GLOBAL CYBER SECURITY CENTER

Newsletter

2016 April

Cyber Security is our mission

editorial

Dear readers,

new digital applications every day come into our lives, changing our habits, introducing new services and innovation, on the technology side and on the business models. The new Information and Communication Technology (ICT) paradigms lead in our societies numerous advantages with a trend that will increase in the coming years, it will be one of the determining factors for the economy of our country.

Companies and governments are working to transform their business successfully through digital technology. Digital Transformation will improve decision making, will increase the competitiveness of the country, accelerating development of new products / services, simplifying relations of citizens with the institutions and increasing transparency for the benefit of the whole community.

The scenario that digitalization promises us is an hyper-connected world where everyone and everything will probably be connected to Internet. In the manufacturing world, for example, the possibility of connecting new sensors and production lines (Internet of Things) will accelerate the digitalization processes increasing competitiveness, improving production and creating more services and, as a consequence, new business model.

On this issue, the European Commission tells us: "The more we depend on the Internet, the more we depend on its Security." In fact, increasing our dependence on the ICT systems, our vulnerability will grow, requiring a leadership on security and actions for reducing the risk.

Cybercrime, digital espionage and activism phenomena are increasing and will represent a serious threats to businesses, governments and citizens.

Digital Transformation cannot ignore the human factor; statistics show that this issue is still one of the main causes of ICT incidents. If we want to improve security and resilience, we cannot consider people as the only weak link in the system, people shall be the key factor.

People need to be educated in order to mitigate the risk, we have to provide them information on security issues via awareness and training campaigns.

The Digital Transformation is first and foremost a business transformation, is not just a technology change, but it touches the organizations at all levels and in particular the people and therefore the society. A successful digital transformation plan requires that security, cyber defense and resilience have to be key ingredients, these components must take a leading role during the project and must be integrated since the beginning.

Even people are essential and will have a primary role in ensuring information security, whether these are users, managers or information security experts. Together they will contribute to the success of this essential digital change for organizations and our country.

On these issues GCSEC is involving companies, universities and researchers with projects that are contributing to accelerate this evolution. This newsletter will be a moment of synthesis and reflection where we will share pills and ideas on cyber security issues, critical infrastructure, information security guidelines and trends, creating the necessary awareness for the challenges that lie ahead; a laboratory of ideas that we will share with you all.
Enjoy the reading

Nicola Sotira
General Manager GCSEC

events

SaS Forum
Date: 28 April, 2016
Location: Milan
http://www.sas.com/sas/events/16/sasforum-milan.html#english

GCSEC will participate at the XI edition of SAS Forum Milan, where with the contribution of SAS experts, customers, partners and universities, the power of analytics will be discussed in multiple application areas: from Customer Intelligence to Risk Management, from Fraud to Digital Transformation.

High Level Meeting Cyber Security. Enabling partnerships for a digitally secure future for EU
Date: 12-13 May 2016
Location: Amsterdam
http://english.eu2016.nl/events/2016/05/12/high-level-meeting-on-cyber-security

GCSEC will participate at the meeting on cyber security hosted by Dutch Ministry of Security and Justice and attended by high-level officials from the member states. The purpose of the meeting is to examine examples of best practice in the field of cyber security with our partners and to discuss future developments in terms of the strengthening of European cooperation. The meeting will have an interdisciplinary character and will be based on several relevant themes, including public-private partnership. The discussions will be conducted in an interactive and innovative manner.

Security Summit
Date: 7-8 June, 2016
Location: Rome
https://www.securitysummit.it/roma-2015/

Security Summit is the Italian event on cyber security that aims to disseminate knowledge on the main security issues facing in the digital world. During the conference are discussed technical and legal topics during plenary meetings,

in this number

"ATM security, a look at the future"

by Elena Mena Agresti, GCSEC

In the last few years the typology and number of attacks against Automated Teller Machine (ATM) systems have increased. The traditional attacks, like physical ATM theft, damages of its components, skimming to capture cardholder data from the magnetic stripe or Card trapping, are giving way to cyber attacks.

