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 perform these fundamental tasks:

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

Is Your Firebox® Ready to Block Ransomware?

Follow these steps to defend your network from malicious malware.

1. APT Blocker

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

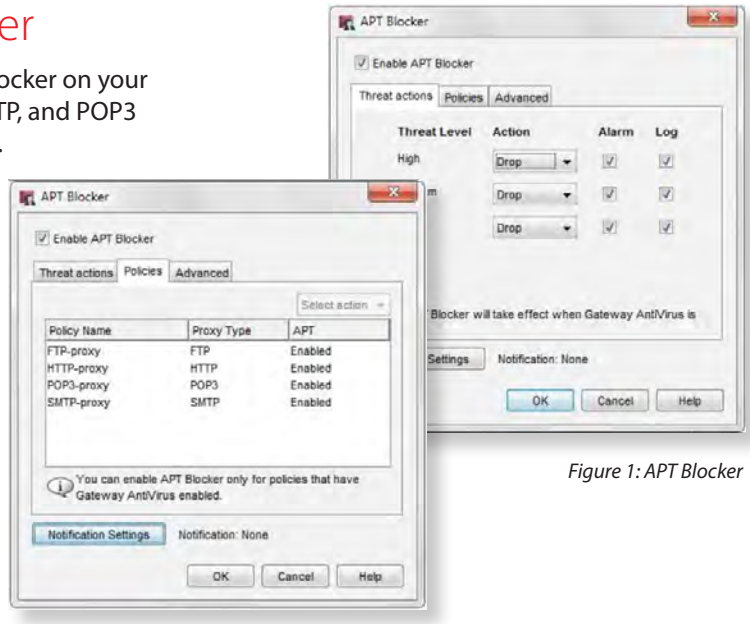

Figure 1: APT Blocker

2. Signature Updates

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

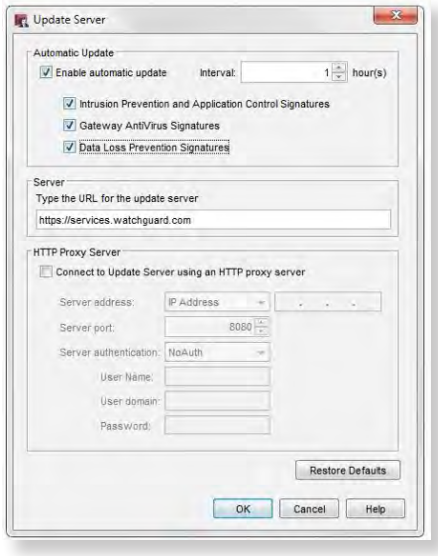

Figure 2: Signature Updates

How to Prevent Ransomware and Other Advanced Malware

3. Application Control

- 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

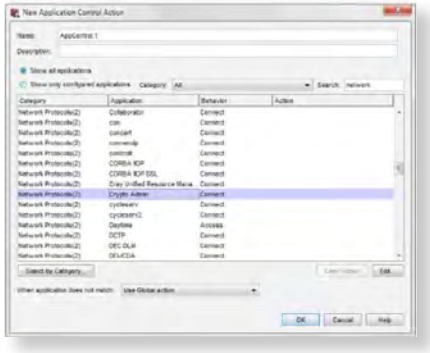

Figure 3: Application Control

4. WebBlocker

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

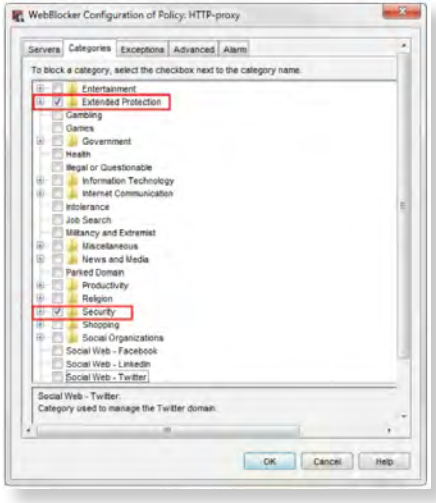

Figure 4: WebBlocker

5. 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 files.

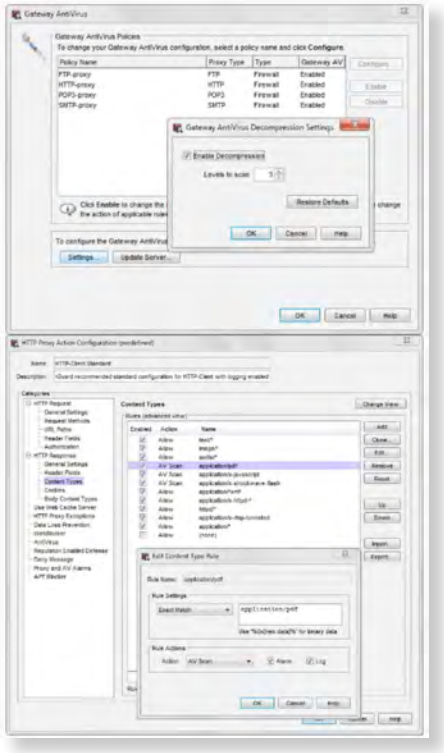

Figure 5: Gateway AntiVirus

6. 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.

