Threatpost | The first stop for security news

- Categories
  - Category List
    - Apple
    - Cloud Security
    - Compliance
    - Critical Infrastructure
    - Cryptography
    - Government
  - Category List
    - Hacks
    - Malware
    - Microsoft
    - Mobile Security
    - Privacy
  - Category List
    - SAS
    - SMB Security
    - Social Engineering
    - Virtualization
    - Vulnerabilities
    - Web Security
  - Authors
    - Dennis Fisher
    - Michael Mimoso
    - Christopher Brook
    - Brian Donohue
    - Anne Saita
  - Additional Categories
    - Slideshows
  - The Kaspersky Lab News Service
- Featured
  - Authors
    - Dennis Fisher
    - Michael Mimoso
    - Christopher Brook
    - Brian Donohue
    - Anne Saita
    - Guest Posts
  - The Kaspersky Lab News Service

Featured Posts

All

 New BIOS Implant, Vulnerability Discovery Tool…

 Breach at Premera Blue Cross Affects…

 Apple Patches WebKit Vulnerabilities in Safari

- Podcasts

Latest Podcasts

All

Threatpost News Wrap, March 13, 2015

Threatpost News Wrap, March 6, 2015

 Patrick Gray on the State of…

 Threatpost News Wrap, February 27, 2015

 Mike Mimoso on SAS 2015

 Costin Raiu on the Equation Group…

Recommended

- Robert Hansen on Aviator, Search Revenue and the $250,000 Security Guarantee
- Threatpost News Wrap, February 21, 2014
- How I Got Here: Jeremiah Grossman
- Chris Soghoian on the NSA Surveillance and Government Hacking

The Kaspersky Lab Security News Service

- Videos

Latest Videos

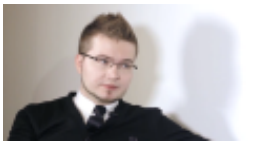
All

Kris McConkey on Hacker OpSec Failures

Trey Ford on Mapping the Internet...


Christofer Hoff on Mixed Martial Arts,...


Twitter Security and Privacy Settings You...


The Biggest Security Stories of 2013


Jeff Forristal on the Android Master-Key...

Recommended

- Twitter Security and Privacy Settings You Need to Know
- Lock Screen Bypass Flaw Found in Samsung Androids
- Facebook Patches OAuth Authentication Vulnerability
- Video: Locking Down iOS

The Kaspersky Lab Security News Service

Search

- Twitter
- Facebook
- Google
- LinkedIn
- YouTube
- RSS

03/20/15 5:50
Latest #Dridex Campaign Evades Detection with AutoClose Function - http://t.co/dDuEgrDx9q

-
-

Welcome > Blog Home>Government > Massive, Decades-Long Cyberespionage Framework Uncovered

473 222 0 0 1 5

Massive, Decades-Long Cyberespionage Framework Uncovered

Follow @dennisf by Dennis Fisher February 16, 2015 , 2:02 pm

CANCUN–Researchers at Kaspersky Lab have uncovered a cyberespionage group that has been operating for at least 15 years and has worked with and supported the attackers behind Stuxnet, Flame and other highly sophisticated operations. The attackers, known as the Equation Group, used two of the zero days contained in Stuxnet before that worm employed them and have used a number of other infection methods, including interdicting physical media such as CDs and inserting their custom malware implants onto the discs.

Some of the techniques the group has used are closely associated with tactics employed by the NSA, specifically the interdiction operations and the use of the LNK vulnerability exploit by Stuxnet.

The Equation Group has a massive, flexible and intimidating arsenal at its disposal. Along with using several zero days in its operations, the attack crew also employs two discrete modules that enable them to reprogram the hard drive firmware on infected machines. This gives the attackers the ability to stay persistent on compromised computers indefinitely and create a hidden storage partition on the hard drive that is used to store stolen data. At the Security Analyst Summit here Monday, researchers at Kaspersky presented on the Equation Group's operations while publishing a new report that lays out the inner workings of the crew's tools, tactics and target list. The victims include government agencies, energy companies, research institutions, embassies, telecoms, universities, media organizations and others. Countries targeted by this group include Russia, Syria, Iran, Pakistan, China, Yemen, Afghanistan, India but also US and UK, between and

several others.

