OPERATION SOCIALIST

THE INSIDE STORY OF HOW BRITISH SPIES HACKED BELGIUM'S LARGEST TELCO

BY RYAN GALLAGHER *@rj_gallagher*

12/13/2014

When the incoming emails stopped arriving, it seemed innocuous at first. But it would eventually become clear that this was no routine technical problem. Inside a row of gray office buildings in Brussels, a major hacking attack was in progress. And the perpetrators were British government spies.

It was in the summer of 2012 that the anomalies were initially detected by employees at Belgium's largest telecommunications provider, Belgacom. But it wasn't until a year later, in June 2013, that the company's security experts were able to figure out what was going on. The computer systems of Belgacom had been infected with a highly sophisticated malware, and it was disguising itself as legitimate Microsoft software while quietly stealing data.

Last year, documents from National Security Agency whistleblower Edward Snowden confirmed that British surveillance agency Government Communications Headquarters was behind the attack, codenamed Operation Socialist. And in November, *The Intercept* revealed that the malware found on Belgacom's systems was one of the most advanced spy tools ever identified by security researchers, who named it "Regin."

The full story about GCHQ's infiltration of Belgacom, however, has never been told. Key details about the attack have remained shrouded in mystery—and the scope of the attack unclear.

Now, in partnership with Dutch and Belgian newspapers *NRC Handelsblad* and *De Standaard*, *The Intercept* has pieced together the first full reconstruction of events that took place before, during, and after the secret GCHQ hacking operation.

Based on new documents from the Snowden archive and interviews with sources familiar with the malware investigation at Belgacom, *The Intercept* and its partners have established that the attack on Belgacom was more aggressive and far-reaching than previously thought. It occurred in stages between 2010 and 2011, each time penetrating deeper into Belgacom's systems, eventually compromising the very core of the company's networks.

> ***"A BREATHTAKING EXAMPLE OF THE STATE-SPONSORED HACKING PROBLEM."***

Snowden told *The Intercept* that the latest revelations amounted to unprecedented "smoking-gun attribution for a governmental cyber attack against critical infrastructure."

The Belgacom hack, he said, is the "first documented example to show one EU member state mounting a cyber attack on another…a breathtaking example of the scale of the state-sponsored hacking problem."

Publicly, Belgacom has played down the extent of the compromise, insisting that only its internal systems were breached and that customers' data was never found to have been at risk. But secret GCHQ documents show the agency gained access far beyond Belgacom's internal employee computers and was able to grab encrypted and unencrypted streams of private communications handled by the company.

Belgacom invested several million dollars in its efforts to clean-up its systems and beef-up its security after the attack. However, *The Intercept* has learned that sources familiar with the malware investigation at the company are uncomfortable with how the clean-up operation was handled—and they believe parts of the GCHQ malware were never fully removed.

The revelations about the scope of the hacking operation will likely alarm Belgacom's customers across the world. The company operates a large number of data links internationally (see interactive map below), and it serves millions of people across Europe as well as officials from top institutions including the European Commission, the European Parliament, and the European Council. The new details will also be closely scrutinized by a federal prosecutor in Belgium, who is currently carrying out a criminal investigation into the attack on the company.

