Executive Brief

# The Next Generation of Cybercrime:

## *How it's evolved, where it's going*

SecureWorks®

secureworks.com

## Table of Contents



## About SecureWorks

SecureWorks is exclusively focused on protecting our clients' digital assets against cyberthreats. We do that with intelligent defenses that combine our proprietary technology, global threat visibility and recognized expertise. We are 100 percent focused on information security – it's all we do. That's why we are trusted in 70 countries by more than 2,900 clients, including more than 85 of the Fortune 500. SecureWorks offers a full suite of Managed Security, Threat Intelligence and Security and Risk Consulting services.

***This paper provides an executive-level primer on cybercrime by covering key profiles of cybercriminals, their methods and their motivations. After reading this Executive Brief, a business leader will understand the nature of the cybercrime threat.***

## Executive Summary

Cybercrime and cybercriminals have been around since businesses first began using the Internet for commerce. The rate of cybercrime and its cost to businesses have increased dramatically over time, transforming cybercrime from a minor inconvenience to a significant risk that must be appropriately managed.

News reports of large-scale data breaches at brand name companies are more frequent than ever. According to a study conducted by the Ponemon Institute, the average cost of a data breach in 2009 was $6.75 million. From the same study, the most expensive reported breach in 2009 cost one organization nearly $31 million.

Clearly, organizations must take strong steps to protect their IT assets from cybercriminals. Cybercrime is pervasive - today's businesses are constantly being probed and attacked by cybercriminals searching for sensitive data and system weaknesses. It is critical that business leaders in a position to drive positive security change understand the risks posed by cybercrime.

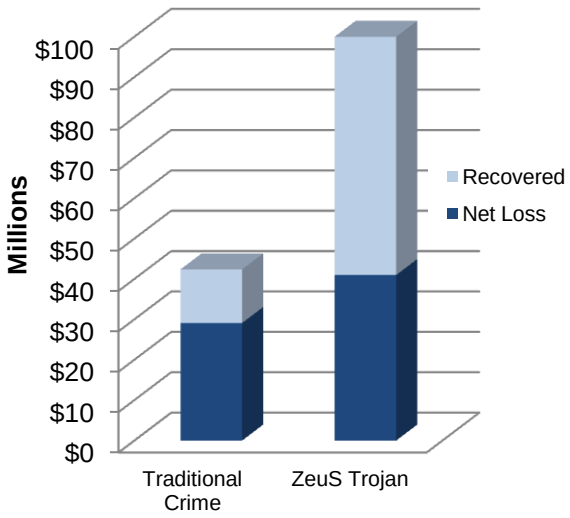
This Executive Brief sheds light on the risk of cybercrime by profiling several "generations" of cybercriminals over time, and pointing out how the criminals, their methods and motivations have evolved. The common adage, "know your adversary," is as true for cybercrime as it is for warfare. By understanding the motivations and methods of cybercriminals, business leaders can better gauge risk and take decisive actions to protect their organizations.

***The average cost of a data breach was $6.75 million in 2009.***

***The most expensive reported breach in 2009 cost nearly $31 million.***

*Source:*
*2009 Annual Study: Cost of a Data Breach*
*Ponemon Institute*

***Losses due to a single cyber threat***




*Source:*
*ZeuS Working Group*

## A Note on the Early Days of Hacking

Hacking has existed for as long as there have been computer systems and networks to abuse. Early cases of hacking predate the turn of the 20th century, when several people were caught abusing fledgling phone networks in the U.S. It was not until the late 1990s that hacking for the purposes of cybercrime exposed businesses to significant risk.

## The First Generation of Cybercriminals

***"Why did I do it? To prove that I could."***

The first generation of cybercrime activity was characterized by rapidly-propagating worms that exploited widespread vulnerabilities. The high-impact threats of this generation included worms such as Blaster, CHI (Chernobyl), NetSky and Sasser, which collectively disrupted millions of computers worldwide.

The motivations for these attacks were notoriety and ego. The three malware authors responsible for the worms mentioned above were all students at the time and financial gain was clearly not a goal. These attacks were meant to be disruptive and make their presence known by causing indiscriminate damage to any vulnerable computer on the Internet – which is what they did. For first generation cybercriminals, the No. 1 priority was getting noticed. However, this made it easy for security researchers and law enforcement authorities to identify and arrest the culprits.

