Ransomware *Royal*

Bruno Caike Durbem de Carvalho[1], **Carlos Alberto da Silva**

[1]Curso de Bacharelado em Sistema da Informação – Faculdade de Computação (FACOM)
Universidade Federal de Mato Grosso do Sul (UFMS).
Av. Costa e Silva, s/n. - Bairro Universitário - CEP 79070-900 - Campo Grande - MS.

{bruno.durbem, carlos.silva}@ufms.br

Abstract. *Considering the absurd rate of attacks on large and medium-sized companies, a current group of hackers has created ransomware capable of encrypting files, creating extensions with the group's name and extorting victims into not paying the ransom. In this article, I'll show you the processes that the group does with open source code, the encrypted files, and what measures we can take to defend ourselves against ransomware attacks.*

Resumo. *Considerando o índice absurdo de ataques em empresas de grande e médio porte, um grupo atual de hacker criou um ransomware capaz de criptografar os arquivos criar as extensões com o nome do grupo com o objetivo de extorquir as vítimas a pagarem um resgate para recuperar seus arquivos. Nesse artigo, mostraremos o modos operandos que o grupo faz com códigos abertos, como ficam os arquivos criptografados, e quais medidas podemos adotar para nos defender dos ataques do ransomware.*

1. Introdução

Um novo grupo de *ransomware* chamado *Royal*, iniciou suas atividades no final de 2022, intensificou significativamente suas operações e desenvolveu seu próprio programa de *ransomware* personalizado que permite aos invasores realizarem criptografia dos dispositivos de armazenamentos. O criptografa com algoritmo AES com os compartilhamentos de rede, encontrados na rede local, em servidores e entre outros dispositivos [Security 2023].

O grupo *Royal* utiliza ataques de *phishing* com arquivos PDF infectados para ganhar acesso rede, além de explorar vulnerabilidades em protocolos inseguros, como Remote Desktop Protocol (RDP), e as credenciais do protocolo da Rede Privada Virtual (VPN) também são utilizados como vetor inicial de ataque.

Além das redes tradicionais baseadas em sistemas Windows, *Royal Ransomware* também tem como alvos sistemas Linux e servidores ESXi.

Apesar de o *Royal* ser um grupo fechado e que não recruta afiliados em fóruns, alguns padrões vistos na análise forense sugerem que esse grupo tem compartilhado os dados e mostrado os detalhes específicos de suas atividades. A *Sophos* está rastreando e monitorando esses casos como um *cluster* de atividades de ameaça [**?**].

A Figura 1 apresenta as porcentagem de ataques de pelos países.

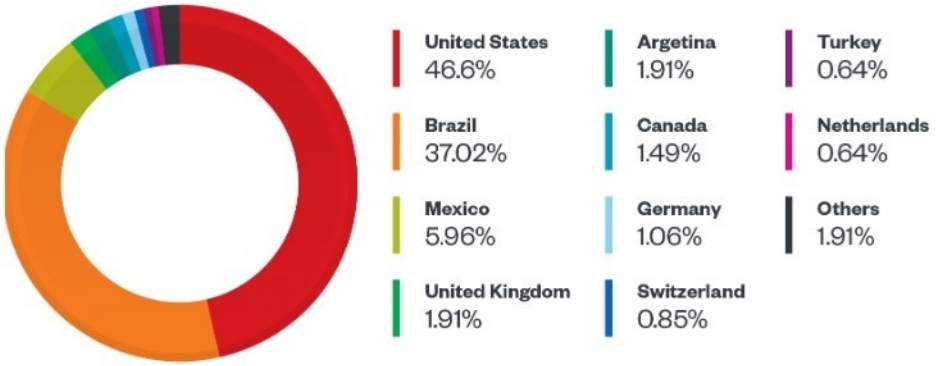

Figura 1. Percentagem de ataques por países [Chavez et al. 2022].

Esse grupo incluem o uso dos mesmos nomes de usuários e suas senhas específicas no momento em que os invasores assumem o controle dos sistemas dos alvos, entregando a carga útil final de um arquivo, como extensão do grupo .royal (com o nome da organização), e executando os comandos nos sistemas infectados com os mesmos lotes de *scripts* e arquivos [OXFORD 2023].

