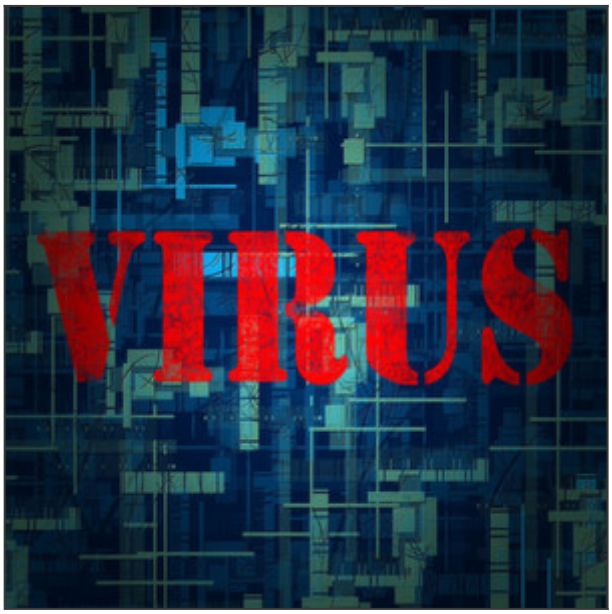
ELEKTRONIK PRAXIS

Malware-Schutz

Das Internet der Dinge gegen gezielte Angriffe schützen

13.09.14 | Autor / Redakteur: Avishai Ziv * / Franz Graser



Wie lassen sich Angriffe in der Embedded-Welt rechtzeitig erkennen und abwenden? Unkonventionelle Erkennungsmethoden und speziell ein sicherer Embedded-Hypervisor lösen das Problem.

Je mehr die Vision des Internet der Dinge mit 15 Milliarden verbundenen Objekten Gestalt annimmt, desto größer werden die Bedenken bezüglich der Sicherheit der Infrastruktur, die das ermöglichen soll. Spektakuläre gezielte Angriffe über verbundene Objekte (man denke an den Kredit- und Debit-Kartendatenklau bei der US-Kaufhauskette Target über einen Hackerangriff auf die POS-Terminals) haben gezeigt, dass das Bewusstsein um die Notwendigkeit und die Herausforderungen beim Umgang mit zielgerichteten Angriffen auf spezielle Teile in der Infrastruktur – seien es Server oder Endgeräte – noch nicht ausreicht.

Greifen verbundene Embedded-Objekte auf dieselben Betriebssysteme im IT-Terminals (Geldautomaten und Kassenterminals) zu, ist diese Embedded-Infrastruktur mittels erprobter Techniken angreifbar. Dies ist besonders alarmierend, wenn verbundene Embedded-Objekte für die Steuerung strategischer Infrastrukturen, zum Beispiel des öffentlichen Stromnetzes, genutzt werden und dadurch zum Ziel sowohl für Hacker als auch für ausländische Regierungen werden.

Willkommen in der Welt der Advanced Persistent Threats

Die IT-Abteilungen von Unternehmens befassen sich seit einiger Zeit mit diesem Problem – mit bislang mäßigem Erfolg. Zwar werden unablässig neue Lösungen zur

Bekämpfung ganz ausgefeilter bösartiger APT-Programmcodes (Advanced Persistent Threat) vorgestellt. Doch bleibt die Detektionslücke alarmierend groß.

Der Hauptgrund: Gängige Sicherheitslösungen können einen tatsächlichen APT-Befall nicht erkennen, sondern konzentrieren sich stattdessen auf gescheiterte Verhinderungsversuche (mittels herkömmlicher Anti-Malware-Technologien) und auf die Beobachtung bereits infizierter Angriffsziele.

Anbieter von Sicherheitsprodukten reagieren zwar schneller als je zuvor auf APT-Infektionsmethoden und ATP-Techniken, sich der Erkennung zu entziehen. Dennoch beträgt die durchschnittliche Aufdeckungszeit bei APT immer noch Monate (der in der Branche akzeptierte Durchschnitt liegt zwischen sechs und neun Monaten).

Hauptursache für die Detektionslücke bei APT (also 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 nicht in Echtzeit mithilfe herkömmlicher Detektionstechnologien aufspüren. Das gilt für Anti-Malware-Anwendungen ebenso wie für Sandboxen.

Die wesentlichen Phasen eines APT-Angriffs

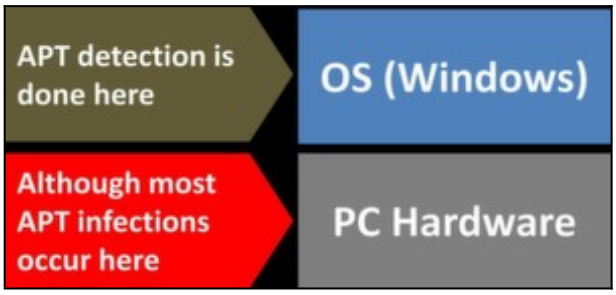
Die Vorbereitungsphasen (Erkundung, Zielidentifizierung, Einholung der Benutzerkontakte und Ähnliches) ebnen den Weg zum für den eigentlichen Angriff. Doch der eigentliche Angriff beginnt erst, wenn das APT das beabsichtigte Ziel erreicht – in der Regel einen Endpunkt.

