Trend Micro™ Titanium™ 2012 and the Microsoft™ Windows™ Firewall

Strong, Fast, Easy-to-use

How Titanium 2012 Boosts the Protection of the Windows Firewall

V1.7a

A Trend Micro Whitepaper | July 2011

Related Documents:

Titanium 2012: State-of-the-Art Endpoint Security

What's New in Titanium 2012?

Table of Contents

1. Executive Summary: Trend Micro Titanium™ 2012 and the Microsoft™ Windows™ Firewall

Consumers often complain that their endpoint security software is intrusive, overly complex, and eats up system resources, even as they continue to demand the best antimalware protection money can buy—all in the context of growing complex threats. In response, Trend Micro has created Trend Micro Titanium™, a three-sibling family of consumer endpoint security products that provide security that's stronger, leaner, and simpler to use than ever before. Not only is Titanium more user-friendly than its predecessors, it has reduced its impact on system resources, while enhancing the state-of-the-art security protections users require.

Trend Micro has accomplished the feat of improving protection while reducing the computer footprint in part by removing its own firewall, deferring to the now maturing Microsoft™ Windows™ Firewall. To address what's missing in the Windows Firewall, Titanium Internet Security and Titanium Maximum Security, the mid-range and high-end versions respectively, add "firewall boosters;" while the whole Titanium family adds other security enhancements, including Web threat protections, to strengthen the security posture of consumers' machines.

This whitepaper outlines the rationale and benefits of this dual strategy; explains how it affects Windows™ XP, Windows™ Vista™, and Windows™ 7 users; and profiles the additional security enhancements Titanium provides.

2. Introduction: The Changing Threat Landscape vs Bloated Security Software

As the Internet has expanded across the globe, threats to computer security have also grown. Long gone are the days when mass viruses or worms were unleashed upon an unwitting public merely to boost a hacker's notoriety. Nowadays, users are more apt to be exposed to blended, stealthy, or well-targeted threats—ones that will steal your identity, your data, or your money, while you're not looking—or even when you are.

In response, security companies have added layer upon layer to their endpoint security products, to address the fact that today's threats can come from multiple vectors—from the Web or email, from instant messaging or social networking sites, from infected files, hidden rootkits, or leaky networks—or a treacherous combination thereof. But as the volume and variety of threats has grown, so has the technical burden on the typical endpoint security product, with the result that good security is often had at the expense of a slower computer—higher CPU, memory, and hard disk usage—and annoying, intrusive pop-ups or complex settings that only software engineers can understand.

What's a security company to do? Trend Micro believes that modern endpoint security technology needs to simultaneously address the shifting threat landscape, better tailoring new antimalware methods to contemporary threats, while cutting the fat from security software in all ways that it can without weakening protection. To meet these dual requirements, seemingly at odds, Trend Micro engineers have come up with an ingenious solution. Why not *remove the firewall* from the endpoint security product, since Windows already provides one, while strengthening both the Windows Firewall itself and the endpoint product's more forward-looking security technologies—the ones that best address just how users get infected today?

So that's precisely what Trend Micro has done. But before we outline the benefits (and some of the gotchas), we'll present a little history.

3. Firewalls Compared: Trend Micro Personal Firewall vs. the Windows Firewall

In the past, when customers installed Trend Micro™ Internet Security (TIS) or Trend Micro™ Internet Security Pro (TIS-Pro)—the immediate predecessors of Titanium Internet Security and Titanium Maximum Security respectively—the Trend Micro™ Personal Firewall (TMPF) was enabled and the Windows Firewall disabled by default. While this had some advantages (all the main network security controls were under one Trend Micro roof), it also had some drawbacks, both from a technology and a user perspective:

- TMPF added to the system resource footprint, since the disabled Windows Firewall components were still present in memory, though they were turned off.
- Some pop-up messages in TMPF confused naïve users, ironically exposing them to more threats (as when they clicked "allow" to a system change when they shouldn't have).

These drawbacks aside, a comparison of TMPF with the Windows Firewall shows that Windows XP SP3 users in particular would appear to have diminished network protection now that TMPF has been removed from Titanium; while Windows Vista and Windows 7 users are also affected, though to a lesser degree.

