BOLETIM DE SEGURANÇA

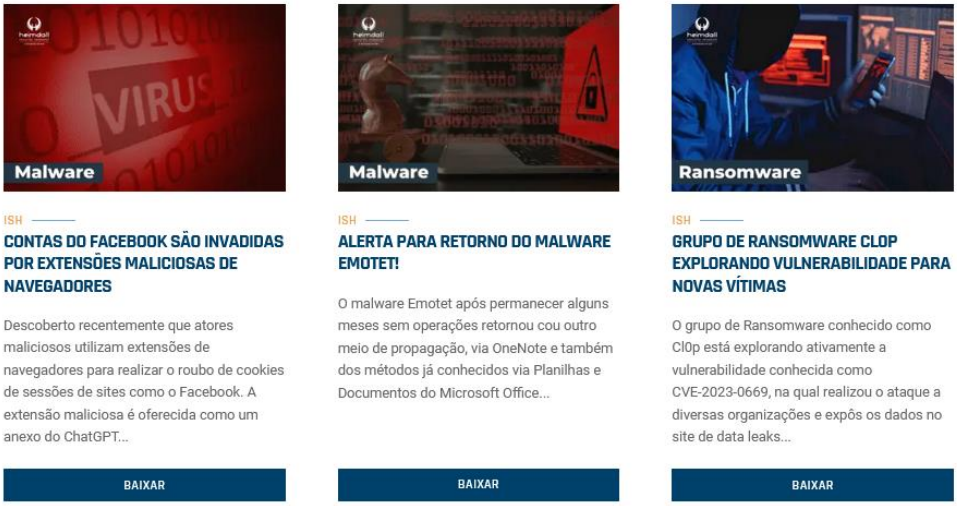
Gangues de ransomware exploram ferramentas do microsoft Azure para exfiltração de dados

heimdall
security research
A DIVISION OF ISH

TLP: CLEAR

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 FIGURAS

1 SUMÁRIO EXECUTIVO

Gangues de ransomware, como BianLian e Rhysida, estão cada vez mais utilizando o Azure Storage Explorer e o AzCopy da Microsoft para exfiltrar dados de redes comprometidas, armazenando-os no Azure Blob Storage. Essa tendência representa uma evolução nas táticas de exfiltração de dados, aumentando a complexidade e os desafios na resposta a incidentes de segurança.

2 DETALHES SOBRE A AMEAÇA

Novas tendências continuam a emergir e transformar o cenário de ameaças. Uma das mudanças mais significativas é o aumento da exfiltração de dados durante ataques de ransomware. Inicialmente, a exfiltração de dados por agentes de ransomware era uma exceção rara, mas hoje se tornou uma tática comum, proporcionando aos criminosos uma vantagem adicional nas negociações, foi observado que agentes de ameaças estão utilizando ferramentas como MEGAsync e Rclone para copiar e sincronizar arquivos remotamente em larga escala, especificamente para exfiltração de dados. Em análises, os investigadores rastrearam os movimentos desses agentes enquanto navegavam por diretórios e compartilhamentos de arquivos em busca de dados confidenciais. Apesar de exfiltrarem grandes volumes de dados, os agentes de ameaças ainda precisam garantir que esses dados contenham informações valiosas e sensíveis.

Dito isto, notou-se recentemente o uso de uma nova ferramenta para exfiltração de dados: o Azure Storage Explorer. A utilização dessa ferramenta na versão AMD64 do Windows OS foi predominantemente observada no grupo de ransomware BianLian, mas também inclui o grupo Rhysida. Este aplicativo da Microsoft, disponível para dispositivos com Windows ARM, Linux e MAC OSX, oferece uma interface gráfica para gerenciar diversos tipos e componentes de armazenamento do Azure, além de permitir o upload e download de pastas e arquivos. As transferências de arquivos envolvendo blobs de armazenamento, compartilhamentos de arquivos, ADLS Gen2 e discos gerenciados são realizadas pela ferramenta de linha de comando AzCopy, especializada em transferência de dados de armazenamento do Azure. Em um dos incidentes mais significativos envolvendo o Azure Storage Explorer, o grupo BianLian utilizou a ferramenta para copiar centenas de arquivos do servidor de arquivos principal de uma empresa.

