heimdall
security research

RELATÓRIO SEMESTRAL DE VULNERABILIDADES

Apontamos as **principais vulnerabilidades** críticas e grupos de Ransomware ativos mais perigosos do primeiro semestre de 2024

SUMÁRIO

LISTA DE TABELAS

LISTA DE FIGURAS

1 SUMÁRIO EXECUTIVO

Este relatório aborda as principais vulnerabilidades cibernéticas identificadas em 2024, com base no catálogo KEV (Known Exploited Vulnerabilities) da CISA e nas estatísticas de ataques de ransomware coletadas pela IS Tecnologia durante o primeiro semestre do ano. A importância deste documento reside na sua capacidade de orientar organizações na priorização de ações de mitigação e na implementação de estratégias de defesa eficazes contra ameaças emergentes.

As vulnerabilidades destacadas neste ano incluem **falhas críticas em sistemas operacionais** amplamente utilizados, softwares de infraestrutura e aplicações web. Estas falhas permitem a execução de código remoto, escalonamento de privilégios e ataques de negação de serviço, representando riscos significativos para a segurança das informações.

O **catálogo KEV** é uma ferramenta vital para organizações que buscam entender quais vulnerabilidades já foram exploradas ativamente por agentes de ameaças. O relatório detalha as vulnerabilidades que foram adicionadas ao catálogo em 2024, destacando a necessidade de patches urgentes e revisão de políticas de segurança.

A **ISH Tecnologia** compilou dados extensivos sobre incidentes de ransomware que impactaram setores críticos no primeiro semestre de 2024. O relatório apresenta os dados de ataques de 2024 em comparação com o ano de 2023, bem como apresenta os principais países e estatísticas de grupos.

Este relatório serve como um recurso essencial para líderes de TI e de segurança cibernética, proporcionando insights críticos que podem ajudar a fortalecer as posturas de segurança contra as sofisticadas ameaças digitais de hoje.

AUTORES
Caique Barqueta
Especialista em Inteligência de Ameaças

Ismael Rocha
Analista de Inteligência de Ameaças Sênior

2 PRINCIPAIS VULNERABILIDADES

A equipe de inteligência apresenta algumas das **principais vulnerabilidades identificadas** no primeiro semestre de 2024.

No relatório, são elencados os produtos afetados, os grupos que realizaram a exploração, a base de pontuação e as possíveis mitigações.

CVE-2024-20253

Base de pontuação: 10 (Crítico)

Esta vulnerabilidade pode causar a execução arbitrário de código em um dispositivo afetado por um invasor/ator não autenticado.

PRODUTO:
Cisco Unified Communications Manager e relacionados.

MITIGAÇÃO:
Aplicação dos patches fornecidos pela Cisco e atualização para as versões mais recentes dos produtos afetados.

EXPLORAÇÕES:
Um dos atores de ameaças que foram identificados como explorando a vulnerabilidade, foi o grupo UNC3886, correlacionado à China, explorou a vulnerabilidade para implantar backdoors em sistemas VMware vCenter. Os atores conseguiram acessar credenciais de ESXi hosts conectados ao vCenter e instalaram backdoors adicionais para manter acesso persistente e realizar comandos não autenticados.

CVE-2024-4577

Base de pontuação: 9.8 (Crítico)

Esta vulnerabilidade pode permitir que atores de ameaças utilize caracteres como opções do PHP, permitindo a execução, revelando o código-fonte dos scripts, execução de códigos PHP arbitrários e outros.

PRODUTO:
Versões PHP 8.1.* antes de 8.1.29, 8.2.* antes de 8.2.20, 8.3.* que usam o Apache e PHP-CGI no Windows.

MITIGAÇÃO:
Necessário aplicar as mitigações de acordo com as instruções do fornecedor.

EXPLORAÇÕES:
O grupo de ransomware conhecido como TellYouThePass utilizou esta falha para implantar webshells e ransomwares em servidores alvos.

