SPECIAL REPORT :: JUNE 2012

NetworkWorld
THE CONNECTED ENTERPRISE

INSIDER

Flame malware

EXTINGUISHING FLAME MALWARE

INSIDE

Flame malware's structure among most complex ever seen

BY ELLEN MESSMER, NETWORK WORLD

Kaspersky Lab Monday shared more details about the sophisticated cyber-espionage Flame malware widely believed to be the work of a nation-state, though the security firm isn't venturing yet to say what country that might be.

Kaspersky Lab is working with OpenDNS to investigate Flame malware tied most closely to cyber-espionage against Iran and Lebanon, and today both companies described what has been found in a week of investigation of Flame command and control (C&C) servers around the world. These servers are being "sinkholed" slowly to cut off ties between the C&C server and Windows-based computers infected with Flame malware, which spies on computer use and can upload content back to Flame's C&C operators.

The Flame cyber-espionage botnet has one of the most elaborate and carefully constructed C&C structures ever identified, according to Roel Schouwenberg, senior research at Kaspersky Lab, who joined with Dan Hubbard, CTO at OpenDNS, to discuss the latest discoveries made since a week ago, when Kaspersky's announcement about the malware apparently caused Flame's C&C operators to suddenly drop offline.

However, Flame appears to be updating itself to possibly reconstitute its capabilities, Schouwenberg warns.

"Flame's goal is cyber-espionage," says Schouwenberg, noting it's "hiding in plain sight," and "there may be a cyber-sabotage component to it."

Flame can send up stolen information in 80 kilobyte chunks, and Flame's operators want to steal PDF files, Office documents and AutoCad files, such as mechanical and building designs. He notes, "Whitelisting technologies would have definitely blocked Flame." Whitelisting prevents unauthorized applications from running on computers. Flame is Windows-based and there doesn't seem to be a Linux component for Flame, Schouwenberg says.

"The Flame command control is unlike anything we've ever seen before," Schouwenberg says. Flame has had more than 80 domains registered for servers that have been identified in far-flung places, from India to Belgium to the Netherlands to Switzerland. The Flame C&C servers do not appear to be based on hacked servers, and domain registrations use fake names that appear to be registered carefully by hand to hotels, shops and doctors' offices, for example, with most of the phony domain registrations registered under fake names for Germany and Austria, but there's no known reason why. These domains and locations associated with Flame registrations are not historically connected with "bad actors and bad neighborhoods," Hubbard points out.

> **"Flame's goal is cyber-espionage. The Flame command control is unlike anything we've ever seen before.**
>
> **ROEL SCHOUWENBERG,** SENIOR RESEARCH AT KASPERSKY LAB

The researchers acknowledge there is still a lot they don't know about Flame because they think they still need to find additional Flame modules to get a bigger picture of what's going on. There's also evidence Flame is updating itself to find alternate C&C paths and has a sophisticated backup operation. So far, there are 196 known victims of Flame in Iran, 54 in Palestine, 48 in Israel, 33 in Sudan, 31 in Syria, and others elsewhere, including 10 in the U.S. The numbers haven't changed a lot from a week ago, Kaspersky says. About 45 of the victims in Iran have had Flame sinkholed to protect against it, as well as 21 in Lebanon and eight in the U.S., among a few others.

Another technical aspect about Flame coming into view is that Microsoft yesterday announced a flaw in its certificate-registration process that appears to have been exploited for purposes of Flame. Kaspersky Lab says it's still seeking to find out more about this and declined to comment on it.

Microsoft on Sunday issued security advisory 2718704 and a related post by engineering staffer Jonathan Ness to notify Microsoft customers that "unauthorized digital certificates have been found that chain up to a Microsoft sub-certification authority issued under the Microsoft root authority."

This all appears to have a bearing on the Flame malware, Microsoft says.

Microsoft says it has revoked three of these certificates associated with the Flame malware by putting them into the "Windows Untrusted Certificate Stores," and "we have also discontinued issuing certificates usable for code signing via the Terminal Services activation and licensing process."

Sometimes use of digital certificates has been by those designing malware to better hide from antivirus software.

Microsoft says it found a flaw in its Terminal Services licensing certification authority process that "when an enterprise customer requests a Terminal Services activation license, the certificate issued by Microsoft in response to the request allows code signing without accessing Microsoft's internal PKI infrastructure."

Microsoft says most antivirus software today will recognize, block and eradicate the Flame malware, but Microsoft is taking the steps it did yesterday to revoke the Terminal Services digital issuance because it's concerned some of the techniques used by Flame could also be "leveraged by less sophisticated attackers to launch more widespread attacks."

