heimdall

security research

A DIVISION OF ISH

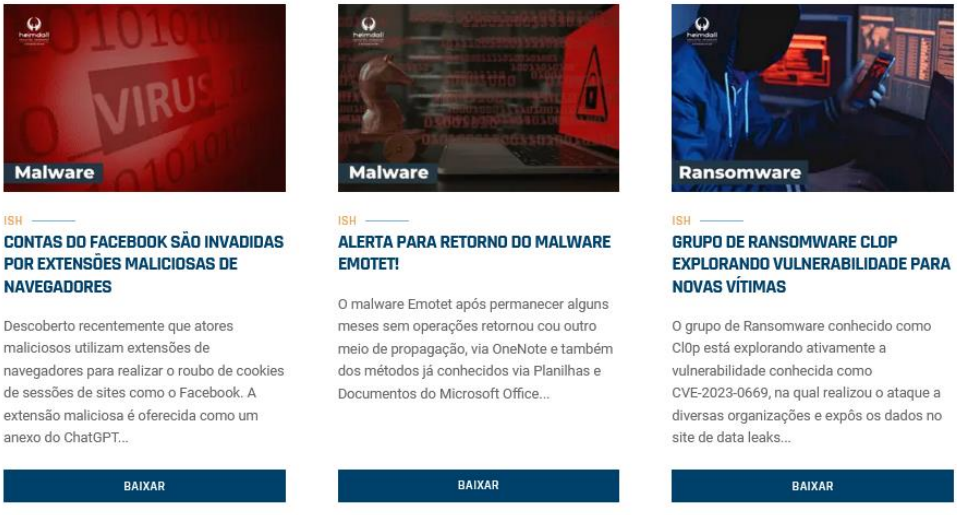
Campanhas de *phishings* para o Brasil e Espanha

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



Sumário

Lista de Tabelas

Lista de Figuras

1 INTRODUÇÃO

A empresa de segurança Perception Point realizou pesquisas e identificação ao longo do mês de 2023, na qual a empresa veio a observar um aumento nas campanhas de e-mail de phishing criadas em português e espanhol. Os referidos e-mails foram projetados para se passar por instituições bancárias espanholas e brasileiras legítimas, sendo que segundo o relatório é induzir usuários desavisados a clicar em um link incorporado ao e-mail.

Os atores de ameaças foram mapeados pela Perception Point atribuindo os atores o nome de "GeoMetrix", sendo que os atores são responsáveis por criar campanhas de phishing, sendo que provavelmente estes agentes estariam obtendo lucros através de vendas de ferramentas de phishing, por meio de vendas para outros cibercriminosos.

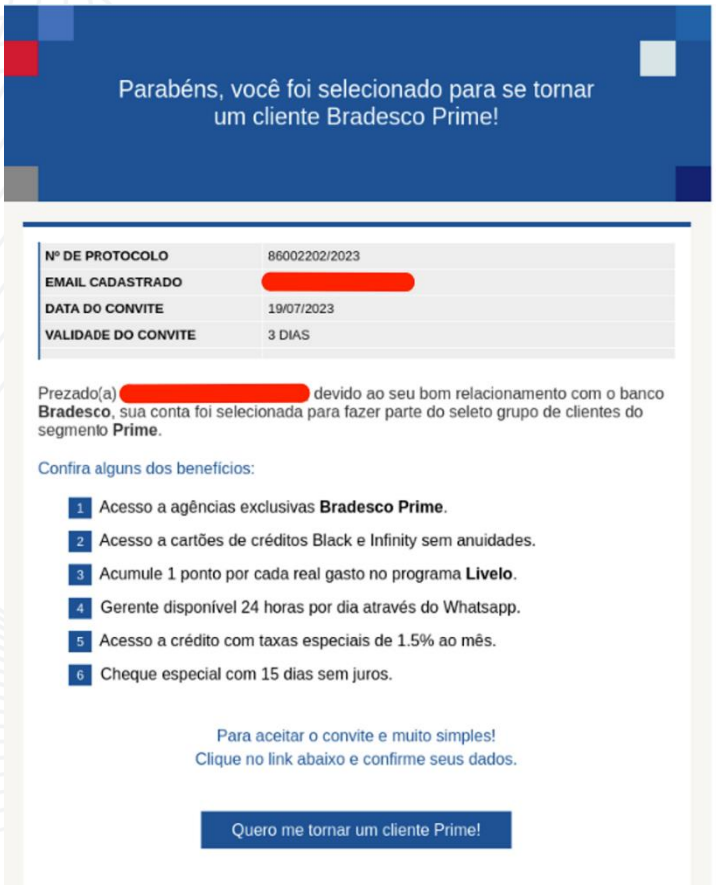


Figura 1 – Exemplo de e-mail de phishing.

