Cyber[Crime | War]

Linking State Governed Cyber Warfare with Online Criminal Groups

Table of Contents

Introduction

In recent years Cybercrime has been front-page news as a result of an increase in profit-motivated internet crimes; and an apparent lack of sufficient security measures that leave standard internet users virtually unprotected from internet crimes.

Software security vendors have been trying to show progress in the fight against cybercrime - with some success. The vast majority of Internet users, however, are still unprotected from internet crime that includes fraud, phishing and identity theft. The success of financial cybercrime has served to fuel further increase in its levels as more and more criminals turn to the Internet as a means for theft.

It is likely this problem would have been shadowed by other IT security issues, were it not for the fact that major corporations are also being targeted - with measurable success - and that attacks are growing more and more sophisticated by the day (check out www.datalossdb.org for statistics and samples).

Cyber warfare (i.e. government warfare conducted over the internet), on the other hand, hasn't drawn considerable media attention[1], mostly because of lack of evidence connecting cyber attacks with government policy or actions. In some circles cyber warfare is not even considered a serious topic of discussion, being closely associated with conspiracy theories.

At the same time governments across the world are investing vast resources in developing cyber warfare weaponry and awareness, as part of their overall defense and offense strategy.

Leading industrial nations, such as the US, Russia and the UK, as well as developing cyber-nations including China and Iran, are trying to make sure they won't stay behind in the cyber

[1] This does not include marketing related "cyber frenzy". See http://www.wired.com/threatlevel/2010/03/cyber-hype/

arms race; while at the same time trying to keep "off the radar" in terms of public and media awareness to their actions.

This paper will explore possible links between the political activities of national governments, and cybercrime activities, through events that included substantial cyber-warfare characteristics. We will also outline a mechanism by which cybercrime is often connected with cyber warfare - to the benefit of both governments and cyber criminals.

Background

While researching last year some "behind-the-scenes" aspects of cybercrime (including technical threats by criminals and business aspects of cybercrime), we uncovered some interesting material from a criminally operated server. This material led us to the conclusion that there are possible links between a certain criminal organization and government/state dealings.

We then observed several famous cases linking cybercrime with political international conflicts, using our experience in order to shed light on mechanisms of cybercrime, and to identify links between cybercrime and state-sponsored cyber-attacks.

Cybercrime

Cybercrime turned into a major concern as computers and the internet became an integral part of daily life. Most research efforts that focus on covering the cybercrime world portray a highly organized environment, sometimes at a level akin to organized-crime.

Targeted and specialized, cybercrime is like a modern economic sector with sub-sectors that specialize in different technologies and markets, actively trading between themselves.

This is a force that adheres to classic economic theories of supply and demand, to rules of international business, marketing, distribution channels, outsourcing and financially-driven innovation.

Cybercrime today is almost completely financially driven, and usually bears no relation to geographies or politics, unless they play a role in revenue generation.

One of the major enablers of this economy is the almost nonexistent legislation against cybercrime. Where legislation does exist, it is rarely enforced effectively. Although modern states do have criminal legislation banning electronic crime, lack of cooperation and coordination between countries renders such legislation ineffective, since cybercrime recognizes no borders and geographical barriers.

The existence of regions in which authorities either turn a blind eye or have lax legislation, provides a safe haven for cyber criminals and enables cybercrime organizations to get away with their activities.

In terms of technology, most of the vulnerabilities and exploits used in cybercrime are well documented, both technologically and financially. Cybercrime tools and skills are often offered for a premium in an active marketplace that exists for creating, selling and exchanging such technologies; a marketplace that thrives in the fringes of legitimate technological markets.

Most of the victims of cybercrime (whether individuals or businesses) are usually covered by local liability and insurance protection, with financial institutions footing the bill for most of the

damages accrued from these activities (it is therefore natural that financial institutions are major consumers of security intelligence services and proactive security actions).

Cyber Warfare

It is well known that advanced nations are allocating considerable resources to cyber warfare and to creating awareness/readiness for cybercrime, as part of a defense and offence strategy on the cyber front.