Note: The table below only addresses the firewall components most relevant to our discussion. Not all features in the firewalls are listed in the table.

Table 1. Trend Micro Internet Security Pro 2010 | Microsoft Windows Firewalls | Titanium Firewall Boosters and Complementary Protections

Firewall Function	Trend Micro Internet Security/Pro 2010	Windows Firewall on XP SP3	Windows Firewall on Vista	Windows Firewall on Win7
Location Change Detection	√		√	√
Firewall Profile Concept	√		√	√
Application Filter	√		√	√
Inbound Firewall Rules	√	√	√	√
Outbound Firewall Rules	√	Partial*	√	√
My Home Network	√			
IPv6 Support	√	M	√	√
		Trend Micro Titanium 2012		
Network-Level Vulnerability/Exploit Detection**	√	T1	T1	T1
Intrusion Detection System	√	T1	T1	T1
Proactive Botnet Protection***		T1	T1	T1
Complementary Protections				
Internet and Email Controls	√	T2	T2	T2
Behavior Monitoring**	√	T2	T2	T2
Browser Exploit Solution**		T2	T2	T2

Key:

* Some outbound protection is provided via Trend Micro Proxy (TMProxy); See Section 3 following.
** Enhanced feature in Titanium 2012
*** New feature in Titanium 2012
√ = Feature Available
M = Absent in Windows Firewall, but Additional Install Available from Microsoft
T1 = Absent in Windows Firewall, but the Titanium Firewall Booster Provides the Feature
T2 = Absent in Windows Firewall, but additional Titanium Protections Complement it
Blank = Feature Absent

To address these missing elements, Titanium 2012 supplements the Windows Firewall protections with “firewall boosters” and other network-related security enhancements, which we’ll discuss in Section 3 of this whitepaper. For those it won’t supplement, it offers the following assessments and remedies for Windows XP SP3 users in particular.

Location Change Detection

To achieve better protection when a user is on the road (roaming through different networks), TMPF in TIS/TIS-Pro implements “Location Change Detection” to correctly identify which physical network environment a user’s PC is connecting to. By doing this, TMPF can set different firewall rules for different network environments. For example, in a public Wi-Fi network environment, TMPF can disable file-sharing-related network ports to better protect the user.

Both Windows Vista and Windows 7 provide Home, Work, Public, and Domain network location settings to adjust for the type of network you’re connected to.

The Windows Firewall in Windows XP SP3 does not provide a Location Change Detection function and though it does provide some of the building blocks of location awareness (such as Network Interface Card (NIC) and IP Address detections), these cannot be leveraged in Windows XP without the rule structure to apply them to the firewall engine. That said, Windows XP laptop users can “harden” the inbound Windows Firewall rules when they’re out of the office by checking the “Don’t Allow Exceptions” function for extra security. In addition, users of any member of the Titanium family obtain additional protection via the Domain Reputation Service in the Trend Micro™ Smart Protection Network™ (SPN) infrastructure, which maintains an up-to-date database of good and bad domains. Finally, Titanium Maximum Security also provides a Wi-Fi protection feature that displays a warning when connected to potentially unsafe wireless networks or hotspots.

Summary: Mobile users of Windows XP don’t have Location Change Detection, but a combination of native and Trend Micro technologies can address the issue.

Remedy: Users of laptops running Windows XP can “harden” the default inbound firewall restrictions by not allowing exceptions when travelling and using Wi-Fi connections. Moreover, Trend Micro’s Domain Reputation Service in the Smart Protection Network (SPN) adds an additional layer of protection by checking good and bad domains, blocking the bad ones. Finally, Titanium Maximum Security users also get an extra layer of Wi-Fi protection: the user is warned when they try to connect to unsafe wireless networks or hotspots.

Firewall Profile Concept

As described above, TMPF provides the capability to detect a location change. TMPF then implements the “Firewall Profile” concept in TIS/TIS-Pro by associating one set of firewall rules (the so-called “firewall profile”) with a network location, to achieve automated location-aware firewall protection. So a firewall profile (like “Direct Internet Connection”, “Home network”, “Office network”, etc) represents a group of “firewall rules” that a user might set, which would then automatically come into play when the new network location is detected.