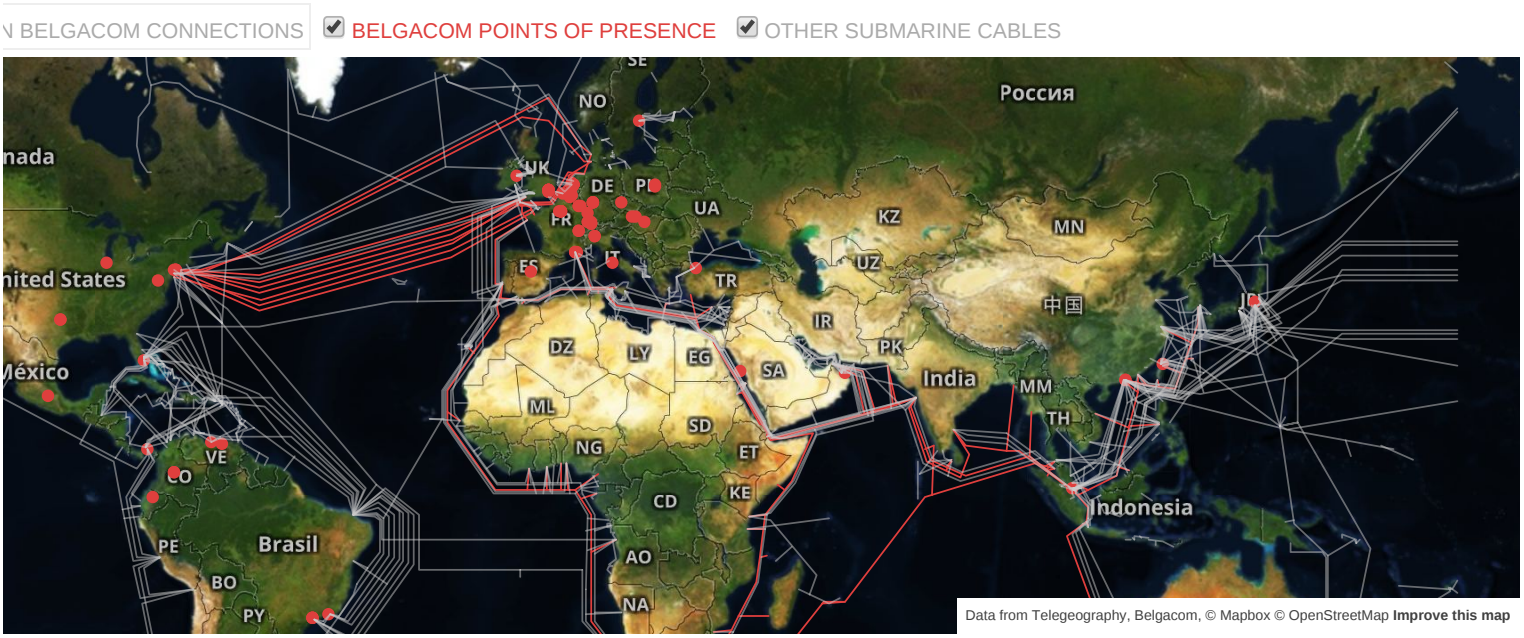
Sophia in 't Veld, a Dutch politician who chaired the European Parliament's recent inquiry into mass surveillance exposed by Snowden, told *The Intercept* that she believes the British government should face sanctions if the latest disclosures are proven.

"Compensating Belgacom should be the very least it should do," in 't Veld said. "But I am more concerned about accountability for breaking the law, violating fundamental rights, and eroding our democratic systems."

Other similarly sophisticated state-sponsored malware attacks believed to have been perpetrated by Western countries have involved Stuxnet, a bug used to sabotage Iranian nuclear systems, and Flame, a spy malware that was found collecting data from systems predominantly in the Middle East.

What sets the secret British infiltration of Belgacom apart is that it was perpetrated against a close ally—and is backed up by a series of top-secret documents, which *The Intercept* is now publishing.

GCHQ declined to comment for this story, and insisted that its actions are "necessary legal, and proportionate."



The beginning

The origins of the attack on Belgacom can be traced back to 2009, when GCHQ began developing new techniques to hack into telecommunications networks. The methods were discussed and developed during a series of top-secret "signals development" conferences, held annually by countries in the so-called "Five Eyes" surveillance alliance: the United States, the United Kingdom, Australia, New Zealand, and Canada.

Between 2009 and 2011, GCHQ worked with its allies to develop sophisticated new tools and technologies it could use to scan global networks for weaknesses and then penetrate them. According to top-secret GCHQ documents, the agency wanted to adopt the aggressive new methods in part to counter the use of privacy-protecting encryption—what it described as the "encryption problem."