2 PRINCIPAIS VULNERABILIDADES

CVE-2024-21887

Base de pontuação: 9.1 (Crítico)

Esta vulnerabilidade pode causar a injeção de comando em componentes web do Ivanti Connect Secure e do Ivanti Policy Securte, permitindo que um administrador autenticado envie solicitações especialmente criadas e execute comandos arbitrários.

PRODUTO:
Ivanti Connect Secure (9.x, 22.x) e Ivanti Policy Secure (9.x, 22.x)

MITIGAÇÃO:
Aplicação dos patches recomendados pela Ivanti e revisão das diretrizes informadas pela CISA em alertas.

EXPLORAÇÕES: Um grupo de ator de ameaças conhecidos como UNC5221 utilizou estas vulnerabilidades para implantar malwares, incluindo malwares do tipo backdoors e webshells em quase 20.000 instâncias.

CVE-2024-24919

Base de pontuação: 8.6 (Alto)

Permite que um invasor leia certas informações nos gateways de segurança da Check Point, uma vez que conectado à internet e habilitado com VPN de acesso remoto ou software blades de acesso.

PRODUTO: Check Point Quantum Security Gateways
Mitigação: Atualização para as versões mais recentes dos produtos da Check Point.

EXPLORAÇÕES: Esta vulnerabilidade foi observada sendo explorada por atores de ameaças com o foco em infraestruturas críticas.

CVE-2024-30080

Base de pontuação: 9.8 (Crítico)

Ocasiona uma execução remota de código no Microsoft Message Queuing (MSMQ).

PRODUTO: Microsoft Message Queuing (MSMQ)
Mitigação: Aplicação dos patches de segurança publicados pela Microsoft em junho de 2024.

EXPLORAÇÕES: Esta vulnerabilidade foi identificada sendo explorada por atores de ameaças do tipo APT e grupos de ransomwares, haja vista a sua facilidade em exploração remota.

CVE-2024-29988

Base de pontuação: 8.8 (Alta)

Esta vulnerabilidade pode ocasionar o desvio de recursos de segurança do prompt do SmartScreen, ou seja, é utilizada para fins de bypass do recurso de segurança.

PRODUTO: Prompt SmartScreen (Microsoft)

MITIGAÇÃO: Aplicação dos patches de segurança mais recente lançados pela Microsoft em abril de 2024.

EXPLORAÇÕES: Esta vulnerabilidade foi utilizada pelo grupo Water Hydra para contornar o Microsoft Defender SmartScreen para entrega

2 PRINCIPAIS VULNERABILIDADES

CVE-2024-1708 e CVE-2024-1709

Base de pontuação:
CVE-2024-1708: **8.4 (Alto)**
CVE-2024-1709: **10 (Crítica)**

Esta vulnerabilidade pode ocasionar a execução de código remoto e impactar diretamente dados confidenciais ou sistemas críticos.

PRODUTO:
ConnectWise ScreenConnect 23.9.7 e anteriores.

MITIGAÇÃO:
Aplicar as atualizações de segurança fornecidas pela ConnectWise para a versão 23.9.10.8817 do ScreenConnect.

CVE-2024-5274

Base de pontuação: 8.8 (Alto)

Permite que um invasor execute código arbitrário dentro de uma sandbox por meio de uma página de HTML criada.

PRODUTO:
Google Chromium V8 anterior a 125.0.6422.112

MITIGAÇÃO:
Aplicar as atualizações de segurança mais recentes fornecidas pelo Google para o Chromium.

CVE-2024-1086

Base de pontuação: 7.8 (Alto)

Esta vulnerabilidade se explorável por obter escalonamento de privilégios locais.

PRODUTO:
Linux Kernel

MITIGAÇÃO:
Aplicar as atuações fornecidas pelo projeto de desenvolvimento de código aberto.