Vale salientar que o usuário, ao clicar no URL inserido na campanha, ele é redirecionado para o site do painel de controle do agente de ameaça, sendo que o site realiza a varredura de geolocalização do usuário. Caso a localização esteja alinha com a geografia visada pelo agente da ameaça, os dados críticos do usuário (como endereço de IP, localização física e endereço de e-mail), sendo registrados no painel de cliques do ator de ameaça.

Na sequência, o usuário é redirecionado para uma URL maliciosa. Este URL malicioso oculta uma dos seguintes payloads:

1. Downloader com malware bancário, como Mekotio, Grandoreiro e Ousaban.
2. Um site de phishing imitando um banco na América Latina.
3. Um site fraudulento de phishing da Trust Wallet.

A empresa disponibilizou ainda um fluxo de execução da campanha:

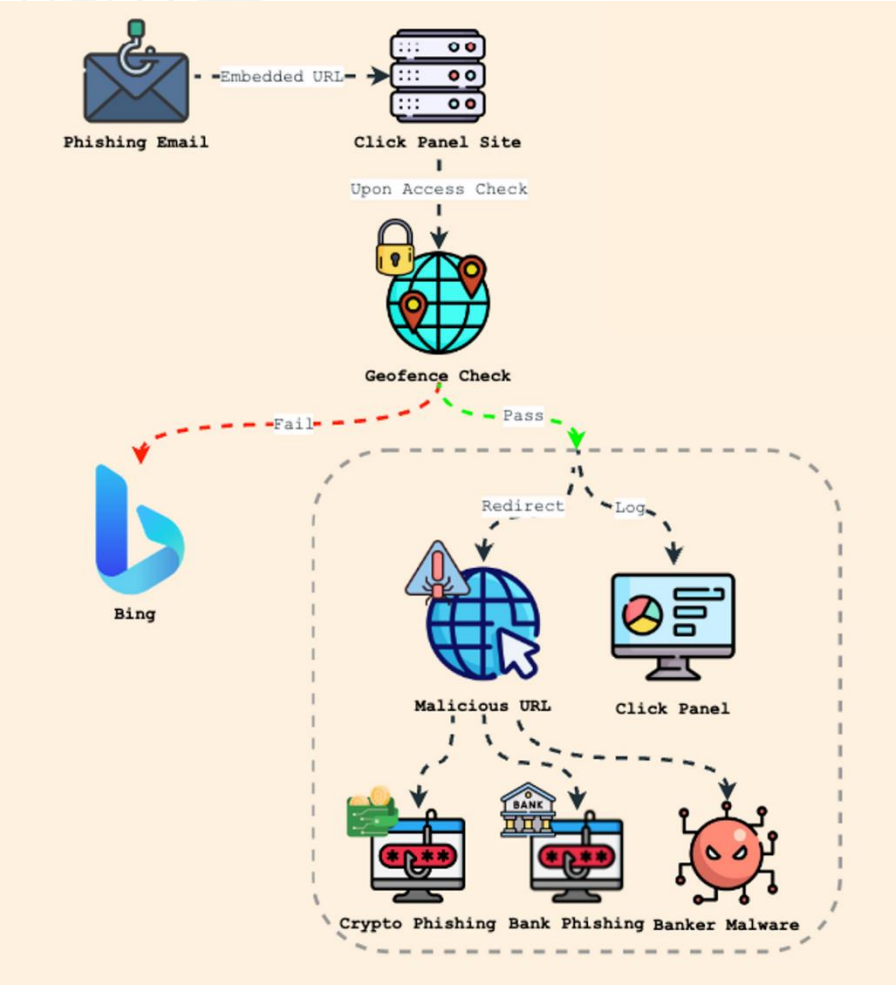


Figura 2 – Diagrama e fluxo de campanha.

