# Leistungstest bei der Verhinderung komplexer Bedrohungen

Datum der Studie: 2. Februar 2017 (Aktualisiert: 12. Februar)

## Zusammenfassung

Cylance hat AV-TEST damit beauftragt, Enterprise-Software zum Schutz von Endpunkten hinsichtlich der Verhinderung komplexer Bedrohungen zu testen. Die Testmethodik wurde gemeinsam entwickelt, um zusätzliche Tests zu den derzeit standardmäßig von AV-TEST durchgeführten Anti-Virus-Schutztests hinzuzunehmen.

CylancePROTECT® wurde gegenüber 5 konkurrierenden Endpunktprodukten von Kaspersky, McAfee, Sophos, Symantec und Trend Micro getestet. Der Test wurde im Dezember 2016 und im Januar 2017 durchgeführt. Dieser Bericht enthält die Ergebnisse von vier Testfällen. Das primäre Ziel bestand darin, die Erkennungs- und Präventionsfunktionen in Bezug auf sowohl bekannte als auch unbekannte schädliche ausführbare Dateien prüfen.

Testfall 1 - Der Urlaubstest: Zweck dieses Tests ist es, ein reales Szenario nachzubilden, bei dem ein Endbenutzer über einen bestimmten Zeitraum hinweg in Urlaub geht. Nach der Rückkehr von seinem Urlaub fährt der Endbenutzer seinen Endpunkt wieder hoch und wird infiziert, bevor die Schutzmaßnahmen auf dem Endpunkt aktualisiert werden können. Dies ist auch ein Szenario, das viele Unternehmen vorfinden. Sie können sich hierdurch letztlich gegebenenfalls dazu gezwungen sehen, extreme Maßnahmen zu ergreifen und beispielsweise Signatur-Updates aufgrund der Beeinträchtigung der Benutzer-Performance um ein Quartal zu verzögern. Dieses Szenario bietet außerdem eine relativ einfache Möglichkeit, um "Zero-Day"-Erkennungs- und Verhinderungsfunktionen zu testen. Beim Test selbst wird das Produkt am Tag 0 eingefroren und dann offline genommen. Dann warten wir sieben Tage ab und sammeln in der Zwischenzeit neue Malware (ausführbare Dateien), die am siebten Tag als neu entdeckt erachtet werden können, und beginnen die Tests. Wir fahren das eingefrorene Produkt ohne Konnektivität zum Internet hoch, so dass die Schutzmaßnahmen grundsätzlich sieben Tage alt sind. Die Produkte waren also nicht in der Lage, sich zu aktualisieren oder Abfragen an die Cloud zu senden. Anschließend haben wir die neu entdeckte Malware ausgeführt, um die Wirksamkeit der überprüften Sicherheitslösung bei der Erkennung und Verhinderung unbekannter Bedrohungen zu testen.

Testfall 2 - Simulierte Angriffe: Beim zweiten Test wurde ein zielgerichteter Angriff simuliert, bei dem ein Angreifer in der Lage war, eine ausführbare Datei in das System einzuschleusen. Diese ausführbaren Dateien wurden von AV-TEST erstellt, um bestimmte Arten von Angriffen zu simulieren, die von den Produkten erkannt und blockiert werden mussten. Diese ausführbaren Dateien beruhen auf heutzutage häufig zu beobachtenden komplexen Angriffen. Die neuen Zero-Day-Dateien wurden auf Systemen erst im Offline-Modus ausgeführt, um die Fähigkeit der Endpunkt-Sicherheitslösungen zu prüfen, tatsächlich unbekannte Angriffe ohne Konnektivität zur Cloud zu erkennen. Anschließend wurde eine Verbindung zur Cloud erlaubt, um die Auswirkungen von Cloud-Abfragen aufzuzeigen.

Testfall 3 - von Websites verteilte Malware: Bei diesem Test wurden ausführbare Malware-Dateien untersucht, die über Websites zugestellt werden. Die URL selbst ist nicht schädlich, es sind die Inhalte der Website, von denen die Bedrohung ausgeht. Bei diesem Test wird die URL-Filterung aller getesteten

Produkte ausgeschaltet, um zu ermitteln, ob sie den schädlichen Charakter der besuchten Website tatsächlich erkennen können.

