TLP: CLEAR

BOLETIM DE SEGURANÇA

Botnet Socks5Systemz transforma mais de 85.000 dispositivos Hackeados em rede de proxy ilegal

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 AMEAÇA

O Socks5Systemz, um malware botnet tem transformados sistemas infectados em nós de saída proxy. O nome deriva do texto usado pelo agente da ameaça no painel de controle.

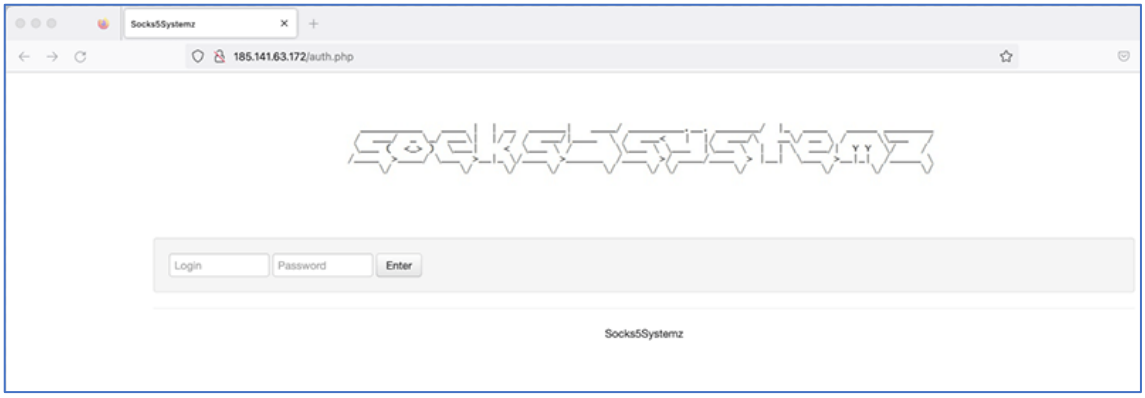

Figura 1 – Página de login do painel C2 do Socks5systemz.

Conforme a Bitsight, várias campanhas de distribuição do malware foram identificadas no último ano porém ele permaneceu discreto até setembro de 2023. Após investigações, foram encontradas postagens em fóruns clandestinos russos com links para o malware, datando de 2013. A imagem abaixo mostra uma dessas postagens, onde o usuário BaTHNK está vendendo um “sistema de backconnect SOCKS5”.

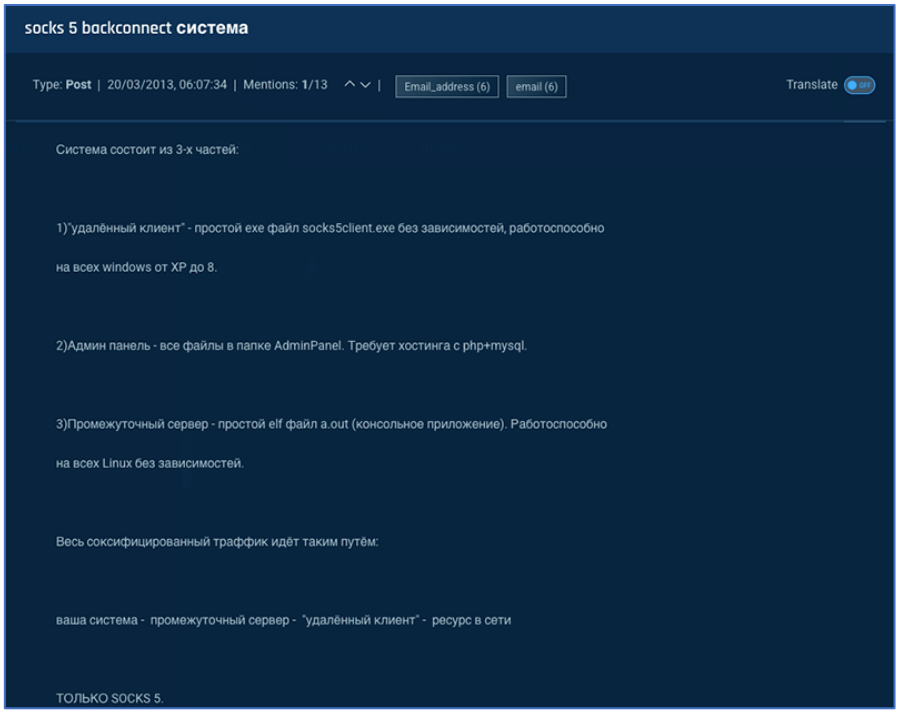

Figura 2 – Postagem arquivada de 2013 no fórum XSS.

