Tenable Malware Detection: Keeping Up With An Increasingly Sophisticated Threat Environment
Table of Contents

Introduction .......................................................................................................................... 3
The Problem ......................................................................................................................... 3
  Signature-based AV is no longer enough ........................................................................... 3
The Organizational Perimeter Has Moved .......................................................................... 4
Tenable Malware Detection ................................................................................................. 5
  Audit Effectiveness of Deployed Security Products ......................................................... 5
Direct and Indirect Malware Detection ............................................................................... 6
Combination of Scan, Sniff and Log Correlation ............................................................... 6
Utilizes Whitelist, Blacklist and Grey-list Intelligence ......................................................... 7
Summary .............................................................................................................................. 7
About Tenable Network Security ......................................................................................... 7
Introduction

With an ever-increasing cyber-threat profile, traditional anti-virus (AV) and anti-malware (AM) products are unable to adequately detect new malware threats facing organizations today. In addition, the rise of the mobile workforce and adoption of BYOD policies introduces another layer of risk with unknown and unmanaged laptops, smartphones and mobile devices accessing sensitive IT resources. These developments leave corporations, government entities and individuals at risk from a wide range of cyber-crime activities.

Relying on traditional signature based AV alone is simply not sufficient to prevent today’s onslaught of new, sophisticated and advanced malware. This whitepaper describes in detail, some trends and statistics on the malware detection. This whitepaper then introduces a multi-vector approach to accurately detect malware in the IT environment, and verify that existing anti malware already deployed are functioning optimally.

- Audits presence, configuration and up-to-date status of AV products
- Leverages direct and indirect malware detection
- Combines assessment scans, network sniffing, and log analysis
- Utilizes known good and known bad process intelligence

The Problem

Every year corporations spend billions of dollars on anti-virus products. There are several different techniques that AV(anti-virus) and AM (anti-malware) products use to detect malicious software trying to install itself, and to identify and remove malware already present on a user’s computer. A significant technique is the use of signatures, which are periodically released from the AV vendor. More recently heuristic analysis has also become more common, which tries to rely on more generic signatures to catch malware variants. Other techniques include malicious activity detection (OS, kernel, registry and network activity) and sandboxing. However there are a couple of major problems with these traditional techniques.

**Signature-based AV is no longer enough**

Signature-based anti virus products are only effective against malware that is known, has been researched by the AV vendor’s research team and the AV signature has been created for that malware. However the problem with this method is that the number of new malicious programs created every day very easily overwhelms these research teams.

There are varying estimates on just how much of the malware is new malware. For example, McAfee reported approximately 100,000 new individual malware samples per day and Kaspersky Labs reporting over 200,000 per day.

These numbers make it impossible for AV vendors to keep their signature databases up to date with the volume of malware being created. In fact the effectiveness of the major AV products has been cited to be extremely low, particularly for new malware samples. In 2010 a test conducted by Cyveillance found AV detection rates of roughly 25%-30% for newly created malware, and a more recent study by Imperva (Dec 2012) cited this figure even lower at 5% detection rates.
AV vendors are unable to generate signatures fast enough to keep organizations secure from new and self-replicating/mutating malware. Often it takes weeks for the AV vendor to publish signatures for new malware. Once again numbers vary, but figures of 2-8 weeks are not uncommon, leaving organizations vulnerable to attack for weeks after the attack has been identified.

Signature based AV products are also rendered ineffective because they are freely available. Hackers and creators of malicious software generally test their wares against most of the available AV products, and specifically design malware to evade AV products.

**The Organizational Perimeter Has Moved**
Up until the recent past organizations could mandate the computer that users could work from, typically provisioning these machines themselves, strictly controlling the software on it and even restricting these machines physically inside the organization’s location, and hence inside the firewall. However this paradigm has shifted as users and organizations adopt the BYOD phenomenon. Applications are also now moving very quickly out of the traditional data center and into the cloud. Corporate users are using cloud applications and services in addition to traditional IT resources to perform their daily job functions.
This trend is reflected on the malware creation as well, with hackers moving swiftly to exploit mobile devices, tablets, web browsers and applications. McAfee reported a drastic increase in mobile malware, particularly on Android but also on iOS in their recent quarterly threat report.

In addition to mobile malware, there has been a dramatic increase in botnets, SQL Injection and cross-site scripting attacks and websites/domains serving malware to unsuspecting visitors. The Aite Group estimated that in 2012 there were over 10,000 new malicious domains being deployed every day.

**Tenable Malware Detection**

Tenable provides a unique, multi-pronged approach to detecting malware in your organization in its SecurityCenter Continuous View (SCCV) security platform. Using a combination of active scanning, network sniffing and log collection capabilities, SC CV detects sophisticated malware that other anti-virus and anti-malware products miss. By uniquely combining these technologies Tenable can identify potentially malicious software running in your environment that has not been classified as good or bad, and can also find Trojans, botnets and advanced persistent threats (APTs). Tenable SCCV provides coverage for mobile, virtual and cloud/SaaS components of a hybrid and dynamic datacenter.

