Solution Brief

Safeguarding Against Macro Malware

In the ***McAfee® Labs Threats Report: November 2015,*** we take an in-depth look at macro malware, a relic of the 1990s that is now seeing a resurgence due to the continued use of macros by enterprises coupled with the increased sophistication of social engineering attacks that are propagating new, stealthier macro malware. A macro is a shortcut used to automate a frequently performed task. It is a piece of code embedded inside a document—typically a Microsoft Office document—and is usually written in the programming language Visual Basic for Applications. When a macro is recorded, it is actually generating a program in Visual Basic for Applications. To combat macro malware, Microsoft built a permission-based step for enabling macros that serves as a double check. Microsoft Office now disables all macros by default, so macros cannot run without the user's permission. This move cooled the ardor of macro malware writers, and malicious macros declined in influence. However in the last year, attackers have leveraged new, stealthier macro malware coupled with social engineering to persistently target enterprises. The number of new macro malware samples is at its highest level in six years.

Today's macro malware attackers primarily leverage phishing email attachments, as well as spam campaigns, compromised web pages, and drive-by downloads to distribute their malware. These techniques are now far more sophisticated than they were in the 1990s, when macro malware first emerged. It has become quite difficult for users to spot these campaigns because they are targeted, short lived, and contain carefully designed attachments that avoid detection.

Here are some recommended policies and procedures to protect against macro malware attacks:

- Enable automatic operating system updates, or download operating system updates regularly, to keep them patched against known vulnerabilities.
- Use updated Microsoft Office software, which has better protection against these kinds of attacks.
- Ensure that the default setting for macro security on all Microsoft Office products is set to high.
- Configure anti-malware software to automatically scan all email and instant message attachments. Make sure email programs do not automatically open attachments or automatically render graphics, and turn off the preview pane.

- Configure browser security settings to medium level or above.
- Use great caution when opening attachments, especially when those attachments carry the .doc or .xls extension.
- Never open unsolicited emails or unexpected attachments—even from known people.
- Beware of spam-based phishing schemes. Don't click on links in emails or instant messages.
- Monitor for unexpected pings to IP addresses such as 1.3.1.2 or 2.2.1.1 from internal computers.
- Note that receipt or billing information documents generally do not need macros.
- Be careful when dealing with empty documents that prompt users to enable macros to view the contents.

How Intel Security Helps Protect Against Macro Malware

McAfee Web Gateway

Malvertising, drive-by-downloads, and malicious URLs embedded in phishing emails are some of the main attack methods used to deliver macro malware. **McAfee Web Gateway** is a robust product that will boost your company's protection against this type of threat.

- **Gateway Anti-Malware Engine**: Signatureless intent analysis filters out malicious content from web traffic in real time. Emulation and behavior analysis proactively protect against zero-day and targeted attacks. The Gateway Anti-Malware Engine inspects files and blocks them from being downloaded by users if the files are malicious.
- **Integration with McAfee Global Threat Intelligence (McAfee GTI):** Real-time intelligence feeds with McAfee GTI file reputation, web reputation, and web categorizations offer protection against the latest threats because McAfee Web Gateway will deny attempts to connect to known malicious websites or websites that use malicious ad networks.

McAfee VirusScan® Enterprise

Detecting and cleaning macro malware is simple with **McAfee VirusScan Enterprise**. McAfee VirusScan Enterprise uses the award-winning McAfee Labs scanning engine to protect your files from viruses, worms, rootkits, Trojans, and other advanced threats. Further protect your company with McAfee VirusScan Enterprise's ability to block ports and filenames; lock down folders, directories, and file shares; and trace and block infections.

- **Proactive protection from attacks**: Integrates anti-malware technology with intrusion prevention to protect against exploits that leverage buffer overflow exploits targeted at vulnerabilities in Microsoft 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 like port blocking, filename blocking, folder/directory lockdown, file share lockdown, and infection tracing and blocking.
- **Real-time security with McAfee GTI integration**: Protection 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 the market.

McAfee Advanced Threat Defense

McAfee Advanced Threat Defense is a multilayered malware detection product that combines multiple inspection engines. By combining multiple inspection engines that apply signature- and reputation-based inspection, real-time emulation, full static-code analysis, and dynamic sandboxing, McAfee Advanced Threat Defense not only detects documents that leverage macros to deliver malware, but also ensures detection and protection against the malware they download after execution.

- **Signature-based detection**: Detects viruses, worms, spyware, bots, Trojans, buffer overflows, and blended attacks. Its comprehensive knowledgebase is created and maintained by McAfee Labs.
- **Reputation-based detection**: Looks up the reputation of files using McAfee GTI to detect newly emerging threats.
- **Real-time static analysis and emulation**: Provides real-time static analysis and emulation to quickly find macro 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 fully analyzes 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**: For a file whose safety cannot be established through the inspection engines above, McAfee Advanced Threat Defense can execute the file code in a virtual runtime environment and observe the resulting behavior. Virtual environments can be configured to match host environments. McAfee Advanced Threat Defense supports custom operating system images of Windows XP SP2 and SP3, Windows 7 (32- and 64-bit), Windows 8 (32- and 64-bit), Windows Server 2003, Windows Server 2008 (64-bit), and Android.

McAfee Threat Intelligence Exchange

Having an intelligence platform that can adapt over time to suit an environment's needs is important. **McAfee Threat Intelligence Exchange** significantly reduces exposure to macro malware attacks, thanks to its visibility into immediate threats such as unknown files or applications being executed in the environment.

- **Comprehensive threat intelligence**: Easily tailor comprehensive threat intelligence from global threat 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 the product's powerful central management and policy enforcement capabilities.
- **Visibility**: McAfee Threat Intelligence Exchange can track all packed executable 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**: Import known bad files hashes and immunize your environment against these known threats through policy enforcement. If any of the indicators trigger in the environment, McAfee Threat Intelligence Exchange can kill all processes and applications associated with the indicators of compromise.

In addition to these Intel Security products, we recommend two additional classes of security technologies.

- **Email gateway security**: Most macro malware enters a system through an attachment to an email message, so a robust email gateway security product that scans all attachments for malware should be part of a good defense against this type of attack.
- **Firewall**: Foundational to any security system is good firewall technology. A firewall can detect many threats at the perimeter, before they enter the trusted network.

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