

Going above and beyond traditional security



Information Security Intelligence Report

A Recap of 2010 and Predictions for 2011



Revision History

ISSUE	DATE	AUTHOR	REVIEWED BY	COMMENTS
Version 1.0	01/26/2011	Iftach Ian Amit	Yoram Golandsky	Public Release



Table of Content



Table of Contents

- 1. General..... 3**
- 2. Executive Summary..... 4**
- 3. Cybercrime 6**
 - 3.1 Aurora6
 - 3.2 Mariposa7
 - 3.3 Social media breaking the perimeter8
 - 3.4 ZeuS-SpyEye.....9
 - 3.5 General Findings and Statistics.....10
 - 3.6 Additional Insights13
- 4. CyberWar 15**
 - 4.1 Stuxnet15
 - 4.2 Aurora16
 - 4.3 Countries building up capabilities17
 - 4.4 Redefining cyber as an dimension of war (NATO/UN/EU strategy).....18
- 5. Prediction for 2011 19**
 - 5.1 Cybercrime advancements19
 - 5.2 Expanding the breadth of information security (VOIP, custom devices)20
 - 5.3 Expanding the digital domain (and attack surface) – smartphones and tablets.....21
 - 5.4 Cyber Race21
 - 5.5 Monitoring on a whole new level (and privacy implications)23
 - 5.6 Information risk management.....24
 - 5.7 Social Media continues to provide attackers a clear avenue of attack25
- 6. About Security Art..... 26**



1. General

This report provides a summary of the significant information security events of 2010, and a general prediction for the state of information security, cybercrime, and cyberwar for 2011. The goal of this document is to provide an analysis of the relevant threats that may affect the ongoing operations of individual businesses, and an indication of what the market is doing to counter these threats.

This report has been adapted for public release, and therefore contains both the intelligence analysis done on open-source feeds, and a generalized approach to the intelligence analysis, in order to appeal to a broader audience rather than to a specific geography or market segment.

As Security-Art believes that threats and the information assets related to them should be as quantifiable as possible, some of the resources and the analysis in this report focus on financial implications that such threats can inflict when launched against a target; be it an individual or a business entity.



2. Executive Summary

Looking back at 2010 shows a widening gap between cybercrime and law enforcement capabilities, in conjunction to nations that have started the cyber-race to develop defensive and offensive capabilities. Most of the attacks analyzed in 2010 depict organizations that fall behind in their defensive strategies as attackers take advantage of a hybrid approach that merges technical merits alongside human weaknesses to cash-out on their attacks.

Cybercrime widens the gap between attack capability and defense mechanisms.

Analyzing several of the major attacks of 2010, Security Art notes that organizations were attacked in two key ways. Firstly, through technical exploits such as Aurora, Mariposa, Zeus, and SpyEye. Secondly, by attacks that bypassed traditional protection methods, and gained access to targets through human-weakness areas such as social media. While businesses focused on defending themselves using security mechanisms such as anti-virus software and perimeter defenses, attackers jumped over these defenses, and proceeded to flood the market with a high volume of malware that now poses a serious threat to security providers in terms of detection rates and response time. However, law enforcement agencies have focused mainly on menial cybercriminals, and have not successfully reduced the impact of online criminal activities. On a national level, we see nations have embarked upon the race to develop defensive and offensive cyber capabilities.

Cyberwar arms race sends nations to shopping frenzy. As CyberWar gained merit (and criticism) during 2010, with the movie-material Stuxnet incident being the poster-boy for news outlets that published every spin-off, speculation, and plain old gossip, the



international scene had its own race for the latest and greatest defense mechanisms. The implications of Aurora and Stuxnet made most countries feel their lack of a critical infrastructure defense and the capability to deliver a similar cyber-blow, and many went shopping for weapons. Security Art witnessed the strategic build up of capabilities in some countries, and a more hurried shopping spree (that usually led to amassment of CyberCrime provided tools) in others. This, and the delayed response of organizations such as the UN, the EU, and NATO, left the scene looking more like the Wild West than Silicon Valley.

