GLOBAL CYBER SECURITY CENTER

Newsletter

2018 May

Cyber Security is our mission

editorial

Living in the bubble?

Blockchain is now the magic keyword in any conventions, finding more and more spaces in all disciplines. We have not to be surprised if football will adopt, one day, in some areas, this technology, maybe for writing in a Digital Ledger for the soccer referee decision.

This is certainly a very current topic and cannot be ignored. Economic data on the Bitcoin Blockchain phenomenon are clear. World Economic Forum forecast is that 10% of global gross domestic product (GDP) will be stored on blockchain technology and analyst of the investment bank UBS are talking of a volume of 300 billion dollars generated within 2027. So, we may easily forecast that the blockchain technology is not going to disappear.

Another keyword, often associated with Bitcoin and Blockchain technology is security, it is implicitly assumed that the technology is safe and therefore risk free.

We have to bear in mind that Bitcoin or cryptocurrencies in general are controlled by a private key, anyone who gains access to the private key can have the access to the currency. This is one of the vulnerabilities that could empty your account. If someone holds cryptocurrency using a third-party service, the risk that the service gets robbed is a possibility, something that happened already in the Bitcoin history. A solution to this would be to keep the currency in your system, which in any case does not guarantee immunity from attacks and requires in any case a security experience that is not so widespread.

Another risk widely considered in the IT are the bugs, something that may cause significant damage to cryptocurrency holdings. This issue, of course, may have an effect on any cryptocurrency infrastructure but we have to imagine what may happen when bugs will play in a smart contracts scenario. Also, this is not the hypothesis of something that already happened and luckily the damage was limited. And if we are able to minimize bugs issue we have to bear in mind that this infrastructure will face worm issue that may exploit all the connected node as a broadcast message in the same network, and the incentive for thieves to deploy worm will be very high.

Another point is related to the fact that the technology has no central authority that may censor forgetting that Government can intervene to kill this process. Today we may convert Bitcoin or in general cryptocurrencies back to a local currency, but authorities or Government may stop this process making cryptocurrencies unusable.

Of course, I did not touch all the aspect of the criminal activities. There are many people that think that Bitcoin will enable illegal activities increasing their bandwidth. I think that this is another realm that requires much more reflection. This is not a critic on the cryptocurrencies platform, but is just an invitation to read also in a critical way everything and keep our eyes open and be informed, one of the GCSEC's mission…

Enjoy your reading

Nicola Sotira
General Manager GCSEC

events

Osservatorio delle Competenze Digitali 2018

Location: Rome, Italy
Date: June 5, 2018
http://www.assintel.it/eventi/osservatorio-delle-competenze-digitali-2018/

How does digital transformation impact on the skills necessary for companies and public administrations? How do the professions in ICT evolve and how are the other professions "digitized"?

These are the main questions from which the 2018 Observatory has started to activate both propositional responses and, above all, an awareness of all the Stakeholders.

Security Summit

Location: Rome, Italy
Date: June 6-7, 2018
https://www.cybersecitalia.it/eventi/

Organized by Clusit - Italian Association for Information Security - and Astrea, a communication and marketing agency, Security Summit is the most important event on the security of information, networks and IT systems in our country. Now in its tenth year, it pursues year after year the mission to increase awareness of IT risks among administrations of all sizes and sectors and among citizens, who increasingly use online services.

BSides Milano and OWASP Day 2018

Location: Milan, Italy
Date: June 16, 2018
http://milano.securitybsides.eu/

With Prof. Stefano Zanero and the Bsides Milano team OWASP is organizing a unique event that will be an OWASP Day together with the Bsides Milan Conference.

The event will show several points of discussion: we will present the state of the art of the Secure Software Initiatives and

in this issue

From WannaCry to WannaShare: a public/private collaboration to build an effective Info Sharing community

by Giovanni Mellini – ENAV

Everyone in the InfoSec community remembers friday May 12, 2017 the day of the WannaCry global attack.

In ENAV, the Italian air navigation service provider where I'm heading the "Information, Systems and Network security" division, we spent the weekend and following days looking for attack IoC (Indicator of Compromise), implementing mitigation and detection strategies and exchanging these info with other italian SOC/CERTs.
We did this in an unstructured way: by email and phone.

