BOLETIM DE SEGURANÇA

Novo ransomware 3AM identificado

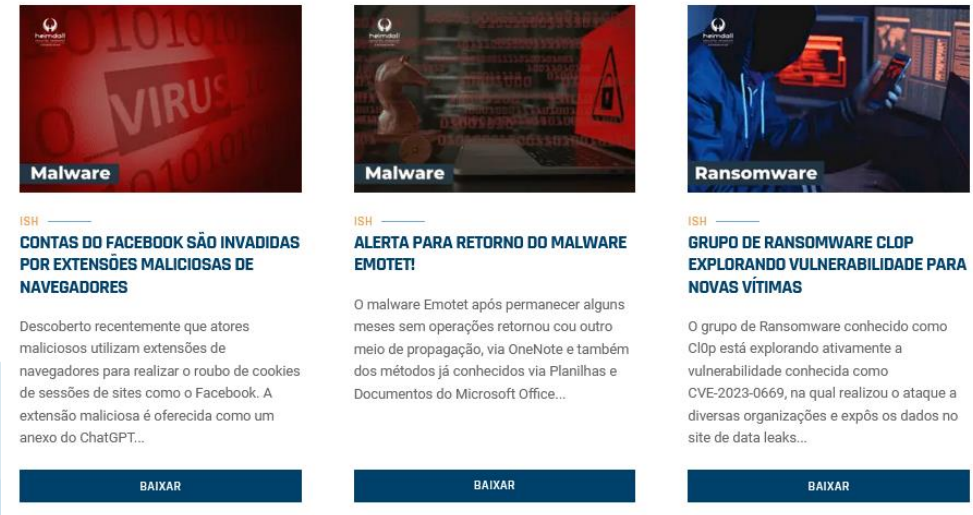
heimdall
security research
A DIVISION OF ISH

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 Tabelas

Lista de Figuras

1 SUMÁRIO EXECUTIVO

Uma nova família de Ransomware identificada pelo nome de "3AM". A operação do ransomware foi observada pela equipe da Symantec na qual um afiliado de ransomware tentou implantar outro ransomware, o LockBit na rede alvo e depois mudou para 3AM quando o LockBit teria sido bloqueado.

O novo ransomware foi escrito em Rust e aparentemente pode ser considerada uma família de ransomware nova.

De acordo com os pesquisadores, o ransomware tenta interromper vários serviços no computador infectado antes de começar a criptografar os arquivos e, após a criptografia ser concluída, ele tenta excluir as cópias do Volume Shadow (VSS).

2 DETALHES DO ATAQUE

De acordo com a Symantec, a primeira atividade suspeita do agente da ameaça envolveu o uso do comando "gpresult" para despejar as configurações de políticas aplicadas no computador para um usuário específico. O invasor também executou vários componentes do Cobalt Strike e tentou elevar privilégios no computador utilizando o PsExec.

Os atores então executaram comandos de reconhecimento como "whoami", "netuser", "quser" e "net share", bem como tentaram aenumerar outros servidores para movimento lateral com os comandos "quser" e "net view".

Para fins de persistência, os atores adicionaram um novo usuário para persistência e usaram a ferramenta "Wput" para exfiltrar os arquivos das vítimas para seu próprio servidor FTP.

Os invasores primeiro tentaram usar o ransomware LockBit, mas quando ele foi bloqueado, eles recorreram ao ransomware 3AM. O uso do ransomware foi de acordo com a Symantec, parcialmente bem-sucedido, já que conseguiram implantar apenas em três máquinas na rede da organização.

3 ANÁLISE DO RANSOMWARE 3AM

O ransomware levou este nome porque após a criptografia anexa as extensão ".threeamtime", apresentando a nota de resgate com o seguinte conteúdo:

```
Hello. "3 am" The time of mysticism, isn't it?

All your files are mysteriously encrypted, and the systems "show no signs of life", the backups disappeared. But
we can correct this very quickly and return all your files and operation of the systems to original state.

All your attempts to restore data by himself will definitely lead to their damage and the impossibility of
recovery. We are not recommended to you to do it on our own!!! (or do at your own peril and risk).

There is another important point: we stole a fairly large amount of sensitive data from your local network:
financial documents; personal information of your employees, customers, partners; work documentation, postal
correspondence and much more.

We prefer to keep it secret, we have no goal to destroy your business. Therefore can be no leakage on our part.

We propose to reach an agreement and conclude a deal.

Otherwise, your data will be sold to DarkNet/DarkWeb. One can only guess how they will be used.

Please contact us as soon as possible, using Tor-browser:

http://threeam7[REDACTED].onion/recovery

Access key:

[32 CHARS SPECIFIED BY -k COMMAND LINE PARAMETER]
```

Figura 1 – Nota de resgate do Ransomware 3AM.

