

Best Practices – Advanced & Zero-Day Malware mit Firebox am Gateway blockieren

Thomas Fleischmann

Senior Sales Engineer, Central Europe

Thomas.Fleischmann@watchguard.com

Agenda

- Aktuelle Situation
 - Zero-Day Attacken
 - Ramsonware
- Lösungsansatz von WatchGuard
 - Multi-Layer Ansatz
- APT Blocker in der aktuellen Version (FireWare 12.0)
 - Unterstützte Formate
 - Neue Funktionen

A stylized globe is centered in the image, rendered in a dark red color. Overlaid on the globe is a complex network of white lines and nodes, resembling a global communication or data network. The nodes are small white circles, and the lines are thin white arcs that crisscross the globe. The background is a solid, vibrant red color. A horizontal white bar is positioned across the middle of the image, containing the text "Aktuelle Situation".

Aktuelle Situation

Aktuelle Situation

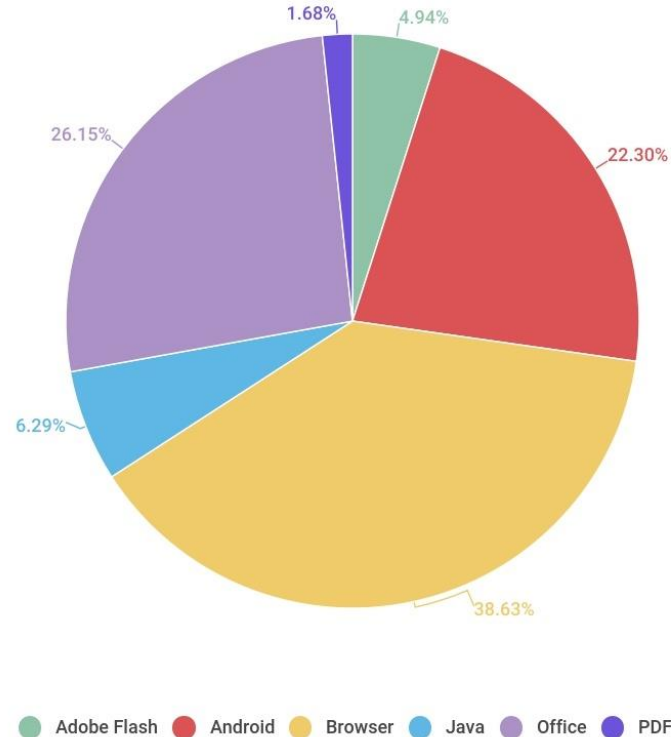
- **Eine Zero Day Exploit Attack (ZETA) ist ein Angriff, der am selben Tag erfolgt, an dem die hierbei ausgenutzte Schwachstelle in der entsprechenden Software entdeckt wird.** In diesem Fall wird die Schwachstelle ausgenutzt, bevor sie vom Softwarehersteller durch einen Fix geschlossen werden kann.

(Quelle: <https://www.kaspersky.de/resource-center/definitions/zero-day-exploit>)



Aktuelle Situation

- Unser Partner Kaspersky hat in seinen aktuellen Bericht zur Sicherheitslage im Q2 2017 folgendes dargestellt:
- Kaspersky Lab hat allein im **zweiten Quartal 2017** mehr als fünf Millionen Angriffsversuche unter Verwendung von Netzwerk-Exploits blockiert.
- Viele zu den Anstieg der Angriffe hat die Veröffentlichung der **Hacker Gruppe Shadow Brokers** beigetragen. Diese hatten Informationen von einem Hack in einen amerikanischen Geheimdienst zu Exploits und Sicherheitslücken verfügbar gemacht.





Ooops, your files have been encrypted!

