eSafe®

EXTREME CAPACITY. MAXIMUM SECURITY.

Attack Intelligence™ Research Center Annual Threat Report

2008 Overview and 2009 Predictions

Aladdin

SECURING THE GLOBAL VILLAGE

Table of Contents

1. Executive Overview

The Aladdin Annual Threat Report is a compilation of research and trend analysis provided by the Aladdin Attack Intelligence Center (AIRC). This report provides an overview of threats discovered in 2008 along with predictions for the threat evolution in 2009, based on comprehensive research and insights into current vulnerabilities, evolving Web applications, and the maturation and adaptations of the business models of eCrime.

The results of this report can be used by organizations to gain insight into current and evolving threats, and to enable the preparation of security programs for 2009 and beyond.

2. Key Predictions for 2009

eCrime: Now Hiring.

The continued global economic crisis, a real-estate market in free fall, and a challenging job market combine to give the business of eCrime a boost. In 2008 we saw eCrime further develop into a sophisticated business that models a "legitimate" organizational structure and its channels. We see eCrime in 2009 thriving, bringing in more than the "classic" technical employees. eCrime will expand its business model and hiring reach to include the unemployed management level and financial industry professionals.

The browser is your new OS.

In conjunction with the maturation of Web 2.0, we're going to see a substantial change in the online experience as we know it. Google's Chrome is proving that with the right combination of "optimized" Web 2.0 technologies, the browser can evolve into a full-on operating system. With Google's Gears technologies already integrated, we wouldn't be surprised to see an Adobe-Air enabled browser sometime soon that would offer a better Desktop-Web integration. And in 2009, watch for more powerful "OS" browsers from the likes of Microsoft, and be prepared for the security challenges that go along with the continued evolution of the Web.

Identity theft goes social.

With more professionals and businesses using social networking, the "value" of Web identities is soaring. Reconnaissance and business intelligence with tools such as Paterva's Maltego (http://www.paterva.com/web3/products/) has become all too easy, and the sheer amount of public data on sites like Facebook, LinkedIn, Bebo and even MySpace make it easier to impersonate, damage or misrepresent a personal or business identity on the Web. We predict that we will see an increase in the amount of Web identity hijacking, and in response, a serious change in the requirements for validating our identities on the Web.

3. 2008 Year in Review

THE BOTTOM LINE: eCrime business gains major traction against traditional security measures

In 2008 the AIRC saw eCrime continuing to make great strides, proving that the sophisticated business model it has been honing over the past few years continues to outsmart most current security measures. The AIRC has seen numerous instances of traditional security measures, such as signaturing and categorization, not just failing to identify the latest attacks, but actually resulting in a degraded user experience by employing a far too strict policy on web content when trying to cope with a newly discovered form of on-demand malware. Following are the main "events" and milestones during 2008 which signify this growth –from both the technological aspect and the business model aspect as well.

3.1. EVENT #1: The discovery of "MalWeb"

A new "breed" of malware has been discovered by AIRC in 2008. As we saw Web content gaining more potent processing power, traditional malware was targeting this as a weak spot to attack. MalWeb, the delivery of malicious exploits on demand, in the browser, is the natural evolution of malware that has been adapted to the ever-expanding Web 2.0 world. Different from malware, which is created in one place and the distributed in its final form, MalWeb is only "born" when it reaches its victim. Current signature and filtering techniques are not helpful in eradicating it, because it is created only when it is triggered - when "served up" by the browser, which runs it and presents it to user. The unique ingredients of MalWeb come from different sources, so it presents in different form each time, making it one of the most critical security threats organizations face today when it comes to securing perimeters and Internet communications.

The complexity of Web 2.0 has lent MalWeb it's most important capabilities: assuming the same media and form as legitimate code and granting it enough power to take advantage of system-level vulnerabilities, simply by running on Web browsers and their add-ons that are required for modern Web 2.0 functionality.

