**Pontifícia Universidade Católica do Rio de Janeiro (PUC-Rio)**

**Departamento de Informática (DI)**

**Disciplina: INF1416 - Segurança da Informação**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

Trabalho 5 - IoT Botnets (Mirai)

Integrantes: Felipe Ferreira (1711087) e Sérgio Gabriel (1611200)

**I. Introdução**

O ano de 2016 foi marcante para o universo da segurança cibernética, com o surgimento da botnet Mirai. Capaz de gerar ataques de negação de serviço em uma escala nunca vista anteriormente, por meio da exploração de dispositivos vulneráveis de Internet das Coisas (IoT), este malware rapidamente tornou-se uma ameaça. Seu código fonte foi liberado na rede por seu criador e então, mais ainda, seu impacto se consolidou de forma ainda permanente, com o surgimento de variantes suas, transformando-se no mais novo problema a ter que ser mitigado. Este trabalho tem como propósitos explorar o funcionamento deste malware e estabelecer uma melhor preparação para ataques como este no futuro.

**II. Descrição**

O Mirai é um malware que transforma sistemas de computador que executam uma versão simplificada do Linux, chamada ARC, em bots (ou “zumbis”) controlados remotamente, que poderão ser usados como parte de um botnet em ataques de rede em larga escala. Ele visa, obviamente, dispositivos que realizam comunicação com a Internet, como câmeras inteligentes, roteadores, termostatos e entre outros.

O ataque em questão consiste em lotar o alvo com mensagens SYN e nunca confirmar com ACK, consumindo os recursos do alvo que, a cada SYN recebido, aloca buffers para atender a futura conexão. Assim, produz um ataque TCP SYN flood a partir de diversos dispositivos/hosts. O objetivo neste ataque é consumir banda na rede do alvo tornando-o

inacessível, e, com isso, inoperante.

O mirai possui outros 9 tipos de ataque, que possuem o mesmo objetivo do SYN flood, porém utilizando outras mensagens, como ACK, UDP, etc.

O Mirai é um malware que infecta dispositivos IoT que são usados como plataforma de lançamento para ataques DDoS. É classificado como um worm, que utiliza a rede como forma de disseminação, e que faz uso de um ataque externo, ativo e indireto: é iniciado no lado de fora do perímetro de segurança por um usuário não autorizado, muda a operação e o estado do sistema e a entidade hostil comanda terceiros na execução dos ataques à(s) vítima(s) fazendo com que o fluxo de dados malicioso seja direcionado à(s) vítima(s) pelos terceiros.

**III. Forma de execução do ataque**

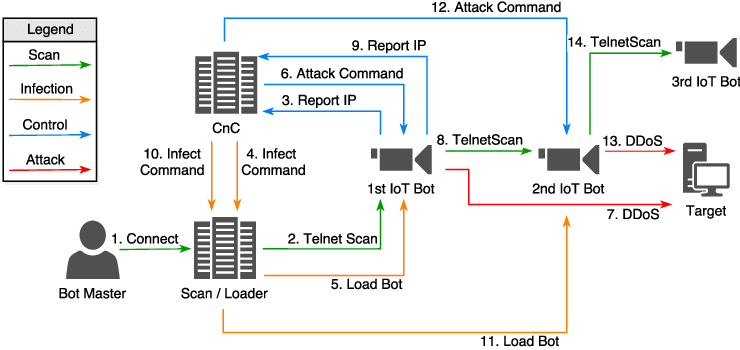
A ideia dos criadores desse flooder é aproveitar a vulnerabilidade dos dispositivos de consumo, no que diz respeito às credenciais de acesso: muitos dispositivos vêm com nomes de usuário e senhas padrão e permanecem assim.

Um invasor (botmaster) inicia o processo conectando-se ao servidor Scan/Loader e iniciando o loader para executar o módulo scanner.c e varrer a Internet em busca de dispositivos IoT vulneráveis com serviços Telnet e portas 23 ou 2323 abertas.

Ao detectar um dispositivo vulnerável, o malware tenta forçar um login bem-sucedido usando uma lista de 62 nomes de usuário e senhas padrão conhecidos. Se for bem-sucedido, as credenciais de login e as informações do dispositivo são enviadas de volta ao servidor C&C e serão usadas posteriormente pelo servidor Scan/Loader para fazer login e entregar o malware ao dispositivo vulnerável. Um comando infect é enviado do servidor C&C para o Scan/Loader server contendo todas as informações necessárias, como detalhes de login, endereço IP, arquitetura de hardware. O Mirai suporta várias arquiteturas de hardware, incluindo arm, mips, sparc e powerpc.

