tenable network security

Comprehensive Malware Detection with SecurityCenter Continuous View™ and Nessus®

February 3, 2015

(Revision 4)

Table of Contents

Overview

Tenable SecurityCenter Continuous View™ (SecurityCenter CV™) allows for the most comprehensive and integrated view of the security posture and activity in your entire IT infrastructure. By monitoring system processes and network traffic, and correlating it with audit results of anti-virus configurations and malware scans, Tenable's SecurityCenter Continuous View can identify a wide range of threats to an organization by using methods beyond traditional vulnerability scanning.

Both SecurityCenter Continuous View and Nessus® have the ability to detect a wide variety of malicious software running on both Windows and Apple systems. Using a low-latency third-party threat intelligence feed, Nessus can leverage a credentialed scan to determine if currently running processes match known malware signatures. Tenable's SecurityCenter Continuous View can then help you identify and determine the extent of malware infections. It is critical to know if malware infected a machine due to one employee clicking on a bad attachment, or if there is a widespread infection that has compromised a significant portion of your environment.

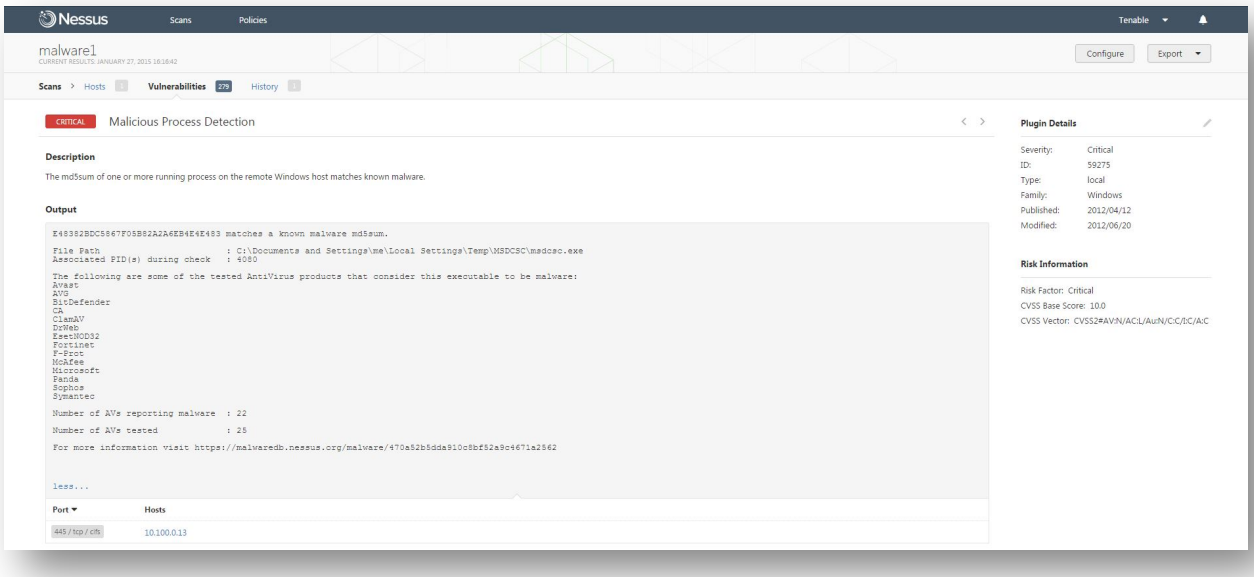
Malware, Botnet Detection, and Anti-Virus Auditing

Nessus, used by itself or within SecurityCenter Continuous View, provides several different methods of detecting a wide variety of malware. Based on the level of access a Nessus scanner has to the target host, these methods can provide in-depth examination of a host to discover an incredible amount of documented malware and more.

Malware Detection

Nessus can leverage a credentialed scan to detect malware on Windows systems. Using a third-party feed of specialized malware information, Nessus can inspect running processes to determine if they match the signatures of known malware, as cataloged by all of the major anti-virus vendors.

