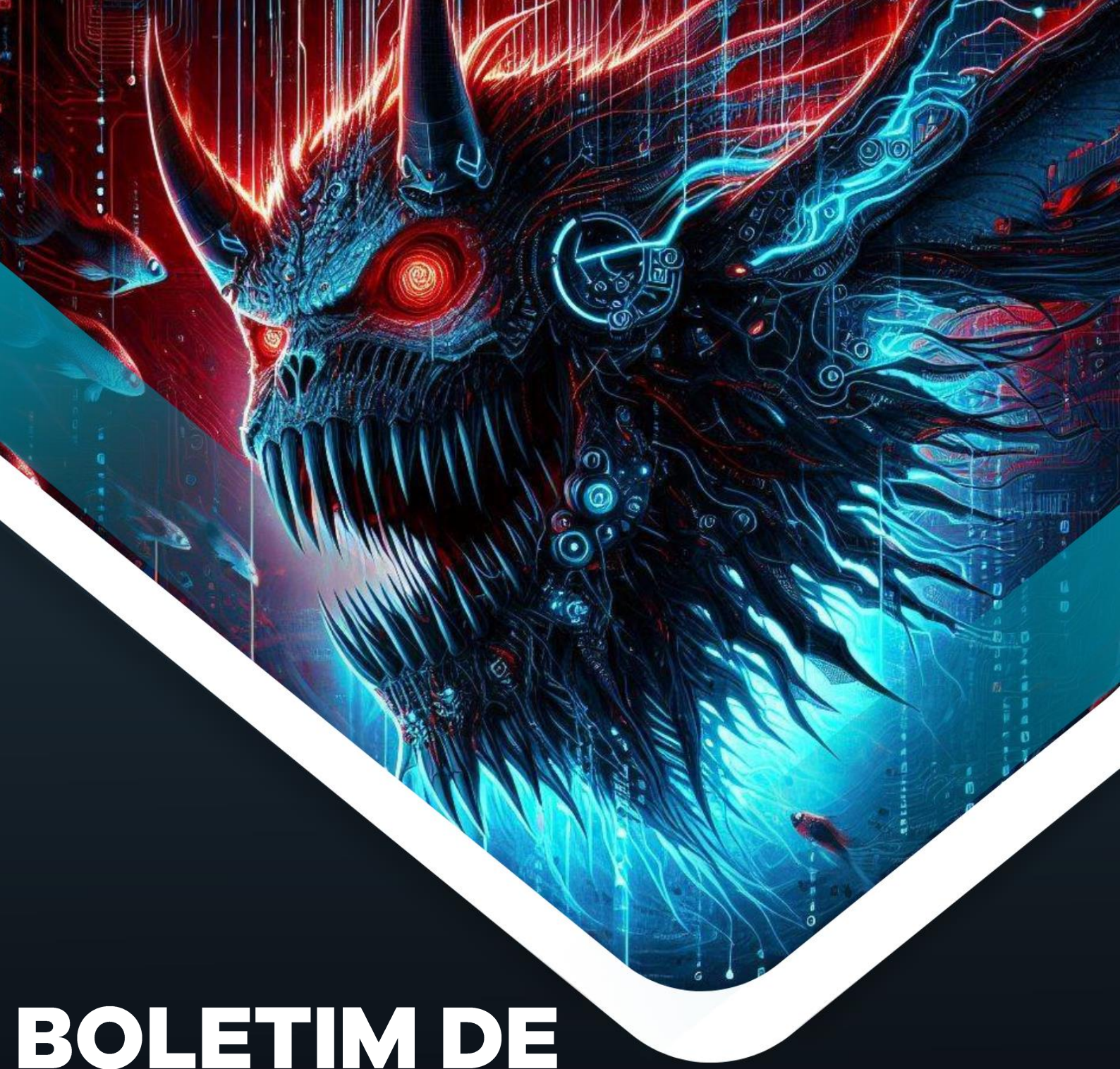


BOLETIM DE SEGURANÇA

Ferramenta de ataque em nuvem utiliza APIs para phishing de SMS em massa

heimdall
security research
A DIVISION OF ISH

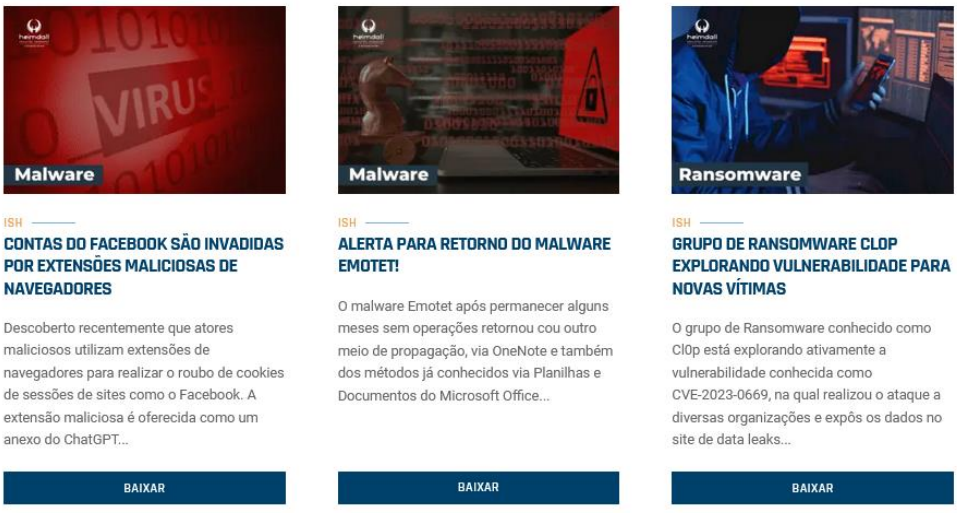
TLP: CLEAR

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

Agentes maliciosos estão utilizando a ferramenta de ataque em nuvem **Xeon Sender** para realização de campanhas de phishing e spam por SMS em larga escala, através de exploração de serviços legítimos.

2 INFORMAÇÕES SOBRE A AMEAÇA

O Xeon Sender, também conhecido como XeonV5 ou SVG Sender, é uma ferramenta de ataque em nuvem usada para enviar mensagens SMS em massa, facilitando campanhas de spam e phishing (smishing). Os invasores utilizam Xeon para enviar mensagens através de diversos provedores de SaaS com credenciais válidas, sem explorar falhas nos serviços. A ferramenta utiliza APIs legítimas para realizar ataques de spam em grande escala.

Os provedores de serviços utilizados incluem:

- *Amazon Simple Notification Service (SNS)*
- *Nexmo*
- *Plivo*
- *Proovl*
- *Send99*
- *Telesign*
- *Telnyx*
- *TextBelt*
- *Twilio*

