Bitdefender®

# WELCHE GEHEIMNISSE VERBERGEN SICH IN IHRER INFRASTRUKTUR?

Ende 2013 führte eine routinemäßige Überprüfung einer Bank in Kiew zu dem Ergebnis, dass deren internen Systeme bereits seit mehreren Monaten von einer bisher unentdeckten Malware überwacht wurden. Dabei konnte die Schadsoftware ihre Spuren erfolgreich verwischen und so jede Bewegung der Mitarbeiter aufzeichnen. Es wurden sogar Videoaufnahmen und Bilder an den Urheber übertragen, ohne dass jemand Verdacht schöpfte.[1]

Als die zielgerichteten Angriffe mit der Malware, die heute unter dem Namen Carbanak bekannt ist, endlich entdeckt wurden, stellte sich heraus, dass über 100 Banken in insgesamt 30 Ländern betroffen waren - einer der größten Bankdiebstähle aller Zeiten. Es wird geschätzt, das weltweit ein Schaden von rund $1 Milliarde Dollar entstand.[2]

Und Carbanak ist nur eines von vielen Beispielen für gezielte Angriffe, bei denen Daten einer Reihe von Schlüsselindustrien weltweit erbeutet wurden, indem sich die Angreifer mithilfe von versteckter Malware unbemerkt Zugriff verschafften. Zwar gibt es viele Belege für solche und ähnlich ablaufende Angriffe, doch fehlten bisher wirksame vorbeugende Technologien, um diesen unsichtbaren Bedrohungen auf die Spur zu kommen.

## WIE SICH MALWARE UNBEMERKT HÖHERE BERECHTIGUNGSLEVEL VERSCHAFFT

Bei der Entwicklung von Betriebssystemen war Sicherheit zweitrangig. Schadcode kann – ebenso wie Ihre Sicherheitssoftware – mit Kernelrechten ausgeführt werden und so Ihre Sicherheitsvorkehrungen umgehen.

Nachdem dieser unbemerkt das System infiltriert hat, bleiben sowohl alle Arbeitsabläufe als auch das System voll funktionstüchtig. Und auch wenn alles in Ordnung zu sein scheint, sollen so nur Datendiebstahl und Cyberspionage verschleiert werden.

## SO MANCHE MALWARE KANN SOGAR IHRE INFRASTRUKTUR IN DIE KNIE ZWINGEN

Der Schaden, den ein erfolgreicher Angriff in einem System anrichtet, verschlimmert sich bis zur Problemlösung noch. Selbst eine relativ harmlose Malware, wie zum Beispiel ein Trojaner, der zum Spam-Versand eingesetzt wird, wirkt sich negativ auf die Systemressourcen eines Unternehmens aus. Durch Ressourcenverbrauch kann es letztendlich sogar zu negativen Auswirkungen beim den Ausgaben kommen; wird dabei noch die Arbeit der Mitarbeiter beeinträchtigt, entstehen durch die verlorene Zeit weitere Einbußen.

## **5 MONATE** KÖNNEN BIS ZUR ENTDECKUNG DES EINDRINGLINGS VERGEHEN

Eine im Februar 2016 durchgeführte Untersuchung hat ergeben, dass ein Unternehmen durchschnittlich **5 Monate** benötigt, um ein Datenleck zu entdecken. Darüber hinaus waren **53 %** der Unternehmen zur Offenlegung der Lecks auf externe Hilfe angewiesen, weil mit internen Mitteln keine Unregelmäßigkeiten zu erkennen waren.[3]

1 http://www.nytimes.com/2015/02/15/world/bank-hackers-steal-millions-via-malware.html
2 https://threatpost.com/carbanak-ring-steals-1-billion-from-banks/111054/
3 https://www2.fireeye.com/rs/848-DID-242/images/Mtrends2016.pdf

