Technical Brief

Stopping Ransomware and Polymorphic Malware

McAfee® Application Control provides highly effective protection.

The recent surge in ransomware and polymorphic malware has motivated organizations to look for more robust protection. This technical brief discusses how McAfee Application Control can protect both servers and desktops from ransomware and zero-day malware.

Background

The biggest threat to businesses today is crypto ransomware, where critical data is encrypted so that users cannot access personal files and a ransom is demanded to provide access. Use of anonymous currency for payment, such as Bitcoin, makes it difficult to follow the money trail and track down criminals. Increasingly, cybercrime groups are devising ransomware schemes to make a quick profit. Easy availability of open source code and drag-and-drop platforms to develop ransomware have accelerated creation of new ransomware variants and help script novices create their own ransomware. Security experts' predictions that ransomware will wreak havoc on the critical infrastructure community in 2016 are already coming true.

Anatomy of Ransomware

Malware needs an attack vector to establish its presence on an endpoint. After presence is established, malware stays on the system until its task is accomplished. The attack vectors for ransomware are standard techniques used by other malware:

- Watering hole attack.
- Zero-day exploits.
- Spear-phishing campaigns using email.

After a successful exploit, ransomware drops and executes a malicious binary on the system. This binary then searches and encrypts valuable files, such as Microsoft Word documents, images, databases, and so on. Once files are encrypted, ransomware prompts the user for a ransom to be paid within 24 to 48 hours to decrypt the files, or they will be lost forever. If a data backup is unavailable, the victim must pay the ransom to recover personal files.

intel Security

Figure 1. CTB-Locker ransomware asking for ransom.

Ransomware attacks and their variants are rapidly evolving to counter preventive technologies for these reasons:

- Easy availability of malware kits that can be used to create new malware samples on demand.
- Use of known good generic interpreters to create cross-platform ransomware. For example, Ransom32 uses Nodejs with a JavaScript payload.
- Use of new techniques, such as encrypting the complete disk instead of selected files.

Preventing Ransomware Infection

After a successful exploit, a malware payload is dropped on the system. Typically, cutting-edge malware like ransomware are polymorphic by design which allows it to easily bypass traditional signature-based security based on file hash. Therefore, relying on file hash will not protect the system, but systems can be protected by blocking execution of unknown executables.

Ransomware can be prevented by creating a list of trusted applications and allowing only these to run. This technology is exemplified by McAfee Application Control, which has a two-layered defense mechanism:

- **Whitelisting:** Prevents execution of binaries coming from untrusted source. This protects against social attacks, such as spear phishing, where a user manually downloads malware and executes it or where a payload is dropped on a system after a user visits a compromised site or opens a compromised file.
- **Memory protection:** Protects from memory exploits used to drop the malware binary. This helps provide protection from zero-day exploits.

McAfee Application Control stops file-based malware from execution and has a configurable framework to prevent execution of scripts by interpreters such as Python, Perl, Ruby, and others. New binaries or scripts are prevented from execution unless they arrive on the system through a trusted mechanism.

McAfee Application Control blocks ransomware by blocking a memory exploit or execution of any new binary that enters the system through an untrusted mechanism. The same generic mechanism is also used to block all other types of file-based malware. Because McAfee Application Control does not depend on a signature, it is a reliable option to block file malware without daily signature-based updates. Using signature-less technology, McAfee Application Control can also block malware if it is polymorphic in nature, and it can also block advanced persistent threats.

How McAfee Application Control Works

During installation, McAfee Application Control scans the entire system to identify executables, such as .exes, installed applications, scripts, and other types. For security, these executables are whitelisted locally so that each system has its own unique local whitelist. Using this approach, McAfee Application Control can be easily deployed without interfering with business continuity.

Protection against new ransomware

When new ransomware enters the system and tries to execute to damage the system, it will be unable to do so. McAfee Application Control will automatically block execution without the need for any additional policy.

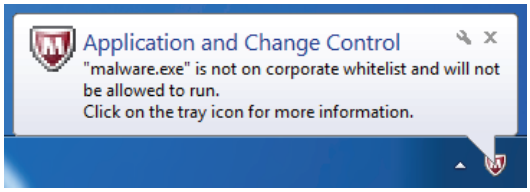


Figure 2. Ransomware execution is prevented.

Execution of ransomware is automatically blocked because it's not part of the local whitelist. The corresponding deny event will be reported locally to the user and centrally to the McAfee® ePolicy Orchestrator® (McAfee ePO™) software administrator. An event is generated on the McAfee ePO console.

Solidcore Events (Advance Filtered)

Event Generated Time	Event Name	Object Name	Reputation (at T	Process Name	Deny Reason
23-Aug-2016 17:47:34	EXECUTION_DENIED	C:\Users\Administrator\Desktop\malware.exe	Not Applicable	C:\Windows\explorer.exe	Local Whitelist- File not present in whitelist
23-Aug-2016 17:42:03	EXECUTION_DENIED	C:\Users\Administrator\Desktop\malware.exe	Not Applicable	C:\Windows\System32\cmd.exe	Local Whitelist- File not present in whitelist
23-Aug-2016 14:30:25	EXECUTION_DENIED	C:\Users\Administrator\Downloads\FramePkg.exe	Not Applicable	C:\Windows\explorer.exe	Local Whitelist- File not present in whitelist

Figure 3. Screen showing deny execution with malware name, process, and deny reason in McAfee ePO software.

