heimdall

security research

A DIVISION OF ISH

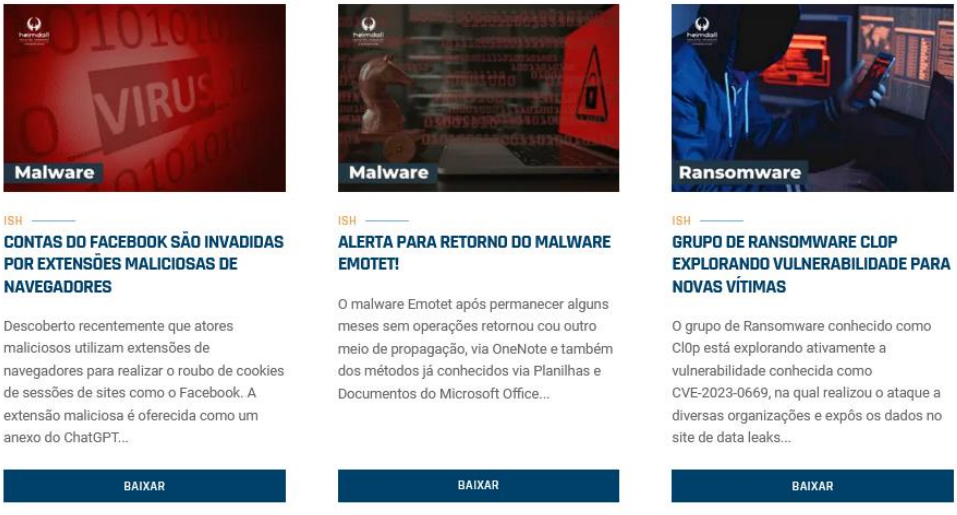
Novo RaaS identificado, Ransomware NoEscape

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



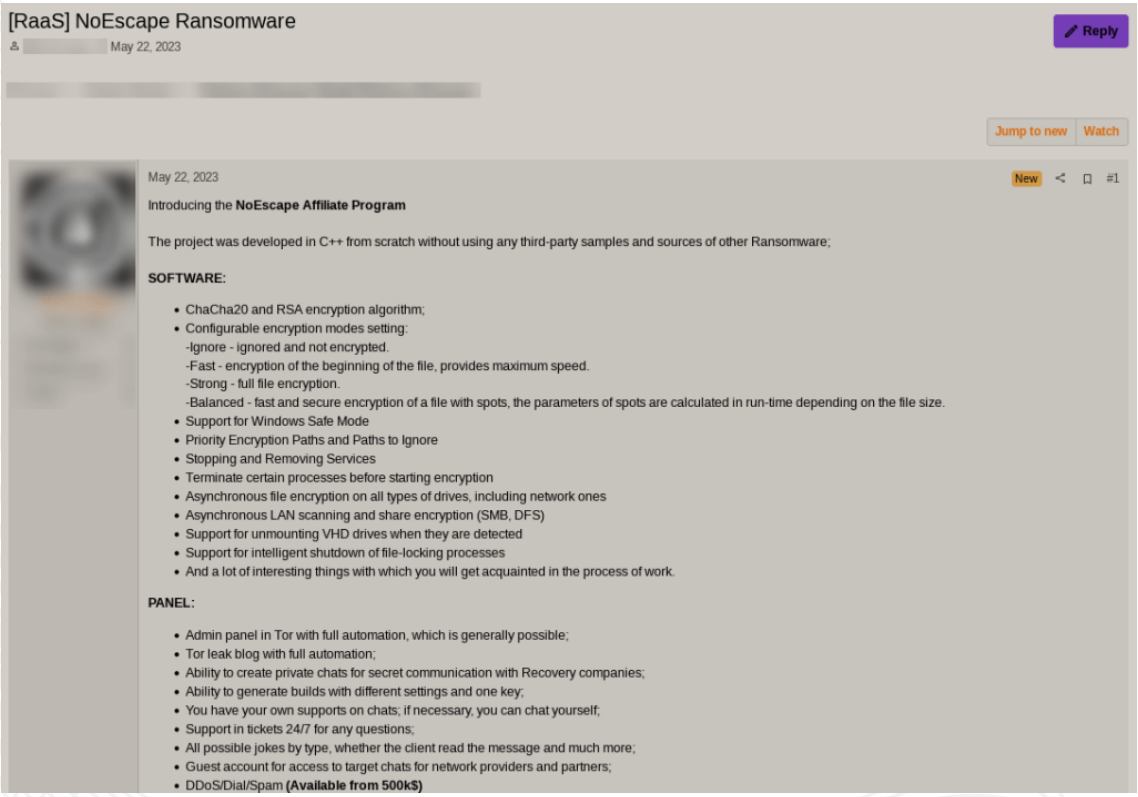
Sumário

Lista de Figuras

1 INTRODUÇÃO

Recentemente um novo programa de ***Ransomware-as-a-Service (RaaS)*** apelidado ou conhecido como **"NoEscape"** foi identificado sendo oferecido em um fórum de cibercrime no final de maio de 2023 e tinha com o intuito procurar novos afiliados para o seu programa.

