Um Estudo Prático sobre o Potencial do Ataque Slowloris a partir de Dispositivos Móveis

Lucas O. C. Aversari[1], Raoni Kulesza[1], Josilene A. Moreira[1]

[1]Centro de Informática – Universidade Federal da Paraíba (UFPB)
Caixa Postal 5.115 – 58.051-900 – João Pessoa – PB – Brasil

astecz360@gmail.com, raoni@lavid.ufpb.br, josilene@ci.ufpb.br

Abstract. *DDoS attacks have become a real and frequent threat to the sites and services offered globally. This work evaluates the potential of running one of these attacks, the worldwide known Slowloris, from Android mobile devices. Generally run from desktops, Slowloris has been adapted by the authors to run on mobile devices. The attacks were fired from one and two smartphones and with variable intensity (250 to 1000 attackers). Server availability metrics, tts, CPU consumption, and memory were evaluated. It has been found that the harmful potential of the mobile version is as high as the desktop version, consuming very little CPU and memory resources.*

Resumo. *Os ataques DDoS têm se tornado uma ameaça real e frequente aos sites e serviços oferecidos no cenário mundial. Este trabalho avalia o potencial da execução de um destes ataques, o Slowloris, mundialmente conhecido, a partir de dispositivos móveis Android. Geralmente executado a partir de desktops, o Slowloris foi adaptado pelos autores para rodar em dispositivos móveis. Os ataques foram disparados a partir de um e dois smartphones e com intensidade variável (250 a 1000 atacantes). Avaliaram-se as métricas disponibilidade do servidor, tts, consumo de CPU e memória. Verificou-se que o potencial danoso da versão móvel é tão alto quanto da versão desktop, consumindo pouquíssimos recursos de CPU e memória.*

1. Introdução

As diversas facilidades oferecidas pelo uso de redes sociais em computadores e dispositivos móveis fazem com que estas possuam números cada vez maiores de usuários e grupos com interesses semelhantes, representando um cenário propício para as mais diversas atividades maliciosas como a realização de ataques de negação de serviço, ou DDoS (do inglês, *Distributed Denial of Service*), envio de *spam*, violações de privacidade e disseminação de *malware* [1]. Nesse contexto, se encaixa uma tendência emergente conhecida como *hacktivismo*, onde grupos hackers realizam ataques e roubo de informações como forma de protesto político ou social [3]. O objetivo visado por estes protestos é a atenção da mídia, do governo e da comunidade Web.

Segundo a Microsoft [5], ataques DDoS são a maior ameaça para os administradores de serviços Web, sendo extremamente populares devido à sua facilidade de implementação e condução, além da difícil atribuição de autoria, devido à sua natureza distribuída. Isso faz com que pessoas, empresas e até mesmo governos façam uso de tal ameaça como forma de guerra cibernética [6]. Na atualidade a maioria

dos ataques DDoS é dirigida à camada de aplicação, com pouca geração de tráfego e baixo consumo de recursos do atacante, também conhecidos como *Slow DDoS*, tendo como o principal representante o Slowloris, implementado por Robert Hansen [7]. Este trabalho visa avaliar o potencial do ataque DDoS Slowloris disparado a partir de dispositivos móveis, a fim de compreender sua capacidade de afetar servidores web.

2. Ataques DDoS e Slowloris

Considerando o cenário de ataques de negação de serviço a partir de dispositivos móveis, podem ser encontradas várias aplicações baseadas na ferramenta desktop LOIC (do inglês, *Low-Orbit Ion Cannon*) [11], desenvolvida pelo grupo de hacktivistas Anonymous, capazes de realizar ataques DDoS do tipo inundação. No entanto, ataques de inundação não se mostram adequados e nem escaláveis ao cenário dos dispositivos móveis, devido à grande quantidade de banda e recursos computacionais por eles consumida. Para este contexto, os ataques slow DDoS são mais adequados.

