heimdall

security research

A DIVISION OF ISH

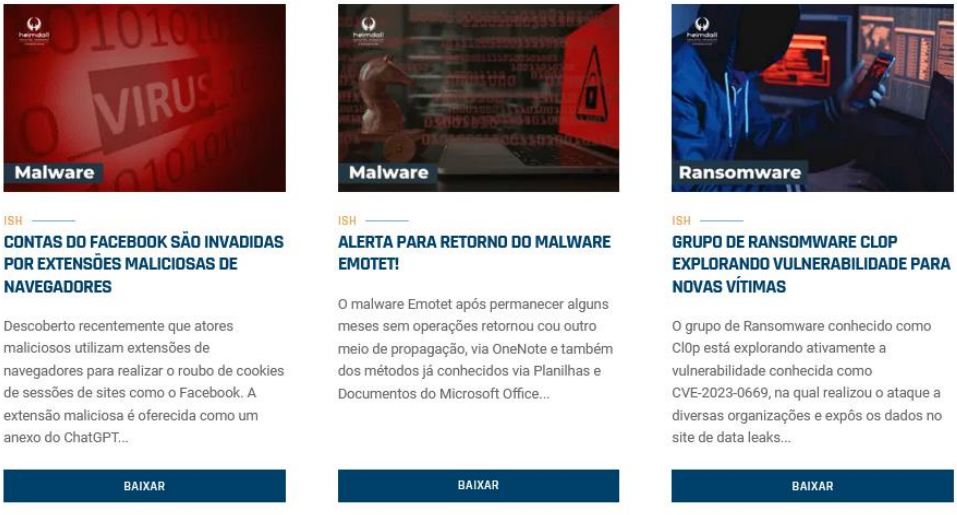
Tipos de ataques cibernéticos comuns em 2023

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 Figuras

1 Ataque Cibernético

Podemos considerar que um **ataque cibernético é um tipo de ação maliciosa** praticada por indivíduos, grupos ou organizações que visam explorar alguma vulnerabilidade em sistemas computacionais com o objetivo de comprometer, danificar, roubar informações ou interromper o funcionamento deste tipo de sistema. Vale salientar que os ataques de cibercriminosos são possíveis devido a erros humanos ou vulnerabilidades em erros de software.

Esses ataques podem ter diversos tipos de motivações, como ganho financeiro, espionagem, ativismo político, vandalismo digital ou simplesmente para ocasionar algum tipo de perturbação.

Como forma de exemplificar, a equipe de inteligência da ISH, Heimdall produziu este boletim para apresentar alguns dos tipos de ciber ataques comuns em 2023.

2 TIPOS DE ATAQUES

- **Ataques de Malwares**

Malware ou "Software Malicioso" é mencionado frequentemente em diversas notícias ou alertas publicados por organizações, pois para os ataques de malwares podem incluir a distribuição de: vírus, Worms, trojans e ransomwares, os quais podem infectar dispositivos e sistemas para roubar informações, danificar dados ou até mesmo exigir algum tipo de resgate financeiro.

Como exemplo, temos o malware do tipo worm conhecido como ILOVEYOU o qual veio a infectar milhões de máquinas Microsoft Windows após o seu lançamento. Vale salientar que o ILOVEYOU não foi o primeiro ataque de malware desenvolvido, porém, foi considerado um dos mais memoráveis.

