Actionable Threat Intelligence

2009 Cyber Threats and Trends

Dec. 12, 2008

An iDefense Topical Research Report
The iDefense® Security Intelligence Team

Contents

1 Executive Summary

The malicious actors targeting the modern enterprise are no longer just "script kiddies." Today's cyber criminals have formed groups, which iDefense refers to as "cartels" for their similarity in structure and operational plan to the American drug cartels of the 1980s. These "cyber cartels" have focused their combined efforts on building their own infrastructure and on attacking Internet infrastructure for profit. From using Fast-flux networks to defeat phishing takedown services, to hiding behind bulletproof hosting services, to establishing entire underground markets to sell iFrame attacks, the bad guys have even fooled home users into purchasing malicious Trojan programs that claim to provide security protection.

Conversely, and adding to the richness of the landscape, was the moderate success that law enforcement had last year. This, notably, includes the FBI's Operation Dark Market where law enforcement officials from various countries launched an elaborate sting and cooperated to arrest several key carders. This bust has proven double-edged, however; while authorities have brought multiple successful cases against noted users of the illicit forum, but the activity has spooked, dispersed and driven most other suspects further underground.

Technical code-based threats continue to grow in sophistication, this year mainly concerning efficiency and stealth. In 2008, hackers targeted home user routers, improved Master Boot Record (MBR) rootkits and defeated virtual machine (VM) security and Two-Factor Authentication (2FA) schemes. This year, for the first time, attackers created working exploits for the Supervisory Control and Data Acquisition (SCADA) systems that run the systems that power critical infrastructure like local waste-management systems and nuclear power plants.

How are such bold criminals able to survive in today's risk-conscious global environment? Much of it has to do with where they are. Cyber security cartels are accepted, if illegitimate businesses in Russia. Muslim extremists have altered their ideologies to justify the use cyber fraud as a way to fund their agendas. Chinese amateur hacker groups practice Cyber espionage practically in the open, and in State-funded competitions. Russian sympathizers have launched two successful hybrid hacktivist cyber warfare campaigns against Estonia and Georgia.

In the seminal 2006 edition of this report, iDefense described the environment as a metaphorical iceberg, with much danger still below the surface of what the security community knew about existing threats. In 2007, analysts noted that enterprise cyber security had changed fundamentally, and was headed toward a peak, or "tipping point." iDefense believed that actors and threats had reached a stage that left the old paradigms either no longer effective, or altogether unmanageable. The cyber security landscape has indeed reached a tipping point, as iDefense will describe in the following pages.

2 Introduction

> *"Little changes can have big effects; when small numbers of people start behaving differently, that behavior can ripple outward until a critical mass or 'tipping point' is reached, changing the world."*
>
> -Mallcom Gladwell, "The Tipping Point: How Little Things Can Make a Big Difference"

One of the most distinct characteristics of the Internet is how quickly and fluidly it evolves, how technology originally designed for research and collaboration today powers millions of lives, both real and virtual. As the Internet has evolved, so have threats to its legitimate users. 2008 was no different, and as described last year's report, we have reached a tipping point, where any modern Internet user, from a child at home to the network engineers of multinational corporations, must rethink what they consider important when securing their assets.

Exhibit 2-1 is a timeline of some of the well-known global cyber security events since the Internet's inception. It all began with the Morris Worm in 1988. Robert Tappan Morris was a college student at the time and decided to try to build a piece of software that, he said, mapped the Internet.[1] That experiment got away from him and soon crippled college and military networks for nearly three days. On the day his experiment went awry, Morris invented malicious code. It so concerned the fledgling security community at the time that it formed the US CERT to combat this new kind of threat.[2]

When the Slammer Worm hit in January 2003 (see Exhibit 2-2) it reportedly "infected more than 90 percent of vulnerable hosts within 10 minutes."[3] Before Slammer, security professionals thought they had time to react to a worm attack. Slammer, in some ways causing a tipping point of its own, changed those perceptions forever.

Cyber warfare is no longer something that might happen in the future. In 2007, Russian sympathizers launched a distributed denial of service (DDoS) attack against the country of Estonia.[4] In 2008, a similar group of Russian sympathizers launched a DDoS attack against the country of Georgia, to coincide with military ground operations in a disputed area.[5] In both cases, the

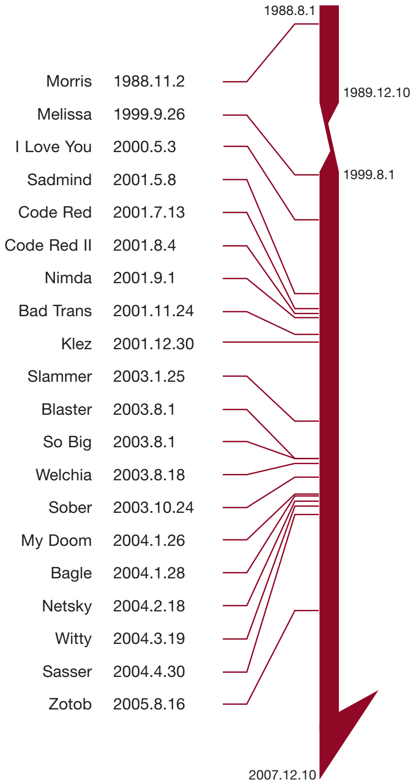


Exhibit 2-1: Global Security Threat Timeline: 1988-2005

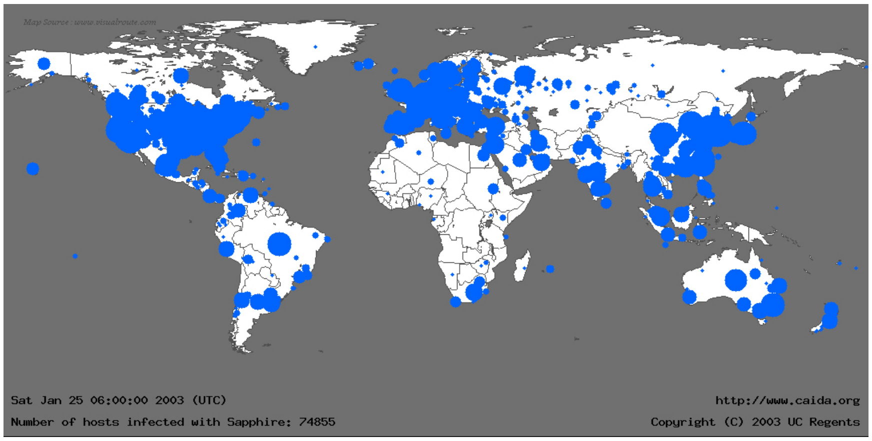

Sat Jan 25 06:00:00 2003 (UTC)
Number of hosts infected with Sapphire: 74855
http://www.caida.org
Copyright (C) 2003 UC Regents

Exhibit 2-2: First 10 Minutes of Slammer's Spread

[1] Robert T. Morris Jr, rotten dot com, http://www.rotten.com/library/bio/hackers/robert-morris

[2] Morris Worm, NationMaster.com, http://www.nationmaster.com/encyclopedia/Morris-worm

[3] "The Spread of the Sapphire/Slammer Worm", Moore, Paxson, Shannon, Staniford, Weaver, http://www.caida.org/publications/papers/2003/sapphire/sapphire.html

[4] Weekly Threat Report for Oct. 13, 2008

[5] Weekly Threat Report for Sept. 1, 2008

events could be characterized as more of a "cyber riot" than a cyber war, but the success of these attacks illustrated that it is possible to launch cyber attacks as an instrument of war to serve a political purpose. Russian hackers, individually and grouped into cartels, are good at attacking an opposing government's infrastructure in campaigns of annoyance and frustration. With these developments, cyber warfare has gone from purely theoretical to technically practical.

Cyber espionage is in the open. PricewaterhouseCoopers says that, "Corporate espionage costs the world's 1,000 largest companies in excess of $45 billion every year."[6] In July 2007, "Germany's SAP … admitted to 'inappropriate downloads' from arch-rival, Oracle in the US."[7] In September 2008, "A former Intel designer who joined arch-rival AMD [was] accused of stealing Intel trade secrets."[8] The situation is no less dire in government circles. It is almost a matter of public knowledge that the Chinese routinely compromise Western networks. The US government is so affected that it will spend billions of dollars over the next few years to shore up security concerns. They are calling this classified operation "Byzantine Foothold," and US government leadership refers to the program as a cyber security "Manhattan Project."[9] [10] Many Chinese amateur hackers belong to State militias that align themselves with prominent universities. Members consist of students and educators, and perform various missions across the Computer Network Operations (CNO) doctrinal spectrum, such as Computer Network Defense, Computer Network Exploitation (CNE) and Computer Network Attack (CNA).

Cyber terrorism is also evolving. Most experts believe that there will be a cyber terrorist attack in the future, but it will most likely be on the front end or back end of a physical attack.[11] This is not a new idea, but one recent development in the Middle East hacker community is indicative that all facets of the security issue are changing. Several religious leaders have issued fatwas, or official Islamic statements that authorize the use of cyber fraud operations in support of Islam,[12] and Islamic cyber cartels have already conducted cyber fraud operations against Western banks to fund their own agendas.

[6] "Corporate espionage: Not if, but when",by Sally Whittle, ZDNET, 18 March 2008, http://www.zdnetasia.com/insight/security/0,39044829,62039063,00.htm

[7] "SAP admits to corporate espionage against Oracle", by Thomas Ricker, 3 Jul 2007, http://www.engadget.com/2007/07/03/sap-admits-to-corporate-espionage-against-oracle/

[8] "The FBI has brought charges against an AMD engineer who used to work for Intel.", ITPro, by Miya Knights, 15 Sep 2008, http://www.itpro.co.uk/606174/updated-amd-engineer-charged-with-intel-espionage

[9] "The New E-spionage Threat", Business Week, Grow, Epstein and Tschang, 10 Apr 2008, http://www.businessweek.com/print/magazine/content/08_16/b4080032218430.htm

[10] The Manhattan Project was the massive US program to develop the first nuclear weapon (atomic bomb) during World War II. It involved thousands pf people focused on one thing: building the atomic bomb.

[11] Black Ice: The Invisible Threat of Cyber-Terrorism by Dan Verton (hardcover – Aug. 19, 2003)

[12] iDefense WTR, 8 Sep 2008

When talking about 2008 and trying to predict what will happen in 2009, three themes begin to emerge:

- **Tipping point:** The cyber security landscape has fundamentally changed, as best described in Malcolm Gladwell's 2002 book. Professionalized cyber criminals have emerged, Muslim extremists use cyber fraud as a way to fund their agendas, amateur hacker groups practice cyber espionage in the open in China and cyber war has become a legitimate tool to accomplish political goals, as in Estonia and Georgia.

- **A focus on infrastructure:** Malicious hackers seem to be applying increased scrutiny to their victims' critical infrastructure (like the DNS and TCP flaws), while building their own infrastructure to increase efficiency and survivability (like fast-flux and bulletproof hosting).

- **Cyber cartels:** iDefense likens the modern cyber criminal organization to the American drug cartels of the 1980s. Their membership is young, aggressive, light on bureaucracy and making money hand over fist.

3 Scorecard from 2008

Following is a scorecard reflecting the accuracy of the predictions in last year's 2007 Cyber Threats and Trends report.[13] iDefense regards predictions as correct or incorrect when available data, either garnered from open sources or from internal iDefense operations, conclusively supports or refutes analyst expectations. When relevant data is lacking, iDefense derives conclusions by consensus between a number of subject matter experts. In the event that data suggests competing conclusions or when analyst observations fail to provide overwhelming evidence, iDefense classifies the accuracy of the prediction as inconclusive.

Prediction	Status
Continued maturation of cyber criminals including bulletproof hosting and other formal infrastructure supporting criminal activity	✓
Increase in malicious code attacks in proportion to social engineering (e.g., phishing)	✓
Politically motivated distributed denial of service attacks	✓
Growth of the Chinese underground with a shift toward financial motivation	✓
Increased aggressiveness from Muslim hackers	✓
Deepening ties between secular Arab hackers and their pro-terrorist counterparts	✓
Malicious activity to accompany any major geopolitical event	✓
Shift toward transaction hijacking (in response to TFA adoption)	✓
Continued targeting of social networking platforms	✓
Continued use of IM for distribution of malicious URLs and files	✓
Increased adoption of fast-flux by organized phishing groups	✓
Increased stealth of attacks	✓
Continued increase in multi-stage attacks	✓
Increased government involvement in Industrial Control System security	✓
Decline of IRC-based command and control (C&C) servers in favor of peer-to-peer (P2P) and Web communications	✓
Emergence of an aftermarket for tools and toolkits for novice criminals	?
Increase in insider incidents, due primarily to increased disclosure	?
Little or no observable state-sponsored hacking from China	?
Large amounts of spam will continue to use common file extensions (i.e., .pdf, .doc, .zip, etc.)	?
Attacks against mobile banking offerings	?
Increase in the number of known vulnerabilities	X
Aggregation of stolen phishing information (i.e., names/addresses) to create targeted attacks	X
Focus on Vista exploitation in the latter half of the year	X
Hacktivists to employ targeted malicious code and spear-phishing attacks against key officials/executives	X
Leveling of DNS vulnerabilities and abuse	X
Introduction of more "month of" initiatives	X
Increase in public reports of bots attacking from within Fortune 500 networks	X

[13] iDefense, *2007 Cyber Threats and Trends*, Dec, 2007

4 Significant Developments in 2008

4.1 Vulnerability Trends

The press hyped a number of partial vulnerability disclosures this year, many of which targeted Internet critical infrastructure. Among the more prominent were Sebastian Muniz's malicious rootkit software for Cisco routers,[14] Robert E. Lee and Jack C. Louis's TCP/IP flaw,[15] Kris Kaspersky's Intel microprocessor flaw[16] and Dan Kaminsky's DNS flaw.[17]

Most noteworthy in this space was Dan Kaminsky's DNS vulnerability, which was significant both for the issue itself and for the international media attention the event garnered, eventually culminating in an article in *Wired*.[18] This new trend highlights the need for security researchers to garner greater media attention for their efforts. Most researchers purposely do not provide full details about their discovery to avoid aiding malicious actors in exploiting it. Their efforts ultimately fail, though, because as soon as one of them publishes anything of note, every other researcher in the community begins a relentless pursuit to determine the missing parts. The original authors claim they are withholding information for the good of the community, but their vague announcements only inspire a rush of activity to uncover the rest. Expect to see more of this activity in 2009.

Software companies have started to follow Microsoft's lead about setting prescribed times to release patches for their products. Cisco Systems Inc. decided to schedule a bi-annual security advisory release on the fourth Wednesday of March and September for its IOS software in response to customers who requested further predictability for the timing of patch releases.[19] Apple Inc. and the Mozilla Foundation are also notorious for compiling fixes for a large number of vulnerabilities in each patch release. There is a chance that these vendors will follow a similar scheduled patch release format in 2009 if given enough feedback from their customer base.

4.2 International Law Enforcement Successes

Law enforcement and private sector researchers collaborated in 2008 to make some high-profile arrests. One of the more public came from the cooperation between Dutch law enforcement and Kaspersky Labs. In August 2008, Dutch law enforcement arrested two individuals in connection with the operation and maintenance of the so-called Shadow Botnet.[20] Lesser-known successes concerned the indictments of Nordin Nasiri of the Sneek hacker group in the Netherlands and Leni de Abreu Neto of Taubate de Brazil for operating a

[14] EuSecWest conference in London, http://www.networkworld.com/news/2008/051408-hacker-writes-rootkit-for-ciscos.html

[15] T2 Conference in Finland, http://blog.robertlee.name/

[16] Hack In The Box (HITB) conference in Malaysia, http://www.infoworld.com/article/08/07/14/Researcher_to_demonstrate_attack_code_for_Intel_chips_1.html

[17] Black Hat in Las Vegas, http://www.doxpara.com/?paged=3

[18] Wired Magazine, December 2008, by Joshua Davis, "Collapse", pgs 200 - 224

[19] "Cisco amends its patch schedule; Next batch March 26", ZDNET, Larry Dignan, http://blogs.zdnet.com/security/?p=939 http://lists.virus.org/cisco-0803/msg00000.html &nbsp

[20] "Dutch police smash Shadow botnet", Iain Thompson, 14 Aug 2008, http://www.vnunet.com/vnunet/news/2223909/dutch-police-smash-shadow-botnet

botnet composed of more than 100,000 infected computers designed to send spam messages.[21] The US FBI concluded a two-year sting operation called Operation Dark Market that resulted in the arrest of Çağatay Evyapan ("Cha0") from Turkey.[22] With these successes, expect to see more collaboration between law enforcement and private researchers in 2009. One down side to this success is the development in the carding community of private members-only forums. It is much more difficult now for researchers and law enforcement personnel to penetrate such forums in search of malicious actors and their cyber cartels. Expect to see paranoia drive more forums to adopt this model in 2009.

4.3 Cyber Warfare as a Reality

A loosely formed, pro-Russian cyber cartel, consisting of hackers from around the world, targeted online Georgian government assets prior to and during the Russian government's military ground operations against the country of Georgia. During the physical warfare, pro-Georgian and pro-Russian sympathizers also engaged in a rudimentary form of information warfare in which both sides attacked the press outlets of the other and targeted Western users with spam pleading their side. This is the second global example of the actual use of cyber warfare in two years; the attacks against Estonia in 2007 were the first. One thing is certain, if a government or private institution gets into a public political fight with Russia in 2009, that institution will most likely have to defend against a cyber warfare campaign conducted by pro-Russian cyber cartels.

4.4 Egyptian Fatwa Permits Politically Motivated Hacking

Egypt's respected Islamic Al-Azhar University fatwa committee is reported in several online news venues to have issued a fatwa (or decree made by Islamic scholars) that authorized hacking for the sake of defending Islam against various Internet-based defamations. The fatwa also authorized cyber fraud operations as a legitimate fundraising activity to support the Islamic agenda. The influence of fatwas issued by various religious authorities in the Middle Eastern hacker community is well documented. Many forums contain text conversations with hackers using religious justifications for their activities. In 2009, secular and religious Middle East hackers with diverse motivations and orientations will increasingly use these fatwas to justify and bolster their hacking activities with little regard to how far removed these may actually be from the focus of the fatwa. This religious justification of hacker activity is the perfect example of why the cyber security landscape has reached a tipping point. Just five years ago, religious leaders did not endorse hacking activity to support their cause.

