**Meet ‘Flame’, The Massive Spy Malware Infiltrating Iranian Computers**

* By [Kim Zetter](http://www.wired.com/threatlevel/author/kimzetter/) Wired Magazine, post May 28, 2012, at: <http://www.wired.com/threatlevel/2012/05/flame/>



Map showing the number and geographical location of Flame infections detected by Kaspersky Lab on customer machines. *Courtesy of Kaspersky*

A massive, highly sophisticated piece of malware has been newly found infecting systems in Iran and elsewhere and is believed to be part of a well-coordinated, ongoing, state-run cyberespionage operation.

The malware, discovered by Russia-based anti-virus firm Kaspersky Lab, is an espionage toolkit that has been infecting targeted systems in Iran, Lebanon, Syria, Sudan, the Israeli Occupied Territories and other countries in the Middle East and North Africa for at least two years.

Dubbed “Flame” by Kaspersky, the malicious code dwarfs Stuxnet in size – the [groundbreaking infrastructure-sabotaging malware](http://www.wired.com/threatlevel/2011/07/how-digital-detectives-deciphered-stuxnet/all/1?utm_source=Contextly&utm_medium=RelatedLinks&utm_campaign=Previous) that is believed to have wreaked havoc on Iran’s nuclear program in 2009 and 2010. Although Flame has both a different purpose and composition than Stuxnet, and appears to have been written by different programmers, its complexity, the geographic scope of its infections and its behavior indicate strongly that a nation-state is behind Flame, rather than common cyber-criminals — marking it as yet another tool in the growing arsenal of cyberweaponry.

The researchers say that Flame may be part of a parallel project created by contractors who were hired by the same nation-state team that was behind Stuxnet and its sister malware, [DuQu](http://www.wired.com/threatlevel/2011/10/son-of-stuxnet-in-the-wild/).

“Stuxnet and Duqu belonged to a single chain of attacks, which raised cyberwar-related concerns worldwide,” said Eugene Kaspersky, CEO and co-founder of Kaspersky Lab, in a statement. “The Flame malware looks to be another phase in this war, and it’s important to understand that such cyber weapons can easily be used against any country.”

Early [analysis of Flame by the Lab](http://www.securelist.com/en/blog?weblogid=208193522) indicates that it’s designed primarily to spy on the users of infected computers and steal data from them, including documents, recorded conversations and keystrokes. It also opens a backdoor to infected systems to allow the attackers to tweak the toolkit and add new functionality.

The malware, which is 20 megabytes when all of its modules are installed, contains multiple libraries,[SQLite3](http://www.sqlite.org/) databases, various levels of encryption — some strong, some weak — and 20 plug-ins that can be swapped in and out to provide various functionality for the attackers. It even contains some code that is written in the [LUA programming language](http://www.lua.org/) — an uncommon choice for malware.

Kaspersky Lab is calling it “one of the most complex threats ever discovered.”

“It’s pretty fantastic and incredible in complexity,” said Alexander Gostev, chief security expert at Kaspersky Lab.

Flame appears to have been operating in the wild as early as March 2010, though it remained undetected by antivirus companies.

“It’s a very big chunk of code. Because of that, it’s quite interesting that it stayed undetected for at least two years,” Gostev said. He noted that there are clues that the malware may actually date back to as early as 2007, around the same time-period when Stuxnet and DuQu are believed to have been created.

Gostev says that because of its size and complexity, complete analysis of the code may take years.

“It took us half-a-year to analyze Stuxnet,” he said. “This is 20-times more complicated. It will take us 10 years to fully understand everything.”

Kaspersky discovered the malware about two weeks ago after the [United Nations’ International Telecommunications Union](http://www.itu.int/en/Pages/default.aspx) asked the Lab to look into reports in April that [computers belonging to the Iranian Oil Ministry](http://english.farsnews.com/newstext.php?nn=8101301227) and the Iranian National Oil Company had been hit with malware that was [stealing and deleting information](http://english.farsnews.com/newstext.php?nn=8101301403) from the systems. The malware was named alternatively in news articles as [“Wiper”](http://www.nytimes.com/2012/04/24/world/middleeast/iranian-oil-sites-go-offline-amid-cyberattack.html)and [“Viper,”](http://www.csmonitor.com/USA/2012/0423/Latest-cyberattack-on-Iran-targets-oil-export-facilities) a discrepancy that may be due to a translation mixup.

