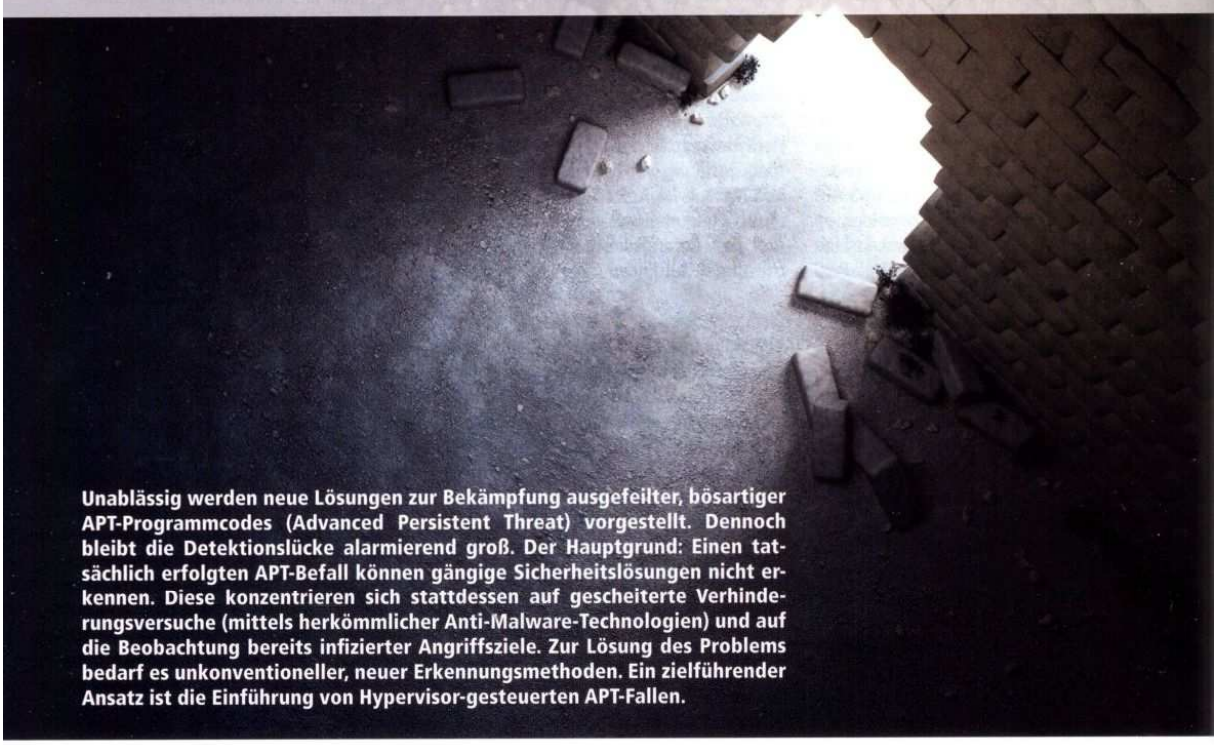
Neue Wege für die APT-Abwehr

Die klaffende Lücke schützen



Unablässig werden neue Lösungen zur Bekämpfung ausgefeilter, bösartiger APT-Programmcodes (Advanced Persistent Threat) vorgestellt. Dennoch bleibt die Detektionslücke alarmierend groß. Der Hauptgrund: Einen tatsächlich erfolgten APT-Befall können gängige Sicherheitslösungen nicht erkennen. Diese konzentrieren sich stattdessen auf gescheiterte Verhinderungsversuche (mittels herkömmlicher Anti-Malware-Technologien) und auf die Beobachtung bereits infizierter Angriffsziele. Zur Lösung des Problems bedarf es unkonventioneller, neuer Erkennungsmethoden. Ein zielführender Ansatz ist die Einführung von Hypervisor-gesteuerten APT-Fallen.

Anbieter von Sicherheitsprodukten reagieren auf neue APT-Infektionsmethoden und -techniken, sich einer Erkennung zu entziehen, schneller als je zuvor. Dennoch beträgt die durchschnittliche Zeit bis zur Entdeckung immer noch Monate. Hauptursache für die Detektionslücke bei APT (das heißt, die Zeit zwischen der ersten Infektion durch einen APT und dem Zeitpunkt seiner Erkennung) sind die ausgefeilten Infektionstechniken der Angreifer. Die meisten Infektionen erfolgen unterhalb des infizierten Betriebssystems und lassen sich daher mithilfe herkömmlicher Detektionstechnologien nicht in Echtzeit aufspüren – das gilt für Anti-Malware-Anwendungen ebenso wie für Sandboxen.

