heimdall

security research

A DIVISION OF ISH

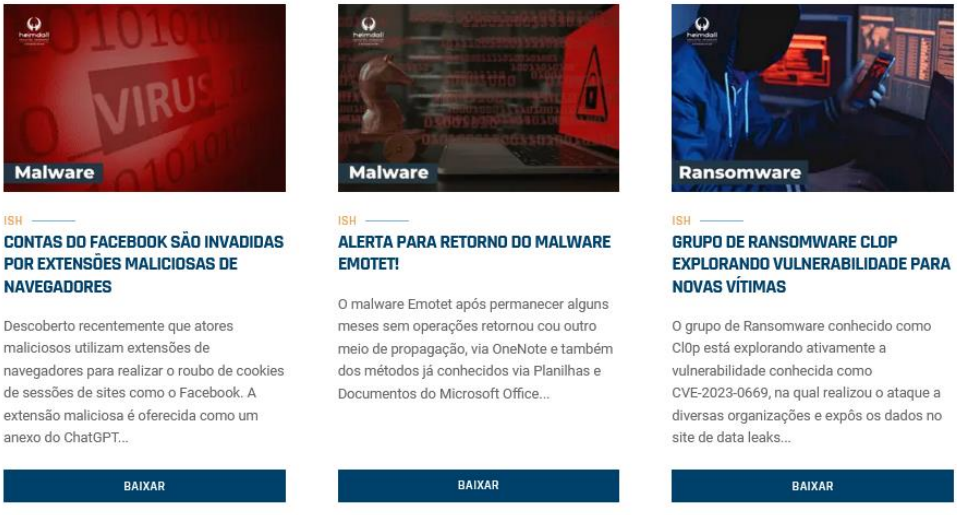
Ransomware SaaS em operação – 0mega

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 Figuras

1 RANSOMWARE SAAS

Um método de realizar a extorsão dos dados está novamente em operação, conhecido como SaaS Ransomware, que nada mais é a operação de ransomwares em locais que se encontram armazenados arquivos de forma remota, como por exemplo a utilização de armazenamentos no Sharepoint da Microsoft 365.

Em posse das informações de que muitas organizações se encontram armazenando seus dados nestes repositórios SaaS, os atores maliciosos visam realizar o sequestro destes dados, realizando a exfiltração e exclusão de demais contas administrativas, para que a organização realize o contato posteriormente para realizar o pagamento e os dados exfiltrados sejam excluídos.

A operação de ransomwares desta forma é diferente das demais, onde é realizado a criptografia dos dados em máquinas locais que se encontra sincronizada com o Sharepoint.

O relatório deste tipo de ataque foi publicado pela equipe de cybersegurança da Obsidian, compartilhando detalhes sobre o ataque a uma organização.

2 DETALHES DO ATAQUE

A princípio, os atores maliciosos realizaram o comprometimento de uma conta de serviço de administração global da Microsoft que era utilizada pela organização e, não possua autenticação de duplo fator (MFA) habilitado, podendo ser realizado a conexão por qualquer local.

Realizaram o acesso através de um host VPS fornecido pelo serviço "VDSinra.ru" o qual oferece servidores em Cloud (VPS/VDS) e se encontra disponibilizado na Rússia. A localização do IP utilizado pelos ataques foi diferente dos acessos que a empresa utilizada.

Na sequência do acesso, a conta de serviço realizou a criação de um **novo usuário no AD**, chamado "0mega", com o **UserPrincipalName**: 0mega@<site da empresa>.com, com o **Departamet**: "Contate-nos https://0mega-connect[.]biz/c/<redacted_guid>" e StreetAddress: contendo um site na rede .Onion.

Essa conta de serviço concedeu a 0mega permissões elevadas, incluindo **"Global Administrator, SharepOint Administrator, Exchange Administrator e Teams Administrator"**, bem como concedeu recursos de administrador do conjunto de sites e vários outros sites e conjuntos do Sharepoint, além de realizar a **remoção de outros administradores existentes no AD em um período de 2 horas**.