When communications are sent across networks in encrypted format, it makes it much harder for the spies to intercept and make sense of emails, phone calls, text messages, internet chats, and browsing sessions. For GCHQ, there was a simple solution. The agency decided that, where possible, it would find ways to hack into communication networks to grab traffic *before* it's encrypted.

The British spies identified Belgacom as a top target to be infiltrated. The company, along with its subsidiary Belgacom International Carrier Services, plays an important role in Europe, and has partnerships with hundreds of telecommunications companies across the world—in Africa, Asia, Europe, the Middle East, and the United States. The Belgacom subsidiary maintains one of the world's largest "roaming" hubs, which means that when foreign visitors traveling through Europe on vacation or a business trip use their cellphones, many of them connect to Belgacom's international carrier networks.

The Snowden documents show that GCHQ wanted to gain access to Belgacom so that it could spy on phones used by surveillance targets travelling in Europe. But the agency also had an ulterior motive. Once it had hacked into Belgacom's systems, GCHQ planned to break into data links connecting Belgacom and its international partners, monitoring communications transmitted between Europe and the rest of the world. A map in the GCHQ documents, named "Belgacom_connections," highlights the company's reach across Europe, the Middle East, and North Africa, illustrating why British spies deemed it of such high value.

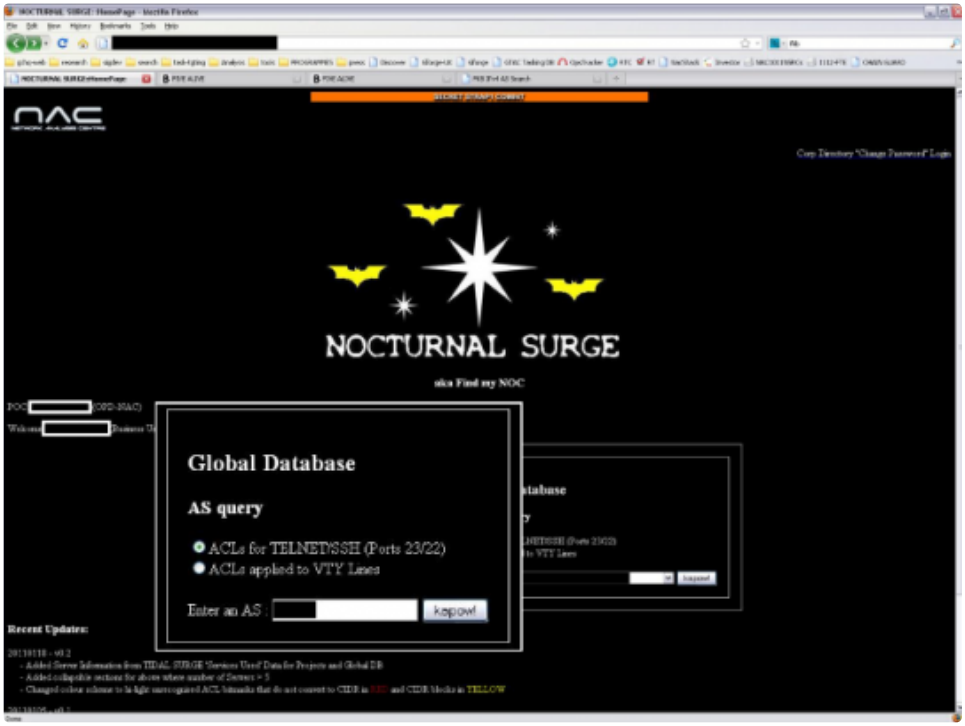
Attack planning

Before GCHQ launched its attack on Belgacom's systems, the spy agency conducted in-depth reconnaissance, using its powerful surveillance systems to covertly map out the company's network and identify key employees "in areas related to maintenance and security."

GCHQ documents show that it maintains special databases for this purpose, storing details about computers used by engineers and system administrators who work in the nerve center, or "network operations center," of computer networks worldwide. Engineers and system administrators are particularly interesting to the spies because they manage networks—and hold the keys that can be used to unlock large troves of private data.