Expanding digital domain and improved understanding of security will reign in 2011.

Our prediction for 2011, drawn from the criminal, political and diplomatic sides of cybercrime that dominated 2010, is that more focus is going to be given to approaching security from a strategic standpoint. Rather than buying "best of breed" products and ticking off compliance sheets, we predict that organizations and countries will apply a more sensible executive-level understanding of what information security means to them. In the expanding personal digital domain (smartphone, tablets, and suchlike), and the continued digitization of all organizational information (from scanned materials to VOIP telephony), security must be applied to more layers than ever before. Countries and organizations will have to adopt additional skill-sets and look for solutions in areas they have not dealt with before.



3. Cybercrime

This section provides an overview of the key events and advancements in cybercrime through 2010. As criminals have proven that online fraud is a viable business strategy, the formerly one-off cybercrime-only shops have evolved into groups that resemble organized crime. The motivation of such groups is still the same—money—but the breadth and focus of their operations have been refined and turned much more efficient, offering larger organizations the kinds of services that used to only be available through black-hat hackers and specialized groups.

The following are some of the more notable areas of interest, followed by a summary of the general findings from the financial industry, and insights that are based on Security Art's experiences during 2010.

3.1 Aurora

The Aurora incident that actually started at the end of 2009, and was much publicized in early 2010, put the issue of industrial espionage and competitive intelligence at the focus of corporations from various industries.

The ability to infiltrate a large number of industry-leading organizations that were thought to be highly secure, has proven again that at the hands of a motivated (read "well paid") attacker, no organization is completely secure. Beyond the publicized reports and analysis related to the attack that struck and stole data from over 40 corporations, in Security Art's view, the main takeaway from the incident is not the shortfalls of protecting an organization from security breaches, but rather the understanding that such incidents will occur, and what needs to be done to first identify them, and then contain and control them.



Some of the affected organizations (such as Google™) were able to react quickly and provide a reasonable response, while others were still stuck in a lethargic state of mind and had to call in experts for assistance late in the game, and deal with more severe implications as the malicious code had been allowed to run for a prolonged period of time in their networks.

3.2 Mariposa

As revenues from running cybercrime operations are rising and getting more media attention, more and more individuals are turning to this lucrative business in an attempt to capitalize on the industry's shortcomings and make a quick buck. The Mariposa story just shows how easily such an operation can be run, but also gives an insight on the more prominent behind-the-scenes players in the industry, and demonstrates how law enforcement deals with this new crime.

In early 2010, the leaders of one of the largest ever tracked botnets were apprehended in Spain. The botnet, dubbed Mariposa, amassed over 12 million victim PCs and spanned private, corporate, and government organizations worldwide. Without going into the already-published details of the tremendous work that was put into researching the botnet and finding out who ran it, we would like to point out some of the key takeaway points of this incident:

- **Public-Private cooperation.** The botnet was researched and analyzed by private companies (mainly Defense Intelligence and Panda Software). The law enforcement side involved the Spanish police, the FBI, and additional agencies in the US and Europe. Without the expertise of the private sector, and the cooperation between law enforcement across countries, this whole operation would not have been even



remotely possible.

- Cutting the head of the snake? Although the ringleaders of the actual botnet were arrested in Spain, the real root cause of the network was not actually tracked down until later in 2010. Without getting to the source of the botnet code (i.e. the group or person who wrote and maintained the software), cracking down on Mariposa would have been inefficient, as it would have been extremely easy to recreate using the same software and techniques. In June 2010, a Slovenian individual nicknamed “Iserdo” was arrested by the joint force of the Slovenian police and an FBI task force. “Iserdo” provided the Spanish gang with the software to run Mariposa to begin with. It’s interesting to note that the FBI was involved in both the Spanish and Slovenian arrests, even though the case was not brought up or prosecuted in the US. Presumably, because major US corporations and government bodies were victimized by Mariposa, and since the code was not exclusively sold to the Spanish gang, the FBI had a strong vested interest in apprehending the writer/distributor of the code.

