

# McAfee Advanced Threat Defense

## Erkennung hochentwickelter Malware

Mit McAfee® Advanced Threat Defense können Unternehmen hochentwickelte getarnte Malware erkennen und mithilfe von Bedrohungsinformationen Aktionen und Schutzmaßnahmen starten. Im Gegensatz zu herkömmlichen Sandbox-Analysefunktionen besitzt diese Lösung zusätzliche Untersuchungsfunktionen, die die Erkennungsmöglichkeiten erweitern und auf diese Weise Stealth-Bedrohungen aufdecken. Durch die enge Vernetzung der Sicherheitslösungen – vom Netzwerk und Endgerät bis zur Untersuchung – können Bedrohungsinformationen sofort in der gesamten Umgebung weitergegeben werden, was den Schutz und die Analysemöglichkeiten verbessert. Die flexiblen Bereitstellungsoptionen unterstützen jede Netzwerkkonfiguration.

Unsere Technologie hat die Vorgehensweise bei der Erkennung grundlegend verändert, indem fortschrittliche Malware-Analysefunktionen mit vorhandenen Abwehrmaßnahmen kombiniert wurden – von der Netzwerkperipherie bis zum Endgerät. Zudem werden Bedrohungsanalysen in der gesamten IT-Umgebung weitergegeben. Durch die gemeinsame Nutzung von Bedrohungsdaten im gesamten Ökosystem unterbrechen unsere Lösungen sofort die Befehls- und Steuerungskommunikation, isolieren kompromittierte Systeme und blockieren weitere Instanzen gleicher oder ähnlicher Bedrohungen, um sie und ihre Auswirkungen zu analysieren sowie Maßnahmen zu ergreifen.

### McAfee Advanced Threat Defense: Erkennung hochentwickelter Bedrohungen

McAfee Advanced Threat Defense erkennt aktuelle Stealth- und Zero-Day-Malware mithilfe eines innovativen, mehrstufigen Ansatzes. Die Lösung kombiniert Analysemodule mit geringem Ressourcenverbrauch wie Virenschutz-Signaturen, Reputationsanalyse und Echtzeitemulation mit dynamischen Analysen (Sandbox) zur Untersuchung des tatsächlichen Verhaltens. Anschließend kommt die tiefgehende statische Code-Analyse zum Einsatz, die Dateiattribute sowie Anweisungen untersucht und auf diese Weise beabsichtigtes oder heimliches Verhalten aufdeckt sowie Ähnlichkeiten mit bekannten Malware-Familien findet. Im letzten Schritt der Analyse sucht McAfee Advanced Threat Defense

### Wichtigste Vorteile von McAfee Advanced Threat Defense

---

#### Umfassende Lösungsintegration

- Integration in vorhandene McAfee-Lösungen, E-Mail-Gateways von Drittanbietern und weitere Produkte, die offene Standards unterstützen
- Schließung der Schutzlücke zwischen Entdeckung und Eindämmung sowie Schutz für das gesamte Unternehmen
- Optimierung von Arbeitsabläufen für schnellere Reaktionen und Behebungsmaßnahmen
- Automatisierte Funktionen

---

Folgen Sie uns



## DATENBLATT

explizit nach Indikatoren für böswilliges Verhalten, die mit Machine Learning über ein Deep Neural Network identifiziert wurden. Diese Kombination ergibt die stärkste sowie fortschrittlichste verfügbare Technologie zum Schutz vor hochentwickelter Malware und schafft ein Gleichgewicht zwischen tiefgehender Untersuchung und Leistungsfähigkeit. Während Methoden mit geringerer Analyselast (z. B. Signaturen und Echtzeitemulation) Leistungsvorteile bieten, indem sie bekannte Malware leichter entdecken, ermöglichen die gründliche statische Code-Analyse, durch Machine Learning gewonnene Informationen sowie Sandbox-Analysen die Erkennung stark getarnter sowie schwer aufzuspürender Bedrohungen. Indikatoren für böswilliges Verhalten, die in einer dynamischen Umgebung nicht ausgeführt werden, können durch Entpacken, tiefgehende statische Code-Analyse sowie Informationen aus Machine Learning aufgedeckt werden.