TMPF also combines the “Firewall Profile Concept” with that of “Security Level” (maximum, medium, low, and minimum) to greatly simplify the configuration effort when a user adjusts the firewall strength. For example, the user will likely set the security level to “maximum” on a “Direct Internet Connection” firewall profile.

The Windows Firewall in Windows XP does not support this feature through its UI, though it does in Windows Vista and Windows 7. For instance, selecting “Windows Firewall with Advanced Security” in Windows Vista or Windows 7 Administrative Tools brings up a window to add and manage Advanced Firewall Settings such as inbound/outbound rules or connection security rules, then applies them to Domain, Private, or Public profiles.

Summary: Mobile users of Windows XP don’t have a Firewall Profile Concept, but a combination of native and Trend Micro technologies can address the issue.

Remedy: The situation is almost identical with the one above. Users of laptops running Windows XP can "harden" the default inbound firewall restrictions by not allowing exceptions when travelling and using Wi-Fi connections. Moreover, Trend Micro's Domain Reputation Service in the Smart Protection Network (SPN) adds an additional layer of protection by checking good and bad domains, blocking the bad ones. Finally, Titanium Maximum Security users also get an extra layer of Wi-Fi protection: the user is warned when they try to connect to unsafe wireless networks or hotspots.

Application Filter

Generally speaking there are two types of firewall rules provided by modern stateful firewalls (including the TMPF, Windows XP SP2, Windows Vista, and Windows 7 firewalls):

1) Network Five-tuple firewall rules (Network Protocol, Source IP, Destination IP, Source Port, Destination Port).
2) Program control firewall rules (or the so-called TMPF Application Filter).

For not so tech-savvy users, the TMPF "program control" firewall rules are easier to understand and set than the Windows firewall rules, while the TMPF Application Filter also triggers system tray pop-ups to notify the user there is an application program trying to connect (for outbound packets) or bind (for inbound packets) to the network protocol stack (TCP/IP). Unfortunately, the latter feature is no longer considered effective because it relies on the user's decision to allow/block the application program—and most of the time the user will just allow the connection. Moreover, the TMPF outbound application filter is no longer considered effective because the majority of malwares today actually use Windows components as a proxy to redirect their outbound traffic. The most famous targets today are Internet Explorer® and svchost.exe; Internet Explorer alone takes 42% of the outbound traffic, according to internal Trend Micro reports. Hence, the decision to default to the Application Filter function in Windows Firewall makes more sense, particularly for Windows Vista and Windows 7, even though Windows XP only provides inbound application filtering for applications like FTP, Internet Mail, Web, and Telnet Servers.

The key way that Titanium Internet Security and Titanium Maximum Security address this problem is through the Unauthorized Change Prevention module, which protects the computer from suspicious changes to the system. It does this by monitoring the behavior of executables via black and white application lists, as well as the program's digital certificate, thus blocking the bad behaviors. Users are protected from outbound bad behavior, such as unauthorized "phoning home," by proactively preventing such infections in the first place.

Summary: The Windows Firewall in Windows XP only provides inbound application protection, while the Windows Firewall in Windows Vista and Windows 7 provides it in both directions. Titanium addresses Windows XP's shortcomings by monitoring applications.

Remedy: Titanium's Unauthorized Change Protection module protects end-user computers from suspicious changes on the host system, protecting users on the Application layer via Black/White application lists and digital certificates, among other functions. See the second section below for more details.

Outbound Firewall Rules

The protection of a stateful firewall is achieved by applying firewall rules to a firewall engine. (Firewall rules are applied by the active network profile). Firewall rules can be categorized by connection or direction—such as inbound rules (incoming to the PC) or outbound rules (outgoing from the PC). Note that the Windows Firewall in Windows XP provides inbound rules, but not outbound ones; while Windows Vista and Windows 7 provide both. That said, even though Windows Vista and Windows 7 have outbound firewall engines, their default outbound firewall rule is “Allow ALL except rule matched.” Moreover, there are no default “Block” outbound firewall rules in Windows Vista and Windows 7, though the user can add rules to change that.

Why should you enable a firewall’s Outbound protection? The answer is fairly simple: to prevent malwares and viruses from sending confidential information back to their botnet servers. When backdoor worms attack your computer, they steal the information and then connect to an external hacker’s server to send the data. Enabling Firewall Outbound Connection will prevent any outbound connection except for the applications you define, thus keeping your system more secure.

