How to Prevent Ransomware and Other Advanced Malware

Including CryptoWall and CryptoLocker

The number of ransomware incidents has exploded in the last few years, infecting hundreds of thousands of systems worldwide. Ransomware is malware that's designed to hold your data hostage unless you pay up. Wait too long —or try to rescue it — and that data can be gone for good.

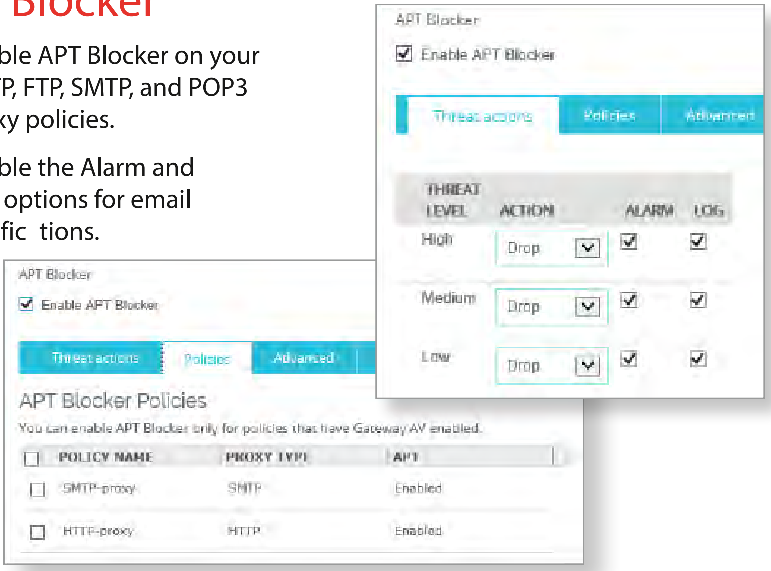
To protect your network and computers from ransomware and other malicious malware, be sure to first pe form these fundamental tasks:

- Backup and recovery
- Segment BYOD (Bring Your Own Devices) from main network
- Run antivirus software on clients

Next, follow these steps on your Firebox for maximum ransomware protection:

1. APT Blocker

- Enable APT Blocker on your HTTP, FTP, SMTP, and POP3 proxy policies.
- Enable the Alarm and Log options for email notific tions.



APT Blocker

☑ Enable APT Blocker

THREAT LEVEL	ACTION	ALARM	LOG
High	Drop	☑	☑
Medium	Drop	☑	☑
Low	Drop	☑	☑

APT Blocker

☑ Enable APT Blocker

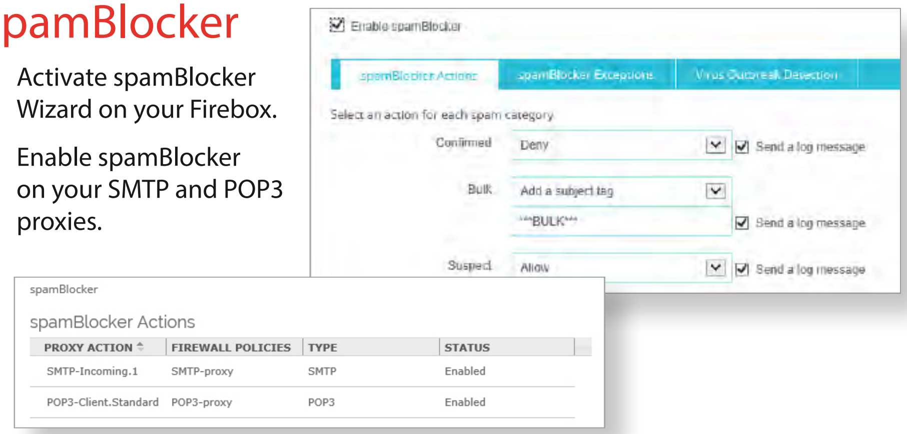
APT Blocker Policies

You can enable APT Blocker only for policies that have Gateway AV enabled.

☐	POLICY NAME	PROXY TYPE	APT
☐	SMTP-proxy	SMTP	Enabled
☐	HTTP-proxy	HTTP	Enabled

2. spamBlocker

- Activate spamBlocker Wizard on your Firebox.
- Enable spamBlocker on your SMTP and POP3 proxies.



