KIM ZETTER SECURITY 02.16.15 02:00 PM

SUITE OF SOPHISTICATED NATION-STATE ATTACK TOOLS FOUND WITH CONNECTION TO STUXNET

Employees work inside the headquarters of Kaspersky Lab, Dec. 9, 2014.

ALEXANDER ZEMLIANICHENKO /GETTY IMAGES

CANCUN, Mexico—The last two years have been filled with revelations about NSA surveillance activities and the sophisticated spy tools the agency uses to take control of everything from individual systems to entire networks. Now it looks like researchers at Kaspersky Lab may have uncovered some of these NSA tools in the wild on customer machines, providing an extensive new look at the spy agency's technical capabilities. Among the tools uncovered is a worm that appears to have direct connections to Stuxnet, the digital weapon that was launched repeatedly against centrifuges in Iran beginning in late 2007 in order to sabotage them. In fact, researchers say the newly uncovered worm may have served as a kind of test run for Stuxnet, allowing the attackers to map a way to targeted machines in Iran that were air-gapped from the internet.

that belong to several highly sophisticated digital spy platforms that they say have been in use and development since 2001, possibly even as early as 1996, based on when some command servers for the malware were registered. They say the suite of surveillance platforms, which they call EquationLaser, EquationDrug and GrayFish, make this the most complex and sophisticated spy system uncovered to date, surpassing even the recently exposed Regin platform believed to have been created by Britain's GCHQ spy agency and used to infiltrate computers belonging to the European Union and a Belgian telecom called Belgacom, among others.

The new platforms, which appear to have been developed in succession with each one surpassing the previous in sophistication, can give the attackers complete and persistent control of infected systems for years, allowing them to siphon data and monitor activities while using complex encryption schemes and other sophisticated methods to avoid detection. The platforms also include an innovative module, the likes of which Kaspersky has never seen before, that re-flashes or reprograms a hard drive's firmware with malicious code to turn the computer into a slave of the attackers. The researchers, who gave WIRED an advance look at their findings and spoke about them today at the Kaspersky Security Analyst Summit in Mexico, have dubbed the attackers the Equation Group and consider them "the most advanced threat actor" they've seen to date.

The researchers have published an initial paper on their findings and plan to publish more technical details over the next few days, but there's still a lot they don't know about the Equation Group's activities.

"As we uncover more of these cyber espionage operations we realize how little we understand about the true capabilities of these threat actors," Costin Raiu, head of Kaspersky's Global Research and Analysis Team told WIRED.

NSA Connections?

Although the researchers have no solid evidence that the NSA is behind the tools and decline to make any attribution to that effect, there is circumstantial evidence that points to this conclusion. A keyword—GROK—

Edward Snowden to The Intercept that describe a keylogger by that name. There are other connections to an NSA spy tool catalog leaked to other journalists in 2013. The 53-page catalog details—with pictures, diagrams and secret codenames—an array of complex devices and capabilities available to intelligence operatives. The capabilities of several tools in the catalog identified by the codenames UNITEDRAKE, STRAITBAZZARE, VALIDATOR and SLICKERVICAR appear to match the tools Kaspersky found. These codenames don't appear in the components from the Equation Group, but Kaspersky did find "UR" in EquationDrug, suggesting a possible connection to UNITEDRAKE (United Rake). Kaspersky also found other codenames in the components that aren't in the NSA catalog but share the same naming conventions—they include SKYHOOKCHOW, STEALTHFIGHTER, DRINKPARSLEY, STRAITACID, LUTEUSOBSTOS, STRAITSHOOTER, and DESERTWINTER.

Other evidence possibly pointing to the NSA is the fact that five victims in Iran who were infected with Equation Group components were also key victims of Stuxnet, which was reportedly created and launched by the U.S. and Israel.

