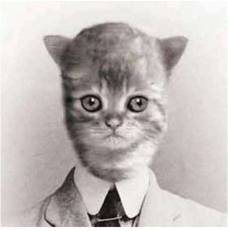
Matthijs R. Koot's notebook

Personal blog. Hobbies: IT, security, privacy, democracy.

Search



Twitter: @mrkoot
LinkedIn: my profile
E-mail: koot at cyberwar dot nl
PGP key: 51F9 8FC9 C92A 1165 (verified via Keybase.io)

Employed at Secura B.V.

MSc in OS3 System & Network Engineering (2005-2006) and PhD in data anonymity (2007-2011) from University of Amsterdam.

Many posts on this blog are scraps of information, published for posterity and reference. Posts prior to Q2/2012 were submitted while I was employed at the University of Amsterdam.

Links

Critical thinking

- Master List of Logical Fallacies
- Taxonomy of Logical Fallacies
- Your Logical Fallacy Is
- Understanding Uncertainty
- A Skeptical Manifesto

Other

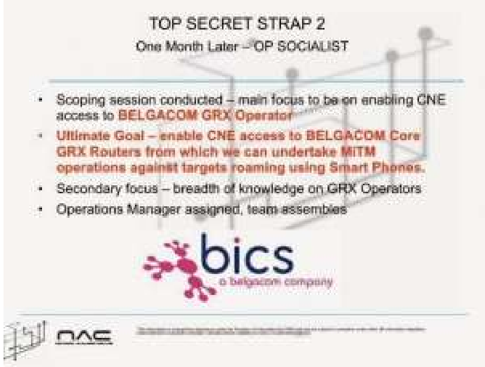
- The 20% Statistician (Daniël Lakens)

Belgacom — “On the brink of catastrophe” (translation)

Posted on 2013-09-23 by mrkoot

UPDATE 2018-09-20: *~~according~~ to Belgian news paper De Tijd, a new confidential report by the Belgian public prosecutor delivered to the Belgian government contains new clues pointing to GCHQ's involvement in the Belgacom hack. The public prosecutor investigated a link to a computer in Indonesia, and when asking for information about its IP address, had learned that the British government had also asked questions about it. Furthermore, computers traced to other countries could be linked to the U.K., because some had been paid using anonymous prepaid payment cards that had been bought in the U.K. And lastly, when computer specialists were able to secure a copy of the malware back in 2013, it was found to contain names like `Daredevil' and `Warriorpride'; from documents leaked via Snowden it is apparent that these names can be linked to CNE activities by GCHQ and the NSA.*
UPDATE 2014-12-13: *10 new documents ~~released~~. Three new stories. latter two in Dutch. 1) ~~The Inside Story of How British Spies Hacked Belgium's Largest Telco~~ (The Intercept), 2) Lees hier hoe de Britse geheime dienst GCHQ Belgacom aanviel (in Dutch, NRC Handelsblad), 3) Britse spionage bij Belgacom ging veel verder dan bekend (in Dutch, NRC Handelsblad)*
UPDATE 2014-11-24: *~~Secret Malware in European Union Attack Linked to U.S. and British Intelligence~~ (The Intercept)*
UPDATE 2014-10-26: *~~GCHQ cyber-attack cost €15m, says Belgacom security head Fabrice Clement~~ (Computing.co.uk)*
UPDATE 2014-05-30: *Slides from Hack in the Box 2014 Amsterdam: HITB2014AMS – Day 2 – On Her Majesty's Secret Service: GRX & A Spy Agency*
UPDATE 2013-12-04: *Flemish newspaper De Tijd ~~reports~~ (in Dutch) that Belgacom is still struggling to control the remains of the malicious spyware at BICS. The remaining malware is said to be “so complex” that it baffles experts.*
UPDATE 2013-11-10: *here are a few Snowden-slides from GCHQ that mention Belgacom (click to enlarge). Der Spiegel ~~reported~~ (in English) that GCHQ used fake, malicious LinkedIn and Slashdot sites to lure Belgacom engineers and get malware on their computers to obtain access to a GPRS roaming exchange (GRX) router system operated by Belgacom-subsidiary BICS.*

