

# YOUR DATA FOR RANSOM

Why Ransomware Is the Exploit of Choice for Today's Cybercriminal

# CAPTURE RANSOMWARE FOR GOOD

Threat actors and cybercriminals were always skilled at breaching networks and stealing data. But it was often complex and time-consuming to turn that data into hard currency.

The introduction of ransomware eliminated the need for data exfiltration and re-selling on underground marketplaces.

Today, it's easier to breach your network, encrypt the data and hold it for ransom until you pay. Without a proactive, real-time cybersecurity strategy in place, organizations are left with few options.

Explore this guide to better understand ransomware and how cloud-based sandboxing can mitigate attacks before they breach your environment and hold your data — and your business — for ransom.

## Overview

**Pg 3** - Ransomware: Are You Protected from the Next Outbreak?

**Pg 4** - The Seven Habits of Highly Effective Ransomware Attacks

**Pg 5** - Ransomware-as-a-Service (RaaS) Is the New Normal

**Pg 6** - Why Network Sandboxing Is Required to Stop Ransomware

**Pg 7** - Stop Ransomware with Capture ATP

**Pg 8** - SonicWall Capture ATP Versus the Latest Malware

# Ransomware: Are You Protected from the Next Outbreak?

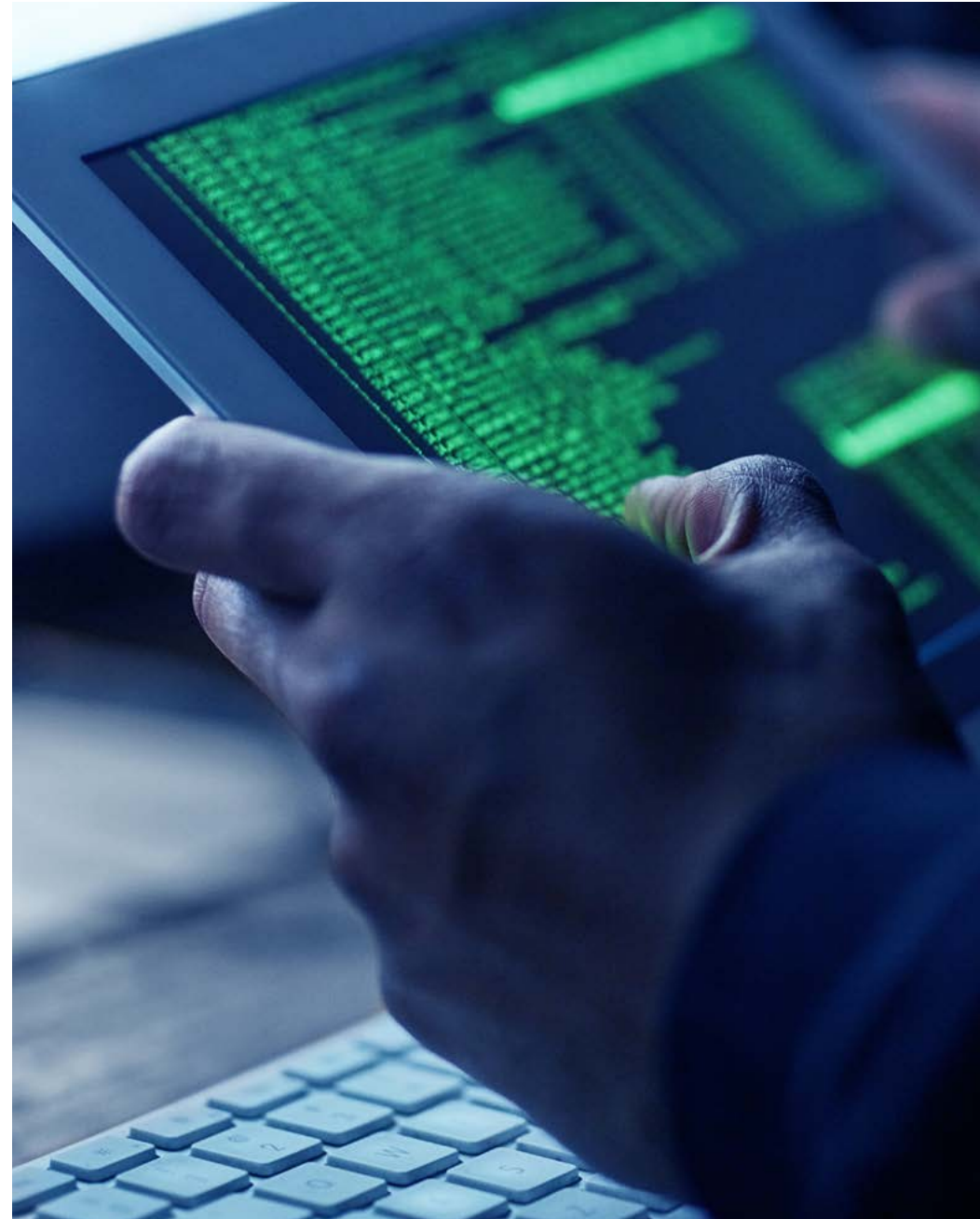
Will you be ransomware's next victim? Can attackers encrypt your data and hold it hostage until you pay a ransom?

