FUTURE CYBER LANDSCAPE AND CYBER SECURITY

Msc. Economic Sciences, Msc. Penal Law, Phd (c) Hergis Jica
ALBANIA

ABSTRACT

Cyber threats is starting to take the upper hand to our virtual environment, to infect any info-system and to be an intensive and permanent danger to all organizations. The critical infrastructure is one of the sectors that can be target of cybercriminals and in this way the security of state can be in the same "danger boat'. The cybercriminals try to damage the systems in their functionality, to make espionage or data theft. Malwares are used more and more to target critical infrastructure or people, organizations, to steal money etc. In the future, the most important deal will be with cyber security because to fight with this threat will be necessary to take different steps like security & design, cyber training etc. The future is Cyber!

Keywords: Cyber, Security, Future, Threats, Data theft, GDPR

The best way to predict your future is to create it
Abraham Lincoln[1]

INTRODUCTION, LITERATURE AND DISCUSSION

The Future of Cybercrime based on the current Trends that we see in Cybercrime today, is very clouded.

Unfortunately, Security moves so quickly that predicting further that this is close to being guesswork. However, let's start talking for Mac users and their environment.

Firstly, Mac Malware is currently on the rise and there is very little reason to think that this will not continue. As Mac gain more and more market share, they become more profitable for criminals to target. Add to this that security on Macs tends to be poorer than on PCs – most Mac users will not have Antivirus, Firewall, Web Blocking and so on installed. In fact, many Mac users are not even aware that there is malware for Macs! Macs are not just an interesting target for Cybercriminals aiming to infect as many machines as possible; they are also an excellent target for Cybercriminals engaged in targeted attacks.

Think about a company for a moment – who in a company is most likely to own a Mac? In many cases, it is upper management, CLevel executives and so on. Now, Macs are not crazily expensive, but they are expensive enough that in most companies they are not issued to all employees. The fact that upper management are most likely to have one, also means these are the people that attackers want to target – as they have access to more company secrets. Due to that fack we can suppose that we will see a rise in Mac malware –especially in the area of targeted attacks.

[1] Born Feb. 12, 1809, in Hardin County, Kentucky. April 14, 1865, Lincoln was assassinated at Ford's Theatre in Washington by John Wilkes Booth. Abraham Lincoln became the United States' 16th President in 1861, issuing the Emancipation Proclamation that declared forever free those slaves within the Confederacy in 1863.

On the mobile side, mobile companies are battling it out for the “inches” of space in your pocket. Whether it is an Android device, or iOS; a smartphone or a tablet – more and more of our time is spent using these devices, and less and less on traditional desktops and laptops. And Criminals are well aware of this fact, they know our “weakness” and for sure they will use that.

The mobile nature of these devices brings its own new security concerns. Using Geolocation, attackers can now not only infiltrate your device, but also track your movements in real-time. That same technology can be used for legitimate means. For example and advertiser may present an add for a Shop “X” that is only a few meters away.

On the other side, some of the traditional malware attacks do not work well on mobile devices. Picture for a moment 10,000 infected phones all part of a mobile botnet, and each of them sending spam or carrying out a DDOS attack. The battery life of most smartphones would have a hard time dealing with this, let alone the mobile network bandwidth. Also when it comes to stealing data, most of the data you have on your phone is already available on your laptop – which is an easier target for criminals. That is not to say that mobile botnets will not exist (in fact they exist already) – simply that their business models need to adapt until battery life improves. However, where mobile devices really excel is as spying devices, for targeted attacks. Look at the mobile spyware called “Flexispy[2]”, which can simply be purchased online. In addition to the normal behavior, you would expect from Spyware, it also has the ability to remotely control the camera and the microphone. That means that the attacker could first check the victims calendar, and when they go into an important board meeting – have the victims phone silently dial the attacker. The attacker can now listen in on the entire conversation-taking place.

Another emerging potential threat is NFC – Near Field Communication[3]. This technology has already been used in Japan for years to allow people to pay for services simply by swiping their phone at a terminal, and the same technology is now arriving to the rest of the world under various names.

Hacktivism really came into its own in the last couple of years, and there is very little reason to see it doing anything but increasing in impact. The internet is a perfect “vehicle” for people to protest. It allows for anonymity, ease of communication, and it is very hard to censor. It also has the possibility for ideas to go viral very easily. Whether Anonymous themselves exists in a few years is irrelevant, groups like them and WikiLeaks have opened Pandora's box for Internet Activists – and once opened it cannot be shut.

