

\\, /

```
>>> Principais Ataques à Segurança da Informação na Atualidade
>>> Redes II
```

Name: j.martins[†]-pigor[‡] (@pucminas)

Date: 9 de março, 2024

[†]João Victor Martins Medeiros

[‡]Pedro Igor Martins dos Reis

>>> Insomniac Games, Inc.

[illegible]

>>> Insomniac Games, Inc.¹

- * Fundada em 1994;
- * 400+ funcionários;
- * PlayStation Studios;
- * Xtreme Software, Inc.;
- * Desenvolvedora de jogos eletrônicos, como:
 - * *Sunset Overdrive* (2014);
 - * *Ratchet & Clank* (2002-);
 - * *Marvel's Spider-Man* (2018-);
 - * *Spyro The Dragon* (1996-2000);
 - * ...

¹<https://insomniac.games/>

>>> Rhysida

```
#####
###$#####
##$ $####
###$###$###
##$####$###
###$####$####
###$###$####
0###$###0#
###$ $###
#####
#####
####
$#####
$#####
$#####
$#####
$ $#####
$ $#####
#####
```

>>> Rhysida

- * Bitcoin;
- * *"Gold Victor"*;
- * *"Vice Society"*;
- * *Ransomware* com extorção dupla;
- * (Provável) Origem Russa, Bielorrussa e Cazaquistão;
- * De acordo com a CISA^a, surgiu em 2021[CIS23];

^aCybersecurity & Infrastructure Security Agency

>>> Modus operandi

conhost.exe ³	Um binário de <i>ransomware</i> .
psexec.exe ⁴	Executa um processo local ou remotamente.
S_0.bat	Um <i>script</i> para preparação de <i>ransomware</i> .
1.ps1	Identifica os arquivos a serem criptografados.
S_1.bat	Copia conhost.exe para C:\Windows\Temp.
S_2.bat	Adiciona a extensão .Rhysida em todo o ambiente.

³ conhost é um arquivo executável legítimo do Windows

⁴ Psexec também é uma ferramenta originalmente legítima da Microsoft

>>> **Modus operandi**

```
rule rw_rhysida {
  meta:
    author      = "Alex Delamotte"
    description = "Rhysida ransomware detection."
    sample      = "69b3d913a3967153d1e91ba1a31ebed839b297ed"
    reference   = "https://s1.ai/rhys"
  strings:
    $typo1 = { 63 6D 64 2E 65 78 65 20 2F ... }
    $cmd1  = { 63 6D 64 2E 65 78 65 20 2F ... }
    $cmd2  = { 63 6D 64 2E 65 78 65 20 2F ... }
    $byte1 = { 48 8D 05 72 AA 05 00 48 8B ... }
    $byte2 = { 48 8D 15 89 CF 03 00 48 89 ... }
  condition:
    2 of them
}
```

Listing 1: Regras YARA fornecidas pela equipe do SentinelOne

>>> Dia do ataque

- * *X-Men* (2030) [Fin23];
- * 50 Bitcoins^a;
- * 7 dias para reagir;
- * 1.6 TB de dados roubados [Pie23];
- * *Marvel's Wolverine* (2026);
- * *Venom: Lethal Protector* (2025) [];
- * Planejamento de uma década liberado;
- * Confirmado no dia 12 de dezembro de 2023;
- * 98% dos dados recolhidos foram publicados;
- * Passaportes e documentos governamentais de funcionários [Car23];

^a09/03, $\approx R\$17.296.275,91$

>>> Medidas preventivas

- * Política *Zero-Trust*;
- * Autenticação de multifator;
- * Sistemas de *anti-phishing* [23]^a;
- * Treinamento de funcionários;

^aAvanan, Barracuda Sentinel, Cofense PDR, ...

Qual das seguintes afirmações abaixo é verdadeira?

- * A) Grupos hackers, incluindo *Rhysida*, empregam técnicas de phishing como seu principal meio de ganhar acesso a sistemas de informação, visando especificamente indivíduos através de e-mails falsos que parecem ser de fontes legítimas.
- * B) O *ransomware* é um tipo de *malware* que, uma vez instalado em um sistema de computador, criptografa arquivos do usuário e exige um pagamento em criptomoeda para a descriptografia, mas não permite aos hackers acesso aos sistemas afetados ou dados.
- * C) Grupos como *Rhysida* operam exclusivamente por motivos financeiros, evitando alvos que possam ter significativas repercussões sociais ou políticas para minimizar a atenção das autoridades de aplicação da lei.
- * D) As campanhas de *ransomware*, como as conduzidas por grupos hackers incluindo *Rhysida*, são notáveis por evitar o uso de técnicas de engenharia social, preferindo explorar vulnerabilidades de software sem interação direta com as vítimas.

>>> Resposta Correta

Qual das seguintes afirmações abaixo é verdadeira?

- * A) Grupos hackers, incluindo Rhysida, empregam técnicas de phishing como seu principal meio de ganhar acesso a sistemas de informação, visando especificamente indivíduos através de e-mails falsos que parecem ser de fontes legítimas.
- * B) O *ransomware* é um tipo de *malware* que, uma vez instalado em um sistema de computador, criptografa arquivos do usuário e exige um pagamento em criptomoeda para a descriptografia, mas não permite aos hackers acesso aos sistemas afetados ou dados.
- * C) Grupos como *Rhysida* operam exclusivamente por motivos financeiros, evitando alvos que possam ter significativas repercussões sociais ou políticas para minimizar a atenção das autoridades de aplicação da lei.
- * D) As campanhas de *ransomware*, como as conduzidas por grupos hackers incluindo Rhysida, são notáveis por evitar o uso de técnicas de engenharia social, preferindo explorar vulnerabilidades de software sem interação direta com as vítimas.

>>> Referências

- [23] 9 top anti-phishing tools and services. <https://www.csoononline.com/article/569867/9-top-anti-phishing-tools-and-services.html>. Acessado em: 09-03-2024. 2023.
- [Car23] Nicole Carpenter. *Insomniac Games, Sony hack, Marvel Wolverine*. <https://www.polygon.com/23998399/insomniac-games-sony-hack-marvel-wolverine>. Acessado em: 09-03-2024. 2023.
- [CIS23] CISA. *Cybersecurity Advisory AA23-319A*. <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-319a>. Acessado em: 09-03-2024. 2023.
- [Fie23] Sarah Fielding. *Insomniac Games hackers leak 1.3 million files after demanding \$2 million ransom*. <https://www.engadget.com/insomniac-games-hackers-leak-13-million-files-after-demanding-2-million-ransom-102134429.html>. Acessado em: 09-03-2024. 2023.
- [Yin23] Wesley Yin-Poole. *Insomniac hackers release stolen data: Leak Wolverine videos, future projects, and more*. <https://www.ign.com/articles/insomniac-hackers-release-stolen-data-leak-wolverine-videos-future-projects-and-more>. Acessado em: 09-03-2024. 2023.