Organizations large and small across industries around the globe are at risk of a ransomware attack. The media mostly reports attacks at large institutions, such as the [Hollywood Hospital](#) that suffered over a week offline in 2016 after a ransomware attack encrypted files and demanded ransom to decrypt the data.

However, small businesses are affected also. In fact, [Kaspersky research reported](#) that small and medium-size businesses were hit the hardest, 42 percent of them falling victim to a ransomware attack over a 12-month period.

Of those, one in three paid the ransom, but one in five never got their files back, despite paying. Whether you are part of a large organization or a small business, you are at risk.

FINISH THE STORY >



# The Seven Habits of Highly Effective Ransomware Attacks

In 2016, SonicWall detected a 600 percent growth in ransomware families. We saw a wide range of ransomware forms and attack vectors in the 2017 Annual Threat Report; some successful, others not so much.

So, what is at the core of any successful attack? If you understand the seven components of a ransomware campaign strategy, you can better defend yourself from one of the most pernicious forms of malware in history.

## 1. Intelligent Target Research

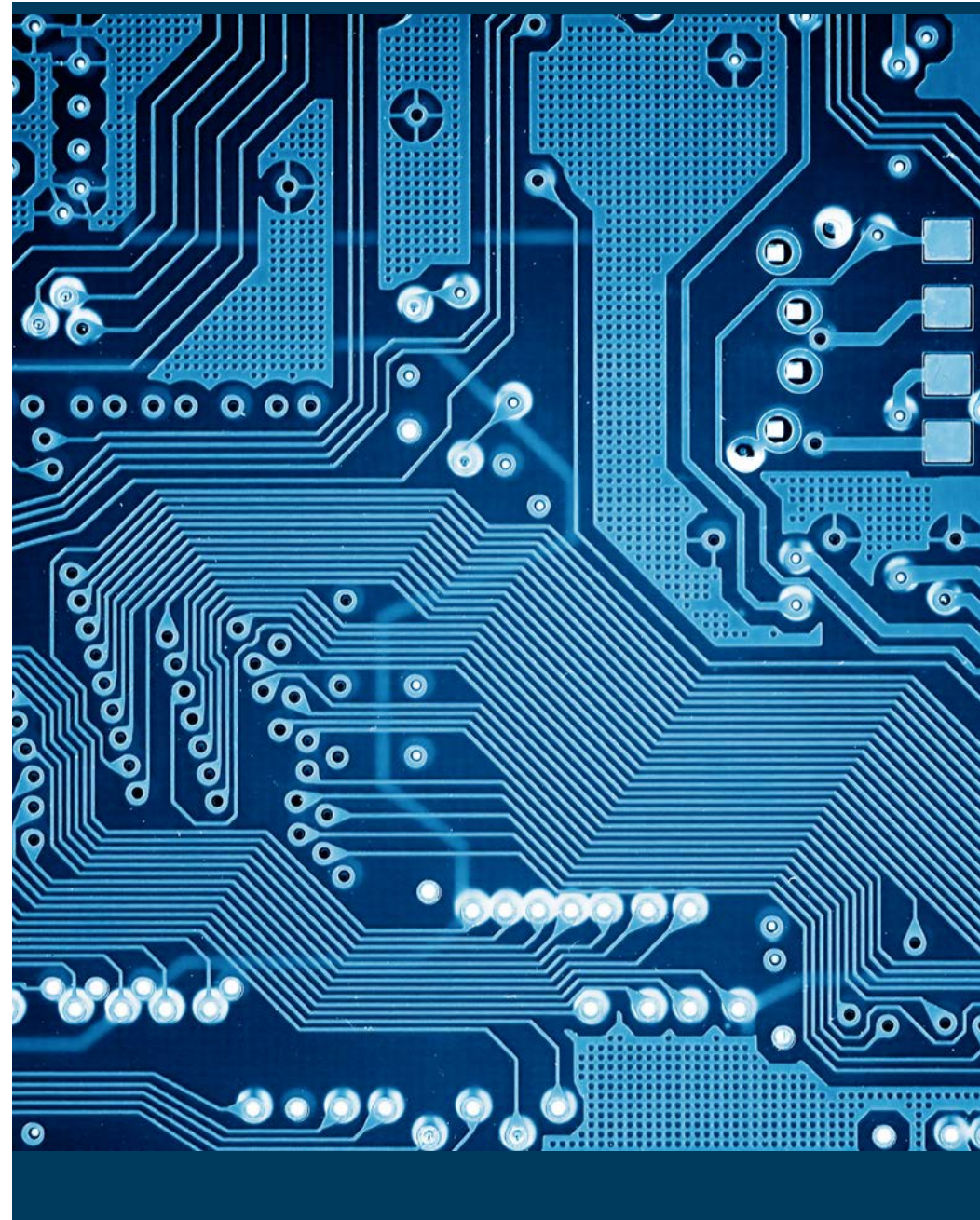
Any good scammer knows how to find the right people in an organization to target with the right message. Hackers know that municipal and healthcare are a ripe choice.