MalWeb is not constrained by the necessity to compile and package attacks into easy signature files, and, as it is scripted in plain text, it allows the same exploit code for a vulnerability to be expressed in any number of ways. Even after the traditional antivirus programs started signing keywords prone to be used by malware, as well as whole snippets of code, MalWeb found a new home in code obfuscation that scrambled any piece of malicious code into an infinite string of incomprehensible text that would turn back into code at the client and exploit the end user.

3.2. EVENT #2: Recession hits the business of eCrime – they step up their business

The business of eCrime has responded to the economy. It has identified their sagging "sales" and jumpstarted its distribution channels in a successful effort to recruit more victims and improve profitability. Neosploit, a toolkit we thought was long gone, has re-emerged from its hibernation with a new and updated version deploying more advanced management, reporting, and exploitation techniques. Netsploit 3.1 was used on an eCrime server that the AIRC had been investigating, and while digging into the technicalities to see what else could be found behind the attack, a unique window was opened. AIRC had a rare opportunity to look behind the scenes into one of the biggest eCrime operation centers ever discovered.

The server exposed to us the inter-workings of the eCrime business model, mirroring the operating procedures in the form of applications and data, thus leading to a fuller understanding of how eCrime works behind the scenes. We saw communications between eCrime groups, their supply/demand models, attack vectors, credential compromise of legitimate sites, and their botnet creation and management. The tip of the iceberg – the MalWeb itself (Neosploit in this case), was in full view for the AIRC researchers to analyze and deliver to law enforcement.

One of the biggest server credentials' compromise ever (more than 200,000 credentials), and a management system that controlled over half a million Trojans (the Sinowal Trojan research) were only a few of the discoveries AIRC uncovered in this research. This information enabled Aladdin and other security companies and law enforcement agencies to work together to gain a better understanding of eCrime, and provide greater security going forward.

RESEARCHER'S NOTE: This major discovery has marked the era of "predictive security." With this information we are for the first time able to move security measures a step in front of the "bad guys" in order to protect corporations and individuals alike against malicious exploits before they happen.

3.3. EVENT #3: Security gets social.

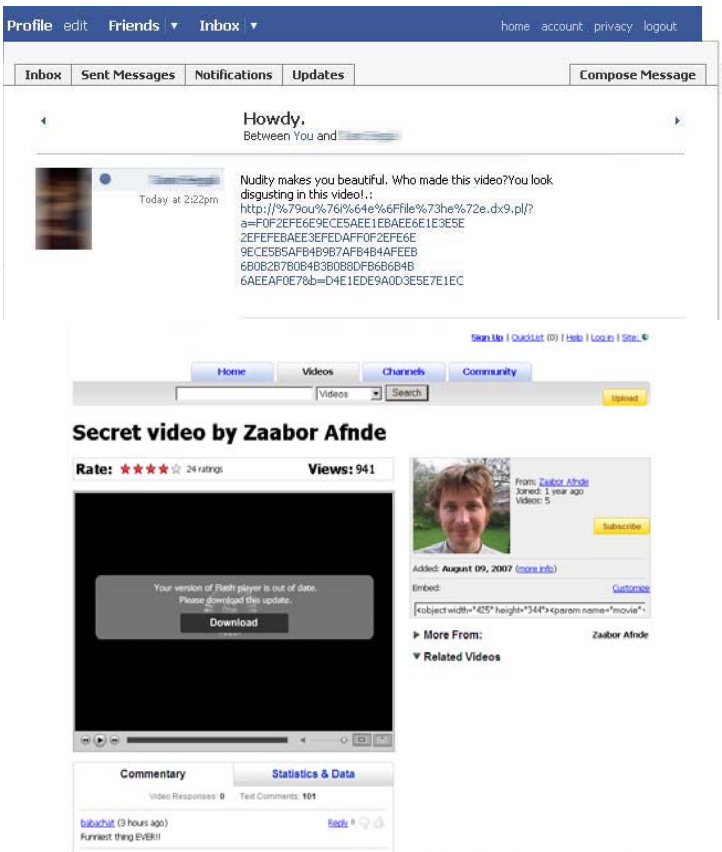
Everyone has been talking about how social networks are a playground for security issues and liability, which was also the case in 2007. eCrime, however, did not just use the socializing aspects of Web2.0 to employ attacks. Instead, it used the social fabric itself and the understanding of Web behavior and site popularity to gain an added advantage in the pursuit of better ROI.

