
# BOLETIM DE SEGURANÇA

Grupos de Ransomware lançam ataques conjuntos em mais de 15 países

heimdall
security research
A DIVISION OF ISH

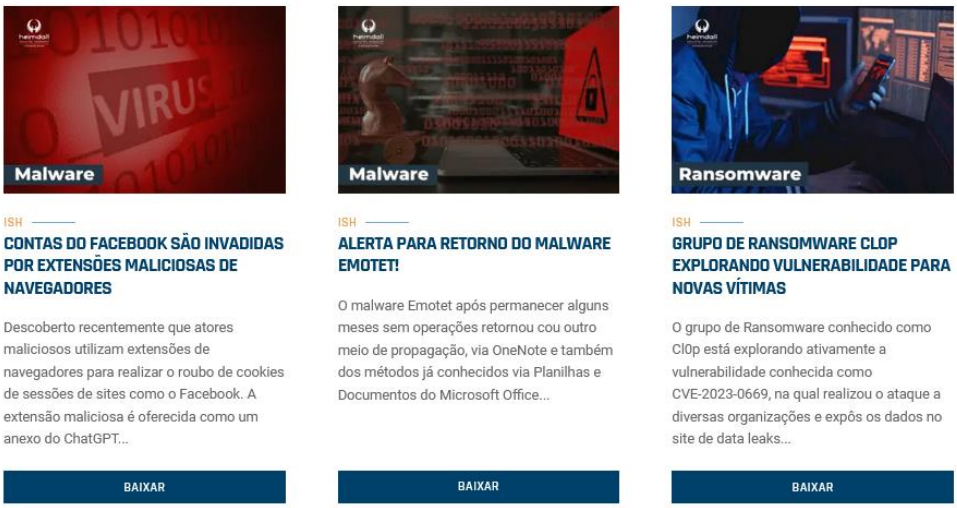
TLP: CLEAR

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

[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

A equipe da TALOS informou que os grupos de ransomware **GhostSec** e **Stormous** operando juntos para conduzir vários ataques de dupla extorsão usando os programas de ransomware **GhostLocker** e **StormousX** contra vítimas em países como, Cuba, Argentina, Polônia, China, Líbano, Israel, Uzbequistão, Índia, África do Sul, Brasil, Marrocos, Catar, Turquia, Egito, Vietnã, Tailândia e Indonésia, de acordo com a avaliação das mensagens de divulgação postadas pelo grupo em seus canais telegram e no site de vazamento de dados do ransomware Stormous.

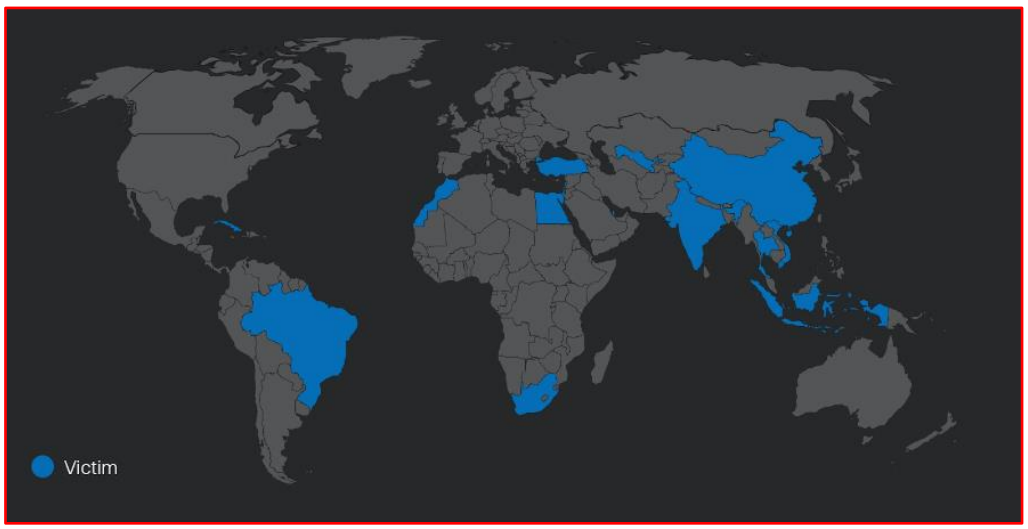



*Figura 1 – Países vítimas dos grupos.*

# 2 INFORMAÇÕES SOBRE O GRUPO

A Talos destacou os ataques contínuos do grupo aos sistemas industriais, infraestrutura crítica e empresas de tecnologia de Israel. Em 12 de novembro de 2023, alegaram que as organizações afetadas também incluíam o Ministério da Defesa Israelense.

