The Washington Post

Back to previous page

U.S., Israel developed Flame computer virus to slow Iranian nuclear efforts, officials say

By Ellen Nakashima, Greg Miller and Julie Tate, Published: June 19, 2012

The United States and Israel jointly developed a sophisticated computer virus nicknamed Flame that collected intelligence in preparation for cyber-sabotage aimed at slowing Iran's ability to develop a nuclear weapon, according to Western officials with knowledge of the effort.

The massive piece of malware secretly mapped and monitored Iran's computer networks, sending back a steady stream of intelligence to prepare for a cyberwarfare campaign, according to the officials.

The effort, involving the National Security Agency, the CIA and Israel's military, has included the use of destructive software such as the Stuxnet virus to cause malfunctions in Iran's nuclear-enrichment equipment.

The emerging details about Flame provide new clues to what is thought to be the first sustained campaign of cyber-sabotage against an adversary of the United States.

"This is about preparing the battlefield for another type of covert action," said one former high-ranking U.S. intelligence official, who added that Flame and Stuxnet were elements of a broader assault that continues today. "Cyber-collection against the Iranian program is way further down the road than this."

Flame came to light last month after Iran detected a series of cyberattacks on its oil industry. The disruption was directed by Israel in a unilateral operation that apparently caught its American partners off guard, according to several U.S. and Western officials who spoke on the condition of anonymity.

There has been speculation that Washington had a role in developing Flame, but the collaboration on the virus between the United States and Israel has not been previously confirmed. Commercial security researchers reported last week that Flame contained some of the same code as Stuxnet. Experts described the overlap as DNA-like evidence that the two sets of malware were parallel projects run by the same entity.

Spokesmen for the CIA, the NSA and the Office of the Director of National Intelligence, as well as the Israeli Embassy in Washington, declined to comment.

The virus is among the most sophisticated and subversive pieces of malware to be exposed to date. Experts said the program was designed to replicate across even highly secure networks, then control everyday computer functions to send secrets back to its creators. The code could activate computer microphones and cameras, log keyboard strokes, take screen shots, extract geolocation data from images, and send and receive commands and data through Bluetooth wireless technology.

Flame was designed to do all this while masquerading as a routine Microsoft software update; it evaded

detection for several years by using a sophisticated program to crack an encryption algorithm.

“This is not something that most security researchers have the skills or resources to do,” said Tom Parker, chief technology officer for FusionX, a security firm that specializes in simulating state-sponsored cyberattacks. He said he does not know who was behind the virus. “You’d expect that of only the most advanced cryptomathematicians, such as those working at NSA.”

Conventional plus cyber

Flame was developed at least five years ago as part of a classified effort code-named Olympic Games, according to officials familiar with U.S. cyber-operations and experts who have scrutinized its code. The U.S.-Israeli collaboration was intended to slow Iran’s nuclear program, reduce the pressure for a conventional military attack and extend the timetable for diplomacy and sanctions.

The cyberattacks augmented conventional sabotage efforts by both countries, including inserting flawed centrifuge parts and other components into Iran’s nuclear supply chain.

The best-known cyberweapon let loose on Iran was Stuxnet, a name coined by researchers in the antivirus industry who discovered it two years ago. It infected a specific type of industrial controller at Iran’s uranium-enrichment plant in Natanz, causing almost 1,000 centrifuges to spin out of control. The damage occurred gradually, over months, and Iranian officials initially thought it was the result of incompetence.

The scale of the espionage and sabotage effort “is proportionate to the problem that’s trying to be resolved,” the former intelligence official said, referring to the Iranian nuclear program. Although Stuxnet and Flame infections can be countered, “it doesn’t mean that other tools aren’t in play or performing effectively,” he said.

To develop these tools, the United States relies on two of its elite spy agencies. The NSA, known mainly for its electronic eavesdropping and code-breaking capabilities, has extensive expertise in developing malicious code that can be aimed at U.S. adversaries, including Iran. The CIA lacks the NSA’s sophistication in building malware but is deeply involved in the cyber-campaign.

The CIA’s Information Operations Center is second only to the agency’s Counterterrorism Center in size. The IOC, as it is known, performs an array of espionage functions, including extracting data from laptops seized in counterterrorism raids. But the center specializes in computer penetrations that require closer contact with the target, such as using spies or unwitting contractors to spread a contagion via a thumb drive.

Both agencies analyze the intelligence obtained through malware such as Flame and have continued to develop new weapons even as recent attacks have been exposed.

Flame’s discovery shows the importance of mapping networks and collecting intelligence on targets as the prelude to an attack, especially in closed computer networks. Officials say gaining and keeping access to a network is 99 percent of the challenge.

“It is far more difficult to penetrate a network, learn about it, reside on it forever and extract information from it without being detected than it is to go in and stomp around inside the network causing damage,” said Michael V. Hayden, a former NSA director and CIA director who left office in 2009. He declined to discuss any operations he was involved with during his time in government.

Years in the making

The effort to delay Iran's nuclear program using cyber-techniques began in the mid-2000s, during President George W. Bush's second term. At that point it consisted mainly of gathering intelligence to identify potential targets and create tools to disrupt them. In 2008, the program went operational and shifted from military to CIA control, former officials said.

Despite their collaboration on developing the malicious code, the United States and Israel have not always coordinated their attacks. Israel's April assaults on Iran's Oil Ministry and oil-export facilities caused only minor disruptions. The episode led Iran to investigate and ultimately discover Flame.

"The virus penetrated some fields — one of them was the oil sector," Gholam Reza Jalali, an Iranian military cyber official, told Iranian state radio in May. "Fortunately, we detected and controlled this single incident."

Some U.S. intelligence officials were dismayed that Israel's unilateral incursion led to the discovery of the virus, prompting countermeasures.

The disruptions led Iran to ask a Russian security firm and a Hungarian cyber-lab for help, according to U.S. and international officials familiar with the incident.

Last week, researchers with Kaspersky Lab, the Russian security firm, reported their conclusion that Flame — a name they came up with — was created by the same group or groups that built Stuxnet. Kaspersky declined to comment on whether it was approached by Iran.

"We are now 100 percent sure that the Stuxnet and Flame groups worked together," said Roel Schouwenberg, a Boston-based senior researcher with Kaspersky Lab.

The firm also determined that the Flame malware predates Stuxnet. "It looks like the Flame platform was used as a kickstarter of sorts to get the Stuxnet project going," Schouwenberg said.

Staff writer Joby Warrick contributed to this report.

More world news coverage: - Greek election results don't quell fears - Chen Guangcheng adjusts to life in America - Iranian exiles in Iraq balking at relocation - Read more headlines from around the world