This detection is performed by uploading a dissolvable agent that installs as a Windows service. The agent generates a list of hashes created from the running processes, encodes them, and sends them to a Tenable server that proxies the query to the third-party malware hash provider. Once this process completes, the agent is removed as the scan completes. Nessus then generates a report that will include any malware detected along with a link to more information including the MD5 hash, when the malware was first discovered, the name each anti-virus company has assigned it, and more detailed information for each finding, as shown in the example screen capture below:



In addition to the multi-vendor in-depth checks, Nessus can often find a malware infection that may be the result of a failure in an anti-virus program (such as not receiving signature updates) or a specific vendor not having the same coverage as peers.

This approach is an ideal complement to any deployment of an existing single or even layered anti-virus strategy because attackers will often specifically create malware payloads that bypass detection. For example, a company may deploy "brand X" anti-virus agents on desktop systems. Attackers may know this and specifically package, or "pack", their malware in a manner that is not detected by "brand X". However, when scanned by Nessus, the hashes of all running processes are compared against an industry index of all known malicious hashes (plugin 59275: Malicious Process Detection). This allows for secondary detection of malware without the need to run multiple anti-virus agents.

In addition to the sizable index of malware detected by plugin 59275, Nessus offers several additional plugins and methods for detecting known malware:

- By using "Malicious Process Detection: User Defined Malware Running" (Plugin ID 65548), additional hashes from your own research or third-parties can be added.
- Based on a Mandiant report, "Malicious Process Detection: APT1 Software Running" (Plugin ID 64687) detects a variety of malware used by a foreign party dubbed "APT1" believed to be operating out of China. This is further augmented by "APT1-Related SSL Certificate Detected" (Plugin ID 64688) that can detect known bad SSL certificates.
- After a recent compromise, Tenable created "Malicious Process Detection: Malware Signed By Stolen Bit9 Certificate" (Plugin ID 64788) to detect any malware signed by a stolen certificate.
- Microsoft Windows Known Bad AutoRuns / Scheduled Tasks (Plugin ID 74442) shows that the Windows system has one or more registry entries that are known to be associated to malware. This indicates that the system may have been compromised by malware.
- Microsoft Windows AutoRuns Unique Entries (Plugin ID 70628) identifies any unique AutoRun settings, which are also unique to any other scanned hosts.
- Unknown Service Detection: Banner Retrieval (Plugin ID 11154) identifies any network services that are unknown. Tenable uses this for our customers to send us information about new services, but it is also an excellent way to find malware running their own proprietary protocols.
- Reputation of Windows Executables: Unknown Process(es) (Plugin ID 70768) identifies all running processes that have an unknown reputation.

Nessus can also detect a wide range of software that may violate corporate policy by comparing the running processes to a list of questionable software (plugin 59641: Malicious Process Detection: Potentially Unwanted Software).