Der APT-Angriff selbst setzt sich aus drei Phasen zusammen:

- Eindringen: Ausnutzung von Schwachstellen im Betriebssystem und/oder der Anwendung, um das eigentliche APT auf dem Endpunkt installieren zu können. Im Embedded-Bereich ist das eine gravierende Schwachstelle, weil Embedded-Endpunkte typischerweise unter veralteten Betriebssystemen wie Windows XP betrieben werden, die nicht länger mit Sicherheitspatches aktualisier werden. Diese ATM- und POS-Terminals sind viel gefährdeter als gewöhnliche PCs.
- Infizieren: Installation des eigentlichen APT, üblicherweise als “Dropping” („Abwurf“) bezeichnet, wohingegen die APT-Komponente (meist mit einem Rootkit-Modul) als „Payload“ („Nutzlast“) 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.
- 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, usw.).

Die klaffende Lücke bei der APT-Erkennung



Die APT-Erkennung benutzt derzeit folgende Methoden:

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

- Existierende Anti-APT-Lösungen konzentrieren ihre Detektion auf die tatsächliche Aktivität des APT auf dem bereits infizierten System (Phase 3) durch das Feststellen und Beobachten der Netzwerkaktivität des APT (in der Regel nur ausgehende Daten). Weder verhindern sie die Infizierung, noch können sie die Infektion vor der Netzwerkaktivität erkennen.

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.

Herausforderungen bei der Erkennung einer APT-Infizierung

Die meisten APT nutzen Low-Level- und Sub-OS-Rootkits, die speziell entwickelt wurden, vom Betriebssystem bzw. jeder in oder auf ihm installierten Sicherheitsanwendung nicht auffindbar zu sein (daher das der Buchstabe P für „persistent“).

Um unauffindbar zu sein und sich dennoch ausreichende Kontrolle über lebenswichtige Funktionen des infizierten Betriebssystems zu verschaffen, benötigt ein Rootkit typischerweise zwei Voraussetzungen:

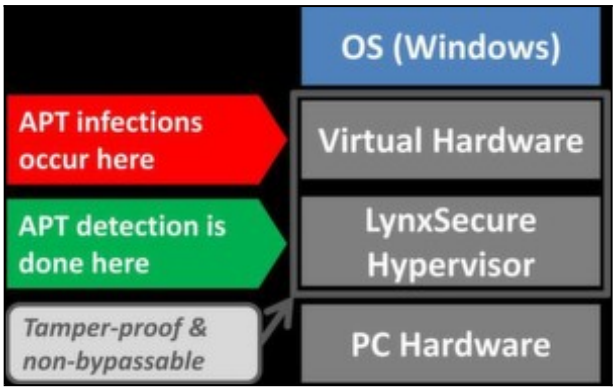
- Selbstinstallation in verborgenen Teilen der Festplatte, auf die das Betriebssystem nicht zugreifen kann (die unpartitionierten Sektoren zwischen den Festplattenpartitionen und der letzte Sektor der Plattte).
- Dem infizierten Betriebssystem übergeordnete Sicherheitsrechte (Untergrabung der OS-Bootsequenz, Selbsstart vor dem OS durch Abänderung der ursprünglichen OS-Bootsektoren -- MBR, VBR, UEFI).

Diese zwei Grundmerkmale von Rootkits sind tödlich effektiv: weil die zum Eindringen

in das Betriebssystem verwendeten Dateiinfektoren 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.

Sub-OS-Erkennung von Sub-OS-Bedrohungen

Wir brauchen eine neue Herangehensweise, 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 APT, muss die Erkennung auf einer Ebene erfolgen, die unter der der Infektion und Aktivität liegt. Diese Ebene kann nur ein Bare-Metal-Hypervisor (wie LynxSecure) sein, der die Hardware von der Software trennt, dem installierten Betriebssystem aber nur blanke virtuelle Hardware anzeigt. Als letztendlich virtuelles Motherboard ist solch ein Hypervisor unsichtbar für APT und von diesen nicht auffindbar.

Der Hypervisor muss speziell für die Erkennung ausgelegt (also ein sogenannter Honeypot) und so rigoros abgehärtet sein, dass er nicht selbst Angriffsziel wird. Hierdurch wird auch jegliche Abhängigkeit von einem OS aufgehoben (ein eklatanter Mangel einiger existierender Lösungen), so dass die Erkennung eine OS-agnostische wird. Als privilegiertester Beobachter auf der Plattform ist der Hypervisor in der Lage, jede Veränderung an der beobachteten Hardware zu erfassen.

