

# ALERTA ISH PASSWORDSTEALER

# Campanha em curso de roubo massivo de credenciais por meio de spear phishing

ID: BS-001.03.2021 DATA: terça-feira, 27 de abril de 2021

**IN** 

### RESUMO

O time de *threat intelligence* da ISH identificou uma campanha em curso de roubo massivo de credenciais, realizado através de uma campanha de *spear phishing*.

## **VETOR INICIAL**

#### E-mail falso de cobrança

O vetor inicial de infecção é um e-mail falso de cobrança de grandes operadoras do Brasil. Ao acessar seu conteúdo, a vítima é direcionada para um PDF malicioso, que instala um Trojan voltado a roubo de senhas. Esse executável realiza injeção de código em processos de navegadores comuns, como Opera, Firefox, Google Chrome e Microsoft Edge. Hooks em dlls importantes do navegador alvo redirecionam o processador para a rotina maliciosa.

*****	***************************************
Hook mode: Usermode	
Hook type: Inline/Trampo	bline
Process: 3504 (firefox.e	exe)
Victim module: ntdll.dll	(0x77050000 - 0x771d0000)
Function: ntdll.dll!LdrL	oadDll at 0x7708eb1a
Hook address: 0x10af520	
Hooking module: firefox.	exe
Disassembly(0):	
0x7708eb1a e9010a028a	JMP 0x10af520
0x7708eb1f 83ec0c	SUB ESP, 0xc
0x7708eb22 a1d4f70777836	55fc00 MOV EAX, [0xfc65837707f7d4]
0x7708eb2b 53	PUSH RBX
0x7708eb2c 8b5d08	MOV EBX, [RBP+0x8]
0x7708eb2f 83c801	OR EAX, 0×1
Disassembly(1):	
0x10af520 55	PUSH RBP
0x10af521 89e5	MOV EBP, ESP
0x10af523 53	PUSH RBX
0x10af524 57	PUSH RDI
0x10af525 56	PUSH RSI
0x10af526 83e4f8	AND ESP, -0x8
0x10af529 83ec50	SUB ESP, 0x50
0x10af52c a110900e018b7c	11031 MOV EAX, [0x31107d8b010e9010]
0x10af535 e8	DB 0xe8
0x10af536 89	DB 0x89
0x10af537 44	DB 0x44
*****	***************************************

Figura 1: Hook

#### Evolução

Essa adquire logins e senhas salvas nos navegadores alvo, formata os dados e os insere em um arquivo de texto para exfiltração. Esses dados são encaminhados para um servidor de comando e controle (C2), onde são concentrados em uma lista com as credenciais obtidas de outras máquinas infectadas.



Figura 2: Registro em Memória

Devido à quantidade de e-mails enviados e ao fato dos atacantes se passarem por diversas operadoras de serviço de abrangência nacional, essa lista concentra um grande número de credenciais tanto para contas particulares como corporativas.

Mesmo sendo recomendada a utilização de versões mais atualizadas de browsers, é importante observar que esse ataque não depende da versão do navegador utilizado, uma vez que não se trata de *exploit* mas sim de injeção de *shellcode* em um processo legítimo.

Como maneira de evitar esse tipo de ataque, oriente sua equipe a não utilizar o e-mail corporativo em cadastros de serviços de qualquer natureza. Mensagens inesperadas na caixa corporativa devem ser ignoradas, com especial cuidado com aquelas que trazem links no corpo do texto.



Figura 3: Exemplo de email malicioso utilizado pelo Trojan

#### Maneiras de mitigar o ataque: Conscientização – Orientação de sua Força de Trabalho

Também instrua seus colaboradores a não salvar as credenciais em navegadores, uma vez que elas são facilmente acessíveis por técnicas maliciosas diversas. Como ação complementar, é possível desativar completamente a opção de salvar senhas para Chrome, Firefox e Internet Explorer via GPO. Para tanto, siga o guia abaixo:

# Maneiras de mitigar o ataque: Técnico - Desativando gerenciadores de senha do Chrome, Edge, Firefox, IE via GPO

Uma boa medida de segurança é a desativação do salvamento de senhas utilizados pelos navegadores de internet. Logo abaixo apresentamos um exemplo de como implementar uma política de grupo (GPO) que desabilite o gerenciador de senhas nativo dos navegadores abaixo. Isso evita que as senhas corporativas sejam salvas nos navegadores, bem como sincronizadas com contas pessoais e estejam disponíveis fora da corporação.