The cyber attack tactics, techniques and procedures could vary from the physical introduction of malwares onto the hard drive, to the point of stealing prepaid card numbers from database. In many cases attackers exploit vulnerabilities of the obsolete ATM operating systems, use malware specifically targeting to ATM systems or directly attack the automation system.

ATM malwares are not new and continue to increase. In 2013, Symantec has detected Ploutus, a malware that exploits a Windows XP vulnerability, opens a back door on the compromised ATM, allowing an attacker to dispense all money in the ATM. It activates the Trojan on demand and reads all cardholder information entered through the keypad.

In October 2014 the Russian security organization Kaspersky Lab has detected Tyupkin[1] an ATM malware that can withdraw cash directly from ATMs without compromising consumers' debit cards. In September 2015 FireEye has identified Suceful[2], the first multi-vendor ATM malware targeting cardholders and the experts of Proofpoint has detected GreenDispencervery[3] a malware very similar to Tyupkin.

Still in 2015 Kaspersky Lab has discovered Carbanak[4], an Advanced Persistent Threat (APT) that with a spear-phishing attack can access to the bank's network to steal money sending remote instructions to ATM system. According with Kaspersky Lab[5] "losses per bank range from $2.5 million to approximately $10 million and total financial losses could be as a high as $1 billion".

Again Kaspersky Lab has revealed two new hacker groups, called Metel and GCMAN[6]. In particular, Metel infects the bank network with a modular malware also known as Corkow installed through a spear-phishing attack. The gang scans network to identify its target, that is the bank operator's money-processing system, obtains access and automates the rollback of ATM transactions and steals money via debit card at different ATM machines. In this way, when attackers withdraw money at ATM the balance on the cards remain the same, allowing for multiple transactions.

[1] http://usa.kaspersky.com/about-us/press-center/press-releases/2014/kaspersky-lab-and-interpol-discover-tyupkin-malware-targeting
[2] https://www.fireeye.com/blog/threat-research/2015/09/suceful_next_genera.html
[3] https://www.proofpoint.com/us/threat-insight/post/Meet-GreenDispenser
[4] https://web.archive.org/web/20150217133401/https://securelist.com/blog/research/68732/the-great-bank-robbery-the-carbanak-apt/
[5] https://securelist.com/blog/research/68732/the-great-bank-robbery-the-carbanak-apt/
[6] https://securelist.com/blog/research/73638/apt-style-bank-robberies-increase-with-metel-gcman-and-carbanak-2-0-attacks/

roundtables and training sessions.

InfoSecurity Europe

Date: 7-9 June, 2016
Location: London
http://www.infosecurityeurope.com

InfoSecurity Europe is the founding event of InfoSecurity Group. This annual conference has evolved into one of the largest and most highly regarded security events held in Europe, a reputation that is bolstered by the conference's free admission. In 2014, approximately 11,500 visitors from over 70 countries attended InfoSecurity Europe. Last year, more than 12,000 visitors came out to see over 260 speakers present on security-related topics, as well as to visit 316 different exhibitors' booths

The 4th International Conference on Cybercrime and Computer Forensics (ICCCF)

Date: 12-14 June 2016
Location: Vancouver, Canada
http://www.apatas.org/icccf/icccf-2016/

For the past four years, APATAS has organized the International Cybercrime and Computer Forensics conference at various locations throughout Asia. In 2016, our 4th annual ICCCF is moving for the first time to Simon Fraser University's Harbour Centre campus and Centre for Dialogue at downtown Vancouver, Canada. North America has been a pioneer in cybercrime research, policy and practice since the mid-1980s. As expected, we have witnessed increasing technological developments in both personal computing and in smart-phone and wireless devices that have had an impact on how technology-enabled crimes have been committed in the Asia Pacific region and beyond. One of the key approaches to understanding such crime is through research and incorporating the outcome of research into policy and practice. The 4th Annual ICCCF 2016 Vancouver, BC, Canada therefore focuses its discussion on 'Cybercrime: Linking Research, Policy, and Practice.

