BOLETIM DE SEGURANÇA

Ransomware Cicada3301, nova ameaça em Rust mirando Sistemas Windows e Linux

heimdall
security research
A DIVISION OF ISH

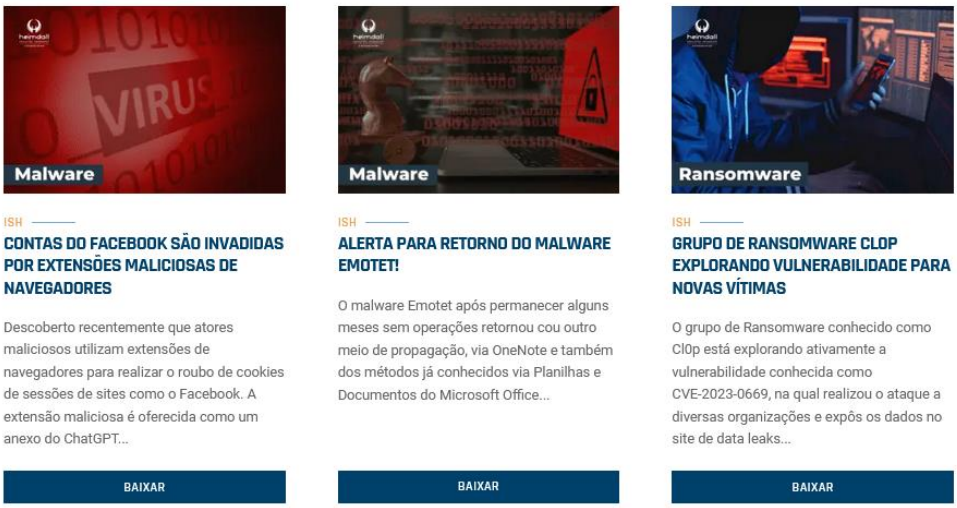
TLP: CLEAR

Receba alertas e informações sobre segurança cibernética e ameaças rapidamente, por meio do nosso **X**.

[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 TABELAS

LISTA DE FIGURAS

1 SUMÁRIO EXECUTIVO

Pesquisadores em segurança cibernética desvendaram detalhes de uma nova variante de ransomware chamada **Cicada3301**. Este malware emergente compartilha características com a operação BlackCat (também conhecida como ALPHV), agora inativa. O Cicada3301 se destaca por ser escrito em Rust e tem como alvo sistemas **Windows** e **Linux,** representando uma nova e séria ameaça para organizações de diferentes portes.

2 INFORMAÇÕES SOBRE A AMEAÇA

Em um cenário de ameaças cibernéticas que evoluem rapidamente, surgiu um novo adversário que se inspira no intrigante Cicada3301, um dos quebra-cabeças mais misteriosos da internet. Nomeado ransomware Cicada3301, ele foi recentemente identificado, após conseguir contornar uma solução de segurança de ponta, especificamente um sistema de detecção e resposta (EDR).

Lançado a pouco tempo, o Cicada3301, escrito na linguagem Rust, até o momento, os pesquisadores acreditam que o Cicada3301 visa principalmente pequenas e médias empresas, explorando vulnerabilidades em ataques oportunistas para obter acesso inicial aos sistemas.

Figura 1 – Tela do fórum do Cicada3301.

Foram identificadas mais de 20 vítimas, principalmente situadas na América do Norte e na Inglaterra. As organizações afetadas variam em tamanho, abrangendo desde pequenas, empresas de médio porte até grandes corporações. Os setores atingidos incluem manufatura/industrial, saúde, varejo e hospitalidade.

Figura 2 – Nota de resgate do malware.

O ransomware Cicada3301 possui várias características em comum com o famoso ransomware BlackCat, que também é desenvolvido em Rust.

Ele conta com uma interface de configuração de parâmetros bem estruturada, registra um manipulador de exceções de vetor e utiliza métodos semelhantes para a exclusão e adulteração de cópias de sombra. A utilização de Rust no desenvolvimento de ransomware está em ascensão, com outros exemplos notáveis como Hive e RansomExx, devido à eficiência e aos recursos multiplataforma que Rust oferece. Entretanto, o Cicada3301 se diferencia por suas inovações significativas, especialmente na maneira como executa e integra credenciais comprometidas, representando uma evolução nas táticas de ransomware.

3 RECOMENDAÇÕES

Além dos indicadores de comprometimento elencados abaixo pela ISH, poderão ser adotadas medidas visando a mitigação da infecção do referido *malware*, como por exemplo:

Mantenha o software atualizado

- Certifique-se de que todos os sistemas e aplicativos estejam sempre atualizados com os patches de segurança mais recentes.

Use autenticação de dois fatores (2FA)

- Implementar 2FA adiciona uma camada extra de segurança, dificultando o acesso não autorizado.

Realize backups regulares

- Faça backups frequentes de seus dados e armazene-os em locais seguros, preferencialmente offline.

Segmente a rede

- Divida a rede em segmentos menores para limitar a propagação do ransomware caso ocorra uma infecção.

Treine os funcionários

- Eduque os funcionários sobre como reconhecer e evitar ameaças de ransomware, como e-mails de phishing.

Implemente segurança de endpoints

- Utilize soluções de segurança robustas para monitorar e proteger todos os dispositivos conectados à rede.

Adote um modelo de Zero Trust

- Este modelo assume que nenhuma entidade, interna ou externa, é confiável por padrão, exigindo verificações contínuas de segurança.

4 INDICADORES DE COMPROMISSOS

A ISH Tecnologia realiza o tratamento de diversos indicadores de compromissos coletados por meio de fontes abertas, fechadas e também de análises realizadas pela equipe de segurança Heimdall. Diante disto, abaixo listamos todos os Indicadores de Compromissos (IOCs) relacionadas a análise do(s) artefato(s) deste relatório.

Indicadores de compromisso do artefato	
md5:	a77d3a4446ae106ccc6c251611231cbc
sha1:	54a8fe5c70ed0007fdd346a9a75977fd9f8ad24a
sha256:	7b3022437b637c44f42741a92c7f7ed251845fd02dda642c0a47fde179bd984e
File name:	csrss.exe

Tabela 1 – Indicadores de Compromissos de artefatos

5 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Morphisec**
- **Thehackernews**

6 AUTORES

- **Leonardo Oliveira Silva**

heimdall
security research
A DIVISION OF ISH