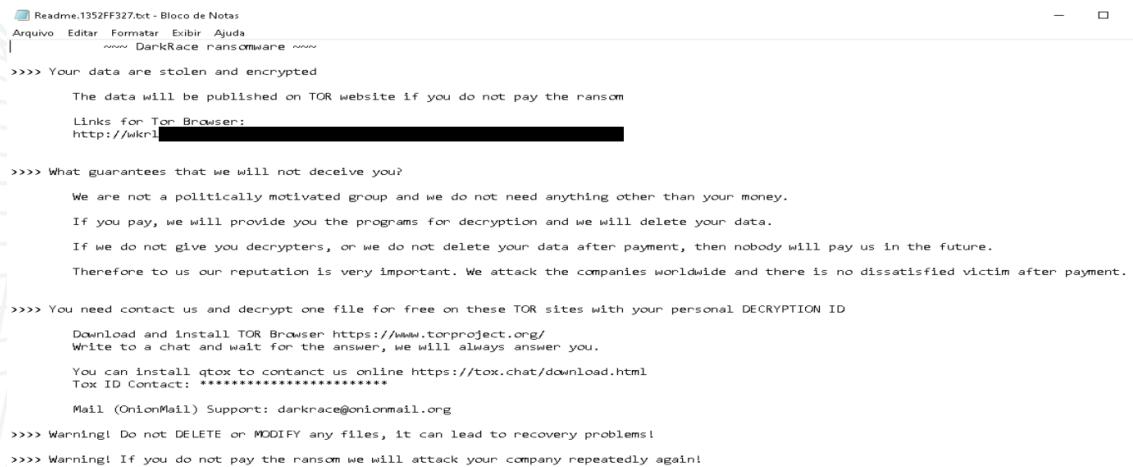
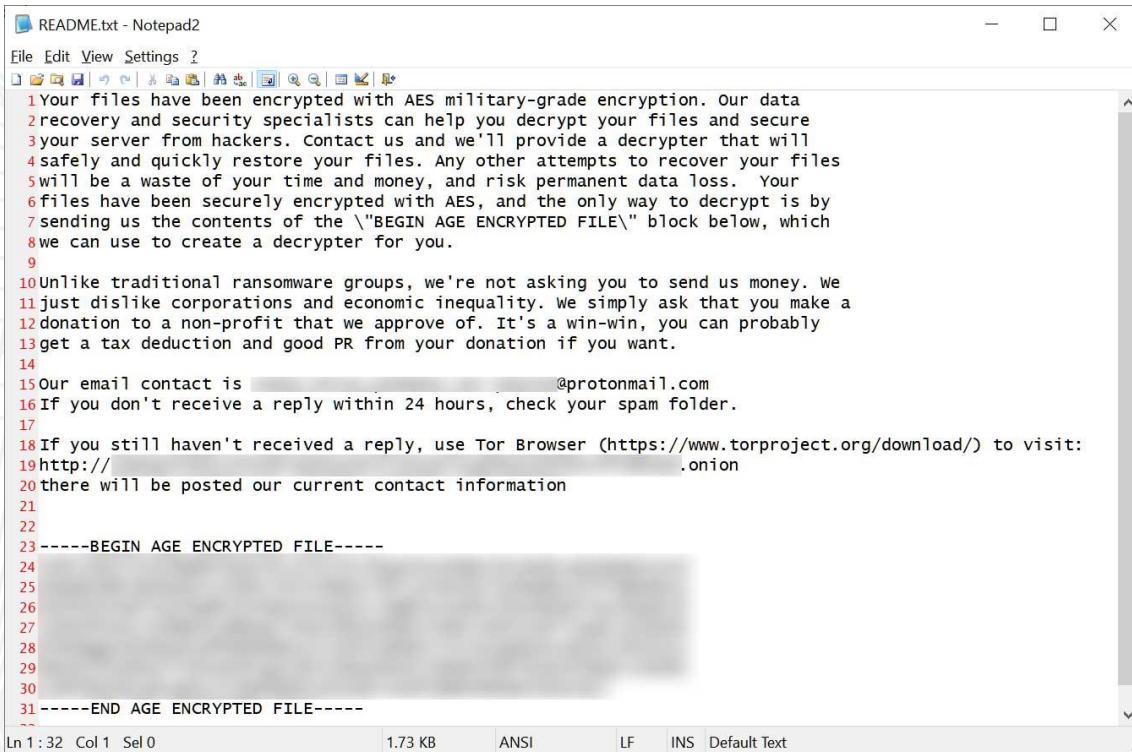


Figura 7 – Nota de resgate do ransomware Darkrace.

- **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.



