FireEye

FireEye Advanced Threat Report – 2H 2011

Contents

Inside This Report

The FireEye Advanced Threat Report for the second half of 2011 is based on research and trend analysis conducted by the FireEye Malware Intelligence Labs. This report provides an overview of advanced targeted attacks in the second half of 2011 and was developed to provide insights into the current threat landscape, evolving advanced persistent threat (APT) tactics, and the level of infiltration seen in organizational networks today. This is not a typical threat report with just tallies of the millions of well-known malware or billions of spam messages.

To complete the threat landscape picture, the FireEye Advanced Threat Report focuses on the threats that have successfully evaded traditional defenses. These are the unknown threats and advanced targeted attacks that are dynamic and stealthy. And, we have found that they are extremely effective at compromising organizations' networks.

FireEye is in the unique position to illuminate this advanced targeted attack activity since our appliances are deployed in enterprises across the globe as the last line of network defense behind firewalls, IPS, and other security gateways. Given this unique position, we are able to share our findings on the advanced threats that routinely bypass signature-, reputation- and basic behavior-based technologies, the $20B spent on IT defenses each year.

This report dives into the FireEye Malware Intelligence Labs' analysis of shared threat data from global deployments of FireEye Malware Protection Systems (MPS). This threat data is anonymized, real-time information shared by brand-name enterprises, government agencies, and educational institutions that subscribe to our Malware Protection Cloud (MPC).

Key Findings

1) The fastest growing malware categories in the second half of 2011 were PPI (pay per installs) and information stealers.

2) Of the thousands of malware families, the "Top 50" generated 80% of successful malware infections.

3) Over 95% of enterprise networks have a security gap despite $20B spent annually on IT security.

4) Spear phishing attacks increase when enterprise security operations centers are lightly staffed or understaffed, particularly during holidays.
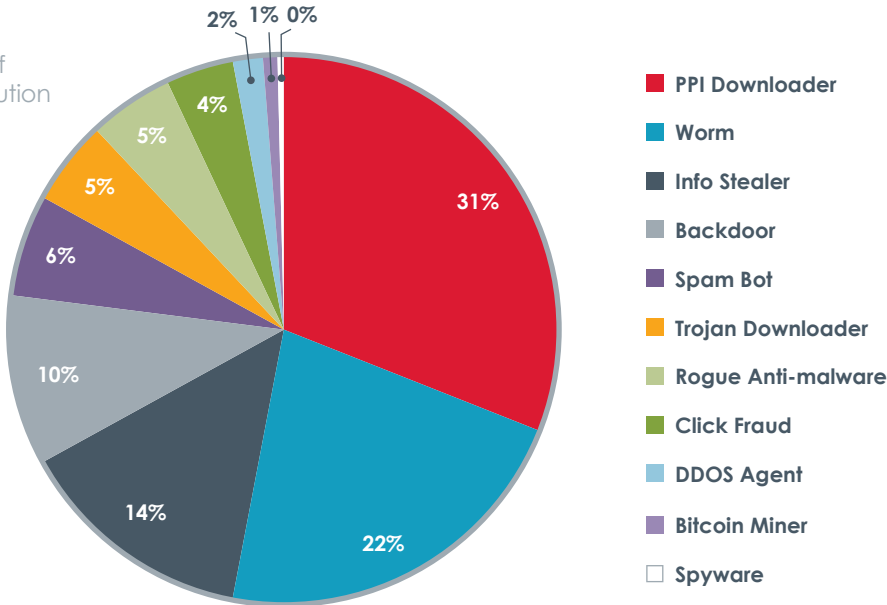
Finding 1: The fastest growing malware categories in the second half of 2011 were PPI (pay per installs) and information stealers

The FireEye research team categorizes malware according to its primary purpose but it is important to note that advanced malware often offers a combination of features. For instance, any malware seen stealing information from a compromised computer falls under the information stealer category, while malware programs that bypass security mechanisms to provide access to compromised machines are classified as a backdoor.

