FireEye™

FireEye Advanced Threat Report – 1H 2012

Contents

Inside This Report

The FireEye® Advanced Threat Report for the first half of 2012 is based on research and trend analysis conducted by the FireEye Malware Intelligence Lab. This report provides an overview of the current threat landscape, evolving advanced malware and advanced persistent threat (APT) tactics, and the level of infiltration seen in organizations' networks today.

This report is not intended to deliver tallies of the massive volumes of well-known malware and spam messages. Rather, this report is intended to complete the picture of the threat landscape by providing an analysis of the unknown threats; the advanced threats that are dynamic, stealthy, and successfully evading traditional security defenses such as firewalls, Intrusion Prevention Systems (IPS), Anti-Virus (AV), and gateways.

FireEye is in a unique position to illuminate this advanced cyber-attack activity. Hundreds of customers around the world have deployed the FireEye Malware Protection System™ (MPS). The FireEye solutions are deployed behind firewalls, next-generation firewalls, IPS, and other security gateways, and represent the last line of defense for organizations. These solutions feature appliances that automatically gather threat intelligence, and send it to the FireEye Malware Protection Cloud,™ which also includes new threat findings from the FireEye Malware Intelligence Lab.

Given this vantage point, FireEye is able to gain a highly informed perspective on the advanced threats that routinely bypass signature-, reputation-, and basic behavior-based technologies—the technologies that organizations spend $20B each year on, but that are failing to thwart today's advanced threats.

Executive Summary

Following is a summary of the key findings this report covers:

- Organizations are seeing a massive increase in advanced malware that is bypassing their traditional security defenses.
- The patterns of attack volumes vary substantially among different industries, with organizations in healthcare and energy/utilities seeing particularly high growth rates.
- The dangers posed by email-based attacks are growing ever more severe, with both link- and attachment-based malware presenting significant risks.
- In their efforts to evade traditional security defenses, cybercriminals are increasingly employing limited-use domains in their spear phishing emails.
- The variety of malicious email attachments is growing more diverse, with an increasing range of files evading traditional security defenses.

Finding 1: Explosion in Advanced Malware Bypassing Traditional Signature-Based Defenses

The malicious advanced malware organizations have to contend with has grown dramatically, not just in terms of volume, but in its effectiveness in bypassing traditional signature-based security mechanisms. On average, organizations are experiencing a staggering 643 Web-based malicious events each week, incidents that effectively penetrate the traditional security infrastructure of organizations and infect targeted systems. This figure includes file-based threats that are delivered over the web and email. File-based threats can be malicious executables, or files that contain exploits targeting vulnerabilities in applications. They are downloaded directly by users, via an exploit, or links in emails. The statistic of 643 infections per week does not include callback activities, which largely happen over the Web.

Compared to the second half of 2011, the number of infections per company rose by 225% in the first half of 2012. If you compare the first six months of 2011 with the first six months of 2012, the increase seen is even larger at 392%.

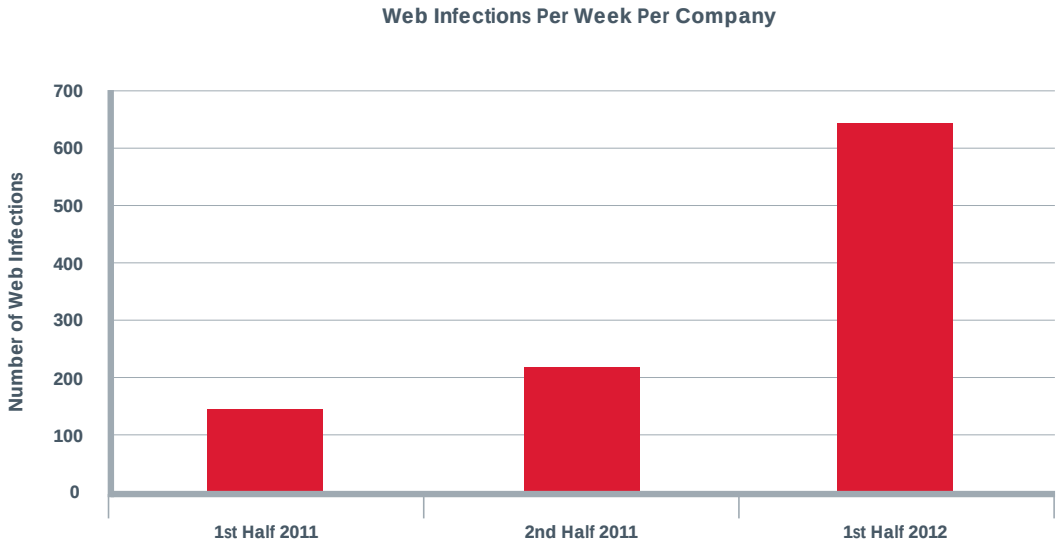
As outlined earlier, it is important to note that these figures aren't the total found in the so-called "wild", but are the number of Web-based infections that successfully evaded organizations' existing security defenses, such as next-generation firewalls and AV. The huge growth in these statistics amply illustrates a few key realities:

