Knowlton Project Analysis Study:

Examining Trends in Cyber Security:
Merging Network Defense and Analysis

March 2013

"*Security is a journey, not a destination*"

www.praescientanalytics.com

INTRODUCTION

Somewhere deep in the business network of a U.S. bank, a computer's hard drive spins. A few lines of hidden code written to the system's directory come alive to complete the simplest of commands. This *beaconing code*[1] reaches out and connects with a malicious server to create a remote connection. The hacker who surreptitiously hooked an employee with a phishing attack[2] now has complete access to the bank's network.

The scenario illustrated above has become commonplace in modern computer networks. But how can this happen today if network security experts have been around for forty years? As far back as 1972, reports commissioned by the U.S. Air Force identified significant security problems in government computer networks. Today cyber security is cited as a top priority among policymakers. President Obama is seeking to allocate $769 million to the Department of Homeland Security alone for information security initiatives. Despite the resources directed towards this effort, private and public organizations continue to lose billions of dollars while their networks are hacked and their intellectual property is stolen.

The cyber security community has not fundamentally changed the way networks have been protected over the past four decades. Much effort has been placed on "building a bigger firewall" - expanding the virtual moats and perimeter defenses that surround networks. This approach proved sufficient until about five years ago, when cyber threats evolved. To circumvent static defenses, malware embedded stealthily within standard network traffic.

The summer and fall of 2008 were turbulent times. The troop surge in Iraq was underway, the presidential race was reaching a fever pitch, and a meltdown on Wall Street plunged the world economy into recession. Yet there was another equally massive shift quietly occurring amid the turmoil. The world's computer networks and the cyber security community were forever changed by the advanced threats proliferating across the globe.

---

[1] Periodic communications from the malicious program to a command and control node.

[2] Specific or mass email which targets a victim with hidden malware.

THE GOOD OLD DAYS

Malicious code is nearly as old as computing itself. Some of the earliest viruses spread via floppy disk by imbedding in the boot sector[3]. Proliferation of such code was limited by human interaction. As computers were increasingly networked together, a new medium emerged that further enabled the spread of malware.

Effective cyber security is defined according to three core pillars: confidentiality, integrity, and availability. The confidentiality of data is the guarantee that only those who are properly authorized may have access to a system's information. Integrity of data is the concept that all information within a system is holistic, complete, and free of errors. Availability of data refers to the amount of time a system is functioning, or has is available to be accessed by the user.

Prior to the mid-2000's the purpose of most malware was to disrupt the availability of networks. Threats came primarily from anarchists who sought to corrupt hard drives and bring down large corporations. Ultimately, the goal of most attacks was to deny the availability aspect of networks. This occurred either through intentional Denial of Service (DoS) attacks or through a flood of network traffic from aggressive scanning[4].

The following are examples of threats targeting network availability, each of which had a significant impact on networks worldwide:

Name: *Melissa (1999)*
Category: *Mass mailing virus*
Infection Vector: *Email*
Payload: *Text injection into open word documents*

At the time of its release, the Melissa virus spread across the globe within hours, faster and any known virus had before. Melissa spread through an email attachment called LIST.DOC and then sent itself to 50 people in the victim's address book. The actual payload was minor, injecting text into open word documents. The real threat from Melissa was a second order effect: it generated a Denial of Service attack against mail servers as a result of its rapid proliferation. Melissa was one of the first well known viruses spread via networks.

---

[3] An area on a data storage device which allows the boot process of a computer to load a program.

[4] A method used to discovers hosts on a network and determine what services they are running.

Name: *SQL Slammer (2003)*
Category: *Network Worm*
Infection Vector: *Remote execution, buffer overflow*[5]
Payload: *Machine shutdown (inadvertent)*

SQL Slammer was a surprisingly efficient network worm consisting of only 376 bytes and spreading through the network via User Datagram Protocol (UDP)[6]. This worm exploits a buffer overflow vulnerability in Windows SQL Server Resolution Service[7]. The effectiveness of SQL Slammer had been unprecedented, within ten minutes it infected over 90% of vulnerable hosts.

The payload for the Slammer worm was little more than instructions for it to propagate. It did not even write itself to disk, only existing in memory. The worm's aggressive scanning and propagation significantly impacted network availability. South Korea's entire internet was shutdown after the crash of their gateway routers.

