Available online at www.sciencedirect.com

SciVerse ScienceDirect

www.elsevier.com/locate/ijcip

Crimeware-as-a-service—A survey of commoditized crimeware in the underground market

Aditya K. Sood[*], *Richard J. Enbody*

Department of Computer Science and Engineering, Michigan State University, East Lansing, Michigan 48824, USA

ARTICLE INFO

Article history:
Received 19 September 2012
Received in revised form
7 January 2013
Accepted 12 January 2013
Available online 18 January 2013

Keywords:
Cyber crime
Underground economy
Commoditized crimeware
Crimeware-as-a-service

ABSTRACT

Crimeware-as-a-service (CaaS) has become a prominent component of the underground economy. CaaS provides a new dimension to cyber crime by making it more organized, automated, and accessible to criminals with limited technical skills. This paper dissects CaaS and explains the essence of the underground economy that has grown around it. The paper also describes the various crimeware services that are provided in the underground market.

1. Introduction

Crimeware-as-a-service (CaaS) is a business model used in the underground market where illegal services are provided to help underground buyers conduct cyber crimes (such as attacks, infections, and money laundering) in an automated manner. The term CaaS is analogous to software-as-a-service (SaaS)—a software delivery model where services are available upon request.

Cyber crime is an epidemic that is affecting today's information society [17,18]. The first cyber criminals were mostly hackers who trespassed in the cyber world for the challenge and thrill. Sometimes, their actions resulted in significant financial losses to victims, but little or no financial gain to themselves. CaaS has enabled cyber criminals to amass significant financial rewards from cyber crime. A recent study by Anderson et al. [20] on the cost of cyber crime estimates the annual losses in the billions of dollars. The study provides extensive details about cyber crime losses by classifying them into direct losses, criminal revenue, indirect losses and indirect costs. Other researchers have proposed cyber crime classification frameworks [21,22]. The frameworks provide insights into the methods chosen by cyber criminals to execute scams for financial gain.

Early cyber criminals compromised systems and stole money for their personal benefit, tackling the technical challenges themselves. Now, there is a separation of technical cyber skills from more traditional non-cyber criminal skills such as money laundering. Technically-savvy criminals are developing cyber crime tools that non-technical criminals can use. An underground economy has grown around these tools to meet the demand. In particular, a SaaS model is emerging within this context, which we refer to as crimeware-as-a-service (CaaS). In the CaaS model, all that the underground buyer has to do is to purchase a crimeware service and a compromised infrastructure. The buyer does not have to worry about compromising an infrastructure, infecting systems, launching distributed denial-of-service (DDoS) attacks or stealing credit card information because these are done automatically by the cyber criminal who provides the crimeware service.

This paper seeks to shed light on the advancements in the underground economy and to show how easy it has become

[*]Corresponding author.
E-mail address: soodadit@cse.msu.edu (A.K. Sood).

1874-5482/$ - see front matter © 2013 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.ijcip.2013.01.002

to conduct cyber-criminal activities. The methodology is based on the concept of active infiltration of malicious domains that serve malware as a part of phishing attacks. This tactic is followed to understand the complete lifecycle of malware infections and the associated attack elements. In addition, an analysis is provided of a number of underground forums that are used explicitly for running crimeware services business. Finally, the CaaS model is examined to identify the crimeware services provided in the underground market that have resulted in a significant increase in cyber crime.

2. Related work

Numerous security researchers have conducted cyber crime research to gain an understanding of the underground economy. Grier et al. [1] have conducted a study on the emergence of the exploit-as-a-service (EaaS) model that is used to execute drive-by-download attacks. It is an art of exploitation in which users are forced to visit malicious domains, which host automated frameworks that exploit vulnerabilities in browsers to distribute malware. The EaaS model was introduced as a part of an automated browser exploitation framework. The research indicated that at least 32 malware families use browser exploit packs to deliver exploits to remote users.

