



# BOLETIM DE SEGURANÇA

**Campanha LockBit Black associada a botnet Phorpiex  
disparando milhões de e-mails de ransomware**



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](#)



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 VÍTIMAS

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	Sumário Executivo .....	6
2	Informação sobre a ameaça .....	7
3	Recomendações.....	9
4	Indicadores de Compromissos .....	10
5	Referências .....	11
6	Autores.....	12

## LISTA DE TABELAS

Tabela 1 – Indicadores de Compromissos de Rede..... 10

## LISTA DE FIGURAS

<i>Figura 1 – Exemplo de e-mail de phishing.....</i>	<i>7</i>
<i>Figura 2 – Nota de resgate LockBit Black.....</i>	<i>8</i>

## 1 SUMÁRIO EXECUTIVO

---

O centro de pesquisa da NJCCIC identificou o surgimento de uma campanha maliciosa denominada LockBit Black disparando milhões de e-mails maliciosos. Esta nova onda de ataques usando o LockBit Black representa uma ameaça cibernética emergente.



## 2 INFORMAÇÃO SOBRE A AMEAÇA

Relatórios de incidentes e análises de centros especializados informaram ao NJCCIC sobre a campanha LockBit Black e identificando que e-mails associados a esta campanha incluem anexos ZIP prejudiciais e utilizam consistentemente os endereços “JennyBrown3422[.]gmail[.]com” e “Jenny[.]gsd[.]com” como remetente.

O anexo ZIP contém uma carga executável compactada que, se executada, criptografará o sistema operacional com o ransomware LockBit Black. As instâncias observadas associadas a esta campanha foram acompanhadas pela botnet Phorpiex (TriK), que entregou a carga útil do ransomware. Foram identificados mais de 1.500 endereços IP de envio exclusivos, muitos dos quais foram geolocalizados no Cazaquistão, Uzbequistão, Irã, Rússia, China e outros países. Os IPs identificados que hospedam executáveis LockBit foram 193[.]233[.]132[.]177 e 185[.]215[.]113[.]66. As linhas de assunto incluíam “your document” e “your photo”.

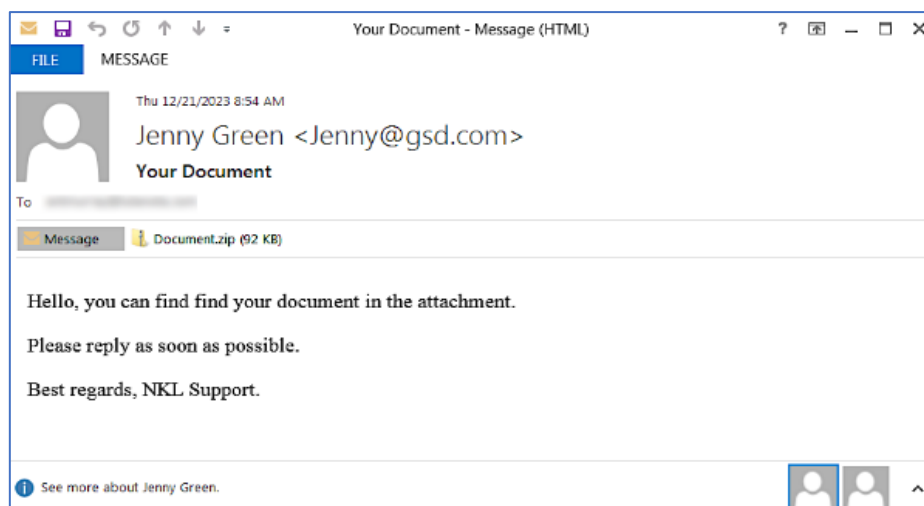
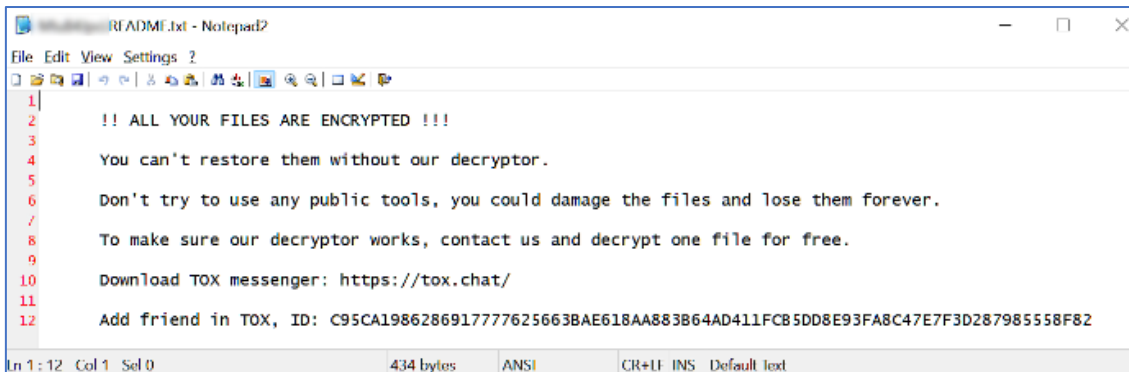


Figura 1 – Exemplo de e-mail de phishing.