Name: *Sasser (2004)*
Category: *Network Worm*
Infection Vector: *Remote execution, buffer overflow*
Payload: *Machine shutdown (inadvertent)*

Purportedly created by a German teenager, this worm self-propagated through networks. The network worm exploits a buffer overflow vulnerability in Window's Local Security Authority Subsystem Service (LSASS)[8]. After Sasser infects the host it begins to scan IP addresses in the network for the same vulnerability - then it continues to spread. Errors in the coding of Sasser caused it to shut down systems, and its aggressive scans ate up the bandwidth in networks. Sasser had serious effects on networks worldwide, from banking systems to airline communication systems.

---

[5] A vulnerability which allows an attacker to overrun expected memory and execute code on a victim.
[6] User Datagram Protocol is a connectionless protocol that can be sent in a one-way stream of data.
[7] A function in windows which allows resolution of data within SQL databases.
[8] Process in Windows operating system that controls the security policy of the system.

PARADIGM SHIFT: 2007-2008

2007 and 2008 represent a turning point for the cyber security industry. According to a study by Kaspersky labs, there was a 189% increase in malware by the end of 2008[9]. The drastic increase alone is troubling, but around 93% of the new malware found were *trojan* programs, also known as *backdoors*[10] and *rootkits*[11] (*fig 1)*. These malicious programs can allow a hacker to gain remote access to a computer, while hiding the connection so it is harder to detect. This fundamental shift began to impact the integrity and confidentiality of information assurance.

Threats that target the integrity and confidentiality of a network's information are in many ways more dangerous than threats to availability. By only slightly modifying a user's data, a hacker can compromise and entire organization's perceived integrity. Also, by using covert backdoors, a malicious actor can bypass most encryption security measures. Once deployed, trojan and rootkit type malware can be very hard to detect. Often the code can hide in the kernel of a system where anti-virus programs don't routinely look. Some more advanced versions create a passive backdoor, triggered when the attacker wants to gain access. The emergence of two specific trojan intrusion sets during 2007 to 2008 showcase these properties.

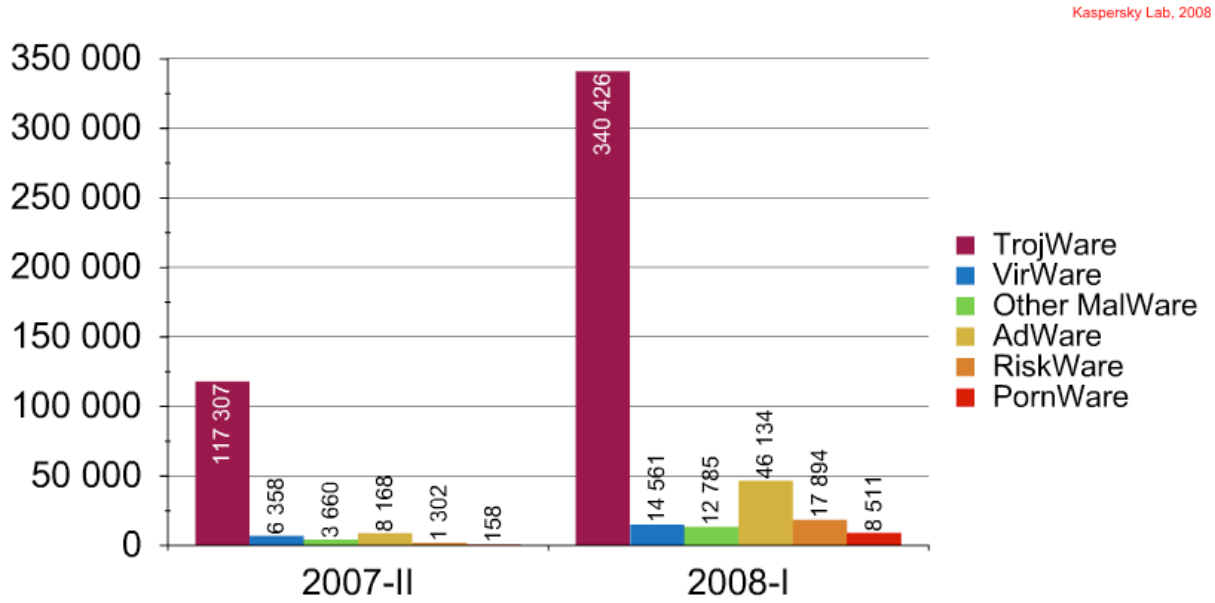

fig. 1 - Number of malicious programs detected 2007 - 2008

[9] Sergey Golovanov et al. "Kaspersky Security Bulletin 2008: Malware Evolution". June 2008.

