Flame virus used world-class cryptographic attack

17:18 8 June 2012
Cybersecurity
Hacking
Jacob Aron, technology reporter

(Image: Altrendo/Getty Images)

The recently discovered computer worm Flame could have been created only by "world-class" cryptographers, say experts in the field who have discovered that the malware uses a previously unseen cryptographic attack.

Flame installs itself on a target computer by hijacking the Windows Update system. Normal updates are signed with a digital certificate that verifies their origin, but Flame's creators were

able to fake their own certificate.

Such certificates are signed by a hash algorithm that converts any digital data into a short sequence of characters. It isn't possible to recover the original data from this sequence, but it can be used to verify it, allowing the hash sequence to act as a virtual "signature". Crucially, it should be very difficult to discover two pieces of data that convert to the same hash sequence - otherwise someone can perform a "collision attack", generating a spoof hash sequence without knowing the original data.

That's exactly what Flame's authors have done, though it isn't the first time the feat has been achieved. In 2008 cryptographer Mark Stevens and colleagues showed that the oft-used MD5 hash algorithm is vulnerable to collision attacks - a feat that required 200 PlayStation 3 consoles to crunch through the numbers to find a match.

Now Stevens and others have analysed Flame's code and discovered it uses a previously unseen variant of the attack, probably developed before his research was published, allowing the attackers to calculate the exact hash sequence used by Microsoft's update system.

"The results have shown that not our published chosen-prefix collision attack was used, but an entirely new and unknown variant," says Stevens. "This has led to our conclusion that the design of Flame is partly based on world-class cryptanalysis."

Whoever designed Flame, they are now trying to cover their tracks. Antivirus firm Symantec says that computers infected with Flame have received a "suicide" update module designed to completely remove the worm. It appears that this module was created on 9 May, just a few weeks before the malware became publicly known.

8 June 2012 Last updated at 11:21 GMT

Flame malware makers send 'suicide' code

The malware is said to have infected more than 600 specific targets

Continue reading the main story

Related Stories

- UN warning on 'risk of cyberwar'
- Flame attack 'sought Iran data'
- Israel rejects Flame malware link

The creators of the Flame malware have sent a "suicide" command that removes it from some infected computers.

Security firm Symantec caught the command using booby-trapped computers set up to watch Flame's actions.

Flame came to light after the UN's telecoms body asked for help with identifying a virus found stealing data from many PCs in the Middle East.

New analysis of Flame reveals how sophisticated the program is and gives hints about who created it.

Clean machine

Like many other security firms Symantec has kept an eye on Flame using so-called "honeypot" computers that report what happens when they are infected with a malicious program.

Described as a very sophisticated cyber-attack, Flame targeted countries such as Iran and Israel and sought to steal large amounts of sensitive data.

Earlier this week Symantec noticed that some Flame command and control (C&C) computers sent an urgent command to the infected PCs they were overseeing.

Flame's creators do not have access to all their C&C computers as security firms have won control of some of them.

The "suicide" command was "designed to completely remove Flame from the compromised computer," said Symantec.

The command located every Flame file sitting on a PC, removed it and then overwrote memory locations with gibberish to thwart forensic examination.

"It tries to leave no traces of the infection behind," wrote the firm on its blog.

Analysis of the clean-up routine suggested it was written in early May, said Symantec.

Crypto crash

At the same time, analysis of the inner workings of Flame reveal just how sophisticated it is.

According to cryptographic experts, Flame is the first malicious program to use an obscure cryptographic technique known as "pre-fix collision attack". This allowed the virus to fake digital credentials that had helped it to spread.

The exact method of carrying out such an attack was only demonstrated in 2008 and the creators of Flame came up with their own variant.

"The design of this new variant required world-class cryptanalysis," said cryptoexpert Marc

Stevens from the Centrum Wiskunde & Informatica (CWI) in Amsterdam in a statement.

The finding gives support to claims that Flame must have been built by a nation state rather than cybercriminals. It is not clear yet which nation created the program.