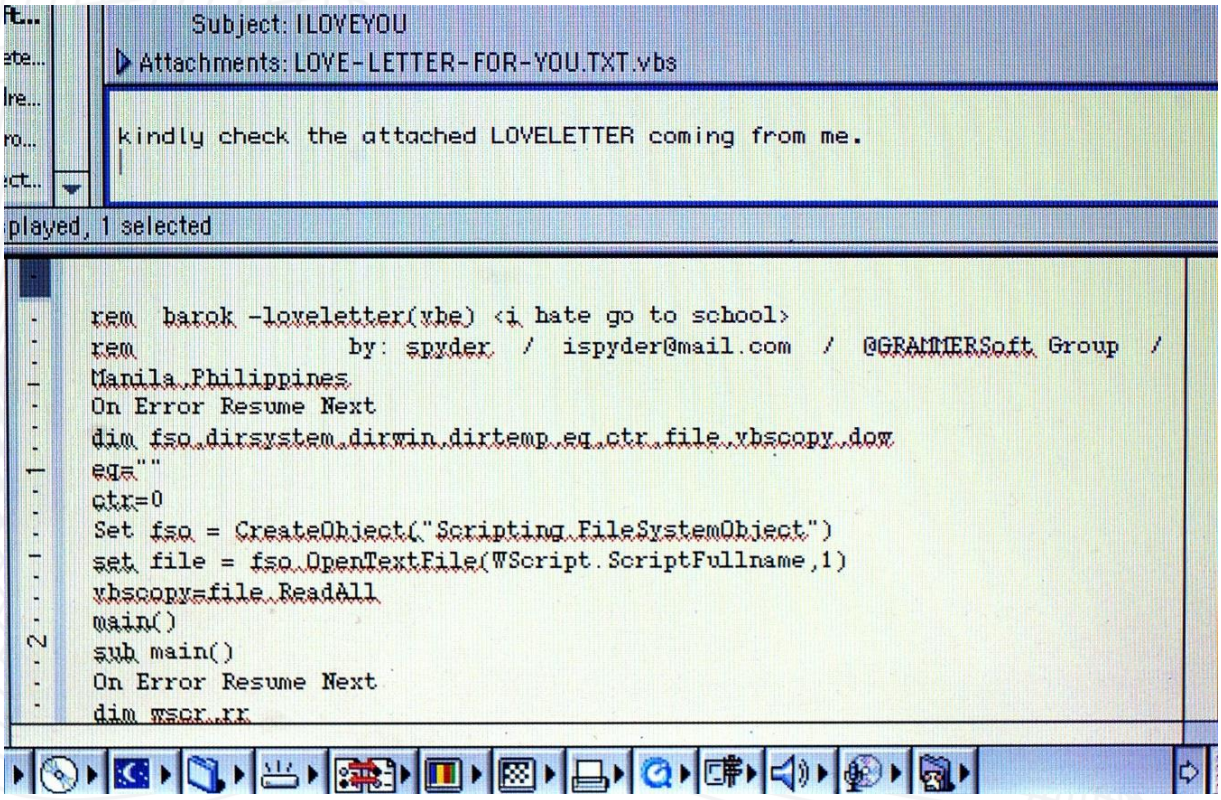


Figura 1 – Malware ILOVEYOU.

- **Ataques de Phishing**

Os ataques de phishing são considerados ataques produzidos e enviados por cibercriminosos contendo conteúdos de mensagens fraudulentas, ocorrendo através de e-mails, com o foco principal de enganar os destinatários ou alvos para que estes acabem fornecendo informações pessoais, credenciais, números de cartões de créditos e outras informações que podem ser relevantes para o cibercriminoso.

Figura 2 – Simulação de ataque phishing.

- **Ataques de Negação de Serviço (DDoS):**

Neste tipo de ataque, o cibercriminoso direciona diversos dispositivos infectados a realizar requisições a determinados sistemas, ou seja, tais sistemas são inundados com tráfego excessivo, tornando-os incapazes de atender às solicitações legítimas dos usuários, resultando na interrupção do serviço.

Como exemplo, podemos mencionar a botnet Mirai, a qual foi uma das maiores botnets já criadas por atores maliciosos, os quais infectaram sistemas executados em processadores ARC, transformando-os em uma rede de bots ou zumbis.