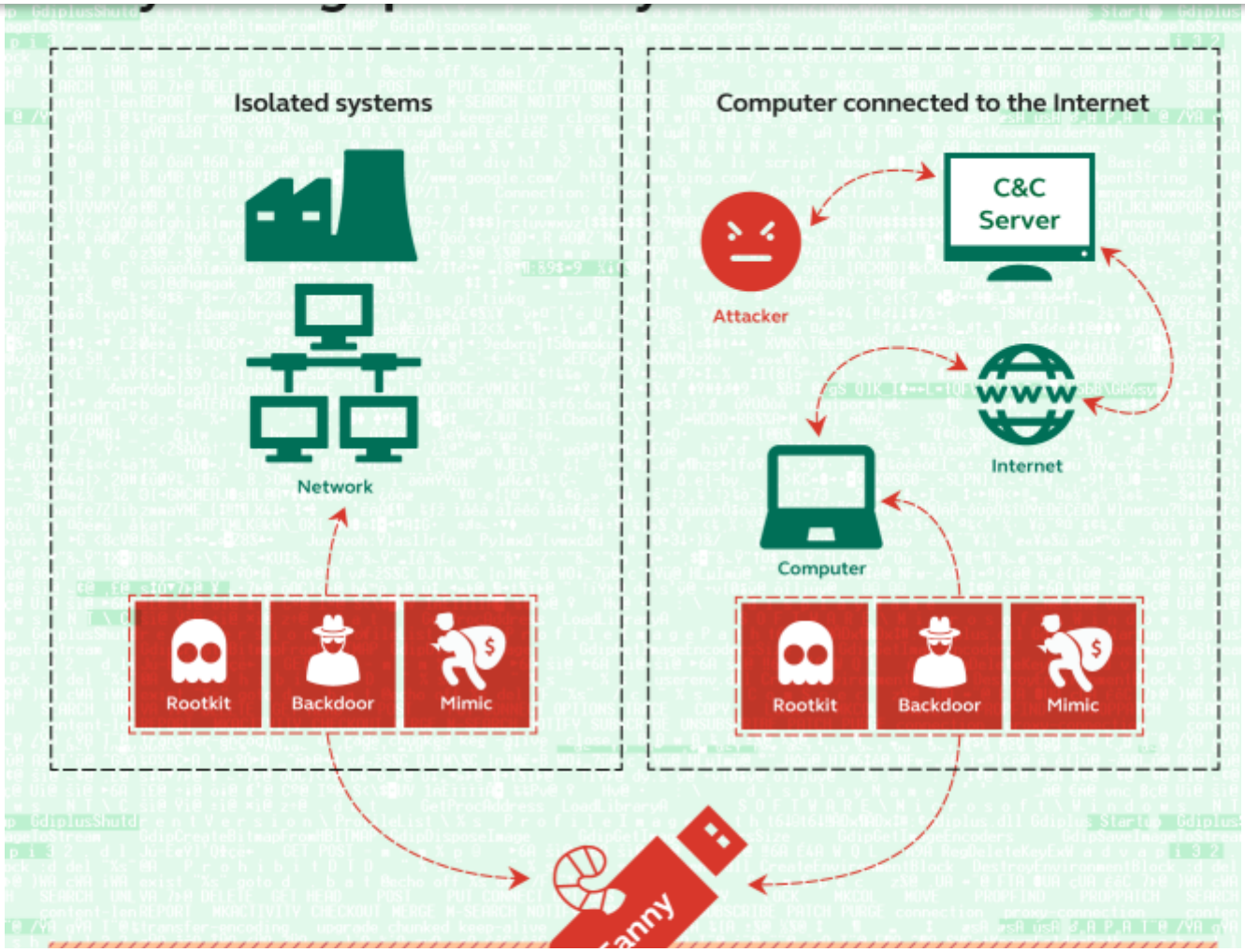
Kaspersky wouldn't identify the Iranian victims hit by the Equation tools, but the five key Stuxnet victims have been previously identified as five companies in Iran, all contractors in the business of building and installing industrial control systems for various clients. Stuxnet targeted industrial control systems used to control centrifuges at a uranium-enrichment plant near Natanz, Iran. The companies—Neda Industrial Group, Kala Electric, Behpajooh, CGJ (believed to be Control Gostar Jahed) and Foolad Technic—were infected with Stuxnet in the hope that contractors would carry it into the enrichment plant on an infected USB stick. This link between the Equation Group and Stuxnet raises the possibility that the Equation tools were part of the Stuxnet attack, perhaps to gather intelligence for it.