This type of attacks has affected many ATMs around the world from Mexico, Russia, USA, Asiatic and European country. In January 2016, The Romanian National Police and the Directorate for Investigating Organised Crimes and Terrorism (DIICOT), with Europol, Eurojust and some European Law Enforcement Authorities, have arrested an international criminal group responsible for a large-scale ATM attacks using Trojan horse.

Cyber attacks to ATM systems are very difficult to identify, the attackers use several techniques to hide or erase their presence and avoid detection. Furthermore the ATM will become the object of attack due the changing operational model of banks that will provide innovative services directly from ATM reducing service delivery from the branch.

The report "ATM Future Trends 2015", published by ATM Marketplace and Auriga, shows U.S. consumers' interest in enlarging the ATM services. According with Coin ATM Radar[7], that tracks the number and location of Bitcoin, there are currently 661 Bitcoin ATMs installed all over the world. US is the leading country with 270 Bitcoin ATMs followed by 101 Canada, 31 UK, 23 Australia, 18 Spain, 16 Finland, 13 Japan and Switzerland, 12 Czech Republic ad 9 Italy.

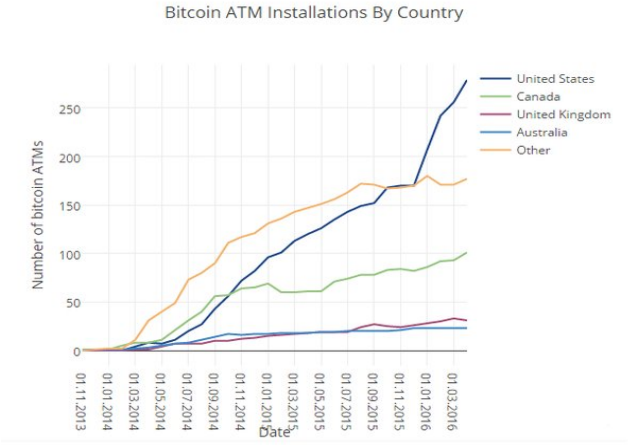

Figure 1: Bitcoin Installations By Country

ATMs are and will be key actors in the banks that are redefining the role of teller. The traditional transactional function related to the management of cash and receipts/payments will be increasingly reduced. From few years we can withdraw and deposit money and checks in ATM. In some places in the world, ATMs allow customers to speak with a remote teller with live-video technologies. The remote teller can assist customers in almost all traditional transactions. With remote tellers, banks can provide 24/7 services where and when the customer want with a cost saving and probably with greater customer satisfaction.

In fact, emerging ATM services will guarantee to customers to obtain email receipts, bill payments, made real-time transaction, cash and withdrawal using mobile app or contactless technologies.

The ATMs market probably will be positively impacted by new technologies and benefit from them but the ATMs will be exposed directly or indirectly to new threats, vulnerabilities and attacks. Furthermore, banks will have to correctly manage the transition period from old and new technologies and the coexistence phase and protect the new authentication systems that could become the weakest link tapped by attackers. ATM deployers are aware that advanced security devices and regulatory compliance are not sufficient to face the "creativity" of criminals. Advanced Persistent Threats are seriously threatening several kinds of infrastructures and ATMs systems could be a profitable target.

The future of ATMs should consider how to improve the countermeasures to fight the new attack typologies, above all considering the new services ATMs could deliver.

For these reasons, GCSEC is coordinating a study to provide an overview of current security concerns of ATMs, considering the classic and emerging threats, the evolution of the ATMs systems and services and the security concerns it implies. The study intends to share experts' recommendations with decision makers, security managers of banks, ATM deployers and security experts in order to aware all stakeholders on security implications behind the services delivered nowadays and in the future.

