Malware Behavior

André Grégio[1]**, Mario Jino (Orientador)**[2]**, Paulo Lício de Geus (Co-Orientador)**[3]

[1]Divisão de Segurança de Sistemas de Informação (DSSI)
Centro de Tecnologia da Informação Renato Archer (CTI) – Campinas – SP – Brazil

[2]Faculdade de Engenharia Elétrica e da Computacão (FEEC)
Universidade Estadual de Campinas (Unicamp) – Campinas – SP – Brazil

[3]Instituto de Computação (IC)
Universidade Estadual de Campinas (Unicamp) – Campinas– SP – Brazil

{gregio,paulo}@lasca.ic.unicamp.br, jino@dca.fee.unicamp.br

Abstract. *Malware attacks are the most dangerous current threat to computer systems security. The main mechanism used for protection against malware is the antivirus, which does not provide sufficient information about the infection and may be easily bypassed by obfuscation and anti-analysis techniques. Therefore, we need to deeply understand what malware samples do during an attack so as to develop effective defense mechanisms. In this work, we delve into malware behavior to propose (i) an extensible, behavior-centric taxonomy, (ii) a dynamic analysis system that extracts behavioral profiles, (iii) detection techniques for Internet Banking malware, (iv) a visualization tool for execution traces, and (v) an instruction-based clustering technique to identify families and code reuse.*

Resumo. *O ataque por* malware *é uma das ameaças mais perigosas para a segurança de sistemas. O principal mecanismo de proteção utilizado é o antivírus, que não provê informações suficientes sobre a infecção e pode ser facilmente superado por técnicas de ofuscação e anti-análise. Logo, é necessário um entendimento profundo sobre as atividades de* malware *durante ataques para que se desenvolva mecanismos de defesa efetivos. Neste trabalho, explora-se o comportamento de* malware *e propõe-se (i) uma taxonomia estensível baseada em comportamento, (ii) um sistema de análise dinâmica que extrai perfis comportamentais, (iii) técnicas para detecção de* malware *para Internet Banking, (iv) ferramentas de visualização de traços de execução e (v) uma técnica de agrupamento baseada em instruções para identificar famílias e reuso de código.*

1. Introduction

The spread of malicious programs through computer networks, mainly the Internet, has been a major threat to the security of interconnected systems. Malicious programs, commonly referred to as **malware**, can be understood as applications whose intent is to compromise a system. Those applications are commonly named as viruses, worms, Trojans, backdoors, keyloggers, and so on. One of the greatest motivations for malware attacks is the underground economy that is already established [Fallmann et al. 2010] [Holz et al. 2009] [Stone-Gross et al. 2011b], based on compromised infrastructures renting (e.g., network-connected systems that are invaded and remote controlled by attackers, such as botnets), sensitive information stealing (e.g., Internet Banking credentials, usernames and passwords of e-mail accounts, credit card numbers) [Stringhini et al. 2012], unsolicited messages (e.g., spam, fake product offers) [Levchenko et al. 2011] [Stone-Gross et al. 2011a] and advertisement clicking [Lauinger et al. 2012]. Thus, the identification of a program as being a known malware (already collected and analyzed, maybe defeated) allows for efficient and effective incident response. The countermeasures taken, for its part, can facilitate the damage containment process, decrease losses, and mitigate side infections through security blocking rules and patch application.

Currently, one of the most popular defense mechanism against malware is still the antivirus (AV). However, the major issue regarding AV engines is the frequent and increasing rise of malware variants. Malware variants correspond to previously identified malware families modified until they either do not match a known signature or are able to evade, compromise or subvert the protection mechanisms to remain stealthy. Another issue that must be taken into account is that malware developers have been embedding self-defense mechanisms to their products, i.e. current malware may disable the operating system native protection (e.g., firewall, AV, security plugins, updates), verify if it is under some kind of analysis and do not present its malicious behavior (e.g., by modifying its execution on-the-fly), be packed in a way that avoids analysis and detection (e.g., checking its integrity in memory), disguise itself as a system application, a legitimate software, or a fake antivirus, and so on.