As shown in Figure 3, ransomware execution is blocked with the reason “File not present in whitelist”.

Finding hidden malware (data at rest)

During installation, McAfee Application Control identifies executables and reports them back to McAfee ePO software as inventory items. On the McAfee ePO software inventory console, you can further analyze executables and view their reputation based on McAfee® Threat Intelligence Exchange and McAfee® Global Threat Intelligence. You can use hashing to find information about unknown binaries from other reputation sources as well. Even if you find any suspicious binaries, there is no need to take action. By default, McAfee Application Control will block it. If you want to create an explicit block rule, you can create a "Ban Application" control policy from McAfee ePO software.

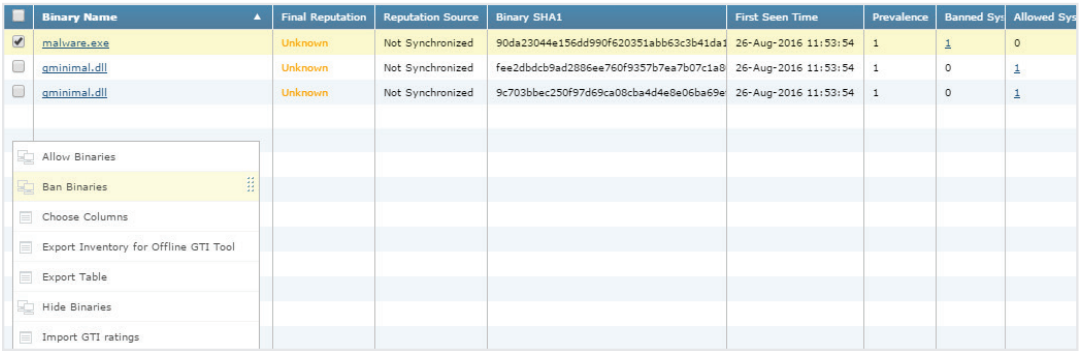


Figure 4. Screen showing suspicious ransomware present on the system.

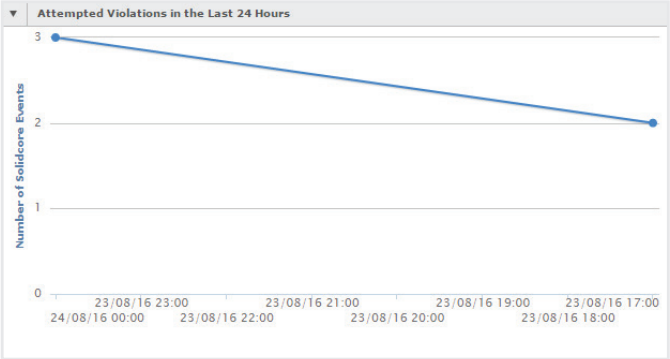
In "Application Inventory," you can review various details such as file location, number of system impacted, and more. You can easily learn more about unknown files by just clicking on the file name in "Application Inventory" or on the events page, as shown in Figure 5.

Monitoring Events Details	
Monitoring Events Information	
Agent GUID	982AF22A-6910-11E6-06BB-B8AC6F89D7FA
Deny Reason	Local Whitelist- File not present in whitelist
Description	Application Control blocked this file because it is not whitelisted. To execute this file, add the file to the whitelist.
Event Display Name	Execution Denied
Event File Name	C:\Users\Administrator\Desktop\malware.exe
Event Generated Time	23/08/16 17:47:34
Event ID	20720
Event Name	EXECUTION_DENIED
Event Sequence Number	34
File MD5	9ee9c2257e7d3e68a1c69208735dd929
File SHA1	90da23044e156dd990f620351abb63c3b41da124
File Type	pe32
Generated by an Updater	No
Generated in an Update Window	No
Object Name	C:\Users\Administrator\Desktop\malware.exe
Parent Process Name	C:\Windows\System32\userinit.exe
Performed By	dinesh-PC\Administrator
Process ID	Not Available
Process Name	C:\Windows\explorer.exe
Reconciliation Status	Not yet Reconciled
Reconciliation Ticket	Not Applicable
Reputation (at Time of Execution)	Not Applicable
Severity	3
System Name	DINESH-PC
User Name	dinesh-PC\Administrator

Figure 5. Screen showing event details with additional information, such as SHA1 and parent process.

Using dashboards and reports

McAfee Application Control offers detailed reporting capabilities to quickly identify malware/ransomware in your environment. You can use pre-defined queries, such as violations in the past 24 hours, list of infected systems, and so on. Alternatively, you can define custom queries to suit your needs.



System Name->Event Display Name	Number of Solidcore Events
DINESH-PC	**44**
Installation Allowed	19
Execution Denied	8
File Write Denied	7
Registry Deleted	4
Registry Write Denied	3
Installation Denied	1
Registry Created	1
Registry Modified	1

Figure 6. Built-in dashboard for tracking.

You can easily identify all infected systems and create a global ban policy to block execution of the malware, and you can permanently remove the malware by deleting the file from the system.

Learn More

For more information on McAfee Application Control, visit http://www.mcafee.com/in/products/application-control.aspx. For additional information on installation and configuration, see the Install Guide and Best Practices Guide.

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