Keep Ransomware from Scratching at Your Door

Table of Contents

Contents

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 attack can gain access to your device in a variety of ways. Whether downloaded from a malicious or compromised website, delivered as an attachment from a phishing email or dropped by exploit kits onto vulnerable systems, once executed in the system 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 either regain access to the device or to receive the decryption key for the captive files.

Ransomware Attacks in the News:

- In late October 2016, three hospitals in the Northern Lincolnshire and Goole NHS Foundation Trust were forced to cancel operations and outpatient appointments after being forced offline as the result of a Globe2 ransomware infection.[1]
- The St. Louis Public Library received a ransom demand of $35,000 to restore data in a ransomware attack that affected over 700 computers across all 17 branches of the library system.[2]
- Hard Times Café in Rockville, Maryland, was forced to close its doors for a week and completely rebuild their POS system after being one of eight local businesses to suffer a ransomware attack in March, 2016. [3]
- Bigfork Public Schools suffered a ransomware attack that locked them out of data including students' grades and the district's directory with contact information for parents and staff, as well as social security numbers. [4]
- In January 2017, hotel staff at Romantik Seehotel Jaegerwirt in the Austrian village of Turracherho-he were unable to issue key cards to new guests, as the result of a ransomware attack that targeted their electronic key system. [5]

In this whitepaper, we will explore the true threat of ransomware to small-to-midsize businesses (SMBs), identify some unique characteristics of ransomware, and discuss ways to mitigate the threat of ransomware attacks.

Ransomware Stalks Small-to-Midsize Businesses

Ransomware is one of the most talked about and publicized security threats in the modern era. What started as a few high-profile attacks caused by a handful of malware variants has developed into a virulent threat landscape in which increasingly unskilled attackers are able to execute highly effective ransomware campaigns against organizations of all sizes and levels of complexity. From January to September of 2016, ransomware attacks against businesses increased by three hundred percent when compared to 2015 in total. During that same period the frequency of ransomware attacks against businesses accelerated from one every two minutes to one every 40 seconds.

Small-to-midsize businesses disproportionately fall victim to ransomware, as they often lack the technical skills and tools needed to prevent infection. According to research, more than 50 percent of small and midsize businesses have fallen victim to ransomware. Of those victims, 48 percent decided to pay the ransom in an attempt to retrieve their data.[7] While paying a ransom is not advised, ransomware often places organizations in the position of having to make a business decision – one where the immediate need for their data may trump their concerns about conceding to the attacker's demand.

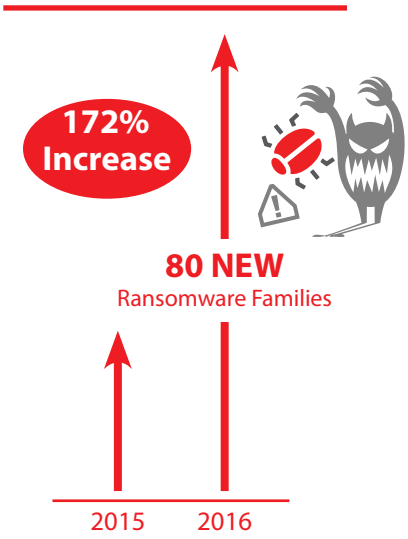
Ransomware Changes the Data Value Paradigm

Security professionals have long talked about the need to protect sensitive data as the threat of identity theft and fraud made prioritizing the security of specific types of data essential. While protecting sensitive data is by no means trivial, organizations are able to rely on a fairly straightforward formula for data protection; identify sensitive data, build protections around where that data is stored and used, and where possible keep the data encrypted.

The protection of sensitive data largely requires that you focus on the data that your attacker will find most valuable, which typically corresponds to the data that an attacker will be able to sell or use for financial gain most easily. Today, this data is highly regulated and for many organizations, its handling requires strict adherence to national and international compliance initiatives.

The emergence of ransomware marks a distinct shift in the data value formula, as attackers no longer need to focus on the market value of the data they collect, but rather derive value based on the importance of that data to you or your business. Even though the data may not be sensitive in its content, it may be business critical for your organization in the short and long term. By holding your data hostage and demanding a ransom for its return, attackers are able to monetize data for which they may have had no other use.

This paradigm shift places a host of new organizations, many of whom have long felt themselves too small to be an appealing target for cyber attacks, firmly in the crosshairs of an increasingly unsophisticated onslaught of attackers.



