NOVO RANSOMWARE

RansomHouse cria ferramenta para automatizar a implantação em seu criptografador

heimdall
security research
A DIVISION OF ISH

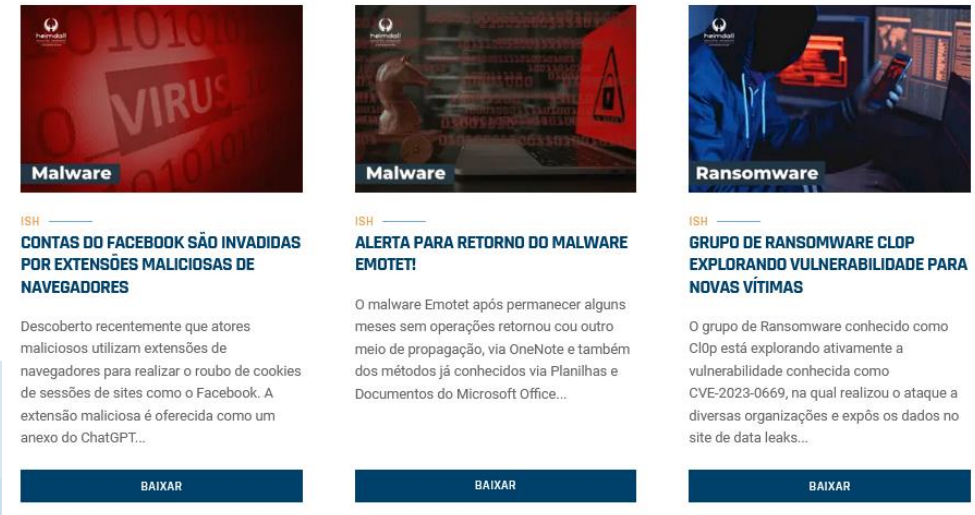
TLP: CLEAR

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



Sumário

Lista de Tabelas

Lista de Figuras

1 NOVA OPERAÇÃO DE RANSOMWARE

Recentemente, foi identificada uma nova operação de **ransomware** denominada '*RansomHouse*', que desenvolveu uma nova ferramenta denominada '**MrAgent**'. Ferramenta essa que tem a capacidade de automatizar a disseminação do software de criptografia de dados através de diversos *hipervisores* **VMware ESXi**. Essa é uma operação de *Ransomware as a Service* (**RaaS**), desde dezembro de 2021, utiliza tática de dupla extorsão.

Os servidores ESXi desempenham um papel fundamental nas operações das empresas hospedando aplicativos e serviços essenciais, como bancos de dados e sistemas de e-mail. Dessa forma, quando esses servidores são alvo de ataques de ransomware, o impacto na continuidade das operações é extremamente elevado, uma vez que interrompe funções críticas. O grupo é identifica-se por usar uma variante de ransomware exclusiva, chamada **Mario ESXi**, junto com MrAgent, para atingir sistemas baseados em Windows e Linux. O ransomware compartilha código com Babuk, o que se torna aparente ao reverter ambas as amostras.

O MrAgent identifica o sistema host, desliga seu firewall e, em seguida, automatiza o processo de implantação de ransomware em vários hipervisores simultaneamente, comprometendo todas as VMs gerenciadas. Essa ferramenta oferece suporte a configurações personalizadas para implantação de ransomware recebidas diretamente do servidor de *command and control* (**C2**). As configurações englobam a criação de senhas para o hipervisor, ajustes no comando de criptografia e seus parâmetros, a programação de uma atividade de encriptação, e a modificação do texto de saudação no display do hipervisor, que passará a exibir uma notificação de resgate.

host.startIn	Number of seconds to wait before starting
host.pass	Password to set on the ESXi host
host.command	Encrypter command
host.args	Arguments to provide to encrypter
host.welcomeMsg	Message to configure in the ESXi /etc/motd file

Figura 1 – Configuração do MrAgent.

O MrAgent possui a capacidade de realizar comandos locais no hipervisor, os quais são instruídos pelo C2, incluindo a exclusão de arquivos e o encerramento de sessões SSH ativas, com o objetivo de minimizar interferências durante a criptografia. Além disso, o software é capaz de coletar e transmitir dados referentes às VMs que estão operando no momento.