Em novembro de 2022,o *ransomware* acelerou as suas atividades maliciosas, assumindo a responsabilidade por um ataque no popular circuito de corridas do Reino Unido, *Silverstone*, que interrompeu dezenas de corridas da Formula 1 e eventos de motocicleta. No mês seguinte, *Royal* lançou um ataque à agência de avaliação de propriedades *Travis Central Appraisal*, paralisando seus servidores, site e e-mail pro mais de duas semanas [Davies 2023].

A Figura 2 mostra o *site* de *Silverstone*, modificado pelo *Royal* adicionando mais um dado ao circuito de corridas.

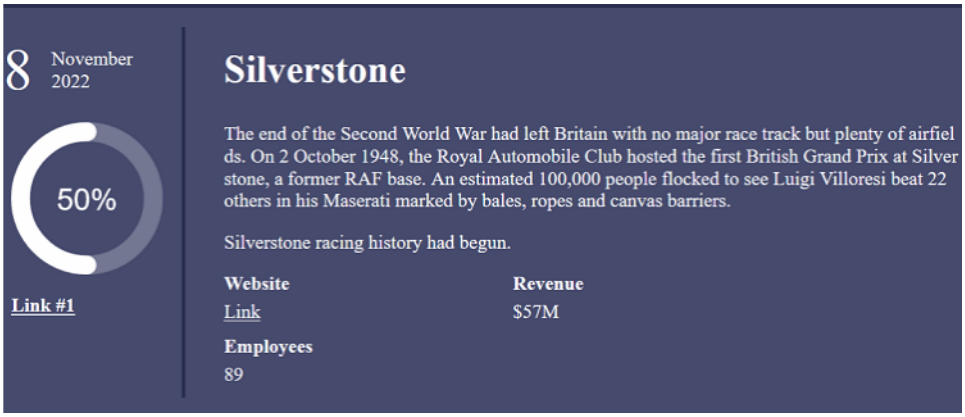

Figura 2. *site Silverstone* em 2022 [Petkauskas 2023]

2. *Ransomware Royal*

O *ransomware* é um dos programas maliciosos mais perigosos que prevalecem no mundo atual. Uma vez infectado, o malware encripta os dados ou bloqueia o sistemas de arquivos, e impede o usuário de acessar os dados e as aplicações até que seja pago o resgate. E mesmo pagando, não há garantia de que o usuário receberá a chave para desencriptar seu dispositivo e terá acesso aos dados.

A caracterização pode ser apresentada como:

- **Inicio da descoberta do *ransomware***: Novembro de 2022
- **Línguagem escrita do *Royal***: C++
- **Descoberta por**: Will Thomas do Equinix Threat Analysis Center (ETAC) Seus resgates variam de 250,000 a mais de 2 milhões para empresas. Em Bitcoin: chegando na casa de 1 milhão.
- **Primos**: BlackCat, ZEON e CONTI. [Meskauskas 2022]
- **Exemplos do Randomware**: T TEN, Adlg e Lol.
- **Invasão**: sistemas das empresas em cidades de Dallas, países como EUA, Reino Unido, Brasil, Europa e América Latina.

2.1. Análise Tatica do *Ransomware*

Ao executar um arquivo do tipo ".exe", o *Royal* recebe argumentos na linha de comando para cifrar os arquivos, e ocultar os dados que estão nos equipamentos dos usuários. O arquivo ".exe"tentará excluir *backups* de cópias usando o outro programa "Vssadmin.exe", com a linha de comando "delete shadows /all /quiet".

O perfil do comportamento, que identifica este *ransomware*, é a execução de três arquivos do tipo ".exe", e sendo um deles, o de exclusão das cópias dos *backups*.

Depois que os backups de arquivos forem excluídos, o *Royal* definirá uma sequência de cifrar (respectivamente), e depois apagar os arquivos originais com as extensões:

- LEIA-ME.TXT
- .DLL
- .EXE
- .png
- .pdf

A linha de criptografia do *Royal* usa o método de *multithread*, identificando o numero de thread que o processador consegue executar, e distribui os *scripts* de cifrar para cada *core de thread*, acelerando o processo de cifrar nesta máquina.

