

RTI-0424

Criticidade: Alta

Relatório de Inteligência

RansomHouse Ransomware



Logical IT

Relatório de Inteligência

RansomHouse Ransomware

Este Relatório de Inteligência descreve as principais informações e atualização sobre a ameaça "RansomHouse Ransomware" e tem como objetivo auxiliar os times estratégicos e operacionais na tomada de decisão dos riscos cibernéticos em seu ambiente.

Público-alvo: Alta Gestão

- Principais decisões: Determinar a relevância da ameaça para tomada de decisão operacional e estratégica e planejar medidas preventivas de segurança.

Público-alvo: SOC

- Principais decisões: Determinar relevância, priorização e triagem de ameaças; Identificar TTPs que podem exigir novas detecções ou atualizações.
- Dados relevantes: Modus Operandi, motivação, setores e países alvos, IOCs; CVEs e TTPs observados.

Público-alvo: Threat Hunt

- Principais decisões: Conduzir pesquisas personalizadas e específicas na rede para o comportamento malicioso relatado.
- Dados relevantes: Modus Operandi, motivação, setores e países alvos, IOCs; CVEs e TTPs observados.

1 Sumário da Ameaça

Essa seção reúne as principais informações atualizadas sobre a ameaça descrita nesse Relatório de Inteligência "RansomHouse Ransomware".

RansomHouse Ransomware	
Tipo de Ransomware	Crypto-Ransomware, RaaS
Threat Actor	RansomHouse Group
Motivação	Financeira
Tipos de Extorsão	Extorsão, Dupla Extorsão, Vazamentos gratuitos
Métodos de infecção	Exploração de serviços vulneráveis, geralmente visando ativos ou aplicativos públicos com vulnerabilidades conhecidas não corrigidas (CVES); Phishing; Engenharia Social.
Comunicação	Telegram: https://t.me/ransom_house
Países alvo	EUA, Europa e Ásia.
Setores alvos	Infraestrutura Crítica, Manufatura, Saúde, Educação.
Descriptografia Gratuita?	Não.
Última atividade	Dezembro/2024

Tabela 1 - Principais informações sobre o RansomHouse Ransomware.

2 RansomHouse Ransomware

Surgindo após o vazamento do código-fonte Babuk no final de 2021, RansomHouse foi vinculado a vários grupos, incluindo White Rabbit , Mario ESXi , RagnarLocker e Dark Angels (Dunghill Leak). Investigações posteriores revelaram associações potenciais do RansomHouse com os grupos Alphv/BlackCat , LockBit 3.0 , BianLian e RagnarLocker .

Snatch e Stormous, também foram identificados como cooperados do RansomHouse, envolvendo-se em atividades híbridas de ransomware/hacktivista que misturam ransomware com operações de influência sob o pretexto de hacktivismo. Enquanto Dark Angels e RansomHouse funcionam principalmente como grupos de ransomware, Snatch e Stormous se alinham com hacktivistas. As causas observadas incluem sentimentos pró-Palestina e pró-Rússia, com foco em atacar entidades dos EUA e da Europa, também envolvendo indivíduos associados, particularmente funcionários do governo.

Conforme o [Analyst1](#), uma análise do alinhamento geopolítico indica que RansomHouse, Snatch e Stormous provavelmente estão alinhados com a Rússia. Isso se baseia na análise de infraestrutura observada revelando conexões originadas de servidores baseados na Rússia e outros artefatos. Além disso, uma análise dos principais canais de mídia pró-Rússia revela forte apoio a esses grupos, reforçando suas narrativas de uma forma que se alinha e apoia a agenda mais ampla do estado russo.

O compartilhamento de dados entre grupos de ransomware introduz novos desafios. Dados roubados anteriormente são reutilizados em tentativas de extorsão, criando falsas impressões de novos ataques. A integração de atividades do tipo hacktivista por grupos como Snatch e Stormous também ressalta a necessidade de medidas de segurança aprimoradas para proteger dados confidenciais e mitigar danos à reputação em níveis governamentais e individuais.

Segundo a [Trellix](#), as táticas, técnicas e procedimentos (TTPs) utilizadas pelo grupo mostram um nível de execução avançado, alavancando servidores de rede de entrega de conteúdo (CDN) para exfiltração de dados e utilização de uma sala de bate-papo baseada em Tor para negociações com as vítimas. Este grupo tenta se diferenciar dos operadores típicos de ransomware cultivando uma imagem de uma "comunidade de mediadores profissionais".

2.1 Motivação

A principal motivação do grupo RansomHouse é financeira. O grupo gerencia uma operação de ransomware como serviço (RaaS) que emprega um modelo de participação nos lucros, onde os afiliados recebem uma parcela substancial dos pagamentos de resgate, enquanto a operadora fica com uma parte menor.

2.2 Modus Operandi

Os ataques do RansomHouse são caracterizados por planejamento e execução meticolosos. O grupo parece investir um tempo significativo em reconhecimento, entendendo a infraestrutura digital de seu alvo e identificando ativos de dados importantes. Essa preparação permite que eles maximizem o impacto de seus ataques, garantindo que possam extrair o maior resgate possível de suas vítimas.

A metodologia de ataque do grupo abrange:

1. Acesso Inicial

- Ataques de phishing: e-mails fraudulentos projetados para induzir os usuários a clicar em links maliciosos ou baixar anexos infectados é um ponto de entrada comum. Esses e-mails muitas vezes imitam comunicações comerciais legítimas, aumentando a probabilidade de serem clicadas.
- Exploração de vulnerabilidades: O grupo aproveita vulnerabilidades conhecidas em softwares, aplicativos web ou configurações mal protegidas de redes.
- Credenciais comprometidas: Utilizam credenciais roubadas adquiridas em fóruns da dark web, ataques de phishing ou por meio de engenharia social.
- Força bruta ou configurações padrão: Testam combinações de senha para acessar redes que ainda utilizam credenciais fracas ou padrões.

