BOLETIM DE SEGURANÇA

Usuários do OneDrive alvos em golpe de phishing que executa script malicioso do PowerShell

heimdall
security research
A DIVISION OF ISH

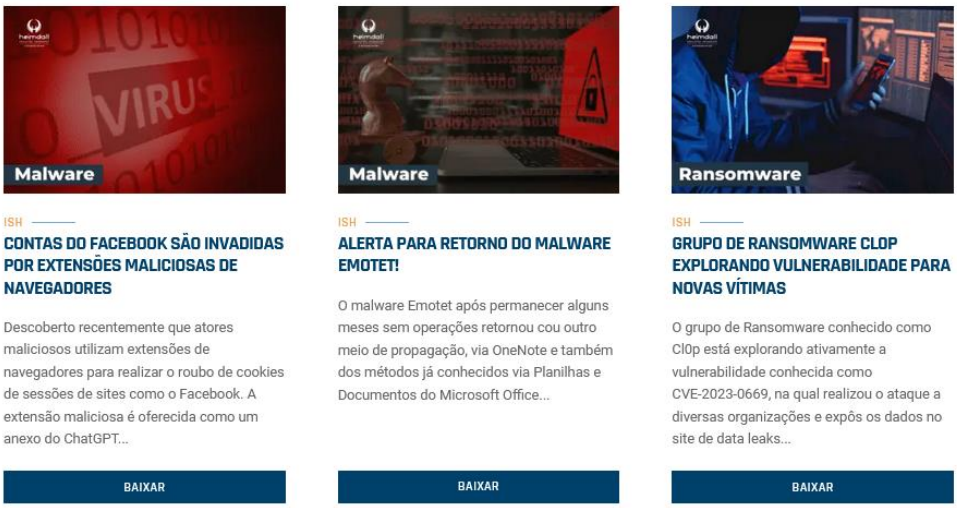
TLP: CLEAR

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

Especialistas em segurança cibernética alertam para uma recente campanha de phishing que mira usuários do Microsoft OneDrive, com a intenção de executar um script mal-intencionado do PowerShell.

2 INFORMAÇÕES SOBRE A AMEAÇA

A Trellix tem monitorado uma campanha de Phishing/downloader altamente sofisticada que visa usuários do Microsoft OneDrive nas últimas semanas. A campanha se baseia fortemente em táticas de engenharia social para enganar os usuários a executar um script do PowerShell, comprometendo seus sistemas. A campanha inicia persuadindo os usuários a clicar em um botão que supostamente orienta sobre como resolver um problema de DNS, aparentemente para permitir o acesso a um arquivo no Microsoft OneDrive. Esta estratégia utiliza a engenharia social ao explorar o senso de urgência do usuário e a expectativa de que o problema de DNS possa ser resolvido, permitindo o acesso ao documento desejado.

O ataque ocorre da seguinte maneira: a vítima recebe um e-mail contendo um arquivo .html. Ao abrir este arquivo .html, ele exibe uma imagem (Figura 1) projetada para criar um senso de urgência para acessar o documento, aumentando a probabilidade de o usuário seguir as instruções fornecidas. O uso de várias imagens é comum em campanhas de phishing, incluindo o uso de códigos QR. Esses elementos visuais são amplamente utilizados nesses ataques para enganar e manipular usuários. A imagem simula uma página do Microsoft OneDrive exibindo um arquivo chamado “Reports.pdf” e uma janela intitulada “Erro 0x8004de86” com a mensagem de erro: “Falha ao conectar ao serviço de nuvem ‘OneDrive’. Para corrigir o erro, você precisa atualizar o cache DNS manualmente.” Esta janela apresenta dois botões: “Detalhes” e “Como corrigir”. Notavelmente, o erro 0x8004de80 é um problema legítimo que pode ocorrer ao acessar o OneDrive.

