heimdall

security research

A DIVISION OF ISH

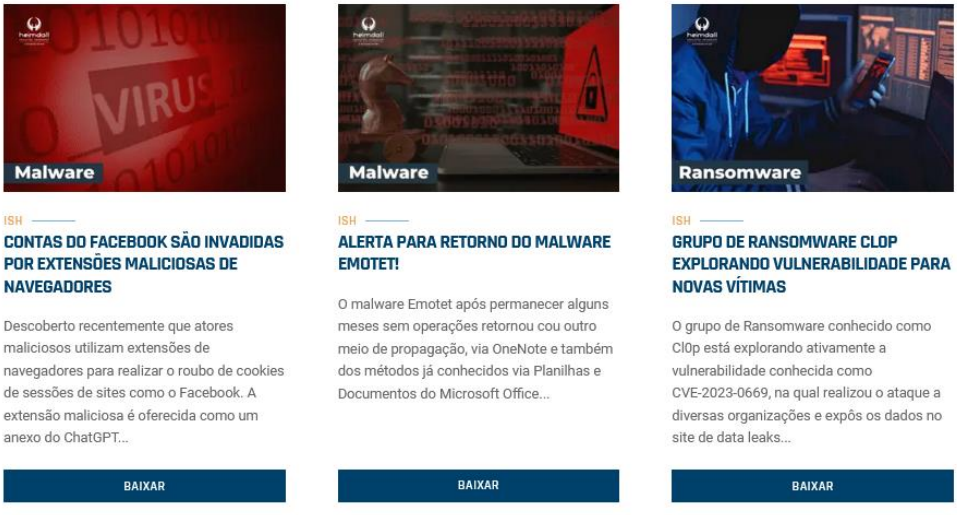
Operação do Ransomware Rhysida

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 INTRODUÇÃO

No dia 04 de agosto de 2023, o Helth Sector Cybersecurity Coordination Center (HC3) divulgou um alerta de segurança sobre um novo ransomware chamado Rhysida, o qual estaria ativo desde maio de 2023.

A operação do Ransomware ainda não está muito clara com relação a origem ou afiliações, sendo que de acordo com o alerta, o grupo de apresenta como uma "equipe de segurança cibernética" que se oferece para ajudar as vítimas a encontrar falhas de segurança em suas redes e sistemas.

Quem são os alvos?

O Ransomware Rhysida tem como alvo as indústrias de educação, governo, manufatura e tecnologia e teria começado a realizar ataques a organizações de saúde pública e de saúde. É visível que o setor de saúde tem um número crescente de ataques de ransomwares nos últimos cinco anos.

2 RESUMO DO RANSOMWARE

De acordo com a publicação realizada pela Trend Micro, foi possível obter a cadeia de ataque relacionada aos atores do ransomware, o qual geralmente chega à máquina da vítima por meio de **Phishing** e, após o **Cobalt Strike** é utilizado para fins de movimentos laterais dentro do sistema.

Na sequência, os atores executam o **PsExec** para implantar scripts do PowerShell e o próprio payload do Ransomware Rhysida. O **PowerShell** (g.ps1), é utilizado pelos atores para encerrar os processos e serviços relacionados a antivírus, excluir cópias de sombra, modificar configurações de protocolos de área de trabalho remoto (RDP) e alterar a senha do diretório ativo (AD).

Segundo a Trend Micro, o script (g.ps1) foi atualizado pelos atores de ameaças durante a execução, identificando uma versão do **PowerShell** do Ransomware Rhysida.

