Solution Brief

Protecting Against Firmware and BIOS Manipulation

In the ***McAfee Labs Quarterly Threats Report: May 2015***, we take an in-depth look into the Equation Group and their attacks against hard disk and solid state drive firmware. The "Equation Group," named for their affinity for ultrasophisticated encryption schemes and the group's associated malware, is now among the most visible and advanced examples of firmware attack ever seen.

One of the most significant finds in the research is hard disk drive (HDD) and solid state drive (SSD) firmware reprogramming modules. HDDs/SSDs whose firmware has been reprogrammed can reload associated malware each time infected systems boot, and the malware persists even if the drives are reformatted or the operating system is reinstalled. Further, the reprogrammed firmware and associated malware is undetectable by security software once they have infected the drive.

During the last several years, Intel Security has observed many examples of malware with firmware/BIOS manipulation capabilities. They have been observed in both academic/PoC and in-the-wild scenarios, including **CIH/Chernobyl**, Mebromi, and **BIOSkit**. We also predicted this specific attack type in the *McAfee Labs 2012 Threats Predictions* report. With the discovery of "Equation Group–specific" samples, we now consider these one of the most visible and advanced examples of firmware attack ever seen.

Safeguarding against Equation Group attacks:

Here are recommended policies and procedures to protect against Equation Group–style attacks:

- Install endpoint security software on all endpoints.
- Enable automatic OS updates, or download OS updates regularly, to keep operating systems patched against known vulnerabilities.
- Install patches from other software manufacturers as soon as they are distributed.
- Encrypt important data and hard drives.
- Eliminate mass phishing campaigns with secure gateway email filtering.

intel Security

- Implement sender identity verification to reduce the risk of cybercriminals being mistaken for trusted parties.
- Detect and eliminate malicious attachments with advanced anti-malware.
- Scan URLs in email when received, and again when clicked.
- Scan web traffic for malware when phishing leads the user on a multiclick journey to infection.
- Educate users on best practices in detecting and acting upon suspicious emails.
- Implement data loss prevention to stop exfiltration in the event of a breach.

How Intel Security can help protect against Equation Group–style attacks

Protecting against firmware and BIOS manipulation attacks should be part of every enterprise's security approach. The focus should concentrate in two areas:

- Establish ways to detect the initial delivery of the Equation Group's malware. The known attack vectors are phishing, CDs, and USB drives. Place special attention in those areas.
- Secure systems from data exfiltration. Although the firmware reprogramming module cannot be detected today, the overall attack objective is very likely to be reconnaissance. Because reconnaissance depends on systematic communication and data exfiltration with a control server, halting that step is critically important.

McAfee Advanced Threat Defense

McAfee Advanced Threat Defense is a multilayered malware detection solution that combines multiple inspection engines that apply signature- and reputation-based inspection, real-time emulation, full static-code analysis, and dynamic sandboxing. McAfee Advanced Threat Defense will help protect against advanced malware that has been instructed to reload by the Equation Group's reprogrammed firmware.

- **Signature-based detection:** Detects viruses, worms, spyware, bots, Trojans, buffer overflows, and blended attacks. Its comprehensive knowledgebase is created and maintained by McAfee Labs, and currently includes more than 150 million signatures.
- **Reputation-based detection:** Looks up the reputation of files using the McAfee Global Threat Intelligence service to detect newly emerging threats.
- **Real-time static analysis and emulation:** Provides real-time static analysis and emulation to quickly find malware and zero-day threats not identified with signature-based techniques or reputation.
- **Full static-code analysis:** Reverse-engineers file code to assess all its attributes and instruction sets, and to fully analyze the source code without execution. Comprehensive unpacking capabilities open all types of packed and compressed files to enable complete analysis and malware classification, allowing your company to understand the threat posed by the specific malware.
- **Dynamic sandbox analysis:** Executes the file code in a virtual runtime environment and observes the resulting behavior. Virtual environments can be figured to match your company's host environments, and supports custom OS images of Windows 7 (32- or 64-bit), Windows XP, Windows Server 2003, Windows Server 2008 (64-bit), and Android.

McAfee Threat Intelligence Exchange

Having an intelligence platform that can adapt to suit your environment's needs is important. **McAfee Threat Intelligence Exchange** significantly reduces exposure to these types of attacks thanks to its visibility into immediate threats such as unknown files or applications.