Malware-Autoren nutzen gern Packtechniken, um die Code-Zusammensetzung zu verändern bzw. Code zu verbergen und auf diese Weise die Erkennung zu erschweren. Die meisten Produkte können den gesamten ursprünglichen ausführbaren (Quell-)Code nicht vollständig zur Analyse entpacken. Aus diesem Grund enthält McAfee Advanced Threat Defense umfassende Entpackfunktionen, die Verschleierungstechniken aufheben und so den ausführbaren Original-Code offenlegen. Die Lösung bietet gründliche Code-Analyse, um nicht nur grundlegende Dateiattribute zu untersuchen, sondern auch Anomalien zu erfassen. Dabei werden Attribute und Anweisungen auf das resultierende Verhalten untersucht.

Gemeinsam ermöglichen die gründliche, statische Code-Überprüfung, Machine Learning und die dynamische Analyse eine vollständige sowie detaillierte Überprüfung auf potenzielle Malware. Die hervorragende Datenanalyse liefert sowohl Übersichtsberichte, mit deren Hilfe Sie das Ausmaß eines Angriffs überblicken und Ihre Maßnahmen Prioritäten zuweisen können, als auch detaillierte Malware-Daten-Berichte.

### Erweiterter Schutz

Durch die starke Integration von McAfee Advanced Threat Defense in Sicherheitsgeräte – von der Netzwerkperipherie bis zum Endgerät – können sofort Maßnahmen ergriffen werden, sobald McAfee Advanced Threat Defense eine Datei als gefährlich einstuft. Diese starke und automatisierte Integration von Erkennung und Schutz ist unverzichtbar.

McAfee Advanced Threat Defense kann sich auf unterschiedliche Weise vernetzen: direkt mit verschiedenen Sicherheitslösungen, über McAfee Threat Intelligence Exchange oder mit McAfee Advanced Threat Defense Email Connector.

Durch die direkte Integration können Sicherheitslösungen Maßnahmen ergreifen, wenn Dateien von McAfee Advanced Threat Defense als gefährlich eingestuft werden. Sie können unverzüglich Bedrohungsdaten in bestehende Prozesse zur Richtlinien erzwingung integrieren und weitere Instanzen der gleichen oder ähnlicher Dateien daran hindern, in das Netzwerk zu gelangen.

### Leistungsstarke Analysefunktionen

- Kombination aus gründlicher statischer Code-Überprüfung, dynamischer Analyse und Machine Learning für genauere Erkennung durch einzigartige Analysedaten
- Fortschrittliche Funktionen unterstützen das Sicherheitskontrollzentrum und ermöglichen Untersuchungen

### Flexible, zentrale Bereitstellung

- Niedrigere Kosten durch zentrale Bereitstellung und Unterstützung mehrerer Protokolle
- Flexible Bereitstellungsoptionen unterstützen jede Netzwerkkonfiguration

### Integrierte Lösungen

- McAfee® Active Response
- McAfee® Advanced Threat Defense Email Connector
- McAfee® Enterprise Security Manager
- McAfee® ePolicy Orchestrator®
- McAfee® Network Security Platform
- McAfee® Threat Intelligence Exchange
  - McAfee® Application Control
  - McAfee® Endpoint Protection
  - McAfee® Security for Email Servers
  - McAfee® Server Security
- McAfee® Web Gateway
- Bro Network Security Monitor
- TAXII (Trusted Automated eXchange of Indicator Information)

## DATENBLATT

Die Erkennungen von McAfee Advanced Threat Defense werden in den Protokollen und Dashboards der integrierten Produkte angezeigt, als wäre die gesamte Analyse in dem jeweiligen Produkt erfolgt. Dadurch werden Arbeitsabläufe optimiert, und Administratoren erhalten die Möglichkeit, Warnungen effizient zu verwalten, indem sie über eine zentrale Benutzeroberfläche arbeiten.

Durch die Integration von McAfee Threat Intelligence Exchange können andere Schutzlösungen, wie zum Beispiel McAfee Endpoint Protection, auf den Funktionsumfang von McAfee Advanced Threat Defense zugreifen. So wird einem breiten Spektrum an integrierten Sicherheitslösungen Zugang zu Analyseergebnissen und Kompromittierungsindikatoren gewährt. Wenn eine Datei von McAfee Advanced Threat Defense überführt wurde, veröffentlicht McAfee Threat Intelligence Exchange diese Bedrohungsinformationen über ein Reputations-Update an alle integrierten Gegenmaßnahmen im Unternehmen.