Since the Windows Firewall in Windows XP does not provide outbound rules, removing the TMPF can expose users to “phone home” malware behavior. However, this presumes that the malware has been able to bypass the inbound firewall rules in the first place. The way it might do this on a consumer’s endpoint machine would be through a Web, Email, or File exposure vector. Fortunately, Titanium provides such protections with its Web Threat Protections (WTP)—Web, Email, and File Reputation Services. These are supplemented in Titanium Internet Security and Titanium Maximum Security with the Unauthorized Change Protection module (see section below).

Note too that Trend Micro Proxy (see section 3 following) can block some but not all outbound requests. It can block HTTP/S on any port, though the current default implementation just uses the standard HTTP/S ports such as 80, 8080, 8081, 443, etc.

Note: Some command-and-control malwares use the Internet Relay Chat as the protocol to communicate to their server. In this case, the malware’s “phone home” will not be blocked by Trend's Web Threat Protection (WTP). However, if the command-and-control malware uses the HTTP protocol and the domain/URL is in our WRS database, the “phone home” will be blocked.

Summary: Although Windows Firewall in Windows XP does not have outbound rules, which could allow a malware to “phone home” if it got installed, Windows XP users can obtain the protection accorded Windows Vista and Windows 7 users by means of Titanium’s WTP and behavior monitoring modules.

Remedy: Titanium’s Web Threat Protection function, which includes Web, Email, File, and Domain Reputation Services; and its Unauthorized Change Prevention module in the mid-range and high-end Titanium products, can together proactively prevent this kind of malware infection from ever occurring. Malwares never get a chance to install and phone home.

IPv6 Support

TMPF and the Windows Vista and Windows 7 Firewalls support IPv6 by default. While the default Windows XP firewall does not support IPv6 by default, a separate downloadable firewall package from Microsoft supplements Windows XP to support IPv6.

Summary: Windows Firewall in Windows XP does not support IPv6 by default.

Remedy: Download and install the IPv6 package from Microsoft.

My Home Network

“My Home Network” in TMPF provides users with a Home Network Map of all computers on the local network (Network Discovery), which they can use to block wireless network users from accessing any computer on the network (Wi-Fi Protection), or to manage and update compatible security software (TIS/TIS-Pro) for those computers (basic Remote Administration). My Home Network is implemented by sending Address Resolution

Protocol (ARP) broadcast packets to the local LAN to identify all neighboring network devices (including other PCs). While this feature is nice to have, in practice, consumer users rarely use it.

Windows XP does not have a similar feature for its Windows Firewall, but Windows Vista and Windows 7 provide the basic layer (only the first of the above three functions) for insight into what's active on your network. This is implemented as a Network Discovery setting that affects whether your computer can see or find other computers and devices on the network and vice versa. Network Discovery can be On or Off, or users can define a Custom mixed state in which some services are enabled and some aren't. As long as the Windows Firewall exception for network discovery is enabled and other firewalls are not interfering with it, the network discovery state is active and shown as Custom.

Summary: This is a "nice to have" feature; Windows XP users do not have a similar function, but the feature is not used much by the average consumer.

Remedy: Windows Vista and Windows 7 can use Network Discovery for basic insight into devices and computers on the home network.

4. Titanium Firewall Boosters and Complementary Protections

As Table 2 reminds us, Trend Micro supplements the Windows Firewall in two main areas, using firewall boosters (T1) and complementary protections (T2), which together provide an up-to-date response to the removal of TMPF. Most of these functions were originally included in TIS/TIS-Pro, though Titanium 5.0 adds a new "browser guard" feature that prevents Microsoft Internet Explorer from running malicious scripts on infected websites.

