Infraestrutura escalável para análise do comportamento das botnets e a propagação por e-mail utilizando SMTP

Scalable infrastructure for botnet behavior analysis and e-mail propagation using SMTP

DOI:10.34117/bjdv7n7-035

Recebimento dos originais: 07/06/2021
Aceitação para publicação: 03/07/2021

Fernando Augusto Garcia Muzzi
Doutor em Engenharia Elétrica pela Universidade de São Paulo
Endereço: Av. Prof. Luciano Gualberto, 380 - Butantã, São Paulo - SP, 05508-010
E-mail: fagmuzzi@gmail.com

Marcelo Teixeira de Azevedo
Doutor em Engenharia Elétrica pela Universidade de São Paulo
Endereço: Av. Prof. Luciano Gualberto, 380 - Butantã, São Paulo - SP, 05508-010
E-mail: marcelo.azevedo@pad.lsi.usp.br

Marco Antonio Quirino da Veiga
Mestre em Engenharia Elétrica pela Universidade de São Paulo
Endereço: Av. Prof. Luciano Gualberto, 380 - Butantã, São Paulo - SP, 05508-010
E-mail: mquirino@pad.lsi.usp.br

Edward David Moreno
Doutor em Engenharia Elétrica pela Universidade de São Paulo
Endereço: Av. Prof. Luciano Gualberto, 380 - Butantã, São Paulo - SP, 05508-010
E-mail: edwdavid@gmail.com

Sergio Takeo Kofuji
Doutor em Engenharia Elétrica pela Universidade de São Paulo
Endereço: Av. Prof. Luciano Gualberto, 380 - Butantã, São Paulo - SP, 05508-010
E-mail: kofuji@pad.lsi.usp.br

RESUMO
Uma Botnet é uma rede formada por bots utilizando códigos maliciosos chamados malware, que compromete a segurança. Hoje em dia tem aumentado o número de pragas digitais como exemplo botnet, por isso a necessidade de estudos e análise do comportamento dessas redes de bots, a necessidade de infraestrutura escalável para análise se torna necessária, utilizando máquinas virtuais, serviços e bots em ambiente confinado sendo importante para verificar os tipos de ataque, comportamento dos bots, impacto na rede e estudar formas de conter os ataques e propagação das Botnets utilizando e-mail, protocolo SMTP e porta 25.

Palavras-chave: Botnet. Infraestrutura, Ataque, DDOS, SMTP.

ABSTRACT
A Botnet is a network formed by bots using malicious code called malware, which compromises security. Nowadays, the number of digital pests such as botnet has increased, so the need for studies and analysis of the behavior of these botnets, the need for scalable infrastructure for analysis becomes necessary, using virtual machines, services and bots in a confined environment it is important to verify the types of attacks, behavior of bots, impact on the network and study ways to contain attacks and propagation of Botnets using e-mail, SMTP protocol and port 25.

Keywords: Botnet, Infrastructure, Attack, DDOS, SMTP.

1 INTRODUÇÃO

Com o aumento do número de computadores têm surgido ameaças de segurança e várias modalidades de crimes digitais, tornando os aspectos de segurança importante [10]. Um dos tipos de ameaça são as botnets. Uma rede que torna o computador da vítima infectado se tornando um zumbi.

Uma entidade conhecida como Botmaster pode enviar comandos para o computador para o computador infectado, conseguindo assim enviar comandos para o computador infectado para fins ilícitos, como ataque de negação de serviço DDoS, envio de Spam.

São necessários novos mecanismos de segurança, conhecer a rede infectada pela Botnet é importante para que se possa detectar e conter esses tipos de ameaças, para isso é necessário que se tenha uma infraestrutura escalável, uma vez que a Botnet é formada por um grande número de computadores infectados, dependendo de uma estrutura escalável para estudos das Botnets.

Botnet é uma rede formada por bots, tornando o computador da vitima infectada, um zumbi, que responde a comandos enviados pelo Botmaster. Dessa forma o Botmaster consegue o controle do computador infectado para fins ilícitos, como a prática de Crimes Digitais como DDoS, Roubo de Senhas, Envio de Spam [1].