Endgeräte mit McAfee Threat Intelligence Exchange können Installationen mit Malware-Erstinfektionen blockieren und präventiven Schutz bereitstellen, wenn die Datei später erneut gefunden wird. Gateways mit McAfee Threat Intelligence Exchange können verhindern, dass die Datei ins Unternehmen gelangt. Außerdem erhalten Endgeräte mit McAfee Threat Intelligence Exchange auch außerhalb des Netzwerks Aktualisierungen zu Dateierkennungen, sodass keine Lücken durch die Out-of-Band-Übertragung von Malware-Code entstehen.

Mit McAfee Advanced Threat Defense Email Connector kann McAfee Advanced Threat Defense vom E-Mail-Gateway E-Mail-Anhänge zur Analyse erhalten. McAfee Advanced Threat Defense analysiert Dateien in den Anhängen und gibt im Header der E-Mail ein Analyseurteil an alle aktiven E-Mail-Gateways zurück. Das E-Mail-Gateway kann anschließend richtlinienbasierte Aktionen vornehmen, beispielsweise den Anhang löschen oder isolieren, damit die Malware das interne Netzwerk nicht infizieren und sich darin ausbreiten kann. Dank eines Offline-Modus können E-Mails mit Anhängen an den Endbenutzer übermittelt und parallel von McAfee Advanced Threat Defense gescannt werden. Das E-Mail-Gateway wartet nicht auf ein abschließendes Urteil zum Anhang. Administratoren können die Ergebnisse der Anhang-Scans in McAfee Advanced Threat Defense oder McAfee Threat Intelligence Exchange anzeigen. Um die Erkennung auf dem E-Mail-Server zu verbessern, integriert sich McAfee Advanced Threat Defense über McAfee Threat Intelligence Exchange in McAfee Security for Email Servers.

### **Austausch von Bedrohungsdaten zur Verbesserung und Automatisierung von Untersuchungen**

Zur Untersuchung und Behebung von Angriffen benötigen Unternehmen einen umfassenden Überblick mit umsetzbaren Bedrohungsdaten, damit sie bessere Entscheidungen treffen sowie angemessene Reaktionen umsetzen können. McAfee Advanced Threat Defense liefert umfassende Bedrohungsdaten, die unkompliziert in Ihrer gesamten Umgebung weitergegeben werden können, um Untersuchungen zu verbessern und zu

## DATENBLATT

automatisieren. Unterstützung für den Data Exchange Layer (DXL) sowie die REST-APIs (Application Programming Interfaces) ermöglicht die Integration anderer Produkte sowie häufig genutzter Standards zum Austausch von Bedrohungsinformationen, z. B. STIX (Structured Threat Information eXpression) und TAXII (Trusted Automated eXchange of Indicator Information). Dadurch können Unternehmen ein kooperatives Sicherheitsökosystem aufbauen, unterstützen und erweitern.

Innerhalb eines McAfee-Ökosystems erfasst und korreliert McAfee Enterprise Security Manager detaillierte Datei-Reputationsdaten sowie Ausführungsereignisse von McAfee Advanced Threat Defense und anderen Sicherheitssystemen, um erweiterte Warnfunktionen und Verlaufsansichten bereitzustellen, die erweiterte Sicherheitsdaten, Risikopriorisierung und Echtzeitinformationen zur Sicherheitslage ermöglichen. Mit den Kompromittierungsindikator-Daten von McAfee Advanced Threat Defense kann McAfee Enterprise Security Manager bis zu sechs Monate alte Daten durchsuchen, um zu überprüfen, ob Hinweise zu diesen Funden in Netzwerk- oder Systemdaten gefunden werden können. Dabei können Systeme aufgedeckt werden, die zuvor mit neu identifizierten Malware-Quellen kommuniziert haben. Die enge Verzahnung mit McAfee Endpoint Protection, McAfee Threat Intelligence Exchange und McAfee Active Response optimiert Reaktionen auf Sicherheitsabläufe sowie den Überblick und ermöglicht Aktionen wie die Veröffentlichung neuer Konfigurationen, Implementierung neuer Richtlinien, Entfernung von Dateien und Ausbringung von Software-Aktualisierungen, die Risiken

präventiv beheben können. Da infizierte Endgeräte im Netzwerk automatisch von McAfee Active Response erkannt und in McAfee Advanced Threat Defense-Berichten erfasst werden, können Sie auf einfache Weise fundierte Entscheidungen treffen und entsprechende Maßnahmen ergreifen. Die Effizienz von Analysten wird verbessert, wenn diese detaillierten Berichte in einem zentralen Arbeitsbereich in McAfee Active Response angezeigt werden.

