Instituto Federal de Educação, Ciência
e Tecnologia de São Paulo
Câmpus Campinas - CTI Renato Archer

Sandnet

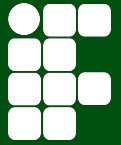
Análise de Tráfego de Rede Produzido por Software Malicioso

Daniel Teixeira - IFSP
Prof. Dr. Alencar de Melo Jr. - IFSP
Prof. Dr. André Ricardo Abed Grégio - UFPR

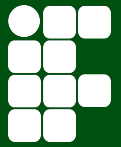
GTER 42 | GTS 28
VI Semana de Infraestrutura da Internet no Brasil

9 de Novembro de 2016

Agenda

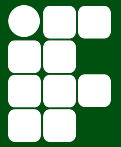


- Introdução
- Contextualização
- Metodologia
- Resultados e conclusões



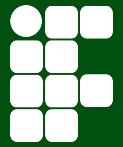
Introdução

- **431 milhões** de novas variantes de *malware* em 2015.
- Estudos sobre **comportamento** dos vírus.
- Análise dinâmica feita em ambientes ***Sandboxes***.
- Conectar à **Internet** sem comprometer outros dispositivos.



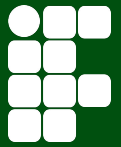
Objetivos

- Aprimorar a análise dinâmica através da emulação da Internet.
  - Definir uma arquitetura de rede para emular a Internet.
  - Implementar protocolos HTTP e DNS para emulação.
  - Integração da sandnet com a sandbox.



Justificativa

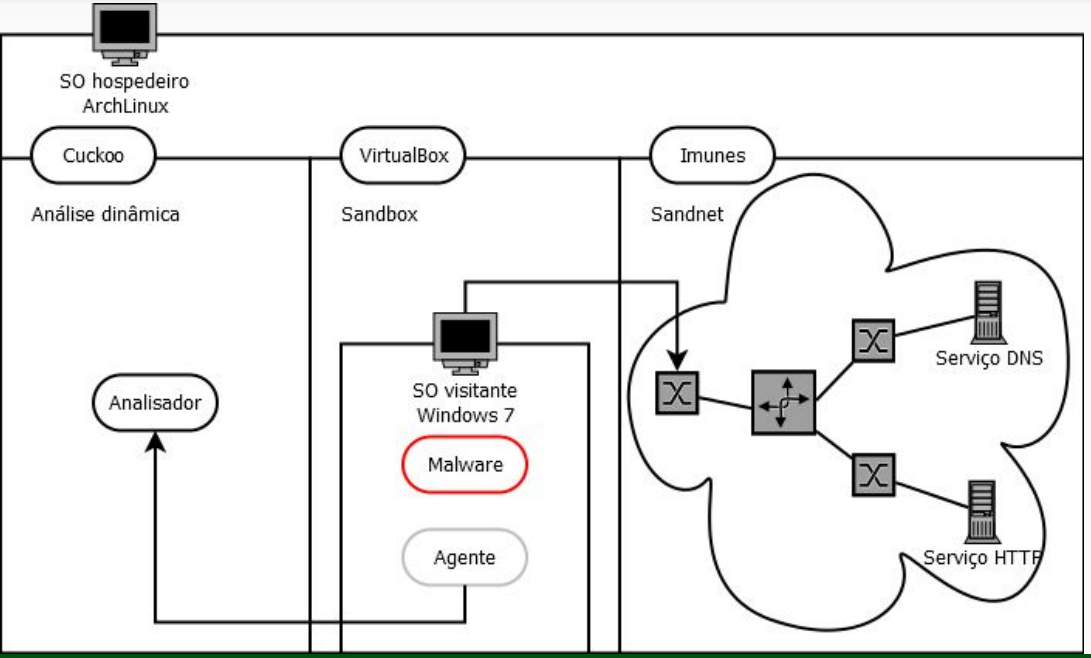
- Aumento de **132,45% de ataques DDoS** em 2015/2.
  - O maior ataque gerou atividades de **240 gigabits por segundo.**
- Exemplares de *malware* **se propagam** pela Internet.
- Análise dinâmica é **incompleta** se não houver acesso a Internet.
- Aprimorar análises dinâmicas com a ferramenta ***Sandnet***.