2 VERIFICAÇÃO DA REGIÃO GEOGRÁFICA

De acordo com a análise realizada, de acordo com os painéis ativos, cada um compartilhando uma estrutura comum:

1. Painel de login apresentada em português.
2. Painel de controle abrangendo os seguintes campos:
    a. Data o clique
    b. Endereço de IP
    c. País
    d. Região
    e. Cidade
    f. Tipo de dispositivo
    g. Hospedagem
    h. E-mail
    i. Status
3. Botões de reinicialização:

ITEM	DATA	IP	PAÍS	UF	CIDADE	DEVICE	HOST	E-MAIL	STATUS
1	19/07/2023 09:34:55		Brazil	MG	Malacacheta	DESKTOP			LIBERADO
2	19/07/2023 09:34:53		Brazil	PR	Goioere	DESKTOP			LIBERADO
3	19/07/2023 09:27:20		Brazil	ES	Cachoeiro de Itap emirim	DESKTOP			LIBERADO
4	19/07/2023 09:27:01		Brazil	ES	Cachoeiro de Itap emirim	DESKTOP			LIBERADO
5	19/07/2023 09:26:25		Brazil	CE	Fortaleza	DESKTOP			LIBERADO
6	19/07/2023 09:26:16		Brazil	CE	Fortaleza	DESKTOP			LIBERADO
7	19/07/2023 09:03:47		Brazil	SP	São Paulo	DESKTOP			LIBERADO
8	19/07/2023 09:01:35		Brazil	SP	Mogi das Cruzes	DESKTOP			LIBERADO
9	19/07/2023 08:57:02		Brazil	SE	Umbauba	DESKTOP			LIBERADO
10	19/07/2023 08:54:35		Brazil	DF	Brasília	DESKTOP			LIBERADO
11	19/07/2023 08:50:19		Brazil	SP	São Paulo	DESKTOP			LIBERADO
12	19/07/2023 08:40:42		Brazil	PR	Maringá	DESKTOP			LIBERADO

Figura 3 – Dados e apresentação do painel de controle das campanhas.

O mecanismo de geofencing envolve três verificações essenciais:

1. **Verificação do User-Agent:** O servidor recupera os dados do User-agent do usuário e faz uma referência cruzada com uma lista de bloqueio.

2. **Verificação do nome do host:** Desde que a verificação do agente do usuário seja aprovada, o servidor recupera os dados do host do usuário usando a função PHP "*gethostbyaddr*". Esses dados do host também são comparados a uma lista de bloqueio.
3. **Verificação de geolocalização:** como etapa final, assumindo que a verificação do host foi aprovada com sucesso, o servidor envia o endereço IP do usuário para um serviço de API de geolocalização IP. O campo "país" recuperado desse serviço é comparado a uma lista de permissões.

Caso o usuário passe com sucesso em todas as três verificações, seus dados serão registrados no painel de cliques e eles serão redirecionados para a URL maliciosa. Se alguma verificação falhar, o usuário será redirecionado para um mecanismo de busca benigno, como o Bing.

O impacto da campanha identificada pelos pesquisadores é de que havia dez painéis diferentes, cada um apresentando um contador de "cliques de sucesso" (Liberados). Ao agregar o número de "cliques de sucesso", em todo os painéis, foi descoberto que o número de usuários infectados ultrapassou a marca de **15.000 vítimas**.

3 EXEMPLO DE CAMPANHA

Como exemplo, a campanha que se destacou foi a campanha se passando pelo Banco do Brasil, na qual o e-mail phishing teris sido bem elaborado, contendo informações visando alertar o destinatário sobre uma grande quantidade de moedas digitais que expiram no dia seguinte e sugerindo que as use imediatamente.

Figura 4 – E-mail phishing enviado.

O e-mail aparentemente inofensivo levava as vítimas a um site de phishing criado, muito parecido com a página de login do Banco do Brasil.