Beginning in 2001, and possibly as early as 1996, the Equation Group began conducting highly targeted and complex exploitation and espionage operations against victims in countries around the world. The group's toolkit includes components for infection, a self-propagating worm that gathers data from air-gapped targets, a full-featured bootkit that maintains control of a compromised machine and a "validator" module that determines whether infected PCs are interesting enough to install the full attack platform on.

"We consider this to be the next level of threats," Costin Raiu, director of the Global Research and Analysis Team at Kaspersky, said in a presentation.

Kaspersky researchers say that the connection between the Stuxnet and Flame group and the Equation Group are concrete and deep.

"There are solid links indicating that the Equation group has interacted with other powerful groups, such as the Stuxnet and Flame operators–generally from a position of superiority. The Equation group had access to zero-days before they were used by Stuxnet and Flame, and at some point they shared exploits with others," the Kaspersky report says.

Once a PC is compromised, the attackers install the EQUATIONDRUG attack platform, which is the main component from which further operations run. The platform includes a variety of modules and has an analog in another platform called GRAYFISH, which is an updated version of the attack framework.

"By default, a core set of modules is installed into the target's computer together with EQUATIONDRUG, giving attackers full control over the operating system. In cases when the basic features of the malware are not enough, EquationDrug supports adding new plugins to extend its functionality. We found more than 30 different plugins for EquationDrug," the report says.

"EquationDrug's core modules, designed for deep hooking into the OS, do not contain a trusted digital signature and cannot run directly on modern operating systems. The code also contains a check whether the OS version is not newer than Windows XP/2003. Some of the plugins were originally designed for use on Windows 95/98/ME. If the target uses a modern operating system like Windows 7, the attackers use the TripleFantasy or GrayFish platforms."

GRAYFISH is the most highly evolved version of its attack infrastructure. The attackers began using this platform about seven years ago and have been improving it as they go.

"GrayFish includes a highly sophisticated bootkit, which is more complex than any other we've ever seen before. This provides an indication of the highest class of developers behind its creation," the Kaspersky researchers said.

"When the computer starts, GrayFish hijacks the OS loading mechanisms by injecting its code into the boot record. This allows it to control the launching of Windows at each stage. In fact, after infection, the computer is not run by itself more: it is GrayFish that runs it step by step, making the necessary changes on the fly."

The trump card for the Equation Group attackers is their ability to inject an infected machine's hard drive firmware. This module, known only by a cryptic name – "nls_933w.dll", essentially allows the attackers to reprogram the HDD or SSD firmware with a custom payload of their own creation.

"Although the implementation of their malware systems is incredibly complex, surpassing even Regin in sophistication, there is one aspect of the EQUATION group's attack technologies that surpasses anything else we have ever seen before. This is the ability to infect the hard drive firmware," the report says.

"We were able to recover two HDD firmware reprogramming modules from the EQUATIONDRUG and GRAYFISH platforms. The EQUATIONDRUG HDD firmware reprogramming module has version 3.0 while the GRAYFISH reprogramming module has version 4.0.1. These were compiled in 2010 and 2013, respectively, if we are to trust the PE timestamps."

The worm that's included with the Equation Group's toolkit is codenamed Fanny and provides a direct link to the Stuxnet group. The worm uses two of the zero days that later were used by Stuxnet, including the LNK file exploit. The Fanny worm spreads from infected machines via USB sticks, using the LNK file zero day, and its main purpose appears to be to reconnoiter and map air-gapped machines, PCs that aren't connected to the Internet or a network.