Apresentamos exemplos de aplicação para os navegadores abaixo. Lembrando que a presente recomendação deve ser adaptada a realidade de sua instituição por um especialista Microsoft:

- Edge
- Internet Explorer (IE)

- Chrome
- Firefox

#### Desabilitando o gerenciador de senha nativo no Edge via GPO

- 1. Faça login em um servidor Windows e abra o Editor de Política de Grupo;
- 2. Baixe os Modelos de Política do Edge, se ainda não o fez;
- 3. No Editor de Política de Grupo, crie um novo GPO para Edge Desabilite PWM;
- 4. Escolha o escopo desejado;
- 5. Clique com o botão direito no novo Objeto de Política de Grupo > Editar;
- No Editor de Gerenciamento de Política de Grupo, vá para Configuração do Usuário > Políticas > Modelos Administrativos > Microsoft Edge;
- 7. Defina as seguintes políticas:
  - a. Desativar a política Ativar Preenchimento Automático para endereços
  - b. Desative a política de Ativar Preenchimento Automático para cartões de crédito
  - c. Em "Gerenciador de senhas e proteção", desative a política Ativar salvar senhas no gerenciador de senhas
  - d. Opcionalmente, você pode ativar a política Desativar a sincronização de dados usando os serviços de sincronização da Microsoft
  - e. Depois de concluídas, as configurações do GPO ficarão assim:

r Configuration (Enabled)				
icies Idministrative Templates				
Microsoft Edge			hic	
Policy	Setting	Comment	The second se	
Disable synchronization of data using Microsoft sync services	Enabled			
Enable AutoFill for addresses	Disabled			
Enable AutoFill for credit cards	Disabled			
Microsoft Edge/Password manager and protection			hic	
Policy	Setting	Comment		
Enable saving passwords to the password manager	Disabled			

8. Certifique-se de que o link GPO esteja habilitado.

#### Testando a funcionalidade

- 1. No computador do usuário, abra um prompt de comando e digite gpupdate /force que solicitará um logout para concluir as novas configurações;
- 2. Abra o Edge e clique nos três pontos para configurações ... > Configurações > Senhas;
- 3. Certifique-se de que a opção "Oferecer para salvar senhas" esteja desativada e seja gerenciada pela organização;



- 4. Observe que 'Entrar automaticamente' ainda está marcado, porque no momento da redação deste guia, não havia configuração de política para desativá-lo;
- 5. Importante: Observe que quaisquer senhas salvas anteriormente no Edge não serão removidas e continuarão a ser mostradas ao usuário, mesmo com o preenchimento automático do Edge desativado.

#### Como desabilitar o gerenciador de senha nativo no Internet Explorer (IE) via GPO

- 1. Faça login em um servidor Windows e abra o Editor de Política de Grupo;
- 2. Crie um novo GPO chamado "IE Desabilite PWM";
- 3. Escolha o escopo desejado;
- 4. Clique com o botão direito no novo Objeto de Política de Grupo > Editar;
- No Editor de Gerenciamento de Política de Grupo, vá para Configuração do Usuário > Políticas > Modelos Administrativos > Componentes do Windows > Internet Explorer;
- 6. Defina os seguintes modelos de política:
  - Ative a política Desativar Preenchimento Automático para formulários
  - Desativar a política Ativar o recurso de preenchimento automático para nomes de usuário e senhas em formulários
- 7. Depois de concluídas, as configurações do GPO ficarão assim:

Lonriguration (Enabled)			hid
cies			Hide
Iministrative Templates			hide
			hide
Policy definitions (ADMX files) retrieved from the local comp	uter.		
Windows Components/Internet Explorer			
Windows Components/Internet Explorer			hide
Windows Components/Internet Explorer Policy	Setting	Comment	hide
Windows Components/Internet Explorer Policy Disable AutoComplete for forms	Setting Enabled	Comment	hide

8. Certifique-se de que o link GPO esteja habilitado.

#### Testando a funcionalidade

- 1. No computador do usuário, abra um prompt de comando e digite gpupdate /force que solicitará um logout para concluir as novas configurações;
- Abra o Internet Explorer e clique no ícone de engrenagem > Opções da Internet > guia Conteúdo > Configurações de preenchimento automático. Veja se as configurações de senha estão esmaecidas:

AutoComplete Settings	
AutoComplete lists possible matches f typed or visited before.	rom entries you've
Use AutoComplete for	
Address bar	
Browsing history	
Favorites	
E Feeds	
Use Windows Search for bet	ter results
Suggesting URLs	
Eorms and Searches	
User names and gasswords on fo	rms
Agk me before saving passw	ords
Manage Passwords	
Delete Aut	Complete history
Delete Auto	Complete history

#### Como desativar o gerenciador de senha nativo no Chrome via GPO

- 1. Baixe os modelos administrativos do Google Chrome aqui: https://support.google.com/chrome/a/answer/187202?hl=en
- Copie o arquivo ADMX ...
   DE pasta baixada 'policy\_templates \ windows \ admx \ chrome.admx & google.admx
   PARA C: \ Windows \ PolicyDefinitions
- 3. Copie o arquivo ADML

DE 'policy\_templates \ windows \ admx \ en-us \ chrome.adml & google.adml PARA C: \ Windows \ PolicyDefinitions \ en-us