O servidor Scan/Loader usa essas informações para fazer login e instruir o dispositivo vulnerável a baixar e executar o binário de carga útil correspondente. Uma vez executado, o primeiro dispositivo IoT infectado torna-se parte da botnet Mirai e pode se comunicar com o servidor C&C. O binário do malware é removido e executado apenas na memória para evitar a detecção. O botmaster agora pode emitir comandos de ataque, especificando parâmetros como duração e, finalmente, o alvo do ataque.

O primeiro bot agora tenta repetir o processo de infecção e propagar a botnet varrendo a Internet em busca de outros dispositivos IoT vulneráveis adicionais com serviços Telnet e portas 23 e 2323 abertas. As novas informações do dispositivo vulnerável IoT são retornadas ao servidor C&C. Um novo comando infect é emitido para o servidor Scan/Loader. O binário de hardware apropriado é carregado no dispositivo IoT vulnerável recém-descoberto. O comando de ataque relevante é emitido ao servidor C&C. O ataque é executado no segundo bot recém-infectado, em conjunto com o primeiro bot. A verificação de dispositivos IoT vulneráveis adicionais é repetida para expandir mais ainda a botnet.

****

**IV. Prevenção e Mitigação**

A arquitetura IoT define quatro camadas principais de percepção, rede, middleware e camada de aplicação. A segurança deve ser implementada em todas as camadas para mitigar efetivamente as ameaças à segurança da IoT, o que não vem sendo feito pelas empresas que desenvolvem tais dispositivos.

Anti-vírus é uma ferramenta de segurança tradicional implantada no ambiente de desktop para se defender contra várias ameaças. Ele usa o método de lista negra baseado em assinatura, onde aplicativos ruins têm acesso negado ao sistema e todos os outros aplicativos podem ser executados livremente. A principal desvantagem desse método é que as assinaturas precisam ser atualizadas continuamente e também não protegem contra ataques de dia zero. Portanto, a maioria dos softwares antivírus adota uma abordagem heurística para detectar ataques de dia zero que resultaram no aumento de falsos positivos.

Outro método alternativo de prevenção é a lista branca (“whitelisting”), que permite que aplicativos autorizados estejam presentes no sistema e bloqueia todos os aplicativos não autorizados. Baixo custo de manutenção, baixo banco de dados de impressão digital de aplicativos de whitelisting, baixa sobrecarga e atualização ocasional do banco de dados torna uma abordagem de whitelisting, solução de segurança perfeita para domínio IoT. A lista de permissões de aplicativos já é usada como a solução eficaz em sistemas de automação e controle industrial.

Embora os ataques DDoS de botnets Mirai possam ser mitigados, não há como evitar ser alvo. No entanto, há como tornar o espaço digital mais seguro para os usuários de dispositivos IoT, caso seu dispositivo esteja reconhecidamente vulnerável.

A principal prioridade deve ser alterar as chaves de login da configuração de fábrica e criar uma senha forte, usando um gerador de senhas aleatórias.

Outra boa prática de mitigação desse ataque é a verificação das portas SSH(22), HTTP/HTTPS(80/443) e, principalmente, as Telnet(23) e Telnet(2323).

Se for caso de perceber algum sinal desse malware, para removê-lo de um dispositivo IoT infectado, os usuários e administradores devem realizar as seguintes ações. Primeiro, desconecte o dispositivo da rede. Segundo, enquanto estiver desconectado da rede e da Internet, execute uma reinicialização. Como o malware Mirai existe na memória dinâmica, a reinicialização do dispositivo limpa o malware. Terceiro, realize a alteração da senha de acesso ao dispositivo.

O usuário somente poderá se reconectar à rede após a realização dos passos acima. Caso o dispositivo seja reconectado antes de alterar a senha, ele poderá ser reinfectado rapidamente pelo malware Mirai.

**V. Referências**

[1]<https://www.avast.com/c-mirai>

[2]<https://malwiki.org/index.php?title=Mirai>

[3]<https://www.kaspersky.com/resource-center/threats/secure-iot-devices-on-your-home-network>

[4]<https://www.techrepublic.com/article/distributed-denial-of-service-ddos-attacks-a-cheat-sheet/>

[5]<https://www.cloudflare.com/pt-br/learning/security/glossary/iot-security/>

[6]<https://www.cloudflare.com/pt-br/learning/ddos/glossary/mirai-botnet/>

[7]<https://www.imperva.com/blog/malware-analysis-mirai-ddos-botnet/>

[8]<https://www.cisa.gov/uscert/ncas/alerts/TA16-288A>

[9]<https://www.researchgate.net/publication/329316466_Towards_Situational_Awareness_of_Botnet_Activity_in_the_Internet_of_Things#pf2>

[10]<https://www.researchgate.net/figure/Mirai-Botnet-Infection-Methodology_fig1_329316466>

[11]<https://ieeexplore.ieee.org/document/8554643>