During 2008 we have mapped major events and the associated legitimate sites related to these events, as they have been targeted by eCrime and exploited to attack visitors. Demonstrating the sophistication of the eCrime business, it's been validated that professional marketing principles are being applied by cybercriminals to improve penetration.

Example: Facebook

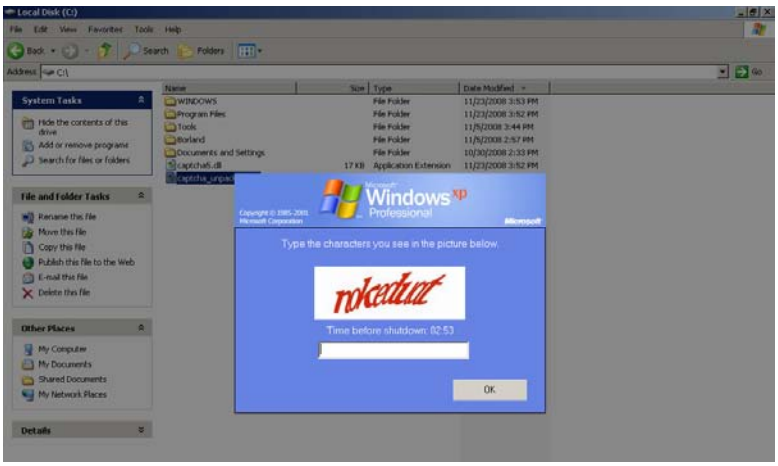
In 2008, we saw worm writers taking advantage of the growing popularity of social networks as a means of distributing their worms. Thousands of Facebook users were infected by a worm called Koobface, which was propagated through Facebook since July 2008.

The worm aimed to install malware with keylogger payload on victim PCs. The worm spread by creating and sending spam messages to the infected users' friends via the Facebook. The sent messages attempted to entice users into clicking on the spammed link. The URL of the link in fact points to a fake YouTube Web page that shows a video player along with what looks like a standard browser message to update your Flash in order to watch the clip. Clicking on the button launches the worm installation.



This attack exploits the user's trust in legitimate hosting providers such as Geocities and Blogger using them as a main redirection point to the fake YouTube pages. In the specific case of Blogger, and in order to randomly create Blogger accounts to be used for the redirections to the malicious domains, the Koobface

variant has been modified to require a little help from the user in reading CAPTCHAs to create accounts for legitimate hosting providers for a later use of attacking other Facebook users.



It's important to note that there are modified variants of the Koobface worm that have been tailored for other social networks such as hi5 and MySpace users.

Example: Antivirus goes Rogue

Another example of using a more "social" approach to generating infected "zombies" that would later turn on their users was the use of fake anti-virus applications to lure users to install them on their systems. 2008 saw considerable growth in the amount of Rogue Antivirus software. Writing and distributing such rogue anti-viruses was done either through spam emails, or by exploits injected into compromised websites.

In addition, writers of rogue antivirus software have built a huge number of websites that attempt to convince users to download their rogue antivirus. These websites convince users that too many viruses have taking over their computer and they need to update.

In general, writes of those rogue software put a tremendous effort behind professional design to lend credibility to their software User Interface. They also distribute the

rogue software under marketing-friendly names, which creates the impression that they are legitimate anti-virus software packages. In some cases, names are almost identical to authentic security software, thus making it difficult for a typical user to distinguish rogue software from legitimate products.

In general, the rogue AV software is very annoying to users. Using Rootkit techniques to avoid detection and removal makes removing a rogue antivirus from an infected system a cumbersome task. The software keeps generating popup alerts and alarming warnings that eventually leave no option for the user except to surrender and buy the full version of the rogue software in hopes that they can get rid of the "alleged" threat.

Example: War and Politics

The last several years has shown that political tensions are usually followed by or preceded by cyber-attacks on targets that can be affiliated with the opposing side. It could even be argued that such attacks may have been part of the governmental efforts in the political arena.