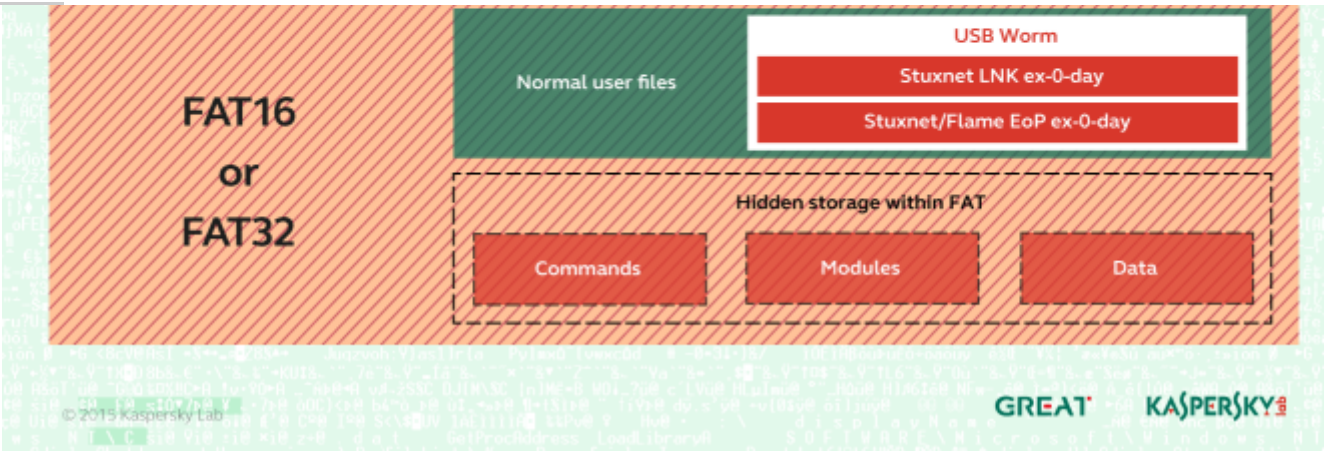
But the newly uncovered worm created by the Equation Group, which the researchers are calling Fanny after the name of one of its files, has an equally intriguing connection to Stuxnet.

It uses two of the same zero-day exploits that Stuxnet used, including the infamous .LNK zero-day exploit that helped Stuxnet spread to air-gapped

.LNK exploit in Fanny has a dual purpose—it allows attackers to send code to air-gapped machines via an infected USB stick but also lets them surreptitiously collect intelligence about these systems and transmit it back to the attackers. Fanny does this by storing the intelligence in a hidden file on the USB stick; when the stick is then inserted into a machine connected to the internet, the data intelligence gets transferred to the attackers. EquationDrug also makes use of the .LNK exploit. A component called SF loads it onto USB sticks along with a trojan to infect machines.

The other zero-day Fanny uses is an exploit that Stuxnet used to gain escalated privileges on machines in order to install itself seamlessly.