Testfall 4 - Falschmeldungen (falsche positive Ergebnisse): Jeder Schutztest sollte durch einen Falschmeldungstest verifiziert werden, um sicherzustellen, dass gute Erkennungsraten nicht auf Kosten von Benutzerfreundlichkeit und falsch positiven Ergebnissen erzielt wurden. Um dies zu überprüfen, haben wir 38 verschiedene häufig verwendete Anwendungen wie etwa Adobe Reader, Google Chrome, Java JDK oder Skype heruntergeladen, installiert und tatsächlich verwendet. Alle Warnmeldungen oder Sperren der getesteten Schutzprodukte wurde vermerkt.

In allen Testfällen konnte CylancePROTECT® seine Effektivität unter Beweis stellen und extrem hohe Verhinderungsraten erzielen. Der Ansatz des Produkts ist äußerst zuverlässig und funktioniert offline, ohne dass regelmäßige Updates erforderlich sind - selbst vor Ausführung der Malware. Zudem zeigt sich bei diesen Tests, wie stark die übrigen Produkte auf regelmäßige Updates, Cloud-Abfragen oder dynamische Analysen angewiesen sind. Die Tests haben gezeigt, dass es CylancePROTECT® gelingt, unbekannte Angriffe zu erkennen, während die meisten anderen getesteten Anbieter hierzu nicht in der Lage waren.

# Testmethodik

## Hardware-Plattform und Betriebssystem

Alle Tests wurden auf identischen Hardware-Plattformen mit den folgenden Spezifikationen durchgeführt.

| | |
|---|---|
| **Betriebssystem** | Windows 10 Professional mit allen am 1. Dezember2016 verfügbaren Patches |
| **Hardware** | • Intel Xeon Quad-Core X3360 CPU<br>• 4 GB RAM<br>• 500 GB HDD (Western Digital)<br>• Intel Pro/1000PL (Gigabit Ethernet) NIC |

## Getestete Produkte

In der folgenden Tabelle sind die getesteten Produkte und ihre jeweiligen Versionen aufgeführt.

| Produktname | Version |
|---|---|
| **CylancePROTECT®** | 1.2.1410.60 |
| **Kaspersky Endpoint Security** | 10.2.5.3201 (mr3) |
| **McAfee Endpoint Security** | 10.2.0.620 |
| **Sophos Endpoint Security and Control** | 10.6.4.1150 |
| **Symantec Endpoint Protection** | 14.0.1886.0000 |
| **Trend Micro OfficeScan** | 12.0.1901 |

## Testfall 1: Urlaubstest

Zweck dieses Tests ist es, die Erkennungsfunktionen eines Produkts gegenüber einer neuen Malware (PE-Dateien) nachzuweisen. Die Sicherheitsmaßnahmen, Signaturen und Modelle für maschinelles Lernen sind eine Woche alt, und das Produkt ist nicht in der Lage, Abfragen an die Cloud zu schicken:

1. Installation: Das Produkt wird installiert und auf die neueste Programmversion und die aktuellsten Signaturen aktualisiert
2. Produkt einfrieren: Ein Disk Image wird an Tag 0 erstellt, und der Zugang zum Internet wird getrennt
3. 7 Tage abwarten, dann neue Malware (PEs) erfassen, die an Tag 7 als neu erkannt gelten.
4. Eingefrorenes Produkt ohne Konnektivität zu jeglicher Form von Internet hochfahren, so dass die Signatur-Update-Datei praktisch 7 Tage alt ist.
5. Neu erkannte Malware (PEs) gegenüber der VUT ausführen
    a. Statische Erkennung: Zunächst Ausführung eines On-Access-Tests, bei dem die Dateien auf die Festplatte kopiert werden und anschließend ein On-Demand-Suchlauf der verbleibenden Dateien durchgeführt wird
    b. Dynamische Erkennung: Anschließend Ausführung aller verbleibenden Exemplare
6. Erfassung der Wirksamkeitsergebnisse.

### Stichprobenauswahl

Für diesen Test wurden 98 Stichproben, die erstmalig am 19. und 20. Januar von AV-TEST erkannt wurden, nach dem Zufallsprinzip ausgewählt. Hierbei handelte es sich in allen Fällen um PE-Dateien, die Backdoors, Downloader, Dropper, generische Trojaner und Viren enthielten.