Xeon Sender é distribuído via Telegram e outros fóruns de hacking. Não há ligação com a família de processadores Intel Xeon. A versão mais antiga conhecida é de 2022, creditada ao identificador @darkworld47. A ferramenta tem sido modificada por diferentes atores, mas sem mudanças significativas nas funcionalidades.

Figura 1 – Diferença entre a versão mais antiga e a mais recente do Xeon Sender.

Uma das versões iniciais do Xeon Sender é atribuída a um canal do Telegram famoso por distribuir ferramentas de hacking crackeadas, também mencionado em versões anteriores do infostealer AlienFox. A versão mais atual do script é creditada a um canal do Telegram com mais de 200 membros, onde o criador publica diversas ferramentas e compartilha instruções detalhadas e capturas de tela demonstrando o funcionamento dessas ferramentas.

Figura 2 – Menu principal do Xeon Sender.

O Xeon Sender é uma ferramenta que permite a realização de ataques de spam por SMS através de nove provedores de SMS em massa. A ferramenta oferece uma CLI simples para que o invasor se comunique com o backend do provedor de serviços alvo usando APIs, facilitando ataques de spam por SMS em massa com pouco esforço. Para funcionar, é necessário que o invasor possua chaves de API do serviço alvo. Habilitar essas APIs de SMS é uma tarefa complexa, regida por regulamentações federais nos EUA, o que leva os invasores a buscar credenciais de contas já verificadas.