Cova et al. [3] have developed a system that analyzes malicious JavaScript code used in drive-by-download attacks. They use a mix of anomaly and emulation based tactics combined with machine learning to verify the authenticity and integrity of JavaScript code that runs on target websites.

On a similar front, Provos et al. [4] have conducted a detailed study on drive-by-download attacks. They collected billions of URLs over a period of 10 months and discovered that approximately three million URLs were used to conduct drive-by-download attacks on the Internet. The study also presents details about users' browsing habits and their understanding of malware.

Caballero et al. [2] have examined the impact of pay-per-install (PPI) services used in the distribution of malware. The study revealed that twelve of the top 20 malware families use PPI services. Stevens [5] has also presented details of the business model chosen by underground sellers to sell PPI services. Polychronakis et al. [6] have explored the lifecycle of web-based malware and have analyzed drive-by-download attacks by focusing primarily on the command and control (C&C) protocols used by malware after infecting a machine.

Franklin et al. [7] have conducted a measurement study that provides better insight into the commodity services used by the underground community; in particular, they measured the threats and prioritized the defenses (including identifying the security vulnerabilities present in underground market products). Miller [8] has noted the existence of a black market that sells and purchases zero-day exploits, i.e., malware that exploits a vulnerability before it is actually disclosed to the software vendor or developer. Gross et al. [11] have discussed the use of rogue anti-virus software installed by malware after a successful infection; the vast majority of this anti-virus software prompts users to pay for security services that do not provide any protection. The initial infection usually occurs as a result of a successful social engineering attack.

An empirical study by Levchenko et al. [12] discusses the details of the spam value chain in end-to-end systems; in particular, they describe a resource-based spam monetization framework to show how business interests are fulfilled using spam. The empirical study revealed that approximately 95% of pharmaceutical and software spam are monetized using custom merchant services.

Leontiadis et al. [15] have investigated the impact of the exploitation of online search engine queries to promote illegal sales of prescription drugs. The study focused on search-redirection attacks in which high ranking websites are compromised and users are forced to visit malicious domains on the fly. John et al. [16] have conducted an in-depth study of exploitation tactics such as search engine optimization (SEO) that are used by attackers to poison search engine queries in order to distribute malware. This study revealed that the top searches in Google and Bing often contain malicious links.

Anderson [9] introduced new terms such as "incentive failures" and "perverse economic incentives" to reflect the losses incurred by users as a result of security failures. Managing security failures and breaches is a challenge to vendors. In a study of online crime, Moore et al. [10] have discussed the similarities and differences in the economics of online cyber crime and conventional crime. Motoyama et al. [13] have studied the emergence of underground forums as a social marketplace and how reputations are developed over time; in particular, this study projects the dynamics of underground forums that support underground market business activities on a large scale. In another study of the underground economy, Thomas and Martin [14] listed several issues with underground forums that make them easy targets for pursuing and prosecuting the miscreants (e.g., forum web servers do not provide enough privacy and protection, which facilitates monitoring). All these studies show that malware authors have monetized the underground market by leveraging the concept of a service culture to spread infections and distribute malware.

3. CaaS—A distribution model

CaaS participants engage a common model in the underground economy. The model involves three basic steps. First, a technically-skilled producer (operator) designs and builds a complete crimeware framework (CaaS) that is hosted on a centralized environment for easy access. Second, an advertiser representing the producer advertises the CaaS on underground forums and Internet Relay Chat (IRC) servers. Third, a buyer purchases the advertised crimeware services for personal gain. Sometimes, the middleman and advertiser are bypassed so that the producer and buyer can deal directly with each other. For protection, most underground sellers have Internet chat request (IRQ) codes and jabber contact ids for dealing anonymously in the underground market. Fig. 1 provides a graphical representation of the CaaS distribution model.

The distribution model presented in Fig. 1 works well for underground marketers. The cost involved in running an