F-Secure

CONFICKER

10 years later—maybe forgotten, but definitely not gone

Conficker AKA Downadup AKA Downup AKA Kido – n.
A network worm that infected millions of PCs beginning in late 2008.

FUN FACT

Conficker got its name by rearranging the letters of “trafficconverter,” a website to which the first variant of the worm attempted to connect, and then adding a “k.”

CONFICKER MAY REPRESENT ONE OF THE GREAT INFOSEC SUCCESS STORIES OF THE EARLY 21ST CENTURY.

Microsoft formed the Conficker Working Group with industry leaders, including F-Secure, relatively early in the outbreak. This effort effectively rendered the worm, and the botnet it created, useless.

BUT

it also represents one of the industry’s great mysteries.

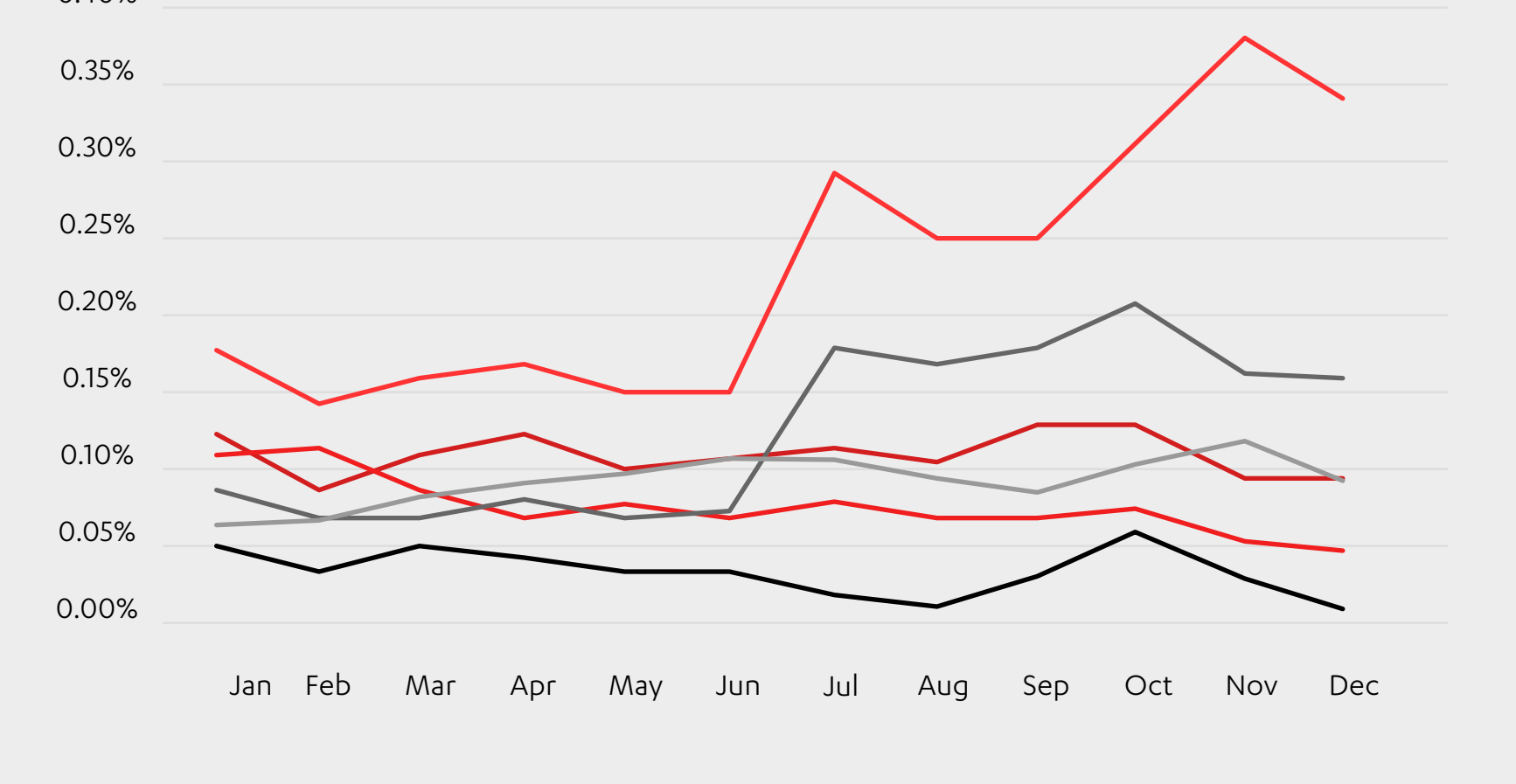
WANTED

A $250,000 reward offered to track down its creators has never been collected. (That we know of.)

THE CONFICKER FAMILY REMAINED THE MOST PREVALENT TYPE OF MALWARE OBSERVED BY F-SECURE LABS FOR MUCH OF THE DECADE.