O Slowloris (HTTP GET) é um ataque slow DDoS realizado através do protocolo HTTP, explorando suas características e vulnerabilidades. O principal foco é o aproveitamento da característica de *timeout* de um servidor Web, que é o tempo máximo em segundos que uma requisição permanece no *buffer* de aplicação até ser atendida. Segundo Cambiaso, Papaleo e Aiello [2] e Karim, Shah e Salleh [14], tal *timeout* pode ser descoberto por meio de um *sniffer* de rede, sendo uma tarefa relativamente simples.

O ataque usando Slowloris é de difícil detecção por parte dos sistemas anti-DDoS, pois consegue gerar tráfego a uma taxa baixa e de pequeno volume. O Slowloris tenta manter muitas conexões com o servidor Web alvo pelo maior tempo possível [15]. O mesmo inicia solicitando várias conexões TCP ao servidor, onde, em cada uma delas, o atacante envia uma requisição GET incompleta. Na etapa seguinte, em algum instante próximo do timeout, um novo cabeçalho incompleto é enviado para manter a conexão ativa. Com a continuidade do ataque, o número de conexões tende a aumentar, consumindo assim todos os recursos da fila de atendimento da aplicação, levando o servidor a um estado de indisponibilidade, não conseguindo, com isso, responder às próximas requisições [7]. Em um cenário de um ataque slow DoS colaborativo utilizando dispositivos móveis ou fixos, todos os dispositivos executando a ferramenta de ataque têm como alvo indisponibilizar um serviço hospedado em um determinado domínio (URL), geralmente um servidor Web. A indisponibilidade tende a se manter enquanto durar o ataque [13].

3. Metodologia

3.1 A Ferramenta de Ataque para Dispositivos Móveis

A ferramenta de ataque adaptada para permitir que os ataques fossem disparados a dispositivos móveis Android é uma versão do utilitário Slowloris que utiliza o mesmo *script* da versão desktop, desenvolvida pelos autores. O código em *perlscript* da versão original foi encapsulado pela biblioteca perlDroid [16] e conta com interface gráfica para simplificar o manuseio. Todos os componentes são empacotados dentro do arquivo de aplicação (.apk), podendo ser instalado e executado em dispositivos Android acima da versão 2.3. A interface projetada para o aplicativo contém apenas campos para inserção da URL a ser atacada e seleção da intensidade do ataque, além de um botão

para iniciar o ataque. O papel da interface é a passagem de parâmetros para o módulo da biblioteca perlDroid, que por sua vez, executa o *perlscript* original da versão *desktop*: "*slowloris.pl*".

São usadas quatro diferentes configurações do ataque nos experimentos: *lite, normal, extreme* ou *uber*, variando entre 250, 500, 750 e 1000 atacantes. Os atacantes são as threads responsáveis pelos envios de requisições HTTP GET para o alvo, com um timeout de 35s definido entre as mesmas. Tal configuração justifica-se pelo fato de o timeout HTTP padrão da maioria dos servidores Web disponíveis no mercado ser de 40s e, segundo a Netcraft, servidores de médio porte são aqueles que possuem capacidade para atender requisições de 750 usuários simultaneamente [17]. As intensidades variáveis permitem que haja a ocupação de 33% (lite), 66% (normal), 100% (extreme) e 133% (uber) do buffer de atendimento do servidor.

3.2 Experimentos e Cenários

Foram realizados experimentos em um cenário composto por um servidor Web, dispositivos móveis executando a ferramenta de ataque Slowloris e um computador executando a ferramenta de simulação de clientes honestos Siege. Utiliza-se o servidor Web Apache 2, configurado, tipicamente, como um servidor de médio porte, capaz de atender 750 clientes simultaneamente [17]). O *timeout* HTTP do servidor foi mantido na sua configuração padrão de instalação de 40 segundos. A escolha do servidor justifica-se através de dados apresentados pela Netcraft, que mostram que aproximadamente 46% dos sites da Internet são hospedados em servidores Apache 2 [17].

Para simulação dos clientes honestos, o software *Siege HTTP load test* foi escolhido, como utilitário de *benchmark* e carga no servidor, devido a sua grande presença e referência na literatura [17]. Em todos os testes, 250 clientes honestos foram simulados pelo Siege como usuários constantes do servidor Web, mantendo uma taxa de ocupação legítima de aproximadamente 33% do *buffer* de atendimento (taxa de ocupação em casos de uso normal para esta categoria de servidores [17]).