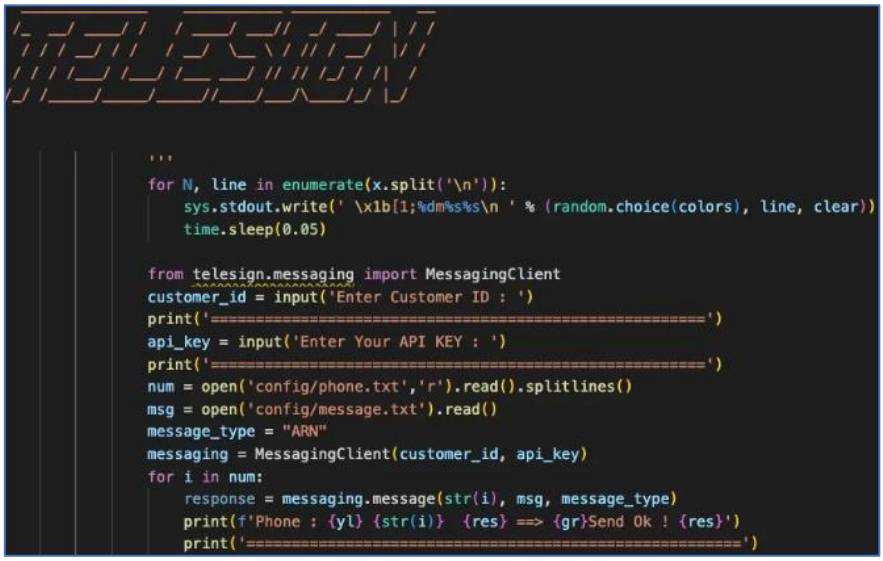
Cada ação específica do provedor de serviço é controlada por um método da classe principal do script. Os métodos requerem vários valores do operador:

- *Chave API*
- *Chave Secreta*
- *Região AWS (para AWS SNS)*
- *ID do cliente (para Telesign)*
- *ID do remetente (número de telefone ou nome, dependendo do provedor)*
- *Conteúdo da mensagem (armazenado em config/message.txt)*
- *Lista de números de telefone dos destinatários (armazenados em config/phone.txt)*

Com esses valores, a ferramenta utiliza a biblioteca requests do Python para criar uma solicitação de API para o serviço alvo, usando as credenciais ou um módulo específico do serviço, como twilio.rest para Twilio e messagebird para MessageBird.

A exceção é o módulo Proovl, que usa urllib do Python e cabeçalhos HTTP criados manualmente. A solicitação Proovl é enviada com a string user-agent Mozilla/5.0 (Windows NT 6.1; Win64; x64), que geralmente é seguida por mais detalhes sobre o cliente, não sendo confiável para engenharia de detecção.

Em cada função específica do provedor, a solicitação inclui o ID do remetente, o conteúdo da mensagem SMS e um dos números de telefone da lista phone.txt. O script percorre a lista phone.txt até que todos os números tenham sido acessados, com um intervalo de 50 milissegundos entre cada iteração.



```
'''
for N, line in enumerate(x.split('\n')):
    sys.stdout.write(' \x1b[1;%dm%s%s\n ' % (random.choice(colors), line, clear))
    time.sleep(0.05)

from telesign.messaging import MessagingClient
customer_id = input('Enter Customer ID : ')
print('================================================')
api_key = input('Enter Your API KEY : ')
print('================================================')
num = open('config/phone.txt','r').read().splitlines()
msg = open('config/message.txt').read()
message_type = "ARN"
messaging = MessagingClient(customer_id, api_key)
for i in num:
    response = messaging.message(str(i), msg, message_type)
    print(f'Phone : {yl} {str(i)}  {res} ==> {gr}Send Ok ! {res}')
    print('================================================')
```

Figura 3 – Função Telesign no Xeon Sender.

Além dos métodos de envio de SMS, o Xeon Sender oferece vários utilitários adicionais:

- **Ferramentas de verificação de contas**: Valida credenciais para contas Nexmo e Twilio.
- **Gerador de números de telefone**: Aceita argumentos para o Código do País e Código de Área, além do comprimento do número de telefone. Utiliza o módulo random do Python para gerar números de telefone conforme especificado.
- **Verificador de telefone**: Verifica a validade de um número de telefone usando a API de verificação de número do APILayer.com.

