BOLETIM DE SEGURANÇA

Alerta sobre Botnet CatDDoS em ataque DDoS

heimdall
security research
A DIVISION OF ISH

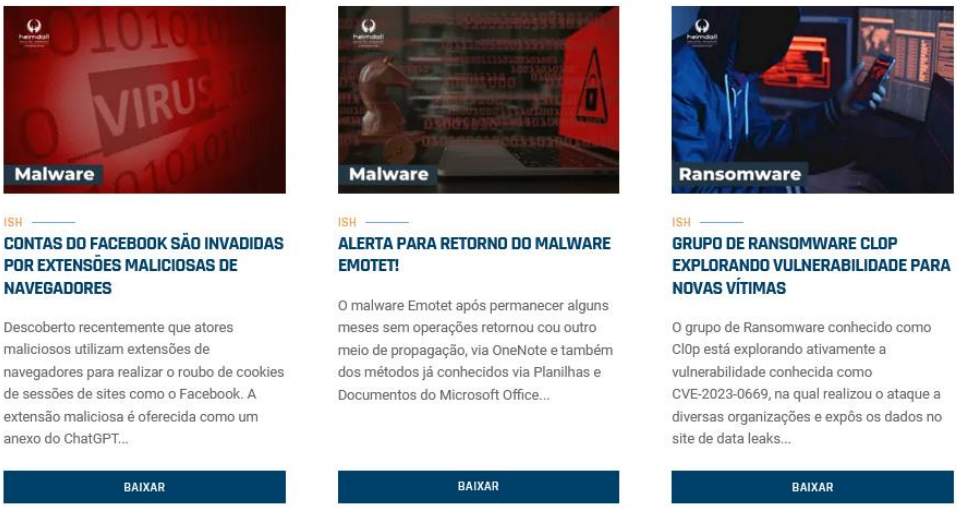
TLP: CLEAR

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

Especialistas da XLab detectaram recentemente que atores maliciosos associados ao botnet CatDDoS têm se aproveitado de vulnerabilidades conhecidas em diversos programas. No decorrer dos últimos três meses, essas brechas foram exploradas para invadir e recrutar dispositivos vulneráveis, integrando-os a uma rede de bots destinada a realizar ataques DDoS distribuídos.

2 DETALHES SOBRE A AMEAÇA

O impacto afeta uma variedade de dispositivos, incluindo roteadores e equipamentos de rede de fabricantes como Apache (com produtos como ActiveMQ, Hadoop, Log4j e RocketMQ), Cacti, Cisco, D-Link, DrayTek, FreePBX, GitLab, Gocloud, Huawei, Jenkins, Linksys, Metabase, NETGEAR, Realtek, Seagate, SonicWall, Tenda, TOTOLINK, TP-Link, ZTE e Zyxel.

Até o momento, não foram detectadas vulnerabilidades específicas, no entanto, a presença de termos como “skylab0day” e “Cacti-n0day” nos parâmetros de execução sugere a possibilidade de uma vulnerabilidade zero-day. “Skylab” parece ser um identificador de rede associado a um grupo de cibercriminosos, e “skylab0day” poderia indicar uma vulnerabilidade zero-day originada desse grupo.

