



# Lippis Report

White Paper

Lippis Report 130:  
**Global IT Security Threat Trends and Future Outlook**

by  
Nicholas John Lippis III  
President, Lippis Consulting

July 2009



## Lippis Report 130: Global IT Security Threat Trends and Future Outlook

Cyber crime and IT security threats are taking a more ominous turn as they seek financial gain by exploiting open Web 2.0 technology vulnerabilities and share “tricks of the trade” via collaborative web sites. Hackers and cybercriminals are launching ever more sophisticated attacks on businesses and individuals, intent on mastering the arts of trust-breaking and reputation-hijacking. The economic motive for cybercrime is well documented and lucrative, which is disturbing on multiple levels.



### Mixed Vendor Networks Drive Complexity & Opex Up

[Listen to the Podcast](#)

First, during the economic downturn with high and growing unemployment more cybercriminals are being recruited with the opportunity to make \$5K to \$10K per week at “entry” level positions; large cybercrime organizations “earn” or more appropriately “steal” tens of millions of dollars annually. Second, with the prospect of large paydays, cybercriminals are increasing their skills to both stay one step ahead of security professionals and to craft even more sophisticated attacks that blend worms, botnets, phishing, etc., over mobile, social networking, cloud computing and traditional Internet vehicles. Attackers are combining old-school methods that exploit Windows vulnerabilities with new complex approaches, resulting in increased difficulty in detecting attacks and diligence on the part of IT security operations to protect corporate assets. There is a good spy versus bad spy force at work and it’s hard to tell who is winning. In this Research Note we expose and highlight key global IT security threats and trends from the first part of this year and provide a future outlook. This Research Note is based in part upon the “Cisco 2009 Mid-year Security Report” available here.



### Cisco Seeks To Add Visibility and Control to Electrical Systems via a Smart Grid Communication Infrastructure

[Listen to the Podcast](#)

The Conficker worm offers insight into global threats and trends, shaping the future outlook for IT security. The Conficker worm propagated globally, infecting tens of thousands of new machines daily during the fall of 2008 and was slowly exposed as a massive botnet with a strong profit motive. These new deceptive exploits are increasingly using different forms of malware to avoid detection and increase reach plus impact. This new breed of exploit proves tricky as it changes form, launches multiple and different attacks and is instructed by its creators to perform new tasks via multiple forms of Internet communications.

For example, an exploit may start as a worm, disabling various Windows services such as Automatic Update and Security Center and block access to websites that allow users to remove the infection. These exploit techniques are not new and that’s the point. Cyber- criminals will use old techniques such as exploiting a Microsoft vulnerability to plant their code onto millions of computers only to turn them into botnets with the ability of the cybercriminals to instruct the bots to perform specific tasks. For example, it’s not uncommon that once infected a bot will then receive instructions directing it to propagate, gather personal information, download and install more malware onto victims’

**Navigating Network Infrastructure Expenditures During Business Transformations**

[Get the White Paper](#)



computers.

For Conficker, researchers realized that on April 1, 2009 the growing botnet would transition to a new method of communicating to its creator. The security industry responded to this threat with a Microsoft patch and a new model of threat mitigation. As April 1 approached, security researchers were able to “dissect” the worm and piece together its plan of attack. On or about April 1, Conficker would begin generating thousands of Internet domain names and attempt to instruct some of them to download updated software. Although the botnet began generating 50,000 domain names per day compared to 500 before the April update, this method of communication was never actually put into place; peer-to-peer functionality was instructed instead. The lesson learned here is that these new breeds of exploits are difficult to dissect and they morph into different forms of malware.

The end game for the large percentage of exploits is to monetize and botnets offer unique attributes for their cybercriminal owners. Botnets are well suited to launch an outbreak of spam, for example. Consider that a botnet distributed spam offering a free trial of software that would allow individuals to read supposedly private SMS messages. The malicious payload delivered via the fake SMS software was the Waledac worm, which the botnet subsequently advertised as a security software to remove it for a fee. Spam and scam techniques rise with high profile global news such as the swine flu where swine flu spam accounted for 4% of global spam traffic. But in addition to these spam and scam approaches botnet owners are also leasing their bots in a software-as-a-service model to other cybercriminals to launch their own exploits, which not only provides revenue to the botnet owner but increases the number of exploits distributed per network of bots. By the way the going rental rate for a bot is 10 to 25¢.

**Cisco IPTV Broadcast  
Regarding Cisco 2009  
Mid-year Security Report**

[Watch the Video](#)

It's this new level of chicanery that has demanded a new model for threat mitigation response. The rapid propagation of these new complex and tricky exploits emphasizes the need for risk and threat management that intelligently determines that attacks can be sourced from anywhere in a network and on the globe. A key takeaway from the Conficker experience is the value of collaboration in fighting back. The Conficker Working Group, composed of more than 100 organizations involved in technology and security was formed in February 2009. ICANN, the organization that coordinates the Internet's naming systems and a member of the Conficker Working Group, was able to compile a list of the domain names Conficker was attempting to contact, thanks to data provided by security researchers tracking the worm. ICANN then passed this information to top-level domain operators, who could then block these domains.