GCHQ developed a system called NOCTURNAL SURGE to search for particular engineers and system administrators by finding their IP addresses, unique identifiers that are allocated to computers when they connect to the internet. In early 2011, the documents show, GCHQ refined the NOCTURNAL SURGE system with the help of its Canadian counterparts, who had developed a similar tool, named PENTAHO.

GCHQ narrowed down IP addresses it believed were linked to the Belgacom engineers by using data its surveillance systems had collected about internet activity, before moving into what would be the final stages prior to launching its attack. The documents show that the agency used a tool named HACIENDA to scan for vulnerable potential access points in the Belgacom's networks; it then went hunting for particular engineers or administrators that it could infect with malware.



The infection

The British spies, part of special unit named the Network Analysis Center, began trawling through their vast repositories of intercepted Internet data for more details about the individuals they had identified as suspected Belgacom engineers.

The spies used the IP addresses they had associated with the engineers as search terms to sift through their surveillance troves, and were quickly able to find what they needed to confirm the employees' identities and target them individually with malware.

The confirmation came in the form of Google, Yahoo, and LinkedIn "cookies," tiny unique files that are automatically placed on computers to identify and sometimes track people browsing the Internet, often for advertising purposes. GCHQ maintains a huge repository named MUTANT BROTH that stores billions of these intercepted cookies, which it

uses to correlate with IP addresses to determine the identity of a person. GCHQ refers to cookies internally as "target detection identifiers."

Top-secret GCHQ documents name three male Belgacom engineers who were identified as targets to attack. *The Intercept* has confirmed the identities of the men, and contacted each of them prior to the publication of this story; all three declined comment and requested that their identities not be disclosed.

GCHQ monitored the browsing habits of the engineers, and geared up to enter the most important and sensitive phase of the secret operation. The agency planned to perform a so-called "Quantum Insert" attack, which involves redirecting people targeted for surveillance to a malicious website that infects their computers with malware at a lightning pace. In this case, the documents indicate that GCHQ set up a malicious page that looked like LinkedIn to trick the Belgacom engineers. (The NSA also uses Quantum Inserts to target people, as *The Intercept* has previously reported.)

A GCHQ document reviewing operations conducted between January and March 2011 noted that the hack on Belgacom was successful, and stated that the agency had obtained access to the company's systems as planned. By installing the malware on the engineers' computers, the spies had gained control of their machines, and were able to exploit the broad access the engineers had into the networks for surveillance purposes.

The document stated that the hacking attack against Belgacom had penetrated "both deep into the network and at the edge of the network," adding that ongoing work would help "further this new access."

By December 2011, as part of a second "surge" against Belgacom, GCHQ identified other cellphone operators connecting to company's network as part of international roaming partnerships, and successfully hacked into data links carrying information over a protocol known as GPRS, which handles cellphone internet browsing sessions and multimedia messages.

The spy agency was able to obtain data that was being sent between Belgacom and other operators through encrypted tunnels known as "virtual private networks." GCHQ boasted that its work to conduct "exploitation" against these private networks had been highly productive, noting "the huge extent of opportunity that this work has identified." Another document, dated from late 2011, added: "Network Analysis on BELGACOM hugely successful enabling exploitation."

GCHQ had accomplished its objective. The agency had severely compromised Belgacom's systems and could intercept encrypted and unencrypted private data passing through its networks. The hack would remain undetected for two years, until the spring of 2013.

center in Brussels.

The discovery

In the summer 2012, system administrators detected errors within Belgacom's systems. At the company's offices on Lebeau Street in Brussels, a short walk from the European Parliament's Belgian offices, employees of Belgacom's BICS subsidiary complained about problems receiving emails. The email server had malfunctioned, but Belgacom's technical team couldn't work out why.