Apart from those aforementioned issues, the AV developers' community is still not tied to a common standard to classify detected malware samples. This slows malware-related incident response procedures, turning them ineffective in certain cases. Nowadays, the boundaries that divide a malware class from another do not exist anymore, since modern malware samples are usually built on functional modules that exhibit, at the same time, the behavior expected from rootkits, Trojan horses, worms, viruses, flooders, spammers and botclients. In this thesis, we address issues related to malware behavior and provide the contributions mentioned in Section 2.

1.1. Objectives

The main goal of this thesis is to provide means to identify malicious behavior in unknown programs, i.e., those not detected by antivirus. To do so, we studied how malware behaves (using a practical approach) and how to use the information acquired from the observed behaviors. The aim is to develop detection techniques, as well as a more meaningful classification scheme, in order to handle the damage malware can cause to an infected system. To this end, forwarding this point, we present the research work done in the context of a Ph.D. thesis as a proposal of addressing the aforementioned needs, aiming to respond to malware incidents in a useful, organized and understandable manner. This is accomplished through the extraction of malicious behavior using a dynamic analysis system that we have been developing, the proposal of a behavior-based taxonomy for classification, the addition of modules for the detection of specialized malware (bankers) and visualization of malware execution traces, and, finally, the introduction of a clustering algorithm to address malware behavior at instruction level.

2. Contributions

The field of malware research is very broad and plenty of effort has been spent by the security community to address the several types of threats that malicious code poses to Internet-connected systems. In this thesis, the focus is on malware behavior and in what can be done with them concerning computer systems defense. Thus, in addition to defining dangerous behaviors and malware classes based on them, we also apply the behavioral profiling on other topics, such as detection, classification, clustering, code reuse identification, visualization and incident response. The main contributions of this thesis are:

- A brief review of the history of malicious programs, a discussion about the current malware naming scheme issues and antivirus labeling, and a survey on the diversity of malware taxonomies according to their types (e.g., worms, bots).
- A definition of the different types of behavior that a malicious program can present, the description of a set of dangerous activities gathered from actually analyzed samples, and the proposal of a behavior-centric malware taxonomy.
- A malware dynamic analysis system that inspects for suspicious behaviors and extracts behavioral profiles from monitored programs.
- An approach to detect information stealing malware that leverages a subset of the defined behaviors and image processing techniques.
- Interactive visualization tools to help in identifying similar behavioral patterns.
- A heuristic to cluster malware based on their memory and registers writing values, as well as an application of this technique to identify code reuse among malware samples from different families.

The thesis full text is available at `http://www.las.ic.unicamp.br/paulo/teses/20121128-PhD-Andre.Ricardo.Abed.Gregio-Malware.behavior.pdf`.

2.1. Behavioral Analysis

Existing taxonomies either address only one type of malware class [Weaver et al. 2003][Cooke et al. 2005][Dagon et al. 2007] [Boldt et al. 2004][Saroiu et al. 2004][Rutkowska 2006], or are closely tied to the standard classes and the current naming schemes [Filiol 2005][Karresand 2003]. Malicious programs behave most of the time similarly to benign programs. Therefore, to "analyze" a program, we need to pinpoint aspects of its behavior that serve to the purpose of characterizing malignity in it. Thus, we defined the **general behavior** and the **suspicious behavior** of a program. We consider the general behavior of a program as the set of actions—tuples "α_i" composed by source, operation (create, delete, write, terminate), object (file, process, network, registry, mutex, memory), and target—performed during its execution by an operating system.

The set of actions that compose a behavior can be divided into groups according to their nature: if an action interferes with the environment, i.e. changes the state of the system, it is part of an **active** subset of the behavior, otherwise, it is **passive**. There is also a subset of the general behavior that is **neutral**, i.e. the actions can be either active or passive, but they do not lead to a malign outcome. When a malicious program is executed, each of its actions can be considered suspicious, revealing important details about the infection. Hence, we define the suspicious behavior as follows:

Definition 1 *Let M_k be a sample whose general behavior $B(M_k)$ is divided into the active behavior $B_A(M_k)$ and the passive behavior $B_P(M_k)$. Then, $B(M_k) = B_A(M_k) \cup B_P(M_k)$. Let $B_N(M_k)$ be the malware's neutral behavior so that $B_N(M_k) \in B_A(M_k) \cup B_P(M_k)$. Thus, the suspicious behavior $B_S(M_k)$ is equal to $B_A(M_k) - B_N(M_k)$.*