Ransomware for Sale! Black Market for Ransomware Tools Minimizes the Barrier to Entry

Ransomware is at epidemic levels as evidenced by a Trend Micro report that showed 80 new ransomware families were discovered in the first half of 2016, an increase of 172 percent from 2015.[8] This ballooning of the ransomware threat can be attributed to the availability of ransomware tools and services offered on the deep web. These tools drive down the level of sophistication required to perpetrate a ransomware attack, enabling would-be attackers with limited computer skills to pull off significant ransomware campaigns.

The emergence of ransomware-as-a-service offerings marks another troubling trend in the war against ransomware. Full service shops now offer everything from malware samples and the hosting infrastructure, to call centers that help victims pay the ransom, all for a percentage of the ransom received.

With all of these tools mere clicks away from our would-be attackers, it should come as no surprise that SMBs are increasingly falling victim to the wave of ransomware attacks. In fact, according to Kaspersky Labs, 42 percent of SMBs fell victim to a ransomware attack over the past 12 months, making ransomware one of the most significant threats SMBs face today.

Exploiting Your Weakest Link: Employees

Employees represent the front line in preventing a ransomware disaster. Unfortunately, for many small-to-midsize businesses these same employees represent their single greatest security weakness. All it takes is one wrong click on a link or a file to set the wheels of a ransomware infection in motion. From using scare tactics like impersonating federal agencies or the police, to delivering malware via emails carefully crafted to target a specific person, attackers are well versed in techniques that increase the likelihood of a click.

The most common way organizations become infected with ransomware involves tricking employees into clicking links or opening files via email. When done en masse and in high volume, this approach is called phishing. A more targeted approached, in which the attack is customized for success against specific organizations or employees, is called spear phishing. Regardless of which approach is used, email remains the leading delivery method for ransomware, with 31 percent of infections coming as the result of clicking a link, and 28 percent as the result of opening an email attachment.[9]

The Growing Cost of Ransomware

It goes without saying that ransomware attacks can be extremely lucrative for our adversaries. In 2016 the average ransom demand was $679, more than double the 2015 average demand of $294.[10] Given predications by the FBI that ransomware would be $1 billion source of income for cyber criminals in 2016,[11] the $679 figured paints a grim picture as to the scope and rate of success of ransomware attacks.

Unfortunately, the total cost of a ransomware attack often makes the ransom demand seem of little consequence. The true cost of a ransomware attack must consider all of the damages done to IT assets, time and money spent recovering data, and losses to customer/employee confidence. In 2016, 34 percent

of ransomware victims reported a loss of revenue, while 20 percent had to stop operations completely in the aftermath of a successful ransomware attack.[12] Further, research indicates that costs to a small business as the result of a successful ransomware attack could reach up to $99,000.[13] Few small businesses could withstand such an attack.

The Challenge in Preventing Ransomware

Until recently, antivirus (AV) products were the primary way to prevent malware, like ransomware, from entering your network or infecting your computers. Antivirus solutions depend on human researchers to find new malware variants and uncover distinct patterns in the malicious files that uniquely identify them. Using these patterns – signatures, if you will – these solutions are able to recognize and block previously discovered malware before it enters your network, or infects your computers.

For a long time, these signature-based solutions seemed sufficient, and helped prevent the majority of malware. However, legacy AV solutions have an Achilles' heel, in that these pattern-based solutions are always reactive, not proactive. A human or automated system must already have found and analyzed a new malware sample before it can create the signatures to block it. In short, it can't identify brand new malware samples when they're first released.

To exploit this issue, attackers have evolved their malware specifically to evade signature-based AV solutions. They've designed malware that loads in stages using dropper files, malware that tries to disable security programs including AV, and malware files that are encoded in different ways to sneak past the latest signatures. These are just a few of the 500+ evasion techniques[14] that researchers have tracked in the latest advanced malware.

In response, AV products have also evolved, using more complex signature rules to catch a wider range of samples (called a malware family) and designing basic heuristic solutions to try to identify new malware based on its file attributes. Unfortunately, criminals have increasingly adopted one very effective evasion technique, which has changed the game, and allowed many new malware samples to get past legacy solutions. That technique is polymorphism.

Polymorphic malware is a fancy term for malware that constantly changes the way it looks to evade signature-based detection. Using methods the criminals call "packing and crypting," attackers can repeatedly change a malware file on a binary level, making it look different to AV software. Even though the malicious executable still does the exact same thing, it looks like a new file, resulting in AV products missing a piece of malware that they previously knew about. Because of polymorphism, we've seen an exponential increase in the amount of new malware variants released year-over-year (Figure 1). With more than 140 million new malware variants each year, signature-based AV simply cannot keep up.

