GLOBAL INFORMATION SOCIETY WATCH 2014

Communications surveillance in the digital age

This report was originally published as part of a larger compilation, which can be downloaded from GISWatch.org

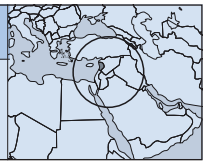
Association for Progressive Communications (APC)
and Humanist Institute for Cooperation with Developing Countries (Hivos)

ISBN: 978-92-95102-16-3

APC-201408-CIPP-R-EN-DIGITAL-207

LEBANON

Surveilling the banking sector in Lebanon



Mireille Raad

Introduction

Many argue that online privacy is a human right, while others insist that it is a negotiated contract between the state and its citizens – a contract in which citizens exchange some of their data in return for national security. So in theory – and in an "ideal state" – citizens could rely on the protection of their home governments to ensure their physical safety while also preserving their online privacy of communications, transactions, identities and speech. But to what extent can states really uphold this contract?

In Lebanon, there is an odd "ideal law" on banking secrecy dating back to 1956. This law did not create secrecy as a privilege to be enjoyed by banks, but as a duty that banks operating in the country must observe. Violation of banking secrecy is a criminal offence. However, in June 2012, Kaspersky Lab announced the discovery of "Gauss", a complex state-sponsored cyber-espionage toolkit targeting major banks in Lebanon and parts of the Middle East. Gauss is designed to steal sensitive data, with a specific focus on browser passwords and online banking account credentials.

This cyber violation violates the Lebanese banking secrecy law and is a direct attack on a nation's sensitive financial transactions and a critical economic organ: the banking sector is one of the few stable sectors in Lebanon and, as many argue, one of the sectors stabilising the economy. If the banking sector collapsed, the country might fall into chaos, experts say.[1]

Due to the complexity and similarities between Gauss and malware like Stuxnet, Flame, Duqu and others, fingers pointed at the United States (US) and Israel, accusing them of being behind Gauss.

Background

> *Lebanon is a very small country. [...] Not much you can do. It is up to major international bodies, like the UN [United Nations], Human Rights Commission or the EU [European Union] or the American people themselves to ask for a change in this behavior.*[2] –Lebanese Telecom Minister Nicolas Sehnaoui commenting on the Edward Snowden/National Security Agency (NSA) leaks in June 2013.

This blunt quote illustrates the simple reality that many developing countries face in a digital age when large-scale mass surveillance and spying on detailed data and sensitive transactions become an act of daily nation bullying. This problem is only accentuated by a digital divide, where most services and servers reside in developed countries; not to mention that only rich countries can actually "afford" to own and operate systems that allow them to perform such acts of mass privacy violation from the comfort of their "homeland".

Sehnaoui's quote comes as no surprise since Lebanon, like much of the Middle East, has a difficult recent history – it is a small diverse country amid big regional powers. Frequent invasions of this country date back to the Assyrians, Persians, Greeks, Romans, Arabs, Fatimids, Crusaders, Ottoman Turks and most recently the French and Israelis.

Recently, Lebanon has also been a focal point of larger geopolitical rivalries in the region between Iran, Saudi Arabia, Syria, Palestine, the Gulf States and of course Israel and the US. So it stands to reason that there is a long history of struggling against external spying on telecommunications and internet servers, with more than a hundred people arrested for collaborating with and spying for foreign states since April 2009.[3]

Tracking the malware

In June 2012, Kaspersky Lab[4] announced the discovery of a malware toolkit spreading in Lebanon and

1 Dockery, S. (2012, August 11). Virus plunges Lebanon into cyber war. *The Daily Star*. www.dailystar.com.lb/News/Local-News/2012/Aug-11/184234-virus-plunges-lebanon-into-cyber-war.ashx#ixzz33c7Yh200

2 Al Saadi, Y. (2013, June 13). The NSA Global Surveillance and Lebanon: 'Not Much We Can Do'. *Al-Akhbar*. english.al-akhbar.com/node/16107

3 Ibid.

4 Kaspersky Lab is a Russian multinational computer security company and the world's largest privately held vendor of software security products. https://en.wikipedia.org/wiki/Kaspersky_Lab

parts of the Middle East. This discovery was made possible only after knowledge gained by in-depth analysis and research conducted on the Flame[5] malware.

