BOLETIM DE SEGURANÇA

Aumento dos ataques do trojan bancário Mekotio ameaça sistemas financeiros na América Latina

heimdall
security research
A DIVISION OF ISH

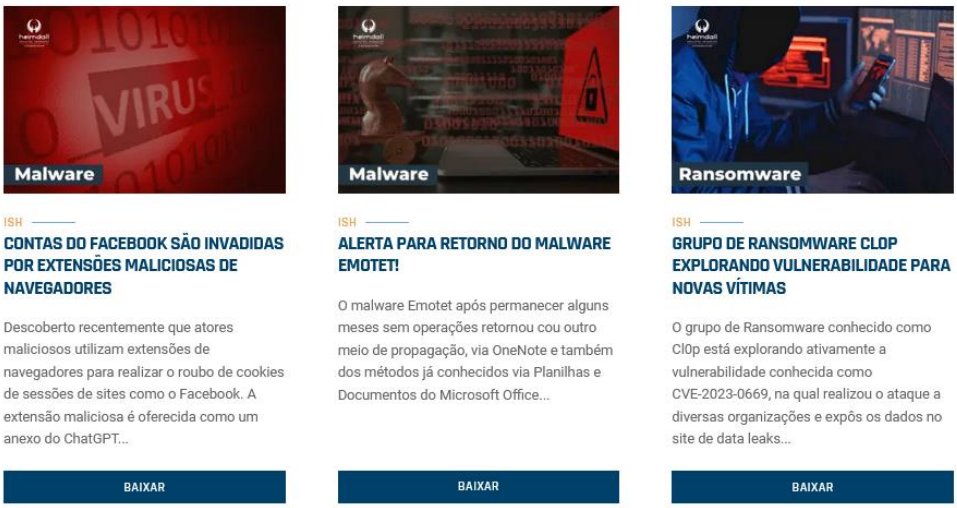
TLP: CLEAR

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

Foi observado pela TrendMicro um aumento nos ataques envolvendo o trojan bancário Mekotio, um malware sofisticado que está em atividade, tendo como principal alvo países da América Latina. Seu objetivo é roubar informações confidenciais, especialmente credenciais bancárias. Originário da região latino-americana, este malware tem sido especialmente ativo no Brasil, Chile, México, Espanha e Peru.

2 CADEIA DE ATAQUE DO MALWARE

O Mekotio geralmente se propaga através de e-mails que se apresentam como sendo de agências fiscais, alegando que o destinatário possui obrigações fiscais pendentes. Esses e-mails incluem um arquivo ZIP anexado ou um link para um site malicioso. Quando o usuário interage com o e-mail, o malware é baixado e executado no sistema, após ser executado, o Mekotio coleta informações do sistema e estabelece uma conexão com um servidor de comando e controle (C&C). Este servidor fornece instruções e uma lista de tarefas para o malware executar.

Dentro do sistema, o Mekotio realiza as seguintes atividades maliciosas:

1. **Roubo de credenciais**: O objetivo principal do Mekotio é roubar credenciais bancárias. Ele exibe pop-ups falsos que imitam sites bancários legítimos, enganando os usuários para que insiram suas informações, que são então coletadas pelo trojan.
2. **Coleta de informações**: O Mekotio pode tirar capturas de tela, registrar pressionamentos de teclas e roubar dados da área de transferência.
3. **Mecanismos de persistência**: O Mekotio emprega várias táticas para manter sua presença no sistema infectado, incluindo adicionar-se a programas de inicialização ou criar tarefas agendadas.

As informações bancárias roubadas são enviadas de volta ao servidor C&C, onde podem ser usadas por agentes mal-intencionados para atividades fraudulentas, como acesso não autorizado a contas bancárias.

