ALERTA DE SEGURANÇA

Violação da Snowflake por ator de ameaça

heimdall
security research
A DIVISION OF ISH

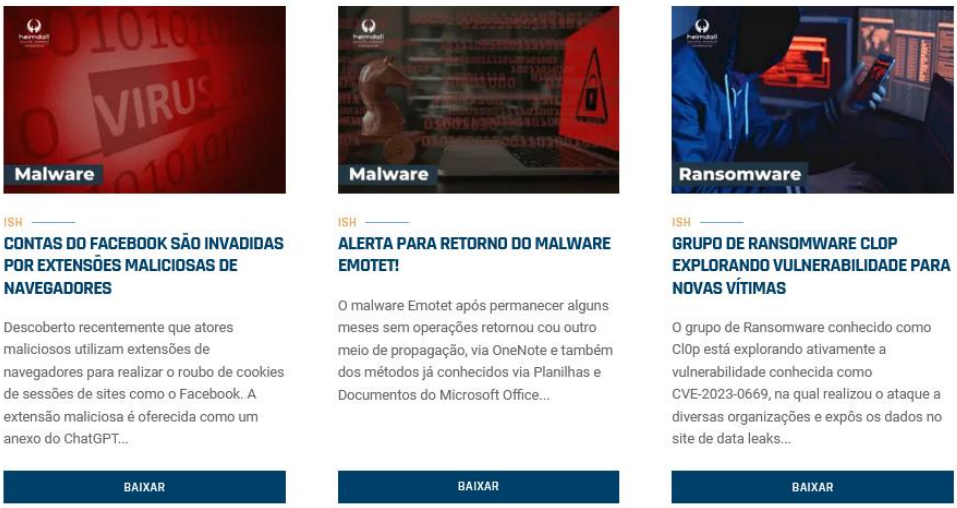
TLP: CLEAR

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 FIGURAS

LISTA DE TABELAS

1 SOBRE OS FATOS IDENTIFICADOS SNOWFLAKE

Um ator de ameaça conhecido como **Shinyhunters e SpidermanData** teria anunciado em um fórum clandestino a venda de aproximadamente 560 milhões de contas de usuários, bem como 1.3 TB de dados de Cartões Bancários.

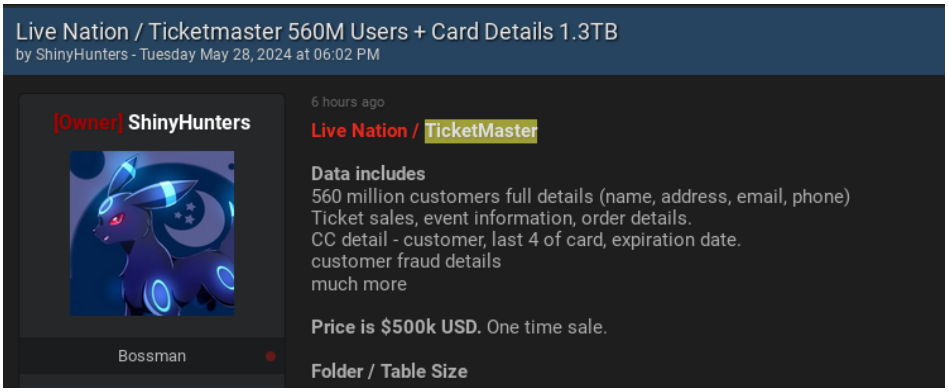


Figura 1 – Publicação no fórum BreachFóruns.

Vale salientar que a publicação teria também sido publicada por outro perfil em um fórum clandestino Russo conhecido como Exploit.in, não havendo a possibilidade de vincular ambos os perfis até o momento. De qualquer forma, a publicação de ambos os atores foi no intuito de extorquir a empresa proprietária.