***Sven Jaschan, author of the NetSky and Sasser worms that wreaked havoc in the spring of 2004. He was arrested the same year by German police following a three-month international investigation.***

## The Second Generation of Cybercriminals

***"Show me the money!"***

The distinguishing feature of second generation cyber-criminals was profit motive. The realization that hacking could easily be used for monetary gain swelled the ranks of the cybercriminal world with hackers looking to cash in.

Botnets -- large networks of infected computers -- became the preferred weapon for cybercriminals, allowing them to pump out millions of spam emails and execute Distributed Denial of Service (DDoS) attacks on businesses. Although the tools used by this generation were more sophisticated than the tactics of their predecessors, these cybercriminals did little to cover their tracks and evade detection.

***Jeanson James Ancheta, owner of the Rxbot botnet that controlled approximately 400,000 infected computers. He was arrested in late 2005 in an elaborate FBI sting operation.***

## The Third Generation of Cyber-criminals

***"Cybercrime goes big time"***

Two distinctions marked the third generation of cybercriminals: organization and discretion. Cybercriminals matured, recognizing the value of working together for ill-gotten gains while setting their sights on larger, more lucrative targets. The methods – worms, Trojans, DDoS, botnets, etc. – were the same as previous generation, but the execution reflected the influence of more traditional criminal enterprises.

Hacker groups had been around for years, seeking power and influence throughout underground hacking communities. However, this new wave of cybergangs had one purpose: profit. For these gangs, cybercrime was just a means to an end – an easier way to extort and conduct fraud.

This generation targeted businesses handling large sums of money, such as financial institutions and gambling services. In October 2003, U.K. bookmakers were extorted by a cybergang using DDoS attacks to shut down their operations. Total losses were estimated at $3M (£2.2M).

In perhaps the largest attempted heist at the time, a cybercriminal worked with insiders at the London branch of Japan's Sumitomo Mitsui Bank to plant a Trojan in the bank's network. He then used the Trojan to steal credentials and attempt to transfer nearly $300M (£220M) to accounts he controlled around the world.

The cybercriminals in both these cases were eventually arrested, but not before causing significant damage and financial loss to their victims.

***Maria Zarubina and Timur Arutchev were part of a Russian cybercrime gang which attacked a number of British bookmakers, resulting in approximately $3M in losses.***

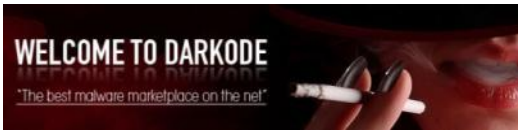
***Yaron Bolondi used a Trojan and help from bank insiders to attempt the theft of £220M from the London branch of Japan's Sumitomo Mitsui Bank.***

## The Fourth Generation of Cybercriminals

***"Want to buy an exploit kit?"***

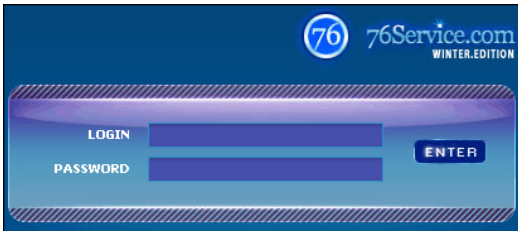
The rise of criminal-to-criminal activity distinguished the fourth generation of cybercriminals. A robust and efficient underground economy emerged, providing the opportunity for cybercriminals to buy and sell goods and services to each other. Distinct, specialized cybercrime businesses came into prominence, including:

- **Exploit Auction Houses**, such as WabiSabiLabi, that provide a marketplace where cybercriminals buy and sell exploit code – including exploits for software vulnerabilities not publicly known.
- **Malware Distribution Services**, such as IFRAMES.BIZ, specialize in pushing out malware to infect thousands of hosts. These services typically have an established distribution medium, such as a network of compromised websites or infected online ads, they use to quickly infect large numbers of computers.
- **Botnet Rentals**, such as 5Socks.net, maintain one or more botnets that are hired out to other cybercriminals. The rented botnets can be used to send spam, host illegitimate sites, steal sensitive information, execute DDoS attacks and conduct many other criminal activities.
- **Next Generation Identity Sellers**, such as 76Service.com, brought buying and selling stolen identity data to a new level. These new services gave cybercriminals an online platform for buying, selling and managing a portfolio of stolen records – taking cues from online stock trading platforms to help the hackers maximize their "investments."
- **Licensed Malware**, such as the Storm Worm, became prevalent in this generation. Malware authors adopted licensing models, forcing other cybercriminals to pay for their malware. This provided more funding for malware authors, and enabled other cybercriminals to quickly purchase high-end malware instead of having to develop it themselves.