3 VULNERABILIDADES ADICIONADAS PELA CISA (KEV)

A **CISA** (America's Cyber Defense Agency) organiza a utiliza um catálogo de vulnerabilidades conhecidas e exploradas ativamente em incidentes de segurança (KEV), dentre as quais listamos abaixo qual o número, base de pontuação e ator de ameaça vinculado a vulnerabilidade.

CVE ID	Score	Data do alerta	Ator(es) de Ameaça
CVE-2023-7101	7.8	02/01/2024	Grupo Chinês (UNC4841)
CVE-2023-7024	8.8	02/01/2024	Grupo Chinês (UNC4841)
CVE-2023-29300	9.8	08/01/2024	Não atribuído
CVE-2023-23752	5.3	08/01/2024	GambleForce
CVE-2016-20017	9.8	08/01/2024	Botnet Mirai
CVE-2023-41990	7.8	08/01/2024	Não atribuído
CVE-2023-27524	9.8	08/01/2024	Não atribuído
CVE-2023-38203	9.8	08/01/2024	GambleForce
CVE-2023-29357	9.8	10/01/2024	Não atribuído
CVE-2023-46805	8.2	10/01/2024	UNC5221, UTA0178 e UTA0188
CVE-2024-21887	9.1	10/01/2024	UNC5221, UTA0178 e UTA0188
CVE-2018-15133	8.1	16/01/2024	Malware Androxgh0st
CVE-2024-0519	8.8	17/01/2024	Não atribuído
CVE-2023-6549	8.2	17/01/2024	Não atribuído
CVE-2023-6548	8.8	17/01/2024	Não atribuído
CVE-2023-35082	9.8	18/01/2024	Não atribuído
CVE-2023-34048	9.8	22/01/2024	UNC3886
CVE-2024-23222	8.8	23/01/2024	Não atribuído
CVE-2023-22527	9.8	24/01/2024	Ransomware BianLian
CVE-2022-48618	7.0	31/01/2024	Não atribuído
CVE-2024-21893	8.2	31/01/2024	UNC5325 e UNC3886
CVE-2023-4762	8.8	06/02/2024	Malware Predator Spyware
CVE-2024-21762	9.8	09/02/2024	Não atribuído
CVE-2023-43770	6.1	12/02/2024	TAG-70, Winter Vivern e Fancy Bear
CVE-2024-21412	8.1	13/02/2024	APT Water Hydra

3 VULNERABILIDADES ADICIONADAS PELA CISA (KEV)

CVE ID	Score	Data do alerta	Ator(es) de Ameaça
CVE-2024-21351	7.6	13/02/2024	APT Water Hydra
CVE-2020-3259	7.5	15/02/2024	Ransomware Akira
CVE-2024-21410	9.8	15/02/2024	Não atribuído
CVE-2024-1709	10	22/02/2024	Ransomware Black Basta, Bl00dy e malware XWORM.
CVE-2023-29360	8.4	29/02/2024	Malware Raspberry Robin
CVE-2020-21338	7.8	04/03/2024	APT Lazarus
CVE-2023-21237	5.5	05/03/2024	Não atribuído
CVE-2021-36380	9.8	05/03/2024	Não atribuído
CVE-2024-23225	7.8	06/03/2024	Não atribuído
CVE-2024-23296	7.8	06/03/2024	Não atribuído
CVE-2024-27198	9.8	07/03/2024	Ransomware BianLian e Jasmin Ransomware
CVE-2019-7256	10	25/03/2024	Não atribuído
CVE-2021-44529	9.8	25/03/2024	Ransomware ALPHA SPIDER
CVE-2023-48788	9.8	25/03/2024	Não atribuído
CVE-2023-24955	7.2	26/03/2024	Não atribuído
CVE-2024-29748	7.8	04/04/2024	Não atribuído
CVE-2024-29745	5.5	04/04/2024	Não atribuído
CVE-2024-3273	9.8	11/04/2024	Não atribuído
CVE-2024-3272	9.8	11/04/2024	Não atribuído
CVE-2024-3400	10	12/04/2024	Não atribuído
CVE-2022-38028	7.8	23/04/2024	Fancy Bear (APT 28)
CVE-2024-4040	10	24/04/2024	Não atribuído
CVE-2024-20359	6	24/04/2024	UAT4356 ou STORM-1849
CVE-2024-20353	8.6	24/04/2024	UAT4356 ou STORM-1849
CVE-2024-29988	8.8	30/04/2024	Não atribuído
CVE-2023-7028	10	01/05/2024	Não atribuído
CVE-2024-4671	9.6	13/05/2024	Não atribuído
CVE-2024-30040	8.8	14/05/2024	Não atribuído
CVE-2024-30051	7.8	14/05/2024	Malware QakBot
CVE-2024-4761	8.8	16/05/2024	Malware QakBot
CVE-2021-40655	7.5	16/05/2024	Não atribuído
CVE-2014-100005	6.8	16/05/2024	Não atribuído
CVE-2024-4947	9.6	20/05/2024	Não atribuído
CVE-2023-43208	9.8	20/05/2024	Não atribuído
CVE-2020-17519	9.1	23/05/2024	Não atribuído
CVE-2024-5274	8.8	28/05/2024	Não atribuído
CVE-2024-4978	8.4	29/05/2024	Não atribuído
CVE-2024-1086	7.8	30/05/2024	Não atribuído
CVE-2024-24919	8.6	30/05/2024	Não atribuído
CVE-2017-3506	7.4	03/06/2024	8220 Gang