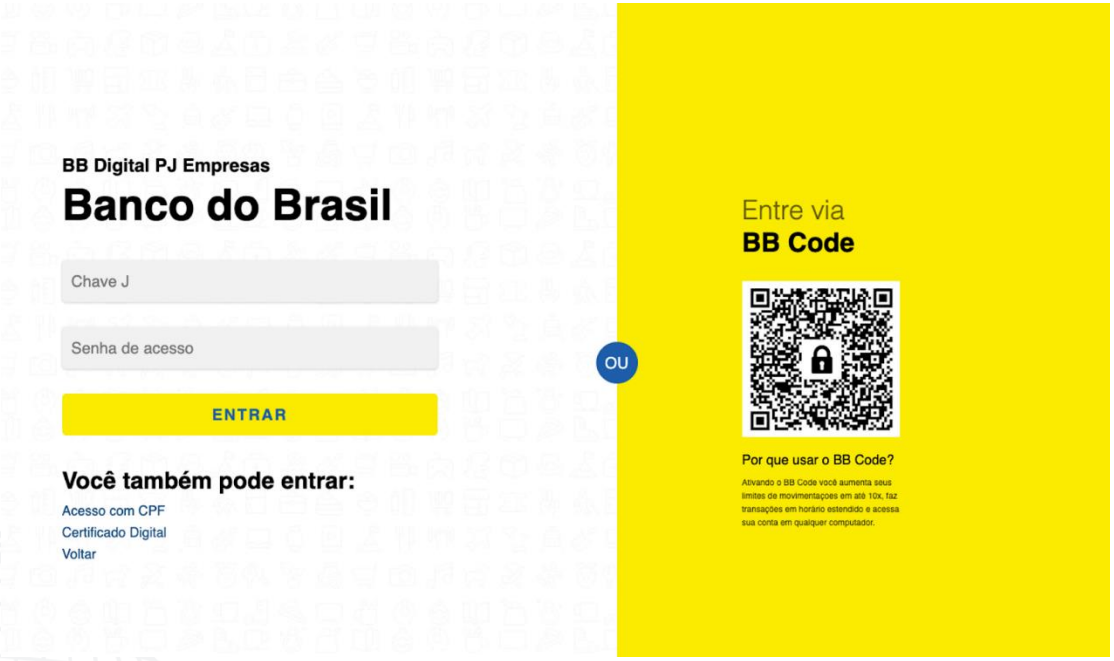


Figura 5 – Página aberta para coleta de credenciais da conta.

A esquerda da página, os usuários eram solicitados a fornecer uma chave e uma senha. A partir daqui, com o fornecimento destes dados iniciava-se uma série de campanhas de phishing destinados a roubar informações bancárias pessoais, sendo que do lado direito da página, era apresentado o "BB Code".

O "BB Code" é um recurso do Banco do Brasil criado para tornar as transferências de dinheiro mais fáceis e seguras. Ele funciona escaneando um código QR com qualquer aplicativo bancário e confirmando a transação no telefone do usuário. Isso então transfere o dinheiro para o destinatário desejado.

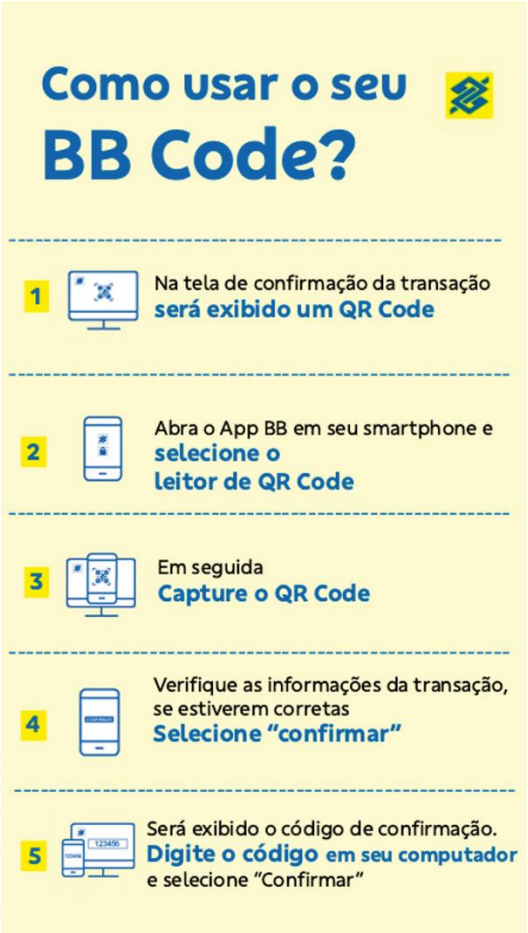


Figura 6 – Passo a passo para fornecimento de transação bancária.