In one example, the political conflict between Georgia and Russia that manifested in a military ground operation was accompanied by cyber-attacks against Georgian government websites. Georgia and security experts accused Russian hackers of launching large, distributed, sustained and almost non-stop denial-of-service attacks on Georgian websites, including those of government ministries and the president's website. The Georgian parliament website, parliament.ge, was defaced and images comparing the Georgian president to Adolf Hitler were placed on its front page.

И кончит он также...

hacked by South Ossetia Hack Crew

Taking it further, in 2008 we saw the "calendar" of security threats align tightly with current affairs. This supports the idea that cybercriminals are continuing to adopt interactive marketing "best practices", taking full advantage of the news and search terms that bring more "customers" into their business. For example, in the United States, the 2008 presidential elections were not only Internet savvy from a candidate campaigning point of view, but also in relation to the malicious eCrime activities surrounding the elections. When Sara Palin's Yahoo email was hacked, cybercriminals piggybacked on the news and attention, distributing an infected version of the leaked images and emails. In another series of incidents, the intensity of the presidential election race between McCain and Obama could be seen not only in the official polls, but also by the ratio of related sites that

were serving up MalWeb. Obama's victory could have been predicted not just by public popularity, but by the sheer number of Obama-related malicious sites.

3.4. EVENT #4: MalWeb does not stop at JavaScript!

MalWeb has started to use the full breadth of technological elements found in Web2.0, including advertisements carrying MalWeb ("Malvertisements"), Flash applications exploited and used as attack vectors, and PDF files carrying additional malicious code, all complement the more traditional "JavaScript-in-a-page" model used earlier in 2008.

Building on the trusted model of kits dating back to 2006, which were perfected and commoditized by mid-2008 (Neosploit being the prime example), new "MalWeb" toolkits have started to include complementary technologies in them such as PDFs in El-Fiesta and ZoPack, Flash and Quicktime in IcePack and AdPack, and many others quickly following suit. We have now come to a point where most of the premium (and part of the freely available) MalWeb Toolkits are offering these more complete attack vectors by default. In 2007, these additional vectors would have been counted as "special" or "custom" additions.

From the other end of the attack vector, we have also watched how Trojan command and control channels have started to turn to the Web as a more reliable alternative to the traditional channels. Sending encrypted data over legitimate channels (HTTP) to legitimate sites which have been set up to capture the data and process it, the model of Trojan 2.0 has started to materialize, causing URL categorization and Web reputation to falter in providing adequate levels of security.

3.5. EVENT #5: It's harvest time for botnets

During 2008, there was significant growth in the amount of botnets, harvesting millions of users to be controlled and joined to perform various attacks. Generally, botnets are used to perform attacks such as sending spam, Denial-of-Service attacks, downloading and installing other Trojans and so on. Botnets are still considered one of the most serious threats on the Internet. The attacks performed by botnets are very effective because they are carried out by thousands of compromised computers.

During 2008, we noticed many new Web-based botnet C&C (Command and Control) servers that make spawning and controlling a new botnet an easy task. These C&C servers have rich functionality and advanced management operations, which allow the hacker to control bots in a productive and effective way.

The Web-based C&C, in contrast with other C&Cs, such as botnets based on IRC channels, have a friendly GUI. The Web-based C&C GUI has multiple sections that provide the botnet herder various options and simplified control:

- Restricting the attacks to specific countries or specific IP addresses ranges, thus making the attacks more targeted
- Assigning tasks for each bot
- Easily obtaining statistics and graphs for the botnet

The simplicity of building such a botnet C&C, in addition to improvements in the ways a herder can execute the botnet, has naturally created growth in the volume seen in 2008.

4. Major Vulnerabilities of 2008

Those who thought that the number of vulnerabilities would significantly drop down in 2008 due to the release of Windows Vista were definitely mistaken. The number of MS vulnerability patches that were released in 2008 was 78, compared to 69 that were published during 2007.