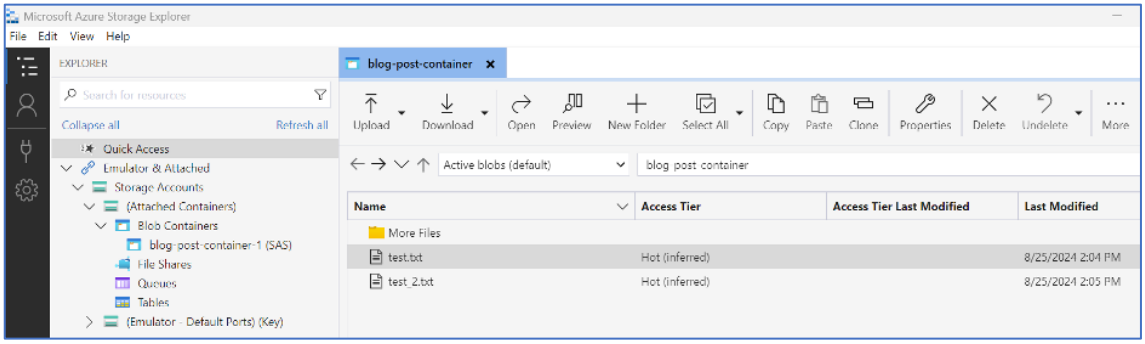


Figura 1 – Explorador de Armazenamento do Microsoft Azure.

Um fator que torna o uso dessa ferramenta para exfiltração de dados especialmente notável é a abordagem proativa dos agentes de ameaça. Em vez de simplesmente utilizar um executável autônomo, eles optaram por instalar o programa no sistema, chegando ao ponto de atualizar a versão do .NET para a versão 8 antes de instalar o Azure Storage Explorer. Durante o processo de instalação, os agentes podem escolher entre instalá-lo apenas para a conta de usuário atual ou para todos os usuários do sistema. O executável principal, StorageExplorer.exe, e os arquivos de programa adicionais são colocados nos

diretórios correspondentes, a menos que o local padrão seja alterado manualmente.

- *%USERPROFILE%\ AppData\Local\Programs\Microsoft Azure Storage Explorer*
- *C:\Program Files\Microsoft Azure Storage Explorer*

O executável AzCopy, quando instalada a versão AMD de 64 bits, está localizado em um subdiretório específico. Quando agentes de ameaça utilizam o Azure Storage Explorer para exfiltração de dados, é comum que eles recorram a essa ferramenta, como observado em várias ocasiões ao carregar arquivos para um contêiner de blob. Essa estratégia é preferida porque o Azure Blob Storage é projetado para gerenciar grandes volumes de dados não estruturados, oferecendo alta escalabilidade. Além disso, é pouco provável que uma conexão de saída para um endereço IP da Microsoft, que hospeda uma conta de armazenamento do Azure, seja bloqueada pelos controles de segurança de rede.

- *app\node_modules\@azure-tools\azcopy win64\dist\bin\azcopy_windows_amd64.exe*

No Azure Blob Storage, seus dados, conhecidos como objetos, são armazenados como “blobs” dentro de contêineres. Esses contêineres são comparáveis aos buckets do Amazon S3 e do Google Cloud Storage, caso você esteja mais familiarizado com esses serviços.

A estrutura do Azure Blob Storage, que é composta por três elementos principais:

1. **Conta de armazenamento**: a entidade principal que fornece um namespace para seus dados.
2. **Contêiner**: um agrupamento lógico dentro da conta de armazenamento que abriga seus blobs.
3. **Blob**: o objeto de dados propriamente dito, armazenado dentro de um contêiner.

Essa estrutura facilita a organização e o gerenciamento dos dados na nuvem, oferecendo uma solução flexível e escalável para armazenamento.

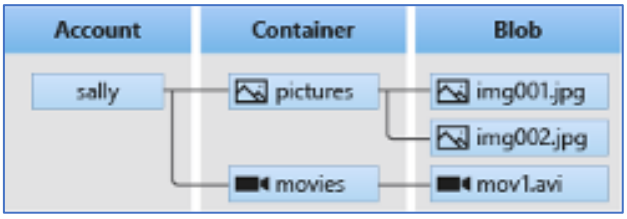


Figura 2 – Microsoft - Introdução ao AzureBlob Storage.