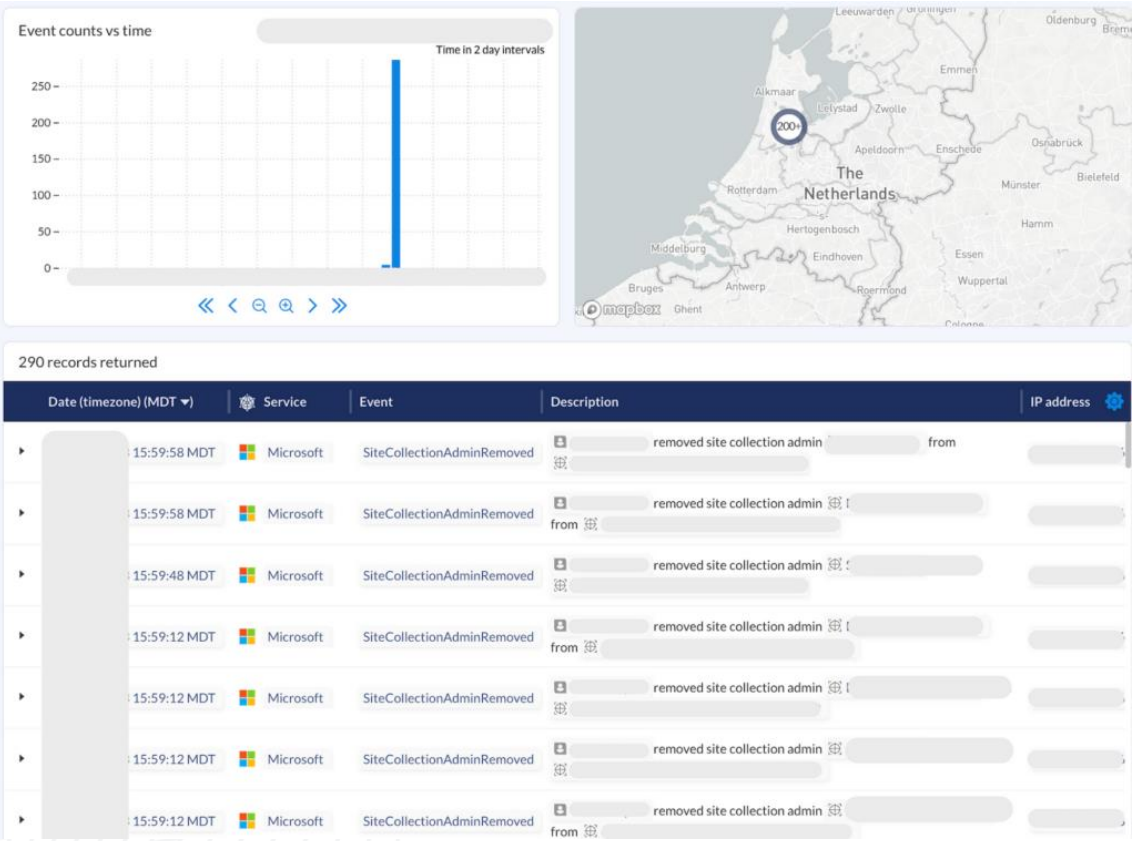


Figura 1 – Local de conexão e remoção de outros usuários Administradores.

Os arquivos que se encontravam armazenados no Sharepoint da organização foram exfiltrados pelo terminal VPS aproveitando o **"sppull"**, um módulo Node.js que simplifica o download de arquivos do SharePoint.

Além disso, os atores maliciosos carregaram arquivos com o nome "**PREVENT-LEAKAGE.txt**" para chamar a atenção para a exfiltração de dados. A atividade foi automatizada utilizando o **"got"**, outra biblioteca Node.js disponível para simplificar as solicitações HTTP.

