# BOLETIM DE SEGURANÇA

## Microsoft alerta para novo Ransomware INC com alvo o setor de saúde dos EUA

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


ISH

**CONTAS DO FACEBOOK SÃO INVADIDAS POR EXTENSÕES MALICIOSAS DE NAVEGADORES**

Descoberto recentemente que atores maliciosos utilizam extensões de navegadores para realizar o roubo de cookies de sessões de sites como o Facebook. A extensão maliciosa é oferecida como um anexo do ChatGPT...

BAIXAR


ISH

**ALERTA PARA RETORNO DO MALWARE EMOTET!**

O malware Emotet após permanecer alguns meses sem operações retornou cou outro meio de propagação, via OneNote e também dos métodos já conhecidos via Planilhas e Documentos do Microsoft Office...

BAIXAR


ISH

**GRUPO DE RANSOMWARE CLOP EXPLORANDO VULNERABILIDADE PARA NOVAS VÍTIMAS**

O grupo de Ransomware conhecido como Cl0p está explorando ativamente a vulnerabilidade conhecida como CVE-2023-0669, na qual realizou o ataque a diversas organizações e expôs os dados no site de data leaks...

BAIXAR

## SUMÁRIO

# LISTA DE TABELAS

# 1 SUMÁRIO EXECUTIVO

A Microsoft identificou uma nova ameaça de ransomware chamada **INC**, direcionada especificamente ao setor de saúde dos Estados Unidos. A declara Microsoft que está monitorando as atividades deste agente de ameaça, o qual tem motivação financeira.

## 2 INFORMAÇÕES SOBRE A AMEAÇA

Este ransomware representa uma ameaça significativa, destacando a necessidade de fortalecer as defesas cibernéticas no setor de saúde para proteger dados sensíveis e garantir a continuidade dos serviços. A cadeia de ataques ocorre da seguinte maneira, o Vanilla Tempest utiliza o GootLoader através Storm-0494 do agente de ameaças, que depois implanta ferramentas como o backdoor Supper, AnyDesk (uma ferramenta legítima de monitoramento remoto) e MEGA (uma ferramenta de sincronização de dados). Na fase seguinte, os atacantes realizam movimentos laterais usando o Protocolo de Área de Trabalho Remota (RDP) e, em seguida, utilizam o Host do Provedor do Windows Management Instrumentation (WMI) para distribuir o ransomware INC.

A Microsoft informou que o Vanilla Tempest está ativo desde pelo menos julho de 2022. Ataques anteriores foram direcionados aos setores de educação, saúde, TI e manufatura, utilizando várias famílias de ransomware, incluindo BlackCat, Quantum Locker, Zeppelin e Rhysida. O agente de ameaças também é conhecido como Vice Society, famoso por usar ransomware já existente para realizar seus ataques. Recentemente, grupos de ransomware como BianLian e Rhysida têm sido observados utilizando o Azure Storage Explorer e o AzCopy para extrair dados sensíveis de redes comprometidas, tentando evitar a detecção. Essas ferramentas, usadas para gerenciar o armazenamento do Azure, estão sendo reaproveitadas para transferências de dados em grande escala para armazenamento em nuvem.

O grupo utiliza uma combinação de técnicas avançadas, como spear-phishing para acesso inicial, exploração de vulnerabilidades conhecidas e o uso de softwares comerciais prontos (COTS) e ferramentas legítimas de sistema (LOLBINs) para reconhecimento e movimentação lateral na rede. Essa abordagem demonstra sua habilidade técnica e capacidade de evitar detecção, tornando a prevenção mais difícil. Os ataques do INC. Ransomware não se limitam à criptografia e bloqueio de dados; eles também envolvem roubo de dados e ameaças de divulgação pública, uma tática conhecida como dupla extorsão. Isso aumenta a pressão sobre as vítimas para pagar o resgate, ameaçando tanto a acessibilidade quanto a confidencialidade dos dados.

O INC. Ransom adota uma abordagem sofisticada e em várias etapas para comprometer sistemas. Eles combinam spear-phishing ou exploração de vulnerabilidades com etapas calculadas para estabelecer controle e executar o ransomware. Aqui está um resumo do processo de ataque:

**Acesso inicial e reconhecimento**

- O grupo começa com spear-phishing ou mirando serviços vulneráveis. Uma vez dentro, usam ferramentas como NETSCAN.EXE para varredura de rede, MEGAsyncSetup64.EXE para compartilhamento de arquivos, ESENTUTL.EXE para gerenciamento de banco de dados e AnyDesk.exe para controle remoto.

**Exploração do RDP**

- Usam credenciais comprometidas para acessar sistemas via RDP, realizando atividades de enumeração, como escanear administradores de domínio e testar conexões de rede, buscando pontos vulneráveis.

**Coleta e preparação de dados**

- Abusam de software legítimo para coletar e preparar dados para exfiltração, usando comandos de arquivamento 7-Zip e ferramentas nativas como Wordpad, Notepad e MSPaint. Instalam MEGASync em servidores para facilitar a transferência de dados roubados.

