Defending Against Known, Unknown, and Evasive Threats with WatchGuard Threat Detection and Response

Table of Contents

Contents

Understanding the Malware Threat to Small to Midsize Businesses....2
What is Driving the Threat?....2
Known, Unknown, and Evasive Malware....2
The Importance of Correlation in Detecting and Preventing Malware....3
Introducing Threat Detection and Response....4
Correlation and Threat Scoring with ThreatSync....4
WatchGuard Threat Scoring Model....4
Threat Scoring for Guided Response....4
Enterprise-grade Threat Intelligence....4
Detecting Malware on the Endpoint: Host Sensor....5
Network Insight: WatchGuard Firebox....6
Advanced Threat Triage with APT Blocker....6
Conclusion....7
About WatchGuard....7

Understanding the Malware Threat to Small to Midsize Businesses

While news of fresh cyber attacks and successful breaches against large organizations may be capturing headlines, the threat to small to midsize businesses (SMBs) is under-reported. The reality is SMBs disproportionately fall victim to cyber attacks and advanced malware. In fact, according to the National Cyber Security Alliance more than 70 percent of all attacks target small to midsize businesses. To make matters worse, roughly 60 percent of these businesses actually go out of business within the six months that follow the breach.

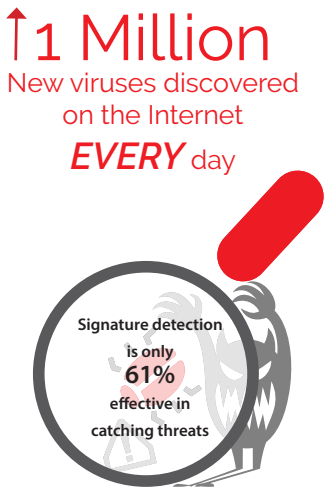
While successful targeted cyber attacks against well-known brands may be able to fill a news day, it also masks the larger malware threat that lurks below the surface. Today, organizations of all sizes are under siege from an unceasing tide of malware. One million new malware samples are discovered every day, and an estimated 12 million Windows malware samples are released every month. With ample security budgets, skilled security teams, and cutting edge technologies at their disposal, large enterprises are well positioned to protect themselves against the deluge of malware trying to sneak in the back door. Yet malware presents especially daunting challenges for SMBs as they face the same threats as enterprises, but with far fewer resources at their disposal.

What Is Driving the Threat?

Hackers are designing malware to be more sophisticated than ever, leveraging zero day threats and evasion techniques to sneak past network defenses undetected. Detecting malware in this virulent threat landscape is vital. In this paper, we'll explain why traditional approaches to malware detection are failing, and illustrate the importance of a correlated approach that enables you to look at network and endpoint behaviors in tandem to detect and prevent advance malware.

Known, Unknown, and Evasive Malware

Every day over one million new malware samples are discovered on the Internet. This number is a bit misleading, however, as it is partly the result of malware's ability to morph itself enough to evade known, signature-based detection engines. The reality is, the malware threat ecosystem is diverse, expansive, and ever-evolving. To better illustrate the malware threat landscape, and what approaches are needed to defend your organization, we classify threats as known, unknown, and evasive.



Known Malware

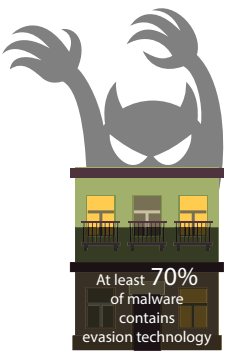
Known malware refers to malware samples that have been seen before in the wild, and can be identified using reputation and signature-based detection techniques. Malware becomes known when security analysts are able to analyze the threat and create a signature for distribution to detection engines. This is a slow and manual process, which quickly becomes overwhelming thanks to the sheer volume of threats that need analysis. Today, signature detection has been shown to only be 61 percent effective in catching threats even two weeks after the malware is discovered.[1] It should be noted that although signature detection is ineffective against the latest threats, endpoints without this protection are 5.5 times more likely to become infected.[2]

Unknown Malware

Unknown malware is malware which has either never been seen in the wild or simply for which no known signature exists. Unknown malware could be completely new, or a variant of an existing known malware that morphs to avoid signature-based detection. Heuristic approaches can greatly improve unknown malware detection, as they look for malicious commands within the suspicious files to identify threats. Similarly, monitoring endpoints for behaviors that could indicate the presence of unknown malware is also effective.