As métricas coletadas no servidor foram a disponibilidade média do domínio (taxa de clientes honestos que consegue efetivamente acessar o site) e o tempo de serviço (TTS, do inglês, *time-to-service*) médio, que representa o intervalo até que elas sejam atendidas pelo servidor. Assim, é possível analisar o impacto na qualidade de serviço dos clientes [13]. Adicionalmente, mais duas métricas foram coletadas: consumo de CPU e memória usados pelas ferramentas de ataque e pelo servidor Web Apache. Todos os testes de ataque tiveram duração capturada de 120 minutos. Cada experimento foi realizado trinta e três vezes (33) e então obtida a média de cada métrica, resultando num nível de confiança de 95%.

Os mesmos parâmetros de configuração foram usados em chamadas ao "*slowloris.pl*" na versão *desktop*. O *hardware* utilizado nos testes foi:

- Atacantes: (2x) Xperia J (MSM7227A@1.00 Ghz, 512 Mb RAM, Android 4.1.2);
- Servidor Web: HP PC 5850 (Athlon 64 X2@3.00 Ghz, 4 Gb RAM, Ubuntu 16.10);
- Clientes: MacBook [2009] (Core2Duo@2.20 Ghz, 6 Gb RAM, OSX 10.12 Sierra);.

4. Resultados

4.1 Avaliando o Impacto do Ataque sobre o Servidor

4.1.1. Ataques Utilizando Um Dispositivo Móvel

A Tabela 1 apresenta os resultados de disponibilidade e tts utilizando um aparelho celular para os ataques. Para fins de comparação são mostrados os resultados para a versão Slowloris *desktop*, com os mesmos parâmetros de configuração.

Tabela 2: Testes com apenas um dispositivo atacante

***Slowloris* Mobile**			***Slowloris* Desktop**		
Intensidade do Ataque	Disponibilidade (%)	TTS (s)	**Intensidade do Ataque**	Disponibilidade (%)	TTS (s)
Lite	100,00	0,08	**Lite**	100,00	0,06
Normal	98,97	0,29	**Normal**	99,68	0,23
Extreme	0,00	∞	**Extreme**	0,00	∞
Uber	0,00	∞	**Uber**	0,00	∞

Os resultados da versão móvel são semelhantes à versão tradicional. As mínimas variações nos resultados se devem às atividades executadas pelo servidor Web no momento dos ataques. Percebe-se que, tanto para a versão mobile como para a versão desktop, o servidor só se torna indisponível a partir de ataques cuja intensidade definida é “Extreme”, já que o número de atacantes é igual ao número máximo de clientes que podem ser atendidos simultaneamente pelo servidor, negando assim, serviço a clientes legítimos.

Outra observação importante é o impacto no tempo de serviço (tts) gerado pelo ataque a partir do momento em que todas as posições do servidor encontram-se ocupadas. Isso ocorre no cenário descrito a partir de ataques “Normal”, onde temos 500 atacantes e 250 clientes usufruindo de um buffer de atendimento de 750 posições no servidor. Ocorre um aumento no tts devido ao fato de que novas requisições feitas pelos clientes tem que esperar para serem atendidas, já que todas as posições disponíveis encontram-se em uso.

4.1.2. Ataques Utilizando Dois Dispositivos Móveis

Percebe-se que, neste cenário, a efetividade do ataque é bem maior do que utilizando apenas um dispositivo. Quando dois dispositivos executando o ataque na intensidade “Normal” (500 atacantes) de forma colaborativa atingem o servidor, o mesmo já se torna indisponível, pois só possui capacidade para atender 750 clientes simultaneamente. É possível perceber o potencial danoso do ataque, principalmente quando realizado de forma colaborativa e distribuída.