O Azure Storage Explorer e as instâncias do AzCopy que ele executa utilizam, por padrão, a configuração de log no nível INFO. Cada uma dessas ferramentas possui uma seção específica na página de configurações do Azure Storage Explorer, onde o usuário pode ajustar o nível de log conforme necessário. Em ambos os casos observados de exfiltração de dados, o nível de log padrão INFO permaneceu inalterado.

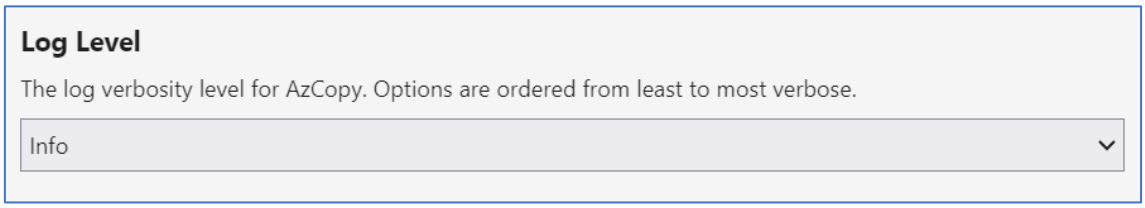


Figura 3 – Configuração de nível de log para AzCopy no Azure Storage Explorer.

O Azure Storage Explorer facilita a obtenção do comando AzCopy para transferências de arquivos, oferecendo um link que permite copiar o comando diretamente para a área de transferência. Se ocorrerem falhas nas atividades de transferência de arquivos, o Azure Storage Explorer disponibiliza um link "Repetir..." para tentar novamente o mesmo comando do AzCopy. Além disso, para investigações de resposta a incidentes, há uma opção "Ir para o arquivo de log do AzCopy", que pode ser bastante útil.

Ao clicar em "Ir para o arquivo de log do AzCopy", a pasta .azcopy correspondente é aberta no Windows Explorer.

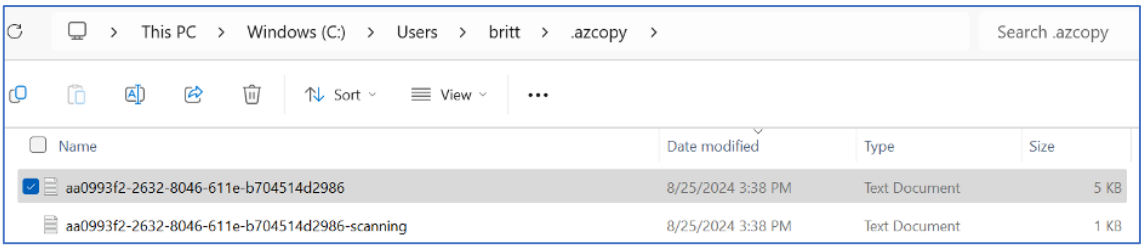


Figura 4 – Conteúdo do log da pasta .azcopy.

Ao iniciar um novo trabalho do AzCopy pelo Azure Storage Explorer, dois tipos de logs são gerados neste diretório. Para investigadores forenses e respondentes de incidentes, o log regular — sem o sufixo "-scanning" — é o mais útil. Ele contém informações como o comando AzCopy gerado e detalhes de atividades de arquivos, incluindo uploads, downloads e cópias em contêineres de armazenamento. O exemplo de log do comando AzCopy abaixo foi gerado com as configurações padrão do Azure Storage Explorer.

Esses logs registram os resultados das operações para todos os arquivos envolvidos no trabalho do AzCopy. Para identificar possíveis exfiltrações de dados, os eventos principais a serem observados são UPLOADSUCCESSFUL e UPLOADFAILED, que aparecem após o evento "Starting transfer" para um arquivo.