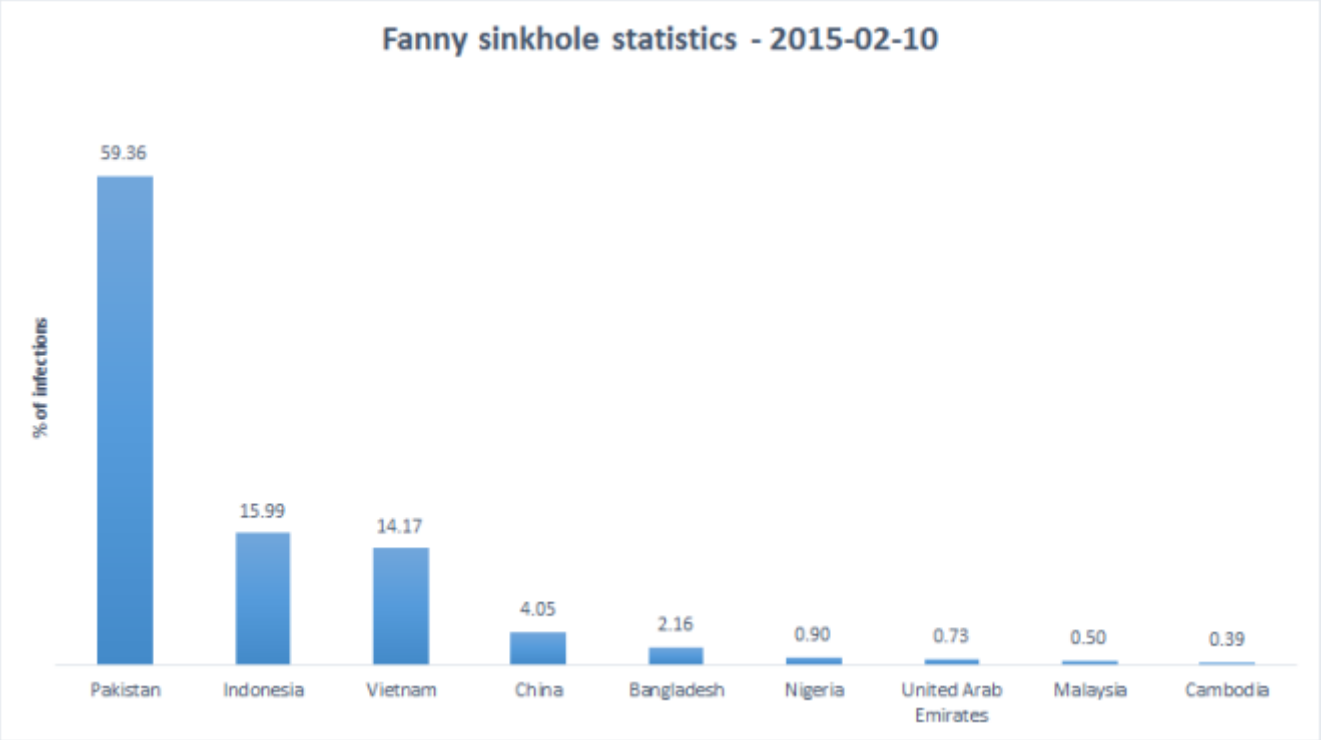
Raiu says he thinks Fanny was an early experiment to test the viability of using self-replicating code to spread malware to air-gapped machines and was only later added to Stuxnet when the method proved a success. Notably, the first version of Stuxnet, believed to have been unleashed in late 2007, didn't use zero-day exploits to spread; instead it spread by infecting the Step 7 project files used to program control systems at Natanz. Fanny was subsequently compiled in July 2008 with the two zero-day exploits. When the next version of Stuxnet was unleashed in 2009, the privilege-escalation

was added to a version of Stuxnet unleashed that March and April.

Fanny may have been used initially as proof-of-concept to test the viability of getting Stuxnet onto air-gapped machines in Iran. Or it could have been used for a different operation entirely, and its developers simply shared the exploits with the Stuxnet crew. The vast majority of Fanny infections detected so far are in Pakistan. Kaspersky has found no infections in Iran. This suggests Fanny was likely created for a different operation.

Pakistan's nuclear weapons program, like Iran's, has long been a U.S. concern. The centrifuge designs used in Iran's uranium-enrichment plant at Natanz came from Pakistan—a Pakistani scientist helped jumpstart Iran's nuclear program with them. Information about the NSA's black budget, leaked by Snowden to the *Washington Post* in 2013, shows that Pakistan's nuclear program, and the security of its nuclear weapons, is a huge concern to U.S. intelligence and there is "intense focus" on gaining more information about it. "No other nation draws as much scrutiny across so many categories of national security concern," the *Post* wrote in a story about the budget.

