Solution Brief

Protecting Against Evasive Malware

As detailed in the McAfee Labs Threats Report: June 2017, evasive malware masks itself to avoid detection. It hides by piggybacking or misusing legitimate applications. It recognizes when it is being analyzed in a sandbox and delays execution, waiting days, weeks, or even months for an opportunity to strike.

Building a security program to protect against evasive malware should be based on three foundational components.

- **People**: Security practitioners must be trained to properly respond to security incidents and to properly manage current security technology. Attackers commonly use social engineering to infect users. Without internal awareness and training, users will leave some windows open for attackers.
- **Process**: Clear structures and internal processes must be in place so that security practitioners can be effective. Security best practices (updates, backups, governance, intelligence, incident response plans, and more) are the keys to a powerful and effective security team.
- **Technology**: Technology supports the team and processes. It should be nurtured and enhanced so that it can adapt to new threats.

Actionable policies and procedures to protect against evasive malware

- The most important defense against malware infections is users. Users must be aware of the risk of downloading and installing applications that come from potentially risky sources. Users must also learn that malware can be inadvertently downloaded while browsing.
- Always keep browsers and add-ons up to date and antimalware on endpoints and network gateways upgraded and updated to the latest versions.
- Do not allow systems on the trusted network that are not distributed and certified by the corporate IT security group. Evasive malware can be easily disseminated by unprotected systems connected to the trusted network.

McAfee™
Together is power.

- Evasive malware can hide inside legitimate software previously Trojanized by an attacker. To prevent a successful attack of this type, we highly recommended tightened software delivery and distribution mechanisms. It is always a good idea to have a central repository of corporate applications from which users can download approved software.
- In instances where users are authorized to install applications that have not been previously validated by the IT security group, educate users to install only applications with trusted signatures from known vendors. It is very common for "harmless" applications offered online to have embedded evasive malware.
- Avoid application downloads from non-web sources. The likelihood of downloading malware from Usenet groups, IRC channels, instant messaging clients, or peer-to-peer systems is very high. Links to websites in IRC and instant messages also frequently point to infected downloads.
- Implement an educational program for phishing attack prevention. Malware is commonly distributed by phishing attacks.
- Leverage threat intelligence feeds combined with antimalware technology. This combination will help speed up threat detection.

How McAfee products can protect against evasive malware

McAfee offers a new generation of security capabilities designed to combat the most evasive modern threats. Drawing on powerful machine learning analysis and application containment tools, organizations can unmask hidden threats and stop them in their tracks—much more quickly and with much less effort.

These capabilities are delivered through the following McAfee products:

Real Protect

Real Protect, part of McAfee's Endpoint Protection solution, combines pre-execution static analysis and post-execution behavioral analysis to stop more malware than any signature-based or static-only solution, all integrated into the McAfee ecosystem. Real Protect applies state-of-the-art machine learning techniques to identify malicious code based on both an in-depth assessment of its static features (pre-execution analysis) and what it does (dynamic behavioral analysis)—all without signatures. Real Protect peels away the latest obfuscation techniques to unmask hidden threats so that zero-day malware has no place to hide.

Dynamic Application Containment

Dynamic Application Containment (DAC), also part of McAfee's Endpoint Protection solution, protects "patient zero" endpoints from new zero-day malware infections. When an endpoint detects a suspicious file, DAC immediately blocks the behaviors that malware often uses (such as changing the registry, writing to a temporary directory, or deleting files). Unlike other techniques that hold up the file (and the user) for minutes at a time, DAC lets the suspicious file load into memory without allowing it to make certain changes to the endpoint or infect other systems while it is under suspicion.

Real Protect and DAC are integrated—with each other, with other third-party security solutions such as SPLUNK, Avecto, ForeScout, and with McAfee Endpoint Protection—to provide a multilayer defense against the most evasive threats. They empower your security team to address all stages of the threat defense lifecycle—detect, correct, and proactively protect—in a fast, automated way.