So how common is "zero day," or new and unique malware? Unfortunately, due to polymorphism this problem has become an epidemic. According to Webroot, 97 percent of the executable malware found on endpoints was unique[16], meaning it hadn't been seen before and likely wouldn't have been caught by signature-based AV solutions. Other experts agree, finding that almost half of the AV products miss newly released malware[17] the day it's released (day 0).

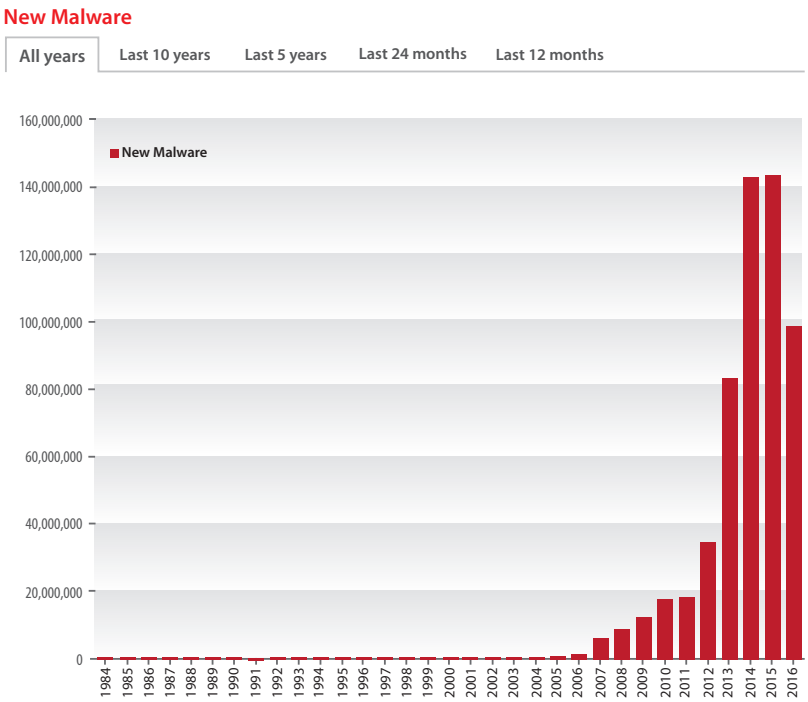


Figure 1: Amount of new malware samples each year according to AV-Test.org[15]

In short, while signature-based AV solutions are still partially useful for quickly preventing a certain threshold of basic malware, they're insufficient at detecting the more common evasive and advanced malware samples seen today, including the more sophisticated ransomware that has plagued many organizations recently.

Detecting Modern Ransomware

While organizations can no longer rely on AV solutions alone, that does not mean they must remain helpless in the face of the ever-evolving ransomware threat. Although ransomware evolves rapidly, many ransomware samples share common characteristics that can be used to identify the threat.

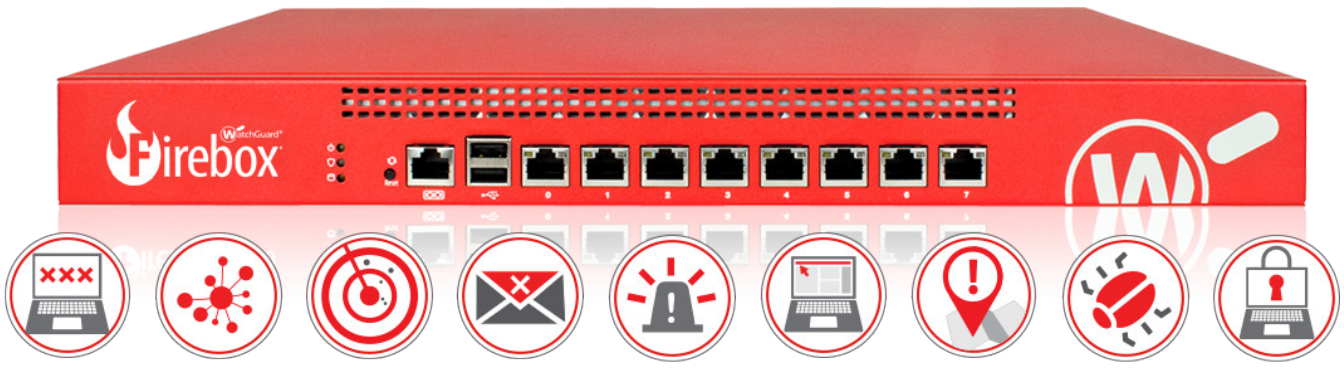
Some common ransomware behaviors:

- **Ransom demand.** While for victims it may not seem so at the time, the very fact that ransomware informs a victim of its presence is a weakness of the attack. By announcing its presence, the malware provides an opportunity for analysis that may aid in preventing identical infections in the future.
- **Encryption and entropy changes.** Few ransomware attackers are skilled enough to have mastered cryptography. In many instances, hackers will rely on standard cryptographic APIs (such as Microsoft CryptoAPI) to ensure their encryption is strong and meets best practices. Fortunately, use of these crypto libraries can help in identifying the ransomware threat before significant damage is done. Further, use of other encryption methods can also aide in detection as they necessarily result in significant entropy changes that can trigger alarms.
- **Hidden command and control channels.** In many cases, completing a ransomware attack requires the malware to connect to a malicious server to acquire the encryption key used to encrypt a victim's files.
- **Privilege escalation.** Ransomware will attempt to gain administrator privileges to disable security features on the compromised systems.
- **Sample deletion.** Ransomware will commonly delete the initial sample that infects a system to prevent further analysis and reverse engineering.

Mitigating the Threat of Ransomware with WatchGuard

At WatchGuard, we believe that protection against ransomware requires an enterprise-grade solution for preventing, detecting, and responding to ransomware attacks as they occur. Key to this approach is the ability to correlate network and endpoint security events with threat intelligence to detect, prioritize and enable immediate action to stop malware attacks.

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.



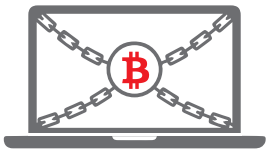
With WatchGuard Total Security Suite, organizations gain:

Visibility at the Endpoint with Threat Detection and Response

By nature ransomware infects endpoint devices. Having visibility into the event activity on these devices makes it possible to detect and remediate the threats before the damage is done. WatchGuard's newest security service, Threat Detection and Response, leverages multiple forms of detection through the WatchGuard Host Sensor to find advanced malware threats. In addition, our innovative Host Ransomware Prevention module provides the ability to detect ransomware incidents as they occur, and kill the related processes before he damage is done.

Key Components of WatchGuard Threat Detection and Response:

- Behavioral Analysis and Honeypots – Since malware threats tend to follow certain behaviors, tracking these steps can provide robust detection for unseen malware variants. Our Host Ransomware Prevention (HRP) 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. If it's determined that the threat is malicious, HRP can automatically prevent a ransomware attack before file encryption on the endpoint takes place.
- Advanced Heuristics – Rather than relying on signatures, TDR uses rules or algorithms to look for commands that could indicate malicious intent. This method of detection can quickly flag a threat without the need for it to execute. TDR leverages over 175 heuristics through the WatchGuard Host Sensor.
- Enterprise-grade Threat Intelligence – WatchGuard Threat Detection and Response leverages enterprise-grade threat intelligence feeds to confirm if a suspicious event on the endpoint is in fact a known threat.



Best-in-Class Network Security with Firebox UTM

The network is an important layer of defense in protecting your organization from ransomware. Visibility into unusual or blocked traffic patterns, visits to malicious or risky websites, as well as detecting botnets and other threats is an essential component of any ransomware defense strategy.

Key Components of WatchGuard UTM Solution:

- Advanced Web Filtering. WebBlocker automatically denies users access to known malicious sites, but also enables URL filtering that can block risky and inappropriate sites that may harbor malware.
- Protection from Email-Based Threats. Using the industry-leading Recurrent Pattern Detection (RPD™) technology, WatchGuard spamBlocker instantly identifies outbreaks as they emerge for continuous protection from email-based threats – blocking nearly 100 percent of unwanted and dangerous emails.
- Known Threat Protection – Using industry-leading, high-performance scanning of traffic on all major protocols, WatchGuard Gateway AntiVirus provides real-time protection against known viruses, trojans, worms, spyware, and rogueware.

Defense Against Zero-Day Threats with WatchGuard APT Blocker

WatchGuard APT Blocker puts a stop to fast-moving and persistent threats by using a next-generation cloud sandbox that simulates physical hardware, exposing malware designed to evade traditional network security defenses.