**Audit Effectiveness of Deployed Security Products**

The ability to verify the effectiveness of your existing security solutions, including AV and AM defenses, is becoming increasingly important because of the two trends described above. Tenable SCCV has the capability to audit hosts and servers for non-existent or misconfigured anti-virus software.
Vulnerabilities are rapidly exploited in organizations that do not keep up with the software updates provided by software vendors, particularly operating system web facing application vulnerabilities. SCCV scans hosts for their patch status and can alert administrators if there are systems in the environment that have security holes due to out of date patches. Using SCCV reports, security analysts can track the effectiveness of their patch, forensic and incident response processes.

Direct and Indirect Malware Detection
Tenable SCCV leverages its Nessus direct assessment scans and indirect PVS scanner to detect malware on Windows systems. Using a dissolvable agent, Tenable SCCV scans the machine’s running processes and compares these to a malware hash provider, generating a report of any malware processes that are discovered.

In addition to this, Tenable SCCV allows you to detect and alert on malware hashes that your own research team may have discovered and want to monitor against. This capability can also be extended to other third-party research that needs to be added to the list of known malware detection. Using this capability, Tenable has built coverage for malware defined by the Mandiant report “Malicious Process Detection: APT1 Software Running” and finds a variety of malware known collectively as APT1. APT1 detection is also augmented by the ability to detect APT1 SSL certificate manipulation. Finally, Tenable SCCV is able to detect a wide range of software that may not appear distinctly on “known bad software” definitions, but that may violate corporate policies and hence is prohibited from organizational networks.

Botnets are a major problem, consisting of millions of unsuspecting hosts in corporations and other organizations. Tenable SCCV is able to find machines that are part of a botnet by evaluating the host itself, by checking the host’s external communications to see if it is sending or receiving traffic to a known botnet, and by comparing DNS entries to malicious URLs and IP addresses. Tenable SCCV is able to detect botnet hosts and activity on its own, independent of any AV or IDS product.

Combination of Scan, Sniff and Log Correlation
Using a multi-vector approach to detecting malware makes Tenable SCCV much more effective at detecting malware in your environment, particularly newly created malware that does not register on traditional security products. SCCV leverages direct vulnerability scans, passive network monitoring and log collection and correlation to find sophisticated attacks.

Host assessment detects malicious processes running on the host. Direct assessment also uncovers “backdoors”, default accounts left unsecured, rootkits, memory resident malware, BIOS exploits and a number of other security breach technologies.

Network sniffing uncovers another class of threats, by passively analyzing network traffic and looking for unauthorized file browsing, manipulation of DNS entries, database access requests, web based attacks targeting web applications and suspect internet communications. Network sniffing is also an extremely useful tool when looking for botnet infiltration, and for the forensic analysis of what activity the bots in your environment have conducted. To help incident response and forensic analysis of malware activity, SCCV is able to collect log data from across the enterprise. This log data can be correlated within the logs themselves, as well as with the assessment scan and network sniffing capabilities to provide richer security context.

For example if a recent scan discovered a new malware process on a particular host, the network monitoring component of SCCV can demonstrate all communications that host is engaged in, and the log correlation component of SCCV can find other instances of that malicious process across the network. Scan and sniff data can also be combined to search for hidden services running unauthorized applications, or worse still – collecting and communicating sensitive information to external command-and-control servers.
Utilizes Whitelist, Blacklist and Grey-list Intelligence

In every organization there are many software components in use that are neither categorized as “good applications”, nor as “malicious software”. This is particularly true for organizations that allow self-provisioned machines and mobile device access to critical services. This "grey-list" of unknowns could consist of thousands of individual software, applications and services, and provides a very large footprint from which attacks can take place.

To bring the risk down, SCCV identifies software that is known good and known bad and the remaining unknown software is tracked as "grey-list". Security teams can separate and isolate these unknown processes, investigate it at a deeper level and if necessary take mitigation actions where processes are found to be exhibiting abnormal behavior, initiating malicious and evasive actions, or even unauthorized according to organizational policies.

Summary

Security threats are growing exponentially, and while traditional security products like anti-virus and anti-malware solutions are a crucial component of an effective layered security program they need to be audited for effectiveness, and complemented by advanced malware detection techniques. Tenable SCCV provides the additional layer of verification and sophisticated malware detection needed to find and deal with the malware that has already infiltrated your organization. By combining its assessment scan, network sniffing and log collection and correlation capabilities, SCCV is able to give security analysts the assurance that malware is not going to damage their organization.

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 24,000 organizations, including the entire U.S. Department of Defense and many of the world’s largest companies and governments. For more information, please visit tenable.com.