3 VULNERABILIDADES ADICIONADAS PELA CISA (KEV)

CVE ID	Score	Data do alerta	Ator(es) de Ameaça
CVE-2024-4577	9.8	12/06/2024	Ransomware TellYouThePass
CVE-2024-4610	7.4	12/06/2024	Não atribuído
CVE-2024-4358	9.8	13/06/2024	Não atribuído
CVE-2024-26169	7.8	13/06/2024	Ransomware Black Basta
CVE-2024-32896	8.1	13/06/2024	Não atribuído
CVE-2020-13965	6.3	26/06/2024	Não atribuído
CVE-2022-2586	7.8	26/06/2024	Não atribuído
CVE-2022-24816	10	26/06/2024	Não atribuído

Tabela 1 – Vulnerabilidades adicionadas pela CISA ao Catálogo KEV.

Um dos fatos interessantes, é que a lista é atualizada conforme os atores de ameaças são detectados pelas organizações como explorando a vulnerabilidade, indicando que, caso uma organização tenha sido vítima de uma exploração de vulnerabilidade e não comunique ou compartilhe o resultado das investigações, fica inviável atribuir um ator de ameaça ou adicionar a CVE junto ao catálogo mantido pela CISA.

ESTATÍSTICAS DE RANSOMWARES

4 ESTATÍSTICAS DE RANSOMWARES

A **ISH Tecnologia** também realiza a coleta de dados estatísticos relacionados às atividades de atores de ransomware. Dentre os dados coletados, foi possível identificar e compartilhar as seguintes estatísticas:

