SWCP Portal

August 2017

From Russia with Malware

Should We Trust Foreign Tech?

With Russian hackers being accused of **stealing personal information**, **launching crippling malware** to lock up users' computers, and **interfering with the 2016 elections**, a lot of people both in and out of government are getting nervous about using any software from Russia.

In particular, questions have arisen about one of the most prominent cybersecurity firms on the planet, **Kaspersky Labs**. This Moscow-based company is a major provider of antivirus security products, both for enterprises and individuals. Their products are considered among the best protection available, and many are employed in other companies' products and antivirus scanners with **400 million users** in 32 countries.

The problem is that for an antivirus program to work, it must have total access to a computer's files and it must freely communicate with a remote database to ascertain threats. This gives the program a great deal of covert potential.

Because of their embedding, half the users of their product may not even be aware of the source. **Known** to have worked with the Russian government against cyberthreats, Kaspersky is now **developing** an OS for the Internet of things

They have a reputation for being on the leading edge of discovering new malware. For instance, Kaspersky was the first firm to identify and describe the infamous **Stuxnet virus**. They also **found** some NSA hacking tools in the wild as well as those from the British GCHQ spy agency.

Note, however, that Stuxnet was an American-Israeli weapon aimed at Iran. The company has been **far less successful** in identifying threats from Russia. This omission seems suspicious.

Kaspersky has long been quietly suspected of having ties to Russia's online spying efforts. The billionaire founder, **Eugene Kaspersky**, was trained by the KGB in electronics and cryptography. While he has insisted on his political independence from the start, that his intention is to investigate and expose "cyber-evil", the real picture is more complicated and rather murky.

He is **known** to attend regular sauna parties with friends, including FSB (the successor of the KGB) agents. But there may have been moles working for Western intelligence in his company, too. In December, a well-respected staff researcher, Ruslan Stoyanov, was **arrested** for possible treason along with the head of the FSB's Center for Information Security and several others.

However, the most damning evidence so far comes from **Kremlin documents**. On certificates issued by the FSB to companies operating in Russia, Kaspersky Labs was listed with a number designating it as a military intelligence unit.

It has long been suspected that Kaspersky's antivirus products might include a **secret backdoor** to allow undetectable access for Russian spy agencies. So in recent months, the FBI has quietly sent its agents out to **question Kaspersky employees** across the country. The interviews took place shortly after it was **disclosed** that former National Security Advisor Michael Flynn had been paid over $11,000 in consulting fees by the company just before taking his new job.

Right after the interviews, the Senate Armed Services Committee approved a bill that would bar the Petagon from using Kaspersky products. The **bill** would even require the Defense Department to sever any contacts with networks that did.

At a Senate Intelligence Committee hearing, the heads of National Intelligence, plus the CIA, NSA, FBI, and the DIA agencies were **asked** whether they would trust Kaspersky products on their own computers. They unhesistatingly said, "No."

The Chinese and the NSA

Of course, the Russians aren't the only cyber-adversaries. The Chinese are not far behind, and they also produce a lot of the devices we depend on from iPhones to routers. Their two largest telecommunications equipment manufacturers **Huawei Technologies Co. Ltd**. and **ZTE Corp**., were **called threats to national security** by the House of Representatives Permanent Select Committee on Intelligence several years ago for furnishing incomplete and evasive answers.

The fear of the Chinese also revolves around backdoors from bad software – either intentionally or inadvertently – or that during cyberwar Chinese-made devices would respond to a specially-coded string of numbers. This so-called "**magic kill packet**" could shut down computers across networks much like those that can wake up devices across local area networks.

Like other backdoors, such packets are mainly theoretical; American cyberintelligence agencies claim that any such built-in technique could be eventually discovered and used by other parties. Nonetheless, the Defense Department is **taking steps** to forbid the use of Chinese Lenovo computers which had been found to be covertly communicating with remote users.

Naturally, our spies are trying the same things out on our foes. Among Edward Snowden's pilfered cache of **NSA documents** were details of how the NSA can intercept new computers and routers within the supply chain and undetectably insert hardware and software backdoors.

One need only look at the drastic **cybersecurity advice** for academic travelers to Russia or China to get an idea of how bad the situation really is. Travelers are advised not to go at all; if they must, to leave devices at home. But if they must take a computer, use an inexpensive temporary device without any personal information on it. Keep it turned off when not using, do not install any software or hardware or download anything while abroad. Then examine, sanitize, and get rid of it as soon as you get back home.

What are ordinary users to do? Fortunately, these days the security software built into platforms like **Windows Defender** and **Windows Updates** are **pretty good**. Probably the best free antivirus scanner is **Avast**, but as always with "free" software, you must be careful during installation, only downloading what you really need. But whatever you use, update it frequently.

Watch out for...

Microsoft Removes Old Favorites

The software giant has **relented**, deciding not to get rid of its ancient but beloved **Paint** program after all, due to the **online outcry** after the announcement. It will be replaced by an **app** free for downloading from the Windows Store.

Windows 10 replaced its equally old and popular **Photo Viewer** utility with a new photo app that many users don't like. For those who upgraded from Windows 7 or 8, it's still on the computer and can easily be **restored** to prominence, while those who freshly installed Windows 10 may have a slightly more difficult **task**.

A number of other programs will be deprecated in the upcoming Fall Update. Check Microsoft Support for a **full list**, and if you don't want loose any of them, be careful what Windows Updates you choose to download and install.

The Sun Is Going Dark

Unless you've been stuck under a rock all summer, you know that an eclipse of the Sun takes place **Monday, August 21**. Here **in Albuquerque**, this rare and fascinating spectacle will reach almost **75%** of full coverage at **11:45 AM**,

Protecting your vision while viewing is vital – sunglasses aren't nearly dark enough. Even cheap paper solar eclipse glasses are quickly being sold out **online**, but some may still be available at places like Lowe's and Wal-mart.

Our local **astronomy society** will set up at Balloon Park; the **UNM Observatory** on Yale and the **Public Library** at Cherry Hill will host parties, and a viewing event held at the **Natural History Museum.** More will doubtless be announced as the day draws nigh. There won't be another comparable sky-show until *2045*, so get ready!

Southwest Cyberport

New Mexico's Expert Internet Service Provider since 1994
505-243-SWCP (7927) ◉ **SWCP.com** ◉ **Help@swcp.com**
5021 Indian School NE, Suite 600, Albuquerque, NM 87110

Archived at: http://www.swcp.com/newsletters/.
Click on blue terms in PDF file to open links.