De acordo com o anúncio, o ransomware foi criado na linguagem de programação **C++** e foi desenvolvido de forma nativa sem a utilização de recursos ou códigos-fontes de terceiros.


[RaaS] NoEscape Ransomware

May 22, 2023

Reply

Jump to new | Watch

May 22, 2023 New #1

Introducing the **NoEscape Affiliate Program**

The project was developed in C++ from scratch without using any third-party samples and sources of other Ransomware;

SOFTWARE:

- ChaCha20 and RSA encryption algorithm;
- Configurable encryption modes setting:
  -Ignore - ignored and not encrypted.
  -Fast - encryption of the beginning of the file, provides maximum speed.
  -Strong - full file encryption.
  -Balanced - fast and secure encryption of a file with spots, the parameters of spots are calculated in run-time depending on the file size.
- Support for Windows Safe Mode
- Priority Encryption Paths and Paths to Ignore
- Stopping and Removing Services
- Terminate certain processes before starting encryption
- Asynchronous file encryption on all types of drives, including network ones
- Asynchronous LAN scanning and share encryption (SMB, DFS)
- Support for unmounting VHD drives when they are detected
- Support for intelligent shutdown of file-locking processes
- And a lot of interesting things with which you will get acquainted in the process of work.

PANEL:

- Admin panel in Tor with full automation, which is generally possible;
- Tor leak blog with full automation;
- Ability to create private chats for secret communication with Recovery companies;
- Ability to generate builds with different settings and one key;
- You have your own supports on chats; if necessary, you can chat yourself;
- Support in tickets 24/7 for any questions;
- All possible jokes by type, whether the client read the message and much more;
- Guest account for access to target chats for network providers and partners;
- DDoS/Dial/Spam **(Available from 500k$)**

Figura 1 – Publicação e venda do Ransomware no fórum.

A empresa Cyble publicou um relatório sobre a análise deste novo tipo de afiliado de ransomwares, a qual apresentamos os detalhes neste alerta.

2 DETALHES DA OPERAÇÃO DO RANSOMWARE

No relatório compartilhado, foram identificados os recursos a seguir do ransomwares como parte do programa de afiliados:

1. A compilação do malware **suporta o algoritmo de criptografia ChaCha20 e RSA**, sendo que poderá ser considerada um método de criptografia híbrida que grupos sofisticados de ransomwares utilizam para criptografar arquivos e proteger as suas chaves. A técnica criptografa todas as chaves ChaCha20 com uma chave ChaCha20 global antes de criptografar a chave global com sua chave pública RSA-2048.

2. A amostra oferece suporte ao modo de segurança do Windows, na qual um script implementa uma série de comandos consecutivos que reinicializa o sistema no modo de segurança e, posteriormente libera o ransomwares. A utilização de modo de segurança pode garantir que o payload desative produtos de seguranças de endpoint e criptografa arquivos reiniciando os sistemas comprometidos.

3. **O uso da varredura LAN assíncrona para identificar os protocolos DFS (Distributed File System) e Server Message Block (SMB)** permitirá que eles executem movimentação lateral, ganhar persistência e evitar a detecção.

4. **Utilização de criptografia compartilhada** envolve uma única chave de criptografia para criptografar todos os arquivos em uma rede ou sistema, em vez de usar uma chave exclusiva para cada arquivo. Permite que o invasor acelere a criptografia para criptografar grandes conjuntos de dados.

5. **Serviço integrado para garantir o anonimato das transações de Bitcoin.**

6. Possui **suporte e atuação com Windows Desktop XP – 11, Windows Server 2003 – 2022, Linux** (incluindo Ubuntu e distribuições baseadas em Debian) e **VMware ESXi**.

Além das características mencionadas, o ransomwares possui outros detalhes, como:

- Suporte para configuração da sua ação por meio de argumentos:
  - Ignore: ignorado e nenhuma criptografia é necessária.
  - Fast: Criptografia apenas do início do arquivo, oferecendo rápida criptografia.
  - Strong: Criptografia completa do arquivo.
  - Balanced: Criptografia rápida e segura do arquivo por pontos.

Quanto ao apoio ao afiliado, o programa oferece os seguintes recursos para a sua operação:

- O painel do administrador está hospedado no Tor e possui finalidades automatizadas.
- O site de vazamento totalmente automatizado está hospedado no Tor com automação total.
- Capacidade de criar chats privados para comunicação secreta com empresas de Recuperação.
- Capacidade de gerar compilações com diferentes configurações e uma chave.
- Facilidade para construir seu próprio suporte no chat.
- Fornece suporte 24 horas por dia, 7 dias por semana.
- Mensagens de prompt para persuadir a vítima a responder à mensagem.
- Carta de convidado para acesso a bate-papos de destino para provedores de rede e parceiros.