Überdies kann ein gut durchdachter Embedded-Hypervisor mit ganz kleiner eigensicherer Codebasis die Installation auf typischen PC-basierten Embedded-Systemen installiert werden, die doch eher über bescheidene Rechenleistung und Speichergröße verfügen. Die geringe Größe des Hypervisors wird das Sicherheitsniveau des Gesamtsystems weiter stärken und die Angriffsoberfläche erheblich reduzieren.

Auf diese Weise werden die heimlichsten Rootkits sofort abgefangen: MBR Wiper (z.B. Dark Seoul), MBR-Infektoren (z.B. TLD4), VBR-Infektoren (z.B. XPAJ), verborgene Dateisysteme nutzende Malware (z.B. ZeroAccess), etc..

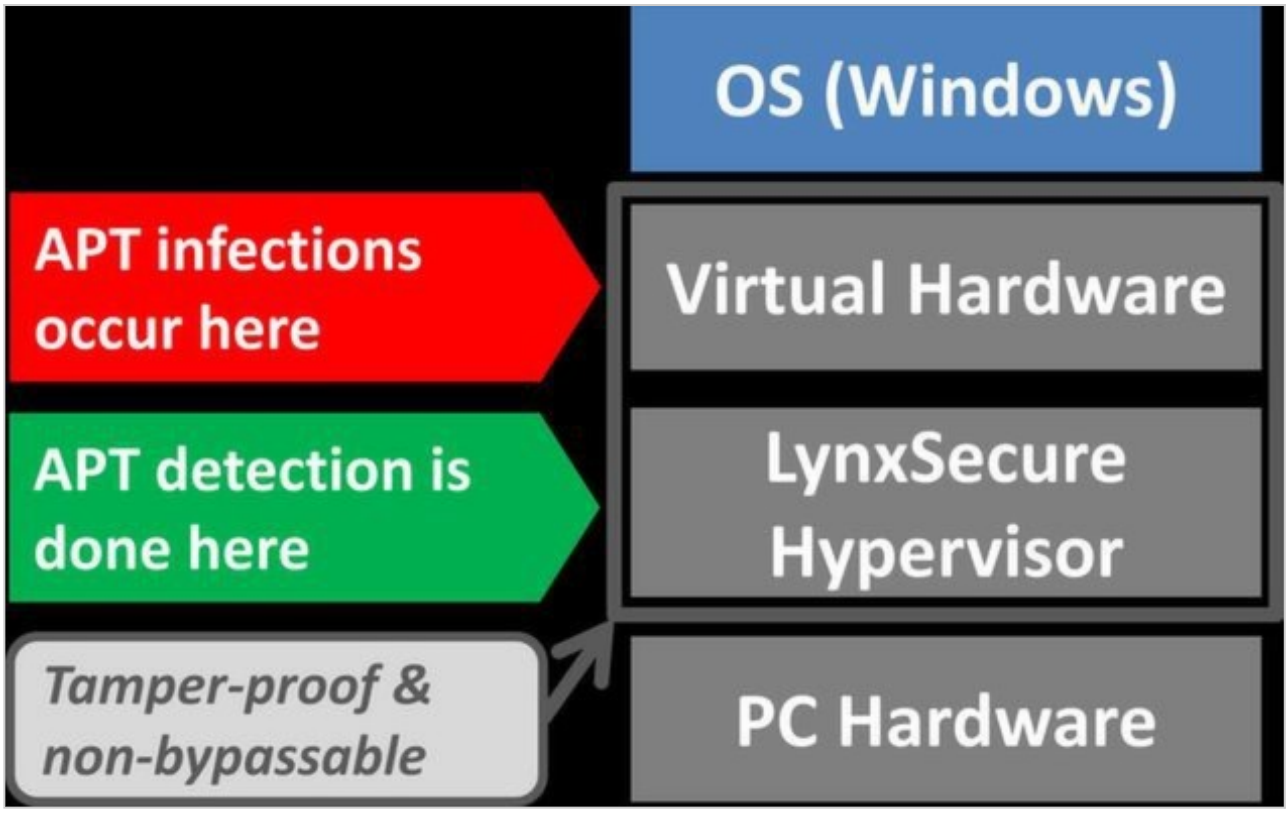
Derzeit erfordert die Ermittlung der genauen Einzelheiten solcher Infektionen eine mühsame und langwierige forensische Analyse: sie verfügt nicht über die forensischen Daten der nicht infizierten Hardware und muss die gesamte Hardware hinsichtlich der Infektion analysieren. Im wahrsten Sinne des Wortes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