In a column for Wired on June 1, Mikko Hypponen, chief research officer for F-Secure, says his company failed to identify Flame as malware even though the software ended up in an F-Secure code archive back in 2010 and 2011. F-Secure's system hadn't flagged it as something dangerous. This may be because Flame was artful in making itself look like a business database system. Hypponen says Flame represented a "failure of the anti-virus industry," adding, "We were out of our league, in our own game." ■

Researchers reveal how Flame fakes Windows Update

BY GREGG KEIZER, COMPUTERWORLD

Security researchers today published detailed information about how the Flame cyber-espionage malware spreads through a network by exploiting Microsoft's Windows Update mechanism.

Their examinations answered a question that had puzzled researchers at Moscow-based Kaspersky Lab: How was Flame infecting fully-patched Windows 7 machines?

Key to the phony Windows Update process was that the hackers had located and exploited a flaw in the company's Terminal Services licensing certificate authority (CA) that allowed them to generate code-validating certificates "signed" by Microsoft.

Armed with those fake certificates, the attackers could fool a Windows PC into accepting a file as an update from Microsoft when in reality it was nothing of the kind.

"Hijacking Windows Update is not trivial because updates must be signed by Microsoft," noted Symantec on Monday in one of a series of blog posts its researchers have written about Flame.

One of the certificates was valid between February 2010 and February 2012, and used to sign the malicious file in late December 2010, adding more information to experts building a timeline of Flame's development and attacks.

Other security experts were even more impressed with what Flame managed. Earlier Monday, Mikko Hypponen, F-Secure's chief research officer and the first to announce that Flame was abusing Windows Update, called the feat "the Holy Grail of malware writers" and "the nightmare scenario" for antivirus researchers.

But as both Symantec and Kaspersky pointed out, Flame doesn't actually compromise Windows Update. It doesn't somehow infiltrate Microsoft's service -- and servers -- to force-feed malicious files to unsuspecting users.

Instead, a Flame-infected Windows PC can, in some situations, make other machines on a network believe it's Windows Update.

A PC compromised by Flame can sniff a networks' NetBIOS information, which identifies each computer, then use that to intercept Windows Updates requests by Internet Explorer (IE). Flame claims to be the WPAD (Web Proxy Auto-Discovery Protocol) server -- a system that provides proxy settings to copies of IE on the network -- and sends a malicious WPAD configuration file to the requesting PC.

As Symantec noted, WPAD hijacking is not new and is, in fact, part of many hacker toolkits.

The rogue WPAD configuration file modifies the victimized machine's proxy settings so that all Web traffic is routed through the Flame-infected system. On that PC, Flame's Web server, dubbed "Munch" kicks in, detects when the requested URL matches Windows Update's and in return sends a downloader disguised as a legitimate update from Microsoft.

To complete the ruse, the downloader was one of several compressed files -- crunched into the "cabinet," or ".cab" file format -- bundled into the single Windows Update.

Once the downloader was installed it retrieved a copy of Flame from the already-infected PC and uses it to compromise the computer.

This complex spreading technique only added to researchers' grudging respect for the threat.

"As we continue our investigation ... more and more details appear [that show] this is one of the most interesting and complex malicious programs we have ever seen," said Alexander Gostev, who leads Kaspersky's research and analysis team, in a Monday blog entry.

Microsoft has revoked three certificates generated by the attackers, making further spoofing of Windows Update files impossible on patched PCs unless there are more rogue certificates in the wild. The company has also blocked others from cranking out new code-signing certificates. ■

Flame Malware: All You Need to Know

What exactly is Flame? What does it do?

Flame is an attack toolkit, which is a lot more complex than Duqu. It is a backdoor, a Trojan, and it has worm-like features, allowing it to replicate in a local network and on removable media if it is commanded so by its master.

Once a system is infected, Flame begins a complex set of operations, including sniffing the network traffic, taking screenshots, recording audio conversations, intercepting the keyboard, and so on. All this data is available to the operators through the link to Flame's command-and-control servers. Later, the operators can choose to upload further modules, which expand Flame's functionality. There are about 20 modules in total and the purpose of most of them is still being investigated.

How sophisticated is Flame and how is it different from other malwares?

Flame is a huge package of modules comprising almost 20 MB in size when fully deployed. Because of this, it is an extremely difficult piece of malware to analyze. The reason why Flame is so big is because it includes many different libraries, such as for compression (zlib, libbz2, ppmd) and database manipulation (sqlite3), together with a LUA virtual machine.

LUA is a scripting (programming) language, which can very easily be extended and interfaced with C code. Many parts of Flame have high order logic written in LUA (the use of LUA is uncommon in malwares) -- with effective attack subrou-

tines and libraries compiled from C++.The effective LUA code part is rather small compared to the overall code.

Kaspersky's estimation of development 'cost' in LUA is over 3000 lines of code, which for an average developer should take about a month to create and debug. There are internally used local databases with nested SQL queries, multiple methods of encryption, various compression algorithms, usage of Windows Management Instrumentation scripting, batch scripting and more.

