McAfee
Together is power.

Schutz vor WannaCry und Petya

Ein Cyber-Großangriff, der auf der WannaCry-Malware-Familie basiert, wurde im Mai 2017 gestartet. WannaCry nutzte eine Schwachstelle aus, die in einigen Microsoft Windows-Versionen enthalten ist. Laut Schätzungen wurden in der Hauptangriffsphase mehr als 300.000 Computer in über 150 Ländern infiziert, und bei allen wurde Lösegeld gefordert.

Der ursprüngliche Angriffsvektor ist unklar, doch bekannt ist, dass ein aggressiver Wurm für die Malware-Verbreitung verantwortlich war. Bereits im März wurde von Microsoft ein kritischer Patch veröffentlicht, der die zugrundeliegende Sicherheitslücke in den unterstützten Windows-Versionen schloss, doch viele Unternehmen hatten diesen Patch noch nicht installiert.

Für Computer mit nicht unterstützten Windows-Versionen (Windows XP und Windows Server 2003) stand kein Patch zur Verfügung. Nach dem WannaCry-Angriff veröffentlichte Microsoft einen speziellen Sicherheits-Patch für Windows XP und Windows Server 2003.

Etwa sechs Wochen später nutzte ein weiterer Cyber-Angriff dieselbe Schwachstelle aus. Petya hatte keine so großen Auswirkungen wie WannaCry, aber diese beiden Angriffe zeigten, dass alte und nicht unterstützte Betriebssysteme weiterhin in kritischen Bereichen eingesetzt werden und in einigen Unternehmen laxe Patch-Update-Prozesse die Regel sind. Weitere Informationen zu diesen Angriffen finden Sie im *McAfee Labs Threats-Report vom September 2017*.

Richtlinien und Vorgehensweisen zum Schutz vor WannaCry und Petya

- **Dateien sichern:** Den wirksamsten Schutz vor Ransomware bieten die regelmäßige Sicherung von Datendateien und die Überprüfung der Prozesse zur Netzwerk-Wiederherstellung.
- **Netzwerkbenutzer sensibilisieren:** Wie andere Malware infiziert auch Ransomware Systeme häufig über Phishing-Angriffe mithilfe von E-Mail-Anhängen, Downloads oder Cross-Site Scripting beim Surfen im Internet.
- **Netzwerkverkehr überwachen und inspizieren:** Hierdurch können Sie ungewöhnlichen Netzwerkverkehr im Zusammenhang mit Ransomware-Verhalten identifizieren.
- **Bedrohungsdaten-Feeds nutzen:** Diese Maßnahme ermöglicht die schnellere Erkennung von Bedrohungen.
- **Code-Ausführung einschränken:** Ransomware ist oft so konzipiert, dass sie unter bekannten Betriebssystemordnern ausgeführt wird. Wenn die Ransomware aufgrund der Zugriffssteuerung keinen Zugriff auf diese Ordner erhält, kann die böswillige Datenverschlüsselung blockiert werden.
- **Administrator- und Systemzugriff einschränken:** Einige Arten von Ransomware sind so konzipiert, dass sie ihre Operationen mithilfe von Standardkonten ausführen. In diesen Fällen kann das Umbenennen von Standardbenutzerkonten und Deaktivieren aller nicht erforderlichen privilegierten und nicht privilegierten Konten zusätzlichen Schutz bieten.
- **Lokale Administratorrechte entziehen:** Verhindern Sie die Ausführung von Ransomware auf einem lokalen System, und stoppen Sie ihre Verbreitung über Administratorberechtigungen. Durch das Entziehen lokaler Administratorrechte blockieren Sie auch den Zugriff auf alle kritischen Systemressourcen und Dateien, die Ransomware mit einer Verschlüsselung angreift.
- **Weitere berechtigungsbezogene Maßnahmen:** Ziehen Sie das Einschränken der Schreibberechtigungen von Benutzern, das Verhindern der Ausführung aus Benutzerverzeichnissen heraus, das Whitelisting von Anwendungen und das Beschränken des Zugriffs auf Netzwerkspeicher oder -freigaben in Betracht. Manche Ransomware benötigt für die Installation oder Ausführung Schreibzugriff auf spezielle Dateipfade. Die Beschränkung des Schreibzugriffs auf eine kleine Anzahl von Verzeichnissen (z. B. „Eigene Dokumente“ und „Downloads“) könnte den Erfolg einiger Ransomware-Varianten verhindern. Darüber hinaus können Sie ausführbare Ransomware-Dateien stoppen, indem Sie diesen Verzeichnissen die Ausführungsberechtigung entziehen. Viele Unternehmen nutzen eine begrenzte Gruppe von Anwendungen für ihre Geschäftstätigkeit. Anwendungen, die nicht in einer Whitelist aufgeführt sind (einschließlich Ransomware), können mithilfe einer entsprechenden Richtlinie von der Ausführung ausgeschlossen werden. Eine weitere Maßnahme im Zusammenhang mit Berechtigungen besteht in einer obligatorischen Anmeldung für freigegebene Ressourcen wie Netzwerkordner.
- **Software warten und aktualisieren:** Eine weitere wichtige Grundregel zum Schutz vor Ransomware ist die regelmäßige Wartung und Aktualisierung der Software, insbesondere durch Betriebssystem-Patches, sowie der Einsatz von Sicherheits- und Malware-Schutz-Software.