A Figura 3 mostra um exemplo de pasta que foi afetada pelo grupo *Royal*.

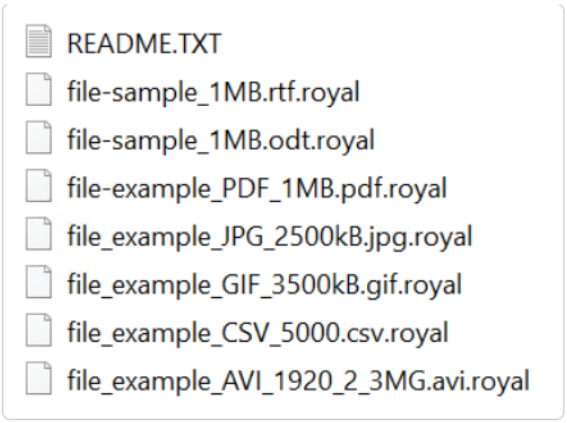

Figura 3. exemplo de sistemas de arquivos [Cybereason 2023].

O Algoritmo 1 apresenta o código para exclusão de cópias de arquivos de *backups* pelo *ransomware Royal*.

Algorithm 1 Algoritmo do *Royal* deletando os arquivos

```
wsprintfW (CommandLine, L"delete shadows  /all  /quiet");
StartupInfo.cb = 104;
memset (&StartupInfo.cb + 1, 0, 100);
memset (&ProcessInformation, 0, sizeof (ProcessInformation));
        If (CreateProcessW (
                L"C:Windows System32 vssadmin.exe",
                CommandLine,
                0i64,
                0i64,
                0,
                0,
                0i64,
                0i64,
                &StartupInfo,
                &ProcessInformation ))
```

2.2. Modo de READE.TXT

Feito o processo de cifrar todos os arquivos do dispositivo da vitima, será gerado um arquivo de texto chamado de "README.TXT", dentro desse arquivo, aparece a mensagem dizendo que os arquivos foram criptografados e mostra que as vitimas devem estabelecer contato com o grupo *Royal*, no site dedicado, e hospedado na rede TOR.

O site consiste principalmente em um serviço de bate-papo para conversar com o grupo. Os usuários tem que pagar para descriptografar seus arquivos.

3. Implementação de Auditoria e Políticas de Segurança

A norma do NIST 800-34r1 [Marianne Swanson et al. 2021] orienta as empresas a como desenvolverem seus mecanismos e ferramentas de defesa por meio de:

- Politicas de seguranças: que possam verificadas a cada 6 meses para testar sua eficacia;
- Plano de Continuidade de negócio (PCN): que permitiria a recuperação da atividades principais da empresas em curto período de tempo;
- Plano de Recuperação de Desastres (PRD): que tenham mecanismos para se recuperar de desastres naturais ou intencionais.
- Plano de Contingência: ativando equipes para tomada de decisão, e ativação dos planos PCN e PRD.
- Mecanismos para Monitoramento, Detecção, e Correção de incidentes de seguranças.

3.1. Ferramenta Antivírus

Existem vários softwares para remoção de *ransomware*, como por exemplo: *Combo Cleaner*, a ferramenta faz a primeira verificação no computador. Ele atualizará a sua base de dados de *malwares*, durante a verificação é mostrado o número de arquivos verificados e o tempo estimado para conclusão. Outro recurso do *Combo Cleaner* é o localizador de arquivos duplicados, exibe uma lista de arquivos duplicados, o usuário remove e recupera o espaço em disco [Motta 2023].

O *Cortex* que fornecem detecção do *ransomware*, interrompe as ameaças no *endpoint*, aplica a segurança na nuvem e evita os ataques cibernéticos. É a única plataforma de segurança baseada no IA.

É importante ressaltar que estas ferramentas de descriptografia do *ransomware* são cobradas taxas por este serviço.