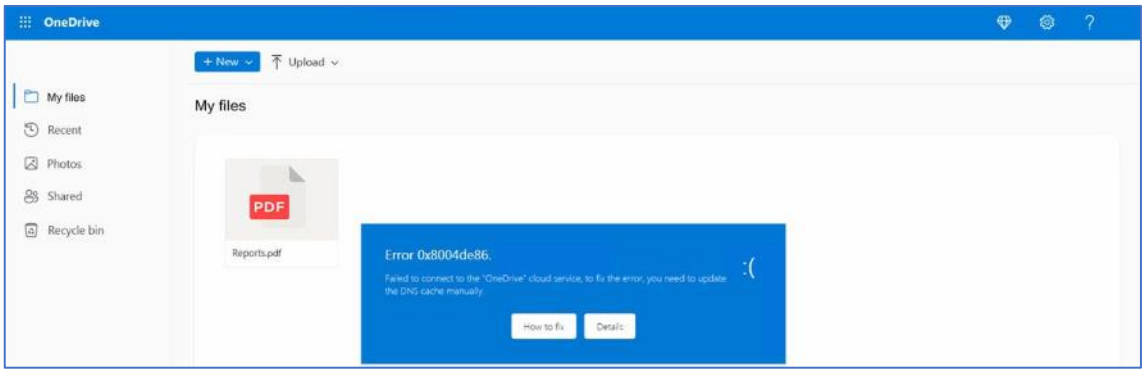


Figura 1 – Página do Microsoft OneDrive com "Erro 0x8004de86".

Ao clicar no botão “Detalhes”, o usuário é direcionado para uma página legítima do Microsoft Learn sobre “Solução de problemas de DNS”. No entanto, o botão “Como corrigir” aciona uma chamada de função GD dentro de um script .js incorporado no arquivo .html e também carrega instruções adicionais para o usuário seguir.

Esta combinação de jargão técnico e mensagens de erro urgentes é uma tática clássica de engenharia social, projetada para manipular as emoções do usuário e incitar ações precipitadas sem consideração cuidadosa.

```
<div id="buttons">
    <a href="#" class="white-button" onclick="GD()">How to fix</a>  
    <a href="https://learn.microsoft.com/en-us/windows-server/networking/dns/troubleshoot/troubleshoot-dns-server" target="_blank" class="white-button">Details</a>
</div>
```

Figura 2 – Ações associadas aos botões "Details" e "How to fix".

Neste ponto, o usuário recebe instruções específicas para abrir o menu Quick Link (Tecla Windows + X), acessar o terminal do Windows PowerShell, colar um comando e executá-lo. Uma inspeção mais detalhada da função GD.

```
function GD()
{
    var Jl = document.getElementById("hidden-content");
    Jl.style.display = "block";
    var ls = document.getElementById("dr");
    ls.select();
    document.execCommand("copy");
    window.getSelection().removeAllRanges();
}

$(document).ready(function()
{
    var ide = $(this).attr("title");
    var p3 = atob(ide);

    $("#dr").val(p3);
    $("#OL").css("display", "block");

    setTimeout(function()
    {
        $("#PZ").css("display", "none");
        $("#em").css("display", "block");
    }, 2000);

    $(document).on("click", function(event)
    {
        if(!$(event.target).closest("#OL").length)
        {
            alert('Failed to connect to the "OneDrive" cloud service');
        }
    });
});
```

Figura 3 – Detalhes da função GD.

Esta campanha demonstra como um simples ataque de engenharia social pode ter consequências devastadoras em um ambiente corporativo. Em um ambiente corporativo, o impacto de tal ataque pode se estender além de violações de dados individuais para incluir comprometimento generalizado da rede, perdas financeiras significativas e danos graves à reputação. Os funcionários, muitas vezes vistos como o elo mais fraco na segurança cibernética, podem inadvertidamente se tornar condutores de malware e outras cargas maliciosas por meio de esquemas de engenharia social cuidadosamente elaborados. Portanto, programas robustos de treinamento e conscientização de funcionários, juntamente com protocolos de segurança rigorosos, são essenciais para mitigar tais riscos.