Evasive Malware

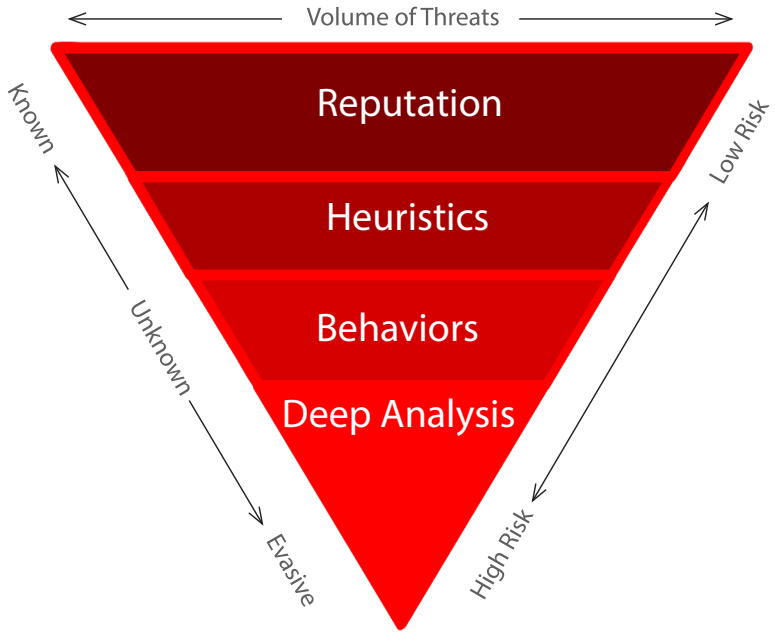
Evasive malware uses encrypted communication channels, kernel-level rootkits, zero day exploits, and environmental detection techniques to slip past defenses. 2014 represents the year when evasive malware went mainstream, with the use of evasive techniques ballooning by 2000 percent in a matter of months.[3] Today, it is estimated that 70 percent of malware contains some form of sophisticated evasion technology.[4] Detecting evasive malware requires the ability to perform deep analysis of files in an environment that emulates a complete operating system and hardware platform.



1 https://www.lastline.com/labsblog/antivirus-isnt-dead-it-just-cant-keep-up/
2 https://news.microsoft.com/2013/04/17/malware-infections-5-5-times-more-likely-without-antivirus-software-finds-new-research-from-microsoft/
3 https://www.sans.org/reading-room/whitepapers/forensics/detecting-malware-sandbox-evasion-techniques-36667
4 https://www.lastline.com/documents/lastLine_deep_content_inspec_tb.pdf

The Importance of Correlation in Detecting and Preventing Malware

All malware follows a pattern of infection that can be analyzed to aide in detection. Typically an attack begins with a user clicking a malicious email, falling victim to a drive-by download, or inserting an infected USB to start the infection process. Once on the target system the malware may attempt to seek out sensitive data, escalate privileges, acquire additional malicious tools, or attempt to spread to other machines on the network. Each of these behaviors provides a trail of evidence on the endpoint and network that can provide visibility into a potential threat. Despite this, it takes organizations an average of over 200 days to detect a successful breach. Unfortunately, the longer a breach goes undetected, the more opportunities an attacker has to cause damage to their target. With so much at stake, reducing the time and resources required to detect unknown and evasive malware is essential. Correlating network and endpoint security events makes this possible. Correlation allows administrators to identify new threats without a known signature, determine which endpoints are infected, follow the path of infection, and identify threat origin. With correlation, administrators have the visibility they need to stop unknown and evasive threats before the damage is done, and prevent successful attacks from spreading to other parts of the organization.

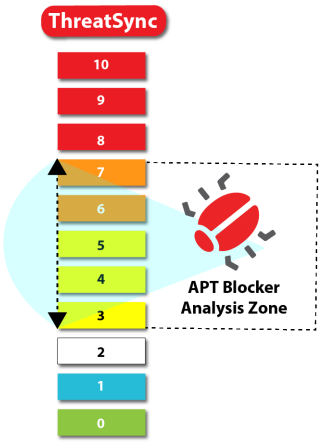


Introducing Threat Detection and Response

Signatures are a great and necessary defense against known threats, but organizations need a way to stop the unknown or new malware variants as well. Threat Detection and Response from WatchGuard is a powerful collection of advanced malware defense tools that correlate threat indicators from Firebox appliances and Host Sensors to enable real-time, automated response to stop known, unknown and evasive threats.