Esse trabalho descreve a Botnet utilizando máquinas virtuais para estudar mecanismos de segurança. A utilização de máquinas virtuais escaláveis para que se possa ter um grande número de nós da Botnet.

Botnet tem sido alvo de diversos tipos de estudos pela comunidade de segurança da informação.

Uma das modalidades de ataque de uma Botnet é o DDoS, onde as máquinas infectadas passam a executar ataques DDoS através dos protocolos TCP e UDP [1] [2] [4].

A propagação dos bots pode ocorrer através diversos forma lista de contatos de email, que usa a porta 25 e o protocolo SMTP (Simple Mail Transfer Protocol) é um protocolo usado no envio de e-mail.

A proliferação dos *botnet* na internet está aumentando, surgindo então à necessidade de métodos para conter esse tipo de ataque. Existem botnets que capturam senhas, número de cartão de crédito.

Nas próximas sessões vamos mostrar as tecnologias utilizando máquinas virtuais, apresentando os resultados obtidos com ataque das *botnets* e análise de resultados e finalmente a conclusão.

2 METODOLOGIA

Para o desenvolvimento da pesquisa, foi necessário a utilização de máquinas virtuais utilizando *vmware workstation* 7 e sistema operacional windows 98 ocupando 6 Mb de memória RAM. Foi utilizado um computador I7 860 com 16 Gb de RAM com 100 máquinas virtuais com o Botnet Rxbot, utilizado servidor IRC e servidor IDS (*Intrusion Detection System*) chamado Snort.

Foram utilizadas 100 máquinas virtuais para a realização dos testes e 4 roteadores utilizando Linux, cada roteador com 25 máquinas virtuais. Foram analisadas 3 amostras, referente a propagação de pacotes utilizando o protocolo SMTP, e coletado o tempo médio de envio.

Foi utilizado um servidor IRC (*Internet Relay Chat*) para ter um uma infraestrutura totalmente isolada do mundo externo.

Foi utilizado um Roteador Linux para rotear diferentes redes e IDS para capturar pacotes.

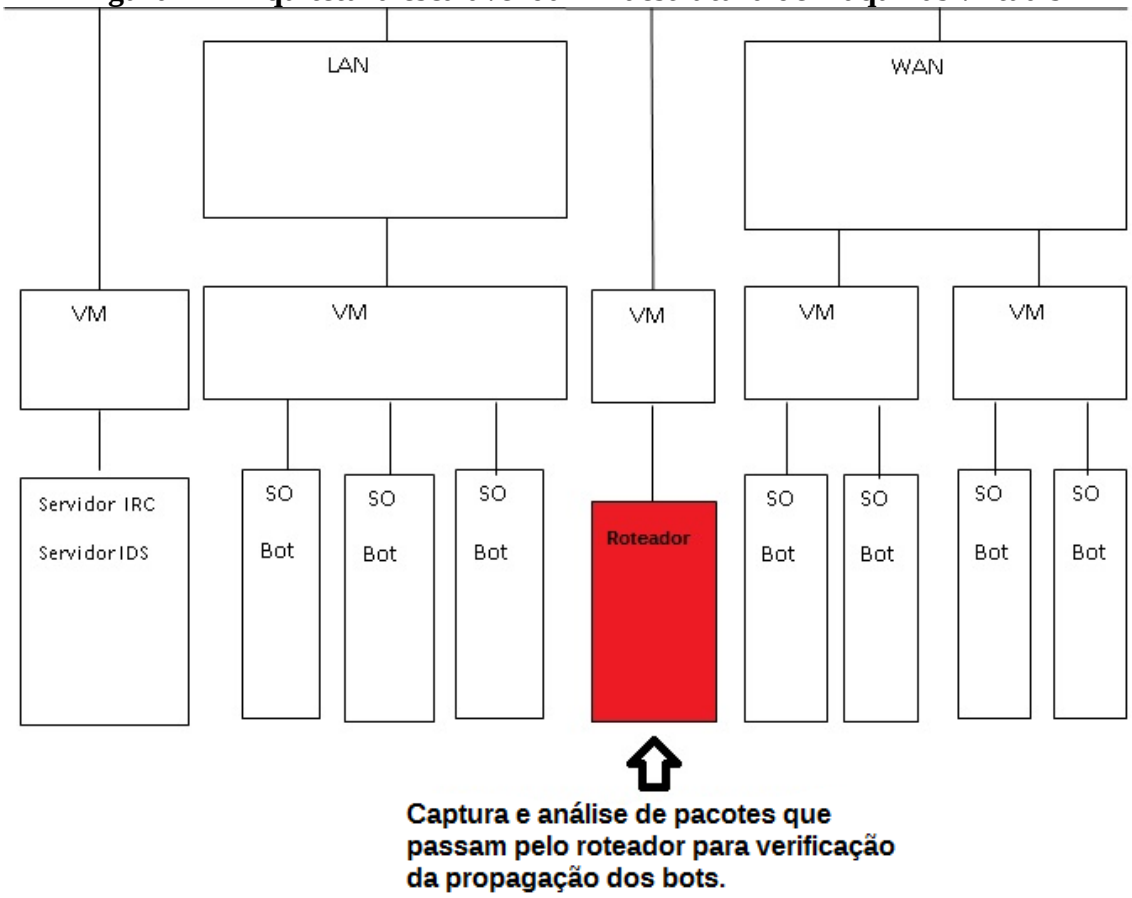
Foi utilizado para análise dos pacotes o Wireshark, software de detecção de pacotes de rede de computadores, para capturar pacotes e verificar as formas de propagação.