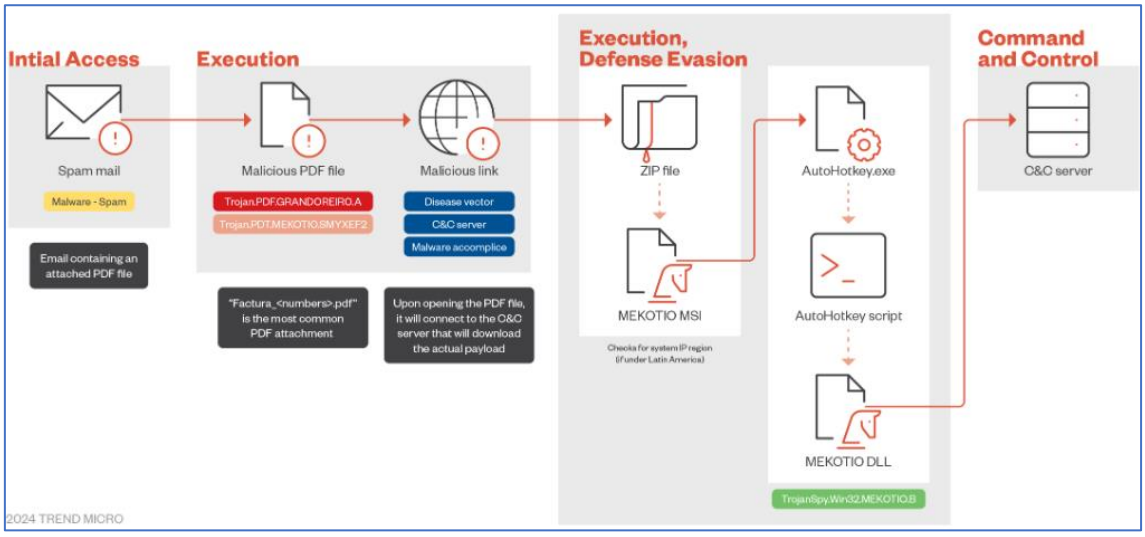


Figura 1 – Cadeia observada do malware.

3 CONCLUSÃO

A ameaça do Trojan Bancário Mekotio representa um risco significativo para organizações no Brasil devido à sua capacidade de roubar credenciais bancárias e informações financeiras sensíveis. Uma vez instalado, o Mekotio pode capturar dados de login e executar comandos remotamente, permitindo que os cibercriminosos realizem transações fraudulentas. A sofisticação e evolução constante deste Trojan tornam as medidas tradicionais de segurança muitas vezes insuficientes. Portanto, é crucial que as organizações implementem soluções robustas de segurança cibernética.

4 MITRE ATT&CK - TTPs

Tática	Técnica	Detalhes
Initial Access	T1566.001 Spear Phishing Attachment	Mekotio é entregue através de e-mails de phishing, contendo um anexo ZIP malicioso ou um link.
Execution	T1059 Command and Scripting Interpreter	O malware é executado quando o usuário interage com o anexo ou link malicioso.
Persistence	T1547 Boot or Logon Autostart Execution	Adiciona-se a programas de inicialização ou cria tarefas agendadas para manter sua presença no sistema.
Credential Access	T1555 Credentials from Password Stores	O trojan rouba credenciais bancárias exibindo pop-ups falsos que imitam sites legítimos de bancos.
Collection	T1113 Screen Capture	Captura de screenshots, registro de teclas e roubo de dados da área de transferência.
Command and Control	T1071.001 Application Layer Protocol: Web Protocols	Mekotio estabelece uma conexão com um servidor C&C para receber instruções.

Tabela 1 – Tabela MITRE ATT&CK.

5 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:

Educação e treinamento de funcionários

- Realize treinamentos regulares de conscientização sobre segurança cibernética para ajudar os funcionários a reconhecer e evitar e-mails de phishing e outros vetores de ataque.
- Enfatize a importância de não clicar em links ou baixar anexos de e-mails suspeitos.

Atualização e patching de software

- Mantenha todos os sistemas operacionais, navegadores e software de segurança atualizados com os patches mais recentes.
- Utilize soluções de gerenciamento de patches para garantir que todos os dispositivos da organização estejam protegidos contra vulnerabilidades conhecidas.

Uso de softwares de segurança

- Implante soluções de segurança, como antivírus e anti-malware, em todos os dispositivos.
- Configure firewalls e sistemas de prevenção/detecção de intrusões (IPS/IDS) para monitorar e bloquear atividades suspeitas.