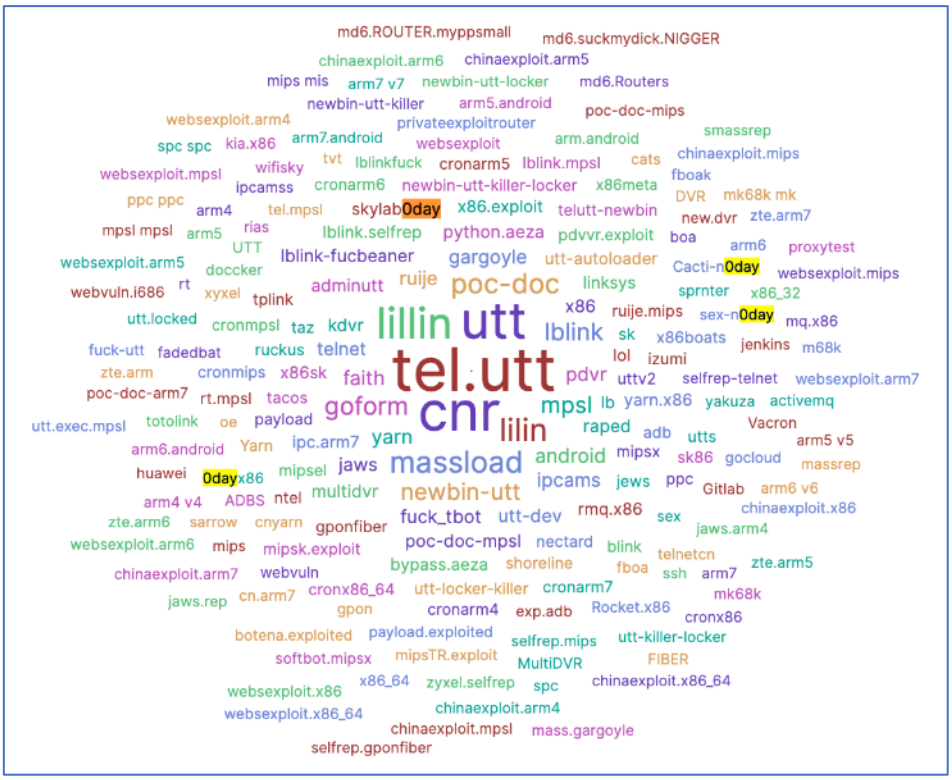


Figura 1 – Indicador skylab0day.

A imagem abaixo revela estatísticas de ataques DDoS. É possível verificar um registro completo das ações de grupos vinculados ao CatDDoS, bem como detalhes abrangentes sobre aspectos como comando e controle, instruções, alvos, entre outros. Observa-se que os alvos desses grupos estão espalhados globalmente, com uma concentração maior nos Estados Unidos, França, Alemanha, **Brasil** e China, afetando setores variados que incluem provedores de serviços em nuvem, instituições educacionais, pesquisa científica, mídia, órgãos governamentais, construção civil, entre outros.

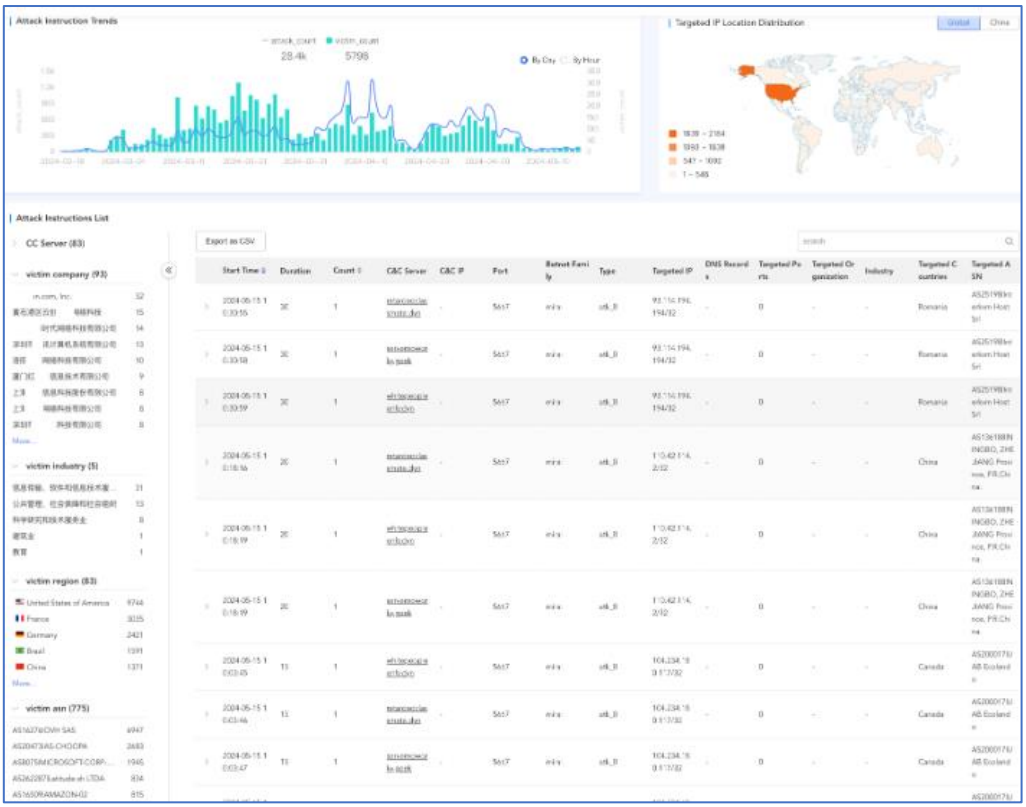


Figura 2 – Estatísticas de ataques DDOS.

