BOLETIM DE SEGURANÇA

Principais vulnerabilidades exploradas e números de ataques de Ransomware em 2023

heimdall
security research
A DIVISION OF ISH

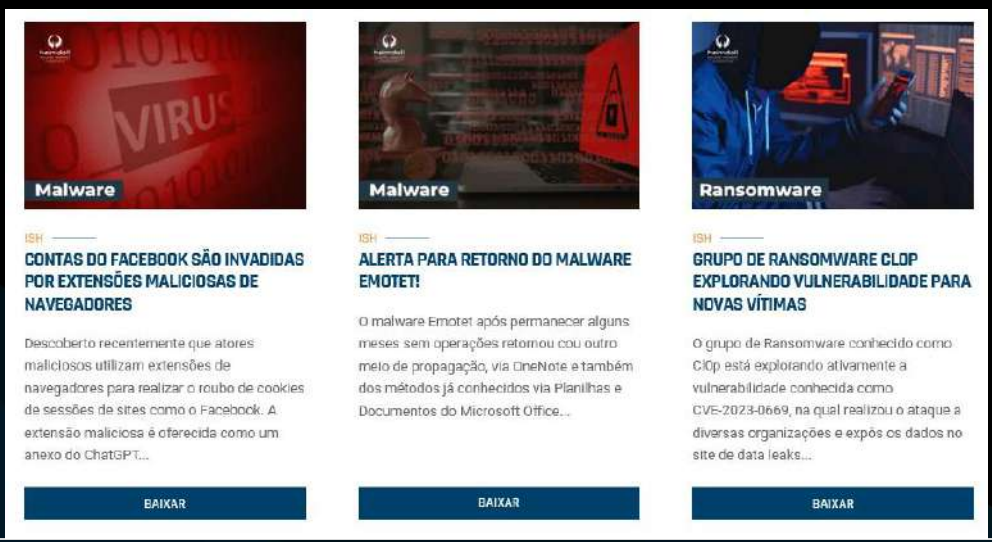
TLP: CLEAR

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



heimdall
security research

Sumário

Lista de Tabela e Gráfico

1 SUMÁRIO EXECUTIVO

Em 2023, o mundo da cibersegurança foi desafiado por uma série de vulnerabilidades críticas e altas, evidenciando a complexidade e a persistência das ameaças digitais. Phishing avançado emergiu como uma ameaça formidável, com cibercriminosos utilizando métodos cada vez mais sofisticados para enganar usuários e obter acesso a informações confidenciais. para ransomware continuou a evoluir, não apenas criptografando dados, mas também ameaçando vazar informações sensíveis, aumentando a pressão sobre as vítimas para o pagamento de resgates.

Vulnerabilidades zero-day, falhas de segurança desconhecidas pelos fabricantes até o momento de sua exploração, foram particularmente problemáticas, pois permitiram ataques antes que correções de segurança pudessem ser implementadas. Além disso, aplicações web se mostraram propensas a uma variedade de ataques, desde injeções de SQL até *cross-site scripting*, abrindo portas para invasores acessarem sistemas e dados sigilosos. Ataques à cadeia de suprimentos de software também foram uma questão séria, com invasores infiltrando-se nos processos de desenvolvimento de software e distribuindo códigos maliciosos em grande escala.

Portanto, a equipe de Inteligência da ISH Tecnologia, Heimdall, elaborou o presente boletim no intuito de apresentar as principais vulnerabilidades exploradas em 2023, números relacionados a atores de ameaças de ransomwares e vulnerabilidades exploradas por estes.

2 TOP 10 PRINCIPAIS VULNERABILIDADES EXPLORADAS EM 2023

Abaixo trazemos informações sobre o **Top 10 vulnerabilidades exploradas em ataques no ano de 2023**. Estas vulnerabilidades abrangem uma gama de falhas, incluindo aquelas que permitem a execução remota de código e o acesso não autorizado a informações confidenciais.

Além disso, foram identificados problemas em diversos softwares os quais serão mencionadas abaixo:

1. **CVE-2023-27350** - PaperCut NG/MF: Várias vulnerabilidades de segurança.

Descrição: Vulnerabilidade crítica no software de gerenciamento de impressão PaperCut, permitindo a execução de código arbitrário e bypass de autenticação.

Detalhes: Devido a exploração por múltiplos malwares, atores de ameaças e ransomwares a mesma foi adicionada ao catálogo de vulnerabilidades conhecidas da CISA.