2. Movimentação Lateral

- Exploração de protocolo de área de trabalho remota: o grupo RansomHouse pode explorar pontos fracos nas configurações RDP ou SMB para obter acesso remoto a um sistema.
- Ataques à cadeia de suprimentos: o grupo demonstrou preferência por atacar as cadeias de suprimentos, comprometendo vendedores e fornecedores para obter acesso a uma rede mais ampla de vítimas. Essa tática permite que os invasores alcancem um número maior de vítimas com uma única intrusão.
- Após obter acesso inicial, exploram a rede para identificar ativos valiosos, como bancos de dados, servidores críticos e informações sensíveis.
- Usam ferramentas legítimas (como PowerShell ou comandos administrativos) para evitar detecção por soluções de segurança.

3. Exfiltração de Dados

- Copiam grandes volumes de informações sensíveis, incluindo: Dados de clientes; Propriedade intelectual; Informações financeiras e estratégicas etc.

4. Extorsão

- Após roubar os dados, entram em contato com a vítima, ameaçando a divulgação e venda dos dados a concorrentes ou na dark web.
- Exigem um pagamento (geralmente em criptomoedas) para evitar que os dados sejam expostos ou usados de maneira prejudicial

5. Divulgação

- Caso a vítima não ceda à extorsão, o grupo pode publicar os dados roubados em sites de vazamentos (data leak sites); e/ou divulgar as informações em fóruns da dark web para aumentar a pressão.

O RansomHouse é conhecido por usar uma grande variedade de ransomware que está disponível em mercados obscuros e não tem seu próprio ransomware de assinatura como base para comparação.

Uma vez que os arquivos são cifrados, uma nota de resgate chamada "*!!READ_ME!!.txt*" é adicionada, fornecendo instruções sobre o resgate dos dados. A nota de resgate afirma que a infraestrutura de rede da vítima foi comprometida, dados críticos foram extraídos e todos os arquivos foram criptografados. Além disso, solicita que a vítima entre em contato com os invasores antes que os dados sejam expostos publicamente, Figura 1.

Figura 1 - Nota de resgate contendo instruções sobre o pagamento. Fonte: RansomHouse Blog

Um dos principais aspectos das operações de ransomware, muitas vezes determinando o sucesso de seus esforços de extorsão, é a utilização de sites de vazamento de dados. Essas plataformas são cruciais

no suporte a táticas de dupla extorsão, onde os atores não apenas criptografam os dados da vítima, mas também ameaçam divulgá-los publicamente, a menos que um resgate seja pago. Figura 2.

The screenshot shows a website with a header containing navigation links: Main, About, Rules, Partners, and FAQ. Below the header is a logo consisting of a stylized roof shape with a letter 'B' inside, and the text '©RansomHouse' underneath. A main text block reads: "Below is a list of companies that either have considered their financial gain to be above the interests of their partners / individuals who have entrusted their data to them or have chosen to conceal the fact that they have been compromised." Below this text are three data cards, each representing a company entry:

Case ID	Status	Action	Action date
17925	DISCLOSED	Encrypted	30/09/2023
34465	DISCLOSED	Encrypted	03/09/2023
47272	DISCLOSED	Encrypted	29/08/2023

Figura 2 – Site Oficial utilizado pelos fraudadores para expor os dados das vítimas. Fonte: RansomHouse Blog.

2.3 Negociação

Utilizando-se de sofisticado nível de comunicação anônima pelo grupo por meio de uma sala de bate-papo baseada em rede Tor mostra uma típica operação moderna de extorsão cibernética. Seu modus-operandi envolve o envio de links de bate-papo aleatórios para cada vítima, tática essa, projetada para evitar o rastreamento e adicionar uma camada de complexidade às suas operações.

A sala de bate-papo apresenta várias guias, incluindo "Bate-papo", "Idioma" e "Página principal", esta última exibindo uma contagem regressiva para pressionar as vítimas a pagarem o valor do resgate exigido, Figura 3.

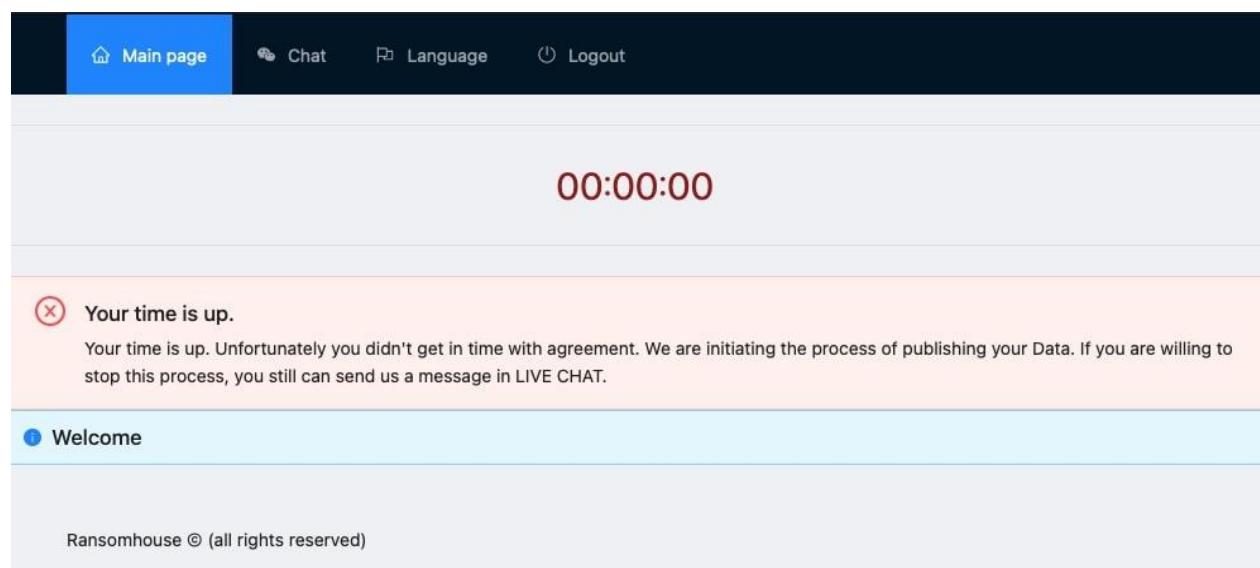
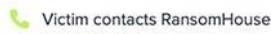


