1. Introduction

Every day it seems that new information becomes public about the latest data breach. Millions of records (read also as personal data) are lost annually and dutifully reported by the nightly news. For example, Forbes reported that the Anthem breach alone allowed the compromise of over 78 million records ("Forbes Welcome," n.d.). However, not all breaches occur because of “elite hackers” breaking into digital networks. Sometimes (as the ACME case below illustrates), the attack can be unintentional and without the knowledge or even participation of the computer user. Sometimes a simple mistake is all that is required to open the door for damage to take place.

Attacks these days can vary greatly between the tools, the techniques and the methods used by the attacker (threat actor). The use of “Trojan software” allows the attacker to embed malware within a seemingly legitimate product. In recent years, a new term has come to the market; “Malware as a service”. History of this term is a bit convoluted, but it seems to begin in the Verizon 2011 Data Breach Investigations Report (Verizon, 2011). Similar to selling Platform as a Service (PaaS) and Software as a Service (Saas), it is possible to purchase malware designed for a specific intent. As easily as it is to acquire and deploy malware the growth in the open market has been exponential. Panda Security published an article stating that they had analyzed and neutralized:

> **“84 million new malware samples** throughout 2015. This is nine million more than the year previous, according to the corresponding data. The figure means that there were **230,000 new malware samples produced daily** over the course of the year.” (Panda, 2016)

As far as the loss, it was reported, “in 2014, the Internet Crime Complaint Center (IC3) received 269,422 complaints with an adjusted dollar loss of $800,492,073” (FBI, 2015). Worse, due to under-reporting of damage from malware, the total cost of malware may never be clear. Many times these numbers show only the larger corporate losses rather than the individual costs. To say that the attacks are very expensive to governments, private companies, and even individuals is quite the understatement.

For years, the security teams at these agencies worked with various concepts of how they should direct protections; typical security measures never

seemed to provide the complete answer. As the attacks became more and more common, the defenses started analyzing these attacks and used that to create new solutions. Instead of simply addressing the discovered vulnerabilities, these researchers were looking to understand the methodologies and anticipate future attack vectors.

In 2000, the Center for Internet Security, Inc. (CIS) formed to “enhance the security readiness and response of public and private sector entities, with a commitment to excellence through collaboration” (Center for Internet Security, 2015, p. 05). Since that time, they have been working with various industries worldwide to help enhance the concept of shared information. By allowing the offense to drive defense, they take actual attack experiences within the industry and develop a prioritized list of controls to help bolster the overall defensive measure. The Critical Security Controls (CSC) “are not limited to blocking the initial compromise of systems, but also address detecting already-compromised machines and preventing or disrupting attackers' follow-on actions” (Tarala, J.)

The CIS includes control families “that can be shown to stop known real-world attacks”. (Center for Internet Security, 2013, p. 03). By focusing on these real events and the specific environment for that company or group, the security team can develop security controls that will address the current high priority items as well as methods to address existing issues. Rather than replacing company policy or procedure, these controls can be used by security management teams as a framework used to evaluate risks across the board and then reprioritize as necessary. There are no silver bullets in security. There are no ‘one-size-fits-all’ solutions. The goal is to give the responding teams the opportunity to review the current posture, review applicable controls and address the gaps between current posture and control framework.

The below attack summary is a case study of how the CIS controls could have prevented or limited exposure during an attack; it is not meant to explain how the information was detected nor is this a timeline of the events. This is also not a forensic review of the activity. This is merely a review of the high-level activities, describing failures and showing how controls would have enhanced the security posture. Also added are the remediations suggested to management in order to prevent or reduce the probability that this activity from being a problem in the future.

Ladies and gentlemen, the story you are about to read is true. The names have been changed to protect the innocent.

2. Attack Summary

An ACME Inc. employee brought a personal laptop into the facility infected (albeit unknowingly) with Poison Ivy and connected it to the corporate network via a wireless access point (AP). The system obtained an IP Address using Dynamic Host Configuration Protocol (DHCP) addressing provided by the core corporate network services. Upon connection, the infected system made an Internet connection to the command and control server (wile.e.coyote.com). Once connected, the threat actor provided the command for the system to scan the local network for available services. While the user noticed that the machine was running slowly, it was late on Friday starting a three-day weekend. The user left the machine powered on with plans to look at it again on Tuesday. The scan identified an open File Transfer Protocol (FTP) service on the internal network that allowed anonymous access. The threat actor, still using the compromised machine, logged into the FTP server, compressed the contents and then transferred the data to the control server (over the internet) using an encrypted outbound VPN connection.