Kaspersky found only one version of Fanny. It arrived in their virus collection system in December 2008 but went unnoticed in their archive until last year. Raiu doesn't know where the Fanny file came from—possibly another anti-virus firm's shared collection.



Kaspersky has found 500 victims in some 30 countries infected with EquationLaser, EquationDrug and GrayFish components. But having been active for more than a decade, it's likely the spy tools have infected tens of thousands of systems. Each time a machine is infected, the malware places a timestamp in the victim's registry along with a counter that increases with each victim. Based on counters found on victim machines, the victims appear to increase at a rate of about 2,000 a month.

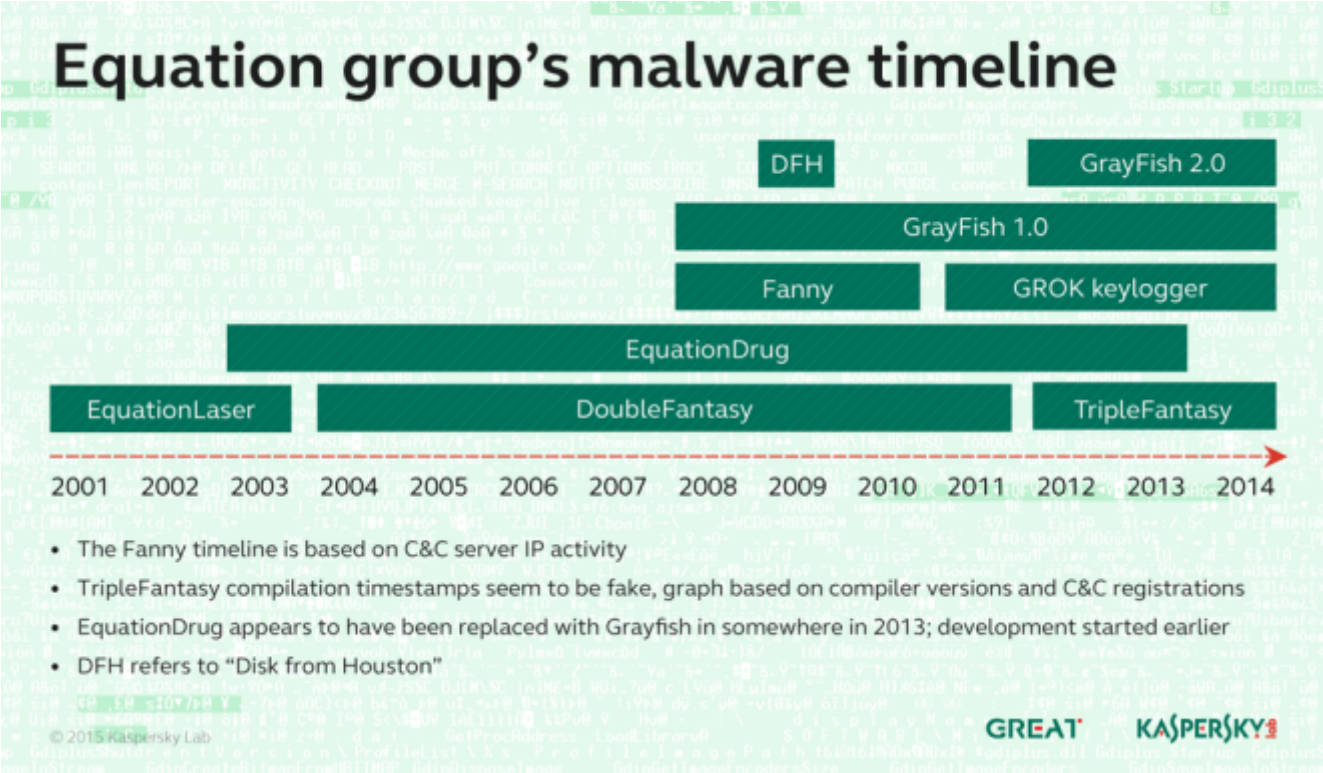
The largest number of victims have been targeted in Iran, but there are also victims in Russia, Afghanistan, Pakistan, Belgium, Germany, Sudan, Lebanon, the Palestinian Territories, the United States and the UK. They include military, government and diplomatic targets, as well as telecoms, nuclear research facilities and individuals, Islamic activists and scholars, the media, and those working on nanotechnology and encryption technologies. Victims found in the U.S. and UK are all Islamic activists or scholars, Raiu says, some with known extremist leanings.