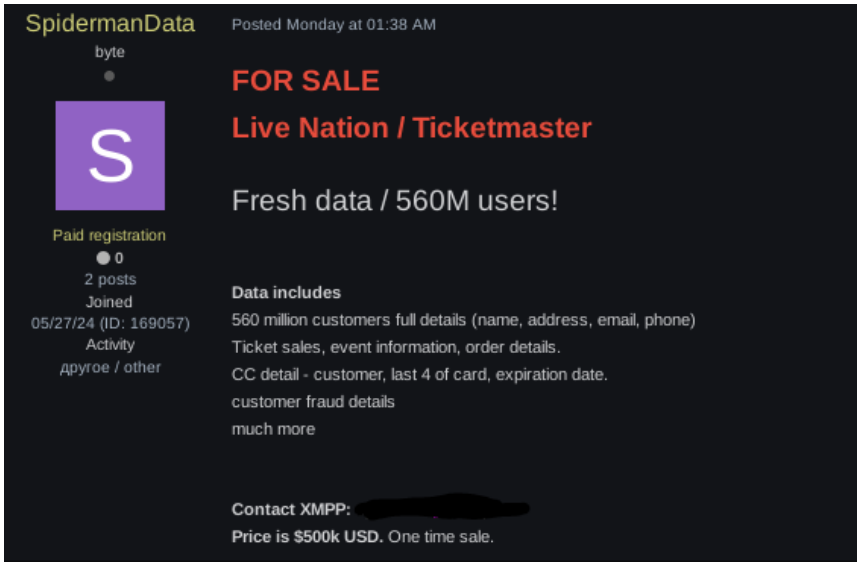
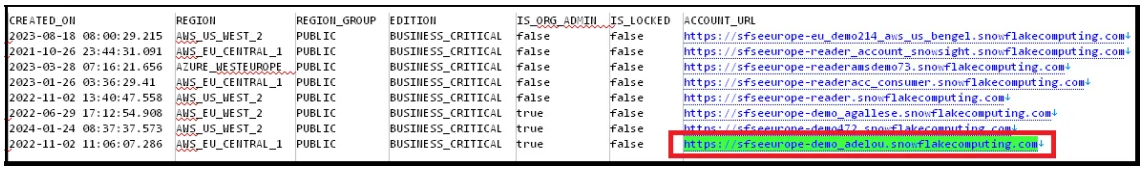


Figura 2 – Publicação no Fórum do Exploit.In.

Antes de abordamos sobre os atores, é válido mencionar que de acordo com as pesquisas, a empresa Snowflake teria sofrido um incidente de segurança em 31

de maio de 2024, na qual a empresa Hudson Rock compartilhou capturas de telas afirmando que um ator de ameaça alegou ter utilizado as credenciais roubadas de um funcionário da empresa para exfiltrar grandes quantidades de dados de clientes, incluindo das empresas Santander e Ticketmaster. A empresa teria afirmado que estariam investigando uma campanha direcionada para os usuários, mas que não havia evidências que sugeriram exfiltração de dados.



CREATED_ON	REGION	REGION_GROUP	EDITION	IS_ORG_ADMIN	IS_LOCKED	ACCOUNT_URL
2023-08-18 08:00:29.215	AWS_US_WEST_2	PUBLIC	BUSINESS_CRITICAL	false	false	https://sfseeurope-eu_demo214_aws_us_bengel.snowflakecomputing.com
2021-10-26 23:44:31.091	AWS_EU_CENTRAL_1	PUBLIC	BUSINESS_CRITICAL	false	false	https://sfseeurope-reader_account_snowsight.snowflakecomputing.com
2023-03-28 07:16:21.656	AZURE_WESTEUROPE	PUBLIC	BUSINESS_CRITICAL	false	false	https://sfseeurope-readeramsdemo73.snowflakecomputing.com
2023-01-26 03:36:29.41	AWS_EU_CENTRAL_1	PUBLIC	BUSINESS_CRITICAL	false	false	https://sfseeurope-readeracc_consumer.snowflakecomputing.com
2022-11-02 13:40:47.558	AWS_US_WEST_2	PUBLIC	BUSINESS_CRITICAL	false	false	https://sfseeurope-reader.snowflakecomputing.com
2022-06-29 17:12:54.908	AWS_EU_WEST_2	PUBLIC	BUSINESS_CRITICAL	true	false	https://sfseeurope-demo_agallese.snowflakecomputing.com
2024-01-24 08:37:37.573	AWS_US_WEST_2	PUBLIC	BUSINESS_CRITICAL	true	false	https://sfseeurope-demo172.snowflakecomputing.com
2022-11-02 11:06:07.286	AWS_EU_CENTRAL_1	PUBLIC	BUSINESS_CRITICAL	true	false	https://sfseeurope-demo_adelou.snowflakecomputing.com

Figura 3 – Informações da empresa Hudson Rock sobre potencial violação.

De qualquer forma, a Snowflake teria publicado um boletim de segurança com indicadores de comprometimento (IoCs) e mais detalhes relacionados a implementar seguranças em suas contas. (Os endereços de IPs se encontram ao final deste relatório).

