FUNDAÇÃO EDSON QUEIROZ
UNIVERSIDADE DE FORTALEZA - UNIFOR
CENTRO DE CIÊNCIAS TECNOLÓGICAS
SEGURANÇA CIBERNÉTICA COM FOCO EM DEVOPS

Caso VirtuaBank - Whale Phishing

Fortaleza-CE
2024

JOSÉ TALLIS DOURADO DIÓGENES
LUCAS GALDINO MOTA
MARCELO BORGES PEREIRA DA COSTA
TESSELE SAMPAIO LOPES

TÍTULO: Caso VirtuaBank - Whale Phishing

Trabalho de Conclusão de Disciplina apresentado ao curso de Especialização em Segurança da Informação com foco com DevOps da Universidade de Fortaleza, para obtenção de aprovação no curso.
Professor: Janilton Luz
Disciplina: Fundamentos de Segurança Cibernética

Fortaleza-CE
2024

Introdução

O phishing é uma ameaça crescente na era digital. É uma técnica astuta usada por cibercriminosos para roubar informações pessoais, financeiras e até mesmo credenciais de login. Existem diversos tipos desse ataque, uma será apresentada neste trabalho, a Whale Phishing.

O Whale Phishing ou Whaling, também conhecido como "phishing de alto escalão", é uma forma específica de ataque cibernético direcionada a executivos de alto escalão em empresas, utilizando e-mails, mensagens de texto ou chamadas telefônicas fraudulentas. Estas comunicações são altamente elaboradas para convencer o destinatário a realizar grandes transações financeiras em favor dos criminosos virtuais, ou a revelar informações sigilosas de natureza pessoal ou corporativa.

Os alvos do ataque são geralmente líderes empresariais de nível C, como CEOs, CFOs e COOs, assim como outros executivos seniores, figuras políticas e líderes de organizações que possuem autoridade para aprovar transações de grande montante ou divulgar informações confidenciais sem necessidade de confirmação externa. Tais indivíduos são frequentemente denominados como "baleias" (*whales*) devido à sua capacidade financeira substancial, comparada à média da população.

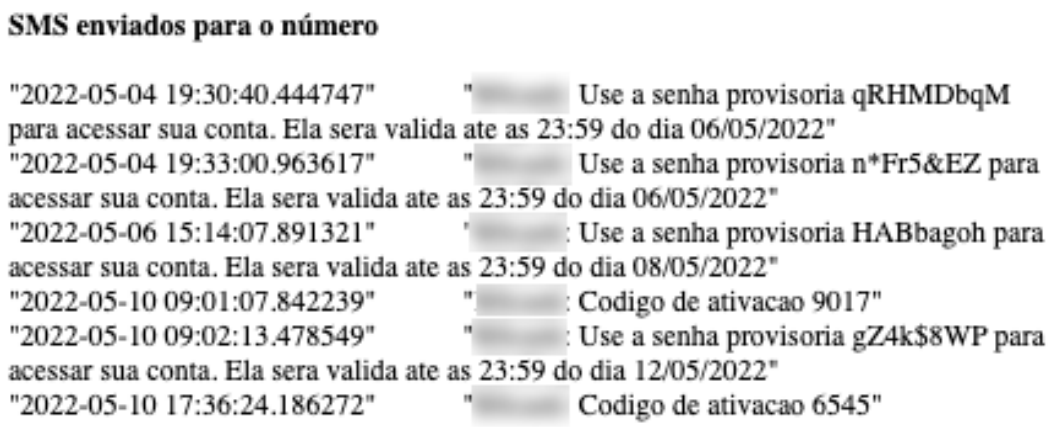
O invasor tipicamente se passa por um colega da mesma organização ou de uma organização associada, de status igual ou superior. As mensagens de Whaling são meticulosamente adaptadas: os perpetradores fazem esforços para replicar o estilo de comunicação do remetente original e, sempre que possível, referem-se a discussões empresariais reais em andamento. Muitas vezes, os golpistas monitoram as interações entre o remetente e o destinatário, e alguns até tentam assumir o controle da conta de e-mail ou mensagem do remetente real, a fim de enviar a mensagem de ataque diretamente, aumentando assim a credibilidade do golpe.

