1.03.04 - Ciência da Computação / Sistemas de Computação

ANÁLISE DE FERRAMENTAS *ANTIMALWARE* EM AMBIENTE DE SIMULAÇÃO PARA TESTES DE PROTEÇÃO E DETECÇÃO DE *BOTNETS*

Jimi Togni[1], Maria Das Graças J. M. Tomazela[2], Aldo Pontes [2]
1. Estudante de Análise e Desenvolvimento de Sistemas da FATEC - Indaiatuba
2. Pesquisador da Faculdade de Tecnologia de Indaiatuba

Resumo:

A internet é parte da vida de todos e estamos nos tornando mais dependentes a cada dia, em contrapartida às facilidades que proporciona, perde-se controle e privacidade das informações. Em vista disso, o objetivo deste trabalho é analisar as possibilidades e potencialidades de sistemas *antibotnet* disponíveis na internet

Buscou-se imparcialidade na obtenção dos resultados, utilizando pontos de restauração de máquinas virtuais, para a execução de todas as ferramentas em ambiente singular, bem como controlar as variáveis possíveis. Para o experimento foram selecionados os *malwares* de *botnet* mais comuns encontrados na internet, bem como ferramentas *antibotnet* mais populares e bem avaliadas por sites e empresas especializadas em segurança da informação.

Dentre as ferramentas testadas, as de uso grátis demonstraram possibilidades e potencialidades capazes de proteger contra objetos maliciosos e danosos, porém, não com o nível de recursos e desempenho apresentados nas ferramentas pagas.

Palavras-chave: *botnet; malware;* vírus.

Introdução:

Em 2010 aconteceram ataques do tipo *ciberguerra* contra países como Irã e China, acredita-se que no Irã sistemas de tecnologia da informação foram atacados por um *malware* de *botnet* chamado StuxNet[1]. Especialistas ocidentais afirmam que esses ataques foram projetados para tentar frear o programa nuclear Iraniano. Na mesma linha do *malware* StuxNet, a empresa de segurança da informação Symantec divulgou um artigo falando sobre um novo *malware* de *botnet,* que foi por eles batizado de Regin[1], segundo a empresa, esse tem como propósito coletar informações que podem ser usadas em operações contra organizações governamentais, operações de infraestrutura, negócios, universidades e até mesmo contra indivíduos. Sua complexidade sugere que em seu desenvolvimento foram usados vários times de desenvolvedores e muitos meses ou anos de desenvolvimento e manutenção[2].

Em 2013, foi comprovado pelo FBI[4] que os servidores, usados pela então secretária de estado Hillary Clinton, haviam sido invadidos por hackers Russos, e que 30.322 e-mails da secretária tiveram que ser entregues ao FBI[4] para que o caso fosse investigado, e mais de 31 mil e-mails foram apagados dos servidores. Uma semana após o ocorrido, a própria secretaria tornou verdadeiras as alegações da mídia, que antes eram apenas suposições. O mesmo grupo russo que realizou o ataque, também teve acesso a várias contas de e-mails de oficiais das forças armadas dos EUA, e também de um membro da família Bush. Todos esses ataques ocorreram graças a computadores infectados por *malwares*, inclusive os de *botnet*[4].

Durante a elaboração deste trabalho, ocorreu o maior ataque de negação de serviço (DDoS) da história, segundo o jornal internacional The Guardian[5]. O ataque aconteceu no dia 20 de setembro de 2016, o tráfego gerado durante o ataque foi de aproximadamente 1.2 *Terabits*[14] por segundo. O ataque partiu de dispositivos contaminados pelo *malware* da *botnet* Mirai, que é composta em grande parte por dispositivos como, câmeras IP, modens, roteadores e dispositivos com placas de redes acoplados em elementos do cotidiano, como televisões, geladeiras, cortinas, portas, catracas e outros dispositivos que são disponibilizados na internet[6].

A partir do contexto apresentado, o objetivo deste trabalho é analisar as possibilidades e potencialidades de sistemas *antibotnet* disponíveis na internet.