Durante uma pesquisa, foi encontrado um módulo proxy para Trickbot (2017) com código muito semelhante e a mesma funcionalidade do Socks5Systemz. O uso do Socks5Systemz como um módulo proxy dentro de outro malware pode explicar a falta de referências a ele antes de novembro de 2023; ele provavelmente operava discretamente, sendo detectado como parte de outro malware, sem chamar a atenção da comunidade de inteligência de ameaças.

Em setembro de 2023, começaram a surgir campanhas amplamente distribuídas do Socks5Systemz usando Privateloader, Amadey e Smokeloader. Esta era a versão autônoma do Socks5Systemz como o payload final. Não se sabe por que o modus operandi mudou, mas pode estar relacionado a mudanças no ecossistema de crimeware que levaram os agentes de ameaças a adotar essa abordagem.

Figura 3 – Telemetria de sistemas infectados coletada do final de novembro de 2023 a janeiro de 2024.

A botnet conhecida como Socks5Systemz V1 está disseminada globalmente, com bots presentes em quase todos os países. No final de janeiro de 2024, a quantidade média diária de bots era aproximadamente 250.000.

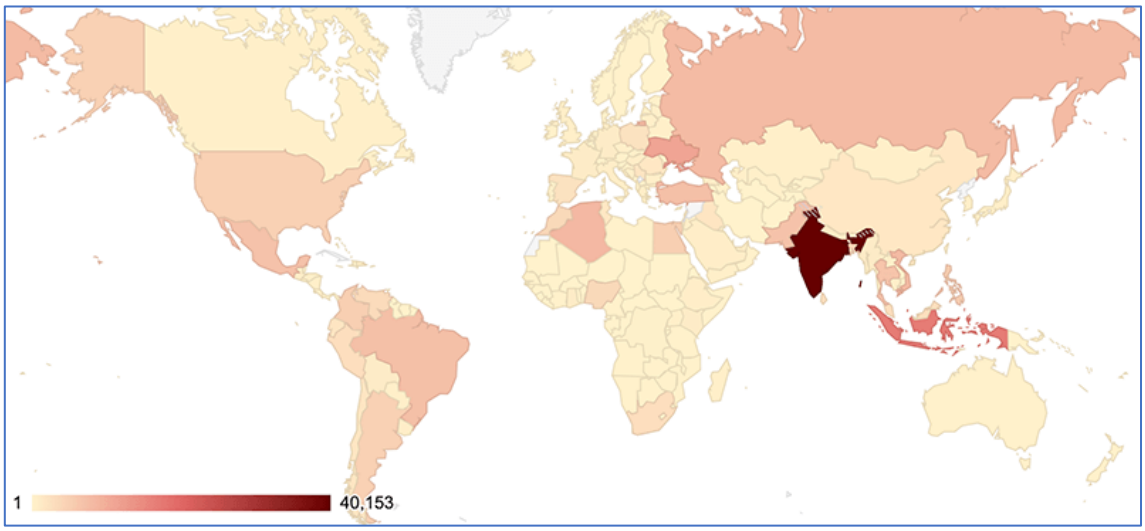

Figura 4 – Dispersão geográfica do botnet Socks5Systemz V1.

País	Infecções
Índia	40153
Indonésia	17027
Ucrânia	11178
Argélia	8255
Vietname	8047
Federação Russa	7826
Peru	7288
Brasil	7224
México	6987
Paquistão	6802
Tailândia	6452
Filipinas	5664
Colômbia	5165
Egito	5164
Estados Unidos	4784
Argentina	4756
Bangladesh	4432
Marrocos	3758
Nigéria	3625
Outros	73573

Tabela 1 – Tabela dos principais países afetados pelas infecções do Socks5Systemz.

Com uma média diária de 250 mil bots, esta botnet é uma das maiores atualmente. Para comparação, a Andromeda, em seu auge, tinha uma média diária de 2 milhões de bots, embora operasse com um modelo de negócios diferente. Malwares proxy semelhantes têm médias diárias entre 15 mil e 50 mil bots.