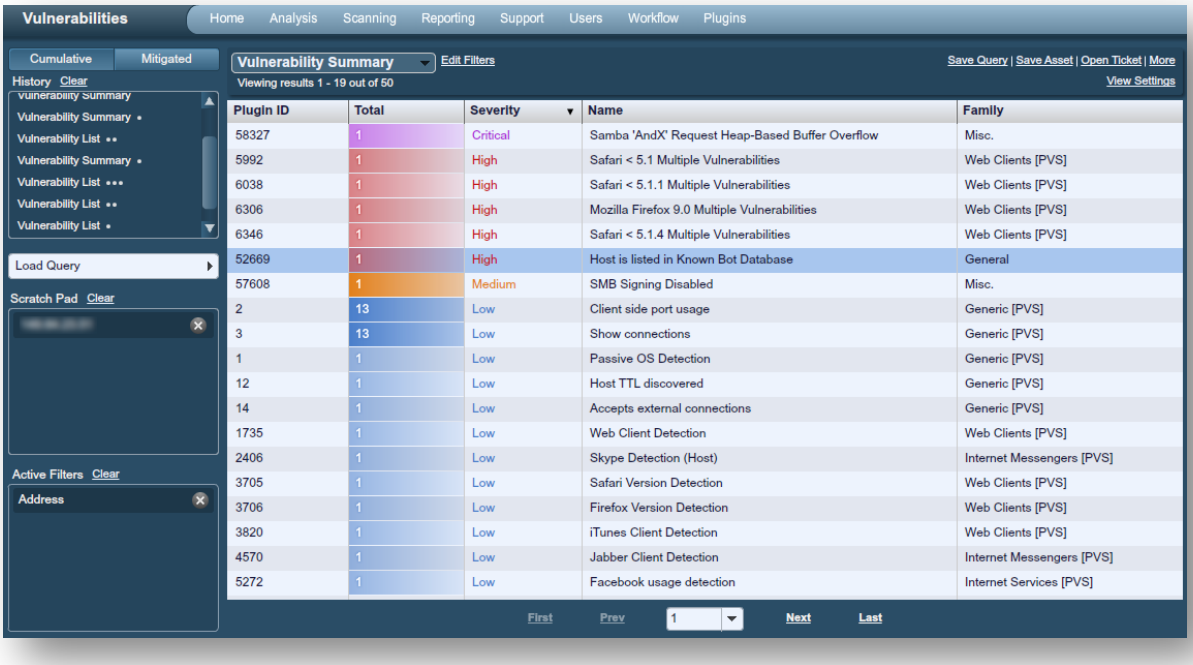
Botnet Detection

Using a third-party information feed, Nessus has several methods to identify if a host is part of an active botnet. According to anti-malware and botnet-tracking companies, botnets account for millions of hosts on the Internet. Any system that is operating as part of a botnet has been fully compromised and represents a serious threat to an organization. Using the following methods, Nessus can often identify such hosts based on reputation and content scanning:

- Host is listed in Known Bot Database (52669): Nessus checks the scanned IP address against a database of known botnet IPs and reports if there is a match.
- Web Site Links to Malicious Content (52670): While performing a web application scan, the lists of external URLs are processed to see if any match with a list of known DNS names and websites that are associated with botnet activity.

- Active Connection to Host Listed in Known Bot Database (58430): The list of connected systems is evaluated to see if any are part of a known botnet. This check requires credentials and will enumerate both outbound and inbound connections with botnet IPs.
- DNS Server Listed in Known Bot Database (58429): Similar to the DNS Changer malware, if a system has been configured with a DNS IP address that is also on a list of known botnet systems, Nessus will report this potential infection.

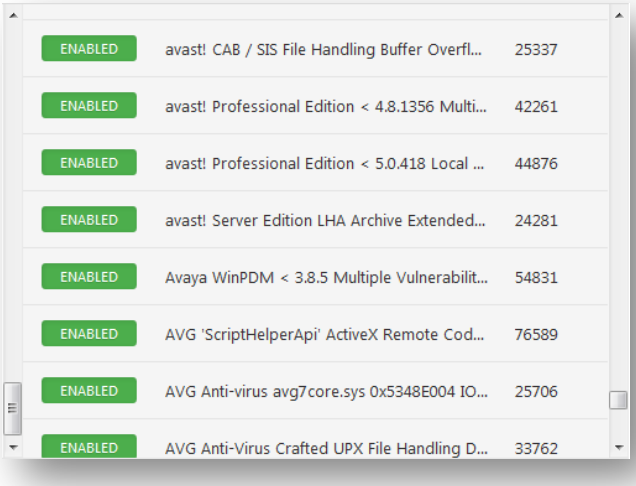
It is important to realize that botnet detection is completely independent of any type of anti-virus, intrusion detection, or "SIEM" type of correlation. Nessus contains all of the information it needs to reliably detect if a system is communicating with a known botnet. Below is a screen capture of an actual detection by Nessus as shown while viewing enterprise scan results with SecurityCenter Continuous View:



In this case, Nessus plugin 52669 fired because the scanned IP was listed in a known, highly reliable, and relevant botnet database.