Why we may never know who created Flame virus

- 06 June 2012 by **Paul Marks**
- Magazine issue 2868. **Subscribe and save**
- For similar stories, visit the **Computer crime** and **Crime and Forensics** Topic Guides

HERE we go again. Antivirus firms are warning that another computer worm has evaded their radar. Nicknamed Flame, it is described as one of the most complex viruses ever and has the power to cripple national infrastructure. But a full two years after the last major threat - Stuxnet - was discovered, its authors have still not been exposed, although new evidence suggests they work for US and Israeli intelligence (see "Obama 'gave full backing to Stuxnet attack on Iran'"). So what chance is there of tracking down the creators of this latest threat?

Parts of Flame surfaced online as far back as 2004, according to Boldizsár Bencsáth of the Crysys Lab at the Budapest University of Technology and Economics in Hungary. Despite this, it was not formally identified until Kaspersky Lab of Moscow, Russia, discovered what was deleting data on hundreds of computers across the Middle East. Iran and Israel took the biggest hits, with Flame even briefly disrupting Iran's oil industry, according to senior Iranian officials.

On 28 May, Kaspersky revealed the cause: an all-in-one "worm, trojan and backdoor" it dubbed Flame. It is a remotely reprogrammable data stealer that can seize, transmit and then delete files. Its six-megabyte heart can download extra modules until it swells to 20 MB, giving it a broad range of data-stealing tricks, says Gavin O'Gorman at Symantec's lab in Dublin, Ireland. "It's most likely this info-stealing is for espionage. It can turn a mic on to record audio, or video what you are doing on screen," he says.

It's stealthy, too. Iran's national Computer Emergency Response Team says the code's malicious components were undetectable by 43 antivirus programs. "Stuxnet, Duqu and Flame are all examples of cases where we - the antivirus industry - have failed," says Mikko Hypponen, founder of antivirus firm F-Secure. But while the industry tries to work out why it failed, it looks almost impossible for the malware's creators to be found.

Here's why. "If I write the code 'print "Hello"' and then load it to a forum via a proxy or Tor connection, what link is there to me? Simply, none. The same principle exists with malware," says Nick Furneaux of e-forensics firm CSITech in Bristol, UK. Attackers can also cover their tracks by bouncing commands to the malware via cascades of servers, says Bencsáth. "If an attacker hides by using multiple jumping points, it is almost impossible to identify them," he says. "And the forensics mostly lead you to a computer that is fully cleared, erased."

To catch them, investigators have to pray their quarry makes a mistake. "I've seen mistakes made in malware such as hard coding IP and email addresses, or a user name, which can be used to find the perpetrator," says Furneaux. Another giveaway is coding style, says O'Gorman: "You might find file-naming conventions or how data is passed between functions

is characteristic of a known coder." Indeed, it was a coding mistake that revealed Stuxnet existed.

Robert Ghanea-Hercock, a security researcher at BT's lab in Ipswich, UK, hopes their emerging AI-based pattern recognition system, Saturn, will snare threats like Flame. It "will sense the subtle network disruptions and cyber footprints left by such attacks", instantly alerting security analysts, he says. This might help, says Bencsáth: "If the attackers are caught mid-attack, and they do not know about it, it becomes possible to track them down."

31 May 2012 Last updated at 09:32 GMT

Flame: Israel rejects link to malware cyber-attack

By Dave Lee Technology reporter, BBC News

Moshe Ya'alon spoke to the country's military radio station about the attack

Related Stories

- Iran 'finds Flame malware fix'
- Massive cyber-attack discovered
- Key Iranian oil terminal 'hacked'

Israel has dismissed suggestions that it might be behind the Flame cyber-attack.

Several media reports linked comments made by the country's vice prime minister with the malware, which has infected more than 600 targets.

However, a spokesman for the Israeli government told the BBC that Moshe Ya'alon had been misrepresented.

Security experts said it was still too early to pinpoint the source of the attack.

Mr Ya'alon, who is also Israel's minister of strategic affairs, discussed the attacks on Israel's military radio station, Army Radio.

"There are quite a few governments in the west that have rich high-tech [capabilities] that view Iran, and particularly the Iranian nuclear threat, as a meaningful threat - and can possibly be involved with this field," he said.

"I would imagine that everyone who sees the Iranian nuclear threat as a significant one, and that is not only Israel, it is the entire Western world, headed by the United States of America, would likely take every single measure available, including these, to harm the Iranian nuclear project."

