Industrial Espionage and Targeted Attacks: Understanding the Characteristics of an Escalating Threat

Olivier Thonnard[1], Leyla Bilge[1],
Gavin O'Gorman[2], Seán Kiernan[2], and Martin Lee[3]

[1] Symantec Research Labs, Sophia Antipolis, France
{Olivier_Thonnard,Leylya_Yumer}@symantec.com
[2] Symantec Security Response, Ballycoolin Business Park, Dublin, Ireland
{Gavin_OGorman,Sean_Kiernan}@symantec.com
[3] Symantec.cloud, Gloucester, UK
Martin_Lee@symantec.com

Abstract. Recent high-profile attacks against governments and large industry demonstrate that malware can be used for effective industrial espionage. Most previous incident reports have focused on describing the anatomy of specific incidents and data breaches. In this paper, we provide an in-depth analysis of a large corpus of targeted attacks identified by Symantec during the year 2011. Using advanced TRIAGE data analytics, we are able to attribute series of targeted attacks to attack campaigns quite likely performed by the same individuals. By analyzing the characteristics and dynamics of those campaigns, we provide new insights into the modus operandi of attackers involved in those campaigns. Finally, we evaluate the prevalence and sophistication level of those targeted attacks by analyzing the malicious attachments used as droppers. While a majority of the observed attacks rely mostly on social engineering, have a low level of malware sophistication and use little obfuscation, our malware analysis also shows that at least eight attack campaigns started about two weeks before the disclosure date of the exploited vulnerabilities, and therefore were probably using zero-day attacks at that time.

1 Introduction

In 2010, Stuxnet [8] and Hydraq [16] demonstrated dangers the security community had long anticipated – that malware could be used for cyber-terrorism, real-world destruction and *industrial espionage*. Several other long term attacks against the petroleum industry, non-governmental organizations and the chemical industry were also documented in 2011 [3]. Such targeted attacks can be extremely difficult to defend against and those high-profile attacks are presumably just the tip of the iceberg, with many more hiding beneath the surface.

While targeted attacks are still rare occurrences today compared to classical, profit-oriented malware attacks, successful targeted attacks can be extremely damaging. One of the recent high profile targeted attacks against RSA has reportedly cost the breached organisation $66 million in direct costs alone [10,22]. Preventing such attacks from

D. Balzarotti, S. Stolfo, and M. Cova (Eds.): RAID 2012, LNCS 7462, pp. 64–85, 2012.

breaching organisations and causing subsequent harm depends on a detailed understanding of the threat and how attackers operate [18,2,17].

To understand the nature of targeted attacks, Symantec collected data on over 26,000 attacks that were identified as targeted during 2011. These attacks were based on emails which contained a malicious payload. Using advanced data analytics based on multi-criteria clustering and data fusion, we were able to identify distinct targeted attack *campaigns* as well as define characteristics and dynamics of these campaigns. Our research clearly demonstrates that a targeted attack is rarely a "single attack", but instead attackers are often quite determined and patient. A targeted attack is rarely an extremely stealthy, tedious and manual attack limited to a very small number of targets. A certain level of automation seems to be used by attackers and thus the notion of "campaigns" exist, yet of a very different amplitude than other malicious, non-targeted activities performed on a much larger-scale. We found also that these targeted attack campaigns can either focus on a single (type of) organization or they can target several organizations but with a common goal in mind. We refer to the latter ones as MOTA, for *Massive Organizationally Targeted Attacks*, and demonstrate their existence by means of some real world data we have analyzed.

A common belief with targeted attacks is that only large corporations, governments and Defense industries, and more particularly senior executives and subject matter experts, are being targeted by such attacks. Our research has shown that, at least for our set of targeted attacks collected in 2011, this was true only for 50% of the attacks. Moreover, while the ultimate goal of attackers is more than often to capture the knowledge and intellectual property (IP) that senior-level employees have access to, they do not have to attack them directly to steal the information they want.

The contributions of this paper are twofold. First, we focus on studying the characteristics of a comprehensive set of targeted attacks sent via email and collected in the wild by Symantec during the year 2011. More particularly, we show how those attacks are being organized into long-running campaigns that are likely run by the same individuals and we provide further insights into their *modus operandi*.

Secondly, we evaluate the *prevalence* and *sophistication* level of those targeted attacks by analyzing more in-depth the malicious attachments used as *droppers*. While a majority of the observed attacks rely mainly on social engineering, have a low level of malware sophistication and use little obfuscation, our analysis also shows that, in at least eight campaigns, attackers launched their attacks about two weeks before the disclosure date of the targeted vulnerabilities, and therefore were using zero-day attacks at that time.

The structure of this paper is organized as follows. In Section 2, we start by defining a targeted attack, describe its profile and common traits, and explain how we identified the set of targeted attacks used for this analysis. Section 3 describes in more details our experimental dataset and the attack features extracted from the emails. Then, in Section 4 we describe how we identified attack campaigns and provide insights into the way these campaigns are being orchestrated by attackers. Finally, in Section 5 we evaluate the prevalence and sophistication level of the malware used as dropper in the targeted attacks involved in those campaigns. Section 6 concludes the paper.