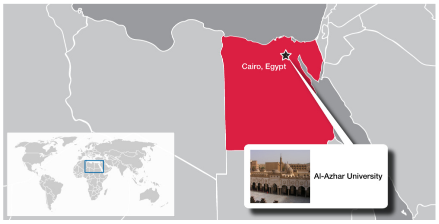


Exhibit 4-1: Al-Azhar University, Cairo, Egypt

[21] "Brazilian charged in U.S. in connection with operating botnet", Elinor Mills, 21 Aug 2008, http://news.cnet.com/8301-1009_3-10022990-83.html?part=rss&amp;subj=news&amp;tag=2547-1_3-0-20

[22] "Turkish Police Arrest Alleged ATM Hacker-Kidnapper ", Ryan Singel, 12 Sep 2008, http://blog.wired.com/27bstroke6/2008/09/turkish-police.html

4.5 Challenges in Cyber Security Policy

Although technically responsible, coordinating defense against and responses to cyber attacks across the nation, the US Department of Homeland Security's (DHS) role in protecting the nation's cyber defenses has been described as poor at best. Public and private groups, including the Center for Strategic and International Studies (CSIS) and the US General Accountability Office (GAO) have repeatedly highlighted failures in the program and criticized the US CERT's recent missteps. CSIS publicly voiced concerns surrounding the role of DHS when it told Congress that the department has been ineffective in coordinating government cyber security efforts and should be stripped of its authority in the area. CSIS also recommended that the authority for coordinating cyber security efforts and enforcing mandates move to the White House. The current US cyber security organization is a layered group of government agencies full of infighting and disorganized priorities. Without strong leadership from the next president, this is unlikely to improve in 2009, despite any improvements in cyber security policy. CSIS organized the Commission on Cyber Security for the 44th Presidency, which consisted of key cyber security leadership from around the US. The commission hopes to make recommendations for a comprehensive strategy to improve cyber security in federal systems and in critical infrastructure to President-Elect Barack Obama.[23] With all the problems facing President-Elect Obama in his first term, it seems unlikely that he will be able to focus on the US cyber security landscape. In an apparent move to strengthen its coverage on these matters, DHS appointed Mischel Kwon as the new director of US-CERT this summer.[24] By all accounts, iDefense feels Kwon is a strong leader and well qualified for the post, though she has a tough job in front of her. As such, iDefense expects little progress in 2009.

[23] http://www.csis.org/tech/cyber/

[24] http://www.csoonline.com/article/400563/DOJ_Staffer_Tapped_to_Head_US_CERT

5 Underground Evolution

5.1 Introduction

Tactics and techniques of the criminal underground continue to evolve in 2008, partially in response to a changing law enforcement landscape, but also because of a natural adjustment due to developments in the underground itself. Serious organized crime groups are now conducting business largely unfettered and the result is a polarizing of the underground.

5.2 Targeted Attacks against Commercial Accounts (BBB Attacks)

Three Romanian cyber cartels, working either together or apart, have been targeting the US financial infrastructure since early 2007. All three cartels used similar phishing schemes to target high-end executives at selected financial organizations. The cartels discovered that there is a difference between the retail and commercial accounts offered by banks. The average customer uses a retail account for typical banking services: savings, checking, etc.; these accounts have traditionally been the phisher's target of choice. The commercial accounts, in contrast, are the accounts that financial organizations use to transfer large sums of money for various purposes. The BBB cartels sought to steal the credentials from these kinds of commercial accounts, targeting selected individuals in corporations with crafted social engineering techniques and often circumventing two-factor authenticating schemes.

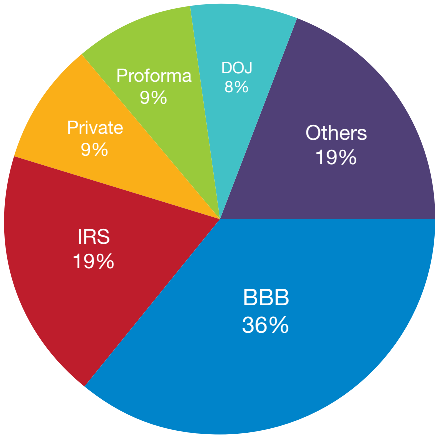


Exhibit 5-1: Spear-Phishing Attack Templates in 2008 by Subject

The moniker "BBB" comes from the first attacks that iDefense discovered. The cyber cartels used a well-designed phishing e-mail message as bait that appeared to come from official channels in the US Better Business Bureau, or BBB. Since then, the cartels have used phishing messages that appear to originate from well-known institutions around the world (see Exhibit 5-1). The majority of the more than 70 attacks since 2007 seem to originate from two cartels, which iDefense analysts close to the issue have dubbed "Group A" and "Group B" (see Exhibit 5-2). The Group A cartel targeted more than 30 commercial banks, but stopped its operation on April 24, 2008. Group B targeted more than 50 commercial banks, but stopped mid-attack in July because the FBI arrested 30 of its members. Group A attacks surprisingly returned in September 2008. Although the past and current BBB cartels have traditionally focused on US institutions, future variations are likely to target other geographic regions. iDefense expects to see more cyber cartels globally and more schemes focusing on commercial accounts in 2009.

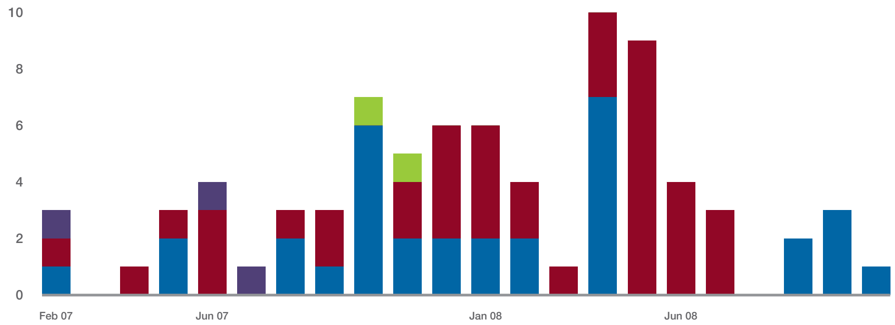


Exhibit 5-2: Monthly Volume of BBB Attacks from February 2007 to November 2008

(Group A, Group B, Group C, Unknown)

5.3 Infrastructure Services for the Underground

Legitimate businesses often outsource infrastructure services to third parties, including building and network management organizations, Internet service providers, etc. Outsourcing allows legitimate businesses to focus on their core business processes and not waste resources on secondary tasks that serve as the core of these other companies. Cyber cartels seek the same services for the exact same legitimate reasons, and even a few illegitimate reasons. They also seek to build their own specialized infrastructure, including Fast-flux networks for phishing and iFrame distribution schemes that help to improve efficiency and aid in evading detection.

5.3.1 Bulletproof Hosting

Bulletproof Internet service providers are legitimate hosting businesses that sell their service primarily to illegitimate organizations. The owners and managers of these organizations purposefully avoid responding to abuse complaints and usually deliberately locate their businesses in countries that have limited to no law enforcement cooperation with the West, where most of their victims reside. This arrangement provides their customers, mostly malicious actors of various sorts, with a safe haven that allows them to evade prosecution. The rise and fall of the Russian Business Network (RBN) was a famous example of this type of organization. The post-RBN era saw the rise of many competing bulletproof hosting providers. The press, in particular Brian Krebs of *The Washington Post*,[25] has been successful at working to take some of these organizations offline. US Intercage (aka Atrivo) became a symbol of malicious networks in 2008 as part of the HostFresh network operating out of Hong Kong. The media published overwhelming evidence collected by many security research sources proving that the network's primary purpose was to host malicious content. In the days and weeks that followed, the network's upstream providers stopped routing Intercage traffic, effectively removing it from the Internet. A similar occurrence happened to the McColo networks based in California. Shining the media spotlight on bulletproof ISPs has proven effective three times in 2008, and that success will likely serve as a model for further efforts in 2009.

Cyber Crime: Rogue ISP Intercage Fights to Stay Online, Mostly Unsuccessful, ID# 473192, Sept. 29, 2008

Provider Name	Origin
AbdAllah	Turkey
STARLINE_EE	Estonia
UATELECOM	Ukraine
UrkTeleGroup	Ukraine
Colocall Ltd.	Ukraine
HopOne	USA
Net Access Corporation	USA
TIMETELEKOM	Malaysia
TELEKOM MALAYSIA BERHAD	Malaysia
TMNET-BORNEO	Malaysia
PIRADIUS NET	Malaysia
Applied Information Management	Malaysia
Starhub Internet	Sinagpore
Madet Ltd.	Russia
Hostfresh	Hong Kong

5.3.2 Fast-Flux Networks

The most effective way to maintain dispersed and untainted IP space is to use dynamically changing and unrelated computing resources. Hackers do this by using a network of compromised computers (called "drones,""bots" or sometimes "zombies") and manipulating the DNS infrastructure to associate a domain name with an ever-changing subset of zombie computers. The zombies follow instructions from a centralized server, which iDefense calls the "mother ship." Content hosted in this fashion has increased persistence, since hackers separate the origin from the victims visiting the domain name through one layer of indirection (single fast-flux or "single-flux"). Attackers can introduce another layer of indirection by manipulating additional DNS mechanisms, resulting in what is known as double-fast-flux or double-flux networks. While "traditional" bulletproof hosting was built upon social aspects (negligent abuse handling or non-existent law enforcement cooperation), the

New Wave of OrderGun Trojans Targets Banks, ID# 472238, Sept. 8, 2008

New Rock Phish-Style Attacks Targeting Commercial Accounts with Malicious Code, ID# 468962, April 24, 2008

[25] http://voices.washingtonpost.com/securityfix/2008/08/report_slams_us_host_as_major.html

next generation of bulletproof hosting relies solely on technology: fast-flux. Criminal organizations maintain enormous botnets for just this purpose and offer fast-flux-based hosting as a service to other criminals. In 2008, attackers used fast-flux network services like ASProx (aka HydraFlux), OlateSuite and the so-called "Storm" worm to send spam, host phishing pages, infect websites with malicious redirection instructions (IFrames) and host exploitation toolkits, which infect additional victims to recruit them into their botnets and sustain service availability. Fast-flux is superior to traditional bulletproof hosting because it depends merely on technology and is infinitely scalable. iDefense expects to see attackers increase their use of fast-flux infrastructure in 2009.

5.3.3 Malicious Software Distribution with IFrames

Since the wide adoption of client firewalls enabled by default with Microsoft Windows XP's service pack 2, self-spreading malicious code (worms) ceased to be effective as a means of propagation. "Drive-by" installations largely replaced worms as a mechanism to distribute malicious content. Attackers modify websites visited by victims accidentally (via typo squatting or DNS manipulation) or purposefully (via spam lure or compromised legitimate site) to covertly redirect the visitor to a website that installs malicious code onto the victim's computer. Hackers achieve this redirection by injecting an invisible inline frame (IFrame) HTML tag into the page that points to the desired malicious page containing an exploitation toolkit. Hackers have formed an entire economy around the distribution of malicious code through IFrames, allowing attackers to specialize in infecting websites and infecting victims with exploit toolkits. The primary means to install an IFrame is with SQL injection. Early in 2007, hackers started using SQL-injection attacks in bulk, infecting tens or hundreds of thousands of sites at a time. iDefense has attributed most of the activity to two attacks: the ASProx botnet and the "Chinese" attacks designed to install gaming Trojans. The goal in both types of attacks is not to steal information, but to infect database-driven websites with malicious IFrames that will redirect visitors to infect them with other malicious code. In 2009, criminals will continue to launch attacks against vulnerable sites, but will improve their methods by targeting more frequently used Web applications that, often times, utilize alternative database back-ends, such as MySQL and PostgreSQL. Secure coding practices are the only defense against SQL injection and every site with a database back-end is a potential target. IFrames were so successful in 2008 that iDefense feels it is unlikely that another distribution method will usurp its position in 2009. iDefense also expects that the exploit toolkits that IFrames deliver will continue to evolve to include the latest vulnerabilities.

5.4 Rogue Security Applications

Cyber cartels have recently incorporated more rogue security applications into their arsenal. These free applications, once installed, falsely report security issues to mislead the victim into purchasing a purported "full" version.[26] [27] The application often times comes bundled with various dangerous malicious codes, usually banking or other information-stealing Trojans. The business

Widespread SQL Injection Attacks Continue to Evolve, Now Exploiting MS08-053, ID# 471117, Sept. 25, 2008

Increase in SQL Injection Attempts to Inject JavaScript and IFrames to Deliver Asprox Trojan, ID# 470239, June 26, 2008

SQL Injection Attacks Continue to Compromise Thousands of Sites, ID# 469014, May 9, 2008

Malicious JavaScript IFrame Attacks Trusted Websites, ID# 467911, March 13, 2008

State of the Hack: An In-Depth Look at a SQL-Injection Attack, ID# 473307, Oct. 6, 2008

Bi-Weekly Malicious Code Review for Feb. 7, 2007, "Super Bowl and CDC Website Compromise: A mass defacement points to a Chinese connection," ID# 457121, Feb. 7, 2007

All iDefense Sources that reference your subject:

Threat Fake CNN Spam Distributes Fake AntiVirus XP 2008 Program, ID# 471186, Aug. 13, 2008

Weekly Threat Report Weekly Threat Report for Aug. 25, 2008, "State of the Hack: Ways of Paying for Fake Security Programs," ID# 471961, Aug. 25, 2008

Rapid Responses:

Antispy Spider Spyware, April 24, 2008

IEAntivirus / FakeAlert DLL, June 18, 2008.

Mass Mailing Malicious E-Cards, Aug. 12, 2008

Sality Autorun Virus, Sept. 23, 2008

According to LUNG analysis, one or two days after installation, the code installs Antivirus XP 2008. This is not documented in our initial report.

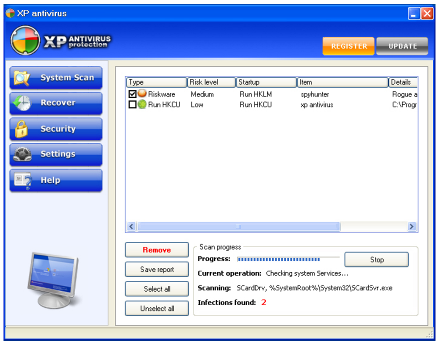
MSx Fake Anti-Virus, Oct. 3, 2008

Analysis of Zeus Trojan HTML Injection Configuration File, Oct. 10, 2008

[26] Dancho Danchez -A Diverse Portfolio of Fake Security Software - Part Eight

[27] Microsoft Lawsuits against Reg Cleaner, http://en.wikipedia.org/wiki/Registry_cleaner

model around rogue security applications encourages third parties to distribute the code and participate in the revenue stream. The huge success of this model of separation between deployment and exploitation, similar to the business models around fast-flux and pay-per-install, will guarantee increased activity and new actors in the near future. “Antivirus XP” and numerous other rogue security applications are some of the most prevalent pieces of malicious code in recent months (see Exhibit 5-3). This type of malicious code emerged in 2004, but iDefense observed a huge spike of activity concerning this vector in 2008. Expect to see continued growth in volume and innovation in the illegal distribution of rogue security applications. The number of methods used to distribute the software will continue to expand, and the number of techniques used to scare users into buying the software will also increase, possibly including regional variations in different languages.



Type	Risk level	Startup	Item	Details
☑ Riskware	Medium	Run HKLM	spyhunter	Rogue a
□ Run HKCU	Low	Run HKCU	xp antivirus	C:\Progr

Scan progress

Progress:

Current operation: Checking system Services...

Scanning: SCardDrv, %SystemRoot%\System32\SCardSvr.exe

Infections found: 2

Exhibit 5-3: Screenshot of Antivirus XP

5.5 Evolution of Trojan Toolkits

Advances in Trojan horse technology contribute to the iDefense theory that the cyber security landscape has blown past its tipping point. Home router DNS attacks, Master Boot Record attacks, virtual machine attacks and two-factor authentication attacks are all significant advances on how hackers load malicious code onto the victim’s system.

Zlob, the router DNS changer, showed how it is possible for hackers to compromise an entire network by gaining non-administrative access privileges to one internal system.[28] Attackers distributed a Zlob variant that changed the DNS settings on popular consumer routers. The Trojan used a brute-force approach and a set of default and common router passwords to break into the routers. This attack does not require administrative access on the infected system to perform the DNS change. The new DNS settings pointed to attacker-controlled servers, which they could then use to redirect all traffic of the victim to any site. This “pharming” attack takes place instantly upon infection and is effective against all the computers in the victim’s local network that receive their DNS setting from the router upon startup.

The Torpig MBR rootkit showed how it is possible to turn publicly available proof-of-concept (POC) code into an effective rootkit that operates below anti-virus and the Windows operating system. The security firm eEye originally published the POC in 2005 and presented further research on the subject at Blackhat in 2007.[29] In just three months after the Black Hat 2008 presentation, attackers developed and tested a working version of the MBR rootkit that was, at the time, undetectable. Two months later, hackers launched new attacks with improved code and infected about 5,000 victims in two attack waves lasting just days. Shortly thereafter, the MBR rootkit became an inherent part in the Torpig banking Trojan.[30] In 2009, iDefense expects to see more malicious codes designed with an MBR rootkit component.

Malicious Code Summary Report for June 25, 2008, “Out of the Lab: Zlob Variant Changes Router DNS Settings,” ID# 470255, June 25, 2008

Stealthy Master Boot Record (MBR) Rootkit Active in the Wild, ID# 466880, Jan. 10, 2008

Multiple Users Distributing MBR Rootkit Version of Torpig Banking Trojan, ID# 467687, March 1, 2008

Bi-Weekly Malicious Code Summary Review for Oct. 17, 2007, “Out of the Lab: Many Torpig Trojans Report to a Single C&C Server,” ID# 464836, Oct. 17, 2007

iDefense Malicious Code Summary Report for Jan. 9, 2008, “Out of the Lab: The Torpig Group, Part 1: Exploit Server and Master Boot Record Rootkit,” ID# 466980, Jan. 9, 2008

iDefense Malicious Code Summary Report for March 12, 2008, “Out of the Lab: The Torpig Group, Part Two: Banking Trojan Fully Integrates MBR Rootkit,” ID# 467900, March 12, 2008

[28] Trend Micro: New ZLOB Rigs Routers, http://blog.trendmicro.com/new-zlob-rigs-routers/

[29] eEye: BootRoot, http://www.blackhat.com/presentations/bh-usa-05/bh-us-05-soeder.pdf, http://research.eeye.com/html/tools/RT20060801-7.html

[30] F-Secure: MBR Rootkit, A New Breed of Malware, http://www.f-secure.com/weblog/archives/00001393.html

Clampi[31] demonstrated how attackers could wrap information-stealing Trojans within a VM environment. Clampi, by itself, was a non-event. Little more than a standard banking Trojan, the interesting aspect of Clampi lay in its use of VM obfuscation techniques to evade forensic analysis.

