heimdall

security research

A DIVISION OF ISH

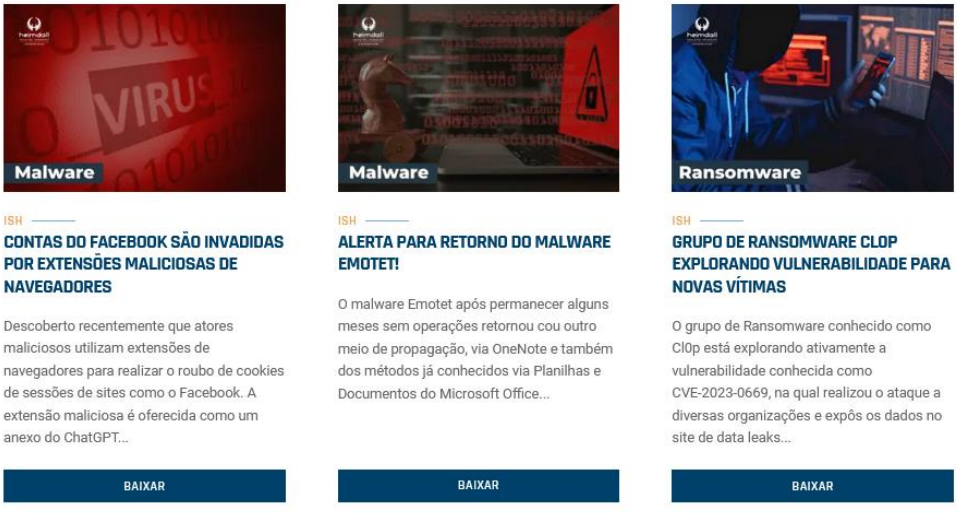
Vulnerabilidades Críticas e Grupos de Ransomwares do 1º Semestre de 2023

Receba alertas e informações sobre segurança cibernética e ameaças rapidamente, por meio do nosso Twitter.

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

1 VULNERABILIDADE

No mundo digital atual, onde a tecnologia desempenha um papel fundamental em quase todos os aspectos de nossas vidas, a segurança cibernética é uma preocupação cada vez mais relevante. Um elemento essencial para entender a segurança cibernética é o conceito de vulnerabilidades. As vulnerabilidades são fraquezas ou falhas em sistemas de software, redes ou infraestrutura que podem ser exploradas por atores de ameaças com más intenções.

Uma vez que os atores de ameaças identifiquem uma vulnerabilidade em potencial, eles podem explorá-la de várias maneiras. Isso pode incluir o desenvolvimento de malware, como vírus, worms, cavalos de Troia ou ransomware, que são projetados para explorar as fraquezas dos sistemas e obter acesso não autorizado. Além disso, eles podem realizar ataques de engenharia social, enganando as pessoas para que revelem informações confidenciais ou executem ações prejudiciais. Também podem ocorrer ataques de negação de serviço, que visam sobrecarregar sistemas e torná-los inoperantes, causando grandes prejuízos financeiros a organizações e governos.

2 TOP VULNERABILIDADES EXPLORADAS EM 2023

Os riscos associados às vulnerabilidades exploradas por atores de ameaças são diversos e podem ter impactos significativos tanto em nível individual quanto em nível organizacional

CVE-2023-23397: Vulnerabilidade de elevação de privilégio (EoP) no Microsoft Outlook. É uma exploração de toque zero, o que significa que a falha de segurança requer baixa complexidade para abuso e não requer interação do usuário.

O invasor envia uma mensagem para a vítima com uma propriedade **MAPI** (Message Application Program Interface) estendida com um caminho **UNC** (Universal Naming Convention) para um **SMB** (Server Message Block) controlado pelo invasor remoto, via **TCP 445**. Hospedado em um servidor controlado pelo invasor, a vulnerabilidade é explorada independentemente de o destinatário ter visto a mensagem ou não.