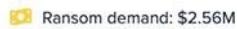
Figura 3 – Chat de negociação. Fonte: Trellix.

O contato inicial da vítima com a RansomHouse desencadeia uma série de ofertas e contraofertas, com o pedido de resgate inicialmente fixado em US\$ 2,56 milhões. O eventual acordo da vítima com um resgate de US\$ 1,25 milhão é cerca de metade da demanda inicial, Figura 4.

Ransom Demand

Victim contacts RansomHouse
NOV 27, 2023

The victim contacts RansomHouse to address the ransom demand.



Ransom demand: \$2.56M
NOV 27, 2023

RansomHouse initially demands \$2.56 million as ransom.

Negotiation

Victim proposes lower amount
NOV 29, 2023

The victim proposes a lower amount in response to the ransom demand.



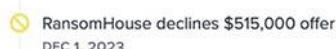
RansomHouse insists on original demand
NOV 29, 2023

RansomHouse maintains its insistence on the original ransom demand.



Victim offers \$515,000
DEC 1, 2023

The victim offers \$515,000 as a counterproposal to the ransom demand.



RansomHouse declines \$515,000 offer
DEC 1, 2023

RansomHouse declines the victim's \$515,000 counteroffer.



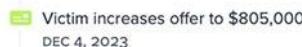
RansomHouse reduces demand to \$2.25M
DEC 2, 2023

RansomHouse reduces the ransom demand to \$2.25 million.



Victim counters with \$600,000
DEC 2, 2023

The victim counters the reduced demand with a \$600,000 offer.



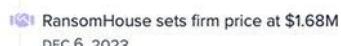
Victim increases offer to \$805,000
DEC 4, 2023

The victim increases the offer to \$805,000 in the negotiation process.



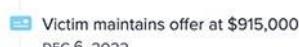
RansomHouse insists on higher amount
DEC 4, 2023

RansomHouse maintains its insistence on a higher ransom amount.



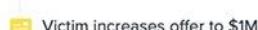
RansomHouse sets firm price at \$1.68M
DEC 6, 2023

RansomHouse sets a firm price at \$1.68 million in the negotiation process.



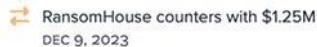
Victim maintains offer at \$915,000
DEC 6, 2023

The victim maintains the offer at \$915,000 during negotiations.



Victim increases offer to \$1M
DEC 9, 2023

The victim increases the offer to \$1 million in the negotiation process.



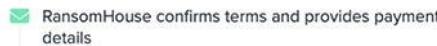
RansomHouse counters with \$1.25M
DEC 9, 2023

RansomHouse counters the victim's offer with a \$1.25 million proposal.

Agreement

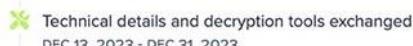
Victim agrees to \$1.25M
DEC 12, 2023

The victim agrees to the \$1.25 million ransom amount proposed by RansomHouse.



RansomHouse confirms terms and provides payment details
DEC 12, 2023

RansomHouse confirms the terms and provides payment details to the victim.



Technical details and decryption tools exchanged
DEC 13, 2023 - DEC 31, 2023

During this period, technical details and decryption tools are exchanged, and security advice is provided.

Figura 4 – Timeline de negociação. Fonte: Trellix.

O pagamento do resgate foi realizado em duas etapas. Inicialmente, 0,1 BTC foram enviados para o endereço "1MmkNa1gRUmVSocZic8wJhehf8NW4GzDZ". Após a confirmação deste pagamento

inicial, foi solicitado o restante pagamento. A análise do Blockchain confirmou que um total de 29.86858000 BTC, aproximadamente US\$ 1,25 milhão, foi transferido para este endereço.

Em 12 de dezembro de 2023, os fundos foram divididos novamente: aproximadamente 30% (8.96037291 BTC) enviados para "1GqGTYE2a9c14jegP1aK9Qj58gYyyt7Dxu", provavelmente o parceiro potencial, e cerca de 70% (20.90764614 BTC) para "bc1q93xvcqux2xl4n03985lyr h8w55et8tt60fcrm", possivelmente a carteira da RansomHouse, Figura 5.

Posteriormente, uma parte desses fundos foi movida para "1A8snaAv9hSMycMRNznWPqtQWJApJpzntJ", rotulado com a plataforma de troca BYBIT pela MetaSleuth, indicando uma possível conversão para fiduciário ou outras criptomoedas, Figura 5.