Malicious Code Summary Report for Aug. 27, 2008, "Out of the Lab: The Clampi Backdoor Trojan," ID# 472002, Aug. 27, 2008

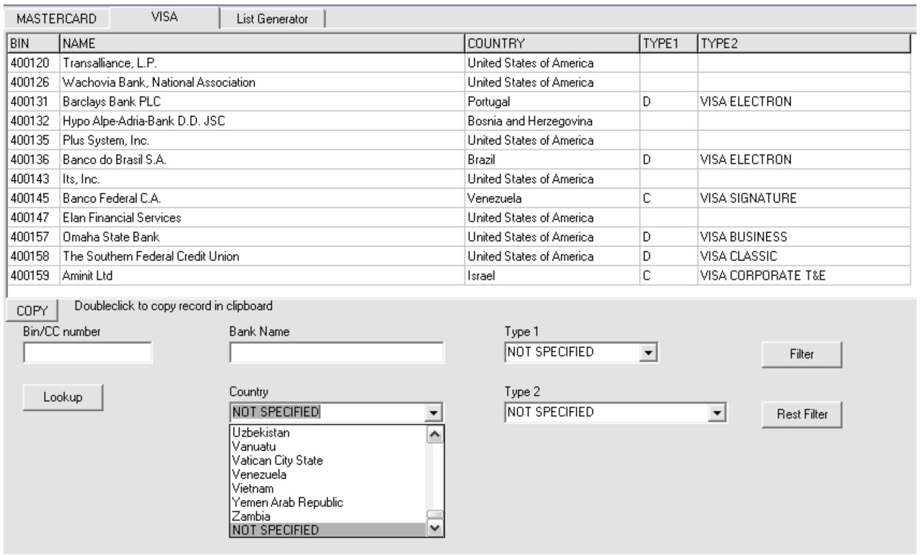
State of the Hack: Virtualizing Obfuscation, ID# 472455, Sept. 15, 2008

Clampi.A Backdoor Trojan Horse Allows Backdoor Access, ID# 467201, Jan. 17, 2008

A long-time member of the banking Trojan malicious code family, Zeus has undergone some very interesting developments in 2008. The attackers have developed JavaScript code that, once injected into the financial institution's Web application, circumvents 2FA by hijacking transactions already approved by the victim. This is one of many ways hackers have been successful with transaction hijacking. As the industry increasingly deploys 2FA solutions, iDefense expects transaction hijacking and 2FA circumvention functionality will appear in more malicious code in the coming year.

5.6 Carding Underground

The phrase "carding" describes an assortment of activities surrounding the theft and fraudulent use of credit and debit card account numbers, including computer hacking, phishing, cashing-out stolen account numbers, re-shipping schemes and Internet auction fraud. Individuals engaged in criminal carding activities are called "carders."[32] The carding infrastructure to sell goods and services is so well organized that buyers can seek a particular bank, card type, owner's date of birth, mother's maiden name, owner's PIN, e-mail or password and be reasonably assured to find what they are looking for. The vendors can give buyers updated information from very detailed databases. Carders sell goods by geographical regions.[33] Vendors try to make transactions as effortless as possible. Tools, such as this Bank Identification Number (BIN) Lookup Tool (see Exhibit 5-4), aid in the request and ordering of dumps.



BIN	NAME	COUNTRY	TYPE1	TYPE2
400120	Transalliance, L.P.	United States of America		
400126	Wachovia Bank, National Association	United States of America		
400131	Barclays Bank PLC	Portugal	D	VISA ELECTRON
400132	Hypo Alpe-Adria-Bank D.D. JSC	Bosnia and Herzegovina		
400135	Plus System, Inc.	United States of America		
400136	Banco do Brasil S.A.	Brazil	D	VISA ELECTRON
400143	Its, Inc.	United States of America		
400145	Banco Federal C.A.	Venezuela	C	VISA SIGNATURE
400147	Elan Financial Services	United States of America		
400157	Omaha State Bank	United States of America	D	VISA BUSINESS
400158	The Southern Federal Credit Union	United States of America	D	VISA CLASSIC
400159	Aminit Ltd	Israel	C	VISA CORPORATE T&E

COPY — Doubleclick to copy record in clipboard

Bin/CC number:

Bank Name:

Type 1: NOT SPECIFIED

Country: NOT SPECIFIED

Type 2: NOT SPECIFIED

Exhibit 5-4: Example of a BIN Lookup Tool Often Employed by Fraudsters

[31] Symantec Report (generic) on Clampi, http://securityresponse.symantec.com/en/uk/home_homeoffice/security_response/writeup.jsp?docid=2008-011616-5036-99

[32] DATA BREACHES: WHAT THE UNDERGROUND WORLD OF "CARDING" REVEALS, Kimberly Kiefer Peretti, U.S. Department of Justice, Computer Crime and Intellectual Property Section, http://www.usdoj.gov/criminal/cybercrime/DataBreachesArticle.pdf

[33] http://Fullz.iwannaforum.com

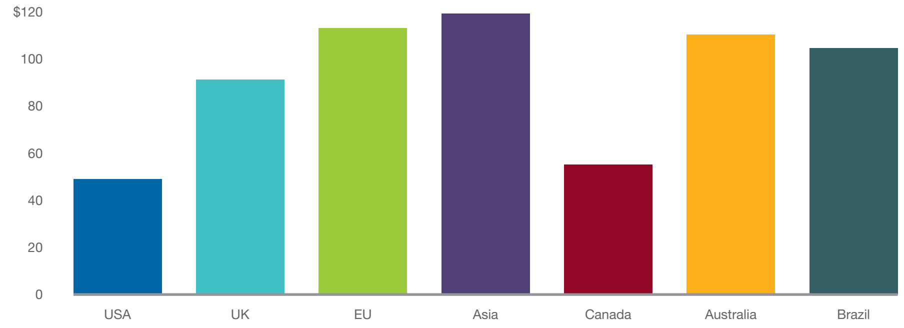


Exhibit 5-5: Average Going Rate of Select Credit Card Dumps in USD

Buyers prefer to concentrate on particular BINs to become more specialized in their fraudulent activity. The buyer may already have an insider working at the merchant or bank and have counterfeit "plastics" or templates that match the bank's products.

"Dumps" are a large segment of the typical goods sold by carding vendors. The associated chart focuses on the ISO standard[34] track 1 and 2 data usually duplicated at point-of-sale merchants such as hotels, restaurants, and other retailers (see Exhibit 5-5). These kinds of dumps are profitable because the initial investment is so small. Dumps from the US are often the cheapest because of the ease of obtaining them. Dumps from Europe and Asia are not as popular because the associate credit cards have an increased security set. Carders refer to these cards as 201s. 201s have a different format and they have a security chip embedded in the card. Most carders stay away from these. In 2009, iDefense believes that dumps will continue to be the most sought-after carding "merchandise."

[34] http://www.textfiles.com/anarchy/CARDING/cc101_2.txt

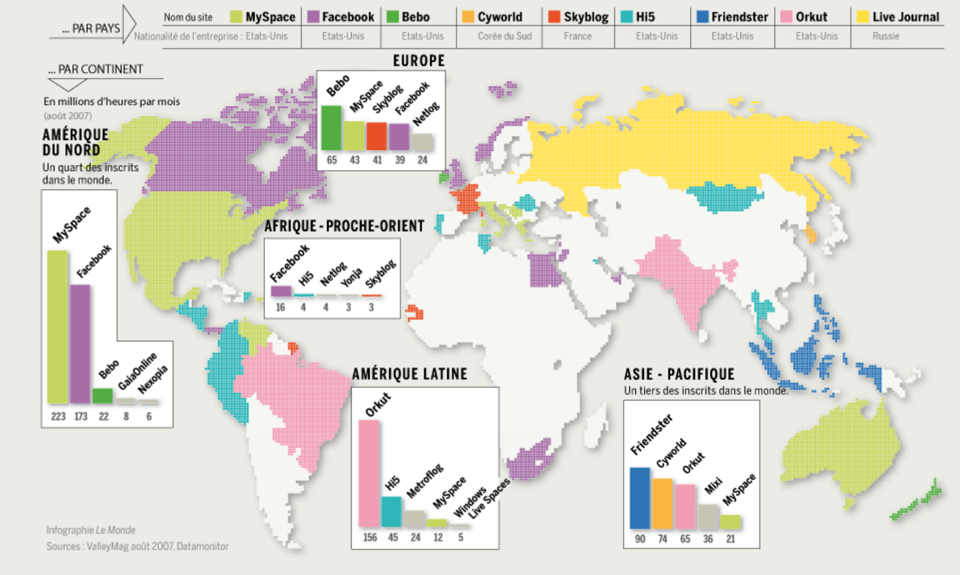


Exhibit 5-6: Preferred Social Networking Sites around the World

5.7 Social Networking

Social networking sites have proliferated in the last five years.[35] Exhibit 5-6[36] displays the sites that are the most popular from around the world. Every aspect of these social networks is under attack with the same techniques that hackers use on other sites: spam, rogue anti-spyware distribution, fake codecs and drive-by exploitation, to name a few. Cyber cartels have formed underground forums, similar to those seen for carding and malicious code distribution, for sharing tools and secrets to circumvent any protection mechanisms that these sites may have deployed. Hackers develop tools for specific networks, and are most often point-and-click operations. iDefense expects the use of social networking sites in cyber attacks to grow in 2009.

5.8 Attacks against Control Systems[37]

To monitor and maintain critical infrastructure, governments implement industrial control systems, commonly referred to as Supervisory Control and Data Acquisition (SCADA), PCS Process Control Systems (PCS) and Distributed Control Systems (DCS). Examples include manufacturing, electric utilities, chemical, pharmaceutical, oil and gas, water and wastewater. Until recently, the relative obscurity of these types of systems amounted to minimal scrutiny by the security research community.

In addition to starting in 2005, the first publicly announced control systems vulnerability was released to the public, spurring a great amount of debate regarding the disclosure of such information. Since then, interest in industrial control systems has climbed steadily, due in part to the introduction of control systems on to standard IT networks and the incorporation of common

[35] http://www.marketingcharts.com/interactive/social-networkings-explosive-growth-to-plateau-in-five-years-2102/

[36] http://www.lemonde.fr/web/infog/0,47-0@2-651865,54-999097@51-999297,0.html

[37] Research conducted by *iDefense partner: Critical Intelligence Inc. - Intellectual Armor for Critical Infrastructure*

IT technologies into control systems. The number of publicly disclosed vulnerabilities has risen since 2005 (see Exhibit 5-7). As of Nov. 15, seven SCADA vulnerabilities have been released to the public. In light of this fact, iDefense feels it is likely that more vulnerabilities will be made public soon, given recent postings on the SCADASEC mail list, and a university news article discussing pending control system vulnerabilities.[38] [39] In addition to notable SCADA vulnerabilities that appeared in the public eye, 2008 marked the release of the first publicly available Metasploit exploitation framework module designed to exploit the issues in these industrial control systems.[40] This exploit was released Sept. 8, 2008, and was quickly followed by five additional exploits, four of which have Metasploit modules. 2008 also saw the first reports of Web-based malicious software that targeted a control system vulnerability.[41] Going into 2009, the increased interest from security researchers, combined with the relative ease of identifying low-hanging fruit in the control systems space will continue, if not accelerate, the upward trend in control system vulnerabilities and exploits. Now that exploits have been placed in to the hands of up-and-coming script kiddies, 2009 brings increased potential for industrial control system compromises.

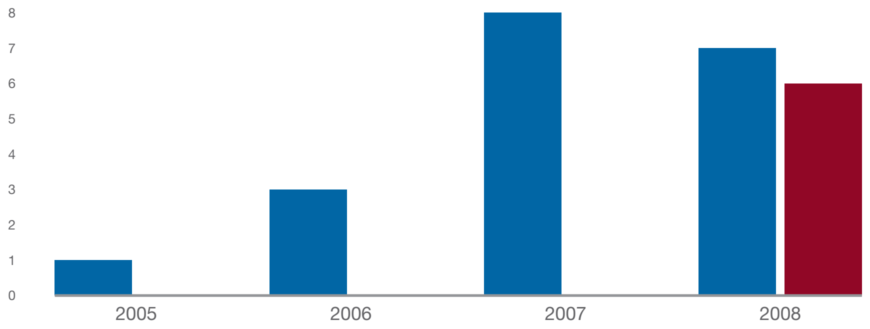


Exhibit 5-7: Disclosed Industrial Control System ***Vulnerabilities*** *and* ***Exploits*** *by Year*

[38] http://scadaperspective.com/pipermail/scada_scadaperspective.com/2008-September/001083.html

[39] http://www.msstate.edu/web/media/detail.php?id=4309

[40] http://snosoft.blogspot.com/2008/09/citectscada-exploit-release.html

[41] http://carnal0wnage.blogspot.com/2008/10/malware-targeting-industrial-control.html

6 Evolution of Regional and National Cyber Security Environments

6.1 Introduction

This section discusses the major trends forecasted for 2009, among six major information security environments: the Russian Federation, the People's Republic of China (PRC), the greater Middle East, Central Asia, Latin America (with a focus on Brazil) and the United Kingdom (UK). The analysis of each region covers developments in cyber crime, cyber warfare and espionage, politically motivated hacking (or hacktivism), official and private-sector responses and the general development of the cyber underground.

Although each region exhibits marked distinctiveness, several commonalities emerge among them:

- The cyber crime environments of each are becoming more dangerous and increasingly interconnected.

- Less-advanced cyber threat environments are catching up to the developed world more quickly than had been estimated hitherto, by most observers.

- International cooperation among law enforcement officials in most regional environments is stronger, though highly uneven, while the higher levels of some governments are more aware of and responsive to the threats than in years past.

- Governments have come to understand and prioritize the now-pervasive threat of cyber espionage and the possibility of cyber warfare. While the ultimate results of this awakening remain unclear, it is safe to say that government-backed—or at least government-allowed— hacking for strategic advantage will increase much more rapidly than in the past.

6.2 Russia

The Russian Federation is and will long remain the most conspicuous haven of the world's most advanced and dangerous cyber crime cartels. No clear lines demarcate the criminal underworld from the official business economy or the state apparatus, and cyber crime is now an inveterate and distinguishing feature of the country's general socio-economic landscape. Indeed, many legitimate Russian businesses now find DDoS attacks and network penetrations to be effective tactics against competitors. Of greatest consequence, however, is the fact that leaders in Moscow have come to regard the country's cyber underground as a political and strategic asset, one to be cultivated and wielded in the pursuit of national interests.

If anything currently characterizes the Russian political climate, it is a sense of justified self-assertion. The general population and the cyber underground already exhibit zeal in embracing a new nationalism acceptant of a more aggressive and strategically uncompromising Russia. This attitude intersects with the Kremlin's valuation of its civilian cyber attack capacity as a strategic asset to provide the motivation and the official encouragement for increasingly

RUSSIA
Estonia
Georgia

Exhibit 6-1: Unaffiliated Russian Hackers Launched Attacks against Estonia in 2007 and Georgia in 2008

hostile hacktivism. Moreover, this attack capacity strengthens apace as politically motivated hackers learn from the 2007 attacks against Estonia and those in 2008 against Georgia. Specifically, cyber cartels have developed visible online rally points and sets of informal rules to facilitate rapid organization for hacktivism in future crises.[42] These developments combine to suggest that the rest of the world can expect a trend of more abundant, more severe and politically driven cyber attacks from Russia. Throughout 2009, politically motivated cyber attacks from the .ru sphere will target countries and firms seen to affect Russia's vital interests negatively, especially during political crises, which the government can frame as issues of national pride or honor.

On a more official level, the Russian state is becoming directly engaged in cyber war preparations. Official security departments now hold occasional meetings with ISPs to coordinate better their response in the event of an attack against the Russian Federation, while they also establish contracts with key security researchers throughout the country to monitor potential attack vectors, such as botnets within the .ru sphere. The state is also becoming more directly involved in the strategic direction of the country's infrastructure and online activity, with government-owned companies and their affiliates gaining control over several major ISPs and websites throughout the last year. Several veteran Russian IT security experts concur that more will follow.[43]

While more virulent hacktivism may be the more novel trend, the sustained expansion and refinement of Russia's cyber crime economy will remain the more constant threat. Russian cyber criminals have been operating for years, some for more than a decade, with relative impunity. This permissive environment has provided them the means to expand, diversify and develop the world's most robust illicit cyber marketplaces. That the most successful cyber crime cartels operate in ways more akin to technology startups is well documented. The underground in which these cartels interact is by far the most advanced in the world, and conspicuously so. It is now more than a market; it is a bedrock institution of the wider international criminal underground, the safest place to conduct illicit business. Some unusually risk-acceptant Russian cyber criminals have begun to attack targets within their own country. That they had hitherto only stolen from foreign, mostly Western, consumers and banks was a major reason that Russian authorities have never done more to curb the problem. iDefense believes that this is likely to change, if only slightly, in 2009. Russian consumers and Russian financial institutions will begin to suffer from cyber crime and call for more effective, official opposition to the problem. As such, Western law enforcement agencies and businesses should find somewhat more willing collaborators in their Russian counterparts, if only at first on egregious and highly public cases. Of course, this does not mean that attacks directed outside of Russia will subside; it means only that Russian law enforcement will gain incentives to oppose some cyber criminals more seriously, thereby making the work of the latter more difficult.

[42] Already groups such as Hack-Wars and Stop Georgia issued manifestos to this effect, while other, "real life" organizations such as the pro-Kremlin youth group Nashi wage in online attacks as a means of making their equally "real life" grievances known.

[43] Interviews with Russian cyber security professionals, identities protected.

6.3 China

The threat of cyber espionage—both strategic and corporate—will continue to grow in frequency and severity, thus remaining the most troubling feature of the cyber environment of the PRC. Throughout 2009, Western and East Asian governments will reveal new instances of apparent Chinese cyber espionage. The Chinese hacking community has continued its shift away from patriotic motivations, which are already without much force outside of brief catharses during political crises, and realigned the more firmly toward desire for financial and prestige gains. In terms of cyber crime, excessive exploitation of Chinese criminals' favorite targets - online game account credentials - mostly in South Korea and the PRC itself, will create incentives for more attacks attempted against Western (mostly US) gaming accounts.