English

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

CMT from Monday to Friday

Payment will be raised on

1/4/1970 01:00:00

Time Left

00:00:00:00

Your files will be lost on

1/8/1970 01:00:00

Time Left

00:00:00:00

[About bitcoin](#)

[How to buy bitcoins?](#)

[Contact Us](#)



Send \$600 worth of bitcoin to this address:

13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94

Copy

Check Payment

Decrypt

Ransomware entwickelt sich



Ransomware-as-a-Service ist aufgetaucht



Customer Service für die Finanztransaktion



Preis steigt nach 72 Stunden



Gezielte Angriffe mit Ransomware sind sehr effektiv



Schneeballsystem

Die Kosten von Einbrüche und Ransomware-Angriffe



- Ransomware verursacht etwa \$ 1 Milliarde Verluste im Jahr 2016
- Weniger als die Hälfte, die bezahlten (45%), bekam ihre Informationen zurück.
- Im Jahr 2016 erhöhte sich die Ransomware-Varianten um 752%
- Mehr als 153.000 Nutzer wurden im Jahr 2016 von mobilen Ransomware getroffen

Ramsonware

- Comeback eines alten Bekannten

Date added (UTC)	Threat	Malware	Host (?)	Domain Registrar (?)	IP address (ASN, Country)
2017-09-20 08:49	Distribution Site	Locky	● rockrak.com	GoDaddy.com, LLC	68.171.49.151 (🇺🇸 United States)
2017-09-20 07:35	Distribution Site	Locky	● lowlender.com	GoDaddy.com, LLC	72.3.203.97 (🇺🇸 United States)
2017-09-20 07:34	Distribution Site	Locky	● mebel.wladim	ENTER-RU	84.53.200.22 (🇷🇺 Russian Federation)
2017-09-20 07:34	Distribution Site	Locky	● hydrodesign.r	NIC, Inc.	66.135.55.8 (🇺🇸 United States)
2017-09-20 07:33	Distribution Site	Locky	● keener-music	Inc.	216.222.196.158 (🇺🇸 United States)
2017-09-20 07:33	Distribution Site	Locky	● dealer.my-be	rar.eu	169.53.41.9 (🇺🇸 United States)
2017-09-20 07:32	Distribution Site	Locky	● countryhome.dmw123.com	Tucows Domains Inc.	66.36.173.184 (🇺🇸 United States)
2017-09-20 07:32	Distribution Site	Locky	● dkck.com.tw	PCHOME	60.199.166.77 (🇹🇼 Taiwan)



The image features a central globe rendered in a dark red color, set against a lighter red background. Overlaid on the globe is a complex network of white lines and nodes, resembling a global communication or data network. The lines are thin and curved, connecting several bright white nodes that are positioned at various points across the globe. The overall aesthetic is modern and technological.

Lösungsansatz von WatchGuard

Schutzmaßnahmen

Awareness
Training



regelmäßige
Backups



Patch
Management



Sichere Netzwerk-
Segmentierung



Endpoint
Security



Lösungsansatz mit WatchGuard Total Security

FUNDAMENTAL SECURITY SERVICES



INTRUSION PREVENTION
SERVICE (IPS)



REPUTATION ENABLED
DEFENSE SERVICE (RED)



SPAMBLOCKER



GATEWAY ANTIVIRUS (GAV)



WEBBLOCKER



APPLICATION CONTROL

ADVANCED SECURITY SERVICES



APT BLOCKER



THREAT DETECTION & RESPONSE



HOST
RANSOMWARE
PREVENTION (HRP)



DATA LOSS PREVENTION
(DLP)