- Users remain very susceptible to clicking on malicious links, especially when those links exploit social engineering tactics.
- Embedding malicious code within Hypertext Transfer Protocol (HTTP) traffic is proving effective at bypassing traditional security mechanisms.
- As a result of these two dynamics, cybercriminals see that their tactics are working, so the number of attacks they launch continues to grow.

Explosive Growth in Advanced Malware Infections

- Growth from 2H 2011 to 1H 2012: 225%
- Growth from 1H 2011 to 1H 2012: 392%

The figure below illustrates the weekly count of Web infections identified by the FireEye Web MPS™ appliances across our global customer base. These levels reflect the number of Web-based malware attacks that originated outside the target organization, successfully evaded traditional filters, and were blocked or infected target systems.



Finding 2: Patterns of Attacks Vary Substantially by Industry—Attacks on Healthcare up 100%, 60% in Energy/Utilities

When assessing the average number of incidents that evade traditional security defenses, patterns and trends vary substantially across industries. For the most part, each industry experiences peaks in attack volumes at different times.

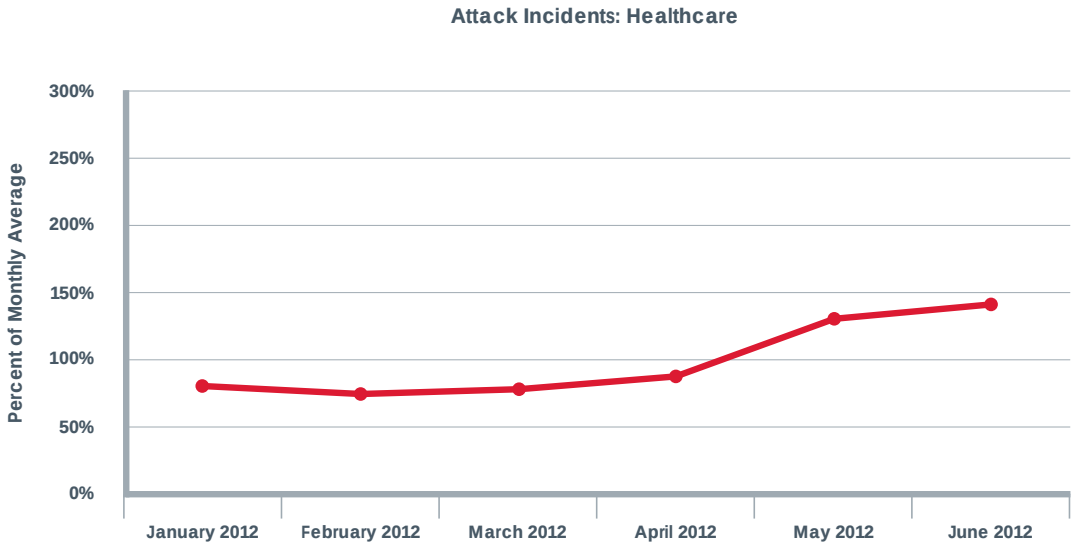
A couple of industries that are prone to high incidents were excluded from this report. Education was excluded since little, if any, control can be had over student systems and in general students are surfing more and visiting more risky sites. Also government was excluded since it is common for government agencies to receive data from FireEye but not send information back to FireEye.