Tabela 3: Testes utilizando dois dispositivos atacantes

***Slowloris* Mobile**			***Slowloris* Desktop**		
Intensidade do Ataque	Disponibilidade (%)	TTS (s)	**Intensidade do Ataque**	Disponibilidade (%)	TTS (s)
Lite	99,48	0,10	**Lite**	99,98	0,11
Normal	0,00	∞	**Normal**	0,00	∞
Extreme	0,00	∞	**Extreme**	0,00	∞
Uber	0,00	∞	**Uber**	0,00	∞

4.2 Consumo de Recursos pela Ferramenta de Ataque

Serão expostos abaixo os dados da utilização de memória e CPU pela ferramenta de ataque móvel quando configurada em cada uma das intensidades de ataque. Percebe-se um uso muito baixo de memória e CPU, mantendo-se abaixo dos 10 Mb e 10%, respectivamente, em todos os casos. Neste caso, são mostrados os resultados apenas da versão para dispositivo móvel, que possui mais restrições nos recursos de CPU e memória. Entretanto, avalia-se este consumo nas diferentes configurações de intensidade dos ataques.

4.2.1 Consumo de Memória

Percebe-se que o uso de memória fica em torno dos 7,75 Mb para os cenários Lite, Normal e Extreme. A baixa utilização de memória se deve ao fato do Android tentar otimizar ao máximo a área de *heap* das *threads* iguais, identificando áreas compartilhadas por elas. Já na versão Uber do ataque, o uso de memória permaneceu próximo aos 10 Mb, acima dos demais, devido à alocação de mais memória, necessária para as 1000 *threads* de ataque. O baixo uso de memória tanto na versão desktop, como na versão móvel, se deve à baixa complexidade das threads atacantes criadas, as quais realizam a simples atividade de enviar um HTTP GET periodicamente (Figura 1).

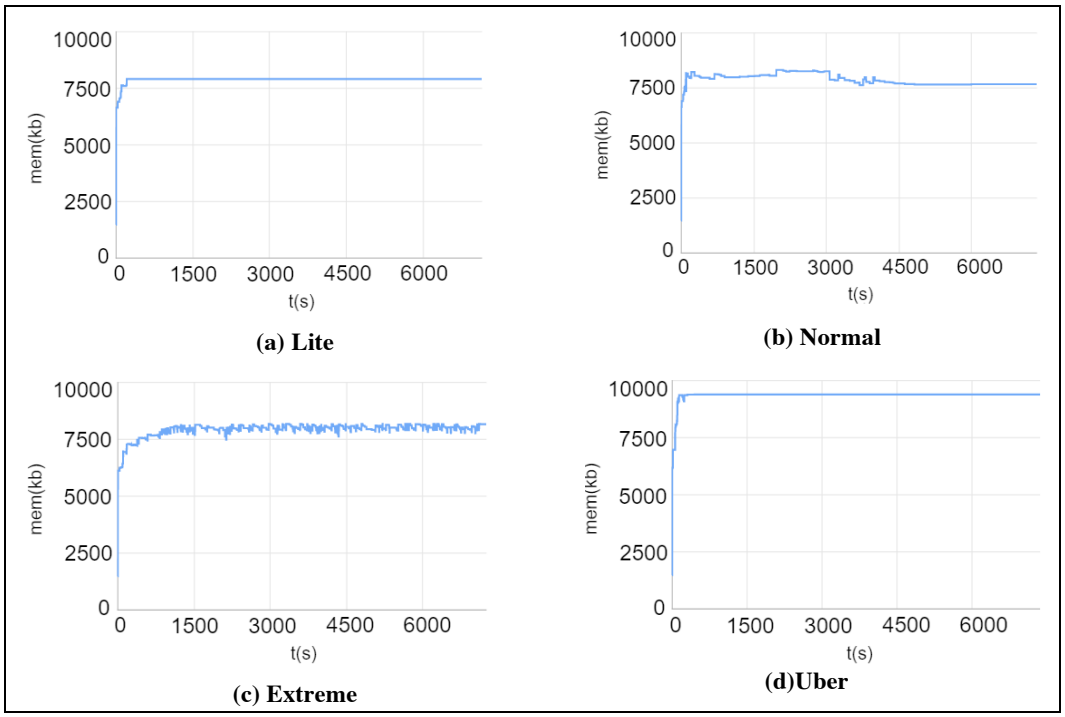

Figura 1: Utilização de memória nas diversas intensidades dos ataques

4.2.2 Consumo de CPU

Verifica-se que uso de CPU tem um pico inicial em torno de 3% no cenário Lite e depois mantém-se abaixo de 2%. Nos cenários Normal e Extreme o pico inicial atinge cerca de 5% e depois cai para menos de 2% também. Este aumento no pico de CPU no