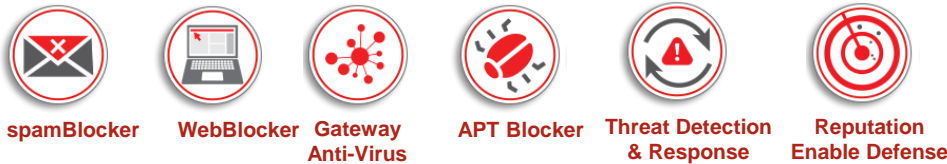


NETWORK DISCOVERY

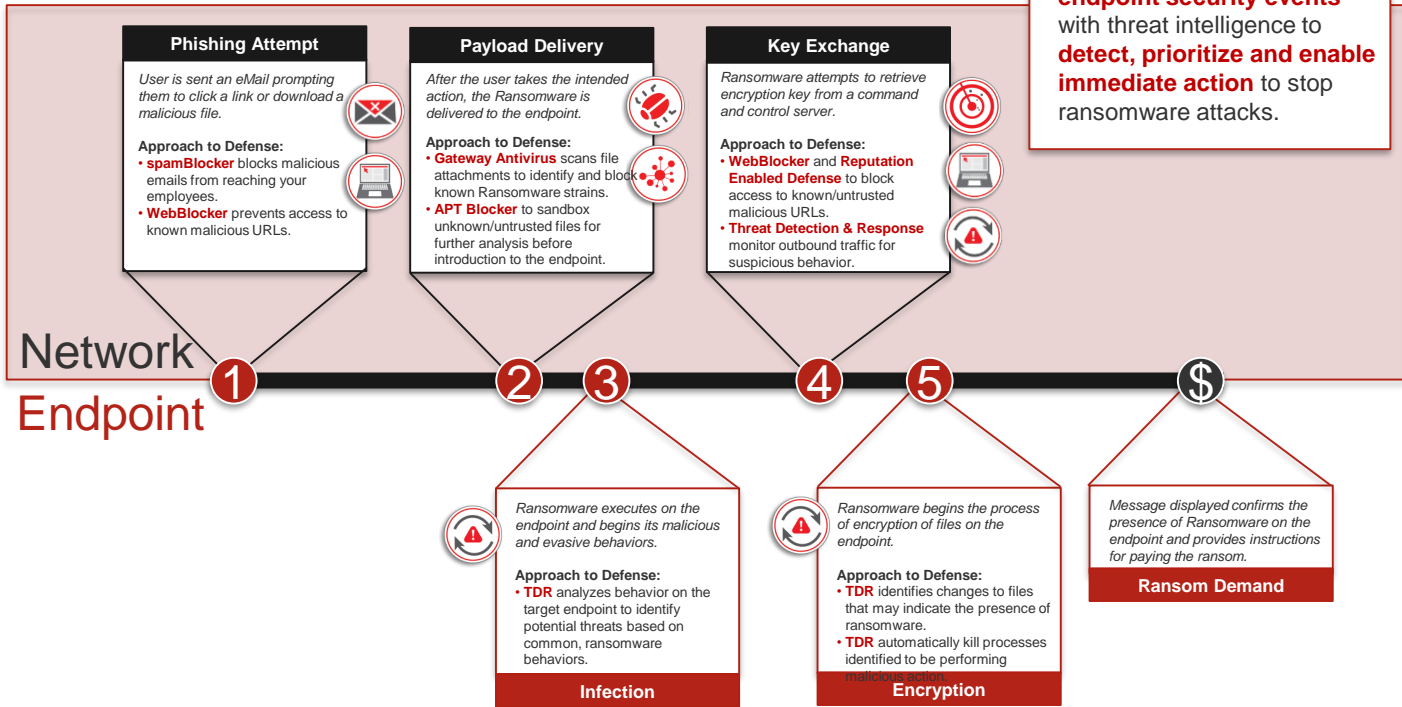


DIMENSION
COMMAND

WatchGuard Firebox UTM mit der Total Security Suite schützt gegen alle 5 Stufen eines Ransomware-Angriffs



The WatchGuard approach to ransomware defense **correlates network and endpoint security events** with threat intelligence to **detect, prioritize and enable immediate action** to stop ransomware attacks.



The image features a central globe rendered in a dark red color, showing the continents. Overlaid on the globe is a complex network of white, glowing lines that form various orbits and paths. At several points along these lines are small, bright white circular nodes. The entire scene is set against a background of horizontal red lines that create a sense of depth and motion. A semi-transparent red horizontal band is positioned across the middle of the image, serving as a backdrop for the text.