3.3 Social media breaking the perimeter

Social media was involved in some of the cases already mentioned in this report. The “threats” of social when media used as part of attack vectors have been often mentioned in the past 2-3 years. The fact remains that as people are still an open variable in the security equation, social media services will remain to be one of the more effective means of breaking the security defenses of an organization.

With a strong showing across all sectors, and a booming business to be made (at least according to the current valuations of companies such as Facebook™ and Twitter™ now



that YouTube™ is part of Google), social media services can be utilized in both mass infections as well as targeted attacks.

In a lot of cases where common botnets are mentioned, we still see how the infection vectors use current trends, mostly based on the most searched terms on search engines, to either infect legitimate sites that fall within the search results, or to create fake websites to sneak into such results. As the potential victims are those who initiated the search, and as a result visited one of these sites, they are less likely to suspect that the website contains malicious code, and by definition have their defenses down to begin with.

Similarly, targeted attacks profile potential insertion vectors to the target using open social media services (usually business related ones such as LinkedIn™ as well as common ones such as Facebook™, Twitter™, Bebo™, and Hi5™ – depending on the geographical region) in order to pinpoint the most likely victim community, and provide it with the right context for an attack that attempts to infiltrate their organization. Such attacks are often very successful, and we can see how attackers are doing their homework properly when preparing the context for such attacks.

3.4 ZeuS-SpyEye

The market for cybercrime was booming in 2010, and the main players in the commercial side of Trojan development experienced what every market that is affected by a growing economy goes through: fierce competition. The ZeuS Trojan has enjoyed a relatively long period as the most successful and sought-after kit used by cybercriminals to conduct online fraud. This has led other groups to develop competing products and take some of the large market share that was still open for grabs in the growing online fraud business. One such competitor is SpyEye. Armed with the right marketing ideas (providing



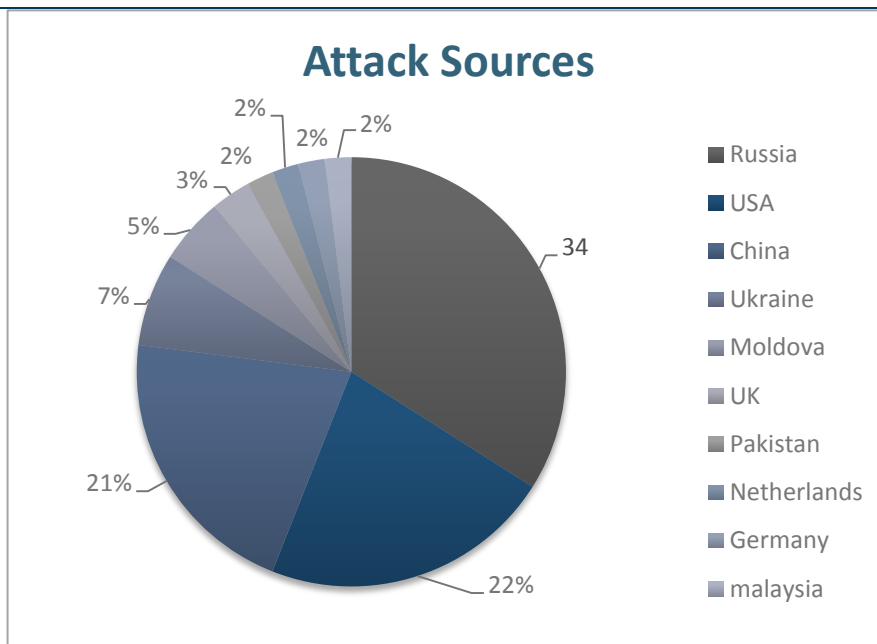
compatibility to the existing ZeuS configuration files), a skilled coding crew (detection rates that were competitive to the ones fresh ZeuS binaries were producing), and savvy competitive thinking (providing a simple configuration option to infect ZeuS victims, while eliminating the ZeuS Trojan already on the system), SpyEye managed to create a very interesting competitor to ZeuS. For example, SpyEye integrated a regional transaction processing system that forced transactions belonging to a financial institution in a specific region to be generated through infected systems in the same geographical area in order to thwart fraud detection systems.