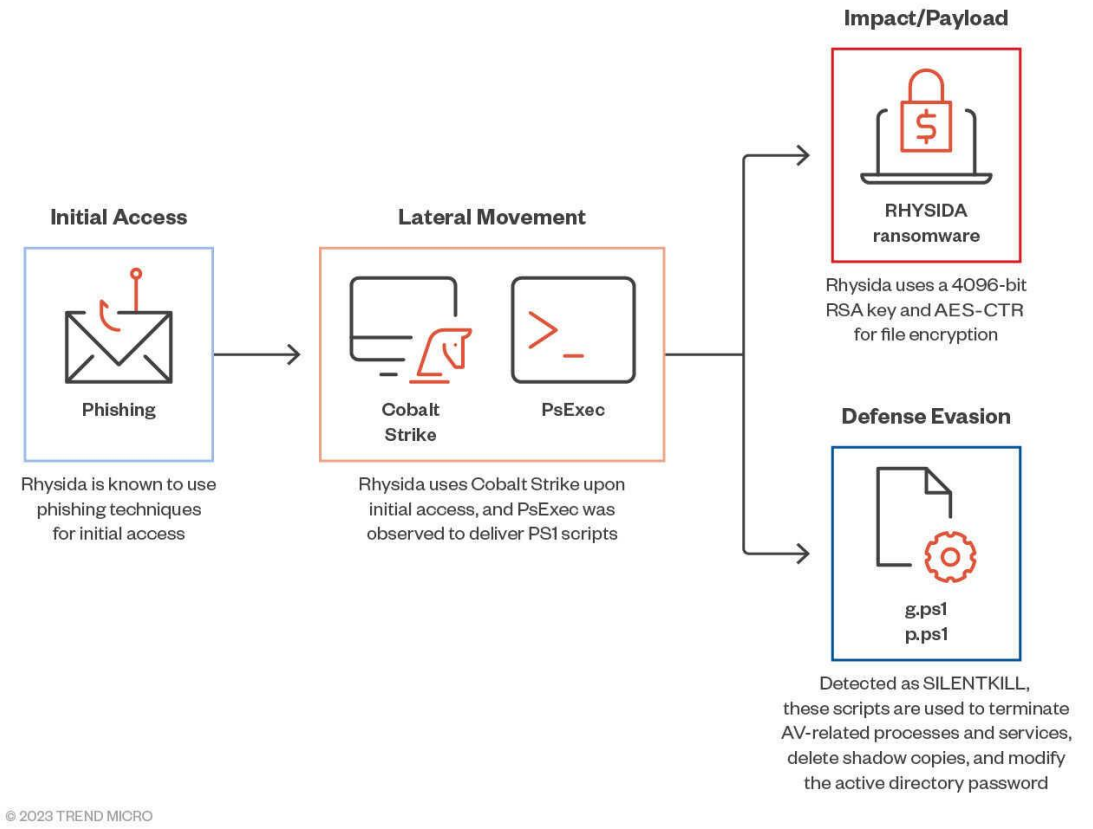


Figura 1 – Cadeia de infecção e ataque do Ransomware Rhysida.

Para fins de criptografia, o Ransomware emprega uma chave **RSA de 4096 bits e AES-CTR** para criptografia dos arquivos, sendo após a criptografia bem-sucedida, ele acrescenta a extensão “.rhysida” e cria a nota de resgate “CriticalBreachDetected.pdf”.

A nota de resgate é diferente dos demais grupos de ransomwares, sendo que ao invés de haver o pedido do resgate definitivo, a nota apresenta um alerta “equipe de segurança cibernética’, notificando as vítimas de que seu sistema foi comprometido e seus arquivos criptografados.

3 Conclusão

Com isto, podemos concluir que o **Ransomware Rhysida** está no início de suas operações e já foi identificado como autor de 36 ataques a organizações, dentre as quais se encontram setores como: Manufatura, Insurance, Tecnologia, Saúde, Bancária e outras, bem como realizou o ataque a diversas companhias a diversos países, incluindo no Brasil.