WHILE OTHER MALWARE FAMILIES ARE NOW MORE COMMON, CONFICKER STILL ATTEMPTS TO INFECT MILLIONS OF MACHINES EVERY YEAR…

DOWNADUP / CONFICKER OVER THE YEARS



Note: Any detection hits visible above 0.01% is a prevalent detection.

WHAT MAKES CONFICKER SO WIDESPREAD, according to the Conficker Working Group:

- Multiple methods of spreading itself
- Ability to infect a computer and then wait for instructions
- Multiple defensive mechanisms that prevent removal
- Multiple versions released in rapid succession
- Quickly exploited vulnerability just after patch was announced
- Millions of machines have still not been patched

TIMELINE

October 23, 2008
Microsoft releases an emergency critical security patch for MS08-067 Windows.

November 20, 2008
Conficker Version A is released and detected the next day.

November 22, 2008
Microsoft issues an additional security alert recommending immediate patching of MS08-067.

December 1, 2008
Following instructions in the code, Conficker A-infected machines connect to trafficconverter.biz. The file that is supposed to be downloaded is not there.

December 29, 2008
Conficker Version B is released.

The same day the UK’s Sheffield Hospitals confirms that 800 of its computers are among the more than a million worldwide that have been infected with the worm.

January 1, 2009
Conficker Version B begins trying to check in at 250 different web domains.

The worm explodes making headlines around the world and exploiting millions of new machines.

“I thought to myself, how can this file work? But apparently it did.”
- Christine Bersasco, F-Secure

“I do distinctly the remember the feeling of impending doom – what will this thing actually collect from the networks as final payload? I also remember the struggle of coming up with a generic detection for it, given that all the samples were produced through heavy use of server-side polymorphism.”
-- Paolo Palumbo, F-Secure

February 12, 2009
Microsoft forms the Conficker Working group and offers a $250,000 bounty for information leading to the arrest of the worm’s creators.

February 16, 2009
The worm’s authors respond with the release Conficker.B++, which doesn’t need to contact any web domains for updates.

Late February, 2009
Conficker C, the first major rewrite of the worm, is spotted. This version connects to more domains, increases defenses and adds “peer-to-peer” capabilities that allow infected computers to communicate over networks.

Despite the industry’s best effort to downplay them, rumors of something big happening on April 1, 2009 begin to spread.

March 31, 2009
All PCs infected with Conficker C begin checking 500 web domains randomly selected from 50,000 URLS.

April 7, 2009
Conficker E is released aimed at infecting computers infected with Conficker C. It installs Waldec, “scareware” that imitates anti-virus software to extort money from users

Mid-April 2009
Conficker A and B has been locked out of all the known domains used for updates. The hype around the April 1 rumors leads to massive press coverage and awareness of the threat and cybersecurity in general.

But the hype just didn’t live up to reality.

As the sense that people had been pranked by the deadline grows, the worm continues to spread but the headlines around it quickly fade.

An estimated 5 to 15 million computers are infected in the initial outbreak.

September 2009
Stuxnet – sometimes called the “first cyberweapon”—is released.

Like Conficker, it exploits the MS08-067 vulnerability. Also, like Conficker, it is unusually complex. Unlike Conficker, we ultimately discovered Stuxnet’s purpose—attacking Iran’s nuclear weapons program.

June 2010
“It is likely that the Conficker Working Group effort to counter the spread did make it more difficult for the author to act with impunity, but the author did not seem to have tried his or her hardest,” the Conficker Working Group reported in its Lessons Learned report.

“I think this was a big step forward in the modern way of fighting against malware and people behind malware.”
-- Veli-Jussi Kesti, F-Secure

“Sometime after the outbreak, I remember the small office where my cousin worked. It seems that Conficker was also working. All their USBs and machines had Conficker in them.”
- Christine Bersasco, F-Secure

WHAT DID WE LEARN?

“For the industry, the learning is that when threats become very popular, people will start panicking. Even when there is already protection.”
- Christine Bersasco, F-Secure

“Working together brings results, but I think the real turning point was when the big malware groups started to get caught.”
-Veli-Jussi Kesti, F-Secure

WHAT DID THE CRIMINALS LEARN?

“Criminals learned to hide their command and control more efficiently along with the importance of proper opsec in their operations to stay under the radar. They also learned that malware that gets too prominent will get cut down.”
-Veli-Jussi Kesti, F-Secure

“But if the goal is to just be destructive, worms that automatically spread via network vulnerabilities are the best way to do it.”
- Christine Bersasco, F-Secure

WHAT SHOULD YOU LEARN?

Run all updates immediately.
And use top-notch internet security software.

FInd out more about conficker and the latest threats at:
BLOG.F-SECURE.COM

F-Secure

Sources: F-Secure “News from the Labs” blog; “The evolution of an extraordinary globe-spanning worm” by Byron V. Acohido; Conficker Working Group’s Lessons Learned; Motherboard’s “The History of Stuxnet: The World’s First True Cyberweapon”