

Integrated Web & Email Security

How Consolidated Cloud Based Security Can Combat Complex Threats

ABSTRACT

Attacks today generally have two primary components – they are web based and employ multiple phases. The first phase of virtually any client side attack is the communication phase. In order to attack an end user, that victim must do something – click on a link, open an attachment, etc. The communication phase of an attack can leverage any number of technologies, but email is commonly the communication medium of choice. Email is anonymous and permits attackers to reach thousands, if not millions of potential victims at minimal cost. Attacks often therefore start with an email arriving in an employee’s inbox and progress when the victim clicks on a link that takes them to a malicious site. With attacks leveraging both web and email traffic, only a consolidated web and email solution will permit enterprises to see the full attack, report on the full threat and most importantly, ensure that the attack is not successful.

OVERVIEW	3
Case Study: How Backdoor Trojan Pirpi Exploited Multiple Channels	3
Stage 1: Social Engineering by Email	3
Stage 2: Web Based Attack to Infect User Machine	4
Stage 3: Persistent Exploitation.....	4
How Zscaler Responded to the Trojan Pirpi Threat.....	4
Integrated Web and Email Security	5
Defense: Social Engineering	5
Defense: Web Based Attack.....	5
Defense: Persistent Exploitation.....	6
Benefits of an Integrated Cloud Security Model.....	6
Conclusion	7

OVERVIEW

Enterprises have for some time, been saddled not only with directly managing security systems, but also with being forced to manage numerous point solutions from different vendors in order to obtain *best of breed* capabilities in each particular security domain. This can lead to a large combination of hardware and software solutions, with each requiring separate subject matter expertise to manage it. More importantly though, such disparate solutions are unable to combine information from separate sources and often fail to detect more complex attacks which involve multiple phases and different protocols. A common attack cycle today involves leveraging email for the social engineering component of the attack, while web traffic is used to actually deliver the malicious payload and manage the persistent exploitation of compromised hosts. Without a consolidated web and email security solution, such attacks may be missed and reporting simply cannot show the full scope of an attack without access to both web and email data.

Zscaler is the first security vendor to create purpose built SaaS (Security as a Service) based web and email security solutions that have been fully integrated from day one. By taking this approach, Zscaler is able to offer web and email security, which provides enterprises with consolidated protection, without the need to manage any hardware or software. With a SaaS based solution, consistent protection is applied across the enterprise regardless of employee location or device.

Case Study: How Backdoor Trojan Pirpi Exploited Multiple Channels

Attacks targeting end users must involve communication with the potential victim and that often occurs via spam or targeted email. Let's look at a recent scenario where spam email was used to social engineer victims to view a compromised website, which ultimately led to a complete compromise of the victim's machine.

