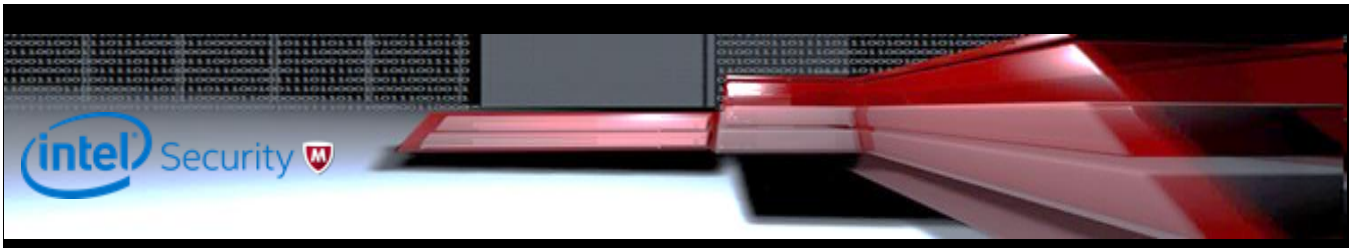

McAfee Malware Support - Best Practices Series

Avoid being compromised by worms

What is a worm?

Unlike viruses worms don't use other files as hosts. They are standalone applications with their own execution and propagation mechanisms and are able to spread across networks effectively. They can use polymorphism and other obfuscation techniques in order to avoid detection. They can disable safe and/or network boot and are commonly integrated with stealth components like rootkits.

Worms are efficient means of compromise and can provide subsequent covert streamline access to the networks they infiltrate. Their reconnaissance abilities are leading them not just to target traditional systems but also have started to explore ways of exploiting vulnerabilities in applications used by smartphones and tablets where they can spread by very effective means, i.e. NFC worms (near-field communication).

Worms spreading mechanisms

It is key to their success to have effective means to propagate and they use different techniques in order to take over the network they infiltrate:

- **Exploit of a vulnerability** in the operating system or an application: they can exploit a single vulnerability or have exploit kit like components in order to maximize replication vectors in different networks. They carry out the attacks scanning IP ranges (random or local) and targeting the ports used by the services affected by these vulnerabilities.
- Use of **autorun** capabilities in Windows placing autorun.inf files pointing to copies of themselves in the root of all fixed and removable USB drives.
- Making copies of themselves on **open network shares** where affected users have write access permissions.
- Using **email** as the propagation vector, not as a product of a spam run, but as its own mechanism. This type of worms are also known as mass mailing worms (@MM).
- As other type of threats they can be introduced to an environment as an attachment in a spam run, via **drive-by downloads** visiting malicious or compromised websites or dropped by a different malware already infiltrated.

They may or may not have a payload, however their presence in the network can be sufficient to cause an effective denial of service. Although not exclusive to worms, it is very common for worms to install a backdoor component and make the systems affected 'zombies' or 'bots' in controlled networks also known as botnets.

Hardening actions

In the case of worms special attention needs to be pay to security practices associated to their distribution mechanisms. These need to be considered in conjunction with the use of McAfee products to avoid being infected.

- Avoid successful use of exploits in your environment by ensuring operating systems and applications used are the latest versions and that they are updated as soon as possible following vendors' patch release cycles.
- Apply principle of least privilege when designing access control policies to network resources. Inability to replicate through the network will limit significantly the impact of the incident.

- Use of administrative accounts only for tasks where they are required.
- Where possible set permissions in network shares as read only.
- Social engineering and spear phishing attacks require personnel to be educated to prevent security breaches:
    - Ensure users are aware of, and can recognise the social engineering techniques including user awareness for phishing emails, a common attack vector. McAfee Foundstone Security Education - Ultimate Hacking: Human - US - UK - DE – FR - India – Australia.
    - Ensure that all end users are educated in safe computing practices and that there is a clear escalation process available to them if they become suspicious.
    - Only purchase security software from trusted vendors and retailers. Do not attempt to download free utilities from untrusted sources (e.g. Peer-to-Peer file sharing applications).
- Make sure your organisation has a plan to deal with a network incidents. Handling this type of attack will require collaboration between different functional groups in the organization as well as a structured approach. McAfee Incident Response Program Development: Get customized incident-response planning will ensure you are equipped to handle this type of incident in the most effective way.
- Employ browser security settings to prevent malicious content from running on compromised web pages. McAfee Foundstone Security Education: Ultimate Hacking: Windows Security US - UK - DE – FR –India - Australia.

Best Practices at the EndPoint

McAfee VirusScan Enterprise (VSE)

Ensure product is configured to prevent any known threats:

- It is kept fully up to date with the latest patch, DAT version and scanning engine.
- All machines in your environment are protected and updated.
- Real time scanning (On Access) is set to scan all files, On Read and On Write. Never turn scanning On Read off - other than when configuring Low-Risk processes.
- Scan exclusion rules should be kept to a minimum and only used when absolutely necessary. In the event of malware being suspected, ensure that any scan exclusions are temporarily disabled if safe to do so. Find how to setup exclusions in the Knowledge Base: KB50998.
- In heavily utilized environments or those where hardware specifications are on the verge of those recommended as a minimum, leverage the use of High-Risk/Default/Low-Risk Process configurations to limit the risk exposure against the performance requirements. Understand this feature KB55139 and learn how to configure it KB58692.
- Consider implementation of Network Drive scanning as an added layer of defence where security needs surpass performance implications.
- Configure product to use the Global Threat Intelligence File Reputation. This technology helps bridge the gap between Zero Day Threats and Signature Based Detections. Learn about recommended GTI File Reputation settings here KB74983. More information here KB53735.