The screenshot shows a Notepad2 window with the file name "README.txt". The content of the file is a ransom note from the MalasLocker ransomware. The text is numbered from 1 to 31, indicating line numbers. The note explains that files have been encrypted with AES and offers decryption via a decrypter provided by the attackers. It also mentions a donation to a non-profit organization and provides an email contact (@protonmail.com) and a Tor2Door link. A redacted section follows, and the note concludes with an end marker.

```
1 Your files have been encrypted with AES military-grade encryption. Our data
2 recovery and security specialists can help you decrypt your files and secure
3 your server from hackers. Contact us and we'll provide a decrypter that will
4 safely and quickly restore your files. Any other attempts to recover your files
5 will be a waste of your time and money, and risk permanent data loss. Your
6 files have been securely encrypted with AES, and the only way to decrypt is by
7 sending us the contents of the \"BEGIN AGE ENCRYPTED FILE\" block below, which
8 we can use to create a decrypter for you.
9
10 Unlike traditional ransomware groups, we're not asking you to send us money. We
11 just dislike corporations and economic inequality. We simply ask that you make a
12 donation to a non-profit that we approve of. It's a win-win, you can probably
13 get a tax deduction and good PR from your donation if you want.
14
15 Our email contact is @protonmail.com
16 If you don't receive a reply within 24 hours, check your spam folder.
17
18 If you still haven't received a reply, use Tor Browser (https://www.torproject.org/download/) to visit:
19 http://
20 there will be posted our current contact information
21
22
23 -----BEGIN AGE ENCRYPTED FILE-----
24
25
26
27
28
29
30
31 -----END AGE ENCRYPTED FILE-----
```

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.

Dear Management,

If you are reading this message, it means that:

- your network infrastructure has been compromised,
- critical data was leaked,
- files are encrypted

The best and only thing you can do is to contact us
to settle the matter before any losses occurs.

Onion Site:

<http://basemmrr> [REDACTED]

Telegram Channel:

<https://t.me/> [REDACTED]

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.

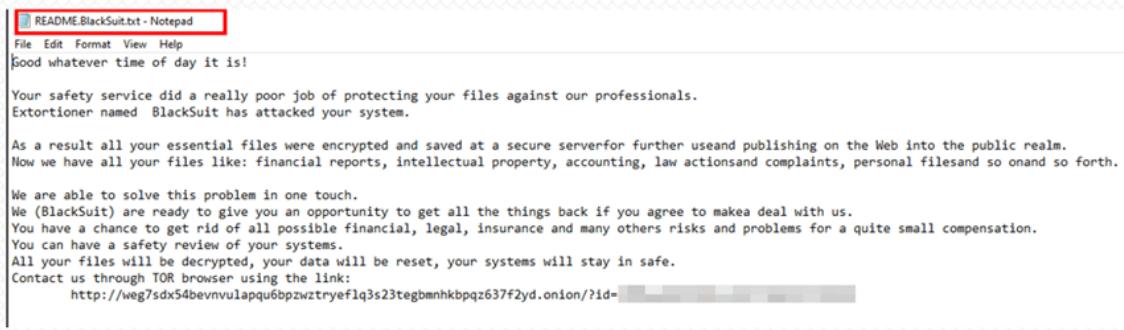


Figura 10 – Nota de resgate do ransomware BlackSuit.

- **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.

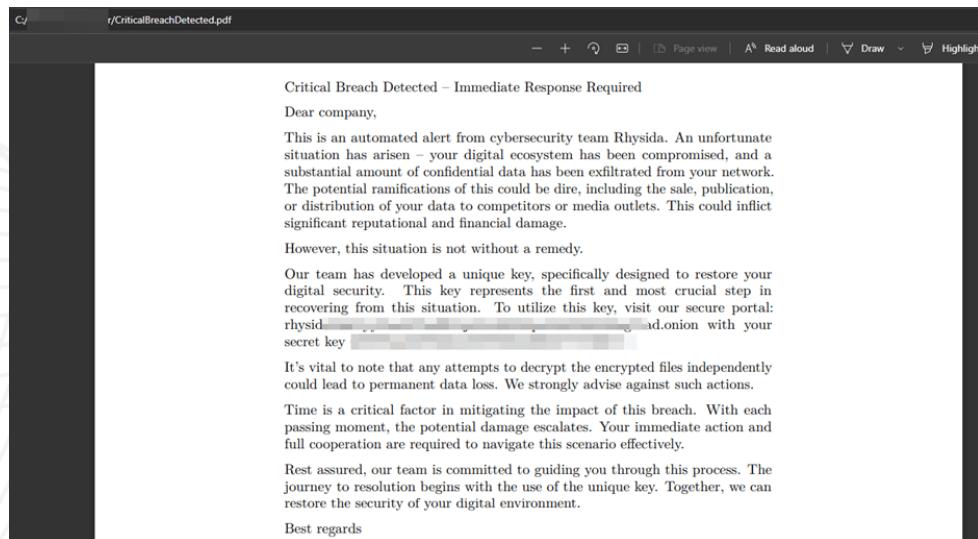


Figura 11 – Nota de resgate do ransomware Rhysida.

- ***Ransomware NoEscape***

Atuando de 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 ransomwaresBabuk.

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.
Get more information from Tor office website:
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.

110,783
IoC TOTAL

Figura 14 – Número de IoCs gerais tratados.

107,700	1,912	1,067	54	16
md5 - IoC	sha256 - IoC	sha1 - IoC	filename - IoC	ip-dst port - IoC

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