[7] http://coinatmradar.com

news

MasterCard's Machine-Learning Network Thwarts ATM Attacks
http://blogs.wsj.com/cio/2016/02/23/mastercards-machine-learning-network-thwarts-atm-attacks/

During a Wall Street Journal interview, MasterCard Inc. says new machine-learning technology has helped it quickly control three separate cyber attacks that targeted automated bank tellers, limiting the damage to about $100,000 each. The Safety Net system, rolled out globally late last year, analyses more than 1.3 billion transactions per day involving MasterCard debit and credit accounts at banks, merchants and ATMs, using algorithms that assess customer behaviour in real-time.

UK Government Chief Scientific Adviser has published a great study on "Distributed Ledger Technology: beyond block chain"
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf

Distributed ledgers offer a range benefits to government and to other public and private sector organisations. This report sets out the findings of a review exploring how distributed ledger technology can revolutionise services, both in government and the private sector. Only when they have other applications — such as smart contracts — layered on top on them, that their full potential can be realised. This study provides recommendations for maximise the opportunities and reduce the risks of this new technology.

First IOS Trojan exploiting apple DRM Design to infecting any apple device
http://researchcenter.paloaltonetworks.com/2016/03/acedeceiver-first-ios-trojan-exploiting-apple-drm-design-flaws-to-infect-any-ios-device/

Team of Palo Alto Network have discovered a new family of iOS malware that successfully infected non-jailbroken devices we've named "AceDeceiver". AceDeceiver is the first iOS malware that abuses certain design flaws in Apple's DRM protection mechanism to install malicious apps on iOS devices regardless of whether they are jailbroken. Apple allows users purchase and download iOS apps from their App Store through the iTunes client running in their computer. They then can use the computers to install the apps onto their iOS devices.

“Collaboration and Information Sharing for Cyber security"

by Giovanni Abbadessa - IBM

WHY GOOD GUYS MUST COLLABORATE TO IMPROVE CYBERSECURITY

The impressive growth of the Internet with billions of connected devices, and its further expansion with the so-called Internet of Things (IoT), allows access in a simple and fast way to data and services, changing the world economic scenario. This positive step is jeopardized by the explosion of computer-related crimes, which exploit system vulnerabilities, to perpetrate illegal activities, with the aim of making a profit, steal confidential information or damage critical infrastructure. According to a study by the Center for Strategic and International Studies, "The Economic Impact of Cybercrime and Cyber Espionage"[8], the global cost of cybercrime is between 300 billion and one trillion dollars a year.

To take advantage of the possibility of unlawful gain, the Cybercrime has evolved and created new business models, moving within a few years from hacker who operated individually, or in small communities, to a business model referred to as Crime- as-a-Service (**CaaS**). **CaaS** provides a broad set of business services: botnets, denial-of-service, customization of malware, tools for data theft and password cracking, phishing services, zero-day-attacks that facilitate virtually any cybercrime and stimulate its innovation and growth. The CaaS model, allowing cybercriminals to work more effectively, sharing the techniques of attack, tools and objectives, makes easier the way such attacks are conducted, improving their success rate (see. "IBM X -force Threat Intelligence Quarterly, 2Q 2015" [9]).

The cooperation level between cybercriminals has been further highlighted by the "Darkode" operation that FBI and Europol led jointly. This operation led to the identification and shutdown of one of the most important hackers forums in English, with branches in twenty countries and the participation of about 250-300 active members. In addition to selling services and tools for the attacks, members of this community shared knowledge, ideas, suggestions, creating a virtual think-tank.

To keep up with these increasingly complex attacks, our attention must be focused on actions at an earlier phase of the cyber attack life cycle, to create a common ground for standardizing threat information. We have to push as much as possible toward early detection and prevention — ideally before the exploit phase happens. To improve your detection capability, it is a must using infrastructures that are able to consume “actionable security intelligence”, to move as much as possible to automatic detection and countermeasure.