Na figura 1 pode-se ver a arquitetura escalável da infraestrutura de máquinas virtuais, um conjunto de máquinas virtuais rodando sistema operacional que ocupa uma quantidade pequena de memória RAM.

Para escalar é possível ter máquinas virtuais em computadores em locais diferentes com sistema operacional e um bot que aponta para o endereço IP do servidor, utilizando o protocolo *IRC*, sendo possível conectar no servidor *IRC*.

O roteador com *IDS* tem o papel de fazer o roteamento entre redes virtuais e promover mecanismos de segurança para alertar o administrador de rede sobre possível ameaça de *Botnet* na rede e alertar sobre a existência de comunicação entre o *Botmaster* e os hosts contaminados com o bot.

Figura 1 – Arquitetura escalável da infraestrutura de máquinas virtuais

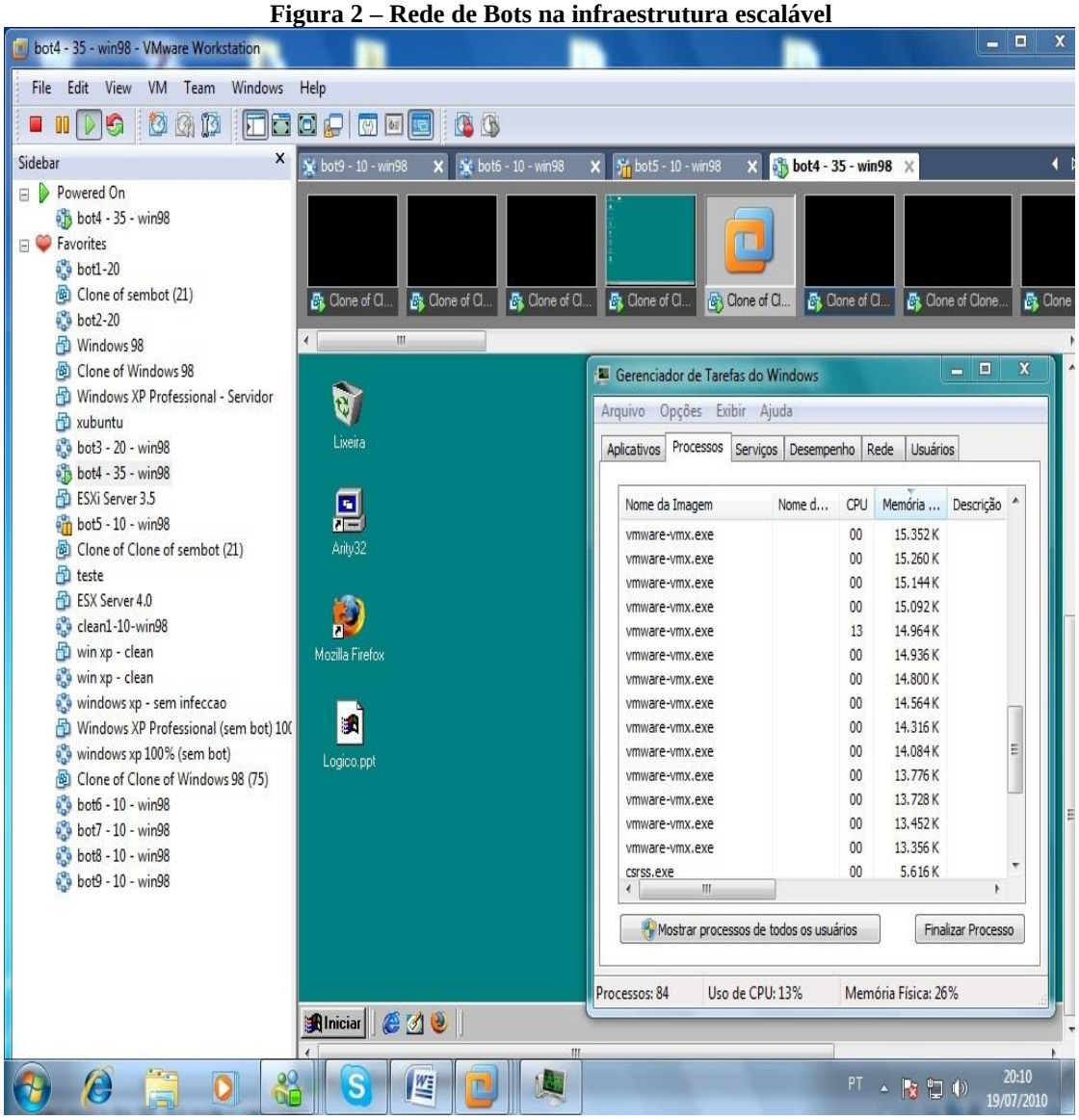


Fonte: (próprios autores).

3 RESULTADOS

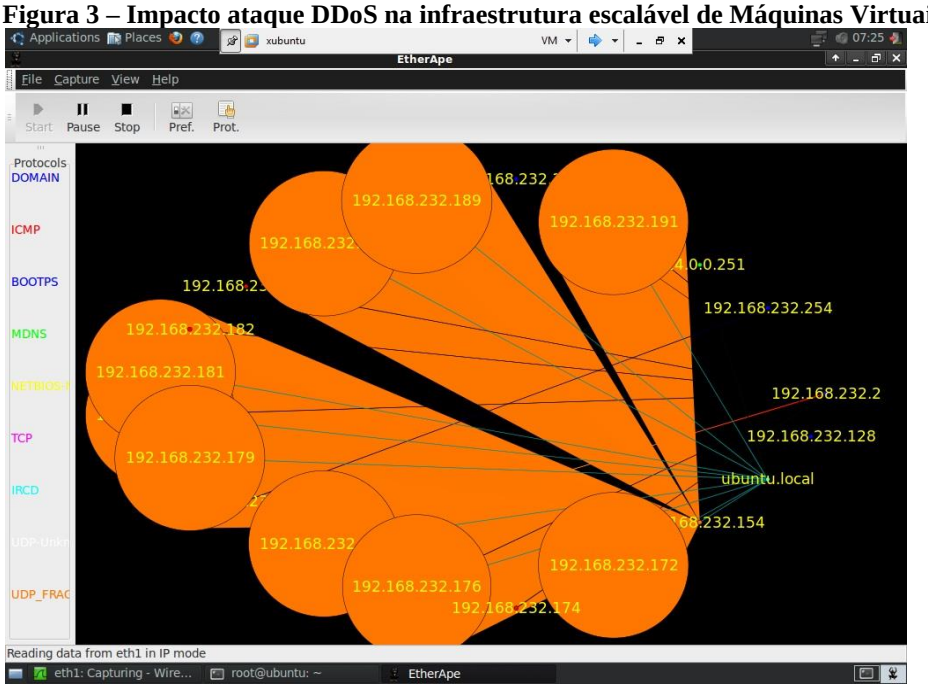
Na figura 2, pode-se ver a máquina virtual com diversos sistemas operacionais Windows 98 infectados com o *bot* e no gerenciador de processos, os processos referentes à máquina virtual *Vmware Workstation* 7.