Stage 1: Social Engineering Via Email

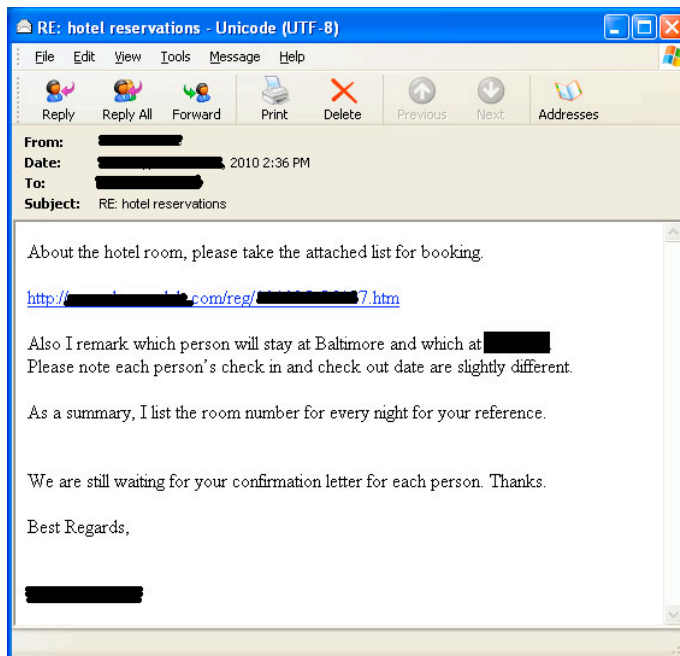


Figure 1 - Spam email message with malicious URL

In the first phase of the attack, the potential victim received an otherwise innocuous looking email message as shown in **Error! Reference source not found..** In this particular attack, the message arrived with the subject line of "RE: hotel reservations" and purported to be from an individual seeking to confirm recently made travel plans – something that is of course common for business travelers. The message followed a predictable format for such attacks – nothing more than a text-based message with a simple URL. The goal of the message was to make initial contact with the victim and use social engineering to trick them into clicking on the link as this is where the attack would actually take place. Gone are the days when exploits are included directly in the message itself. Email is now always scanned for malware and most enterprises follow best practices by restricting any executable binary attachments. Therefore email is now leveraged by attackers not as an attack vector itself but rather as a social engineering tool, which serves as a catalyst for

the overall attack.

Stage 2: Web Based Attack to Infect User Machine

Those individuals that clicked on the link were taken not to an attacker owned and controlled site, but rather an otherwise legitimate website which had recently been compromised. Whenever possible, attackers infect third party sites rather than set up their own. Why? Because a legitimate site has already developed a positive reputation and it will therefore not be blocked by URL filters of static security tools which regularly scan web sites to determine if they are hosting any malicious content. While the compromised site in this scenario would eventually be given a negative reputation once the attack was uncovered, the attackers had a window of several hours if not days to piggyback on the good name of the site in question. Unfortunately, due to the relatively poor state of web application security today, the challenge is trivial for attackers looking to infect legitimate websites en masse. They simply need to write a script that will scour the web looking for pages vulnerable to common injection attacks.

The attack in this example included some additional intelligence to narrow the scope of the attack only to those browsers most likely to be exploitable. Therefore, the injected content first identified the browser type and version, only delivering the malicious payload to clients using Internet Explorer 6 or 7. Others were simply redirected to a blank page.¹ Moreover, the attack would only be delivered once to each requesting IP address, further complicating efforts to identify the attack. This is a relatively common attack pattern. Attackers want to remain as stealthy as possible, as the longer they can go without raising suspicion, the longer the attack will succeed and the more victims they will infect. As this attack involved a so-called 0day vulnerability, no patch was in place for the attack, and anyone using a vulnerable browser became a victim simply by clicking on the link in the email message. No further action was required.

Stage 3: Persistent Exploitation

At this stage, the attacker had full control of the victim machine. Depending upon the goal of the attack, the machine could be recruited into a botnet army to be used for later malicious purposes. Data could be exfiltrated from the machine; it could be used as a catalyst for another attack, or any other purpose that the criminal chose to leverage it for.

In this case, the infected machines contacted yet another compromised server to receive further instruction, which arrived in the form of encrypted files with a .gif extension. The victim machine then had a permanent backdoor installed that could be used to remotely control the machine. Imagine such a machine on your corporate network. An attacker would have complete access to a trusted machine on your network, simply because one of your employees clicked on a link in an email message. A frightening thought indeed.

How Zscaler Responded to the Trojan Pirpi Threat

Zscaler works closely with Microsoft via their MAPP (Microsoft Active Protections Program) initiative and as such was immediately informed of the attacks once they were brought to Microsoft's attention.² Microsoft also shared private information about the attacks, enabling Zscaler to quickly deploy protection within hours of initial notification.³ A patch for the 0day vulnerability (CVE-2010-3962) did not become available for 41 days following the initial Microsoft Security Advisory; yet during that time, Zscaler customers were shielded from attack simply by leveraging the Zscaler service.

¹ <http://www.symantec.com/connect/blogs/new-ie-0-day-used-targeted-attacks>

² <http://www.microsoft.com/technet/security/advisory/2458511.mspx>

³ http://zscaler.com/sec_advisory_november3_2010.html

Integrated Web and Email Security

Using the previous example, which is relatively typical of combined web and email attacks, let's look at the full attack cycle in order to understand the various points at which the attack could have been stopped.