On the defense side, the aim of cyber warfare is to protect infrastructure, military capabilities and civilian institutions.

On the offence side, the aim of cyber warfare is to target an adversary's critical infrastructure, alter their view of the battlefield (both kinetic and virtual), and affect their population (propaganda).

Cyber warfare capabilities range from the more traditional SIGINT (Signal Intelligence), including espionage (both internally and externally), development of offensive capabilities to render information systems inaccessible or inoperable (including falsifying information), and developing defensive capabilities to protect critical IT-reliant infrastructure from attacks.

Most cyber capabilities developed by advanced countries over the last decade focus on military aspects of cyber warfare: stealth vehicles, jamming devices, anti-jamming, secure communication capabilities, etc.

Less attention was given to “classic” computer attacks involving personal computers and servers. As a result, governments often found themselves following civilian market developments in this field, rather than leading the innovation.

Past Events and Making the Links

In order to underscore the recent developments in cybercrime and cyber warfare, we will review a number of major cyber warfare events:

Estonia

Much has been written on cyber events revolving around the Estonian-Russian cyber war. This was an online-only conflict spurred by the relocation of a soviet-era bronze statue in Tallinn in 2007[2]. While some call it the first cyber warfare, others denounce the notion, claiming there was no direct involvement in cyber activities on the part of the two governments supposedly at war.

Both are right. Estonia was indeed the first public case of effective cyber warfare, which brought the country’s IT infrastructure to a standstill.

For a country like Estonia, which is heavily reliant on its IT infrastructure (most of its banking activities, for example, are done online and so is voting and numerous other government functions) - the result was the same as warfare targeted a civilian population: for three weeks the country’s major infrastructure, including the banking sector, media and governments, ceased to work as a result of a DDoS attack (distributed denial of service).

[2] For additional background on the Estonia-Russia cyber-conflict see http://en.wikipedia.org/wiki/2007_cyberattacks_on_Estonia

On the other hand, who waged this war? The obvious answer would be Russia. There was no proof, however, of direct links between any Russian government or military entities and the cyber attacks on Estonia.

Yet this is exactly how cyber warfare is waged: a Russian official, in answer to claims that Russia was behind the attacks, stated that "If you are implying [the attacks] came from Russia or the Russian government, it's a serious allegation that has to be substantiated. Cyber-space is everywhere" (Vladimir Chizhov, Russian Ambassador to the EU).

Tracing back the attacks, we can see each and every one came from civilian networks. More notably, the attacks had a form characteristic to attacks used by cyber criminals to extort online businesses (that rely on providing uninterrupted service for their revenue generation).

For background on the techniques and operations, check out a riveting recount of battling such threats (with success) here: http://www.csoonline.com/article/print/220336 and here: http://www.wired.com/wired/archive/14.11/botnet_pr.html (which shows what happens when you try to openly and directly fight spammers).

In the Estonian case, the attacks were not just simple hack-and-deface attacks (attributed to the Nashi - a Russian youth political movement), but also an all-out DDoS (Distributed Denial of Service) that brought the country's infrastructure to its knees for over three weeks.

This DDoS attack came from a botnet that was later associated more closely with a Russian cybercrime group operating out of St. Petersburg, with links to the RBN (Russian Business Network). RBN has been extensively covered in cybercrime research and was linked to Russian politics on more than one occasion[3].

This leads to the question, how and why would a criminal organization whose main objective is financial get involved in a purely political issue? How could that involvement come in such an organized and timed manner, in response to the events in Tallinn (events that were clearly generating political reactions from the Russian Government)?

The only conclusion is obvious: one of the lines of business of Russian groups linked to the attacks is what is called "botnet[4] rental".

Rented botnets have been successfully offered as a service by cybercrime groups, since they realized that such a huge computing power can be better utilized when rented "by the hour" to multiple users – much like the early computer systems were, and the way supercomputers are rented today.