Cyber espionage, conducted by both the PRC government and private entities, will continue in 2009 in the same manner as in the last several years, but with notable growth in the activity of its inchoate Net Militia units (See Exhibit 6-2). It is important to note that the PRC operates on at least two different levels in matters of cyber espionage. On one hand, they conduct government-sanctioned information warfare operations against perceived enemies, as do other major powers such as the US, the UK and Russia. What makes the PRC different is its willingness to use amateur hacking groups in lower-level cyber espionage campaigns, essentially compromising unclassified computers of targeted government and contracted workers, collecting all the documents that reside on the hard drive and bringing them back to China. One long-standing worry, now finally receiving due attention, is that Chinese hardware manufacturers are already designing built-in vulnerabilities in CPUs, chipsets and other hardware likely to be used in the systems of potential targets abroad. For now, no adequate solutions to this problem exist, but for planning purposes, intelligence analysts should understand that some electronic equipment manufactured in China has been compromised.

Exhibit 6-2: Hainan University Net Militia Members Demonstrate Cyber Warfare

The PRC's most significant cyber crime trend in 2009 will be an increase in the theft of Western gaming account credentials and attacks against competing businesses within the country. For years, Chinese cyber criminals have targeted gamers in their own country and among their neighbors, especially South Korea. Indeed, the extensive success of such attacks is the very reason why newer or more ambitious cyber criminals are seeking new targets. With past experience having honed their techniques, attackers have only to adapt attack variants to an Anglophone environment to penetrate a much larger and richer reservoir of targets in the US and, to a lesser extent, the EU and Australia.

Among the most pervasive, yet lesser-known, threats throughout the telecommunications and IT sectors in China are the use of cyber attacks to gain advantage over, or retaliate against, their business rivals. Tech companies and data centers are open about the fact that unknown hackers penetrate their networks and that companies look for ways to strike back. Even universities and data centers are not immune to the problem.

Moreover, these cyber attacks are not illegal in China, though even if they were, law enforcement would not likely do much to pursue such cases.[44]

iDefense predicts that a strong proliferation will occur in China in the number of computer viruses transmitted via wireless phone networks, including those sent through SMS messages. SMS mass-mailing techniques used by cyber criminals can send upwards of 350,000 spam SMS messages in a day. The sheer prevalence of mobile phones and PDAs in China, along with the relatively cheap and low level of technology required to send spam SMS messages with credential-stealing malicious software and the like, makes a sharp increase in this kind of wireless hacking in China — and indeed in many other places in the world — likely in 2009.

6.4 The Greater Middle East and Central Asia

Malicious cyber activity, including cyber crime, ideological hacktivism and militant Islamic use of online resources in the greater Middle East and Central Asia, will increase steadily in terms of frequency, complexity and impact, although only a handful of the most skilled actors will attain Western, Russian or Chinese levels of ability in 2009.

Hacker Groups: Middle East Political Environment Shapes Indigenous Hacker Trends, ID# 470496, July 7, 2008

The politically and ideologically motivated sector of the Middle Eastern hacker population is arguably the region's largest and most prolific segment of hackers. Hackers of all persuasions typically identify, to varying degrees, with the more controversial among the region's political and religious issues. The following is a list that will inspire more attack campaigns among hackers of Middle Eastern origin, those living both in the region and elsewhere:[45] This kind of hacktivism— such as the kind witnessed in the overwhelming response of Muslim hackers against the 2008 republication of the now-infamous Jyllands-Posten cartoon caricatures of the Islamic prophet Mohammed— will continue to make itself felt online, particularly whenever religious and political tensions between the Islamic world and the West, for example, are running high.

Potential Islamic Hacktivism Issues in 2009

- The Israel-Palestine conflict
- The Arab/Iranian dispute over the official name of the Persian (or Arabian?) Gulf
- The Sunni-Shiite Muslim sectarian conflict
- The Kurdish separatists and nationalists conflict
- Religiously motivated issues

Turkish ultranationalist hacker groups are numerous, well organized, possess considerable hacking skills, and are prolific in their hacking activities. They also enjoy a significant amount of popular support among a wide segment of the Turkish public. Media outlets often openly praise these hacktivists as "terrorism fighters in the virtual world." The Ayyildiz Team is one of the more famous hacktivist cartels in Turkey. Perhaps no other team has made website defacement such a fine practice (see Exhibit 6-3) as this group. This makes legal action against any of them all the more problematic and unlikely. Turkish ultranationalist hackers have launched intensive cyber hacktivism campaigns against online interests of the EU, Greece, the Kurdish PKK and virtually every other group or interest that has in some way or another, as they perceive it, "maligned the Turkish nation."

HACKED
AYYILDIZ TEAM
"BUNDAN ÖTESİ YA İSTİKLÂL YA ÖLÜM!"

Exhibit 6-3: Ayyildiz TeamCalling Card Left on victim's website defacements

One important related trend in 2008 was the propensity among Middle Eastern

[44] Source: multiple interviewees among IT security firms, software development companies and academic institutions in the cities of Nanjing, Chengdu, Chongqing and Beijing, China, November, 2008

[45] https://portal.vrsn.com/sites/idefense/papers/Intel%20Papers/Published%20Papers/Weekly%20Threat%20Reports/2008/iDefense_Threat_20080707.doc - Hacker Groups: Middle East Political Environment Shapes Indigenous Hacker Trends

hackers — particularly Arabic-speaking users with ideological leanings — to justify their actions online with religious fatwas, or Islamic decrees, no matter how tenuous their reasoning may be. It is likely that such fatwas will continue to emanate on an occasional basis from various eminent, and not-so-eminent Islamic scholars and jurists. The proliferation of various fatwas from such sources as Al-Azhar University will provide fodder for ever more Islamic grey- and black-hat hackers to justify their activities. It is also likely that, in 2009, militant jihadists will attempt to co-opt ostensibly non-militant Middle Eastern hackers to take advantage of their stronger hacking skills. This is likely to include collaboration with more traditional cyber criminals. Hacktivists have indicated a strong interest within some jihadist circles, regarding carding and banking fraud techniques as alternative income sources.

At present, Turkish hackers constitute the most extensive and active community of non-ideological cyber criminal cartels in the greater Middle East. As such, in 2009, Turkish cyber crime and hacking are likely to increase, including carding, bank hacking, identity theft and associated illicit activities. The late 2008 arrest of Cagatay Evyapan and his gang provides a compelling example of Turkish hackers' growing ambitions in ATM fraud and carding.[46]

There is a significant community of carders active on various Arabic-language forums, many of whom appear to hail from Algeria, Morocco and elsewhere throughout North Africa. Moreover, iDefense analysts have observed Arabic-speaking carders and hackers exchanging credit card, PayPal and other stolen credentials, most of which were apparently stolen from American and European nationals.[47] Yet, compared to their ideologically motivated counterparts, Arab carders tend to be much more anonymous and low-key with their activities, making them harder to measure or identify. Nevertheless, as stated earlier, ideological hacktivists and cyber terrorists will attempt to co-opt criminals' more developed skills. It is probable that the Russian cyber crime model of offering paid services to any customer will replicate itself more among Middle Eastern hackers, with their ideologically motivated counterparts as their customers and collaborators.

Looking forward, Central Asia is primed to become an important new source of criminal and ideologically motivated hacking. Internet access and the role of the Internet in general is spreading in the former Soviet republics of Central Asia (i.e., Kazakhstan, Uzbekistan, Tajikistan, Turkmenistan and Kyrgyzstan). The Central Asian republics have a long shared history with Russia, even writing their own languages in variants of the Russian Cyrillic alphabet, while they also retain deep economic and significant political ties to Russia. Yet, most of the Central Asian countries have populations that speak languages similar to Turkish and share cultural ties to Turkey, which could promote ties between Turkish and up and coming Central Asian hacker communities. Most Internet access in Central Asian countries, such as Uzbekistan and Turkmenistan, remains severely limited and very expensive. Assuming world trends toward wider and more readily available Internet access hold true for Central Asia, it is likely that an ever-growing online population, including some

[46] https://portal.vrsn.com/sites/idefense/papers/Intel%20Papers/Published%20Papers/Weekly%20Threat%20Reports/2008/iDefense_Threat_20080922.doc - Actor Profile: Turkish Police Arrest Notorious ATM Hacker, Carding Ring Leader and Kidnapper

[47] https://portal.vrsn.com/sites/idefense/papers/Intel%20Papers/Published%20Papers/Weekly%20Threat%20Reports/2008/iDefense_Threat_20080818.doc - Cyber Crime: The Arab Carding Community: A Closer Look

criminal elements, will make itself known in Central Asia as the year 2009 progresses.

Given the volatile mix of widespread poverty in Central Asia, a talented but desperately poor youth demographic, low local employment prospects, linguistic and cultural ties with Turkish, Russian and Iranian hackers — to say nothing of repressive and corrupt governments dominating Central Asia, and the already prominent role of indigenous militant Islamist movements fighting these governments — it is unfortunately necessary to predict that Middle Eastern ideological hacktivism, cyber-terrorism and more traditional cyber crime will meet and coalesce with the Russian hacking scene in Central Asia. The only potential mitigating factors against this nightmare scenario are the increasing nationalism and cultural chauvinism among Russian cyber criminals.

6.5 Latin America

Cyber crime in Brazil, constituting the vast majority of all that occurs in Latin America in 2008, has remained on a steady upward trajectory, essentially reflecting the wider Internet penetration and increasing numbers of online banking customers (see Exhibit 6-4). Brazilian cyber criminals have long operated in a relatively permissive environment where a core of several dozen expert Trojan horse authors supply hundreds of acceptant and creative phishers. Nevertheless, a small but active community of fraudsters, who prefer the use of card skimmers and other physical means of data theft, are equally active. Most Brazilian hackers and cyber criminals are proficient enough in English and Spanish that they will encounter little difficulty liaising with their counterparts in the rest of Latin America and the Anglophone world to find new tools and techniques.

Law enforcement organs in most parts of Latin America, and especially those in Brazil, have never been backed by the force of legislation to deter and

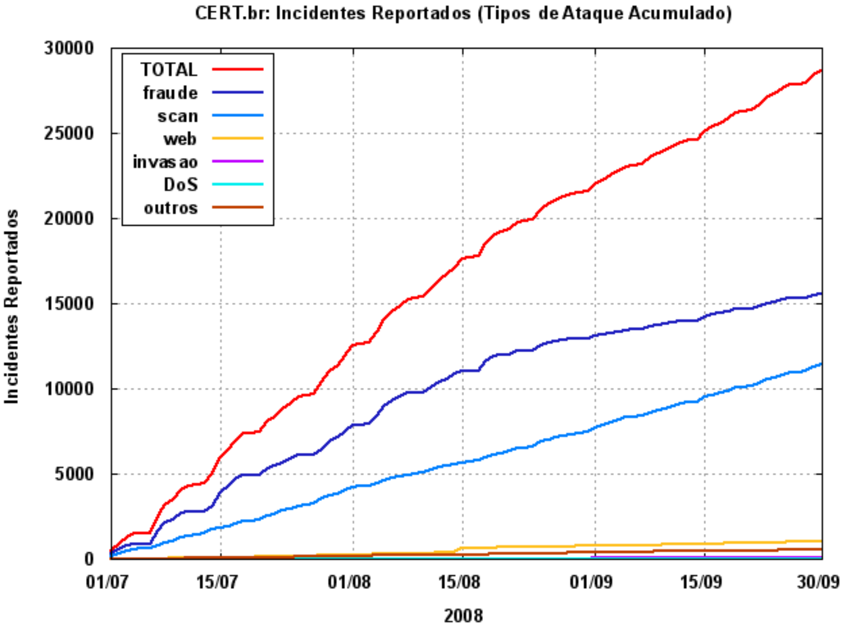


Exhibit 6-4: Increase of Reported Cyber Attacks in Brazil, from July to September 2008 from CERT.br

Title: Incidents Reported (Types of attack - accumulated)
Y axis: Number of Reported Incidents
X Axis: time (Q3/08) from July 1st to Sept 30th

Source:
http://www.cert.br/stats/incidentes/2008-jul-sep/tipos-ataque-acumulado.html

combat cyber crime. This fact, combined with insufficient clarity of mission, is the primary complaint among Brazilian law enforcement officials tasked with investigations in cyber space.[48] This is finally beginning to change, though; Brazil, Argentina, Chile and Mexico have all initiated cyber legislation where none existed or drastically increased the resources necessary to properly prosecute cyber crimes. In June 2008, Argentina approved an extensive update to its criminal code to cover cyber crimes, including malicious code distribution and system breaches,[49] while Brazil expects to have a new set of cyber crime laws approved by the beginning of 2009. The Chilean government is also currently building upon earlier efforts by requiring banks to implement two-factor authentication technologies to secure only transactions.[50] The effects of these developments will show themselves in force during 2009 as law enforcement officers begin to make use of their new, official powers.

Law enforcement will also likely show marked progress throughout 2009 in the other most important aspect of fighting cyber crime: inter-departmental and international cooperation. Brazilian police told iDefense analysts in early 2008 that a key cause of their difficulties was the lack of cooperation among different police units throughout the country.[51] Officials also noted that Brazilian cyber criminals were dealing more with collaborators in other countries, and demanding that other police forces do so. Indeed, by mid-2008, a few examples of cooperation between the Brazilian Federal Police and their counterparts in Spain[52] and the US had led to the dismantling of major, interconnected cyber fraud cartels.[53] By all accounts, this is only the beginning. International cooperation is a key part of the new strategy to fight cyber crime, which, though now in the later stages of development by the Federal Police's most talented agents, will begin to show its effects in 2009.

Banks in Latin America, particularly those in Brazil, have also been progressing rapidly in their abilities to counter cyber fraud. Most have instituted two-factor authentication for all online banking customers and are currently expanding their internal security capabilities.[54] This is already beginning to decrease the success rate of certain types of longstanding phishing attacks, combined with banking Trojans. United with the invigorated law enforcement capabilities discussed above, the cyber security environment will grow tougher for cyber criminals.

Two broad classes of trends will characterize the Latin American threat environment in 2009: first, an intensification of activity by both criminals and authorities; second, deeper levels of integration with cyber crime environments

Actor Profile: Turkish Police Arrest Notorious ATM Hacker, Carding Ring Leader and Kidnapper, ID# 472619, Sept. 23, 2008

Cyber Crime: The Arab Carding Community: A Closer Look, ID# 471352, Aug. 19, 2008

[48] iDefense, *Global Threat Research Report: The Cyber Security Environment of Brazil*, May, 2008

[49] Staff Writer, "Argentina Modifies Its Criminal Code to Include Information Technology Crime", *Internet Business Law Services*, July 7, 2008, at http://www.ibls.com/internet_law_news_portal_view.aspx?s=latestnews&id=2090

[50] Press Release, "Entrust Helps Chilean Financial Institutions Comply with Government Regulations", *Reuters*, May 30, 2008, at http://www.reuters.com/article/pressRelease/idUS120754+30-May-2008+PRN20080530

[51] Interviews with agents of the Brazilian Federal Police and officers of the Organized Crime Unit of the Sao Paulo Police Department.

[52] Staff Writer, "Five Brazilian fraudsters arrested in Spain in March 2008", *Mir Nuevas*, April 3, 2008, at http://www.mir.es/DGRIS/Notas_Prensa/Ultimos_comunicados/np031001.html

[53] Elinor Mills, Brazilian Charged in the US on Suspicion of Operating Botnet", *CNet News*, August 21, 2008, at http://news.cnet.com/8301-1009_3-10022990-83.html

[54] Staff Writer, Banco Itau Secures More than 1.6 Million Customers", *Reuters*, May 7, 2008, at http://www.reuters.com/article/pressRelease/idUS72470+07-May-2008+PRN20080507

in other parts of the world. While cyber crime in Brazil and the rest of Latin America will continue to increase marginally in frequency and severity, the rapid improvement of law enforcement's capacity to respond to cyber threats will prove to be the more consequential development throughout 2009.

6.6 United Kingdom

The criticality and resourcefulness of London's financial system are presently driving a significant increase in private sector cyber security provision. Nearly the entire financial community is engaged in cultivation of more mature in-house security teams and the implementation of the latest fraud detection systems, 2FA schemes and chip-and-PIN technologies. The UK Payments Association (APACS) notes that chip-and-PIN continues to have a positive effect on card fraud committed in the UK, with retail fraud falling by two-thirds from £218.8 million in 2004 to £73.0 million last year.[55] So far, the results are promising; however, there are already indications that highly skilled and knowledgeable cyber criminals are finding ways around even these robust countermeasures. Of special note are criminals' efforts to compromise chip-and-PIN devices at the manufacturing stage — a novel development, which has led to several massive compromises of financial data in the UK. The financial system is not the only victim either. Throughout 2008, no fewer than five public statements made by high-level policymakers hit the press to note that the UK is presently under persistent cyber espionage attacks by foreign entities, though the full extent of these was left unelaborated.[56] The UK government is also under near-constant criticism in the media for its inability to keep reasonable control of sensitive data.[57] The number of such reported incidents through mid-year 2008 exceeded those for the whole of 2007. Also, data lost were often of a more serious character, namely that belonging to the Ministry of Defense or the intelligence services.[58]

Adding to public concern is the inability of the government to build and empower an adequate law enforcement body to focus upon cyber threats. According to veterans of the UK's financial IT security community, the 2007 closure of the National High-Tech Crime Unit (NHTCU), whose functions have been taken over by the Serious Organized Crime Agency (SOCA), left a "yawning gap" in Britain's ability to fight cyber crime. Meanwhile, members of the Corporate IT Forum have called on the Home Office to keep its promise to establish a police unit to deal with high-tech criminal cartels,[59] though disagreements in Parliament have hindered progress. Labour's new government did not agree with the Lords Science and Technology Committee suggestion, made in early 2008, that lawlessness "was rife" on the Internet, citing unwillingness to add to the burden on the industry by passing more regulations. Still, the Home Office has finally approved the creation of a central Police e-Crime Unit (PeCU), a year after the idea was first proposed by the Association of Chief Police Officers and the Metropolitan Police. The PeCU will be based at Scotland Yard and is expected to begin work early next year,

[55] http://news.bbc.co.uk/2/hi/uk_news/politics/7327082.stm

[56] http://www.silicon.com/publicsector/0,3800010403,39330307,00.htm

[57] http://www.theinquirer.net/gb/inquirer/news/2008/10/29/277-breaches

[58] http://www.theregister.co.uk/2008/10/14/mod_bigger_loss/

[59] http://www.homeoffice.gov.uk/rds/pdfs08/hosb0708.pdf

providing specialized computer forensics training and coordinating efforts across multiple police forces.[60]

The UK will remain among the world's most heavily targeted information security environments throughout 2009, though promising developments at Scotland Yard will begin to make an impact later in the year. Even if presently suffering a relatively intense economic contraction, the UK is a wealthy and highly internationalized country with an extensively digitized economy, standing as a fundamental hub of the global financial and commerce systems. Moreover, Britain wields the best military forces and intelligence apparatus in the EU, and remains a first-order politico-diplomatic power on the world stage. As such, it remains a salient, accessible and high-value target of cyber crime and cyber espionage, despite the fact that its IT networks are as advanced, and well protected as most of the rest of the developed world. Its main weakness resides neither in its critical IT infrastructure nor in its information security community, but rather in a persistent incoherence at the level of national law enforcement policy and leadership. Such conditions make the UK a sort of crucible of cyber malevolence in which leading edge exploitation techniques bring vast rewards to those criminals and spies ambitious and skilled enough to take them. All of the above characterization will hold throughout 2009.[61]

Interestingly, cyber security in the UK is fast becoming among the most recognized problems in business and government. The British press has been increasingly attentive to such issues, especially the government's shortcomings and the dangers to banking customers, and a stream of surveys repeatedly highlights this crowing concern among the public. As such, it is likely that the UK will emerge as the first society in which most of the population gains a general awareness of the importance of cyber security, though without an understanding of its dynamics. This means that security professionals and policymakers in the rest of the developed world should watch Britain closely, in 2009 and beyond, to learn from the promises and perils encountered by firms and government institutions as they navigate this shift in perception.