momento da inicialização ocorre devido à maior quantidade de *threads* criadas. Apenas no cenário Uber é que o percentual mantém-se acima de 6%. O maior uso de CPU ocorre devido à sobrecarga causada pela virtualização de um número relativamente grande de *threads* (Figura 2).

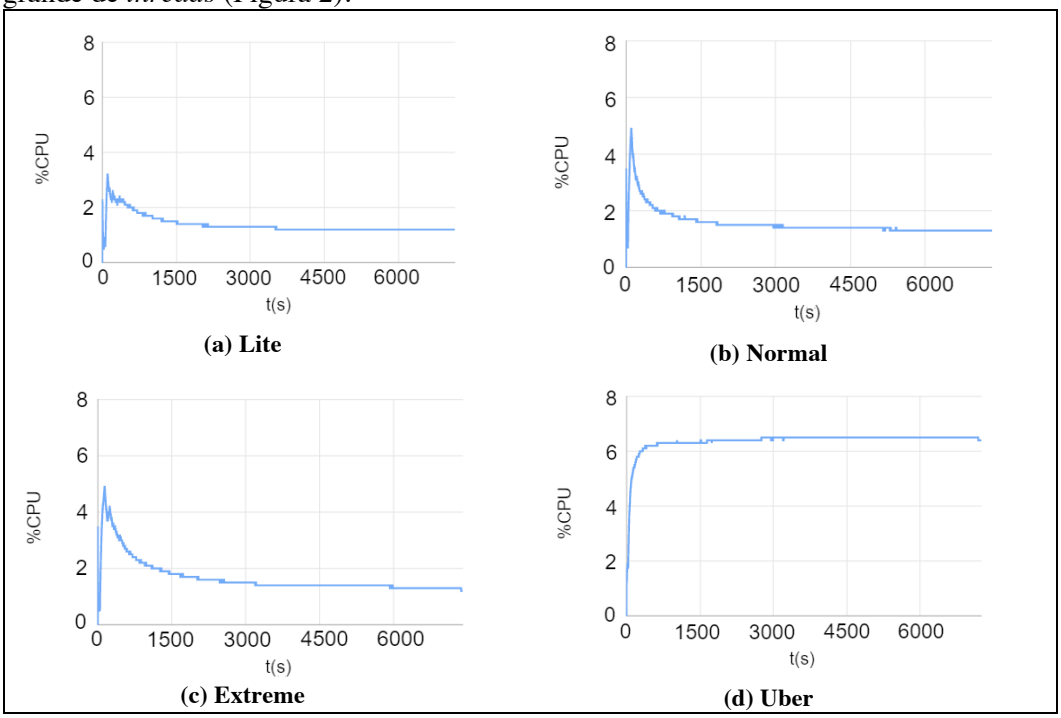

Figura 2: Consumo de CPU nas diversas intensidades dos ataques

5. Conclusões

Sabendo que os dispositivos móveis representam uma grande fatia da massa de dispositivos que acessam a Internet na atualidade, o presente artigo teve como objetivo avaliar o potencial do ataque DDoS Slowloris a partir de dispositivos móveis. Ficou demonstrado que, mesmo no ambiente limitado de um hospedeiro móvel e sem dispor de todas as funcionalidades de um kernel Linux padrão, a execução do *script* original de ataque *slow* DDoS por um dispositivo Android é viável em termos de desempenho e uso de recursos, podendo causar grandes prejuízos a serviços Web.