Pontuação da vulnerabilidade: CVSS v3 9.8 - **Critica**
Vetor de Ataque: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVE-2023-27350: PaperCut NG/MF

Vulnerabilidade de execução remota de código do PaperCut, permite que atacantes remotos ignorem a autenticação nas instalações afetadas do **PaperCut NG 22.0.5** (**Build 63914**). A autenticação não é necessária para explorar esta vulnerabilidade. A falha específica existe na classe **SetupCompleted**. O problema resulta de controle de acesso impróprio. Um invasor pode aproveitar essa vulnerabilidade para ignorar a autenticação e executar código arbitrário no sistema alvo.

Pontuação da vulnerabilidade: CVSS v3 9.8 - **Critica**
Vetor de Ataque: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVE-2023-26360: Adobe ColdFusion

As versões **2018 Update 15** (**e anteriores**) do **Adobe ColdFusion** e **2021 Update 5** (**e anteriores**) são afetadas por uma vulnerabilidade de controle de acesso impróprio que resulta na execução arbitrária de código no contexto do usuário. A exploração dessa vulnerabilidade não requer interação do usuário.

Pontuação da vulnerabilidade: CVSS v3 9.8 - **Critica**
Vetor de Ataque: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVE-2023-34362: MOVEit

Vulnerabilidade no **MOVEit Transfer** um aplicativo MFT, possui uma vulnerabilidade de injeção de SQL no aplicativo da web MOVEit Transfer que pode permitir que um invasor não autenticado obtenha acesso ao banco de dados do MOVEit Transfer. Dependendo do mecanismo de banco de dados usado (MySQL, Microsoft SQL Server ou Azure SQL), um invasor pode inferir informações sobre a estrutura e o conteúdo do banco de dados e executar instruções SQL que alteram ou excluem elementos do banco de dados, a exploração de sistemas não corrigidos pode ocorrer via HTTP ou HTTPS.

Pontuação da vulnerabilidade: CVSS v3 9.8 - **Critica**
Vetor de Ataque: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVE-2023-28771: Zyxel ZyWALL/USG

Vulnerabilidade de manuseio impróprio de mensagens de erro nas versões **4.60** a **4.73** do firmware da série **Zyxel ZyWALL**/**USG**, versões **4.60** a **5.35** do firmware da série **VPN**, versões **4.60** a **5.35** do firmware da série **USG FLEX** e versões **4.60** a **5.35** do firmware da série **ATP**, que podem permitir que de um invasor não autenticado execute alguns comandos do sistema operacional remotamente enviando pacotes criados para um dispositivo afetado.

Pontuação da vulnerabilidade: CVSS v3 9.8 - **Critica**
Vetor de Ataque: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVE-2023-28252: Vulnerabilidade de elevação de privilégio do driver do sistema de arquivos de log comum do Windows. O invasor altera o valor de deslocamento que aponta para uma estrutura específica do Common Log File System (CLFS) na memória do computador. Eles o substituem por um deslocamento que direciona para uma estrutura criada com códigos maliciosos. Essa ação fornece um ponteiro para a memória controlada no nível do usuário, concedendo privilégios de leitura/gravação ao kernel do invasor. As estruturas CLFS são componentes integrais do sistema de log de uso geral CLFS usado pelos sistemas operacionais Windows. Essas estruturas consistem em arquivos de log físicos, fluxos de log, registros de log e outros elementos relacionados.

Esta vulnerabilidade afeta todas as versões com suporte de servidores e clientes Windows, incluindo Windows 11; permitindo que até mesmo os invasores locais explorem potencialmente a vulnerabilidade sem qualquer necessidade de interação do usuário e com métodos de ataque relativamente simples.

Pontuação da vulnerabilidade: CVSS v3 7.8 - **Alta**
Vetor de Ataque: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CVE-2023-28205 e **CVE-2023-28206**: Apple

CVE-2023-28205 é um problema de uso gratuito no mecanismo do navegador **WebKit**, usado pelo Safari e todos os navegadores da Web no **iOS** e **iPadOS**. A falha pode ser desencadeada por meio de conteúdo da Web criado com códigos maliciosos e pode levar à execução arbitrária de códigos.