Além dos endereços de IPs, as conexões de client como “RapeFlake” ou “DBeaver_DBeaverUltimate” em execução no Windows Server 2022 deveria ser examinada, haja vista que são conhecidas por estarem associadas à exfiltração de dados.

A equipe de inteligência realizou a pesquisa sobre o ator de ameaças, na qual ShinyHunters, também conhecido como ShinyCorp, é um grupo de cibercriminosos que emergiu em 2020. Rapidamente ganhou notoriedade por realizar uma série de violações de dados de grande escala. Embora o nome, inspirado em Pokémon, possa sugerir um grupo de fãs inofensivos, a realidade é que o ShinyHunters está fortemente envolvido em atividades criminosas online, com especialização na aquisição e comercialização de extensos bancos de dados.

O grupo emprega uma variedade de estratégias para se infiltrar e explorar vulnerabilidades em sistemas digitais. Aqui está uma visão geral simplificada de como os ShinyHunters normalmente conduzem suas operações de hacking, como, vasculhando repositórios GitHub, explorando buckets de nuvem inseguros, visa sites e ferramentas de desenvolvedor, implementação de ataques de phishing.

Outro detalhe relevante, é que o telegram utilizado pelo ator de ameaça em questão foi possível identificar que ele já teria se manifestado em outras comunidades de ransomwares, que inclusive, teria afirmado que havia realizado o ataque a uma organização, cuja organização teria sido mencionada como vítima de um dos notórios grupos de ransomware, conhecidos como Scattered Spider (ALPHV/ Black Cat). É valido salientar que isto não comprova realmente que o ator

de ameaça estaria envolvido com ransomware, mas que são informações relevantes dada ao suposto incidente de segurança anunciado.

Em atualização aos dados coletados, a empresa Snowflake não teria confirmado o relatório mencionado anteriormente, mas em vez disso afirmou que o ator de ameaça teria comprometido contas de clientes nessas violações e não explorou nenhuma vulnerabilidade ou configuração incorreta nos produtos da organização.

O provedor do serviço de nuvem teria alertado na sexta-feira (03 de junho de 2024) os seus clientes que estaria investigando um “aumento” nos ataques direcionados a algumas de suas contas.

De acordo com o CISO da Snowflakes, Brad Jones afirmou que foi tomado o conhecimento do acesso potencialmente não autorizado a determinadas contas de clientes em 23 de maio de 2024. Durante a investigação, foi observado um aumento na atividade de ameaças a partir de meados de abril de 2024 a patir de um subconjunto de endereços IP e clientes suspeitos que acreditaram estar relacionados aos acessos não autorizados.

O CISO ainda adiciou que não acreditava que a atividade teria sido causada por qualquer vulnerabilidade, configuração incorreta ou atividade maliciosa no produto Snowflake.

Foi realizada ainda conforme mencionado acima, um boletim com os Indicadores de Comprometimento (IoCs), bem como de acordo com a publicação da Snowflake, pelo menos **165 organizações provavelmente foram impactadas pelo ataque.**

2 RELATÓRIO PUBLICADO PELA GOOGLE

A Google através da equipe de resposta a incidente e inteligência de ameaças conhecida como Mandiant, teria identificado uma campanha de atores de ameaças direcionadas a instâncias de banco de dados de clientes Snowflake com a intenção de roubo de dados e extorsão.

A Mandiant classificou e nomeou a ameaça como **UNC5537**, um ator de ameaças com motivação financeira suspeito de ter roubado um volume significativo de registros de ambientes de clientes Snowflake. O UNC5537 estaria comprometendo sistematicamente instâncias de clientes Snowflake usando credenciais de clientes roubadas, anunciando dados de vítimas para venda em fóruns de crimes cibernéticos e tentando extorquir muitas das vítimas.

Eles concluíram ainda que todos os clientes das quais a Mandiant respondeu estaria rastreado até as credenciais dos clientes comprometidos da Snowflake.

Segundo a Mandiant, em abril de 2024, eles teriam recebido a inteligência sobre ameaças em registros de banco de dados que foram posteriormente determinados como originados da instância Snowflake de uma vítima. O ator de ameaça utilizou as credenciais roubadas para acessar as instâncias Snowflake do cliente e, por fim, exfiltrar dados valiosos. No momento do comprometimento, a conta não tinha autenticação multifator (MFA) habilitada.