Even though organizations are providing awareness education, people still click on cleverly created social media posts and emails. In addition, hackers can go to any public lead-generation database and find the right set of victims for a phishing campaign.

## 2. Effective Delivery

Since 65 percent of ransomware attacks happen through email, a scammer can easily send that infected attachment to someone in accounts payable claiming it is an

[SEE THE FULL LIST >](#)



# Ransomware-as-a-Service (RaaS) Is the New Normal

Business models always have to tackle the method of distribution; will they sell directly or through a channel of distributors or a mix of both? The same goes for ransomware developers.

Many are electing to take their successful code and sell it as a kit, which eliminates many risks and the hard work of distribution — all the while collecting a cut of the prize.

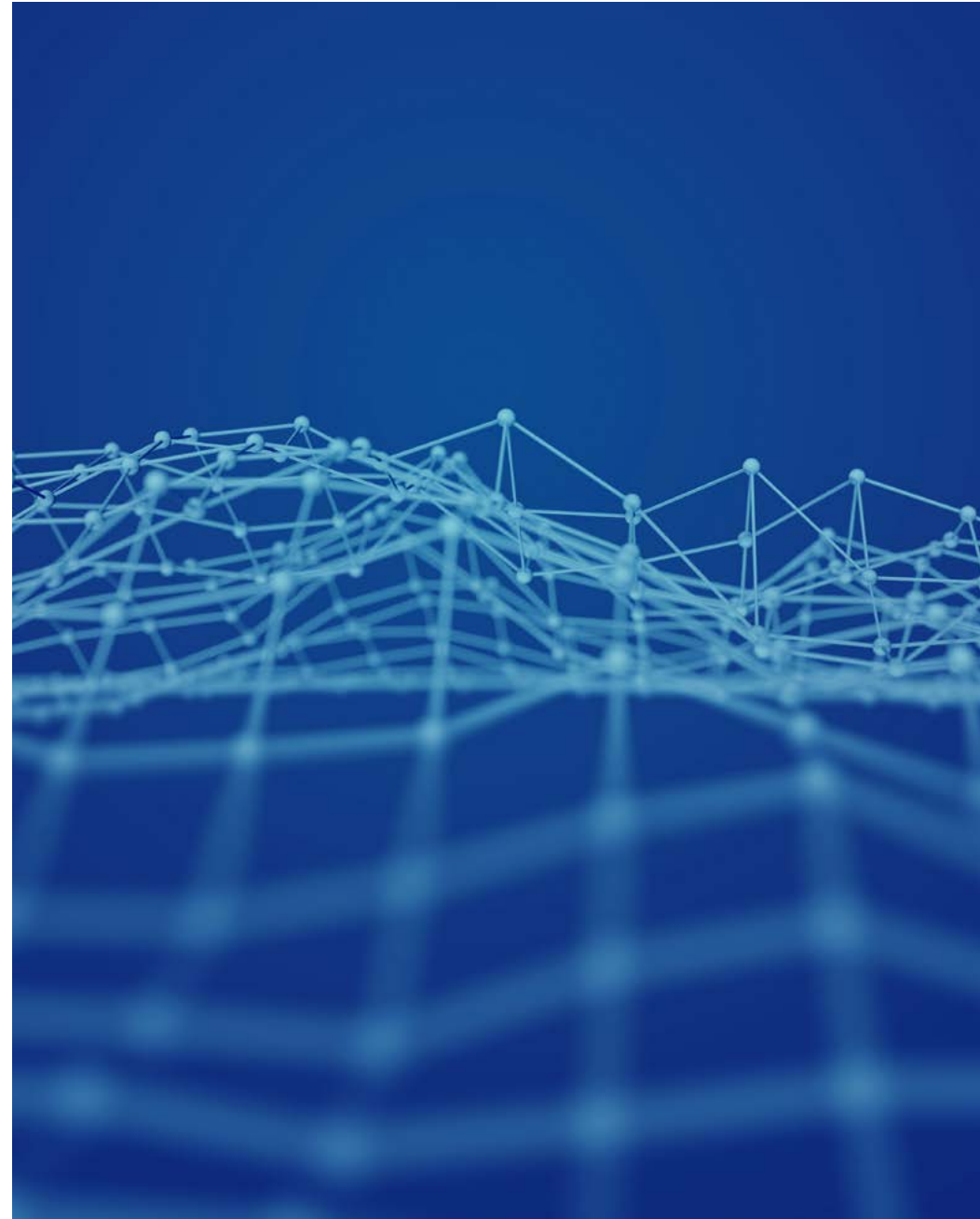
Throughout the past year, and even until the large-scale WannaCry attacks, floating between the peaks of the infamous events are small, focused attacks en masse from rebranded exploit kits. SonicWall has discovered a mix of developer hobby/chaos-malware, rebranded ransomware and repackaged RaaS ransomware.

