BOLETIM DE SEGURANÇA

Zergeca, nova botnet escrita em GO identificada

heimdall
security research
A DIVISION OF ISH

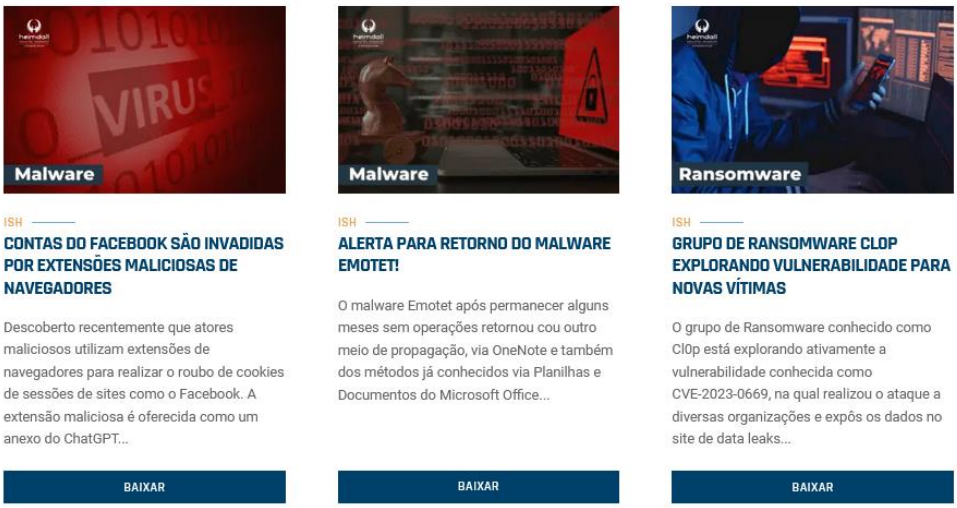
TLP: CLEAR

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

Uma nova botnet escrita na linguagem de programação GO foi identificada por pesquisadores de segurança, chamada **Zergeca** e a mesma é capaz de conduzir ataques distribuídos de negação de serviço (DDoS).

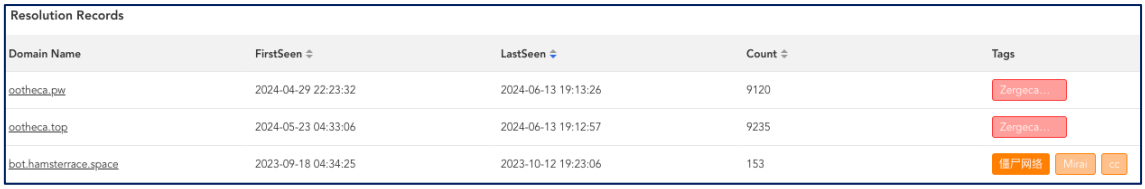
2 DETALHES SOBRE A AMEAÇA

A Zergeca não é apenas uma botnet DDoS comum; ela é capaz de realizar seis métodos diferentes de ataque e possui funcionalidades adicionais como proxy, escaneamento, autoatualização, persistência, transferência de arquivos, shell reverso e coleta de informações sensíveis do dispositivo. Do ponto de vista da comunicação de rede, a Zergeca tem características exclusivas, tais como:

- Suporte a diversos métodos de resolução de DNS, com prioridade para DOH na resolução C2.
- Uso da biblioteca incomum Smux para o protocolo de comunicação C2, criptografado através de XOR.

3 ATIVIDADES DA AMEAÇA

Conforme a pesquisa, em de abril de 2024, o endereço *84[.]54.51[.]82* começou a ser usado como o servidor C2 para Zergeca.



Resolution Records

Domain Name	FirstSeen	LastSeen	Count	Tags
potheca.pw	2024-04-29 22:23:32	2024-06-13 19:13:26	9120	Zergeca...
potheca.top	2024-05-23 04:33:06	2024-06-13 19:12:57	9235	Zergeca...
bot.hamsterrace.space	2023-09-18 04:34:25	2023-10-12 19:23:06	153	僵尸网络 Mirai cc

Figura 1 – Registros observados.