6.7 Epilogue: The Impact of the Global Financial Crisis

Any organization with an interest in security must consider all of the analyses presented in this section in light of the unfolding global financial crisis and economic downturn. While such phenomena occur periodically, this is the first to coincide with a dramatically worsening global cyber security situation. As such, the impact on cyber crime and economically oriented cyber espionage remains unclear; however, the sheer operational turmoil caused by the restructuring currently affecting nearly every major financial institution will open up unprecedented opportunities for exploitation by cyber criminals, corporate spies among unethical competitors and official cyber spies of unfriendly governments. Such conditions, where enormous losses and risks surround decision makers, can often foster more risk-acceptant attitudes, especially when mistrust is already pervasive and uncertain futures leave many with a sense of having little to lose. Unfortunately, the very conditions that

[60] http://www.theregister.co.uk/2008/10/01/pceu_cybercops_approved/

[61] Interviews with Graeme Pinkney (Barclays), Sandro Bucchianeri (VeriSign Credit Suisse Consultant), Alex Hudson (RBS)

foretell an increase in malicious activity targeting financial organizations are likely to obscure the incidence of the attacks, making this a doubly dangerous time for the global financial system.

The link between economic crises and increasing political tension is well established, if still not formalized with precision sufficient to predict the exact timing and locations of either. Nevertheless, militaries and intelligence agencies in most of the world's major and mid-range nations had already begun thinking seriously about cyber warfare and cyber espionage before the current economic contraction. Although it remains too early to say with certainty, governments and critical industries must at least begin to prepare for an intensification of political wrangling among countries between which tension already exists. Economic difficulties cause nations to shift their priorities, sometimes rapidly; doing so often leaves power gaps or even outright vacuums. Other interested actors who have fared relatively better often find such occasions opportune moments for expanding their interests. Moreover, with national governments and regional institutions stepping in to bolster and reorient their respective economic spheres, one cannot ignore the possibility of a wave of protectionist measures throughout most countries, especially the great powers. Such developments tend to produce disillusionment, suspicion and scapegoating by those polities, which suffer the most. The result is often intensified strategic rivalry, which, at the present time, could find easy expression in cyberspace. Specifically, beginning now and throughout 2009, state-directed or state-approved hacking for strategic and economic advantage is likely to increase at its most unprecedented rate to date, perhaps as much as the past 3-5 years combined. Once the evidence of this increase begins to surface, the consequent perceptions of a more dangerous world will push governments and firms to respond with more stringent, often aggressive strategies of cyber warfare, espionage and counterespionage.

7 Disruptors

In the commercial world, the notion of a business disruptor concerns ideas or technologies that emerge and fundamentally change the way a business sector operates. the Model T car from the Ford Motor Company (see Exhibit 7-1). Other companies competed with Ford in the early 1900s, but when the company implemented and later streamlined the assembly line process to build the Model T in 1914, Ford produced more cars than all other automakers combined. That year, Ford built nine out of 10 cars purchased globally.[62] That is a business disruptor. One modern-day example of a business disruptor is the combination of iTunes, the iPod and pirated music (see Exhibit 7-2). These two technologies and one cultural phenomenon together, have fundamentally changed how the world buys music. The compact disc as a medium for music distributing has been dying for the past decade.[63] It is conceivable that the CD will soon follow the path of the vinyl LP, cassette and 8-track tape as the primary commercial means for dissemination of music. The change from CD music to digital music downloads is a business disruptor.

Exhibit 7-1: Ford's use of the Assembly line to build the Model T caused a change in the auto industry

Exhibit 7-2: iTunes and iPod combine to cause a Music Industry Business Disruptor

In this sense, there also exist security disruptors, which result from new technologies or developments in the culture that will fundamentally change how the business enterprise secures its environments. This section will discuss five such fundamental changes:

- The Metaverse
- IPv6
- Top-Level Domains and International Domain Names
- Cyber Terrorism
- Mobile Platforms

7.1 Multi-User Online Environments: The Metaverse

Multi-user online environments (MOEs) refer to the entire set of persistent online environments that range from massively multiplayer online role-playing games (MMORPGs), such as World of Warcraft (WoW) or City Of Heroes, to other virtual worlds, like Habbo Hotel and Second Life, where gaming is not as important as the social networking aspect of the environment (see Exhibit

[62] "The Model T Ford", 2008, http://www.modelt.ca/background.html

[63] "Sales of Music, Long in Decline, Plunge Sharply ", Ethan Smith, 21 Mar 2007, http://online.wsj.com/public/article/SB117444575607043728-oEugjUqEtTo1hWJawejgR3LjRAw_20080320.html?mod=rss_free

7-3). These environments connect many simultaneous users through the Internet. These programs differ from regular computer games because their environments are perpetual and often referred to as virtual, persistent worlds. Users log on, join the game and leave whenever they wish, but the game continues with other players in a hyper-real, richly rendered, three-dimensional space. Players control “avatars,” which are in-game characters that have attributes and interact with other avatars and the game’s environment.

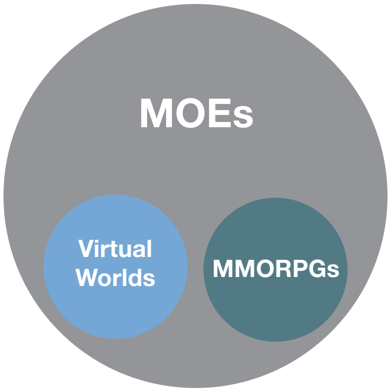


Exhibit 7-3: Venn Diagram that shows that MMORPGs and Virtual Worlds are are both MOEs

Independent sources predict that the MOE user base will exponentially grow from 16 million users today to over one billion users in the next decade (see Exhibit 7-4)[64] Sub-economies have emerged within most MOEs where players buy and sell in-game items and currency. Most MOEs have some of the same characteristics as the popular social networking sites of today, such as mySpace and Facebook. Heavyweight research organizations, like IBM and Linden Labs, are trying to make it possible to move MOE avatars between virtual worlds seamlessly, maintaining the avatar’s identity in terms of appearance, personal information and banking status. Although some research questions remain unanswered (like the matter of trust management as avatars move from world to world), researchers are making progress. Within the next 10 to 15 years, these virtual environments may converge into one Metaverse, similar to the way author Neil Stephenson outlined the Metaverse in his 1992 novel, *Snow Crash*. If this prediction comes true, these MOEs may become the next graphical user interface (GUI) for users accessing the Internet.

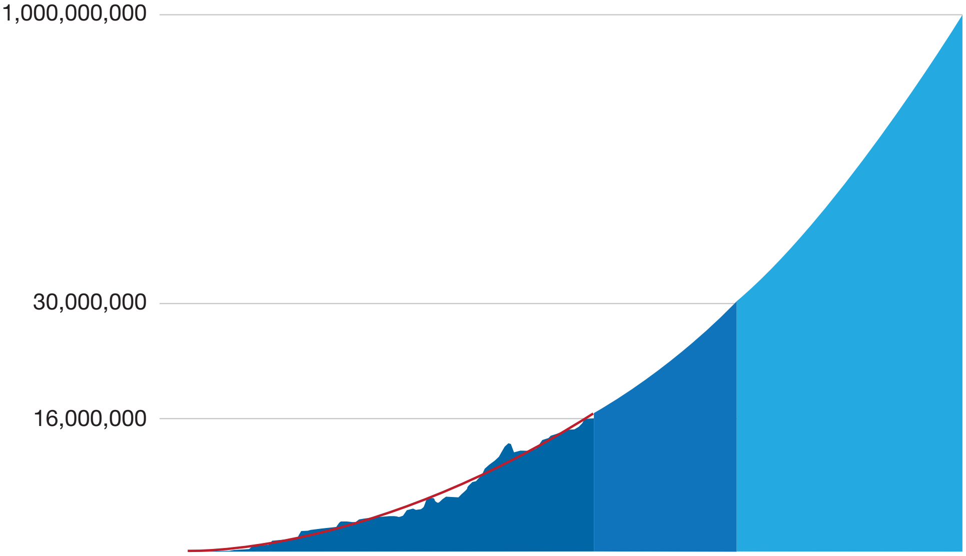


Exhibit 7-4: MOE Exponential Growth 1997-2018

The social nature of MySpace, Facebook and WOW depends largely on the accessibility of users. Users are not anonymously reading text and commenting on random blogs with surreal usernames anymore. Users are not “invisible.” Social networking sites and MOEs thrive off applications that make user actions visible to others. The most obvious example is the ability to see another avatar walk around, but it is the same impact as Facebook users commenting on another’s wall. Other FaceBook users witness and attribute everything that is typed. In the future, this “visibility” of the user could

[64] “1 billion virtual world and MMO users by 2018”, techRadar, 5 Jun 2008, http://www.techradar.com/news/gaming/1-billion-virtual-world-and-mmo-users-by-2018-383126

represent an enormous change to the way we use the Internet.

Today, MOE designers build these environments in a way that allows participants to change their personal space easily. The code comes built-in with hooks that players can use to modify their surroundings. If the average gamer can build structures like those shown in Exhibit 7-5, what might an excellent hacker be able do with access to the same tools and access to an ubiquitous avatar with his or her personal information or credit card information? Although some MOE developers are thinking about security—most recently, Blizzard announced the availability of two-factor authentication for WoW[65] —many developers have not even begun to think about the security precautions necessary when the world transitions to the Metaverse.

7.2 IPv6: A More Sino-Centric Internet

IPv6 is the next IP protocol on deck and will eventually replace IPv4. The difference between IPv4 and IPv6 is staggering. According to Charles Kozierok, if you could map all of the IPv4 IP addresses onto the petal of a flower, the space needed to hold all of the IPv6 IP addresses would be as large as our solar system (see Exhibit 7-6).[66]

Once the world adopts IPv6, everything will have an IP address. Everything in the average house, from bedside lamps to garage door openers, will be IP addressable. This is relevant because the pool of IPv4 addresses is quickly running out. According to some researchers, as of October 2008, the central registry for IPv4 addresses will be exhausted around November 2010.[67] Despite this prediction, IPv6 adoption rates continue to remain incredibly low, especially in the West. Arbor networks released a report in July 2008 detailing the IPv4 versus IPv6 traffic; the research found that tunneled IPv6 traffic accounted for only approximately 0.0026 percent of the IPv4 traffic.[68]

Exhibit 7-5: 2d Life Buildings built by average game players

www.jpl.nasa.gov

Exhibit 7-6: Analogous Comparison of Space Available in IPv4 (left) and IPv6 (right)

[65] "Blizzard Authenticator FAQ", Blizzard, http://us.blizzard.com/support/article.xml?articleId=24660

[66] Kozierok, "The TCP/IP Guide: A Comprehensive, Illustrated Internet Protocols Reference"

[67] "Regional registry IPv4 address exhaustion in...", Matt Ford, http://penrose.uk6x.com

[68] "IPv6 Report", Arbor NEtworks, http://www.arbornetworks.com/IPv6research

Exhibit 7-7 displays Kozierok's estimated times for the deployment of IPv6 in the US and China. Kozierok predicts that most modern networks will be capable of handling IPv6 network traffic by 2019 and that Internet users will start passing IPv6 traffic by 2023.[69] In the summer of 2008, the US government declared that it was IPv6 capable,[70] meaning it has the ability to pass IPv6 traffic. According to Google, adoption rates are occurring much more frequently, at least in some parts of the world (see Exhibit 7-8).[71] Iljitsch van Beijnum, from ars technica, says that it is unclear why Russia and Ukraine have high adoption rates but he does have an idea about the US and France. It has to do with the deployment of routers that are IPv6 capable. In France's case, one of the major Internet Service Providers uses a home router that is IPv6 capable. In the US, Apple's market share has been increasing these past few years and most of those owners use a IPv6 capable router. But, as Danny McPherson from Arbor Networks says, "There's a big difference between measuring end systems or clients capable of usable IPv6 connectivity (what Google measured) and how much actual traffic on [a defined subset of] the Internet is IPv6 (what we measured)."[72]

China, on the other hand, deployed a working IPv6 network for the Beijing Olympics as a showcase to the world that they are a modern nation. It was the first installment of a much larger network improvement project called China's Next Generation Internet (CNGI): "The China's Next Generation Internet project (CNGI) is a government of China initiative that seeks to make an early entry into using the IPv6-governed Internet space, with the objective of gaining the first mover advantage. This breakthrough will allow Chinese researchers, academics and entrepreneurs to develop new applications and widgets using IPv6-supported functionality."[73] Even though China is sixth on the capability chart, they are poised to take an early adopter role of the technology as the nation's IPv6 network grows.

All of this leads to an interesting hypothesis. New ideas, important concepts, and technological initiatives regarding how to use the gigantic pool of addresses offered by IPv6 may not originate from the United States and predominantly Western countries and the "Western cultural sphere" as they have for the most part done. Instead, these addresses may come increasingly from China and by extension a cultural sphere more influenced by Far Eastern values and concepts. Especially over greater periods, this could result in a next generation of subtle but profound technological innovations spreading through the Internet from China and the Far East. This could result in China, and perhaps more generally the Chinese and Far Eastern cultural sphere, gaining much more influence and stature around the world through the Internet. China has managed to leverage its position to gain the incredibly important "first adopter" advantage with IPv6 through its speedy adoption of

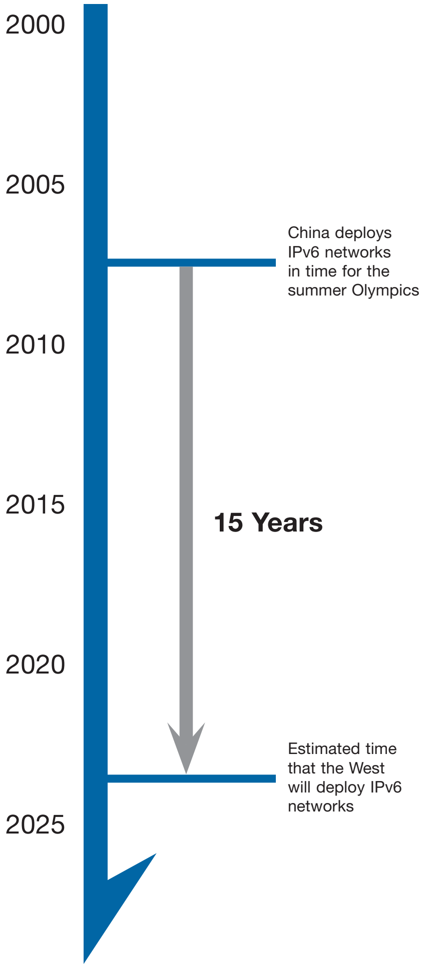

2000
2005
2010
2015
2020
2025
China deploys IPv6 networks in time for the summer Olympics
15 Years
Estimated time that the West will deploy IPv6 networks

Exhibit 7-7: IPv6 Adoption Estimates

Country	IPv6 Penetration
Russia	0.76%
France	0.65%
Ukraine	0.64%
Norway	0.49%
US	0.45%
China	0.24%
Japan	0.15%

Exhibit 7-8: Google Estimates of IPv6 Capability

[69] Kozierok, "The TCP/IP Guide: A Comprehensive, Illustrated Internet Protocols Reference"

[70] "Feds: We are ready for IPv6 D-Day", By Carolyn Duffy Marsan, Network World , June 26, 2008, http://www.networkworld.com/cgi-bin/mailto/x.cgi?pagetosend=/export/home/httpd/htdocs/news/2008/062608-ipv6-federal-government.html&pagename=/news/2008/062608-ipv6-federal-government.html&pageurl=http://www.networkworld.com/news/2008/062608-ipv6-federal-government.html&site=lanwan

[71] http://arstechnica.com/news.ars/post/20081113-google-more-macs-mean-higher-ipv6-usage-in-us.html By Iljitsch van Beijnum, Nov 13, 2008, "Google: more Macs mean higher IPv6 usage in US"

[72] http://asert.arbornetworks.com/2008/11/google-report-on-ipv6-capable-clients/, Danny McPherson, Nov. 14, 2008

[73] "IPv6 and the 2008 Beijing Olympics",by Kaushik Das, IPv6.com, http://www.ipv6.com/articles/general/IPv6-Olympics-2008.htm

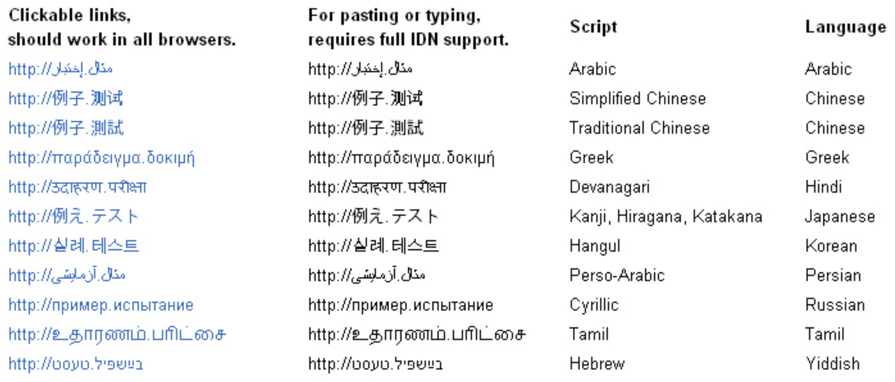
the technology. The enormity of the IPv6 address space will provide immense latitude to continue technological innovations, particularly with regard to networking and connectivity. This potential shift of first mover advantage to China is the reason that IPv6 could prove a security disruptor.