Kaspersky researchers discovered the first component belonging to the Equation Group last March while investigating the Regin malware. The first piece of puzzle found was a driver file that showed up on a system in the Middle East that was also infected with Regin and several other known families of nation-state malware Kaspersky recognized. This apparently high-value target was cluttered with so much malware Kaspersky dubbed it the "magnet of threats".

They initially believed the driver was part of Regin or another malicious family. It used very advanced stealth techniques to avoid detection and was only discovered because of the way it tried to hijack a specific Windows function to sniff network traffic. This triggered an alert in the Kaspersky software. It was using "some nasty techniques to hook into Windows," says Vitaly Kamluk, principal security researcher for Kaspersky. The techniques, in fact, had been described years before in a 2005 book titled Subverting the Windows Kernel. "[The attackers] were following the instructions that were uncovered in the book," Kamluk says.

After adding detection for the driver to their security products, Kaspersky found the malicious driver on other machines as well as additional components related to it. As they collected modules and pieced them

servers—more than 300 in all—that the attackers had set up to communicate with their malware. Kaspersky managed to sinkhole about a dozen of the domains so that traffic that would have once headed from victim machines to the attackers' domains got re-routed to a server the researchers controlled instead. In this way they were able to uncover more victims. The attackers had allowed the registration for a number of their domains to expire. Kaspersky monitored the domains and simply bought up each as it expired.



As they pieced together components, they were able to establish a timeline and see that EquationLaser was an early-generation implant the attackers used between 2001 and 2004, while EquationDrug was the next-generation tool that came into use sometime around 2003. It was continuously developed and expanded by the attackers until 2013. Over time, it became a robust and full-blown platform composed of numerous plug-ins or modules that could be remotely slipped on to an infected system at will, once the attackers established a foothold on it.

EquationDrug was supplanted by the even more sophisticated GrayFish. Two versions of GrayFish have been uncovered—the first apparently developed in 2008 and the second in 2012, based on compilation timestamps. EquationDrug stopped being used in mid-2013 right around the time the first leaks from NSA whistleblower Edward Snowden were published. The first