Another surprising element is the Flame package's large size. The practice of concealment through large amounts of code is one of the specific new features in Flame.

What are the ways it infects computers?

Flame can infect computers through USB sticks, Autorun Infector, local networks, printer vulnerabilities etc.

Flame appears to have two modules designed for infecting USB sticks, called "Autorun Infector" and "Euphoria". Kaspersky Labs haven't seen use of any zero-days till now; however, the worm is known to have infected fully-patched Windows 7 systems through the network, which might indicate the presence of a high-risk zero-day.

How does Flame steal information?

Flame appears to be able to record audio via the microphone, if one is present. It stores recorded audio in compressed format, which it does through the use of a public-source library. Recorded data is sent to the C&C through a covert SSL channel, on a regular schedule.

The malware has the ability to regularly take screenshots; and interestingly will take screenshots when certain "sensitive" applications are run, for instance, IM's. Screenshots are stored in compressed format and are regularly sent to the C&C server -- just like the audio recordings.

Another curious feature of Flame is its use of Bluetooth devices. When Bluetooth is available and the corresponding option is turned on in the configuration block, it collects information about discoverable devices near the infected machine. Depending on the configuration, it can also turn the infected machine into a beacon, and make it discoverable via Bluetooth and provide general information about the malware status encoded in the device information.

What type of data and information are the attackers looking for and who gets affected?

Kaspersky, from it's initial analysis, derives that motive of Flame is to look for any kind of intelligence -- e-mails, documents, messages, discussions inside sensitive locations etc.

Flame appears to be much, much more widespread than Duqu, with probably thousands of victims worldwide. The targets are also of a much wider scope, including academia, private companies, specific individuals and so on.

Does Flame have any similarities with Duqu or Stuxnet? Is the same group the created them behind Flame?

Flame has no major similarities with Stuxnet/Duqu. Flame appears to be a project that ran in parallel with Stuxnet/Duqu, and it doesn't use the Tilded platform unlike Duqu. However the presence of some links can indicate that the creators of Flame had access to technology used in the Stuxnet project -- such as use of the "autorun.inf" infection method, together with exploitation of the same print spooler vulnerability used by Stuxnet.

It's possible that the authors of Flame used public information about the distribution methods of Stuxnet and put it to work in Flame.

According to Kaspersky's research, the operators of Flame artificially support the quantity of infected systems on a certain constant level. This can be compared with a sequential processing of fields -- they infect several dozen, then conduct analysis of the data of the victim, uninstall Flame from the systems that aren't interesting, leaving the most important ones in place. After which they start a new series of infections.

Can Flame self-replicate like Stuxnet?

The replication part appears to be operator commanded, like Duqu, and also controlled with the bot configuration file. Most infection routines have counters of executed attacks and are limited to a specific number of allowed attacks.

Debarati Roy, CIO India with help from Aleks Gostev, Chief Security Expert, Global Research and Expert Analysts Team (GrEAT), Kaspersky Lab.

The Flame virus: FAQs

BY JARED NEWMAN, PC WORLD

A frightening computer virus called Flame is on the loose in Iran and other parts of the Middle East, infecting PCs and stealing sensitive data. Now, the United Nations' International Telecommunications Union warns that other nations face the risk of attack.

But what is Flame, exactly, and is it cause for concern among ordinary PC users? Here's what you need to know about what Kaspersky calls "one of the most complex threats ever discovered."

Flame virus: The basics

Kaspersky describes Flame as a backdoor and a Trojan with worm-like features. The initial point of entry for the virus is unknown -- spearphishing or infected websites are possibilities -- but after the initial infection, the virus can spread through USB sticks or local networks.

Flame is meant to gather information from infected PCs. As Kaspersky's Vitaly Kamlyuk told RT, the virus can sniff out information from input boxes, including passwords hidden by asterisks, record audio from a connected microphone and take screenshots of applications that the virus deems important, such as IM programs. It can also collect information about nearby discoverable Bluetooth devices. The virus then uploads all this information to command and control servers, of which there are about a dozen scattered around the world.

The virus is reminiscent of the Stuxnet worm that wreaked havoc on Iran in 2010, but Kaspersky says Flame is much complex, with its modules occupying more than 20 MB of code. "Consider this: it took us several months to analyze the 500K code of Stuxnet. It will probably take year to fully understand the 20MB of code of Flame," the firm said.

What Are Flame's Origins?

Flame has been in the wild since 2010, according to Kaspersky, but its creation date is unclear. The virus was discovered a month ago after Iran's oil ministry learned that several companies' servers had been attacked. That finding led to more evidence of attacks on other government ministries and industries in Iran.

Iran has claimed that the attacks also wiped the hard drives of some machines, but Kaspersky claims that the malware responsible, called Wiper, isn't necessarily related. Wiper attacks were isolated to Iran, while Flame has been found in other countries.