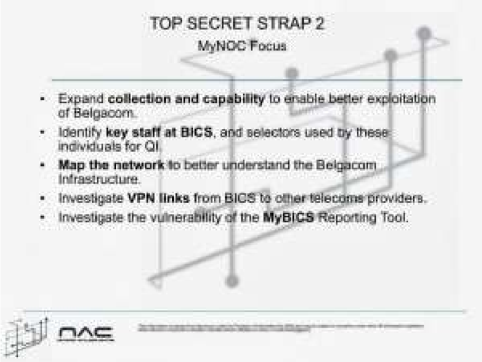
Adam Shostack
Albert Benschop (UvA)
Alessandro Acquisti's The Economics of Privacy
Amsterdam Platform for Privacy Research (UvA-APPR)
Archive of Privacy/Security/Hacking Videos
Arno Reuser's OSINT resources
Bits of Freedom
IEEE Cipher S&P Calendar
Cryptome
Cyber CoE (US Army)
DCAF
DefenceTalk
Didier Stevens
Electronic Frontier Foundation
Electrospaces (Peter Koop)
Eric Rescorla
Harvard National Security Journal
IEEE Information Theory Society
Inlichtingendiensten.nl
IntelNews.org
Intelligence & Information
Intelligence and National Security Alliance
Jaap-Henk Hoepman
Jeroen van der Ham
Jesus Oquendo
Krypt3ia
Light Blue Touchpaper
MIT OpenCourseWare
Netherlands Intelligence Studies Association (NISA)
Open & Free Tech Community
Pew Research Center
Privacy International
Privacy by Design
Signal Identification Guide
Richard Bejtlich
Ross Anderson's Economics and Security Resource Page
Simon Davies



TOP SECRET STRAP 2
One Month Later – OP SOCIALIST

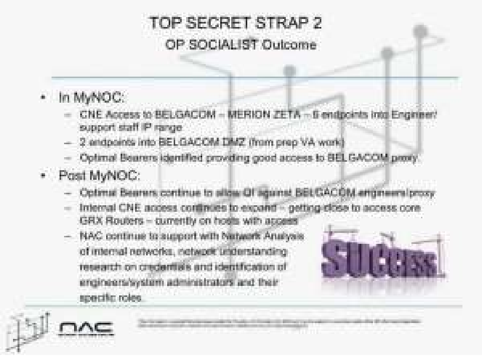
- Scoping session conducted – main focus to be on enabling CNE access to BELGACOM GRX Operator
- **Ultimate Goal – enable CNE access to BELGACOM Core GRX Routers from which we can undertake MITM operations against targets roaming using Smart Phones.**
- Secondary focus – breadth of knowledge on GRX Operators
- Operations Manager assigned, team assembles

bics
a belgacom company
NAC



TOP SECRET STRAP 2
MyNOC Focus

- Expand **collection and capability** to enable better exploitation of Belgacom.
- Identify **key staff at BICS**, and selectors used by these individuals for QI.
- **Map the network** to better understand the Belgacom Infrastructure.
- Investigate **VPN links** from BICS to other telecoms providers.
- Investigate the vulnerability of the **MyBICS** Reporting Tool.



TOP SECRET STRAP 2
OP SOCIALIST Outcome

- In MyNOC:
  - CNE Access to BELGACOM – MERION ZETA – 6 endpoints into Engineer/ support staff IP range
  - 2 endpoints into BELGACOM DMZ (from prep VA work)
  - Optimal Bearers identified providing good access to BELGACOM proxy
- Post MyNOC:
  - Optimal Bearers continue to allow QI against BELGACOM engineers/proxy
  - Internal CNE access continues to expand – getting close to access core GRX Routers – currently on hosts with access
  - NAC continue to support with Network Analysis of internal networks, network understanding research on credentials and identification of engineers/system administrators and their specific roles.

UPDATE 2013-09-27: *The Belgacom compromise reinforces the correctness of the “Two Axioms for the Information Age” (I don’t know who first coined these): 1) Any device with software-defined behaviour can be tricked into doing things its creators did not intend; 2) Any device connected to a network of any sort, in any way, can be compromised by an external party.*

Here is a careful English translation of this original article by Peter De Lobel and Nikolas Vanhecke in Belgian news paper De Standaard. Hyperlinks and parts in [] are mine.