O caso apresentado no presente trabalho trata-se de um típico exemplo do Whale Phishing, o qual será detalhado e posto evidências reais do ataque. A empresa alvo em questão terá seu nome preservado e será chamada de forma fictícia como VirtuaBank.

Caso

No dia 02/05/2022, foi efetuada a criação de um domínio similar ao domínio oficial do cliente. O domínio criado teve como diferença a adição de uma letra a mais ao nome do domínio oficial. Por exemplo, o domínio oficial seria algo como "@unifor.br" e o domínio criado foi nomeado "@uniifor.br". Após a criação, foi enviado um e-mail para pessoas-chave da empresa em questão, dados estes obtidos através do perfil no LinkedIn dos envolvidos. Nos dias 03 e 04 do mesmo mês, através desses e-mails, conseguiram realizar um SIM Swap em duas pessoas da empresa, uma delas sendo a própria CEO e a outra, uma gerente do setor financeiro da empresa. Com o número dessas pessoas em mãos, foi possível solicitar um reset de senha para o acesso ao sistema.

Figura 1 - SMS enviados para o SIM Falso

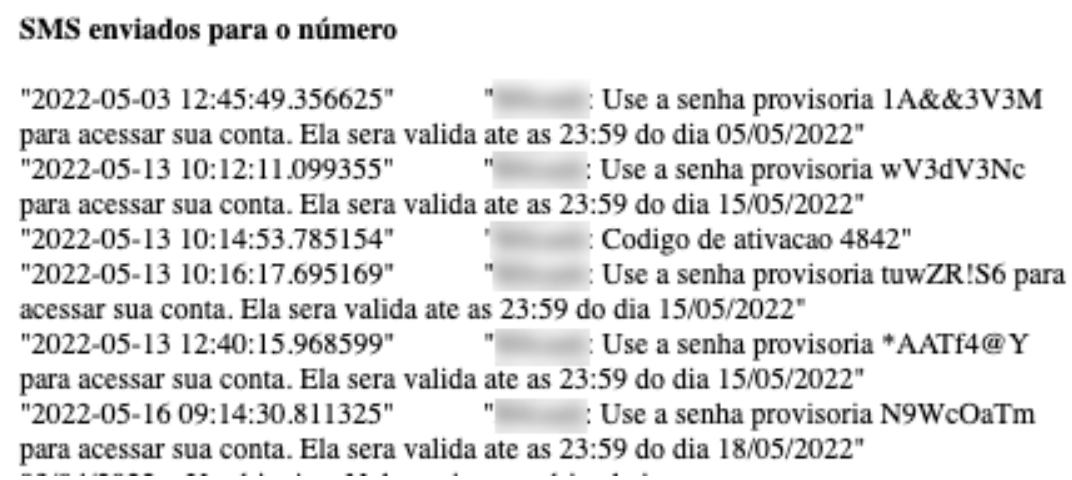


SMS enviados para o número

"2022-05-04 19:30:40.444747" "[redacted] Use a senha provisoria qRHMDbqM para acessar sua conta. Ela sera valida ate as 23:59 do dia 06/05/2022"
"2022-05-04 19:33:00.963617" "[redacted] Use a senha provisoria n*Fr5&EZ para acessar sua conta. Ela sera valida ate as 23:59 do dia 06/05/2022"
"2022-05-06 15:14:07.891321" "[redacted]: Use a senha provisoria HABbagoh para acessar sua conta. Ela sera valida ate as 23:59 do dia 08/05/2022"
"2022-05-10 09:01:07.842239" "[redacted]: Codigo de ativacao 9017"
"2022-05-10 09:02:13.478549" "[redacted]: Use a senha provisoria gZ4k$8WP para acessar sua conta. Ela sera valida ate as 23:59 do dia 12/05/2022"
"2022-05-10 17:36:24.186272" "[redacted] Codigo de ativacao 6545"

Fonte: Própria (2022)

Figura 2 - SMS enviados para o SIM Falso.