Por exemplo, se um agente de ameaça usar o Azure Storage Explorer ou o AzCopy para importar ferramentas ou programas maliciosos, os eventos DOWNLOADSUCCESSFUL e DOWNLOADFAILED mostrariam detalhes sobre os arquivos trazidos do Azure para a rede. Outro cenário possível, especialmente com a crescente adoção de serviços de nuvem, envolve o Azure Storage Explorer já instalado em um sistema. Isso pode permitir que um agente de ameaça copie dados para uma conta de armazenamento que ele controla. Nesses casos, os eventos COPYSUCCESSFUL e COPYFAILED são cruciais.

Importante notar que a configuração “Logout On Exit” no Azure Storage Explorer não é ativada por padrão, mantendo todas as sessões válidas do Azure Storage ao reabrir o aplicativo.

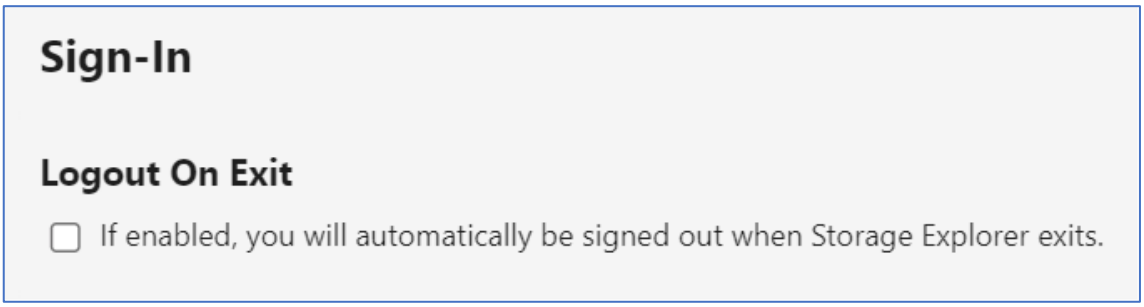


Figura 5 – Configuração padrão para Logout na saída.

No término do arquivo de log do AzCopy, há um resumo crucial e informativo que pode ser utilizado para examinar a exfiltração de dados e outros possíveis usos do Azure Storage Explorer por agentes maliciosos.

```
2024/08/25 20:17:27 JobID=91629f80-e740-c04c-6af2-41ef18edd14d, Part#=0,
TransfersDone=170 of 170
2024/08/25 20:17:27 all parts of entire Job 91629f80-e740-c04c-6af2-
41ef18edd14d successfully completed, cancelled or paused
2024/08/25 20:17:27 is part of Job which 1 total number of parts done
2024/08/25 20:17:29 100.0 %, 170 Done, 0 Failed, 0 Pending, 0 Skipped, 170
Total, 2-sec Throughput (Mb/s): 0.4784
2024/08/25 20:17:29 Closing Log
```

Figura 6 – Resumo final do exemplo de entrada do log de atividades do trabalho do AzCopy.

3 RECOMENDAÇÕES

São elencadas abaixo pela ISH, medidas que poderão ser adotadas visando a mitigação da referida *ameaça*, como por exemplo:

Autenticação Multifator (MFA)

- Habilite a autenticação multifator para todas as contas de usuário. Isso adiciona uma camada extra de segurança, dificultando o acesso não autorizado.

Backup regular

- Realize backups regulares e armazene-os em locais separados e seguros. Isso garante que você possa restaurar seus dados sem pagar o resgate.

Atualizações e patches

- Mantenha todos os sistemas e softwares atualizados com os patches de segurança mais recentes. Isso ajuda a corrigir vulnerabilidades que podem ser exploradas por ransomware.

Monitoramento contínuo

- Utilize ferramentas para monitorar continuamente suas cargas de trabalho e detectar atividades suspeitas.

Segmentação de rede

- Implemente a segmentação de rede para limitar a propagação de ransomware. Isso envolve dividir a rede em segmentos menores e controlar o tráfego entre eles.

Educação e treinamento

- Treine seus funcionários sobre as melhores práticas de segurança cibernética e como identificar e evitar ataques de phishing, que são uma porta de entrada comum para ransomware.

Plano de resposta a incidentes

- Desenvolva e teste regularmente um plano de resposta a incidentes. Isso inclui procedimentos claros para isolar sistemas infectados e restaurar operações rapidamente.

4 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Modepush**
- **Bleepingcomputer**

5 AUTORES

- **Leonardo Oliveira Silva**

heimdall
security research
A DIVISION OF ISH