A técnica utilizada não é inédita, mas a quantidade massiva de e-mails distribuindo malware e o emprego do ransomware LockBit Black como a primeira fase da carga maliciosa conferem notoriedade à estratégia, apesar de não possuir a complexidade de outros ataques virtuais. Os especialistas da Proofpoint detectaram, a partir de abril de 2024, e por aproximadamente uma semana, uma série de campanhas de grande escala, com milhões de e-mails propagados pelo botnet Phorpiex, que disseminavam o ransomware LockBit Black.

Segundo os pesquisadores, essa foi a primeira ocasião em que se observou o ransomware LockBit Black, também referido como LockBit 3.0, sendo distribuído através do Phorpiex em uma escala tão ampla.



```
1 |
2 |      !! ALL YOUR FILES ARE ENCRYPTED !!!
3 |
4 |      You can't restore them without our decryptor.
5 |
6 |      Don't try to use any public tools, you could damage the files and lose them forever.
7 |
8 |      To make sure our decryptor works, contact us and decrypt one file for free.
9 |
10 |     Download TOX messenger: https://tox.chat/
11 |
12 |     Add friend in TOX, ID: C95CA1986286917777625663BAE618AA883B64AD411FCB5DD8E93FA8C47E7F3D287985558F82
```

Figura 2 – Nota de resgate LockBit Black.

Inicialmente, disseminava-se via dispositivos USB e mensageiros como Skype e Windows Live Messenger, evoluindo para um trojan de IRC que distribuía spam por e-mail. Com um crescimento gradual, o Phorpiex alcançou a marca de controlar mais de um milhão de dispositivos infectados. Após anos em operação, os responsáveis tentaram comercializar o código-fonte do malware em fóruns especializados, após desativarem sua infraestrutura. Além disso, foi empregado na distribuição de milhões de e-mails de sextortion, atingindo mais de 30.000 e-mails por hora, e recentemente adotou um módulo para alterar endereços de carteiras de criptomoedas na área de transferência do Windows, substituindo-os por endereços de atacantes.



### 3 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:

#### **Varredura de e-mail**

- Utilize filtros de e-mail para detectar e bloquear mensagens de phishing enviadas por membros infectados da botnet.

#### **Treinamento de conscientização sobre segurança**

- Eduque os funcionários sobre como identificar e-mails maliciosos, incluindo phishing, extorsão e spam.

#### **Implementação de segurança ativa**

- Garanta a implementação de soluções de segurança que impeçam ativamente a infecção de redes por malwares.

#### **Cautela com anexos desconhecidos**

- Seja cauteloso ao abrir anexos em e-mails, mesmo que pareçam vir de uma fonte confiável.

#### **Políticas de acesso**

- Adote o princípio do menor privilégio, garantindo que os usuários tenham apenas o acesso necessário para realizar suas tarefas.
- Implemente MFA em todas as contas e sistemas críticos para adicionar uma camada extra de proteção.

#### **Patching e atualizações**

- Mantenha todos os sistemas e softwares atualizados com os patches de segurança mais recentes para corrigir vulnerabilidades conhecidas.
- Utilize ferramentas de gestão de patches para automatizar o processo de atualização e reduzir a exposição a vulnerabilidades.

#### **Segmentação de rede**

- Separe segmentos de rede para limitar a movimentação lateral do ransomware em caso de comprometimento.
- Utilize VPNs seguras para conexões remotas, garantindo que o tráfego seja criptografado e monitorado.

## 4 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 URL, IPs e Domínios

Indicadores de URL, IPs e Domínios	
IP	193[.]233[.]132[.]177 185[.]215[.]113[.]66

Tabela 1 – 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.

## 5 REFERÊNCIAS

---

- Heimdall by ISH Tecnologia
- [Cyber.nj](#)
- [Bleepingcomputer](#)

## 6 AUTORES

---

- Leonardo Oliveira Silva



heimdall  
security research

A DIVISION OF ISH