SOLUTION BRIEF

Protecting Against WannaCry and Petya

A large cyberattack, based on the WannaCry malware family, was launched in May 2017. WannaCry exploited a vulnerability in some versions of the Microsoft Windows. It is estimated that more than 300,000 computers in 150 countries were infected during the main attack, each demanding a ransom payment.

The initial attack vector is unclear, but an aggressive worm helps spread the malware. A critical patch was released by Microsoft in March to remove the underlying vulnerability in supported versions of Windows, but many organizations had not yet applied this patch.

Computers running unsupported versions of Windows (Windows XP, Windows Server 2003) did not have an available patch. Microsoft released a special security patch for Windows XP and Windows Server 2003 after the WannaCry attack.

About six weeks later, another cyberattack exploited the same vulnerability. Petya did not have as much impact as WannaCry, but these two attacks exposed the continued use of old and unsupported operating systems in critical areas and laid bare lax patch-update processes followed by some organizations. A thorough analysis of these attacks is detailed in the *McAfee Labs Threats Report: September 2017.*

Policies and procedures to protect against WannaCry and Petya

- **Back up files:** The most effective procedure to thwart ransomware is to regularly back up data files and verify network restore procedures.
- **Educate network users:** Like other malware, ransomware often infects a system through phishing attacks using email attachments, downloads, or cross-scripting web browsing.
- **Monitor and inspect network traffic:** This step will help identify abnormal traffic associated with ransomware behaviors.
- **Use threat intelligence data feeds:** This practice may help detect threats faster.
- **Restrict code execution:** Ransomware is often designed to run under well-known operating system folders. If the ransomware cannot reach these folders due to access control, malicious data encryption can be blocked.
- **Restrict administrative and system access:** Some types of ransomware are designed to use default accounts to perform their operations. With this type of ransomware, renaming default user accounts and disabling all unnecessary privileged and nonprivileged accounts can create extra protection.
- **Remove local administrative rights:** Prevent ransomware from running on a local system and stop its spread based on administrative privileges. The removal of local administrative rights also blocks access to any critical system resources and files that ransomware targets for encryption.
- **Other permission-related practices:** Consider restricting user-write capabilities, preventing execution from user directories, whitelisting applications, and limiting access to network storage or shares. Some ransomware requires write access to specific file paths to install or execute. Limiting writes permission to a small number of directories (for example, My Documents and My Downloads) may halt some ransomware variants. Ransomware executables can also be stopped by the removal of execution permission from those directories. Many organizations use a limited set of applications to conduct business. Nonwhitelisted applications, including ransomware, can be blocked from executing by maintaining a whitelist-only policy for applications. One further permissions practice is to require a login at shared resources such as network folders.
- **Maintain and update software:** Another important basic rule for protecting against ransomware is to maintain and update software, in particular operating system patches, as well as security and antimalware software.

It is extremely important to reduce the attack surface, especially from phishing, which is one of the most popular techniques used by ransomware. For email consider the following practices:

- **Filter email content:** Securing email communications is a key procedure. The possibility of a successful attack will be reduced if network users receive fewer spam emails that might contain potentially malicious and unsafe content.
- **Block attachments:** Attachment inspection is an important step in reducing the attack surface. Ransomware is often delivered as an executable attachment. Enact a policy that some file extensions cannot be sent by email. Those attachments could be analyzed with a sandboxing solution and could be removed by the email security appliance.

How McAfee products can protect against WannaCry

McAfee Network Security Platform (NSP)

McAfee NSP quickly responds to prevent exploits and protect assets within networks. The McAfee NSP team works diligently to develop and deploy user-defined signatures (UDS) for critical matters. Within a 24-hour period during the WannaCry attack, McAfee created and uploaded several UDS for customers to deploy on their network sensors. In this case, the UDS explicitly targeted the exploit tools EternalBlue, Eternal Romance SMB Remote Code Execution, and DoublePulsar. McAfee also released related indicators of compromise that could be added to a blacklist to block potential threats associated with the original Trojan.

Read more about NSP signatures here.