Figura 2 – Rede de Bots na infraestrutura escalável



Na figura 3, pode-se ver o impacto na rede de máquinas virtuais através de ataque DDoS (udpflood), através do envio de comando de ataque para os bots pelo botmaster.

Figura 3 – Impacto ataque DDoS na infraestrutura escalável de Máquinas Virtuais



Fonte: (próprios autores).

Na figura 4, pode-se ver o envio de comando 'udpflood' para os todos os bot iniciar ataque DDoS contra o host 192.168.163.131.

Figura 4 - Ataque *DDoS* utilizando *udpflood*

```
08:44 <@root> .udpflood 192.168.163.131 1000 4096 100
 [08:44] [@root(+i)] [2:localhost/#a(+n)]
[#a]
```

Fonte: (próprios autores).

Na figura 5, podem-se ver os pacotes de ataque *DDoS* capturados pelo *IDS*, o host com endereço IP 10.10.0.3 efetuando ataque contra o *host* com endereço IP 192.168.163.131, ou seja, todos os *bots* efetuam ao mesmo tempo ataque *DDoS* contra o host alvo.

Figura 5 - Pacotes Capturados pelo IDS no Roteador utilizando Máquina Virtual

```
[**] [123:8:1] (spp_frag3) Fragmentation overlap [**]
[Priority: 3]
08/03-00:50:01.646453 10.10.0.3 -> 192.168.163.131
UDP TTL:127 TOS:0x0 ID:19712 IpLen:20 DgmLen:1160
Frag Offset: 0x0172   Frag Size: 0x0474

[**] [123:8:1] (spp_frag3) Fragmentation overlap [**]
[Priority: 3]
08/03-00:50:01.667019 10.10.0.2 -> 192.168.163.131
UDP TTL:127 TOS:0x0 ID:29696 IpLen:20 DgmLen:1161
Frag Offset: 0x0172   Frag Size: 0x0475
```

Fonte: (próprios autores).

Na figura 6, pode-se ver o Botmaster comando de ataque DDoS "*udpflood 192.168.163.131 1000 4096 100*", contra o host com endereço IP 192.168.163.131. Os dois bots BRA|01712 e o BRA|68744 enviaram 1000 pacotes cada um contra o *host*. O *Botmaster* pode enviar diversos tipos de comandos de ataque aos *bots*, como *icmpflood*, *udpflood*, *syncflood*, *tcpflood*, sendo ataques *DDoS*, ataque distribuído de negação de serviço.

Figura 6 - Botmaster comando de ataque DDoS

```
08:45 <@root> .udpflood 192.168.163.131 1000 4096 100
08:45 < BRA|01712> -udp- Sending 1000 packets to: 192.168.163.131. Packet
                   size: 4096, Delay: 100(ms).
08:45 < BRA|68744> -udp- Sending 1000 packets to: 192.168.163.131. Packet
                   size: 4096, Delay: 100(ms).
```

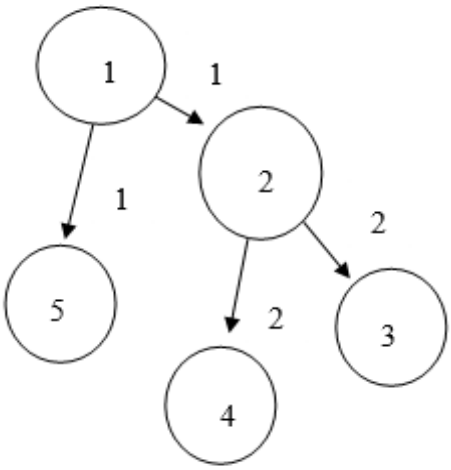
Fonte: (próprios autores).