[10] An unintended and unauthorized way to access a computer system.

[11] An advanced type of malicious software that allows an attacker persistent access to a system.

Name: *Zeus (2007)*
Category: *Trojan/Persistent*
Infection Vector: *Drive-by-download, phishing*
Payload: *Covert information exfiltration, backdoor*

Originally developed as a "do-it-yourself" crimeware kit, Zeus malware and its variants have become one of the most widespread infections in the world. Since 2007, millions Zeus infections have been reported on U.S. government and commercial networks worldwide. There are many variants of Zeus that use different infection vectors, but the most common method is through phishing or malicious downloads on the web.

Zeus was one of the first large scale intrusions to hide on systems and discreetly extract users' sensitive information. Once the trojan is installed, it monitors users' key strokes for passwords, account numbers, and other personal identifying information. Using victims' personal banking information, networks of hackers then funnel money to overseas bank accounts and money launderers. In 2010, the FBI estimated that thieves had used Zeus to steal more than $70 million[12].

Because Zeus usually injects itself onto a system through legitimate traffic it can be difficult to detect. The malware also continues to evolve, avoiding detection from anti-virus software.

Name: *Conficker (2008)*
Category: *Network Worm*
Infection Vector: *Remote execution, removable media, map shares*
Payload: *Self propagation, backdoor*

Perhaps no malware intrusion set shocked the information security community more than Conficker. First appearing in late 2008, infections from Conficker were so widespread and dynamic that it was dubbed the world's first "superworm". Early versions of Conficker exploited a buffer overflow vulnerability less than 30 days from Microsoft's announcement. Because this network worm did not require user interaction to spread, it completely infected large enterprise networks within minutes.

Ultimately, there were more than five main versions of Conficker that were discovered. In subsequent versions, the worm also spread through removable media (like USB thumb drives) and mapping default network shares (*fig 2)*. Conficker was also dangerous in how well it hides on systems. Advanced stealth

[12] FBI Press Office. *International Cooperation Disrupts Multi-Country Cyber Theft Ring.* 21 October 2010.

measures were seen; from modifying system time of install to mask forensics, to encrypting the file, to creating a pseudorandomly generated algorithm that conducts health checks with one of 50,000 domains every three hours. One of the more frightening aspects about Conficker's hardening is the use of MD6[13] hash based encryption. When Conficker B appeared in late December 2008 it used a 256 bit MD6 hash based encryption. MD6 encryption had only been talked about as a theory by the esteemed cryptographer Ron Rivest 30 days prior! To quote and industry analyst: "Not only are we not dealing with amateurs, we are possibly dealing with people who are superior to all of our skills in crypto[grapghy]."

Conficker also has the distinction of being one of the only intrusion sets to prompt the formation of worldwide working group, bringing together analysts from government, industry, and security firms to combat the near 15 million unique IP addressees infected. The damage caused by Conficker is almost too diverse to calculate - nearly every country in the world had been infected. There were disruptions and shutdowns in critical government networks, the U.S. Department of Defense even banned all USB media based on this incident.