When asked to clarify Mr Ya'alon's comments by the BBC, a spokesman for the minister said: "There was no part of the interview where the minister has said anything to imply that Israel was responsible for the virus."

Retreating Flame

Other speculation has linked the US with the malware. An anonymous US official told NBC News the country was behind the attack - but conceded he had "no first-hand knowledge" of the matter. The US has also denied responsibility.

Many analysts said Stuxnet, a past high-profile attack which shares some similarities with Flame, could have been orchestrated by both countries.

Leading security expert Ralph Langner said in 2011 that Mossad - Israel's security agency - had collaborated in the attack with US intelligence. Both countries deny involvement.

Russian security firm Kaspersky Labs, which was among the first to reveal details of Flame, told the BBC that it could take months, or even years, to determine where it had originated.

The malware is said to have infected over 600 specific targets

However, its researchers have noted that whoever was behind the malware appeared to be retreating slowly.

"It's very tough to shut down 80+ command and control servers down at the same time," explained Roel Schouwenberg, senior security researcher.

"Some of them are not active anymore. I think this is some sort of effort to buy themselves some time and change the game plan if the need would arise.

"We've seen it in the past, that after some period of silence, that the operation is rebooted."

The United Nations has described Flame as a significant espionage tool which could affect critical infrastructure - and issued its "most serious" cyber security warning to date.

However, others have suggested the threat had been overplayed.

"We seem to be getting to a point where every time new malware is discovered it's branded 'the worst ever'," said US security researcher Marcus Carey.

28 May 2012 Last updated at 13:17 GMT

Flame: Massive cyber-attack discovered, researchers say

By Dave Lee Technology reporter, BBC News

The malware is said to have infected over 600 specific targets

Continue reading the main story

Related Stories

- What a future cyberwar will look like
- Key Iranian oil terminal 'hacked'
- Oil hack attacks may 'cost lives'

A complex targeted cyber-attack that collected private data from countries such as Israel and Iran has been uncovered, researchers have said.

Russian security firm Kaspersky Labs told the BBC they believed the malware, known as Flame, had been operating since August 2010.

The company said it believed the attack was state-sponsored, but could not be sure of its exact origins.

They described Flame as "one of the most complex threats ever discovered".

Research into the attack was carried out in conjunction with the UN's International Telecommunication Union.

They had been investigating another malware threat, known as Wiper, which was reportedly deleting data on machines in western Asia.

In the past, targeted malware - such as Stuxnet - has targeted nuclear infrastructure in Iran.

Others like Duqu have sought to infiltrate networks in order to steal data.

This new threat appears not to cause physical damage, but to collect huge amounts of sensitive information, said Kaspersky's chief malware expert Vitaly Kamluk.

"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," he said.

More than 600 specific targets were hit, Mr Kamluk said, ranging from individuals, businesses, academic institutions and government systems.

Iran's National Computer Emergency Response Team posted a security alert stating that it believed Flame was responsible for "recent incidents of mass data loss" in the country.

The malware code itself is 20MB in size - making it some 20 times larger than the Stuxnet virus. The researchers said it could take several years to analyse.

Iran and Israel
Mr Kamluk said the size and sophistication of Flame suggested it was not the work of independent cybercriminals, and more likely to be government-backed.

Continue reading the main story

Analysis


Professor Alan Woodward Department of Computing, University of Surrey
This is an extremely advanced attack. It is more like a toolkit for compiling different code based weapons than a single tool. It can steal everything from the keys you are pressing to what is on your screen to what is being said near the machine.

It also has some very unusual data stealing features including reaching out to any Bluetooth enabled device nearby to see what it can steal.

Just like Stuxnet, this malware can spread by USB stick, i.e. it doesn't need to be connected to a network, although it has that capability as well.

This wasn't written by some spotty teenager in his/her bedroom. It is large, complicated and dedicated to stealing data whilst remaining hidden for a long time.

- Prof Alan Woodward on Twitter

He explained: "Currently there are three known classes of players who develop malware and spyware: hacktivists, cybercriminals and nation states.

"Flame is not designed to steal money from bank accounts. It is also different from rather simple hack tools and malware used by the hacktivists. So by excluding cybercriminals and hacktivists, we come to conclusion that it most likely belongs to the third group."