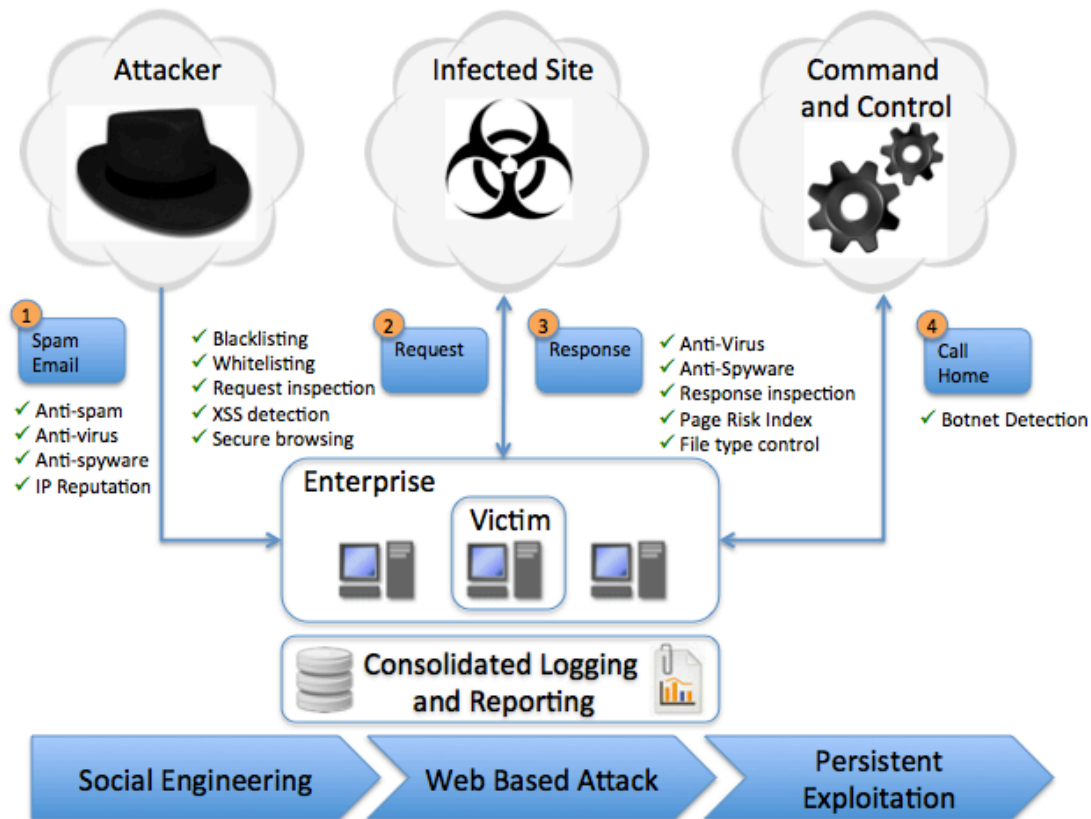


Figure 2 - Zscaler protections at each attack phase

Defense: Social Engineering

Stopping an attack at the earliest possible point should be the goal of any security strategy. With a consolidated web and email solution, this is not only possible, but spam detection is continually enhanced by intelligence gained from monitoring web traffic. For example, as web pages and domains are found to be hosting malicious content, either on malicious sites owned by attackers, or more likely legitimate sites that have become infected, this information can feed the email inspection engines. Should messages be identified which are designed to social engineer employees into visiting such sites, the message can be blocked before the employee even has the option of following the malicious link.

With cloud based email inspection, Zscaler inspects millions of messages each day from corporations around the world. In doing so, dynamic spam detection rules are constantly updated with real-time data, ensuring that knowledge is consolidated from multiple vantage points, which ensures that an attack on one Zscaler customer benefits all customers as protections are continually updated as new attacks are identified.

Defense: Web Based Attack

Zscaler's cloud based architecture permits full bi-directional inspection of all web content, even for traffic traversing an SSL encrypted tunnel. This inline inspection is critical to ensure that block/allow decisions are not based on static historical scans of web traffic, but on actual content. Recall from the Trojan Pirpi example that the payload was delivered only to victims with vulnerable browsers (IE 6 and 7) and additionally, was delivered only once per IP address. If blocking malicious code relied on past results from historical scans of the malicious page, they could easily be based on a benign response and then incorrectly allow the malicious payload through.

