

### The New Threat Reality

If the last decade is any indication of the types and volume of spam that companies are likely to see going forward, then it is clear that they are in for quite a battle from a variety of new, random and complex attacks with potentially catastrophic results. Spam started out simply enough as a way for advertisers to quickly and cheaply get their messages to a large audience. With thousands, to potentially millions, of unsuspecting people as targets, even meager response rates of less than one percent produced profitable spam campaigns and turned the in-box into the next “great” junk-mail marketing medium.

It wasn’t long before email users declared spam a nuisance and the world witnessed the birth of the first anti-spam filters and Real-Time Black List (RBL). Unfortunately, as quickly as new spam-fighting technology and filters have been deployed to stop spam, spam emailers have been equally innovative, changing their tactics to bypass virtual roadblocks in pursuit of just a few users that would open the emails and click. It is these email users who are the target. Clever technology combined with email user-error and ignorance has often placed cyber criminals at a slight advantage, proving that filters and corporate policies cannot stop everyone from opening doors to personal information and corporate networks.

This raging battle between good and evil has never been as strong as it is today as spammers and cyber criminals are constantly working to stay one step ahead of the latest email security improvements. They know that if they can get their messages around the filters into email in-boxes – even a few – they have a chance of turning clicks and information into profits. Like the scammers, security solution providers are constantly working to thwart the criminals, moving beyond simply stopping the campaigns to predicting from where and when the next threat will strike.

This white paper will focus on defining the new threat reality, which includes new tactics and designs, embedded links, spear phishing, malware and mobile attacks that are more sophisticated and catastrophic. We will provide examples and analysis of the next generation of spam and scams in an effort to arm organizations with the knowledge and tools to keep them from becoming tomorrow’s victims.

### Seven Emerging Email Threats

The following outlines seven threats that have emerged recently and are likely to continue to trend upward in the future.

#### ***Blended Threats***

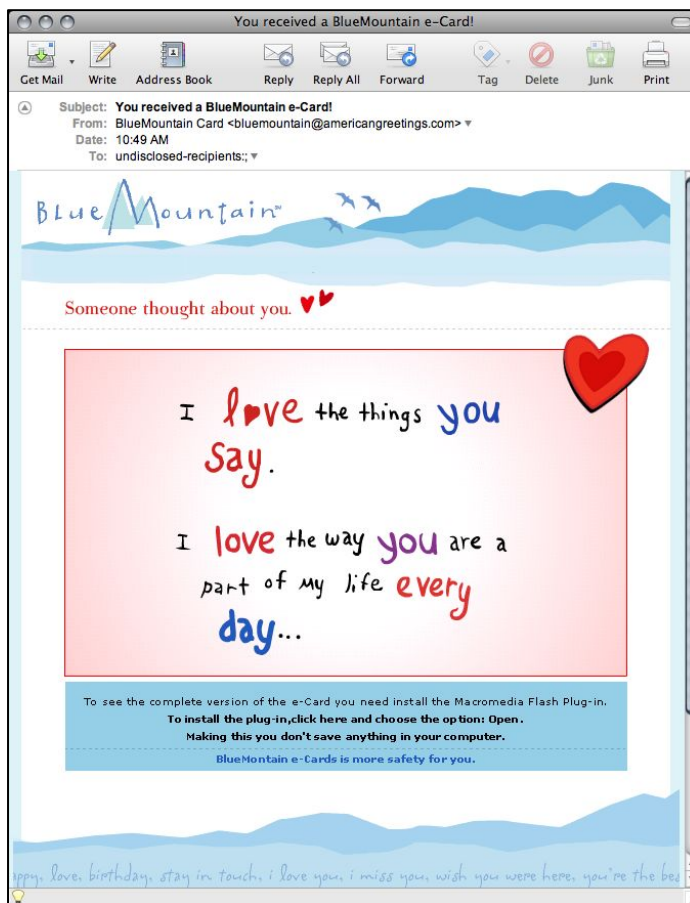
One of the most rapidly growing types of spam today comes in the form of blended threats. In the early days of spam, messages typically served a single purpose; trying to get unsuspecting email users to respond to an email by buying a product or clicking on a link in an email. For many early spam campaigns, the person or entity sending the email made money when the email was opened or when recipients clicked on links embedded in the email. While the spam was unwanted, it was typically easy to spot, and quickly deleted. The level of the threat, however, quickly changed when the embedded links or attachments became malicious in nature. Cyber criminals started to use email to send viruses and malware executables, as well as linking to web sites that had malware embedded in the site’s HTML code. A simple click on a link or opening an attachment could launch a virus giving remote

access to a scammer half-way around the world or sending personal financial information stored on the PC to a host location.