McAfee Host Intrusion Prevention (HIPS)

McAfee HIPS 8.0 with NIPS Signature 6095 provides protection against all four of the known variants of WannaCry. Refer to KB89335 for the latest information on these configurations.

Custom Sig #1: WannaCry Registry Blocking Rule
Use Standard Subrule
Rule Type = Registry
Operations = Create, Modify, Change Permissions
Parameters, include Registry Key
Registry Key = \REGISTRY\MACHINE\SOFTWARE\WanaCrypt0r
Executable = *

Custom Sig #2: WannaCry File/Folder Blocking Rule
Use Standard Subrule
Rule Type = Files
Operations = Create, Write, Rename, Change read-only/hidden attributes, Parameters include Files
Files = *.wnry
Executable = *

McAfee Endpoint Protection (ENS) and McAfee VirusScan Enterprise (VSE) Adaptive Threat Protection configurations

McAfee Endpoint Security 10.5—Adaptive Threat Protection

McAfee Endpoint Security 10.5 with Adaptive Threat Protection Real Protect & Dynamic Application Containment (DAC) provides protection against known or unknown exploits for WannaCry.

- Configure the following setting in the Adaptive Threat Protection—Options Policy:
  - Rule Assignment = Security. (The default setting is Balanced.)
- Configure the following rules in the Adaptive Threat Protection—Dynamic Application Containment policy:
  - Dynamic Application Containment—Containment Rules

Refer to KB87843: List of and best practices for ENS Dynamic Application Containment Rules and set the recommended DAC rules to "Block" as prescribed.

McAfee Endpoint Security 10.1, 10.2, and 10.5—Threat Prevention

McAfee Endpoint Security 10.x Threat Prevention with AMCore content Version 2978 or later provides protection against all four of the currently known variants of WannaCry.

McAfee VirusScan Enterprise 8.8

McAfee VirusScan Enterprise 8.8 with DAT content 8527 or later provides protection against all four of the currently known variants of WannaCry.

McAfee Endpoint Security (ENS) Protection and McAfee VirusScan Enterprise (VSE) Access Protection proactive measures

The McAfee ENS and McAfee VSE Access Protection rules will prevent the creation of the .wnry file. This rule stops the encryption routine, which creates encrypted files that contain a .wncryt, .wncry, or .wcry extension. By implementing the block against .wnry files, other blocks are not necessary for the encrypted file types.

Read more about McAfee VSE Access Protection Rules configuration.

Configure the endpoint security system to protect against file encryption from WannaCry (and future unknown variants)

Customers not using McAfee ENS Adaptive Threat Protection security may not have McAfee-defined content protection against not yet released variants. We recommend configuring repository update tasks with a minimal refresh interval to ensure new content is applied when it is released by McAfee.

Additional protections against the encryption routine can be configured using McAfee VSE/ENS Access Protection rules, or McAfee HIPS custom rules. Refer to KB89335 for the latest information on these configurations.

McAfee VSE and McAfee ENS Access Protection rules, and McAfee HIPS customer signatures will prevent the creation of the .wnry file.

The rules prevent the encryption routine, which creates encrypted files that contain a .wncryt, .wncry, or .wcry extension.

By implementing the block against .wnry, other blocks are not necessary for the encrypted file types.

Refer to KB89335 (accessible to McAfee registered customers) for the latest information on these configurations.

McAfee Advanced Threat Defense (ATD)

McAfee ATD machine learning can convict a sample on a "medium severity" analysis.

McAfee ATD has observed the following:

Behavior classification:

- Obfuscated file
- Spreading
- Exploitation through shellcode
- Network propagation

Dynamic analysis:

- Elicited ransomware behavior
- Encryption of files
- Created and executed suspicious scripting content
- Behavior such as a Trojan macro dropper

To date with WannaCry, McAfee ATD has observed 22 process operations, including five runtime DLLs, 58 file operations, registry modifications, file modifications, file creations (dll.exe), DLL injections, and 34 network operations.