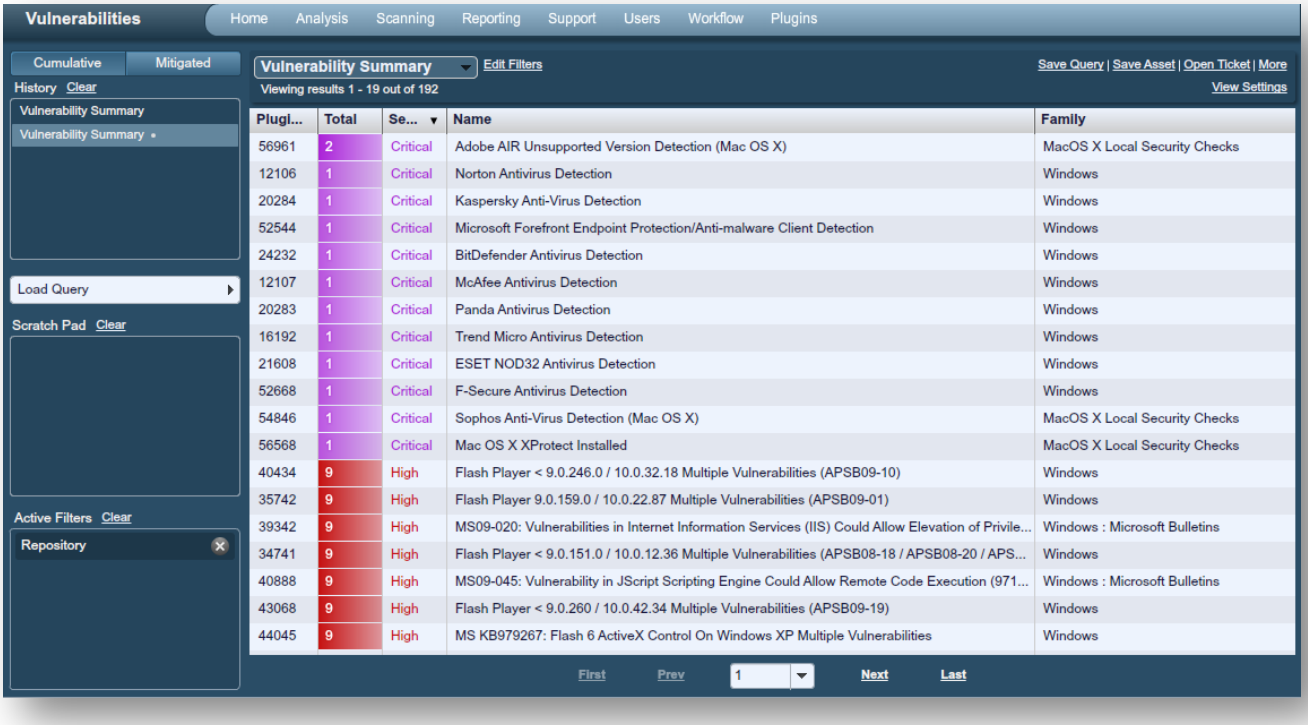
Anti-Virus Auditing

Nessus has over 100 plugins that examine anti-virus software for vulnerabilities, as well as missing or outdated signatures. These cover a wide range of vendors including Trend Micro, McAfee, ClamAV, Bitdefender, Kaspersky, ESET, F-Secure, and more. The ability to audit servers to determine if anti-virus signatures are being updated properly provides a second level of protection for an organization. Below is a sample screen capture from a Nessus scan policy creation screen in which checks for multiple leading anti-virus vendors can be selected.



Partial list of anti-virus related plugins

Data from these types of scans is shown in this screen capture from SecurityCenter Continuous View:

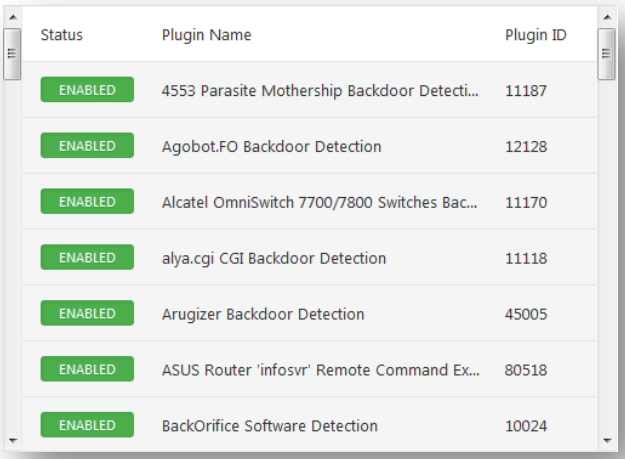


Nessus considers the detection of anti-virus agents without up to date signatures to be of “Critical” severity.

In addition to Nessus plugins, Tenable offers 12 audit policies that Nessus can leverage to determine if a particular vendor’s anti-virus software is installed, currently running, and/or configured to start after system boot-up. These checks can help ensure any type of network-wide anti-virus program is working as expected and is providing the appropriate level of defense.