## Testfall 2: Simulierte Angriffe

Wenn Angreifer zielgerichtete Angriffe durchführen, können sie entweder bestehende Malware/Tools ändern oder neue Tools erstellen, um sicherzustellen, dass keine entsprechenden Signaturen vorliegen. Um einen solchen zielgerichteten Angriff zu simulieren, hatte AV-TEST Binärdateien für fünf mögliche Angriffsszenarien erstellt. Diese wurden dann auf zwei verschiedene Weisen modifiziert, um 15 Testfälle zu schaffen.

1. Installation: Das Produkt wird installiert und auf die neueste Programmversion und die aktuellsten Signaturen aktualisiert
2. Der Test wurde in drei Schritten durchgeführt: die ersten beiden ohne Internetzugang, der letzte mit Internetzugang.
    a. Statische Erkennung (Offline): Zunächst Ausführung eines On-Access-Tests, bei dem die Dateien auf die Festplatte kopiert werden und anschließend ein On-Demand-Suchlauf der verbleibenden Dateien durchgeführt wird
    b. Dynamische Erkennung (Offline): Anschließend Ausführung aller verbleibenden Exemplare
    c. Dynamische Erkennung (Online): Verbindung des Systems mit dem Internet und Ausführung aller verbleibenden Exemplare
3. Erfassung der Wirksamkeitsergebnisse.

### Stichprobenauswahl

Es wurden fünf verschiedene Tools mit den nachfolgend aufgeführten Verhaltensweisen erstellt. Alle Tools wurden in C/C++ erstellt und mit Microsoft Visual C++ kompiliert

| | Persistenz | Payload |
|---|---|---|
| **Angriff 1** | Registry: HKCU | Abruf von Zugriffsdaten und Upload an einen externen Server |
| **Angriff 3** | Startup-Ordner | Abruf von Zugriffsdaten und Upload an einen externen Server |
| **Attack 3** | - | Herunterladen und Ausführung weiterer ausführbarer Datei |
| **Angriff 4** | - | Änderung von HDD-Sektoren |
| **Angriff 5** | - | Verschlüsselung von Dateien |

*Table 1: Simulated attacks*

Die fünf sich hieraus ergebenden Testfälle wurden dann mit zwei verschiedenen Ansätzen modifiziert. Im ersten Ansatz wurde ein Abschnitt zur PE-Datei hinzugefügt. Im zweiten Ansatz wurden Daten an das Ende der PE-Datei angehängt.

Hieraus ergaben sich 15 verschiedene Dateien mit unterschiedlichen Hashes.

## Testfall 3: Über Websites verteilte Malware

Viele Infizierungen geschehen heutzutage über Websites. Die meisten Schutzprodukte verwenden einen mehrschichtigen Ansatz, um diese zu blockieren. Sie versuchen, die URL und den schädlichen Inhalt abzudecken. Verschiedene Produkte haben hier verschiedene Prioritäten, und einige konzentrieren sich gegebenenfalls stärker auf eine URL-Blockierung als andere. Allerdings ist es für Angreifer recht leicht, die URL zu verändern und so diese Art der Erkennung zu umgehen. Dieser Test zielt daher darauf ab, die Erkennungsrate bei einer Zustellung der schädlichen PE-Datei über eine Website zu messen, wenn keine URL verfügbar ist.

1. Installation: Das Produkt wird installiert und auf die neueste Programmversion und die aktuellsten Signaturen aktualisiert
2. URL-Filterung des Produkts ausschalten, falls verfügbar.
3. Das Opfer greift auf die Website zu, wo die Datei heruntergeladen und ausgeführt wird
4. Erfassung der Wirksamkeitsergebnisse.

### Stichprobenauswahl

Für diesen Test wurden 69 Websites, die Malware verbreiten, nach dem Zufallsprinzip ausgewählt.

## Testfall 4: Falschmeldungen

Es wäre leicht, ein Schutzprodukt zu erstellen, das bei allen Schutztests 100% erreicht, gleichzeitig jedoch auch bei allen gutartigen Dateien falsch positive Meldungen liefert. Daher haben wir getestet, wie die Produkte auf häufig ebenso wie weniger häufig eingesetzte Software reagieren, wenn diese von ihrer ursprünglichen Quelle heruntergeladen und auf dem Computer installiert und verwendet wird. Jedes Mal, wenn das Sicherheitsprodukt etwas erkannt und eine Warnmeldung geschickt oder eine Aktion blockiert hat, wurde dies zur Ermittlung des Ergebnisses vermerkt.

### Stichprobenauswahl

Insgesamt wurden 38 verschiedene häufig ebenso wie weniger häufig verwendete Anwendungen für die Tests verwendet. Die vollständige Liste ist im Anhang am Ende dieses Dokuments angegeben.

