TLP: CLEAR

BOLETIM DE SEGURANÇA

Campanha de Backdoor J-magic contra roteadores Juniper

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

LISTA DE TABELAS

LISTA DE FIGURAS

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 alvos potencialmente afetados por essa ameaça que será descrita neste relatório, incluem:

- *Industria*
- *Energia*
- *Manufatura*
- *Telecomunicações*
- *Tecnologia da Informação (TI)*

2.2 IMPACTO FINANCEIRO POTENCIAL

- *Perda de dados sensíveis*
- *Interrupção operacional*
- *Custos de remediação*
- *Responsabilidades legais*

2.3 OBJETIVO DA AMEAÇA

O principal objetivo da ameaça é explorar vulnerabilidades em roteadores corporativos, especialmente de alto nível, como os da Juniper, para obter acesso remoto não autorizado e controle completo sobre esses dispositivos. Através de " mágic packet". A ameaça visa principalmente empresas em setores estratégicos, aproveitando-se da infraestrutura de rede para impactos devastadores. A campanha demonstra alta sofisticação e risco operacional significativo.

3 TÁTICO

3.1 INFORMAÇÕES SOBRE A AMEAÇA

Pesquisadores identificaram uma campanha denominada "J-magic", que visa roteadores corporativos da Juniper. Os atacantes utilizam um backdoor que permanece passivo até receber um "pacote mágico" específico, permitindo controle remoto do dispositivo comprometido. A campanha esteve ativa de meados de 2023 até pelo menos meados de 2024, afetando setores como semicondutores, energia, manufatura e tecnologia da informação. O malware utilizado é uma variante do "cd00r", que opera passivamente, monitorando o tráfego TCP em busca de cinco parâmetros predefinidos. Ao receber um desses "pacotes mágicos", o agente envia um desafio secundário. Após a conclusão desse desafio, é estabelecido um shell reverso, permitindo que os operadores controlem o dispositivo comprometido.

3.2 OPERAÇÃO E CAPACIDADE DA AMEAÇA

A campanha "J-magic" revelou operações sofisticadas e capacidades avançadas por parte dos atores maliciosos envolvidos. Abaixo segue um detalhamento:

Implantação de malware "cd00r":

- O malware utilizado pelos atacantes é uma variante do conhecido "cd00r", que opera passivamente e é capaz de evitar detecção por mecanismos de segurança tradicionais.

Monitoramento passivo do tráfego de rede:

- Após a implantação, o malware monitora o tráfego TCP em busca de parâmetros específicos associados a magic packets.

Controle remoto:

- Depois que a autenticação é bem-sucedida, o malware estabelece um shell reverso que permite aos atacantes executarem comandos remotamente no roteador comprometido.

Persistência na memória:

- A ameaça opera exclusivamente na memória do dispositivo, tornando difícil sua detecção e eliminação sem reinicialização completa ou análise detalhada do tráfego e processos ativos.

Movimentação lateral e exfiltração de dados:

- Embora o relatório não mencione especificamente movimentação lateral, o controle remoto concedido pelo shell reverso poderia ser utilizado para explorar outros dispositivos conectados à rede comprometida.
- Dados sensíveis também podem ser extraídos, embora os alvos específicos desta campanha não tenham sido detalhados.

Evasão de detecção:

- O malware opera de forma passiva, não gerando tráfego de saída até receber o pacote mágico. Isso dificulta sua detecção por sistemas tradicionais de segurança como firewalls ou IDS.

Autenticação segura para controle remoto:

- A inclusão de uma sequência de desafio-resposta para ativar o shell reverso garante que apenas operadores autorizados possam acessar o dispositivo.

Controle completo do dispositivo comprometido:

- O shell reverso permite aos atacantes executarem qualquer comando no roteador, configurando-o como ponto de entrada para outras atividades maliciosas.

