Preventing Ransomware Attacks with Host Ransomware Prevention

Introduction

Small and midsize businesses and distributed enterprises continue to fall victim to advanced malware attacks that have serious impact on business productivity and continuity. Ransomware, a type of advanced malware that denies victims to data and systems, has been shown to disproportionately target SMBs making these attacks the single greatest security threat facing them today. Unfortunately, whether due to cost or complexity, many small-to-midsize businesses have simply lacked the resources they need to effectively stop ransomware attacks, leading to devastating consequences.

Host Ransomware Prevention, a component of the WatchGuard Host Sensor enables organizations of all sizes to detect, and even prevent, ransomware attacks before the damage is done.

What is Ransomware?

Ransomware is a type of advanced malware attack that takes hold of a device, either locking the user out entirely or encrypting files so they cannot be used. This type of malware can infect your device in a variety of ways. Whether downloaded from a malicious or compromised website, delivered as an attachment in a phishing email or dropped by exploit kits onto vulnerable systems, once executed the ransomware will either lock the computer or encrypt predetermined files. The attacker will then make themselves known with an "official" ransom demand, as well as thorough instructions and timelines on how to make a payment to regain your assets.

Phishing for Access

One of the most common methods of delivering ransomware is through a phishing email attack. These targeted emails are often written in a way that the unsuspecting users would never know that it wasn't from a legitimate sender. They often contain a malicious link or download that grants the hacker passage to not just this device, but opens the door to your entire organization. SMBs are a key target for this type of attack, with over 40% of spear-phishing attacks aimed at organizations with fewer than 250 employees in 2015. (Verizon)

Ransomware for Sale

The sophistication of the average cybercriminal is at an all-time low. Today we can fall victim to attacks that require little or no technical skill because malware tools and services are widely available. The dark web gives criminals the ability to buy incredibly sophisticated malware variants or even have malware designed for specific targets. Even worse, the success of Ransomware has led to the emergence of ransomware-as-a-service enabling non-technical criminals to purchase not only the malware, but the means to deliver it and collects the profits as a service. This takes a complicated operation that usually needs multiple world class hackers and puts it in the hands of anyone looking to attack organizations of any size.

Defending against Ransomware

Ransomware attacks are no joke, and they are a menace to SMBs and distributed enterprise organizations. However, these tricky attacks share common behaviors that can be used in malware detection. Leveraging behavioral analysis to catch the malware attempts to evade detection and perpetrate its attack enables organizations to better defend against these attacks.

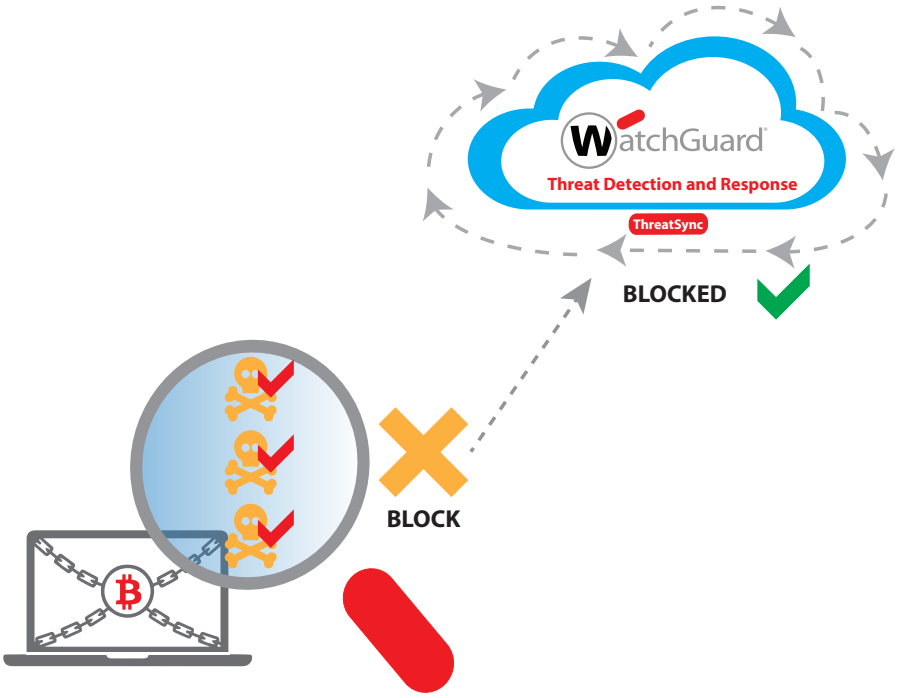
WatchGuard's newest security service, Threat Detection and Response, includes a ransomware specific module within the lightweight WatchGuard Host Sensor. Host Ransomware Prevention leverages a behavioral analytics engine and a decoy directory honeypot to monitor a wide array of characteristics determining if a given action is associated with a ransomware attack or not. If it's determined that the threat is malicious, HRP can automatically prevent a ransomware attack before file encryption on the endpoint takes place.

Total Security through Correlation

With WatchGuard Total Security Suite, organizations of all sizes can now defend against advanced malware threats, including ransomware attacks. Total Security Suite is the first UTM service offering that not only enables organizations of all sizes detect and remediate ransomware attacks, but actually prevent them as well.

Individually, each of these solutions can protect against a stage of a ransomware attacks. WebBlocker automatically denies users access to known malicious sites, and can also enables URL filtering which can block risky and inappropriate sites as well. With APT Blocker, users benefit from award-winning network sandboxing capabilities to detect suspicious threats, detonate them in a virtual environment, and stop the attack from executing on the network. Host Ransomware Prevention leverages behavioral analysis to specifically detect ransomware attacks, and prevent them before file encryption occurs.

WatchGuard's Total Security Suite combines these advanced security services to protect against ransomware providing the most comprehensive set of security services available in one offering available on the market today.



For more information on Host Ransomware Prevension, please visit our website at **www.watchguard.com/TDR.**

About WatchGuard

WatchGuard® Technologies, Inc. is a global leader in network security, secure Wi-Fi, and network intelligence products and services to more than 75,000 customers worldwide. The company's mission is to make enterprise-grade security accessible to companies of all types and sizes through simplicity, making WatchGuard an ideal solution for distributed enterprises and SMBs. WatchGuard is headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia Pacific, and Latin America. To learn more, visit WatchGuard.com.

For additional information, promotions and updates, follow WatchGuard on Twitter @WatchGuard, on Facebook, or on the LinkedIn Company page. Also, visit our InfoSec blog, Secplicity, for real-time information about the latest threats and how to cope with them at www.secplicity.org.

U.S. SALES 1.800.734.9905 INTERNATIONAL SALES +1.206.613.0895 www.watchguard.com