## Allgemeine Hinweise zur Testmethodik:

Im Zusammenhang mit der Erstellung von Angriffssimulationstools gibt es ein Thema, auf das wir gerne kurz näher eingehen möchten.

Wenn der Schutz vor neuen oder zielgerichteten Angriffen getestet werden soll, ist es immer erforderlich, eigene Testfälle zu erstellen. Dies kann geschehen, indem entweder bestehende Malware modifiziert oder eigene Angriffssimulationstools erstellt werden. Beides wird kontrovers diskutiert, nicht nur innerhalb der Anti-Malware-Branche. Wir haben uns dafür entschieden, eigene Angriffssimulationstools zu erstellen, um volle Kontrolle über diese zu haben und sicherstellen zu können, dass sie keinen Schaden anrichten.

Die Anti-Malware Testing Standards Organization (AMTSO) hat mehrere Dokumente mit Best Practices für Anti-Malware-Tests erstellt. Eines dieser Dokumente trägt den Titel "Issues Involved in the ‘Creation’ of Samples for Testing” (Probleme im Zusammenhang mit der 'Erstellung' von Probeexemplaren für Testzwecke. Dieses Dokument diskutiert die Argumente für und gegen eine Modifizierung von Malware oder die Erstellung eigener Dateien, beispielsweise der von uns verwendeten Angriffssimulatoren. Das Dokument verbietet die Erstellung neuer Malware-Exemplare zu Testzwecken nicht, heißt dies jedoch auch nicht explizit gut. Es hängt jeweils davon ab, was genau mit dem Test erreicht werden soll. Nach ausführlicher Prüfung des Dokuments sind wir davon überzeugt, dass unser Ansatz im Einklang mit der vorgebrachten Argumentation steht.

## Testergebnisse

Die Testergebnisse für alle anderen Anbieter bis auf CylancePROTECT® sind in anonymisierter Form dargestellt. Anstatt genaue Produktnamen zu verwenden, werden die Produkte jeweils mit Anbieter 1 bis 5 bezeichnet. Sie sind anhand des Ergebnisses in Testfall 1 sortiert, und derselbe Anbieter hat in allen drei Testfällen jeweils stets dieselbe Nummer.

Im ersten Testfall wurden 98 neue Proben verwendet, die offline und mit 7 Tage alten Signaturdatenbanken erkannt werden mussten. Die in Abbildung 1 dargestellten Ergebnisse zeigen, dass Cylance in diesem Test bei weitem das beste Ergebnis erzielen konnte.