"First, when an USB stick is infected, Fanny creates a hidden storage area on the stick. If it infects a computer without an internet connection, it will collect basic system information and save it into the hidden area of the stick. Later, which a stick containing hidden information is plugged into a computer infected by Fanny having an Internet connection, the data will be scooped from the hidden area and sent to the C&C. If the attackers want to run commands on the air-gapped networks, they can save these commands in the hidden area of the USB stick. When the stick is plugged into the air- gapped computer, Fanny will recognize the commands and execute them. This effectively allowed the Equation group to run commands inside air-gapped networks through the use of infected USB sticks, as well as map the network infrastructure of such networks," the report says.

The Equation Group has been seen using at least seven vulnerabilities in various applications, four of which were zero days when the group began using them. One of the exploits the group used was for a vulnerability in Internet Explorer that had been used first by the Google Aurora attackers in 2009.

"The EQUATION group captured their exploit and repurposed it to target government users in Afghanistan," the report says.

As sophisticated and comprehensive as this group's toolset is, perhaps the most interesting tactic they employ is interdicting CDs bound for specific targets and inserting their malware. In one case, the attackers sent attendees of a scientific conference a CD that contained the proceedings from the meeting. Not all of the participants received the malware-infected discs.

"The CD-ROM uses 'autorun.inf' to execute an installer that will first attempt to escalate privileges using two known EQUATION group exploits. Next, it attempts to run the group's DOUBLEFANTASY implant and install it into the victim's machine. The exact method by which these CDs were interdicted is unknown. However, we do not believe the conference organizers did this on purpose, considering the

super-rare DOUBLEFANTASY malware, together with its installer with two zero-day exploits, doesn't end up on a CD by accident," the report says.

Another incident included an installation CD for Oracle software that included a Trojan dropper for the Equation Group's malware. This is a tactic that, through the Edward Snowden documents, has been attributed to operations conducted in the past by the National Security Agency.

Kaspersky researchers have sinkholed several of the C&C domains used by the Equation Group attackers and have so far counted more than 500 victims, but the total over the lifetime of the campaign is likely far higher. The C&C infrastructure includes hundreds of domains in a number of countries, including the United States, the UK, Italy and Germany.

Nearly all of the C&C domains and servers were shut down by the attackers last year, but some were still active as late as last month. But Raiu said that there are no samples of the Equation Group's tools from 2014.

"The scariest thing about them is that we don't have any samples from 2014. So somewhere in 2013 these guys went off the radar," he said. "We have no idea what they did in 2014, which is very, very scary."

About Dennis Fisher

Dennis Fisher is a journalist with more than 13 years of experience covering information security.

View all posts by Dennis Fisher →

Latest Tweet from: Dennis Fisher

Categories: Government, Hacks, Malware, Security Analyst Summit, Web Security

Comments (5)

1. *xjetmx* February 16, 2015 @ 6:46 pm
1

what does C&C mean?

Reply ↓

- *Simon* February 17, 2015 @ 10:17 am
2

C&C is command and control.

Reply ↓

- *Anonymous* February 17, 2015 @ 10:19 am
3

Command & Control.

Reply ↓

- *Actually* February 17, 2015 @ 4:15 pm
4

Actually C&C stands for Command & Conquer! The attackers are gamers! We should regulate gaming NOW!

Reply ↓

2. *Nitor* February 16, 2015 @ 7:21 pm
5

Two questions:
1. Was this- or Stuxnet- discovered on the computers at Fukushima Diachi?
2 would the Japanese Government or Tepco admit it if it was?

Reply ↓

Leave A Comment

Your email address will not be published. Required fields are marked *

Name

Email

Comment

You may use these HTML tags and attributes: `<a href="" title=""> <abbr title=""> <acronym title=""> <b> <blockquote cite=""> <cite> <code> <del datetime=""> <em> <i> <q cite=""> <strike> <strong>`

I'm not a robot

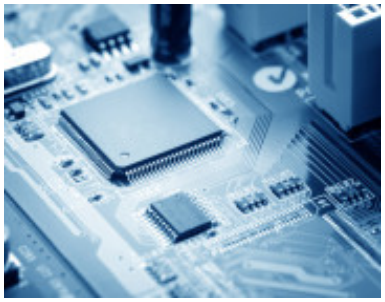
reCAPTCHA
Privacy - Terms

Post Comment

Notify me of follow-up comments by email.