Metodologia:

A metodologia definida para realizar este trabalho foi uma pesquisa experimental, que, segundo Gil (2002), consiste em definir um objetivo de estudo, escolher as variáveis capazes de influenciar o objetivo e definir as formas de controlar e observar os efeitos que essas variáveis podem gerar no objetivo. A pesquisa foi voltada especificamente para *malwares* de *botnet*.

Foram escolhidos os 19 *malwares* mais populares no ano de 2016 segundo referencias citadas no Quadro 1.

Quadro 1: *Malwares* selecionados para teste

Nome	Tamanho atual	Referencia
Zbot/Zeus	> 15.000	Kaspersky Lab[9]
Zeus Gameover	-	
Confiker	-	
Kelihos	-	
Nercus	-	
Sality4	-	
Artro	-	
SpyEye	> 5.000	Symantec
CryptoLocker	-	
Dridex	-	
Citadel	-	
Carberp	> 25.000	
Gbot	> 59.000	Sonicwall[10]
Ponmocup	> 1.500.000	Microsoft[11]
TDSS	> 90.000	ESET[12]
Gozi	> 23.000	SecureWorks[13]
Loky	-	-
Ramnit	-	-
Mirai	> 4.000.000	Malwaretech[6]

Para a análise de ferramentas de detecção e contenção de *malware*, optou-se por utilizar três ferramentas de uso gratuito e três ferramentas pagas. As ferramentas selecionadas são apresentadas no Quadro 2, os arquivos de instalação foram obtidos no site oficial de seus fabricantes.

Para cada item avaliado, foi atribuído um valor que varia de 0 a 5, para que fosse possível medir quantitativamente o desempenho das ferramentas.

Quadro 2: Ferramentas selecionadas para teste

Nome	Fabricante	Licença
Avira Antivirus	Avira Operations GmbH & Co	Grátis
AVG Antivirus	AVG Technologies	
Avast Antivirus	Avast Softwarer	
Symantec Norton Secuity	Symantec	Pago
Kaspersky Internet Security	Kaspersky Lab	
MCAffe Internet Security	Intel Security	

Para itens que possuíssem resultados percentuais, como utilização de CPU e memória RAM, foram feitas 3 medições ao longo de seu monitoramento, feito isso, o valor médio entre as três medições foi convertido em seu resultado final. Os itens avaliados foram:

Desempenho: Este trabalho limita-se a avaliar o consumo de CPU e memória RAM durante a execução da varredura completa;

Eficiência: Considera a quantidade de detecção e remoção de *malwares* de cada uma das ferramentas;

Usabilidade: Os critérios foram: efetividade, eficiência e satisfação em um contexto de uso especifico (ISO 9241-11)[15].

Transparência: Neste quesito foi avaliada a quantidade de informações que a ferramenta deixa transparecer ao usuário;

Qualidade de Diagnóstico: Foi analisada a qualidade com que a ferramenta mostra seus resultados ao usuário;

Tempo de varreduras: Foi observado o tempo total que a ferramenta levou para executar a verificação completa do sistema;

Bloqueio do tráfego de rede malicioso: Capacidade de bloquear o tráfego malicioso entre *bot* e central de comando e controle;

Pontos positivos: Funções extras que a ferramenta possui;

Pontos negativos: Falta de recursos básicos ou primários para ferramentas *antimalware.*

Para possibilitar a análise das ferramentas, optou-se por utilizar a ferramenta de virtualização KVM/QEMU. Foram criados pontos de restauração do sistema operacional da máquina virtual, para que o ambiente estivesse sempre na mesma configuração.

Resultados e Discussão:

Na Figura 1 é apresentado o resultado da captura do tráfego de rede suspeito gerado em decorrência da conexão do *malware* de *botnet* com a central de comando e controle, Vale ressaltar que, apenas um *malware* de *botnet*, o Zbot, foi executado no sistema antes da instalação das ferramentas *antimalware*, para que fosse possível analisar a interação entre o *bot* e a central de comando e controle. Pode-se notar que o computador infectado está enviando requisições do tipo *DNS* para o servidor da empresa Google. Essas requisições são destinadas a domínios suspeitos na internet, como por exemplo a tentativa de conexão com os endereços: iqvteykdxpcunt.net, vvnkqdlggrat.com, ip1f12fe98.dynamic.kabel-deutschland.de, entre outros que podem ser verificados como maliciosos no site do departamento de justiça dos Estados Unidos[7].