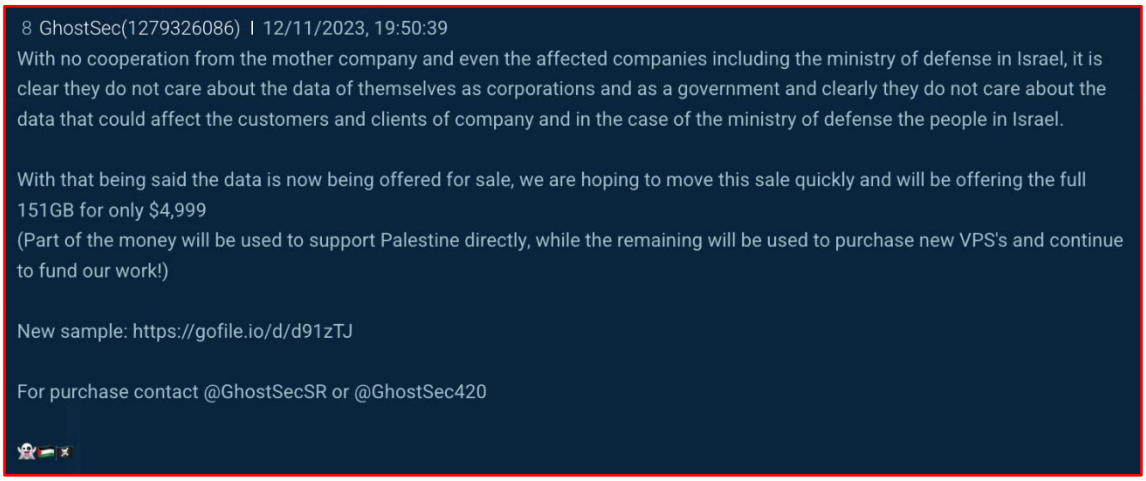



*Figura 2 – Exemplo de mensagens no telegram do Ghostsec.*

Esse grupo de hackers que afirma fazer parte de um grupo moderno de Cinco Famílias que inclui **ThreatSec**, **Stormous**, **Blackforums** e **SiegedSec** em seus canais como telegram. Suas motivações incluem setores financeiros, conduzindo ataques de extorsão simples e duplos contra vítimas em várias regiões geográficas. Eles também conduziram vários ataques de negação de serviço (DoS) e derrubaram sites de vítimas, de acordo com mensagens do canal telegram. Suas afirmações também nos mostraram que seu foco principal é arrecadar fundos para hacktivistas e atores de ameaças por meio de suas atividades cibercriminosas.