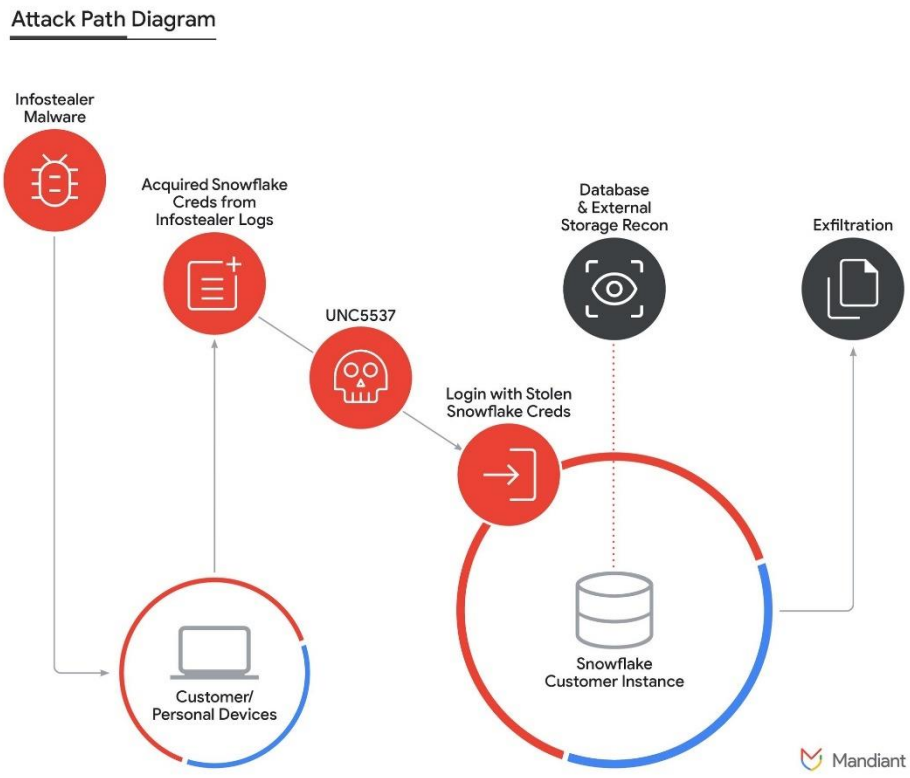


Figura 4 – Linha do tempo da campanha até a exfiltração dos dados.

A campanha e maioria das credenciais utilizadas pelo UNC5537 estavam disponíveis em infecções históricas por infostealers, algumas das quais datavam de 2020. A violação, teria resultado em vários compromissos bem-sucedidos, devido a três fatores:

1. Contas afetadas não foram configuradas com a autenticação multifator habilitada.
2. As credenciais identificadas na saída do malware infostealer ainda eram válidas.
3. As instâncias de clientes Snowflake afetas não tinham listas de permissões de rede em vigor para permitir acesso apenas de locais confiáveis.

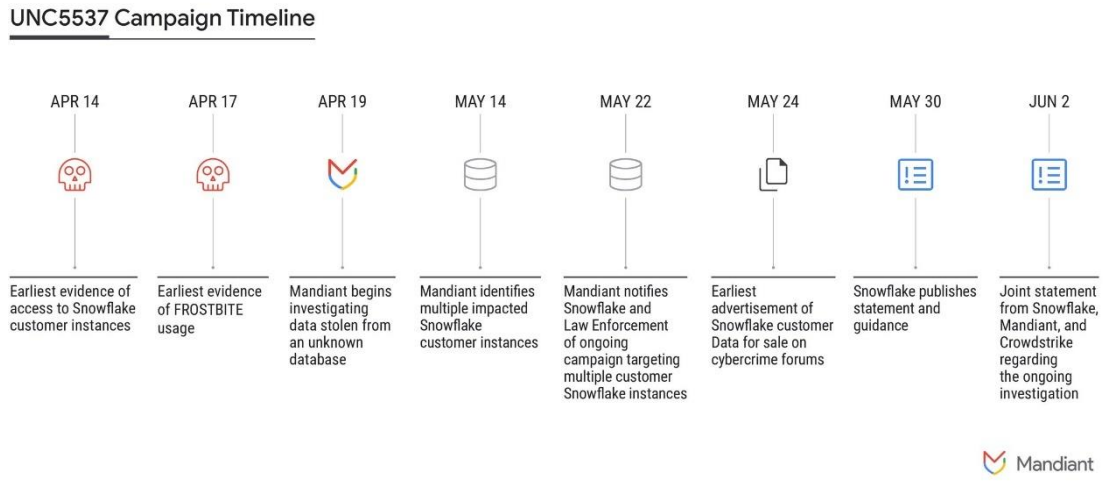


Figura 5 – Cronograma da campanha utilizada pelo ator de ameaça.