With SpyEye taking a considerable enough portion of the market share from ZeuS, and providing a platform that is extensible enough for the creation of custom plugins, the ZeuS crew started to feel the pressure. In a classic move taken straight from business schools, ZeuS and SpyEye announced their merger in late 2010, with new combined-effort Trojan kits scheduled to follow in early 2011. This shows again, that much like the legitimate commercial market, the players in the cybercrime sector operate under similar rules and motivations, which is the cause of the successful infection rates and the development and growth strategy of such providers.

3.5 General Findings and Statistics

The following findings, which are relevant to the financial industry, were identified in many analyzed industry reports. These findings are summarized here, and enhanced with Security Art's analysis and insights for financial institutions.

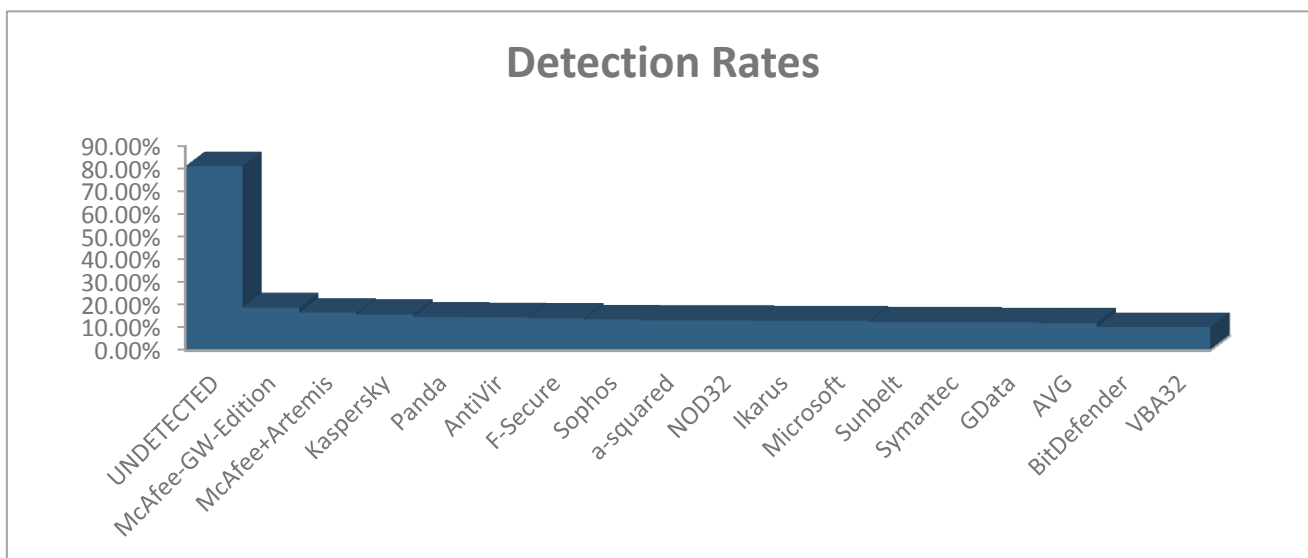
- Attacks are coming from the US, Russia, and China, as these countries are highly populated and have a high rate of Internet connectivity. Nevertheless, targets outside the US are not immune to attacks, and are also susceptible to attacks from the US.



- The most sought after industry in terms of attacks is the financial sector; this is the industry that can make the most money for criminals.
- The attack vectors remain mostly traditional: web browsers, email, and social engineering (phishing).
- Attacks on web infrastructure are less prevalent as they yield much less gain for the attacker. Nevertheless, some attacks still probe websites and web interfaces for openings such as XSS and SQL-injections, which are mostly used to lure customers and steal their identities.
- Consumers are the main targets for financial fraud. As such, criminals have focused on identity theft at major databases such as webmail, social networks, and healthcare institutions. These identities can then be used for financial fraud in order to capitalize on the initial attacks. Financial institutions should be aware of such “non-market related” security breaches, as they will have a secondary impact on them.