7.3 Top-Level Domains and International Domain Names: A Balkanized Internet

On June 26, 2008, the board of the Internet Corporation for Assigned Names and Numbers (ICANN) accepted a recommendation to allow applicants to self-select their domain name. Currently, users have access to only 21 top-level domain (TLD) names, like .org, .com and .info. If ICANN approves the new recommendations, domain names could be anything. Amazon could apply for .book, Oracle for .database and Las Vegas for .SinCity. Upon approval, ICANN expects the new naming convention to be available by the second quarter of 2009.[74]

Internationalized Domain Names (IDNs) are domain names or Web addresses written in non-English-language characters.[75] ICANN is moving toward authorization to implement this idea in late 2009. Essentially, Internet users will be able to enter URLs like the ones listed in Exhibit 7-9, in letters and fonts that are not strictly English. On Oct. 2, 2008, the ICANN International Domain Name Charter Working Group (IDNC WG) published a request for information to assess how many countries are interested in a fast-track process to implement IDNCs.[76] Russia's President Medvedev has voiced interest in establishing a ".fr" (".фр") domain name using Cyrillic Russian characters.

Together, these two technology changes represent a significant security disruptor. The initial obstacles and difficulties in accessing foreign language (and specifically non-Roman alphabet) scripts on computers is problematic. Computers must have the suitable language support packs and keyboards



Clickable links, should work in all browsers.	For pasting or typing, requires full IDN support.	Script	Language
http://مثال.إختبار	http://مثال.إختبار	Arabic	Arabic
http://例子.测试	http://例子.测试	Simplified Chinese	Chinese
http://例子.測試	http://例子.測試	Traditional Chinese	Chinese
http://παράδειγμα.δοκιμή	http://παράδειγμα.δοκιμή	Greek	Greek
http://उदाहरण.परीक्षा	http://उदाहरण.परीक्षा	Devanagari	Hindi
http://例え.テスト	http://例え.テスト	Kanji, Hiragana, Katakana	Japanese
http://실례.테스트	http://실례.테스트	Hangul	Korean
http://مثال.آزمایشی	http://مثال.آزمایشی	Perso-Arabic	Persian
http://пример.испытание	http://пример.испытание	Cyrillic	Russian
http://உதாரணம்.பரிட்சை	http://உதாரணம்.பரிட்சை	Tamil	Tamil
http://בײַשפּיל.טעסט	http://בײַשפּיל.טעסט	Hebrew	Yiddish

Exhibit 7-9: IDNs Examples

[74] "Biggest Expansion in gTLDs Approved for Implementation", ICANN, 26 June 2008, http://www.icann.org/en/announcements/announcement-4-26jun08-en.htm

[75] "Internationalized Domain Names", Verisign, http://www.verisign.com/information-services/naming-services/internationalized-domain-names/

[76] "ICANN Seeks Interest in IDN ccTLD Fast-Track Process", ICANN, 2 Oct. 2008, http://www.icann.org/en/announcements/announcement-02oct08-en.htm

installed to allow proper text display and entry in these languages. A certain level of language-barrier-induced “Balkanization” may occur with Chinese Internet users, for example, not readily able to access websites in Arabic-language domains, or English speakers not able to access Slovak or Korean sites.[77]

While this may present something of an obstacle to Internet communication, surfing and business transactions at first, factors like the already widespread Unicode standard, the use of simple pre-written URL links, and the likely proliferation of search engine-based IDN translation schemes are likely to lessen these obstacles over time. Existing businesses are likely to register multiple language versions of their websites across different IDNs to access new markets.

In the near future, the Internet could splinter more sharply into language-specific Internet sectors, in a way more pronounced than is already the case. At first, the impact to business may be a switch away from the global digital economy described in Tom Friedman’s book, The World is Flat to something of a “Balkanized” Internet with more sharply distinguished language barriers that complicate doing business around the globe. ICANN’s introduction of IDNs in particular will mean that the true intricacy of the world will be reflected on the Internet more so than ever before. This will present some disruptive obstacles, but at the same time—especially as Internet use rises rapidly among non-English speakers—will create immense new opportunities for business and interaction.

7.4 Overreaction to Cyber Terrorism

The security community regularly debates exactly what a cyber terrorist attack might look like. iDefense defines cyber terrorism by what it is and by what it is not (see Exhibit 7-10):

Cyber Terrorism	Not Cyber Terrorism
Causes or threatens violence or significant socio-economic or political disruption	Communication between two terrorists via the Internet
Targets civilians	Terrorist Propaganda
Pursues political and/or ideological goals	Operational Support of Terrorist Actions
Possesses a psychological impact	
Most likely will accompany a physical attack	

Exhibit 7-10: Cyber Terrorism Defined by iDefense

The fact that there has not been a cyber terrorist attack, ever, might mean that the bar is set very high for the chance of a terrorist to succeed in this area. Even so, some experts worry that there will be one of these kinds of attacks in the next 10 to 15 years. It will happen on the front end or the back end of a physical attack, but it will happen.[78]

[77] http://ancienthistory.about.com/b/2005/05/04/tower-of-babel.htm, By N.S. Gill, May 2005

[78] Black Ice: The Invisible Threat of Cyber-Terrorism by Dan Verton (hardcover – Aug. 19, 2003)

Terrorism Disruptor

The potential for a cyber terrorism attack within the next decade is not the security disruptor. The security disruptor, in this case, is what comes after the attack and after federal governments decide to do something about it. The evidence of the first valid cyber terrorist attack will most likely lead to a profusion of policy and bureaucratic "experiments" whereby nations attempt to gain better control over their cyber threat environments. Early attempts will likely be incoherent and excessive. Mistakes will outweigh successes. Civil liberties and the safety of the Internet may suffer. Think of what the government did after the Enron scandal; ultimately, they passed the Sarbanes-Oxley (SOX) Act of 2002: "[SOX] came into force in 2002 and introduced major changes to the regulation of financial practice and corporate governance."[79] Essentially, the act causes businesses to enact very costly administrative procedures in an effort to prevent Enron-type situations from developing again. "[Some] have correctly stated SOX was mostly worthless, a statement now proved true [since the legislation did nothing to stop the current financial crisis]."[80]

" In a six-week downward spiral [in the fall of 2001], Enron disclosed a stunning $638 million third-quarter loss, the Securities and Exchange Commission opened an investigation into the partnerships and the company's main rival backed out of an $8.4 billion merger deal.

Enron filed for protection from creditors on December 2 in the biggest corporate bankruptcy in U.S. history. Its stock, worth more than $80 about a year ago, has tumbled to less than a dollar a share. Enron's collapse left investors burned and thousands of employees out of work with lost retirement savings."

"Explaining the Enron bankruptcy", CNN, January 13, 2002, http://archives.cnn.com/2002/US/01/12/enron.qanda.focus/

Leaders will make many mistakes in building up full-scale cyber warfare and terrorism response capabilities. The impact to business could potentially be SOX-type legislation that adversely affects how companies run their business. One potential new law might call for a ban on responsible and full disclosure concerning vulnerability information. Responsible disclosure refers to the concept that vulnerability researchers work with vendors before going public with the information. Full disclosure refers to the practice of making the details of security vulnerabilities public regardless of any potential interaction between the researcher and the vendor. The idea that going public with vulnerability information may be against the law will fundamentally change how enterprises protect their networks. This is just one example of how a government may overreact to a cyber terrorist attack and is indicative of why iDefense considers cyber terrorism a disruptor.

7.5 Mobile Phones: A New Attack Platform is Coming

Mobile phones and PDAs have been around for years. Every year, since the beginning of the mobile phone platform, security pundits, including iDefense, have claimed that this would be the year criminal elements would go after the mobile platform. Although there have been some proof-of-concept tests about how to accomplish these tasks, there has not been much incentive for the criminal element to pursue the devices. Until recently, there has been no money in it and these devices did not really have the widespread connectivity to the Internet that laptops and desktops enjoy. This changed in 2007. Financial institutions started to deploy out-of-band authentication schemes to authenticate money transactions. Banking customers use this technique when they wish to move money between accounts. The client logs into the banking website and starts the process to move money. The bank authenticates the transaction by sending an SMS message to the client's mobile phone. The client receives the message and returns it to the bank with a PIN number. The

[79] "The Sarbanes-Oxley Act", Addison-Hewitt Associates, http://www.soxlaw.com

[80] "The Mortgage Crisis, Enron, and Sarbanes-Oxley (SOX) ", 11 Oct 2008, Panes of Glass, http://panesofglass.org/economics/the-mortgage-crisis-enron-and-sarbanes-oxley-sox/

bank receives the returned SMS message and authorizes the transaction. This authentication prevents man-in-the-middle (MitM)-type attacks that originate from the client's browser.

Applets allowing users to execute monetary transactions have started to emerge for smart phones. In 2008, PayPal announced a new applet that allowed Blackberry users to conduct PayPal transactions on the phone.[81] Indeed, vendors are encouraging development of such "mini-applets" by publishing their own software development kits for the platforms in the public sphere In Brazil, one start-up has 60,000 customers using their phones as a credit card. The buyer goes to the store, chooses his items and proceeds to the checkout stand. The cashier rings the items up and sends the bill to the buyer's mobile phone via SMS. The buyer inputs his PIN to authorize the sale and sends the bill back to the cashier via SMS. The vendor applies the charges to the buyer's monthly phone bill.

As the US starts to catch up to Europe in the deployment of 3G networks, mobile devices are looking like better and better targets to the underground.[82] In August 2008, Adam Gowdiak of Security Explorations in Poland announced to the world that he had discovered vulnerabilities in Nokia's S40 mobile phone operating system and the underlying Sun Microsystems J2ME engine. The vulnerabilities, he claimed, allowed an attacker to obtain complete control over any Nokia S40 phone. Nearly 100 million phones worldwide use the Nokia S40 platform.

As the technology for the mobile phone platform evolves, four operating systems have emerged, all of which follow most, if not all, of the rules of the open source community: Google's Android, Apple's iPhone, Windows Mobile and Symbian) (see Exhibit 7-11).

Google's Android

- Completely Open
- Runs any hardware
- Free UI
- No Cost for Carriers to use
- Turns odd phones like the RAZR into a smartphone

Apple's iPhone

- Fairly Open and well documented
- Costly
- OS Kernel can not be sold to Third parties (bundled with the device)
- SDK is popular and free

Windows Mobile

- Closed Operating System
- Common UI across platforms
- Developers can build third party applications via .NET Compact Framework

Symbian

- Currently not Open Source but will be soon
- Will exist under the royalty-free Eclipse Public License
- Most widely used mobile operating system in the world today

Exhibit 7-11: Mobile Operating Systems

In contrast to the other smart phone operating systems, the iPhone uses a completely different distribution model. Applications can only be loaded onto the iPhone through the iTunes Application store, and Apple controls this process. In this model, Apple can completely control what users legitimately run on the phone and Apple has installed a built in "kill switch" if an application proves malicious. Apple has stirred much opposition for such a "closed" model, which is effectively white-listing for phones. Every program that runs on the iPhone is pre-approved; nothing else should run. For users to add anything to the phone outside of this process, they have to hack the phone, voiding their warranties and taking the risk upon themselves.

As the mobile platform starts to spread as a legitimate means to access the Internet, technology experts still tend to forget that not everybody in the world today has a broadband connection to their house.[83] In the next 10 to 15 years, especially in the East, the main Internet access platform will most likely be the mobile device. The same tasks that people use laptops for today will migrate to their mobile phones. Personal and professional data will reside there,

[81] "PayPal Launches Its First Mobile Service on a Downloadable Application", Digital Transactions, April 2008, http://www.digitaltransactions.net/newsstory.cfm?newsid=1754, April 2008

[82] http://reviews.cnet.com/4520-11288_7-5664933-1.html, cnet reviews, Ben Patterson, Mar 2008

[83] "BROADBAND INTERNET STATISTICS TOP WORLD COUNTRIES WITH HIGHEST INTERNET BROADBAND SUBSCRIBERS IN 2007", Internet World Stats, http://www.internetworldstats.com/dsl.htm

including company proprietary information and entertainment and individual information. The impact to the business is that strategies for securing these devices are at their incipient stages:

- Encrypting transmissions between employees
- Encrypting data at rest on the platforms
- Securing the platform from attack
- “Kill switches” for lost devices

The way ahead is clear though. The same processes and procedures that enterprises are just now using to secure the laptop must be applied to the smart phone.

8 Conclusion and Predictions

Throughout the year, iDefense collects information into information categories that it calls “critical information requirements” (see Exhibit 8-1). In the current set are four larger categories and a number of sub-categories within each, and iDefense has placed its predictions into these categories. In addition, iDefense understands that its various predictions affect distinct organizations differently. For example, commercial organizations will worry more about the anticipated volume increase of rogue security applications than the critical infrastructure organizations will. As such, each prediction lists the consequences for the type of organization that it affects. This includes government intelligence, law enforcement, critical infrastructure and commercial sector organizations.

This report began with a scorecard of how well iDefense did predicting security events for 2008. It is only fitting that it ends with a new set of predictions for 2009. After reviewing the headlines, analyzing the evolving cyber cartel tactics and procedures documented in numerous iDefense publications, and scrutinizing developments in countries from around the world, iDefense offers its predictions.

Political
Cyber Espionage
Cyber War
Cyber Hacktivism
Cyber Terrorism
Electronic Political Process
Information Control
Use of IT Security Issues for the Political Process

Response
Critical Infrastructure Protection
Policy
Software
Law Enforcement

Cyber Crime
Tools and Technologies
Incidents
Notes from the underground

Actors
Groups/movements
Individuals
Government

Exhibit 8-1: iDefense Critical Information Requirements

2009 Predictions	**Consequences for** Government Intelligence (**GI**) Law Enforcement (**LE**) Critical Infrastructure (**CI**) Commercial Sector (**CS**)
Actors - Groups Expect more software vendors to deploy a schedule for patch releases.	**CS**: Potentially make patch planning easier **CI**: Potentially make patch planning easier
Actors - Individuals Expect more partial vulnerability disclosures from prominent security researchers. Other security researchers will focus whenever this situation develops.	**GI**: Increased likelihood of attacks against critical infrastructure. **CI**: Increased likelihood of attacks against critical infrastructure. **CI**: Expect senior management to hear about it in the news. **CS**: Expect exploits to occur afterward. **CS**: Expect senior management to hear about it in the news. **GI**: Expect senior management to hear about it in the news. **LE**: Expect senior management to hear about it in the news.
Cyber Crime – Notes from the Underground IFrames were so successful in 2008 that it is unlikely that another distribution method will usurp its position in 2009.	**CS**: User anti-phishing education is no longer sufficient
Cyber Crime – Notes from the Underground Expect to see continued growth in volume and innovation in the illegal distribution of rogue security applications.	**CS**: More security incidents
Cyber Crime – Notes from the Underground Expect China's cyber cartels to expand into the theft of Western gaming and financial account credentials	**LE**: China becomes a more complex security environment; law enforcement, not just the intelligence community, must begin to learn about the new Chinese criminals. **CS**: The set of potential attackers that target financial institutions will grow larger **CS**: Will necessitate changes in fraud detection.
Cyber Crime – Notes from the Underground Expect Chinese businesses' use of corporate infiltration and disruption attacks against competitors to increase.	**CS**: Foreign enterprises doing business in China must expect almost overt cyber attack and penetrations schemes from competitors.
Cyber Crime – Notes from the Underground Expect Middle Eastern cyber cartels to conduct more fraud operations	**LE**: Increased necessity for law enforcement to understand and respond to nodes of these cartels in the US **CS**: The set of potential attackers that target financial institutions will grow larger

Cyber Crime – Notes from the Underground Expect more member only carding forums	**LE**: Less-effective discovery **CS**: Less-successful credential recovery.
Cyber Crime – Notes from the Underground Expect to see more schemes focusing on commercial accounts globally in 2009.	**LE**: Cooperation with foreign law enforcement becomes more necessary **CS**: Global business operations are now potential targets; not just the US. **CS**: Increased losses
Cyber Crime – Notes from the Underground Expect to see more use of fast-flux networks	**LE**: Traceback operations will be less effective **CS**: Current phishing takedown measures will be less effective
Cyber Crime – Notes from the Underground Expect transaction hijacking and 2FA circumvention to appear in malicious code more frequently.	**GI**: Consider incorporating into Computer Network Operations planning **CS**: Increased Losses **CS**: Current fraud detection less effective
Political - Cyber Espionage Expect the People's Republic of China's use of amateur hacking groups to continue, but diminish	**GI**: More unclassified government documents will exfiltrate to the East
Political - Cyber Hacktivism Expect Islamic hackers to use fatwas to justify and bolster their hacking activities with little regard to how far removed these may actually be from the focus of the fatwa.	**LE**: Potentially will bring more young zealots into the hacking fold. **GI**: Potentially will bring more young zealots into the hacking fold.
Political - Cyber Hacktivism Expect militant jihadists to co-opt ostensibly non-militant Middle Eastern hackers to take advantage of their stronger hacking skills.	**LE**: May produce an increase in the skill level of fundamentalist cyber operations. **GI**: May produce an increase in the skill level of fundamentalist cyber operations. **GI**: General Middle Eastern security environment grows more complex.
Political - Cyber War Expect any geopolitical controversy involving Russia to have a cyber warfare component.	**GI**: Consider bolstering defense against DDOS directed at government networks. **CS**: General periodic increases in attacks against some firms in targeted countries
Response - CIP Expect the number of SCADA vulnerabilities to increase.	**CI**: Increased threat to critical infrastructure **GI**: Increased threat to critical infrastructure **LE**: Increased threat to critical infrastructure **CS**: Increased threat to critical infrastructure
Response - CIP Expect to see more Bullet Proof hosting services taken down via the press	**CS**: Current fraud detection less effective as spam flows become more volatile; rogue ISPs move to fast-flux networks **CS**: Creation of many small and dispersed bulletproof hosting services **LE**: May interfere with on-going investigation

Response - Policy Economic Crisis creates conditions for drastic worsening of cyber security	**LE**: Increased workload for personnel and courts **CS**: Decreasing budgets; confusion; more attacks, especially from insiders
Response - Policy Expect continued improvement to US cyber security policy, but little improvement in execution of it	**GI**: Continued incoherence; infighting over budget; lack of solid leadership; misaligned priorities **LE**: Continued incoherence; infighting over budget; lack of solid leadership; misaligned priorities **CS**: Consider exerting pressure on government for private sector to assist **CS**: Expect little tangible help from US government

Risk Graphing Methodology

The preceding predictions and their associated consequences are exhibited graphically in the following risk matrices. Each separate graph pertains to each of the four specific organizational types to which each prediction's consequences apply; one for government intelligence, another for law enforcement, yet another for the commercial sector, and a final one for critical infrastructure. In viewing these graphics, two points should be kept in mind. First, not every graph will contain all predictions because not every prediction implies a consequence for all four of the different organizational types. For example, cyber fraud tactics have consequences for the commercial sector but not so much for intelligence agencies. Second, the likelihood score for any given prediction will be the same on any of the four graphs in which it occurs, because the likelihood of the prediction's occurrence is independent of which targets it impacts. However, the consequence score will vary from graph to graph because each of the four organizational types will experience different consequences from the occurrence of each single prediction. For instance, the perpetuation of fast flux networks means one thing to banks, but something different to police. Beyond these explanatory points, the following graphical representations follow the basic conventions of risk analysis matrices.