McAfee Web Gateway (MWG)

McAfee Web Gateway (MWG) is a product family (appliance, cloud, and hybrid) of web proxies that provides immediate protection against WannaCry variants delivered through the web (HTTP/HTTPS) using multiple real-time scanning engines.

Known variants will be blocked by McAfee Global Threat Intelligence (GTI) reputation and antimalware scanning as web traffic is processed through the proxy.

The Gateway Anti-Malware (GAM) engine within MWG provides effective prevention of variants that have not yet been identified with a signature ("zero-day" threats) through its process of behavior emulation—conducted on files, HTML, and JavaScript. Emulators are regularly fed intelligence by machine learning models. GAM runs alongside GTI reputation and antimalware scanning as traffic is processed.

Coupling MWG with ATD allows for further inspection and an effective prevention and detection approach.

McAfee Threat Intelligence Exchange (TIE)

McAfee Threat Intelligence Exchange (TIE) further enhances a customer's security posture. With the ability to aggregate reputation verdicts from ENS, VSE, MWG, and NSP, TIE can quickly share reputation information related to WannaCry with any integrated vector. By providing the ability to use GTI for a global reputation query, TIE also enables integrated products to make an immediate decision prior to execution of the ransomware payload, leveraging the reputation cached in the TIE database.

As one endpoint protects, detects from any related variants, and updates the reputation score to TIE, this fully encompassing approach extends protection by disseminating this information to all endpoints integrated with TIE. This bidirectional sharing of threat intelligence is duplicated in capability with MWG and NSP. Thus, as the potential threat attempts to infiltrate through the network or web, MWG and NSP will provide protection and detection and share this intelligence with TIE to inoculate endpoints—immediately protecting the enterprise with no further execution of the convicted variant on a potential "patient zero" in the environment.

How McAfee products can protect against Petya

McAfee provides protection against the initial Petya attack in the form of advanced malware behavior analysis with Real Protect Cloud and Dynamic Neural Network (DNN) analysis techniques available in McAfee Advanced Threat Defense.

ATD 4.0 introduced a new detection capability using a multilayered, back-propagation neural network (DNN) leveraging semisupervised learning. DNN looks at certain features exercised by malware to come up with a positive or negative verdict to determine whether the code is malicious.

Whether in standalone mode or connected to McAfee endpoint or network sensors, ATD combines threat intelligence with sandbox behavior analysis and advanced machine learning to provide zero-day, adaptable protection. Real Protect, part of the Dynamic Endpoint solution, also uses machine learning and link analysis to protect against malware without signatures and provide rich intelligence to the Dynamic Endpoint and the rest of the McAfee ecosystem. Real Protect combined with Dynamic Application Containment provided early protection against Petya.

Multiple McAfee products provide additional protection to either contain the attack or prevent further execution.