There were several major vulnerabilities that were detected and published in 2008:

MS08-14 – MS Excel Vulnerability

Due to memory corruption error, attackers could exploit this vulnerability to execute arbitrary code. This vulnerability in Excel was used by attackers to propagate Trojans, and the hype of using the exploit was realized in March, 2008, when the exploit was published.

Adobe Flash Player Vulnerability

An integer overflow was discovered in Adobe Flash Player that allowed remote attackers to execute arbitrary code via crafted SWF files. The vulnerability was discovered in April, 2008, and in few days leaked into the wild. A day or two after the vulnerability information was released we began to see reports of many Websites with the malicious SWF installed. Attackers used this vulnerability to install Trojans.

Kaminsky DNS Cache Poisoning Flaw Exploit

In July, 2008, the security world was shaken when the Kaminsky DNS cache poisoning vulnerability was published. The exploit targets a flaw in DNS implementations which allows the insertion of malicious DNS records into the cache of the target nameserver. With this exploit, an attacker could poison major DNS caches, and during standard Web surfing of "trusted" sites users would be taken to malicious websites unknowingly.

MS08-78 IE 0-Day

This new vulnerability was published at the beginning of December, 2008, and is found in IE version 5, 6 and 7, and was given the name "XML exploit." A day after it was published, many sites were discovered with this vulnerability.

5. Looking Forward to 2009

PREDICTION #1: eCrime continues to grow in a down economy

Based on the proven business model and the high ROI that the industry of eCrime has managed for itself as a whole, we expect eCrime to continue growing as a business. This prediction considers current economic factors, cost of labor and their ability to "ride" on the front curve of technology.

In conjunction with the general economy, and notably the struggling financial sector, cybercrime presents an interesting appeal - a steady income stream, work-from-home capabilities, and a temporary means to an end that could overcome a problematic job market. In the past, the concept of cybercrime appealed mainly to those in the technology sector, for example students facing a local economy that has failed to offer legitimate jobs.

In the future, we believe we will also see management and financial experts finding eCrime as an alternative to a weak job market, offering better and more efficient ways to increase their incomes, understanding the untapped resources that eCrime can access (mainly corporate data and financial data). The impersonal activities associated with eCrime (e.g. – online operations, not dealing directly with people or their stolen goods) may also be factors in luring more "non-traditional" recruits into the eCrime business.

On the other hand, considering that law enforcement has not been extremely successful in mitigating eCrime activities on a worldwide scale, we do expect to see more investment in core training and enforcement methodology for the law enforcement sector in 2009. After seeing the growth in the business of eCrime and the relative ease of evasion (both legal and technological), law enforcement will be given another nudge in efforts to enforce eCrime and privacy laws. We also expect that law enforcement will begin to tighten cooperation between their agencies and their counterparts worldwide. Jurisdiction issues, legislation and politics have been major issues to date in the attempt to crack down on eCrime.

Multiple examples of these shortcomings were observed during 2008 – from the "putting out fires" approach observed during AIRC research on the major eCrime server, to the shutdown of two major network providers. These actions brought a short period of solace, but the eCrime activity has proven to be resilient, and has managed to get back to the same level of operations, and in some cases even surpassing it.

PREDICTION #2: The Web as the new OS

Web 2.0 marked the beginning of the true "network computer" that was envisioned almost 10 years ago, as useful applications found a better hosting platform on the Web than they would have on the traditional desktop. With the decrease in the cost of online storage (multiple gigabit email accounts are now a commodity), and the increase in computing power available for free (mashup platforms, cloud computing and a plethora of freely available enterprise class code projects), building full-featured applications has become a matter of will.

The next phase in this evolution is a consolidation move – having all the pieces connected seamlessly, working together from one central place. We already see the signs of cross-platform integrations, when Internet companies agree on protocols, and enable their applications to be used everywhere. From social networking, to sales tools, and office applications, everything that we use today online would be accessible and connected.

The missing pieces include authentication models, which represent a historical battle that is awakening again (from the passport days to today's OpenSocial and cross-application authentication) and a security model to accompany it.