O afiliado, após se movimentar lateralmente pela rede, ele criptografa os arquivos e exige um resgate e, caso o resgate não seja pago, os criminosos frequentemente venderão os dados roubados ou publicação os dados em blogs.

A operação do NoEscape oferece ainda um serviço para DDoS/Spam por meio de USD 500.000, podendo ser aproveitado como uma técnica de extorsão adicional para ameaçar e pressionar empresas-alvo para pagamentos.

Por meio de pesquisa em fontes abertas, foi identificada uma análise realizada pela TrendMicro sobre um arquivo malicioso em 29 de março de 2023, o qual foi despejado por meio de outro malware baixado por um usuário ao visitar sites suspeitos.

3 ATUALIZAÇÃO DA OPERAÇÃO

Após os detalhes acima serem capturados, foi possível obter informações adicionais por meio do pesquisador EVIL RABBIT que publicou no twitter uma imagem do painel usado pelo grupo de ransomwares **NoEscape**.

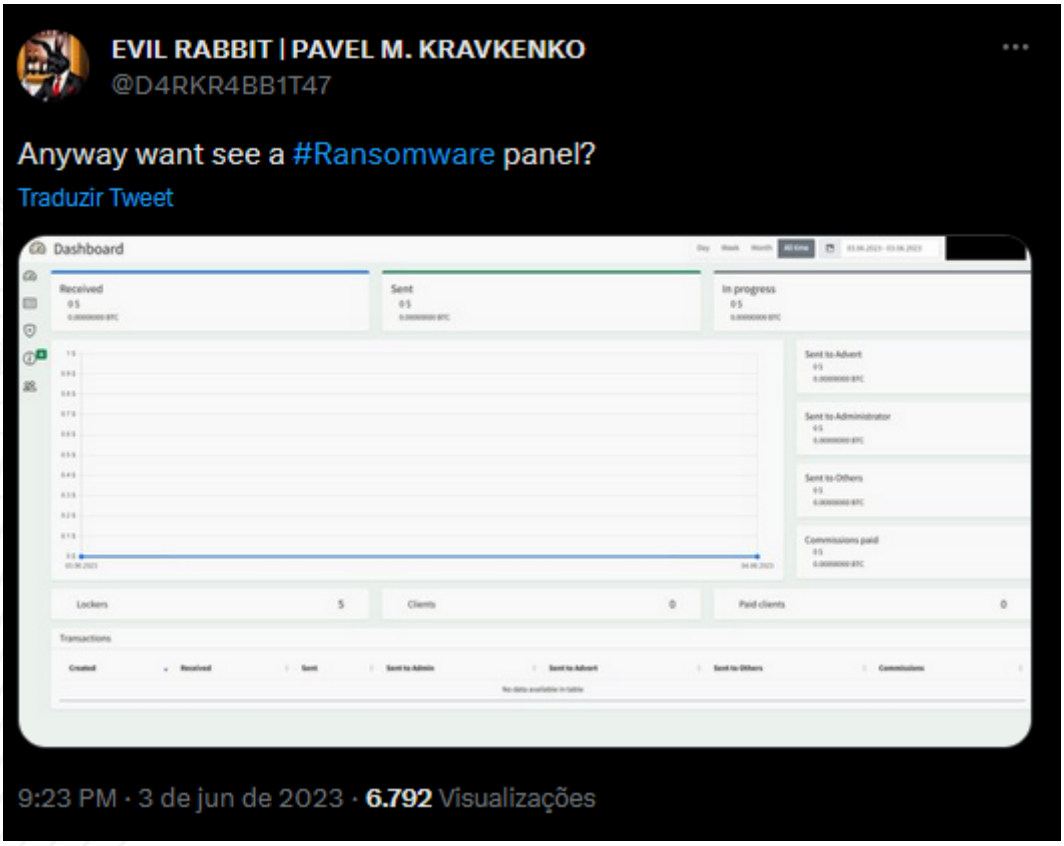


Figura 2 – Publicação via Twitter do pesquisador EVIL RABBIT.

Além de compartilhar detalhes do painel, é possível verificar ainda amostras associadas a essa família de ransomwares. O afiliado do ransomwares possui uma opção para criação de ransomwares em formatos .exe e .dll, para Windows 7 ou superior, injeção reflexiva de DLL para Windows 7 e superior, arquivos executáveis para Windows XP e executáveis ELF para servidores Linux/ESXi.