McAfee Endpoint Security

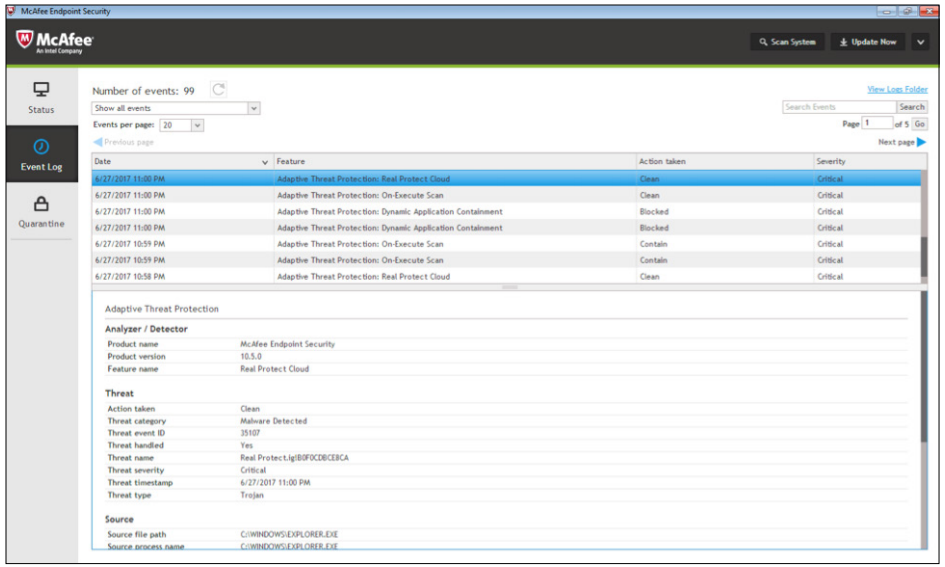
Threat Prevention

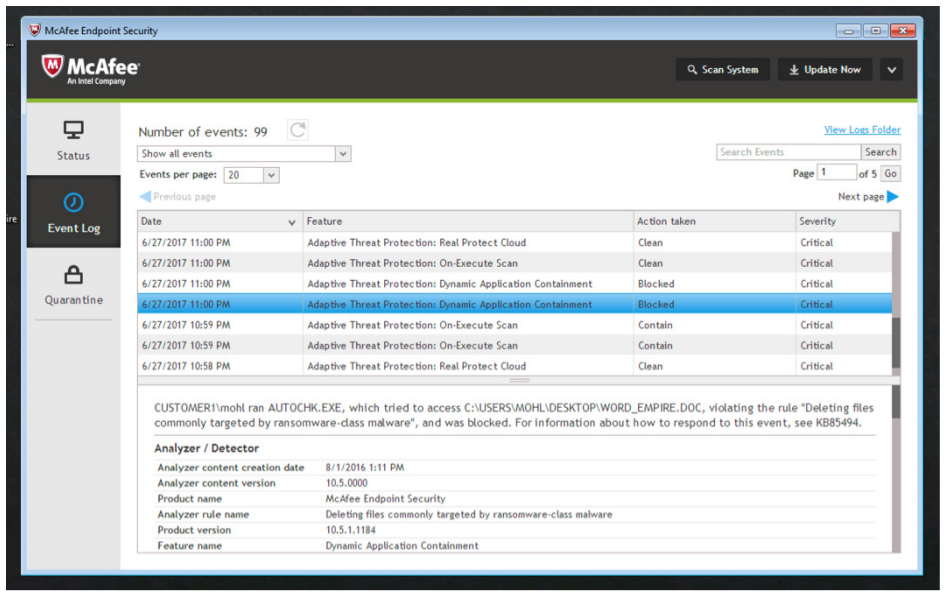
- McAfee Endpoint Security with McAfee Global Threat Intelligence and On Access Scan policy with the sensitivity level set to "Low" protect against known samples and variants.
- Learn more about recommended McAfee GTI file reputation settings in KB74983, with further information in KB53735.
- McAfee Threat Intelligence Exchange with GTI protects against known samples and variants.

Systems using McAfee ENS 10 are protected from known samples and variants with both signatures and threat intelligence.

Adaptive Threat Protection

- Adaptive Threat Protection (ATP), with rule assignment configured in "Balanced mode" (the default in the setting ATP\Options\Rule Assignment), will protect against both known and unknown variants of the Petya ransomware.
- The ATP module protects against this unknown threat with several layers of advanced protection and containment:
  - ATP Real Protect Static uses client-side pre-execution behavioral analysis to monitor unknown malicious threats before they launch.
  - ATP Real Protect Cloud uses cloud-assisted machine learning to identify and clean the threat, as shown at right above.
- ATP Dynamic Application Containment (DAC) successfully contains the threat and prevents any potential damage from occurring (DAC events noted at right below).