INDICATIVOS DE ATAQUES A ORGANIZAÇÕES VÍTIMAS DE RANSOMWARES

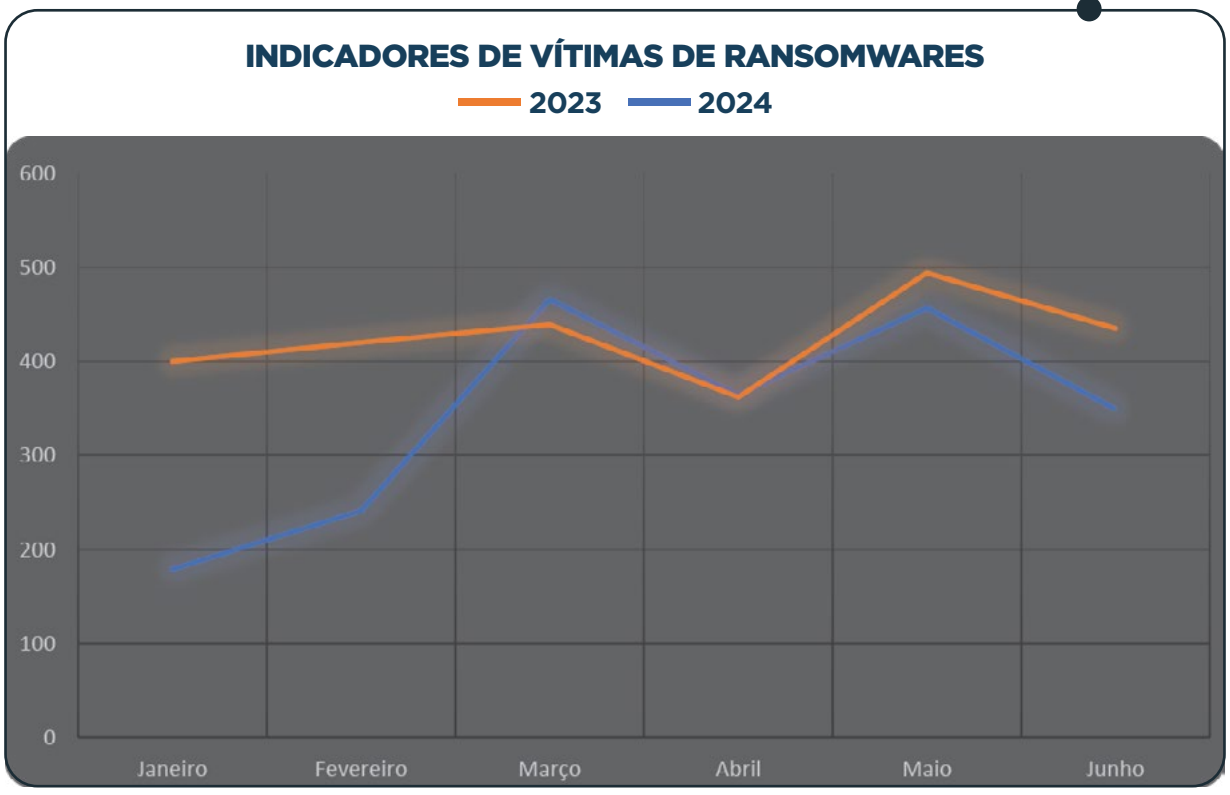

Figura 1 – Gráfico demonstrando a evolução ao longo do 1º semestre de 2024.

4 ESTATÍSTICAS DE RANSOMWARES

Conforme exemplificado no gráfico a seguir, foi possível observar um leve crescimento de ataques ao longo dos meses de 2024, com uma grande queda em abril, seguida de um retorno significativo em maio, com um pico de ataques em ambos os anos, 2023 e 2024.

A queda em 2024 pode estar relacionada aos problemas enfrentados com as forças da lei pelas operações de ransomware LockBit e ALPHV, visto que suas atividades foram parcialmente paralisadas durante este período, mas retornaram nos meses seguintes. A equipe observou um aumento de 24,02% em comparação com o primeiro semestre de 2023 em valores totais.

Em relação aos meses específicos, foi possível verificar que em janeiro houve um aumento de 123,46%, enquanto em março ocorreu uma diminuição de 5,79% em comparação ao mesmo período de 2023.

PRINCIPAIS GRUPOS DO PRIMEIRO SEMESTRE DE 2024

Foi possível também identificar que no primeiro semestre, os grupos de ransomwares Lockbit, Ransomhub, Play, 8base e BlackBasta seguiram como top ofensores.