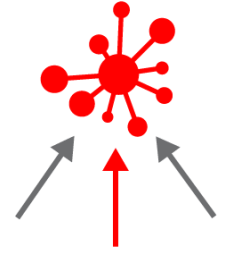
APT Blocker

APT Blocker

- APT Blocker ist ein Next Generation Sandbox Verfahren, welches ermöglicht, moderne Malware, wie etwa Ransomware oder APTs, schnell und sicher zu erkennen.
- Die Analyse der unbekanntes Datei erfolgt in einen Daten Center, welches in Amsterdam steht.
- Welche technische Voraussetzungen und Funktionen sind beim APT Blocker in der aktuellen Version gegeben?

APT Blocker

Unterstützte Firebox Proxy Richtlinien



- HTTP-proxy
- HTTPS-proxy, wenn der APT Blocker innerhalb der HTTP Proxy Action für die Content Inspection eingeschaltet ist
- FTP-proxy
- SMTP-proxy
- IMAP-proxy
- POP3-proxy

APT Blocker

Unterstützte File Formate für die Datei Analyse

- Windows PE (Portable Executable) Dateien
Dies beinhaltet .cpl, .exe, .dll, .ocx, .sys, .scr, .drv, und .efi Erweiterungen, welche in 32-bit und 64-bit Versionen von Windows Betriebssysteme verwendet werden.
- Adobe PDF Dokumente
- Microsoft Office Dokumente
- Rich Text Format (RTF) Dokumente
- Android ausführbare Dateien(.apk)
- Apple Mac Applikation Dateien(.app)
- JavaScript (.js) Dateien (nur in E-Mail Anhängen)

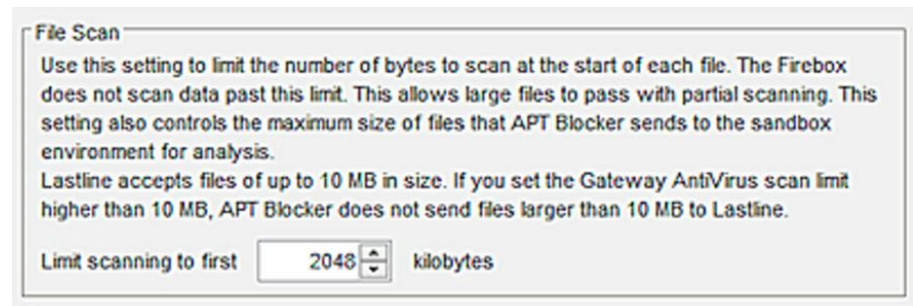
- Kompression Formate: gzip, tar, zip, rar und 7z