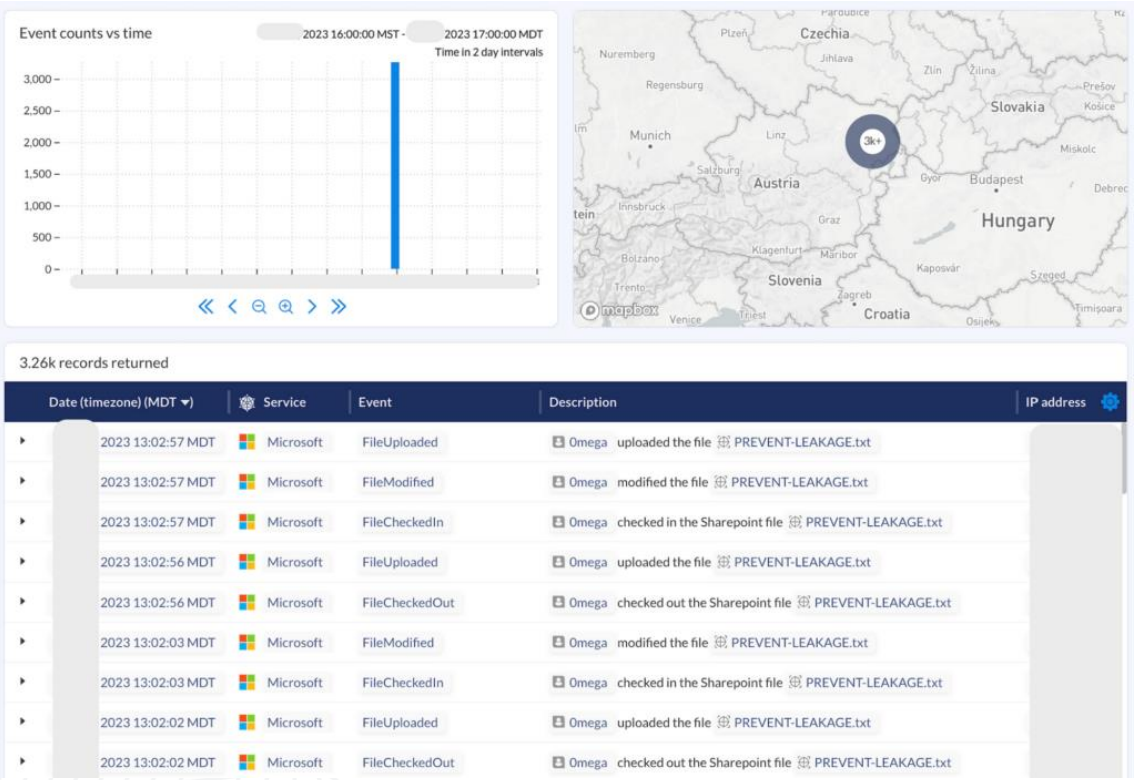


Figura 2 – Upload do arquivo Prevent-Leakage.txt.

Os sites apresentados pelos atores permitiram que a empresa violada conversasse com os operadores do ransomwares e negociassem o pagamento, visando sempre no sentido de evitar que os dados sejam publicados online.

Tal operação, foi observada sendo praticada por atores maliciosos conhecidos como Omega, cuja operação se deu no mês de julho de 2022m havendo também a disposição de um site na rede Onion para publicação de suas vítimas, estando ativo até a presente data com a última publicação de uma vítima em fevereiro.

Figura 3 – Site de dataleak do 0mega Ransomware.

3 DICAS DE DETECÇÃO

Para que haja a identificação destes ataques, é de extrema importância que os logs de auditoria do Office365 estejam habilitados, bem como algumas características podem ser identificadas:

- **Contas de serviços:**
  - Alerta de logins com geolocalização de IP diferente.
  - Alertas de logins que podem afirmar que a conta teve acesso de dois países diferentes.
  - Alerta de qualquer comportamento que não esteja nos padrões da organização.
- **Novos usuários do AD:**
  - Alertas sobre a criação de novos usuários no AD com os recursos:
    - *UserPrincipalName: 0mega@<dominio>.com*
    - *MailNickname: 0mega*
    - *DisplayName: 0mega ou Zero Mega*
    - *Departament: Contact us <site 0mega>*
    - *StreetAddress: <Site na rede .Onion>*
  - Além de alerta para criação de outros usuários criados no AD que receberam privilégios.
- **Novos grupos no AD:**
  - Alerta sobre qualquer novo grupo no AD chamado "_0mega_prevent_leakage".
- **Arquivos do SharePoint:**
  - Alerta sobre qualquer arquivo chamado "PREVENT-LEAKAGE.txt"
  - Alerta sobre uploads de arquivos de alto volume ou operações de check-in com extensão .txt.
- **Agentes de usuários**
  - Alerta para qualquer atividade do Microsoft 365 de um agente de usuário "sppull ou got".

4 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Publicação Obsidian operação Omega Ransomware RaaS**
- **Publicação Omega Ransomware – Bleeping Computer**

heimdall
security research

A DIVISION OF ISH