Os principais métodos utilizados pelo IP 84[.]54.51[.]82 para disseminar amostras incluem o uso de senhas fracas no Telnet e a exploração de determinadas vulnerabilidades conhecidas, os identificadores das vulnerabilidades relevantes são os seguintes:

```
Telnet Weak Password
CVE-2022-35733
CVE-2018-10562
CVE-2018-10561
CVE-2017-17215
CVE-2016-20016
```

Figura 2 – Explorações observadas.

Detalhes das vulnerabilidades acima

CVE-2022-35733

- Essa vulnerabilidade afeta gravadores de vídeo digital da UNIMO Technology (modelos UDR-JA1004, UDR-JA1008 e UDR-JA1016) com versões de firmware até 1.0.20.13 e 2.0.20.13. Envolve a ausência de autenticação para uma função crítica, permitindo que um atacante remoto não autenticado

execute comandos arbitrários do sistema operacional via uma solicitação especialmente criada para a interface web do dispositivo. Esta questão tem uma pontuação CVSS crítica de 9.8.

CVE-2018-10562

- Essa vulnerabilidade impacta roteadores GPON. Ela envolve uma falha na implementação do mecanismo de login, permitindo que atacantes remotos acessem o dispositivo e executem comandos arbitrários sem a devida autenticação.

CVE-2018-10561

- Semelhante ao CVE-2018-10562, essa vulnerabilidade também afeta roteadores GPON. Explora um problema com a interface de gerenciamento web, permitindo que atacantes ignorem a autenticação e potencialmente controlem o dispositivo.

CVE-2017-17215

- Essa vulnerabilidade é encontrada em roteadores Huawei HG532. Permite que atacantes remotos executem comandos arbitrários via a interface UPnP do dispositivo. O problema ocorre devido à validação inadequada da entrada do usuário, levando a vulnerabilidades de injeção de comando.

CVE-2016-20016

- Uma vulnerabilidade que afeta modelos de DVR CCTV da MVPower, incluindo os modelos TV-7104HE (firmware 1.8.4 115215B9) e TV7108HE. Esta vulnerabilidade é crítica (com uma pontuação CVSS de 9.8) e permite que um atacante remoto não autenticado execute comandos arbitrários do sistema operacional com privilégios de root. O problema está relacionado a uma "web shell" acessível via o URI "/shell". Esta falha foi explorada ativamente entre 2017 e 2022, sendo conhecida como "JAWS webserver RCE" devido à identificação fácil pelo campo HTTP response server.

4 MITRE ATT&CK - TTPs

Tática	Técnica	Detalhes
Initial Access	T1190 Exploit Public-Facing Application	Exploração de vulnerabilidades conhecidas em aplicativos expostos à internet para obter acesso inicial.
Execution	T1059 Command and Scripting Interpreter	Uso de scripts para executar comandos em sistemas comprometidos.
Persistence	T1543.003 Create or Modify System Process	Criação de serviços de sistema para garantir a execução na inicialização.
Privilege Escalation	T1068 Exploitation for Privilege Escalation	Uso de vulnerabilidades para escalar privilégios.
Defense Evasion	T1027 Obfuscated Files or Information	Uso de criptografia XOR e empacotamento com UPX modificado para evadir a detecção.
Discovery	T1046 Network Service Scanning	Varredura de portas e serviços vulneráveis na rede.
Lateral Movement	T1021 Remote Services	Movimentação lateral através de serviços remotos vulneráveis e Telnet com senhas fracas.
Collection	T1005 Data from Local System	Coleta de informações sensíveis dos dispositivos infectados.
Command and Control	T1573.001 Encrypted Channel	Comunicação encriptada com o servidor de C2 usando DNS over HTTPS (DoH) e a biblioteca Smux.
Impact	T1498 Network Denial of Service	Condução de ataques DDoS, incluindo SYN flood, ACK flood e HTTP POST flood.

Tabela 1 – Tabela MITRE ATT&CK.

5 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:

Utilização de senhas fortes e únicas

- Senhas fracas ou reutilizadas são vulneráveis a ataques de força bruta. Utilize senhas complexas, com combinações de letras maiúsculas e minúsculas, números e caracteres especiais. Ferramentas de gerenciamento de senhas podem ajudar a manter essas senhas seguras.

Evitar links e anexos suspeitos

- Cibercriminosos frequentemente utilizam phishing para distribuir malware. Não clique em links ou abra anexos de e-mails de remetentes desconhecidos. Verifique sempre a autenticidade das comunicações antes de interagir com elas.