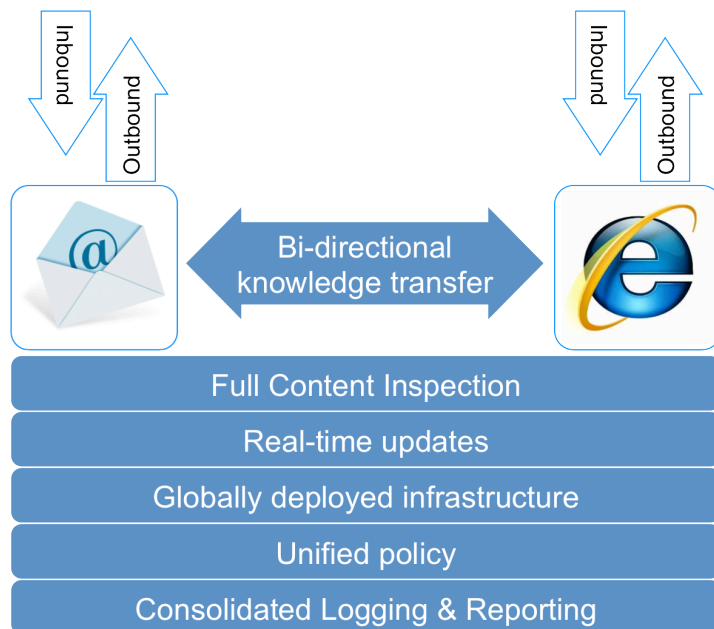
Full content inspection is necessary to identify malicious payloads, which could be buried within virtually any response, from any site. URL filtering alone is no longer a viable security measure given the high volume of legitimate sites that are being infected each and every day. Should security vendors simply block a known malicious or infected site, attackers can quickly move to a new location. While URL based blocks provide an initial layer of defense, they fail to provide a complete solution. Considering the Trojan Pirpi example, following notification of the Oday attack from Microsoft through their MAPPs program, Zscaler was able to develop and deploy protections identifying the payload itself, regardless of where it may have resided. This ensured that customers remained protected from the attack even if it were deployed elsewhere or alternate groups launched similar attacks.

Defense: Persistent Exploitation

While preventive controls seek to prevent exploitation in the first place, detective controls must not be ignored. Machines can become infected either due to inconsistently applied security policies or due to a new attack vector for which protections were not in place. Regardless, systems must be monitored for such compromises and when identified, quickly quarantined to prevent further damage. Zscaler monitors all outbound communication to identify traffic from compromised machines to botnet command and control servers. As with all Zscaler Advanced Security controls, this involves not just monitoring the destination of a request to block contact with known command & control (C&C) sites, but also full content inspection to identify contact with newly established C&C servers.

Benefits of an Integrated Cloud Security Model

With separate web and email solutions, supplied by different vendors, enterprises are left to manage two sets of



unique infrastructure. This not only doubles the level of effort to manage and maintain the systems, but critically, fails to benefit from the synergies offered by a consolidated solution. With Zscaler, established policies apply to web and email traffic alike. For example, when a data leakage protection (DLP) policy is established to monitor all outbound communication for credit card numbers in order to comply with PCI standards, that same policy applies to both web requests and email messages. This just makes sense. As demonstrated previously, attackers leverage multi-phased attacks that take advantage of both web and email as avenues to communicate with potential victims. Likewise, data can accidentally or intentionally leak from an enterprise via any communication channel. Enterprises should not be forced to manage separate solutions for each and every communication channel, nor should they be stuck with disparate

Figure 3 - The Benefits of consolidated web and email security

reporting that fails to recognize attacks crossing from one protocol to another.

Beyond the practical benefits of managing a single consolidated solution, security is greatly enhanced by leveraging knowledge transfer from one platform to the other. Zscaler Labs, the research and development arm of the company, is constantly researching emerging attack techniques. Additionally, Zscaler's Interrogator™ Oday analysis engine is continually mining both Web and email data in an effort to uncover previously unknown threats. With attackers merging web and email into more comprehensive attacks, it is simply not possible to obtain a full view of the threat landscape without mining data from both platforms.

Conclusion

Enterprises are becoming increasingly mobile, while attacks against end users are evolving in sophistication at a frightening pace. Employees are constantly under attack as the weak link in the security chain. Attackers know that if they can compromise a single trusted device within an enterprise, they then have a platform from which to launch additional attacks. In such an environment, enterprises must seek security solutions that can protect end users whether they are in the office or on the road and regardless of the device that they are working on.

Moreover, with attacks that involve multiple phases, consolidated solutions are required which can protect against such threats by implementing unified policies and consolidated reporting. With SaaS-based and fully consolidated web and email security solutions, Zscaler is able to provide consistent protection across the enterprise, without the headache of adding technology that must be managed and maintained.