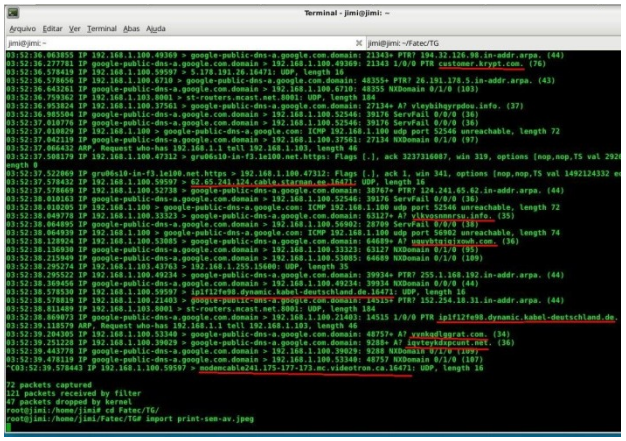

Figura 1: Tentativas de conexão entre *malware* de *botnet* e sua central de comando e controle

Esta captura de tráfego foi realizada com o *malware* de *botnet* chamado Zeus em execução na máquina virtual, na qual foram realizadas as avaliações das ferramentas *antimalware*. Todas as ferramentas foram instaladas e sua verificação foi executada já com este *malware* em execução no sistema operacional.

A ferramenta Avira detectou um número maior que as outras ferramentas, além disso, esse número, 866, foi bastante discrepante do número de *malwares* selecionados para este trabalho.

Outras ferramentas tiveram uma boa relação entre detecção, contenção e eliminação dos *malwares* por eles encontrados, foram os casos de AVG, Sysmantec Norton Security, KasperSky. A ferramenta McAfee, encontrou um número bem baixo de *malwares*, porém todos os artefatos encontrados foram eliminados, bem como, foi eliminado o tráfego entre central de comando e controle, e computador infectado.

Quanto ao bloqueio do tráfego de rede entre central de comando e controle e o computador infectado, dentre as ferramentas gratuitas analisadas, nenhuma foi capaz de conter a comunicação, bem como, não foram capazes de eliminar o arquivo executável infectado pela *botnet*. Já as ferramentas pagas, todas foram capazes de conter o tráfego de rede malicioso, porém, apenas a ferramenta Kaspersky Total Security foi capaz de eliminar o arquivo infectado em tempo de execução do sistema operacional. O Quadro 3, mostra os arquivos totais, infectados e excluídos ou movidos, obtidos com os testes de cada ferramenta.

Contudo, quatro ferramentas tiveram pouca dispersão em seus resultados, foram elas, AVG Free Antivírus com 63 arquivos infectados encontrados, Avast Free Antivírus com 18, Symantec Norton Security com 48 e McAfee com 10 arquivos, em relação a duas ferramentas que ficaram muito fora da média, são elas, Avira Antiviris Free com 866 e Kaspersky Toral Security com 366 arquivos. Esses resultados são apresentados no Quadro 3.

Quadro 3: Compilação dos resultados

Ferramenta *Antimalware*	Total de arquivos infectados	Total de arquivos excluídos ou movidos	Tempo
Avira Antiviris Free	866	15	22:34
AVG Antiviris Free	63	63	22:35
Avast Antiviris Free	18	18	Não informado
Symantec Norton Security	48	48	Não informado
McAfee LiveSafe	10	10	Não informado
Kaspersky Toral Security	366	366	42:07

Para possibilitar o cálculo de uma média entre todos os indicadores, nos valores que se referem a monitoramento, ou seja, consumo médio de CPU e memória RAM, foi usada a seguinte formula para gerar uma pontuação: (100% - percentual médio)/10, como pode ser visualizado no Quadro 4.

Quadro 4: Compilação dos resultados

Ferramenta	Usabilidade	Transparência	CPU	Memória	Média Final
Avira Antiviris Free	3	2	0,6	0,1	1,4
AVG Antiviris Free	1	3	0,5	0,1	1,1
Avast Antiviris Free	4	1	0,6	0,1	1,4
Symantec Norton Security	5	5	0,2	0,1	2,6
McAfee LiveSafe	3	3	0,3	0,1	1,6
Kaspersky Total Security	5	5	0,3	0,1	2,6

Pode-se dizer que, os resultados são satisfatórios ao demonstrarem esta proximidade entre duas ferramentas grátis e duas ferramentas pagas.

