NOW
www.nowlebanon.com
August 19, 2012

What is Gauss hiding?

Talking to Jarno Limnéll, cyber security expert
Matt Nash

A newly discovered computer virus, dubbed Gauss, seems aimed at Lebanon's Hezbollah, but one of the virus's functions is still shrouded in mystery. (AFP Photo)

Earlier this month, a new virus was found infecting computers almost exclusively located in the Middle East. Russian anti-virus software company Kaspersky Lab, which found the virus, said it was likely created approximately one year ago and was first deployed in September or October of 2011. Lebanon seems to have been singled out as a target as the virus specifically sought to steal usernames and passwords from customers who bank online with six Lebanese lenders. Dubbed Gauss by Kaspersky, the malware is certainly a tool for espionage, but its other capabilities remain a mystery.

Researchers have not yet fully decrypted the virus, so they are not sure what it is fully capable of. In fact, the "mystery code," is encrypted very strongly, prompting Kaspersky's Roel Schouwenberg to tell Wired magazine that the attention to encryption "really makes one wonder what is so special that they have gone through all that trouble. It must be something important."

NOW Lebanon spoke with Jarno Limnéll, director of cyber security at Stonesoft Corporation, to get his thoughts on what Gauss might really be up to.

When you first heard about Gauss, who did you think it was targeting?

Jarno Limnéll: I think that when more than two-thirds of infected computers are located in Lebanon, and I think that when we most probably know that Gauss was produced by the factories (meaning Israel and the US) as Stuxnet, I'm pretty sure the main target is to follow the banking flows in Lebanon, and what is the most important, most interesting issue for the United States and Israel in Lebanon, that's Hezbollah. [They are] especially [concerned] about the money flowing between Syria, Iran and Lebanon, meaning Hezbollah. This is only money, but as we all know, getting to know how the money is moving it tells you quite a lot, for example, about the arms trade.

What do you think Gauss's mystery code is hiding?

Limnéll: It's very hard to say anything about it, but I think it might involve some kind of surveillance, even a more sophisticated tool, targeting Hezbollah. It could be just one way to get in, to know more about how the organization works, what are their current activities with Iran, with Syria at the current moment. [The US and Israel] are more interested at this moment to follow what Hezbollah is doing and how they are cooperating or doing what Iran hopes them to do at this moment.

Stuxnet was designed to disrupt centrifuges that Iran is using to enrich uranium. Do you think Gauss was partially designed to disrupt Hezbollah's military or communication systems?

Limnéll: No, to be short, and in my opinion, I don't believe there's that kind of mystery code in this. I think whatever the mystery code is, it is there more or less for surveillance purposes. I don't think in this malware there is a physical part of it that would create some sort of disorder. I think this is surveillance malware. But, at the same time, those speculations you gave me about the mystery code, I would not be surprised at all if there is another malware already in Lebanon doing something like this but that we are not aware of it yet.

Gauss was discovered almost by accident as researchers were looking for variants of a related virus – Flame. Do you think we will see more of these types of viruses in the near future?

Limnéll: I'm pretty sure that within the next few months, there will be at least one or two of these kinds of findings in the Middle East. I think these activities will increase. And there's another aspect I think is important to bring up. For superpowers, if you want to show you have the capabilities, every now and then you have to expose your capabilities – what you are able to do, what kind of malwares you are already sending out – even if this is, as we all know, very dangerous policy. I think the main issue about the Stuxnet wasn't about disrupting the nuclear facilities of Iran, I think the main aspect of Stuxnet was, especially afterward when the United States unofficially admitted that they were behind it, was to show their capabilities to the world. To say, "Hey, we are building these kind of sophisticated cyber weapons and we are not hesitating to use them." This is a very strong message.

www.nowlebanon.com/NewsArticleDetails.aspx?ID=429131#