Based on this, we proposed a naming scheme to identify potentially dangerous behaviors in unknown programs, producing the taxonomy shown in Table 1. Moreover, we evaluated over 12 thousand known malware samples collected from phishing e-mail messages, honeypots, public datasets and colleagues' cooperation. We submitted them to three antivirus engines in order to obtain their detection labels. At the time of scanning, $\approx 20\%$ of them were undetected by the selected AVs, $\approx 50\%$ were undecided, i.e., the AV did not agree with the detection label, and the remainder samples were labeled similarly. Then, the samples were submitted to dynamic analysis with our system, BehEMOT (Behavioral Evaluation of Malicious ObjecTs), which inspected for suspicious behaviors. This allowed us to perform the behavioral profiling of the monitored programs, as well as to identify these "unknown"—or "clean"–programs as suspicious (Figure 1).

Table 1. Proposed malware classes, suspicious behaviors and associated labels.

Class	Behavior	Label
Evader	Removal of Evidence	RemEvd [RE]
	Removal of Registries	RemReg [RR]
	AV Engine Termination	TerAVe [TA]
	Firewall Termination	TerFwl [TF]
	Notification of Updates Termination	TerUpd [TU]
	Language Checking	LngChk (Suspicious) [LC]
Disrupter	Scanning of Known-Vulnerable Service	VulScn [VS]
	E-mail Sending (Spam)	EmlSpm [ES]
	IRC/IM Known Port Connection	IrcPrt [IP]
	IRC/IM Unencrypted Commands	IrcCom [IC]
Modifier	Creation of New Binary	NewBin [NB]
	Modification of Existing System Binary	ChgBin [CB]
	Creation of Unusual Mutex	UnkMut [UM]
	Modification of the Name Resolution File	HstChg [HC]
	Modification of the Browser Proxy Settings	PacLdn [PL]
	Modification of the Browser Behavior	BhoInj [BI]
	Persistence	Persis [Pe]
	Download of Known Malware	DldKmw [DK]
	Download of Unknown File	DldUnk [DU]
	Driver Loading	DrvLdn [DL]
Stealer	Stealing of System/User Data	InfStl [IS]
	Stealing of Credentials or Financial Data	CrdStl [CS]
	System/user Information Reading	InfRdn (Suspicious) [IR]
	Process Hijacking	PrcHjk [PH]

We used our dynamic analysis system (BehEMOT) and knowledge about malware behavior to detect bankers, proposing BanDIT (Banker Detection and Infection Tracker). BanDIT employs a methodology composed of file system change identification, network traffic pattern matching, and image processing. Thus, we were able to identify whether a

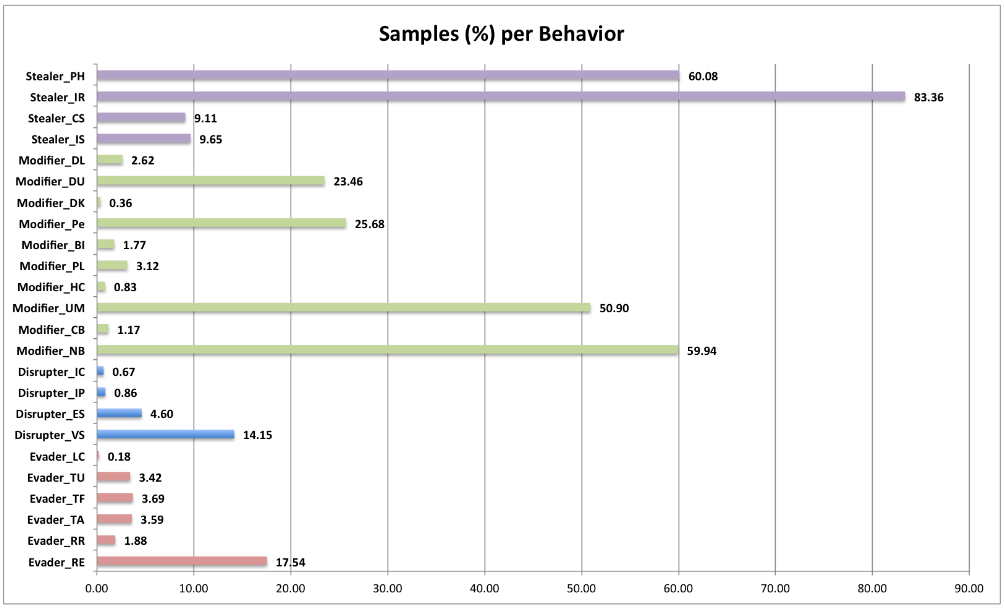

Figure 1. Behaviors observed in evaluated samples.