The info exchange was effective, we shared a lot of data, but I was aware that our SOC analysts wasted a lot of time doing activities that could be easily automated: IoC gathering, parsing of unstructured data and injection into our detection systems.
I think that everyone agrees that this time could be used for value-added activities like coordination, real-time analysis and mitigation strategies, for example detection of lateral movements based on WannaCry behavior and sinkholing of killswitch servers (see https://scubarda.com/tag/wannacry/ for details).

After things calmed down I was thinking on how to automate the info gathering process with a simple goal in mind: automatically use the information received from trusted sources, with the ability to enrich and re-share.
This means for me to start building an active and effective info sharing network: a community.

Building a community is a complex task but in this case we had an advantage: the trust - the key to building a community – derived from a destructive event with info and best practices exchange. We could not miss the opportunity.
In a few months the community had grown and everyone agreed to work on a bottom-up paradigm to build an effective info sharing network; today there are 60 people representing 25 public and private companies and entities that are working together to reach this goal.

technical speeches about the new researches in Application Security.
We will organize a round table regarding women in Application Security.
As conclusion of the day, we organize a round table discussing the most interesting subjects came out during the event.
Conference goal is creating a debate on which will be the evolution of the research for the Web Application Security, and how to start a secure software initiative.

news

Malware campaign expands to add cryptocurrency mining and iOS phishing attacks

https://threatbrief.com/malware-campaign-expands-to-add-cryptocurrency-mining-and-ios-phishing-attacks/

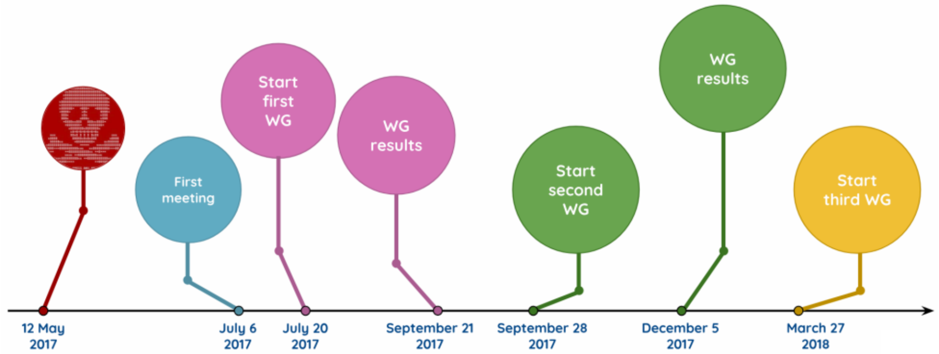
A rapidly evolving information-stealing malware campaign has added iOS device phishing and cryptocurrency mining to its arsenal, having previously just focused on Android targets. Dubbed Roaming Mantis, the initial attacks mostly targeted South East Asia, but now the malware has been updated with the capability to specifically target users across Europe and the Middle East.
Those behind the criminal operation have even expanded attacks to cater for 27 different languages — including English, Spanish, Hebrew, Chinese, Russian and Hindi — in order to help coordinate successful infections. The additional languages have been added via an automatic translator.

Malicious php script infects 2400 websites

https://threatpost.com/malicious-php-script-infects-2400-websites-in-the-past-week/132161/

A botnet dubbed Brain Food is giving webmasters indigestion with related attacks that push bogus diet pills and IQ-boosting pills via web pages hosted on legitimate sites. So far, spammers have been successful, thanks to an effective Hypertext Preprocessor (PHP) script (also called Brain Food) that has adroitly avoided detection on websites hosting the pitches.

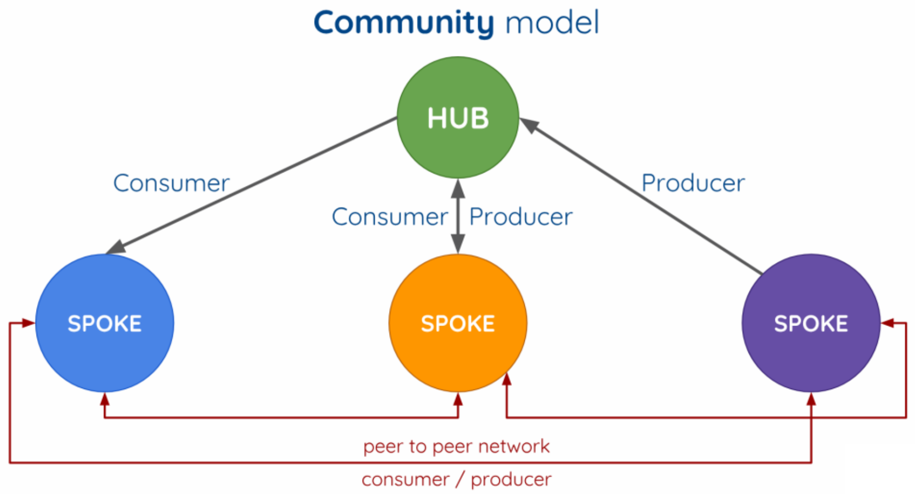
Over the past four months, researchers at Proofpoint said they have tracked 5,000 Brain Food compromised websites. In a post outlining its research Friday, Proofpoint said 2,400 of those compromised sites have been active over the past seven days pushing dubious pills under the false premise the product claims made were originally on television shows Shark Tank and on identified as Entertainment Today.