The Estonian botnet operation could only have been carried out by a botnet with enough capacity to immobilize the Estonian infrastructure. This means that most of the botnet was utilized at once. This is something that is rarely done, since botnets are typically rented in small chunks to maximize financial potential.

An operation of this scale would have to be commissioned by government agencies, which probably already had ties with criminal groups operating within the RBN. The fact that RBN has, on several occasions, been associated with Russian officials and the fact that it was resurrected after its dispersion is another indication of the involvement of Russian government agencies in the Estonian cyber war.

Our conclusion is that there is a substantial link between cybercrime and cyber warfare in the case of shut-down of the Estonian infrastructure during 2007.

[3] For additional references on the RBN political links see http://www.theage.com.au/news/security/the-hunt-for-russias-web-crims/2007/12/12/1197135470386.html

[4] For additional background on botnets see http://en.wikipedia.org/wiki/Botnet

Georgia

The Russian-Georgian war in August 2008 poses a more interesting dilemma: during the conflict itself (which was kinetic, as opposed to the Estonian conflict that was purely computer-generated) there were more than a few incidents where cyber attacks were synchronized with troop movements on the ground.

The initial cyber attack was directed at the Georgian president's website. It was a simple yet effective DDoS attack:

flood http www.president.gov.ge
flood tcp www.president.gov.ge
flood icmp www.president.gov.ge

The DDoS was quieted down by the Russians for a few days: the C&C servers (Command and Control servers used to manage a botnet) deployed in the initial attack were taken offline as Russian troops crossed the border towards Georgia,.

Shortly after the ground troops started engaging the Georgian forces, six new C&C servers started issuing DDoS attack commands on select Georgian websites, including:

www.president.gov.ge
www.parliament.ge
apsny.ge
news.ge
tbilisiweb.info
newsgeorgia.ru
os-inform.com
www.kasparov.ru
hacking.ge mk.ru
newstula.info
skandaly.ru

The interesting part is the difference between the initial C&C servers that launched the attack on the president's website, and the six C&C servers that launched the attacks on the rest of the websites.

The six servers that launched the later attacks were much more capable and less dedicated to the Georgia attack: while commanding their botnets to attack Georgian Internet facilities, the servers were also taking care of "regular business": attacking sites that included Porn, adult escort services, carder forums[5] and gambling sites.

This is a clear indication that a cybercrime group has been managing the later C&C servers. Other indices include the fact that the servers themselves were registered through www.naunet.ru - a known "bulletproof hosting" provider in Russia; and the fact that the domains used for lunching the attacks were registered and hosted by www.steadyhost.ru - a known front for cybercrime activities.

Steadyhost.ru is using a network provided by its parent company, "Innovative IT solutions". "Innovative IT Solutions" is masked by a mail-drop in London, and actually owns and operates the subnet used for hosting the servers that attacked the Georgian websites (at IP addresses 74.86.81.232-239 and 75.126.142.96-111).

Criminal activities conducted by the "bulletproof" host in Russia, along with the Georgian attacks, included (like in the case of RBN in the Estonian cyber attack) mostly criminal activities such as forgery, money laundering and renting out botnets for spamming and extortion purposes.

It is our opinion that those three variables – commercial criminal activities by the attacking servers, ties to Russian entities as well as criminal entities - together with the Kremlin's

[5] Forums in which "carders" (criminals in the credit card fraud industry) are trading stolen cards and criminal related information.

policy and tactics regarding operation of RBN and similar businesses in Russia, make a clear case for a connection between the Russian Government and cybercrime. A connection that in the Georgian case was used to deploy one of the most synchronized kinetic-cyber attacks in history, while enabling the Russian government to deny any connection between the two.

Twitter, Google and the APT

The grouping of the Twitter and Google incidents during 2009 and 2010 is not coincidental. Although the media has attributed the incidents to two different countries (Iran and China), if we check their methods of operation we can see they are quite similar and link back to the "classic" cybercrime methods of operation we have witnessed over the past few years.