Today, scammers have taken malicious spam to another level, distributing emails with blended threats that phish for personal or corporate information, as well as install viruses and route recipients to websites that lead to immediate malware execution. In addition, these emails come disguised in graphical wrappers that mimic trusted sites like national and community banks, and contain files that have trusted extensions, including .doc, .pdf and .jpg.

A new e-Card spam campaign discovered In December 2009 appeared to come from American Greetings' BlueMountain.com.

The email, with the subject line "You received a BlueMountain e-Card!," suggests that users "need to install the Macromedia Flash Plug-in" to see the "complete version" of the e-Card. The entire body of



of the email, including the header and footer of a legitimate Blue Mountain e-Card, was an executable. Clicking on any part of the message would launch a browser window, and depending on a user's browser security settings, could have automatically downloaded a virus with a single click. The spam was distributed by a botnet and had been aggressively targeting Internet Service Providers. The virus was also identified as a banking Trojan, which are used by cyber criminals to steal banking credentials from computer hard drives or web forms or by capturing keystrokes. Most banking Trojans stay dormant until an unsuspecting customer logs on to his or her banking website. The Trojan then steals usernames and passwords and sends the information back to its creator(s). People like e-cards and trust sites like BlueMountain.com. Consequently, senders with bad intentions are utilizing commonly used Internet services, going as far as designing the fake emails and corresponding web sites to have the same look and feel as the actual brands.

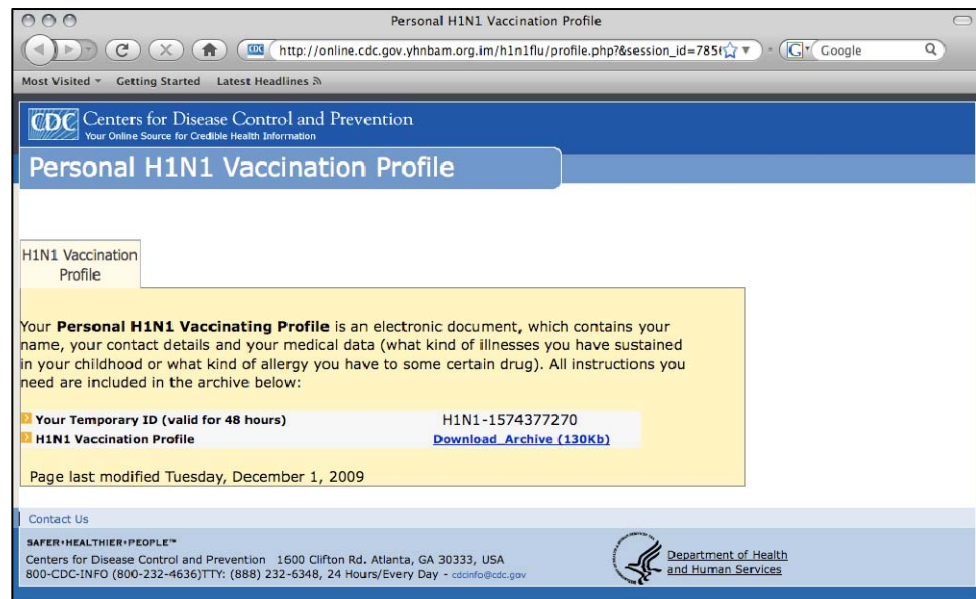
### Classic Phishing

While blended threats are on the rise, classic phishing campaigns still pose a significant threat to email users and corporate networks. Not only are swindlers using phishing attacks to target average consumers, such as the Nigerian 419 phishing campaign that continues to find victims, they are also targeting business professionals, including the legal community that is fighting to stop them. Today's

phishing attacks have also stolen the branding elements of trusted organizations, once again hoping that email users are not paying attention to the details.

Among recent examples of highly publicized phishing attacks is one involving the Center for Disease Control and Prevention (CDC) during the height of the H1N1 Vaccination concern.

The email with the subject line "State Vaccination H1N1 Program," suggested that recipients "need to create your personal H1N1 (swine flu) Vaccination Profile on the cdc.gov website." When users clicked on the embedded "Create Personal Profile" link in the email, they were sent to a page that had a CDC-



branded header and footer, as well as the U.S. Department of Health and Human Services logo. Visitors to the site were notified that their "Personal H1N1 Vaccination Profile" is an "electronic document, which contains your name, your contact details and your medical data" and needs to be downloaded. The file was actually an executable that contained a Trojan virus identified as W32/Vacc.A!tr. Email recipients that downloaded the "electronic document" would have installed the virus on their computer allowing the malware to use the computer to send out additional spam. For those that visited the site, but did not download the file, the fake web site also contained malware that exploited recent vulnerabilities in Adobe Reader and Flash software.