Backdoors & Default Accounts

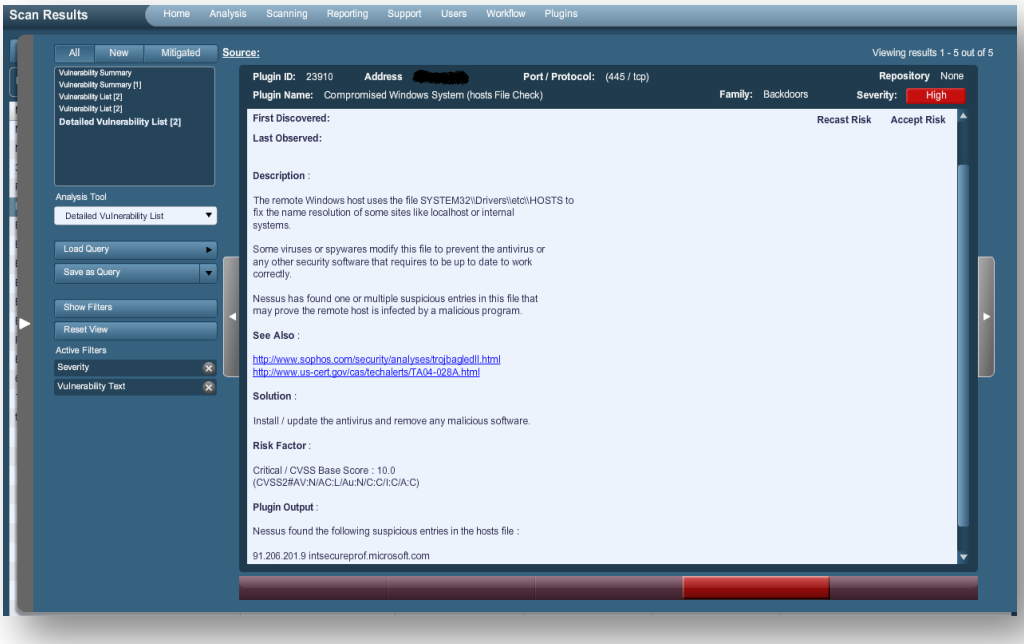
One of the Nessus plugin families that can assist with detecting malware is called "**Backdoors**". This family contains a variety of plugins that look for known backdoors, adware, and some high-profile infections such as Conficker, Stuxnet, and Zeus. When possible, Nessus will attempt to remotely detect the presence of these types of malware. Some of the plugins are designed to require authentication so Nessus can access files on a system (e.g., "`hosts`") to inspect it for signs of compromise or malware. In addition, Nessus can detect the presence of some rootkits (e.g., D13HH and wh00t) via the presence of default accounts left for subsequent access.



Status	Plugin Name	Plugin ID
ENABLED	4553 Parasite Mothership Backdoor Detecti...	11187
ENABLED	Agobot.FO Backdoor Detection	12128
ENABLED	Alcatel OmniSwitch 7700/7800 Switches Bac...	11170
ENABLED	alya.cgi CGI Backdoor Detection	11118
ENABLED	Arugizer Backdoor Detection	45005
ENABLED	ASUS Router 'infosvr' Remote Command Ex...	80518
ENABLED	BackOrifice Software Detection	10024

Partial list of plugins in the "Backdoors" family

Below is a screen capture of a hit for Nessus plugin 23910 that analyzes the contents of a Windows "hosts" file to see if it has been modified to include suspicious content:



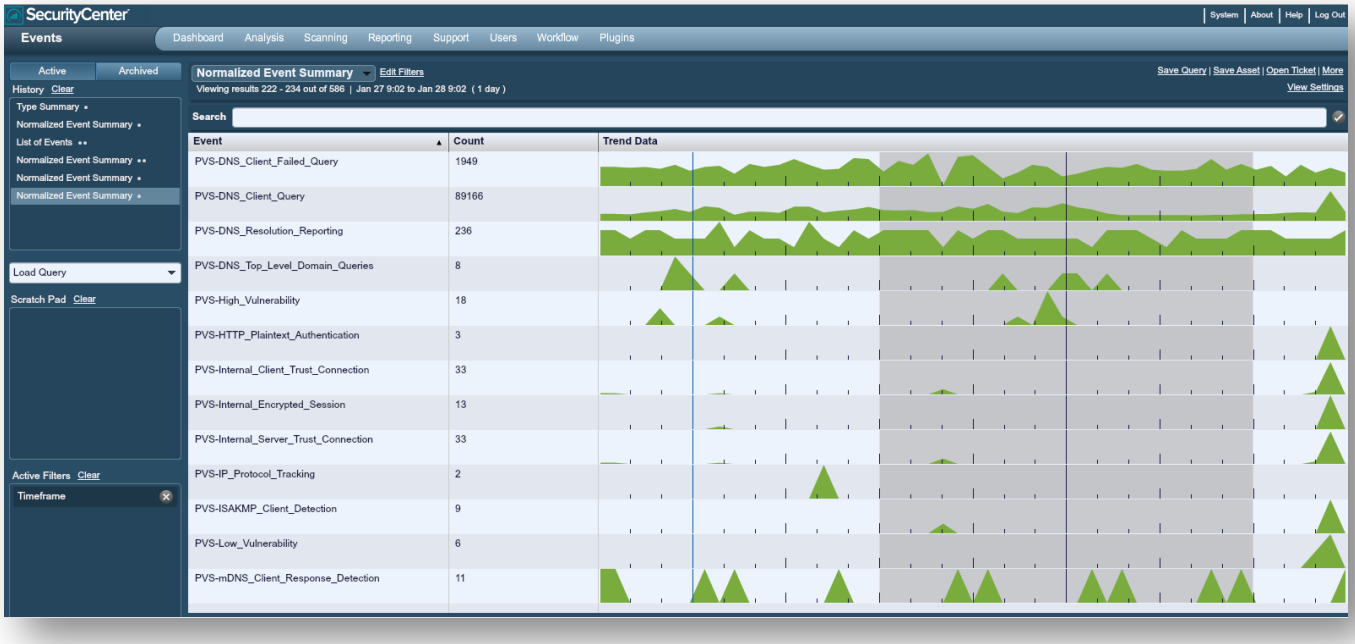
Real-Time Traffic and System Monitoring

To further assist in the fight against malware, Tenable's SecurityCenter Continuous View includes components for real-time network activity monitoring - Passive Vulnerability Scanner™, and system event/activity monitoring - Log Correlation Engine™.

SecurityCenter Continuous View has the ability to passively analyze network traffic, looking for a wide variety of events and vulnerabilities. This includes file browsing, DNS lookups, software protocols in use, web browser user-agents, potential policy violations, and more. Using this collection of events, SecurityCenter Continuous View is well suited to help you determine the presence or extent of a malware infection. SecurityCenter Continuous View can also gather and accept an incredible amount of logs from just about every system on a network, and can correlate these log entries to make them a useful tool in understanding user or malware activity on the network.

Network Activity Monitoring

SecurityCenter Continuous View logs all types of traffic for forensic analysis and alerting. Below is an example screen capture of various types of network traffic in real-time and then logged as seen through SecurityCenter Continuous View:



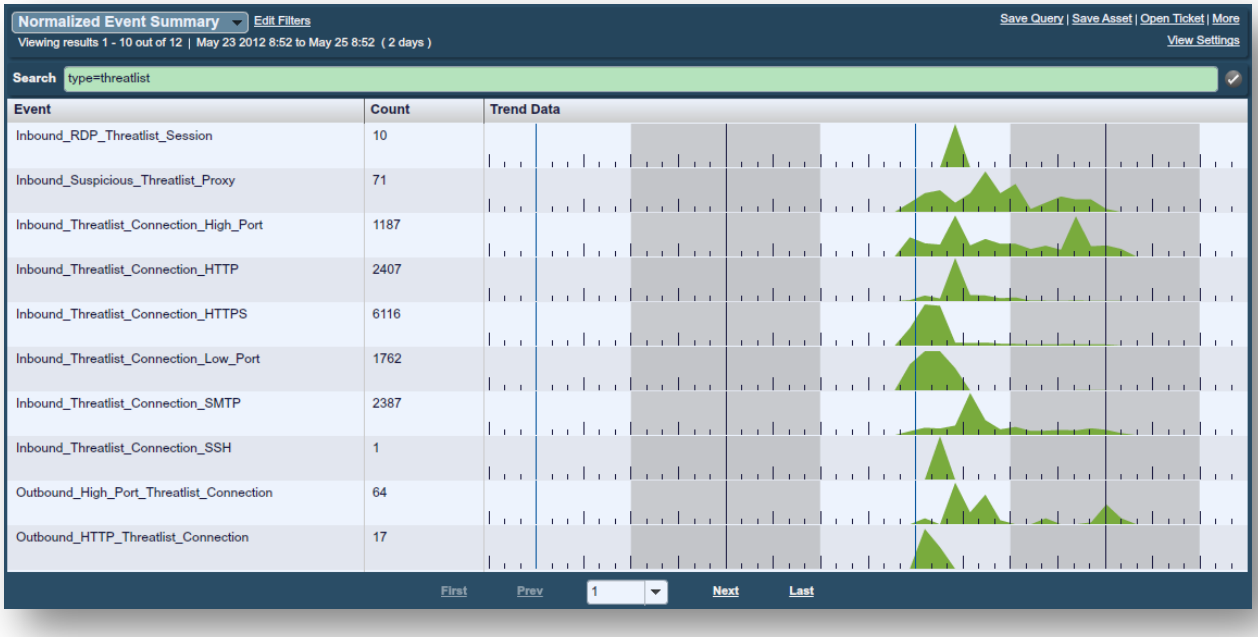
Converting network sessions to actionable logs has tremendous value for analyzing malware infections including:

- Providing evidence of infections
- Complementing intrusion detection logs with actual forensic analysis of network traffic
- Providing easy access to web sites, DNS queries performed, and SSL certificates used in conversation
- Logging all file transfers via SMB, NFS, FTP, and other protocols both inside and outside the network
- Correlating these logs with internal network user IDs regardless if they are mobile or have systems in dynamic DHCP environments

Botnet Activity Monitoring

SecurityCenter Continuous View correlates intrusion logs, firewall, connection, NetFlow, authentication, and real-time logs with a highly accurate list of botnet IP addresses. It creates alerts based on the direction of the connection as well as the type of connection. This allows organizations to determine when they are scanned by malicious botnets and when an internal server reaches out to a botnet site.

Below is a screen capture of botnet events gathered by SecurityCenter Continuous View:



SecurityCenter Continuous View tags botnet events with the term “threatlist”. In the above screen capture, there were a variety of network connections, including recognized applications such as RDP (Windows Remote Desktop), which originated from IP addresses known to be part of a botnet.

System Process Monitoring

SecurityCenter Continuous View also gathers logs from Windows and Linux systems, including application execution on those systems. Gathering application data from across an enterprise is useful for forensic analysis of infected systems. SecurityCenter Continuous View can also leverage this data to summarize and alert when certain key conditions occur including:

- When a system runs a new executable for the first time
- When a new executable is run on the network for the first time
- When a known executable is invoked in a new manner for the first time

All of these events can potentially be associated with virus outbreaks.

For example, if Nessus detects malware running as a process named 1738d.exe, SecurityCenter Continuous View provides the ability to search event logs from every system for the same process name. Such a query will help give an idea of the extent of the infection. Even better, SecurityCenter Continuous View can query the logs to look for errors, unusual login

behavior, USB device insertions, and other events related to the infected system. With a few fast queries, it is often possible to isolate where malware first took hold on the network and where it spread.

Conclusion

Deploying malware detection software throughout an organization is essential for a base level of security protection. Regardless of vendor, malware detection is not foolproof, especially when it comes to polymorphic malware that can evade detection. Utilizing the real-time network monitoring and log correlation components of Tenable's SecurityCenter Continuous View provides a second level of validation and protection. More importantly, continuous monitoring of the security state and activity of the IT enterprise can enable customers to reduce their attack surface, eliminate blind-spots, and strengthen their defenses against advanced malware.

About Tenable Network Security

Tenable Network Security provides continuous network monitoring to identify vulnerabilities, reduce risk and ensure compliance. Our family of products includes SecurityCenter Continuous View™, which provides the most comprehensive and integrated view of network health, and Nessus®, the global standard in detecting and assessing network data. Tenable is relied upon by more than 20,000 organizations, including the entire U.S. Department of Defense and many of the world's largest companies and governments. For more information, visit tenable.com.