Regin APT Attacks Among the Most Sophisticated Ever Analyzed

By Brian Donohue

Published: 2014-11-25 · Archived: 2026-04-05 16:05:09 UTC

Nearly every organization involved in the business of tracking advanced persistent threat campaigns is talking about a new highly sophisticated attack platform called “Regin” (pronounced: reɪ*gən – like the former U.S. president). The general consensus is that Regin is the work of a well-funded nation-state, though it’s impossible to point a finger at any particular country and blame them with certainty.

It would appear as though a number of individuals and organizations had been keeping dossiers on Regin, because as soon as Symantec issued their first version of the report over the weekend, other reports began streaming out, adding to the initial findings. More than one company and more than one researcher – including Kaspersky Lab’s Global Research and Analysis Team – have called this the most sophisticated attack campaign ever analyzed.

According to Kaspersky Lab’s findings, the Regin APT campaign targets telecom operators, government institutions, multi-national political bodies, financial and research institutions and individuals involved in advanced mathematics and cryptography. The attackers seem to be primarily interested in gathering intelligence and facilitating other types of attacks. While much of the intelligence gathered includes spying on emails and documents, the attack group also relentlessly targets telecommunication companies, which is normal, and at least one GSM provider, which is not so normal.

GSM stands for Global System for Mobile Communications. It’s a standard for cellular communications between mobile phones. The best way to think of GSM is as the second generation (2G) of mobile communication technologies—the predecessor of 3G and 4G networks. However, according to reports, GSM is the default standard for mobile networks used by the majority of telecoms. It’s available in more than 219 countries and territories and it demands a 90 percent share of the mobile telecom market.

They could have had access to information about which calls are processed by a particular cell, then redirected these calls to other cells, activated neighbor cells and performed other offensive activities.

“The ability of this group to penetrate and monitor GSM networks is perhaps the most unusual and interesting aspect of these operations,” Kaspersky Lab’s Global Research and Analysis Team reported yesterday. “In today’s world, we have become too dependent on mobile phone networks which rely on ancient communication protocols with little or no security available for the end user. Although all GSM networks have mechanisms embedded which allow entities such as law enforcement to track suspects, there are other parties which can gain this ability and further abuse them in order to launch other types of attacks against mobile users.”

The attackers were able to steal credentials from an internal GSM Base Station Controller belonging to a large telecom operator that gave them access to GSM cells in that particular network, Kaspersky Lab said. My Threatpost colleague, Mike Mimoso, noted that Base Station Controllers manage calls as they move along a mobile network, allocating resources and mobile data transfers.

“This means that they could have had access to information about which calls are processed by a particular cell, redirected these calls to other cells, activated neighbor cells and performed other offensive activities,” Kaspersky Lab researchers wrote. “At the present time, the attackers behind Regin are the only ones known to have been capable of preforming such operations.”

In other words, the Regin actors can not only passively monitor cellular communications metadata, but they can also actively reroute cellular calls from one number to another.