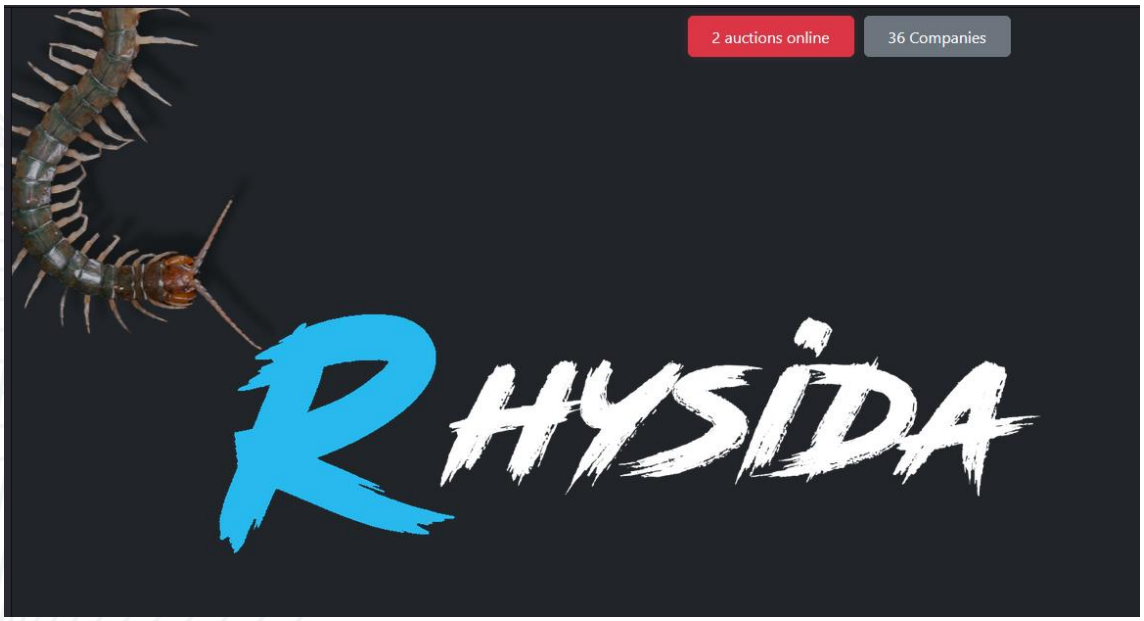


Figura 2 – Capa da página do site do Ransomware.

4 TTPs – MITRE ATT&CK

Tática	Técnica	Detalhes
Acesso Inicial TA0001	Phishing T1566	Rhsyida utiliza iscas de phishing para acessos iniciais.
Movimentação Lateral TA0008	Remote Services: PsExec T1021.002	Utilização da ferramenta PsExec para execuçao remota
	Remote Services: Cobalt Strike T1021.002	Utilização da ferramenta para movimentação lateral
Persistência TA0003	Tarefa/Trabalho agendado: Tarefa agendada T1053.005	Quando executado com o argumento "-S", ele criará uma tarefa agendada camada Rhsd que executará o Ransomware.
Execução TA0002	Comando e Intérprete de Script: Shell de comando do Windws T1059.003	Ele utiliza o cmd.exe para executar comandos para execução.
	Interpretador de Comandos e Scripts: PowerShell T1059.001	Utiliza o PowerShell para criar uma tarefa agendada chamada Rhsd apontado para o Ransomware
Evasão de Defesa TA0005	SilentKill	Utiliza script para encerrar processos e serviços relacionados à segurança, excluir cópias de sombra, modifica configurações de RDP e altera a senha do AD.
	Remoção do Indicador: Exclusão de Arquivos T1070.004	Rhysida se exclui após a execução. A tarefa agendada "Rhsd" criada também seria excluída após a execução.
	Remoção do Indicador: Limpar Logs de Eventos do Windows T1070.001	Ele utiliza o wevutil.xe para limpar os logs de eventos do Windows.
Descoberta TA0007	Descoberta de arquivos e diretórios T1083	Enumera e procura arquivos para criptografar em todas as unidades locais.
	Descoberta de Informações do Sistema T1082	Obtém as informações: Número de processadores Informações do Sistema
Impacto TA0040	Inibe a Recuperação do Sistema T1490	Executa o vssadmin para remover cópias de sombra de volumes.
	Dados criptografados para impacto T1486	Utiliza uma chave RSA de 4096 bits e Cha-Cha20 para criptografia dos arquivos. Ele evita criptografar arquivos com as strings: • .bat