CVE-2023-28206 é um problema de gravação fora dos limites no **IOSurfaceAccelerator** que pode ser explorado por um aplicativo malicioso para executar código arbitrário com privilégios de kernel.

A primeira pode ser usada para executar um ataque de clique zero, resultando na instalação silenciosa de malware no dispositivo de destino. A segunda permite que os invasores escapem da caixa de proteção do Safari (ou seja, aumentem os privilégios) e obtenham acesso total ao sistema.

Pontuação da vulnerabilidade: CVSS v3 8.8 - **Alta**
Vetor de Ataque: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Pontuação da vulnerabilidade: CVSS v3 8.6 - **Alta**
Vetor de Ataque: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H

CVE-2023-2033: Navegador Chrome

Vulnerabilidade no V8 no Google Chrome anterior a 112.0.5615.121 permite que um invasor remoto explore potencialmente a corrupção de **heap** por meio de uma página **HTML criada**.

Pontuação da vulnerabilidade: CVSS v3 8.8 - **Alta**
Vetor de Ataque: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

CVE-2023-2868: Barracuda

Vulnerabilidade de injeção de comando remoto no produto **Barracuda Email Security Gateway** (somente fator de forma do dispositivo) que afeta as **versões 5.1.3.001-9.2.0.006**.

A vulnerabilidade surge de uma falha em limpar de forma abrangente o processamento do arquivo **.tar** (arquivos de fita). A vulnerabilidade decorre da validação de entrada incompleta de um arquivo .tar fornecido pelo usuário no que se refere aos nomes dos arquivos contidos no arquivo. Como consequência, um invasor remoto pode formatar especificamente esses nomes de arquivo de uma maneira específica que resultará na execução remota de um comando do sistema por meio do operador **qx** do **Perl** com os privilégios do produto Email Security Gateway.

Pontuação da vulnerabilidade: CVSS v3 9.8 - **Critica**
Vetor de Ataque: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:L

OBS. Informamos que todas estas vulnerabilidades se encontram no catálogo de vulnerabilidades exploradas conhecidas da CISA devido a suas explorações por cibercriminosos em ataques cibernéticos.

3 RANSOMWARE

Para falarmos sobre os principais grupos de ransomwares que se fizeram ativos no 1º semestre do ano de 2023, precisamos explicar o que corresponde a referida ameaça.

Ransomware é um tipo de malware criado para prejudicar o acesso ao usuário o acesso a seus arquivos que se encontram armazenados no seu computador. O acesso é rompido por meio de criptografia dos arquivos e posteriormente o ransomware apresenta uma nota de resgate exigindo para que o usuário ou organização realize o pagamento de determinada quantia para tornar os referidos arquivos acessíveis novamente.

Existem diversos tipos de grupos de ransomwares que se encontram ativos atualmente, bem como atuam no formato de ***Ransomware-as-a-Service (RaaS)***, sendo disponível para diversos atores de ameaças a realizarem a compra do ransomware e prejudicarem organizações.

4 ESTATÍSTICAS DE RANSOMWARES

A ISH Tecnologia, por meio de monitoramento destes grupos e atores de ameaças relacionadas a Ransomwares, apresentam a identificação de estatísticas e números relacionados ao início de 2023 até o presente mês (junho), com o foco em alertar as organizações da prática destes tipos de ataques cibernéticos.

Dos meses de **Janeiro a Junho**, é possível verificar que 2 grupos mais se deram destaques em ataques cibernéticos, sendo o **LockBit3** e o **AlphV/BlackCat**, sendo que juntos, acabaram por anunciar mais de **730** organizações vítimas de seus ataques cibernéticos.

Grupo de Ransomware	Organizações vítimas
LockBit3	526
AlphV/BlackCat	207
Bainlian	166
Clop	137
Royal	119
Play	110
8base	98
Blackbasta	66
Medusa	59

Apenas no mês de **Junho** (até dia 22/06), foi possível observar uma disputa entre os grupos de ransomware **Cl0p** e **LockBit3**, sendo que ambos apresentam aproximadamente 60 organizações vítimas cada um dos grupos.