In the second half of 2011, pay-per-install (PPI) downloaders, worms, backdoors, and information stealers represented the four most prevalent categories of malware. PPIs are malware programs that charge a fee to download or distribute other malware programs. These programs differ from normal downloaders/droppers in that a PPI malware author gets paid for every successful install of another malware program. Of the top four malware categories, information stealers and backdoors present the greatest threat to enterprises.

A special category called Bitcoin Miner has also been created since the FireEye Malware Protection Cloud (MPC) showed a phenomenal increase in this class of malware. Bitcoins are virtual currencies stored in "wallets" on user's computers. This category of malware was seen stealing these wallets and uploading them to the attacker's command and control servers. Although this malware can be categorized as an information stealer, we chose to separate it out to show its prevalence in the second half of 2011.

Figure 1: Breakdown of second half of 2011 malware categories distribution

Legend:
- PPI Downloader — 31%
- Worm — 22%
- Info Stealer — 14%
- Backdoor — 10%
- Spam Bot — 6%
- Trojan Downloader — 5%
- Rogue Anti-malware — 5%
- Click Fraud — 4%
- DDOS Agent — 2%
- Bitcoin Miner — 1%
- Spyware — 0%

The majority of worm infections that we saw were attributed to machines infected with the Conficker worm. Even after 3 years, since it was first detected, Conficker still continues to remain one of the more popular worms infecting machines worldwide.

The graph below shows the most widespread information stealing malware that we observed during the second half of 2011.

Figure 2: Most popular information stealers in second half of 2011
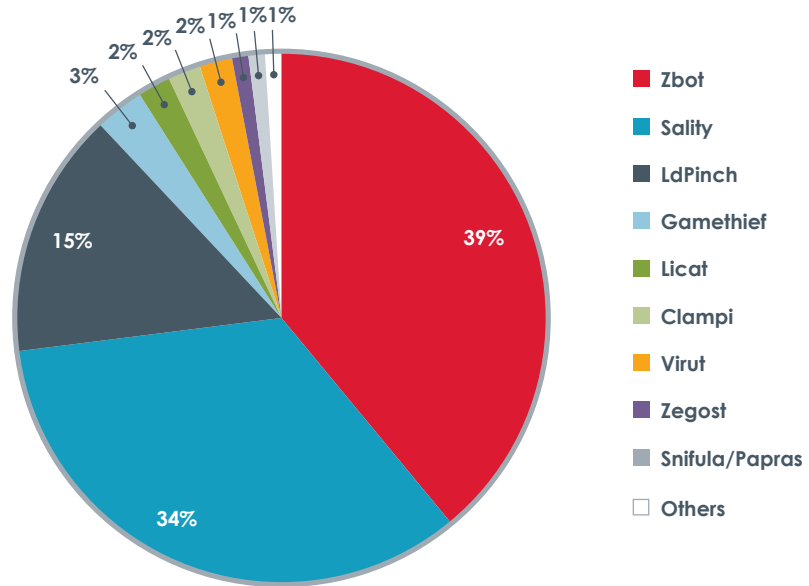
Following are descriptions of several of these information stealing malware programs:

- **Zbot** saw an increase in newer variants in 2011. We speculate that the rise in different variants of Zeus is connected to the leak of its source code. Primarily a banking trojan, Zbot is a threat to small, medium, and large enterprises.

- **Sality** is a malicious program that has the ability to overwrite executable files. It is also known to contain Trojan components. Some variants of Sality also contain the ability to steal sensitive personal or financial data. In the FireEye MPC labs we saw that the use of Sality was almost as widespread as Zbot.

- **LdPinch** is a piece of malware that did not make it to the 1H 2011 Advanced Threat Report. In the latter half of 2011, we saw a tremendous increase in machines infected with LdPinch. The powerful program is capable of stealing account credentials from various services.

- **Licat** is believed to be associated with Zbot.

- **Zegost** is primarily a keylogger.

- **Clampi** is a Trojan capable of stealing users' passwords and other sensitive financial information.

Finding 2: Of the thousands of malware families, the "Top 50" generated 80% of successful malware infections

In the second half of 2011, we saw that the top 50 malware families generated 80% of successful infections. Reviewing the top 50 malware families, we noticed that the more successful code bases have been optimized to be dynamic and deceptive.