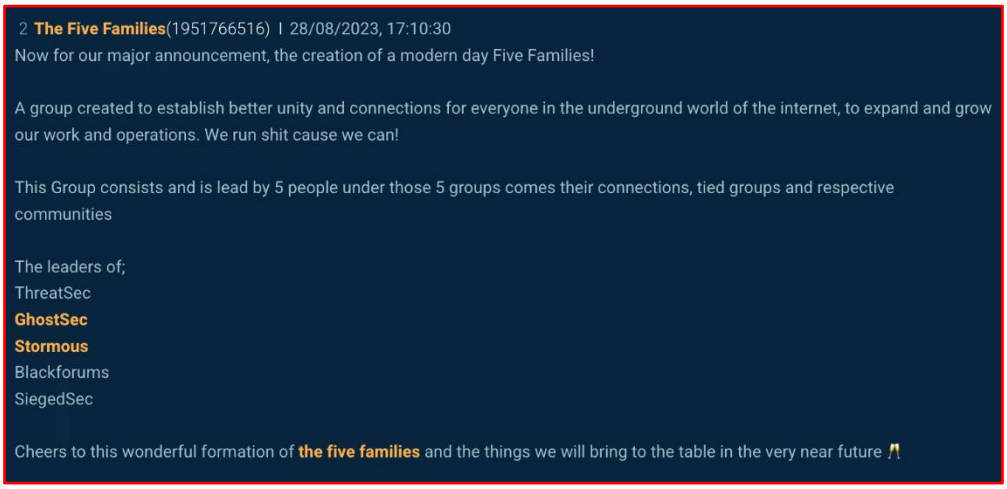



*Figura 3 – Famílias de grupos do telegram.*

Em outubro de 2023, GhostSec anunciou sua nova estrutura de *ransomware-as-a-service* (**RaaS**) chamada GhostLocker . Após suas operações colaborativas bem-sucedidas com o grupo de ransomware Stormous em julho de 2023 contra os ministérios cubanos, em 14 de outubro de 2023, o grupo Stormous anunciou que usaria o programa de ransomware GhostLocker além de seu programa StormousX.

O grupo compartilhou seus modelos de diagramas de fluxo de trabalho para afiliados e membros e não membros em seus canais do telegram.

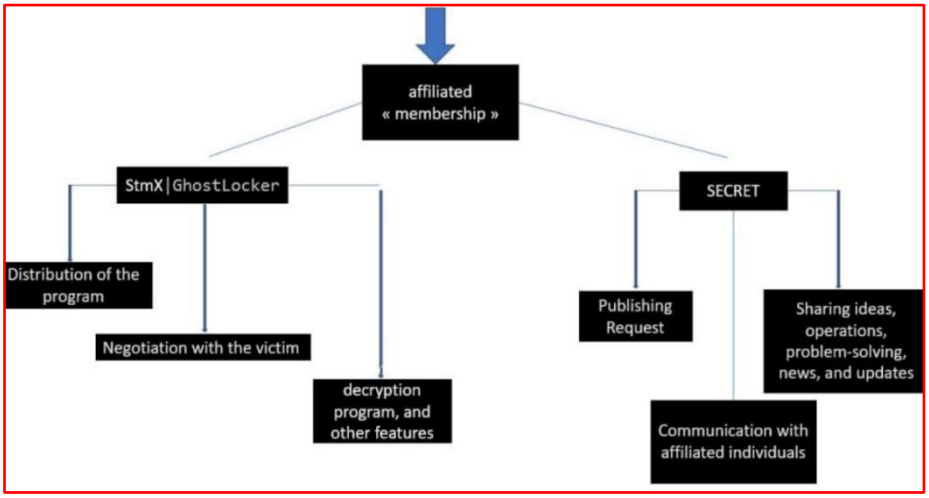



*Figura 4 – Modelo de trabalho de membros do Stmx_GhostLocker.*

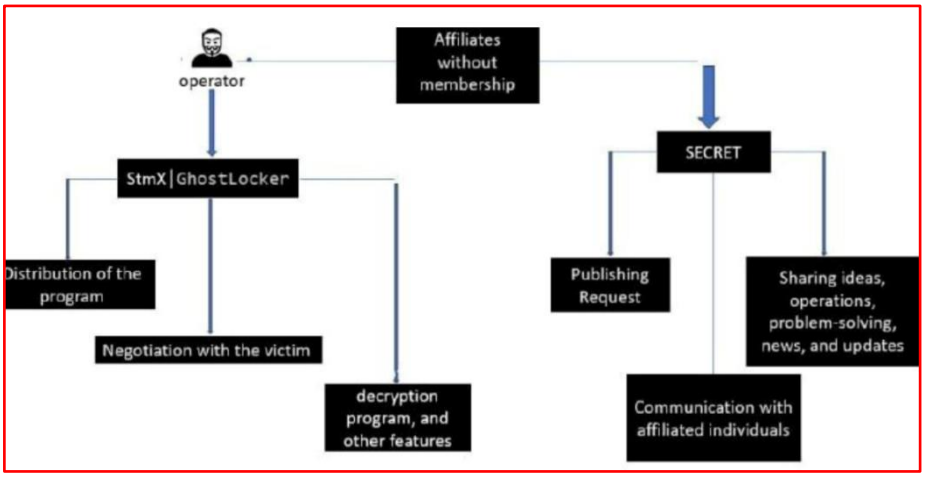



*Figura 5 – Modelo de trabalho de não membros do Stmx_GhostLocker.*

# 3 EVOLUÇÃO DO GRUPO

Em novembro de 2023, o grupo GhostSec anunciou a versão 2.0, de seu ransomware GhostLocker chamada GhostLocker 2.0. Recentemente, foi observado que suas operações começaram a anunciar sua versão mais recente do Golang, “GhostLocker 2.0”, chamando-a de “GhostLocker V2” e mencionando seu trabalho contínuo no GhostLocker V3, indicando sua evolução contínua no desenvolvimento de seu conjunto de ferramentas.