> ### *On the brink of catastrophe (2013-09-21)*
>
> *Ping. It’s Friday the 13th. Around 11 o’clock in the morning, the IT consultants that Belgacom employs at its largest customers in the private and public sector receive a message. The message doesn’t say much, except for an urgent request to cancel all appointments of that forenoon. An “emergency conference call” will take place instead.*
>
> *The news that is brought in that call makes the IT consultants gasp for breath. A piece of malicious software has been found on the network of BICS, a daughter*

Social Engineering
Sources And Methods
The Potomac Institute Cyber Center
Transparency International Defence
Video lectures of mathematics
contagio malware dump

Recent Posts

Dutch General Intelligence & Security Service (AIVD) disrupts activities of Russian intelligence officer targeting the International Criminal Court
EU Member States expel >120 Russian diplomats in an apparent coordinated effort to reduce Russian intelligence presence in the EU
Russian and Chinese services use LinkedIn to target & recruit persons to spy on Dutch companies, says General Intelligence & Security Service (AIVD)
Dutch govt expels two Russians using diplomatic cover to commit espionage on behalf of Russia's civil foreign intelligence agency SVR; pursued information on AI, semiconductors & nano tech
Submarine communication cables and the Netherlands: translation of a letter from the Dutch state secretary of Economic Affairs and Climate Policy

Recent Comments

Germany's data retention bill requires metadata to be kept in the country – TechGoor on Dutch telecom data retention law ruled invalid by court in The Hague
The foreign intel angle on Spygate: What probably didn't happen, and what probably did – The Optimistic Conservative on June 15th 2014: Dutch Joint Sigint Cyber Unit (JSCU) officially started

company of Belgacom. It is hard to grasp even for well-informed insiders. The BICS network is so wide and deep that it is promptly clear to everybody that this is not just a Belgian problem. This problem is at least of European proportions. Because whoever controls BICS, controls the communication of a large part of the world. “This could have been larger than 9/11”, says one source who closely followed the case. Without a grain of irony.

The pressure on the teams of the Dutch digital defender Fox-IT, that started cleaning up together with an army of Belgacom employees last weekend, was enormous.

It was their second attempt, various sources confirm. A first attempt to remove the villainous software from the infected computers at Belgacom in the last weekend of August was cancelled. “At the time, not all conditions were met required to remove everything at once”, it was said. Some computers turned out to run the alternative operating system Linux, known of the penguin logo, not Windows. “The risk was too big that we could not remove everything at once. In that case you should not touch it. Or the adversary will know that the virus has been found”, states someone politically involved.

Strict conditions

The investigation of the hacking started on July 19th, when Belgacom went to court. During their work, investigators at the intelligence services, police and justice were very wary of a leak about the entire operation. In early September they informed the Belgian cabinet on strict conditions: the list of attendees of that meeting was kept closely. If a politician would have wanted to reveal the news before the malware was dealt with, the investigators would press charges for breach of confidentiality of the investigation. “We could not risk everything going wrong due to someone talking”, it is said.

Belgacom was not infected with some common viruses, but with very professional malware that costed lots of money to develop. “We had to re-invent ourselves to do this”, an investigator said. “In other investigations there is a fixed idea of where you're going, but in in this case it was continuously starting over because it was so difficult to get a grasp of the malware”.

Gradually it became clear that the hackers are not only interested in the communications in the Middle-East, where BICS holds a solid position via South-African minority shareholder MTN. “They have been looking around and took what they could”, state sources involved in the investigation. They are clear about one thing: the attack originated from the United States. “We determine that by the signature of the malware, but especially by where the trails lead. They partially run through the UK. We think the US is the main destination. And the past weeks at the US Embassy, you notice some embarrassment when you request exchange of information.” Yesterday, the German weekly magazine Der Spiegel reported that the UK intelligence service GCHQ (Government Communications Headquartes) are responsible for the attacks. It based that claim on slides disclosed by whistleblower Edward Snowden. The news that GCHQ is behind the Belgacom attack is a surprise to at least the services working on the affair.

The malware could do anything

Cryptome – My Blog on Dutch govt expels two Russians using diplomatic cover to commit espionage on behalf of Russia’s civil foreign intelligence agency SVR; pursued information on AI, semiconductors & nano tech

Resetting the privacy discussion - Kris Joseph on The many interpretations and perspectives of privacy

Por qué el proyecto de ley de propiedad intelectual amenaza a la industria tecnológica del Reino Unido on Full translation of the Dutch government’s statement on encryption

Archives

June 2022
April 2022
February 2022
December 2020
October 2020
June 2020
May 2020
April 2020
December 2019
September 2019
July 2019
June 2019
May 2019
April 2019
November 2018
October 2018
September 2018
June 2018
October 2017
September 2017
June 2017
May 2017
April 2017
August 2016
May 2016
April 2016
March 2016
February 2016
January 2016
December 2015
November 2015
October 2015
September 2015
August 2015

The malware at Belgacom actually consists of a complex system of complementary viruses. They are all connected. If a problem is imminent or if they are detected, they can signal each other. “It is somewhat like a human virus, which also mutates continuously”, states someone involved who monitors the situation for his service. “For example, one part is responsible for searching and storing information, while another part is continuously looks for pathways to the internet to transfer information. Other pieces of code are responsible for circumventing firewalls, or carry out surveillance. If someone detects the hacking or attempts to remove a part of it, the virus that is acting as a guard promptly signals the other parts. Because you don’t know what the malware is capable of, everything can go horribly wrong at the last step.”