Dabei kommt es darauf an, die Angriffsfläche zu verkleinern - insbesondere für Phishing, eine der beliebtesten Techniken bei Ransomware. Halten Sie sich in Bezug auf E-Mails an folgende Regeln:

- **E-Mail-Inhalt filtern:** Die Absicherung der E-Mail-Kommunikation ist von entscheidender Bedeutung. Wenn Netzwerkbenutzer weniger Spam-E-Mails mit potenziell böswilligem und unsicherem Inhalt erhalten, sind erfolgreiche Angriffe unwahrscheinlicher.
- **Anhänge blockieren:** Das Prüfen von Anhängen ist ein wichtiger Schritt zur Verkleinerung der Angriffsfläche. Ransomware wird oft als ausführbarer Anhang verbreitet. Aktivieren Sie eine Richtlinie, die durchsetzt, dass bestimmte Dateierweiterungen nicht per E-Mail gesendet werden können. Diese Anhänge könnten mit einer Sandbox-Lösung analysiert und von der E-Mail-Sicherheits-Appliance entfernt werden.

So schützen McAfee-Produkte vor WannaCry

McAfee Network Security Platform (NSP)

McAfee NSP reagiert schnell, um Ausnutzungen zu vermeiden und Netzwerkressourcen zu schützen. Das McAfee NSP-Team ist intensiv damit beschäftigt, benutzerdefinierte Signaturen für kritische Probleme zu entwickeln und bereitzustellen. Innerhalb von 24 Stunden nach Beginn des WannaCry-Angriffs erstellte sowie veröffentlichte McAfee mehrere benutzerdefinierte Signaturen, und stellte diese Kunden für deren Netzwerksensoren zur Verfügung. In diesem Fall bezogen sich die Signaturen explizit auf die Exploit-Kits EternalBlue, Eternal Romance SMB Remote Code Execution und DoublePulsar. McAfee veröffentlichte zudem entsprechende Kompromittierungsindikatoren zur Ergänzung der Blacklist, damit potenzielle, mit dem ursprünglichen Trojaner zusammenhängende Bedrohungen blockiert werden.

Weitere Informationen zu NSP-Signaturen finden Sie hier.

McAfee Host Intrusion Prevention (HIPS)

McAfee HIPS 8.0 mit NIPS-Signatur 6095 schützt vor allen vier bekannten WannaCry-Varianten. Die neuesten Informationen zu diesen Konfigurationen finden Sie unter KB89335.

Benutzerdefinierte Signatur 1: WannaCry-Registrierungsblockierungsregel
Standard-Unterregel verwenden
Regeltyp = Registrierung
Prozesse = Berechtigungsparameter erstellen, anpassen, ändern; einschließlich Registrierungsschlüssel
Registrierungsschlüssel = \REGISTRY\MACHINE\SOFTWARE\WanaCrypt0r
Ausführbare Datei = *

Benutzerdefinierte Signatur 2: WannaCry-Datei/Ordner-Blockierungsregel
Standard-Unterregel verwenden
Regeltyp = Dateien
Prozesse = Schreibgeschützte/verborgene Attribute erstellen, schreiben, umbenennen, ändern; Parameter umfassen Dateien
Dateien = *.wnry
Ausführbare Datei = *

Konfigurationen des Moduls Adaptiver Bedrohungsschutz für McAfee Endpoint Protection (ENS) und McAfee VirusScan Enterprise (VSE)

McAfee Endpoint Security 10.5 – Adaptiver Bedrohungsschutz

McAfee Endpoint Security 10.5 mit dem Modul Adaptiver Bedrohungsschutz und den Funktionen Real Protect sowie Dynamische Eindämmung von Anwendungsprozessen (Dynamic Application Containment, DAC) schützt vor bekannten sowie unbekannten Exploits für WannaCry.