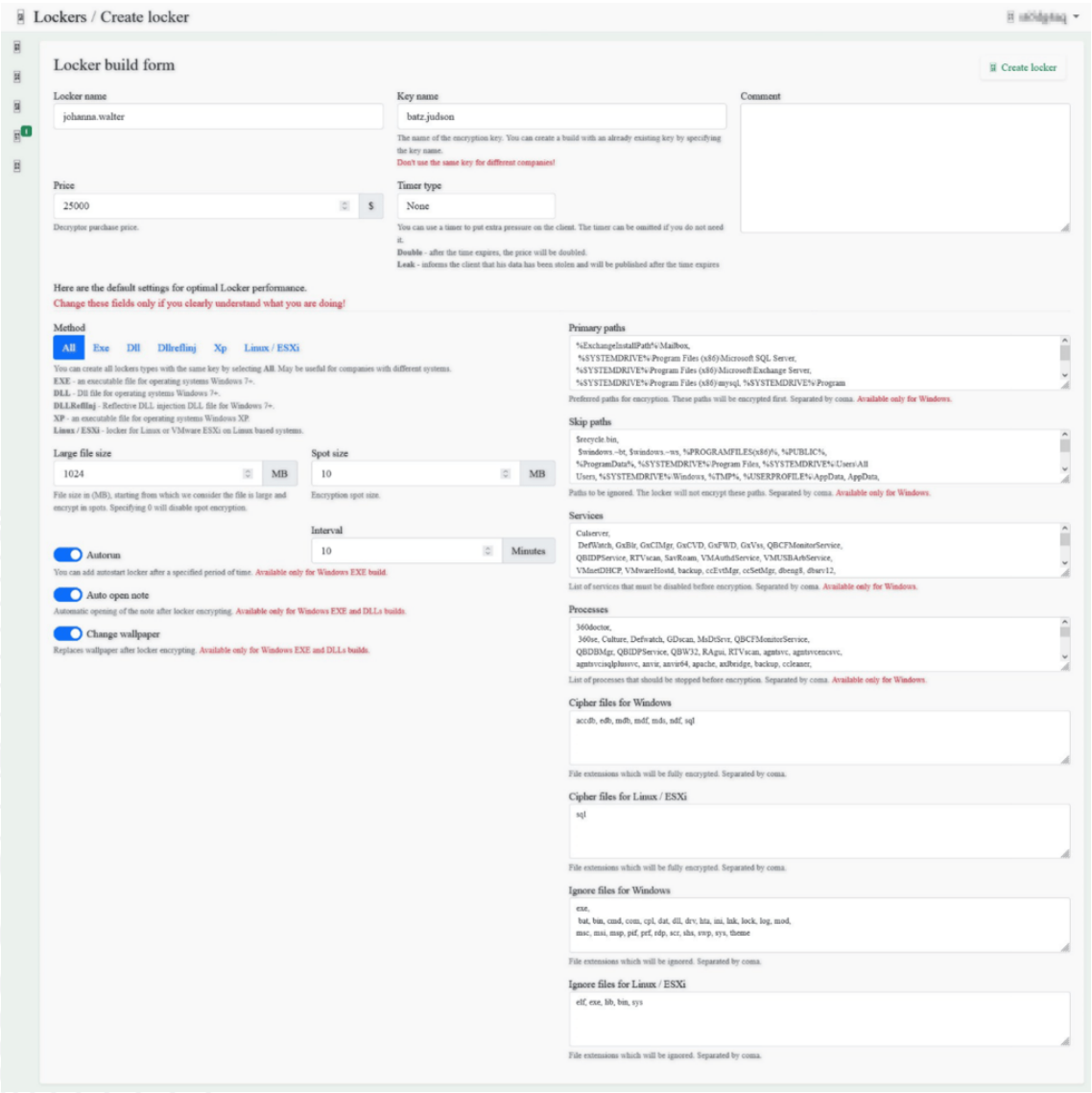


Figura 3 – Print da tela de builder do Ransomware NoEscape.

A referida página de criador do ransomware permite que os afiliados definam várias configurações para criar os executáveis do ransomwares, incluindo especificar o tamanho de arquivos grandes nos quais a criptografia é aplicada em vez de criptografar o arquivo inteiro e outros detalhes.

4 ANÁLISE TÉCNICA

A análise do arquivo executável do Ransomware é possível observar que é um ransomwares baseado em 32 bits em GUI escrito e compilado no Microsoft Visual C/C++.