Kaspersky researchers searched through their reporting archive, which contains suspicious filenames sent automatically from customer machines so the names can be checked against whitelists of known malware, and found an MD5 hash and filename that appeared to have been deployed only on machines in Iran and other Middle East countries. As the researchers dug further, they found other components infecting machines in the region, which they pieced together as parts of Flame.

Kaspersky, however, is currently treating Flame as if it is not connected to Wiper/Viper, and believes it is a separate infection entirely. The researchers dubbed the toolkit “Flame” after the name of a module inside it.



Flame is named after one of the main modules inside the toolkit. *Courtesy of Kaspersky*

Among Flame’s many modules is one that turns on the internal microphone of an infected machine to secretly record conversations that occur either over[Skype](http://www.skype.com/intl/en-us/home) or in the computer’s near vicinity; a module that turns Bluetooth-enabled computers into a Bluetooth beacon, which scans for other Bluetooth-enabled devices in the vicinity to siphon names and phone numbers from their contacts folder; and a module that grabs and stores frequent screenshots of activity on the machine, such as instant-messaging and email communications, and sends them via a covert SSL channel to the attackers’ command-and-control servers.

The malware also has a sniffer component that can scan all of the traffic on an infected machine’s local network and collect usernames and password hashes that are transmitted across the network. The attackers appear to use this component to hijack administrative accounts and gain high-level privileges to other machines and parts of the network.

Flame does contain a module named Viper, adding more confusion to the Wiper/Viper issue, but this component is used to transfer stolen data from infected machines to command-and-control servers. News reports out of Iran indicated the Wiper/Viper program that infected the oil ministry was designed to delete large swaths of data from infected systems.

Kaspersky’s researchers examined a system that was destroyed by Wiper/Viper and found no traces of that malware on it, preventing them from comparing it to the Flame files. The disk destroyed by Wiper/Viper was filled primarily with random trash, and almost nothing could be recovered from it, Gostev said. “We did not see any sign of Flame on that disk.”

Because Flame is so big, it gets loaded to a system in pieces. The machine first gets hit with a 6-megabyte component, which contains about half-a-dozen other compressed modules inside. The main component extracts, decompresses and decrypts these modules and writes them to various locations on disk. The number of modules in an infection depends on what the attackers want to do on a particular machine.

Once the modules are unpacked and loaded, the malware connects to one of about 80 command-and-control domains to deliver information about the infected machine to the attackers and await further instruction from them. The malware contains a hardcoded list of about five domains, but also has an updatable list, to which the attackers can add new domains if these others have been taken down or abandoned.

While the malware awaits further instruction, the various modules in it might take screenshots and sniff the network. The screenshot module grabs desktop images every 15 seconds when a high-value communication application is being used, such as instant messaging or Outlook, and once every 60 seconds when other applications are being used.

Although the Flame toolkit does not appear to have been written by the same programmers who wrote Stuxnet and DuQu, it does share a few interesting things with Stuxnet.

Stuxnet is believed to have been written through a partnership between Israel and the United States, and was first launched in June 2009. It is widely believed to have been designed to sabotage centrifuges used in Iran’s uranium enrichment program. DuQu was [an espionage tool](http://www.wired.com/threatlevel/2011/10/son-of-stuxnet-in-the-wild/) discovered on machines in Iran, Sudan, and elsewhere in 2011 that was designed to steal documents and other data from machines. Stuxnet and DuQu appeared to have been built on the same framework, using identical parts and using similar techniques.

But Flame doesn’t resemble either of these in framework, design or functionality.



Researchers aren't certain how Flame infects its initial target before spreading to other machines, but this graph suggests possible infection vectors.*Courtesy of Kaspersky*

Stuxnet and DuQu were made of [compact and efficient code](http://www.wired.com/threatlevel/2012/03/duqu-mystery-language-solved/) that was pared down to its essentials. Flame is 20 megabytes in size, compared to Stuxnet’s 500 kilobytes, and contains a lot of components that are not used by the code by default, but appear to be there to provide the attackers with options to turn on post-installation.

“It was obvious DuQu was from the same source as Stuxnet. But no matter how much we looked for similarities [in Flame], there are zero similarities,” Gostev said. “Everything is completely different, with the exception of two specific things.”