Metodologia

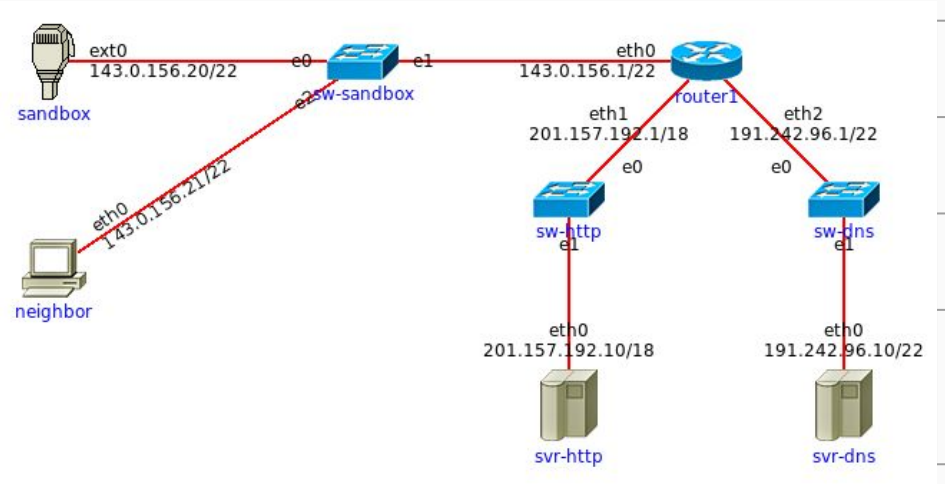
- Ferramenta de análise dinâmica e *sandbox*.
  - Cuckoo & VirtualBox
- Ferramenta para emular topologia da Internet.
  - Imunes
- Serviços de DNS e HTTP.
  - Bind9 lighttpd
- Ferramenta para coleta de dados de rede.
  - Wireshark

Metodologia

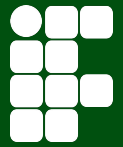


- **Cuckoo:** análise dinâmica.
- **Virtualbox:** *sandbox* com MV.
- **Imunes:** topologia de rede (*sandnet*).
- **Serviços de rede:** scripts e programas adaptados.

Sandnet

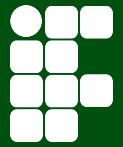


Nó	Endereço IP	Propósito
svr-http	201.157.192.10	HTTP
svr-dns	191.242.96.10	DNS
sandnet	143.0.156.20	Conecta com o Cuckoo



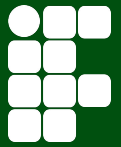
Resultados

- **57%** dos exemplares utilizaram a Internet.
- Atividade de rede em portas conhecidas como **445**.
- Tentativa de acesso a outros nós via protocolo **ICMP**.
- Resolução de endereços suspeitos: `fukyu.jp`
- **Download** de servidores suspeitos: `/updata/ACC13.jpg`



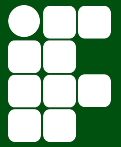
Conclusões

- Alternativa **viável** para análises de tráfego de rede.
- Análise dinâmica **aprimorada**.
- Segurança de ter uma Internet emulada e **contida**.



Trabalhos futuros

- Implementar outros serviços.
- Usar exemplares de outras regiões.
- Emular nós por endereços IP.
- Utilizar a Sandnet como *proxy*.



Referências

AHRENHOLZ, J. Comparison of CORE network emulation platforms. 2010 - MILCOM 2010 MILITARY COMMUNICATIONS CONFERENCE. Anais...IEEE, out. 2010 Disponível em: <http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5680218>

AKAMAI TECHNOLOGIES. Akamai's State of the Internet Security Report Q2 2015. Disponível em: <https://www.akamai.com/us/en/multimedia/documents/content/akamai-state-of-the-internet-security-report-q2-2015.pdf>. Acesso em: 20 out. 2015.

BICKING, I. Virtualenv. Disponível em: <https://virtualenv.pypa.io/en/stable/>. Acesso em: 1 jun. 2016.

BOTACIN, M. F.; GRÉGIO, A. R. A.; DE GEUS, P. L. Uma Visão Geral do Malware Ativo no Espaço Nacional da Internet entre 2012 e 2015. p. 1–10, 2015.

CUCKOO FOUNDATION. Automated Malware Analysis - Cuckoo Sandbox. Disponível em: <http://www.cuckoosandbox.org>. Acesso em: 1 dez. 2015.

DOCKER INC. Docker. Disponível em: <https://www.docker.com/>. Acesso em: 1 jun. 2016.

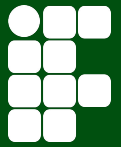
EGELE, M. et al. A survey on automated dynamic malware analysis techniques and tools. ACM Computing Surveys, v. V, n. 2, p. 1–49, 1 fev. 2011.

