Menu

CBC news

Creating undetectable computer virus 'surprisingly simple'

Posted: May 30, 2012 3:39 PM ET
Last Updated: May 30, 2012 6:59 PM ET

The Flame virus that reportedly hit computers in at least seven Middle Eastern countries has been touted for its sophistication and ability to hide from anti-virus software.
iStock

Since the **Flame computer virus** was discovered earlier this week, much attention has been focused on the cleverness of this piece of malicious code.

Some online security experts say the fact that Flame — alternatively known as Flamer or sKyWIper — went unnoticed for possibly as long as five years years highlights another problem: the poor state of virus detection.

“Why does detection suck so much in the year 2012?” asks Brian Bourne, a Toronto-based cyber-security expert and founder of the SecTor cyber-security conference.

“Why can’t we detect bad [code] behaviour?”

Flame was found to have infected a total of 5,000 computers in at least seven Middle Eastern countries. It is thought to be 20 times more powerful than Stuxnet, the worm that disabled Iranian nuclear facilities in 2010.

Discovered by the Moscow-based anti-virus firm Kaspersky Lab, Flame has the ability to collect data, take screen shots, copy instant messaging chats, initiate Bluetooth connections with other devices and activate computer microphones to record conversations, among other things.

Most of the compromised computers were found in Iran, although there were also infections in Israel and the Palestinian territories, Sudan, Syria, Lebanon, Saudi Arabia and Egypt.

Targeted attack

A major virus outbreak, such as the ILOVEYOU worm in 2000, can infect hundreds of thousands if

not millions of machines within a matter of days.

One of the reasons the Flame attack stayed undetected so long is that it infected only about 5,000 machines in a two-year span, which suggests a targeted, long-term surveillance scheme.

Bourne says due to the relatively small distribution of the virus, the likelihood that Flame would be found and submitted to anti-virus software makers, so they could create a detection program, would be quite low.

While anti-virus software makers such as Kaspersky and Symantec create detection programs, Bourne says that most patches are based on “signatures,” which are based on analyzing the behaviour patterns of existing bad code.

One of the inherent flaws in cyber security, says Bourne, is the fact that anti-virus software is unable to identify entirely new types of viruses that don't exhibit documented behaviour.

“Until they get a sample of a bad piece of code, they don’t know how to detect it,” Bourne says.

“There are very smart people at Kaspersky and Symantec who haven’t figured it out yet.”

Limits of anti-virus technology

Those in the anti-virus business say their software does precisely what is designed to do.

“Anti-virus is a known threat detection technology," says Dave Marcus, director of advanced research and threat intelligence for McAfee Labs.

"If you throw something at it that it hasn’t seen before, it’s not really equipped to deal with it.”

Liam O’Murchu, a researcher at Symantec, admits that most anti-virus technology has been based on signatures, but says makers of security software have been expanding their tools of detection by looking at reputational and behavioural technology.

"Like if a program connects to the internet, but has no user interface, that’s something that we would deem as slightly more suspicious,” says O'Murchu.

He acknowledges, however, that even that sort of technology didn’t catch the Flame attack. He says this shows that whoever authored the Flame virus, “did extensive testing against many [existing] security products.”

The fact remains that it is relatively easy to trick even the best detection software.

“Bypassing anti-virus [software] is not all that difficult for virus writers,” says Dave Lewis, a Toronto-based cyber security expert who has worked with a number of Canadian tech companies and runs Liquidmatrix, a blog about internet safety matters.

Lewis says that a savvy hacker can simply change the composition of a string of known malicious code, “while allowing it to execute in the same manner.”

Tweaking existing code

“It’s surprisingly simple to take a sample of code off the internet that is detected, make a few small changes, and have it go undetected,” says Bourne. “You wouldn’t like to know how easy it is.”

Given the inherent shortcomings of virus detection, Lewis says organizations need to hire more people to monitor their systems.

“They have to spend the money to hire somebody with a brain to sit there, because they can’t just get the machine to go Click, Click, Next — ‘OK, I’m secure.’ It doesn’t work that way,” says Lewis.

He proposes increased review of system log files in order to monitor the appearance of new and possibly pernicious files. He also suggests creating a “gold standard” of vigilance for new files.

As part of their marketing message, purveyors of anti-virus software often suggest that computer users need to do more to protect themselves.

To illustrate this, McAfee just released a study suggesting that one in six Canadians is browsing the web without any security.

Bourne says he doesn’t like to blame the average computer user for his or her lack of vigilance.

“Expecting that a user will become expert enough to know what to do and when to do it and when not do it just doesn’t sound reasonable,” he says.

“We can point at them all we want and say, ‘Hey, weren’t you silly to click on that,’ but at the end of the day it’s the responsibility of the people making the operating systems and the software to provide as many protection mechanisms as we can.”

Related

Newly discovered malware most lethal cyberweapon to date
Cyber security Q&A: How to improve your online safety

- **Top Stories**
- **World**
- **Canada**
- **Politics**
- **Money**
- **Health**
- **Arts & Entertainment**
- **Technology & Science**
- **Offbeat**

Back To Top

Please enable JavaScript to use the search.

Search

Mobile only Full site

News

Sports

My Region

- Switch Site
- Terms of Use

- Privacy Policy

Back To Top