- Konfigurieren Sie im Modul Adaptiver Bedrohungsschutz die folgende Einstellung in der Optionsrichtlinie:
  - Regelzuweisung = Sicherheit (Die Standardeinstellung lautet „Ausgleich“.)
- Konfigurieren Sie im Modul Adaptiver Bedrohungsschutz die folgenden Regeln für die dynamische Eindämmung von Anwendungsprozessen:
  - Dynamische Anwendungsbeschränkung – Einschlussregeln

Weitere Informationen finden Sie unter KB87843: List of and best practices for ENS Dynamic Application Containment Rules (Liste der im ENS-Modul dynamische Anwendungsbeschränkung enthaltenen Regeln und empfohlene Vorgehensweisen). Legen Sie für die empfohlenen DAC-Regeln wie oben beschrieben die Einstellung „Blockieren“ fest.

McAfee Endpoint Security 10.1, 10.2 und 10.5 – Bedrohungsschutz-Modul

Das Modul Bedrohungsschutz von McAfee Endpoint Security 10.x mit AMCore-Inhalt Version 2978 oder höher bietet Schutz vor allen vier derzeit bekannten WannaCry-Varianten.

McAfee VirusScan Enterprise 8.8

McAfee VirusScan Enterprise 8.8 mit DAT-Datei 8527 oder höher bietet Schutz vor allen vier derzeit bekannten WannaCry-Varianten.

Proaktive Maßnahmen mit McAfee Endpoint Security (ENS)-Schutz und McAfee VirusScan Enterprise (VSE)-Zugriffsschutz

Die Zugriffsschutzregeln von McAfee ENS und McAfee VSE verhindern die Erstellung der .wnry-Datei. Diese Regel stoppt die Verschlüsselungsroutine, mit der verschlüsselte Dateien mit den Erweiterungen .wncryt, .wncry oder .wcry erstellt werden. Durch die Blockierung von .wnry-Dateien sind für die verschlüsselten Dateitypen keine anderen Blockierungen erforderlich.

Weitere Informationen zur Konfiguration von McAfee VSE-Zugriffsschutzregeln.

Konfigurieren Sie das Endgerätesicherheitssystem so, dass Dateiverschlüsselungen durch WannaCry (sowie zukünftige, bislang unbekannte Varianten) verhindert werden.

Kunden, die das Modul Adaptiver Bedrohungsschutz von McAfee ENS nicht verwenden, verfügen möglicherweise nicht über von McAfee definierten Inhaltsschutz vor noch nicht veröffentlichten Varianten. Wir empfehlen, Tasks zur Repository-Aktualisierung mit möglichst kurzen Aktualisierungsintervallen zu konfigurieren, damit neue Inhalte nach der Veröffentlichung durch McAfee sofort angewendet werden.

Zusätzlichen Schutz vor Verschlüsselungsroutinen erzielen Sie mit der Konfiguration von McAfee VSE/ENS-Zugriffsschutzregeln oder benutzerdefinierten Regeln in McAfee HIPS. Die neuesten Informationen zu diesen Konfigurationen finden Sie unter KB89335.

Die Zugriffsschutzregeln von McAfee ENS und McAfee VSE sowie die benutzerdefinierten Signaturen von McAfee HIPS verhindern die Erstellung der .wnry-Datei.

Diese Regeln stoppen die Verschlüsselungsroutine, mit der verschlüsselte Dateien mit den Erweiterungen .wncryt, .wncry oder .wcry erstellt werden.

Durch die Blockierung von .wnry-Dateien sind für die verschlüsselten Dateitypen keine anderen Blockierungen erforderlich.

Die neuesten Informationen zu diesen Konfigurationen finden Sie unter KB89335 (für registrierte McAfee-Kunden verfügbar).