The awareness that collaboration and sharing of information about vulnerabilities, threats and attacks improve security was a common heritage from the birth of the first CERT, but the actual realization of this paradigm has always clashed with the reluctance of companies or administrations to share such information.

Beside companies’ reluctance to share information about attacks and vulnerabilities, there is also a real difficulty due to way to find a common way to describe what has been discovered. More, the sharing process takes time and resources. To overcome these difficulties some standards has been deployed. We will illustrates a few, recommending to read the ENISA document “Standards and tools for exchange and processing of actionable information”[10] to find more info. Until 1999 there was no common way to describe a vulnerability, each vendor used its own names for security vulnerabilities. The consequences were potential gaps in security coverage and no effective interoperability among the disparate databases and tools. This issue has been solved introducing Common Vulnerabilities and Exposures (CVE®), a dictionary of common names (i.e., CVE Identifiers) for publicly known cyber security vulnerabilities[11]. CVE's common identifiers make it easier to share data across separate network security databases and tools and provide a baseline for evaluating the coverage of an organization’s security tools.

Similarly, FIRST developed the Common Vulnerability Scoring System (CVSS) an open framework for communicating the characteristics and severity of software vulnerabilities, to permit an easy categorization of the risks related to a specific vulnerability.

ENISA has published a study on Security Incidents Indicators
https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/studies/security-incidents-indicators

To address this issue, indicators are used, accompanied by thresholds, to assess the impact of incidents. This approach allows evaluation of incidents from various perspectives, such as business perspective, compliance with regulations, root causes, impact on customers etc. Incidents can vary in nature, and this report tries to include as many indicators as possible, so that as many types of incidents as possible are covered.

UK and US to simulate cyber-attack on nuclear plants
http://www.theguardian.com/uk-news/2016/mar/31/uk-us-simulate-cyber-attack- nuclear-plants-test-resilience

Britain and the US plan to cooperate by exploring the resilience of nuclear infrastructure to a terrorist attack. In particular, countries will stage a war-game later this year, simulating a cyber attack on a nuclear power plant, to test the readiness of the government and utility firms.

Homeland Security Department Launches Cyber Threat Sharing Platform
http://blogs.wsj.com/cio/2016/03/21/homeland-security-department-launches-cyber-threat-sharing-platform/

The U.S. Department of Homeland Security launched a platform that allows the government and private sector to exchange cybersecurity threat information with one another, part of a larger federal push to bolster cybersecurity. The platform uses technical specifications including the Trusted Automated eXchange of Indicator Information (TAXII), which defines a set of services and message exchanges that, when implemented, enable sharing of actionable cyber threat information.

Megabreach: 55 MILLION voters' details leaked in Philippines
http://www.theregister.co.uk/2016/04/07/philippine_voter_data_breach/

A massive data breach appears to have left 55 million Philippine voters at much greater risk of identity fraud and more. Security researchers warn that the entire database of the Philippines’ Commission on Elections (COMELEC) has been exposed in what appears to be the biggest government related data breach in history. The COMELEC website was compromised and

[8] http://csis.org/publication/economic-impact-cybercrime-and-cyber-espionage
[9] https://ibm.biz/Bd4PAx
[10] https://www.enisa.europa.eu/activities/cert/support/actionable-information/standards-and-tools-for-exchange-and-processing-of-actionable-information/at_download/fullReport
[11] https://cve.mitre.org/about/

Recognizing the importance of sharing data on incidents, the DHS Office of Cyber security and Communications, National Cyber security and Communications Integration Center, and US-CERT are leading efforts to automate and structure operational cyber security information sharing techniques across the globe. This is where the Trusted Automated Exchange of Indicator Information (**TAXII**), Cyber Observable Expression (**CybOX**) and Structured Threat Information Expression (**STIX**) come in. They are an open community-driven effort and a set of free, available specifications that would help with the automated exchange of cyber threat information in a standardized format. They are not pieces of software themselves, but rather standards that software can use. The combination of STIX and TAXII allow to more easily share threat information with your constituency and peers [12] [13].