Grupo de Ransomware	Organizações vítimas
Clop:	60

Lockbit:	59
8base:	31
Alphv/BlackCat	31
Play:	19
Bainlian:	17
Snatch:	15
Qilin:	13
Rhysida:	11
Medusa:	10

Já no mês de Maio de 2023, foi observado uma grande publicação de organizações pelo grupo de ransomware 8base, um grupo recém descoberto e anunciado pela ISH, visto que possuem e publicaram muitas organizações brasileiras dentre as suas vítimas.

Grupo de Ransomware	Organizações vítimas
LockBit3	78
8base	67
Bainlian	48
Alphv/BlackCat	41
Akira	33
Royal	26
Nokoyawa	25
Play	25
Medusa	16
Monti	12

Além disso, a TheRecordedMidia, publicou um estudo com base nos ataques identificados de ransomwares uma métrica e estatísticas de segmentos mais visados por grupos de ransomwares de acordo com cada mês de 2023, havendo a identificação de que no mês de Abril de 2023, os grupos de ransomwares tiveram com foco o ataque a organizações no segmento de **Saúde**.

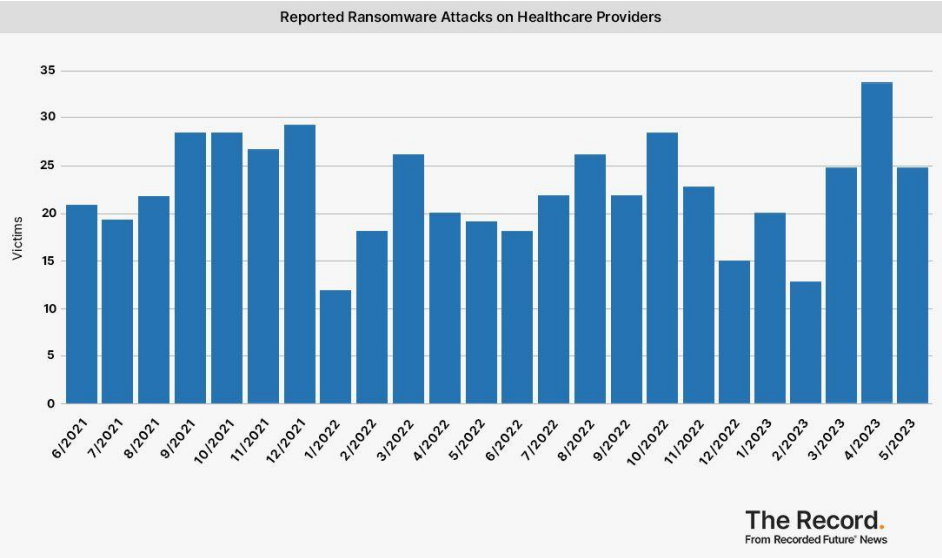


Figura 1 – Gráfico relacionado a ataques do segmento de saúde.

Já com relação a órgãos e **governo**, foi possível verificar que no mês de **Abril** também teria sido um mês proeminente para os grupos de ransomwares.