McAfee Advanced Threat Defense (ATD)

Die Machine Learning-Komponente von McAfee ATD kann eine Probe mit einer Analyse mit „mittlerem Schweregrad“ als gefährlich erkennen.

Dabei analysiert McAfee ATD Folgendes:

Verhaltensklassifizierung:

- Verschleierte Datei
- Ausbreitung
- Ausnutzung über Shellcode
- Ausbreitung im Netzwerk

Dynamische Analyse:

- Ransomware-Verhalten festgestellt
- Verschlüsselung von Dateien
- Verdächtiger Skriptinhalt erstellt und ausgeführt
- Verhalten wie bei einem Makro-Dropper-Trojaner

Bisher hat McAfee ATD in Bezug auf WannaCry 22 Prozesse festgestellt, einschließlich 5 Laufzeit-DLLs, 58 Dateioperationen, Registrierungsänderungen, Dateiänderungen, Dateierstellungen (dll.exe), DLL-Injektionen sowie 34 Netzwerkprozesse.

McAfee Web Gateway (MWG)

Bei McAfee Web Gateway (MWG) handelt es sich um eine Produktfamilie (Appliance-, Cloud- und Hybridvariante) von Web-Proxys, die mithilfe mehrerer Echtzeit-Scan-Module sofort vor WannaCry-Varianten, die über das Web (HTTP/HTTPS) übertragen werden, schützen.

Bekannte Varianten werden basierend auf Reputationsinformationen von McAfee Global Threat Intelligence (GTI) blockiert, während bei der Verarbeitung des Web-Datenverkehrs über den Proxy Malware-Schutz-Scans durchgeführt werden.

Die Gateway Anti-Malware (GAM) Engine von MWG blockiert effektiv Varianten, die bisher noch nicht mit einer Signatur identifiziert werden können (sogenannte Zero-Day-Bedrohungen). Hierfür wird das Verhalten anhand von Dateien, HTML und JavaScript emuliert. Die Emulatoren erhalten regelmäßig aktuelle Informationen von den Machine Learning-Modellen. GAM wird während der Datenverkehrverarbeitung parallel zur GTI-Reputation und den Malware-Schutz-Scans eingesetzt.

Aufgrund der Kombination von MWG und ATD können weitere Untersuchungen durchgeführt und ein effektiver Ansatz zur Blockierung sowie Erkennung von Bedrohungen umgesetzt werden.

McAfee Threat Intelligence Exchange (TIE)

McAfee Threat Intelligence Exchange (TIE) verbessert die Sicherheitslage von Unternehmen zusätzlich. TIE aggregiert die Reputationsdaten aus ENS, VSE, MWG und NSP und kann für WannaCry relevante Informationen schnell über alle integrierten Kanäle weitergeben. Da TIE über GTI weltweite Reputationsdaten abrufen kann, können integrierte Produkte sofort Entscheidungen treffen, bevor Ransomware-Schaddaten ausgeführt werden. Hierfür werden die Reputationsdaten in der TIE-Datenbank genutzt.

Während ein Endgerät alle relevanten Varianten erkennt und abwehrt sowie den Reputationsfaktor in TIE aktualisiert, erweitert dieser umfassende Ansatz den Schutz, indem diese Informationen an alle mit TIE integrierten Endgeräte verteilt werden. Die Wirksamkeit dieses bidirektionalen Austauschs von Bedrohungsdaten wird durch die in MWG und NSP enthaltenen Funktionen verdoppelt. Während die potenzielle Bedrohung versucht, das Netzwerk oder Web zu infiltrieren, bieten MWG und NSP Erkennung sowie Schutz und geben die Informationen an TIE weiter, um andere Endgeräte zu schützen. Auf diese Weise wird das gesamte Unternehmen sofort geschützt – und die neu erkannte Bedrohungsvariante kann auf keinem potenziellen „Patient Null“ im Unternehmen ausgeführt werden.

So schützen McAfee-Produkte vor Petya

McAfee bietet Schutz vor dem ursprünglichen Petya-Angriff in Form hochentwickelter Analysen von Malware-Verhalten. Hierfür kommen die in McAfee Advanced Threat Defense enthaltenen Analysetechniken von Real Protect Cloud und Dynamic Neural Network (DNN) zum Einsatz.