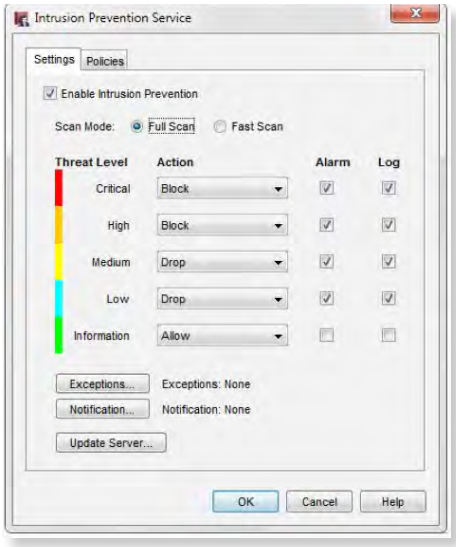

Figure 6: Intrusion Prevention (IPS)

How to Prevent Ransomware and Other Advanced Malware

7. Reputation Enabled Defense

- Enable Reputation Enabled Defense.
- Turn on the **Alarm** and **Log** options for notifications.

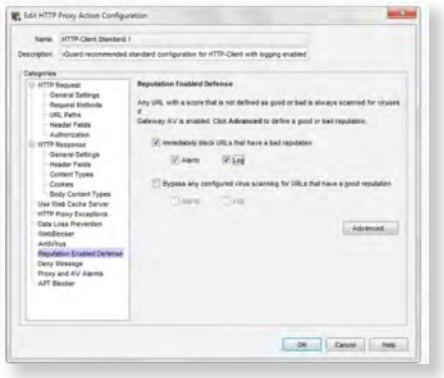

Figure 7: Reputation Enabled Defense

8. Dimension

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

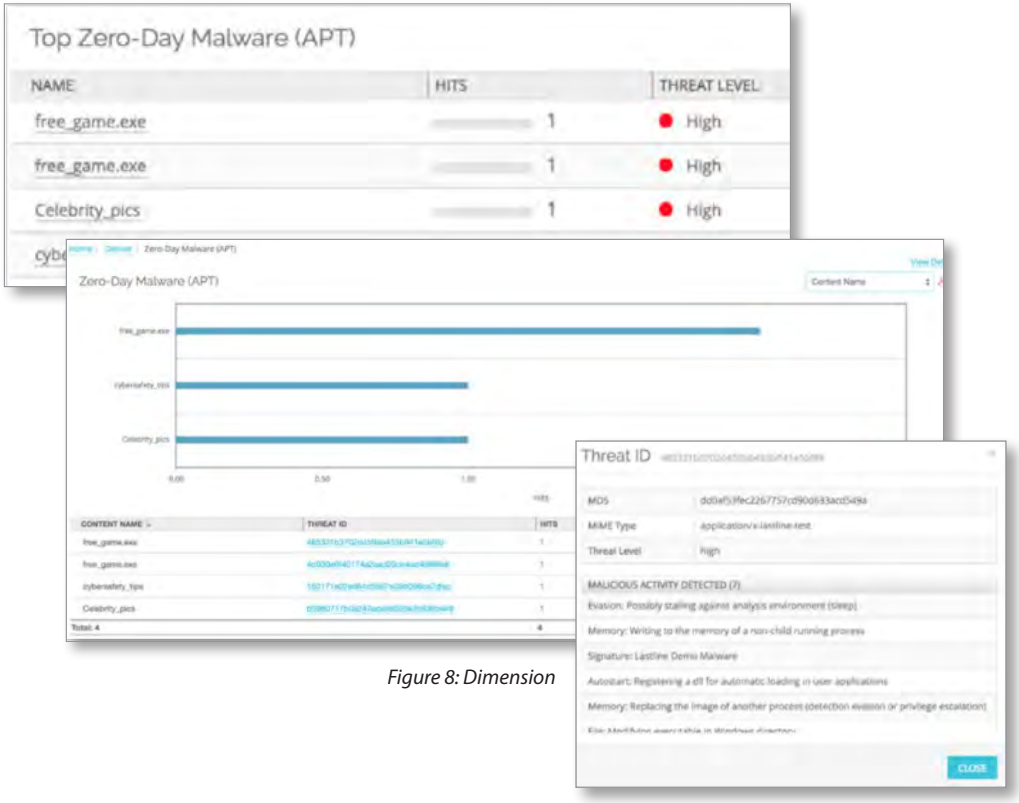

Figure 8: Dimension

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

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