Notify me of new posts by email.

Recommended Reads



0 431 0 0 0 2

March 19, 2015 , 7:00 am
Categories: Featured, Hacks, Malware, Vulnerabilities

New BIOS Implant, Vulnerability Discovery Tool to Debut at CanSecWest

by Michael Mimoso

Researchers are expected to present at CanSecWest a BIOS rootkit that automates BIOS vulnerability discovery and implants persistent malware.

Read more...

0 22 0 0 0 0

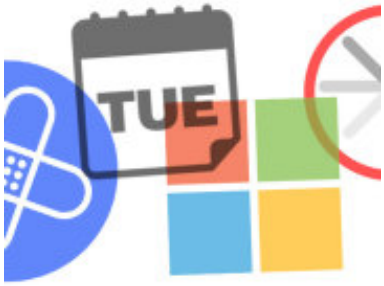
March 16, 2015 , 12:59 pm
Categories: Privacy, Web Security

Facebook Transparency Report: US Data Requests Dip Slightly

by Michael Mimoso

Facebook’s Transparency Report for the latter half of 2014 shows slightly fewer U.S. government requests for user data; the company also updates its Community Standards.

Read more...



March 13, 2015 , 2:20 pm
Categories: Apple, Microsoft, Podcasts

Threatpost News Wrap, March 13, 2015

by Dennis Fisher

Dennis Fisher and Mike Mimoso discuss the new patch for the fiver-year-old LNK vulnerability used by Stuxnet, the new iOS patches and the other news of the week.

Read more...

Top Stories

All Major Browsers Fall at Pwn2Own Day 2

March 20, 2015 , 11:26 am

New BIOS Implant, Vulnerability Discovery Tool to Debut at CanSecWest

March 19, 2015 , 7:00 am

Pharming Attack Targets Home Router DNS Settings

February 27, 2015 , 2:07 pm

PHP Applications, WordPress Subject to Ghost glibc Vulnerability

January 29, 2015 , 3:02 pm

CryptoLocker Variant Coming After Gamers

March 12, 2015 , 3:57 pm

Massive, Decades-Long Cyberespionage Framework Uncovered

February 16, 2015 , 2:02 pm

Cryptowall 3.0 Slims Down, Removes Exploits From Dropper

February 9, 2015 , 12:00 pm

[Lack of CSPRNG Threatens WordPress Sites](#)

February 12, 2015 , 11:47 am

[Of Ghost glibc Vulnerability Patching and Exploits](#)

January 28, 2015 , 1:28 pm

The Final Say

From Kaspersky Blogs

[A practical guide to making up a sensation....](#)

There are many ways to make up something sensationalist in the media. One of

the practical ways is to speculate and create conspiracy theories. Unfortunately, there’s a demand for such stories a...

Read more...

Analog OPSEC 101 – operational security in the phy...

For a long time we´ve been interested in operational security (OPSEC), and although you can find tons of cool technical tips about protecting digital information, we always felt that something was m...

Read more...

Windows Hello: Biometric Authentication by Default...

Windows 10 will offer users the ability to authenticate themselves with biometric identifiers rather than passwords...

Read more...

Pay to play again: a cryptolocker variant goes aft...

A cryptolocker variant is coming after online gamers, and there is more to this story than meets the eye. Looks like cybercriminals found a great way to get to the people who are all too willing to pa...

Read more...

Protecting Android devices...

Android smartphones and tablets are very popular among students for several reasons. First, they are relatively affordable. Second, they are flexible, so users can choose the most suitable set-up for ...

Read more...

Authors

Dennis Fisher
Michael Mimoso
Christopher Brook
Brian Donohue
Anne Saita