As history tells us, the security component will lag behind, and we will have an uphill battle once the platforms are launched because of early adoption issues. This will mark the beginning of a true WebOS, where one does not need anything on the local PC except for a decent browser.

WebOS is definitely not a new idea, but it has never managed to catch up by itself in the past. The hurdle to date has not been technological, but more behavioral for the user. Now with technologies that are helping to bridge the gap (Google's Gears, Microsoft's Silverlight and Adobe's Air as examples), we predict a better adoption of this new WebOS. We see a user having most of his information on the Web, with some pieces of the data stored locally for offline use, and we see a rally to adoption with both end-users as well as companies, who have been the first to adopt the more enterprise versions of these applications.

From the security perspective, we will have a challenge, as parts of the data are not "seen" by standard gateway appliances, and the mere concept of cloud computing in conjunction with local offline storage (as minimal as it may be) is going to be ground for major innovation. Traditional security models will fall even further behind in light of the corresponding attack vectors that would utilize the new platform.

PREDICTION #3: Social networking gets real

The last prediction for 2009 involves the "softer" issue of identities. Not identities in the form of identity theft, which is "old" news, but in the context of online identities. With real-life networking, maintaining a network is very time consuming, much more so than the online networking counterpart. The mere number of actual maintainable connections a person can have is ever increasing, and the shift towards an online version is understandable.

But what happens when one does not retain control over his online persona? Most professionals these days have enough public data, that it can be easily aggregated and used to build a complete online persona. In several experiments performed at the AIRC, as well as at other facilities, a simulated fake online persona ended up connecting to the real network of acquaintances rather easily. The damage potential of this phenomenon will be devastating – both on the personal level (creating difficulties in employment, ruining social and professional connections, damaging reputations, etc...), as well as on a financial level such as stealing customers, corporate data, etc.

What started as a benign "fun" way to socialize, grew into a professional way to maintain one's network and make new connections. But we see this quickly turning into an online nightmare that will include identity hijacking (rather than identity theft) and damage to both personal and corporate reputations unless a more reliable, trustworthy model of easily connecting an online persona to a true person catches up with social networking sites.

6. About the Attack Intelligence™ Research Center

The Aladdin Attack Intelligence Research Center (AIRC) is a premier facility for Internet threat detection and cybercrime investigation. The mission of the AIRC is to deliver security research and intelligence that educates, supports and strengthens the security community, and drives innovation in Aladdin's content security solutions. Based in Tel Aviv, the AIRC is comprised of global security researchers and law enforcement and cybercrime specialists dedicated to finding and eradicating Internet threats that compromise legitimate business safety. AIRC goes beyond traditional threat detection to provide business intelligence around evolving threats, predict future trends in Internet security, and uncover the inner workings and affects of the business of eCrime. For more information, visit www.Aladdin.com/AIRC.

7. About Aladdin

Aladdin Knowledge Systems (NASDAQ: ALDN) is an information security leader with offices in 12 countries, a worldwide network of channel partners, and numerous awards for innovation. Aladdin eToken is the world's #1 USB-based authentication solution, offering identity and access management tools that protect sensitive data. Aladdin HASP SRM boosts growth for software developers and publishers through strong anti-piracy protection, IP protection, and secure licensing and product activation. Aladdin eSafe delivers real-time intelligent Web gateway security that helps protect data and networks, improve productivity, and enable compliance. Visit www.Aladdin.com.

Aladdin
SECURING THE GLOBAL VILLAGE

For more contact information, visit: **www.Aladdin.com/contact**

North America: +1-800-562-2543, +1-847-818-3800 • UK: +44-1753-622-266 • Germany: +49-89-89-4221-0
France: +33-1-41-37-70-30 • Benelux: +31-30-688-0800 • Spain: +34-91-375-99-00 • Italy: +39-022-4126712
Portugal: +351-21-412-36-60 • Israel: +972-3-978-1111 • China: +86-21-63847800 • India: +91-22-67255943
Japan: +81-426-607-191 • Mexico: +52-1-55-4159-9733 • All other inquiries: +972-3-978-1111