We observed that very few malware families accounted for larger infection rates. 50% of the cases were attributed to malware families ranked 1 – 13 in the second half of 2011.

How do criminals make their malware and domains dynamic? Point-and-click toolkits

This shift could indicate that the top ranked malware programs increasingly use advanced techniques to avoid detection by conventional security devices. For example, toolkits are increasingly being used to "drop" malware on vulnerable machines. In 2011, FireEye detected hundreds of thousands of malicious domains hosting the BlackHole toolkit. The increasing use of toolkits and newer techniques for obfuscating and encrypting code makes it difficult for conventional security devices, which rely on signatures and heur–istics, to detect attacks. Malware "dropped" by toolkits such as BlackHole engage in theft of intellectual property and financial fraud, targeting both organizations and individuals.
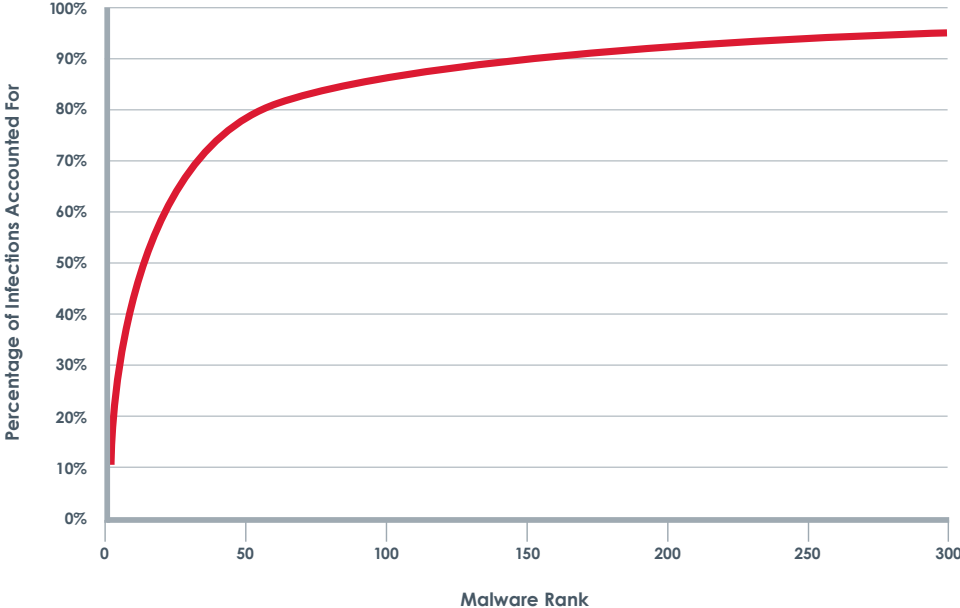

Figure 3: Cumulative fraction of all cases accounted for by malware callback protocol through a particular rank in popularity

FireEye uses a unique method to detect these kinds of advanced attacks. The company has a virtual execution (VX) engine that can inspect such malware, isolate any callbacks that the malicious code is making and take the actions necessary to thwart the attack.

Criminals make code appear new by packing, encrypting, or otherwise obfuscating the nature of the code. Malware toolkits like Zeus (banking Trojan) and BlackHole (drive-by downloads) automate this process today.

By moving their malware to an unknown site (often a compromised server or zombie), and using short URLs, cross-site scripting or redirects to send traffic to that site, the criminals can stay ahead of reputation-based defenders.

Criminals invest in toolkits and dynamic domains because signatures and reputation engines have become adept at blacklisting known bad content and "bad" or "risky" sites. Any stationary criminal assets will quickly be blacklisted, therefore these assets must move to remain valuable.