A Mandiant identificou que o ator de ameaças teria utilizado de fontes de diversas variantes de malwares infostealers, como: VIDAR, RISEPRO, REDLINE, RACOON STEALER, LUMMA e METASTEALER.

A fase de **Reconhecimento** e **Acesso Iniciais** às instâncias do cliente Snowflake geralmente ocorria por meiod a interface de usuário nativa baseada na Web (SnowFlake UI, também conhecido como SnowSight) e/ou ferramenta de interface de linha de comando em execução no Windows Server 2022. A Mantiant identificou acesso adicional aproveitando um invasor nomeado como “rapeflake”, rastreado pela Mandiant como FROSTBITE.

O ator de ameaça teria executado repetidamente comandos SQL semelhantes em várias instâncias Snowflake de clientes para preparar e exfiltração de dados.

O rastreamento da Mandiant concluiu que o ator de ameaça estaria utilizando um cluster distinto desde maio de 2024, cujo ator UNC5537 tem como

alvo centenas de organizações em todo o mundo e frequentemente extorque as vítimas para obter ganhos financeiros. O ator de ameaça também opera sob vários pseudônimos em canais no Telegram e fóruns de crimes cibernéticos.

Quanto a infraestrutura do invasor, o UNC5537 utilizou principalmente endereços de IP VPN Mullvad ou Private Internace Access (PIA) para acessar instâncias SnowFlake das vítimas. Ao exfiltrar dados, a Mandiant observou o uso de sistemas VPS da ALEXHOST SRL (AS200019), um fornecedor moldavo. O UNC5537 foi observado armazenado dados de vítimas roubadas em vários provedores internacionais de VPS, bem como no provedor de armazenamento em nuvem MEGA.

Por fim, a Mandiant concluiu que a campanha não é o resultado de nenhuma ferramenta, técnica ou procedimento particularmente novo ou sofisticado. O amplo impacto desta campanha é a consequência do crescente mercado de infostealers e das oportunidades perdidas para proteger ainda mais as credenciais.

3 EMPRESA PURE STORAGE CONFIRMOU VIOLAÇÃO

A empresa Pure Storage, fornecedora líder de sistemas e serviços de armazenamento em nuvem, confirmou que invasores violaram o seu espaço de trabalho Snowflake e obtiveram acesso ao que a empresa descreveu como informações de telemetria.

Embora as informações expostas também incluíssem nomes de clientes, nomes de usuários e endereços de e-mail, elas não continham credenciais para acesso ao *array* ou quaisquer outros dados armazenados nos sistemas dos clientes.

De acordo com o comunicado, a Pure Storage afirmou que as informações afetadas incluem nomes de empresas, nomes de usuários LDAP, endereços de e-mail e o número da versão do software Purity.

4 MITRE ATT&CK - TTPs

Tática	Técnica	Detalhes
Reconnaissance	T1589.001 T1589.002 T1598	Os adversários podem enviar mensagens de phishing para obter informações confidenciais que podem ser usadas durante a segmentação.
Initial Access	T1566 T1078.002 T1078.004	Consiste em técnicas que utilizam vários vetores de entrada para obter sua posição inicial dentro de uma rede.
Credential Access	T1528	Consiste em técnicas para roubar credenciais, como nomes de contas e senhas.
Discovery	T1580	Um adversário pode tentar descobrir infraestrutura e recursos disponíveis em um ambiente de infraestrutura como serviço (IaaS).
Lateral Movement	T1210 T1072	Consiste em técnicas que os adversários usam para entrar e controlar sistemas remotos em uma rede.
Collection	T1530 T1213	Consiste em técnicas que os adversários podem usar para coletar informações e nas fontes das quais as informações são coletadas que são relevantes para cumprir os objetivos do adversário.
Exfiltration	T1567	Consiste em técnicas que os adversários podem usar para roubar dados da sua rede.

Tabela 1 – Tabela MITRE ATT&CK.