### Fortschrittliche Funktionen erleichtern Untersuchungen

McAfee Advanced Threat Defense bietet zahlreiche hochentwickelte Funktionen, zum Beispiel:

- **Konfigurierbare Unterstützung für Betriebssysteme und Anwendungen:** Bei den Analyse-Images können bestimmte Umgebungsvariablen angepasst werden, um Bedrohungen zu analysieren und Untersuchungen zu unterstützen.
- **Interaktiver Benutzermodus:** Ermöglicht Analysten die direkte Interaktion mit Malware-Exemplaren.
- **Umfangreiche Entpackfunktionen:** Verkürzen die für Untersuchungen benötigte Zeit von Tagen auf Minuten.
- **Vollständiger Logikpfad:** Ermöglicht tiefgehendere Probenanalysen, da die Ausführung zusätzlicher Logikpfade erzwungen wird, die in typischen Sandbox-Umgebungen ruhend bleiben.
- **Einsendung von Exemplaren an mehrere virtuelle Umgebungen:** Beschleunigt die Untersuchung, da ermittelt wird, welche Umgebungsvariablen für die Dateiausführung erforderlich sind.

## DATENBLATT

- **Detaillierte Berichte:** Stellt für Untersuchungen wichtige Informationen bereit, zum Beispiel MITRE ATT&CK™-Zuordnung, Disassemblierungsausgaben, Speicherabbilder, Aufrufdiagramme für Grafikfunktionen, eingebettete oder gelöschte Dateiinformationen, API-Protokolle der Benutzer und PCAP-Informationen. Bedrohungszeitachsen erleichtern die Visualisierung der Ausführungsschritte von Angriffen.
- **Integration von Bro Network Security Monitor:** Stellt einen Bro-Sensor in einem verdächtigen Netzwerksegment bereit, um Datenverkehr zu überwachen sowie zu erfassen und Dateien zur Untersuchung an McAfee Advanced Threat Defense weiterzuleiten.

## Bereitstellung

Die flexiblen Bereitstellungsoptionen von McAfee Advanced Threat Defense unterstützen jede Netzwerkconfiguration. McAfee Advanced Threat Defense ist als lokale Hardware-Appliance sowie als virtuelle Appliance verfügbar. Sie unterstützt private sowie öffentliche Clouds, die im Azure Marketplace verfügbar sind.

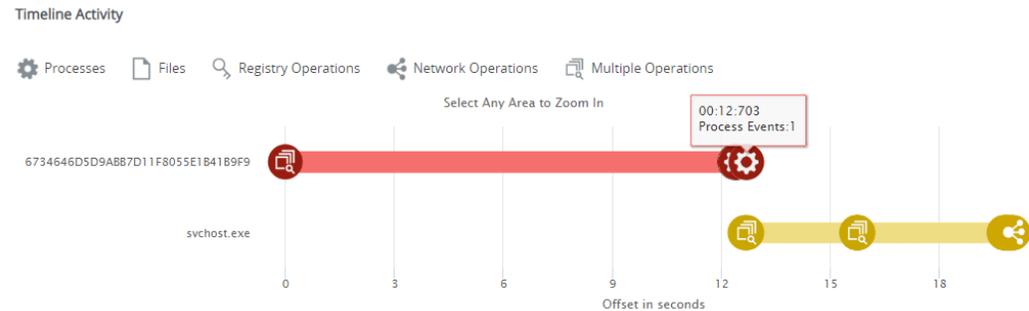


Abbildung 1. Zeitachsenaktivität visualisiert Ausführungsschritte der analysierten Bedrohung.