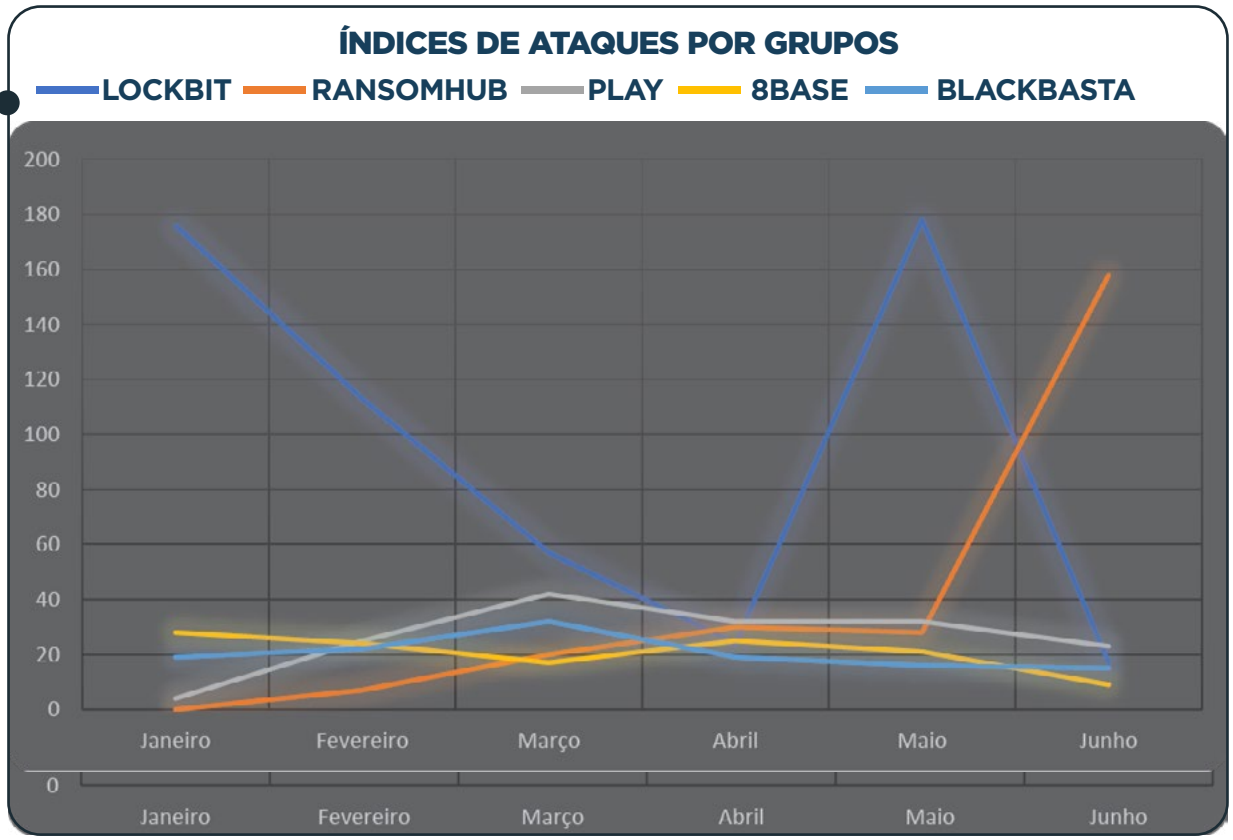

Figura 2 – Gráfico demonstrando TOP 5 grupos de ransomwares ativos no 1º Semestre de 2024.

É importante observar que grupos de Ransomwares como o **Play, 8base e BlackBasta** mantiveram-se anunciando organizações vítimas e com suas operações em uma média de ataques, havendo apenas o diferencial do Ransomhub e LockBit com grandes altas.

PAÍSES DAS ORGANIZAÇÕES ANUNCIADAS PELOS GRUPOS DE RANSOMWARES

A equipe divulga também os principais países das organizações listadas e anunciadas por grupos de ransomwares.