Funcionamento exclusivo na memória:

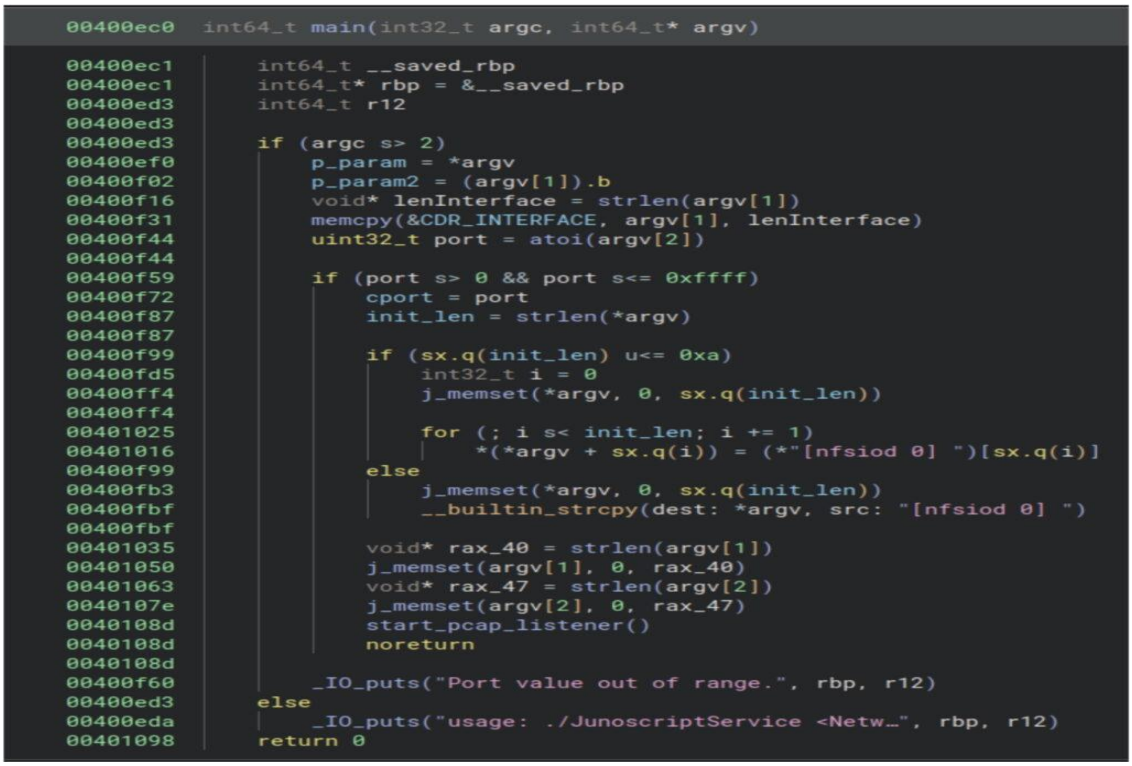
- O funcionamento na memória impede que o malware deixe rastros no armazenamento do dispositivo, dificultando sua análise forense e remoção.

Compatibilidade com infraestrutura crítica:

- Ao visar roteadores corporativos da Juniper, a ameaça compromete dispositivos cruciais para o funcionamento de redes corporativas e industriais.

A investigação dessa campanha foi iniciada após a descoberta de uma amostra de malware carregada no VirusTotal. O arquivo era identificado como "**JunoscriptService**", nome que imita o serviço de script de automação Junos. Por ter sido encontrado em um repositório público, não foi possível obter informações sobre o vetor inicial de acesso.

Após ser carregado em um roteador infectado, o malware aguarda que uma interface e uma porta sejam fornecidas via linha de comando durante a execução. Caso esses parâmetros sejam recebidos, o malware renomeia-se como "[nfsiod 0]", mascarando-se como um servidor de E/S assíncrono NFS local. Em seguida, apaga rastros sobrescrevendo os argumentos anteriores da linha de comando. Com o processo renomeado, ele inicia a função start_pcap_listener().



```
00400ec0  int64_t main(int32_t argc, int64_t* argv)

00400ec1      int64_t __saved_rbp
00400ec1      int64_t* rbp = &__saved_rbp
00400ed3      int64_t r12
00400ed3
00400ed3      if (argc s> 2)
00400ef0          p_param = *argv
00400f02          p_param2 = (argv[1]).b
00400f16          void* lenInterface = strlen(argv[1])
00400f31          memcpy(&CDR_INTERFACE, argv[1], lenInterface)
00400f44          uint32_t port = atoi(argv[2])
00400f44
00400f59          if (port s> 0 && port s<= 0xffff)
00400f72              cport = port
00400f87              init_len = strlen(*argv)
00400f87
00400f99              if (sx.q(init_len) u<= 0xa)
00400fd5                  int32_t i = 0
00400ff4                  j_memset(*argv, 0, sx.q(init_len))
00400ff4
00401025                  for (; i s< init_len; i += 1)
00401016                      *(*argv + sx.q(i)) = (*"[nfsiod 0] ")[sx.q(i)]
00400f99              else
00400fb3                  j_memset(*argv, 0, sx.q(init_len))
00400fbf                  __builtin_strcpy(dest: *argv, src: "[nfsiod 0] ")
00400fbf
00401035              void* rax_40 = strlen(argv[1])
00401050              j_memset(argv[1], 0, rax_40)
00401063              void* rax_47 = strlen(argv[2])
0040107e              j_memset(argv[2], 0, rax_47)
0040108d              start_pcap_listener()
0040108d              noreturn
0040108d
00400f60          _IO_puts("Port value out of range.", rbp, r12)
00400ed3      else
00400eda          _IO_puts("usage: ./JunoscriptService <Netw…", rbp, r12)
00401098      return 0
```