ATD 4.0 führt eine neue Erkennungsfunktion ein, die ein mehrschichtiges, neuronales Netzwerk mit Backpropagation für teilüberwachtes Lernen nutzt. DNN achtet auf typisches Malware-Verhalten, um eine Code-Probe als schädlich oder harmlos einzustufen.

Unabhängig davon, ob ATD eigenständig agiert oder mit McAfee-Endgeräte- bzw. Netzwerksensoren vernetzt ist, kann die Lösung Bedrohungsdaten mit Sandbox-Verhaltensanalysen sowie hochentwickeltem Machine Learning kombinieren und bietet auf diese Weise anpassbaren Zero-Day-Schutz. Die in der Dynamic Endpoint-Lösung enthaltene Funktion Real Protect verwendet ebenfalls Machine Learning sowie Link-Analysen. Real Protect kommt ohne Signaturen aus und liefert umfangreiche Informationen für Dynamic Endpoint sowie das restliche McAfee-Ökosystem. In Kombination mit der dynamischen Eindämmung von Anwendungsprozessen bot Real Protect bereits früh Schutz vor Petya.

Einige McAfee-Produkte bieten zusätzlichen Schutz, der Angriffe entweder eindämmen kann oder deren weitere Ausführung verhindert.

McAfee Endpoint Security

Bedrohungsschutz

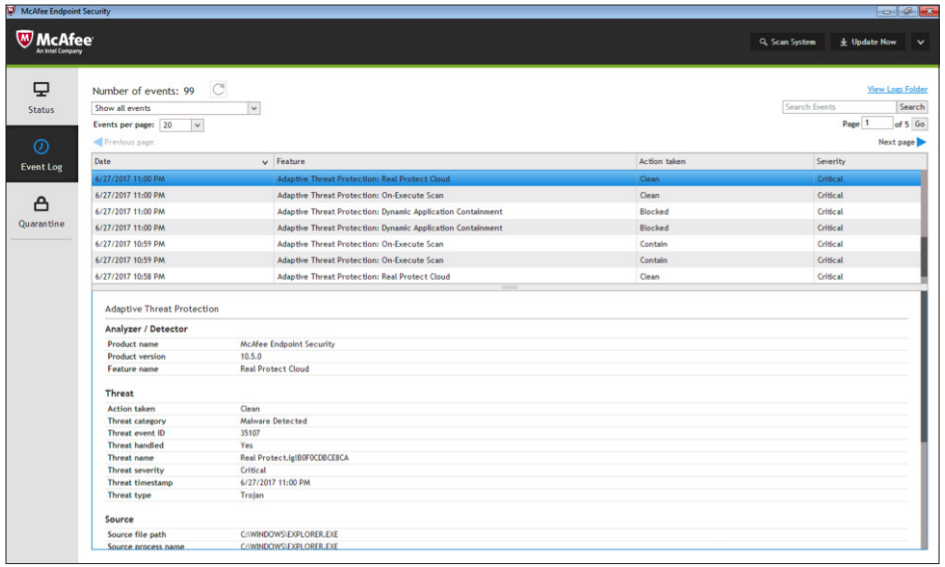
- McAfee Endpoint Security in Kombination mit McAfee Global Threat Intelligence und der aktivierten Richtlinie „On-Access-Scan“ (mit der Sensibilitätsstufe „Niedrig“) schützt vor bekannten Mustern und Varianten.