- There is no correlation between the vulnerability market (which shows a constant increase in reported and 0-day vulnerabilities) and the actual breaches. Most attacks still use known vulnerabilities that have security patches.
- Actual detection rates are much lower than the publicized figures. When testing sample detection rate in real time (that is, at the same time that the sample is being distributed by the criminals), the best detection rate is around 17% (McAfee gateway in conjunction with Artemis), and falls below 10% for the bottom half of AV vendors (out of 41 tested).





3.6 Additional Insights

The insights listed here are based on findings that were only included in a small number of reports, but were found to be highly significant by Security Art cybercrime experts. These findings are enhanced with Security Art's insights in terms of an indication of potency to fight fraud, and the required corporate commitment and strategic planning for such operations.

- Most corporations are behind in their information security practices. Most of the effort is put into “best practices” and “industry standard” protections that have not been proven effective. A very small percentage of organizations actually adapt these best practices to their business, while most stay relatively vulnerable to advanced attacks.
- There is almost no adoption of the defense in depth strategy. Most organizations focus on perimeter protection (i.e. “best practices”) and fail to create meaningful defense mechanisms in business processes and internal layers. Additionally, the battlefield has been extended not only within the organization, but also outwards – to consumer systems.
- There is a major lack of attention to internal education of employees and third-party suppliers about information security. While a lot of the data breaches come from the inside or are executed with the help of an insider, organizations still look outside for attackers.
- There is a focus on security investment in terms of products and applications. This approach has been proven as ineffective, and should be replaced with the implementation of inexpensive, easy to fix issues that plague business processes, and basic technology used through the business.



- Organizations fail to test themselves against the threats they face. Testing is still very much “90’s” and uses old techniques and methodologies. Organizations should adopt more “red team” testing with a broad scope that utilizes the newest tools and techniques that criminals have adopted.



4. CyberWar

During 2010, the term "CyberWar" got a lot of criticism from the media and from professional security circles, but at the same time it was one of the most sought after topics when dealing with government and corporate organizations. This section contains a brief overview of the top events that made the term itself a controversy, and some analysis by Security Art on how the market actually evolved in the past year.

4.1 Stuxnet

It was unbelievable how much attention was paid to the Stuxnet incident in private information security circles as well as (and maybe especially in) the media. Again, this report does not aim to re-iterate the good research that has been already been produced (Security Art itself participated in one such research publication which can be found on our website: [CSFI-CWD Stuxnet Report](#)), but tries to look a bit beyond it to examine the implications of the incident on a global level.

One of the most interesting elements of the Stuxnet incident is the fact that the impacted targets were not really accessible to the attacker, nor were they connected by a direct link to any public network. This made the infection vector itself much more complicated than ones usually covered by the general media, and as such brought flair of suspense and mystery to the whole ordeal. Nevertheless, this modus operandi is often used in targeted attacks on organizations with the same topology; where the sensitive systems are buried behind multiple layers of separation, and a lot of work needs to be done in order to map out the accessible routes to such systems, and to figure out a viable way to infect them.



The same method of infecting a laptop belonging to a person of interest with a Trojan in order to be able to sift relevant data out for analysis and further planning, was also used in the 2007 incident where the Syrian nuclear reactor was destroyed. The data that was gathered beforehand helped not only to verify that the reactor was being used for nefarious purposes, but also helped to identify the right means of attacking it, and provided assistance in mapping out the cyber element of the attack, allowing aircrafts to seamlessly evade any early warning and radar system across two countries.

This is another example that the Cyber front is just that – a front, and is also usually associated with a kinetic front in order to maximize impact. Such a kinetic front can be as simple as having someone on location or in contact with a crucial element of the operation to enable the cyber part, or vice versa, where the cyber element is a supporting role to the kinetic element.

