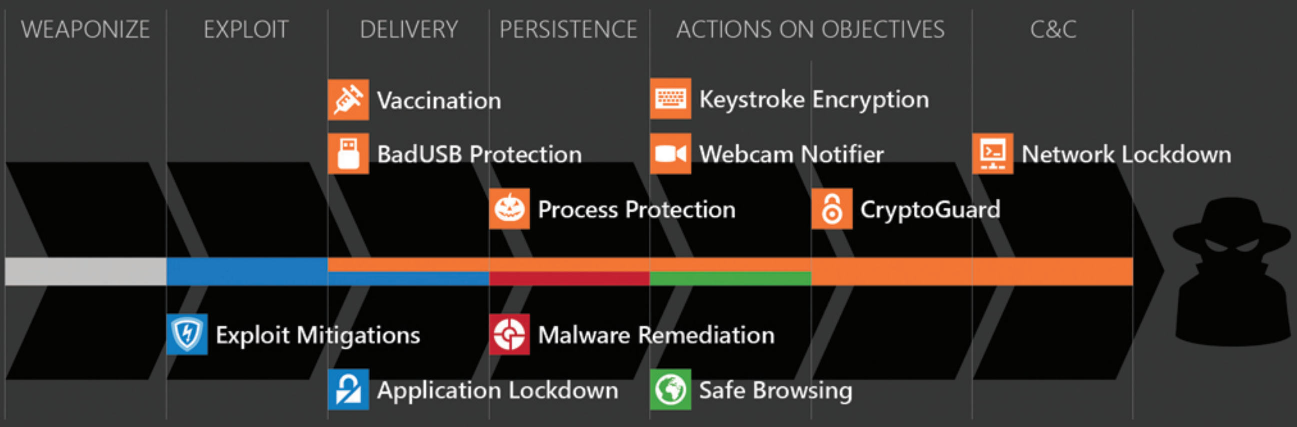
SurfRight

Bullet-proof vest for your applications and data, stops exploits and malware from cyber-insurgents and (nation-state) attackers

Disrupting the Cyber Kill Chain®

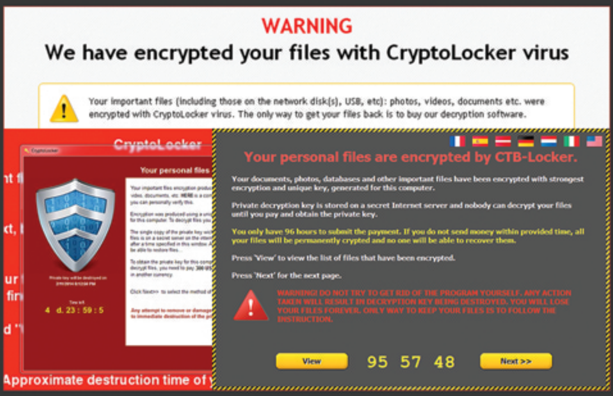
Alternative endpoint security solutions only focus on blocking malware delivery from web pages and email attachments, but HitmanPro.Alert also recognizes the capabilities of more devious attackers. It is purpose-built to disrupt attacks in real-time across the entire threat life-cycle or Cyber Kill Chain®. HitmanPro.Alert not only offers exemplary exploit technique prevention and advanced malware remediation, its many Risk Reduction features also limit motivated and skilled attackers' abilities when they do succeed in compromising the endpoint.



Disrupting individual chains of the Cyber Kill Chain® with multiple signature-less technologies

CryptoGuard stops ransomware

The exclusive Risk Reduction features of HitmanPro.Alert include behavior-based protection against high-impact crypto-ransomware, a prolific threat that slips by web filters and antivirus defenses every day. This type of infection—also generalized as cryptolocker—goes after images, documents, and other personal and critical data on local disks and networked drives. Cryptolocker malware encrypts the computer files of its victims and demands ransom money for the decryption key. The signature-less operation of HitmanPro.Alert's **CryptoGuard** technology universally prevents spontaneous encryption of data by cryptolockers. Even when trusted files or processes are hijacked for unsolicited encryption—as observed in cryptolockers "VaultCrypt", "CryptoWall" and "CTB-Locker"—it is stopped and reverted by HitmanPro.Alert, without interaction from users or IT support personnel.



WARNING

We have encrypted your files with CryptoLocker virus

Your important files (including those on the network disk(s), USB, etc): photos, videos, documents etc. were encrypted with CryptoLocker virus. The only way to get your files back is to buy our decryption software.

CryptoLocker

Your personal files

4 d. 23 : 59 : 5

Approximate destruction time of y

Your personal files are encrypted by CTB-Locker.

Your documents, photos, databases and other important files have been encrypted with strongest encryption and unique key, generated for this computer.

Private decryption key is stored on a secret Internet server and nobody can decrypt your files until you pay and obtain the private key.

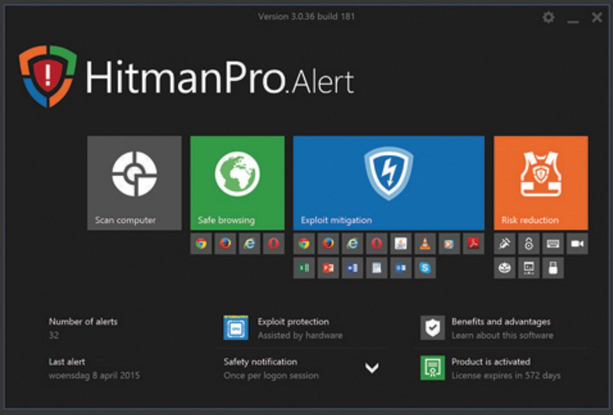
You only have 96 hours to submit the payment. If you do not send money within provided time, all your files will be permanently crypted and no one will be able to recover them.