Among the countries affected by the attack are Iran, Israel, Sudan, Syria, Lebanon, Saudi Arabia and Egypt.

"The geography of the targets and also the complexity of the threat leaves no doubt about it being a nation-state that sponsored the research that went into it," Mr Kamluk said.

The malware is capable of recording audio via a microphone, before compressing it and sending it back to the attacker.

It is also able to take screenshots of on-screen activity, automatically detecting when

"interesting" programs - such as email or instant messaging - were open.

'Industrial vacuum cleaner'
Kaspersky's first recorded instance of Flame is in August 2010, although it said it is highly likely to have been operating earlier.

Prof Alan Woodward, from the Department of Computing at the University of Surrey said the attack is very significant.

"This is basically an industrial vacuum cleaner for sensitive information," he told the BBC.

He explained that unlike Stuxnet, which was designed with one specific task in mind, Flame was much more sophisticated.

"Whereas Stuxnet just had one purpose in life, Flame is a toolkit, so they can go after just about everything they can get their hands on."

Once the initial Flame malware has infected a machine, additional modules can be added to perform specific tasks - almost in the same manner as adding apps to a smartphone.

Iran falls victim to another cyberattack

7:48 PM Tuesday May 29, 2012

Expand

Photo / Thinkstock

A Russian-based internet security firm says a powerful spyware virus, with unprecedented data-snatching capabilities, has attacked computers in Iran and elsewhere in the Middle East.

Iran did not disclose any damage done by the virus. But a unit of the Iranian communications and information technology ministry said it produced an anti-virus capable of identifying and removing the new malware, dubbed "Flame."

Russian digital security provider Kaspersky Lab, which identified the virus, said in a release posted on its website late Monday that "the complexity and functionality of the newly

discovered malicious program exceed those of all other cyber menaces known to date."

The virus' origin has not been identified, but suspicion immediately fell on Israel, famous for its technological innovation and its tireless campaign against Iran's suspect nuclear program.

Israel's vice premier did little to deflect that speculation in an interview Tuesday.

"Whoever sees the Iranian threat as a significant threat is likely to take various steps, including these, to hobble it," Vice Premier Moshe Yaalon told Army Radio.

"Israel is blessed with high technology, and we boast tools that open all sorts of opportunities for us."

Tehran's nuclear and other industrial facilities have suffered periodic cyber attacks dating back to 2010, when the Stuxnet virus disrupted controls of some nuclear centrifuges. Iran claims the computer viruses have done no serious harm to Iran's nuclear or industrial facilities, and sees them as part of a campaign by Israel, the US and their allies to undermine the Iranian nuclear program.

The US and its allies suspect Iran's nuclear program aims to develop atomic weapons. Iran says its program is meant to produce fuel for future nuclear power reactors and medical radioisotopes needed for cancer patients.

- AP

Flame: world's most complex computer virus exposed

The world's most complex computer virus, possessing a range of complex espionage capabilities, including the ability to secretly record conversations, has been exposed.

An Iranian technician works at the Uranium Conversion Facility near Isfahan. Stuxnet attacked Iran's nuclear programme in 2010 Photo: AP

By Damien McElroy, Christopher Williams

7:06PM BST 28 May 2012

Comments

Middle Eastern states were targeted and **Iran** ordered an emergency review of official computer installations after the discovery of a new virus, known as Flame.

Experts said the massive malicious software was 20 times more powerful than other known cyber warfare programmes including the Stuxnet virus and could only have been created by a state.

It is the third cyber attack weapon targeting systems in the Middle East to be exposed in recent years.

Iran has alleged that the West and Israel are orchestrating a secret war of sabotage using yber warfare and targeted assassinations of its scientists as part of the dispute over its nuclear

programme.

Stuxnet attacked Iran's nuclear programme in 2010, while a related programme, Duqu, named after the Star Wars villain, stole data.

Related Articles

- Iran targeted by 'Flame' espionage virus
  28 May 2012
- Flame: anatomy of a super-virus
  29 May 2012
- Flame virus: who is behind the world's most complicated espionage software?
  29 May 2012
- America and China 'engaging in cyber war games'
  17 Apr 2012
- Iranian nuclear scientist latest victim of sabotage efforts
  11 Jan 2012
- 'Spy virus' targets nuclear firms
  19 Oct 2011

Flame can gather data files, remotely change settings on computers, turn on computer microphones to record conversations, take screen shots and copy instant messaging chats.