Another concept that is unlikely to go away is Cyberwarfare, and Cyber weapons. Stuxnet[4] was the first major attack to hit the news, followed by Duqu[5] and Flame[6] – and since then there is almost a new major APT discovered every month. In fact, knowledge of Nation-based espionage is now commonplace, and it’s assumed that most major nations are actively involved in this. Nations all around the world will ramp up their espionage and cyber capabilities, as well as their ability to defend themselves. Often when you hear a government

[2] http://www.flexispy.com/
[3] http://nearfieldcommunication.org/
[4] https://en.wikipedia.org/wiki/Stuxnet
[5] https://en.wikipedia.org/wiki/Duqu
[6] https://en.wikipedia.org/wiki/Flame_(malware)

talking about having more control over access to the internet, it is not simply to monitor their own citizens – but also to attempt to defend them from attacks from outside the country.

One of the big issues now with Cyber weapons is attribution. If a country launches a missile at a neighbor, that neighboring country can discover where the missile came from –and declare war on the aggressor. In Cyberspace however it is incredibly difficult to say with certainty where an a attack came from – and that is something you want to be sure of before dispatching your Air force on a bombing run.

Right now the leading countries have enough of an advantage that they will want it to stay that way, but as major military powers catch up with each other it is not too far-fetched to expect treaties on the use of Cyber weapons to arrive in the next number of years.

What about further out technologies to keep an eye on? Do you know what this is? This is Google Glass[7], an Android powered Augmented Reality device which Google has recently stopped working on. However this device really sparked the imagination for the whole world of Augmented Reality – in other words overlaying content on your normal vision. Right not I think it is about another 3-5 years before such devices go mainstream (with VR devices being mainstream in the next 18 months). Think about the possible attacks here though – what happens when an attacker can actually hack what you can see? That can be a real game changer.

Another area that will become a haven for cybercriminals is the so-called "Internet of Things[8]" or IOT for short. IOT refers to the connection of many embedded devices to the existing Internet infrastructure. This very broad area covers everything from Smart TV, Home Automation systems all the way to Internet connect Fridges that can send a tweet when you need milk. At the end of the day, all of these devices are just small computers –with a OS, network stack and everything else you would expect –and are mostly either Linux or Android based. Imagine having 20 such devices around your house. Now what happens when an attacker first infects your laptop and then moves laterally around your home network to all your smart devices? How does the ordinary person remove a malware from their internet connected Toaster? While there are of course Hollywood attack scenarios based around this of triggering gas explosions and so on, in reality for a financial criminal the main use is a huge amount of easy to infect and extremely difficult to clean machines that they can use for SPAM / DDOS.

Nowadays, devices like 'pacemakers" and "insulin' pumps can now be remotely controlled, and have been demonstrated to be able to be hacked and deliver lethal dosages / charges.

Technology will become more and more entwined, even inseparable, from the lives of humankind and another area to look at – vehicle communications systems, aka Car-To-Car communication. German[9] car manufacturers in particular have been investing heavily in the technology which will allows Cars to not only talk to each other, but also to traffic lights, signals etc. There are many useful applications of this such as automated traffic management, reduced insurance costs for proven good drivers and further out Self-driving vehicles. There are a number of potential hacks here too however – such as Tracking vehicles, or altering

[7] http://en.wikipedia.org/wiki/Project_Glass
[8] Jacob Morgan, Forbes Contributor, A Simple Explanation Of 'The Internet Of Things', May 13, 2014
[9] https://www.reuters.com/article/us-audi-trafficsignals-idUSKCN10Q1KL?

traffic signals. In fact researchers "Charlie Miller and Chris Valasek'[10] successfully remotely took full control of a Jeep - allowing for things like turning of the brakes, or injecting more fuel into the engine!

The General Data Protection Regulation[11] (GDPR) that is come in enforce on 25 May 2018. This regulation was made to harmonize data privacy laws across Europe, to protect and empower all EU citizens data privacy and to reshape the way organizations across the region approach data privacy.

The GDPR has come to us by necessity and we will see changes on language with no more complicated terms from business, the consent from the user in required and the silence its not any more an option. The transparency is one other important point on the transfer of data outside of the EU because the user must be noticed, the collect of data must be on well defined purpose and the automated decision its not any more an option without the possibility of the contest by the user. More stronger rights for the user as the user have the right to be informed on data breach, the user can be able to move his data from one place to another, the user have the right to copy his data that some business have on him and for sure the user have the right "to be forgotten' so he can clear his data from the companies.

So us we can see, new world with new rules and the future is coming and for sure the law enforcement agencies will have the first problems due to the open source information.

Lets finish with a quote: Winston Churchill[12] once said, *"If you're going through hell, keep going."* And, *"Never, never, never give up"*.

[10] Johana Bhuiyan, Famed hackers Charlie Miller and Chris Valasek are joining Cruise after leaving Didi and Uber, Jul 28, 2017

[11] https://www.eugdpr.org/

[12] Sir Winston Leonard Spencer-Churchill (30 November 1874 – 24 January 1965) was a British politician, army officer, and writer, who was Prime Minister of the United Kingdom from 1940 to 1945 and again from 1951 to 1955.