Following, we'll highlight four of the most highly targeted industries and their respective numbers. The figures below illustrate the monthly incidents, including inbound attacks as well as outbound exfiltration and communication attempts. These incidents were identified by the FireEye MPS appliances deployed globally within the networks of customers and technology partners.

Healthcare

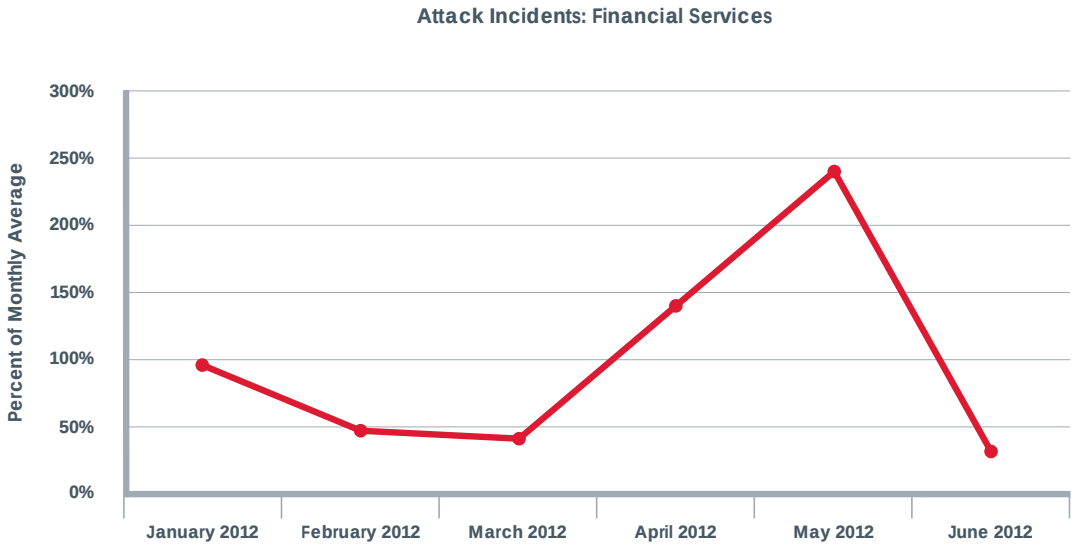
Between January 2012 and June 2012, the number of events detected at healthcare organizations has almost doubled. Compared to other industries, however, there has been a more consistent pattern of malicious activity, indicating a persistent and steady threat confronting these organizations.

As healthcare organizations move toward the adoption of electronic health record systems and digitally store and manage personally identifiable information (PII), these sensitive assets seem to be coming under increasing attack by cybercriminals.