The toolkit had different modules named after famous mathematicians and philosophers like Godel, Lagrange and Gauss. The module named "Gauss" implements the data-stealing capabilities. The Kaspersky investigation estimated that Gauss began operations in mid-2011. Its infiltration into systems is conducted in a controlled and targeted fashion, ensuring stealth and secrecy.

The main functionality of the malware includes:

- Intercepting browser history, cookies and passwords.
- Harvesting and sending detailed system configurations of infected machines, including specifics of network interfaces, computer drives and BIOS.[6]
- Infecting USB sticks (flashdrives) with a data-stealing module using the same LNK vulnerability that was previously used in Stuxnet and Flame, but in a more "intelligent" way that under certain circumstances is capable of "disinfecting" the drive.
- Listing the content of the system drives and folders.
- Stealing credentials for various banking systems in the Middle East (Bank of Beirut, EBLF, BLOM Bank, Byblos Bank, Fransabank and Credit Libanais). It also targets users of Citibank and PayPal. The online banking Trojan functionality found in Gauss is a unique characteristic that was not found in any previously known cyber weapons.
- Hijacking account information for social networks, email and instant messaging accounts.
- Installing a font called "Palida" with an unknown objective, but speculations suggest it is used to remotely detect infected machines.
- Using advanced techniques for handling high traffic load balancing, load distribution and fault tolerance known as Round-robin DNS[7] – which suggests that the makers of the malware were expecting high traffic volumes.
- An encrypted code with an unknown objective.
- Communication with command and control servers.

The above technical specifications clearly connect Gauss to Flame – Flame is connected to Stuxnet – which prompted Kaspersky Lab to call it a "nation-state sponsored cyber-espionage toolkit"[8] rather than a tool for criminal theft – something that gives Gauss a geopolitical dimension.

Once the news of the malware broke, the Lebanese Central Bank[9] issued a note to all commercial banks to take the necessary measures to protect computer systems. Some bankers confidently said that they are not concerned about any virus, insisting that they had nothing to hide. "Let them [the Americans] browse our accounts. They won't find anything suspicious because all our clients are well-known," one banker told *The Daily Star*,[10] while another denied the existence of the virus altogether.

The head of the IT department in the Central Bank of Lebanon said that the Lebanese banks had upgraded their software security systems to block *any* virus designed to spy on transactions and operations: "The anti-virus program blocks all known viruses and this has been going on for a long time. But the Gauss virus did not have time to inflict harm on the systems," he said.[11]

However, a group of independent security professionals who claim having first-hand experience dealing with the Gauss malware in Lebanese banks issued a statement[12] that was published on several Lebanese blogs. It stated that banks are still vulnerable, and raised the concern that by conveying simplistic views about Gauss, the banking sector is not truly willing to fight back.

Conclusion

Technology trumps all. In a borderless interconnected cyberspace, states – even the most tech-savvy ones – are seldom able to uphold contracts they make with their citizens on digital rights, even if they want to. This claim is backed by stories from across the globe,

5 Flame is arguably the most complex malware ever found, and is used for targeted cyber espionage in Middle Eastern countries. https://en.wikipedia.org/wiki/Flame_(malware)

6 The fundamental purposes of the BIOS are to initialise and test the system hardware components and to load the operating system. https://en.wikipedia.org/wiki/BIOS

7 https://en.wikipedia.org/wiki/Round-robin_DNS

8 Kaspersky Lab. (2012, August 9). Kaspersky Lab discovers 'Gauss' – a new complex cyber threat designed to monitor online banking accounts. *Kaspersky Lab*. www.kaspersky.com/about/news/virus/2012/Kaspersky_Lab_and_ITU_Discover_Gauss_A_New_Complex_Cyber_Threat_Designed_to_Monitor_Online_Banking_Accounts