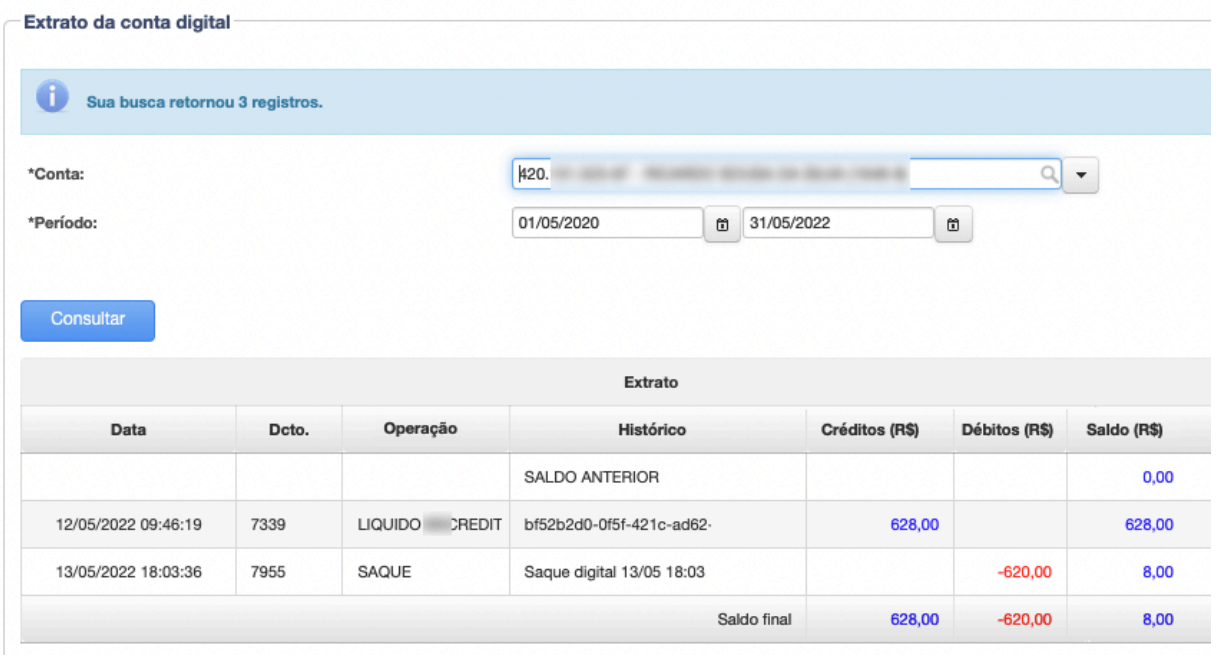


SMS enviados para o número

"2022-05-03 12:45:49.356625" "[redacted]: Use a senha provisoria 1A&&3V3M para acessar sua conta. Ela sera valida ate as 23:59 do dia 05/05/2022"
"2022-05-13 10:12:11.099355" "[redacted]: Use a senha provisoria wV3dV3Nc para acessar sua conta. Ela sera valida ate as 23:59 do dia 15/05/2022"
"2022-05-13 10:14:53.785154" "[redacted]: Codigo de ativacao 4842"
"2022-05-13 10:16:17.695169" "[redacted]: Use a senha provisoria tuwZR!S6 para acessar sua conta. Ela sera valida ate as 23:59 do dia 15/05/2022"
"2022-05-13 12:40:15.968599" "[redacted]: Use a senha provisoria *AATf4@Y para acessar sua conta. Ela sera valida ate as 23:59 do dia 15/05/2022"
"2022-05-16 09:14:30.811325" "[redacted]: Use a senha provisoria N9WcOaTm para acessar sua conta. Ela sera valida ate as 23:59 do dia 18/05/2022"

Fonte: Própria (2022)

Depois, com o acesso ao sistema garantido, foram criadas quatro novas contas-remuneração e solicitado um empréstimo em cada uma dessas quatro contas. Tendo acesso às contas da CEO e da gerência financeira, foi possível aprovar o empréstimo solicitado pelas novas contas. Após a aprovação dos empréstimos, foi realizado um saque mediante ATMs 24 horas no estado de São Paulo.



Extrato da conta digital

Sua busca retornou 3 registros.