Table 2. Titanium Firewall Boosters and Complementary Protections

Firewall Boosters	**Trend Micro Internet Security Pro 2010**	**Windows Firewall on Windows XP SP3**	**Windows Firewall on Vista**	**Windows Firewall on Windows 7**
		Trend Micro Titanium 2012		
Network-Level Vulnerability/Exploit Detection	√	T1	T1	T1
Intrusion Detection System	√	T1	T1	T1
Proactive Botnet Protection		T1	T1	T1
Complementary Protections				
Internet and Email Controls	√	T2	T2	T2
Behavior Monitoring	√	T2	T2	T2
Browser Exploit Solution		T2	T2	T2

Key: √ = Feature Available
T1 = Absent in Windows Firewall, but Titanium 2012 Firewall Booster Provides the Feature
T2 = Absent in Windows Firewall, but additional Titanium 2012 Protections Complement it
Blank = Feature Absent

Firewall Boosters

Network-Level Vulnerability/Exploit Prevention

Network viruses (e.g., worms) are so described because of their ability to directly spread from one computer to another without user intervention. Network viruses typically achieve this by sending specially-crafted code that exploits system and application vulnerabilities on target computers.

Titanium's Network Content Inspection Technology (NCIT) allows it to check payloads in network packets (TCP/UDP) against rules in a Network Content Inspection Pattern (NCIP), then to drop or accept packets based on the results. The Network Content Inspection Engine (NCIE) can do both inbound and outbound network packet scans using enhanced patterns and rules created and modified by the TrendLab anti-malware team. These rules are automatically updated to the endpoint whenever a major network-level vulnerability is found.

For example, because the Conficker/Downad worm uses an exploit of a particular vulnerability to spread, TrendLabs can create a rule based on distinct exploit-related characteristics in the payloads of Conficker/Downad packets. The network engine is then able to drop Conficker/Downad packets and possibly other malicious packets that contain the same exploit. In short, NCIT can detect not only the payload of the network viruses, but also the underlying network packet-level vulnerabilities used by these viruses, therefore stopping all variants of viruses exploiting the same vulnerability.

Intrusion Detection System (IDS)

The Intrusion Detection System (IDS) provided by TMPF is included in Titanium 2012 and provides strong detection capability* for a variety of network intrusions, including such things as the "Ping of Death," "Trace Route," and "SYN Flood"—typical indicators that an intrusion may be taking place. While most of these attack techniques have been around for quite some time and are not the latest-and-greatest in a hacker's arsenal, Trend Micro still considers them dangerous enough to continue to provide them as a Windows Firewall Booster. (Note though, that home routers/Wi-Fi access points often provide similar features by default.)

***Note:** A January 2009 report from West Coast Labs entitled *Trend Micro Worry-Free Business Security [WFBS] Comparative Testing Report*, which gave the results of comparative lab tests of Trend Micro™ Worry-Free™ Business Security 5.0 and three competitors, included important details about the IDS function in Worry-Free Business Security's firewall—the same Trend Micro IDS component used in Titanium. When compared with the IDS function in the competitors' products, Trend Micro's WFBS 5.0 IDS detected and logged some 30,000 intrusion attempts, while Symantec's Endpoint Protection 11.0 logged only one, and McAfee's Total Protection Advanced 4.5 and Microsoft's Live OneCare for Servers (Beta) logged none.

Proactive Botnet Detection

Botnets are considered one of the most prevalent and dangerous threats lurking on the Web today, in part because the number of botnet unique binaries is huge and increasing, rendering file-based detection reactive and ineffective. The damage botnets cause can range from information theft and malware infection to fraud and other crimes. A botnet refers to a network of bots or zombie computers widely used for malicious criminal activities like spamming, distributed denial-of-service (DDoS) attacks, and/or spreading FakeAV malware variants. A botnet connects to command-and-control (C&C) servers, enabling a bot master or controller to make updates and to add new components to it.

Since file-based detection is reactive, to better combat botnets Titanium 2012 incorporates network-layer botnet detection and cleanup using Trend Micro's new Network Content Inspection Technology (NCIT). NCIT detects known and unknown botnet infections based on suspicious network traffic behavior. Botnet binaries may vary, but they rely on the internet to receive and send commands, upload data, etc. As such, botnet network traffic has specific characteristics and commonalities within the same botnet family. NCIT extracts these common network traffic traits and uses them to detect thousands of botnet infections. The approach is highly generic. To detect thousands of new and known Zeus variants, for example, only a few NCIT rules are required.

Titanium's NCIT protects you from botnets that use both non-standard and standard ports to communicate to a C&C server; and supports TCP/UDP protocols, including HTTP, SMB, FTP, IRC, as well as popular IM/P2P, SMTP, and POP3 protocols, etc.