This particular hoax posed a threat to email users and corporate networks, and also forced the CDC to scramble to address the media attention.

## ***Spear Phishing***

A spear phishing campaign is a highly targeted form of phishing that typically focuses on a single organization. Recent examples of spear phishing campaigns however are more sophisticated, targeting a large number of domains with highly personalized and customized messages. Emails appear as if they come from a trusted source, such as an employer who would normally send an email to the entire company or a well-known organization. Because of the familiar sender ID, email recipients may not pay attention to the other details in the email, and are likely to do what the email asks.

One example of this type of phishing attack occurred on the campus of Dominican University in Chicago in the spring of 2009. As a result of the attack, Dominican was blacklisted by several major

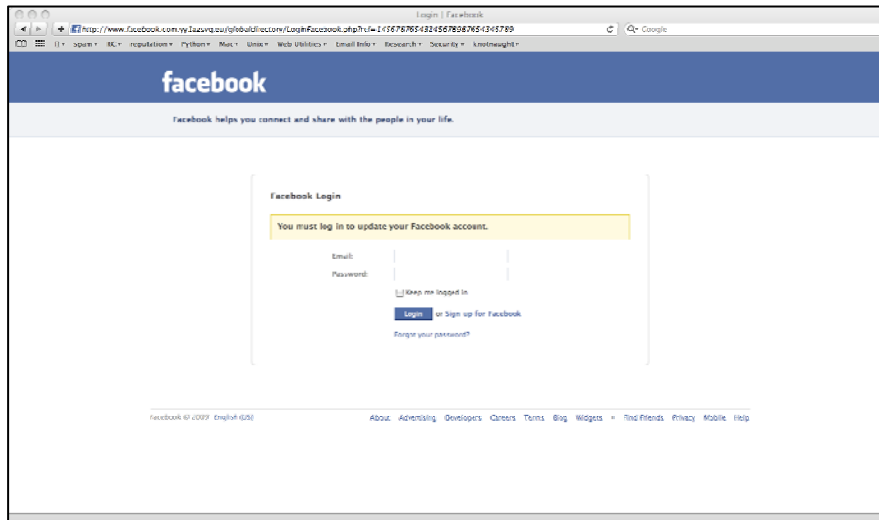
email providers, including MSN, Yahoo and Hotmail. The phishing emails warned users that their university web mail accounts were going to be cancelled unless they replied to the emails with their usernames and passwords. Unfortunately, some users became victim to the scam, and it wasn't long before their email accounts were being used to send spam messages around the world. The attack forced the university's IT department to constantly monitor its email queues to determine which accounts were being spoofed, while the multiple attacks frustrated efforts to clean the university's domain.

### **Novel Media:**

Another significant target of this New Threat Reality is specifically targeted at social networking sites like Facebook, Twitter, MySpace, etc. These sophisticated phishing attacks combine email and spoofed social networking sites in an attempt to solicit personal and financial information.

With more than 400 million users, Facebook has almost become ubiquitous, making Facebook users a prime target for cyber criminals. By spoofing the branding elements of these social networking sites, criminals prey on users' comfort levels with these brands to gather personal information that will grant them access to a variety of private and confidential data.

While Facebook has been the object of numerous spam campaigns, in the fall of 2009, scammers distributed a massive blended-threat Facebook spam attack that included a phishing scam and a notorious banking Trojan virus. A link within the spam email took users to a spoofed Facebook login page requesting the user's Facebook account information. After entering their credentials, users were then prompted to download "updatetool.exe," a Zbot Trojan variant that is known to scour the infected hard-drive for personal banking information and various login credentials, as well as perform key-logging and other nefarious activities.



As noted by the image above, the spoofed Facebook login page was fairly sophisticated and used www.facebook.com in the sub-domain portion of the malicious URL. As a result, people with small screen resolution or small browser windows/address bars size might think they are actually on Facebook's login page.

It is this familiarity and user comfort level with these popular sites and services that spam developers are

now targeting. Unfortunately in the above example, many anti-virus engines did not detect the campaign, and the spam campaign reached many inboxes across the country.

### **Rapid-Evolution Malware**

While viral mutation is nothing new to the industry, polymorphic virus technology continues to defeat many anti-virus engines that are the first line of defense. The ability for the virus to change its binary code each time it infects a file makes it difficult for traditional anti-virus engines to detect a pattern, and thus stop the virus from spreading. Embedding malware onto computers and networks has become a key motivator behind spam campaigns, and without the appropriate behavior-based malware detection and real-time defenses, polymorphic viruses may go undetected.

Viral mutating malware can corrupt computer systems while going undetected for extended periods of time. Depending on if/when the malware is detected, the virus can do everything from modifying files to point to malicious web sites to actually making a system inoperable.

