The Russian security research group Kaspersky Labs announced they had found a new computer virus infecting thousands of computers in the Middle East. Called "Gauss," after a filename found in its codebase, the malware can capture information about the infected computer, including Internet browsing histories, user login details, and system configuration details. The existence of Gauss suggests that countries may be using cyber warfare for more than just countering imminent threats, and that, with the rules of digital engagement so ambiguous, there's little to restrain or guide cyberwar's development.

Kaspersky Labs was blunt: Gauss, it says, is likely a “nation-state sponsored banking Trojan” built by the same programmers behind Stuxnet and Flame, the recent, sophisticated digital pathogens often speculated as designed by the United States and Israel. However, unlike these viruses, which both targeted Iran, Gauss appears to have a very different target: the banking system of Lebanon.

Gauss is the latest in a line of massive malware attacks, and much like its predecessors, it appears to be so complex and sophisticated that it's assumed to have been built by a sovereign state. Gauss uses the same platform as Flame, a “cyber espionage” program that was found in a number of locations in Iran in early 2012 and was capable of comprehensive surveillance of infected computers. Flame itself bore a strong family resemblance to Stuxnet, a 2010 virus that targeted the Iranian nuclear research program.

Like Flame, Gauss transmits detailed records of user activity back to its central command. Like Stuxnet, it carries a special encrypted “payload” that targets machines that carry specific system configurations. Stuxnet’s
payload would identify and disable nuclear research systems, but the encryption for the Gauss payload has not yet been broken, and its purpose remains unknown.

Researchers have found evidence suggesting the United States may have developed three previously unknown computer viruses for use in cyber warfare. Anti-virus software makers Symantec of the US and Kaspersky Lab of Russia say about a dozen computers in Iran and Lebanon are infected. The researchers say the malware fits the profile of military operations. The US has already been linked to the Stuxnet Trojan that attacked Iran's nuclear programme in 2010 and the Flame cyber surveillance tool that was uncovered in May. However, unlike Flame and Stuxnet, which targeted a rogue state's government networks, Gauss goes after the commercial sector in a country that has normalized relations with the United States. Out of more than 2,500 identified instances of Gauss, nearly two-thirds of have been found in Lebanon. And, unlike the broad spying capacity of Flame, Gauss seems designed for the narrow purpose of capturing transaction data from financial institutions and digital payment providers; specifically, Lebanese banks Fransabank, Bank of Beirut, BLOM, Credit Libanais, Byblos Bank, and EBLF, as well as siphoning data from PayPal and Citibank.

Why Lebanon? Why banks? Stealing financial transaction data is traditionally the province of, say, shadowy underground criminal gangs. Lebanon is a small country better known for its vibrant nightlife and perpetual domestic volatility. Neither its banking sector nor the state itself are obvious targets for the U.S. or Israeli intelligence services, which, though they haven't been connected to Gauss, are the only groups with both the know-how and, if they truly were behind Stuxnet and Flame, the track record.

However, Lebanon's size belies its importance as a regional entrepôt and banking haven; its cosmopolitan libertarianism, along with old-world discretion, have long made the country a popular choice for foreign depositors of all profiles and persuasions.

These are not mere corner retail banks serving up loans, mortgages, and checking accounts to Lebanese citizens. They are among the most private banks in the world, bound by genteel conventions of secrecy long since abandoned elsewhere. Since 1956, domestic and foreign banks operating in Lebanon have been legally required to protect the names and assets of their clients from all inquiring authorities.

U.S. financial regulators, concerned with money laundering and terrorism financing, have long given special attention to the opacity and reach of the Lebanese banking system. A 2000 advisory by the U.S. Department of Treasury Financial Crimes Enforcement Network instructed all U.S. banks to "give enhanced scrutiny to all financial transactions originating in or routed to or through Lebanon." In 2011, the Lebanese Canadian Bank was shuttered after the U.S. revealed that the Lebanese militant group Hezbollah was using the bank to launder money from cocaine profits, Mexican cartels, and African conflict diamonds. This year, the entire national banking system has come under scrutiny, accused of assisting members of the Syrian and Iranian regimes evade international sanctions and launder money that's also being funneled to Syria's ongoing conflict. The Kaspersky researchers think that Gauss first made its way onto Lebanese computers in late summer 2011, as violence worsened in Syria and Iranian nuclear talks stalled. Without the decrypted contents of the Gauss payload, it's impossible to know the virus' full capabilities, but it's not difficult to conjecture a likely purpose. Gauss appears to be capable of tracing the flow of illicit funds through some of the region's largest financial clearing houses, offering its designers unprecedented access to data on how money flows and between whom, on organizational networks, and on funding sources -- a veritable intelligence bonanza for anyone who might have an interest in that sort of thing.

The past few years have witnessed a remarkable evolution in cyber warfare. Only two years ago, Stuxnet seemed like science fiction: it stunned researchers with its scale, sophistication, and the sheer resources that had apparently gone into its development. Its deployment has raised serious questions about computer science and ethics, but was otherwise hailed as a non-kinetic, non-lethal way to temporarily derail Iranian nuclear ambitions. Flame -- an American-Israeli espionage effort against Iran -- received a similar reception in the U.S. But Gauss appears to be quite different, and is an indication of the slippery nature of the rules of engagement for cyberspace. It raises questions about the difference between private and public targets, the potential unintended consequences of malicious code reaching beyond its intended targets, and the security of the global financial transactions system -- if the bank vault is indeed a line that states are now willing to cross. And although Gauss appears to be primarily for surveillance, it's possible that it could also be a weapon, as it contains an executable payload of unknown scope. Even if it's not, Gauss's potential as spyware and attack software blurs the line between cyber war and cyber espionage, and its use may fall under the rules of...
engagement for cyber warfare set out by the U.S. Department of Defense.

The rules primarily sanction reactive defensive actions, with executive approval required for a targeted cyber assault against an enemy. However, these rules of engagement are currently up for revision, with greater power for proactive defense among the proposals.

--

Maan Barazy

Certified Shari'a Adviser and Auditor (CSAA- AAOIFI Certified) - MA Islamic Comparative Jurisprudence - BS International Economics

Managing Partner And CEO of Data and Investment Consult-Lebanon - The Centre For Islamic Finance - Consultant Researcher and Lecturer

--

You received this message because you are subscribed to the Google Groups "Kantakji Group" group. To post to this group, send email to kantakjigroup@googlegroups.com

To unsubscribe from this group, send email to kantakjigroup+unsubscribe@googlegroups.com

For more options, visit this group at http://groups.google.com/group/kantakjigroup?hl=en

--