Press 'View' to view the list of files that have been encrypted.

Press 'Next' for the next page.

WARNING! DO NOT TRY TO GET RID OF THE PROGRAM YOURSELF. ANY ACTION TAKEN WILL RESULT IN DECRYPTION KEY BEING DESTROYED. YOU WILL LOSE YOUR FILES FOREVER. ONLY WAY TO KEEP YOUR FILES IS TO FOLLOW THE INSTRUCTION.

CryptoLocker, TorrentLocker and CTB-Locker ransomware extortion screens



Version 3.0.36 build 181

HitmanPro.Alert

Number of alerts
32

Last alert
woensdag 8 april 2015

Exploit protection
Assisted by hardware

Safety notification
Once per logon session

Benefits and advantages
Learn about this software

Product is activated
License expires in 572 days

Advanced user interface for power users and IT professionals

Risk reduction

Other Risk Reduction features focus e.g. on anti-espionage, such as kernel-level **Keystroke Encryption**, **Webcam Notifier** and **BadUSB Protection**. Moreover, **Vaccination** and **Process Protection** will deter or make malware self-terminate, where **Safe Browsing** and **Application Lockdown** reveal malware that hide inside or attempt to piggyback on trusted programs to gain persistence or hoist in additional payloads.

Whether computers are targeted indiscriminately or singled out in a watering-hole or spear-phishing attack, HitmanPro.Alert offers high-performance protection without requiring virus signatures or prior knowledge of attacks. The install-and-forget software is just 5 MB in size and runs on 32-bit and 64-bit versions of Windows XP, Windows Vista, Windows 7, Windows 8.1 and Windows 10.

SurfRight | Lansinkesweg 4 | 7553 AE | Hengelo | The Netherlands
Phone +31 74 250 4147 | www.surfright.com | info@surfright.com

More information & download: www.hitmanpro.com/alert
For a free license, send an e-mail to: sales@hitmanpro.com

Exemplary exploit technique prevention

Hardware-assisted Control-Flow Integrity

HitmanPro.Alert further raises the bar for exploit attacks. Its innovative hardware-assisted Control-Flow Integrity (CFI) technology is a new approach to prevent attackers from hijacking control-flow of internet-facing applications, like web browsers, Office and other productivity software. To defeat security technologies like DEP and ASLR, control-flow attacks are nowadays common practice. These attacks are invisible to antivirus and other cyber-defenses as there are no malicious files involved. Instead, the attack is constructed in real-time by combining short pieces of benign code, that are part of existing applications, like Internet Explorer and Adobe Flash Player—a so-called code-reuse or return-oriented programming (ROP) attack.

HitmanPro.Alert achieves this new capability by leveraging an unused hardware feature in mainstream Intel® processors to track code execution, assisting detection of advanced exploit attacks in real-time. Employing hardware-traced records has a significant security benefit over software stack-based approaches. Stack-based solutions like Microsoft EMET, rely on stack data, which is—especially in case of a ROP attack—under control of the attacker, who in turn can mislead the defender. In contrast, the hardware-traced data examined by HitmanPro.Alert is more reliable and tamper resistant—a definite edge over existing solutions.

Description	MBAE 1.06	EMET 5.2	Traps 3.1.3	Alert 3.0
Enforce Data Execution Prevention (DEP) Prevents exploit code running from data memory	Yes	Yes	Yes	Yes
Mandatory Address Space Layout Randomization (ASLR) Prevents predictable code locations	- BottomUp only	Yes OS Limited	Yes Including XP	Yes Including XP
Null Page Stops exploits that jump via page 0	-	Yes	Yes	Yes
Dynamic Heap Spray Stops attacks that spray suspicious sequences on the heap	- Pre-allocated	- Pre-allocated	Yes	Yes
Stack-based Anti-ROP Stops return-oriented programming attacks (ROP)	Yes	Yes 32-bit only	Yes	Yes
Hardware-assisted Control-Flow Integrity (CFI) Stops advanced ROP attacks	-	-	-	Yes Intel® only
Caller Stops exploit code that facilitates attacks executing on the heap	Yes	Yes 32-bit only	-	Yes
Import Address Table Filtering (IAF) Stops attackers that lookup API addresses in the IAT	-	- EAF, EAF+	-	Yes
Stack Pivot Stops abuse of the stack pointer	Yes	Yes	Yes	Yes
Stack Exec Stops attacker's code on the stack	Yes	Yes	-	Yes
Load Library Blocks libraries that load reflectively or from UNC paths	Yes UNC path only	Yes UNC path only	Yes	Yes
Shellcode Stops code execution in the prescense of exploit shellcode	-	-	-	Yes
Application Lockdown Stops logic-flaw attacks that bypass mitigations	Yes	-	Yes Manually	Yes
Process Protection Stops attacks that perform process hijacking or replacement	-	-	-	Yes
Ransomware Protection Stops attackers that encrypt documents for extortion	-	-	-	Yes
Man-in-the-Browser Detection Reveals intruders that manipulate critical browser functions	-	-	-	Yes
Malware Scan and Remediation Integrated Anti-Malware	-	-	-	Yes

The table above is a product feature comparison, not a review.

For an independent product review and comparison, see "MRG Effitas Real World Exploit Prevention Test March 2015", available from: **www.hitmanpro.com/reviews**