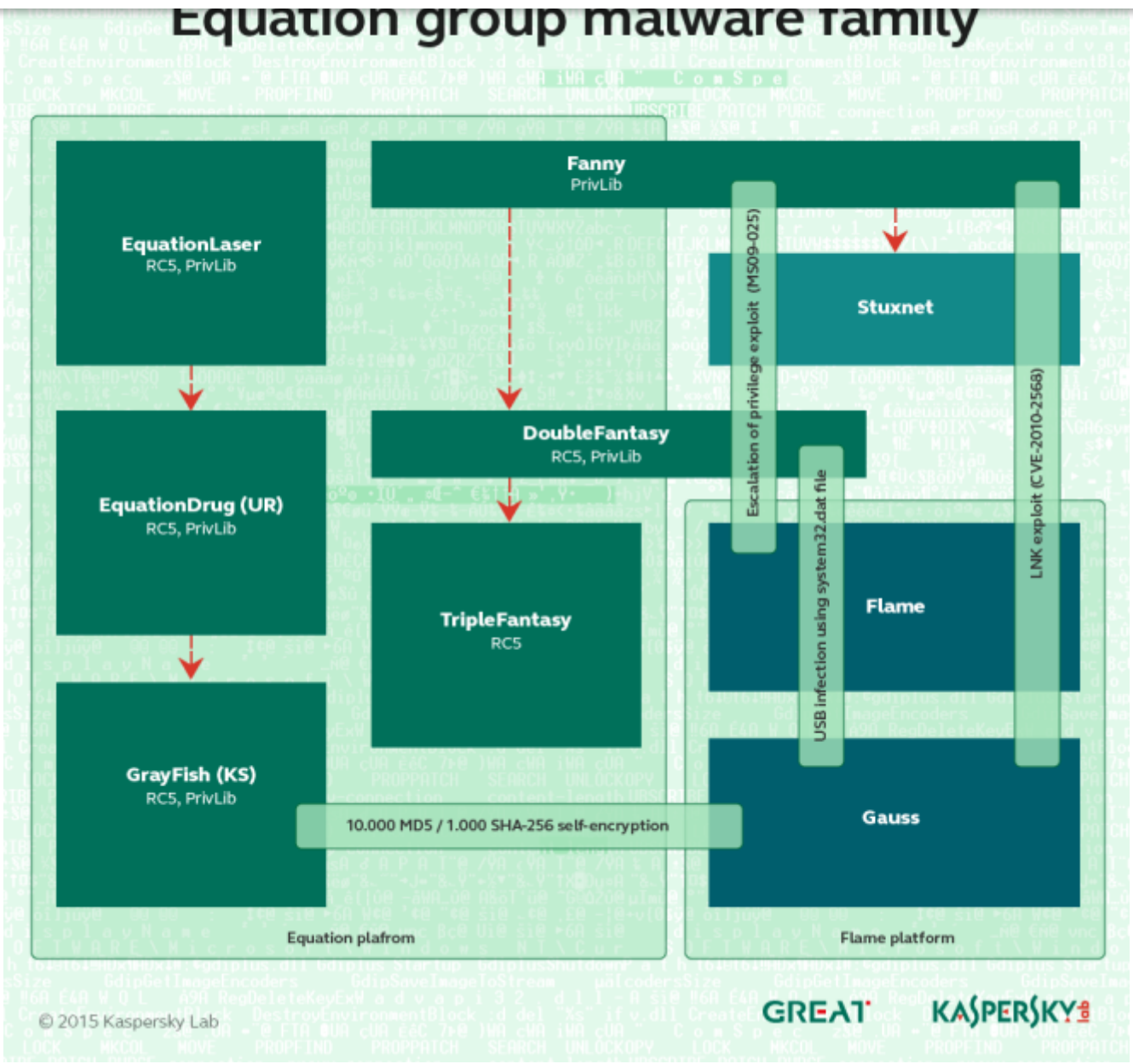
first leaks.

Enter GrayFish

GrayFish works on all the latest Windows operating systems as well as Windows 2000. It's the most sophisticated platform of the three. Its components all reside in the registry of infected systems, making the malware nearly invisible to detection systems.

GrayFish uses a highly complex multi-stage decryption process to unpack its code, decrypting and executing each stage in strict order, with each stage containing the key to unlock the subsequent one. GrayFish only begins this decryption process, however, if it finds specific information on the targeted machine, which it then uses to generate the first key to launch the decryption. This allows the attackers to tailor the infection to specific machines and not risk having it decrypt on unwanted systems. The magic key that initiates this process is generated by running a unique ID associated with one of the computer's folders through the SHA-256 algorithm 1,000 times. The final hash becomes the key to unlock the malware and launch the nested decryption scheme.

It's very similar to a process used by Gauss, another piece of malware believed to have been created by the team behind Stuxnet that Kaspersky discovered in 2012. Gauss had a mysterious payload that has never been unlocked because it can only be decrypted by a key generated by running specific data on the targeted machine through the MD5 algorithm 10,000 times. The scheme, as used in both GrayFish and Gauss, not only serves to prevent the malware from unleashing on non-targeted machines, it also prevents security researchers and victims from unlocking the code without knowing the specific data needed to generate the hash/decryption key.



In addition to the encryption scheme, GrayFish uses a sophisticated bootkit to hijack infected systems. Each time the computer reboots, GrayFish loads malicious code from the boot record to hijack the booting process and give GrayFish complete command over the operating system, essentially making GrayFish the computer's operating system. If an error occurs during this process, however, the malware will immediately halt and self-destruct, leaving the real Windows operating system to resume control, while GrayFish quietly disappears from the system.