# Bitdefender und Citrix kämpfen gemeinsam gegen verborgene Bedrohungen in Ihrer Infrastruktur

## WIE FÄNGT MAN ETWAS, DAS MAN NICHT SEHEN KANN?

Falls Rootkits oder Kernel-Exploits das Betriebssystem so überlistet haben, dass sie unbemerkt bleiben, können Sie selbst von hoch entwickelten Sicherheitslösungen nur schwer entdeckt werden, wenn diese Sicherheitslösungen ausschließlich auf dem Gast ausgeführt werden. Das Geheimnis liegt darin, die VM von außen zu betrachten, und gleichzeitig die Prozesse zu überwachen, die innerhalb der VM ablaufen.

Dieser Ansatz erfordert einen Bare-Metal-Hypervisor, also ein Tool, das in der Vergangenheit nicht für Sicherheitszwecke eingesetzt wurde. Der Hypervisor liefert den Kontext für die virtuellen Maschinen, bleibt dabei aber von ihnen isoliert.

Als Teil einer bisher beispiellosen Zusammenarbeit im Kampf gegen gezielte Angriffe, haben Bitdefender und Citrix ihre Expertise in Virtualisierungs- und Sicherheitsfragen gebündelt. Gemeinsam wurde eine weitere Sicherheitsebene geschaffen, die volle Transparenz in allen Vorgänge Ihrer Infrastruktur ermöglicht, dabei aber für Malware unerreichbar bleibt.

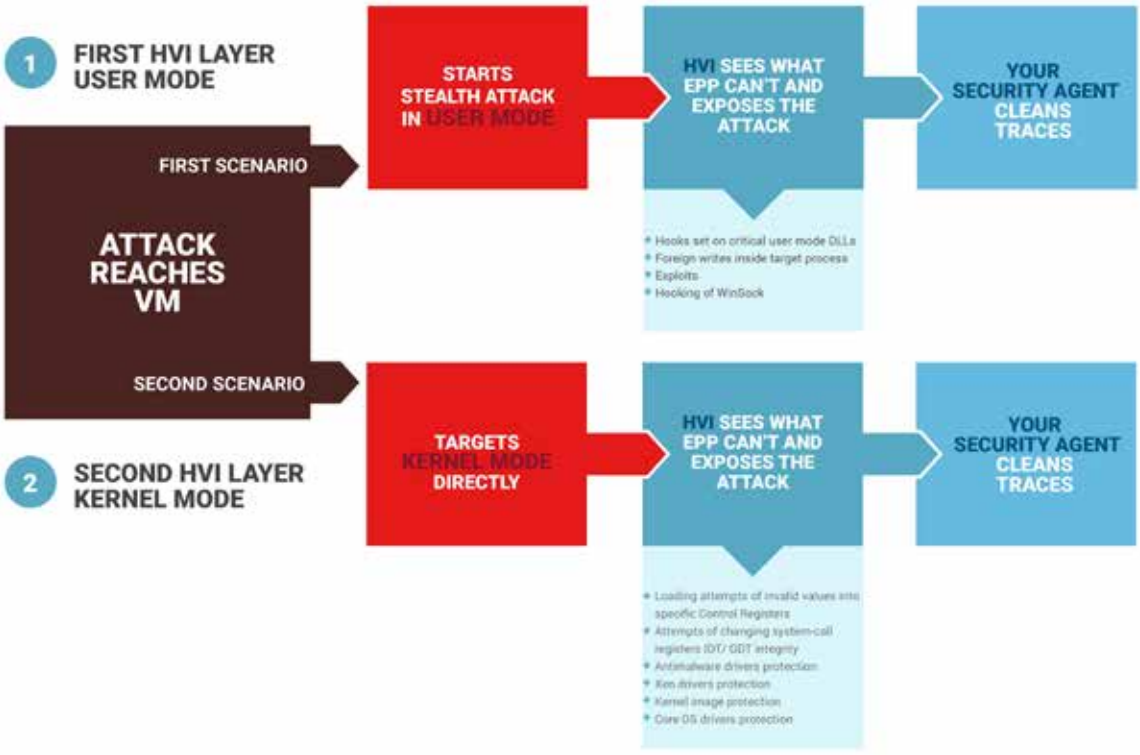
## EINE LÖSUNG, DIE BISHER ALS UNMÖGLICH GALT