Com apenas uma instância em execução da ferramenta proposta, é possível indisponibilizar um serviço Web considerado de médio porte. Tal capacidade de realização e portabilidade de ataques permite que uma única pessoa possa utilizar dos seus dispositivos Android para ações maliciosas, prejudicando centenas de outros usuários que desejam acessar legitimamente os serviços disponíveis no alvo. Assim, usuários podem fazer uso de seus dispositivos móveis para colaborar com ataques DDoS difundidos por grupos de ativistas em redes sociais, representando um potencial cenário de ataques colaborativos, os quais precisam ser conhecidos e evitados.

Podemos identificar como trabalho futuro aumentar a escala das avaliações para números mais próximos de um ataque distribuído e/ou colaborativo real, utilizando redes sociais e massas de usuários.

Referências

[1] MAKRIDAKIS, A.; ATHANASOPOULOS, E.; ANTONIADES, D.; IOANNIDIS, S.; MARKATOS, E.. Understanding the Behavior of Malicious Applications in Social Networks. IEEE Networks, 2010.

[2] CAMBIASO, E.; PAPALEO, G.; CHIOLA, M.; AIELLO, M. Mobile executions of Slow DoS Attacks. Logic Jnl IGPL, V. 24, No. 1, p. 54–58, 16/10/2015.

[3] R. GANDHI; A. SHARMA; W. MAHONEY; W. SOUSAN; Q. ZHU; P. LAPLANTE. Dimensions of cyber-attacks: Cultural, social, economic, and political," Technology and Society Magazine, IEEE, vol. 30, no. 1, pp. 28–38, 2011.

[4] S. KUMAR; K. M. CARLEY. Approaches to Understanding the Motivations Behind Cyber Attacks, em Intelligence and Security Informatics. (ISI), 2016 IEEE International Conference em, Tucson, Arizona USA, Set. 2016.

[5] MICROSOFT. Microsoft Library: Security Issues with IP. Disponível em: https://technet.microsoft.com/en-us/library/cc959354.aspx. Acesso em 20/11/2016.

[6] S. KUMAR; K. CARLEY.. Understanding DDoS Cyber-Attacks using Social Media Analytics. IEEE Networks, 2016.

[7] DANTAS, Y, G. Estratégias para tratamento de ataques de negação de serviço na camada de aplicação em redes IP. 2015. 77f. Trabalho de Conclusão de Curso (Especialização) Curso de Ciência da Computação, Universidade Federal da Paraíba, João Pessoa/PB, 2015.

[8] J. LEWIS; S. BAKER. The economic impact of cybercrime and cyber espionage, Center for Strategic and International Studies, Washington,DC, pp. 103–117, 2013.

[9] G. MEZZOUR, Assessing the Global Cyber and Biological Threat, dissertação Ph.D., Symantec Research Labs, 2015.

[10] B. LIU; L. ZHANG. A survey of opinion mining and sentiment analysis, em Mining text data. Springer, 2012, pp. 415–463.

[11] LOIC – Low Orbit Ion Cannon. Disponível em: https://play.google.com/store/apps/details?id=genius.mohammad.loic. Acesso em 12/05/2017.

[12] OP TANGO DOWN, Disponível em: http://www.anonymousbrasil.com/tango-down/. Acesso em 10/06/2017.

[13] DANTAS, Y, G.; NIGAM, V.; FONSECA, I. A Selective Defense for Application Layer DDoS Attacks, Intelligence and Security Informatics Conference (JISIC), Hague, 8/12/2014.

[14] A. KARIM; S. A. A. SHAH; R. B. SALLEH; M. ARIF; R. M. NOOR; S. SHAMSHIRBAND. Mobile Botnet Attacks – an Emerging Threat: Classification, Review and Open Issues. Trans. on Internet and Information Systems, v. 9, 2015.

[15] SLOWLORIS DDoS Attack. Disponível em: https://security.radware.com/ddos-knowledge-center/ddospedia/slowloris/. Acesso em 20/11/2016.

[16] PERLDROID. Disponível em: https://code.google.com/archive/p/perl-android-apk/. Acesso em 20/11/2016.

[17] NETCRAFT. NetCraft WebServer Survey. Disponível em: https://news.netcraft.com/archives/2016/09/19/september-2016-Web-server-survey.html. Acesso em 20/11/2016.