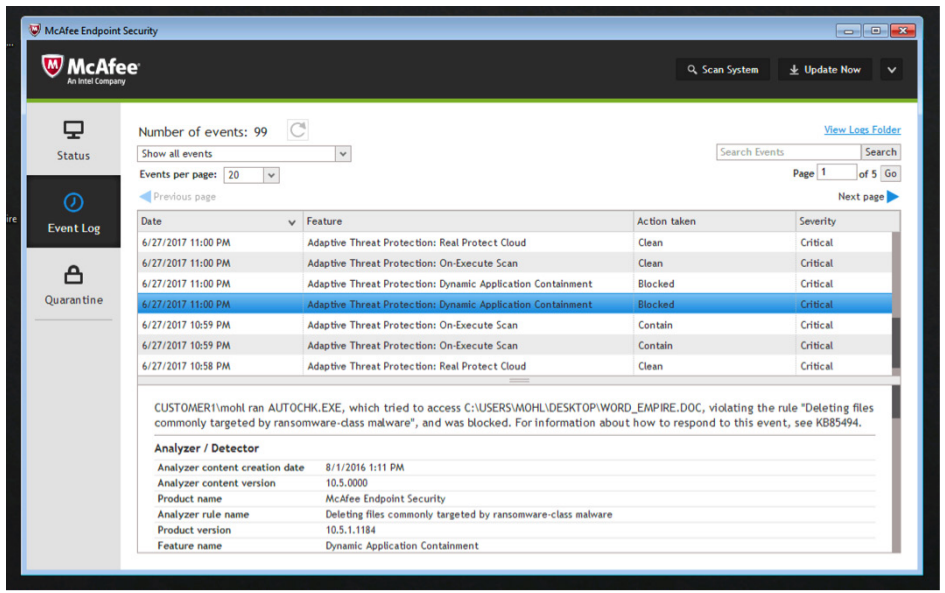
- Weitere Informationen zu empfohlenen Einstellungen für die Dateireputationsfunktion von McAfee GTI finden Sie im Wissensdatenbank-Artikel KB74983, weitere Details im Artikel KB53735.
- McAfee Threat Intelligence Exchange mit GTI schützt vor bekannten Mustern und Varianten.

Systeme, die McAfee ENS 10 verwenden, sind dank Signaturen und Bedrohungsdaten vor bekannten Mustern und Varianten geschützt.

Adaptiver Bedrohungsschutz

- Wenn im Modul Adaptiver Bedrohungsschutz (ATP) die Regelzuweisung im Modus „Ausgleich“ ausgeführt wird (der Standardeinstellung unter „ATP\Optionen\ Regelzuweisung“), sind die Systeme vor bekannten sowie unbekannten Varianten der Ransomware Petya geschützt.
- Das Modul ATP schützt dank mehrerer hochentwickelter Schutz- und Eindämmungsfunktionen vor unbekannten Bedrohungen:
  - ATP Real Protect Static verwendet Client-seitige Verhaltensanalysen noch vor der Ausführung, um unbekannte Bedrohungen zu erkennen.
  - ATP Real Protect Cloud verwendet Cloud-gestütztes Machine Learning, um die Bedrohung zu identifizieren und zu beseitigen (siehe Abbildung rechts oben).
- Die ATP-Funktion zur dynamischen Eindämmung von Anwendungsprozessen (DAC) dämmt die Bedrohung erfolgreich ein und verhindert so potenzielle Schäden (DAC-Ereignisse siehe Abbildung rechts unten).