- 4. Em um servidor Windows, abra o Editor de Política de Grupo
- 5. Crie um novo GPO chamado "Chrome Desabilite PWM"
- 6. Escolha o escopo desejado
- 7. Clique com o botão direito do mouse em Objeto de Política de Grupo > Editar
- Vá para Configuração do usuário > Políticas > Modelos administrativos > Google > Google Chrome
- 9. Edite as seguintes configurações:
  - a. Habilite a política de configurações de login do navegador, clique em Opções e selecione Desabilitar login do navegador
  - b. Desative a política de Ativar Preenchimento Automático para Endereços
  - c. Desative a política de Ativar Preenchimento Automático para cartões de crédito
  - d. Em "Gerenciador de Senhas", desative a política Ativar salvar senhas no gerenciador de senhas
- 10. Depois de concluídas, as configurações do GPO ficarão assim:

Configuration (Enabled)			
icies			
dministrative Templates			
Policy definitions (ADMX files) retrieved from the local con	nputer.		
Google/Google Chrome			
Policy	Setting	Comment	
Browser sign in settings	Enabled		
Browser sign in settings		Disable browser sign-in	
Policy	Setting	Comment	
Enable AutoFill for addresses	Disabled		
Enable AutoFill for credit cards	Disabled		
Google/Google Chrome/Password manager			
Policy	Setting	Comment	
Enable saving passwords to the password manager	Disabled		

11. Certifique-se de que o link GPO esteja habilitado

#### Testando a funcionalidade

- 1. No computador do usuário, abra um prompt de comando e digite gpupdate /force que solicitará um logout para concluir as novas configurações.
- 2. Abra o Chrome e clique no ícone do perfil no canto superior direito. Veja se o usuário não está conectado.



3. Abra o Chrome, clique nos três pontos ... > Configurações > Senhas . Veja se a oferta para salvar senhas está desmarcada e gerenciada pela organização.

← Passwords	Q Search passwords
Offer to save passwords	

#### Como desabilitar o gerenciador de senha nativo no Firefox via GPO

- 1. Faça login em um servidor Windows que você usa para gerenciar suas Políticas de Grupo.
- 2. Baixe o arquivo .zip de modelos de política do Firefox mais recente <u>https://support.mozilla.org/en-US/kb/customizing-firefox-using-group-policy-windows</u>

3. Copie o ADMX arquivo

DE pasta baixada 'policy\_templates\_v1 ## \ windows \ firefox.admx & mozilla.admx. PARA C: \ Windows \ PolicyDefinitions

4. Copie o arquivo ADML

DE 'policy\_templates \ windows \ en-us \ firefox.adml & mozilla.adml

PARA C: \ Windows \ PolicyDefinitions \ en-us

- 5. Abra o Editor de Política de Grupo
- 6. Crie um novo GPO chamado "Firefox Desativar PWM"
- 7. Escolha o escopo desejado
- 8. Clique com o botão direito na nova política de grupo > Editar
- 9. Abra Configuração do usuário > Políticas > Modelos administrativos > Mozilla > Firefox
- 10. Edite as seguintes políticas:
  - a. Desativar a política Desativar contas do Firefox
  - b. Desabilite a política Ofereça para salvar logins
  - c. Desative a política Oferecer para salvar logins (padrão)
  - d. Desative a política do Gerenciador de Senhas
- 11. Depois de concluídas, as configurações do GPO ficarão assim:

User Configura	ation (Enabled)			bide
Policies				hide
Administra	tive Templates			hide
Po	olicy definitions (ADMX files) retrieved from	the local computer.		
Mozilla	a/Firefox			hide
P	Policy	Setting	Comment	
D	isable Firefox Accounts	Disabled		
0	ffer to save logins	Disabled		
0	ffer to save logins (default)	Disabled		
P	assword Manager	Disabled		

12. Certifique-se de que o link GPO esteja habilitado.

#### Testando a funcionalidade

- 1. Faça login como um usuário que faz parte do escopo, abra a linha de comando e execute gpupdate / force.
- 2. Abra o Firefox e selecione Logins e senhas na barra de menu.
- 3. Certifique-se de que a mensagem "Página bloqueada" seja exibida.



## **RECOMENDAÇÕES FINAIS**

#### Firewall e Filtro Web

Por fim, mantenha-se atento a domínios e endereços IP suspeitos em logs de ferramentas como Firewall e Filtro Web, visto que esse ataque utiliza processos legítimos para alcançar o servidor de comando (*command & control*), não sendo suficiente inspecionar apenas o tráfego de aplicações que você julgar suspeitas.

Políticas de uso consciente dos ativos da corporação bem como a monitoração de uso de recursos corporativos bem como manter referências a estas ações na Política de Segurança da Informação são formas com eficácia abrangente em casos semelhantes a este.

Limitar os acessos administrativos somente a equipes especializadas deve ser uma prática dos administradores de rede e esquipes de segurança cibernética.

Implementação de soluções de análise de comportamento (UEBA - User and Entity Behavior Analytics) podem compor a suas soluções de segurança com resultados importantes, analisando comportamentos anômalos em seu ambiente.