9 https://en.wikipedia.org/wiki/Banque_du_Liban

10 Habib, O. (2012, September 14). Lebanese banks develop anti-virus system. *The Daily Star*. www.dailystar.com.lb/Business/Lebanon/2012/Sep-14/187818-lebanese-banks-develop-anti-virus-system.ashx#axzz3AFd4RS4h

11 Ibid.

12 www.plus961.com/2012/10/no-our-banks-are-still-vulnerable-to-cyber-attacks

```
<body onload='javascript:var detective = new Detector();
if(detective.detect("Palida
Narrow")||detective.detect("Palida"))
{window.location="PortalSecurityAlert.aspx"}'>
```

Screenshot from BLOM Bank current online banking portal (https://eblom.blombank.com)

stories that are similar to the Lebanese one. Many of these we have learned from the Snowden revelations.

Those revelations changed the conversation on privacy and surveillance from a government-citizen debate into an international debate between states. "Spying", which traditionally was a "targeted" operation on specific political actors in foreign states, turned into mass surveillance and catch-all, detailed monitoring and wiretapping of terabytes of data per second.

This mass surveillance is enabled by technology and can exist only because of it. Huge amounts of data on our social interactions and economic transactions simply exist "online". Technology, with its algorithms, cheap storage and processing cycles is able to store and "make sense" of data that is almost humanly "un-crunchable". This data needs to be captured only once – it can be copied and can never really be "returned".

However, technology comes with costs, ranging from research and development to the day-to-day operating costs of large systems. This only adds insult to injury by increasing the digital divide between poor and rich and enabling rich countries to have the "advantage" of big data over many other nations.

Privacy protection measures also come at a high cost for governments and the private sector. They also come with a hit on user-friendly interfaces and interactions. Security and usability have always been at odds.

The digital divide is already raising concerns and plays a major role in surveillance, since most of the services and infrastructure like internet exchange data centres are hosted in "rich" countries or owned by companies who follow the legal jurisdictions of those countries. This gives those countries easier access to large amounts of data being routed through their territories or legal reason to demand disclosure of data from companies who have to comply with their laws, not the laws its clients are subject to.

The best option that countries have to uphold their contract with their citizens and protect privacy is to try to keep as much of the data as possible within their own territories – for example, Germany and France are leading efforts to secure EU traffic by keeping it within borders. German Chancellor Angela Merkel has called for creating a "European communications network" – something that poses a new risk of "fragmenting" the internet. In response to that call, US President Barack Obama announced the extension of US citizen privacy protections to EU citizens.[13]

This announcement shows how much power dynamics and politics are at play in international surveillance and how different people using the "open internet" – our biggest common shared resource – are not treated equally, while equality is paraded as an international human right that everyone must uphold.

Action steps

There is no direct action point with immediate outcome that can be taken to tackle extraterritorial surveillance. But here are some of the ideas that can be helpful:

- The internet is a global, open and shared resource that everyone helped build and everybody uses. The benefits of accessing the internet have been demonstrated in many studies. Data is what we share on the internet – without data and metadata, the internet is an expensive set of cables. We should lobby to include privacy of data on the internet as a global human right, and offer easy and solid safeguards for all countries to abide by, with clear punishments for those who refuse to.
- Inform local policy makers of different research being done, especially of the International Principles on the Application of Human Rights to Communications Surveillance.[14]
- Localise and strengthen the ability of activists to debate these issues in each country.
- Have media discussions with the general public, especially inside the US or countries more likely to conduct surveillance.
- Increase awareness and the technical abilities to counter surveillance.

13 MacAskill, E. (2014, June 25). US to extend privacy protection rights to EU citizens. *The Guardian*. www.theguardian.com/world/2014/jun/25/us-privacy-protection-rights-europe

14 https://en.necessaryandproportionate.org/text