- Trumplocker
- AlmaLocker
- Jigsaw
- Lambda
- Derialock
- Shade
- Popcorn
- Jaff

Recently, one author showed how easy it is to launch a ransomware attack within an hour ... **with zero hacking skills.**

So, what does this mean to an organization like yours? Should this scare you? Simply put, attacks from more sources equals more attacks. But SonicWall has your back.

[CONTINUE READING >](#)



# Why Network Sandboxing Is Required to Stop Ransomware

Next-gen firewalls leverage signatures and heuristics with great success. But when defending against today's malicious attacks, they are no longer sufficient. The challenges of targeted attacks and zero-day threats make the addition of sandboxing critical to an effective security posture.

The growth of external threats today is astounding. Attackers combine the opportunistic nature of automation with a software vendor's mindset to continually evolve their threats — all in an effort to have as broad a reach as possible, without detection.

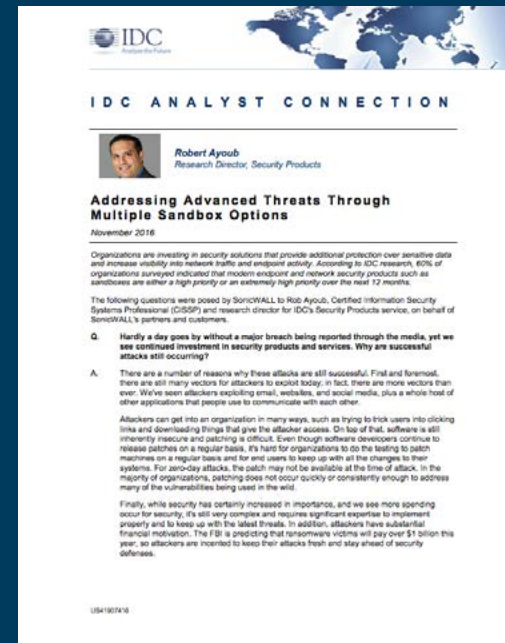
And given the negative impact incurred by any organization that suffers a data breach or ransomware attack, detecting malicious code before it has an impact within your network is imperative for IT organizations.

The real challenge isn't the ransomware that has already spread around the internet; it's targeted attacks and zero-day threats.

Targeted attacks involve never-before-seen code purpose-built for the organization being attacked, while zero-day threats exploit newly discovered vulnerabilities for which vendors have yet to issue patches.