O Xeon Sender carece do refinamento necessário para aplicações mais profissionais. Embora o script inclua algum tratamento de erros, há pouca clareza em certas chamadas de API. Métodos que interagem com vários provedores de SMS, como Send99, Plivo, TextBelt e Nexmo, possuem condições de tratamento de erros e relatam uma mensagem de status.

No entanto, provedores maiores como AWS SNS e Twilio apenas retornam uma mensagem de “Success”, independentemente do resultado da solicitação ou do código de status HTTP do servidor. Além disso, o uso de variáveis ambíguas, como letras únicas ou letras combinadas com números, dificulta a depuração. O ator utiliza extensivamente bibliotecas Python específicas de cada provedor para criar solicitações de API, o que gera desafios únicos de detecção. Cada biblioteca e os logs dos provedores são distintos, tornando difícil para as equipes identificar o uso indevido de um serviço específico.

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:

Monitore chamadas de API

- Rastreie e analise regularmente chamadas de API, especialmente aquelas relacionadas a permissões de SMS e listas de distribuição.

Implemente detecção de anomalias

- Use sistemas de detecção de anomalias para identificar atividades incomuns, como grandes uploads de números de telefone.

Restrição do acesso à API

- Limite o acesso à API apenas a pessoal e aplicativos necessários, reduzindo o risco de uso não autorizado.

Auditorias regulares

- Conduza auditorias frequentes de suas permissões de envio de SMS e listas de distribuição para garantir que não haja alterações não autorizadas.

Use autenticação multifator (MFA)

- Implemente MFA para acessar sistemas e APIs confidenciais para adicionar uma camada extra de segurança.

Atualize as políticas de segurança

- Mantenha suas políticas de segurança atualizadas com as ameaças mais recentes e garanta que todos os membros da equipe estejam cientes delas.

Inteligência de ameaças

- Utilize serviços de inteligência de ameaças para se manter informado sobre novas táticas e ferramentas usadas por invasores como o Xeon Sender.

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 compromisso do artefato	
md5:	5b0d81a3a43123e5ed21d0445e738414
sha1:	078e90c959e3290a4f716fbf4e1d09fe46aaa68b
sha256:	0a0e4d5c99cbe0508d5b267e1036e446702479d6e1caf0c6305277aa316a3631
File name:	XEONV5

Indicadores de compromisso do artefato	
md5:	cdcae80dbeade68923e43ffe8168ad9e
sha1:	08d7091b7a9907a6f5894f31cd34e3e8e11cc026
sha256:	f947f0c1173fadc14d77bb92a117a8c7b9dc25c7ea97ecf7a7b251c5527fd200
File name:	XEONV5.py

Indicadores de compromisso do artefato	
md5:	1cac493ff9b21bb4a3fbaf4af2bc0034
sha1:	3597915cfbbcc7ea135bf889a89bff635c825e0d
sha256:	cf74ab9e5dc188f48701f20b6a464d1271e888d30842c72d6d73c00135e4931d
File name:	SVG SMS V5.py

Indicadores de compromisso do artefato	
md5:	6969d9d9cb39debc65f690e34934af67
sha1:	4863a15f85cd0f16ad65434de2122324c04a868a
sha256:	ca7414e6a55673a97aab70e2c1849b2579d2e956b6831b45f0a7f6eeb6909256
File name:	sm2s.py

Indicadores de compromisso do artefato	
md5:	93325d9dc7c8338620920ce3b2b07ed2
sha1:	4e6e8b074943c7fab3206ddb0abf571ffaf68523
sha256:	e621113e8c4e84c0f88fc997f52d85cec54c3fd07e222f26f3968ebced1ff530
File name:	SVG SMS V5.py

Tabela 1 – Indicadores de Compromissos de artefatos

5 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- SentinelOne
- Thehackernews

6 AUTORES

- **Leonardo Oliveira Silva**

heimdall
security research
A DIVISION OF ISH