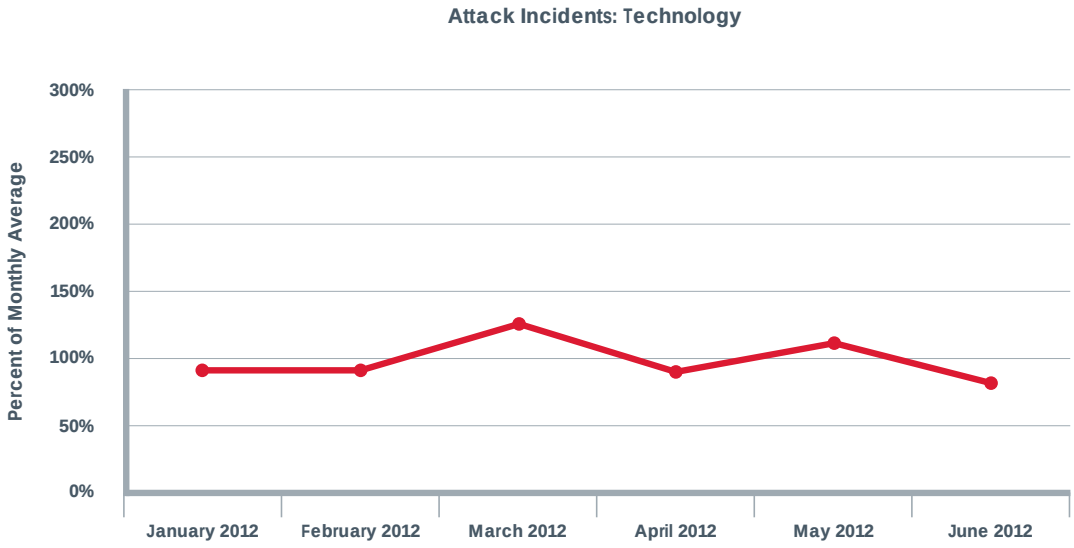
Financial Services

Between the second half of 2011 and the first half of 2012, the financial services industry has seen a massive increase in terms of the average number of events per customer for that industry. In one month alone (May 2012), the industry saw more events than the entire second half of 2011. Compared to healthcare, there have been more dramatic fluctuations in this market. The most dramatic shift discovered was a huge spike in May 2012, followed by a drop-off in June, which was a pattern also seen in May and June of 2011.



Technology

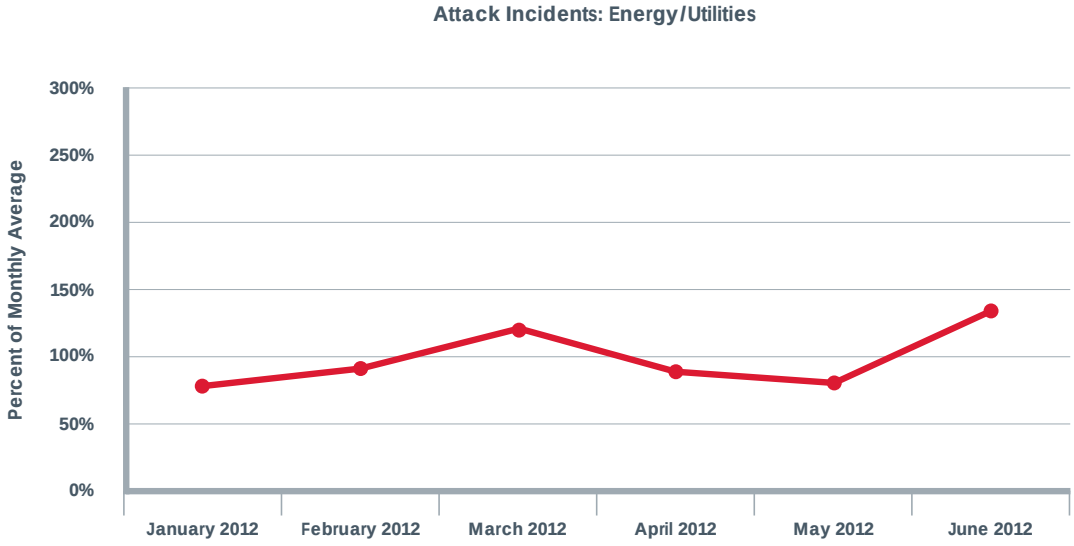
Companies in the technology sector continue to be the most targeted organizations. While total numbers have remained relatively stable on a month-to-month basis, overall numbers remain high compared to other industries.



Energy/Utilities

In the energy/utilities sector, there have also been some significant fluctuations in incidents, however the overall trend indicates a huge increase. In the past six months, energy and utility organizations have seen a 60% increase in incidents.

As the Night Dragon attack dramatically illustrated, critical infrastructures of energy and utility companies are under attack. In this case, criminals went after intellectual property, information on ongoing exploration, and records associated with bids on oil and gas reserves. Due to current geopolitical dynamics, data surrounding the sources of fossil fuel-based energy in particular are some of the most targeted assets.



If one looks across all industries two things emerge. First, no industry is immune from advanced attacks that have successfully bypassed traditional security. Second, when you compare the absolute volume of attacks across industries, those with high intellectual property or customer data are the most targeted. The highly targeted industries include technology, manufacturing, education, financial services, energy/utilities, and governments.