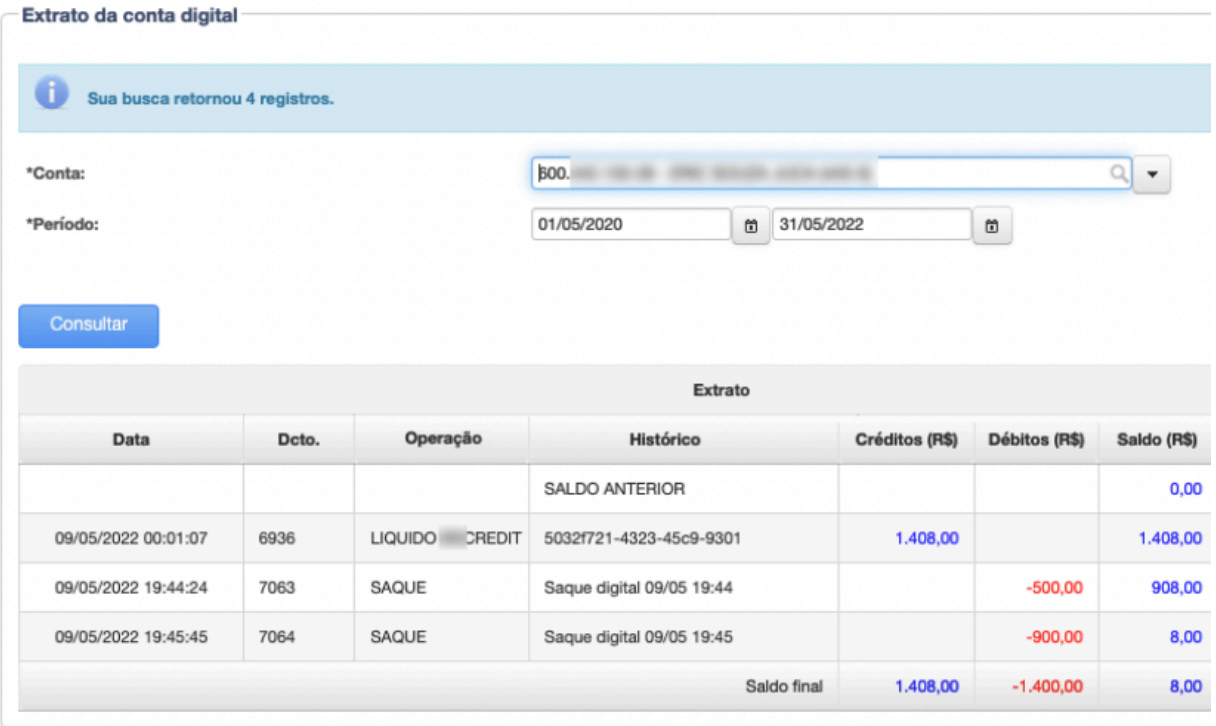
*Conta: 420.

*Período: 01/05/2020 31/05/2022

Consultar

Extrato

Data	Dcto.	Operação	Histórico	Créditos (R$)	Débitos (R$)	Saldo (R$)
			SALDO ANTERIOR			0,00
12/05/2022 09:46:19	7339	LIQUIDO CREDIT	bf52b2d0-0f5f-421c-ad62-	628,00		628,00
13/05/2022 18:03:36	7955	SAQUE	Saque digital 13/05 18:03		-620,00	8,00
			Saldo final	628,00	-620,00	8,00



Extrato da conta digital

Sua busca retornou 4 registros.

*Conta: 800.

*Período: 01/05/2020 31/05/2022

Consultar

Extrato

Data	Dcto.	Operação	Histórico	Créditos (R$)	Débitos (R$)	Saldo (R$)
			SALDO ANTERIOR			0,00
09/05/2022 00:01:07	6936	LIQUIDO CREDIT	5032f721-4323-45c9-9301	1.408,00		1.408,00
09/05/2022 19:44:24	7063	SAQUE	Saque digital 09/05 19:44		-500,00	908,00
09/05/2022 19:45:45	7064	SAQUE	Saque digital 09/05 19:45		-900,00	8,00
			Saldo final	1.408,00	-1.400,00	8,00

Extrato da conta digital

Sua busca retornou 4 registros.