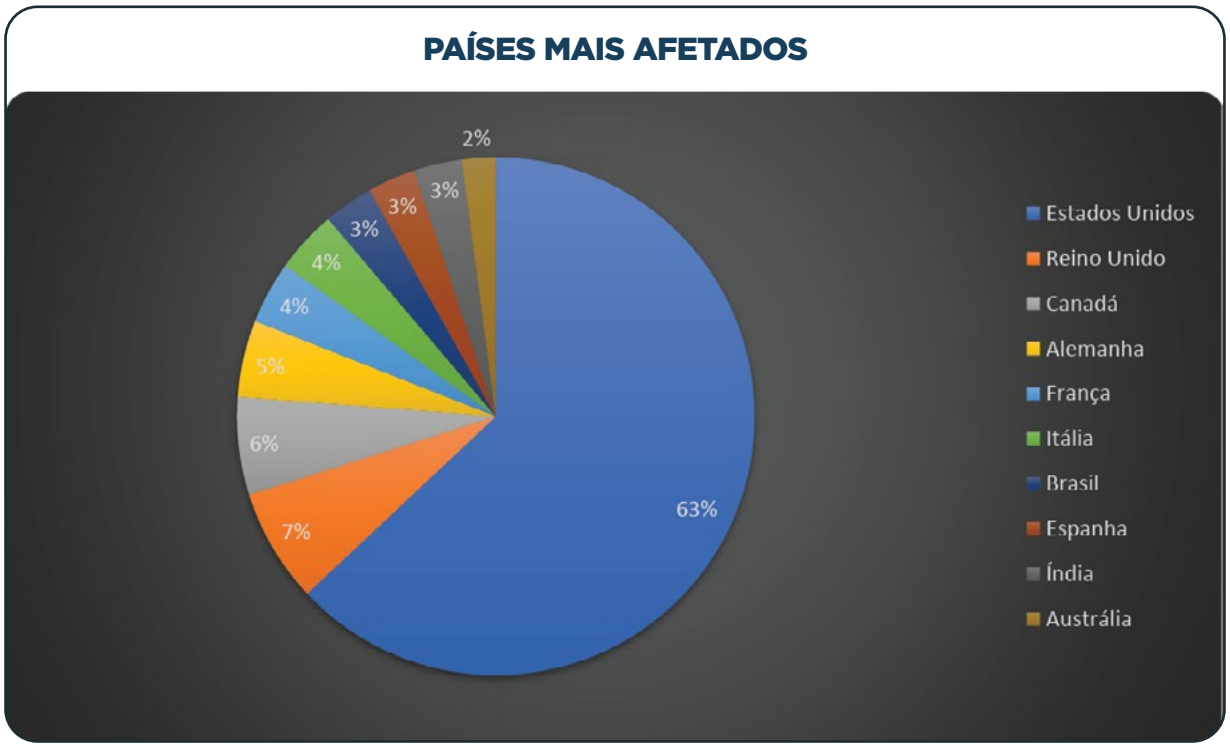

FIgura 3 – Gráfico relacionado aos ataques de ransomwares anunciados por países.

É possível observar que os Estados Unidos se mantiveram na liderança das organizações vítimas, seguido pelo Reino Unido e Canadá. Já o Brasil ocupou o 7º lugar de organizações anunciadas pelos atores, de acordo com as estatísticas apontadas a seguir.

4 ESTATÍSTICAS DE RANSOMWARES

PAÍSES	PORCENTAGEM DE ATAQUES
Estados Unidos	63%
Reino Unido	7,1%
Canadá	6,1%
Alemanha	4,8%
França	3,9%
Itália	3,9%
Brasil	3,1%
Espanha	3%
Índia	3%
Austrália	2,1%

Tabela 2 – Países mais afetados por ataques no 1º semestre.

OBSERVAÇÃO

A porcentagem poderá se alterar, haja vista que a depender da companhia poderá haver uma margem de erro relacionado a localização matriz/filial.

AUTORES

Caique Barqueta
Especialista em Inteligência de Ameaças

Ismael Rocha
Analista de Inteligência de Ameaças Sênior

REFERÊNCIAS

Heimdall by ISH Tecnologia