



# BOLETIM DE SEGURANÇA

Ator de ameaça iraniano foca no Brasil



heimdall  
security research

A DIVISION OF ISH



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](#)



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 com 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

1	Identificação de APT Iraniano.....	5
2	Referências.....	7

## Lista de Figuras

Figura 1 – Cronograma de campanha de Acesso do Sponsoring ..... 5

## 1 IDENTIFICAÇÃO DE APT IRANIANO

Um ator de ameaça iraniano conhecido como Charming Kitten teria sido associado a uma nova onda de ataques a diferentes entidades no Brasil e em outros dois países, Israel e Emirados Árabes Unidos.

O ator estaria utilizando um backdoor anteriormente então documentado chamado **Sponsoring**. A empresa ESET teria rastreado os atores de ameaça sob o nome **Ballistic Bobcat (APT35/APT42)**, onde foi possível observar que o grupo destaca principalmente organizações de educação, governo e saúde, bem como ativistas de direitos humanos e jornalistas.

De acordo com a empresa pelo menos 34 vítimas do Sponsor foram detectadas até o momento, com os primeiros casos de implantações datando em setembro de 2021.

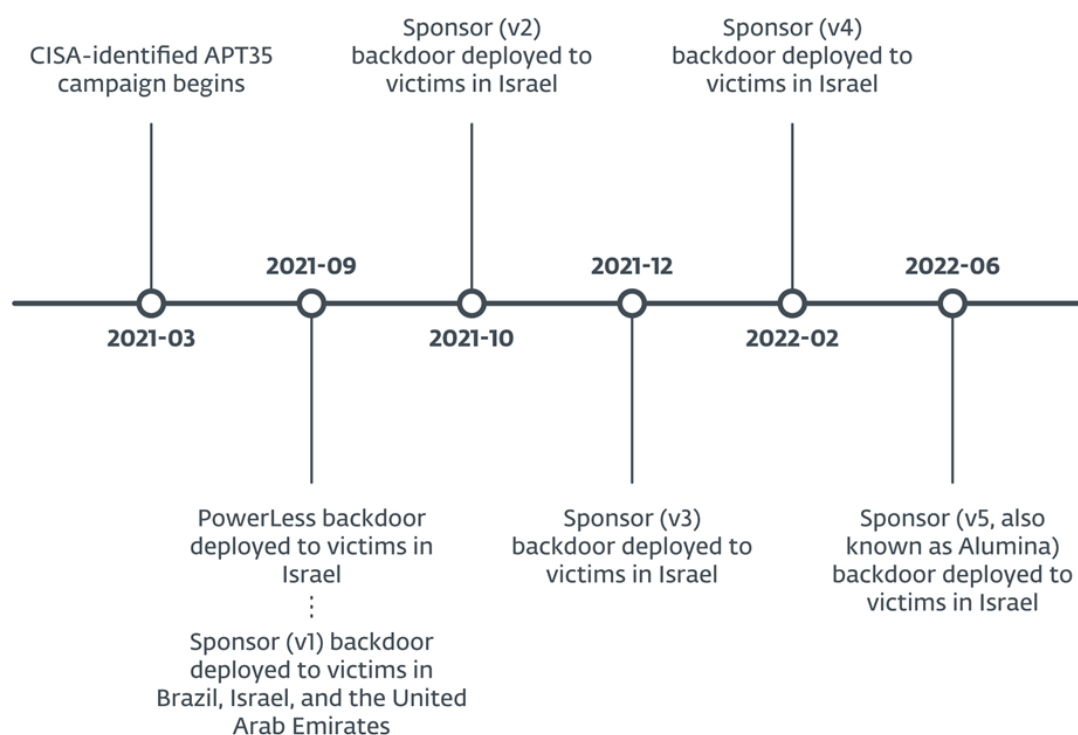


Figura 1 – Cronograma de campanha de Acesso do Sponsoring.

Para acesso inicial, o Ballistic Bobcat obteve acesso inicial explorando vulnerabilidades conhecidas em servidores Microsoft Exchange expostos à Internet, onde primeiro realizaram varreduras do

sistema ou rede para identificar pontos fracos ou vulnerabilidades potenciais e, posteriormente explorando este ponto fraco.

O backdoor utilizado do Sponsoring utiliza arquivos de configuração em disco, criados por um arquivo em lote (.bat), e ambos são inócuos para ignorar os mecanismos de defesas.

De acordo com a empresa, os atores utilizaram ainda um kit de ferramentas chamado Merlin, o qual conseguiu um shell reverso no servidor e na sequência, os operadores do Ballistic Bobcat lançaram o novo backdoor.

O referido malware foi escrito na linguagem C++, sendo projetado para coletar informações do host e processar instruções recebidas de um servidor de comando e controle, cujos dados são enviados ao ator como retorno. As ações maliciosas incluem: execução de comandos e arquivos, download de arquivos e atualização da lista de servidores controladores pelo invasor.

Como forma de se proteger, é de suma importância que as organizações se atentem para com quaisquer dispositivos expostos à internet e garantir uma determinada vigilância quando novos produtos e serviços expostos a internet surgirem na organização.

## 2 REFERÊNCIAS

---

- Heimdall *by* ISH Tecnologia
- [Relatório](#) ESET – Ballistic Bobcat



heimdall  
security research

A DIVISION OF ISH