APT Blocker

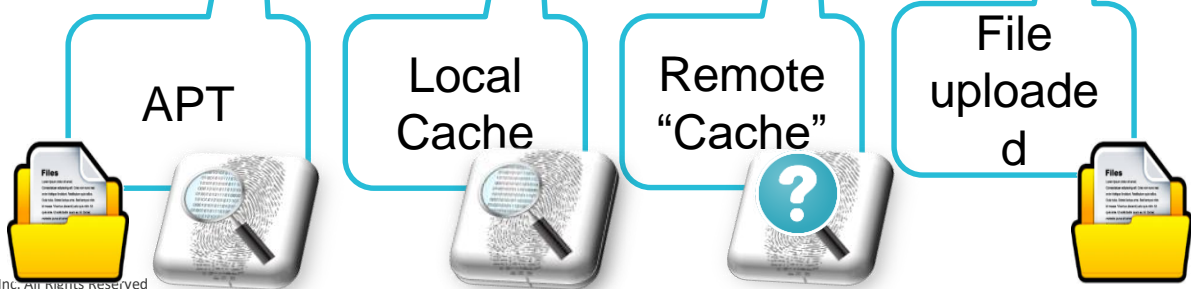
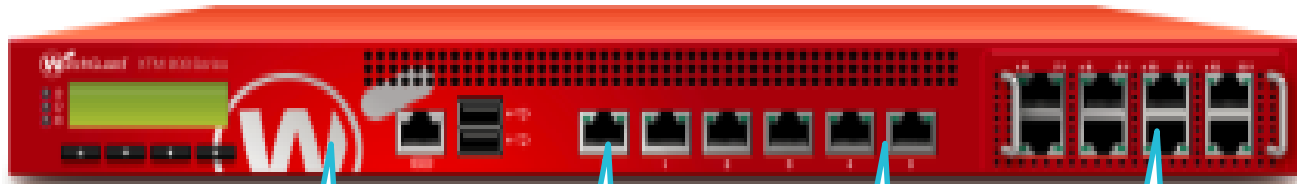
- Zusammenspiel mit den Gateway Anti-Virus (GAV)
- APT Blocker und GAV laufen im selben Prozess
- Wenn der GAV eine Datei als „sauber“ klassifiziert, werden die Dateien, die vom APT Blocker untersucht werden können, an diesen übergeben.

Voraussetzung:

- Datei liegt vollständig vor und ist nicht grösser als 10 MB.
 - Hier muss das eingetragene „Scan Limit“ des GAV beachtet werden.



Analyse



Neu Funktion in der FireWare Version 12.0

- Im Bereich SMTP- und IMAP-Proxy wurde das Verhalten des APT Blocker erweitert.
- Im SMTP Proxy ist das Standard Verhalten, dass eine Datei, die unbekannt ist, an das Daten Center zur Analyse gesendet wird, und die Datei den Endbenutzer zugestellt wird.
- Das Verhalten kann man verändern, in den man den Punkt „Release messages immediately when attachments are submitted for APT Blocker analysis“ deaktiviert.
- Der SMTP Proxy hält nun die Verbindung und sendet die Datei zur Analyse hoch in das Daten Center.
- Wenn der APT Blocker in der Zeit des Halten der Verbindung eine Rückmeldung erhält, wendet er seine Richtlinie an.
- Wenn die Zeit nicht ausreicht, dann beendet der SMTP Proxy die Verbindung mit einer Meldung 451. Der absende Server wird dann die Email nach ca. 10 Minuten versuchen, wieder zu zustellen.

Neu Funktion in der FireWare Version 12.0

- Bei IMAP Proxy ist das Verhalten ähnlich
 - Der IMAP Proxy untersucht alle Datei Anhänge in der Email.
 - Die Email wird erst zugestellt, wenn alle Anhänge analysiert sind und ein eindeutiges Ergebnis vorliegt.
 - Wenn der Timeout vor der Analyse eintritt, wird beim nächsten Abruf der Dateien das nun vorliegende Ergebnis verwendet und die Email mit oder ohne Anhang zugestellt.
-
- Konfigurations-Ansicht im SMTP-Proxy:

APT Blocker

- Enable APT Blocker

The SMTP proxy uses APT Blocker when Gateway AntiVirus is enabled.

- Release messages immediately when attachments are submitted for APT Blocker analysis

Select this option to enable the SMTP proxy to immediately release messages with attachments that are submitted for APT Blocker analysis.

Auswertung von APT Blocker Ereignisse

- Eine wichtige Funktion ist die Möglichkeit mit Hilfe von WatchGuard Dimension eine Auswertung von Angriffen zu erhalten.