Na figura 7, pode-se ver a propagação dos bots através da rede utilizando máquinas virtuais, foi analisado o comportamento dos bots para infectar outros computadores através da rede, sendo que a *botnet* se propaga através dos recursos compartilhados da rede, contaminando os *hots*, nota-se alguns dados preliminares que a propagação ocorre de modo aleatório de acordo com a comunicação dos hosts em rede.

A análise dos dados gerados a partir de ataque *DDoS* demonstra segmentos de pacotes *UDP* sem confirmação de pacote, o que causa um grande impacto na rede, provocando uma inundação de pacotes *UDP*, consequentemente a rede fica lenta e o host alvo do ataque fica inativo não respondendo, travando e gerando grande tráfego de pacotes na rede e colisão de pacotes.

A partir das análises do comportamento das *Botnets* será possível estudar formas de contenção de ataque das *Botnets* e contenção da propagação dos Bots.

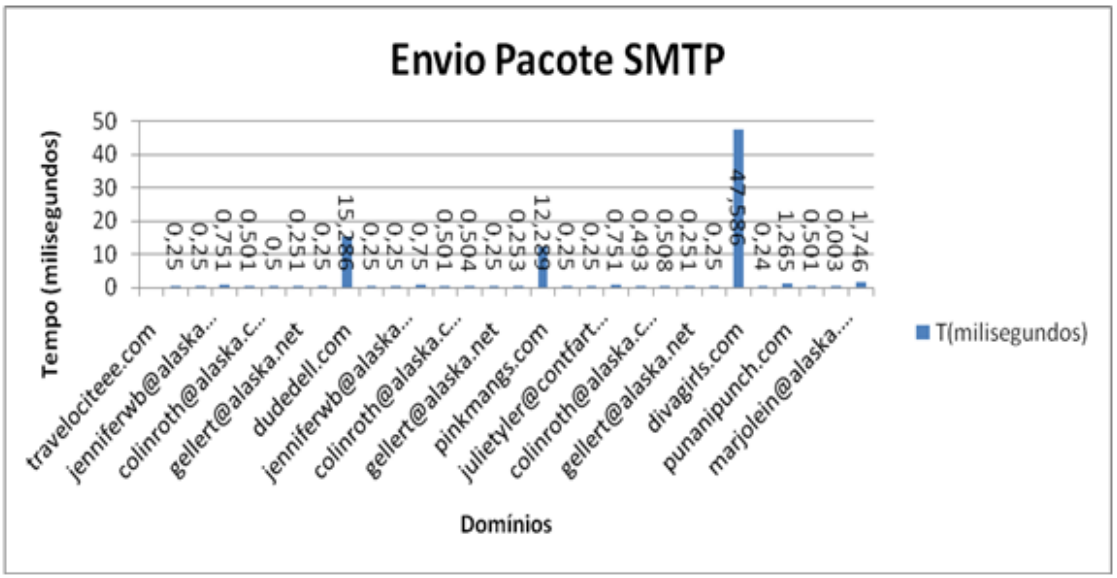
Figura 7 - Grafos de propagação da Botnet na rede escalável virtualizada



Fonte: (próprios autores)

Uma das formas de propagação dos bots ocorre por meio do envio de e-mail. Na Figura 8 pode-se ver o tempo e os domínios de e-mails utilizados para disseminar através da internet os bots e contaminar outros computadores. Foram utilizadas 100 máquinas virtuais para a realização dos testes e 4 roteadores utilizando Linux, cada roteador com 25 máquinas virtuais. Foram analisadas 3 amostras, referente a propagação de pacotes utilizando o protocolo SMTP, e coletado o tempo médio de envio.