malware is a banker or not in 98.8% of cases, as well as to find IP and e-mail addresses involved in malware attacks.

We also used BehEMOT's output to search for visual similarities among execution behavior of malware samples assigned to the same family, as illustrated in Figure 2. Finally, we introduced another way for the extraction of behavioral profiles: to trace the malware execution using a debugger and to log arithmetic and logic instructions that modify values in memory or registers. To this end, we proposed a clustering algorithm able to group samples with a certain level of similarity, whose results may be used in the search of code reuse among malware.

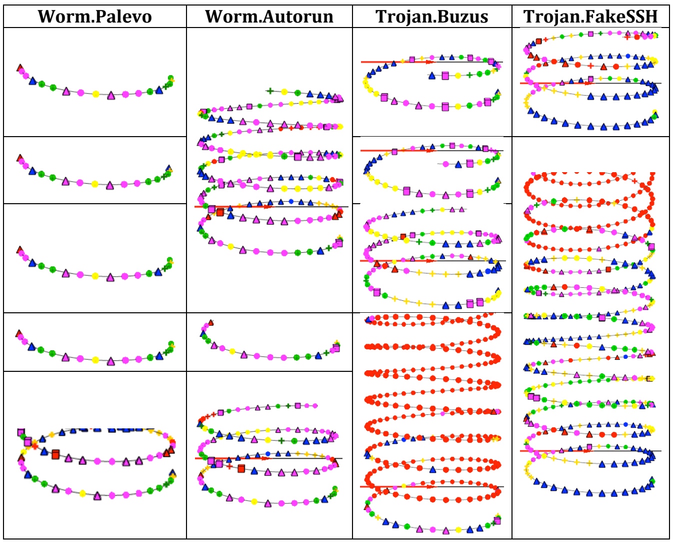

Figure 2. Visualization of execution behavior extracted from malware families.

3. Publications

The following list includes the published results related to this thesis (I assisted in the mentoring of the students whose papers I am not the first author). Most of them (international and national) are ranked by Brazilian Qualis Ranking 2012-2014.

