BOLETIM DE SEGURANÇA

RansomHub atacou 210 alvos em setores críticos

heimdall
security research
A DIVISION OF ISH

TLP: CLEAR

Acesse boletins diários sobre agentes de ameaças, *malwares*, indicadores de comprometimentos, TTPs e outras informações no *site* da ISH.

Boletins de Segurança – Heimdall

ISH

CONTAS DO FACEBOOK SÃO INVADIDAS POR EXTENSÕES MALICIOSAS DE NAVEGADORES

Descoberto recentemente que atores maliciosos utilizam extensões de navegadores para realizar o roubo de cookies de sessões de sites como o Facebook. A extensão maliciosa é oferecida como um anexo do ChatGPT...

BAIXAR

ISH

ALERTA PARA RETORNO DO MALWARE EMOTET!

O malware Emotet após permanecer alguns meses sem operações retornou cou outro meio de propagação, via OneNote e também dos métodos já conhecidos via Planilhas e Documentos do Microsoft Office...

BAIXAR

ISH

GRUPO DE RANSOMWARE CLOP EXPLORANDO VULNERABILIDADE PARA NOVAS VÍTIMAS

O grupo de Ransomware conhecido como Cl0p está explorando ativamente a vulnerabilidade conhecida como CVE-2023-0669, na qual realizou o ataque a diversas organizações e expôs os dados no site de data leaks...

BAIXAR

SUMÁRIO

LISTA DE TABELAS

1 SUMÁRIO EXECUTIVO

O grupo de ransomware **RansomHub** tem sido responsável pela criptografia e exfiltração de dados de pelo menos 210 vítimas, conforme relatado pelo governo dos EUA. Este grupo de cibercriminosos tem focado em setores críticos, causando preocupações significativas sobre a segurança e resiliência das infraestruturas afetadas e, obtendo grandes ganhos financeiros com suas ações maliciosas.

2 INFORMAÇÕES SOBRE A AMEAÇA

As vítimas do grupo RansomHub abrangem uma ampla gama de setores críticos. Entre eles estão os setores de água e esgoto, tecnologia da informação, serviços e instalações governamentais, assistência médica e saúde pública, serviços de emergência, alimentação e agricultura, serviços financeiros, instalações comerciais, manufatura crítica, transporte e infraestrutura crítica de comunicações. Esses ataques destacam a vulnerabilidade de infraestruturas essenciais e a necessidade urgente de medidas de segurança reforçadas para proteger contra ameaças cibernéticas.

O RansomHub, anteriormente conhecido como Cyclops e Knight, é uma variante de ransomware como serviço que se destacou como um modelo de serviço eficiente e bem-sucedido. Recentemente, atraiu afiliados de alto nível de outras variantes importantes, como LockBit e ALPHV, segundo agências governamentais. Em uma análise divulgada no final do mês passado, a ZeroFox destacou que a atividade do RansomHub está em crescimento constante, essa variante de ransomware representou cerca de 2% de todos os ataques no primeiro trimestre de 2024, subindo para 5,1% no segundo trimestre e alcançando 14,2% até o momento no terceiro trimestre. Cerca de 34% dos ataques do RansomHub foram direcionados a organizações na Europa, em contraste com 25% no cenário geral de ameaças. O grupo é notório por utilizar a técnica de dupla extorsão, onde dados são exfiltrados e sistemas são criptografados para forçar as vítimas a pagar o resgate. As vítimas são instruídas a entrar em contato com os operadores através de uma URL .onion exclusiva. Empresas que se recusam a pagar o resgate têm suas informações divulgadas em um site de vazamento de dados, com um período de exposição que varia de três a 90 dias.

3 CADEIA DE ATAQUES

O acesso inicial aos sistemas das vítimas é obtido explorando vulnerabilidades conhecidas em dispositivos como Apache ActiveMQ (CVE-2023-46604), Atlassian Confluence Data Center e Server (CVE-2023-22515), Citrix ADC (CVE-2023-3519), F5 BIG-IP (CVE-2023-46747), Fortinet FortiOS (CVE-2023-27997) e Fortinet FortiClientEMS (CVE-2023-48788), entre outras falhas de segurança. Após essa fase, os afiliados realizam reconhecimento e escaneamento de rede utilizando ferramentas como AngryIPScanner, Nmap e outros métodos *living-off-the-land* (LotL). Os ataques do RansomHub também incluem a desativação de softwares antivírus com o uso de ferramentas personalizadas para evitar detecção.