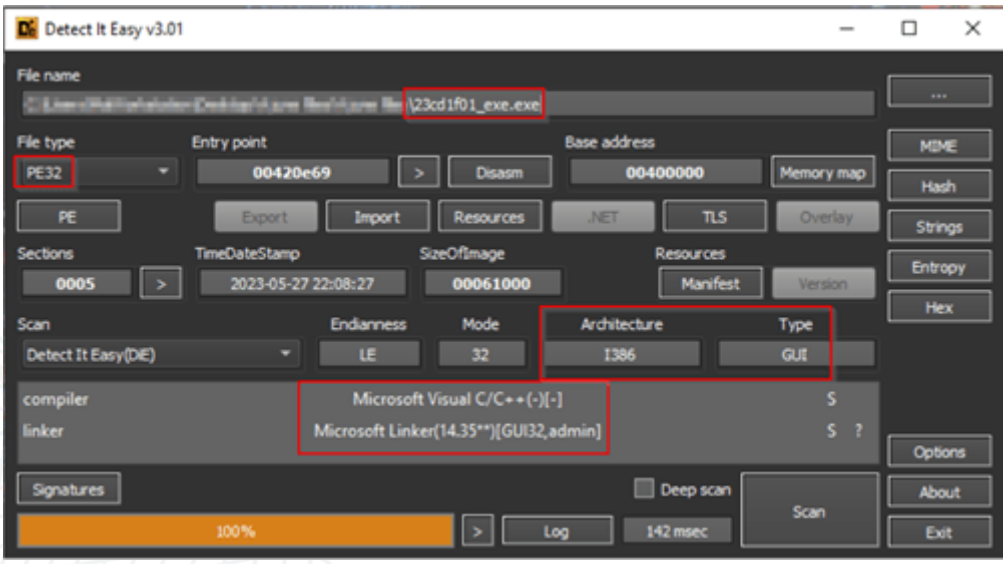


Figura 4 – Detalhes do arquivo PE.

Após a execução, o ransomwares cria um mutex denominado **"Global\\{ *5d202e6e-b33a-4833-abfb-2391bc075089}"*** para garantir que apenas uma única instância do malware esteja em execução no sistema da vítima.

O Ransomware, após criar o Mutex ele realiza a modificação dos valores de registro específicos para desabilitar o Controle de Acesso do Usuário (UAC), um recurso de segurança do Windows.

Lembrando que o UAC solicita aos usuários permissão ou credenciais de administrador antes de permitir ações que possam afetar as configurações ou arquivos do sistema.

Logo, ele realiza a modificação do valor de registro **"EnableLUA"** abaixo para **"0",** onde o malware desativa o Controle de Conta de Usuário (UAC) no sistema de destino.

- `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\EnableLUA = "0"`

A chave **“ConsentPromptBehaviorAdmin”** foi definida como **“0”**, indicando que o comportamento do prompt de consentimento para ações que exigem privilégios de administrador foi modificado. Por padrão, esse valor geralmente é definido como “1”. O prompt de consentimento serve para solicitar confirmação ou credenciais de administrador do usuário antes de permitir que a ação prossiga.

- `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\ConsentPromptBehaviorAdmin = “0”`

O Ransomware ainda realiza o encerramento de vários **processos** e **serviços**, como:

```
"kill_processes":
["360doctor","360se","Culture","Defwatch","GDscan","MsDtSrvr",
"QBCFMonitorService","QBDBMgr","QBIDPService","QBW32","RAgui",
"RTVscan","agntsvc","agntsvcencsvc","agntsvcisqlplussvc","anvi
r","anvir64","apache","axlbridge","backup","ccleaner","ccleane
r64","dbeng50","dbsnmp","encsvc","excel","far","fdhost","fdlau
ncher","httpd","infopath","isqlplussvc","java","kingdee","msac
cess","msftesql","mspub","mydesktopqos","mydesktopservice","my
sqld-nt","mysqld-opt","mysqld","ncsvc","ocautoupds","ocomm","o
cssd","onedrive","onenote","oracle","outlook","powerpnt","proc
exp","qbupdate","sqbcoreservice","sql","sqlagent","sqlbrowser"
,"sqlmangr","sqlserver","sqlservr","sqlwriter","steam","superv
ise","synctime","taskkill","tasklist","tbirdconfig","thebat","
thunderbird","tomcat","tomcat6","u8","ufida","visio","wdswfsaf
e","winword","wordpad","wuauclt","wxServer","wxServerView","xf
ssvccon"]
```

Figura 5 – Processos encerrados pelo ransomware.

```
"kill_services":
["Culserver","DefWatch","GxBlr","GxCIMgr","GxCVD","GxFWD","GxV
ss","QBCFMonitorService","QBIDPService","RTVscan","SavRoam","V
MAuthdService","VMUSBArbService","VMnetDHCP","VMwareHostd","ba
ckup","ccEvtMgr","ccSetMgr","dbeng8","dbsrv12","memtas","mepoc
s","msexchange","msmdsrv","sophos","sql","sqladhlp","sqlagent"
,"sqlbrowser","sqlservr","sqlwriter","svc$","tomcat6","veeam",
"vmware-converter","vmware-usbarbitator64","vss"]
```

Figura 6 – Serviços encerrados pelo ransomware.