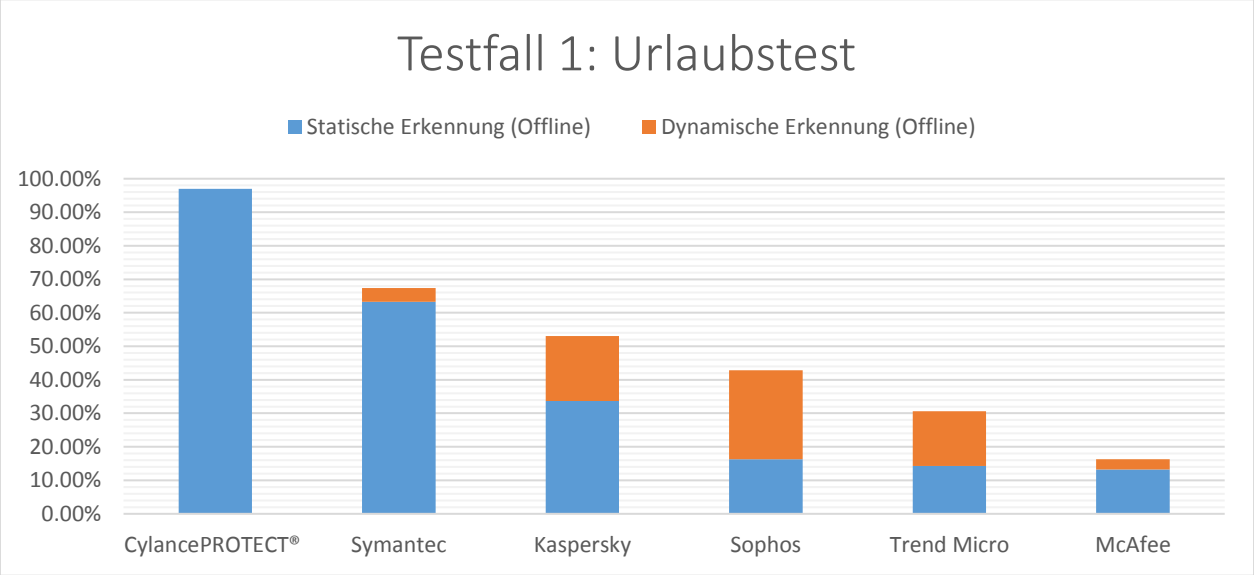


*Abbildung 1: Statische und dynamische Erkennungsergebnisse mit neuer Malware*

CylancePROTECT® erkannte mehr als 97 % der Proben, bevor diese ausgeführt wurden. Das nächstbeste Produkt erkannte 67%, und der Durchschnitt von Anbieter 1 bis Anbieter 5 lag bei einer Erkennungsrate von lediglich 42 %. Allerdings auch nur bei einer Kombination aus statischer und dynamischer Erkennung. Die statische Erkennung alleine lieferte für die Anbieter 1 bis 5 einen noch niedrigeren Durchschnittswert von 28 %. Das beste Produkt kam auf 63 %, verglichen mit 97 % für Cylance.

Dies mag zwar kein typischer Anwendungsfall sein, er kann jedoch durchaus eintreten. Manche Unternehmen wenden Updates gegebenenfalls nicht regelmäßig an, oder Mitarbeiter kehren nach dem Urlaub zu einem Rechner zurück, der nicht auf dem neuesten Stand ist und veraltete Signaturdatenbanken aufweist. Zudem können Cloud-Abfragen fehlschlagen. Bei mehreren Anbietern haben wir Ausfälle beobachtet, und einige Produkte reagieren zudem hochempfindlich auf Netzwerkprobleme. Selbst wenn die Internet-Verbindung funktioniert, können Cloud-Anfragen fehlschlagen, wenn es z.B. zu Paketverlusten kommt. Dies kann in öffentlichen WLANs wie Starbucks oder auch an Flughäfen vorkommen. Es gibt weitere Fälle, in denen Offline-Tests relevant sein könnten, und wir empfehlen, die folgenden Optionen bei der Beurteilung von Sicherheitsprodukten zumindest zu diskutieren:

- Einzelhandels-POS/Geldautomat - In manchen Implementierungsfällen ist die gesamte Netzwerkkommunikation beschränkt, auf eine einzige Anwendung innerhalb des POS/Geldautomaten reduziert oder durch die Firewall eingeschränk.
- Ablenkungstaktik - Kompromittierung eines Netzwerksegments, so dass sich die Sicherheitsfachkräfte voll und ganz darauf konzentrieren und der Angreifer an anderer Stelle Schaden anrichten/Daten herausschleusen kann
- Bottom-up DDos - Könnte mit der voranstehenden Taktik kombiniert werden: Kompromittierung eines Netzwerksegments und Verursachung von Schäden (wäre auch in Universitäten, Regierungsstellen, im Gesundheitswesen, etc. ein Fall)
- Malware, die die Verbindung angreift

Sehr viel wichtiger sind allerdings die technischen Implikationen dieses Tests: CylancePROTECT® benötigt weder regelmäßige Signatur-Updates noch Cloud-Abfragen, um neue Dateien erkennen zu können - selbst bevor diese ausgeführt werden. Die übrigen getesteten Produkte hingegen sind auf aktuelle Signaturdatenbanken und Cloud-Abfragen angewiesen, um ein zusätzliches Maß an Erkennung zu erreichen.

Die Ergebnisse in Abbildung 2 zeigen den Erfolg bei der Erkennung neuer Binärdateien, die Angriffe auf einen Endpunkt simulieren. Die Abbildung zeigt die Offline-Erkennung. Wieder einmal konnte CylancePROTECT® alle Bedrohungen erkennen, bevor diese ausgeführt wurden - selbst ohne Internet-Konnektivität.