Flame's creator is also unknown, but a nation-state was likely behind it. The virus is not designed to steal money from bank accounts, and is much more complex than anything commonly used by "hacktivists," so a nation-created virus is the only other possibility that makes sense.

Who is at Risk?

The United Nations' International Telecommunications Union is now warning other nations to "be on alert" for the virus, which could potentially be used to attack critical infrastructure. In a statement to Reuters, the U.S. Department of Homeland Security said it was "notified of the malware and has been working with our federal partners to determine and analyze its potential impact on the U.S."

Security firms have not been warning of any direct risk to average Internet users. Sophos' Graham Cluley noted that Flame has only been discovered in a few hundred computers. "Certainly, it's pretty insignificant when you compare it to the 600,000 Mac computers which were infected by the Flashback malware earlier this year," Cluley wrote in a blog post. ■

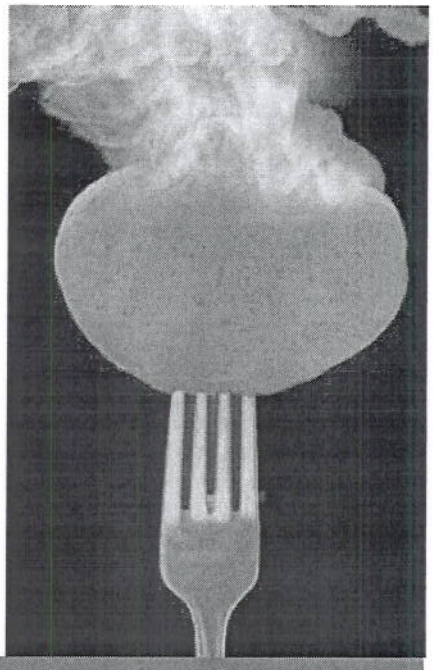
Iran's discovery of Flame turning into political hot potato

BY ELLEN MESSMER, NETWORK WORLD

With Iran's computer-emergency response center now decrying Windows-based cyber-espionage software known as Flame (or alternately Flamer or Skywiper) it says it discovered infecting its oil-ministry computers, the uproar is reaching into the United Nations, which is investigating the malware.

The U.N.'s International Telecommunication Union (ITU) will issue a warning to countries about the Flame computer virus that was discovered in Iran, with Marco Obiso, cyber security coordinator for the ITU saying Flame was a dangerous tool that could be used to potentially attack critical infrastructure.

Obiso is quoted by Reuters as saying Flame was likely created by a "nation-state," and Obiso voiced the opinion that Flame is "much worse than Stuxnet," the malware discovered two years ago that appeared to target programmable logic controllers in



Iranian nuclear facilities. No one claimed official responsibility for that, but suspicions centered on Iran's adversaries the U.S. and Israel.

In comparison to Stuxnet, however, Flame malware appears to be for broader cyber-espionage purposes on infected Windows machines. Kaspersky Lab, which was commissioned by the ITU to analyze Flame, is also now saying Flame is likely a cyber-espionage weapon developed by a nation-state.

Even as technical research proceeds to better understand the highly complex and encryption-hidden Flame, some are noting that the political ramifications of what's unfolding are significant.

Flame is being spotted in other Middle East countries and Europe; researchers in Budapest say it's been uncovered in Hungary.

"This is not a flash in the pan," says Chris Bronk, professor and fellow in information technology at Rice University. With Iran going directly to the U.N. division of the ITU to report its discovery of Flame, and the ITU calling on Kaspersky to conduct a technical analysis, the issue of cyber-espionage and critical infrastructure protection has now landed squarely on the political stage. Diplomatic circles to date have not found this topic an easy one to understand or deal with, Bronk points out.

The ITU, based in Geneva, has had a long history in traditional telecommunications related to global standards, but its role is not now as important as it was decades ago. These days, the ITU is interested in expanding its global political role at the U.N. by taking on cyber-security issues, Bronk says.

Most of the major anti-malware companies global in operation, but even the fact that the ITU selected Kaspersky, a Russian-based company, to do the analysis rather than an American-based one such as Symantec or McAfee will be a fact remembered by many as the significance of Flame becomes better understood, Bronk adds.

"The report emphasizes that Skywiper/Flame "may have been active for as long as five to eight years, or even more."

In response, Kaspersky said it was natural for the ITU to commission it to analyze Flame because Kaspersky has worked on several cyber-security projects with the ITU. Roel Schouwenberg, senior researcher at Kaspersky, said it will take some time to fully understand Flame, but the research is being done independently of Iran or any other country. So far, Kaspersky has found 189 instances of infections have been identified in Iran, 98 in Israel and Palestine, 30 in Syria, plus a few more elsewhere in the Middle East.