Finding 3: The Intensified Dangers of Email-Based Attacks, Both Via Links and Attachments

While the APT attacks that have been reported on in recent years have exhibited a range of different tactics, it is clear that there is one very common characteristic: email is the primary channel through which the attacks are initiated. Operation Aurora, GhostNet, Night Dragon, the RSA breach, and the majority of the other APTs that have been publicly documented have been initiated at least in part through targeted spear phishing emails. The bottom line is that organizations looking to stop APTs absolutely have to have capabilities for detecting and guarding against these kinds of attacks.

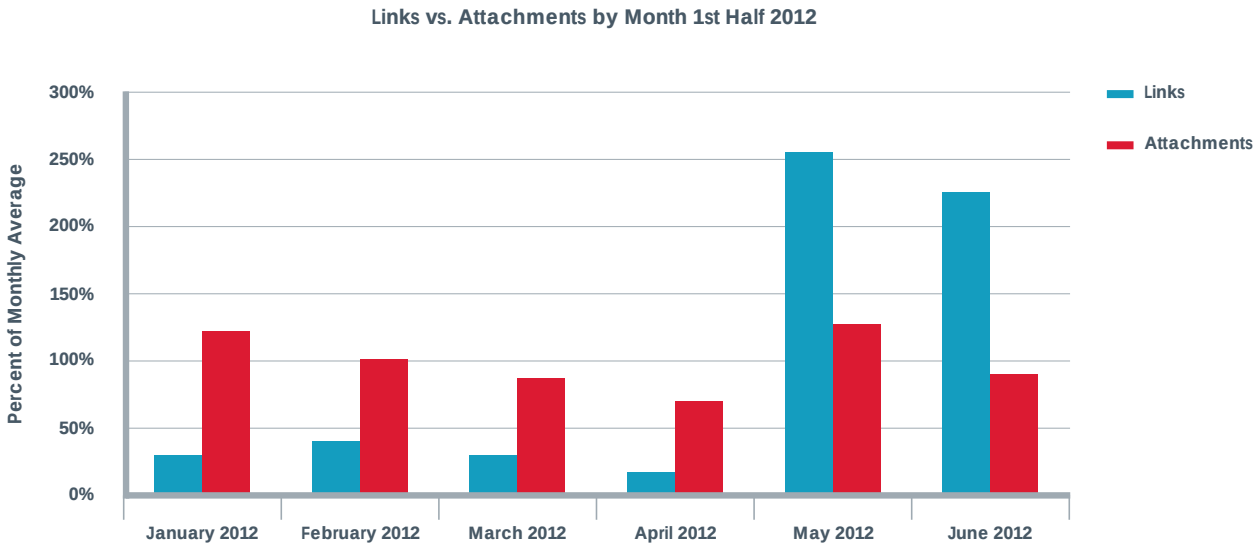
To gain entry into an organization's network, cybercriminals are launching their attacks through spear phishing emails. These emails either use attachments that exploit zero-day vulnerabilities or malicious and dynamic URLs. Between 1Q 2012 and 2Q 2012, there was a 56% increase in the amount of email-based attacks that successfully penetrated organizations' traditional security mechanisms.

During the course of 2012, there has been significant fluctuation in the amount of malware delivered via attachments versus links. In January 2012, the number of malicious links represented about 15% of the volume of malicious emails. By May and June however, the volume of malicious links outnumbered malicious attachments.

Moving forward, we expect to see continued fluctuation in the relative numbers of these categories on a monthly basis, but don't expect that either one will dramatically or permanently overtake the other in the long term. The critical takeaway is that both of these types of threats exist in significant numbers, and that organizations need to guard against both of these threat vectors to effectively strengthen their security posture.

As zero-day application vulnerabilities are patched, file attachments used in attacks wane and cybercriminals return to Web-based vectors. However, as we have seen in the past, a new crop of zero-day application vulnerabilities is always just around the corner, leading cybercriminals to return to file attachment-based attacks.

The figure below illustrates the monthly blend of malicious URLs or malicious attachments identified by the FireEye Email MPS™ appliances across our global customer base. These levels reflect the use of Web- and attachment-based infection vectors that were able to successfully evade traditional filters as they arrived from outside the target organization. Spear phishing emails may use malicious URLs, malicious attachments, or both to exploit OS and application vulnerabilities. By blending multiple malicious URLs with malicious attachments, cybercriminals seek to increase their success rate.