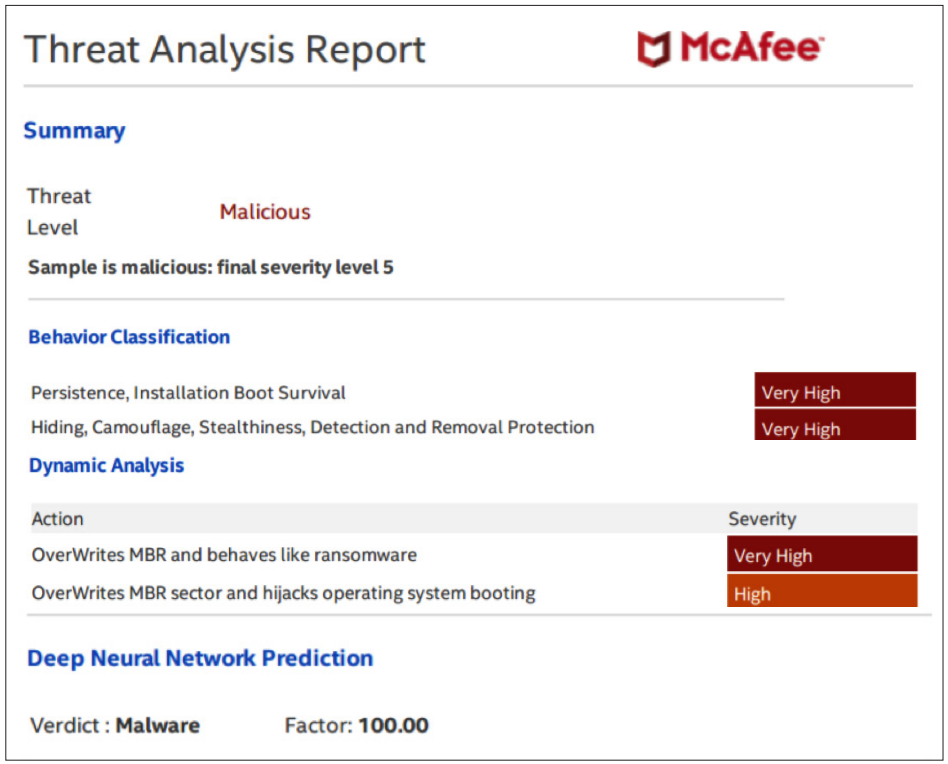


McAfee Advanced Threat Defense

- McAfee Advanced Threat Defense 4.0 identifiziert Bedrohungen mithilfe eines neuralen Netzwerks für tiefgreifendes Lernen und einer Funktion zur dynamischen Sandbox-Analyse. Die Ergebnisse werden proaktiv über das Ökosystem verteilt, um vor Cyber-Angriffen zu schützen (siehe Abbildung unten).

McAfee Enterprise Security Manager

McAfee Enterprise Security Manager (ESM) ist eine Lösung für Sicherheitsinformations- und Ereignis-Management, die handlungsrelevante Informationen und Integrationen zur Priorisierung, Untersuchung und Abwehr von Bedrohungen bietet. Das Suspicious Activity Content Pack und das Exploit Content Pack für McAfee ESM wurden aktualisiert und enthalten nun WannaCry-spezifische Regeln, Warnmeldungen sowie Watchlists, damit Sie potenzielle Infektionen erkennen und identifizieren können. Diese Aktualisierungen helfen auch beim Schutz vor Petya. Beide Pakete können kostenlos über die McAfee ESM-Konsole heruntergeladen werden. Standard-Korrelationsregeln in McAfee ESM können Benutzer ebenfalls warnen, wenn bei horizontalen SMB-Scans erhöhte Werte festgestellt werden.



Ähnlich wie WannaCry bietet der Petya-Angriff eine Gelegenheit für die Analysten von Sicherheitskontrollzentren, eine Lektion für die Zukunft zu lernen. Wenn die Sicherheitsverantwortlichen diese empfohlenen Vorgehensweisen verstehen und automatisieren, können sie die nächste Angriffswelle schneller abwehren.

McAfee Web Gateway

Bei McAfee Web Gateway (MWG) handelt es sich um eine Produktfamilie (Appliance-, Cloud- und Hybridvariante) von Web-Proxys, die mithilfe mehrerer Echtzeit-Scan-Module eine zusätzliche Schutzebene bietet und so vor Petya-Varianten schützt, die über das Web (HTTP/HTTPS) übertragen werden. Bekannte Varianten werden basierend auf Reputationsinformationen von GTI blockiert, während bei der Verarbeitung des Web-Datenverkehrs über den Proxy Malware-Schutz-Scans durchgeführt werden.

Die Gateway Anti-Malware Engine von MWG blockiert effektiv Zero-Day-Varianten, die bisher noch nicht mit einer Signatur identifiziert werden können. Hierfür wird das Verhalten anhand von Dateien, HTML und JavaScript emuliert. Die Emulatoren erhalten regelmäßig aktuelle Informationen von den Machine Learning-Modellen. GAM wird während der Datenverkehrverarbeitung parallel zur GTI-Reputation und den Malware-Schutz-Scans eingesetzt.

Aufgrund der Kombination von MWG und ATD können weitere Untersuchungen durchgeführt und ein effektiver Ansatz zur Blockierung sowie Erkennung von Bedrohungen umgesetzt werden.

McAfee-Produkte, die DAT-Dateien verwenden

McAfee hat eine Extra.DAT veröffentlicht, die den Schutz vor Petya ermöglicht. McAfee veröffentlichte zudem eine Notfall-DAT, die diese Bedrohung abdeckt. Nachfolgende DAT-Dateien enthalten entsprechende Schutzsignaturen. Die neuesten DAT-Dateien finden Sie in der Wissensdatenbank im Artikel KB89540.

Weitere Informationen

Regelmäßig aktualisierte technische Details finden Sie in folgenden Artikeln der McAfee-Wissensdatenbank: KB89335, KB87843, KB74983, KB53735 und KB89540.

McAfee
Together is power.

Ohmstr. 1
85716 Unterschleißheim
Deutschland
+49 (0)89 3707 0
www.mcafee.com/de

3530_0917
SEPTEMBER 2017