2. **CVE-2023-24880** - Windows SmartScreen: Vulnerabilidade de Bypass de recurso de segurança.

Descrição: Permite que atacantes contornem as defesas do Mark of the Web (MOTW) no SmartScreen e no Microsoft Office's Protected View.

Detalhes: Devido a exploração por múltiplos malwares, atores de ameaças e ransomwares a mesma foi adicionada ao catálogo de vulnerabilidades conhecidas da CISA.

3. **CVE-2023-0669** - Fortra GoAnywhere MFT: Vulnerabilidade de Execução de Código Remoto

Descrição: Falha de injeção de comando na ferramenta Fortra's GoAnywhere Managed File Transfer, permitindo a execução remota de código.

Detalhes: Devido a exploração por múltiplos malwares, atores de ameaças e ransomwares a mesma foi adicionada ao catálogo de vulnerabilidades conhecidas da CISA.

4. **CVE-2023-23397** - Microsoft Outlook: Vulnerabilidade de Elevação de Privilégio

Descrição: Permite que atacantes contornem medidas de autenticação no NTLM da Microsoft Outlook, facilitando o acesso não autorizado.

Detalhes: Devido a exploração por múltiplos malwares, atores de ameaças e ransomwares a mesma foi adicionada ao catálogo de vulnerabilidades conhecidas da CISA.

5. **CVE-2023-34362** - MOVEit Transfer: Vulnerabilidade de Injeção SQL

Descrição: Vulnerabilidade grave de injeção SQL no MOVEit Transfer, levando à execução arbitrária de código e interrupções de dados,

Detalhes: Devido a exploração por múltiplos malwares, atores de ameaças e ransomwares a mesma foi adicionada ao catálogo de vulnerabilidades conhecidas da CISA.

6. **CVE-2023-29059** - Cliente Desktop 3CX: Vulnerabilidade da Cadeia de Suprimentos

Descrição: Violação sofisticada no cliente desktop 3CX VOIP, permitindo que atacantes injetem código malicioso.

7. **CVE-2023-28252** - Driver do Sistema de Arquivos de Log Comum do Windows (CLFS): Vulnerabilidade de Elevação de Privilégio.

Descrição: Afeta o driver CLFS no Windows, permitindo que atacantes adquiram privilégios no nível do sistema.

Detalhes: Devido a exploração por múltiplos malwares, atores de ameaças e ransomwares a mesma foi adicionada ao catálogo de vulnerabilidades conhecidas da CISA.

8. **CVE-2023-2868** - Barracuda Email Security Gateway: Vulnerabilidade

Descrição: Falha crítica de injeção de comando remoto no Barracuda Email Security Gateway.

Detalhes: Devido a exploração por múltiplos malwares, atores de ameaças e ransomwares a mesma foi adicionada ao catálogo de vulnerabilidades conhecidas da CISA.

9. **CVE-2023-20887** - VMware Aria Operations for Networks: Vulnerabilidade de Injeção de Comando.

Descrição: Vulnerabilidade de injeção de comando. Um agente mal-intencionado com acesso de rede ao VMware Aria Operations for Networks pode executar um ataque de injeção de comando, resultando na execução remota de código.

Detalhes: Devido a exploração por múltiplos malwares, atores de ameaças e ransomwares a mesma foi adicionada ao catálogo de vulnerabilidades conhecidas da CISA.

10. **CVE-2023-22952** - SugarCRM: Vulnerabilidade de Execução de Código Remoto

Descrição: Falha de bypass de autenticação e execução remota de código no SugarCRM.

Detalhes: Devido a exploração por múltiplos malwares, atores de ameaças e ransomwares a mesma foi adicionada ao catálogo de vulnerabilidades conhecidas da CISA.

3 TOP 10 – Principais Grupos de Ransomwares ativos em 2023

De acordo com o monitoramento contínuo de divulgação através de canais de *Data Leaks* ou sites de vazamento e publicações dos atores de ransomware, foi possível observar as ações dos grupos mais ativos no ano de 2023 até o dia 05 de dezembro de 2023, sendo descrito abaixo:

Grupos:	Número de Vítimas anunciadas:
Lockbit:	969
Alphv:	432
Clop:	375
Play:	277
Bianlian:	272
8base:	247
Akira:	160
Medusa:	140
Noescape:	123
Royal:	120

Tabela 1 – Informações e números de publicações de grupos de Ransomwares.