Figura 1 – Função principal.

Após ser implantado em um dispositivo, o atacante utiliza malware de código aberto, sendo a amostra analisada uma variante personalizada do cd00r, originalmente disponibilizado no Packet Storm em 2000. O J-magic e o SeaSpy compartilham algumas características, como a presença de cinco condições para os pacotes mágicos, embora essas condições sejam distintas em cada amostra. Também foram identificadas semelhanças nos nomes de funções, como "reverse_shell" e ">>" (indicando uma sessão de terminal de comando). Contudo, como esses nomes são amplamente usados, a correlação técnica entre as duas amostras é considerada baixa. Uma diferença importante é que o J-magic possui um certificado usado no componente de autenticação do desafio mencionado, algo não encontrado nas amostras públicas do SeaSpy. Assim, embora haja alta confiança de que o malware J-magic seja uma variante do cd00r, a correlação com a família SeaSpy é considerada de baixa confiança, com base nas informações disponíveis.

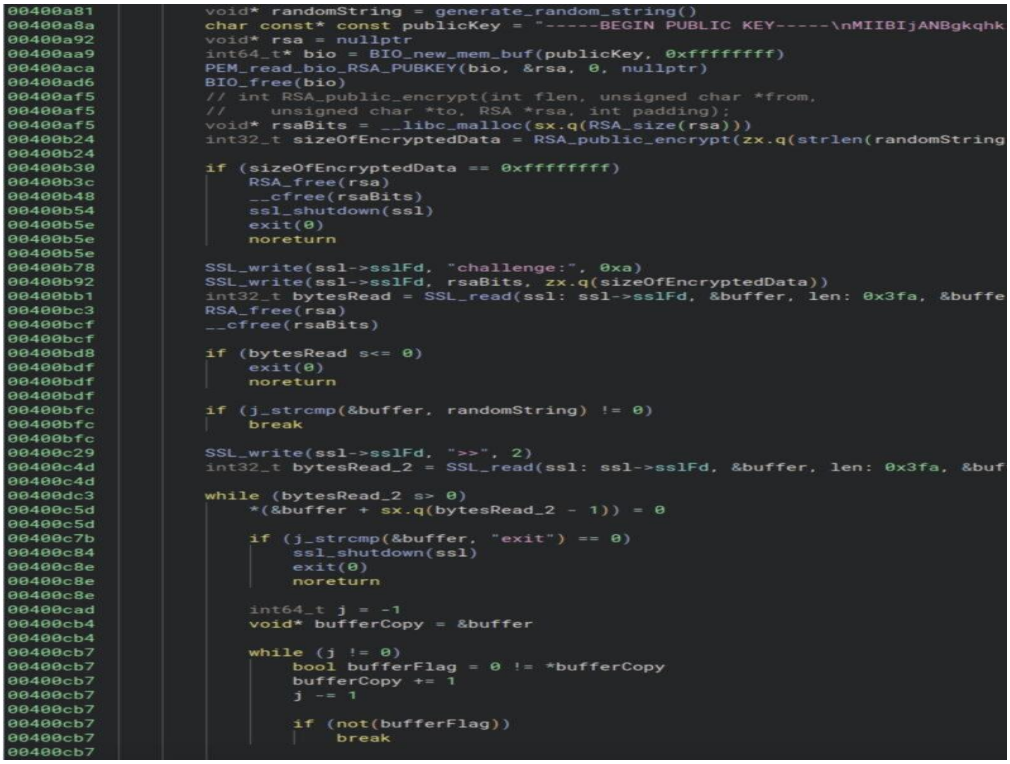


Figura 2 – Comandos de processamento de shell reverso.