Depois de obter acesso, os afiliados do RansomHub criam contas de usuário para manter a persistência, reativam contas desativadas e utilizam o Mimikatz em sistemas Windows para coletar credenciais e escalar privilégios para o nível de SYSTEM, conforme um comunicado do governo dos EUA. Os afiliados então se movem lateralmente dentro da rede utilizando métodos como Protocolo

de Área de Trabalho Remota (RDP), PsExec, AnyDesk, Connectwise, N-Able, Cobalt Strike, Metasploit, entre outros amplamente usados para comando e controle (C2).

Outro aspecto notável dos ataques do RansomHub é o uso de criptografia intermitente para acelerar o processo, com exfiltração de dados observada através de ferramentas como PuTTY, buckets Amazon AWS S3, solicitações HTTP POST, WinSCP, Rclone, Cobalt Strike, Metasploit, entre outros. O grupo obtém credenciais legítimas de repositórios públicos para acessar inicialmente o ambiente Amazon Web Services (AWS) de uma organização, conforme explicação de pesquisadoras de segurança. Apesar das permissões limitadas das credenciais comprometidas. Os agentes de ameaças utilizam ferramentas como Amazon Simple Storage Service (S3) Browser e WinSCP para coletar informações sobre as configurações dos buckets S3, acessar objetos S3 e excluir dados.

Os ataques de ransomware evoluíram significativamente, indo além da simples criptografia de arquivos para adotar estratégias de extorsão complexas e multifacetadas, incluindo esquemas de extorsão tripla. A extorsão tripla eleva o nível de ameaça, adicionando meios adicionais de interrupção além da criptografia e exfiltração. Isso pode envolver a execução de um ataque DDoS contra os sistemas da vítima ou a extensão de ameaças diretas a clientes, fornecedores ou outros associados da vítima, causando mais danos operacionais e de reputação.

4 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:

Mantenha seus sistemas e softwares atualizados

- Instale todas as atualizações e patches de segurança regularmente para corrigir vulnerabilidades que podem ser exploradas por ransomware.

Faça backups regulares

- Mantenha cópias de segurança de seus dados importantes em locais seguros e desconectados da rede principal. Isso garante que você possa recuperar seus dados sem pagar o resgate.

Use soluções de segurança confiáveis

- Instale e mantenha atualizados softwares antivírus e antimalware. Eles podem detectar e bloquear ameaças antes que causem danos.

Eduque os funcionários

- Treine sua equipe para reconhecer e evitar e-mails de phishing e links suspeitos. A conscientização é uma das melhores defesas contra ataques de engenharia social.

Implemente autenticação multifator (MFA)

- Adicione uma camada extra de segurança exigindo múltiplas formas de verificação antes de conceder acesso a sistemas críticos.

Restrinja privilégios de acesso

- Limite os direitos de acesso dos usuários apenas ao que é necessário para suas funções. Isso minimiza o impacto caso uma conta seja comprometida.

Utilize redes seguras

- Evite usar redes Wi-Fi públicas para acessar informações sensíveis. Se necessário, use uma VPN para garantir uma conexão segura.

5 INDICADORES DE COMPROMISSOS

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 Compromissos (IOCs) relacionadas a análise do(s) artefato(s) deste relatório.

Indicadores de compromisso do artefato	
md5:	3e8238b198c8e5364a054c07514b3cc9
sha1:	36a85de3e6daf48f0a803c03319386992a3202a4
sha256:	68b4b9b9fee2913f7a5d2b8280eb08df9f02fefc451f08bd288345e544ec1675
File name:	2024-05-03_3e8238b198c8e5364a054c07514b3cc9_snatch

Indicadores de compromisso do artefato	
md5:	0cd4b7a48220b565eb7bd59f172ea278
sha1:	a7ca950c6dadd02ab8fafdba8f984266fc2f9b7c
sha256:	7539bd88d9bb42d280673b573fc0f5783f32db559c564b95ae33d720d9034f5a
File name:	amd64.exe

Indicadores de compromisso do artefato	
md5:	57b8cb35b0578b012c4dcf80095747d5
sha1:	dc6d7ca6bbd6a56061649ea3a21a917401f4bb89
sha256:	5d2f77971ffe4bab08904e58c8d0c5ba2eefefa414599ebac72092e833f86537
File name:	smbexec.exe

Indicadores de compromisso do artefato	
md5:	09e382be8dc54551cbfc60557d5a70b0
sha1:	b312a5003d6919d5985630dbd655d306a318ce13
sha256:	ea9f0bd64a3ef44fe80ce1a25c387b562a6b87c4d202f24953c3d9204386cf00
File name:	L2.exe

Tabela 1 – Indicadores de Compromissos de artefatos

6 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **CISA**
- **Zerofox**
- **Thehackernews**

7 AUTORES

- **Leonardo Oliveira Silva**
- **Ismael Pereira Rocha**

heimdall
security research
A DIVISION OF ISH