3.2. Prevenção do ataque

Como prevenção, as seguintes ações são necessárias no ambiente computacional:

- Implementar uma política de execução de backup isolados e imutáveis, que descreva os procedimentos e testes de restauração enquanto antes. Deve prever locais fisicamente segmentados e seguros para armazenamento de mídias, além de incluir um plano de recuperação.
- Utilizar o conceito de segmentação de rede como ação de prevenção contra disseminação de *ransomware* e restrição de movimentos na rede(usar ferramentas para detecção de qualquer atividades maliciosas ou movimentação de arquivos pelo usuário).
- Reforçar campanhas de educação de usuários sobre ameaças recebidas por e-mail, de modo a identificar ataques de engenharia social e prevenir infecções por malware, a inserção de um banner aos e-mails externos e o bloqueio de anexos suspeitos.
- Ativar o Controle de Aplicativos para bloquear a execução de arquivos maliciosos.
- Com base nos resultados da pesquisa nos equipamentos ligados na empresa, isolar as máquinas infectadas fazendo uma ação de correção e excluir o arquivo principal.

- Desativar hiperlinks nas maquinas em e-mails secundários recebidos.
- Adotar autenticação de multifator (MFA) para todos os serviços críticos que disponibilizam este recurso. Exemplo: e-mail, redes virtuais privadas (VPN), sistemas da empresa e acessos a pasta de rede. [Gov 2023]

A Figura 4 mostra procedimento autenticação por dois fatores MFA, como mais uma barreira de seguranca no sistema da vitima.

Figura 4. fonte: elaborada pelo autor (2023).

3.3. Plano de Contingência

As infecções do tipo *ransomware* são projetadas para encriptar os sistemas de arquivos em dispositivos de armazenamento internos e externos, infectá-los e até mesmo distribuído por toda a rede local. Por este motivo, é importante isolar o dispositivo infectado. E se possível desativar a rede e desligar todos os dispositivos de armazenamento [Meskauskas 2022].

Identificar o tipo de ataque, e notificar as autoridades responsáveis pela empresa. Na sequencia fazer um relatório da infecção para a autoridade do *Computer Emergency Response TEAM* (CERT) ou a polícia local.

Recuperar dados usando o backup recente, podendo restaurá-los após verificação de todo os sistemas, e da remoção do *ransomware*, e garantir que o sistema esteja seguro.

Não é recomendados pagar o resgate do *ransomware*, pois não tem garantia de recuperação dos arquivos, e incentiva os criminosos a continuar realizando os ataques e prejudicar outros usuários [TechTudo 2023].

4. Trabalhos relacionados

As semelhanças exclusivas deste *ransomware Royal*, incluem o uso dos mesmos nomes de usuário e senhas específicas no momento em que os invasores assumem o controle dos

sistemas dos alvos, entregando a carga útil final de um arquivo. Dados compactados que foram incorporados com algoritmos com o nome da organização e executando comandos nos sistemas infectados com os mesmo lotes de *scripts* e arquivos [Advisor 2023].

Parecido com o *ransomware Royal*, o *LockBit* é um software malicioso projetado para bloquear o acesso do usuário aos sistemas de computador em troca do pagamento de um resgate. O *LockBit* funciona como um *ransomware-as-a-Service* (RaaS), compartilha comportamentos com as formas estabelecidas de *ransomware* direcionado [Kaspersky 2023]. Durante as invasões, os afiliados da LockBit foram observados usando várias ferramentas são usadas para uma série de atividades cibernéticas maliciosas, como reconhecimento de rede, acesso remoto, tunelamento, despejo de credenciais e vazamentos de arquivos. O uso do *PowerShell* e de *scripts* em lote é observado como artefatos de ferramentas profissionais de teste de penetração, como *Metasphoit* e *Cobalt Strike* [Agency 2023].

5. Conclusão e Trabalho futuros

A segurança da informação vive um grande desafio na atualidade. O surgimento de novas ameaças todos os dias, somado ao fato do interesse cada vez maior por esse mercado dos ataques, faz com que a descoberta de novas técnicas de reconhecimento e classificação de *ransomwares* e melhoria das atuais, sejam determinante.