The glitch was left unresolved until June 2013, when there was a sudden flare-up. After a Windows software update was sent to Belgacom's email exchange server, the problems returned, worse than before. The administrators contacted Microsoft for help, questioning whether the new Windows update could be the reason for the fault. But Microsoft, too, struggled to identify exactly what was going wrong. There was still no solution to be found. (Microsoft declined to comment for this story.)

Belgacom's internal security team began to suspect that the systems had been infected with some sort of virus, and the company decided it was time to call in outside experts. It hired Dutch computer security firm Fox-IT to come and scan the systems for anything suspicious.

SOURCES FAMILIAR WITH THE INVESTIGATION DESCRIBED THE MALWARE AS THE MOST ADVANCED THEY HAD EVER SEEN.

Before long, Fox-IT discovered strange files on Belgacom's email server that appeared to be disguised as legitimate Microsoft software. The suspicious files had been enabling a highly sophisticated hacker to circumvent automatic Microsoft software updates of Belgacom's systems in

order to continue infiltrating the company's systems.

About a month after Belgacom had identified the malicious software, or malware, it informed Belgian police and the country's specialist federal computer crime unit, according to sources familiar with the incident. Belgian military intelligence was also called in to investigate the hack, together with Fox-IT.

The experts from Fox IT and military intelligence worked to dissect the malware on Belgacom's systems, and were shocked by what they found. In interviews with *The Intercept* and its reporting partners, sources familiar with the investigation described the malware as the most advanced they had ever seen, and said that if the email exchange server had not malfunctioned in the first place, the spy bug would likely have remained inside Belgacom for several more years.

A deep breach

While working to assess the extent of the infection at Belgacom, the team of investigators realized that the damage was far more extensive than they first thought. The malware had not only compromised Belgacom's email servers, it had infected more than 120 computer systems operated by the company, including up to 70 personal computers.

The most serious discovery was that the large routers that form the very core of Belgacom's international carrier networks, made by the American company Cisco, were also found to have been compromised and infected. The routers are one of the most closely guarded parts of the company's infrastructure, because they handle large flows of sensitive private communications transiting through its networks.

Earlier Snowden leaks have shown how the NSA can compromise routers, such as those operated by Cisco; the agency can remotely hack them, or physically intercept and bug them before they are installed at a company. In the Belgacom case, it is not clear exactly which method was used by GCHQ—or whether there was any direct NSA assistance. (The NSA declined to comment for this story.)

Either way, the malware investigators at Belgacom never got a chance to study the routers. After the infection of the Cisco routers was found, the company issued an order that no one could tamper with them. Belgacom bosses insisted that only employees from Cisco could handle the routers, which caused unease among some of the investigators.

"You could ask many security companies to investigate those routers," one of the investigators told *The Intercept*. By bringing in Cisco employees to do the investigation, "you can't perform an independent inspection," said the source, who spoke on condition of anonymity because he was not authorized to speak to the media

A spokesman for Cisco declined to comment on the Belgacom investigation, citing company policy. "Cisco does not comment publicly on customer relationships or specific customer incidents," the spokesman said.

Shortly after the malware was found on the routers, Fox-IT was told by Belgacom to stop its investigation. Researchers from the Dutch security company were asked to write-up a report about their findings as soon as possible. Under the conditions of a non-disclosure agreement, they could not speak about what they had found, nor could they publicly warn against the malware. Moreover, they were not allowed to remove the malware.

Between late August and mid-Sept. 2013, there was an intense period of activity surrounding Belgacom.

On August 30, some parts of the malware were remotely deleted from the company's infected systems—apparently after the British spies realized that it had been detected. But the malware was not completely removed, according to sources familiar with the investigation.

Two weeks later, on Sept. 14, employees from Belgacom, investigators, police and military intelligence services began an intensive attempt to completely purge the spy bug from the systems.

During this operation, journalists were tipped off for the first time about the malware investigation. *The Intercept*'s Dutch and Belgian partners *NRC Handelsblad* and *De Standaard* reported the news, disclosing that sources familiar with the investigation suspected NSA or GCHQ may have been responsible for the attack.