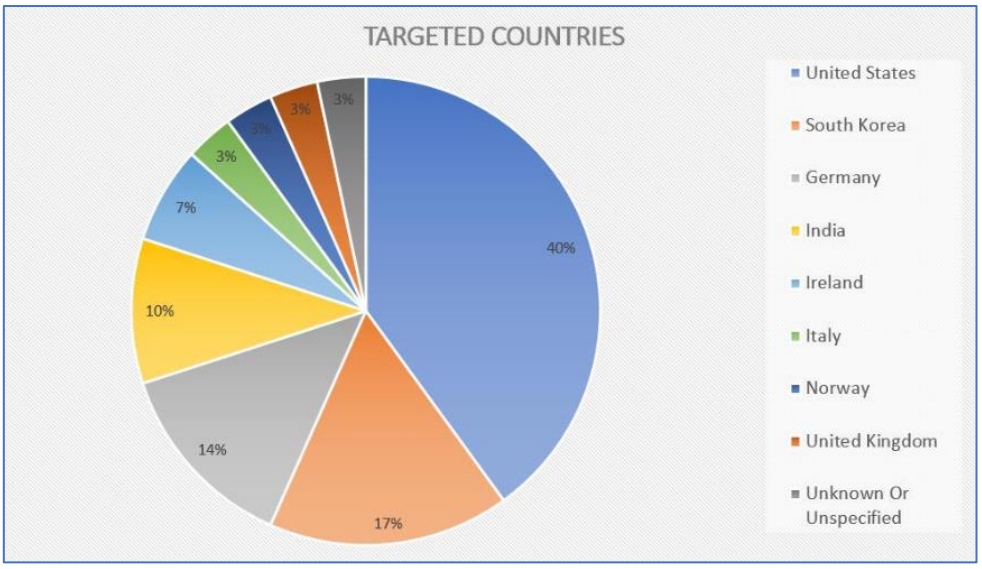


Figura 4 – Países alvo.

Essa ameaça destaca o perigo constante da engenharia social no mundo da segurança cibernética. Utilizando-se das emoções e da confiança dos usuários, os cibercriminosos conseguem penetrar até mesmo nos sistemas mais protegidos. As organizações precisam manter-se alertas, investindo continuamente na educação de seus colaboradores e fortalecendo as medidas de segurança para se protegerem contra ataques de tal sofisticação. A abrangência global desse ataque sublinha a importância da colaboração internacional e do intercâmbio de informações para combater de maneira eficaz essas ameaças.

3 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:

Verifique os e-mails com atenção

- Procure sinais reveladores de phishing, como erros de digitação, caracteres estranhos no texto e endereços de remetentes inconsistentes.

Links de e-mails desconhecidos

- Evite clicar em links enviados por e-mail, a menos que seja um que você tenha solicitado.

Monitoramento de contas regularmente

- Mantenha-se atualizado sobre as atividades em suas contas online.

Mantenha o seu navegador atualizado

- As atualizações do navegador geralmente incluem patches de segurança que podem protegê-lo contra ataques de phishing.

Cuidado com as janelas de pop-up

- Muitos ataques de phishing usam pop-ups como uma forma de coletar informações pessoais.

Não forneça informações pessoais via e-mail

- Os e-mails não são um meio seguro para compartilhar informações pessoais ou confidenciais.

Faça uma gestão inteligente de e-mails

- Esteja ciente de e-mails que apelam para emoções como medo ou urgência.

4 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:	04cdff477585cb0747ecd20052f03c2e
sha1:	8eae88d58b300613fc506b5b7e4cbcb083c5a0a9
sha256:	f3df02bf4d10415bfd8d33e0659c038465616e2190086a77dfbe0c73d229f68c
File name:	script.a3x

Indicadores de compromisso do artefato	
md5:	c56b5f0201a3b3de53e561fe76912bfd
sha1:	2a4062e10a5de813f5688221dbeb3f3ff33eb417
sha256:	237d1bca6e056df5bb16a1216a434634109478f882d3b1d58344c801d184f95d
File name:	AutoIt3.exe

Indicadores de compromisso do artefato	
md5:	763d557c3e4c57f7d6132a444a930386
sha1:	77aaf9c8b944f7178067430aef42f60a2ac1f41c
sha256:	5316fc2cb4c54ba46a42e77e9ee387d158f0f3dc7456a0c549f9718b081c6c26
File name:	unknown

Indicadores de compromisso do artefato	
md5:	d0ad617ed1812822eebc9592d49a575c
sha1:	f1ea42688227d5ed1c0e0c6c4b5cbd518a95ffaf
sha256:	7d7c6953c3918487997038fa8b53e369ee2fa7a0e23731fa823f1dc3d574f784
File name:	1.zip

Tabela 1 – Indicadores de Compromissos de artefatos

Indicadores de URL, IPs e Domínios

Indicadores de URL, IPs e Domínios	
URL	hxxps://kostumn1[.]ilabserver[.]com

Tabela 2 – 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.

5 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- Trellix
- Thehackernews

6 AUTORES

- **Leonardo Oliveira Silva**

heimdall
security research
A DIVISION OF ISH