Complementary Protections

Titanium also bolsters the network-layer security posture of the consumer's computer by complementing the Windows Firewall protections at the application layer.

Internet and Email Controls

Trend Micro's cloud/client-based Internet (aka Web Threat Protection) and Email Controls are important parts of the Smart Protection Network (SPN) and are comprised in part by Web, Email, File, and Domain Reputation Services (the newest addition to the SPN, which blocks the DNS query when the domain name is suspicious). These gather the respective reputations of websites, IP Addresses, files and applications, as well as domains, to protect users from exposure to the malware in bad URLs, emails and instant messages, as well as files and domains. These cloud/client-based services are correlated with each other and include intelligent feedback loops, to provide state-of-the-art, real-time protections for the global community of Trend Micro customers, including users of endpoint protection solutions such as Titanium.

According to TrendLabs threat statistics data, the majority of threats come from the Internet via malware posted on malicious, hacked websites. Titanium blocks malicious web sites automatically when the user browses the internet, but also comes into play when malicious URLs are placed in phishing emails or instant messages. If a user clicks the link in the email, they're automatically blocked. This ability has now been extended to URLs on Social Networking Sites such as Facebook, MySpace, Twitter, or Mixi (in Japan).

In addition, as part of its Internet Controls, Titanium provides Wi-Fi protection, which displays a warning when connected to potentially unsafe wireless networks or hotspots.

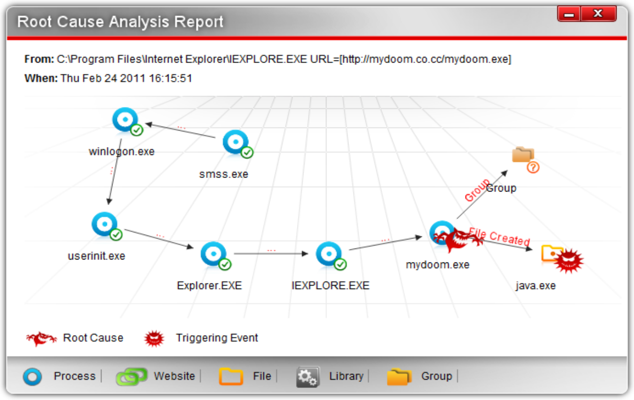
Finally, Titanium includes a process brought over from TIS/TIS-Pro called Trend Micro Proxy (TmProxy), an ISO OSI (Open System Interconnection) Layer 7 (Application Layer) traffic scanning process that runs on the user's local machine, scanning for malware like spam, viruses, private data, bad URLs, as well as changes to the Hosts file, etc. TmProxy receives network traffic redirected by a subcomponent, then parses the network protocol and scans the content inside. The whole process works like a local network proxy on the user's machine—which is why the component is called TmProxy. Currently, the network protocol parsers supported by TmProxy include HTTP/S, SMTP, POP3, and popular IM programs. Additionally, Trend Micro Proxy can block some but not all outbound requests. It can block HTTP/S on any port, but the current implementation just uses the standard HTTP/S ports such as 80, 8080, 8081, 443, etc.

Behavior Monitoring

Most malicious executables dropped by infected websites or included in phishing emails or instant messaging—such as FakeAV, Trojans, or Bots—are proactively stopped by Titanium's real-time and disk scans, supported by the Web, Email, Domain, and File reputation systems of the Smart Protection Network. However, when malicious programs do manage to get past the exposure and infection protection layers, they can still be stopped at the execution layer. As malicious programs install and execute, the endpoint security product's behavior monitoring ability needs to address the fact that malicious executables are often packed and encrypted; can drop other files as part of a whole infection strategy; and once launched and installed, can make malicious system changes to your system, to steal data or hijack it. This problem is exacerbated by malicious programs present on USB drives.

Titanium 2012 has enhanced its unauthorized change prevention / behavior monitoring capabilities by providing an enhanced emulation mode that efficiently unpacks encrypted malware and runs it in a protected environment in both real-time and manual scan modes, scans the unpacked files, then compares them against file and system signatures, as well as heuristic rules. If malicious, the malware is stopped from completing its execution. Titanium then cleans the machine of all system changes, restoring it to health.