4.2 Aurora

Yes, it's true, Aurora also appeared in our cybercrime section earlier in this report...nevertheless, it's important to remember the big picture of what Aurora means at a nation-state level. The techniques and capabilities that were exposed during the research on Aurora clearly indicate that the source was related to cybercrime operations, however the data that was targeted, and the specific mix of organizations that were impacted by the incident, are clearly the mark of higher planning.

This puts cybercrime in a very interesting position for some countries that have yet to develop a proper cyber-offensive capability, as well as for ones that need to be able to provide plausible deniability for cyber-related actions that were taken on their behalf. The mere fact that the political playground was more dynamic in relation to the evolution of how



the Aurora event unfolded over time, just shows how well connected these two worlds are (that of cybercrime and nation-state cyberwar).

Similar events in the past, where states used criminal outlets to execute their cyber actions (such as in the case of Russia's conflicts with both Estonia and Georgia), enabled the state actor to either test their cyber offensive capability, or carry out an offensive without being directly linked to it.

4.3 Countries building up capabilities

Similar to cybercrime in how it sparked interest from many players that wanted in on the game, the cyberwarfare field drew the attention of a lot of governments who suddenly realized that they had been procrastinating, and failed to not only properly defend their critical infrastructure, but also to amass a certain offensive capability in the cyber front.

Such nations are in the right place and time to be tempted to use an alternative "shortcut" in terms of building short term capabilities. When we look back at cases such as Aurora, Estonia, and Georgia, we see that the already-accessible offensive nature of cybercrime can provide a strategic path if needed. These are very problematic situations, especially when you take into account that law enforcement is nowhere near understanding how to solve cybercrime due to politics, jurisdiction, and bureaucracy.

The countries that took the longer and safer route have started to invest heavily in several fronts of building cyber capabilities. The notable ones have critical infrastructure defense, are building a viable and effective emergency response infrastructure coupled with a proactive cyber-intelligence theater that can deliver actionable intelligence and advance warning on aggressors, and finally have offensive capabilities in both technical means and human capital.



4.4 Redefining cyber as an dimension of war (NATO/UN/EU strategy)

During 2010, several efforts were made by military and political organizations to clearly define cyber in terms of diplomatic relationships and the attribution of actions and responsibilities in that realm. A notable effort has been NATO's cyber commons strategy creation for 2011, which was published in part at the Lisbon summit on November 20th, 2010. Adding cyber to the general strategy that nations should adopt is an important step in the right direction.

Nevertheless, Security Art believes that jumping too far ahead on the warfare side, before making additional and substantial progress on the criminal frontier is a far from perfect plan. The diplomatic and strategic elements should first be built on a framework that can prove itself on the criminal side; otherwise it risks being implemented as an empty promise.

Additionally, defining a cyber dimension strategy that only includes capabilities to "detect, assess, prevent, defend, and recover" in case of a cyber attack, clearly misses the deterrence factor that NATO has been notable for, as well as an offensive retaliatory capability to counterpart the defensive elements.



5. Prediction for 2011

Being able to predict the future in a market that has such fascinating and complex dynamics is almost impossible, and even would be somewhat pretentious. Nevertheless, we believe that based on our experience and indicators that have proven to be consistent over time (which are mostly non-technical), we can mark some areas that would evolve in a specific direction. Here is our analysis for the information security arena for 2011:

5.1 Cybercrime advancements

Cybercrime has proven that it can be a daunting element to be dealt with. From the early days of localized groups with a specific specialization, it has turned into a multi-billion dollar business that has attracted organized crime elements that now dominate the business. By contrast, law enforcement kept treating online crime with a rather traditional approach, and as such has widened the gap between the volume of criminal activity, and the ability to contain it and apprehend the people behind it.

Furthermore, as the technical and strategic capabilities of law enforcement focused on lower hanging fruits, most of the criminal prosecutions have only reached the “foot soldiers”, regardless of the media spins that accompanied such actions. We predict that as countries try to set the record straight and build more cross-national task forces that enable law enforcement to act swiftly and without borders, the business of cybercrime will continue to out-manuever the enforcers.