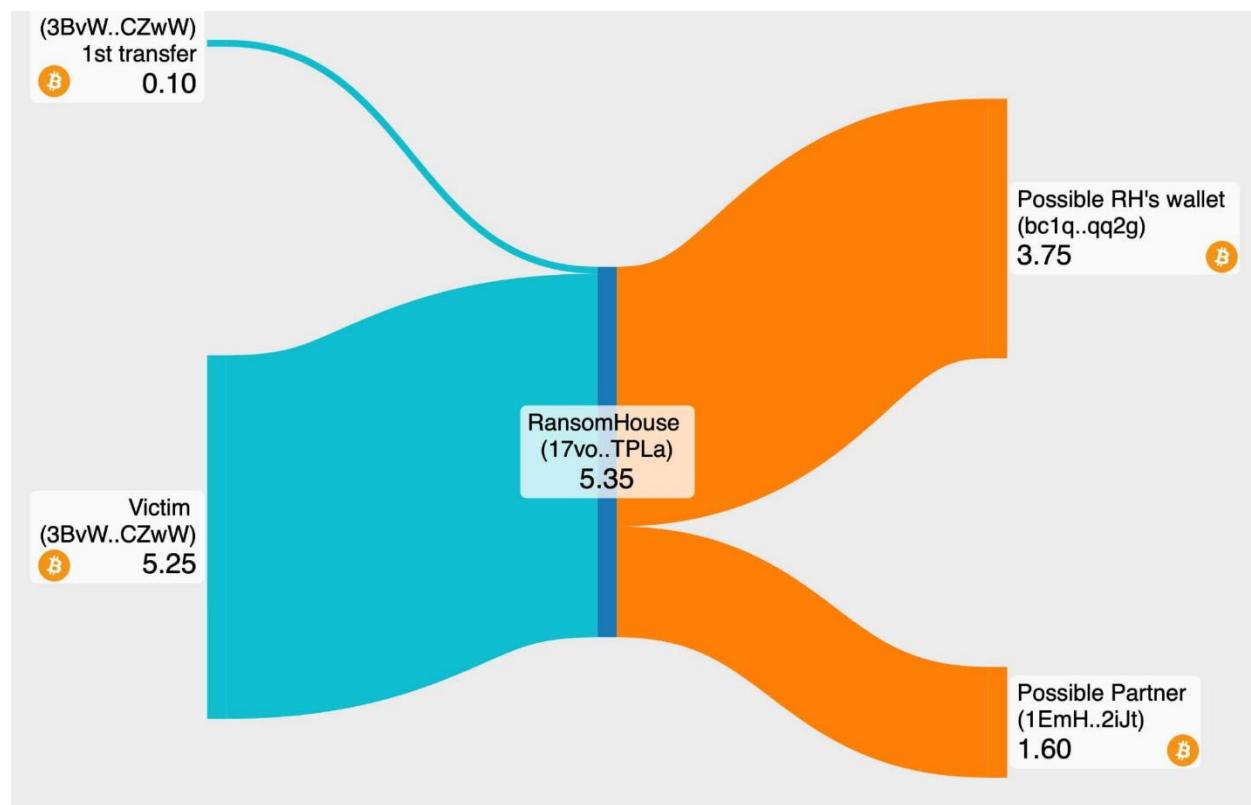


Figura 5 – Movimentação do pagamento do resgate. Fonte: Trellix.

Durante a análise realizada, observou-se que a transferência dos dados extraídos foi realizada para o site "MEGA", serviço de compartilhamento de arquivos. O volume total era de 61,2 GB, distribuídos em cinquenta arquivos zip, cada um com aproximadamente um gigabyte.

2.4 Vítimas

O grupo RansomHouse tem como alvo principal países como Estados Unidos, Europa e Ásia. Os 10 principais setores mais afetados pelo RansomHouse de 1º de janeiro de 2023 a 22 de maio de 2024 foram os setores: farmacêuticos, tecnológicos, assistência médica, serviços de suporte empresarial e aeroespacial, Figura 6.