☑ Enable spamBlocker

Select an action for each spam category

Confirmed	Deny	☑ Send a log message
Bulk	Add a subject tag ***BULK***	☑ Send a log message
Suspect	Allow	☑ Send a log message

spamBlocker

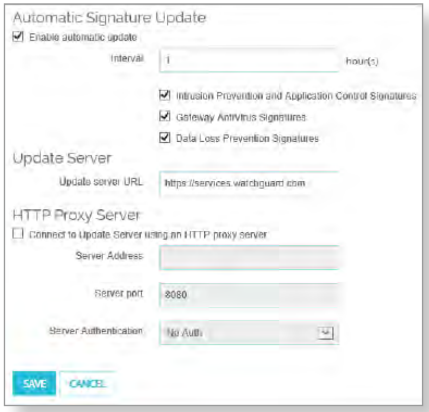
spamBlocker Actions

PROXY ACTION	FIREWALL POLICIES	TYPE	STATUS
SMTP-Incoming.1	SMTP-proxy	SMTP	Enabled
POP3-Client.Standard	POP3-proxy	POP3	Enabled

How to Prevent Ransomware and Other Advanced Malware

3. Signature Updates

- Make sure the signatures for Gateway AntiVirus, IPS, and Application Control are up to date.



Automatic Signature Update

☑ Enable automatic update

Interval: 1 hour(s)

☑ Intrusion Prevention and Application Control Signatures
☑ Gateway AntiVirus Signatures
☑ Data Loss Prevention Signatures

Update Server

Update server URL: https://services.watchguard.com

HTTP Proxy Server

☐ Connect to Update Server using an HTTP proxy server

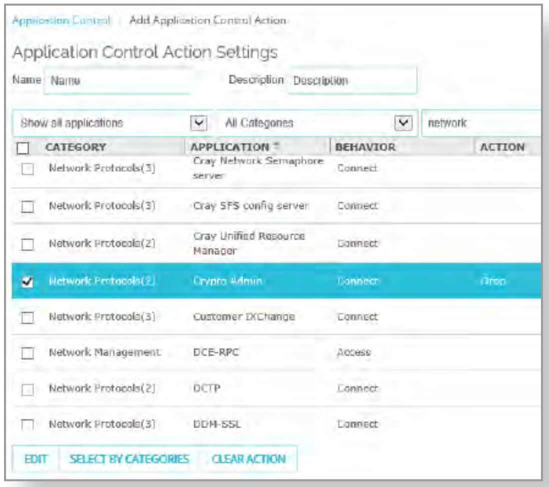
Server Address:

Server port: 8080

Server Authentication: No Auth

4. ApplicationControl

- Enable Application Control on all outgoing policies.
- Set action to Drop for the Crypto Admin application within Network Protocols.
- Block the following applications: BitComet, BitLord, BitTorrent Series, aMule, easyMule, eMule, eMule Plus.



Application Control Action Settings

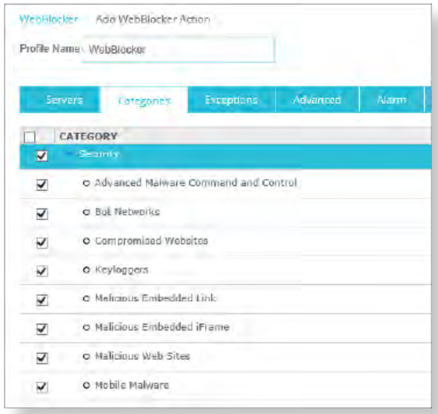
Name: Name
Description: Description

Show all applications | All Categories | network

☐	CATEGORY	APPLICATION	BEHAVIOR	ACTION
☐	Network Protocols(3)	Cray Network Semaphore server	Connect	
☐	Network Protocols(3)	Cray SFS config server	Connect	
☐	Network Protocols(2)	Cray Unified Resource Manager	Connect	
☑	Network Protocols(2)	Crypto Admin	Connect	Drop
☐	Network Protocols(3)	Customer IXChange	Connect	
☐	Network Management	DCE-RPC	Access	
☐	Network Protocols(2)	DCTP	Connect	
☐	Network Protocols(3)	DDM-SSL	Connect	

5. WebBlocker

- Enable WebBlocker on your HTTP and HTTPS proxy policies.
- Make sure Extended Protection and Security are selected.