In the first incident, an “out of nowhere” attack on December 18th 2009 affected Twitter’s DNS server in the US in a way that allowed the attackers to point traffic intended for Twitter to attacker-controlled servers.

The attack was attributed to a group called the “Iranian Cyber Army” (as identified by the webpage presented to users trying to access www.twitter.com).

There was no “Iranian Cyber Army” before the Twitter attack. There is, however, a group called “Ashiyane” that was active both in the political side of hacking and directly in cybercrime. Ashiyane has a small sub-group called the “Iranian Cyber Army”.

Ashiyane had been training hackers for some time and their forums were running contests called “wargames”. The contest targeted different websites, prompting an “all-out” attack on these sites in order to gain access, steal data, modify it, implant false data or deface the site.

Some of the targets named during these "wargames" were clearly related to critical infrastructure (such as a natural gas provider in the US).

At the same time, Ashiyane was conducting more traditional cybercrime activities such as credit card fraud, breaches to customer databases, to financial institutions and to personal information used for spamming and identity theft.

The operational duality of a cybercrime organization – conducting "commercial" alongside political cybercrime - is endorsed by governments who benefit first from an affective and highly covert form of combat, and second from the income generated by commercial criminal activities.

The Twitter attack was carried out using stolen credentials used to manage the DNS services used by Twitter. This kind of data theft is often carried out by cybercrime organizations in order to gain access to business data. The data is then sold for the purpose of corporate espionage, to extort businesses or disrupt their services. This practice is a notable part of the “training” provided at the Ashiyane group as part of its criminal activity.

Another factor tying the Twitter cyber crime activity to the Iranian government was the move by the Iranian army to seize an Iraqi oil well on December 18th - the same exact day the Twitter DNS attack took place.

A kinetic action done in conjunction with a cyber-attack on Twitter - a major resource of anti-Iranian messaging (and a channel for opposition groups to speak out to the world) - is a textbook example of how a government can combine cyber warfare with traditional warfare to great effect.

Google's experience with the Chinese government (together with Adobe and a few dozen other companies operating in the US) is almost the same as that of Twitter and the Iranian government.

Although the notion of “APT” (Advanced Persistent Threat) started to pop up in the media only in early 2010, the concept has been known by cybercrime researchers for a long time. In fact, most of the tools used in cybercrime in the past 3-4 years are actually APTs, such as trojans, rootkits and keyloggers.

All of them go undetected most of the time (hence their continued success) and perform advanced functions, from network scanning to selective information gathering and providing additional footholds over the breached networks.

Google has been hit by a somewhat older version of the threat (dubbed Aurora) that has a fairly simple command and control structure and local capabilities. The interesting part in the breach (which affected over 40 companies) that ended up on the news is the fact that the attacks were highly targeted and abused undisclosed vulnerabilities. This enabled the perpetrators to install the trojans on Google's equipment.

Again, attacks came from servers linked to China, and again, this does not necessarily mean the Chinese government commissioned attacks on US companies. However, one cannot ignore the connection between the Chinese government and these criminal activities, especially when their targets do not yield any of the typical revenues of cybercrime and when these attacks serve political aims (in Google’s case one of the goals was to infiltrate the mail accounts of Chinese human rights activists).

Conclusion

Having seen how cybercrime and cyber warfare interconnect, along with the covert nature of cyber warfare and the near impossibility of cracking down on it, it is obvious that combat in the cyber sphere cannot be handled in the traditional form of combat.

While in the past command and control of national cyber warfare was in the hands of a central agency with direct reports, its future looks more like international espionage: including agents that can only be partially trusted, suppliers of arms (technology) that are also active in underground or illegal activities and presence in countries that may not be directly involved.

On the bright side, current efforts by law enforcement agencies to battle cybercrime may actually turn out to be useful against cyber warfare. We also foresee a move toward international cyber-treaties which would be based on the lessons learned at the field battling cybercrime. Treaties along the lines of the recent US-Russian nuclear arms treaty, signed at the end of March 2010 may pave the way for similar ones on the cyber front.