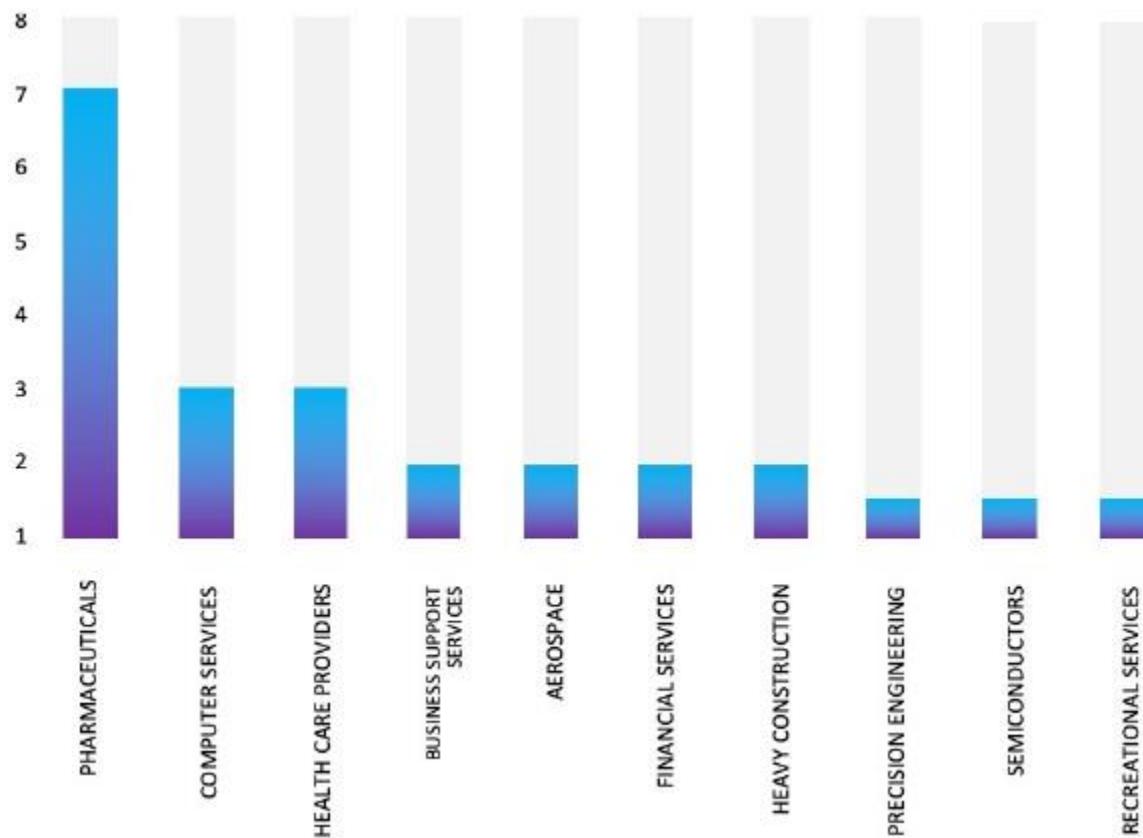


Figura 6 – Top 10 setores mais atacados pelo RansomHouse. Fonte: Cyfirma.

Este ano o Brasil foi alvo do grupo 2 vezes, sendo:

- Vítima 1: Governamental – Data do ataque: 01/11/2024
- Vítima 2: Serviços Comerciais – Data do ataque: 14/12/2024

3 Técnicas, Táticas e Procedimentos (TTPs)

O ransomware RansomHouse, assim como muitas variantes modernas de ransomware, utiliza uma variedade de táticas e técnicas alinhadas com o framework MITRE ATT&CK. Embora os detalhes possam variar com base na interação exata do ataque, threat actor, vítimas etc., algumas táticas e técnicas mais comuns utilizadas pelo ransomware em 2024 incluem, mas não se limitam a:

Tática	Técnica ID	Breve Descrição	Referência
Exploits	T1110.003	Tentativa de acesso usando senhas comuns em várias contas.	T1110.003
	T1078	Uso de contas válidas para obter acesso não autorizado.	T1078
	T1190	Exploração de vulnerabilidades em aplicações expostas.	T1190
	T1203	Exploração de vulnerabilidades em softwares do cliente.	T1203
	T1059	Execução de comandos maliciosos usando interpretadores de comando.	T1059
Defesa contra Detecção	T1027	Ofuscar arquivos ou informações para evitar detecção.	T1027
	T1562.001	Desativar ou modificar ferramentas de defesa.	T1562.001
	T1070.001	Apagar logs de eventos do Windows para ocultar atividades.	T1070.001
	T1070.004	Deletar arquivos para remover evidências.	T1070.004
Movimentação Lateral	T1021	Uso de serviços remotos para mover-se lateralmente na rede.	T1021
Instalação	T1072	Uso de ferramentas de implantação de software para instalar malware.	T1072
	T1547	Persistência por meio de inicialização automática ou execução durante o logon.	T1547
	T1108	Garantir acesso redundante a um sistema comprometido.	T1108
	T1136	Criação de novas contas em sistemas comprometidos.	T1136
	T1505.003	Instalação de Web Shells em servidores comprometidos.	T1505.003
	T1053	Execução programada de tarefas para persistência ou execução.	T1053
	T1047	Uso do Windows Management Instrumentation (WMI) para instalação de componentes.	T1047
C2 (Comando e Controle)	T1071	Uso de protocolos de aplicação para comunicação C2.	T1071
	T1071.001	Comunicação C2 usando protocolos web.	T1071.001

	T1071.002	Uso de protocolos de transferência de arquivos para C2.	T1071.002
	T1071.004	Comunicação C2 via consultas DNS.	T1071.004
	T1105	Transferência de ferramentas para sistemas comprometidos.	T1105
	T1572	Encapsulamento de tráfego para ocultar a comunicação.	T1572
Ações & Objetivos	T1074	Preparação e organização dos dados coletados antes da exfiltração.	T1074
Ações & Objetivos	T1070	Remoção de indicadores para ocultar atividades.	T1070
	T1491	Alteração não autorizada de sites ou aplicações para propaganda ou desmoralização.	T1491
	T1490	Desativação de recursos de recuperação do sistema.	T1490
	T1489	Parada de serviços críticos do sistema.	T1489
	T1486	Criptografar dados para extorsão ou impacto operacional.	T1486
Reconhecimento	T1585.001	Criação de contas em redes sociais para operações maliciosas.	T1585.001
	T1589	Obter informações de identidade das vítimas.	T1589
	T1135	Identificação de compartilhamentos de rede.	T1135
	T1046	Varredura para identificar serviços na rede.	T1046
	T1082	Descoberta de informações sobre o sistema.	T1082
	T1047	Usar WMI para identificar sistemas na rede.	T1047
	T1047	Uso de WMI para interagir com sistemas remotos.	T1047
Preparação	T1587.001	Desenvolvimento de malware para objetivos maliciosos.	T1587.001
Execução	T1059.003	Execução via Windows Command Shell.	T1059.003
	T1059.001	Execução via PowerShell.	T1059.001
	T1059.005	Execução via Visual Basic.	T1059.005
Ações & Objetivos	T1566	Phishing para entregar malwares ou explorar informações.	T1566
	T1204	Exigência de execução do usuário para abrir malware.	T1204
Exfiltração de Dados	T1567	Exfiltração de dados por meio de serviços web.	T1567
Ações & Objetivos	T1566.001	Phishing com anexo de e-mail malicioso.	T1566.001
	T1566.002	Phishing com link malicioso em e-mail.	T1566.002
Exfiltração de Dados	T1041	Exfiltração de dados via canal de comando e controle.	T1041
Execução	T1204.001	Execução de link malicioso, frequentemente via email.	T1204.001

Tabela 3- Principais TTPs do ransomware RansomHouse.