1. **An Empirical Analysis of Malicious Internet Banking Software Behavior.** André Ricardo Abed Grégio, Vitor Monte Afonso, Victor Furuse Martins, Dario Simões Fernandes Filho, Paulo Lício de Geus, Mario Jino. ACM Symposium on Applied Computing (SAC). Coimbra, Portugal, March, 2013. **Qualis A1**.
2. **Tracking Memory Writes for Malware Classification and Code Reuse Identification.** André Ricardo Abed Grégio, Paulo Lício de Geus, Christopher Kruegel, Giovanni Vigna. 9th Conf. on Detection of Intrusions and Malware and Vulnerability Assessment (DIMVA), LNCS, Springer. Greece, July 2012. **Qualis B1**.
3. **Pinpointing Malicious Activities through Network and System-Level Malware Execution Behavior.** André Ricardo Abed Grégio, Vitor Monte Afonso, Dario Simões Fernandes Filho, Paulo Lício de Geus, Mario Jino, Rafael Duarte Coelho dos Santos. 12th International Conference on Computational Science and Its Applications (ICCSA), LNCS, Springer Verlag. Brazil, June 2012. **Qualis B1**.
4. **Interactive, Visual-Aided Tools to Analyze Malware Behavior.** André Ricardo Abed Grégio, Alexandre Or Cansian Baruque, Vitor Monte Afonso, Dario Simões Fernandes Filho, Paulo Lício de Geus, Mario Jino, Rafael Duarte Coelho dos Santos. 12th International Conference on Computational Science and Its Applications (ICCSA), LNCS, Springer Verlag. Brazil, June 2012. **Qualis B1**.
5. **A Hybrid Framework to Analyze Web and OS Malware.** Vitor Monte Afonso, Dario Simões Fernandes Filho, André Ricardo Abed Grégio, Paulo Lício de Geus, Mario Jino. IEEE International Conference on Communications (ICC), Proceedings of the IEEE ICC'12. Canada, June 2012. **Qualis A2**.
6. **A Malware Detection System Inspired on the Human Immune System.** Isabela Liane Oliveira, André Ricardo Abed Grégio, Adriano Mauro Cansian. 12th International Conference on Computational Science and Its Applications (ICCSA), LNCS, Springer Verlag. Brazil, June 2012. **Qualis B1**.
7. **Behavioral analysis of malicious code through network traffic and system call monitoring.** André Ricardo Abed Grégio, Dario Simões Fernandes Filho, Vitor Monte Afonso, Rafael Duarte Coelho dos Santos, Mario Jino, Paulo Lício de Geus. Defense, Security and Sensing 2011, Proc. of SPIE. USA, April 2011.
8. **Visualization techniques for malware behavior analysis.** André Ricardo Abed Grégio, Rafael Duarte Coelho dos Santos. Defense, Security and Sensing 2011, Proceedings of SPIE. USA, April 2011.
9. **A hybrid system for analysis and detection of web-based client-side malicious code.** Vitor Monte Afonso, André Ricardo Abed Grégio, Dario Simões Fernandes Filho, Paulo Lício de Geus. IADIS International Conference WWW/Internet (ICWI'2011), Proceedings of ICWI, 2011. **Qualis B2**.
10. (In Portuguese) **Análise Visual de Comportamento de Código Malicioso.** Alexandre Or Cansian Baruque, André Ricardo Abed Grégio, Paulo Lício de Geus. Workshop de Trabalhos de Iniciação Científica e de Graduação (WTICG), Anais do XI SBSEG. Brazil, 2011.

11. (In Portuguese) **Sistema de coleta, análise e detecção de código malicioso baseado no sistema imunológico humano.** Isabela Liane Oliveira, André Ricardo Abed Grégio, Adriano Mauro Cansian. Conferência IADIS Ibero-Americana WWW/Internet (CIAWI), Anais da CIAWI, 2011.
12. (In Portuguese) **Análise Comportamental de Código Malicioso através da Monitoração de Chamadas de Sistema e Tráfego de Rede.** Dario Simões Fernandes Filho, André Ricardo Abed Grégio, Vitor Monte Afonso, Rafael Duarte Coelho dos Santos, Mario Jino, Paulo Lício de Geus. Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSEG), Anais do X SBSEG. Brazil, October 2010. **Qualis B4**.
13. (In Portuguese) **xFile: Uma Ferramenta Modular para Identificação de Packers em Executáveis do Microsoft Windows.** Victor Furuse Martins, André Ricardo Abed Grégio, Vitor Monte Afonso, Dario Simões Fernandes Filho, Paulo Lício de Geus. Workshop de Trabalhos de Iniciação Científica e de Graduação (WTICG), Anais do X SBSEG. Brazil, October 2010.
14. **Malware distributed collection and pre-classification system using honeypot technology.** André Ricardo Abed Grégio, Isabela Liane Oliveira, Rafael Duarte Coelho dos Santos, Adriano Mauro Cansian, Paulo Lício de Geus. Data Mining, Intrusion Detection, Information Security and Assurance, and Data Networks Security. Proceedings of SPIE Defense, Security and Sensing, USA, 2009.
15. (In Portuguese) [*Book Chapter*] **Técnicas para Análise Dinâmica de Malware.** Dario Simões Fernandes Filho, Vitor Monte Afonso, Victor Furuse Martins, André Ricardo Abed Grégio, Paulo Lício de Geus, Mario Jino, Rafael Duarte Coelho dos Santos. Minicursos do SBSEG 2011, pp.107–147, SBC, Brazil, 2011.