Antes de realizar a criptografia dos dados, o ransomwares utiliza as funções API **FindFirstVolumeW()** e **FindNextVolumeW()** para pesquisar e identificar volumes acessíveis no sistema de destino. Na sequência, o malware despeja a nota de resgate chamada **"HOW_TO_RECOVER_FILES.txt"** em vários diretórios.

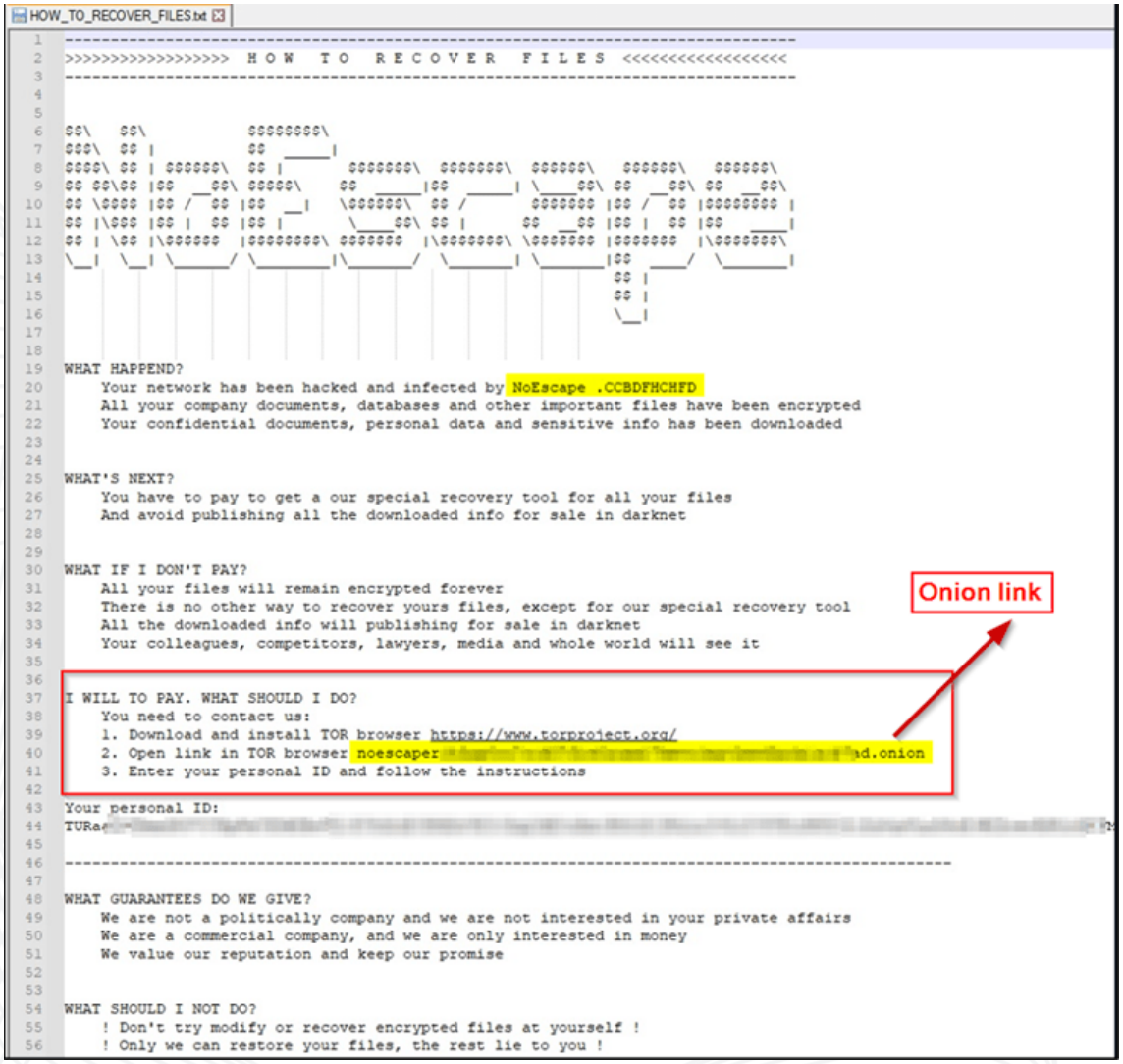


Figura 7 – Nota de resgate do Ransomware.