Key Components of WatchGuard ATP Blocker Solution:

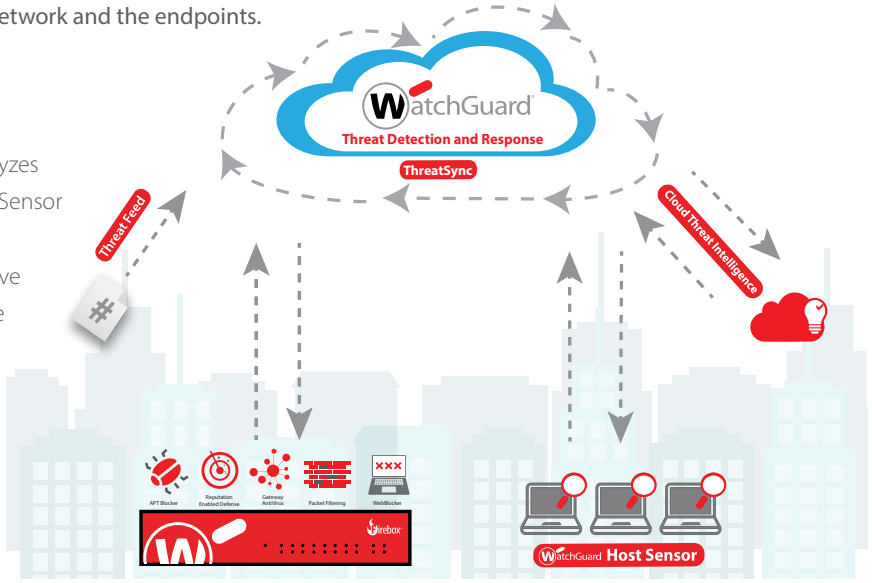
- **Behavioral Analysis**. WatchGuard APT Blocker focuses on behavioral analysis to determine if a file is malicious, identifying and submitting suspicious files to a cloud-based sandbox where the code is emulated, executed, and analyzed to determine its threat potential.
- **Full System Emulation.** Modern malware, including advanced persistent threats, ransomware, and zero-day attacks, are designed to recognize and evade traditional defenses. APT Blocker's full system emulation – which simulates physical hardware including CPU and memory – provides the most comprehensive level of protection against advanced malware.

Actionable Insight with the ThreatSync Correlation Engine

Looking at security through the lens of correlation is really the only way to get a full picture of your organization's security. ThreatSync, WatchGuard's cloud-based correlation and threat scoring engine, provides actionable insight into the threats attacking both the network and the endpoints.

Key Components of WatchGuard ThreatSync Solution:

- End-to-End Visibility. ThreatSync collects, correlates and analyzes event data from the WatchGuard Firebox, WatchGuard Host Sensor and threat intelligence feeds.
- Comprehensive Threat Scoring. By providing a comprehensive threat score and rank, security teams know which threats are the most critical and require immediate attention.



1. http://www.bbc.com/news/uk-england-humber-37822084
2. https://threatpost.com/st-louis-public-library-recovers-from-ransomware-attack/123297/
3. http://wtop.com/money/2016/03/hard-times-cafe-in-rockville-hit-with-ransomware/
4. http://flatheadbeacon.com/2016/11/23/malicious-software-hits-bigfork-school-district-computer-system/
5. http://www.thelocal.at/20170128/hotel-ransomed-by-hackers-as-guests-locked-in-rooms
6. https://securelist.com/analysis/kaspersky-security-bulletin/76757/kaspersky-security-bulletin-2016-story-of-the-year/
7. https://www.carbonite.com/en/news/ponemon-institute-ransomware-release/
8. https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-as-a-service-ransomware-operators-find-ways-to-bring-in-business
9. https://blog.barkly.com/ransomware-statistics-2016
10. http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/ISTR2016_Ransomware_and_Businesses.pdf
11. http://money.cnn.com/2016/04/15/technology/ransomware-cyber-security/
12. https://www.scribd.com/document/320027570/Malwarebytes
13. https://business.kaspersky.com/cryptomalware-report-2016/5971/
14. http://labs.lastline.com/evasive-malware-gone-mainstream
15. https://www.av-test.org/en/statistics/malware/
16. http://webroot-cms-cdn.s3.amazonaws.com/7814/5617/2382/Webroot-2016-Threat-Brief.pdf
17. http://labs.lastline.com/lastline-labs-av-isnt-dead-it-just-cant-keep-up

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

Part No WGCE66990_021217