4 Indicadores de Comprometimento (IOC)

Em geral, os indicadores de compromisso são variáveis, pois os atacantes podem mover, adicionar ou alterar informações técnicas de sua infraestrutura de acordo com o ataque, campanha ou atores ou de ameaça. As datas de submissão dos IoCs foram extraídas da ferramenta Virus Total.

Tipo	IoC	Primeira Submissao	Última Submissao
Official Blog	zohlm7ahjwegcedoz7lrdrti7bvpoфymcayotp744qhx6gjmxbuo2yid[.]onion	-	-
MD5	d2853c1d92c73dc047cdb1f201900a99	2023-09-21	2024-12-03
	ef46880a8583da64cebea1e8f8cb1fb3	2023-09-09	2023-09-20
	b7e2f4a5bc67256189e6732fbce86520	-	-
	0c93cac9854831da5f761ee98bb40c37	2023-06-19	2024-11-05
	ff6f16b00c9f36b32cd60fecd4dfc8e9	-	-
	286bd9c2670215d3cb4790aac4552f22	-	-
	4dd6250eb2d368f500949952eb013964	2021-12-12	2023-08-21
	57cd8e220465aa8030755d4009d0117c	2020-12-19	2024-10-23
	6d3041b89484c273376e5189e190d235	-	-
	8d070a93a45ed8ba6dba6bfbe0d084e7	-	-
	952482949f495fb66e493e441229ae4b	-	-
	a991bdbf1e36d7818d7a340a35a4ea26	-	-
	b219672bcd60ce9a81b900217b3b5864	2023-05-29	2023-05-29
	b4b1e285b9f666ae7304a456da01545e	-	-
	c517519097bff386dc1784d98ad93f9d	-	-
SHA256	c57e59314aee7422e626520e495effe0	-	-
	caffdb648a0a68cd36694f0f0c7699d7	-	-
	d1ce3117060e85247145c82005dda985	-	-
	3934b3da6bad0b4a28483e25e7bab919d7ed31f2f51cca22c56535b9f8183a0e	2023-09-26	2024-11-10
	2c1a4fe4a2ac4f0a49052f9521458136eb477fe23665dc4b7076fb32de3005d	2023-11-16	2023-11-16
	0a77e537c64336f97a04020e59d17d09d459d1626a075878e2b796d1e1033038	2023-10-26	2024-11-30
	d36afcfe1ae2c3e6669878e6f9310a04fb6c8af525d17c4ffa8b510459d7dd4d	2023-09-21	2024-11-10
SHA1	3F2FD2DFD27BF3CAFBCF0946E308832E11A1D9C1	-	-

URLs	files.catbox[.]moe	-	-
	vipjobsglobal[.]com	-	-
	dreamy-jobs[.]com	-	-
	wazayif-halima[.]com		
IPs	Descrição		
	89.208.107.158	Servidor C2 conhecido	
188.126.89.20:23762	Servidor C2 conhecido		

Tabela 4- Principais IoCs do ransomware RansomHouse.

5 Vulnerabilidades e Exposições Conhecidas (CVEs)

O grupo RansomHouse costuma obter acesso ao ambiente das vítimas por meio da exploração de serviços vulneráveis, geralmente visando ativos ou aplicativos públicos com vulnerabilidades conhecidas não corrigidas (CVES). Foram listados a seguir as principais vulnerabilidades exploradas pelo grupo de acordo com seu nível de criticidade e sistemas afetados.

CVE-2024-3400 CVSS: 10 Explorado Ativamente

Descrição: Uma injeção de comando como resultado de uma vulnerabilidade arbitrária de criação de arquivos no recurso GlobalProtect do software PAN-OS da Palo Alto Networks para versões específicas do PAN-OS e configurações de recursos distintas pode permitir que um invasor não autenticado execute código arbitrário com privilégios de root no firewall. O Cloud NGFW, os dispositivos Panorama e o Prisma Access não são afetados por essa vulnerabilidade.

Sistemas Afetados: paloaltonetworks pan-os v. 11.1.0 e anteriores

CVE-2020-10148 CVSS: 9.8 Explorado Ativamente

Descrição: A API SolarWinds Orion é vulnerável a um desvio de autenticação que pode permitir que um invasor remoto execute comandos da API. Essa vulnerabilidade pode permitir que um invasor remoto ignore a autenticação e execute comandos de API, o que pode resultar no comprometimento da instância da SolarWinds. As versões 2019.4 HF 5, 2020.2 da plataforma SolarWinds Orion sem hotfix instalado e 2020.2 HF 1 são afetadas.