The virus was discovered by a Russian security firm that specialises in targeting malicious computer code.

It made the 20 megabyte virus available to other researchers yesterday claiming it did not fully understand its scope and said its code was 100 times the size of the most malicious software.

Kaspersky Labs said the programme appeared to have been released five years ago and had infected machines in Iran, Israel, Sudan, Syria, Lebanon, Saudi Arabia and Egypt.

"If Flame went on undiscovered for five years, the only logical conclusion is that there are other operations ongoing that we don't know about," Roel Schouwenberg, a Kaspersky security senior researcher, said.

Professor Alan Woodward from the department of computing at the University of Surrey said the virus was extremely invasive. It could "vacuum up" information by copying keyboard strokes and the voices of people nearby.

"This wasn't written by some spotty teenager in his/her bedroom. It is large, complicated and dedicated to stealing data whilst remaining hidden for a long time," he said.

The virus contains about 20 times as much code as Stuxnet, which attacked an Iranian uranium enrichment facility, causing centrifuges to fail. Iran's output of uranium was suffered a severe blow as a result of the Stuxnet activities.

Mr Schouwenberg said there was evidence to suggest the code was commissioned by the same nation or nations that were behind Stuxnet and Duqu.

Iran's Computer Emergency Response Team said it was "a close relation" of Stuxnet, which has itself been linked to Duqu, another complicated information-stealing virus is believed to be the work of state intelligence.

It said organisations had been given software to detect and remove the newly-discovered virus at the beginning of May.

Crysys Lab, which analyses computer viruses at Budapest University. said the technical evidence for a link between Flame and Stuxnet or Duqu was inconclusive.

The newly-discovered virus does not spread itself automatically but only when hidden controllers allow it.

Unprecedented layers of software allow Flame to penetrate remote computer networks undetected.

The file, which infects Microsoft Windows computers, has five encryption algorithms, exotic data storage formats and the ability to steal documents, spy on computer users and more.

Components enable those behind it, who use a network of rapidly-shifting "command and control" servers to direct the virus, to turn microphone into listening devices, siphon off documents and log keystrokes.

Eugene Kaspersky, the founder of Kaspersky Lab, noted that "it took us 6 months to analyse Stuxnet. [This] is 20 times more complicated".

Once a machine is infected additional modules can be added to the system allowing the machine to undertake specific tracking projects.

Flame virus: who is behind the world's most complicated espionage software?

Flame, a newly-discovered computer virus built for espionage has been named as the most complicated piece of malicious software ever created, and speculation as to who is behind it is sweeping the web.

Iran's presdient, Mahmoud Ahmadinejad, visiting the Natanz Uranium Enrichment Facility, target of Stuxnet Photo: AP

9:37AM BST 29 May 2012

Comments

Eugene Kaspersky, the founder of Kaspersky Lab, one of the security organisations that have investigated Flame since its discover earlier this month, is sure of at least one thing.

e_kaspersky Eugene Kaspersky

The complexity of #TheFlame, geography & targets leave no doubt this #malware was state-sponsored. FAQ: http://t.co/Rq5rGcMw #cyberwar

via TweetDeck Favorite Retweet Reply

Other experts already agree that the complexity of the software and its espionage-specific capabilities strongly suggest a state intelligence agency is responsible.

Reuters journalist Jim Finkle notes that Kaspersky Lab has suggested the team that created the

Stuxnet virus, which was designed to cause phiysical damage to the Iranian nuclear programme, may be behind Flame.

techwriterjim Jim Finkle

#Flame virus may be work of nation state behind #Stuxnet, Kaspersky says, though adds code itself bears no resemblance. #cybersecurity

via web Favorite Retweet Reply

Related Articles

- Flame: the world's most complex computer virus
  28 May 2012
- Iran targeted by 'Flame' espionage virus
  28 May 2012
- 'Western powers and Israel' launched Iran cyber attack
  21 Jan 2011

Given the pattern of the Flame infection known so far - Iran, the West Bank, Syria, Egypt - and its technological prowess, Israel has quickly emerged as many commentators' prime suspect.