O Ransomware não realiza a criptografia nas extensões dos arquivos abaixo, bem como nos diretórios e a seguir:

```
"ignore":
["exe","bat","bin","cmd","com","cpl","dat","dll","drv","hta","
ini","lnk","lock","log","mod","msc","msi","msp","pif","prf","r
dp","scr","shs","swp","sys","theme"]

"skip":
["$recycle.bin","$windows.~bt","$windows.~ws","%PROGRAMFILES(
x86)%","%PUBLIC%","%ProgramData%","%SYSTEMDRIVE%\\Program
Files","%SYSTEMDRIVE%\\Users\\All Users","%SYSTEMDRIVE%\\Windo
ws","%TMP%","%USERPROFILE%\\AppData","AppData","%AppData%","EF
I","Intel","MSOCache","Mozilla","Program
Files","ProgramData","Tor Browser","Windows","WINDOWS","boot",
"google","perflogs","system volume
information","windows.old"],
```

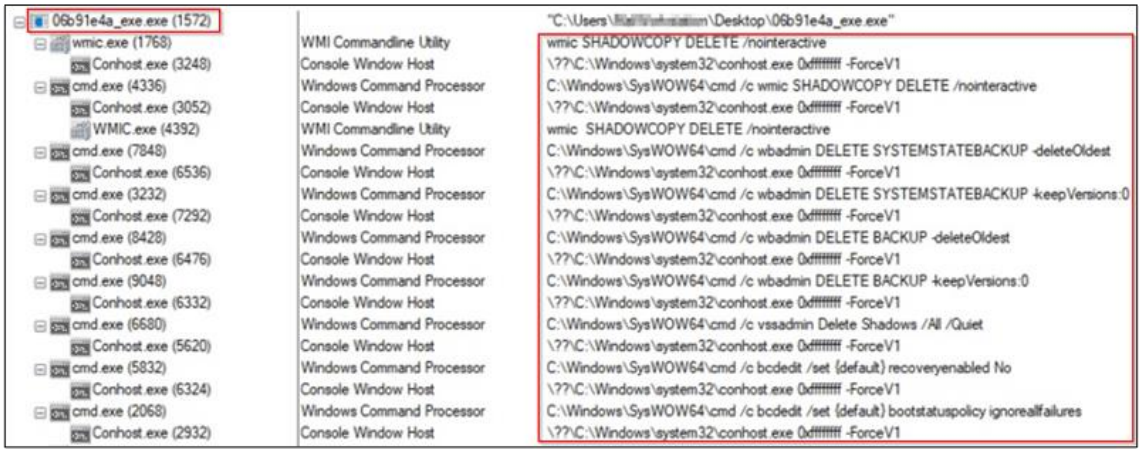
Figura 8 – Arquivos e pastas que não são criptografados.

Após a criptografia, o ransomwares altera o nome dos arquivos, adicionando a extensão **“.CCBDFHCHFD”.**

Para prejudicar a recuperação do sistema, o ransomwares executa uma série de comandos para excluir as cópias de sombras e backups do sistema por meio dos comandos:

- `wmic SHADOWCOPY DELETE /nointeractive`
- `wbadmin DELETE SYSTEMSTATEBACKUP -deleteOldest`
- `wbadmin DELETE SYSTEMSTATEBACKUP -keepVersions:0`
- `wbadmin DELETE BACKUP -deleteOldest`
- `wbadmin DELETE BACKUP -keepVersions:0`
- `vssadmin Delete Shadows /All /Quiet`
- `bcdedit /set {default} recoveryenabled No`
- `bcdedit /set {default} bootstatuspolicy ignoreallfailures`

Como exemplo, ilustra a sequência de comandos executados pelo NoEscape Ransomware:



06b91e4a_exe.exe (1572)		"C:\Users\[redacted]\Desktop\06b91e4a_exe.exe"
wmic.exe (1768)	WMI Commandline Utility	wmic SHADOWCOPY DELETE /nointeractive
Conhost.exe (3248)	Console Window Host	\??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
cmd.exe (4336)	Windows Command Processor	C:\Windows\SysWOW64\cmd /c wmic SHADOWCOPY DELETE /nointeractive
Conhost.exe (3052)	Console Window Host	\??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
WMIC.exe (4392)	WMI Commandline Utility	wmic SHADOWCOPY DELETE /nointeractive
cmd.exe (7848)	Windows Command Processor	C:\Windows\SysWOW64\cmd /c wbadmin DELETE SYSTEMSTATEBACKUP -deleteOldest
Conhost.exe (6536)	Console Window Host	\??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
cmd.exe (3232)	Windows Command Processor	C:\Windows\SysWOW64\cmd /c wbadmin DELETE SYSTEMSTATEBACKUP -keepVersions:0
Conhost.exe (7292)	Console Window Host	\??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
cmd.exe (8428)	Windows Command Processor	C:\Windows\SysWOW64\cmd /c wbadmin DELETE BACKUP -deleteOldest
Conhost.exe (6476)	Console Window Host	\??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
cmd.exe (9048)	Windows Command Processor	C:\Windows\SysWOW64\cmd /c wbadmin DELETE BACKUP -keepVersions:0
Conhost.exe (6332)	Console Window Host	\??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
cmd.exe (6680)	Windows Command Processor	C:\Windows\SysWOW64\cmd /c vssadmin Delete Shadows /All /Quiet
Conhost.exe (5620)	Console Window Host	\??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
cmd.exe (5832)	Windows Command Processor	C:\Windows\SysWOW64\cmd /c bcdedit /set {default} recoveryenabled No
Conhost.exe (6324)	Console Window Host	\??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
cmd.exe (2068)	Windows Command Processor	C:\Windows\SysWOW64\cmd /c bcdedit /set {default} bootstatuspolicy ignoreallfailures
Conhost.exe (2932)	Console Window Host	\??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1

Figura 9 – Arvore de processos do Ransomware.