Finding 3: Over 95% of enterprise networks have a security gap despite $20B spent annually on IT security

Consistent with the first half of 2011 data we collected, we see that virtually all enterprises continue to be compromised by malware. Over 95% of enterprises had malicious infections inside their network each week. Almost 80% of enterprises averaged an infection rate of more than 75 per week.
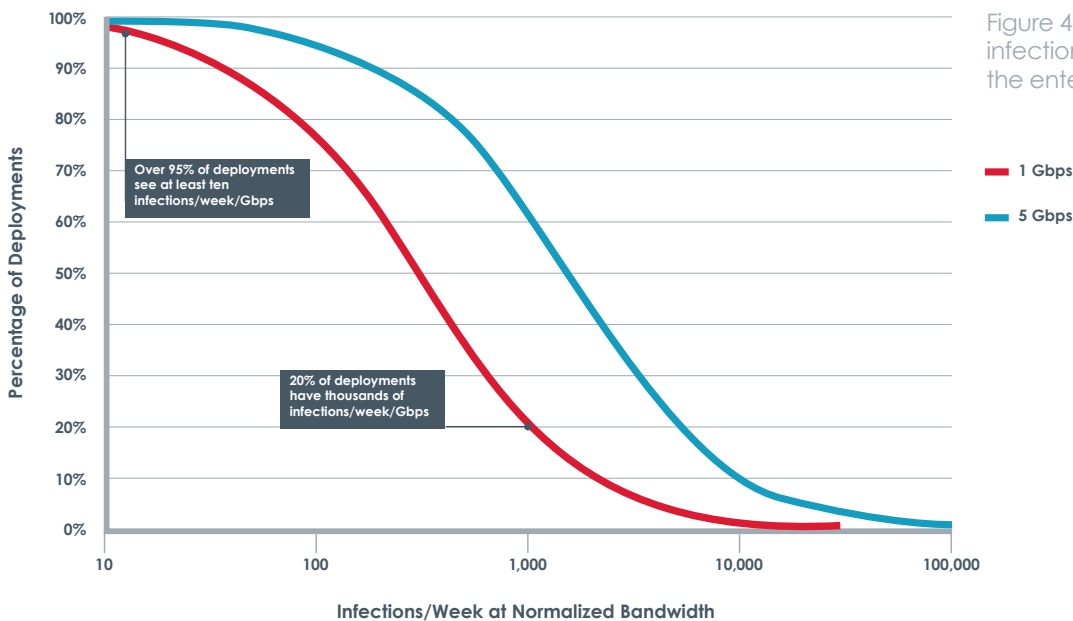

Figure 4: Widespread infections seen across the enterprise

These stats have been collected from the FireEye customer base, where other security devices have been deployed. The consistency in infection rate has proven the point that existing security devices are unable to catch these advanced threats. These traditional security mechanisms can no longer keep up with the highly dynamic, multi-stage attacks that have become common today for advanced targeted attacks.

Note: FireEye detects malware already active within the network, as well as new malware attacking the network. FireEye systems deployed inline with active blocking act as an effective countermeasure for these types of incidents, and would have reduced the incident counts seen in Figure 5.

Figure 5: Infection rate (cases/week/Gbps)

Infection Rate (Cases/Week/Gbps)
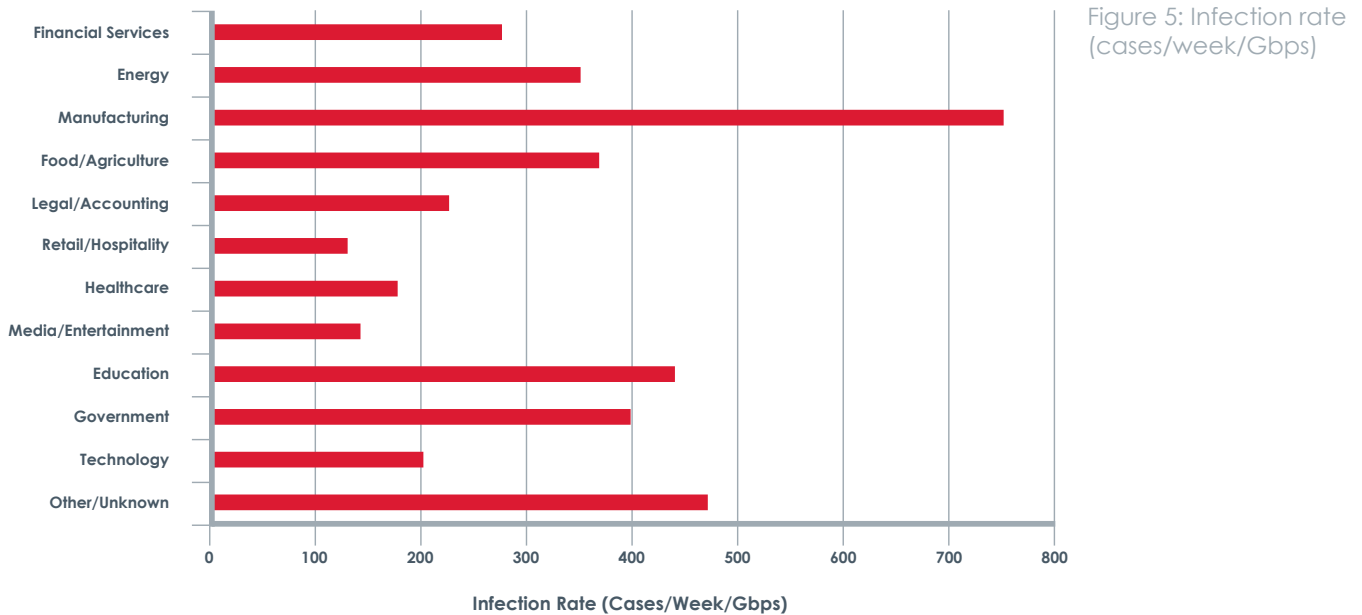
Even the most security-conscious industries are fraught with dangerous infections