***Sites such as dark0de serve as markets for buying and selling malware.***


***Malware Distribution Services, like the full-service "pay-per-install" site installconverter.com, specialize in pushing out malware and infecting thousands of computers in a short amount of time.***



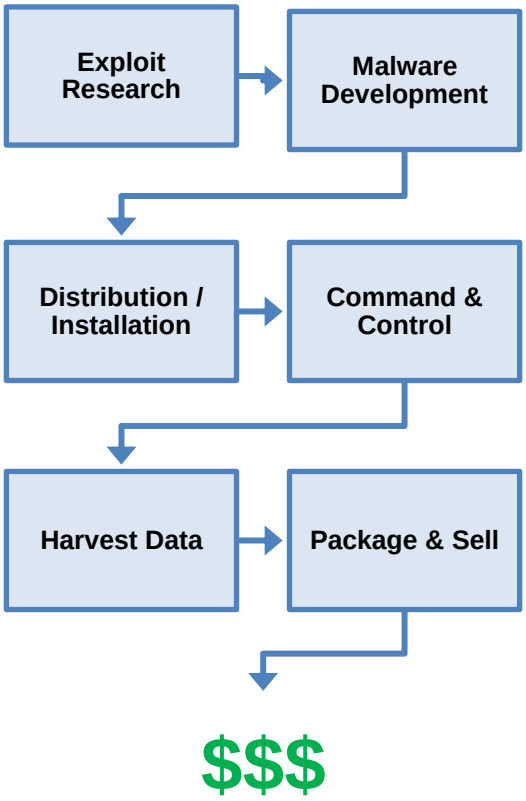

***76Service.com is one of many cybercriminal websites designed for buying, selling and managing portfolios of stolen identity data.***

- **Social Networks for Cybercriminals** also emerged, with sites providing reputational rankings of buyers, sellers and partners in the cybercrime marketplace. This included "trusted" entities performing escrow functions when one or more "untrusted" parties are involved in a cybercrime operation.

As the cybercrime economy matured, it brought cybercriminals the benefits of specialization and distributed risk. Cybercriminals talented in finding new vulnerabilities and writing exploits could specialize in that area and easily fund their work by selling their exploits. The same dynamic applied to malware authors, distributors, botnet owners, and others in the cybercrime supply chain. As a result of this specialization, the sophistication of cyberattacks increased across the board and everything sped up.

With greater specialization and distribution of functions, cybercriminals were able to distribute the risk of getting caught. For example, malware authors no longer had to steal data and conduct fraud to make money – they could sell their malware for profit without engaging in higher risk activities. This also made it more difficult for authorities to track and prosecute all of those involved in cybercrime operations.

***Specialists developed for every function in the cybercrime supply chain***



## The Current Generation of Cybercriminals

***"How can I serve you malware today?"***

Moving beyond the fourth generation – to the present --- cybercriminals today are continuing to refine and fine-tune each element of the cybercrime supply chain. The current batch of successful cybercriminals are more entrepreneurial and business-savvy than past generations, fueling the growing cybercrime economy with cash. As a result, attacks continue to grow in sophistication and frequency.

### Next Gen Pay-Per-Install

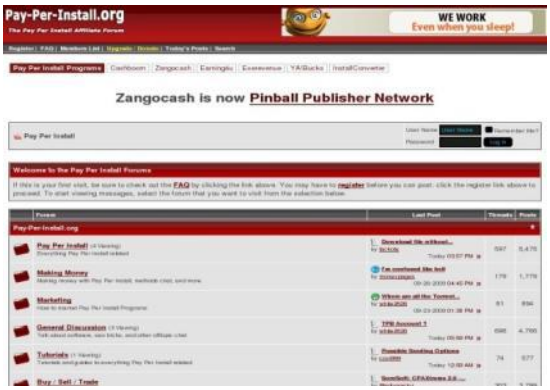
Pay-Per-Install (PPI) malware distribution schemes have been a key area of growth. The business model for these scams has matured into a system in which a single PPI site may partner with thousands of "affiliates" who distribute malware. These affiliates are paid based on the number of malware installs they produce, with typical affiliates reporting more than 10,000 installs a month. A PPI scam with a thousand affiliates can easily infect millions of systems every month.

PPI sites are now taking steps to improve the productivity of their affiliates. Some sites offer help developing content for affiliate scams. Many provide guidance or tutorials on how to make their malware less detectable by antivirus software, or "FUD" (Fully Un-Detectable). Even live support is available for affiliates of certain PPI sites.