Key Components of TDR:

- ThreatSync. An innovative threat correlation engine that collects security events from the endpoint and network, correlates the data with third-party threat feeds, and delivers a threat score to guide automated or manual response.
- Host Sensor. The Host Sensor provides visibility into the endpoint and also facilitates response on the endpoint when a threat is detected. The Host Sensor also includes a Host Ransomware Prevention module that blocks the execution of ransomware on an endpoint before encryption occurs.
- WatchGuard Firebox. In TDR, the Firebox acts as both the first line of defense against malware entering your network, as well as a de facto network sensor, capturing and sending security event data to ThreatSync for correlation.



Correlation and Threat Scoring with ThreatSync

ThreatSync collects, correlates and analyzes event data from the Firebox, WatchGuard Host Sensor and threat intelligence feeds. Event data from other security services on the Firebox, including APT Blocker, Reputation Enabled Defense (RED), Gateway AntiVirus and WebBlocker, is sent to ThreatSync to be matched with endpoint data collected from the Host Sensor.

ThreatSync analyzes and scores **indicators** (i.e., individual network and endpoint events), and correlates indicators into **incidents** to provide a comprehensive threat score.

WatchGuard Threat Scoring Model:

- 8, 9, 10 Severe
- 6, 7 High
- 3, 4, 5 Suspicious
- 2 Suspect
- 1 Remediated
- 0 Benign

Captured network and endpoint events that ThreatSync determines have a relationship automatically receive the most severe threat score of 10.

Threat Scoring for Guided Response

ThreatSync not only provides visibility into events taking place on both the network and the endpoint, it delivers a comprehensive threat score and rank, so IT teams know which threats are the most critical and require immediate attention. Threat prioritization enables organizations to decrease time to detection and remediation, as well as decrease the number of dedicated resources required to remove threats.
With policies enabled, after ThreatSync receives that malicious network event and correlated malicious endpoint event, it will either quarantine the file, kill the process or delete the registry key persistence on the endpoint, as well as display the mitigated network event. The same actions can also be performed manually through our one-click, manual remediation.

Enterprise-grade Threat Intelligence

ThreatSync consumes and analyzes enterprise-grade threat intelligence feeds to ensure it is up to date with the latest indicators of compromise. These threat feeds provide lists of known malware signatures and IP addresses, MD5 hashes of malware files, or URLs or domain names of botnet command and control (C&C) servers. These lists can be critical in stopping new threats from infiltrating your environment and gaining access to critical data. There are a lot of vendors that make it their business to build and manage these lists, charging customers high fees for access.

Threat Detection and Response extends these threat intelligence capabilities to SMB organizations. ThreatSync compares the event data collected from the Firebox and Host Sensor with our various threat feeds to quickly determine if the threat has been seen elsewhere. If the threat is known to the threat feeds, it will quickly engage with the Firebox and/or Host Sensor to remediate the threat.

Detecting Malware on the Endpoint: Host Sensor

Threat Detection and Response leverages multiple forms of detection through the WatchGuard Host Sensor to find advanced malware threats.

- Signatures – As mentioned before, signatures are a critical line of defense in the fight against malware. You always want to have an arsenal of collected known threats. 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.
- Heuristics –In addition to signatures, TDR uses both static and dynamic heuristics (decision rules) that indicate if a file or process is suspicious. Static or file heuristics try to determine if a suspect program is suspicious by examining the structure and contents of the file in a pre-execution or inactive state. Dynamic or process heuristics scan a running process for suspicious characteristics associated with that specific process. Together, both work to identify seemingly benign files that present a potentially real threat. In many cases, this method of detection can quickly flag a new or unseen threat without the need for it to execute – or as the process is running but hasn't yet taken any actions. TDR leverages over 175 heuristics through the WatchGuard Host Sensor.
- Behavioral Analysis – Since malware threats tend to follow certain behaviors, tracking these steps can provide robust detection for more complex, polymorphic unseen or evasive malware variants. This form of detection goes beyond dynamic heuristics in not just monitoring characteristics of running process, but identifying what actions those processes are taking in the file system. Some actions could be establishing persistence, replication, strategic deletion, enumerating a file system, encryption, and others. This form of detection monitors chains of behaviors and increases a risk profile as they exhibit increasingly malicious intent. Our Host Ransomware Prevention module tracks behaviors traditionally associated with ransomware attacks to actually prevent these attacks before the ransomware file encryption takes place.