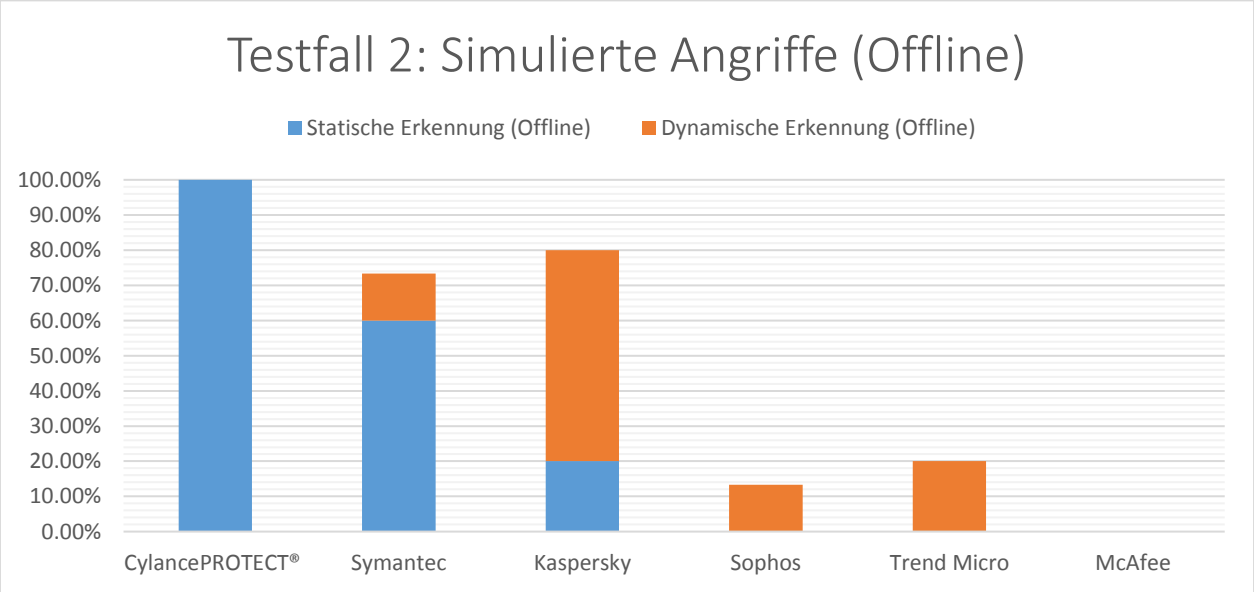


*Figure 2: Detection of new binaries simulating attacks*

Neben CylancePROTECT® gab es nur zwei weitere Anbieter, die in der Lage waren, einige der Dateien offline zu erkennen, bevor sie ausgeführt wurden. Die meisten anderen Erkennungen beruhten auf einer Verhaltensanalyse während der Ausführung der Tools. Zwei Anbieter erzielten eine zusätzliche Erkennung, nachdem der Test mit Online-Erkennung durchgeführt worden war. Diese Ergebnisse sind in Abbildung 3 dargestellt.