O GhostLocker 2.0 criptografa os arquivos na máquina da vítima usando a extensão de arquivo “. ghost” e descarta e abre uma nota de resgate. A nota de resgate mudou em relação à versão anterior, onde a operadora diz aos usuários para protegerem o ID de criptografia exibido na nota de resgate e compartilhá-lo com eles em seu serviço de bate-papo durante a negociação, clicando em “Clique em mim”. A operadora menciona ainda que os dados roubados da vítima serão divulgados caso ela não consiga contatá-la em sete dias.

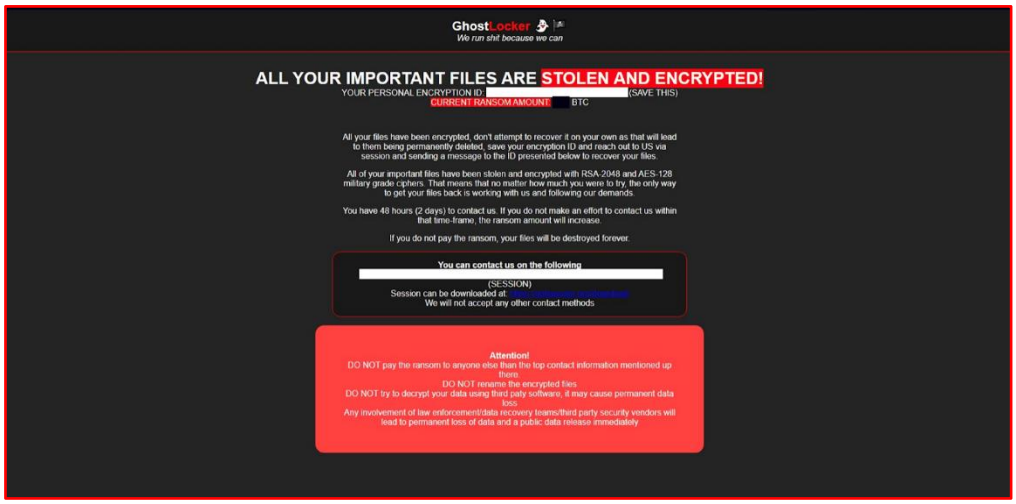



*Figura 6 – Nota de resgate do GhostLocker.*


*Figura 7 – Nota de resgate do GhostLocker 2.0*

O GhostLocker 2.0 procura os arquivos de destino na máquina da vítima de acordo com a lista de extensões de arquivo definida pelo autor e, antes que a rotina de criptografia seja iniciada, ele fará o upload dos arquivos de destino para o servidor C2 por meio da URL "**hxxp[://] 94[.]103[.]91[.]246[/]upload**" usando o método de postagem HTTP. O ator configurou o ransomware para exfiltrar e criptografar os arquivos que possuem extensões de arquivo **.doc**, **.docx**, **.xls** e **.xlsx**.


*Figura 8 – Função para exfiltrar arquivos para o servidor C2*

Após a exfiltração bem sucedida, o malware criptografa os arquivos alvo e anexa ". ghost" como a extensão dos arquivos criptografados. Durante o processo de criptografia, o malware ignora a pasta "C:\Windows". Após completar a rotina de criptografia, o ransomware insere a nota de resgate incorporada em um arquivo HTML com o nome de arquivo "Ransomnote.html" na área de trabalho da vítima e inicia usando o comando `Iniciar` do Windows.

