Instituto Nacional de Telecomunicações

Mestrado em Telecomunicações
TP546 - Internet das Coisas e Redes Veiculares.

RELATÓRIO DA ATIVIDADE Nº03

Segurança em dispositivos IoT

Alunos:
Eylen Jhuliana Mercado Ontiveros
Everton Vilhena Cardoso

Eylen Jhuliana Mercado Ontiveros
Everton Vilhena Cardoso

RELATÓRIO DA ATIVIDADE Nº02

Segurança em dispositivos IoT

10 de outubro, 2024

1 Resumo

A segurança em redes IoT podem ser abordados por meio de medidas preventivas. A conscientização sobre as vulnerabilidades e a implementação de controles adequados são passos fundamentais para proteger os dispositivos IoT e garantir a continuidade dos serviços que dependem dessa tecnologia. Este relatorio busca apresentar um dos problemas de segurança mas comunes em redes IoT tais como o Malware Mirai e as medidas eficazes para mitigá-lo.

2 Introdução

A Internet das Coisas (IoT) está transformando diversos setores ao conectar dispositivos e sistemas em uma vasta rede de comunicação, desde eletrodomésticos até infraestruturas críticas em saúde, transporte e indústrias. Ao permitir a comunicação e automação em larga escala, a IoT oferece benefícios como maior eficiência, controle em tempo real e redução de custos operacionais. No entanto, essa conectividade global também introduz sérios desafios relacionados à segurança cibernética. Com milhões de dispositivos conectados e frequentemente distribuídos, a IoT se torna um alvo crescente para cibercriminosos que buscam explorar vulnerabilidades.

O portal Statista [i] prevê que os dispositivos IoT (routers, câmaras, caixas NAS e componentes domésticos inteligentes) multiplicam-se todos os anos. O número ultrapassará os 29 bilhões até 2030. À medida que o número de dispositivos ligados aumenta, aumenta também a necessidade de proteção contra várias ameaças.

Os dispositivos IoT, muitas vezes com capacidades limitadas de processamento e armazenamento, não possuem mecanismos robustos de segurança, o que abre caminho para uma série de ataques cibernéticos, como ataques de autenticação fraca, falta de criptografia robusta, e a incapacidade de realizar atualizações de software frequentes.

Existem diferentes tipos de ataques, sendo que um dos mais comuns são os Ataques de Negação de Serviço Distribuído (DDoS) visa sobrecarregar um dispositivo ou uma rede com um volume excessivo de tráfego, tornando o serviço indisponível para seus usuários legítimos. Um exemplo famoso foi o ataque da botnet Mirai, que sequestrou câmeras e roteadores IoT para lançar um grande ataque DDoS, causando interrupções em serviços da internet em 2016. Ataques DDoS continuam sendo uma das principais ameaças devido à facilidade com que os dispositivos IoT podem ser usados como "zumbis"para gerar tráfego malicioso. Este trabalho tem como objetivo focar em no ataque da botnet Mirai, apresentando como um ataque pode ser realizado e as medidas eficazes para mitigá-lo.

3 Desenvolvimento

3.1 Introdução ao malware Mirai

Com o crescente interesse no potencial da IoT e dispositivos conectados, os atacantes encontraram oportunidades para explorar esses dispositivos. Segundo Kolias, C. et al.(2017), novos malwares e botnets (ou seja, uma rede de dispositivos ou robôs interconectados que são controlados por um atacante através de um servidor de Comando e Controle (C&C)) estão sendo especificamente desenvolvidos para atacar dispositivos IoT. O BASHLITE [v] foi um desses primeiros malwares usados para infectar dispositivos IoT. Outro software malicioso conhecido como Mirai, sendo a botnet IoT mais estudada, utilizada para criar ataques de negação de serviço distribuídos (DDoS) com picos de tráfego avançados, reportados até 1 Tbit.

Em setembro de 2016, o Mirai foi usado para criar enormes botnets que atacaram simultaneamente sites e provedores de serviços de grande porte, por exemplo:.

- Ataque DDoS potente em IoT aproveita código-fonte publicado [iv]
- Ataque DDoS de 1 Tbit atinge a OVH [1]
- Ataque DDoS utiliza Mirai
- Ataque DDoS com pico de tráfego não divulgado atinge a Dyn [2]
- Criminosos cibernéticos recebem penas de prisão
- Ataque DDoS de 620 Gbits reportado pelo proprietário

