The Grotesqueness of the “Federal Hack” of the German Government Network

Posted on **March 19,2018** by **sanna**

[Editor's note: This article was originally published on the web site of the FM4 radio channel of the Austrian Broadcasting Corporation. We have translated the text in order to make the content accessible for our English-speaking audience. We will follow-up on it with an article of our own about attribution, digital warfare, security intelligence, and the DeepINTEL conference.]

A friendly secret service knew more about espionage against the German government network than the German counterintelligence. Three months after the hack was discovered, the attackers are still somewhere in this huge federal network.

By Erich Möchel for fm4.orf.at

One week after the announcement of the attack on the security network of the German Federal Government details only leak slowly. The first official statement on Friday claiming that the alleged Russian Trojan suite was already under control was a blatant misinformation and had to be denied afterwards. According to official information, the German Government was tipped off in mid-December by a friendly intelligence service. That a secret service of a third state apparently knew more about espionage Trojans in the German government network than the German counterintelligence is an embarrassment beyond compare. The authorities can not even say now when this "federal hack" began, although they reportedly already knew about it three months ago. Not least because of this, a news blackout was imposed.

Tips among Friends

The attacked "Informationsverbund Berlin - Bonn" (IVBB) "is a huge, historically grown data network under the aegis of the German Interior Ministry, to which the German Bundestag, the Federal Council, the Federal Chancellery, the Federal Ministries and the Federal Court of Audit are connected as well as " various security authorities " from Berlin, Bonn and other locations. Who, apart from the the Federal Office for Information Security, these "various security authorities" might be can be counted on the fingers of one hand using only three fingers:

The Federal Bureau of Investigation, the secret services of the Federal Office for the Protection of the Constitution and the BND. The latter must also have been tipped off by the "friendly secret service" that attackers had infiltrated the information network of the German Federal Government. Further it was said that allegedly the invasion of the IVBB was part of a worldwide attack of supposedly Russian "hackers" against allies of the West, already going on since 2017. What’s more: The German authorities were already informed since December 19th.

A Question of Time

So the German authorities had three months to discover the intact parts of the malware and the artifacts of already deleted code and to stay on track of the attackers. This led to the actual target, namely the German

Foreign Ministry, where a dozen or more contaminated computers were discovered. Assuming that the statement of the government is correct not much more is known yet, but of course, this can't be verified. As for the duration of the attack it was said quite early on that the attackers could have already penetrated the network in early 2017, later on that it could have happened even earlier in 2016.

This has been the case for every comparable attack in the last ten years: each time the attackers were already much longer in the attacked network, as was initially suspected. And it is even more difficult to get rid of them, which is why such a high-level military cyber attack is also referred to as "Advanced Persistent Threat" (APT). It is a permanent threat because the malware consists of many small modules. If even one is overlooked by the defenders while cleaning up, the next attack will start soon. From the Equation Group (NSA) to Russian and Chinese Cyber Troops to the North Korean Lazarus Group, all major players use largely identical methods of attack.

Operational Sequence of a State Attack

First, one scouts the target network looking for points of attack, then, in several places, one smuggles in tiny programs, which are completely unremarkable on their own - the NSA calls them "Implants" or "Beacons". Their only function is not to attract attention internally for as long as possible, but to react to network scans from the outside with a "sign of life". As soon as the actual attack starts, further software modules are smuggled in at these marked locations in the target network. All of them are encrypted and just merge into a Trojan suite behind the firewalls. To counter such an attack is a purely Sisyphean task as long as the hidden implants of the attackers are still hidden somewhere in the net, because as soon as a network segment has been cleaned and control regained, the attack starts all over again in another segment.

The Hack of the German Bundestag in 2015

Exactly the same had happened in 2015 in the network of the German Bundestag. After the discovery of the attack in early May a weeks-long game of cat and mouse began, until, after three months, the Federal Office for Security (BSI) threw in the towel. It was decided to exchange all the hardware, which involved a total of 20,000 PCs. If they also thought of changing the routers, switches, printers or firewalls is not known. A few kilobytes of space on any device and a network connection is sufficient for the implant to continue its work - Namely by doing nothing, only sending a short ping to a command / control server somewhere on the Internet at a programmed time. Finding something like this in a huge network that was originally made up of mainframe computers and Windows 95 PCs and grew wild in all directions for two decades, is hardly feasible. Here everything is cross-linked and a segment of the network is the German Bundestag. So it is quite possible that some implants of the unknown attackers have survived the great clean-up of the Bundestag in 2015 unscathed.

Open Questions

From the first day on it was rumoured again that "the Russians" were responsible, first supposedly APT 28 ("Fancy Bear"), and then there was talk of APT 29 ("Cozy Bear"). This is not unlikely, because just a handful of nation states could pull off something like that. The infamous APT 28, to which the attacks during the US election campaign were attributed, has already been blamed for the hack of the Bundestag in 2015. This Cyber unit is the counterpart of the CIA coders, its task is operational and often includes psychological operations, thus influencing the public and politics.

APT 29, on the other hand, is comparable to the NSA Equation Group, involving the best programmers and therefore the most sophisticated software with the best camouflage. Of course, one does not want to squander these in propaganda operations - this is all about espionage at the highest level.

Regarding the question who tipped of the German BND, there are three possible answers: Either the British GCHQ or the NSA – but also the French intelligence service can not be ruled out.

Posted in:High Entropy,Security Intelligence | Tagged:Bundestag,Infrastructure,SecInt,Security | With 0 comments