But analysis of samples of Flame is now being done by several security firms, and some of the earlier published analysis has also come from the Budapest University of Technology and Economics in its Laboratory of Cryptography and System Security (CrySyS). This laboratory today issued a lengthy report on the malware (which it calls sKyWIper), noting its findings are still a work in progress.

The report states that Flame/Flamer/Skywiper has infected undisclosed systems in Hungary as well. The technical analysis of the malware suggests it's "another info-stealer with a modular structure incorporating multiple propagation and attack techniques, but further analysis may discover components with other functionalities."

The report emphasizes that Skywiper/Flame "may have been active for as long as five to eight years, or even more."

According to the Hungarian report, the malware "uses compression and encryption techniques to encode its files. More specifically, it uses five different encryption methods (and some variants), three compression techniques, and at least five file formats (and some proprietary formats, too). It uses special code-injection techniques. Quite interestingly, Skywiper stores information that it gathers on infected systems in a highly structured format in SQLite databases. Another uncommon feature of Skywiper is the usage of the Lua scripting language. Skywiper has very advanced functionality to steal information and to propagate. Multiple exploits and propagation methods can be freely configured by the attackers. Information gathering from a large network of infected computers was never crafted as carefully as in Skywiper. The malware is most likely capable to use all of the computers' functionalities for its goals. It covers all major possibilities to gather intelligence, including keyboard, screen, microphone, storage devices, network, wifi, Bluetooth, USB and system processes."

The report, which calls it arguably the "most complex malware ever found," concludes that Flame/Skywiper was "developed by a government agency of a nation state with significant budget and effort, and may be related to cyber warfare activities." ■

'Flame' cyber-weapon went undiscovered for four years

VirusTotal logged components years ago

BY JOHN E DUNN, TECHWORLD

The Flame 'super-malware' must have been infecting computers for as long as four years and was less invisible to antivirus software than assumed, an analysis by security company AlienVault has concluded.

On the face of its AlienVault's analysis is just another forensic guess after peering at the important mssecmgr.ocx Win32 PE (portable executable) file, which 'exports' a clutch of progamming functions. As pulled apart by the Hungarian CrySys Lab, this contains debug entries suggesting a 2011 creation date.

However, an older version of the same file references a smaller number of functions and comes with a compilation date in 2008, which suggests a longer development timeline for the software.

Compellingly, running the MD5 file hashes (think of them as file fingerprints) through the VirusTotal website, which runs suspect files against 40 antivirus products and records the signature of each file as it is doing so, elements of Flame turn out to have popped up on the system in the past.

Some of these components turn out to have been seen across the same 2008-2011 data range with CrySis reporting a single file, Wavesup3.drv, was detected as long ago as December 2007. This later turned up in the UAE in April 2008 and Iran in March 2010.

That VirusTotal brushed past these files would not mean that an antivirus system would have detected Flame for what it was; many files might be noticed but only marked as suspect in an isolated, 'generic' way.

What is does suggest is that Flame has been around for years in a number of forms, modified over time, and there are probably more parts to its design yet to be discovered.

What these dates don't reveal is when the malware (or parts of it) were actually deployed and where, let alone by whom with what aim.

"An extraordinary claim requires extraordinary evidence," as cosmologist Carl Sagan once famously said, but with Flame (or Flamer or SKyWIper - the industry can't agree on the name) it has been evidence in the form of a large collection of smaller fragments.

Ever since it was publicised earlier this week, Flame has divided experts, most of whom work for security vendors which have a lot to gain from security crises and, in a strange way, something to lose - none of them appear to have detected it.

The shock of Flame is less its targets (if they include Iran and its allies that is predictable) or even its complexity (although that is notable) but the fact that nobody noticed it until May 2012.

As interesting as Flame is, it's positively baroque when set next to the other famous examples of what are now seen as state-sponsored malware. Stuxnet was austere, Duqu incredibly enigmatic. With its module for everything, Flame is over the top and possibly careless. Experts have hit a dead end on the first two but Flame looks as if it will give them work for months or even years to come. ■

Price tag for Microsoft piece of Flame malware $1 million

BY TIM GREENE, NETWORK WORLD

Back when the Microsoft Update piece of the Flame espionage-software package was still undetected it could have sold for $1 million on the malware black market, a security researcher says.

"That discovery is worth a lot of money," says Marcus Carey, security researcher at vulnerability-management firm Rapid7, "at least six figures and probably more -- seven figures. That's how elite that attack is."

Since Flame and its components were unmasked, though, that has all changed. "Nobody's going to pay that now," he says.

The vulnerability that first came to light Sunday when Microsoft issued a rare out-of-cycle security update was an obscure part of a complex and stealthy platform that had evaded detection for more than four years.

In particular, Flame exploited Microsoft Terminal Services by having its certificate authority generate fake digital signatures that authenticated malware as legitimate Microsoft updates. This allowed the attackers to alter and update its code at will.