Over the weekend, the Network Operations Center (NOC) tracked a large amount of data over an encrypted channel. While able to identify both the source and destination, without the encryption keys, they were unable to decrypt the traffic to identify the content. The destination was not on the current list of known malicious sites (the list was out of date by four months). The help desk technician then opened a work ticket for the local desktop services to investigate.

Early Tuesday morning the user noticed that this was still acting erratic even after a reboot. The user then called the help desk to open a ticket. The helpdesk technician was able to tie IP address of this machine to the traffic identified over the weekend. When the desktop technician arrived, it was determined that the machine in question is not a corporate machine and does not have all the standard protection software. A quick scan using a boot time tool found the Poison Ivy signature. At this point, the technician confiscated the machine for forensic investigation and the tickets closed.

Bill Knaffl, bill.knaffl@gmail.com

The forensics team determined a known malware tool named Poison Ivy compromised the machine. They also found a temporary file, left over by the scanning, that included the directory listing of the FTP site. Many of the folders within the directory we named after previous high-value programs. These files included parts lists, price quotes and even proprietary drawings. Included in the information, were patents from the current Chief Executive Officer (Mr. R. Runner) as well as legal documents describing the purchasing and legal aspects of these programs.

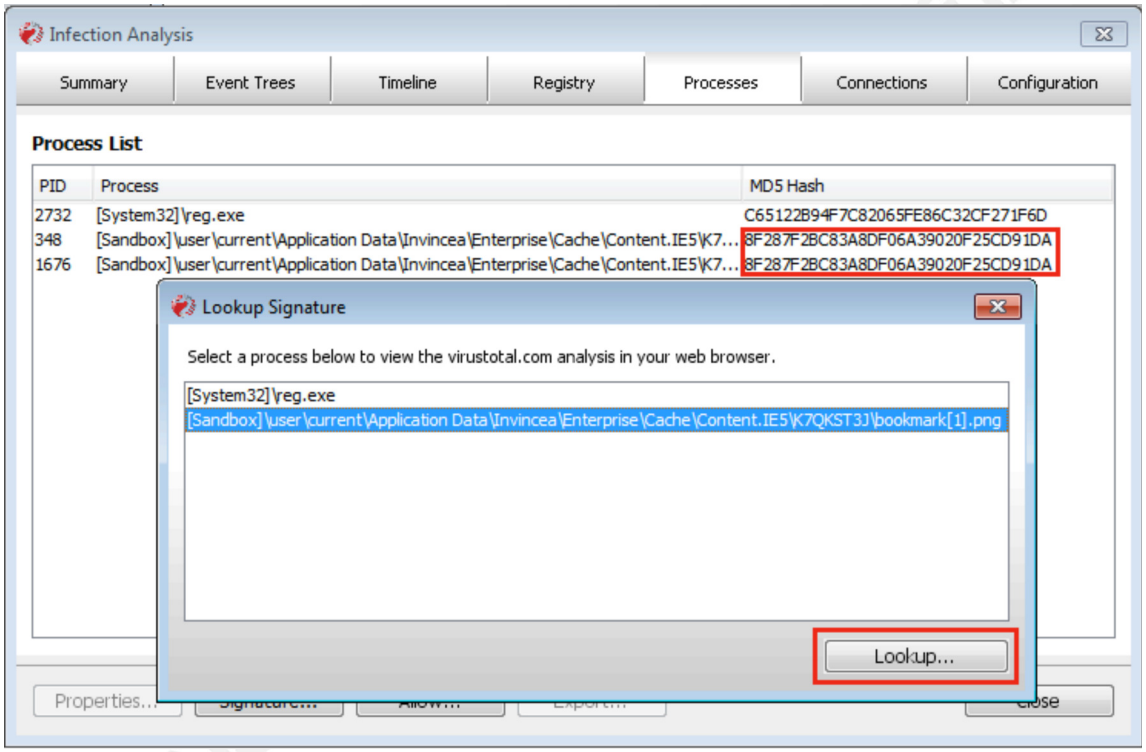

Figure 1 - Infection Analysis

Bill Knaffl, bill.knaffl@gmail.com