Network Insight: WatchGuard Firebox

Hackers leverage a host of servers and assets that are external to the target organization to facilitate their attack. Advanced malware, for example, often requires command and control servers to receive commands, exfiltrate information, request encryption keys and infect systems. Attackers may also like to keep an inventory of systems they have successfully infected, so they often design the malware to heartbeat, or make periodic "check-in" calls out to command and control channels. Insight into network traffic, including attempts to communicate with domains and IP addresses that are known to be associated with malicious behavior, can provide an indication that a threat is present in your environment.

Firebox appliances enhance detection even further by allowing TDR to correlate network behaviors and events captured by WatchGuard security services. As enterprise-grade security services, APT Blocker, Reputation Enabled Defense (RED), Gateway AntiVirus and WebBlocker are designed to defend against the latest threats, but each can provide information that could indicate the presence of a threat. Security events are captured by each of these security services and sent to ThreatSync for correlation and scoring for a more complete threat picture.

WebBlocker
This service references a cloud-database of over 50 million global sites known to be malicious – including websites in English, German, Spanish, French, Italian, Dutch, Japanese, and Traditional and Simplified Chinese.

- **Security Event:** Connection to a site in a blocked content category.

Reputation Enabled Defense
RED identifies threats using a reputation lookup that scores URLs as good, bad, or unknown. The lookup relies on a powerful, cloud-based reputation database that aggregates data from multiple feeds, including industry-leading antivirus engines.

- **Security Event**: Connection to site with a bad reputation attempted.
- **Security Event:** Communication with a botnet command and control server attempted.

Gateway AntiVirus
Gateway AV scans traffic on all major protocols (HTTP, HTTPS, FTP, TCP, UDP, SMTP, and POP3) using continually updated signatures and heuristics to detect and block all types of malware.

- **Security Event**: Gateway AntiVirus detected a virus in web traffic.
- **Security Event:** Gateway AntiVirus detected a virus in email traffic.

APT Blocker
Focuses on behavior analysis to determine if a file is malicious. APT Blocker identifies and submits suspicious files to a cloud-based next-generation sandbox, a virtual environment where code is analyzed, emulated, and executed to determine its threat potential.

- **Security Event:** APT Blocker detects/blocks a threat in web traffic.
- **Security Event:** APT Blocker detects/blocks a threat in email communications.

Advanced Threat Triage with APT Blocker

While threat scores provide powerful guidance in dealing with threats, the evolving nature of malware means indicators graded as suspicious could be early warning signs of yet-to-be-identified malware. Now, thanks to tight integration with WatchGuard APT Blocker, suspicious files can be sent for deep analysis and re-scoring in a next-generation cloud-sandbox.

APT Blocker uses full system emulation (CPU and memory) to get detailed views into the execution of a malware program. After first running through other security services such as gateway antivirus and intrusion prevention, files are fingerprinted and checked against an existing database. If the file has never been seen before, it is analyzed using the system emulator, which monitors the execution of all instructions.

APT Blocker analyzes everything the malware does from CPU instructions executed and network connections requested, to the files, memory, and devices the malware may have accessed. APT Blocker is also able to spot the evasion techniques that other sandboxes miss, including timing delays, waiting for user actions, malicious OS actions, encryption of communications to C&C infrastructure, and the fragmentation of files that only execute when reassembled.

If APT Blocker discovers a threat, ThreatSync will automatically update the threat score to guide response.

Conclusion

This white paper presents the capabilities of the Threat Detection and Response platform to detect, verify and respond to the known, unknown, and evasive threats impacting your organization. You should now have a better understanding of TDR:

- TDR detects known, unknown and evasive malware that most antivirus products miss leveraging sensors on both endpoints and the network
- TDR not only detects malware that existing security technologies do not, but quickly responds to and remediates these threats
- TDR endpoint and network sensor correlation, in addition to third-party threat intelligence feeds, provide greater visibility and verification of threats
- ThreatSync decreases false positives through aggregated threat scoring and analytics
- TDR delivers a faster, more efficient response to threats through policy-based automated remediation, targeting a single malware process, as well as bulk remediation actions
- Tight integration with APT Blocker allows for advanced threat triage and deep analysis of suspicious files
- ThreatSync offers configurable email alerts for detected incidents and indicators, as well as threats that have been remediated on the network and endpoint

To learn more, visit www.watchguard.com/tdr

About WatchGuard

WatchGuard® Technologies, Inc. is a global leader in network security, providing best-in-class Unified Threat Management, Next Generation Firewall, secure Wi-Fi, and network intelligence products and services to more than 80,000 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.

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