Real Protect and DAC can be leveraged to:

- Unmask attacks by stripping away obfuscation techniques to see more malware threats.
- Limit an attack's impact: Contain, shield, and prevent damage to systems, either before an attack occurs or before it can cause irreversible damage.
- Track and adapt: Use automated, integrated defenses to perform a wider range of security operations without having to think about them or manually activate them.

See a video demonstration of evasive malware containment using Real Protect and DAC.

Dynamic Application Containment configuration best practices
DAC rules in the McAfee Default policy are set to only report, thereby reducing false positives. Adaptive Threat Protection provides two additional predefined DAC policies: McAfee Default Balanced and McAfee Default Security. These policies set recommended rules to block, based on the security profile:

- McAfee Default Balanced provides a base level of protection while minimizing false positives for many common unsigned installers and applications.
- McAfee Default Security provides aggressive protection, but might cause false positives more frequently on unsigned installers and applications.

Evaluate the impact of DAC rules by using the McAfee Default policy with rules set to report. To determine whether to set rules to block, monitor the logs and reports. After collecting DAC violation allowed (event ID 37280), set Enterprise Level Reputations or DAC exclusions before enforcing the McAfee Default Balanced policy.

DAC can exclude processes from containment based on name, MD5 hash, signature data, and path. If your organization signs tools that are deployed internally, add these signatures as exclusions to reduce false positives.

DAC rules have flood control, which limits the number of events generated to once per hour, per rule, and per process. DAC flood control tracks processes by process ID. When a process restarts, the operating system assigns it a new ID, which resets the flood control even though the process name is the same. For example, if Process A violates DAC rule A 100 times per hour, you receive one event per hour. If Process A restarts during that hour, flood control resets for Process A and you receive another event if it continues to violate DAC rule A. If Process B violates the same DAC rule A, you receive a second event (with Process B details). Read this for more information about specific best practices on McAfee-defined DAC rules.

Run McAfee's GetClean tool on the deployment base images for production systems to ensure that clean files are sent to McAfee Global Threat Intelligence (GTI) to be categorized. This tool helps to ensure that McAfee GTI does not provide an incorrect reputation value for your files. For more information, see the GetClean Product Guide (PD23191).

McAfee Cloud Threat Detection
Easily enhance McAfee protections to convict advanced malware and expose evasive threats by leveraging McAfee Cloud Threat Detection (CTD). Get access to McAfee ePO Cloud, enable McAfee CTD, and integrate it with your McAfee products.

To use McAfee CTD capability with your McAfee security products, take these actions:

- Enable McAfee CTD in McAfee ePO Cloud.
- Enable McAfee CTD in your McAfee security product interface and obtain the provisioning key.
- Use the provisioning key to generate an activation key in the McAfee ePO Cloud interface.
- Use the activation key to activate your McAfee security product.

The detailed instructions vary for obtaining the provisioning key and activating a product. Please refer to the product guide for detailed information about integrating McAfee CTD with your McAfee product.

When the integrated products start sending files for analysis to McAfee CTD, you can view your usage information on the Subscriptions page in McAfee ePO Cloud.

McAfee Active Response

- McAfee Active Response is built to find and respond to advanced threats. When used in association with threat feeds such as McAfee GTI, SecureWorks, or ThreatConnect, evasive threats can be searched for and eliminated before they have a chance to spread.
- Custom collectors can be used to build specific tools to find and identify indicators of compromise associated with Trojanized applications.
- Triggers and reactions can be built by the user to define actions when specific conditions are met. For example, when specific hashes or filenames are found, a "delete" action can automatically occur.

Further Reading

Neutralize Advanced Threats: Adapt Layered Defenses for Comprehensive Malware Protection

McAfee Security Advice Center: Top 10 Ways to Defend Against Malware and Trojans

McAfee Endpoint Security: Frequently Asked Questions

 3187_0617_brf-protecting-against-evasive-malware
June 2017

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