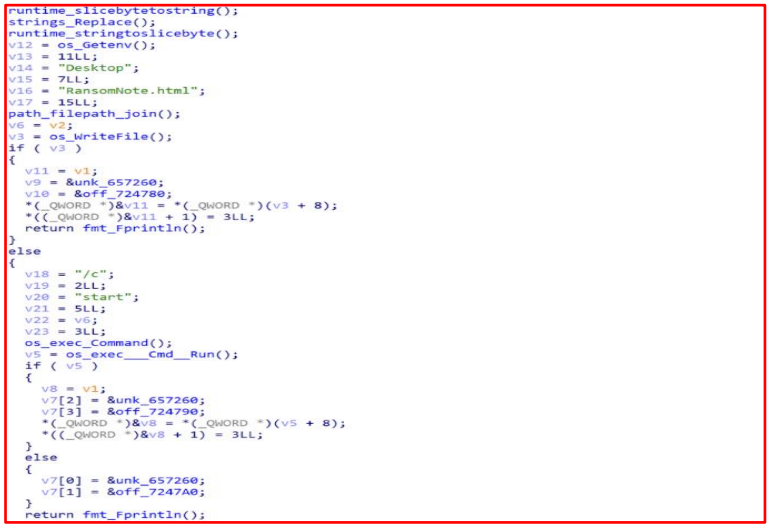



*Figura 9 – Função que abre a nota de resgate*

# 4 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:

**Autenticação Multifator (MFA)**

- Implemente MFA em todos os pontos de acesso remoto. Isso adiciona uma camada extra de segurança, exigindo mais do que apenas uma senha para autenticação.

**Senhas Fortes**

- Incentive o uso de senhas fortes e alterações regulares de senha. Senhas fracas são vulnerabilidades que os cibercriminosos podem explorar.

**Bloqueio Automático de Conta**

- Configure políticas de bloqueio automático de conta após várias tentativas de login malsucedidas. Isso ajuda a evitar ataques de força bruta.

**Listas de Conexões Permitidas**

- Crie listas de permissões de IPs usando firewalls. Isso restringe o acesso apenas a endereços IP confiáveis.

**Backup Regular e Criptografado**

- Mantenha backups regulares de seus dados importantes. Certifique-se de que esses backups sejam criptografados e armazenados offline para evitar que ransomwares os afetem.

**Atualizações de Software**

- Mantenha seus programas e sistemas operacionais atualizados com as versões mais recentes. Isso ajuda a corrigir vulnerabilidades conhecidas.

**Conscientização dos Colaboradores**

- Eduque seus funcionários sobre práticas seguras de navegação na web, phishing e como identificar ameaças. A conscientização é fundamental para evitar ataques de spearphishing.

**Teste Constante de Backups**

- Verifique regularmente se seus backups estão funcionando corretamente e se você pode restaurar os dados quando necessário.

# 5 INDICADORES DE COMPROMISSOS

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 do artefato | |
|---|---|
| **md5:** | f001329114937fbc439f251c803ba825 |
| **sha1:** | 95ae81de52655fac3f1b226f1896690566090640 |
| **sha256:** | a1b468e9550f9960c5e60f7c52ca3c058de19d42eafa760b9d5282eb24b7c55f |
| ***File name:*** | 9Q38eDOocR4AHEY2Ewkjc8OWNwlxGN5R.exe |

| Indicadores de compromisso do artefato | |
|---|---|
| **md5:** | 8ad67a1b7a5f2428c93f7a13a398e39c |
| **sha1:** | d4f71fc5479a02c8ff57c90fc67b948adb5604e0 |
| **sha256:** | 8b758ccdfbfa5ff3a0b67b2063c2397531cf0f7b3d278298da76528f443779e9 |
| ***File name:*** | qCjSIzgTycC9WKT4KfnzGoXbAB4udBU7.exe |

Tabela 1 – Indicadores de Compromissos de artefatos

### Indicadores de URL, IPs e Domínios

| Indicadores de URL, IPs e Domínios | |
|---|---|
| **URL** | hxxp[://]94[.]103[.]91[.]246/incrementLaunch<br>hxxp[://]94[.]103[.]91[.]246/addInfection<br>hxxp[://]94[.]103[.]91[.]246/victimchat?id=[EncryptionID]<br>hxxp[://]94[.]103[.]91[.]246/login?next=<br>hxxp[://]94[.]103[.]91[.]246/upload |
| **IP** | 94[.]103[.]91[.]246 |

Tabela 2 – Indicadores de Compromissos 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.

# 6 REFERÊNCIAS


- **Heimdall *by* ISH Tecnologia**
- Ciscotalos
- Thehackernews

heimdall
security research
A DIVISION OF ISH