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

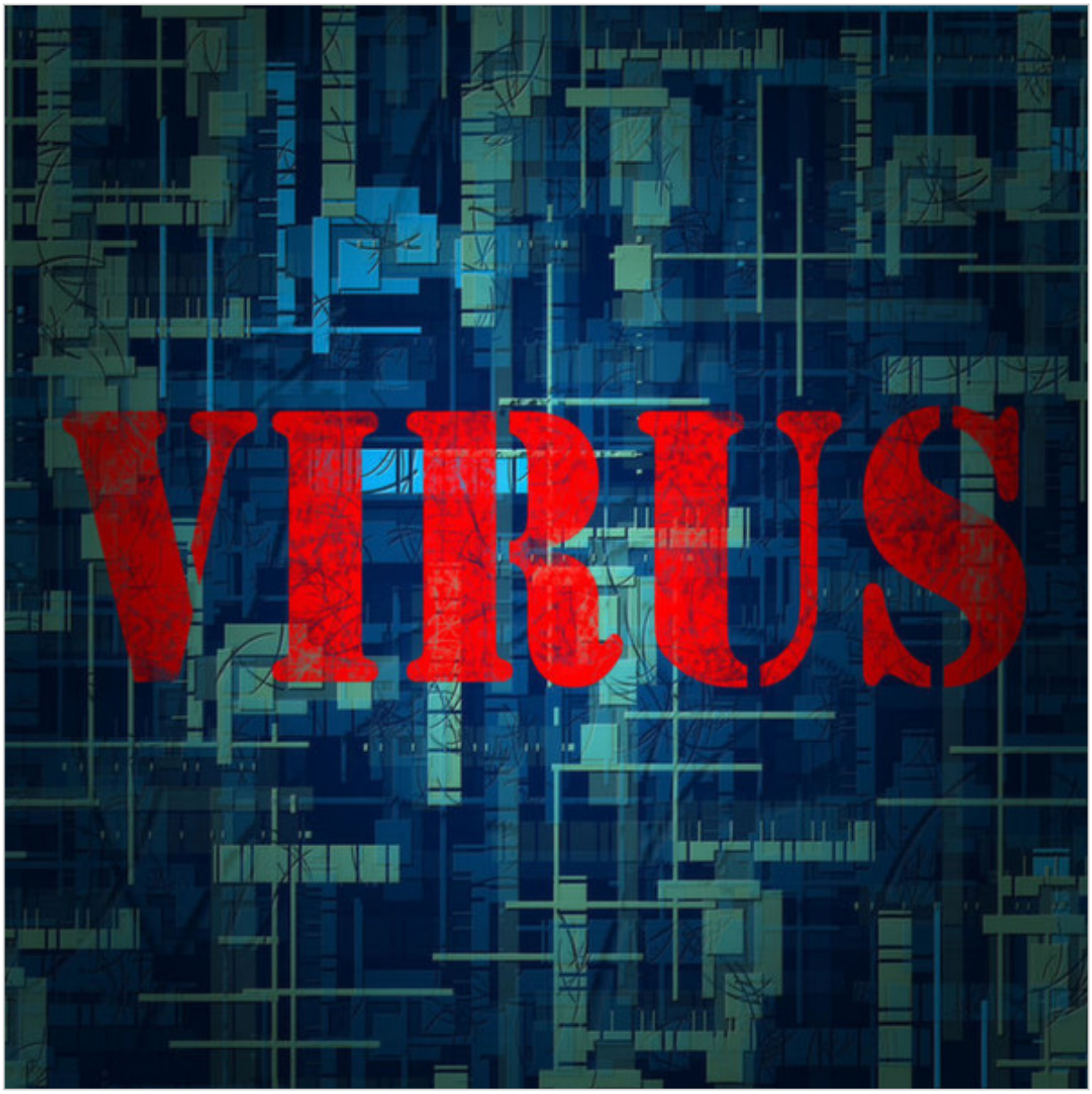
Zur erfolgreichen Eindämmung von APT-Angriffen ist ein Out-of-the-Box-Ansatz erforderlich, dessen Funktionalität im Gegensatz zum fertigen, geschlossenen Abwehrsystem vom Anwender frei definierbar ist. Der Einsatz eines sicheren Embedded-Hypervisors als Ebene zur proaktiven Erkennung holt aus der „Box“ (nämlich dem attackierten Betriebssystem) die Sicherheit wortwörtlich heraus.

//**FG**

* * Avishai Ziv ist Vice President of Cyber Security Solutions bei Lynx Software Technologies.



Wie die APT-Erkennung erfolgen sollte (schematische Darstellung) (Grafik: Lynx Software Technology)



Malware bedroht zunehmend auch Embedded-Software. Da die Bedrohungen immer perfider und ausgefeilter werden, ist eine robuste Abwehrstrategie notwendig. (Bild: Clipdealer)