But that was just one feature of the entire Flame architecture. Other sophisticated elements include the ability to delete all or parts of itself from infected machines and then overwrite those parts to eliminate any trace.

It also had a command-and-control infrastructure "unlike anything we've ever seen before," according to Kaspersky Lab researchers. It operated out of 80 domains, and the servers involved were apparently unhacked machines deployed in legitimate businesses. The servers attempted updates to set alternative C&C paths, Kaspersky says.

Creators of Flame were among the elite of malware creators, Carey says. "They had to have a higher aptitude -- a world-class understanding of how to exploit software and of cryptography."

The Microsoft piece of Flame involved a technique called MD5 collisions that have been known since 2008 but that had never been applied to Microsoft software before, he says. ■

Stuxnet and Flame share code, development teams

Kaspersky Lab says early version of Stuxnet has a Flame module

BY ELLEN MESSMER, NETWORK WORLD

The recently discovered Flame cyber-espionage malware has a direct connection to the Stuxnet malware used to attack programmable logic controllers at Iranian nuclear facilities two years ago, according to Kaspersky Lab, which says Flame and Stuxnet share some technical code that reveals a common development effort of some sort.

The early version of Stuxnet has a Flame module, said Roel Schouwenberg, senior researcher at Kaspersky Lab, who joined with colleague Vitaly Kamluk to share Kaspersky's latest findings today about what the security firm says reveals a direct relationship between those who developed the cyber-weapon Stuxnet and those who developed the Windows-based cyber-espionage tool Flame. He called them "two parallel operations" that were coordinated in some form.

The New York Times reported that President Barack Obama ordered use of the Stuxnet cyber-weapon to attack Iran, charges the White House hasn't refuted. This has triggered a special investigation to find out where in the administration a leak about Stuxnet occurred.

Now, Kaspersky's assertions that Stuxnet and the more-recently discovered Flame -- which Iran's computer-response team in May claimed was found on computers infecting its oil-ministry computers -- are connected, the stakes may be raised even further in the political world.

In a briefing today, Kaspersky researchers emphatically said they stand by the assertion that the early version of Stuxnet, Stuxnet.A, has a "Flame module" (which they're referring to as "Resource 207"), which was used as a transport mechanism, specifically for USB spreading and an autorun function in Windows and a privilege-escalation vulnerability (which has since been patched by Microsoft). Kaspersky was commissioned by the United Nations' division the International Telecommunication Union to analyze Flame. The ITU has issued an alert to the world's countries about Flame, calling it dangerous.

Kaspersky Lab now thinks the Flame malware predated the Stuxnet platform, and that source code from Flame was shared with the developers of Stuxnet, and that both may be coordinated through the same entity.

Schouwenberg said it's important for the future of the cybersecurity community that the world understand the nature of these cyber-weapons.

Stuxnet two years ago was targeting Iranian infrastructure to slow down the programmable logic controllers at facilities where the U.S. believes Iran is trying to develop a nuclear weapon. But as The New York Times noted in its article, Stuxnet began to run wild in cyberspace, apparently not under control of its creators, which The New York Times says is the U.S. and Israel working in a cyber-weapon co-development project.

If Stuxnet hadn't been able to do certain "safety checks, it could have caused a power outage in the U.S.," Schouwenberg asserted.

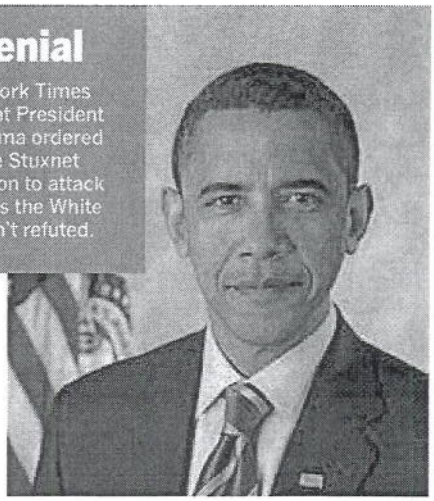
Kaspersky Lab's assertion is that Stuxnet and Flame share some common source code and that this indicates cooperation between development teams may be greeted with some skepticism.

Kaspersky's assertions to say there's a definite connection between Stuxnet and Flame, simply because some common source code was found "is a bit of a stretch," said Chris Bronk, professor and fellow in information technology at Rice University, who's attending a cybersecurity conference in Orlando this week. He said other anti-malware vendors will eventually weigh in with their analysis on this, and more needs to be heard.

But he acknowledged if it turns out to be true, as The New York Times asserts and the White House has so far not denied, that the U.S. has put malware code for use in covert action out in the wild, then you end up educating the public in general on how to do this, he pointed out.

No denial

The New York Times reported that President Barack Obama ordered use of the Stuxnet cyber-weapon to attack Iran, charges the White House hasn't refuted.