Em comparação com o ano anterior, foi possível identificar que alguns tipos de aumentos em comparação com os dados coletados, como por exemplo o grupo **ALPHV/BlackCat**, que no ano de 2022 teria somado 222 vítimas e no ano de 2023 teria publicado 432 vítimas, um aumento de 94,59% de vítimas.

Outro grupo que chama atenção é o **Bianlian**, o qual em 2022 somou o total de 95 empresas vítimas e em 2023, teria somado 272 vítimas, um aumento de 186,32% em comparação com os anos.

Vale salientar que o levantamento abordou dados apenas até o início de dezembro, havendo ainda a possibilidade de um grande aumento por parte dos grupos até o fim do ano de 2023.

Somente até a data da elaboração do relatório, foram somadas mais de 4.881 publicações de vítimas por atores de ransomware apenas em 2023, um aumento de 12,92% em comparação com o ano de 2022.

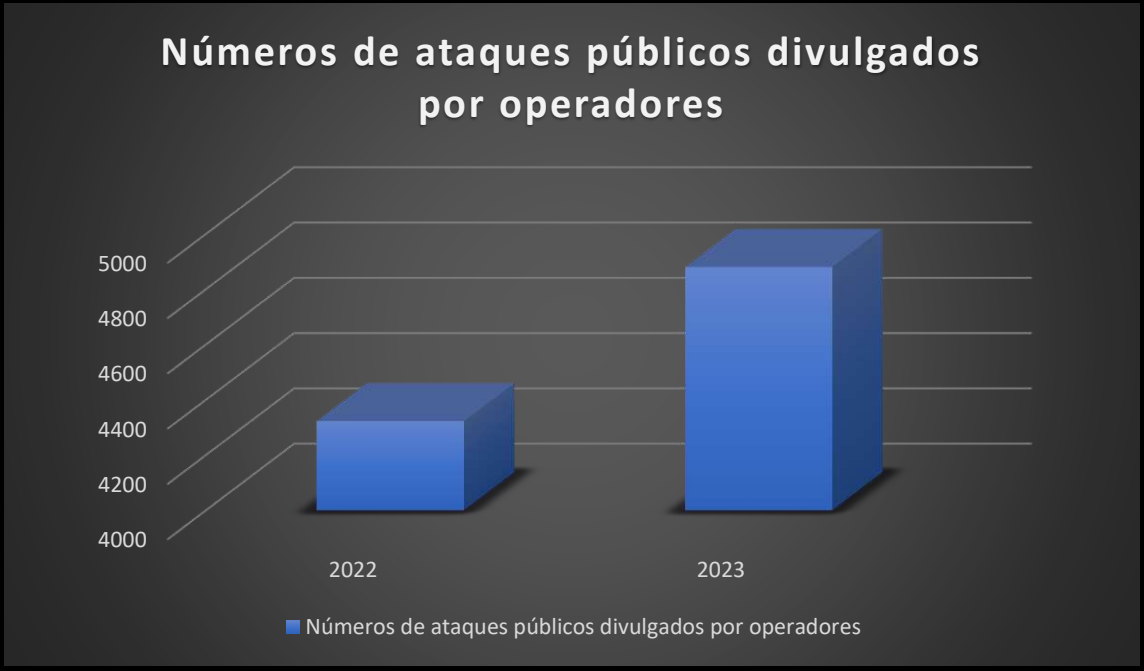


Gráfico 2 – Comparativo anual dos ataques de Ransomwares até a primeira semana de Dezembro de 2023.

4 Explorações de Vulnerabilidades por Ransomwares

A equipe de Inteligência, Heimdall, conseguiu identificar as vulnerabilidades nas quais grupos de ransomwares estavam realizando explorações para lança seus ataques finais de resgates, sendo apresentados abaixo:

CVE-2023-27350 – A vulnerabilidade no PaperCut NG/MF foi observada sendo explorada por atores maliciosos a partir de meados de abril de 2023, incluindo tentativas do *Bl00dy Ransomware Gang* e o ransomware Clop contra servidores PaperCut em instituições educacionais.

CVE-2023-24880 – A vulnerabilidade no Windows SmartScreen foi observada sendo explorada pelo grupo de ransomware Magniber a partir de março de 2023.