O Ransomware é um executável de 64 bits escrito em Rust e reconhece e recebe parâmetros de linha de comando:

- **-k:** 32 caracteres Base64, referidos como "chave de acesso" na nota de resgate.
- **-p:** Desconhecido
- **-h:** Desconhecido
- **-m:** Método, onde o código verifica um dos dois valores antes de executar a lógica da criptografia.
  - local
  - net
- **-s:** Determina compensações nos arquivos para criptografia para controlar a velocidade da criptografia. Isso é expresso na forma de dígitos decimais.

Os parâmetros de linha de comando "-m" e "-h" são mutuamente exclusivos e, a utilização dos parâmetros **"local" e "net"** são argumentos utilizados pelo grupo de ransomware **Conti**.

Quando executado, o ransomware tenta executar os seguintes comandos:

```
"netsh.exe" advfirewall firewall set rule "group=”Network Discovery”" new enable=Yes
"wbadmin.exe" delete systemstatebackup -keepVersions:0 -quiet
"wbadmin.exe" DELETE SYSTEMSTATEBACKUP
"wbadmin.exe" DELETE SYSTEMSTATEBACKUP -deleteOldest
"bcdedit.exe" /set {default} recoveryenabled No
"bcdedit.exe" /set {default} bootstatuspolicy ignoreallfailures
"wmic.exe" SHADOWCOPY DELETE /nointeractive
"cmd.exe" /c wevtutil cl security
"cmd.exe" /c wevtutil cl system
"cmd.exe" /c wevtutil cl application
"net" stop /y vmcomp
"net" stop /y vmwp
"net" stop /y veeam
"net" stop /y Back
"net" stop /y xchange
"net" stop /y backup
"net" stop /y Backup
"net" stop /y acronis
"net" stop /y AcronisAgent
"net" stop /y AcrSch2Svc
"net" stop /y sql
"net" stop /y Enterprise
"net" stop /y Veeam
"net" stop /y VeeamTransportSvc
"net" stop /y VeeamNFSSvc
"net" stop /y AcrSch
"net" stop /y bedbg
"net" stop /y DCAgent
"net" stop /y EPSecurity
"net" stop /y EPUpdate
"net" stop /y Eraser
"net" stop /y EsgShKernel
```

```
"net" stop /y FA_Scheduler
"net" stop /y IISAdmin
"net" stop /y IMAP4
"net" stop /y MBAM
"net" stop /y Endpoint
"net" stop /y Afee
"net" stop /y McShield
"net" stop /y task
"net" stop /y mfemms
"net" stop /y mfevtp
"net" stop /y mms
"net" stop /y MsDts
"net" stop /y Exchange
"net" stop /y ntrt
"net" stop /y PDVF
"net" stop /y POP3
"net" stop /y Report
"net" stop /y RESvc
"net" stop /y Monitor
"net" stop /y Smcinst
"net" stop /y SmcService
"net" stop /y SMTP
"net" stop /y SNAC
"net" stop /y swi_
"net" stop /y CCSF
"net" stop /y ccEvtMgr
"net" stop /y ccSetMgr
"net" stop /y TrueKey
"net" stop /y tmlisten
"net" stop /y UIODetect
"net" stop /y W3S
"net" stop /y WRSVC
"net" stop /y NetMsmq
"net" stop /y ekrn
"net" stop /y EhttpSrv
"net" stop /y ESHASRV
```

```
"net" stop /y AVP
"net" stop /y klnagent
"net" stop /y wbengine
"net" stop /y KAVF
"net" stop /y mfefire
"net" stop /y svc$
"net" stop /y memtas
"net" stop /y mepocs
"net" stop /y GxVss
"net" stop /y GxCVD
"net" stop /y GxBlr
"net" stop /y GxFWD
"net" stop /y GxCIMgr
"net" stop /y BackupExecVSSProvider
"net" stop /y BackupExecManagementService
"net" stop /y BackupExecJobEngine
"net" stop /y BackupExecDiveciMediaService
"net" stop /y BackupExecAgentBrowser
"net" stop /y BackupExecAgentAccelerator
"net" stop /y vss
"net" stop /y BacupExecRPCService
"net" stop /y CASAD2WebSvc
"net" stop /y CAARCUpdateSvc
"net" stop /y YooBackup
"net" stop /y YooIT
```

O ransomware irá então verificar o disco e todos os arquivos que correspondam aos critérios predefinidos e serão em seguida, criptografados e os originais excluídos. O ransomware criará o arquivo **"RECOVER-FILES.txt"** em cada pasta verificada. Este arquivo contém a nota de resgate.