The cost of the entire detection and cleaning operation is correspondingly high. Fox-IT, the Dutch cyber security/defence company that is commissioned by Belgacom to first make inventory of the problems and then solve them, is a familiar name. “For the first two weeks they estimated the costs to be one million euro”, states a well-placed source. And then adds that the entire operation lasted ten weeks. Moreover, Fox-IT did not expect that, at a certain point, it had to allocate all of its employees to this case. A price tag of over five million euro, then? “It won’t be far off.”

But what was so terrifying about this cyber attack? And why the panic that something would go wrong? Telephone data about conversations with countries such as Afghanistan, Yemen and Syria that disappear, how could that have such an impact? They are ‘just’ stolen phone data, right? The involved expert sitting opposite us, looks dead serious. There is drama in his voice, but considering the contents of what he says, that is not unjustified. “This was highly performing malware and it was present in the nerve centre of communications. Anything that a highly privileged network operator of Belgacom could do, this system could do as well. I don’t have to make a drawing of it? It had all the keys, all the passwords and full control. We must dare to classify this as a big crisis. This could have been a catastrophe. And people don’t seem to realize.”

Sensitive customers

Perhaps it wouldn’t hurt to make that drawing. BICS calls itself a “wholesale carrier”. Two words, four syllables, but behind it is a network that spans the entire globe and the beating heart of which is located in our capital, Brussels. BICS provides the hardware infrastructure that carries internet traffic, phone conversations, text messages and mobile data of telecom companies and government institutions. And the more sensitive the customer, the more likely he is the end up at BICS. The daughter company of Belgacom markets itself with the argument that they never ever look at what travels over its cables. “We provide the cables for you, and you just send whatever you want over them”, is what it basically boils down to.

A glance at the list of BICS’ customers makes one dizzy. The financial transport center Swift, Electrabel, bpost, Belgocontrol, they are all connected to BICS. The NATO in Evere, the European Commission and Parliament, SHAPE, the Supreme Headquerters Allied Powers Europe, in Bergen; BICS, BICS, BICS. Even the headquarters of the NATO Allied Air Command, in Ramstein, Germany, from where the 2011 air attacks on Libya where coordinated, depends on BICS. Among the military, it is pointed out that military communications has an extra layer of security; but that pointing-out happens with a degree of humility that is very

July 2015
June 2015
May 2015
April 2015
March 2015
February 2015
January 2015
December 2014
November 2014
October 2014
September 2014
August 2014
July 2014
June 2014
May 2014
March 2014
February 2014
January 2014
December 2013
November 2013
October 2013
September 2013
August 2013
July 2013
June 2013
April 2013
March 2013
January 2013
December 2012
October 2012
September 2012
August 2012
July 2012
June 2012
May 2012
April 2012
February 2012
January 2012
December 2011
November 2011
September 2011
August 2011
July 2011
June 2011
May 2011
April 2011
March 2011
February 2011

unusual to the military. “Every organisation, not just the government, must now begin to wonder whether it is dependent of one single provider, of one single network. And specially how well it is secured itself”, states someone who was at the front row of the affair. “Belgacom, that is critical infrastructure. How can Belgium keep running without it? Those are the questions that we must ask now. Because the organisation responsible for the attack has in fact the capability to completely disrupt Belgacom and BICS.” A different source confirms, reluctantly, the doom scenarios: “You can’t think of it. It would be larger than 9/11. The planes would pretty much fall out of the sky.” As a figure of speech? “Hm, yeah.”

Lifeline

A governmental source points out the consequences of even a limited disruption of phone communications and internet. “If a crisis occurs, what is the first thing a human does? Grasp their phone. Imagine that that lifeline is lost. Not just for you, but also for the emergency services, hospital, the fire department…? And for the police? At first glance it isn’t, because they use the ~~Astrid network~~ [a Belgian national radio communications network intended for emergency services]. But that network only works apart from BICS for local communications. For interregional communications it is just as dependent on BICS as the rest. Hence, it is no coincidence that police chief Catherine De Bolle started looking for a backup for the communications system of the federal police on that Friday the 13th, just before the big cleaning operation would have started.

