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

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 notifications.

2. spamBlocker
   • Activate spamBlocker Wizard on your Firebox.
   • Enable spamBlocker on your SMTP and POP3 proxies.
3. Signature Updates

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

4. 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.

5. WebBlocker

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

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.
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.

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

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

Protect your business and customers from ransomware and other malicious malware today.
For more information, visit www.watchguard.com/aptblocker.