McAfee Malware Support - Best Practices Series

Avoid being compromised by file infectors

What are file infectors?

File infectors are what we have traditionally understood as computer viruses: malicious code attached to other files, generally executables, allowing their code to be executed every time the host file is run. Once executed their replication mechanisms are initiated with different degrees of success and vary from infecting particular types of files on local drives, removable media, or remote locations to residing in memory and attaching themselves to files as they are accessed by the system or users. There are some that also put in place their own re-start mechanisms to ensure persistence and deliver their payload. They can be polymorphic, making each iteration unique, use a variety of obfuscation techniques and employ stealth components like rootkits to prevent detection and removal.

Some file infectors have been around for a long time and re-appear as new versions introducing new features and techniques to avoid detection and improved propagation techniques. For example, W32/Sality was first discovered in 2003 and new variants have been discovered regularly to date.

Payloads

By design, file infectors tend to be destructive. The speed of propagation and infected files are the most characteristic payload associated to these threats.

Modern threats classified as file infectors have payloads that are largely the same as those associated with other types of malware, but simple backdoors and data exfiltration are very common. Other payloads can be the delivery of remote access tools (RATs) or any pay per install application, file encryption, website redirection or being used as an open relay for the delivery of spam messages.

Infected File Cleaning

Generally systems affected by file infectors can be cleaned and environments restored to their original state prior to the infection. However, it is important to understand some of the challenges associated with the cleaning process.

The self-replicating nature of file infectors often means that removal is more challenging. Although it would be simple to just delete the infected files, it is often an undesirable action due to the potential loss of important data.

The structure of an infected file must be changed to accommodate the viral code. Some file infectors make fundamental changes that require the reversal of complex code relocations and encryption cycles which can result in file corruption. Sometimes it needs to be considered that the speed by which files are being infected cannot be matched by the cleaning process. This can lead to instances where making file shares read only and in some cases segregating infected machines may be a requirement.

There are cases where recovery is either impossible or impractical. Using backups to recover files affected by these threats may sometimes be faster and in some occasions the only way to restore infected files to their original state prior to the infection.

For these reasons, backups should be maintained to prevent any data loss in the event of file loss or file corruption due to malicious file infection.

First Infection & Propagation Vectors

The first vector of infection or distribution mechanism for file infectors does not differ from other malware families. They can be introduced to an enterprise environment through dropper files associated to spam runs. They can also be introduced by visiting compromised or malicious web sites through drive-by downloads or downloaded by other Trojans, backdoors or malware in general. Less commonly in the enterprise environment the initial vector can also be through peer-to-peer file sharing. Once the initial infection succeeds and the file infector is executed, its own propagation vectors are initiated ensuring not just replication in local, removable and network drives, but also in some cases placement of re-start mechanisms to ensure survival across reboots and effective network propagation.

Once the file infector is executed, it will initiate its propagation cycle. Depending on the way it manipulates the files it infects it can be classify into different categories:

- Inserting code into them: **Prepending**, **appending**, **mid-infectors** and **spread** across the structure. Once malicious code is inserted the header is modified as needed to ensure the inserted code is executed first.

- **Overwriting** infected files: a variety of the first type but where the original code is not respected. It helps to keep its presence covert by not increasing the file size.

- **Companion** viruses take advantage of the order of execution of files in Windows. Should the same file name exist with different extensions, .com, .exe and .bat, they will be executed in this order. They can also make very small changes in the names of the original files and take over their names.

- **Macro** viruses only affect macros within applications. Macros are designed to help automate tasks or modify standard commands within applications. When affected by a macro virus, the malicious code is executed when commands are invoked or simple when the applications are opened or closed, generally word processors, without the user knowledge.

- **Boot Sector** viruses overwrite or relocate the original code in the boot sector ensuring execution on every reboot.

Hardening actions

The hardening actions need to include general security practices in conjunction with the use of McAfee products to avoid being affected. They also need to be twofold to take into account possible first vectors of infection and the following internal spreading mechanisms.

- Known good backups: have a good backup policy that is enforced and that backups are regularly checked.
- Always ensure the files from external sources are virus checked by either VSE or one of the command line scanners prior to being executed in your environment
- Apply principle of least privilege when designing access control policies to enterprise resources. This will help minimize the impact of a file infector especially on most valuable assets.
- Use of administrative accounts only for tasks where they are required.
- Where possible set permissions in network shares as read only for normal users.
- Avoid being affected by the exploit of any known vulnerabilities either as initial introduction vector or aiding the propagation of the threat by ensuring all applications used are the latest versions and that they are regularly patched as soon as possible following vendors' patch release cycles.
- Make sure your organisation has a plan to deal with a possible incident. Handling file infector incidents require a structured approach to ensure prompt and effective detection and removal. 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 of 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 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.
- 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 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.

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