5 RECOMENDAÇÕES

Atualizações de segurança

- Mantenha todos os sistemas e softwares atualizados com as últimas correções de segurança.

Autenticação de multi fator e logon único (SSO)

- Implemente a autenticação de dois fatores sempre que possível para adicionar uma camada extra de segurança.

Educação em Segurança Cibernética

- Realize treinamentos regulares de conscientização em segurança cibernética para os funcionários.

Monitoramento de rede

- Monitore continuamente a rede para detectar atividades suspeitas.

Backup de dados

- Mantenha backups regulares de dados importantes.

Firewalls e Antivírus

- Use firewalls e software antivírus para proteger contra ameaças.

Gerenciamento de senhas

- Use gerenciadores de senhas para criar e armazenar senhas fortes e únicas para cada conta.

Criptografia de dados

- Criptografe dados sensíveis para protegê-los, mesmo em caso de violação.

Política de acesso

- Implemente uma política de acesso mínimo, garantindo que os funcionários tenham apenas o acesso necessário para realizar suas tarefas.

Plano de resposta a incidentes

- Tenha um plano de resposta a incidentes de segurança cibernética em vigor para garantir uma ação rápida em caso de violação

6 INDICADORES DE COMPROMISSOS

Indicadores fornecidos pelo relatório da empresa **Snowflak** e da **Mandiant.**

104.223.91.28	185.213.155.241	102.165.16.161	194.230.145.76
198.54.135.99	198.44.136.82	104.129.24.115	194.230.147.127
184.147.100.29	93.115.0.49	104.129.24.124	194.230.148.99
146.70.117.210	204.152.216.105	104.223.91.28	194.230.158.107
198.54.130.153	198.44.129.82	146.70.117.210	194.230.158.178
169.150.203.22	185.248.85.59	146.70.117.56	194.230.160.237
185.156.46.163	198.54.131.152	146.70.119.24	194.230.160.5
146.70.171.99	102.165.16.161	146.70.124.216	198.44.129.82
206.217.206.108	185.156.46.144	146.70.165.227	198.44.136.56
45.86.221.146	45.134.140.144	146.70.166.176	198.44.136.82
193.32.126.233	198.54.135.35	146.70.171.112	198.54.130.153
87.249.134.11	176.123.3.132	146.70.171.99	198.54.131.152
66.115.189.247	185.248.85.14	154.47.30.137	198.54.135.35
104.129.24.124	169.150.223.208	154.47.30.150	198.54.135.67
146.70.171.112	162.33.177.32	162.33.177.32	198.54.135.99
198.54.135.67	194.230.145.67	169.150.201.25	204.152.216.105
146.70.124.216	5.47.87.202	169.150.203.22	206.217.205.49
45.134.142.200	194.230.160.5	169.150.223.208	206.217.206.108
206.217.205.49	194.230.147.127	173.44.63.112	37.19.210.21
146.70.117.56	176.220.186.152	176.123.3.132	37.19.210.34
169.150.201.25	194.230.160.237	176.123.6.193	45.134.140.144
66.63.167.147	194.230.158.178	176.220.186.152	45.134.142.200
194.230.144.126	194.230.145.76	184.147.100.29	45.155.91.99
146.70.165.227	45.155.91.99	185.156.46.144	45.27.26.205
154.47.30.137	194.230.158.107	185.156.46.163	45.86.221.146
154.47.30.150	194.230.148.99	185.204.1.178	5.47.87.202
96.44.191.140	194.230.144.50	185.213.155.241	66.115.189.247
146.70.166.176	185.204.1.178	185.248.85.14	66.63.167.147
198.44.136.56	79.127.217.44	185.248.85.59	79.127.217.44
176.123.6.193	104.129.24.115	192.252.212.60	87.249.134.11
192.252.212.60	146.70.119.24	193.32.126.233	93.115.0.49
173.44.63.112	138.199.34.144	194.230.144.126	194.230.145.67
37.19.210.34	185.248.85.14	194.230.144.50	96.44.191.140
37.19.210.21			

Tabela 2 – Indicadores de Redes de endereços de IPs.

7 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Publicação da Snowflake sobre incidente de segurança**
- **Comunicado e publicação sobre UNC5537 – Google Threat Intel**
- **Informações sobre vinculação de ataques**
- **Comunicado Pure Storage sobre violação**
- **Publicação da Ticketmaster sobre incidente de segurança**
- **SocRadar**

heimdall
security research
A DIVISION OF ISH