2 MODUS OPERANDI O GRUPO

Segundo a Trellix, o grupo RansomHouse disponibiliza um ambiente de chat baseado em rede Tor para interagir com suas vítimas, oferecendo dois idiomas para bate-papo: inglês e chinês. Adicionalmente, mantém um blog dedicado a expor detalhes de vazamentos de dados, incluindo informações sobre as vítimas e os dados roubados. Este portal inclui ainda uma área de FAQ/regras, evidenciando o esforço do grupo em apresentar-se de maneira profissional e fornecendo informações sobre seu modus-operandi e formas de comunicação.

Figura 2 – Tela de captura censurada da página de vazamento.

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.

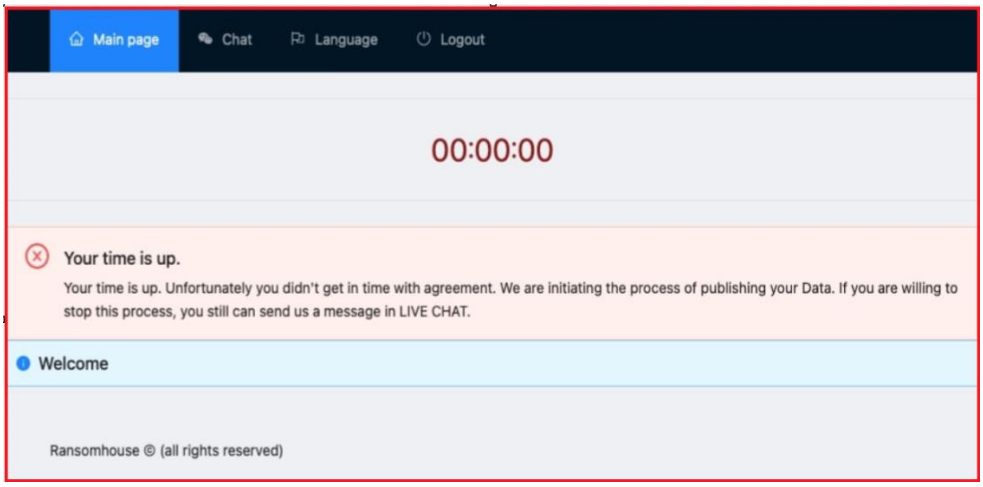


Figura 3 – página inicial do site de vazamento".

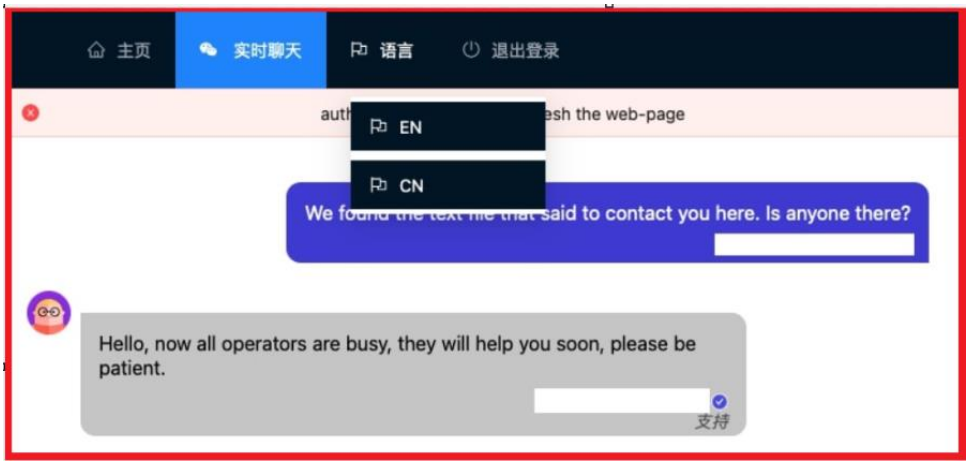


Figura 4 – Idiomas disponibilizados

Abaixo é possível observar uma negociação, um interessante jogo de gato e rato. 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.