Sistemas Afetados: solarwinds orion_platform 2020.2; solarwinds orion_platform 2019.4; solarwinds orion_platform 2020.2.1

CVE-2022-1388 CVSS: 9.8 Explorado Ativamente

Descrição: Nas versões F5 BIG-IP 16.1.x anteriores à 16.1.2.2, nas versões 15.1.x anteriores à 15.1.5.1, nas versões 14.1.x anteriores à 14.1.4.6, nas versões 13.1.x antes da 13.1.5 e em todas as versões 12.1.x e 11.6.x, solicitações não reveladas podem ignorar a autenticação REST do iControl. Nota: As versões de software que atingiram o fim do suporte técnico (EOTs) não são avaliadas.

Sistemas Afetados: f5 big-ip_global_traffic_manager *;

[CVE-2023-22515](#) CVSS: 9.8  Explorado Ativamente

Descrição: A Atlassian foi informada de um problema relatado por alguns clientes em que invasores externos podem ter explorado uma vulnerabilidade até então desconhecida em instâncias do Confluence Data Center e do Server acessíveis ao público para criar contas de administrador não autorizadas do Confluence e acessar instâncias do Confluence.

Sistemas Afetados: atlassian confluence_data_center *; atlassian confluence_server *.

[CVE-2023-34362](#) CVSS: 9.8  Explorado Ativamente

Descrição: Foi encontrada uma vulnerabilidade de injeção de SQL no aplicativo web MOVEit Transfer que poderia permitir que um invasor não autenticado obtivesse 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.

Sistemas Afetados: moveit_transfer *.progress moveit_cloud *;

[CVE-2023-35708](#) CVSS: 9.8  Explorado Ativamente

Descrição: Um invasor poderia enviar uma carga útil criada para um endpoint do aplicativo MOVEit Transfer, o que poderia resultar na modificação e divulgação do conteúdo do banco de dados MOVEit. Essas são as versões corrigidas da DLL drop-in: 2020.1.10 (12.1.10), 2021.0.8 (13.0.8), 2021.1.6 (13.1.6), 2022.0.6 (14.0.6), 2022.1.7 (14.1.7) e 2023.0.3 (15.0.3).

Sistemas Afetados: moveit_transfer *.progress

[CVE-2023-3519](#) CVSS: 9.8  Explorado Ativamente

Descrição: Execução remota de código não autenticada.

Sistemas Afetados: citrix netscaler_application_delivery_controller *;

[CVE-2019-0604](#) CVSS: 9.8  Explorado Ativamente

Descrição: Existe uma vulnerabilidade de execução remota de código no Microsoft SharePoint quando o software não consegue verificar a marcação de origem de um pacote de aplicativos, também conhecida como "Vulnerabilidade de execução remota de código do Microsoft SharePoint". Esse ID CVE é exclusivo do CVE-2019-0594.

Sistemas Afetados: microsoft sharepoint_foundation 2013; microsoft sharepoint_server 2010; microsoft sharepoint_enterprise_server 2016; microsoft sharepoint_server 2019.

CVE-2024-23897 CVSS: 9.8  Explorado Ativamente

Descrição: O Jenkins 2.441 e versões anteriores, o LTS 2.426.2 e versões anteriores não desativam um recurso de seu analisador de comandos CLI que substitui um caractere '@' seguido por um caminho de arquivo em um argumento com o conteúdo do arquivo, permitindo que invasores não autenticados leiam arquivos arbitrários no sistema de arquivos do controlador Jenkins.

Sistemas Afetados: jenkins *.

CVE-2019-19781 CVSS: 9.8  Explorado Ativamente

Descrição: Um problema foi descoberto no Citrix Application Delivery Controller (ADC) e no Gateway que permitem a travessia de diretórios.

Sistemas Afetados: citrix application_delivery_controller_firmware V.10.5, 11.1, 12.0, 12.1 e 13.0

CVE-2023-4966 CVSS: 9.4

Descrição: Divulgação de informações confidenciais no NetScaler ADC e no NetScaler Gateway quando configurado como um Gateway (servidor virtual VPN, ICA Proxy, CVPN, RDP Proxy) ou servidor virtual AAA.

Sistemas Afetados: citrix netscaler_application_delivery_controller *

CVE-2023-35036 CVSS: 9.1

Descrição: Um invasor poderia enviar uma carga útil criada para um endpoint do aplicativo MOVEit Transfer, o que poderia resultar na modificação e divulgação do conteúdo do banco de dados MOVEit.

Sistemas Afetados: progress moveit_transfer *.

CVE-2024-21887 CVSS: 9.1  Explorado Ativamente

Descrição: Uma vulnerabilidade de injeção de comando nos componentes web do Ivanti Connect Secure (9.x, 22.x) e do Ivanti Policy Secure (9.x, 22.x) permite que um administrador autenticado envie solicitações especialmente criadas e execute comandos arbitrários no dispositivo.

Sistemas Afetados: Ivanti Policy Secure v. 9.x, 22.x, Ivanti Connect Secure v.9.x, 22.x

[CVE-2021-34473](#) CVSS: 9.1  Explorado Ativamente

Descrição: Vulnerabilidade de execução remota de código do Microsoft Exchange Server

Sistemas Afetados: microsoft exchange_server 2016; microsoft exchange_server 2013; microsoft exchange_server 2019; microsoft exchange_server 2019; microsoft exchange_server 2016.

[CVE-2021-34523](#) CVSS: 9.0  Explorado Ativamente

Descrição: Vulnerabilidade de execução remota de código do Microsoft Exchange Server

Sistemas Afetados: microsoft exchange_server 2016; microsoft exchange_server 2013; microsoft exchange_server 2019; microsoft exchange_server 2019; microsoft exchange_server 2016.