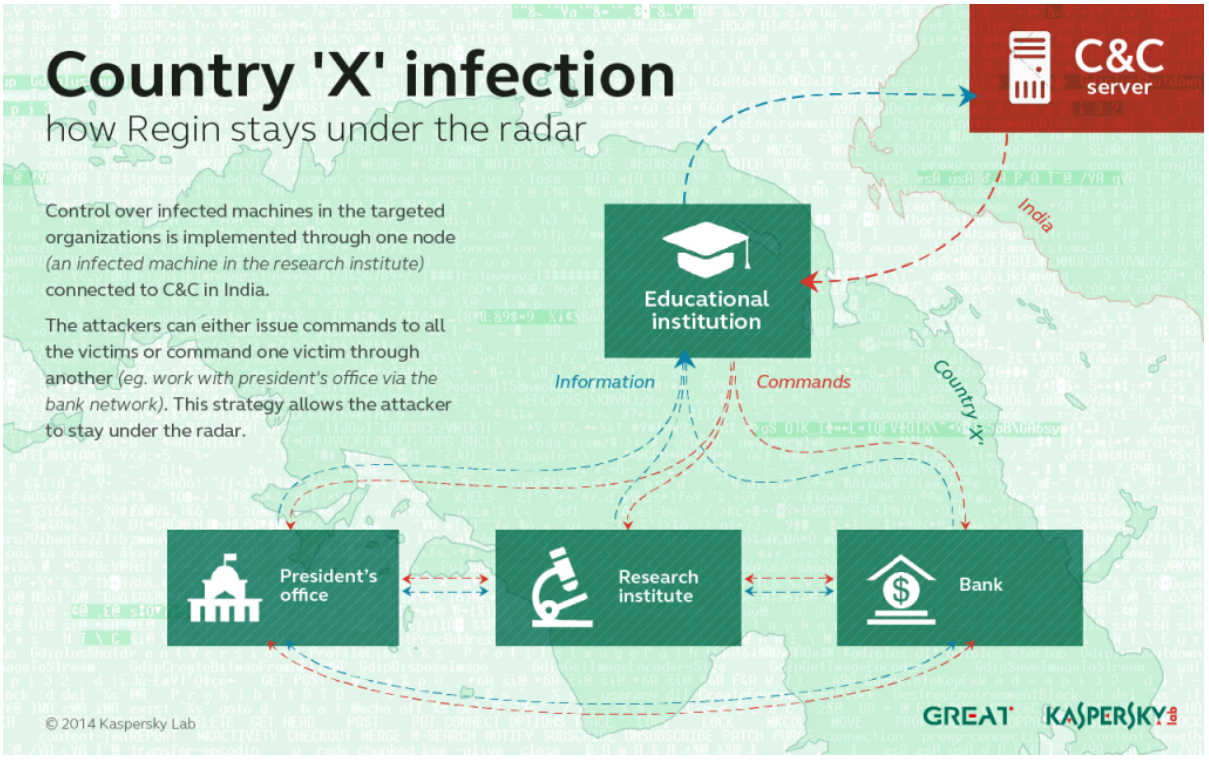
> #Regin #APT targets the usual victims plus a famed cryptographer and the GSM standard, according to @Kaspersky
>
> Tweet

Another bizarre and curious aspect of the Regin attack group is the story of a famed Belgian cryptographer and mathematician named Jean-Jacques Quisquater. In February of this year, reports began emerging that Quisquater’s personal computer had been hacked six months earlier. While it isn’t unusual for prominent academics to be targeted in cyberattacks, the case of Quisquater was slightly different because of some similarities between the attack that targeted his machine and a separate attack that targeted the Belgian telecom, Belgacom.

The latter incident was the subject of an Edward Snowden revelation claiming that the NSA and its British counterpart, GCHQ, had orchestrated the attack. Of course, many media outlets have alleged that these similarities do suggest that U.S. and British intelligence were behind both attacks. While neither Kaspersky Daily nor Kaspersky Lab will cosign those allegations, it was reported by a number of news outlets at the time and is worth mentioning.

In addition to the story of Quisquater and the fact that it targets GSMs, the Regin attack platform also boasts incredible technical sophistication, particularly in its pervasiveness. The attackers established backdoors with their command infrastructure to ensure inconspicuous persistence on the networks of their victims. All of the campaign’s communication traffic was encrypted to make sure attacks weren’t observed, both between the attackers and their control servers and between the victim’s machines and the attack infrastructure.

Most of Regin’s communications occur between infected machines – dubbed ‘communication drones’ – on the victim’s network. The reason for this is twofold: it allows for deep access while also limiting the amount of data exiting the network en route to a command and control server. When you see data leaving your network and traveling to an unknown network, that raises alarms. So this in-network, peer-to-peer communication makes it more difficult for network monitors to realize an attack is occurring.



In one unnamed Middle Eastern country, every single victimized network identified by Kaspersky lab, communicates with all of the other networks in a sort of peer-to-peer structure. The network included the president's office, a research center, an educational institution's network and a bank. One of the victims contains a translation drone that is able to forward the stolen data packets outside of the country, to the command and control server located in India.

"This represents a rather interesting command-and-control mechanism, which is guaranteed to raise very few suspicions," researchers wrote. "For instance, if all commands to the president's office are sent through the bank's network, then all of the malicious traffic that is visible to the president's office's sysadmins will only be with the bank, in the same country."

Regin is deployed in five stages, giving the attackers deep access to a victimized network as each stage loads subsequent parts of the attack. Modules in the first stage contain the only executable stored on the victim's computer, and they're all signed with phony Microsoft and Broadcom digital certificates in order to seem legitimate.

Kaspersky products detect modules from the Regin platform as: Trojan.Win32.Regin.gen and Rootkit.Win32.Regin. Kaspersky Lab has also released a full-length technical paper if you would like to dig a bit deeper.

Source: https://www.kaspersky.com/blog/regin-apt-most-sophisticated/6852/