But the most impressive GrayFish component is one that can be used to reflash the firmware of hard drives. Firmware is the code resident on hardware that makes the device work. Kaspersky uncovered two versions of a module used for reflashing or reprogramming firmware—one version for the

appears to have been compiled in 2010 while the GrayFish one bears a 2013 timestamp. The module reflashes the firmware with malicious code that gives the attackers a persistent foothold on the system even if the owner reformats the hard drive or wipes the operating system and reinstalls it in an attempt to clean the machine of malware. Between them, the two versions can reprogram 12 different brands of hardware drives, including ones made by Samsung and Seagate. To pull off this feat, the modules use a slew of undocumented commands that are specific to each vendor, which the Kaspersky researchers call "an astonishing technical accomplishment" that is a testimony to the group's high-level skills.

The attackers did make one mistake, however. It appears that one of the developers of the GROK trojan left his username—rmgree5—behind in the file.

Method of Infection

To infect victims, the attackers used multiple methods—such as the Fanny worm or infected USB sticks and zero-day exploits. They also used web-based exploits to infect visitors to certain web sites. The researchers counted at least seven exploits the attackers at least four of which were zero-days when the attackers used them. Notably, one of the exploits had been used before in the so-called Aurora attack that struck Google in late 2009. That hack was attributed to China, but the Kaspersky researchers say the Equation Group apparently recycled it to use in their own later attack against government targets in Afghanistan.

One of the most interesting cases of infection, however, concerned a scientist who was targeted after visiting the U.S.

Trouble in Texas

The scientist had attended an international scientific conference in Houston, Texas sometime around 2009 and received the infection on a conference CD-ROM sent to him after he returned home. The disk contained a slideshow of photos from the gathering. But it also contained three exploits, two of them zero-days, that triggered malware from the Equation Group to load to his

and sent a sample of the malware to Kaspersky's archive, but the researchers only discovered it last year when they began investigating the Equation Group's operations. They were able to identify and contact the victim. Raiu won't name the scientist or indicate his area of research, but he likened the attack to a recent one that occurred against noted Belgian cryptographer and academic Jean-Jacques Quisquater. Quisquater's computer had been infected with the Regin spy tool.

It's unclear how the attackers infected the CD-ROM sent to the scientist, but documents leaked by Edward Snowden describe NSA and CIA interdiction efforts that involve intercepting computer hardware as it's in transit from a factory or seller and then implanting it with spy tools before repackaging it and sending it on to the customer. The same method might have been used in this case. It's not known if other conference attendees received infected disks.

Although the Equation Group findings are significant, they still represent only a very small subset of nation-state malware out in the wild from not only the U.S. but other actors as well. And given that the samples Kaspersky found are at least a year old, they may not be state-of-the-art any more.

"The thing that scares me the most is that we don't have any samples from the Equation Group from 2014," Raiu says, suggesting the group's capabilities may have already been surpassed by even more sophisticated wares.

Update 1.17.15: To clarify in which NSA documents the GROK keylogger component is named.

SECURITY

The Equifax Breach Exposes America's Identity Crisis

LILY HAY NEWMAN

BUSINESS

Facebook May Have More Russian Troll Farms to Worry About

ISSIE LAPOWSKY

HACK BRIEF

Patch Your Android Phone To Prevent an Evil 'Toast' Attack

ANDY GREENBERG

SECURITY

How to Protect Yourself From That Massive Equifax Breach

LILY HAY NEWMAN

CRYPTOCURRENCY

Why It's So Easy to Hack Cryptocurrency Startup Fundraisers

LILY HAY NEWMAN

POLITICS

The DNC's Technology Chief is Phishing His Staff. Good.

ISSIE LAPOWSKY

GET OUR NEWSLETTER

WIRED's biggest stories delivered to your inbox.

Enter your email

SUBMIT

FOLLOW US ON YOUTUBE

Don't miss out on WIRED's latest videos.

FOLLOW