Unfortunately, this, and the inability of law enforcement to go after the people higher up the food chain of online crime, police actions do not actually stop the business from further



expansion. It merely delivers surface wounds to an operation that is well designed to withstand losses at the lower levels.

5.2 Expanding the breadth of information security (VOIP, custom devices)

Businesses and other organizations are much more dependent on technology as they move forward in the never-ending race for cost cutting and optimizations of their operations. Additional measures are put in to conserve human resources, and minimize the dependency on legacy technologies. New technologies are introduced without paying attention to the risk they introduce. and these have never been mapped by analysts and consultants as part of enterprise risk management.

Some of the examples that we met in 2010 include VoIP integration pitfalls, and the proliferation of “custom” software and hardware that is designed for a specific market segment. Such integrations have proven to introduce more issues than value as the cost of retrofitting security post-factum has raised the overall cost of ownership (especially in major corporations).

We expect that as risk-based decision making techniques adopted by organizations matures, the breadth of the scope of information security will expand appropriately, and will eventually reach the proper executive level decision-making.



5.3 Expanding the digital domain (and attack surface) – smartphones and tablets

With the electronic frontier expanding more than ever, and technology dominating almost every aspect of our business and personal lives, there are more opportunities for information gathering on targets before employing more traditional means of human intelligence.

We expect that as people become more connected, and businesses start to more naturally adopt such technologies, a considerable amount of re-training for employees and businesses in general will be required. The alternative to that would be a mental switch in the approach to information security, privacy, and the borders between personal and business. We do not anticipate this will occur until a major corporate espionage or a nation-state level event happens. The WikiLeaks incident could be considered as a precursor to such change, but it is currently too riddled with politics and technology (which had almost nothing to do with the leaks themselves).

5.4 Cyber Race

At a nation-state level, our expectation is that as many countries find themselves behind in terms of their cyber capabilities (be it defensive, intelligence, or offensive), a race to catch up with the leading players will ensue. This prediction is not precisely a forward looking one, as it is mainly based on our experience during 2010 with several government entities, and the amount of work on both technology as well as capability building that has been done in a relatively short amount of time.

Such a race is actually needed, as the situation where a small number of key players holding advanced technology usually lead to increased instability at the diplomatic level,



which is then balanced by the multi-national effort to equate the playing field. This is something that we have been privy to in discussions with the relevant organizations.

As such, we also anticipate a couple of additional major changes to the state of the cyber realm in 2011:

- **DDoS attacks ensue** – As more tools are available to cybercriminals as well as to state actors and terrorist organizations, we believe that the use of a major scale DDoS (Distributed Denial of Service) attack would be imminent. The impact of such attacks has proven itself highly useful in criminal rings (especially when demanding “protection” money from online gambling sites). The same can also be applied on a national level, and basically blackout an entire region or country.
- **Act of Cyberterror** – Cyberterrorism has not really picked up speed, as the more traditional means of using the Internet for covert communication is the main avenue for terror right now. Nevertheless, the accessibility of the tools and capabilities provided at the criminal level has started to reach terror organizations and provide them with additional means of applying pressure to the countries they target. We predict that during 2011, a terror organization will test the usage of the cyber realm as part of their arsenal.



5.5 Monitoring on a whole new level (and privacy implications)

As additional technological devices (mobile communication gadgets) are being used by all of us on a daily basis, businesses need to start considering adding such devices to their security monitoring scope, whether at the business or personal level. Such monitoring, which is currently limited mostly to web browsing, email, and instant messaging, is crucial for composing a complete picture of threats and exposures for a business. With the expansion of such monitoring, privacy issues are bound to rise again as employees begin to understand that all their communications are being monitored; but then would become more acceptable as businesses develop new privacy guidelines and integrate these into their employment agreements. Such guidelines would need to iterate the necessity of monitoring all communications as a safety measure for doing business, or provide an alternative for conducting personal communications in separate environments. Additionally, the proliferation of VoIP that replaces older PSTN communications also re-enables businesses to effectively monitor voice communications because the need for specialized equipment is no longer an entry barrier to tracking and containing inappropriate communications (whether on a personal, ethical, business, or malicious/criminal level).