Top Zero-Day Malware (APT)

[View All](#)

NAME	HITS	THREAT LEVEL
INFO_347663_eratung.zip(4097.zip)	1	● High

[9940747.zip\(26747.zip\)](#)

Malware (APT)

[830561775258.zip\(32670.zip\)](#)
[227542.zip\(23514.zip\)](#)
804

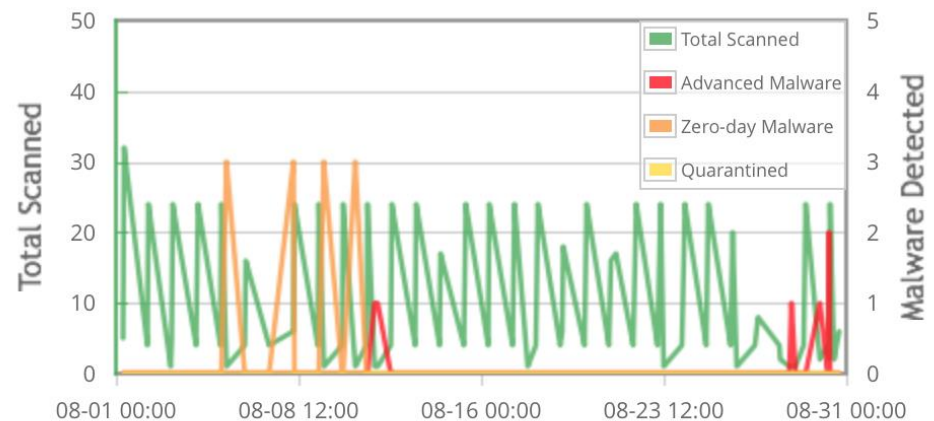
Total scanned

6

 Advanced
malware

12

Zero-day

[View Summary](#)


APT Blocker und TDR

- In der aktuellen Version von TDR wird die Sandbox Funktion von APT Blocker ebenfalls für unbekannte Dateien verwendet.
- Kennt TDR eine Datei nicht anhand des Hash Wertes und findet TDR keine Informationen zu dieser Datei im Netz, dann wird ein Upload der Datei zum Daten Center für die Analyse durchgeführt.

Additional information for process: setup.exe

Hash only found on this host

Date Created 08/25/2017 9:54:01 PM

Command C:\WINDOWS\TEMP\CR_477C8.tmp\setup.exe --type=crashpad-handler /prefetch:7 --monitor-self-annotation=ptype=crashpad-handle
r --database=C:\WINDOWS\TEMP\Crashpad --url=https://clients2.google.com/cr/report --annotation=channel= --annotation=plat=Win
64 --annotation=prod=Chrome --annotation=ver=60.0.3112.113 --initial-client-data=0x1d8,0x1e4,0x1e8,0x1dc,0x1ec,0x7ff7d558f920,0
x7ff7d558f908,0x7ff7d558f8e0

Thread Count 0

MD5 9A4947855C14AB9B61DFEDEA5885F39B

Threat Details

Score **3**

Threat Feed **NOT MATCHED** --- MATCHED

Malware Verification Service **BENIGN** --- **UNSEEN** --- POTENTIAL --- MALICIOUS (Search on: [VirusTotal](#) | [MetaScan](#) | [Google](#))

Heuristics **BELOW THRESHOLD** --- **SUSPICIOUS**
(Temp Dir EXE Location [DETAILS](#))

Loaded Modules

MODULE PATH	MD5
c:\Windows\System32\oleaut32.dll	70AD4B9AAE5AFE52C6B21DC3F768BA2E
c:\Windows\System32\psapi.dll	84C974C056801F0263FFD2DCA37C7CE2
c:\Windows\System32\bcryptprimitives.dll	C2CD640973CFFAA8EB636648F7ECCA3C
c:\Windows\System32\ws2_32.dll	C488F09F9FC8EED3420E1A309AE7C0BD
c:\Windows\System32\ole32.dll	5DEE7F9B7FF84C1EFCB7C83F0B6D3E9B

Sandbox Analysis by APT Blocker

Threat has been added to the Sandbox. [View Report](#)UNKNOWN --- **CLEAN** --- LOW --- MEDIUM --- HIGH



Live Demo



THANK YOU