[CVE-2021-21974](#) CVSS: 8.8

Descrição: O OpenSLP usado no ESXi (7.0 antes do ESXi70u1c-17325551, 6.7 antes do ESXi670-202102401-SG, 6.5 antes do ESXi650-202102101-SG) tem uma vulnerabilidade de estouro de pilha. Um agente mal-intencionado residente no mesmo segmento de rede do ESXi que tenha acesso à porta 427 pode acionar o problema de estouro de pilha no serviço OpenSLP, resultando na execução remota de código.

Sistemas Afetados: vmware cloud.foundation *, vmware esxi 6.*

[CVE-2024-24919](#) CVSS: 8.6  Explorado Ativamente

Descrição: Possivelmente permitindo que um invasor leia determinadas informações nos gateways de segurança da Check Point, uma vez conectado à Internet e ativado com VPN de acesso remoto ou Mobile Access Software Blades. Uma correção de segurança que atenua essa vulnerabilidade está disponível.

Sistemas Afetados: checkpoint quantum_security_gateway_firmware r80.40; checkpoint clouguard_network_security*

[CVE-2023-0669](#) CVSS: 7.2  Explorado Ativamente

Descrição: O Fortra (anteriormente HelpSystems) GoAnywhere MFT sofre de uma vulnerabilidade de injeção de comando de pré-autenticação no License Response Servlet devido à desserialização de um objeto arbitrário controlado por um atacante. Esse problema foi corrigido na versão 7.1.2.

Sistemas Afetados: fortra goanywhere_managed_file_transfer *.

6 Prevenção

Para lidar com essa ameaça, é essencial iniciar com medidas preventivas, que incluem:

- Atualizar e aplicar patches regularmente em todos os sistemas para mitigar vulnerabilidades conhecidas;
- Segmentar as redes para limitar a disseminação de ransomware dentro da organização;
- Limitar o uso de serviços de desktop remoto como o RDP e SMB;
- Monitorar atividades de acessos remotos;
- Implementar medidas de segurança avançadas, incluindo proteção de terminais, soluções anti-ransomware e segmentação de rede, para detectar, prevenir e limitar a propagação de ataques de ransomware;
- Implementar soluções DLP e aprimorar o monitoramento da rede para detectar, controlar e responder a atividades suspeitas de exfiltração de dados;
- Monitorar o tráfego da rede em busca de atividades incomuns que possam indicar uma infecção por ransomware;
- Implementar backups de dados regulares e garanta que eles sejam armazenados off-line ou em um ambiente de nuvem seguro;
- Realizar treinamentos de conscientização sobre segurança para que os funcionários reconheçam tentativas de phishing e outros métodos comuns de entrega de ransomware;
- Implementar a autenticação de múltiplo fator (MFA) para proteger o acesso remoto e os sistemas críticos;
- Realizar auditorias regulares de segurança e avaliações de vulnerabilidade para identificar e corrigir possíveis falhas de segurança;
- Certifica-se de que todos os sistemas tenham software antivírus e antimalware atualizado instalado e em execução.

7 Conclusão

Tradicionalmente, os ataques de ransomware envolvem criptografia e exfiltração de dados, com alguns casos envolvendo roubo de dados sem criptografia. No entanto, a colaboração entre grupos como RansomHouse, Dark Angels e outros introduz uma nova abordagem em que os dados roubados são reciclados entre os agentes de ameaças, levando a tentativas enganosas de extorsão que simulam novos ataques. Esse fenômeno ressalta a importância de as organizações aprimorarem suas medidas de segurança cibernética para proteger contra violações iniciais e mitigar os riscos representados pelo uso indevido subsequente de dados roubados.

Além disso, o envolvimento de grupos como Snatch e Stormous em operações de influência, camufladas sob o disfarce de hacktivismo, adiciona outra camada de complexidade. Essas operações têm como alvo dados sensíveis e visam manipular a opinião pública e influenciar narrativas geopolíticas. A defesa contra essas ameaças requer uma abordagem abrangente que inclua defesas de segurança cibernética robustas, protocolos rigorosos de proteção de dados e respostas estratégicas para mitigar danos à reputação em níveis governamentais e individuais.

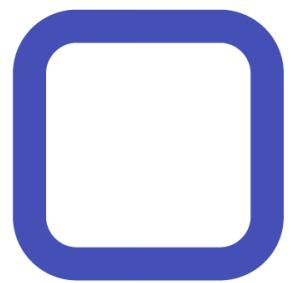
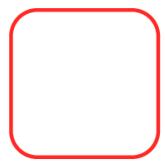
Algumas medidas específicas incluem limitar o uso de serviços de desktop remoto como o RDP, aplicar autenticação multifator (MFA) em todas as conexões de VPN, desabilitar o protocolo SMB versão 1 e atualizar para a versão 3, além de exigir a autenticação Kerberos para comunicações laterais SMB. Monitorar e registrar o tráfego SMB também pode ajudar a identificar comportamentos anormais ou prejudiciais.

Entender as metodologias, IOCs e alvos da RansomHouse é crucial para desenvolver estratégias de defesa eficazes, mitigar o impacto de seus ataques e, finalmente, reduzir o risco de ser vítima desse grupo de ransomware.

8 Referências

Principais referências utilizadas como fontes de pesquisa neste Relatório de Inteligência foram listadas a seguir. Acesso realizado em 16 de dezembro de 2024.

- **Analyst1:** [RansomHouse: Stolen Data Market, Influence Operations & Other Tricks Up the Sleeve](#)
- **Cyfirma:** [Weekly Report – 24 May 2024](#)
- **Polaris:** [RansomHouse](#)
- **Trellix:** [RansomHouse Am See](#)



Logical IT