Covert action against U.S. adversaries such as Iran using modern-day cyber-weapons can be debated as appropriate or not. In cyber-espionage, "the outcomes may be preferable to wars," Bronk said, the kind of wars where kinetic weapons such as bombs are used to blow things up physically.

But as information about what the U.S. may have done in this area of cyber-weapons becomes more known, the result is that it puts the U.S. in an awkward position in "trying to stand as a pillar for secure cyberspace," another stance the U.S. government tries to take, Bronk pointed out.

In an editorial in The New York Times, Mikko Hypponen, researcher at F-Secure, expressed disappointment about the turn of affairs that seems to show the U.S., with Israel, engaging in covert cyberattacks against infrastructure of another country. He wrote that American officials have opened a Pandora's box, and they will likely regret the decision.

"The downside for owning up to cyberattacks is that other governments can now feel free to do the same," Hypponen wrote. ■

Experts dispute sandboxing would have stopped Flame

BY ANTONE GONSALVES, CSO

At least one vendor is making the argument that sandboxing technology would have protected computer systems against Flame, but some experts are not convinced it would have caught theA'A highly sophisticated malware package believed to be built for cyber-espionage.

Julian Waits, vice president of the Advanced Technology Group at GFI Software, argued this week in the company's blog that sandboxing would have been the backstop for antivirus software, which was unable to detect the stealthy Flame. GFI sells sandboxing technology, so the post was self-serving. Nevertheless, Waits' arguments, which other experts dispute, are worth considering in the context of a layered approach to security.

Sandbox technology runs on a virtual machine along with operating systems and business applications, watching files for unusual activity. When a suspicious file is spotted, the technology alerts security pros while logging unusual behavior, such as application changes and unusual network traffic. It is then up IT staff to decide what to do.

While sandboxing doesn't actually quarantine the file, the technology does spot threats before they can do significant damage, Waits argues. Some sandboxing technology can also generate signatures for the malware, which can be inserted in intrusion detection systems and even some anti-virus systems to prevent future infections.

Flame had evaded detection for four years, before Microsoft discovered it. Such malware can't be discovered by AV software because no signatures exist for it. "Most perimeter-based security technology can't catch it," Waits told CSO on Friday. "Those are all based on the what we know."

Despite the logic in Waits' arguments, other experts disagreed that sandboxing would have caught Flame, which Kaspersky Lab said had a command-and-control infrastructure built by people with a "world-class understanding of how to exploit software and cryptography."

"It seems to be one of the most sophisticated Windows-affecting malware, and I'm afraid sandboxing may not be effective in containingA'A it due to the way it infects systems," Xuxian Jiang, an assistant professor in the Computer Science Department at North Carolina State University, said in an e-mail interview.

Scott Crawford, managing research director for Enterprise Management Associates, said sandboxing in general has its limitations. If applications in the sandbox-protected virtual environment have access to outside directories, file systems or other resources, then the malware can spread without detection.

"If that leads to enabling attack capabilities, then sandboxing would not be as effective, and may, in fact, be irrelevant," Crawford said by email.

One lesson learned from Flame is the need for multiple layers of security, so when one technology fails, a second or third may succeed. "How malware is designed requires a far more comprehensive approach than expanding a signature library, and compels vendors to provide much more in the way of ongoing research and analysis," 451 Research analystA'A Steve Coplan said.

Flame is just the latest example of how the threat landscape has changed considerably over the last few years. Hackers have gone from distributing large numbers of malware-carrying spam to targeting specific organizations with advanced techniques meant to steal high-value information. Targets typically operate in the defense industry, financial services, manufacturing, international law and government.

Experts believe Flame was built for targeted attacks against networks in the Middle East. ■

Microsoft's reaction to Flame shows seriousness of 'Holy Grail' hack

BY GREGG KEIZER, COMPUTERWORLD

The exploit of Microsoft's Windows Update system by the sophisticated Flame cyber espionage malware was a "significant" event in the history of Windows hacking, experts said today.

And by its response, Microsoft appears to agree: It not only issued an immediate fix just days after the malware's public unveiling with one of its increasingly-rare "out-of-band" updates, but it has turned its certificate-generation process upside down and will revamp how it secures Windows updates.

"It was a very significant," said Wolfgang Kandek, chief technology officer with Qualys, in an interview today. "It's the Holy Grail of exploits, and until now it had only been done in research."

Kandek wasn't the first to link the term "Holy Grail" with Flame: Earlier in the week, Mikko Hypponen, F-Secure's chief research officer and the first to announce that Flame was somehow using Windows Update, called the feat "the Holy Grail of malware writers" and "the nightmare scenario" for antivirus researchers.And yesterday, Alexander Gostev, who leads Kaspersky's research and analysis team, said the Windows Update deception was "better than any zero-day exploit ... it actually looks more like a 'god mode' cheat code."