Um hoch entwickelte Bedrohungen zu neutralisieren, darf man sich nicht auf die Informationen verlassen, die das Betriebssystem liefert. Hypervisoren stellen saubere, systemnahe Informationen über den Speicher bereit, der von den einzelnen virtuellen Maschinen verwendet wird.

Um diese Informationen zu liefern, hat Citrix eigens eine API für XenServer entwickelt, die über den Hypervisor Einblicke in den Raw-Speicher jeder virtuellen Maschine ermöglicht.

Auf dieser Ebene erfolgt lediglich ein Rohzugriff auf den Speicher auf unterster Ebene, wodurch bisher eine Analyse unmöglich war. Es gibt weltweit nur eine Handvoll Menschen, die auf dieser Ebene Sicherheitprogramme schreiben können.

Heute stellt Bitdefender seine Technologie für die Hypervisor Introspection (HVI) vor. Diese zukunftsweisende Lösung erkennt verdächtige Aktivitäten, indem sie direkt im Raw-Speicher aktiv wird - und damit derart tiefe Einblicke ermöglicht, dass das Verbergen von Malware unmöglich wird.



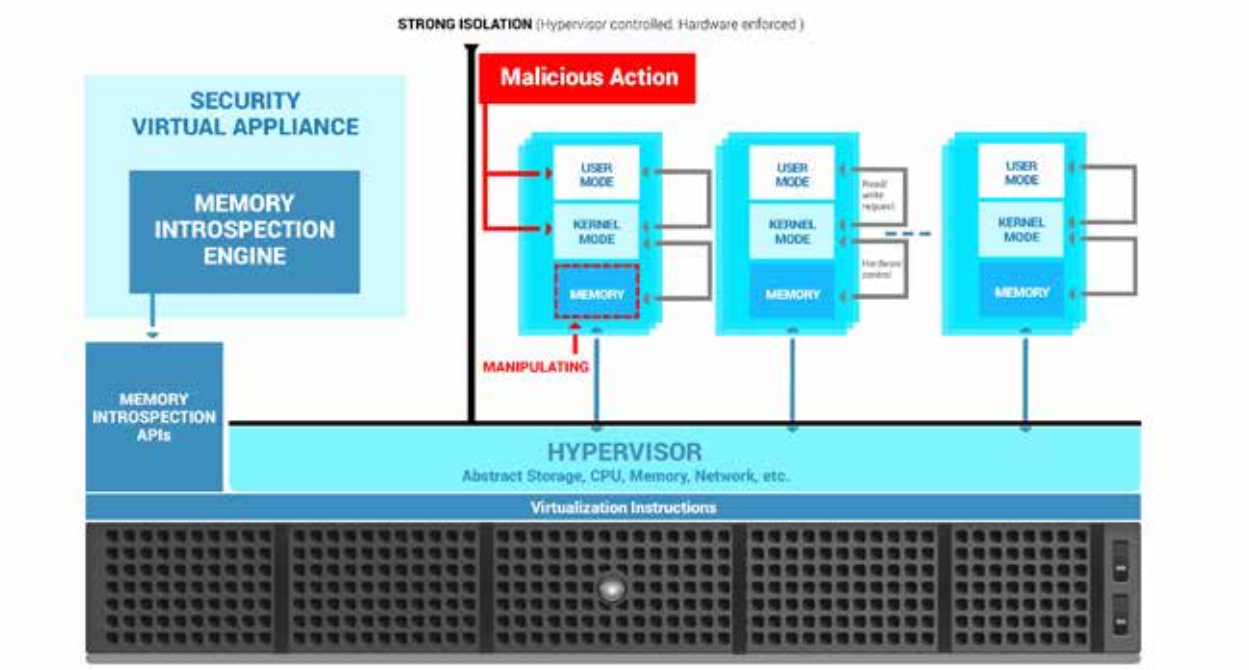