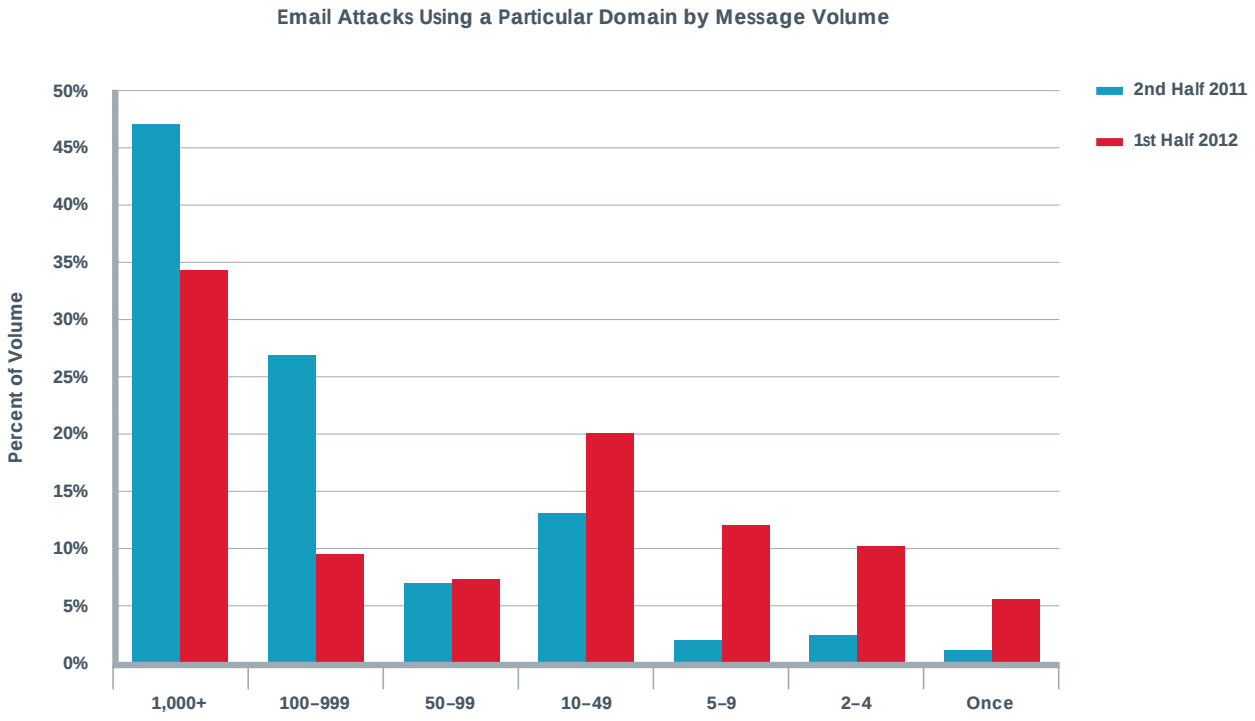


Finding 4: Increased Prevalence of Limited-Use Domains in Spear Phishing Attacks

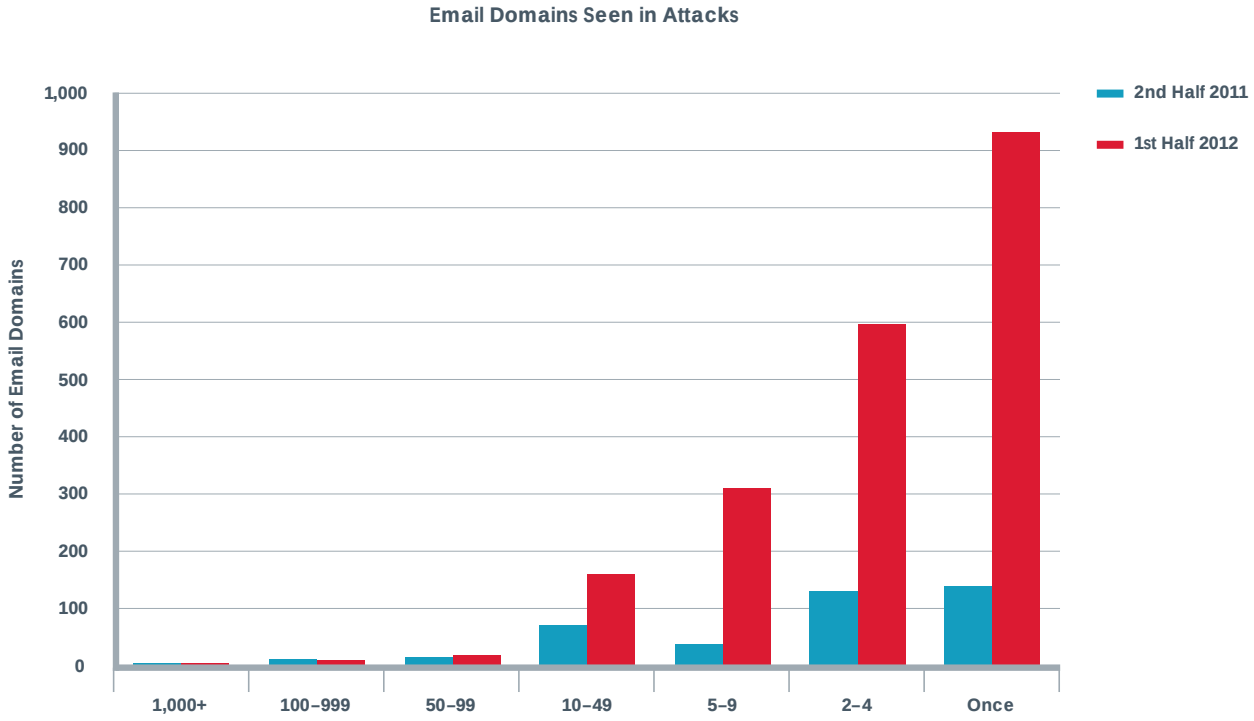
In their efforts to bypass organizations' security mechanisms, cybercriminals have continued to employ increasingly dynamic tactics. The continued explosion of malicious domains used in spear phishing attacks illustrates the unsolvable problem facing technologies that rely on backward-facing signatures, domain reputation analysis, and URL blacklists.

Criminals are increasingly employing malicious URLs for only a brief period of time before they move on to using others. "Throw-away" domains are malicious domain names used only a handful of times, say in 10 or fewer spear phishing emails. These domains are so infrequently used that they fly under the radar of URL blacklists and reputation analysis and remain largely ignored and unknown. As the chart on the next page illustrates, the number of throw-away domains identified increased substantially in the first half of 2012.

The figure below illustrates the classification of email attacks, broken down by the volume using a particular malicious domain. Again, these attacks were identified by the FireEye Email MPS appliances across our global customer base. We see that in the second half of 2011 and the first half of 2012, the number of spear phishing emails using a particular domain over 1,000 times remained stable. However, during that same period, we see that spear phishing attacks using a particular domain between 10 and 99 times dramatically increased. By limiting the use of particular domains, cybercriminals try to stay under the radar of reputation- and signature-based filters.



The chart below illustrates how the use of these throw-away domains has skyrocketed. Through social engineering, cybercriminals are personalizing emails and then using throw-away domains to bypass the signature- and reputation-based mechanisms that organizations rely on to filter out malicious emails. It is important to note that these URLs are sometimes randomly generated, and sometimes tailored to a specific tactic. In the second half of 2011, domains that were seen just once comprised 38% of total malicious domains used for spear phishing. In the first half of 2012, that figure grew to 46%. The graph below shows that the overall volume of spear phishing emails is increasing and our domain analysis also shows the ratio of emails that use limited-use domains is also on the rise.