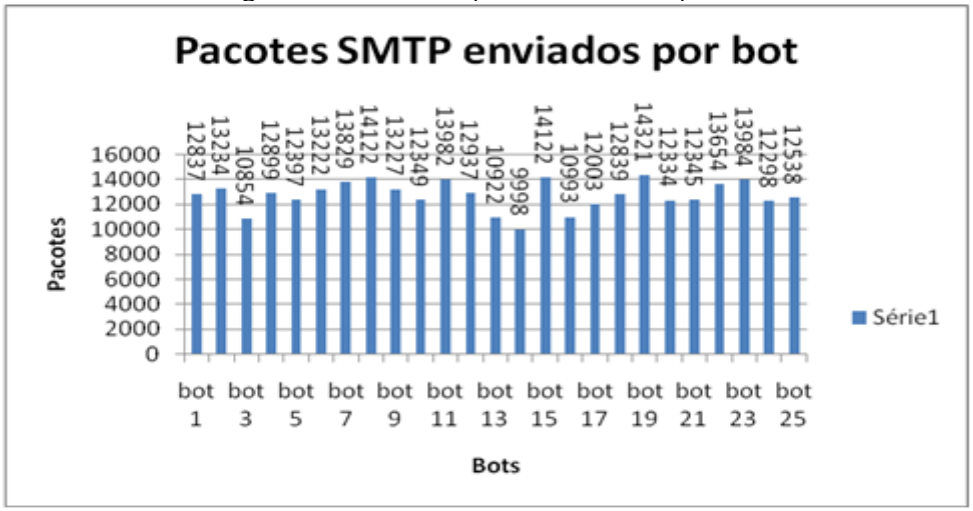
Figura 8 – Envio de pacotes utilizando protocolo SMTP



Fonte: (próprios autores).

A Figura 9 mostra os pacotes do tipo SMTP enviados por bot. Nota-se que o bot 19 foi o responsável pela maior quantidade de envio de pacotes, 14.321. A média foi de 12.729,6 enviados em um tempo de 3 horas.

Figura 9 – Pacotes do tipo SMTP enviados por *bot.*



Fonte: (próprios autores).

4 TRABALHOS RELACIONADOS

A Sandia, em Livermore, Califórnia, está realizando pesquisas de análise das *Botnets*, utilizando Supercomputador "Cluster" Dell Thundebird com 4.480 microprocessadores Intel e um milhão de sistemas operacionais para estudar o comportamento de programas invasivos conhecidos como botnet. Utilizando Sistema Operacional Linux e "*Wine*" Emulador de sistema operacional Windows.

O Google criou um Simulador denominado "*BoNeSi*" para simular ataques *DDoS* e estudar o impacto do ataque *DDoS*, que utilizado os protocolos ICMP, UDP, TCP e HTTP para realizar simulação de ataques [9].

Existem várias pesquisas utilizando diversos recursos tecnológicos, como "*Cluster"*, Computação em Grade "*Grid Computing*" e Computação em Nuvem "*Cloud Computing*", para realizar estudos sobre comportamentos das Botnets.

5 CONCLUSÃO

Verificou-se o funcionamento da rede de *bots* em ambientes utilizando máquinas virtuais em infraestrutura escalável, para ser possível observar os padrões de comportamento dos *bots*, no qual foi possível observar a propagação dos *bots* por meio do protocolo SMTP, ou seja, por e-mail. A contribuição deste estudo é a especificação de uma infraestrutura de análise de *Botnet*, das quais a principal qualidade é a melhoria da infraestrutura de ambiente confinado, utilizando técnicas de virtualização e escalabilidade.