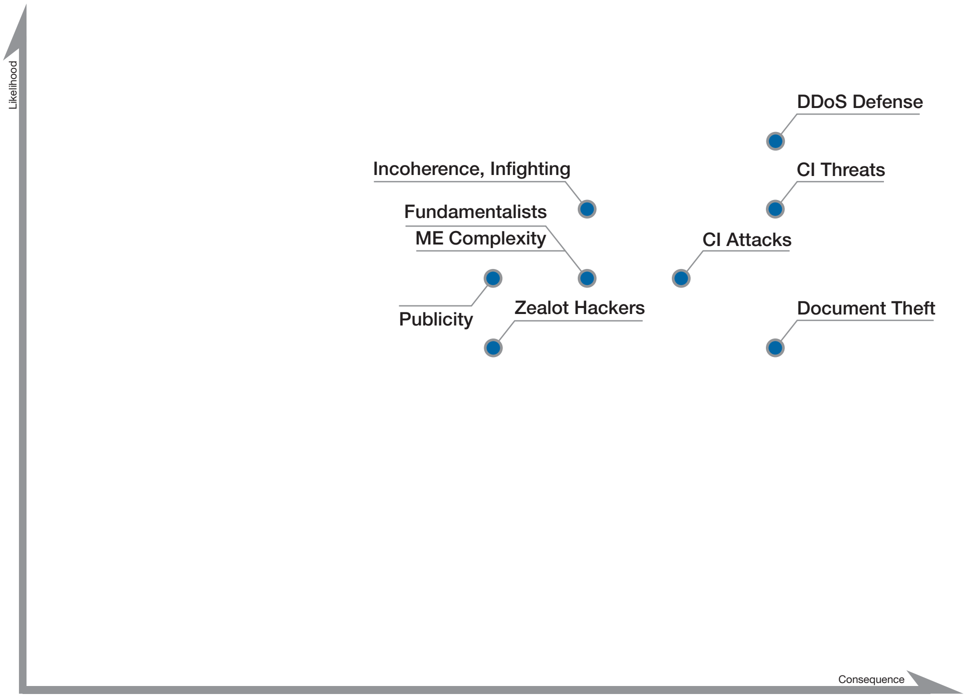
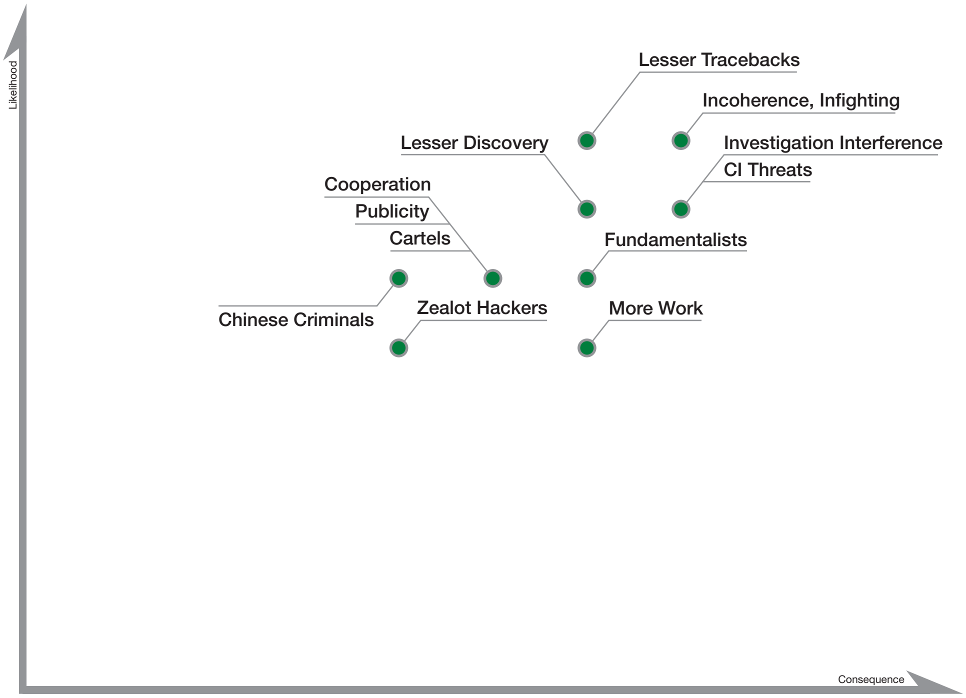
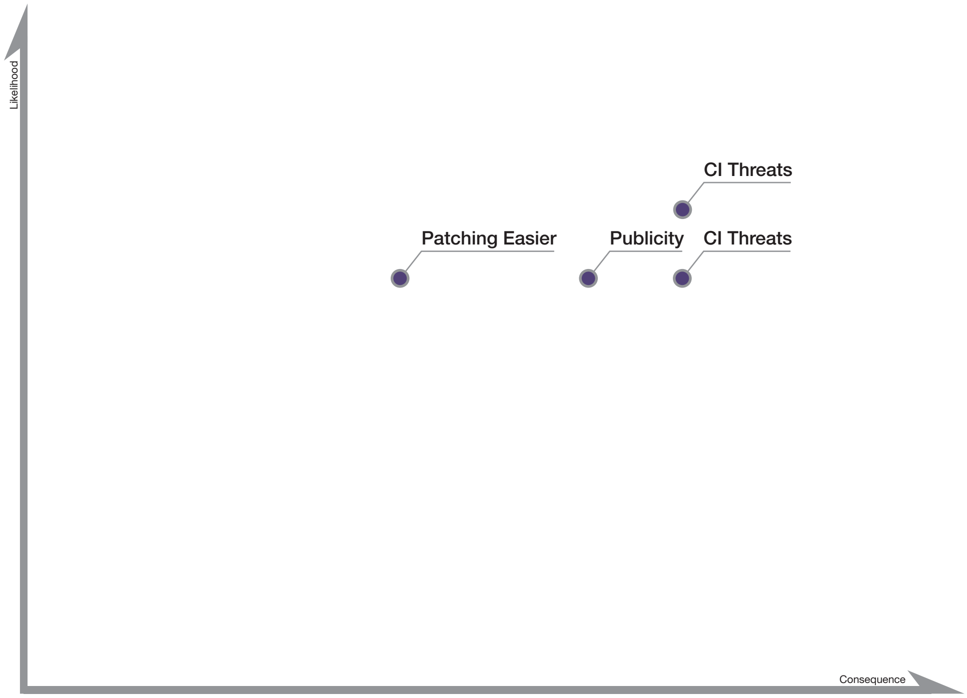


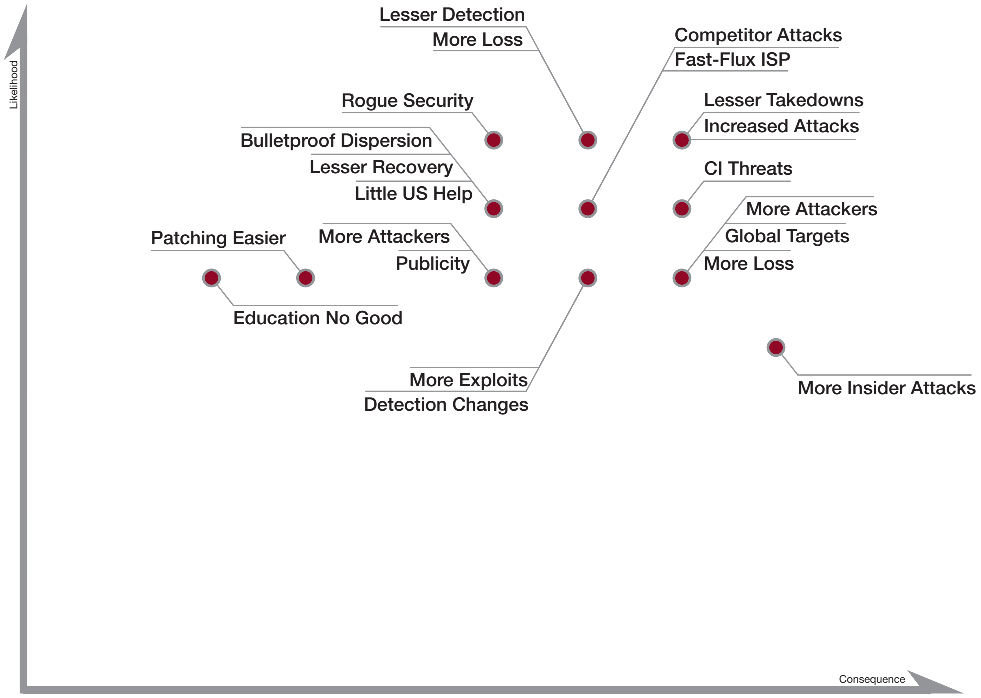
Exhibit 8-3: Risk Matrix of iDefense Predictions for Government Intelligence Organizations



Risk Matrix of iDefense Predictions for Law Enforcement Organizations



Risk Matrix of iDefense Predictions for Critical Infrasturcture Organizations



Risk Matrix of iDefense Predictions for Commercial Sector Organizations

Exhibit 8-3 depicts the results from likelyhood determination and impact analysis for the predicted threats and puts the threat environment for 2009, as iDefense sees it, into perspective. As detailed above, the risk matrix is separated into matrices for the 4 different sectors.

Not all of the predictions provided by iDefense are actually threats. Some of the trends for 2009 may provide an opportunity for certain kinds of organizations to improve their situation, mainly government intelligence agencies and law enforcement. Specifically, law enforcement agencies should consider to follow the money trail when it comes to the expected volume growth in the illegal distribution of rogue security applications. Furthermore, government intelligence agencies should consider exploiting the specific trends within its offensive Computer Network Operations plans:

- Expect Chinese businesses' use of corporate infiltration and disruption attacks against competitors to increase.
- Expect to see more use of fast-flux networks.
- IFrames were so successful in 2008 that it is unlikely that another distribution method will usurp its position in 2009.
- Expect any geopolitical controversy involving Russia to have a cyber warfare component.
- Expect transaction hijacking and two-factor authentication circumvention to appear in malicious code more frequently.
- Expect to see continued growth in volume and innovation in the illegal distribution of rogue security applications.

Going back to the themes discussion introduced at the beginning of this paper, iDefense identified three major topics that reappear throughout the predicted threats and disruptors like a red thread: *tipping point*, infrastructure, and cyber cartels. Gladwell characterizes a tipping point with three traits: "… one, contagiousness; two, the fact that little causes can have big effects; and three, that change happens not gradually but at one dramatic moment …"[84]

In each area of the cyber security landscape, iDefense can point to discrete events that completely changed the environment. The dramatic moment for cyber war came in 2007 when Russian sympathizers took down Estonian networks with nothing more than a DDoS attack. For cyber espionage, the moment came in 1999 when two Chinese colonels published a book called *Unrestricted Warfare*.[85] The PLA has been following that philosophy of Asymmetric War ever since. For Cyber hacktivism, the event came in February 2006 when pro-Muslim hackers launched a withering cyber attack against websites that hosted a cartoon of the Islamic prophet Mohammed. For cyber terrorism, the milestone came just last year, when religious leaders at various levels issued fatwas justified the use of cyber attacks to support the Islamic agenda. Nevertheless, the one dramatic moment that impacted everything,

[84] "The Tipping Point: How Little Things Can Make a Big Difference", Gladwell, p9, 2000.

[85] Footnote 85: iDefense Topical Research Report *An Analysis of Chinese Cyber Espionage,* ID# 464562 , Oct. 10, 2007

the event that caused the tipping point more than any other, was the moment that also propelled advances in cyber crime. That moment came with the aggregation of compromised computers into cohesive units, known commonly as botnets.

Everything that is serious and dangerous about the Internet today can be traced back to the first use of these ingenious automatons, the backbone *infrastructure* od cyber crime. Botnets are a free resource, anonymous and infinitely scalable. They allow the *cyber cartels* to build infrastructure that facilitates their movement within the white noise created by the flotsam and jetsam of Internet traffic. They are the essential tool that has propelled the cyber security landscape on its current trajectory, past the tipping point, and into a much more portentous state.

We are now approaching a crossroads. Either malicious activity continues to flourish online, or law enforcement begins to get the upper hand. Now, both scenarios are equally likely with competing evidence supporting each. As indicated by the events referenced in this document, malicious use of cyber space is now past a tipping point, and failure to contain its growth in the short-term will make it exponentially difficult to do so in the long-term. In developed countries, intelligence and law enforcement agencies have accepted the benefits and challenges cyber space poses to them, and they are going head-to-head with state-sponsored and criminal activity. It is even possible that this struggle will characterize the way in which the Internet evolves throughout 2009.

9 Appendices

Appendix A: 2008 iDefense Publications

Global Threat Research Reports:

The Cyber Threat Landscape in the United Arab Emirates
ID# 467325, Feb. 4, 2008
The United Arab Emirates (UAE) is rightfully famous for its rapid development from a loose grouping of fishing villages and Bedouin into a major economic hub. The UAE's role as a regional and international business and trade center attracts millions of workers and billions in investments. Unfortunately, the same attributes also make the UAE a convincing foil for cyber crime.

The Cyber Threat Landscape of Brazil
ID# 469361, May 12, 2008
Unlike its more dynamic counterparts, the cyber threat environment of Brazil is characterized by a highly specialized, ultra-specific focus on fraud conducted via banking Trojans disseminated by sophisticated phishing attacks.

The Cyber Threat Landscape of Russia
ID# 470162, June 16, 2008
This Global Threat Research Report provides contextual, political and economic background research on the Russian Federation's recent history and current affairs. It includes an overview of Russian telecommunications and information technology sectors, Internet penetration and usage trends, and a discussion of those aspects of the Russian regulatory environment pertaining to IT and the cyber landscape as a whole.

The Cyber Threat Landscape in the United Arab Emirates (Update)
ID# 471047, Aug. 1, 2008
The United Arab Emirates (UAE) is rightfully famous for its rapid development from a loose grouping of fishing villages and Bedouin into a major economic hub. The UAE's role as a regional and international business and trade center attracts millions of workers and billions in investments. Unfortunately, the same attributes also make the UAE a convincing foil for cyber crime.

The Cyber Threat Landscape of India
ID# 472125, Sept. 4, 2008
This iDefense Global Threat Research Report examines the primary elements that constitute the cyber-threat environment of India and influencing social and economic factors. The overall assessment is that India's economic progress over the past two decades places India on the economic radar of cyber criminals and demonstrates the enormous economic returns available for malicious actors.

The Cyber Threat Landscape of Indonesia
ID# 474375, Nov. 4, 2008
The defining characteristics of Indonesia's information security environment are its relative lack of socio-economic development and its poised potential for rapid, beneficial enhancement. Although Indonesia lags behind its "Asian Tiger" neighbors in most socio-economic and IT-security indicators, many of

the most important elements that underpin development are in place or, with outside assistance, can soon become as such.

The Cyber Threat Landscape of China
ID# 476126, Nov. 24, 2008
China is a vast country where statistics and figures on various facets are staggering by any measure or standard that is applied. These facets range from the number of spoken Chinese dialects, the variety of regional cuisines, ethnic groups and subgroups, and of course the population figures.

The Cyber Threat Landscape of Saudi Arabia
ID# 476549, Nov. 28, 2008
Saudi Arabia is a challenging but potentially rewarding place to do business. After first providing an overview of the telecommunications and information technology (IT) environment, the IT and IT security-related aspects of the Saudi legal system, and an overview of the socio-political situation from an IT security perspective, this report will explore some aspects of doing business in Saudi Arabia, especially from regulatory, cyber crime and cyber security points of view.

Topical Research Reports:

Banking Trojans - An Overview
ID# 467292, Jan. 31, 2008
This report aims to familiarize readers with different Trojans, techniques and the toolkits that use them. Although iDefense examines toolkits to show the ease with which malicious actors can use Trojans in their attacks, this is not the sole purpose of this report. It is instead to impart knowledge of the overall landscape of banking Trojans, so organizations can make specific decisions and create mitigation strategies to combat the threat from banking Trojans.

Silentbanker Unmuted - An In-Depth Examination of the Silentbanker Trojan Horse
ID# 467374, Feb. 7, 2008
Silentbanker's primary threat comes not from its features, which are reminiscent to that of nearly a dozen other banking Trojan families, but rather from the overall threat of the attackers responsible for it. iDefense has attributed every attack since May to the same group of attackers, meaning this Trojan is not likely a free-standing toolkit for resale.

The Russian Business Network: Rise and Fall of a Criminal ISP
ID# 467712, March 3, 2008
The saga of the Russian Business Network (RBN) is that of a small-scale operation that grew into "the baddest of the bad" Internet service provider (ISP), and then experienced a sudden disintegration. This is not to say that RBN's leadership or the organization's clients also disintegrated; instead, its ability to function so brazenly obstructed, RBN continued operations along the newer business model of diffuse operations across multiple, often nominally legal, Internet service providers.

IFrame Attacks - An Examination of the Business of IFrame Exploitation
ID# 468235, March 28, 2008
When users open a Web page with Internet Explorer, Firefox or any other Web browser, they only notice the page they typed in the address bar. Regular users rarely realize that, to resolve some pages completely, their computers must connect to other, often unknown websites. Few users are aware of these in-line frames, or "IFrames," since they are transparent to everyday users.