*Conta: 010

*Período: 01/05/2020 31/05/2022

Consultar

Extrato

Data	Dcto.	Operação	Histórico	Créditos (R$)	Débitos (R$)	Saldo (R$)
			SALDO ANTERIOR			0,00
11/05/2022 07:17:20	7203	LIQUIDO CREDIT	f16f6998-c8ad-4615-9224-	1.230,00		1.230,00
11/05/2022 12:33:21	7259	SAQUE	Saque digital 11/05 12:33		-1.000,00	230,00
11/05/2022 12:34:53	7260	SAQUE	Saque digital 11/05 12:34		-200,00	30,00
			Saldo final	1.230,00	-1.200,00	30,00

Extrato da conta digital

Sua busca retornou 8 registros.

*Conta: 003

*Período: 01/05/2020 31/05/2022

Consultar

Extrato

Data	Dcto.	Operação	Histórico	Créditos (R$)	Débitos (R$)	Saldo (R$)
			SALDO ANTERIOR			0,00
10/05/2022 00:31:28	7082	LIQUIDO CREDIT	137342af-a66d-43bc-a61e-af1aa13b9db6	1.200,00		1.200,00
10/05/2022 10:20:50	7127	DOC/TED	TED		-1.200,00	0,00
10/05/2022 13:18:48	7158	ESTORNO DE DOC/TED	REF DCTO 7127 - RETORNO DE CREDITO NAO PAGO	1.200,00		1.200,00
10/05/2022 18:58:31	7179	SAQUE	Saque digital 10/05 18:58		-1.200,00	0,00
12/05/2022 11:28:42	7402	ESTORNO DE SAQUE	REF DCTO 7179 - TECBAN NAO DEBITOU A CONTA	1.200,00		1.200,00
13/05/2022 17:57:02	7953	SAQUE	Saque digital 13/05 17:57		-1.000,00	200,00
13/05/2022 17:58:37	7954	SAQUE	Saque digital 13/05 17:58		-200,00	0,00
			Saldo final	3.600,00	-3.600,00	0,00

ATM	Data / Hora	Valor
41897	22/05/2013 17:57	R$ 1.000,00
41897	22/05/2013 17:58	R$ 200,00
35723	22/05/2011 12:33	R$ 1.000,00
35723	22/05/2011 12:34	R$ 200,00
41897	22/05/2013 18:03	R$ 620,00
60544	22/05/2009 19:44	R$ 500,00
60544	22/05/2009 19:45	R$ 900,00
	EQUIPAMENTO Nº 41897	
	FRANGO ASSADO CAIEIRAS II	
	RODOVIA DOS BANDEIRANTES km , 34 NOVA CAIEIRAS	
	CAIEIRAS - SP CEP - 07721-000	
	EQUIPAMENTO Nº 35723	
	SUP ENXUTO LIMEIRA III	
	R COMENDADOR VICENTE LEONE, 200 JD N S DE FATIMA	
	LIMEIRA - SP CEP - 13482-376	
	EQUIPAMENTO Nº 60544	
	SUPERMERCADOS NAGUMO LOJA18	
	AV OLIVEIRA FREIRE, 480 PARQUE PAULISTANO	
	SAO PAULO - SP CEP - 08080-570	

Após o ocorrido, foram implementadas novas medidas de segurança para evitar tais fraudes novamente. Como, por exemplo:

- Implementação da utilização de DeviceID, onde bloqueia o uso de mais de um dispositivo móvel para acessar a conta e, caso ocorra a troca de aparelho, é necessário entrar em contato diretamente com o Banco Digital para informar e autorizar a troca do acesso.
- A possibilidade de pedidos de empréstimos por meio de contas-remuneração foi encerrada.
- Para ser feito um reset de senha, agora é necessário um código enviado por SMS e também por e-mail.
- Outras medidas organizacionais.

