Flame, Stuxnet and Duqu: an abbreviated history of cyber attacking Iran

Rory Crump

The cyber-security community has given Flame mixed reviews after preliminary attempts to dissect the spying malware's bloated code. Kaspersky Lab called Flame "one of the most complex threats ever discovered." Symantec and McAfee were more reserved, seeing enough similarities between Flame's sophistication and past sibling cyber attacks – Stuxnet and Duqu – to throttle concerns the Internet is doomed. But as competing security outfits debate the origin, species and pervasive threat of the virus, all agree on a short list of nations capable of directing such grandiose espionage. Iran's unrepentant nature and doomsday attitude serve only to fuel speculation. Stuxnet, Duqu and now Flame, all aimed at Iran and all spooky reminders of today's silent theater of war. The cyber-attack stage is no longer novel, but the deeper cyber-security analysts cut into Flame, the more different it becomes.

Turns out Flame is big, sneaky, and a sign of the times. Unique enough – and dangerous enough - for the ITU, the United Nation's security blanket, to issue their most serious cyber warning yet. Stuxnet had a specific target, a specific objective. But Flame may be designed to lurk around the Middle East and come and go as it pleases, dressing down widespread targets from wanted countries in wanton fashion.

"Flame is a sophisticated 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," said Alexander Gostev at Kaspersky Lab, the Russian Internet security company responsible for untangling Flame.

Flame can record Skype conversations, take screenshots of e-mails and instant messages, collect usernames and passwords across local networks, and turn Bluetooth-enabled computers into beacons. What is Stuxnet famous for?

Discovered in 2010, Stuxnet was intended to sabotage industrial facilities, or engage in industrial espionage. Over half its hits were reported in Iran, and the subsequent impact and media attention were likened to a Hollywood movie. Stuxnet was groundbreaking, the first virus to infiltrate industrial processes and empower an invisible enemy. Symantec referred to the perpetrators as "skilled and well resourced."

Iran's nuclear centrifuges came under Stuxnet's fire, tripping uranium enrichment labs and an estimated 16,000 computers along the way. The worm's more commercial target was Siemens SCADA equipment, responsible for monitoring and controlling specific processes within Iran's nuclear facilities. The U.S. government was genuinely pleased with Iran's nuclear disruption.

Duqu came on the heels of Stuxnet and the two will be forever linked, as security professionals determined both shared near-identical code and similar targets. Stuxnet attacked machinery while Duqu focused on information theft – Bonnie and Clyde gone cyber. Together, at the time, considered ultra-complex pieces of malware to analyze. Although Israel took most of the heat for the unprecedented incident, the authors remain officially unknown.

Flame, on the other hand, certainly shares the same general target with Stuxnet and Duqu: Iran. But unleashes its insidious power on different victims. Early reports indicated Flame was targeting individuals, not particular companies or processes. Leading geo-politicos to think Flame was more a snoop than

a barbarian, but malicious nonetheless. Now, after shutting down Internet links to its crude oil complex last month, Iran officials announced Flame had sucked the data out of key oil networks. And banking on the discrete, fairly benign nature of the virus, vital sectors of the Iranian economy appear to be in Flame's crosshairs.

Kaspersky claimed it would take years to determine what is really beneath the thousands of lines of code - purposely misdated and built to mislead. And despite what Iran says about fanning the flames with a virus antivenom, the same may be said for determining Flame's ultimate destinations, Iran and elsewhere. It may take awhile.

In Flame's case, size does matter. It's heavyweight malware, coming in at 20 megabytes and dwarfing Suxnet in both size and functionality. It must be loaded in pieces and contains a kill module that can be activated if needed, sweeping up stray malware and then disappearing. Flame houses complex libraries, multi-level encryption, SQLite3 databases, and mix and match plug-ins adaptable to the attacker's information needs. It has units named Beetlejuice, Frog, Snack, and Gator – 20 in all – each with a different function. Flame is massive, and it needs to be in order to pack such a modular design and pull all those disparate functions.

But isn't malware supposed to be lean, slippery and engineered with clandestine features. Easier to hide and download. Better to keep a low profile. Flame's rotund figure should be a detriment. Stuxnet was measured in kilobytes with compact, cryptic code designed for a special op, not a multi-media buffet. But according to Gostev, "the large size of the malware is precisely why it wasn't discovered for so long." And Kaspersky found Flame by surprise, while investigating a different malware in the Middle East at the request of the ITU.

Another reason for Flame's girth could be – by design - its life expectancy and long-term goals. The modular design allows the authors to adjust behaviors, make changes on the fly. Kaspersky has detected Flame infections in Sudan and Syria, too. And depending the source, Flame has been infecting machines for at least two years. So Flame could remain a moving target for less advanced countries on the creator's black list - while it hunts new targets within those same fragile infrastructures.

So who would launch such a mischievous, in some ways brilliant, cyber attack on Iran, a country still playing weak digital defense. Those brave enough, or politically motivated enough, have called out Israel and the U.S. Or assuming mutual interests, we could imagine some combination of the two. Israel has a high-tech reputation and has not exactly denied involvement. And the U.S. has simply denied comment. China, Germany and Russia have now been thrown in the mix as countries with Flame-capable skills. But it never really pays to take credit for spying. Just keep spying and keep Iran chasing their tail – whoever you are.

According to the cyber-security community, malware assassins fall into one of three categories: cyber-criminals, hactivists and nation states with hidden agendas. Kaspersky, Symantec and McAfee all intimate Flame's design and targets fit only one profile. So which nation state is it? Considering the size, breadth and trickery of Flame, that identification may take years. Based on the fallout from Stuxnet and Duqu, we may never really know.