Organizations need to be most concerned with these types of attacks, which are usually far more successful than their older counterparts. So, what's the best way to prevent a threat from emanating from within your network?

Download the complimentary IDC report to understand how sandboxing helps mitigate advanced threats.



## Free IDC Report

Addressing Advanced Threats Through Multiple Sandbox Options


[DOWNLOAD THE REPORT >](#)


# Stop Ransomware with Capture ATP


SonicWall Capture Advanced Threat Protection (ATP) service is a cloud-based, multi-engine sandbox designed to discover and stop unknown, zero-day attacks (e.g., ransomware) at the gateway with automated remediation.


This service is the only advanced threat-detection offering that combines multi-layer sandboxing — including full system emulation and virtualization techniques — to analyze suspicious code behavior.

This powerful combination detects more threats than single-engine sandbox solutions, which are compute-environment specific and susceptible to evasion.

 Stops ransomware in real time

 Broad file type analysis

 Multi-engine advanced threat analysis

 Rapid deployment of remediation signatures

 Reporting and alerts

 Block until verdict

To learn more about the SonicWall Capture Advanced Threat Protection service, download the data sheet or visit [sonicwall.com/capture](https://sonicwall.com/capture).

## How does Capture ATP work?



**SonicWall® CAPTURE ADVANCED THREAT PROTECTION SERVICE**  
Safeguard your network from cybercriminals who use SSL/TLS

For effective zero-day threat protection, organizations need solutions that include malware-analysis technologies and can detect evasive advanced threats and malware — today and tomorrow.

To protect customers against the increasing dangers of zero-day threats, SonicWall Capture Advanced Threat Protection Service — a cloud-based service available with SonicWall firewalls — detects and can block advanced threats at the gateway until verdict. This service is the only advanced threat-detection offering that combines multi-layer sandboxing, including full system emulation and virtualization techniques, to analyze suspicious code behavior. This powerful combination detects more threats than single-engine sandbox solutions, which are compute-environment specific and susceptible to evasion.

The solution scans traffic and extracts suspicious code for analysis, but unlike other gateway solutions, analyzes a broad range of file sizes and types. Global-threat intelligence infrastructure rapidly deploys remediation signatures for newly identified threats to all SonicWall network security appliances, thus preventing further infiltration. Customers benefit from high-security effectiveness, fast response times and reduced total cost of ownership.

**Benefits:**

- High security effectiveness against unknown threats
- Near real-time signature deployment protects from follow on attacks
- Reduced total cost of ownership

**Diagram:** Traffic enters from the left, passing through SSL decryption, Network anti-virus, Cloud anti-virus, Botnet blocking, URL filtering, and Intrusion prevention. It then reaches a Gateway firewall. From there, it goes to a Sandbox for analysis. The analysis results in a Verdict, which is then used for Judgment. The final output is Filtered traffic. The process is supported by a Multi-engine SonicWall Capture cloud.

A cloud-based, multi-engine solution for stopping unknown and zero-day attacks at the gateway

GET THE DATA SHEET >

# Demo: SonicWall Capture ATP Versus the Latest Malware

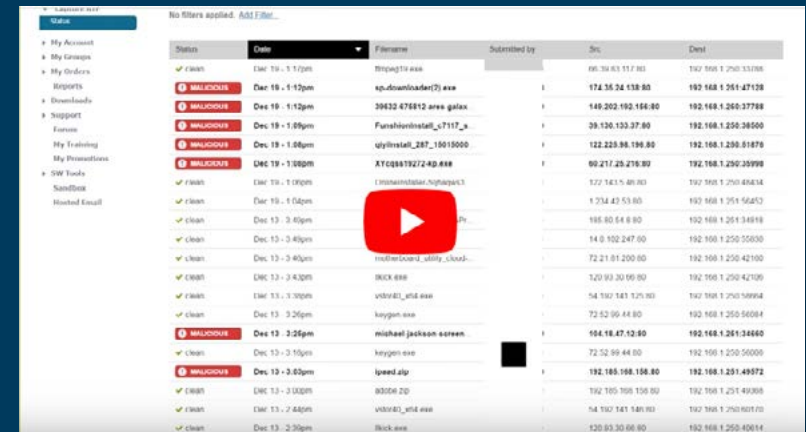
o protect customers against the increasing dangers of zero-day threats (e.g., ransomware), SonicWall Capture Advanced Threat Protection – a cloud-based service available with SonicWall firewalls – detects and blocks advanced threats at the gateway until verdict.