## EINE INNOVATIVE NEUE SICHERHEITSEBENE, DIE IHRE SYSTEMRECHTE SCHÜTZT

Die Zusammenarbeit von Bitdefender und Citrix verschafft Rechenzentrumsbetreibern die Möglichkeit, jetzt auf Informationen zu reagieren, die bisher nicht zugänglich waren.

**Bitdefender Hypervisor Introspection (HVI)**

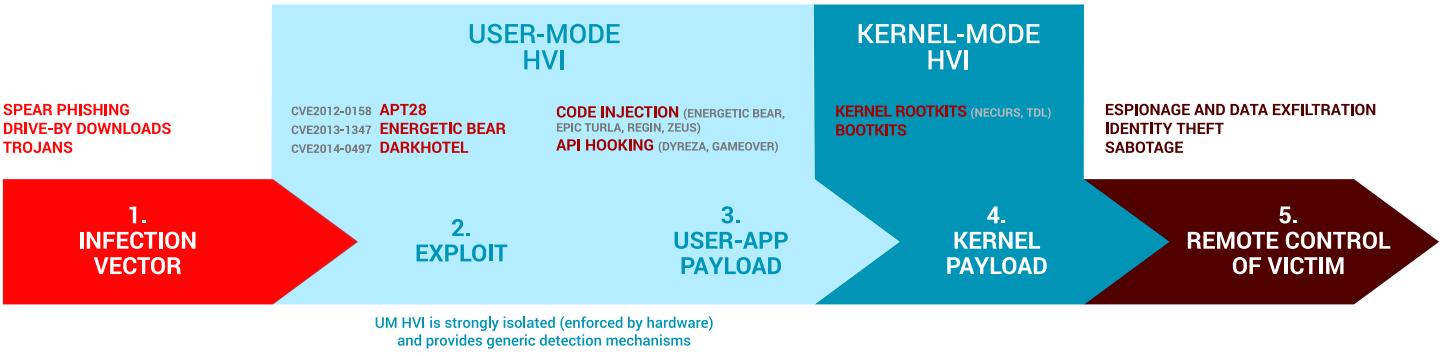
HVI erkennt auch Angriffe, die sich bereits seit Tagen, Wochen oder sogar Monaten in Ihrer Infrastruktur verborgen haben, um unbemerkt Informationen und Daten zu sammeln. HVI geht von Anfang an nicht von einem sauberen System aus; Sie können HVI anweisen, mit den entsprechenden Tools eine Bereinigung auf den produktiven virtuellen Maschinen durchzuführen - ein Vorgang, der nur vorübergehend Ressourcen im Live-System beansprucht. Ihr eigentlicher Endpunktschutz übernimmt aus der virtuellen Maschine heraus den Rest.

HVI kann auch zukünftige Sicherheitsverletzungen verhindern und lässt Sie alle Aktivitäten in Ihrem Rechenzentrum lückenlos überwachen.




## NACHWEISLICHER SCHUTZ VOR GEZIELTEN ANGRIFFEN

HVI erkennt und stoppt bekannte zielgerichtete Angriffe wie Carbanak, Turla, APT28, NetTraveler oder Wild Neutron bereits im Vorfeld, ohne die von den Angreifern ausgenutzten Schwachstellen zu kennen.