Filename: 2015-05-07-Alpha-Crypt-ransomware-sample\_exe\_(2)  
 File Hash: A08784F5691A0A8CE6249E1981DEA82C  
 Threat Level: Very High

Tactics | Techniques 8 24

| Initial Access                      | Execution                         | Persistence                      | Privilege Escalation                  | Defense Evasion                  | Credential Access                  | Discovery                    | Lateral Movement                    | Collection                         | Exfiltration                                  | Command and Control                   |
|-------------------------------------|-----------------------------------|----------------------------------|---------------------------------------|----------------------------------|------------------------------------|------------------------------|-------------------------------------|------------------------------------|---|---------------------------------------|
| Drive-by Compromise                 | CMSTP                             | Accessibility Features           | Access Token Manipulation             | Access Token Manipulation        | Account Manipulation               | Account Discovery            | Application Deployment Software     | Audio Capture                      | Automated Exfiltration                        | Commonly Used Port                    |
| Exploit Public-Facing Application   | Command Line Interface            | AppCert DLLs                     | Accessibility Features                | BITS Jobs                        | Brute Force                        | Application Window Discovery | Distributed Component Object Model  | Automated Collection               | Data Compressed                               | Communication Through Removable Media |
| Hardware Additions                  | Control Panel Items               | Applet DLLs                      | AppCert DLLs                          | Binary Padding                   | Credential Dumping                 | Browser Bookmark Discovery   | Exploitation of Remote Services     | Clipboard Data                     | Data Encrypted                                | Connection Proxy                      |
| Replication Through Removable Media | Dynamic Data Exchange             | Application Shimming             | Applet DLLs                           | Bypass User Account Control      | Credentials in Files               | File and Directory Discovery | Login Scripts                       | Data Staged                        | Unsafe Transfer Size Limits                   | Custom Command and Control Protocol   |
| Spearphishing Attachment            | Execution Through API             | Authentication Package           | Application Shimming                  | CMSTP                            | Credentials in Registry            | Network Service Scanning     | Pass the Hash                       | Data from Information Repositories | Exfiltration Over Alternative Protocol        | Custom Cryptographic Protocol         |
| Spearphishing Link                  | Execution Through Module Load     | BITS Jobs                        | Bypass User Account Control           | Code Signing                     | Exploitation for Credential Access | Network Share Discovery      | Pass the Ticket                     | Data from Local System             | Exfiltration Over Command and Control Channel | Data Encoding                         |
| Spearphishing via Service           | Exploitation for Client Execution | Bootkit                          | DLL Search Order Hijacking            | Component Firmware               | Forced Authentication              | Password Policy Discovery    | Remote Desktop Protocol             | Data from Network Shared Drive     | Exfiltration Over Other Network Medium        | Data Obfuscation                      |
| Supply Chain Compromise             | Graphical User Interface          | Browser Extensions               | Exploitation for Privilege Escalation | Component Object Model Hijacking | Hooking                            | Peripheral Device Discovery  | Remote File Copy                    | Data from Removable Media          | Exfiltration Over Physical Medium             | Domain Fronting                       |
| Trusted Relationship                | InstallUI                         | Change Default File Association  | Extra Window Memory Injection         | Control Panel Items              | Input Capture                      | Permission Groups Discovery  | Remote Services                     | Email Collection                   | Scheduled Transfer                            | Fallback Channels                     |
| Valid Accounts                      | LSASS Driver                      | Component Firmware               | File System Permissions Weakness      | DCShadow                         | Kerberoasting                      | Process Discovery            | Replication Through Removable Media | Input Capture                      |   | Multi-Stage Channels                  |
|                                     | Mhta                              | Component Object Model Hijacking | Hooking                               | DLL Search Order Hijacking       | LLMNR/NBNS Poisoning               | Query Registry               | Shared Webroot                      | Man in the Browser                 |   | Multi-hop Proxy                       |

Abbildung 2. Ergebnisse werden dem MITRE ATT&CK™-Framework zugeordnet.

Filename: 2015-05-07-Alpha-Crypt-ransomware-sample\_exe\_(2)  
 File Hash: A08784F5691A0A8CE6249E1981DEA82C  
 Threat Level: Very High

