Super Cyber Weapons Released: 'Rocra' found on State Networks

by staff report via minnie - CSM & RawStory *Wednesday, Jan 16 2013, 9:51pm*
international / prose / post

The US and Israel are directly LIABLE for all Corporate losses from variant State cyberweaponry

> When computer security experts recently discovered the hugely sophisticated and obviously state-sponsored cyberspy worms Stuxnet and Flame, many wondered out loud whether organized criminals might soon get their hands on similar malware tools that can siphon almost any sensitive information from even the best-guarded system.

The answer may have been staring at them from their computer screens all along.

On Monday, the Russian Internet security firm Kaspersky Labs announced that it has hunted down a previously unknown, advanced cyber-espionage network that it calls "Red October" (after Tom Clancy's novel), which has probably been vacuuming top-secret data from diplomatic, scientific, and corporate computers around the world since 2007.

According to the firm, the network is still active.

"Red October operations started five or more years ago, and during that time attackers went unnoticed," says Igor Soumenkov, a malware expert with Kaspersky Labs. "That is why discovery of other attacks of the same class is possible, and we do expect it."

But unlike Stuxnet and Flame, which were almost certainly cyberweapons deployed by the United States and its allies against adversaries like Iran, victims of the new Red October malware, or Rocra for short, span the globe.

Kaspersky says in its report that it began investigating the network after a tip from an anonymous partner, and has so far identified hundreds of infections worldwide, all of them in top locations such as government networks, diplomatic institutions, nuclear and aerospace agencies, and international trade groups.

The largest number of attacks – almost 100 – have struck computers in Russia and the former Soviet Union. But, Kaspersky says, "there are also reports coming from North America and Western European countries such as Switzerland or Luxembourg."

The attackers designed custom software to attack particular computer systems, experts say, using "unique modular architecture" comprising malicious extensions, data-grabbing modules, and backdoor trojans. Information extracted was often reused to gain entrance to other systems, by making it easier for the hackers to guess passwords and bypass security barriers.

'Mothership' cloaked

The network of infected computers was controlled by a vast infrastructure created by the attackers, including more than 60 domain names and server hosting locations in several countries, mainly Russia and Germany. Kaspersky says the network was cleverly camouflaged to hide the location of the "mothership" control server.

The level of Red October's sophistication is comparable to the best state-sponsored efforts, such as Stuxnet and Flame, but could conceivably be the work of rogue operatives from the criminal world, says Mr. Soumenkov.

"This is the first attack that can be compared, judging by its complexity, with state-sponsored attacks like Flame," he says.

"But at the same time it can hardly be referred to as state-sponsored. It is unknown whether the collected data was used by attackers themselves, or was sold to other interested parties.... We are talking about the most sensitive types of data like confidential documents, e-mail exchanges, contact information. Scientific information was targeted as well, judging by the profiles of some victims," he adds.

While declining to name any culprits as yet, Kaspersky says based on several factors, including "numerous artifacts left in executables of the malware, we strongly believe that the attackers have Russian-speaking origins."

They also suggest that Chinese hackers may have been involved in setting up the network.

"It's probably not correct to say that this threat comes from Russia," says Alexei Lukatsky, a consultant for CISCO in Russia.

"The servers are situated in Russia and in Germany, but when we're talking about hosting servers, any company or any person from any part of the world can actually do it. The Internet has no borders.... The same is true about the claim of Chinese traces. The only context where Chinese experts can be mentioned here is the fact that the vulnerabilities used for this type of programs were identified first by Chinese specialists," Mr. Lukatsky says.

This is the second time Kaspersky has uncovered a major global cyberthreat, which could raise questions among the suspicious-minded about whether it may be acting as a cat's paw, or even agent, for Russian intelligence interests. Its exposure of Flame last year was probably quite untimely from the US point of view.

"It strikes me as odd that this was exposed by a private company working on a private order," says Alexei Kondaurov, a former KGB major general. "Where are FAPSI [the former Russian equivalent of the US National Security Agency], the CIA, and other agencies that are supposed to be on top of these threats? Maybe Kaspersky is interested in advertising itself, and that's why there's so much noise about this?"

[In hacker terms it's called reverse engineering and improving or creating a variant from the original code.

Variants are much more difficult to detect and are usually more devastating in effect. In common parlance this is called 'blow back!' The Israeli-US designed Stuxnet was a cyber weapon designed to trash Iranian nuclear centrifuges, it succeeded but at what cost? Every hacker on the planet was aware that a monster would soon be created and released into the 'wild' via reverse engineering and variations of the Stuxnet code that was now freely running around the net -- too easy. So today we have 'Red October' and a few more undetected 'superworms' doing their highly destructive and costly dirty work.

Hackers can't thank imbecile Americans and Israelis enough for all the help -- we can always rely on the dumb yanks and hyper reactive Jews for over kill -- in the case of Stuxnet it truly was a sledge hammer used on a mosquito and the repercussions will prove far more devastating for the US and Israel than any risk of the Iranians obtaining a nuclear bomb, much less using it -- YOU SUPREMELY IRRESPONSIBLE, DUMB FUCK'S!]

http://www.rawstory.com/rs/2013/01/16/red-october-malware-found-snooping-on-russian-state-networks/