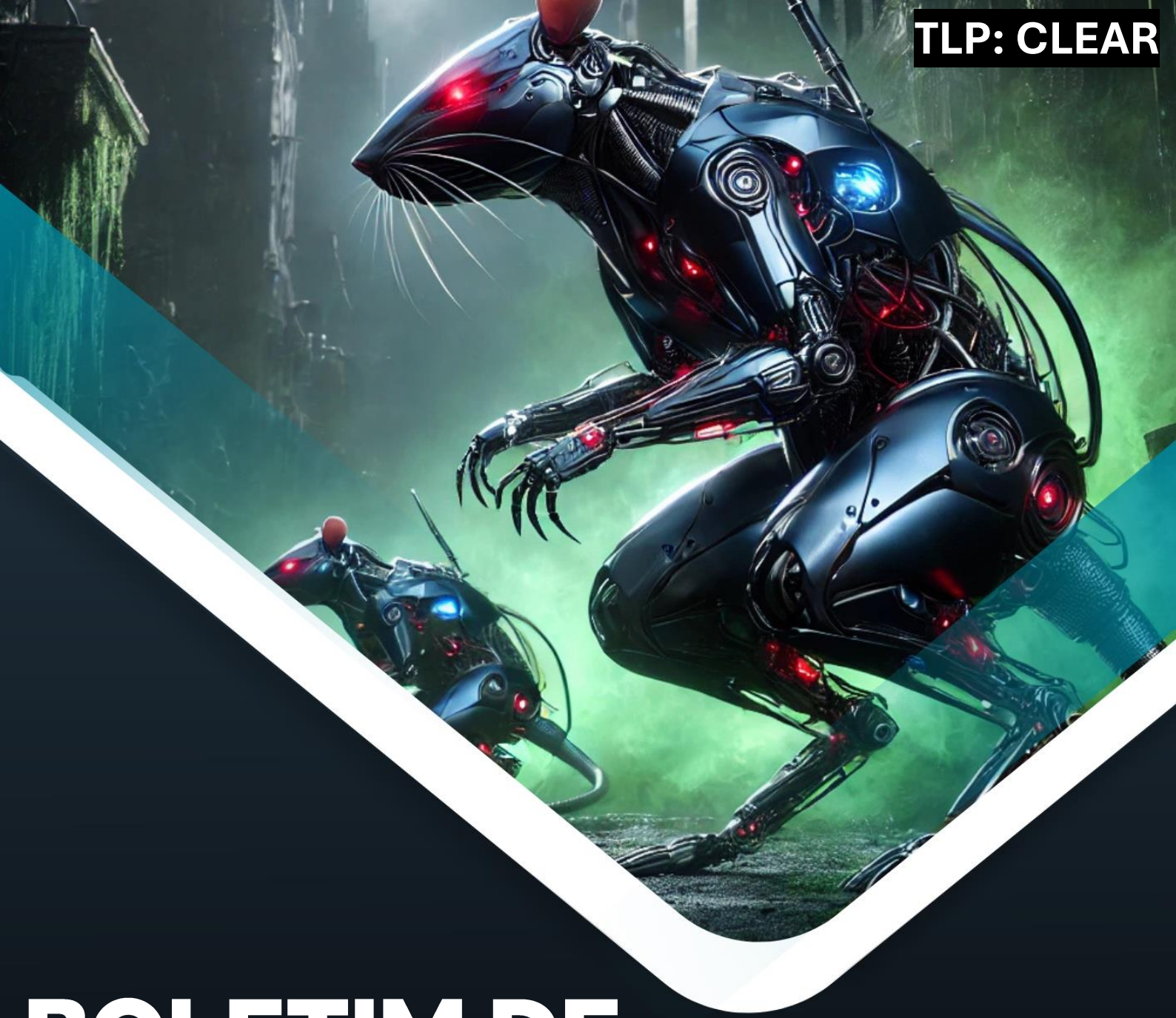
TLP: CLEAR



BOLETIM DE SEGURANÇA

FBI alerta sobre ataques do malware HiatusRAT a webcams e DVRs

heimdall
security research

Acesse a nossa nova comunidade através do WhatsApp!

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

1 INFORMAÇÕES SOBRE A AMEAÇA

O *Federal Bureau of Investigation* (FBI) emitiu um alerta para chamar a atenção para referente as campanhas de varredura do **HiatusRAT** contra webcams e DVRs de marca chinesa. O HiatusRAT é um Trojan de acesso remoto (RAT) que, na sua versão mais recente, tem sido utilizado desde julho de 2022. Inicialmente, a campanha Hiatus visava dispositivos de borda de rede desatualizados. Em março de 2024, os operadores do HiatusRAT realizaram uma campanha de varredura focada em dispositivos de **Internet das Coisas** (IoT) nos EUA, Austrália, Canadá, Nova Zelândia e Reino Unido. Eles analisaram câmeras da web e DVRs em busca de vulnerabilidades, como CVE-2017-7921, CVE-2018-9995, CVE-2020-25078, CVE-2021-33044, CVE-2021-36260 e senhas fracas fornecidas pelos fabricantes. Muitas dessas falhas ainda não foram corrigidas pelos fornecedores, especificamente, os atacantes miraram dispositivos Xiongmai e Hikvision com acesso telnet. Para realizar as varreduras, eles utilizaram o Ingram – uma ferramenta de verificação de webcam. Além disso, usaram a ferramenta de código aberto para ataques de força bruta. As portas TCP visadas como, 23, 26, 554, 2323, 567, 5523, 8080, 9530 e 56575.