### ***Highly Permuted, Short-lived Campaigns***

In an effort to further circumvent today's anti-spam technology, many spam emailers have increased the randomness and shortened the duration and reach of their campaigns. What were once massive attacks spread out over several days have now become focused attacks played out in a matter of minutes. Many anti-virus engines and anti-spam filters simply miss these campaigns because of the higher degrees of randomization. Before they know it, companies have become victims as security filters are unable to respond to the real-time threats. The randomness further complicates the situation because security administrators don't have the information they need to create filtering rules that will thwart future campaigns of this type.

### ***Smartphone Attacks***

With more people using Smartphones to send and receive email, network administrators are learning the hard way that security must extend beyond the desktop and the corporate network. Cyber criminals have started to develop sophisticated botnets specifically for Smartphones. Once installed on the phone, intruders have the ability to use the phone just as they would an infected computer.

An iPhone worm discovered in November 2009 took advantage of iPhone users who had unlocked their phones and failed to change the default password. This particular bot launched a popup window notifying the iPhone owner that his/her phone has been hacked. The victim was then sent to a web site that demanded a \$5 ransom payment to remove the malware. A second iPhone bot detected the same month also targeted "jailbroken" iPhones. The bot gave the hacker the ability to use the phone to spread spam, pilfer data and seize online accounts. In this attack, the worm also changed the default system password making it difficult for users to regain control.

While the two iPhone examples mentioned above targeted people that had modified their phones' security settings, the growing and widespread adoption of Smartphones has presented a significant challenge for users and their employers.

## **Combating the New Threat Reality**

In order to combat this New Threat Reality, companies need to understand that the attack methods of hackers and cyber criminals have changed and will continue to evolve. Unfortunately, security technology has not always kept pace with the threats. Spam was once seen as a nuisance with low overall impact on email users and networks. The massive attacks were spread out over long periods of time, making it easier for corporate defenses to filter out the spam and prevent any widespread problems. Email was the preferred medium and spam typically had a single purpose. Statistical

defenses were adequate in thwarting the campaigns while false negatives and false positives were the focus for email security solution providers.

Today, the threats are more sophisticated and potentially catastrophic. The campaigns have intrinsically evil purposes and the attacks are shorter and more targeted. The threats also now include multiple components, incorporating elements of social media and privilege escalation in an attempt to bypass security and access private and confidential files, resources and information.

Today's defenses must be deterministic and precise, understanding cognition, behavior, decision and action, while delivering fast response rates and sustainable blockage rates. Reactionary solutions are no longer enough, as the new threats require real-time dynamic feedback that will protect users from yesterday's campaigns, as well as help predict where spam and phishing attacks will come from tomorrow.

Red Condor's proprietary email security technology was developed to protect against the emerging catastrophic messaging threats not handled by most anti-virus, anti-spam (AVAS) vendors. To meet these modern challenges and requirements, Red Condor has developed the Zero Minute Defense Network and added layers of filters, which gather real-time knowledge to rapidly create new detection and protection rules. These rules are then pushed out continuously to customers through Red Condor's fully managed Hosted Service and MAG network appliances. It is the company's combination of global reach, speed of rule execution, breadth of rules and layers of defenses that is helping Red Condor provide customers with the tools to effectively face the new threat reality.

Clearly, not all email security solutions are built to defend against emerging email threats. Regardless of whether someone is using a desktop, laptop, netbook, tablet or Smartphone, an organization's umbrella of security needs to protect any device connected to their networks and deliver real-time filtering that quickly stops the threat before it reaches the inbox. Implementing a security solution that can meet tomorrow's threat reality with equally sophisticated, real-time defenses, precision filtering and speed will give companies a better chance of avoiding any intended catastrophe.

## About Red Condor

Red Condor ([www.RedCondor.com](http://www.RedCondor.com)) is revolutionizing spam fighting with its next generation technology. Red Condor's highly accurate email filter, hybrid architecture Vx Technology™, and fully managed appliances lead to a dramatic reduction in the cost of owning a premium spam filter. With solutions for small businesses, as well as ISPs with millions of email inboxes, Red Condor has a cost effective, timesaving solution that is rapidly gaining market share. The system's design has built in zero tolerance for lost email, and a near zero false positive rate while achieving long term spam block rates greater than 99%. Red Condor Archive is a secure message archiving service with lifetime retention and unlimited storage. The company's next generation technology is backed by a 24x7 customer care center staffed by email security experts at Red Condor's headquarters.

### RedCondor

1300 Valley House Drive, Suite 115  
Rohnert Park, CA 94928

Toll Free: 888-9NOSPAM  
1-888-966-7726

[www.RedCondor.com](http://www.RedCondor.com)