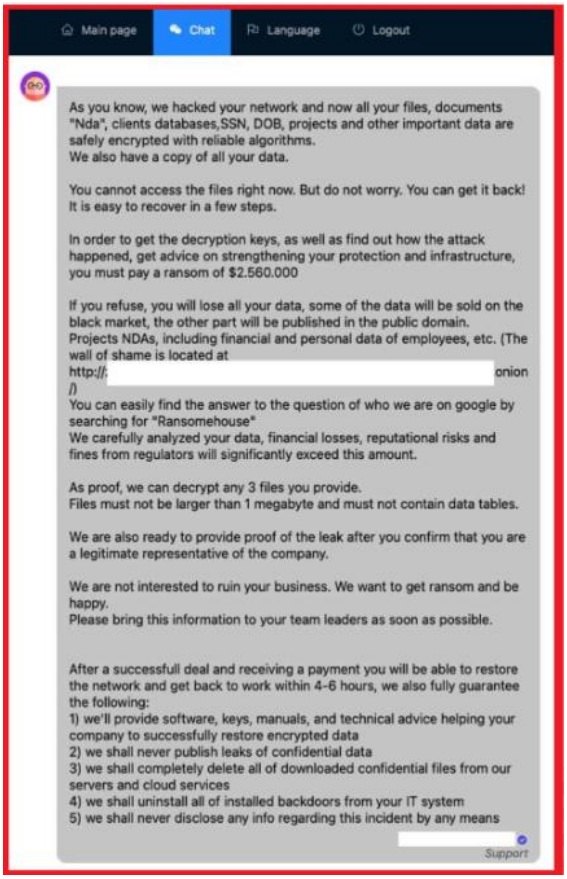


Figura 5 – Parte da negociação de pagamento

Figura 6 – Cronograma das Negociações

A transferência dos dados extraídos foi realizada para o MEGA, que é um serviço de compartilhamento de arquivos. O volume total era de 61,2 GB, distribuídos em cinquenta arquivos zip, cada um com aproximadamente um gigabyte.

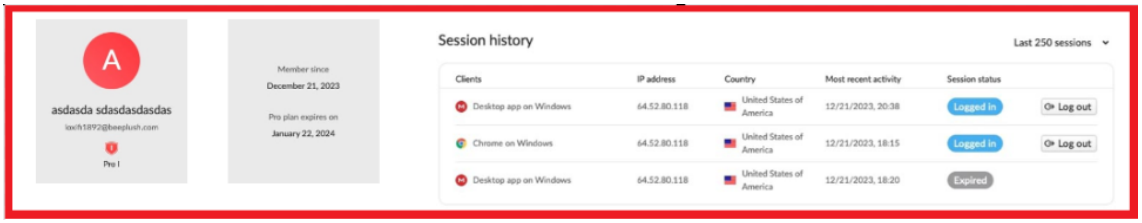


Figura 7 – Contas Mega Pro relacionadas

Diante dos fatos, há algumas observações importantes da negociação de duas semanas. A prova de descriptografia parcial foi fornecida e a ferramenta de descriptografia foi liberada diretamente após o pagamento final. Os pagamentos aconteceram em duas transações, primeiro uma transação de **0,1** *BITCOIN* (**BTC**), após a qual a segunda transação continha o restante do pedido de resgate, convertido em BTC com base na taxa de câmbio da época. Por último, a RansomHouse mostra alguma flexibilidade na negociação, embora ainda saia com mais de um milhão de dólares em resgate. O acordo final inclui um acordo de

não divulgação, juntamente com a recuperação de dados com o descriptografador fornecido. A conversa de negociação acabou sendo removida da página do Tor em 31 de dezembro de 2023.

O pagamento do resgate foi realizado em duas etapas. Inicialmente, 0,1 BTC foram enviados para o endereço "*1MmkNa1gRUmVSocZic8wJhehef8NW4GzDZ*". 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 "*bc1q93xvcqux2xl4n03985lyrh8w55et8tt60fcrmy*", possivelmente a carteira da RansomHouse. 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.