Logo, os atores de ameaças por trás da campanha exploraram o recurso visando usá-lo para induzir as vítimas a transferir dinheiro diretamente para eles. Ao fazer o processo parecer fácil e seguro, eles acabaram identificando uma maneira convincente de roubar dinheiro das vítimas inocentes.

De acordo com a empresa, devido as evidências coletadas durante a investigação, foi possível mensurar que os atores maliciosos estariam ganhando dos seguintes modelos:

- Phishing-as-a-Service (PhaaS): sendo oferecido o serviço na qual os clientes são cobrados por "cliques" bem-sucedidos, bem parecido com o "Malware-as-a-Service".
- Vendas de kits de phishing: Outra possível fonte de receita para o GeoMetrix poderia ser a venda de kits de phishing prontos para o uso. (incluindo, painel, domínio e lista de alvos de spam).

4 Conclusão

De acordo com a empresa, devido as evidências coletadas durante a investigação, foi possível mensurar que os atores maliciosos estariam ganhando dos seguintes modelos:

- ***Phishing-as-a-Service (PhaaS):*** sendo oferecido o serviço na qual os clientes são cobrados por "cliques" bem-sucedidos, bem parecido com o "Malware-as-a-Service".
- **Vendas de kits de phishing:** Outra possível fonte de receita para o GeoMetrix poderia ser a venda de kits de phishing prontos para o uso. (incluindo, painel, domínio e lista de alvos de spam).

Logo, é possível concluir que o GeoMetrix mapeado pela empresa é considerado como uma plataforma que permite que outras pessoas realizem atividades maliciosas, incluindo phishing e distribuição de malwares.

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:

- **Desconfie de e-mails suspeitos**: Se você receber um e-mail inesperado, especialmente se pedir informações pessoais, financeiras ou senhas, seja cauteloso. Verifique o remetente e a gramática do e-mail, pois os phishing muitas vezes contêm erros.
- **Verifique os URLs**: Antes de clicar em qualquer link, passe o mouse sobre ele (sem clicar) para ver o URL real. Certifique-se de que o URL corresponda ao site legítimo e não a um domínio ligeiramente modificado.
- **Não clique em links suspeitos**: Evite clicar em links em e-mails, mensagens ou redes sociais, a menos que esteja absolutamente certo de sua origem. Em vez disso, digite manualmente o URL do site no navegador.
- **Cuidado com as mensagens de urgência**: Muitos golpes de phishing tentam criar um senso de urgência para pressioná-lo a agir rapidamente sem pensar. Se você receber uma mensagem urgente, entre em contato diretamente com a empresa ou serviço por meio dos canais oficiais, em vez de clicar em links no e-mail.
- **Use autenticação em dois fatores (2FA)**: Sempre que possível, ative a autenticação em dois fatores para suas contas. Isso adiciona uma camada extra de segurança, exigindo um segundo método de verificação além da senha.
- **Atualize software e sistemas**: Mantenha seu sistema operacional, navegadores e aplicativos atualizados. As atualizações frequentes geralmente incluem correções de segurança que podem proteger contra vulnerabilidades exploradas pelos phishing.
- de seguro social, por e-mail, mensagem de texto ou telefone, a menos que esteja certo da legitimidade da solicitação.
- **Use um filtro de spam**: Configure um filtro de spam eficaz para ajudar a bloquear e-mails suspeitos antes que eles cheguem à sua caixa de entrada.

6 IoCs

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.

URLs de distribuição e endereços IP C2:

226.120.168[.]184
202.34.109[.]208
86.203.178[.]68
124.245.72[.]148
1.161.178[.]68
145.166.205[.]92
240.91.74[.]97
85.27.205[.]92
cliente.appoupelainternet[.]com
recoverymetacustom.z29.web.core.windows[.]net
recovercustomertrust.z29.web.core.windows[.]net
brbrasilonline[.]online
centersjwpoll[.]com
resgateseguro-seg[.]com
clientesegurodesco[.]com
seg-primeparavoce[.]com

Tabela 1 – Indicador de Compromisso 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**
- **Peception Point – Operation Geometrix do Brasil**

heimdall
security research

A DIVISION OF ISH