O CatDDoS, é uma evolução do Mirai, surgido em agosto de 2023, manteve sua estrutura de comunicação similar à versão original, tornando o relatório inicial ainda relevante para análises atuais. Surgiu a teoria de que a ameaça pode ter cessado suas atividades em dezembro anterior. Registros do canal Aterna foram removidos, e uma mensagem do desenvolvedor sinalizando o encerramento foi postada no grupo. A disseminação ou vazamento do código-fonte originou variantes como RebirthLTD, Komaru e Cecilio Network.

Recentemente, as variantes v-2.0.4 (CatDDoS) e v-Rebirth (RebirthLTD) estiveram ativas, ambas empregando o algoritmo chacha20 para criptografar dados em suas comunicações, com chave e nonce coincidentes. A v-2.0.4 se distingue por utilizar um domínio OpenNIC como seu C2. Já a RebirthLTD, que inicialmente foi baseada no código do Mirai, adotou o código do CatDDoS e vem sendo atualizada regularmente. A variante v-snow_slide operou discretamente por um período e agora se encontra inativa. Por outro lado, a v-ihateyou, que parece ter características ligadas ao CatDDoS, na verdade não segue suas especificações de comunicação e descriptografia, assemelhando-se mais ao Mirai, e parece ser uma variante efêmera.

A variante v-snow_slide viu sua atividade finalizada após o encerramento das operações da Aterna, levantando suspeitas de que fosse uma criação desta entidade. Análises de engenharia reversa revelaram a preservação de extensos segmentos do código Fodcha, incluindo a utilização da criptografia xxtea, o emprego de domínios OpenNIC para C2 e uma estrutura de switch-case semelhante, além da combinação de algoritmos xxtea e chacha20 no protocolo de comunicação. Esses indícios sugerem um possível ressurgimento do Fodcha. Curiosamente, a variante emprega termos como 'N3tL4b360G4y' e 'paloaltoisgaytoo' em suas comunicações com o C2, aparentemente como uma forma irônica de "homenagem" a uma conhecida empresa de segurança.

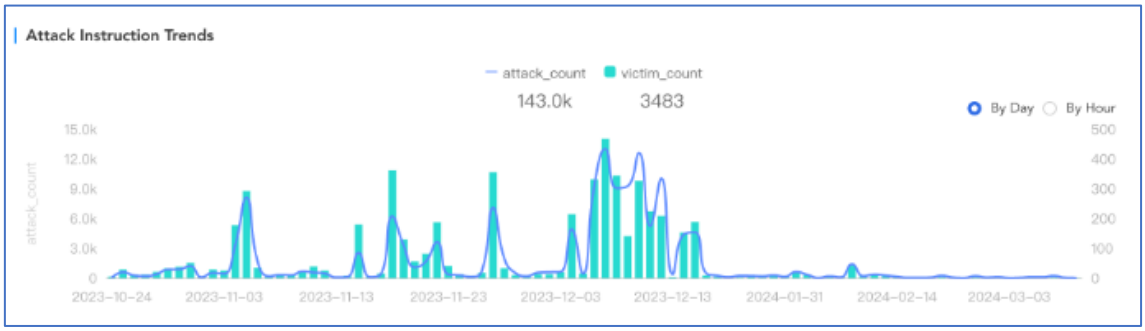


Figura 3 – Tendências de instruções de ataque.

Na análise, notou-se que, além dos alvos usuais, muitos correspondiam a outras variantes ou infraestruturas C2 de distintas famílias de malwares. Esse padrão é similar ao observado em discussões no Telegram, onde há uma rivalidade contínua entre operadores de botnets, indicando que conflitos entre esses agentes podem ser uma característica comum em botnets IoT, não sendo exclusiva do CatDDoS.

```
2024-04-06 07:24:26 rebirth-network.su -> 185.234.66.97(omgnoway.geek)
2024-04-12 08:46:50 omgnoway.geek -> 45.142.182.80(cnc.tsuki.army)
2024-04-12 09:07:47 omgnoway.geek -> 87.246.7.66(rebirth-network.su)
2024-04-12 17:18:41 rebirth-network.su -> 185.234.66.97(omgnoway.geek)
2024-04-17 04:02:45 9wg0dstmud.pirate -> 87.246.7.66(rebirth-network.su)
2024-04-17 13:05:35 secure-core-rebirthltd.su -> 45.142.182.80(cnc.tsuki.army)
2024-04-26 23:41:51 45.142.182.80(cnc.tsuki.army) -> retardedclassmate.dyn
2024-04-27 17:37:19 retardedclassmate.dyn -> 212.70.149.13(RebirthTLD Download Server)
```

Figura 4 – Operadores de botnet.