This coordinated effort went a long way toward blunting the impact of the worm and subsequent botnet and is now the new model for how researchers share information and develop defenses to mitigate a new breed of exploits. From the above the following IT security global threat trends and outlook are offered:

**Morphing Exploits Will Become The Norm:** The days of a single exploit, be it a worm, virus, botnet, spam, etc., are over. Today's cybercriminals use all of these “tools” and their unique attributes to inflict harm with an ever-increasing profit motive.

**Botnets are the Tool of Choice:** These networks of compromised computers serve as an efficient means of launching an attack. In addition, it's becoming clear that botnet owners are renting out these networks to fellow criminals, effectively offering comprised resources using the SaaS model to deliver spam, malware, etc.

**Spam Will Only Increase:** One of the most established ways to reach millions of computers with legitimate sales pitches or links to malicious websites, spam remains a major problem in the spreading of worms and malware, as well as clogging Internet traffic. A staggering 180 billion spam messages are sent each day representing on average about 90 percent of all email traffic. Botmasters are increasingly using spam to promote the propagation of worms, spyware and online scams which will only increase the amount of spam going forward.

**Spamdexing:** Many types of businesses have long used search engine optimization to be listed more prominently in searches conducted on Google and other sites. The tactic, involving packing a website with relevant keywords or

search terms, is increasingly being used by cybercriminals seeking to disguise malware as legitimate software. Because so many tend to trust and not be suspicious of rankings on leading search engines, they may readily download one of the fake software packages assuming it is legitimate. The creators of Conficker used spamdexing to promote fake security software, and other malware. Be careful during major news cycles as spammers are increasingly using social engineering via spamdexing to offer fraudulent and dishonest solutions.

**New Attacks Target Social Networking:** The rise of social networking has made it easier to launch attacks. The hundreds of millions of people engaging in these online communities are more likely to click on links and download content they believe were sent by people they know and trust.

**Text Message Scams Only To Increase:** Since the start of 2009 at least two or three new campaigns have surfaced every week targeting handheld mobile devices. The rapidly growing mobile device audience is unfortunately a new frontier for fraud, irresistible to criminals. With some 4.1 billion mobile phone subscriptions worldwide, a criminal may cast an extraordinarily wide net and still walk away with a nice profit, even if the attack yields only a small fraction of victims. The Conficker creators used spam to offer a free trial of software that would allow individuals to read supposedly private SMS messages.

The above list of global security trends and associated outlook point to ever more sophisticated exploit techniques at the same time as hackers and cybercriminals increasingly target popular new platforms such as smartphones, Web 2.0 technologies and social networking sites. Furthermore, as cloud computing takes off it is highly likely that it will be an irresistible target for cybercriminals, and hackers as well, to launch their exploits. Remember the above list has manifested itself only during the last six months highlighting how fast cybercriminals and hackers have become in modifying their techniques.

But security researchers have modified their defense techniques to confront these new challenges, and IT security operations can too. During the first half of '09 there were new positive and potent methods for combating these threats. First, security researchers and the organizations they notify and work with have stepped up their use of collaboration technologies. Collaboration is being used by the "good" guys to quickly identify threats and develop mitigation solutions. Collaboration between security researchers, standard organizations, vendors, service providers and law enforcement is the new organizing principal to understand threat nature and development mitigation solutions. For example, ICANN, mentioned above, was extremely effective at organizing a massive mitigation response to Conficker that significantly reduced its impact and damage thanks to its collaboration with the Conficker Working Group.

In addition to collaboration the United States government has stepped up its focus and is providing leadership on cyber security, thanks to President Obama's efforts. Following a formal "60-Day Review" of cyber security in the US, President Obama announced that he will appoint a "cyber security coordinator" to oversee "a new comprehensive approach to securing America's digital infrastructure." The Obama administration is expected to keep the spotlight on making improvements and embracing innovative thinking in both U.S. cyber security and technology policy.

IT security operations organizations have seen a shift over the years from exploits attacking specific IT vulnerabilities to the use of social media, scams, blended attacks through spam/web, etc., motivated by wreaking havoc or thrill seeking which has now nearly fully transitioned toward a financial gain motive. Because of this trend, security operations may have been lulled into becoming less diligent about patching and closing IT vulnerabilities, thinking that these older forms of attacks are on the decline. But remember, Conficker used an old technique of writing code that exploits a vulnerability infecting millions of computers/companies/individuals, but they did this with the motive not to just wreak havoc, but to gain financially and steal data.

The key insight here is that security operations are well advised to continue conducting vulnerability assessments across the entire IT infrastructure as a best security practice. The grim fact is that the new trends used by cybercriminals are the exploitation of both old and new techniques to gain their financial goal. This means that security operations are well advised to stay on top of traditional security methods as 'you never know' what attackers are going to use next. In addition to the above, we offer a set of recommendations in the Cisco 2009 Mid-year Security Report available [here](#).