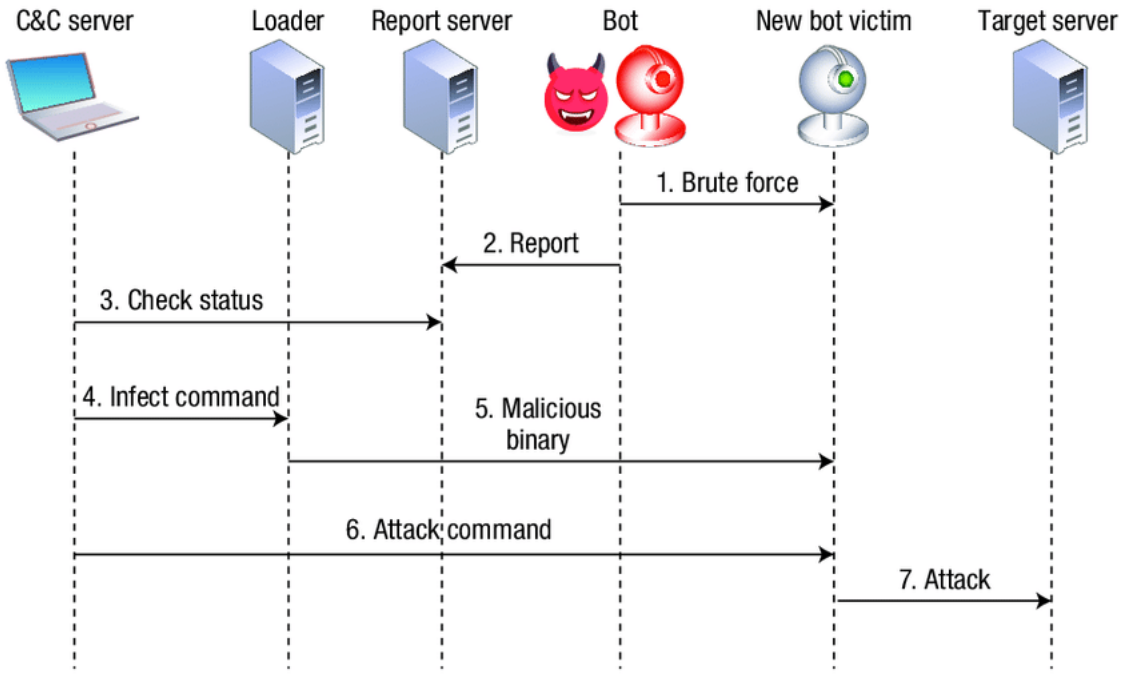
Esses eventos foram divulgados até mesmo em sites que não são focados em segurança, pois levantaram questões sobre a segurança dos dispositivos IoT, especialmente porque a maioria dos dispositivos IoT infectados eram sistemas de segurança residencial voltados para o consumidor.

3.2 Funcionamento do botnet Mirai

A parte mais desafiadora no ataques, foi que o Mirai não utilizou algo especial para infectar os dispositivos IoT, ele usou uma simples técnica de força bruta com uma lista predefinida de credenciais padrão para vários dispositivos IoT. Probes TCP SYN foram enviados para endereços IPv4 aleatórios (exceto redes privadas e certos sub-redes) nas portas TCP 23 e 2323 do Telnet e caso houvesse uma resposta dos dispositivos pingados, ele tentaria fazer login usando as credenciais padrão e, se bem-sucedido, reportaria as credenciais a um servidor C&C. Um arquivo de varredura seria então baixado do servidor para descobrir a arquitetura subjacente e, finalmente, o malware Mirai apropriado seria executado e aguardava comandos de ataque do servidor.

[2]Provedor francês de hospedagem.
[2]Provedor de serviços DNS.

Figura 1: Comunicação e operação da botnet Mirai.



Fonte: Extraído de Kolias et al. (2017)

Os dispositivos infectados ainda funcionavam como esperado, com alguns problemas ocasionais de recursos que os faziam parecer lentos, de modo que seus usuários não conseguiam detectar que havia algo errado com seus dispositivos. Uma vez que os alvos foram escolhidos, eles receberam comandos de ataque do servidor C&C e iniciaram os ataques DDoS, que eram difíceis de mitigar, já que provinham de dispositivos com muitos endereços IP diferentes. Segundo Antonakakis et al. (2018), o número de dispositivos infectados pelo Mirai atingiu um total de 600.000.

3.3 Medidas de mitigação

Behal, S., et al.(2017) demostra que inicialmente uma solução simples para mitigar o malware, foi reiniciar os dispositivos IoTs infectados e mudar as credenciais de login, mas a maioria dos usuários não estavam conscientes do problema, e muitos fornecedores não se preocupavam em corrigir os dispositivos para torná-los mais seguros, que frequentemente não tinham os recursos necessários ou capacidades para atualizar.

Para mitigar o risco de infecção pelo Mirai e outros malwares semelhantes, podem ser tomadas medidas como:

- Alterar senhas padrão e usar senhas fortes

  O malware Mirai se propagou explorando credenciais padrão ou fracas que são frequentemente deixadas sem alteração em dispositivos IoT. Alterar as senhas padrão por senhas únicas e complexas em cada dispositivo é uma das medidas mais básica e mas eficazes, para impedir o acesso não autorizado.

- Atualizações regulares de firmware

  Muitos dispositivos IoT são vulneráveis porque os fabricantes não liberam atualizações frequentes ou os usuários não aplicam as atualizações de firmware disponíveis. Manter o firmware dos dispositivos IoT atualizado é crucial para corrigir vulnerabilidades de segurança conhecidas.