Richard Silverstein, a US-based commentator and critic of the Israeli government, has made widely-shared **claims** "my senior Israeli source confirms that it is a product of Israeli cyberwarfare experts".

The Jerusalem Post thinks Vice President Ya'alon may even have already hinted Israel is behind Flame.

yaakovkatz Yaakov Katz

Deputy PM Ya'alon hints at possible #Israel role in 'Flame' virus. Says country blessed with great technology. #JPost http://t.co/Jr6HBSKq

via Tweet Button Favorite Retweet Reply

As ever with cyber espionage some are also casting suspicious glances towards Beijing and Washington.

RDG1871 ajb1871

Flame : Massive cyber-attack discovered, researchers say - who is it then? Chinese have my money. BBC - http://t.co/gVU6LfyY

via TweetDeck Favorite Retweet Reply

sibutcher Sandra Ionno Butcher

Reuters-'Flame' Cyber Weapon in #Iran, 20x amt code in Stuxnet. CIA, State, NSA, US Cyber Command "declined to comment" http://t.co/MLMiTTyB

via web Favorite Retweet Reply

But its worth remembering that two years after it was discovered, nobody knows for sure who was behind Stuxnet, and as Eugene Kaspersky notes, Flame is a much more complicated problem.

e_kaspersky Eugene Kaspersky

It took us 6 months to analyze #Stuxnet. #TheFlame is 20-times more complicated http://t.co/wZdsqloz

via TweetDeck Favorite Retweet Reply

Rob Rosenberger, of the computer security debunking website **Vmyths.com**, meanwhile offers a skeptical take on the debate.

vmyths Rob Rosenberger

@e_kaspersky Any truth to the rumor I'm spreading that Tom Cruise spread #Flame virus for CIA while filming "M:I Ghost Protocol"? :-)

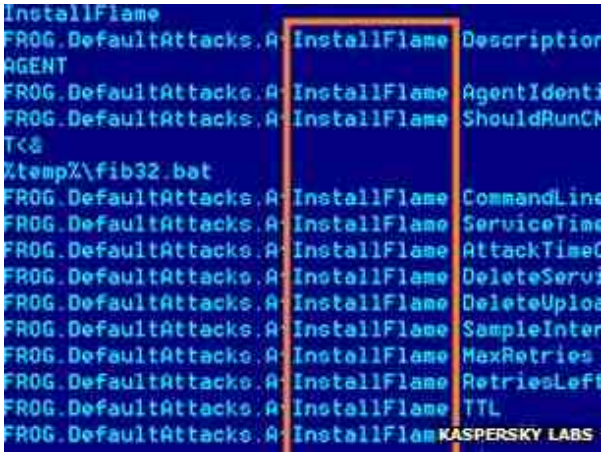
via Twitter for Android Favorite Retweet Reply

But what do you think?

Who is most likely to be behind the Flame virus?

29 May 2012 Last updated at 15:25 GMT

Iran 'finds fix' for sophisticated Flame malware



The sophistication of Flame helped it avoid detection by security software

Continue reading the main story

Related Stories

- Massive cyber-attack discovered
- Key Iranian oil terminal 'hacked'
- Oil hack attacks may 'cost lives'

Iran says it has developed tools that can defend against the sophisticated cyber attack tool known as Flame.

The country is believed to have been hit hard by the malicious programme which infiltrates networks in order to steal sensitive data.

Security companies said Flame, named after one of its attack modules, is one of the most complex threats ever seen.

Iran says its home-grown defence could both spot when Flame is present and clean up infected PCs.

Hard work

Iran's National Computer Emergency Response Team (Maher) said in a statement that the detection and clean-up tool was finished in early May and is now ready for distribution to organisations at risk of infection.

Flame was discovered after the UN's International Telecommunications Union asked for help from security firms to find out what was wiping data from machines across the Middle East.

An investigation uncovered the sophisticated malicious programme which, until then, had largely evaded detection.

An in-depth look at Flame by the Laboratory of Cryptography and System Security at Hungary's University of Technology and Economics in Budapest, said it stayed hidden because it was so different to the viruses, worms and trojans that most security programmes were designed to catch.