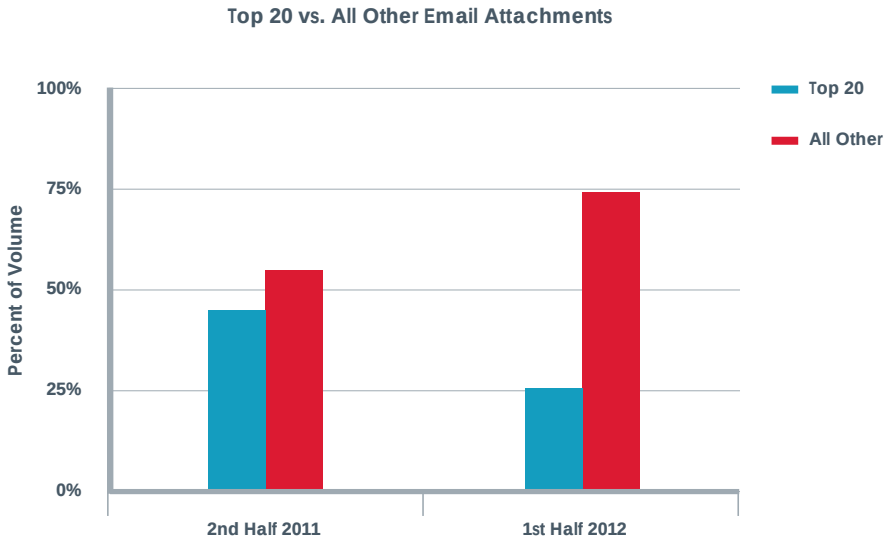


Finding 5: Increased Dynamism of Email Attachments

As outlined earlier, email-based attacks are used to initiate the bulk of the APTs reported, and guarding against both malicious attachments and URLs distributed via email is a critical mandate for organizations. Email-based attacks are the first tactic cybercriminals employ in order to get through the target's perimeter defenses and gain a foothold in the network. As security teams seek to guard against malicious email attachments, however, they are encountering a fundamentally evolving dynamic in the makeup of these files. Just like URLs, the use of malicious attachments is growing increasingly dynamic.

Over the past twelve months, the diversity of attachments that led to infections has expanded dramatically. In the second half of 2011, the top 20 malicious attachments accounted for 45% of attachments that evaded organizations' perimeter defenses. In the first half of 2012, the variety of malicious attachments increased so that the top 20 malicious attachments only accounted for 26%, nearly half of the figure in the second half of 2011. These numbers make clear that cybercriminals are changing their malware more quickly, employing a longer list of file names, and reproducing malware and morphing it in an automated fashion. In this way, the task of creating signature-based defenses to thwart these malicious files grows increasingly difficult.

Between the second half of 2011 and the first half of 2012, the average number of times a given malicious attachment was sent in an email dropped from 2.44 to 1.87.



Conclusions

As this report amply illustrates, organizations are under persistent attack, and the attacks being waged continue to grow more dynamic, effective, and damaging. For organizations that continue to rely solely on firewalls, IPS, AV, and other signature-, reputation-, and basic behavior-based technologies, it is abundantly clear that compromises and infections will continue to grow. To effectively combat these attacks, it is imperative that organizations augment their traditional security defenses with technologies that can detect and thwart today's advanced, dynamic attacks. This requires capabilities for guarding against attacks being waged on the Web, and those being perpetrated through email, including spear phishing emails that use malicious attachments and URLs.

Methodology

The analysis in this report is based on data collected by FireEye Web and Email Malware Protection System deployments, which detect inbound Web attacks, malicious attachments, and multi-protocol malware callbacks. The 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 that were drawn from mainly large and medium-sized enterprises and from many different vertical segments. Where applicable, customer growth was factored into the analysis and refinements were made to the infection analysis so comparisons should not be made to previous reports.

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 influenced by 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 leader in stopping advanced targeted attacks that use advanced malware, zero-day exploits, and APT tactics. The FireEye solutions supplement traditional and next-generation firewalls, IPS, anti-virus, and gateways, which cannot stop advanced threats, leaving security holes in networks. FireEye offers the industry's only solution that detects and blocks attacks across both Web and email threat vectors as well as latent malware resident on file shares. It addresses all stages of an attack lifecycle with a signature-less engine utilizing stateful attack analysis to detect zero-day threats. Based in Milpitas, California, FireEye is backed by premier financial partners including Sequoia Capital, Norwest Venture Partners, and Juniper Networks.

FireEye, Inc. | 1440 McCarthy Blvd. Milpitas, CA 95035 | 408.321.6300 | 877.FIREEYE (347.3393) | info@FireEye.com | www.FireEye.com