Autenticação e controle de acesso

- Implemente autenticação multifator (MFA) para todas as contas de usuário, especialmente para acessos remotos e contas com privilégios administrativos.
- Revise regularmente os direitos de acesso dos usuários e restrinja o acesso aos dados e sistemas críticos com base na necessidade de saber.

Backups regulares

- Realize backups regulares dos dados críticos e verifique a integridade desses backups.
- Armazene os backups de forma segura e em locais separados da rede principal para evitar que sejam comprometidos em caso de ataque.

Monitoramento e resposta a incidentes

- Utilize sistemas de monitoramento de rede e endpoints para detectar atividades anômalas e potencialmente maliciosas.

- Estabeleça um plano de resposta a incidentes que inclua procedimentos para isolar, mitigar e remediar infecções por malware.

Segmentação de rede

- Implemente a segmentação da rede para limitar a movimentação lateral de atacantes dentro da infraestrutura da organização.
- Utilize VLANs e outras técnicas de segmentação para separar sistemas críticos de outras partes da rede.

Políticas de senhas

- Estabeleça políticas rigorosas de criação e atualização de senhas.
- Use senhas fortes e únicas para todas as contas e evite o uso de senhas padrão ou fáceis de adivinhar.

Revisões de segurança e auditorias

- Realize auditorias de segurança regulares e testes de penetração para identificar e corrigir vulnerabilidades.
- Avalie continuamente as políticas e procedimentos de segurança para garantir que estejam alinhados com as melhores práticas e requisitos regulatórios.

6 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:	d447a2f6c83e2f6c18bad592ed029bdd
sha1:	5e92f0fcddc1478d46914835f012137d7ee3c217
sha256:	b6a82774b81a965033716351d92dd0a75f494069b4b4436d21327c06c917e6e0
File name:	Factura_883152.pdf

Indicadores de compromisso do artefato	
md5:	00329d659b4166066737320f725cfd93
sha1:	f68d3a25433888aa606e18f0717d693443fe9f5a
sha256:	e082dc1c11afff40efe2cf92e36ac37129b78320b5cc656f4b80488307770eab
File name:	Factura_184710.pdf

Indicadores de compromisso do artefato	
md5:	38a9671a253750cbe517ce75af2117e3
sha1:	3fe5d098952796c0593881800975bcb09f1fe9ed
sha256:	008c7e556beba4a5d026211259114ba686013b5fd5f9cb9e677b2641bd2c2fc5
File name:	Factura_420349.pdf

Indicadores de compromisso do artefato	
md5:	3e4f3d7f962653220759a1169c3bad45
sha1:	1087b318449d7184131f0f21a2810013b166bf37
sha256:	a7112aa5b398fc7a77100164c818b5e17612d828320b4e3e1f895e56b4fd6797
File name:	MSI78BB.tmp

Indicadores de compromisso do artefato	
md5:	6c81cf6d72baffb7cfe0d62d8d17d5f4
sha1:	ef22c6b4323a4557ad235f5bd80d995a6a15024a
sha256:	439eecb230fb53b817ae535d6a6d978066134b4b52e49e065e9ddeff5f2bbbd3
File name:	MSI73E8.tmp

Tabela 2 – Indicadores de Compromissos de artefatos

Indicadores de URL, IPs e Domínios

Indicadores de URL, IPs e Domínios	
URL	hxxps://intimaciones[.]afip[.]gob[.]ar[.]kdental[.]cl/Documentos_Intimacion/ hxxps://techpowerup[.]net/cgefacturacl/descargafactmayo/eletricidad/ hxxps://christcrucifiedinternational[.]org/descargafactmayo/eletricidad/
Domínio	tudoprafrente[.]org tudoprafrente[.]co:7958
IP	23[.]239[.]4[.]149:80 68[.]233[.]238[.]122:80

	34[.]117[.]186[.]192:80 68[.]221[.]121[.]160:9095 68[.]221[.]121[.]160:80

Tabela 3 – 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.

7 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **TrendMicro**
- **MITRE ATT&CK**

8 AUTORES

- **Ismael Pereira Rocha**

heimdall
security research
A DIVISION OF ISH