GALAL, H. S.; MAHDY, Y. B.; ATIEA, M. A. Behavior-based features model for malware detection. Journal of Computer Virology and Hacking Techniques, v. 12, n. 2, p. 59–67, 4 maio 2016.

GRAZIANO, M.; LEITA, C.; BALZAROTTI, D. Towards network containment in malware analysis systems. Proceedings of the 28th Annual Computer Security Applications Conference on - ACSAC '12. Anais...: ACSAC '12.New York, New York, USA: ACM Press, 2012.

ISSA, A. Anti-virtual machines and emulations. Journal in Computer Virology, v. 8, n. 4, p. 141–149, 19 nov. 2012.

KERRISK, M. namespaces(7) - Linux manual page. Disponível em: <http://man7.org/linux/man-pages/man7/namespaces.7.html>. Acesso em: 1 dez. 2015.



Referências

KNESCHKE, J. LIGHTTPD, fly light. Disponível em: <https://www.lighttpd.net/>. Acesso em: 28 maio. 2016.

MONGODB INC. MongoDB. Disponível em: <https://www.mongodb.com/>. Acesso em: 1 jun. 2016.

MOSER, A.; KRUEGEL, C.; KIRDA, E. Exploring Multiple Execution Paths for Malware Analysis. 2007 IEEE Symposium on Security and Privacy (SP '07). Anais...IEEE, maio 2007 Disponível em: <http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=4223228>

NAPPA, A.; RAFIQUE, M. Z.; CABALLERO, J. The MALICIA dataset: identification and analysis of drive-by download operations. International Journal of Information Security, v. 14, n. 1, p. 15–33, 21 fev. 2015.

OPEN VSWITCH COMMUNITY. Open vSwitch. Disponível em: <http://openvswitch.org/>. Acesso em: 1 jun. 2016.

ORACLE. VirtualBox. Disponível em: <https://www.virtualbox.org/>. Acesso em: 1 jun. 2016.

PROVATAKI, A.; KATOS, V. Differential malware forensics. Digital Investigation, v. 10, n. 4, p. 311–322, dez. 2013.

PYTHON SOFTWARE FOUNDATION. Python Programming Language. Disponível em: <http://www.python.org/>. Acesso em: 1 jun. 2016.

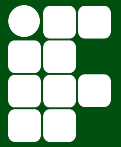
RODRIGUEZ, R. J.; RODRIGUEZ GASTON, I.; ALONSO, J. Towards the Detection of Isolation-Aware Malware. IEEE Latin America Transactions, v. 14, n. 2, p. 1024–1036, fev. 2016.

ROSSOW, C. et al. Sandnet: Network traffic analysis of malicious software. Proceedings of the First Workshop on Building Analysis Datasets and Gathering Experience Returns for Security - BADGERS '11. Anais...: BADGERS '11.New York, New York, USA: ACM Press, 2011.

SCHILLER, C. et al. Botnets: The Killer Web Applications. [s.l.] Syngress Publishing, 2007.

STEWART, J. Behavioural malware analysis using Sandnets. Computer Fraud & Security, v. 2006, n. 12, p. 4–6, dez. 2006.

SYMANTEC CORPORATION. 2015 Symantec Internet Security Threat Report.



Referências

UNIVERSITY OF ZAGREB. Imunes. Disponível em: <http://imunes.net/>. Acesso em: 1 jun. 2016.

VASILESCU, M.; GHEORGHE, L.; TAPUS, N. Practical malware analysis based on sandboxing. 2014 RoEduNet Conference 13th Edition: Networking in Education and Research Joint Event RENAM 8th Conference. Anais...IEEE, set. 2014 Disponível em: <http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6955304>

VINET, J.; GRIFFIN, A. Arch Linux. Disponível em: <https://www.archlinux.org/>. Acesso em: 1 jun. 2016.

ZEC, M.; MIKUC, M. Operating system support for integrated network emulation in imunes. First Workshop on Operating System and Architectural Support for the on demand IT InfraStructure, 2004.

ZHUGE, J. et al. Studying Malicious Websites and the Underground Economy on the Chinese Web. In: JOHNSON, M. E. (Ed.). . Managing Information Risk and the Economics of Security. Boston, MA: Springer US, 2009. p. 225–244.

Obrigado

Daniel Teixeira
daniel.t.dt+ifsp@gmail.com

Dúvidas?