Wesentliche Phasen eines APT-Angriffs

Die „Vorbereitungsphasen" (Erkundung, Zielidentifizierung, Einholung der Benutzerkontakte etc.) ebnen den Weg zum beziehungsweise schaffen die Grundlage für den eigentlichen Angriff. Dennoch, der eigentliche Angriff beginnt erst, wenn das APT das beabsichtigte Ziel erreicht – in der Regel ein Endpunkt. Der APT-Angriff selbst setzt sich aus drei Phasen zusammen:

1. **Eindringen:**
- Ausnutzung von Schwachstellen im Betriebssystem und/oder der Anwendung, um das eigentliche APT auf dem Endpunkt installieren zu können.

2. **Infizieren:**
- Installation des eigentlichen APT, üblicherweise als „Dropping" („Abwurf") bezeichnet, wohingegen die APT-Komponente (meist mit einem Rootkit-Modul) als „Payload" („Sprengladung") bezeichnet wird.
- Dies ist DAS kritische Stadium, in dem das Angriffsziel beeinträchtigt ist: Das APT gewinnt genug Macht über das Zielsystem, um seine böswillige Aktivität frei auszuführen.

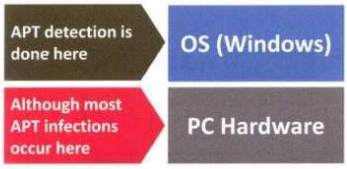
3. **APT-Aktivität:**
- Die beabsichtigte böswillige Aktivität auf dem infizierten und beeinträchtigten Zielsystem (Kommunikation mit dem C&C-Server, Sammeln persönlicher Informationen, Datenlöschung, Löschung des MBR, Verwandlung des Computers in einen Zombie etc.).

Bisherige Methode unzureichend

Die APT-Erkennung erfolgt derzeit in der Regel auf folgende Weise:

- Gängige Anti-Malware-Produkte (Client-Anwendungen, Gateways, Sandboxen und Cloud-Dienste) versuchen das Eindringen innerhalb des Kontexts ihres Host-Betriebssystems (meist Windows) zu erkennen und zu verhindern (entsprechend Phase 1 des APT-Angriffs).

- „APT-Lösungen" konzentrieren ihre Detektion durch das Feststellen und Beobachten der Netzwerkaktivität des APT (in der Regel nur ausgehende Daten) auf die tatsächliche Aktivität des APT auf dem bereits infizierten System (entsprechend Phase 3 des APT-Angriffs). Weder verhindern sie die Infizierung, noch können sie die Infektion vor der Netzwerkaktivität erkennen (Phase 2). Es gibt keine Lösung, die den eigentlichen APT-Infizierungsvorgang erkennt, die gefährlichste und ausschlaggebende Phase eines APT-Angriffs, und deshalb exakt zum Zeitpunkt des Geschehens Alarm schlägt. Daher die APT-Detektionslücke.



Die APT-Detektionslücke (schematische Darstellung). Quelle: LinuxWorks

Die Herausforderungen bei der Erkennung einer APT-Infizierung

Die meisten APTs nutzen Low-Level- und Sub-OS-Rootkits, die speziell entwickelt wurden, um vom Betriebssystem und jeder in oder auf ihm installierten Sicherheitsanwendung nicht auffindbar zu sein (daher das „P" für „persistent", „andauernd"). Um unauffindbar zu sein und sich dennoch ausreichende Kontrolle über lebenswichtige Funktionen des infizierten Betriebssystems zu verschaffen, benötigt ein Rootkit typischerweise zwei Sachen:

1. Selbstinstallation in verborgenen Teilen der Festplatte, auf die das Betriebssystem nicht zugreifen kann (die unpartitionierten Sektoren zwischen den Festplattenpartitionen und der letzte Sektor der Platte).
2. Dem infizierten Betriebssystem übergeordnete Sicherheitsrechte (Untergrabung der OS-Boot-Sequenz, Selbststart vor dem OS durch Änderung der ursprünglichen OS-Bootsektoren – MBR, VBR, UEFI).