5.6 Information risk management

The challenge to properly manage information risk in today's ever changing environment has quickly made its way into the top ten issues that companies deal with today. As new technologies are introduced and threat landscape rapidly changes, and with the race for compliance (SOX,SAS70,PCI,ISO2700x, etc) which creates a misperception of a low risk and secured environment, risk oriented businesses look for probabilistic methods of running their information risk management practice, methods that support risk-informed decision making.

There are a handful of frameworks and methodologies that aim to simplify the process and provide a natural business-oriented taxonomy for information risk management. Our opinion is that practical management-oriented methodologies that can provide a simple taxonomy and a unified result (monetary), which can be integrate to the organization's entire risk portfolio, would be more likely to be adopted than methodologies based on expert intuition or weighted scores. This is mainly because executive management is expecting to manage its entire risk portfolio according to one baseline, which is likely to be monetary.



5.7 Social Media continues to provide attackers a clear avenue of attack

This prediction is the most substantiated, as it is based on the actual behavior of the market over the past two years. Social media has been used in increasing volumes by attackers as a means of more precisely targeting victims. The implied trust that such a media provides allows attackers to convince their potential victims to access malicious content, and back it up with a context that is both socially connected (coming from friends/relatives) as well as relevant (timed to correspond with major events that have news coverage).

A quick recap of every major or local news and Internet meme shows how quickly attackers adapt their attack vector. These attacks are usually deployed either by crafting “smart” emails that discuss the news item, or by creating fake websites that would show up when the related search terms are used on search engines. More often we can see even legitimate websites that are ranked high for the news item being attacked to carry out the malicious code so that innocent visitors that try to catch up with the latest news would be exposed to the attackers' malice.

We expect that in 2011 this attack vector would continue and be even further refined and honed by attackers in order to provide more assurance to the potential victims, and to disguise itself as one of the legitimate resources related to the context.



6. About Security Art

Security Art is an information security and information risk management powerhouse which specializes in combating cybercrime and quantifying information risk to monetary values.

We believe that our multidisciplinary approach and years of hands-on experience allow us to give businesses the strategic path to address all their information security and information risk-management needs. Security Art provides a wide range of services that are based on the understanding that the modern business requires a truly multidisciplinary approach to information risk. Our hands-on knowledge of development, operations, and business facets of organizations means that we can speak to anyone in their own language and facilitate a faster turnover.

One of our most advanced and comprehensive services is the "Red Team Testing" service. When approaching a business problem, a different kind of mindset is needed. Security Art's approach is to challenge all layers of the business operation. Red Team testing encapsulates this attitude, taking into account all aspects of the business operating environment. Our unique propositions include often neglected aspects of a traditional security assessment, such as intelligence gathering, profiling, process analysis, 3rd party suppliers, physical security, general social engineering, and of course, the actual technical ability to infiltrate your information assets, the ability to perform a clean exfiltration, and/or modify your data. The team often utilizes custom-built tools and Trojans that simulate a persistent attacker as well as other attacks and exfiltration.



Our Red Team testing provides our customers with a real-world view of actual threats, as well as showing how their controls and monitoring systems handle them.

Another high interest topic is cybercrime and cyberwar. Security Art specializes in these two linked fields, and offers workshops and other educational engagements for its customers. These engagements can be anything from a single lecture to a training week. The real gain from our cybercrime and cyberwar workshops is your understanding and awareness, coupled with hands on experience of techniques and methodologies employed by hackers worldwide.

We're a different breed of security power house:

- We have a strong back-office research and develop team
- We use patent pending, self-developed software tools
- We use cutting technology and cutting edge business tools

We take a proactive approach which can and will prevent, or at least significantly minimize, cybercrime and fraud. We'll design a fraud, data-theft, and embezzlement simulation scenario, and put it to the test. You don't want to be caught unprepared!

For more information or to schedule a free meeting with one of our cybercrime experts, please email info@security-art.com