Blog Home (https://blog.checkpoint.com/) > Intelligence Report: Equation Group

MARCH 26, 2015

Intelligence Report: Equation Group

By **Check Point Research Team**

SHARE

f

(//www.facebook.com/sharer.php?u=https%3A%2F%2Fblog.checkpoint.com%2Fsecurity%2Fintelligence-report-equation-group%2F)

Executive Summary

The Equation Group, active since 2001, is a highly advanced and secretive

Equation was published by Kaspersky during their 2015 Security Analyst

EquationDrug and GrayFish, is capable of reprogramming hard disk drive

(http://en.wikipedia.org/wiki/Firmware). The group is using advanced tec

high degree of covert behavior. There are indications of about 500 malwa

(//twitter.com/share?url=https%3A%2F%2Fblog.checkpoint.com%2Fsecurity%2Fintelligence-report-equation-group%2F&text=Intelligence%20Report:%20Equation%20Group)

(//www.linkedin.com/shareArticle?mini=true&url=https%3A%2F%2Fblog.checkpoint.com%2Fsecurity%2Fintelligence-report-equation-group%2F)

(//www.reddit.com/submit?url=https%3A%2F%2Fblog.checkpoint.com%2Fsecurity%2Fintelligence-report-equation-group%2F)

(mailto:?subject=Intelligence%20Report:%20Equation%20Group&body=https%3A%2F%2Fblog.checkpoint
report-equation-group%2F)

Overview

The group was named Equation due to the hackers' evident fondness for
the sophisticated methods used throughout their operations. The Equatic
encryption algorithm. Some of the most recent modules also use RC6, R(
hashes.

These tweets are from the Kaspersky 2015 Security Analyst Summit:

- The #EquationAPT group is probably one of the most sophisticated cyl
- The #EquationAPT group interacted with other powerful groups, such
- Two zero-day exploits were used by the Equation group before they we

Equation Group Key Points

- "Fanny", which is one of the malwares used by Equation Group, was a
to the internet such as nuclear power plants and electricity companie
system, and then sending all information when it is plugged into a cor
- "Grok" is another malware used by the group, which is a key-logger tl
which are accessed through the infected computer.
- Some C&C servers used by the Equation group were registered as far
- The earliest known malware samples were compiled in 2002.
- Equation interacted with, and appears superior to, the Stuxnet and Fla

List of Relevant Signatures & Indicators

Check Point sees active infected hosts in Europe, US and the Persian Gul

The following IPS protections, Anti-Virus and post-infection Anti-Bot indi Group:

1. The IPS blade contains at least five different protections which will pr exploited by the Equation Group:
   1. CVE-2010-2568: Microsoft Windows Shell LNK File Parsing Code E
   2. CVE-2012-0159: Microsoft Windows Malformed TrueType Font Rem
   3. CVE-2012-1723: BlackHole Toolkit v2 JAVA Payload Stage Code Exe
   4. CVE-2012-4681: Oracle Java 7 Applet RCE Gondvv
   5. CVE-2013-3918: Microsoft Windows InformationCardSigninHelper
2. The Anti-Virus blade will prevent the malware from infecting custome detect computers or networks already infected with the malware:
   - The blades include 113 indicators which were first published on Fe

Unique Methods of Hard-Disk Firmware Infection A unique feature researchers and engineers around the world with an unprecedented tech plugin in place that enables the functionality of reprogramming hard driv firmware upgrade feature of hard drives and solid state disks by various compartments, invisible to operating systems and typically left unnoticed

This specially crafted code enables persistence of the Equation tools (or wipe and clean operating system installation. The reprogrammed firmwa the computer as needed. The unique HDD firmware infection is the persi

This capability requires a significant engineering effort, including specific model, testifying to the proportions of man-months and millions in USD i will see this implemented by common cybercriminals anytime soon, due software.