Após a criptografia, o malware tenta executar o seguinte comando para excluir cópias de backups de sombra de volume:

```
vssadmin.exe delete shadows /all /quiet
```

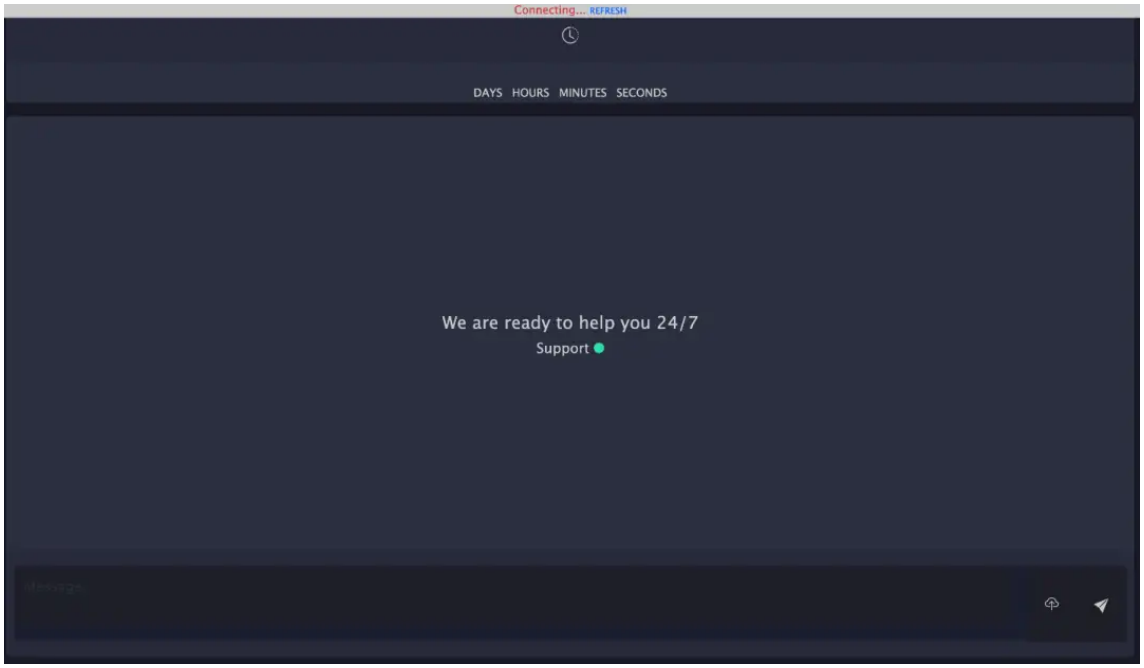


Figura 2 – Portal de conexão com o Ransomware 3AM.

A utilização de novas famílias de ransomware podem parecer frequentes, porém o que chamou a atenção dos pesquisadores foram de que o ransomware 3AM nunca foi utilizado, apenas quando o ransomware LockBit foi detectado este passou a utilizar outro.

4 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	
sha256:	079b99f6601f0f6258f4220438de4e175eb4853649c2d34ada72cce6b1702e22
sha256:	307a1217aac33c4b7a9cd923162439c19483e952c2ceb15aa82a98b46ff8942e
sha256:	680677e14e50f526cced739890ed02fc01da275f9db59482d96b96fbc092d2f4
sha256:	991ee9548b55e5c815cc877af970542312cff79b3ba01a04a469b645c5d880af
sha256:	ecbdb9cb442a2c712c6fb8aee0ae68758bc79fa064251bab53b62f9e7156febc

Tabela 1 – Indicadores de Compromissos de artefatos.

URLs de distribuição e endereços IP C2:

185.202.0[.]111
212.18.104[.]6
85.159.229[.]62

Tabela 2 – Indicadores de Compromisso de Rede

Obs: Os *links* e endereços IP elencados acima podem estar ativos; cuidado ao realizar a manipulação dos referidos IoCs, evite realizar o clique e se tornar vítima do conteúdo malicioso hospedado no IoC.

5 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Relatório Symantec – Ransomware 3AM**

heimdall
security research
A DIVISION OF ISH