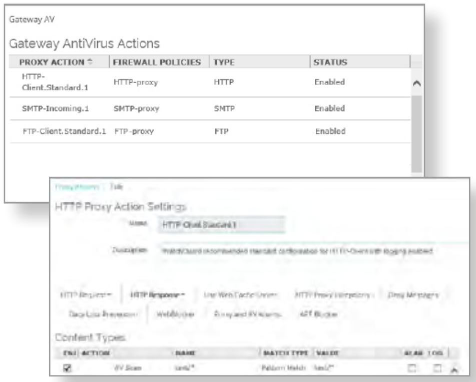


Profile Name: WebBlocker

☐	CATEGORY
☑	Security
☑	○ Advanced Malware Command and Control
☑	○ Bot Networks
☑	○ Compromised Websites
☑	○ Keyloggers
☑	○ Malicious Embedded Link
☑	○ Malicious Embedded iFrame
☑	○ Malicious Web Sites
☑	○ Mobile Malware

6. Gateway AntiVirus

- Enable Gateway AntiVirus on your HTTP, FTP, SMTP, POP3, TCP-UDP proxy policies.
- In the global Gateway AntiVirus settings, select the Enable Decompression option.
- In the HTTP Response > Content Types proxy action settings for Gateway AntiVirus, set the action to AV Scan.
- In the HTTP Response > Body Content Types proxy action settings for Gateway AntiVirus, set the action to Deny or AV Scan for .exe file .



Gateway AntiVirus Actions

PROXY ACTION	FIREWALL POLICIES	TYPE	STATUS
HTTP-Client.Standard.1	HTTP-proxy	HTTP	Enabled
SMTP-Incoming.1	SMTP-proxy	SMTP	Enabled
FTP-Client.Standard.1	FTP-proxy	FTP	Enabled

HTTP Proxy Action Settings

Name: HTTP-Client.Standard.1

Description: [illegible]

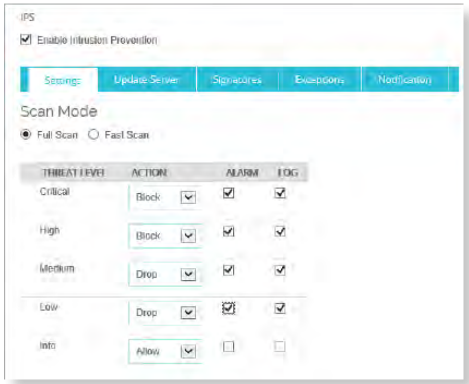
Content Types

ENABLE	ACTION	NAME	MATCH TYPE	VALUE	ALARM	LOG
☑	AV Scan	[illegible]	Pattern Match	[illegible]	☐	☐

How to Prevent Ransomware and Other Advanced Malware

7. Intrusion Prevention (IPS)

- Enable IPS on all outbound policies.
- Set action to Block for Critical and High threat level traffic.
- Choose Alarm and Log for each threat level.
- Select Full Scan or Fast Scan depending on data sensitivity level.