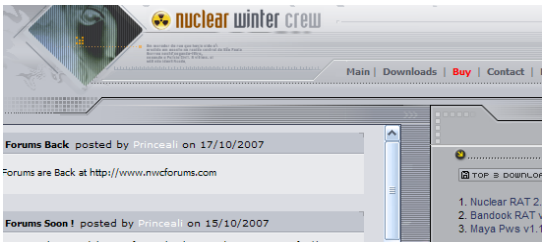
A key player in the PPI cybercrime business is Pay-Per-Install.org. While this site has set up affiliate programs, it primarily serves as a forum and marketplace where cybercriminals can discuss which PPI programs are yielding the highest profits. The Pay-Per-Install organization gets referral bonuses from other affiliate programs and provides a full range of help guides and tutorials.

### Malware Tech Support

Building on the previous generation's trend of licensed malware, today's malware is increasingly commercialized. Malware kits now include tech support for paying cybercriminals to help them better utilize the tools. Of course, most malware authors sell their tools with a disclaimer that they should be used for "research only."




***Pay-Per-Install.org is a forum and marketplace for the PPI business where cybercriminals discuss the best "affiliate" PPI programs and how to make money installing malware.***




***Nuclear RAT and Bondook RAT malware tools have been used in both the Better Business Bureau (BBB) and Internal Revenue Service (IRS) targeted email scams. Developed by the Nuclear Winter Crew, the tools boast a long list of features, English interfaces and support forums.***

There are few legal consequences for selling malware – as long as the author does not use the malware himself to compromise a computer, it is generally ***not*** illegal. Most malware authors also operate in countries that shield them from civil actions, removing that risk as well. This allows malware authors to provide instructions, support forums and other technical support for their "product." In turn, this lets them sell their malware to any cybercriminal willing to pay – not just those savvy enough to operate it without guidance. As a result, they can sell their malware to a larger market and make more money.

## "Point-and-Click" Cybercrime

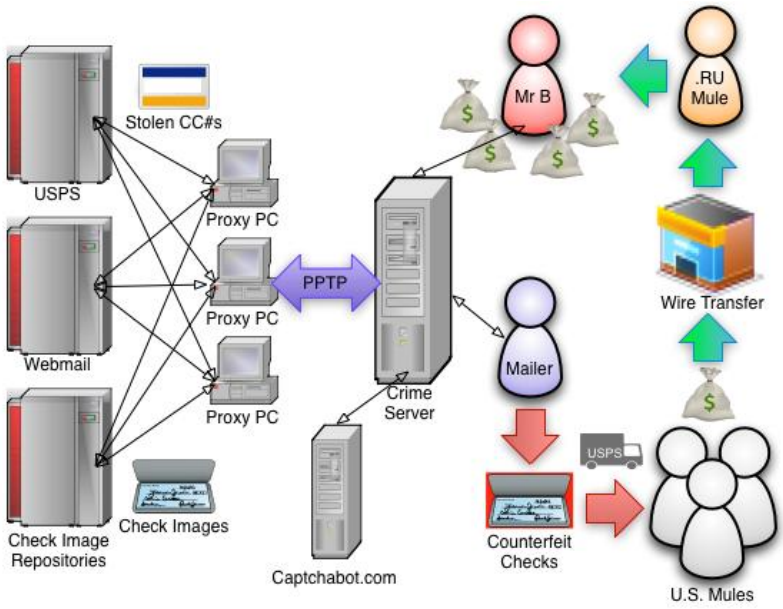
Threats in the current generation are increasingly automated, allowing cybercriminals to be more productive in less time. Cybercriminals take advantage of malware tools and scripting techniques to automate various stages of their schemes.

Less skilled hackers can purchase tools to easily identify vulnerable targets, compromise systems and steal data. More sophisticated cybercriminals may buy tools or develop custom tools and scripts on their own. In some cases, integration across multiple tool sets that perform distinct functions has been observed in larger cybercrime schemes.