CVEs	INFORMAÇÕES
CVE-2017-7921	Autenticação inadequada em dispositivos Hikvision, permitindo que invasores aumentem privilégios e acessem informações confidenciais.
CVE-2018-9995	Dispositivos DVR de várias marcas permitem que invasores ignorem a autenticação usando um cabeçalho de cookie específico.
CVE-2020-25078	Dispositivos D-Link permitem a divulgação de senhas de administrador através de um endpoint não autenticado.
CVE-2021-33044	Vulnerabilidade de desvio de autenticação em produtos Dahua, permitindo que invasores ignorem a autenticação construindo pacotes de dados maliciosos.
CVE-2021-36260	Vulnerabilidade de injeção de comando em produtos Hikvision, permitindo que invasores executem comandos maliciosos devido à validação de entrada insuficiente.

Tabela 1 – CVEs exploradas pelo HiatusRAT.

2 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:

Atualize seus dispositivos regularmente

- Certifique-se de que todos os dispositivos, especialmente webcams e DVRs, estejam com o firmware e software atualizados para corrigir vulnerabilidades conhecidas.

Use senhas fortes e únicas

- Evite senhas padrão ou fracas. Utilize combinações complexas de letras, números e símbolos para dificultar o acesso não autorizado.

Desative portas desnecessárias

- Feche portas de rede que não são utilizadas, como Telnet, para reduzir a superfície de ataque.

Segmente sua rede

- Isole dispositivos IoT do restante da rede para limitar o impacto de um possível comprometimento.

Monitore atividades suspeitas

- Utilize ferramentas de monitoramento para detectar comportamentos anômalos que possam indicar a presença de malware.

Implemente soluções de segurança robustas

- Utilize softwares anti-malware e firewalls para proteger seus dispositivos contra ameaças conhecidas e desconhecidas.

Realize backups

- Identifique e crie backups offline para ativos críticos.

Políticas de segurança

- Implemente políticas de listagem para aplicativos e acesso remoto, permitindo que apenas sistemas executem programas conhecidos e autorizados, de acordo com uma política de segurança previamente estabelecida.

3 INDICADORES DE COMPROMETIMENTO (IOC)

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 Comprometimento (IOCs) relacionadas a análise do(s) artefato(s) deste relatório.

Indicadores do artefato	
md5:	0932a5b7dcc829c03f229c25d7dc5031
sha1:	da1cd4b75787d8c3079ca4b7709bf788e7e2021e
sha256:	6eb7357c0492960150286418e2a2f18513f50e925630bf2e6235422143f2e6c6
File name:	update_mips32.sh.txt

Indicadores do artefato	
md5:	ff8e26ec2573f482abbd1a8fdd80fc81
sha1:	525c04e97a0e2b38243f11debec9e100cc51fb15
sha256:	6e21e42cfb93fc2ab77678b040dc673b88af31d78fafe91700c7241337fc5db2
File name:	6e21e42cfb93fc2ab77678b040dc673b88af31d78fafe91700c7241337fc5db2.elf

Indicadores do artefato	
md5:	9690a3e310ed96073035c4cc3436fa9c
sha1:	5ec68cd73e3ca516b2518bc3307f5381bcc52b20
sha256:	193481c4e2cbd14a29090f500f88455e1394140b9c5857937f86d2b854b54f60
File name:	q8m32

Indicadores do artefato	
md5:	5a07d8566930c9ead926c2f079620510
sha1:	5afe05692cb7893b454ee65911e98ffc362d925b
sha256:	774f2f3a801ddfe5d8a9ab1b90398ee28ee2be3d7ad0fa75eacbdf7ab51f6939
File name:	HiatusratbgjcehbhacI_browsingElf.elf

Tabela 2 – Indicadores de Comprometimento

Indicadores de URL, IPs e Domínios

Indicadores de URL, IPs e Domínios	
IP	104[.]250.48[.]192 46[.]8.113[.]227 66[.]42.108[.]185 149[.]248.0[.]203 207[.]246.80[.]240 45[.]63.70[.]57 155[.]138.213[.]169 66[.]135.22[.]245 107[.]189.11[.]105

Tabela 3 – Indicadores de Comprometimento de Rede.

Obs: Os *links* e endereços IP elencados acima podem estar ativos; cuidado ao realizar a manipulação dos referidos IoCs, evite realizar o clique e se tornar vítima do conteúdo malicioso hospedado no IoC.

4 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **FBI**
- **Bleepingcomputer**
- **NVD**

5 AUTORES

- **Leonardo Oliveira Silva**

heimdall
security research
A DIVISION OF ISH