Mantenha os softwares atualizados

- Muitos ataques exploram vulnerabilidades em softwares desatualizados. Mantenha todos os seus dispositivos e softwares atualizados com as últimas correções de segurança para mitigar esses riscos.

Configurações de segurança

- Verifique e atualize regularmente as configurações de segurança de todos os seus dispositivos, incluindo dispositivos IoT. Alterar senhas padrão e configurar corretamente as opções de privacidade e segurança pode prevenir acessos não autorizados.

Monitoramento e resposta

- Implementar soluções de monitoramento de rede que possam identificar atividades suspeitas e responder rapidamente a incidentes pode ajudar a detectar e neutralizar ameaças antes que causem danos significativos.

6 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:	23ca4ab1518ff76f5037ea12f367a469
sha1:	1001b06820145ac69f3d440f1cc25990eb14cc71
sha256:	7db9189afd00c2b60b7f892ef1b86d040fb1cf02145c7d2e414ef77ba3335c11
File name:	geomi

Indicadores de compromisso do artefato	
md5:	9d96646d4fa35b6f7c19a3b5d3846777
sha1:	ffb6b44c5911efb7397a02da9b66f83a42e3fd20
sha256:	6b81d548c0fbd7a2275bb0d29deca0de96c1584ce7aadaf4f5dac3cb28ee9c29
File name:	6b81d548c0fbd7a2275bb0d29deca0de96c1584ce7aadaf4f5dac3cb28ee9c29

Indicadores de compromisso do artefato	
md5:	d78d1c57fb6e818eb1b52417e262ce59
sha1:	04e8b08cda521a6f939f46856449ea53f846083a
sha256:	b55b1947a11de7ee2cb3aaede12ce15c85abf2b607d1ebd8f5ed56e3a6ef7c43
File name:	b55b1947a11de7ee2cb3aaede12ce15c85abf2b607d1ebd8f5ed56e3a6ef7c43

Indicadores de compromisso do artefato	
md5:	604397198f291fa5eb2c363f7c93c9bf
sha1:	34e38f2ceeed80c34f3aa8bd663654f50e6fa2b1
sha256:	0dbbe5616de71c5753768de555203fb9eb2f1e72a8cb5bdce0559bc5cdfa3b2e
File name:	0dbbe5616de71c5753768de555203fb9eb2f1e72a8cb5bdce0559bc5cdfa3b2e

Indicadores de compromisso do artefato	
md5:	6ac8958d3f542274596bd5206ae8fa96
sha1:	4a6cb6640b7a43ccfc6ee9921f0e88ba84da8a0b
sha256:	2e9df8987212300815928e0426e9358b1380a1eaba38270d03dd69e421686b5b
File name:	db0fa4b8db0333367e9bda3ab68b8042.i686

Indicadores de compromisso do artefato	
md5:	980cad4be8bf20fea5c34c5195013200
sha1:	d419c3ba75ec203cd002734114cc04d3dc735cfb
sha256:	cea6e4aa15d7c6a2b2c794a660afaf96d43462e0b74436600a2c8a2288ad0c27
File name:	7db9189afd00c2b60b7f892ef1b86d040fb1cf02145c7d2e414ef77ba3335c11_patched_by_xlab

Indicadores de compromisso do artefato	
md5:	60f23acebf0ddb51a3176d0750055cf8
sha1:	d729aa662ea7d652908326dc5d91b97d836ba936
sha256:	7e62e3e8911c0cb19df3477df0603fddeff82223e1cc6da7fb1698f512ff2cd2

File name:	7e62e3e8911c0cb19df3477df0603fddeff82223e1cc6da7fb1698f512ff2cd2

Indicadores de compromisso do artefato	
md5:	f68139904e127b95249ffd40dfeedd21
md5:	d7b5d45628aa22726fd09d452a9e5717

Tabela 2 – Indicadores de Compromissos de artefatos

Indicadores de IPs e Domínios

Indicadores de URL, IPs e Domínios	
Domínio	ootheca[.]pw ootheca[.]top bot.hamsterrace[.]space
IP	84[.]54.51[.]82

Tabela 3 – 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.

7 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **blog.xlab**
- **MITRE ATT&CK**

8 AUTORES

- **Ismael Pereira Rocha**

heimdall
security research
A DIVISION OF ISH