Conclusões:

Foi possível constatar que existem excelentes ferramentas *antibotnet* disponíveis para o usuário final, que são disponibilizadas gratuitamente para uso, ou ferramentas de licença não gratuitas. Observou-se que, dentre as ferramentas testadas, as de uso grátis apresentam possibilidades e potencialidades capazes de proteger o usuário final de objetos maliciosos e danosos ao seu computador, porém, não com o nível de desempenho e possibilidades de recursos que as ferramentas não pagas oferecem.

Portanto, pode-se afirmar que este trabalho atingiu seu objetivo, apresentando com imparcialidade, os resultados obtidos com ferramentas populares no mercado de *antimalware*[8], seus pontos positivos e negativos, quantificando e qualificando os dados obtidos de forma clara e objetiva.

Referências Bibliográficas

GIL, Carlos Antônio. **Como elaborar projetos de pesquisa**. 4. ed. São Paulo: Atlas, 2002.

CERT.BR. **Cartilha de Segurança para Internet. Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil,** Brasilia, 2016. Disponível em: <http://cartilha.cert.br/malware.> acesso em 15/10/2016

ZHENG B. et al. **The New Era of Botnets**, Santa Clara CA: McAfee Labs, 2010

COHEN, F. B. e COHEN, D. F. **A short course on computer viruses.** 2ª edição. John Wiley & Sons, Inc. New York, 1994

BABSON, B et al. **Active Network Based DDoS Defense**. Proceedings of the DARPA Active Networks Conference and Exposition. Em University at Albany, Albany. 2011

PAUL BÄCHER et al. **The nepenthes platform:** An efficient approach to collect malware. In Diego Zamboni and Christopher Krügel, editora RAID: volume 4219 do LNCS, paginas 165–184. Springer, 2006.

---

1 - Conforme disponível em:
<http://www.symantec.com/connect/blogs/regin-top-tier-espionage-tool-enables-stealthy-surveillance>
acesso em 21/out/2016;

2 - Conforme disponível em:
<http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/regin-analysis.pdf>
acesso em 21/out/2016;

3 - Conforme disponível em:
<http://www.politico.com/magazine/story/2016/09/hillary-clinton-emails-2016-server-state-department-fbi-214307>
acesso em 21/out/2016;

4 - Conforme disponível em:
<https://vault.fbi.gov/hillary-r.-clinton>
acesso em 21/out/2016;

5 - Conforme disponível em:
<https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet>
acesso em 20/out/2016;

6 - Conforme disponível em:
<https://intel.malwaretech.com/botnet/mirai/?h=24#>
acesso em 20/out/2016;

7 - Conforme disponível em:
<https://www.justice.gov/opa/file/763786/download>
acesso em 20/out/2016;

8 - Conforme disponível em:
<http://www.pcmag.com/article2/0,2817,2388652,00.asp>
<http://www.pcmag.com/article2/0,2817,2372364,00.asp>
acesso em 20/out/2016;

9 - Conforme disponível em:
<https://securelist.com/analysis/publications/35962/the-advertising-botnet/>
acesso em 10/nov/2016;

10 - Conforme disponível em:
<https://www.mysonicwall.com/sonicalert/searchresults.aspx?ev=article&id=292>
acesso em 10/nov/2016;

11 - Conforme disponível em:
<https://www.microsoft.com/security/portal/threat/encyclopedia/entry.aspx?Name=TrojanDownloader%3AWin32%2FPonmocup.A&ThreatID=146443>
acesso em 10/nov/2016;

12 - Conforme disponível em:
<http://www.eset.com/us/resources/white-papers/The_Evolution_of_TDL.pdf>
acesso em 10/nov/2016

13 - Conforme disponível em:
<https://www.secureworks.com/research/gozi>
acesso em 10/nov/2016;

14 - Conforme disponível em:
<http://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/>
acesso em 04/fev/2017;

15 - Conforme disponível em:
<https://www.iso.org/standard/16883.html>
acesso em 04/fev/2017.