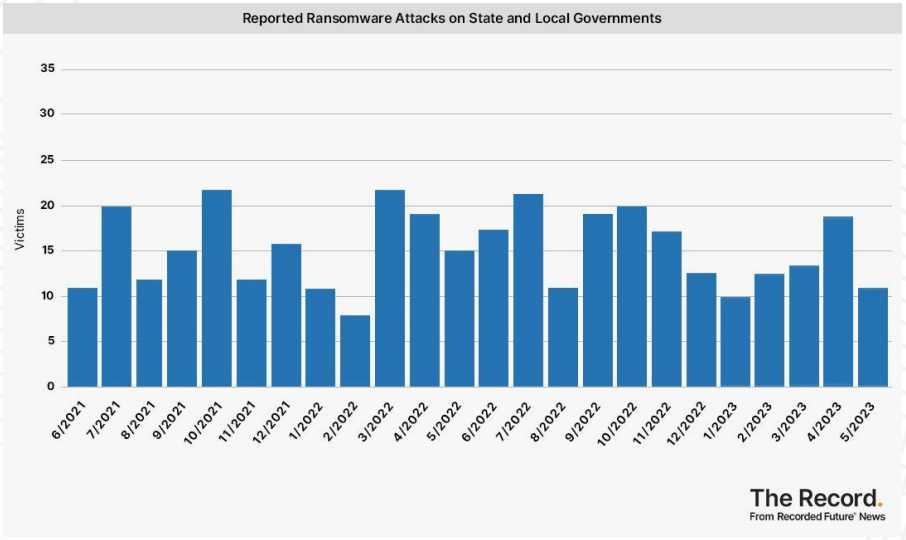


Figura 2 – Gráfico relacionado a ataques de ransomware com foco em governos.

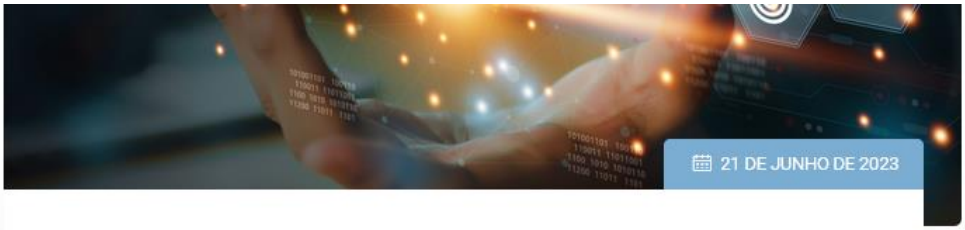
5 RECOMENDAÇÕES PARA VULNERABILIDADES

A ISH Tecnologia, por meio das ações abaixo, aplicar medidas de mitigação da infecção do referido *malware* e de outras ameaças, por exemplo:

- **Realização de *backups* regulares:** Armazene cópias de segurança de todos os dados importantes em um local seguro e desconectado.
- **Realização de atualizações de *softwares*:** Mantenha todos os *softwares* de ativos atualizados, incluindo sistemas operacionais e aplicativos.
- **Utilização de proteção de rede**, como *firewalls*, antivírus e outras medidas de segurança para proteger sua rede.
- **Realização do trabalho de conscientização** com os colaboradores, ensinando aos mesmos a reconhecer e evitar ameaças, como *phishing* e/ou clicar em *links* maliciosos.
- **Monitoração regular da sua rede e sistemas** para identificar e responder rapidamente a qualquer atividade suspeita.
- **Criação e aplicação de um plano de resposta de incidentes**, sendo que em caso de ataques de *ransomware* poderão ser utilizados e conterão informações como questões relacionadas a *backups* e recuperação de sistema.
- **Verificações constantes de vulnerabilidades em serviços**, para que caso haja a existência de vulnerabilidades, estas sejam corrigidas de acordo com o fornecedor evitando-se a possibilidade de exploração.

6 RECOMENDAÇÕES PARA ATAQUES RANSOMWARES

A ISH, publicou uma **série de recomendações contra ataques de ransomwares**, estando estes disponíveis no site do blog da ISH, sendo necessário apenas clicar aqui.



ATAQUES CIBERNÉTICOS E ROUBO DE DADOS: VEJA COMO PROTEGER SUA EMPRESA

Por Caique Barqueta: Ataques de ransomwares têm se aperfeiçoado cada vez mais. Cibercriminosos estão empregando outras táticas de extorsões, como o roubo de informações antes que seja realizado a criptografia, atuando como uma "**dupla extorsão**", já que os atores exigem o pagamento para não publicar os dados exfiltrados da vítima.

Os impactos que esses ataques podem ocasionar para as empresas pode ser algo extremamente crítico, afetando a parte reputacional e financeira da organização. Pensando nisso, a **CISA (Agência de Segurança Cibernética e de Infraestrutura dos Estados Unidos)** publicou um guia com as melhores práticas de prevenção contra ransomware, além de dicas e ações que as

Figura 3 – Publicação no Blog ISH.

7 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **theRecordMedia – Publicação: Mapa de Ransomware**

heimdall
security research

A DIVISION OF ISH