- **Comprehensive threat intelligence:** Easily tailor comprehensive threat intelligence from global intelligence data sources. These can be McAfee GTI or third-party feeds, with local threat intelligence sourced from real-time and historical event data delivered via endpoints, gateways, and other security components.
- **Execution prevention and remediation:** McAfee Threat Intelligence Exchange can intervene and prevent unknown applications from being executed in the environment. If an application that was allowed to run is later found to be malicious, McAfee Threat Intelligence Exchange can disable the running processes associated with the application throughout the environment due to its powerful central management and policy enforcement capabilities.
- **Visibility:** McAfee Threat Intelligence Exchange can track all packed executables files and their initial execution in the environment, as well as all changes that occur thereafter. This visibility into an application's or process' actions from installation to the present enables faster response and remediation.
- **Indicators of compromise (IoCs):** Import known bad files hashes and McAfee Threat Intelligence Exchange can immunize your environment against these known bad files through policy enforcement. If any of the IoCs trigger in the environment, McAfee Threat Intelligence Exchange can kill all processes and applications associated with the IoC.

McAfee VirusScan for Enterprise

McAfee VirusScan® Enterprise uses the award-winning McAfee scanning engine to protect files from viruses, worms, rootkits, Trojans, and other advanced threats.

- **Proactive protection from attacks:** Integrates anti-malware technology with intrusion prevention to protect against attacks that leverage buffer overflow exploits targeted at vulnerabilities in applications.
- **Unbeatable malware detection and cleaning:** Protects against threats such as rootkits and Trojans with advanced behavioral analysis. Stops malware in its tracks through techniques including port blocking, filename blocking, folder/directory lockdown, file-share lockdown, and infection tracing and blocking.
- **Real-time security with McAfee GTI integration:** Protects against known and emerging threats across all threat vectors—file, web, email, and network—with the support of the most comprehensive threat intelligence platform in market.

McAfee Network Security Platform

McAfee Network Security Platform is designed to perform deep inspections of network traffic. McAfee Network Security Platform combines advanced inspection techniques—including full protocol analysis, threat reputation, behavior analysis, and advanced malware analysis—to detect and prevent both known and zero-day attacks on the network.

- **Comprehensive malware defense:** Combines file reputation from McAfee GTI, deep file analysis with JavaScript inspection, and signatureless, advanced malware analysis to detect and defeat zero-day threats, custom malware, and other stealthy attacks.
- **Leverages advanced inspection techniques:** Includes full protocol analysis, threat reputation, and behavior analysis to detect and prevent both known and zero-day attacks on the network.

- **Integration with McAfee Global Threat Intelligence:** Combines real-time file reputation, IP reputation, and geolocation feeds with rich contextual data about users, devices, and applications for fast, accurate response to network-borne attacks.
- **Security Connected:** Actionable integration with McAfee Advanced Threat Defense enables McAfee Network Security Platform to submit suspect files found in monitored traffic to McAfee Advanced Threat Defense, and deny or allow them based on findings from McAfee Advanced Threat Defense.

McAfee DLP Monitor

McAfee Data Loss Prevention (DLP) Monitor gathers, tracks, and reports on data in motion across the entire network. Easily uncover unknown threats to data and take actions to protect it to ensure your organization does not suffer the next big data breach.

- **Examine network traffic:** McAfee DLP Monitor's industry-leading data scanning and analysis capability examines network traffic at a deep level.
- **Quickly identify data:** Real-time discovery quickly details how data is being used, who is using it, and where it is going, providing you with information to act on. McAfee DLP Monitor can quickly identify more than 300 content types traversing any port or protocol, ensuring your organization is not blind.
- **Perform detailed forensics:** Conduct forensic analysis to correlate current and past risk events, detect risk trends, and identify threats. Allows you to quickly understand the situation, and develop rules and policies to address it.

McAfee DLP Prevent

McAfee Data Loss Prevention (DLP) Prevent protects against data loss by ensuring that data leaves the network only when appropriate—whether through email, webmail, instant messenger, wikis, blogs, portals, HTTP/HTTPS, or FTP transfers. Being able to rapidly identify and mitigate exfiltration attempts makes the difference between keeping your prized data safe and being the next news headline.

- **Gain visibility to security incidents:** Customized views and incident reports provide summary and detailed views of security incidents and your mediation actions.
- **Proactively enforce policies for all types of information:** Enforce policies for information you know is sensitive, as well as for information you may not know about. With a wide range of built-in policies—from compliance to acceptable use to intellectual property—you can match entire and partial documents to a comprehensive set of rules to protect all your sensitive information.

McAfee. Part of Intel Security.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com