In addition, Titanium's behavior monitoring incorporates threat diagnostics, cross-correlating upstream and downstream events, processes, and system changes that malware can make, so that a multi-stage infection process can be tracked and stopped. It can identify other malware components, such as droppers, downloaders, etc., from a single infection. Once identified, Titanium will perform a total cleanup these components in the infection chain. The infection chain map (called the Root Cause Analysis or RCA report) will be displayed to user, showing where the malware comes from, what components the malware creates, etc.



Root Cause Analysis Report

From: C:\Program Files\Internet Explorer\IEXPLORE.EXE URL=[http://mydoom.co.cc/mydoom.exe]

When: Thu Feb 24 2011 16:15:51

Figure 1. Root Cause Analysis Report

Titanium 2012 also lets you increase the aggressiveness of the function. By elevating your behavior monitoring protection against unwanted system changes to "Hypersensitive" you can increase the sensitivity of your system to malicious applications and more aggressively stop them in their tracks.

Finally, Titanium 2012 has enhanced its behavior monitoring protection against malicious *autorun* programs on USB drives, enabling the function by default, while providing digital signature and whitelist checks for valid *autorun* programs.

Browser Exploit Solution

Web threats while browsing—including drive-by downloads of malicious files, cross-site request forgeries, Web Trojans, malvertisements, and so on—continue to grow exponentially by means of browser exploits. A browser exploit is a form of malicious code that takes advantage of a flaw or vulnerability in a browser with the intent to alter a user's browser settings or execute code without their knowledge. Malicious code may exploit ActiveX, HTML, images, Java, JavaScript, and other Web technologies and cause the browser to run arbitrary code. Many malware writers today use JavaScript to infect or deliver malware, using a 0-day browser exploit, and may use obfuscation and encryption to avoid detection. One of the major issues is so-called detection avoidance, which means malicious content is served selectively depending on the company, region, referrer, language, and the browser that provides the immediate context for the infection. So how can an endpoint security solution protect you from browser exploits?

The enhanced Browser Exploit Solution (BES) in Titanium 2012 addresses browser vulnerabilities that can be exploited in both Internet Explorer and Firefox. These include browser plug-in vulnerabilities that can be exploited for ActiveX/BHO, Adobe, or other media plug-ins; as well for Java extensions. BES addresses browser exploits by including such protections as behavior-based pattern matching; DOM Parser, JS Emulation, and Script-based exploit detection, using heuristics; generic shellcode detection; enhanced signature-based detection, and other methods.

5. Conclusion: Building a Better Consumer Endpoint Security Product

As the threat landscape has changed—with threats now coming particularly from the Web—consumers need endpoint security products that more adequately address the latest threat vectors. At the same time, users are tired of bloated endpoint security software that needlessly consumes computer resources. Trend Micro Titanium has addressed both concerns by providing state-of-the-art Web threat protections, while lightening the load on the endpoint by removing its personal firewall in favor of the firewall already present in Windows operating systems. And where concerns might be raised over any missing network security features, Titanium steps up to the plate and compensates for the handicaps.

As this whitepaper has shown, the missing features in Windows XP SP3 in particular can be largely addressed by taking some precautions using the Windows Firewall settings themselves and by utilizing the Firewall Boosters and Complementary Protections in Trend Micro Titanium 2012, which apply to all current Windows versions. The Network Content Inspection, Intrusion Detection System, and Proactive Botnet Detection boosters still provide the core network-layer protections for Windows users, blocking most intrusion attempts, or attempts to hijack your computer for a botnet; while the Trend Micro Internet and Email Protection, Unauthorized Change Prevention, and Browser Exploit Solution modules take up the slack, providing state-of-the-art complementary protections on the Web or right on the host computer itself. Windows XP's missing outbound filtering, for example, is taken care of by the multiple protective layers in Titanium—by the cloud/client Web and File reputation services, or by the Behavior Monitoring module residing locally on the computer.

In short, building a better consumer endpoint security product has meant trimming the fat from the software, while at the same time enhancing it for the modern threat landscape. The Trend Micro Titanium family does just that—and is stronger, faster, and easier-to-use because of it.

July 2011

Malware Definition Sources: Wikipedia, TrendLabs

Authors: Michael Miley, Katie Wen, Jerry Liao, William Kam