Zu den zielgerichteten Angriffen, die von HVI erkannt werden, gehört auch eine von Bitdefender im Jahre 2015 aufgedeckte, breit angelegte Cyberspionage-Kampagne mit dem Namen APT28. Dabei infiltrierten die Angreifer vollkommen unbemerkt die Systeme von Politikern, Cybersicherheitsbehörden, Telekommunikationsanbietern und Luft- und Raumfahrtunternehmen in den USA und Osteuropa, erbeuteten Passwörter und verschafften sich Systemrechte.

Ganz zufällig trafen sich zu eben dieser Zeit Spitzenpolitiker aus Weißrussland, Russland, Deutschland, Frankreich und der Ukraine zu einem Gipfeltreffen in Minsk, um sich auf einen Waffenstillstand im ostukrainischen Donbass zu einigen.[4]

4 http://download.bitdefender.com/resources/media/materials/white-papers/en/Bitdefender_In-depth_analysis_of_APT28–The_Political_Cyber-Espionage.pdf

## MINIMALE INVESTITIONEN. EINFACHE BEREITSTELLUNG.

Anders als bei anderen Anbietern, bei denen Sie Ihren bisherigen Endpunktschutz durch die neue Lösung ersetzen müssen, kann HVI ergänzend zu bereits installierter Sicherheitssoftware eingesetzt werden. Dabei wird eine neue Sicherheitsebene geschaffen, die mit jeder bereits vorhandenen Lösung für den Endpunktschutz kompatibel ist.

HVI lässt sich auch in Kombination mit bereits installierten agentenbasierten Lösungen einsetzen und verhindertso, dass sich Angreifer in Ihrer Infrastruktur Systemrechte verschaffen oder sich Ihren Gastsystemen verbergen.

## JETZT AUSPROBIEREN

Lernen Sie mehr über Bitdefender Hypervisor Introspection, und bitten Sie um eine Demonstration auf www.bitdefender.de/hvi

## SYSTEMANFORDERUNGEN

### Unterstützte Gast-Betriebssysteme

Windows-Desktop-Betriebssysteme:

· Windows 10
· Windows 8.1
· Windows 8
· Windows 7

Windows-Server-Betriebssysteme:

· Windows Server 2012 R2
· Windows Server 2012
· Windows Server 2008 R2

Linux-Betriebssysteme:

· Debian 8.2, 64-bit
· Ubuntu 16.04 LTS, 64-bit
· Ubuntu 15.04, 64-bit
· Ubuntu 14.04 LTS 64-bit
· CentOS 7, 64-bit
· Red Hat Enterprise Linux 7, 64-bit

### Host-Anforderungen

CPU-Micro-Architektur:

· Jeder Intel® Sandy Bridge-Prozessor oder neuere Versionen, die Intel® Virtualization-Technologie unterstützen.

· VT-x oder VT-d-Endungen müssen in BIOS aktiviert sein.

Software-Anforderungen:

· XenServer 7 oder höher

Bitdefender

Bitdefender ist ein Anbieter von Sicherheitstechnologien, dessen Lösungen über ein innovatives Netzwerk aus Value-Added-Kooperationen, Vertriebspartnern und Wiederverkäufern in über 100 Ländern verfügbar sind. Seit 2001 konnte Bitdefender immer wieder mit preisgekrönter Sicherheitstechnologie für Unternehmen und Privatanwender überzeugen und sich als einer der führenden Anbieter von Sicherheitslösungen für Virtualisierungs- und Cloud-Technologien etablieren. Bitdefender hat seine preisgekrönten Technologien mit den passenden Vertriebskooperationen und Partnerschaften kombiniert und seine globale Marktposition durch die strategische Zusammenarbeit mit den weltweit führenden Virtualisierungs- und Cloud-Technologieanbietern gestärkt.

Alle Rechte vorbehalten. © 2017 Bitdefender. Alle hier genannten Handelsmarken, Handelsnamen und Produkte sind Eigentum des jeweiligen Eigentümers. Weitere Informationen erhalten Sie unter www.bitdefender.de.

BD-NGZ-Mar.30.2017-Tk#.84225