Every company studied in every industry looks to be vulnerable and under attack. Even the most security-conscious industries—such as financial services, healthcare, and government sectors, which have intellectual property, personally identifiable information, and compliance requirements—show a significant infection rate.

Based on this data, we see that today's cyber criminals are nearly 100% effective at breaking through traditional security defenses in every organization and industry, from the security savvy to security laggards.

Finding 4: Spear phishing attacks increase when enterprise security operations centers are lightly staffed or understaffed, particularly during holidays

The figure below illustrates the daily count of malicious email attachments identified by the FireEye Email MPS appliances across our entire US-based customers. These levels reflect the daily count of incoming malicious attachments that were able to successfully evade initial SPAM and AV filters, as they arrived from outside the target organization.
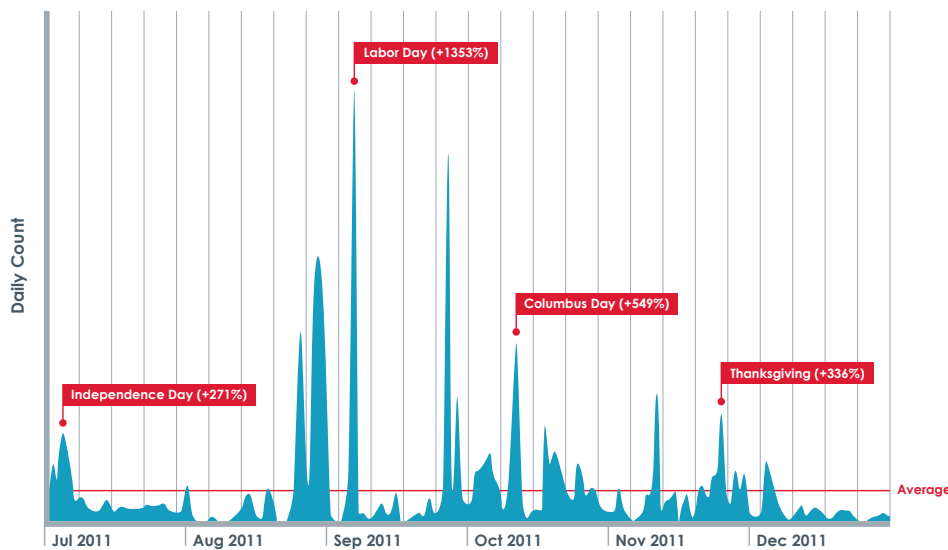

Figure 6: 2H 2011 malicious email attachments by relative volume

One common trend appears to be that attackers heavily leverage this infection vector on or around major national holidays. The concept is simple: national holidays are typically when enterprise security operations centers are lightly staffed or understaffed. Therefore, attackers' operations have a higher chance of success and are able to maintain a longer foothold within the target organization around this time frame, in order to maximize exfiltration operations.