One of these is an interesting export function in both Stuxnet and Flame, which may turn out to link the two pieces of malware upon further analysis, Gostev said. The export function allows the malware to be executed on the system.

Also, like Stuxnet, Flame has the ability to spread by infecting USB sticks using the autorun and .lnk vulnerabilities that Stuxnet used. It also uses the same print spooler vulnerability that Stuxnet used to spread to computers on a local network. This suggests that the authors of Flame may have had access to the same menu of exploits that the creators of Stuxnet used.

Unlike Stuxnet, however, Flame does not replicate automatically by itself. The spreading mechanisms are turned off by default and must be switched on by the attackers before the malware will spread. Once it infects a USB stick inserted into an infected machine, the USB exploit is disabled immediately.

This is likely intended to control the spread of the malware and lessen the likelihood that it will be detected. This may be the attackers’ response to the out-of-control spreading that occurred with Stuxnet and accelerated the discovery of that malware.

It’s possible the exploits were enabled in early versions of the malware to allow the malware to spread automatically, but were then disabled after Stuxnet went public in July 2010 and after the .lnk and print spooler vulnerabilities were patched. Flame was launched prior to Stuxnet’s discovery, and Microsoft patched the .lnk and print spooler vulnerabilities in August and September 2010. Any malware attempting to use the vulnerabilities now would be detected if the infected machines were running updated versions of antivirus programs. Flame, in fact, checks for the presence of updated versions of these programs on a machine and, based on what it finds, determines if the environment is conducive for using the exploits to spread.

The researchers say they don’t know yet how an initial infection of Flame occurs on a machine before it starts spreading. The malware has the ability to infect a fully patched Windows 7 computer, which suggests that there may be a zero-day exploit in the code that the researchers have not yet found.

The earliest sign of Flame that Kaspersky found on customer systems is a filename belonging to Flame that popped up on a customer’s machine in Lebanon on Aug. 23, 2010. An internet search on the file’s name showed that security firm Webroot had reported the same filename appearing [on a computer in Iran on Mar. 1, 2010](https://www.prevx.com/filenames/X835863115482163633-X1/Z-~ZFF042.TMP.html). But online searches for the names of other unique files found in Flame show that it may have been in the wild even earlier than this. At least one component of Flame appears to have popped up on [machines in Europe on Dec. 5, 2007 and in Dubai on Apr. 28, 2008](https://www.prevx.com/filenames/2285400525247160256-X1/WAVESUP3.DRV.html).

Kaspersky estimates that Flame has infected about 1,000 machines. The researchers arrived at this figure by calculating the number of its own customers who have been infected and extrapolating that to estimate the number of infected machines belonging to customers of other antivirus firms.

All of the infections of Kaspersky customers appear to have been targeted and show no indication that a specific industry, such as the energy industry, or specific systems, such as industrial control systems, were singled out. Instead, the researchers believe Flame was designed to be an all-purpose tool that so far has infected a wide variety of victims. Among those hit have been individuals, private companies, educational institutions and government-run organizations.

Symantec, which has also begun analyzing Flame (which it calls “Flamer”), says the majority of its customers who have been hit by the malware reside in the Palestinian West Bank, Hungary, Iran, and Lebanon. They have received additional reports from customer machines in Austria, Russia, Hong Kong, and the United Arab Emirates.

Researchers say the compilation date of modules in Flame appear to have been manipulated by the attackers, perhaps in an attempt to thwart researchers from determining when they were created.

“Whoever created it was careful to mess up the compilation dates in every single module,” Gostev said. “The modules appear to have been compiled in 1994 and 1995, but they’re using code that was only released in 2010.”

The malware has no kill date, though the operators have the ability to send a kill module to it if needed. The kill module, named browse32, searches for every trace of the malware on the system, including stored files full of screenshots and data stolen by the malware, and eliminates them, picking up any breadcrumbs that might be left behind.

“When the kill module is activated, there’s nothing left whatsoever,” Gostev said.

UPDATE 9am PST: Iran’s Computer Emergency Response Team [announced on Monday](http://www.certcc.ir/index.php?name=news&file=article&sid=1894) that it had developed a detector to uncover what it calls the “Flamer” malware on infected machines and delivered it to select organizations at the beginning of May. It has also developed a removal tool for the malware. Kaspersky believes the “Flamer” malware is the same as the Flame malware its researchers analyzed.