Plano para prevenção de novas ocorrências

A equipe sugere uma campanha dentro da empresa focada na conscientização a respeito do phishing , focando em alertar aos funcionários sobre como isso pode ser prejudicial não só para a empresa quanto para cada um de forma pessoal. Através do phishing, aqueles que mordem a isca podem acabar com suas informações pessoais roubadas, suas finanças comprometidas e sua privacidade invadida. Phishing chega geralmente disfarçado de e-mails, mensagens de texto ou até mesmo telefonemas fingindo ser de pessoas, ou empresas confiáveis. A seguir, um exemplo de campanha que pode ser compartilhado dentro da empresa usando-se da gestão de mudança (GMUD) a fim de garantir o sucesso desta iniciativa. Aqui está um plano básico seguindo os princípios da GMUD:

1. Avaliação Inicial:

Realizar uma análise detalhada do ambiente atual da organização em relação à segurança cibernética e à conscientização sobre phishing. Além de identificar lacunas e áreas de melhoria em termos de conhecimento, comportamento e práticas de segurança dos funcionários.

2. Definição de Objetivos:

Estabelecer objetivos claros e mensuráveis para a campanha de conscientização sobre phishing, como reduzir o número de cliques em e-mails de phishing em uma determinada porcentagem.

3. Engajamento da Liderança:

Garantir o apoio e a participação ativa da alta administração na campanha, comunicando a importância da segurança cibernética e a necessidade de conscientização sobre phishing para toda a organização.

4. Desenvolvimento de Recursos:

Criação de materiais de treinamento e conscientização de alta qualidade, incluindo vídeos, infográficos, e-mails simulados de phishing e folhetos informativos, adaptando os recursos para atender às necessidades específicas dos diferentes departamentos e níveis hierárquicos.

5. Treinamento e Capacitação:

Conduzir sessões de treinamento presenciais ou online para todos os funcionários, abordando conceitos básicos de segurança cibernética e estratégias para identificar e evitar ataques de phishing, fornecer orientações práticas sobre como relatar tentativas de phishing suspeitas.

6. Simulações de Phishing:

Realizar campanhas de e-mails simulados de phishing para avaliar a prontidão dos funcionários. E utilizar os resultados das simulações para identificar áreas adicionais de treinamento e conscientização.

7. Comunicação Contínua:

Manter uma comunicação regular e transparente sobre questões de segurança cibernética e phishing, sempre que possível, destacar exemplos reais de ataques de phishing e suas consequências para conscientizar os funcionários sobre os riscos.

8. Reforço Positivo:

Reconhecer e recompensar os comportamentos seguros dos funcionários, como relatar e-mails de phishing suspeitos, desta forma, criando uma cultura que valorize a segurança cibernética e a conscientização sobre phishing.

9. Avaliação e Melhoria Contínua:

Avaliar regularmente o progresso da campanha e o impacto nas métricas de segurança cibernética.

Utilizar feedback dos funcionários para aprimorar os materiais de treinamento e as estratégias de conscientização.

Conclusão

Proteger-se contra o phishing requer vigilância constante e educação. Reconheça os sinais. E-mails e mensagens de texto fraudulentos muitas vezes apresentam sinais de alerta, como erros de gramática, URLs suspeitas e pedidos urgentes para fornecer informações confidenciais. Ao estar ciente dos sinais de alerta e tomar medidas para verificar a legitimidade das comunicações online, você pode proteger suas informações pessoais e financeiras.

Desconfie de Pedidos Inesperados, empresas legítimas nunca solicitarão informações confidenciais por e-mail. Caso receba um pedido inesperado para fornecer informações pessoais ou financeiras, verifique diretamente com a empresa por meio de meios seguros.

Ao receber e-mail ou mensagens virtuais verifique os links antes de clicar, passe o mouse sobre ele para ver o URL completo. Se parecer suspeito ou não corresponder ao site esperado, não clique. Conserve-se antenado das informações mais relevantes sobre o tema, como também mantenha seu software, navegador e sistema operacional atualizados. Muitas vezes, as atualizações incluem correções de segurança importantes que podem protegê-lo contra ameaças de phishing.

Por fim, eduque-se e sempre que possível eduque outros, converse com amigos e familiares sobre os perigos do phishing e como reconhecê-lo. A educação é uma das melhores defesas contra essa ameaça. Não caia na isca do phishing - seja esperto, fique seguro!