Vale salientar, que o Ransomware após a criptografia dos dados da organização, publica os dados através do seu site presente na rede Tor, como forma de extorsão para a organização vítima realizar o pagamento.

Figura 10 – Site de vazamento de dados do Ransomware na rede Tor.

5 TTPs – MITRE ATT&CK

Tática	Técnica	MITRE ATT&CK
Execution	User Execution	T1204
	System Services	T1569
Persistence	Boot or Logon Autostart Execution	T1547
Defense Evasion	Impair Defenses	T1562
	Impair Defenses: Safe Mode Boot	T1562.009
	Indicator Removal	T1070
Lateral Movement	Remote Services: SMB/ Windows Admin Shares	T1021.002
Impact	Inhibit System Recovery	T1490
	Data Encrypted for Impact	T1486
	Service Stop Service Stop	T1489
	Network Denial of Service	T1498

6 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:

- **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.

7 IoCs

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 Compromissos (IOCs) relacionadas a análise do(s) artefato(s) deste relatório.

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	e91f3fa192567ef5b7fb88847994a248
sha1:	02b1d9f82766a1641880060f8c1db94c9e94c6d9
sha256:	ddae4987dfc8fa45f03a363b64d3662a5dc9d71dcc70117a85a6bab9cee88525

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	989ae3d195203b323aa2b3adf04e9833
sha1:	31a45521bc672abcf64e50284ca5d4e6b3687dc8
sha256:	d30d7676a3b4c91b77d403f81748ebf6b8824749db5f860e114a8a204bca5b8f
File name:	NoEscape.exe

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	65f35ae4203cf5041a0aaa358dd3d74c
sha1:	ea1f7940271fc80d06b2f222506020b650ad41bc
sha256:	68e5caa3f0fd4adc595b1163bf0dd30ca621c5d7a6ad0a20dfa1968346daa3c8
File name:	1ce30fbd_dll.dll

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	9ea0d4448472cdeeb290e8006e8b1e9b
sha1:	30f71a24c15dd81965b12996a79d914acf4f169e
sha256:	2cd1ca52a5d404176f0ec7debeceb4ba3c95b139061f86ac971195b02d854b0c
File name:	06b91e4a_exe.exe

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	bd69a645fa69fd8d5ba56b9c3f468711
sha1:	12dc0a2de3ad30201107bfcb679de5acacf31e5c
sha256:	68ff9855262b7a9c27e349c5e3bf68b2fc9f9ca32a9d2b844f2265dccd2bc0d8
File name:	23cd1f01_exe.exe

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	c850f6816459e3364b2a54239642101b
sha1:	30c60f18279ed5fd36e3ac2d3ba5ddbdc5d1f624
sha256:	21162bbd796ad2bf9954265276bfebea8741596e8fe9d86070245d9b5f9db6da
File name:	164f8295_linux.elf

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	473d65d1231ccdfa0099d463b09cf9b9
sha1:	9cbc7417fa5ce2f6d87026337fc7892e4f485819
sha256:	07c70968c66c93b6d6c9a90255e1c81a3b385632c83f53f69534b3f55212ced9
File name:	bd83e75f_dllreflinj.dll

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	47ae17d89c2d9b6acdc7458f5df1c6f7
sha1:	d38c613020cb4616783c8535380e28404f7eaebf
sha256:	9d346518330eeefbf288aeca7b2b6243bc158415c7fee3f2c19694f0e5f7d51c
File name:	ca3ec998_xp.exe

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	34de9725e232ba82275bb0dcf9282e16
sha1:	b17403e7dcb992ba8d2b56dd843406264d3910e5
sha256:	aa5a487db37ce176e17c7abbb2b1d460ba926344e46737f2f64b65bf5a4a3e58
File name:	script_esxi.sh

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	17d55dc09e2a3f10d4ee45156c2c53f1
sha1:	317f296131b37a73c9a5d253015821dfdc8b1190
sha256:	16d9e969457a76874e7452e687a7b6843c65ef75d1a4404d369074ad389f6c38
File name:	script_linux.sh

8 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Trend Micro:**
  - **Ransomware NOESCAPE A**
  - **Ransomware NOESCAPE B**
- **AnyRun – Ransomware NoEscape**
- **Relatório Cyble – Ransomware NoEscape**

heimdall
security research

A DIVISION OF ISH