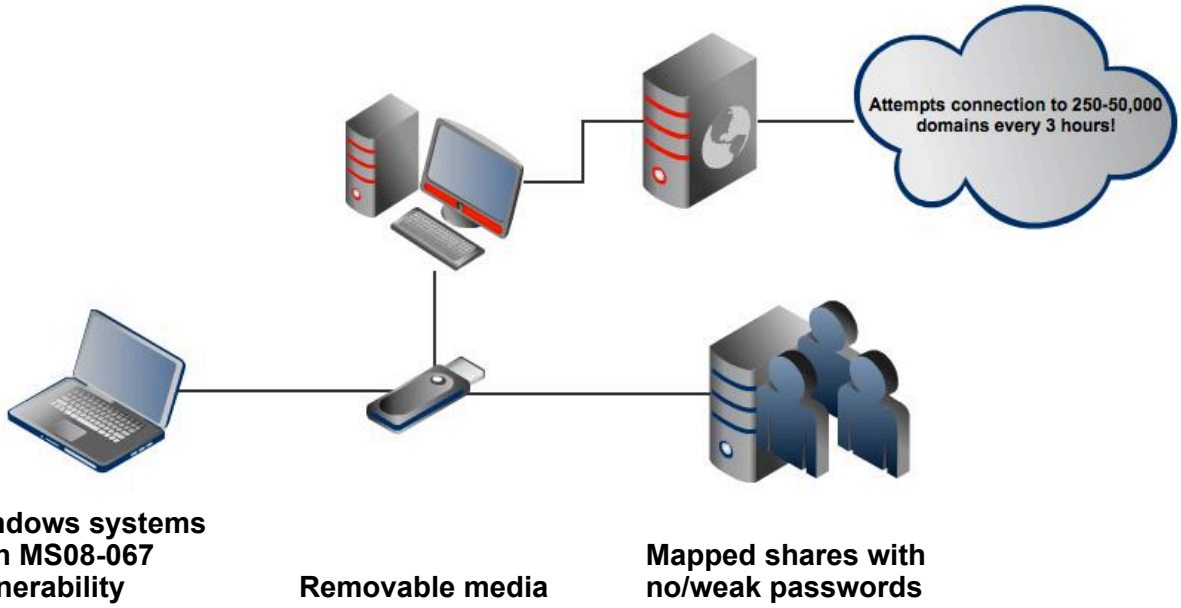

fig. 2 - Infection vectors used by the Conficker worm

[13] MD5 or MD6 refers to Message Digest Algorithm. It is essentially a 128 or 256 bit value produced by combining data with a cryptographic hash function. The result can be used to check data integrity.

CYBER SECURITY TODAY

What control measures have the public and private sectors implemented to mitigate advanced cyber threats? In 2011 alone the U.S. spent $55 billion on cyber security, a total that is estimated to increase to $86 billion by 2016[14]. Most of this spending goes into perimeter defense systems such as firewalls, intrusion detection systems (IDS), and Virtual Private Networks (VPN). These systems are relatively easy to setup and are simple means for assuring minimum security compliance. Additional measures include anti-virus or monitoring systems.

The problem with most of these measures are that they are signature-based—they are designed to detect threats that they have seen before and know to look for again. If the systems are not loaded up with the latest signatures, threats can still get in. Even algorithmically-based threat detection and encryption methods are only so effective; determined hackers can still manage to find ways around them. Phishing attacks are a good example of this. When an employee opens a malicious email, it often contains an embedded link or invisible code, which then connects to a hacker's listening post and infects the machine. Since all these connections occur over seemingly legitimate traffic, they are almost impossible to detect. Not even cyber industry leaders are free from threat: the security giant RSA was infiltrated using a similar method. Perimeter security also focuses on preventing penetration from the internet and does little to deter the growing challenge of insider threats.

In short, cyber hacking events continue to rise because most companies use static security measures to fight the dynamic threat. Private companies lose millions of dollars each year from intellectual property theft. The average organization's cost of a data breach in 2010 was estimated to be $7.2 million. A recent study conducted by Verizon and the U.S. Secret Service illustrates how current cyber security measures fall short of protecting networks[15]:

- Almost 50 percent of the breaches investigated were attributed to insiders.
- 87 percent of breached organizations had evidence of the breach in their log files and did not detect it.
- 48 percent of breaches were attributed to users who intentionally abused their right to access corporate information.
- Most breaches in their sample (85 percent) were not considered "difficult" and could have been avoided without "hi-tech" or expensive measures.

---

[14] "Global Security Spending to Hit $86B in 2016". Infosecurity Magazine. 14 September 2012.

[15] Verizon RISK Team and United States Secret Service. *2010 Data Breach Investigation Report*. 2010.