IPS

☑ Enable Intrusion Prevention

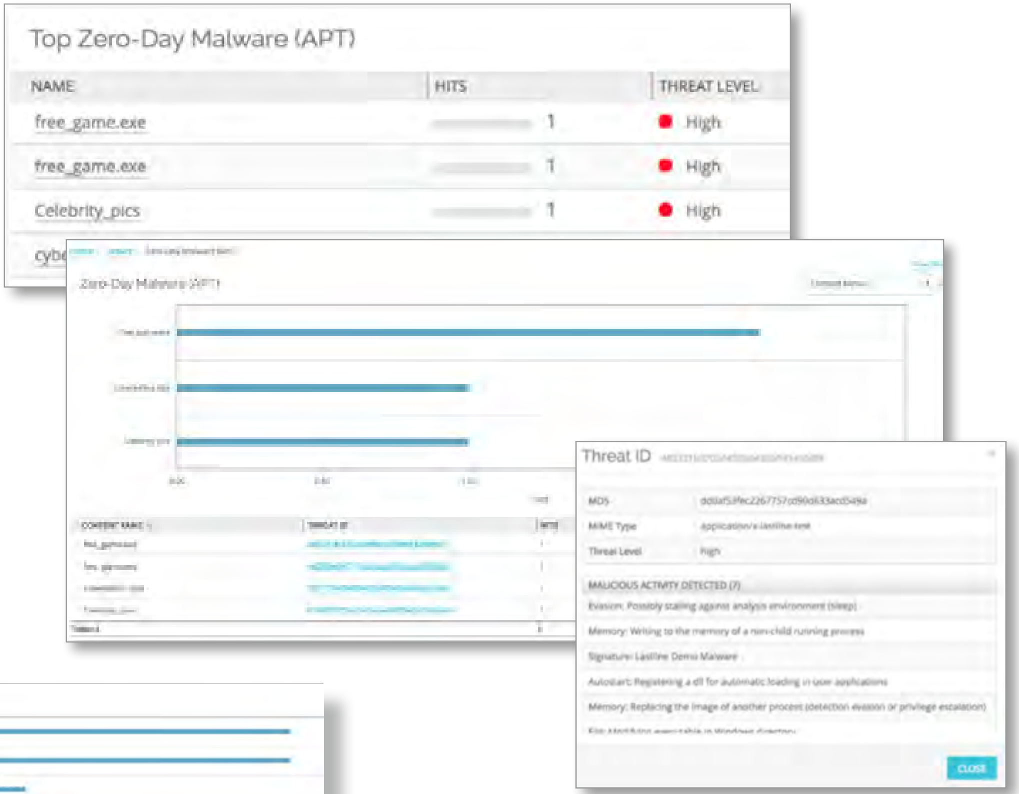
Scan Mode

● Full Scan ○ Fast Scan

THREAT LEVEL	ACTION	ALARM	LOG
Critical	Block	☑	☑
High	Block	☑	☑
Medium	Drop	☑	☑
Low	Drop	☑	☑
Info	Allow	☐	☐

8. Dimension

- Use dashboard, logs, and reports to monitor for APTs and zero day malware.



Top Zero-Day Malware (APT)

NAME	HITS	THREAT LEVEL
free_game.exe	1	● High
free_game.exe	1	● High
Celebrity_pics	1	● High
cybe		

Zero-Day Malware (APT)

Threat ID

MD5	dd0af53fec2267757cd90d633acd549a
MIME Type	application/x-lastline-test
Threat Level	high

MALICIOUS ACTIVITY DETECTED (7)

Evasion: Possibly stalling against analysis environment (sleep)

Memory: Writing to the memory of a non-child running process

Signature: Lastline Demo Malware

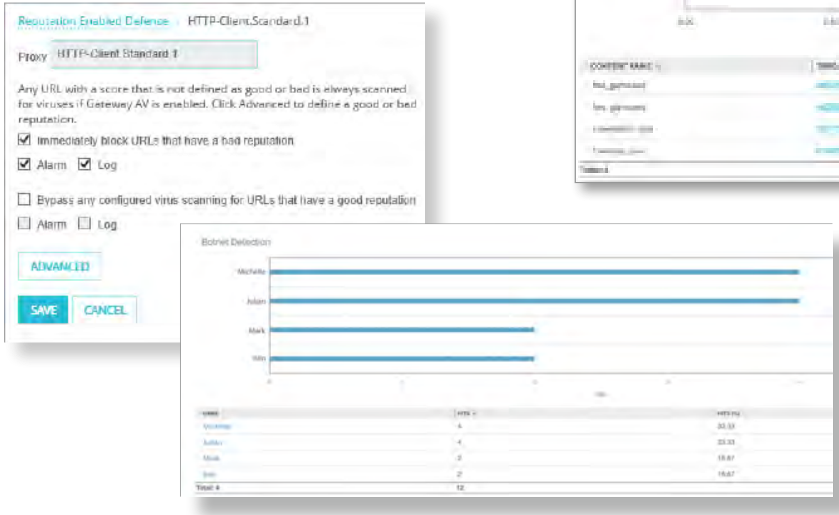
Autostart: Registering a dll for automatic loading in user applications

Memory: Replacing the image of another process (detection evasion or privilege escalation)

File: Modifying executable in Windows directory

9. Reputation Enabled Defense

- Enable Reputation Enabled Defense.
- Turn on the Alarm and Log options for notifications.
- Enable **Botnet Detection** - known botnet sites will be added to the Blocked Sites List



Reputation Enabled Defense / HTTP-Client.Standard.1

Proxy: HTTP-Client Standard 1

Any URL with a score that is not defined as good or bad is always scanned for viruses if Gateway AV is enabled. Click Advanced to define a good or bad reputation.

☑ Immediately block URLs that have a bad reputation

☑ Alarm ☑ Log

☐ Bypass any configured virus scanning for URLs that have a good reputation

☐ Alarm ☐ Log

Protect your business and customers from ransomware and other malicious malware today.

For more information, visit www.watchguard.com/aptblocker.