How long would it take before Belgacom was up and running again after a destructive cyber attack, is unclear. “But it is clear that we are not prepared to counter this type of attacks right now”, states a high-ranking source. “That awareness must finally start to grow. I am very apprehensive for the feeling of relief that I already observe in some people. ‘Ah well, that has been nicely dealt with. It’s over.’ It’s not, mind you. Whoever doesn’t realise, this week, that it is urgent, will never get it. Playing things down now is dangerous.”

After De Standaard brought the news of large-scale hacking at Belgacom, it turned out that the Ministry of Foreign Affairs and the cabinet of the prime minister had been hacked. “And this is merely the top of the iceberg”, states a source who was involved in the problems at Belgacom. Because telecom is one thing, but there are many other critical sectors that are the fundament of a country. Transportation, for example. Trains, trams, busses, highways, airplanes, everything involves computer networks and everywhere one should be cautious for cyber attacks. The energy supply is another critical fundament. And last but not least: the banking sector of a country. Luxembourg has already contacted the Belgian cyberservices [?] to obtain more information about the malware that hit Belgacom.

Awareness

Besides budgets and well-paid IT personnel, the remedy against the growing cyberthreat will be found in improved awareness. “Belgium wants to invest in knowledge and innovation, but if one sector is vulnerable to espionage, it is that one. Just as many computers of the global diplomatic network of Foreign Affairs have post-its one them with the passwords, many small companies are slacking in their security”, a cyber specialist states. “And if you dare ask whether their Chinese interns are thoroughly screened, they look at you as if you’re from another planet.” Whether the gravity of the situation is apparent to everyone, is *doubtful. In official communications, Belgacom states that it currently has no evidence of impact on its customers or their data. Understandly, the company does not want to trigger hysteria, but it sounds like down-playing nonetheless. "What should we write then?", states spokesman Jan Margot in his response. "The infection was at dozens of computers in our own system. They have been cleaned together with the entire network."*

BICS too doesn't say much about it. "There are no indications of an impact on the telecomnetwork of BICS", it ~~states~~ in a press release. "A number of our IT systems are integrated in the infrastructure of Belgacom and are affected in that way, but that remained outside the network that carries customer traffic."

"That's all put rather euphemistically", according to the investigators involved. "But you cannot accuse them of lying. A lot of thought went into every comma of the communication."

Joke

Did Belgium become the joke of de European mainland as a result of the compromise of Belgacom? Intelligence services are continuously in contact with each other and exchange information. For the image of our country, the past week has been anything but stellar, but it is emphasised nonetheless that in such contacts it is often also about personal relations between people. "Moreover, all countries have problems and everyone tries to rise above them."

What about ethics? Isn't it schizophrenic that our country, Belgium, receives information about threats that the US or others have stolen from us? "That is the eternal paradox", a recipient of such information states. Diplomatically it is the hardest. But if you receive information about a serious threat such as terrorism, you cannot ignore it. Then you have different things on your mind.

EOF

Uncategorized

← Ben Nagy's thoughts on "Cryptopocalypse"

Project Symbolon completed: the Dutch Joint SIGINT Cyber Unit (JSCU) is born →

3 thoughts on "Belgacom — "On the brink of catastrophe" (translation)"

Victor Escudero Rubio says:
2013-09-29 at 14:59

I have elaborated a nice presentation about this telecom carrier being hacked by the British spy agency. http://www.vescudero.net/2013/09/international-wholesale-carrier-hacked.html

Reply

mrkoot says:
2013-11-10 at 14:00

Excellent! Thanks for adding that.

Reply

Vytautas says:
2015-01-28 at 06:47

Thanks for trying to keep your important article up to date by adding other links. Interesting story that has not gotten the attention it deserves since Belgacom is located in the same country as HQ of NATO and EU. Also important for it shows that state made APT’s do not allways come from the “list of usual suspects” (RF, CN, NK,IR). All cyber powers are engaging in this kind of dangerous activity.

Reply

Leave a Reply

Your email address will not be published. Required fields are marked *

Comment

Name *

Email *

Website

□

Save my name, email, and website in this browser for the next time I comment.

Post Comment

Powered by GovPress.