CYBER ANALYTICS

To truly combat advanced cyber threats one has to understand there is no panacea. Cyber security is a constant fight - it is a journey not a destination. If a system is fully patched and all software is updated it may stop 70% of malicious actors. Adding anti-virus and perimeter defense solutions will likely stop an additional 10%. But the remaining 20% of actors are the top tier who specialize in advanced persistent threats (*fig 3*). No matter what security measures are in place, a determined hacker will get through them. Static security infrastructure are just a deterrent, much like the lock on your front door.

There are a wide array of commercial and government organizations that are targeted by top tier cyber actors. Companies that hold valuable intellectual property are profitable areas where hackers can strike. The military and the defense industrial base are also targeted by state actors trying to steal classified information.

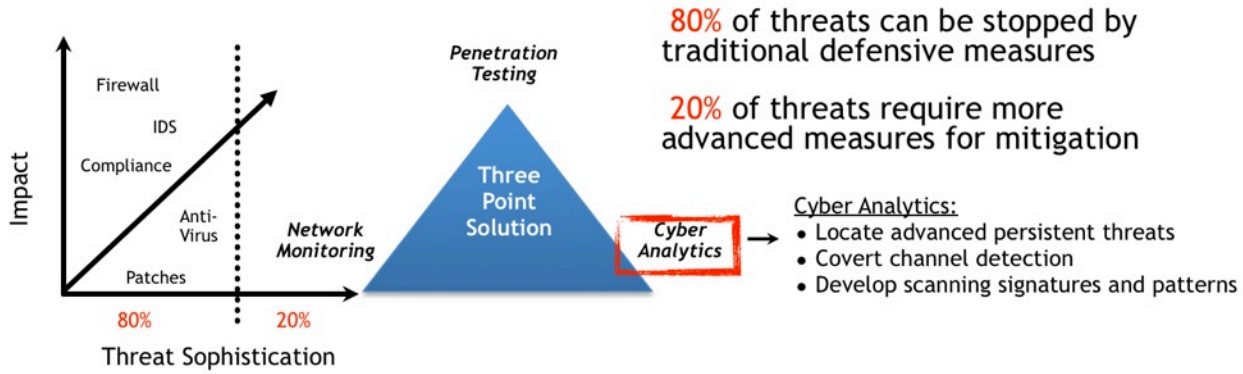

fig. 3 - Fighting the advanced 20% of cyber threats

Defending against such advanced threats requires a more interactive approach. In addition to meeting all compliance standards, the most effective way to mitigate advanced threats is through a three point solution: network monitoring, penetration testing, and cyber analytics. Historically, only the federal government and intelligence agencies could afford to cultivate the skills needed for these services. Now, modern cyber espionage is so prolific that it has become cost effective to integrate the three point solution in order to stop threats.

Through network monitoring, operators can have greater awareness of the network and prioritize critical nodes for defense. Penetration testing can be used periodically to identify vulnerabilities in the network. A complete assessment test should include social engineering attacks to test employee response against

tailored attacks. Documenting employee response to various social engineering attacks can help produce a stronger information technology policy for an organization.

Cyber analytics is perhaps one of the newest fields in information security. This service blends aspects of intelligence analysis and cyber security. Network traffic and system logs are essentially a huge data source for cyber analysts. By using advanced analytics; one can detect infiltrations faster, regardless of their source. Pairing advanced software platforms with a human analyst is the most effective way to detect an infiltration. Intelligence analysts excel in finding unique patterns among massive databases.

Consider the four phases of a hacker's attack: reconnaissance, scanning, exploitation, and persistence. If an organization consolidates systems logs and network traffic, analysts can sift through the data at each phase. Analysts can link associated events among multiple sources and replay how an attack occurred. Tracing patterns over time, analysts can determine the signature of a scan and assign it to specific actors. This will enable prediction of when an attack will occur. Traffic from backdoor beaconing can be found quickly and blocked at the gateway. The source of data will be irrelevant - analysts can just as easily identify traffic from an insider threat as they can from internet based attacks.

Static cyber defense architecture will continue to be a key tool in the fight against malicious actors, but they are only part of the solution. A holistic approach to cyber security is a much more effective method of minimizing the impact of a network intrusion. By merging the skill sets of information assurance and intelligence analysis, the new field of cyber analytics will soon integrate into business models.