Risk of Search and Confiscation of IT Devices by Chinese and US Government Officials
ID# 468306, March 31, 2008
Current law affords complete authority for customs officials in the US and the People's Republic of China to search the laptops of foreigners, and indeed US and Chinese citizens, respectively, traveling throughout or working within that country. In principle, encryption should not deter the officials of either country, who are empowered to demand the unlocking of encrypted files or segments of the hard drive; they can also hold the laptop until its owner unlocks the encrypted information or until state resources become available to crack it.

A Nodal Analysis of Islamic Extremist Websites
ID# 469291, May 9, 2008
Since the beginning of the twenty-first century, the use of Internet technology by Islamic extremist-oriented terrorists to further their ideological and political goals has expanded greatly, in many ways mirroring the drastic expansion of worldwide Internet usage itself. A number of trends in the worldwide Islamic extremist-oriented terrorist movement and its evolving Internet presence are increasingly attracting the attention of iDefense analysts.

BBB - An Analysis of Targeted Spear-Phishing Attacks
ID# 471185, Aug. 8, 2008
Since February 2007, more than 65 waves of highly targeted e-mail fraud attacks have attempted to compromise worldwide corporations and financial institutions; these attacks, called "spear phishing" or "whaling," use trickery and trust to convince users to click a link, which installs malicious code on their computer.

Tracking and Detecting Trojan Command-and-Control (C&C) Servers
ID# 472109, Sept. 11, 2008
Information-stealing Trojan horse programs quietly infect systems, capture valuable information and transmit it back to a central command-and-control (C&C) server. While some attackers create custom Trojans for specific purposes, less-technical criminals use simple toolkits to create binaries for their own use. These toolkits generate slight variations on a single Trojan that report to different C&C servers, but use the same mechanisms to capture and report data.

Taking Virtual Worlds Seriously: Implications to the Intelligence and Law Enforcement Communities
ID# 475258, Nov. 14, 2008
Given the anticipated pervasiveness of multi-user online environments (MOEs), intelligence and law enforcement communities (ILECs) worldwide should now spend some portion of their resource budget to monitor, track and understand

how these MOEs progress over the next 15 years and to actively engage in these environments in preparation for future missions.

Common Tactics for Committing Cyber Fraud
ID# 476124, Nov. 24, 2008
Credit card fraud has long been a problem for consumers, merchants and banks. Consumers are targeted with increasing frequency and the scale of merchant breaches is also rising. Financial institutions around the world are concerned with the current level of fraud and the costs to their bottom line, though most points of compromise are beyond their control.

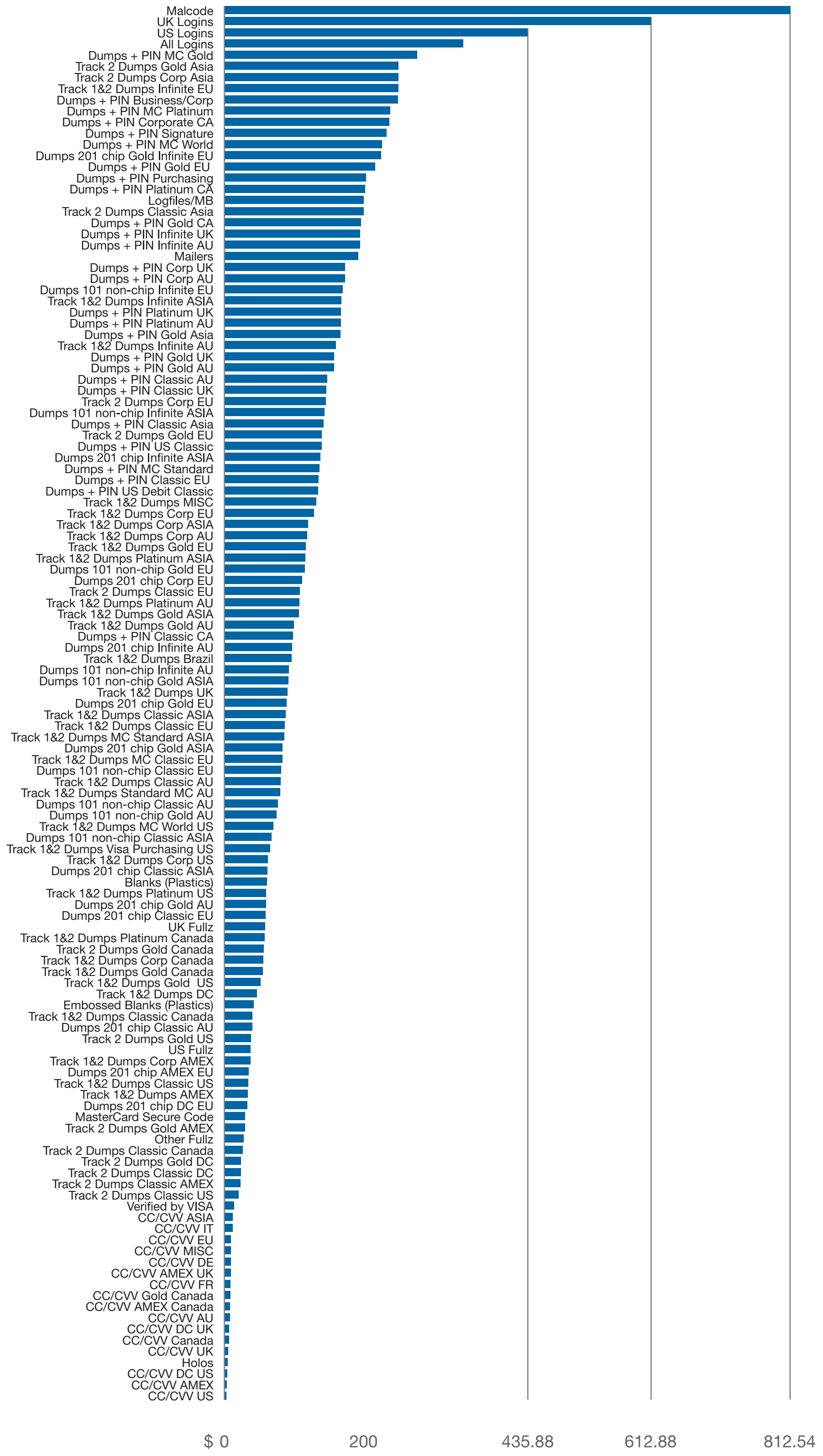
Mobile Security
ID# 477465, Nov. 24, 2008
This report details the weaknesses that have allowed mobile malicious code to spread in the past, how attackers may abuse these systems in the future and what organizations can do to protect mobile users. The introduction of a diversity of mobile payment systems and traditional threats applied to mobile devices makes such devices attractive targets for hackers.

General Focused Intel Topics – 2008:

Following are just some of the Focused Intelligence topics that iDefense customers requested in 2008:

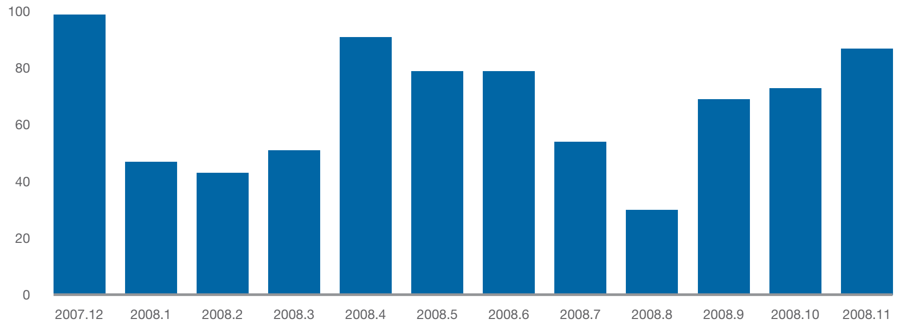
- Open-Source Software
- Security Standards
- Virtual Worlds
- India Outsourcing
- Two-Factor Authentication
- VoIP Security
- Buffer Overflow Protection
- Data Execution Prevention
- Chinese Threats to Financial Institutions
- Application Security Best Practices
- 2008 Olympics Threats
- Prague
- Budapest
- Southern Africa
- Poland
- India
- Indonesia
- Hong Kong
- Taiwan
- Saudi Arabia
- Chinese Hacker Community
- IFrames
- Phishing
- Fast-Flux Phishing
- DDoS Attacks
- Credit Card Fraud (“Carding”)

Appendix B: Underground Carding Statistics

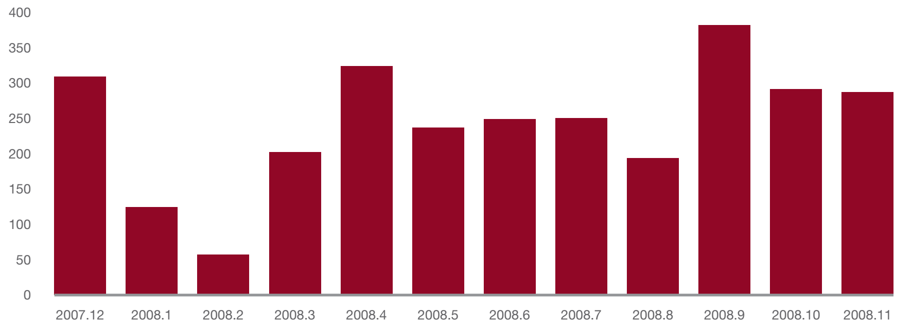


Average Going Rate for Select Illicit Goods in the Cyber Fraud Underground

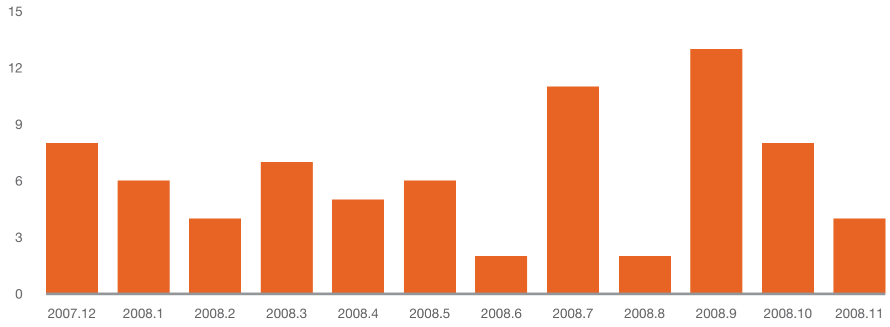
Appendix C: Malicious Code Statistics



Worms in the Last 12 Months



Trojan Horses in the Last 12 Months



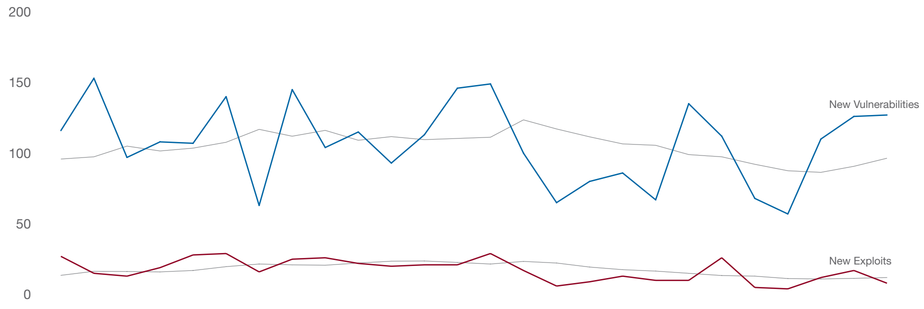
Viruses in the Last 12 Months

Appendix D: Vulnerability Statistics

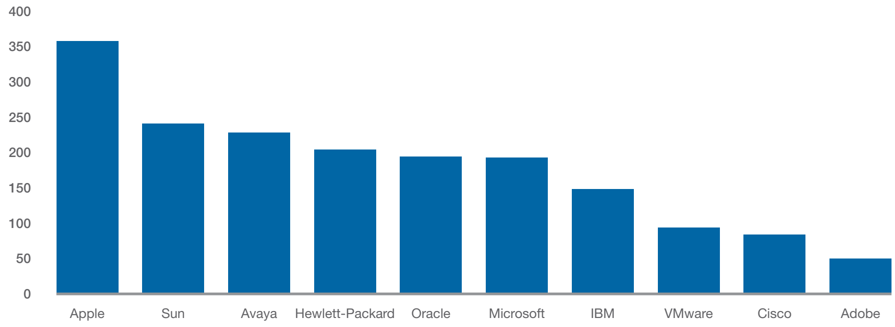
Microsoft SIR Report

Microsoft Product	Product Version	CVE ID#	# Exploits Verified	# Exploits (!Verified)	Avg # of days for Exploit	% of Verified Exploit to Security Bulletin	% of Exploits to Security Bulletins
IE	5	1	0	0			
	5.01	6	0	0			
	6	10	1	0		10%	10%
	7	10	0	2			20%
Office	2000	18	0	0			
	XP	17	1	1		5.88%	11.76%
	2003	16	2	1		12.50%	18.75%
	X-Mac	0	0	0			
	2004-Mac	12	0	0			
	2007	8	0	0			
	2008-Mac	5	0	0			
Windows	98	0	0	0			
	ME	0	0	0			
	2000	13	2	2		15.38%	30.77%
	XP	19	0	2		5.56%	10.53%
	2003	18	1	3			22.22%
	Windows Vista	14	0	1			7.14%
	2008	8	0	0			
Others	Live OneCare	2	0	0			
	Antigen for Exchange	2	0	0			
	Antigen for SMTP	2	0	0			
	Windows Defender	2	0	0			
	Forefront Client Security	2	0	0			
	Forefront Security for Exchange	2	0	0			
	Forefront Security for Sharepoint	2	0	0			
	Standalone System Sweeper	2	0	0			
	Visual Basic 6 SP6	5	0	4			80.00%
	Active Directory	2	0	0			
	ADAM	2	0	0			

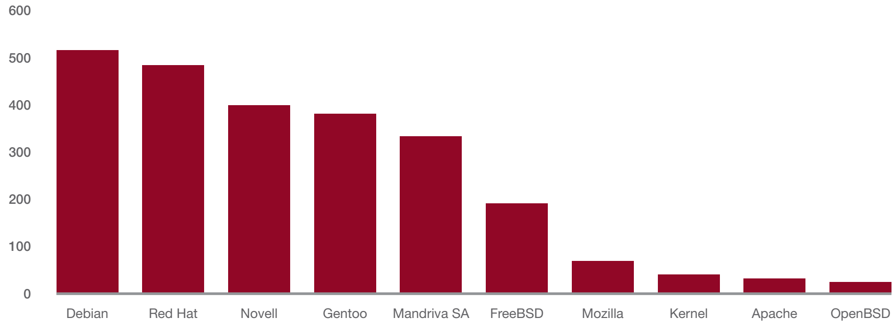
Microsoft Product	Product Version	CVE ID#	# Exploits Verified	# Exploits (!Verified)	Avg # of days for Exploit	% of Verified Exploit to Security Bulletin	% of Exploits to Security Bulletins
	IIS 5	1	0	0			
	IIS 5.1	2	0	0			
	IIS 6	2	0	0			
	IIS 7	1	0	0			
	Works 6 File Converter	3	1	0		33.33%	33.33%
	Visual Studio .NET 2k2 SP1	2	0	0			
	Visual Studio .NET 2003 SP1	2	0	0			
	BizTalk Server 2000	2	0	0			
	BizTalk Server 2002	2	0	0			
	Commerce Server 2000	2	0	0			
	Internet Security and Acceleration Server 2000 SP2	2	0	0			
	Project 2000 SR1	1	0	0			
	Project 2002 SP1	1	0	0			
	Project 2003 SP2	1	0	0			
	Visio 2002 SP2	2	0	0			
	Visio 2003 SP2/SP3	2	0	0			
	Visio 2007 & SP1	2	0	0			
	AD LDS	1	0	0			
	SharePoint Services 2.0	1	0	1			100.00%
	Works 7	1	0	0			
	Windows Live Mail	1	0	0			
	Windows CE	1	0	0			
	Exchange Server 5.0	1	0	0			
	Visual Studio 6	1	0	0			
	Windows Installer	1	0	0			
Total		238	8	17		3.36%	10.50%



2008 Vulnerability and Exploit Trend

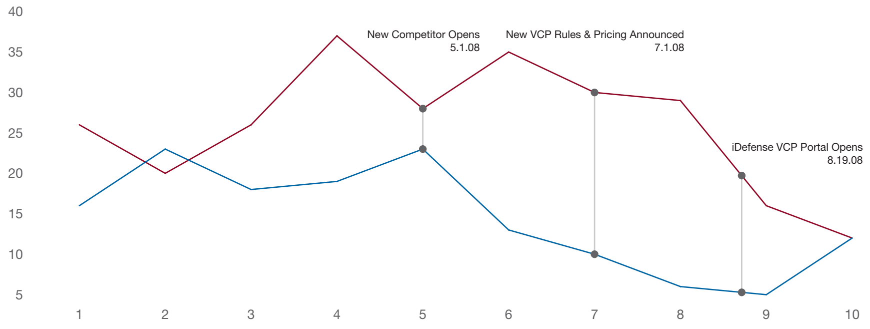


Top 10 Closed Source Vendors by Vulnerability Count

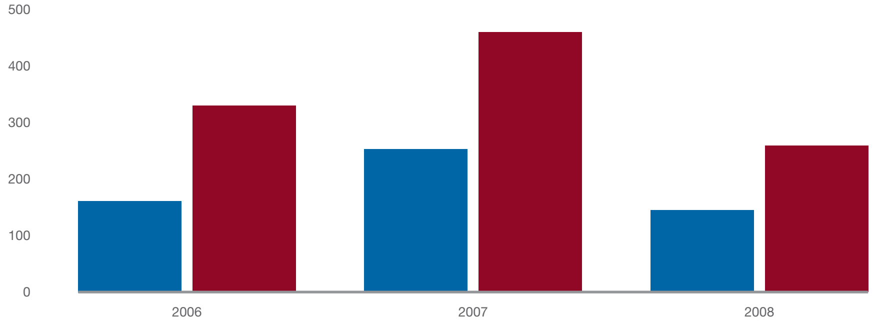


Top 10 Open Source Vendors by Vulnerability Count

Appendix E: Labs Statistics



2008 Accepted and Rejected Vulnerability Contributor Program (VCP) Submissions



Accepted and Rejected Vulnerability Contributor Program (VCP) Submissions, 2006-2008