Tactics | Techniques 8 24

| Initial Access | Execution                     | Persistence                  | Privilege Escalation      | Defense Evasion                 | Credential Access | Discovery                              | Lateral Movement     | Collection | Exfiltration                | Command and Control                 |
|----------------|-------------------------------|------------------------------|---------------------------|---------------------------------|-------------------|--|----------------------|------------|-----------------------------|-------------------------------------|
|                | Command Line Interface        | Hidden Files and Directories | Access Token Manipulation | Access Token Manipulation       |                   | Process Discovery                      | Third-party Software |            | Data Encrypted              | Commonly Used Port                  |
|                | Execution Through API         | Modify Existing Service      | Process Injection         | File Deletion                   |                   | System Network Configuration Discovery |                      |            | Unsafe Transfer Size Limits | Connection Proxy                    |
|                | Execution Through Module Load |                              |                           | Hidden Files and Directories    |                   | System Shadowing Discovery             |                      |            |                             | Standard Application Layer Protocol |
|                | Scripting                     |                              |                           | Indicator Blocking              |                   |  |                      |            |                             | Uncommonly Used Port                |
|                | Third-party Software          |                              |                           | Masquerading                    |                   |  |                      |            |                             |                                     |
|                |                               |                              |                           | Modify Registry                 |                   |  |                      |            |                             |                                     |
|                |                               |                              |                           | Obfuscated Files or Information |                   |  |                      |            |                             |                                     |
|                |                               |                              |                           | Process Injection               |                   |  |                      |            |                             |                                     |
|                |                               |                              |                           | Scripting                       |                   |  |                      |            |                             |                                     |
|                |                               |                              |                           | Timestamp                       |                   |  |                      |            |                             |                                     |

Copyright © 2018 McAfee, LLC. All rights reserved.  
 Copyright © 2018 The MITRE Corporation. This work is reproduced and distributed with the permission of The MITRE Corporation.

Abbildung 3. Eine gefilterte Ansicht der Ergebnisse in Abbildung 2 zeigt den Bericht zu erkannten Techniken.

## DATENBLATT

### Details zu McAfee Advanced Threat Defense

|                                       |  |                              |
|---------------------------------------|--|------------------------------|
| Formfaktoren der physischen Appliance | ATD-3100<br>1 HE-Rackmontage   | ATD-6100<br>1 HE-Rackmontage |
| Formfaktoren der virtuellen Appliance | v1008<br>ESXi 5.5, 6.0, 6.5, 6.7<br>Hyper-V Windows Server 2012 R2, Windows Server 2016<br>Azure Marketplace |                              |

### Erkennung

|                              |  |
|------------------------------|--|
| Unterstützte Dateitypen      | PE-Dateien, Adobe-Dateien, Microsoft Office Suite-Dateien, Bilddateien, Archive, Java, Android Application Package-Dateien, URLs   |
| Analysemethoden              | McAfee Anti-Malware Engine, GTI-Dateireputation (Datei/URL/IP-Adresse), Gateway Anti-Malware (Emulation und Verhaltensanalyse), dynamische Analyse (Sandbox), gründliche Code-Analyse, benutzerdefinierte YARA-Regeln, Machine Learning mit Deep Neural Network  |
| Unterstützte Betriebssysteme | Windows 10 (64-Bit), Windows 8.1 (64-Bit), Windows 8 (32-Bit/64-Bit), Windows 7 (32-Bit/64-Bit), Windows XP (32-Bit/64-Bit), Windows Server 2016, Windows Server 2012, Windows Server 2012 R2, Windows Server 2008, Windows Server 2003, Android<br><br>Alle Sprachversionen der Windows-Betriebssysteme werden unterstützt. |
| Ausgabeformate               | STIX, OpenIOC, XML, JSON, HTML, PDF, Text  |
| Übertragungsmethoden         | Integration von Einzelprodukten, RESTful-APIs, manuelle Einreichungen und McAfee Advanced Threat Defense Email Connector (SMTP)  |

### Weitere Informationen

Wenn Sie weitere Informationen wünschen oder McAfee Advanced Threat Defense evaluieren möchten, wenden Sie sich an Ihren Vertriebsrepräsentanten, oder besuchen Sie

[www.mcafee.com/de/products/advanced-threat-defense.aspx](http://www.mcafee.com/de/products/advanced-threat-defense.aspx)



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

McAfee und das McAfee-Logo sind Marken oder eingetragene Marken von McAfee, LLC oder seinen Tochterunternehmen in den USA und anderen Ländern. Alle anderen Namen und Marken sind Eigentum der jeweiligen Besitzer. MITRE ATT&CK und ATT&CK sind Marken der MITRE Corporation. Copyright © 2018 McAfee, LLC. 4169\_1118  
NOVEMBER 2018