The same day the story broke, on Sept. 16, Belgacom issued a press release. "At this stage there is no indication of any impact on the customers or their data," it said. "At no point in time has the delivery of our telecommunication services been compromised. "

Then, on Sept. 20, German news magazine *Der Spiegel* published documents from Snowden revealing that British spies were behind the hack, providing the first confirmation of the attacker's identity.

Significant resources

In the aftermath of the revelations, Belgacom refused to comment on GCHQ's role as the architect of the intrusion. Top officials from the company were called to appear before a European Parliamentary committee investigating the extent of mass surveillance revealed by Snowden.

The Belgacom bosses told the committee that there were no problems with Belgacom's systems after a "meticulous" clean-up operation, and again claimed that private communications were not compromised. They dismissed media reports about the attack, and declined to discuss anything about the perpetrator, saying only that "the hackers [responsible] have considerable resources behind them."

People with knowledge of the malware investigation watched Belgacom's public statements with interest. And some of them have questioned the company's version of events.

"There was only a partial clean-up," said one source familiar with the malware investigation. "I believe it is still there. It is very hard to remove and, from what I've seen, Belgacom never did a serious attempt to remove it."

Belgacom declined to comment for this story, citing the ongoing criminal investigation in Belgium.

Last month, *The Intercept* confirmed Regin as the malware found on Belgacom's systems during the clean-up operation.

The spy bug was described by security researchers as one of the most sophisticated pieces of malware ever discovered, and was found to have been targeting a host of telecommunications networks, governments, and research organizations, in countries such as Germany, Iran, Brazil, Russia, and Syria, as well as Belgium.

GCHQ has refused to comment on Regin, as has the NSA, and Belgacom. But Snowden documents contain strong evidence, which has not been reported before, that directly links British spies to the malware.

Aside from showing extensive details about how the British spies infiltrated the company and planted malware to successfully steal data, GCHQ documents in the Snowden archive contain codenames that also appear in samples of the Regin malware found on Belgacom's systems, such as "Legspin" and "Hopscotch."

One GCHQ document about the use of hacking methods references the use of "Legspin" to exploit computers. Another document describes "Hopscotch" as part of a system GCHQ uses to analyze data collected through surveillance.

Ronald Prins, director of the computer security company Fox-IT, has studied the malware, and played a key role in the analysis of Belgacom's infected networks.

"Documents from Snowden and what I've seen from the malware can only lead to one conclusion," Prins told *The Intercept*. "This was used by GCHQ."

———

Documents published with this article:

- Automated NOC detection
- Mobile Networks in My NOC World
- Making network sense of the encryption problem
- Stargate CNE requirements
- NAC review – October to December 2011
- GCHQ NAC review – January to March 2011
- GCHQ NAC review – April to June 2011
- GCHQ NAC review – July to September 2011
- GCHQ NAC review – January to March 2012
- GCHQ Hopscotch
- Belgacom connections

———

Photo: Belgacom headquarters: Paul O'Driscoll/Getty; Map: Ingrid Burrington and Josh Begley; Belgacom operations center, Paul O'Driscoll/Bloomberg via Getty.

✉ Email the author: ryan.gallagher@theintercept.com

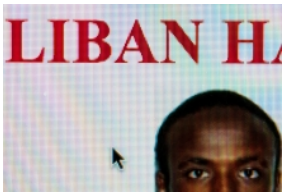
SHOW COMMENTS

Comments closed.

RECOMMENDED

House of Cards: Tom Ridge's Code Rich

How Guantánamo Diary Escaped the Black Hole and Got Past the Censors (Mostly)



Under Suspicious Circumstances, FBI Places Brother of No-Fly Litigant on Most Wanted Terrorist List

Spanish Peacekeeper Is the Latest Example of Israel Killing United Nations Personnel

How Washington Mourned Tommy Boggs, Friend to the Worst People in the World

House of Cards: A DC Real Estate Column

Canada Casts Global Surveillance Dragnet Over File Downloads

How to Leak to The Intercept