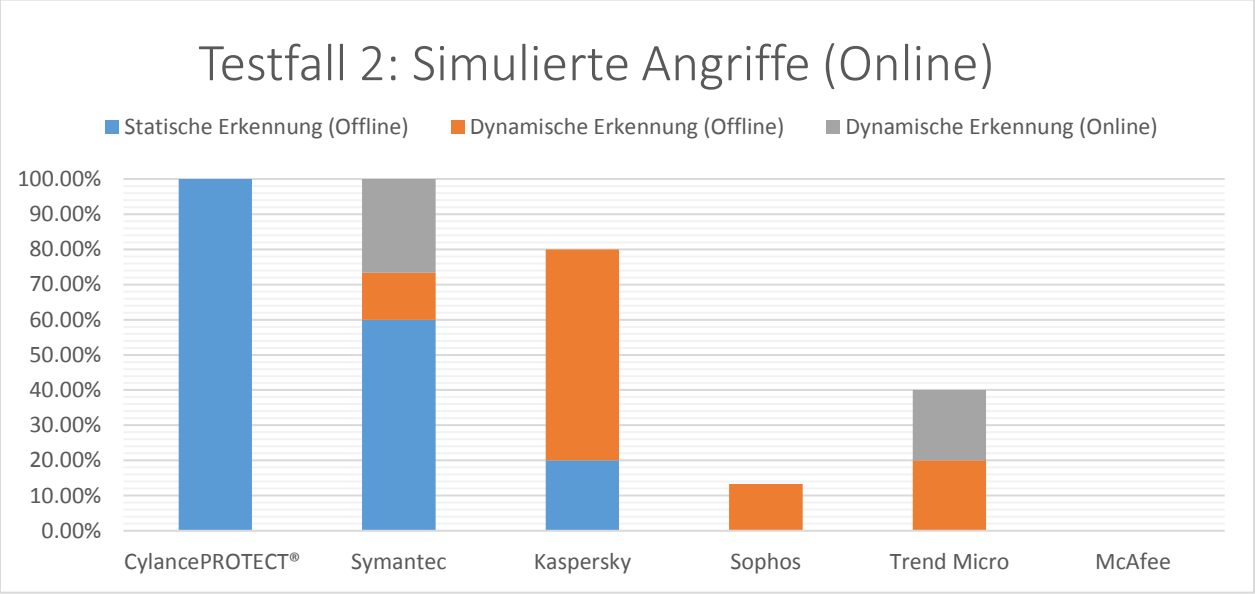


*Abbildung 3: Erkennung neuer Binärdateien, die Angriffe simulieren (mit Online-Erkennung)*

Diese zusätzlichen Online-Erkennungen waren bei einem der Produkte in erster Linie reputationsbasierte Entscheidungen. Dieses Produkte meldet zwar durchaus, dass die Dateien neu seien und niemals zuvor gesehen wurden. Als verdächtig wurden sie jedoch nicht eingestuft. Die folgende Tabelle zeigt die Erkennungsleistung je Produkt.[1]

| Testfall: | 1 | 2 | 3 | 4 | 5 | 1S | 2S | 3S | 4S | 5S | 1A | 2A | 3A | 4A | 5A |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| CylancePROTECT® | S | S | S | S | S | S | S | S | S | S | S | S | S | S | S |
| Anbieter 1 | D | D | R | R | R | S | S | S | S | S | S | S | S | R | S |
| Anbieter 2 | D | D | S | - | D | D | D | S | - | D | D | D | S | - | D |
| Anbieter 3 | - | D | - | - | - | - | D | - | - | - | - | - | - | - | - |
| Anbieter 4 | D | - | - | DO | - | D | - | - | DO | - | D | - | - | DO | - |
| Anbieter 5 | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - |

*Tabelle 2: Erkennung je Malware-Exemplar (Erkennungstyp: S = Statisch offline, D = Dynamisch offline, DO = Dynamisch online, R = Reputation)*

Im letzten Testfall mussten die Produkte Malware erkennen, die über Websites verbreitet wird - allerdings ohne ihre URL-Filterungskomponente. Es überrascht kaum, dass sich hierbei ein ähnliches Bild wie in den vorherigen Tests abzeichnete. CylancePROTECT® konnte einmal mehr fast alle Testfälle mit statischer Erkennung ermitteln, während der eine verbleibende Fall bei Ausführung der heruntergeladenen Binärdatei erkannt wurde.

[1]Erläuterung zu Tabelle 1:
Test Fall 1S = Probe 1 mit hinzugefügten Abschnitt
Test Fall 1A = Probe 1 mit angehängten Daten zum Ende der Datei