O objetivo geral deste trabalho foi o de apresentar o ataque de *ransomware*, além de sugerir como um usuário pode se prevenir para garantir a segurança dos dados de seu dispositivos de armazenamento, e como se prevenir contra estes ataques. Concluise que os resultados deste trabalho foram satisfatórios, pois me permitiu adquirir mais conhecimentos e mecanismos de proteção.

Visando trabalhos futuros, sugiro a elaboração de uma ferramenta que descriptografa os arquivos dos usuários sem afetar o sistema operacional e a rede local. Introduzindo procedimentos e ideias que buscam os melhorar os resultados de detecção e recuperação, como menos custo computacional, realizando uma filtragem inicial, e na sequencia uma fase mais complexa para incrementar a técnica de análise de arquivos infectados.

Referências

Advisor, C. (2023). Descobertas conexões entre os grupos hive, royal e black basta. https://www.cisoadvisor.com.br/descobertas-conexoes-entre-os-grupos-hive-royal-e-black-basta/. [Acessado em 10 de outubro de 2023].

Agency, A. C. D. (2023). Compreendendo os atores de ameaças de ransomware: Lockbit. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-165a. [Acessado em 30 de novembro de 2023].

Chavez, I. N., Gelera, B., de Jesus, M., Ladores, D. O., and Morales, K. J. (2022). Conti team one splinter group resurfaces as royal ransomware with callback phishing attacks. https://www.trendmicro.com/pt_br/research/22/l/conti-team-one-splinter-group-resurfaces-as-royal-ransomware-wit.html. [Acessado em 25 de novembro de 2023].

Cybereason, S. G. (2023). Royal rumble: Análise do royal ransomware. https://www.cybereason.com/blog/royal-ransomware-analysis. [Acessado em 15 de novembro de 2023].

Davies, E. (2023). The royal blackcat ransomware: What you need to know. https://www.tripwire.com/state-of-security/royal-blackcat-ransomware-what-you-need-know. [Acessado em 28 de novembro de 2023].

Gov, E. C. (2023). Alerta 02/2023 royal ransomware. https://www.gov.br/ctir/pt-br/assuntos/alertas-e-recomendacoes/alertas/2023/alerta-02-2023. [Acessado em 02 de novembro de 2023].

Kaspersky (2023). Ransomware lockbit — o que você precisa saber. https://www.kaspersky.com.br/resource-center/threats/lockbit-ransomware. [Acessado em 28 de novembro de 2023].

Marianne Swanson, P. B. et al. (2021). Contingency planning guide for federal information systems, NIST 800-34r1. https://www.nist.gov/privacy-framework/nist-sp-800-34. [Acessado em 03 de dezembro de 2023].

Meskauskas, T. (2022). vírus ransomware royal (.royal) - opções de remoção e desencriptação. https://www.pcrisk.pt/guias-de-remocao/11718-royal-ransomware. [Acessado em 19 de junho de 2023].

Motta, S. (2023). Detecte malwares no pc com o combo cleaner. https://www.softdownload.com.br/detecte-malwares-pc-combo-cleaner.html. [Acessado em 29 de novembro de 2023].

OXFORD, U. (2023). Ataques recentes apontam que os três grupos estão compartilhando manuais dos crimes ou afiliados externos. https://www.sophos.com/pt-br/press/press-releases/2023/08/sophos-uncovers-new-connections-between-hive-royal-and-black-basta. [Acessado em 25 de outubro de 2023].

Petkauskas, V. (2023). Silverstone formula one circuit posted on ransomware leak site. https://cybernews.com/news/silverstone-formula-one-ransomware/. [Acessado em 10 de novembro de 2023].

Security, B. C. (2023). Relatório de ransomware: lockbit em modo de ataque. https://b2b-cyber-security.de/pt/ransomware-report-lockbit-im-angriffsmodus/. [Acessado em 20 de novembro de 2023].

TechTudo (2023). O que é ransomware? entenda como funciona e como remover o malware. https://www.techtudo.com.br/guia/2023/05/o-que-e-ransomware-entenda-como-funciona-e-como-remover-o-malware-edghtml. [Acessado em 30 de novembro de 2023].