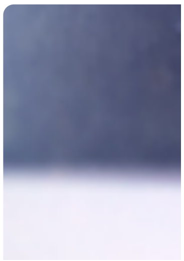
Synopsis The Equation group is a highly sophisticated organization that exploitation) operations dating back to 2001, and perhaps as early as 199 some of which surpass the well-known "Regin" (a sophisticated malware Equation group is probably one of the most sophisticated cyber-attack gr actor.

References

Wikipedia: http://en.wikipedia.org/wiki/Equation_Group (http://en.wikipe

Securelist: http://securelist.com/files/2015/02/Equation_group_question (http://securelist.com/files/2015/02/Equation_group_questions_and_ans

You may also like



(https://blog.checkpoint.com/2023/02/01/the-rise-of-the-code-package-threat/)

SECURITY (HTTPS://BLOG.CHECKPOINT.COM/SECURITY/) FEBRUARY 1, 2023

The Rise of the Code Package Threat (https://blog.checkpoint.com/2023/02/01/the-rise-of-the-code-package-threat/)

Highlights: Check Point details two recent attacks detected and blocked ...

(https://blog.checkpoint.com/research/ransomware-stopped-working-harder-started-working-smarter-botnets-phishing/)

RESEARCH (HTTPS://BLOG.CHECKPOINT.COM/RESEARCH/) OCTOBER 23, 2018

When Ransomware Stopped Working Harder and Started Working Smarter (https://blog.checkpoint.com/research/ransomware-...

Observing Ransomware's Evolution in Delivery Tactics Written by Check Point's ...

(https://blog.c
elections-thre

SECURITY (I

Democra
Threat L
(https://l

By Gal Fenig

(https://blog.c

RESEARCH

The Past
Cryptom
White Pa

Every month

COMPANY

About Us (https://www.checkpoint.com/about-us/)

Careers (https://careers.checkpoint.com/careers/)

Leadership (https://www.checkpoint.com/about-us/leadership/)

Newsroom (https://www.checkpoint.com/press-releases/)

Investor Relations (https://www.checkpoint.com/about-us/investor-relations/)

Merchandise Store (https://checkpointcompanystore.com/)

Contact Us (https://www.checkpoint.com/about-us/contact-us/)

TECHNICAL RESOURCES

User Center Sign In (https://usercen

Advisories (https://www.checkpoint.com/advisories/)

Threat Map (https://threatmap.checkpoint.com/)

Threat Wiki (https://threatwiki.checkpoint.com/threatwiki/public.htm)

URL Categorization (https://www.checkpoint.com/urlcat/)

App Wiki (https://appwiki.checkpoint.com/appwikisdb/public.htm)

EXPAND & LEARN

Resource Center (https://www.checkpoint.com/resources/

Cyber Hub (https://www.checkpoint.com/cyber-hub/)

Check Point Research (https://research.checkpoint.com/)

Check Point Blog (https://blog.checkpoint.com/)

Customer Stories (https://www.checkpoint.com/customer-stories/)

Product Knowledge Center (https://www.checkpoint.com/customer-stories/)

SUPPORT & SERVICES

Support Center (https://support.checkpoint.com/)

Infinity Global Services (https://www.checkpoint.com/services/infi global/)

IGS Portal (https://igs.checkpoint.com/)

☎ Contact Sales

North America:

+1-866-488-6691 (tel:1-866-488-6691)

International:

+44-125-333-5558 (tel:44-125-333-5558)

☎ Contact Support

North America:

+1-888-361-5030 (tel:1-888-361-5030)

International:

+44-114-478-2845 (tel:44-114-478-2845)

YOU DESERVE THE BEST SECURITY™

Copyright (https://www.checkpoint.com/copyright/) | Privacy Policy (https://www.checkpoint.com/privacy/) | Cookie Settings | Get the Latest News (https://pages.checkpoint.com/subscribe.html)

Follow Us

(https://www.facebook

(https://twitter.com/ch

(https://www.linkedin.c point-software-technologies)

(https://www.youtube.c