Use of Access Protection Rules:

- Configure Access Protection rules to prevent the creation of autorun.inf files.
- Utilize Access Protection Rules for the prevention of unknown threats from being installed and to allow for the potential payload from taking place, by preventing creation and/or execution of files in commonly used directories by malware. Testing of these rules is required to leverage with exceptions for known good applications and ensure proper balance between corporate security and business needs.

McAfee Deep Defender

- Provides real time, kernel level protection to avoid being compromised by rootkits and zero day threats so commonly used by worms through on-going low level behavioural monitoring. Prevents the stealth components of files infectors from successfully compromising systems.
- Find out more: McAfee Deep Defender Best Practices Guide.

McAfee Application Control

- Effective way to block unauthorised applications and code on servers, corporate desktops and fixed function devices.
- It will prevent files being compromised effectively and stop file infectors spreading across the network.
- Implementing a whitelisting solution requires a good understanding of changes necessary in addition to well understood and limited mechanisms for delivering these changes.
- Read more here.

McAfee Host Intrusion Prevention (HIP)

- Provides a comprehensive protection through the use of behavioural analysis, signatures and a dynamic stateful firewall. This together with the use of GTI cloud technology to block and log communications to networks known to have a negative reputation as classified by McAfeeLabs will be a major factor in reducing or eliminating the vectors of infection such as the use of exploits including zero-day attacks.
- HIP will be also able to prevent the payloads and/or connection to botnet from where to carry out additional attacks or download secondary or tertiary drops.
- Block only high-severity signatures initially. High level of protection with few false events. Medium-severity signatures operate on behaviors and generally require some tuning to ensure configuration is suitable to all different setups and customized environments across your organization.
- Segregate desktops to reflect applications and privileges.
- Pick a few important user groups, pilot with representative users committed to providing feedback, test that applications still work correctly, and then roll out broadly when policies are proven to not disrupting productivity.
- Regular monitoring and regular maintenance are required to maintain the accuracy and effectiveness of protection. Budget time to review logs and update rules at least weekly once you complete deployment (KB73399).
- Start with IPS, then add firewall, then add application blocking as needed (KB71794).
- Use adaptive mode for brief periods only when able to monitor rules created.
- Take the time to verify that the traffic you are seeing is indeed malicious. Use packet captures, network IPS, or similar tools at your disposal.
- Read more: Adopting Host Intrusion Prevention - Best practices for quick success.

SiteAdvisor Enterprise (SAE)

- Based on McAfee Global Threat Intelligence (GTI) web reputation and web categorization services to identify sites that are hosting malware, infected by malware, and hosting inappropriate content.
- Identifies sites considered safe and not safe with a color scheme:
  - Green = Safe (Very low or no risk issues)
  - Yellow = Caution (Minor risk issues)
  - Red = Warning (Serious risk issues)
  - Grey = Unknown (Not rated yet, use caution)
  - McAfee Secure = Tested Daily for hacker vulnerabilities
- Very easily deployed and configured through ePolicy Orchestrator.
- FAQs for SiteAdvisor Enterprise (KB73457).

- Provides authorization/blocking of websites.
- Reactions based on safety ratings.
- It provides another layer of protection on the end point. It can be used with IE, Firefox and Chrome.
- As well as providing protection against malicious or compromised websites it can help to educate users into safer browsing habits.

- Use effective anti-spam protection to prevent malicious emails from entering your network.

Best Practices at the Gateway

McAfee Next Generation Firewall

- Integrates application control, intrusion prevention system (IPS), and evasion prevention.
- Get further details in the datasheet available for download here.
- FAQs for Next Generation Firewall can be found in KB78980.

McAfee Firewall Enterprise

- Proxy based firewall provides application identification, reputation-based global intelligence, automated threat feeds, encrypted traffic inspection (SSH/SSL), intrusion prevention, antivirus and content/URL filtering.
- FAQs and Facts can be found in: KB61399.

McAfee Email Gateway

- Detailed appliance configuration best practices can be found in PD24115
- Using a mail MEG gives not only the ability to stop malicious e-mail and e-mail containing malicious code but it is able to block e-mail based on different features – i.e. Based on a particular text string detection here.
- Restrict attachment types that are allowed through the gateway. Prevent .EXE, .VBS, PIF, .SCR, CPL, VBE or COM from going through. If a different extension is used for propagating a threat over email ensure it is included in this list.
- Powerful antispam scanning technologies to identify and block incoming spam with over 99% accuracy. Spam Filtering Best Practices here.
- Working in conjunction with GTI cloud reputation services, Email Gateway uses the message, network, and web reputation service to identify email messages carrying malicious payloads.

McAfee Advanced Threat Defence

- McAfee Advanced Threat Defense detects today's stealthy, highly sophisticated packers, encrypted payloads and zero-day malware with an innovative, layered approach. It combines low-touch antivirus signatures, reputation, and real-time emulation defenses with in-depth static code and dynamic, malware analysis (sandboxing) to analyze the actual behavior of malware.
- FAQs for Advanced Threat Defense

McAfee Network Security Platform

- Discovers and blocks sophisticated threats in the network. Using advanced threat detection techniques, it defends against stealthy attacks with extreme accuracy at speeds of up to 80 Gbps,
- FAQs for Network Security Platform

McAfee Web Gateway

- Ultimate antimalware protection against web threats.

- Layered approached at the gateway combining local and cloud-based protection.
- MWG Best Practices and Common Scenarios here.

More E-Mail and Web Security product details are available here. Read more about our Solution Services US – UK - DE – India – Australia - Japan.

- Ultimately, if you need specialized help call our Incident Response & Forensics Team: US - UK - DE - FR – India - Australia
- **Emergency? Hacked999@Foundstone.com**