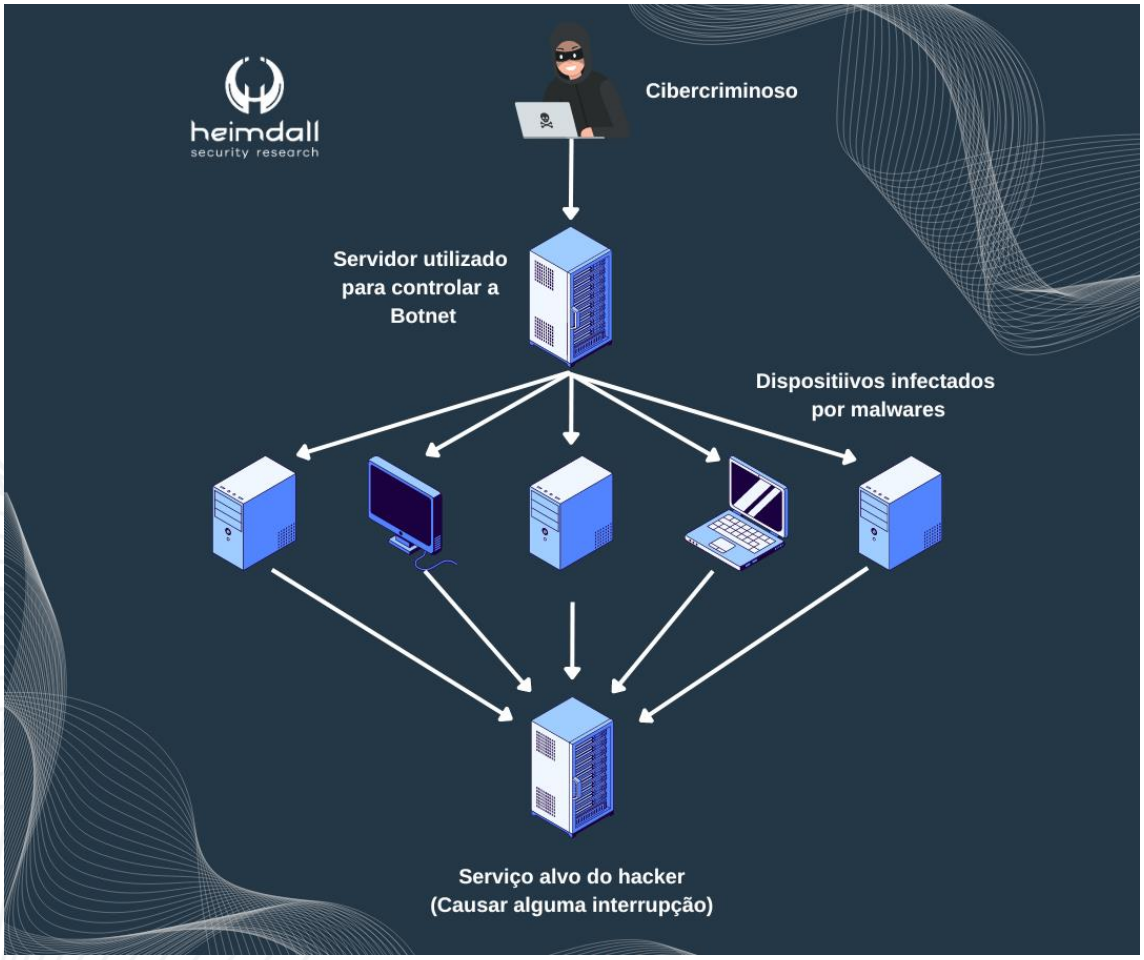


Figura 3 – Exemplificação de um ataque DDoS e uma Botnet.

- **Man-in-the-Middle (MitM)**

Os ataques MitM, é considerado um tipo de ataque cibernético na qual um ataque intercepta e monitora a comunicação entre duas partes, sem que ambas as partes saibam disso.

Neste tipo de ataque o cibercriminoso se posiciona entre as vítimas e intercepta ou modifica a comunicação, podendo ler, alterar ou até mesmo injetar novos dados no fluxo de informações.

O ataque Man-in-the-Middle pode ser realizado de várias maneiras, como:

- **Redirecionamento de tráfego:** o ataque pode redirecionar o tráfego de rede através de técnicas como ARP spoofing ou DNS spoofing, fazendo com que a vítima se comunique diretamente com o atacante.

- **Interceptação de redes Wi-Fi não seguras:** Em redes Wi-Fi não seguras, um cibercriminoso pode facilmente se infiltrar entre o dispositivo da vítima e o ponto de acesso, interceptando toda a comunicação.
- **Ataques de certificados:** Em conexões seguras (HTTPS), um atacante pode falsificar certificados digitais para fingir ser um servidor legítimo, permitindo a interceptação de dados criptográficos.

• Ataques de Senhas

Os ataques de senhas podem ser considerados um tipo de ataque cibernético que têm como alvo as credenciais de autenticação, como nomes de usuários e senhas, utilizadas para acessar contas online e sistemas.

Os cibercriminosos buscam obter acesso não autorizado a contas pessoais, redes corporativas, serviços online e outros sistemas, explorando vulnerabilidades nas práticas de segurança ou utilizando técnicas específicas.

A seguir, listamos alguns dos ataques comuns de senhas:

- **Ataques de Força Bruta:** um cibercriminoso tenta todas as combinações possíveis de senhas até encontrar a correta. Isso é mais eficaz quando as senhas são fracas e curtas.
- **Ataques de Dicionário:** o cibercriminoso utiliza uma lista de palavras comuns ou senhas populares para tentar adivinhar a senha correta. Essa é a abordagem mais rápida do que a força bruta, pois se concentra em senhas mais prováveis de serem usadas.
- **Ataques de Força Bruta:** os cibercriminosos utilizam algoritmos para ajustar as tentativas de senha para realizar o login em diversas contas ou uma conta específica.
- **Roubo de dados:** Quando ocorre algum tipo de vazamento de dados, os ataques podem obter acesso às informações de login de usuários e, em seguida, tentar usar essas credenciais em outras contas que possam pertencer à mesma pessoa.

- **Ataques de Injeção**

Neste tipo de ataque, o cibercriminoso insere códigos maliciosos em sistemas, aplicativos ou banco de dados, explorando falhas de segurança para executar ações não autorizadas.

Como exemplo, o SQL (Structured Query Language) é uma linguagem comum usada para interagir com banco de dados, na qual o cibercriminoso injeta código SQL malicioso nas entradas do usuário, que então é executado pelo banco de dados do aplicativo. Por meio desse ataque, o invasor obtém acesso não autorizado ao banco de dados SQL.

3 OUTROS TIPOS DE ATAQUES CIBERNÉTICOS

Neste boletim, mencionamos alguns dos principais tipos de ataques cibernéticos, sendo que existem diversos outros. Lembrando ainda que existem variações de ataques que foram mencionados neste alerta, coo por exemplo Ataques de Ransomwares, Spear-Phishings e outros.

Portando, é de suma importância estar atento sobre todos os tipos de ataques cibernéticos que estão sendo utilizados pelos atores de ameaças (cibercriminosos), visto que podem prejudicar o funcionamento de uma organização, ocasionando prejuízos financeiros e reputacional.

4 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**

heimdall
security research

A DIVISION OF ISH