An investigation into a check counterfeiting ring known as BigBoss revealed a highly automated system for check fraud that encompassed:

- Creating a botnet
- Stealing credentials to online services, especially check image archival services
- Stealing check images from these services
- Printing counterfeit checks using commercial-grade check printing software
- Scraping job websites to find job-seeker email addresses
- Spamming those addresses to recruit "money mules" to cash the forged checks

***"BigBoss" Check Counterfeiting Operation***




***The BigBoss cybercrime ring uses a highly automated system to steal digital check images and commit large-scale check fraud. In the last year, it is estimated that this group printed more than $9M worth of counterfeit checks of small amounts less than $3,000.***

- Recruiting “money mules” to cash the checks and wire the funds to the cybercriminals’ accounts.
- Shipping forged checks to the mules

The high degree of automation allowed the BigBoss ring to operate at a much larger scale. The forged checks were always for an amount below $3,000 to avoid holds that are usually placed on larger check deposits, yet it is estimated that the BigBoss crime ring printed more than $9M worth of counterfeited checks in the last year.

## APT: Advanced Persistent Threats

The term Advanced Persistent Threat, or APT in short, became prominent in 2010 as a name for targeted attacks on specific organizations by determined, well-coordinated cybercriminals. In the cybersecurity community, APT most often refers to sophisticated attacks aimed at governments and corporations to gather intelligence or achieve specific nonfinancial objectives.

APTs are frequently attributed to nation-states or agents of nation-states. On some occasions, APTs have been linked to terrorist and fringe political groups.

The most recent high-profile APT cyber-attack was “Operation Aurora,” which targeted Google and several other organizations. The attacks were sourced to China and used a combination of sophisticated reconnaissance and targeting, advanced Zero-Day exploits, commercial malware and custom-developed malware. The intent of the attacks was to gain access to enterprise and government networks, create a multipurpose botnet and carry out cyber-espionage.

APTs are not unique to the current generation of cybercriminals; these kinds of threats have been active for years, executing operations such as “Titan Rain” to gather intelligence. However, the skill and sophistication of APTs has evolved along with the cybercrime community, and few organizations are prepared to fend off a highly coordinated and determined attack from an APT.

The New York Times
Expect the World®

Evidence Found for Chinese Attack on Google

By JOHN MARKOFF
Published January 19, 2010

SAN FRANCISCO - Now, by analyzing the software used in the break-ins against Google and dozens of other companies, Joe Stewart, a malware specialist with SecureWorks, a computer security company based in Atlanta, said he determined the main program used in the attack contained a module based on an unusual algorithm from a Chinese technical paper that has been published exclusively on Chinese-language Web sites.

***ADVANCED – using the best methods available to penetrate systems, gather intelligence and evade detection.***

***PERSISTENT – focused on a specific objective and target, not fast financial gain.***

***THREAT – organized, coordinated and sophisticated operations by skilled agents.***

## Recommendations for Business Leaders

Cybercriminals are constantly evolving with changing methods, tools and motivations. The only constant is that tomorrow's cybercriminal will pose a greater threat to businesses than today's. Business leaders must assume that the defenses in place now will not be sufficient next year, and they must be strategic in how they allocate their security resources.

Business leaders should consider these next steps:

- Conduct a comprehensive information security risk assessment. Similar to a classic SWOT business analysis, strategic management of information security risk is based on understanding strengths, weaknesses, opportunities and threats. A full risk assessment should identify the strengths and weaknesses in your security posture, compare them to confirmed and likely threats, and provide prioritized recommendations for reducing risk.

- Investments in security products should be made where necessary to support risk-based information security policy. Simply buying the latest security technologies without strategic direction results in wasted capital and high opportunity costs. Security investments based on policy with organizational acceptance have a much higher likelihood of success and consistently yield better performance.

- Security technology alone is far from sufficient. Expertise, either in-house or via a strategic security partner, is essential to staying ahead of cybercriminals. Mature processes are also key, enabling more effective day-to-day security operations as well as mid-to-long term functional management.

- Most businesses should forego bleeding-edge security technologies unless they are the only viable option available to mitigate high-risk threats. Not only are second- and third-generation products more effective, they are usually less expensive and easier to operate. Businesses should consider cost-effective ways (such as real-time monitoring and management services) to improve the performance of their existing technologies before making large investments in first-generation products.

- Establish a threat intelligence function to monitor trends and emerging threats that impact your business. To compensate for limited visibility across the cyberthreat landscape, leading organizations establish relationships with peers, industry groups, government agencies and vendors to source intelligence.

## Learn More

SecureWorks offers comprehensive information security services to help protect businesses from cyberthreats, including Managed Security Services, Threat Intelligence, and Security and Risk Consulting Services. For more information about information security solutions offered by SecureWorks, please call 877-905-6661 (toll-free), email info@secureworks.com or visit us at www.secureworks.com.