We used an incremental approach made of small working groups whose goal is the building of operational prototypes to test small tasks and deploy it:

- we agreed to use STIX as language for IoC description and TAXII as transport mechanism, respecting the need to know principle (no useless data has to be shared);
- we tested the interoperability between available open-source software (don't reinvent the wheel) focusing on IoC consumption and sharing. Software tested include MineMeld, Cabby, MISP, OpenTAXII;
- we integrated the CERT-PA InfoSec public feed into the STIX/TAXII network and started to use the IoC in operations (SOC/CERT);
- we allowed IoC producers to push their IoC into the community network so they could be shared with other parties.

The community is based on a simple hub and spoke model where each node can be a consumer and/or a producer.
Producers and consumers both benefit from community participation:



- indicators pushed into the network are immediately available for consumption, increasing the whole community protection level;
- trusted parties can contribute in an easy and standard way;
- threat evolution can be easily tracked.

At the end we are moving from WannaCry to WannaShare, increasing situational awareness during crisis and regular security operations.

Interested in learning more? Ping me at giovanni [dot] mellini [at] enav [dot] it

High-level vulnerabilities discovered in 84% of Android shopping apps
https://www.helpnetsecurity.com/2018/05/23/android-shopping-apps/
More than 84% of the shopping apps have three or more high-level security vulnerabilities, according to a security assessment by Appknox and Seworks.

A total of 274 vulnerabilities were detected among the top 50 Android mobile shopping apps, and all had security risks. The apps were tested across 34 different security testing categories.

Why You Must Treat Artificial Intelligence (AI) As A Very Special Technology
https://www.forbes.com/sites/steveandriole/2018/05/20/why-you-must-treat-artificial-intelligence-ai-as-a-very-special-technology/2/#d91f68e6ca00

There are lots of technologies that attract our attention – and money – these days. We're obsessed with blockchain, cryptocurrency, IOT, big data analytics, cybersecurity3-D printing and drones. We're excited about virtual reality, augmented reality and mixed reality. We love talking about driverless cars, ships and planes. We can't wait for 5G and Wi-Fi domes that solve all of our network access problems; and while we're getting a little worried about social media and privacy, we're still addicted to our ever-more-powerful smartphones. We buy everything online. We're into wearables.

But there's one technology that we all need to embrace: artificial intelligence (AI). While there are other families in the disruptive digital technology world, this one is special and one you cannot afford to treat as just another emerging technology. AI powers, amplifies and therefore supersedes them all.

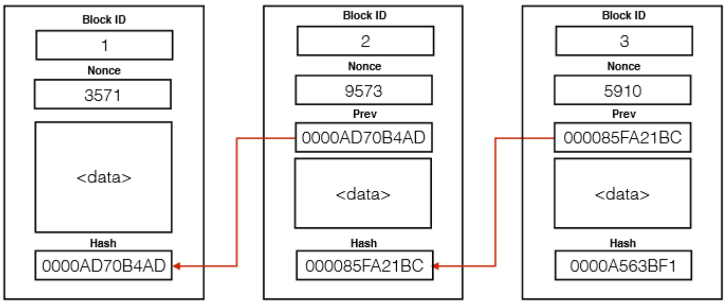
Teen phone monitoring app leaked thousands of user passwords
https://www.zdnet.com/article/teen-phone-monitoring-app-leaks-thousands-of-users-data/
At least one server used by an app for parents to monitor their teenagers' phone activity has leaked tens of thousands of accounts of both parents and children.