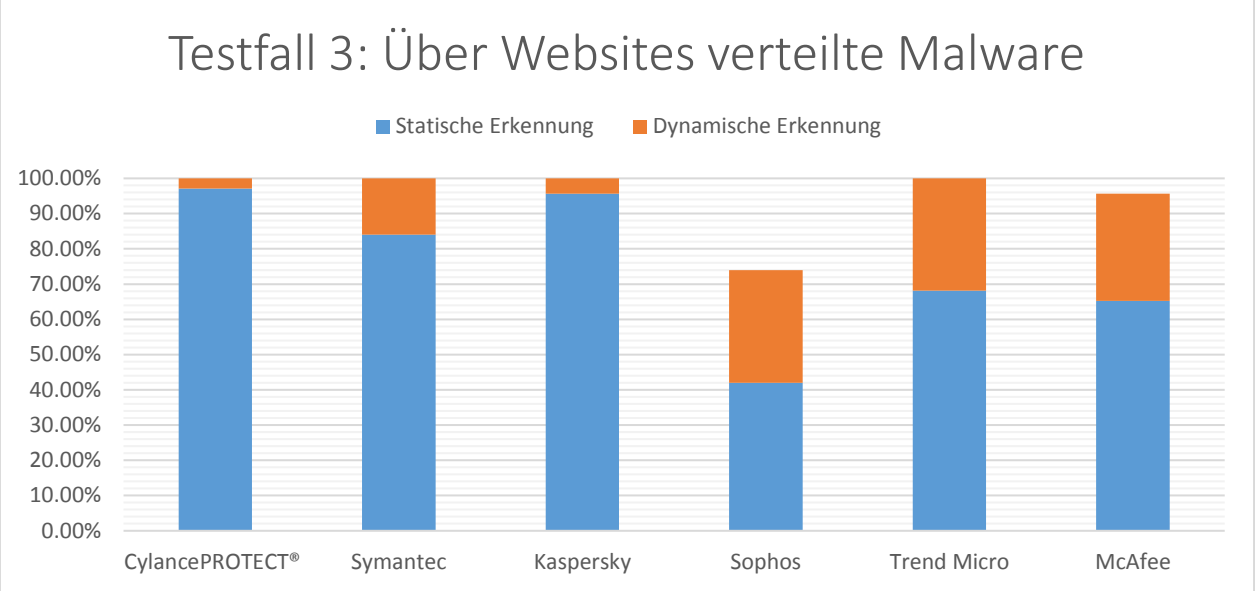


*Abbildung 4: Erkennung ausführbarer Dateien, die über Websites verbreitet wurden*

Die übrigen Produkte erkannten 71 % der Proben anhand statischer Erkennung und weitere 22 % anhand einer dynamischer Erkennung nach Ausführung. Anbieter 3 hatte bei der Erkennung ernsthafte Probleme, als die URL-Filterkomponente herausgenommen wurde. Hierdurch sank die Erkennungsquote auf 73.

In Bezug auf Falschmeldungen gab es bei keinem der getesteten Produkte ernsthafte Probleme. Bei CylancePROTECT® wurden allerdings zweimal installierte Dateien erkannt - für Android Studio sowie für Samsung SideSync. Die übrigen Produkte erzeugten keine falsch positiven Meldungen.

Alle drei Testfälle zeigen, dass CylancePROTECT® über einen äußerst zuverlässigen Ansatz verfügt, der offline funktioniert, ohne dass regelmäßige Updates erforderlich sind - selbst vor Ausführung der Malware. Zudem zeigt sich bei diesen Tests, wie stark die übrigen Produkte auf regelmäßige Updates, Cloud-Abfragen oder dynamische Analysen bzw. eine verhaltensbasierte Erkennung angewiesen sind. Die Tests haben gezeigt, dass CylancePROTECT® in der Lage ist, unbekannte Angriffe zu erkennen und zu verhindern, während die meisten anderen Anbieter mit neuen Angriffen Probleme hatten.

Die von AV-TEST durchgeführten regelmäßigen Tests zeigen, dass die Produkte durchaus Schutz vor standardmäßiger Malware bieten, wenn sie Zugang zur Cloud haben, sämtliche Schutzebenen nutzen können und ihre Signaturdatenbanken auf dem neusten Stand sind. Wie oben gezeigt, reicht dies jedoch nicht mehr aus, um effektiven Schutz vor neuen und unbekannten Bedrohungen zu bieten.

# Anhang

## Liste der für den Falschmeldungstest verwendeten Produkte

| | | |
|---|---|---|
| 7-zip 16.04 | HD Clone 6.0.7 | Samsung Sidesync 4.5.0.86 |
| Adobe Reader DC 2015.020.20039 | iTunes 12.5.3 | Skype 7.30.0.105 |
| Argusmonitor 3.3.7 | Java JDK 8u112 | Snappy Driver R513 |
| Android Studio 2.2 | Kindle for PC 1.17.44183 | Steam 3.61.93.65 |
| Classic Ftp 2.38 | Libre Office 5.2.3 | Teamviewer v12.0.71503.0 |
| Clone BD 1.0.8.8 | Linux Multi Media Studio 1.1.3 | Thunderbird 45.5.1 |
| doPDF 8.8 | Mycommander 3.3 | Tomahawk 0.8.4 |
| DVR Studio HD 4.11 | MyPhoneexplorer 1.8.7 | Tor Browser 6.0.7 |
| Firefox 50.02 | Nettalk 6.7.16 2.12.1 | Ultravnc 1.2.12 |
| Freecad 0.16 | Notepad++ 7 | VLC Media Player 2.2.4 |
| Gimp 2.8.18 | Opera 41.0.2353.69 | Vmware Player 12.5.1-4542065 |
| Google Chrome 55.0.2883.75 m | Picard 1.3.2 | Winrar 5.40 |
| Google Earth 7.1.7.2606 | Residualvm 0.2.1 | |