Prior to the start of the actual holiday, attackers appear to experiment with multiple campaigns, as illustrated by the smaller spikes in traffic, leading up to the relative maximal peak. After measuring initial success, their final techniques are refined and corresponding attacks are significantly amplified during the 3 days around the national holiday.

For the second half of 2011, it appears Labor Day was the most prolific holiday for attackers utilizing this vector, as malicious attachment levels reached 1,353% above the bi-annual average, Columbus Day following a distant second (549%), followed by Thanksgiving (336%), and Independence Day (271%), accordingly.

That said, it appears attack levels dropped well below the average during Christmas and New Year's holidays. One possible theory is that while security operations teams are lightly staffed around that time frame, there are also significantly fewer employees working during those holidays, so there are fewer opportunities for targeted users to actually open malicious attachments. Therefore, attackers may focus their efforts around national holidays where 50% or more of the total employees are likely to still be working, yet security operations teams may not necessarily be above 50% staffing levels.

Conclusions

Advanced, dynamic malware, toolkits, and APT tactics like blended spear phishing attacks continue to put virtually every enterprise at risk of data theft and disruption. Although enterprises are investing $20B per year on IT security systems, cybercriminals are able to evade traditional defenses, such as firewalls, IPS, antivirus, and gateways, as they are all based on older technology: signatures, reputation, and crude heuristics.

Criminals are maximizing their penetration rates using multi-vector attacks over Web and email. They are also utilizing multi-stage attacks that take advantage of the disparate, un-integrated nature of today's products. They exploit application vulnerabilities, initiate callbacks from within the trusted network, download binaries over various protocols, and exfiltrate data seemingly at will. Advanced malware is today's new status quo, but unfortunately most companies are still trying to use traditional tools to detect it. Because the majority of products rely on signatures with some level of reputation/behavior analysis, they are not as effective as companies would like to stop advanced targeted attacks.

We believe enterprises need to reinforce traditional defenses with a new layer of security that detects and blocks these sophisticated, single-use attacks. New technologies are needed that can recognize advanced targeted attacks entering through Web and email, and thwart attempts by malware to call back to command and control centers. This extra defense is designed specifically to fight the unknown threats, such as zero-day and APT attacks, thereby closing the IT security gap that exists in all enterprises.

Methodology

The analysis in this report is based on observations by FireEye Web and Email Malware Protection System deployments, which detect inbound Web attacks, malicious attachments, and multi-protocol malware callbacks. The 2011 data set in this report was obtained from the FireEye Malware Protection Cloud where subscribing customers share and receive anonymized malware intelligence data. The sample size represented several million incident submissions and were drawn from mainly large and medium-sized enterprises and from many different vertical segments.

Frequently we may see many symptoms of malware on a given infected client: the inbound exploitation, multiple malicious binaries being downloaded, and then callback evidence of multiple malware families. Often, to become infected with one piece of malware is to become infected with many pieces. For the purpose of this analysis, we aggregate all evidence of malware that we have on a given client IP address into an "infection." That infection is the unit of analysis throughout this report. If a given IP address shows no symptoms for seven consecutive days, we consider that infection closed and any further symptoms will count as a new infection.

All the usual caveats apply here: we are observing complex enterprise networks, of unknown topology, typically from the egress points where such networks touch the Internet. Our infection counts could be off due to DHCP lease expirations that do not preserve IP addresses on release, physical moves of equipment, particularly laptops, presence of multiple systems behind internal NAT devices, etc.

About FireEye, Inc.

FireEye is the leading provider of next-generation threat protection focused on combating advanced malware, zero-day and targeted APT attacks. FireEye's solutions supplement security defenses such as traditional and next-generation firewalls, IPS, antivirus and Web gateways, which can't stop advanced malware. These technologies leave significant security holes in the majority of corporate networks. FireEye's Malware Protection Systems feature both inbound and outbound protection and a signature-less analysis engine that utilizes the most sophisticated virtual execution engine in the world to stop advanced threats that attack over Web and email. Our customers include enterprises and mid-sized companies across every industry as well as federal agencies. Based in Milpitas, California, FireEye is backed by premier financial partners.