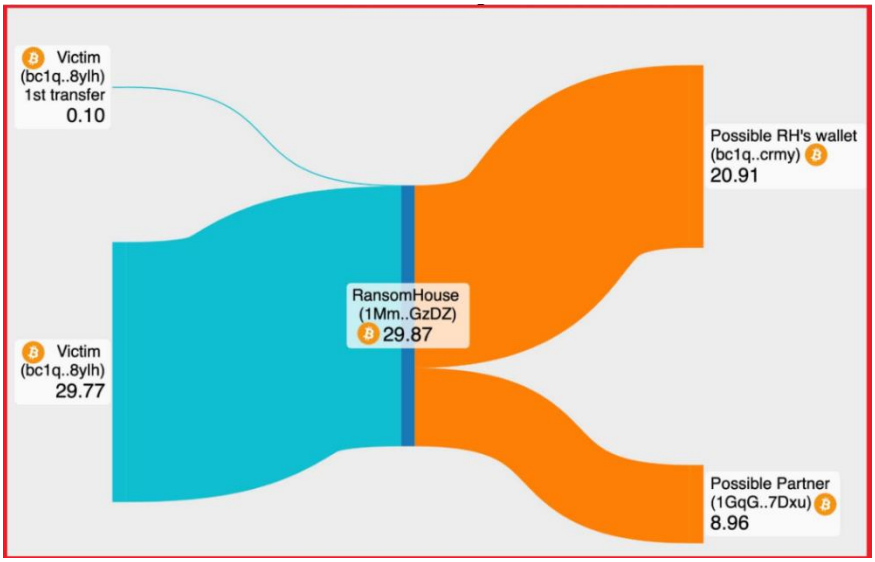


Figura 8 – Transferência dos Bitcoins

4 VÍTIMAS AO LONGO DO TEMPO

O grupo RansomHouse prosseguiu as suas operações com atividade ao longo de todo o ano de 2023. Neste ano foi observado um aumento significativo em Março, com 12 vítimas, enquanto outros meses registaram uma taxa mais constante de dois a cinco ataques.

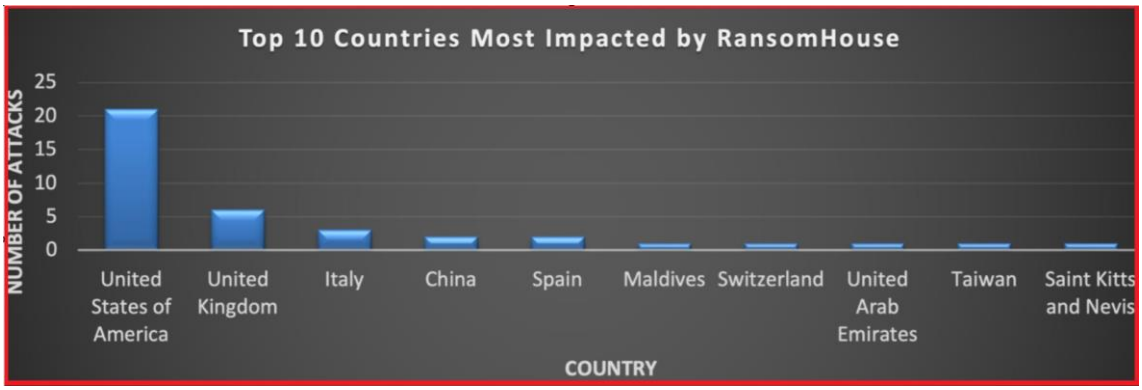


Figura 9 – Principais países impactados

Segundo a Acronis, o RansonHouse visou notoriadamente a Itália, marcando uma tendência significativa nas suas operações sofrendo uma parcela substancial de ataques. Entretanto, em 2023 os Estados Unidos surgem como seu alvo principal, sofrendo aproximadamente 47,37% de todos os ataques. Se pararmos para analisar, a tendência tem como foco principal a América do Norte e a Europa Ocidental, em que os setores industriais foram os mais visados, compreendendo cerca de quase 44,74% das atividades da RansomHouse em 2023.