3.3 TABELA MITRE ATT&CK

Este tópico apresenta as Táticas, Técnicas e Procedimentos (TTPs) identificados nesta ameaça, conforme o framework MITRE ATT&CK, oferecendo uma visão tática detalhada sobre o comportamento do adversário. O objetivo é permitir o mapeamento das técnicas utilizadas pelos atacantes, facilitando a implementação de contramedidas eficazes e o aprimoramento das defesas de segurança.

Tática	Técnica	Detalhes
Resource Development	T1587.001 Develop Capabilities	Desenvolvimento do malware e componentes de malware que podem ser usados durante a segmentação. Isto inclui a criação de backdoors, como a variante personalizada de “cd00r” usada na campanha J-magic.
Execution	T1204.002 User Execution	Um adversário pode contar com a abertura de um arquivo malicioso pelo usuário para obter execução. Nesta campanha, o malware espera que parâmetros específicos sejam fornecidos através da linha de comando durante a execução.
Defense Evasion	T1036 Masqueradin	Na campanha J-magic, o malware se renomeia para imitar serviços

		legítimos, como “[nfsiod 0]”, para evitar a detecção.
Command and Control	T1205 Traffic Signaling	O malware J-magic monitora "pacotes mágicos" contendo parâmetros predefinidos para estabelecer um shell reverso para controle remoto.

Tabela 1 – Tabela MITRE ATT&CK.

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:

Atualizar o firmware dos roteadores regularmente:

- Certifique-se de que os roteadores, especialmente dispositivos Juniper e similares, estejam executando as versões mais recentes do firmware, corrigindo vulnerabilidades conhecidas que possam ser exploradas.

Monitorar tráfego de rede e detectar padrões anômalos:

- Utilize ferramentas de análise de tráfego e sistemas de detecção de intrusão (IDS) para identificar pacotes não convencionais, como "magic packets", que podem ativar malwares passivos.

Implementar controles de acesso seguros:

- Restrinja o acesso administrativo aos roteadores apenas a usuários autorizados. Utilize autenticação multifator (MFA) para acessar interfaces de gerenciamento e dispositivos críticos.

Desativar funções não utilizadas:

- Desative funções ou serviços não essenciais nos roteadores, como Wake-on-LAN ou portas abertas que possam ser exploradas por atacantes.

Configurar listas de controle de acesso (ACL):

- Estabeleça ACLs nos roteadores para limitar o tráfego permitido, bloqueando pacotes de entrada que não sejam estritamente necessários para o funcionamento normal da rede.

Realizar auditorias de configuração:

- Inspecione regularmente as configurações dos roteadores para verificar a presença de alterações não autorizadas, como renomeações de processos ou comandos inesperados.

Treinamento e sensibilização da equipe:

- Treine os administradores de rede e segurança sobre as técnicas utilizadas nesta campanha, garantindo que estejam preparados para identificar sinais de comprometimento e responder rapidamente a incidentes.

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 COMPROMETIMENTO (IOC)

Indicadores do artefato	
md5:	9a6fae96eb301768a67714b0cf65e170
sha1:	7edc911b31b4f5dc401725c9b52e876a9fd00f3e
sha256:	5e3c128749f7ae4616a4620e0b53c0e5381724a790bba8314acb502ce7334df2
File name:	JunoscriptService

Indicadores do artefato	
md5:	4ca4f582418b2cc0626700511a6315c0
sha1:	0ea36676bd7169bcbf432f721c4edb5fde0a46a9
sha256:	3f26a13f023ad0dcd7f2aa4e7771bba74910ee227b4b36ff72edc5f07336f115
File name:	BarracudaMailService

Tabela 2 – Indicadores de Comprometimento

6 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Lumen**
- **Bleepingcomputer**

7 AUTORES

- **Leonardo Oliveira**

heimdall
security research
A DIVISION OF ISH