"Flame is not a widespread threat"
Graham Cluley Sophos

In addition, said the report, Flame tried to work out which security scanning software was

installed on a target machine and then disguised itself as a type of computer file that an individual anti-virus programme would not usually suspect of harbouring malicious code.

Graham Cluley, senior technology consultant at security firm Sophos, said the programme had also escaped detection because it was so tightly targeted.

"Flame isn't like a Conficker or a Code Red. It's not a widespread threat," he told the BBC. "The security firm that talked a lot about Flame only found a couple of hundred computers that appeared to have been impacted."

Mr Cluley said detecting the software was not difficult once it had been spotted.

"It's much much easier writing protection for a piece of malware than analysing what it actually does," he said. "What's going to take a while is dissecting Flame to find out all of its quirks and functionality."

It is not yet clear who created Flame but experts say its complexity suggests that it was the work of a nation state rather than hacktivists or cyber criminals.

Iran suffered by far the biggest number of Flame infections, suggest figures from Kaspersky Labs in a report about the malicious programme.

Kaspersky said 189 infections were reported in Iran, compared to 98 in Israel/Palestine and 32 in Sudan. Syria, Lebanon, Saudia Arabia and Egypt were also hit.

In April, Iran briefly disconnected servers from the net at its Kharg island oil terminal as it cleared up after a virus outbreak - now thought to be caused by Flame.

In the same statement that announced its home-grown detection tool, Iran said Flame's "propagation methods, complexity level, precise targeting and superb functionality" were reminiscent of the Stuxnet and Duqu cyber threats to which it had also fallen victim.

Stuxnet is widely believed to have been written to target industrial equipment used in Iran's nuclear enrichment programme.

UN to issue warning on Flame computer virus
Nations to be told virus is a dangerous espionage tool that could potentially be used to attack critical infrastructure.

Last Modified: 29 May 2012 23:25

The Flame virus was discovered in parts of the Middle East and follows the 2010 Stuxnet virus attack on Iran [Getty]

A United Nations agency charged with helping member nations secure their national infrastructures plans to issue a sharp warning about the risk of the "Flame" computer virus that was recently discovered in Iran and other parts of the Middle East.

"This is the most serious [cyber] warning we have ever put out," said Marco Obiso, cyber security coordinator for the UN's Geneva-based International Telecommunications Union.

The confidential warning will tell member nations that the Flame virus is a dangerous espionage tool that could potentially be used to attack critical infrastructure, he told Reuters news agency in an interview on Tuesday.

"They should be on alert," he said, adding that he believed Flame was likely built on behalf of a nation state.

The warning is the latest signal that a new era of cyber warfare has begun following the 2010 Stuxnet virus attack that targeted Iran's nuclear program. The United States explicitly stated for

the first time last year that it reserved the right to retaliate with force against a cyber attack.

'Nation state involved'

Evidence suggests that the Flame virus may have been built on behalf of the same nation or nations that commissioned the Stuxnet worm that attacked Iran's nuclear program in 2010, according to Kaspersky Lab, the Russian cyber security software maker that took credit for discovering the infections.

Kaspersky Lab said the Flame virus is unprecedented in size and complexity, with researcher Roel Schouwenberg marveling at its versatility.

Schouwenberg said there is evidence to suggest that the people behind Flame also helped craft Stuxnet. Many suspect Stuxnet was the work of Israeli intelligence.

Israel's vice premier did little to deflect suspicion about the country's possible involvement in the attack.

"Whoever sees the Iranian threat as a significant threat is likely to take various steps, including these, to hobble it," Moshe Yaalon told Army Radio when asked about Flame. "Israel is blessed with high technology, and we boast tools that open all sorts of opportunities for us."

"I think it is a much more serious threat than Stuxnet," the UN's Obiso said.

He said the ITU would set up a program to collect data, including virus samples, to track Flame's spread around the globe and observe any changes in its composition.

Kaspersky Lab said it found the Flame infection after the ITU asked the Russian company to investigate recent reports from Tehran that a mysterious virus was responsible for massive data losses on some Iranian computer systems.

So far, the Kaspersky team has not turned up the original data-wiping virus that they were seeking and the Iranian government has not provided Kaspersky a sample of that software, Obiso said.