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:

Atualizações de software

- Mantenha todos os seus aplicativos e sistemas operacionais atualizados. Os cibercriminosos por trás do CatDDoS exploram vulnerabilidades conhecidas em vários softwares. Portanto, aplicar patches e atualizações de segurança é crucial.

Fontes seguras

- Baixe aplicativos apenas de fontes oficiais e seguras.

Antivírus

- Use um antivírus de confiança e mantenha-o atualizado. Se você suspeitar que seu dispositivo está infectado, execute uma varredura completa.

Monitoramento de rede

- Monitore o desempenho da sua rede. As atividades promovidas por botnets consomem banda e diminuem o desempenho da rede.

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:	248e177711ceb989be4cfaf99d2889f6
sha1:	5a1124cee1a26f84aa151a68e1dbdebd6fe7a247
sha256:	43915b047d2b7c23209150d5be1d084a520e312abbf05af67c3c17a05912f19f
File name:	5356de50d524ed4ff2f4c815ee2e0d389542df51eda110feca31615e4aca7c31.elf.rewr

md5:	2ab78374d7ab2fb3c5dddcbe6d714856
sha1:	f34e17c84d66117156826997aec6136e10d7cb9e
sha256:	fab6a3d74d967a0fc1d2e6fe1f85e8b644ccbdc08bf168b65088dadabe7c109c
File name:	x86_64

md5:	921edfdfa4410c765417758bf954ebb1
sha1:	5538eb7e09395f5bfefae1af26b4c17cb5631da0
sha256:	f2877683ed5b9030c88b677166d73ef8eebbdff77867528ae77dc5d3e0ffd86f
File name:	arm7

md5:	547f2d34b74862e7e9048509cfa8685b
sha1:	7f55aab44fd9939c7a0c81d78838d81991209ec4
sha256:	836adc5adb7f0f0d28496c76ec82fc85a04305871ff7c91550f17fcc22fa4692
File name:	xaarch64

md5:	8ef8c40b4039b046e9a94f00dc0dec66
sha1:	d9d569b0567dd406bf09c33e4ac71966138fbbd2
sha256:	456309d596537395d5c6323e5c5ff566523f82b466ed094fa05049ed12c08150
File name:	8ef8c40b4039b046e9a94f00dc0dec66.virus

md5:	d5cffec8b95a0bb5b2e88e71ebbf6e64
sha1:	e81dc79de33af42ee6e9e489ae1305165649ef28
sha256:	0447946cd5232378c9f31be399f8bdb9aea13743cb12973484bfcc04d74c0fa6
File name:	0447946cd5232378c9f31be399f8bdb9aea13743cb12973484bfcc04d74c0fa6.elf

md5:	26621649b23e0e5ff36d9264812a72df
sha1:	4e7c2c86b37d7f44ef2f80974cc60c068e205526
sha256:	918fff71477dd5659b133dc62baca2189f13260c69442b1662b0d1cf2342638c
File name:	x86_32

Tabela 1 – Indicadores de Compromissos de artefatos

Indicadores de URL, IPs e Domínios

Indicadores de URL, IPs e Domínios	
Domínio	catddos.pirate i-like-dicks.pirate chinks-eat-dogs.africa jm1hj56glo.pirate siegheil.hiter.su omgnoway.geek phhfr59rqd.parody 9wg0dstmud.pirate hsjupldf2z.pirate 9fz0cqekwr.parody 4m8mdkx76o.indy fd9vsneghh.libre chinkseatblahajs.libre francothesped.geek akira-cuddles-blahajs.pirate rebirthltd.dev scan.rebirthltd.dev rebirthltd.com scan.rebirthltd.top xysk5eeyj0j5n.xyz lsagjogu8ztaueghasdjsdigh.cc fuck-niggers.xyz secure-core-rebirthltd.su secure-network-rebirthltd.ru hitler.su kz.hitler.su
IP	212.70.149.10 212.70.149.14 87.246.7.194 87.246.7.198 87.246.7.66 89.32.41.31 103.161.35.44 31.220.1.44 194.169.175.20 194.169.175.31 194.169.175.39 194.169.175.40 194.169.175.43

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**
- XLab
- Thehackernews

6 AUTORES

- **Leonardo Oliveira Silva**

heimdall
security research
A DIVISION OF ISH