Aziende

Equation Group Takes Precise Calculations

Publish Date: 2015年2月18日

Recent reports have indicated of a threat actor group, Equation that hit enterprises and large organizations in various industries and entities like governments, financial institutions, military, telecommunications, and transportation among others across the globe.

The said targeted attack employed different malware tools in order to infiltrate their target networks. These tools include EQUATIONDRUG (detected as TROJ_DOTTUN.VTH), DOUBLEFANTASY (detected as TROJ_EQUATED.A), EQUESTRE, TRIPLEFANTASY (detected as TROJ_EQUATED.A), GRAYFISH (detected as

Minacce informatiche correlate

- RTKT_DOTTUN.VTH
- BKDR_LASSRV.B
- WORM_FANNY.AA
- TROJ_DOTTUN.

TROJ_EQUATED.A), GRAYFISH (detected as TROJ_EQUATED.A), FANNY (detected as WORM_FANNY.AA), and EQUATIONLASER (detected as BKDR_LASSRV.B). Accordingly, it shares similarities with Stuxnet, Flame, and Regin. Case in point, both Stuxnet and this targeted attack exploits a vulnerability found in shortcut files that allows random execution of code on the infected system.

How do user systems get infected with Equation?

Attackers use the following propagation means/methods in order to spread Equation infection:

- Removable drives or USBs
- CDs distributed in certain events
- Exploits
- Fanny malware

Based on reports, attackers did their threat intelligence on their target networks via checking what sites and forums they (users) often visit. Once attackers have this information, they will put exploits on the said websites/forums, which the users download without their knowledge. Another delivery mechanism they used is via shipped physical media that were supposedly tampered.

What exploits were used in this targeted attack campaign?

Equation leveraged vulnerabilities to penetrate its targeted network. For instance, it used two exploits related to Stuxnet such as Windows Kernel EoP exploit (covered in MS09-025) and LNK vulnerability (covered in CVE-2010-2568). This leads to the conclusion that this attack may also be related to this threat. Attackers also leveraged the zero-day exploit found in Internet Explorer, which was covered in CVE-2013-3918. In addition, it also used two TFF exploits addressed in MS12-034 and MS13-081, respectively.

I am already using Trend Micro products. Am I protected from this threat?

Yes. Trend Micro product users are protected from this targeted attack via the following solutions:

Custom Defense Solutions:

Deep Discovery provides 360-degree network-wide visibility, insight and control that enterprises and government organizations need in order to reduce the risk of Advanced Persistent Threats (APTs) and targeted attacks.

Deep Discovery uniquely detects and identifies evasive threats in real-time, and

VTH

Vulnerabilità correlate

- Microsoft Windows Shortcut Remote Code Execution Vulnerability
- Win23k TrueType Font Parsing Vulnerability (CVE-2012-0159)
- (MS13-090) Cumulative Security Update of ActiveX Kill Bits (2900986)

Deep Discovery uniquely detects and identifies evasive threats in real-time, and provides in-depth analysis and actionable intelligence needed to prevent, discover and contain attacks against corporate data.

Trend Micro Deep Discovery Inspector is able to protect users and enterprises from Equation through a customized sandbox that identifies and analyzes the behavior of malware tools such as EQUATIONDRUG (detected as TROJ_DOTTUN.VTH), DOUBLEFANTASY (detected as TROJ_EQUATED.A), EQUESTRE, TRIPLEFANTASY (detected as TROJ_EQUATED.A), GRAYFISH (detected as TROJ_EQUATED.A), FANNY (detected as WORM_FANNY.AA), and EQUATIONLASER (detected as BKDR_LASSRV.B) that are invisible to standard security.

Cloud and Data Center Security

Trend Micro Deep Security provides a comprehensive server security platform designed to protect virtualized data centers from data breaches and business disruptions while enabling compliance.

Trend Micro Deep Security users are protected from the exploits used by Equation campaign in order to infiltrate the network via the following DPI rules:

For TTF exploit addressed in MS12-034:

- 1005008 - Win32k TrueType Font Parsing Vulnerability (CVE-2012-0159)

For LNK vulnerability covered in CVE-2010-2568:

- 1004314 - Identified LNK/PIF File Over SMTP
- 1004293 - Identified Microsoft Windows Shortcut File Over Network Share
- 1004294 - Identified Microsoft Windows Shortcut File Over WebDav
- 1004308 - Identified PIF File Over HTTP
- 1004304 - Identified Suspicious Microsoft Windows Shortcut File Over Network Share
- 1004302 - Microsoft Windows Shortcut Remote Code Execution

For CVE-2013-3918:

- 1005779 - Microsoft Internet Explorer ActiveX Control Code Execution Vulnerability (CVE-2013-3918)
- 1005785 - Restrict Information Card Signin Helper ActiveX Control

Endpoint Solutions

Properly-configured endpoint solutions can ensure the prevention of coming into the machine or network. Components of OfficeScan Corporate Edition (OSCE) such as SmartScan, Web Reputation Service, Behavior Monitoring, and Smart Feedback offer the best protection against the attacks by Equation group via detecting the malicious files.

Worry-Free Business Security/Services (WFBS/WFBS-SVC) is also equipped with technologies to detect and remove all related malware tools related to the Equation group in the machine or network.
Trend Micro detects the following malware tools related to this attack as:

- BKDR_LASSRV.B (EquationLaser)
- TROJ_EQUATED.A (DoubleFantasy)
- TROJ_DOTTUN.VTH (EquationDrug)
- TROJ_EQUATED.A (GrayFish)
- WORM_FANNY.AA (Fanny)
- TROJ_EQUATED.A (TripleFantasy)

tuitamenteinostriserviziper30g

i
o
r
n
i

Inizia la prova gratuita oggi stesso