Concluiu-se que ter uma infraestrutura escalável é importante para estudar o comportamento das *Botnets* e analisar o comportamento dos *bots*. Além de analisar a comunicação entre o *Botmaster* e os *bots* é uma forma de verificar como ocorre o envio de comandos e qual o perfil da *Botnet*. Analisar o fluxo de pacote a partir do roteador é importante para verificar pacotes de ataques e a comunicação da rede de *Bots.* E através da análise de comportamento dos bots é possível criar mecanismos de contenção de ataques e técnicas de detecção de *botnets*.

Utilizou-se a análise do comportamento da rede de bots, chamada botnet onde foi possível analisar e verificar propagação dos bots pela internet por meio do envio de e-mails utilizando o protocolo SMTP e porta 25 para propagar–se e tentar infectar o computador de destino para o qual foi enviado o E-mail.

Foram analisadas 3 amostras, referente a propagação de pacotes utilizando o protocolo SMTP, e coletado o tempo médio de envio, A média foi de 12.729,6 enviados em um tempo de 3 horas.

Pode-se observar que essa forma de propagação tem um alto risco de contaminação de computadores e dispositivos conectados as redes que utilizando envio e recebimento de e-mails, por se tratar de uma forma bastante utilizada para envio de mensagem e sendo difícil a detecção já que utiliza o protocolo SMTP e porta 25 e o código malicioso (*malware*) referente ao *bot* está anexado ao e-mail.

Uma das maneiras de contenção seria um antivírus atualizado contendo a assinatura para o tipo de *bot* contendo o código malicioso, porém nem sempre os computadores ou dispositivos estão com um antivírus atualizado, sendo assim necessário formas de contenção ou mitigação da propagação da botnet.

Existem outras formas de detecção do ataque de *bots* como, por exemplo, um IDS (*Intrusion Detection System*), Sistema de detecção de intrusão para detecção de tentativas de ataques, por exemplo do tipo DDoS (*Distributed Denial of Service*), ataque de negação distribuída de serviço.

Em trabalhos futuros, as análises feitas neste estudo podem ser usadas para aperfeiçoamentos das técnicas de análise de *botnets*.

REFERÊNCIAS

[1] Yong-Hee Jeon, “Introduction and Analysis of Botnet Techniques”, Proceedings of the Korea Institutes of Information Security and Cryptology, Vol. 18 No. 3, pp. 101-108, June 2008.

[2] Kyoung-Soo Han, Eul-Gyu Im, “A Study on the Traffic Analysis of P2P Botnet in Honeynet Environment”, Proceedings of the 12th Conference on Next Generation Communication Software (NCS 2008), pp. 10-13, December 2008.

[3] Han-Woo Lee et al., “DNS-based Botnet Detection System”, Proceedings of the Korea Information Processing Society Conference, Vol. 13 No. 2, November 2006.

[4] David Barroso, “Botnets - The Silent Threat”, ENISA Position Paper No. 3, November 2007.

[5] M.C.Sacchetin, A.R.A. Grigio, L.O. Duarte, and A. Montes, “Botnet Detection And Analysis Using Honeynet”, Proceedings of the International Journal of Forensic Computer Science, 2008.

[6] Zhaosheng Zhu, Guohan Lu, Yan Chen, Z.J. Fu, P. Roberts, and Keesook Han. Botnet research survey. pages 967{972, 28 2008-Aug. 1 2008.

[7] G.P. Scha_er. Worms and viruses and botnets, oh my! rational responses to emerging internet threats. Security Privacy, IEEE, 4(3):52{58, May-June 2006.

[8] David Dagon, Guofei Gu, Christopher P. Lee, and Wenke Lee. A taxonomy of botnet structures. Computer Security Applications Conference, Annual, 0:325{339, 2007.

[9] BoNeSi: The DDoS Botnet Simulator. Disponível em: http://code.google.com/p/bonesi/. Acesso em: 25 jul. 2010.

[10] Azevedo, Marcelo Teixeira de. Cibersegurança em sistemas de automação em plantas de tratamento de água. 2010. Dissertação (Mestrado em Sistemas Eletrônicos) - Escola Politécnica, University of São Paulo, São Paulo, 2010. doi:10.11606/D.3.2011.tde-10012011-121525. Acesso em: 2018-06-16.