What had those researchers reaching for

superlatives was the Flame makers' theft of digital "signatures," or certificates, that labeled code as Microsoft's, and then the use of those certificates to "sign" malicious files that posed as legitimate Windows updates.

The combination allowed Flame to infect fully-patched Windows XP, Vista and Windows 7 PCs that were on the same network as an already-infected system.

With a complex series of operations that involves three of its many modules, "Snack," "Munch" and "Gadget," Flame sniffs out victims, intercepts connection requests to Windows Update and serves up malware, including a copy of Flame, that masquerades as a valid update.

Third-party security researchers had mapped out those maneuvers and modules, but until Microsoft's revelation that its certificates had been fraudulently generated, didn't see the point.

"Once they confirmed [the certificate theft], it filled in the missing puzzle pieces," Liam O Murchu, director of operations for Symantec's security response center, said in an email reply to questions. "Without a Microsoft certificate these components did not make sense."

But it may be Microsoft's own moves since Monday, May 28, when Kaspersky Lab first released an analysis of Flame, that is the best evidence of the hack's gravity.

"You can get a pretty good idea by what Microsoft's done that they think this is very urgent," said Kandek. "They released the patch on Sunday, even though Patch Tuesday was just a little over a week away."

June's Patch Tuesday -- the name for Microsoft's religiously-scheduled security updates -- is next week.

Microsoft revoked three certificates -- those used to sign code in Flame -- on Sunday, June 3, only six days after Kaspersky disclosed the malware, an extremely rapid response for the company. The same day, Microsoft modified the Terminal Services licensing certificate authority (CA), the one hackers had exploited, so it could no longer issue code-signing certificates of any kind.

It's rare that Microsoft issues an emergency update rather than wait for the next Patch Tuesday. Last year, Microsoft shipped only one, and that was just two days before 2011's close. In 2010, Microsoft delivered four out-of-band updates and 104 on Patch Tuesdays.

On Wednesday Microsoft announced it would revamp how Windows updates are secured, saying that it would dedicate a new CA to Windows Update, in effect unlinking the service from all other Microsoft-generated certificates. The update to end users and enterprises -- the latter for WSUS, or Windows Server Update Services -- is to start reaching customers this week.

Andrew Storms, director of security operations at nCircle Security, said that should have been how Microsoft treated Windows Update from the get-go.

"Windows Update should have been an entirely different [certificate] stream than anything else," said Storms. "It's just too darned important to have been intermingled with any other chain of trust. For all that Microsoft has done to better their security practices, I'm pretty surprised they didn't think of this attack vector previously."

Storms was also critical of Microsoft's vague description of their plans to harden Windows Update.

"The Windows Update team needs to describe in more detail how they are going to fix the problem. Until then, I bet a lot of people will be thinking twice about the security of Windows Update," said Storms.

Users should deploy last Sunday's certificate revocation update as soon as possible, Microsoft has said, to protect themselves from possible copy-cat hackers. ■

Microsoft's moves against Flame may throw wrench in Patch Tuesday

Microsoft today said it would deliver seven security updates next week, three critical, to patch 28 bugs in Windows, Internet Explorer, Office and other programs in its portfolio.

But Microsoft's promise to start pushing an update to Windows Update this week -- part of its response to the Flame espionage malware -- could disrupt this month's patching, one expert warned.

The number of updates was right on the average so far this year of seven per month, yet another indication that although Microsoft once used an even-odd schedule, patching more vulnerabilities in the even months, it has discarded the model.

"It's totally flat-lined," said Andrew Storms, director of security operations at nCircle Security. "The up-and-down is totally gone."

This month's Patch Tuesday will fix the largest number of vulnerabilities -- 28 all told -- this year. In May, Microsoft fixed 23 security flaws.

Of the seven updates, Microsoft tagged three as "critical," the highest threat ranking in its four-step scoring, and the other four as "important," the next-most serious rating.

One update will address all supported versions of IE, ranging from the 11-year-old IE6 to last year's IE9; four will affect Windows; and the remaining pair will tackle vulnerabilities in all versions of Office on Windows and Dynamics AX 2012, an enterprise resource planning (ERP) product.

Storms singled out the IE update, identified in the advance notification as one of the three critical bulletins, as most likely to climb to the top of users' to-do lists.

"That's going to be the obvious one to deploy first," Storms said, using the long-established logic of security professionals to patch the browser with haste because of its widespread use and its broad attack surface.

Marcus Carey, a security researcher at Rapid7, agreed. "Browser exploits provide the most bang for the buck," Carey said in an email Thursday.

Storms suspected that the IE update will include a patch for one or more of the bugs used by a French security company to hack the browser at the 2012 version of Pwn2Own, an annual contest that pits researchers against software for cash prizes.

— Gregg Keizer, Computerworld