4. Conclusion

This document discussed several aspects related to the behavior of malicious programs, from the definition of potentially dangerous activities performed during an infection and the proposition of a behavior-based taxonomy, to the detection, clustering and visualization of malware. Our main objective is to provide a better understanding of how the diversity of current malware samples actually behave, as well as to aid in the development of practical and effective incident response procedures. To that extent, we discussed malware history and existing taxonomies, as well as introduced our own general and extensible taxonomy. Our proposal, yet of simple use and easy to understand, provides an overall view of malware infection. We evaluated the proposed behavior-centric taxonomy with over 12 thousand malware samples collected in the wild, showing that our analysis allows the identification of suspicious behaviors even in malware undetected by antiviruses. We also presented a system for Internet Banking malware detection, which was builti upon our dynamic analysis system. In addition, we leverage two interactive visualization tools that take advantage of behavioral profiles to aid in computer security incident response procedures. Furthermore, we introduce a novel way to classify malware with a good precision ($> 80\%$) that considered the values written in memory or registers.

References

Boldt, M., Carlsson, B., and Jacobsson, A. (2004). Exploring Spyware Effects. In *Nordic Workshop on Secure IT Systems (NORDSEC)*, Helsinki, Finland.

Cooke, E., Jahanian, F., and McPherson, D. (2005). The zombie roundup: understanding, detecting, and disrupting botnets. In *Proceedings of the Steps to Reducing Unwanted Traffic on the Internet on Steps to Reducing Unwanted Traffic on the Internet Workshop*, SRUTI'05, pages 39–44, Berkeley, CA, USA. USENIX Association.

Dagon, D., Gu, G., Lee, C. P., and Lee, W. (2007). A Taxonomy of Botnet Structures. In *23rd Annual Computer Security Applications Conference (ACSAC)*, pages 325–339.

Fallmann, H., Wondracek, G., and Platzer, C. (2010). Covertly probing underground economy marketplaces. In *Seventh Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA)*.

Filiol, E. (2005). *Computer viruses: from theory to applications*. Springer.

Holz, T., Engelberth, M., and Freiling, F. (2009). Learning more about the underground economy: a case-study of keyloggers and dropzones. In *Proceedings of the 14th European conference on Research in computer security*, ESORICS'09, pages 1–18.

Karresand, M. (2003). Separating Trojan Horses, Viruses and Worms - A Proposed Taxonomy of Software Weapons. In *IEEE Information Assurance Workshop*.

Lauinger, T., Kirda, E., and Michiardi, P. (2012). Paying for piracy? an analysis of one-click hosters' controversial reward schemes. In *15^{th} Internationa Symposium on Research in Attacks, Intrusions and Defenses (RAID)*.

Levchenko, K., Pitsillidis, A., Br, N. C., Halvorson, T., Kanich, C., Kreibich, C., Liu, H., Mccoy, D., Weaver, N., Paxson, V., Voelker, G. M., and Savage, S. (2011). Click trajectories: End-to-end analysis of the spam value chain. In *In Proceedings of IEEE Symposium on Security & Privacy*, pages 431–446.

Rutkowska, J. (2006). Introducing Stealth Malware Taxonomy. `http://invisiblethings.org/papers/malware-taxonomy.pdf`. Acesso realizado em 28 de fevereiro de 2012.

Saroiu, S., Gribble, S. D., and Levy, H. M. (2004). Measurement and Analysis of Spyware in a University Environment. In *Proceedings of the ACM/USENIX Symposium on Networked Systems Design and Implementation (NSDI)*, pages 141–153.

Stone-Gross, B., Abman, R., Kemmerer, R., Kruegel, C., Steigerwald, D., and Vigna, G. (2011a). The Underground Economy of Fake Antivirus Software. In *Proceedings of the Workshop on Economics of Information Security (WEIS)*.

Stone-Gross, B., Holz, T., Stringhini, G., and Vigna, G. (2011b). The Underground Economy of Spam: A Botmaster's Perspective of Coordinating Large-Scale Spam Campaigns. In *USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET)*.

Stringhini, G., Egele, M., Kruegel, C., and Vigna, G. (2012). Poultry markets: On the underground economy of twitter followers. In *Workshop on Online Social Network (WOSN)*. ACM.

Weaver, N., Paxson, V., Staniford, S., and Cunningham, R. (2003). A Taxonomy of Computer Worms. In *Proceedings of the 2003 ACM Workshop on Rapid Malcode (WORM)*, pages 11–18, New York, NY, USA.