CVE-2023-0669 – Vulnerabilidade do Fortra GoAnywhere MFT foi observada sendo explorada pelo grupo de ransomware Clop, afetando a solução GoAnywhere MFT e levando ao roubo de dados.

CVE-2023-23397 – Vulnerabilidade no Microsoft Outlook ativamente explorada desde pelo menos abril de 2022, usada para invadir redes de organizações governamentais, militares, de energia e de transporte na Europa e outros locais.

CVE-2023-34362 – Vulnerabilidade do MOVEit Transfer a qual foi explorada pelo Ransomware Clop, também conhecido como TA505, a partir de 27 de maio de 2023.

CVE-2023-29059 – Vulnerabilidade no Cliente Desktop 3CX explorada ativamente por atores de ameaças que podem ter utilizado a vulnerabilidade para entregar ransomwares.

CVE-2023-28252 – Vulnerabilidade no Driver do Sistema de Arquivos de Log Comum do Windows (CLFS) explorada por atores de ameaças do Ransomware Nokoyawa.

CVE-2023-2868 – Vulnerabilidade no Barracuda Email Security Gateway: explorada ativamente por atores de ameaças que podem ter utilizado a vulnerabilidade para entregar ransomwares.

CVE-2023-20887 – Vulnerabilidade da VMware Aria Operations for Networks explorada ativamente por atores de ameaças que podem ter utilizado a vulnerabilidade para entregar ransomwares.

CVE-2023-22952 – Vulnerabilidade do SugarCRM explorada ativamente por atores de ameaças que podem ter utilizado a vulnerabilidade para entregar ransomwares.

5 Conclusão

Os ataques cibernéticos, especialmente aqueles realizados por atores maliciosos e grupos de ransomware, continuam a ser uma ameaça significativa no cenário digital. Esses adversários exploram vulnerabilidades em sistemas e redes, muitas vezes visando lacunas na segurança cibernética e falhas de software. A sofisticação desses ataques tem crescido, com táticas que incluem phishing, exploração de senhas fracas e aproveitamento de brechas de segurança não corrigidas. Além disso, o impacto desses ataques vai além do dano financeiro, afetando a reputação das organizações e a segurança dos dados dos usuários.

É importante que as empresas e indivíduos adotem práticas robustas de segurança cibernética, como atualizações regulares de software, treinamento em conscientização de segurança e implementação de soluções de segurança avançadas. A colaboração entre organizações e agências de segurança também é crucial para combater essas ameaças e as organizações e governos do país.

6 RECOMENDAÇÕES

Poderão ser adotadas medidas visando a mitigação contra as referidas ameaças informadas neste relatório, como por exemplo:

Atualizações e patches de segurança

- Mantenha todos os sistemas e softwares atualizados. Instale patches de segurança regularmente para corrigir vulnerabilidades conhecidas.

Soluções de antivírus e anti-malware

- Utilize soluções robustas de antivírus e anti-malware, e mantenha-as atualizadas para detectar e prevenir ameaças.

Educação e treinamento de funcionários

- Realize treinamentos frequentes com os funcionários sobre segurança da informação, incluindo a identificação de e-mails de phishing e práticas seguras de navegação na internet.

Backup de dados

- Faça backups regulares de dados importantes e assegure que eles sejam armazenados de forma segura, preferencialmente desconectados da rede principal.

Controle de acesso e autenticação de usuários

- Implemente políticas rigorosas de controle de acesso, incluindo autenticação multifatorial, para restringir o acesso a informações sensíveis.

Firewall e segurança de rede

- Utilize firewalls para monitorar e controlar o tráfego de entrada e saída na rede. Implemente também outras tecnologias de segurança de rede, como IDS/IPS (Sistema de Detecção/Prevenção de Intrusões).

Análise de vulnerabilidades e testes de intrusão

- Realize análises regulares de vulnerabilidades e testes de penetração para identificar e corrigir falhas de segurança antes que sejam exploradas.

Isolamento e segmentação de rede

- Divida a rede em segmentos para limitar a propagação de ataques e facilitar a gestão da segurança.

Planos de resposta a incidentes

- Desenvolva e mantenha um plano de resposta a incidentes de segurança para lidar eficientemente com quaisquer violações de segurança.

Monitoramento contínuo e análise de logs

- Monitore constantemente os sistemas para atividades suspeitas e revise regularmente os logs de segurança.

7 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Consulta a base do NIST referente a Vulnerabilidades públicas;**

heimdall
security research

A DIVISION OF ISH