**Movimento lateral e acesso a credenciais**

- Movem-se lateralmente pela rede, acessando vários servidores e usando ferramentas como Advanced IP Scanner e Internet Explorer para explorar a rede. Executam comandos de acesso a credenciais, usando ferramentas como lsassy.py para extrair credenciais de login.

**Criptografia e implantação de arquivos**

- No estágio final, implantam o ransomware usando wmic.exe e PSExec (disfarçado como winupd) para iniciar o executável de criptografia em vários endpoints, automatizando o processo com arquivos em lote ou scripts.

**Solução de problemas e adaptação**

- Quando encontram dificuldades, como a incapacidade de executar o ransomware em certos servidores, tentam várias vezes com comandos de depuração, mostrando sua adaptabilidade e persistência.

# 3 MITRE ATT&CK - TTPs

| Tática | Técnica | Detalhes |
|---|---|---|
| **Initial Access** | T1566<br>T1190 | Consiste em técnicas que usam vários vetores de entrada para ganhar sua posição inicial dentro de uma rede. |
| **Execution** | T1059 | Consiste em técnicas que resultam em código controlado pelo adversário em execução em um sistema local ou remoto. |
| **Persistence** | T1078 | Consiste em técnicas que os adversários usam para manter o acesso aos sistemas em reinicializações, credenciais alteradas e outras interrupções que podem cortar seu acesso. |
| **Privilege Escalation** | T1068 | Consiste em técnicas que os adversários usam para obter permissões de nível mais alto em um sistema ou rede. |
| **Defense Evasion** | T1027 | Consiste em técnicas que os adversários usam para evitar a detecção durante seu comprometimento. |
| **Credential Access** | T1003 | Consiste em técnicas para roubar credenciais como nomes de contas e senhas. Técnicas usadas para obter credenciais incluem keylogging ou credential dumping. |
| **Discovery** | T1016 | Consiste em técnicas que um adversário pode usar para obter conhecimento sobre o sistema e a rede interna. |
| **Lateral Movement** | T1021.001 | Consiste em técnicas que os adversários usam para entrar e controlar sistemas remotos em uma rede. |
| **Collection** | T1074 | Consiste em técnicas que os adversários podem usar para reunir informações e as fontes de onde as informações são coletadas que são relevantes para seguir os objetivos do adversário. |
| **Exfiltration** | T1486 | Consiste em técnicas que adversários podem usar para roubar dados da sua rede. Depois de coletar dados, os adversários geralmente os empacotam para evitar a detecção ao removê-los. |
| **Command and Control** | T1105 | Consiste em técnicas que adversários podem usar para se comunicar com sistemas sob seu controle dentro de uma rede de vítima. |
| **Impact** | T1485 | Consiste em técnicas que os adversários usam para interromper a disponibilidade ou comprometer a integridade ao manipular processos comerciais e operacionais. |

Tabela 1 – Tabela MITRE ATT&CK.

# 4 RECOMENDAÇÕES

Para se defender contra as táticas sofisticadas do INC. Ransom, as organizações precisam adotar uma abordagem de segurança multicamadas. Aqui estão algumas recomendações importantes para aprimorar as defesas de segurança cibernética contra essas ameaças de ransomware:

**Atualize e aplique patches regularmente nos sistemas**

- Garanta que todos os softwares, especialmente aplicativos críticos e amplamente usados, sejam atualizados e corrigidos regularmente. Isso ajuda a fechar vulnerabilidades que podem ser exploradas por grupos de ransomware.

**Segurança de e-mail**

- Como spear-phishing é um vetor de acesso inicial comum, implemente soluções avançadas de segurança de e-mail. Elas devem incluir detecção de phishing, sandboxing para anexos de e-mail e treinamento de usuários para reconhecer e relatar e-mails suspeitos.

**Proteção de endpoint**

- Implante plataformas avançadas de proteção de endpoint (EPP) que podem detectar, prevenir e responder a ameaças usando técnicas como análise comportamental e aprendizado de máquina.

**Segmentação e monitoramento de rede**

- Segmente sua rede para limitar o movimento lateral de invasores. Use sistemas de detecção de intrusão (IDS) e sistemas de prevenção de intrusão (IPS) para monitorar o tráfego de rede em busca de atividades suspeitas.

**Implemente a autenticação multifator (MFA)**

- Adiciona uma camada extra de segurança para acessar sistemas e dados confidenciais, dificultando o acesso de invasores, mesmo que tenham credenciais comprometidas.

**Backups regulares e criptografia de dados**

- Faça backups regulares de dados críticos e garanta que eles sejam armazenados com segurança, de preferência fora do local ou na nuvem. Criptografe dados confidenciais para adicionar uma camada adicional de proteção.

# 5 REFERÊNCIAS


- **Heimdall *by* ISH Tecnologia**
- Thehackernews
- Bleepingcomputer
- SocRadar

# 6 AUTORES

- **Leonardo Oliveira Silva**

heimdall
security research
A DIVISION OF ISH