		• .bin • .cab • .cmd • .com • .cur • .diagcab • .diagcfg • .diagpkg • .drv • .dll • .exe • .hlp • .hta • .ico • .msi • .ocx • .ps1 • .psm1 • .scr • .sys • .ini • .Thumbs.db • .url • .iso Evita criptografar arquivos encontrados nas seguintes pastas: • $Recycle.Bin • Boot • Documents and Settings • PerfLogs • ProgramData • Recovery • System Volume Information • Windows • $RECYCLE.BIN • ApzData Ele criptografa todas as unidades do sistema de A a Z. Ele solta a seguinte nota de resgate: “CriticalBreachDetected.pdf”
	Desfiguração: Desfiguração interna T1491.001	Ele altera o papel de parece da área de trabalho após a criptografia e impede que o usuário o altere de volta, modificando o valor do registro “NoChangingWallpaper”.

Tabela 1 – Tabela de acordo do MITRE ATT&CK.

5 IoCs

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:	0c8e88877383ccd23a755f429006b437
sha1:	69b3d913a3967153d1e91ba1a31ebed839b297ed
sha256:	a864282fea5a536510ae86c77ce46f7827687783628e4f2ceb5bf2c41b8cd3c6
File name:	09648299.exe

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	1e256229b58061860be8dbf0dc4fe67e
sha1:	338d4f4ec714359d589918cee1adad12ef231907
sha256:	d5c2f87033a5baeeb1b5b681f2c4a156ff1c05ccd1bfdaf6eae019fc4d5320ee
File name:	conhost.exe

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	59a9ca795b59161f767b94fc2dece71a
sha1:	b07f6a5f61834a57304ad4d885bd37d8e1badba8
sha256:	250e81eeb4df4649ccb13e271ae3f80d44995b2f8ffca7a2c5e1c738546c2ab1
File name:	bad_rhy_mayb.exe

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	0c8e88877383ccd23a755f429006b437
sha1:	69b3d913a3967153d1e91ba1a31ebed839b297ed
sha256:	a864282fea5a536510ae86c77ce46f7827687783628e4f2ceb5bf2c41b8cd3c6
File name:	fury_ctm1042.bin

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	599aa41fade39e06daf4cdc87bb78bd7
sha1:	2543857b275ea5c6d332ab279498a5b772bd2bd4
sha256:	6903b00a15eff9b494947896f222bd5b093a63aa1f340815823645fd57bd61de
File name:	nedimfud.exe

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	41948cd77a6cf817b77be426968a6ad3
sha1:	7abc07e7f56fc27130f84d1c7935a0961bd58cb9
sha256:	2a3942d213548573af8cb07c13547c0d52d1c3d72365276d6623b3951bd6d1b2
File name:	ruhsat.pdf.exe

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	db50086280878a064a1b5ccc61888bcd
sha1:	eda3a5b8ec86dd5741786ed791d43698bb92a262
sha256:	3bc0340007f3a9831cb35766f2eb42de81d13aeb99b3a8c07dee0bb8b000cb96
File name:	Invoice.zip

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	59a9ca795b59161f767b94fc2dece71a
sha1:	b07f6a5f61834a57304ad4d885bd37d8e1badba8
sha256:	250e81eeb4df4649ccb13e271ae3f80d44995b2f8ffca7a2c5e1c738546c2ab1
File name:	bad_rhy_mayb.exe

Tabela 2 – Indicadores de Compromissos.

URLs de distribuição e endereços IP C2:

https[:]//ipapi[.]com/json/

Tabela 3 – Indicador de Compromisso de Rede

Obs: Os *links* e endereços IP elencados acima podem estar ativos; cuidado ao realizar a manipulação dos referidos IoCs, evite realizar o clique e se tornar vítima do conteúdo malicioso hospedado no IoC.

6 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Alerta publicado pela HC3 – Ransomware Rhsyida**

heimdall
security research

A DIVISION OF ISH