Ao examinar a infraestrutura C2 e investigar um dos servidores de backconnect associados ao Socks5Systemz, operando com o endereço IP 109.236.51[.]104, entre fevereiro de 2022 e novembro de 2023, os registros DNS passivos revelam o seguinte:

Query	Type	Source	Count	Response	First Seen	Last Seen	Duration
109-236-81-104.hosted-by-worldstream.net	A	D	534	109.236.81.104	2023-12-11, 01:01	2024-05-03, 01:58	143d 23h 48m
hpf.proxy.am	A	B	11	109.236.81.104	2019-07-16, 06:38	2021-02-13, 20:23	1y 213d 14h
design.proxy.am	A	D	10	109.236.81.104	2018-03-20, 07:19	2019-01-17, 22:16	303d 14h 56m
hpf.proxy.am	A	D	97	109.236.81.104	2018-02-15, 18:23	2021-08-09, 22:21	3y 176d 2h
api.proxy.am	A	D	1387861	109.236.81.104	2018-02-12, 17:36	2021-08-30, 06:14	3y 199d 11h
api.proxy.am	A	B	44	109.236.81.104	2018-02-12, 17:36	2021-04-29, 23:08	3y 77d 4h

Figura 5 – Registros PDNS para 109.236.51[.]104.

Isso indica que o IP de um servidor C2 para Socks5Systemz foi reutilizado de um servidor hospedado em design.proxy[.]am, hpf.proxy[.]am e api.proxy[.]am.

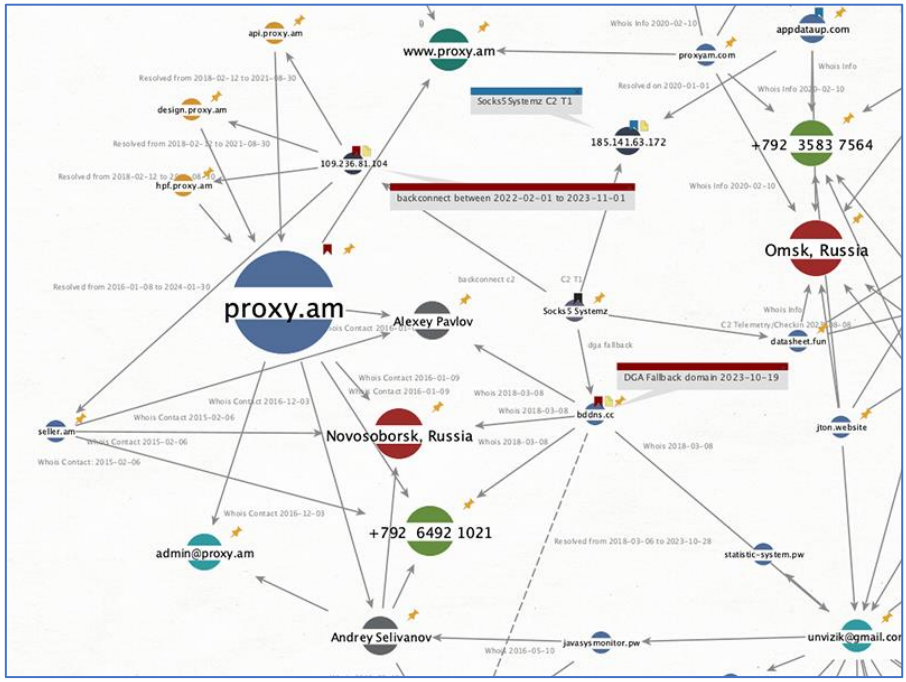

Figura 6 – Gráfico de relacionamento entre bddns[.]cc, proxy[.]am e 109.235.81[.]104.

Entre dezembro de 2023 e outubro de 2024, foram implementadas várias mudanças na infraestrutura de malware e C2. Com identificação das seguintes alterações:

Nova infraestrutura

- Total de 26 servidores (14 servidores de backconnect, 6 servidores C2, 5 servidores de nomes e 1 servidor de fallback)
- Maior distribuição geográfica na Europa
- Novos provedores de hospedagem
- Novos domínios de fallback

Atualizações de malware

- Protocolo C2 atualizado
- Novas chaves RC4, novos caminhos de URL e novo formato de dados de beacon
- O protocolo de backconnect agora utiliza a porta 2023/TCP
- Ofuscação aprimorada, dificultando a extração estática da configuração do malware

Apesar dessas mudanças, a funcionalidade principal do malware permanece a mesma.