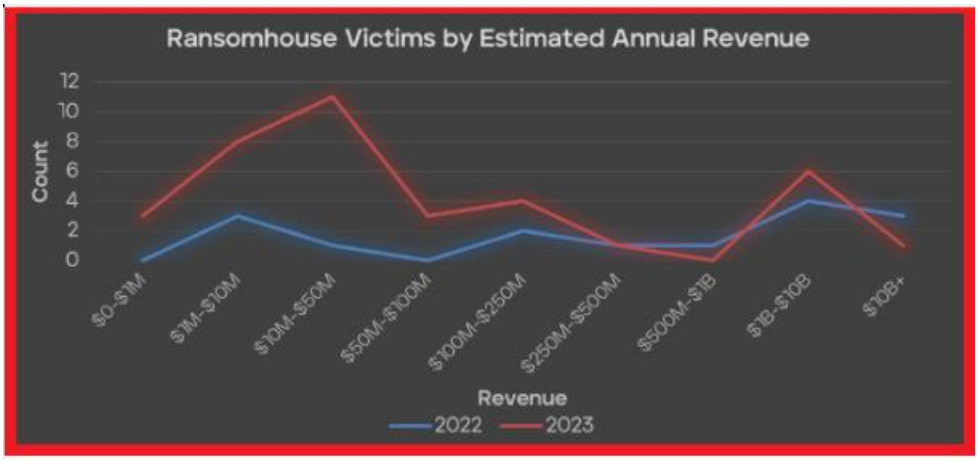


Figura 10 – Estimativas de vítimas

5 IOC

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 de artefato malicioso/ analisado	
md5:	d2853c1d92c73dc047cdb1f201900a99
sha1:	5b1541ee4ccfc020a081361ea8d6fe48d20e602a
sha256:	8189c708706eb7302d7598aeee8cd6bdb048bf1a6dbe29c59e50f0a39fd53973
File name:	mrAgent

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	ef46880a8583da64cebea1e8f8cb1fb3
sha1:	51cfd3290e562367bc5b0930eb5ad70586979b75
sha256:	bfc9b956818efe008c2dbf621244b6dc3de8319e89b9fa83c9e412ce70f82f2c
File name:	Q1NS7auqvcPWuqPIL1H2whKRCL0Tp6

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	e79984ea02b2049b1e74452013529da5
sha1:	6bb0c60195d90b032a3488b50a38a797dfcf9104
sha256:	3934b3da6bad0b4a28483e25e7bab919d7ed31f2f51cca22c56535b9f8183a0e
File name:	soft

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	446237df80b3f155519b5fde00a82087
sha1:	23f83a96144ace88b0491ab519ead733342da0e6
sha256:	2c1a4fe4a2ac4f0a49052f9521458136eb477fe23665dc4b7076fbd32de3005d
File name:	f26514808.elf

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	e56c97cb4f9df25845cda36e3cd7d597
sha1:	048b3942c715c6bff15c94cdc0bb4414dbab9e07
sha256:	2c1475f1b49a8b93a6c6217be078392925535e084048bf04241e57a711f0f58e
File name:	emario.elf

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	dd2fee6e1ace30b2d3be7b45f2fd6a82
sha1:	b348b50aa1868140d750f633d4bd7c8cebc86f1c
sha256:	0a77e537c64336f97a04020e59d17d09d459d1626a075878e2b796d1e1033038
File name:	linux.out

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	0dcbb7c7af77efd4a2b39f2303806fcd
sha1:	0a18d66e3f72e21b9a507739dbeb009d017dcfe0
sha256:	d36afcfe1ae2c3e6669878e6f9310a04fb6c8af525d17c4ffa8b510459d7dd4d
File name:	e_mario.out

Tabela 1 – IoCs relacionadas ao malware.

6 CONCLUSÃO

O detalhamento do ransomware RansomHouse revela suas características únicas em comparação com outros grupos de ransomware. Os desafios significativos que ele apresenta para a segurança cibernética. Através da análise técnica, observou-se que o RansomHouse é um software malicioso avançado, capaz de criptografar dados de vítimas e exigir resgate em troca da chave de descriptografia. Seu método de infecção, geralmente por meio de uma abordagem de comunicação direta com as vítimas, utilizando canais como Telegram e sites na Dark Web para anunciar suas vítimas, destaca a necessidade de uma maior conscientização e educação em segurança digital.

As consequências do ataque por RansomHouse vão além da perda de dados; elas afetam a reputação das organizações, causam interrupções operacionais e podem levar a perdas financeiras significativas.

7 RECOMENDAÇÕES

Além dos indicadores de comprometimento elencados pela ISH, poderão ser adotadas medidas visando a mitigação da infecção do referido *malware*, como por exemplo a implementação de uma arquitetura de confiança zero para evitar acessos não autorizados, realizando varreduras regulares de vulnerabilidade, especialmente em dispositivos voltados para a internet, e mantendo softwares e sistemas operacionais atualizados com as versões mais recentes.

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.

Essas estratégias não apenas ajudam a proteger contra ameaças específicas como o RansomHouse, mas também fortalecem a postura geral de segurança cibernética das organizações contra uma variedade de vetores de ataque.

8 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Trellix**
- **bleepingcomputer**
- **Acronis**

heimdall
security research
A DIVISION OF ISH