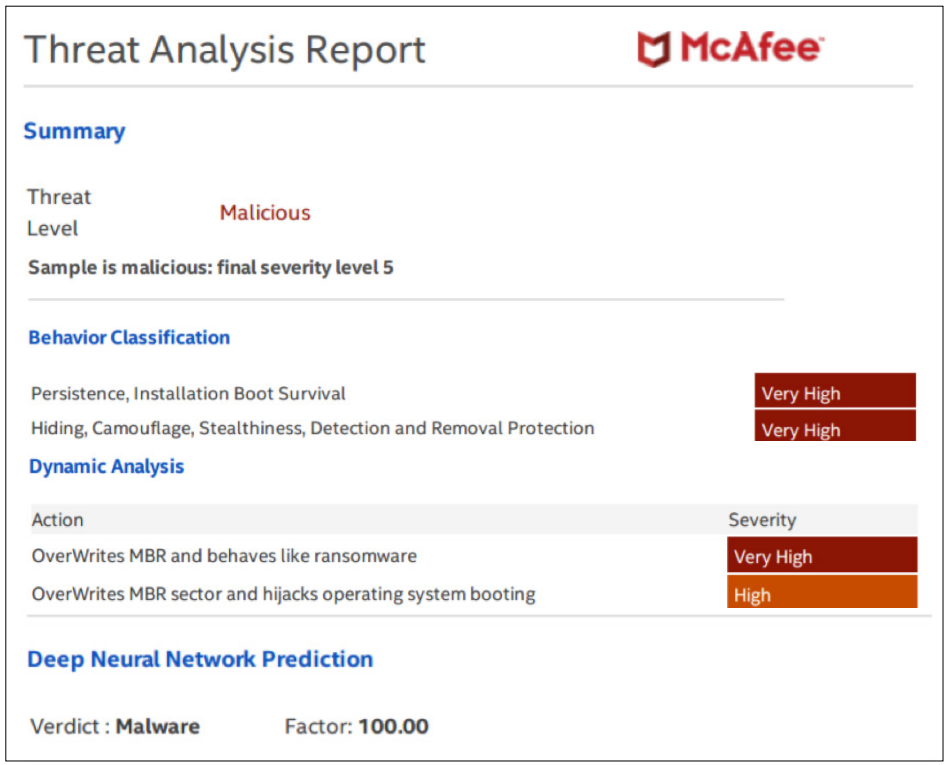
McAfee Advanced Threat Defense

- McAfee Advanced Threat Defense 4.0 with Deep Neural Network and Dynamic Sandbox identified the threat and proactively updated the cyber defense ecosystem. (See below.)

McAfee Enterprise Security Manager

McAfee Enterprise Security Manager (ESM) is a security information and event management solution that delivers actionable intelligence and integrations to prioritize, investigate, and respond to threats. The Suspicious Activity Content Pack and Exploit Content Pack for McAfee ESM have been updated with WannaCry-specific rules, alarms, and watch lists so you can find and identify possible infections. These updates will also help protect against Petya. Both packs are available for download in the McAfee ESM console at no cost. Default correlation rules in McAfee ESM can also alert users of increased levels of horizontal SMB scans.

Similar to WannaCry, the Petya attack presents a learning opportunity for security operations center analysts. Understanding and automating these best practices will help security practitioners handle the next fast-moving attack.



McAfee Web Gateway

McAfee Web Gateway is a product family (appliance, cloud, and hybrid) of web proxies that provides another potential layer of protection against Petya variants delivered through the web (HTTP/HTTPS) using multiple real-time scanning engines. Known variants will be blocked by GTI reputation and antimalware scanning as web traffic is processed through the proxy.

The Gateway Anti-Malware engine within MWG provides effective prevention of "zero-day" variants that have not yet been identified with a signature through GAM's process of behavior emulation—conducted on files, HTML, and JavaScript. Emulators are regularly fed intelligence by machine learning models. GAM runs alongside GTI reputation and antimalware scanning as traffic is processed.

Coupling MWG with ATD allows for further inspection and an effective prevention and detection approach.

McAfee products using DAT files

McAfee released an Extra.DAT to include coverage for Petya. McAfee also released an emergency DAT to include coverage for this threat. Subsequent DATs will include coverage. The latest DAT files are available via Knowledge Center article KB89540.

For Further Reading

Frequently updated technical details can be found in the McAfee Knowledge Center articles KB89335, KB87843, KB74983, KB53735, and KB89540.

McAfee
Together is power.

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