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:

Use segurança de endpoint

- Instale e mantenha atualizado software antivírus e antimalware para detectar e prevenir ameaças.

Mantenha o software atualizado

- Certifique-se de que todos os sistemas operacionais, aplicativos e firmware estejam sempre com as últimas atualizações e patches de segurança.

Aumente a segurança da rede

- Utilize firewalls, sistemas de detecção e prevenção de intrusões (IDS/IPS) e configure corretamente os roteadores e switches para bloquear tráfego malicioso.

Eduque os funcionários

- Realize treinamentos regulares sobre segurança cibernética para que todos estejam cientes das práticas seguras e dos riscos de phishing e outras ameaças.

Use filtragem de e-mail

- Implemente soluções de filtragem de e-mail para bloquear anexos e links suspeitos que possam conter malware.

Execute backups regulares de dados

- Mantenha backups atualizados e verifique regularmente a integridade dos mesmos para garantir que você possa recuperar dados em caso de ataque1.

Monitore a atividade da rede

- Utilize ferramentas de monitoramento para detectar atividades incomuns ou suspeitas na rede, permitindo uma resposta rápida a possíveis incidentes.

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:	075a974d14a2b012c9d788bd4ade329a
sha1:	3d04e0af21433e93f3620d5cea1f4a32702ba298
sha256:	36cffd7d54385e0473cb7f7bf2d33910027428837725c4d3649ff1af2d88cb2b
File name:	075a974d14a2b012c9d788bd4ade329a.vírus

Indicadores do artefato	
md5:	5237853dbebaefb1dfa86130dd1d39fa
sha1:	c2a42211c8970e1f10cc13261d5e133739c196f4
sha256:	e185e43f039f7a97672db4a44597abd6d2bf49c08d7bc689318a098ec826bb00
File name:	e185e43f039f7a97672db4a44597abd6d2bf49c08d7bc689318a098ec826bb00.exe

Indicadores do artefato	
md5:	98b539f752bc0735b9e6b19999731d6a
sha1:	6b58d1dc84db0fc83bc8cd7ceaace406c2f3827c
sha256:	0fc2f189aa3ebc1ff836079e49dac9758ab5e807d7ab4b42ff37c2376bcc2705
File name:	98b539f752bc0735b9e6b19999731d6a.vírus

Indicadores do artefato	
md5:	8b4a85fb7df7b9f47c36977a5e39793e
sha1:	7a6fa117f6c150ac9a5423d984292b465fce51d8
sha256:	bf34984756336bc78428f3f856be287ef364afa3330cac5facf019c39be73657
File name:	7a6fa117f6c150ac9a5423d984292b465fce51d8.bin

Tabela 2 – Indicadores de Comprometimento

Indicadores de URL, IPs e Domínios

Indicadores de URL, IPs e Domínios	
IP	141[.]98[.]234[.]31 81[.]31[.]197[.]38 45[.]155[.]250[.]90 152[.]89[.]198[.]214 91[.]211[.]247[.]248 185[.]208[.]158[.]248 185[.]237[.]207[.]107 185[.]208[.]158[.]202 79[.]132[.]128[.]13 176[.]10[.]111[.]126 194[.]62[.]105[.]143 195[.]154[.]176[.]209 89[.]105[.]201[.]183 46[.]8[.]225[.]74 88[.]80[.]150[.]13 195[.]154[.]174[.]225 62[.]210[.]201[.]223 185[.]141[.]63[.]209 195[.]154[.]173[.]35 195[.]154[.]174[.]12 62[.]210[.]204[.]81 62[.]210[.]204[.]131 185[.]141[.]63[.]216 195[.]154[.]185[.]134 88[.]80[.]148[.]252

Tabela 3 – 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**
- **Bitsight**
- **Thehackernews**

5 AUTORES

- **Leonardo Oliveira Silva**

heimdall
security research
A DIVISION OF ISH