How powerful is Capture ATP? We took the most dangerous and newest malware from around the internet and pit it against SonicWall technology to show how we stop advanced real-world threats that are relentless in attacking everyday businesses.

By just using Gateway Anti-Virus (GAV) and Capture ATP, we demonstrate how the malware was identified and mitigated in real time. Capture ATP finds what malware wants to do from the application, to the OS, to the software and on to the hardware.

From there, global threat intelligence infrastructure rapidly deploys remediation signatures for newly identified threats to all SonicWall network security appliances, thus preventing further infiltration.

Customers benefit from high-security effectiveness, fast response times and reduced total cost of ownership.



Status	Date	Filename	Submitted by	Src	Dest
clean	Dec 19 - 1:12pm	httpget.exe		66.248.63.117.80	192.168.1.250.33388
<b>MALICIOUS</b>	Dec 19 - 1:12pm	sp_downloader(2).exe		174.26.24.138.80	192.168.1.251.47126
<b>MALICIOUS</b>	Dec 19 - 1:12pm	39432476812_area_gate...		149.202.192.164.80	192.168.1.250.37788
<b>MALICIOUS</b>	Dec 19 - 1:09pm	Furshvinstal_7117_x...		39.120.132.37.80	192.168.1.250.38000
<b>MALICIOUS</b>	Dec 19 - 1:08pm	qylvinstal_287_10010000		122.225.86.194.80	192.168.1.250.81878
<b>MALICIOUS</b>	Dec 19 - 1:08pm	ATCG8192724D.888		90.217.29.216.80	192.168.1.250.35998
clean	Dec 19 - 1:09pm	(Microsoft.WindowsP...		172.14.15.49.80	192.168.1.250.48434
clean	Dec 19 - 1:04pm			1.234.43.43.80	192.168.1.251.56253
clean	Dec 19 - 3:45pm			185.80.64.8.80	192.168.1.251.34818
clean	Dec 19 - 3:45pm			14.0.102.247.80	192.168.1.250.55630
clean	Dec 19 - 3:45pm	redirection_start_chek...		72.21.81.200.80	192.168.1.250.42100
clean	Dec 19 - 2:42pm	Block.exe		320.93.30.99.80	192.168.1.250.42709
clean	Dec 19 - 1:30pm	vst041_mta.exe		54.192.141.175.80	192.168.1.250.58964
clean	Dec 19 - 3:26pm	keygen.exe		72.52.99.44.80	192.168.1.250.56084
<b>MALICIOUS</b>	Dec 19 - 3:26pm	mishaal_jackson_screen...		504.16.47.12.80	192.168.1.251.34660
clean	Dec 19 - 3:15pm	keygen.exe		72.52.99.44.80	192.168.1.250.56000
<b>MALICIOUS</b>	Dec 19 - 3:05pm	lpsend.zip		192.168.168.168.80	192.168.1.251.49972
clean	Dec 19 - 3:03pm	00304 ZIP		192.165.168.168.80	192.168.1.251.49368
clean	Dec 19 - 7:44pm	vst041_mta.exe		54.192.141.149.80	192.168.1.250.60170
clean	Dec 19 - 2:50pm	Block.exe		120.83.30.66.80	192.168.1.250.40814

WATCH THE FULL DEMO >



## About Us

Over a 25 year history, SonicWall has been the industry's trusted security partner. From network security to access security to email security, SonicWall has continuously evolved its product portfolio, enabling organizations to innovate, accelerate and grow. With over a million security devices in almost 200 countries and territories worldwide, SonicWall enables its customers to confidently say yes to the future.

If you have any questions regarding your potential use of this material, contact:

SonicWall Inc.  
5455 Great America Parkway  
Santa Clara, CA 95054

Refer to our website for additional information.

[www.sonicwall.com](http://www.sonicwall.com)

© 2017 SonicWall Inc. ALL RIGHTS RESERVED.

SonicWall is a trademark or registered trademark of SonicWall Inc. and/or its affiliates in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners.

The information in this document is provided in connection with SonicWall Inc. and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of SonicWall products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, SONICWALL AND/OR ITS AFFILIATES ASSUME NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL SONICWALL AND/OR ITS AFFILIATES BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF SONICWALL AND/OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. SonicWall Inc. and/or its affiliates do not make any commitment to update the information contained in this document.