The mobile app, TeenSafe, bills itself as a "secure" monitoring app for iOS and Android, which lets parents view their child's text messages and location, monitor who they're calling and when, access their web browsing history, and find out which apps they have installed.

PDS2 and new money

by Francesco Corona – Professor and director of Hacking and Security Engineering Master's program

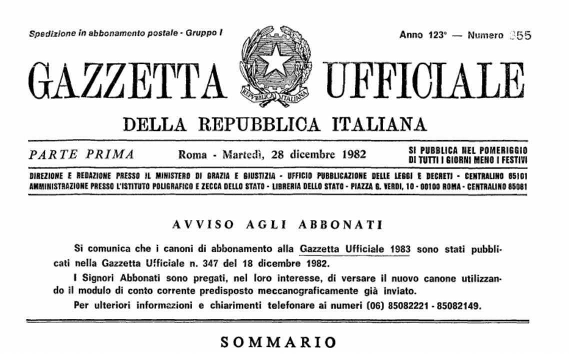
We are witnessing an ever-increasing phase of monetary dematerialization. The PSD2 will facilitate, in the coming years, this process already started with the first Directive 2007/64 / EC (so-called PSD, Payment Services Directive), in which all service providers of monetary circulation are substantially placed on the same level, thus implementing a competitive mechanism in which the public role essentially becomes that of regulating the money supply and in a desirable way also that of any "supplier" of complementary virtual currency.



- **Block Number:** An integer unique number that represents the block.
- **Nonce:** An integer random number
- **Data:** The set of information stored in the blockchain (e.g. transactions, contracts, documents, etc...)
- **Hash:** the hash code of the block. It depends on all the previous fields. More over this alphanumerical string is characterized by the presence of four initial characters equal to 0. See Section 3.2 for more details.

Therefore, the public role is best considered in consideration of the fact that the Authority appointed to the control will on one hand supervise the economic transactions of all intermediaries in a typical value chain (Customers-Intermediaries-Banks-Authority) and on the other guarantee the monitoring and control of transactions on its own national territory in order to promptly determine the monetary flows of digital payments to better implement their fiscal policies.

The recent PSD2 legislation will also impose evolving economic scenarios no longer based on the current model of trust between customers and banks but on the logic of consensus in which we will see new intermediaries of transactions. The subjects of a chain of economic value or transaction will own a block of information with their own access keys. Therefore, a successful transaction will consist of different blocks of ownership of the bank that will have the consent and therefore the access keys of all individuals. These block-chain models have already demonstrated their intrinsic robustness with bitcoin-based payments and can be used for the management of new complementary government currencies to be added to the euro or to other legal tender currencies on specific baskets of goods and services.



Spedizione in abbonamento postale - Gruppo I Anno 123° — Numero 355

GAZZETTA UFFICIALE

DELLA REPUBBLICA ITALIANA

PARTE PRIMA Roma - Martedì, 28 dicembre 1982 SI PUBBLICA NEL POMERIGGIO DI TUTTI I GIORNI MENO I FESTIVI

DIREZIONE E REDAZIONE PRESSO IL MINISTERO DI GRAZIA E GIUSTIZIA - UFFICIO PUBBLICAZIONE DELLE LEGGI E DECRETI - CENTRALINO 65101
AMMINISTRAZIONE PRESSO L'ISTITUTO POLIGRAFICO E ZECCA DELLO STATO - LIBRERIA DELLO STATO - PIAZZA G. VERDI, 10 - 00100 ROMA - CENTRALINO 85081

AVVISO AGLI ABBONATI

Si comunica che i canoni di abbonamento alla Gazzetta Ufficiale 1983 sono stati pubblicati nella Gazzetta Ufficiale n. 347 del 18 dicembre 1982.

I Signori Abbonati sono pregati, nel loro interesse, di versare il nuovo canone utilizzando il modulo di conto corrente predisposto meccanograficamente già inviato.

Per ulteriori informazioni e chiarimenti telefonare ai numeri (06) 85082221 - 85082149.

SOMMARIO

Already in the 1980s, on the basis of the Malaga agreements, Italy formulated a ministerial regulation with the approval of the International Monetary Fund for the use of a scriptural currency called Franco Oro, a coin used in telephone circuits and which could be restored with different names and functions to relaunch specific national and transnational market economies.

Interested in learning more? Ping Prof. Francesco Corona at f [dot] corona[at] unilink [dot] it