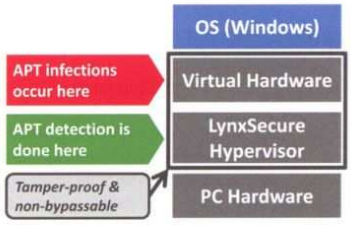
Diese zwei Grundmerkmale von Rootkits sind tödlich effektiv: Weil die zum Eindringen in das Betriebssystem verwendeten Datei-Infektoren häufig polymorph sind, verändern sich Rootkits viel langsamer. Neue Versionen dieser Rootkits tauchen einmal alle 12 bis 18 Monate auf. Da sie so verborgen und unauffindbar sind, besteht wenig Anlass für Veränderungen.

Ein Hypervisor-basierter Honeypot: Sub-OS-Erkennung von Sub-OS-Bedrohungen

Um gegen APTs erfolgreich agieren zu können, ist eine neue Herangehensweise erforderlich, die zwei kritische Aufgaben erledigt: erstens die Erkennung der eigentlichen APT-Infektion in Echtzeit und zweitens die Versorgung der zur Bedrohungsabwehr Beauftragten mit sofortigen forensischen Daten, um deren Analyse- und Reaktionszeiten signifikant zu verkürzen.

Angesichts der schwer zu erfassenden und heimlichen Natur von APTs muss die Erkennung auf einer Ebene erfolgen, die unter der Ebene der Infektion und Aktivität liegt. Diese Ebene kann nur ein „Bare Metal"-Hypervisor wie beispielsweise LynxSecure sein, der Hardware von der Software trennt, dem installierten Betriebssystem aber nur blanke virtuelle Hardware anzeigt. Als letztendlich „virtuelles Motherboard" ist solch ein Hypervisor unsichtbar für APTs und so von diesen nicht auffindbar.

Der Hypervisor muss speziell dafür ausgelegt sein, die „Aufmerksamkeit von APTs auf sich zu ziehen (das heißt ein Honeypot, also eine Art Falle), und so rigoros abgehärtet sein, dass er nicht selbst zum Angriffsziel wird. Hierdurch wird auch jegliche Abhängigkeit von einem OS aufgehoben (ein eklatanter Mangel einiger existierender Lösungen), so dass die Erkennung OS-agnostisch wird. Als privilegiertester Beobachter auf der Plattform ist der Hypervisor in der Lage, jede Veränderung an der beobachteten Hardware zu erfassen. Auf diese Weise werden die heimlichen Rootkits sofort abgefangen: MBR Wiper (zum Beispiel Dark Seoul), MBR-Infektoren (zum Beispiel TLD4), VBR-Infektoren (zum Beispiel XPAJ), verborgene Dateisysteme nutzende Malware (zum Beispiel ZeroAccess) etc.



Wie APT-Erkennung erfolgen sollte (schematische Darstellung). Quelle: LinuxWorks

Live-Forensik an Bord

Derzeit erfordert die Ermittlung der genauen Einzelheiten solcher Infektionen eine mühsame und langwierige forensische Analyse: Sie verfügt nicht über die forensischen Daten der nicht infizierten Hardware und muss die gesamte Hardware hinsichtlich der Infektion analysieren. Im wahrsten Sinne des Wortes: die Nadel im Heuhaufen suchen.

Der Hypervisor jedoch erlaubt die Erstellung eines sofortigen und abgestimmten forensischen Berichts, der nur die infizierten Bereiche enthält, mit einer automatischen Analyse der sauberen vs. infizierten Zustände (ein Hypervisor behält immer das „Gold Image", in diesen Fall: ein sauberes, nicht infiziertes Masterbild).

Zur erfolgreichen Eindämmung von APT-Angriffen ist ein „Out-of-the-Box"-Ansatz erforderlich, dessen Funktionalität im Gegensatz zum fertigen, geschlossenen Abwehrsystem vom Anwender frei definierbar ist. Der Einsatz eines sicheren Hypervisors als proaktive Erkennungsebene holt die Sicherheit wortwörtlich aus der „Box" (nämlich das attackierte Betriebssystem) heraus. ■

AVISHAI ZIV,
Vice President of Cyber Security Solutions, LynuxWorks, Inc.

Für Abonnenten ist dieser Artikel auch digital auf www.datakontext.com verfügbar

Weitere Artikel/News zum Schwerpunkt unter www.datakontext.com/spionage