- Desabilitar serviços desnecessários

  Muitos dispositivos IoT vêm com serviços e portas abertas que não são utilizados, o que pode ser um ponto de entrada para o malware. Desativar ou bloquear serviços e portas desnecessários, como Telnet e SSH, pode reduzir a superfície de ataque.

- Usar firewalls e segmentação de rede

  Proteger a rede onde os dispositivos IoT estão conectados é fundamental. O uso de firewalls pode ajudar a bloquear tráfego suspeito e impedir que dispositivos comprometidos comuniquem-se com servidores de comando e controle (C&C). Além disso, segmentar os dispositivos IoT em uma sub-rede separada ou usar redes virtuais (VLANs) pode limitar o impacto de uma infecção ao isolar esses dispositivos da rede principal.

- Monitoramento e detecção de anomalias

  Implementar soluções de monitoramento de rede pode ajudar a detectar comportamentos anômalos que possam indicar uma infecção por malware, como picos no tráfego de rede ou tentativas de comunicação com servidores externos desconhecidos. Ferramentas de detecção de intrusões (IDS) podem ser úteis nesse cenário, permitindo uma resposta rápida a ameaças em potencial.

4 Conclusão

A segurança em redes IoT é um desafio contínuo, mas técnicas avançadas de detecção e medidas de controle podem ajudar a mitigar os riscos associados a ataques.

A proliferação de dispositivos IoT trouxe inúmeros benefícios, mas também introduziu novos desafios de segurança cibernética. Este trabalho destaca a gravidade dos ataques da botnet Mirai, que exploram vulnerabilidades comuns em dispositivos IoT para realizar ataques de negação de serviço distribuídos (DDoS). Esses ataques não apenas comprometem a funcionalidade dos dispositivos, mas também podem causar interrupções significativas em serviços críticos.

A Mirai botnet exemplifica como a falta de medidas de segurança robustas pode ser explorada por atacantes. Dispositivos com autenticação fraca, baixo poder de processamento e falta de atualizações são alvos fáceis. Esse malware se aproveita dessas fraquezas para se propagar rapidamente e recrutar dispositivos IoT em sua rede tornando a maliciosa.

Para mitigar esses riscos é apresentada várias medidas de mitigação. A implementação de autenticação forte, como senhas complexas e autenticação multifator, é essencial para proteger dispositivos IoT. Além disso, garantir que os dispositivos recebam atualizações regulares de firmware pode corrigir vulnerabilidades conhecidas e prevenir ataques. O monitoramento contínuo da rede é outra medida crucial, que permite a detecção precoce de atividades suspeitas e a resposta rápida a incidentes de segurança.

Conhecer sobre as vulnerabilidades e a implementação de controles adequados é fundamental para garantir a continuidade dos serviços que dependem dessa tecnologia e proteger os dispositivos IoT.

5 Referências bibliográficas

(i) Lionel Sujay Vailshery, "Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025," statista.com, Jun. 2024. https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/.

(ii) Vitaly Morgunov, "Overview of IoT threats in 2023," securelist.com, Sep. 21, 2023. https://securelist.com/iot-threat-report-2023/110644/.

(iii) Roberta Prescott, "Devido à negligência de fabricantes com segurança, crescem ataques DDoS providos a partir de IoTs" Abranet - Associação Brasileira de Internet, Dez. 05, 2016. https://www.abranet.org.br/Noticias/Devido-a-negligencia-de-fabricantes-com-seguranca,-crescem-ataques-DDoS-providos-a-partir-de-IoTs-1271.html

(iv) Michael Mimoso, "Source Code Released for Mirai DDoS Malware" Threatpost, Oct. 03, 2016. https://threatpost.com/source-code-released-for-mirai-ddos-malware/121039/

(v) Mark Vicente, Byron Gelera, Augusto Remillano II, Chizuru Toyama, Jakub Urbanec, "Bashlite Updated with Mining and Backdoor Commands" Trend Micro Incorporated., Apr. 03, 2019. https://www.trendmicro.com/en_us/research/19/d/bashlite-iot-malware-updated-with-mini
html

(vi) Editorial BCC, "Massive web attack hits security blogger" The BBC, Sep. 22, 2016. https://www.bbc.com/news/technology-37439513

(vii) Kolias, C., Kambourakis, G., Stavrou, A., and Voas, J. (2017). DDoS in the IoT: Mirai and other botnets. Computer, 50(7):80–84.

(viii) Behal, S. and Kumar, K. (2017). Characterization and Comparison of DDoS Attack Tools and Traffic Generators: A Review. IJ Network Security, 19(3).

(ix) Angrishi, K., Turning Internet of Things(IoT) into Internet of Vulnerabilities (IoV): IoT Botnets, (2017). CoRR, abs/1702.03681.

(x) Antonakakis, M., April, T., Bailey, M., Bernhard, M., Bursztein, E., Cochran, J., Durumeric, Z., Halderman, J. A., Invernizzi, L., Kallitsis, M., Kumar, D., Lever, C., Ma, Z., Mason, J., Menscher, D., Seaman, C., Sullivan, N., Thomas, K., and Zhou, Y. (2017). Understanding the Mirai Botnet. In Proc. of USENIX Security Symposium.