TAXII is a set of specifications for exchanging cyber threat information to help organizations share information with their partners. TAXII is not an information sharing program itself and does not define trust agreements, governance, or other non-technical aspects of collaboration. Instead, TAXII empowers organizations to share the information they choose with the partners they choose.

STIX is a language for having a standardized communication for the representation of cyber threat information. Similar to TAXII, it is not a sharing program or tool, but rather a component that supports programs or tools. The STIX language has a number of constructs or components. CybOX provides a common structure for representing cyber observables across and among the operational areas of enterprise cyber security. CybOX can be used for threat assessment, log management, malware characterization, indicator sharing and incident response. Putting all together, we can say that STIX is a language that can use CybOX words, and the communication is possible with TAXII.

You have already noticed that should move your capability to discover earlier that something nasty is occurring. How can you accomplish this? Here you can find a non-exhaustive list of some threat sharing platforms that would improve your capabilities to discover and to make actionable information on vulnerabilities and threats.

IBM launched one years ago **X-Force Exchange** (XFE) [14] a “free cloud-based threat intelligence sharing platform" that enables security experts:

- to seek, through a simple and intuitive interface, information on the latest threats;
- to aggregate data in order to be make them easily usable and eventually sharable among the your security peers, using STIX and TAXII standards;
- to use the information provided on XFE also through APIs, to integrate them in near real-time mode in your operational processes, improving the analysis and response phases.

Security vendor AlienVault already runs the **Open Threat Exchange**[15] (OTX), a crowd-sourced threat intelligence sharing platform. It delivers community-generated threat data, enables collaborative research, and automates the process of updating your security infrastructure with threat data from any source. OTX enables anyone in the security community to actively discuss, research, validate, and share the latest threat data, trends, and techniques, strengthening your defenses while helping others do the same. Facebook has just launched in a beta version **ThreatExchange** [16], with Yahoo, Tumblr, and Dropbox joining the initiative.

Widespread and effective threat intelligence sharing can provide defenders a better chance to detect, divert and avoid threats. It is time to look into and keep what is the best for your organizations.

defaced on 27 March by Anonymous Philippines before a second hacker group, LulzSec Pilipinas posted COMELEC’s entire database online days later. All sorts of sensitive information – including passport information and fingerprint data – appears to have been included in the data dump.

New National Cyber Security Centre set to bring UK expertise together

https://www.gov.uk/government/news/new-national-cyber-security-centre-set-to-bring-uk-expertise-together

The new National Cyber Security Centre will be the authoritative voice on information security in the UK and one of its first tasks will be to work with the Bank of England to produce advice for the financial sector for managing cyber security effectively.
In setting up the NCSC , The UK government will adopt structured consultation with the private sector. The objectives are to raise awareness of government intent; undertake genuine dialogue that shapes service delivery; demonstrate serious commitment to listen; and develop sustainable engagement channels.

Study on effect that a coordinated cyber attack on the UK's power distribution network

http://www.lockheedmartin.com/us/what-we-do/information-technology/cybersecurity/blackout.html

The Cambridge Centre for Risk Studies at the University of Cambridge Judge Business School and Lockheed Martin have been working together on the first study of its kind to explore the effect that a coordinated cyber attack on the UK's power distribution network could have.

[12] https://securityintelligence.com/how-stix-taxii-and-cybox-can-help-with-standardizing-threat-information/
[13] https://www.us-cert.gov/Information-Sharing-Specifications-Cybersecurity
[14] https://exchange.xforce.ibmcloud.com/
[15] https://www.alienvault.com/open-threat-exchange
[16] https://developers.facebook.com/products/threat-exchange