



Anchiva Network threat defence White Paper

Contents

- Overview
- Anchiva RapidRx Threat Detection Network
- Intelligent Pattern Recognition Technology
- Malicious Sites Filtering Technology
- Heuristic Behavior Association Analysis Technology
- Web Server Protection
- Internet Application or content Analysis and Control Technology
- Conclusion

Consolidated multi-vector internet threat protection

Overview

The RapidRx Labs is Anchiva’s professional malware research team that focuses on virus, malicious threats, and security lapse research. Since starting research operations in 2005, Anchiva’s RapidRx Labs quickly established itself as a world class malware research organization by actively participating in the malware research community and absorbing world leading malware research elites.

Dynamics, polytropism, and exponential augmentation are the primary features of today’s internet threats and abuse of internet privileges in the workplace. Updated with the latest threat and application intelligence collected from the RapidRx network, Anchiva’s SWG successfully develop Intelligent pattern Recognition Technology, Malicious Sites Filtering Technology, and Heuristic Behavior Association Analysis Technology. With these technologies, Anchiva’s SWG establish a multi layer internet security protection solutions including web application or content analysis and control, web threat protection, providing effective defense to known and unknown network threat as well as zero-hour malware.

Anchiva RapidRx Threat Detection Network

The three primary components of Anchiva’s Threat Detection Network are the Anchiva collecting network, the Anchiva threat center, and the ASDN (Anchiva Services Distribution Network).

Figure 1 below shows the sample collection and analysis process of Anchiva collecting network. RapidRx researchers work diligently and consistently to identify new internet threats by efficiently and accurately analyzing information gathered from a broad collection source. RapidRx actively participates in the malware research community and has been credited with discovering and reporting many new malware threats to the Wildlist Organization (www.wildlist.org). Using multiple collection sources (honeynets, web crawlers, customer feedback, heuristics analysis, and exchange) gives the RapidRx team a broad view malware threats, allowing for the identification of the most active malware threats.

Once the samples are collected, approximately 90% of malware samples are analyzed using IPR technology while the remaining 10% is analyzed manually by RapidRx researchers. As new malware and new malware variants are discovered, Anchiva Malware Signature Library and Anchiva Malicious Sites Database are generated and fed through a strict automated test verification system that tests the accuracy of the signature to detect the new malware. Once the detection accuracy is verified, the signatures are then uploaded to the ASDN for distribution to the field.

Deployed at data centers around the world, the ASDN serves real-time threat intelligence updates to SWG deployed at customer's networks. Comprised of upgrade servers, it guarantees prompt distribution of signature libraries of malware, malicious sites, and web application control to Anchiva SWG.

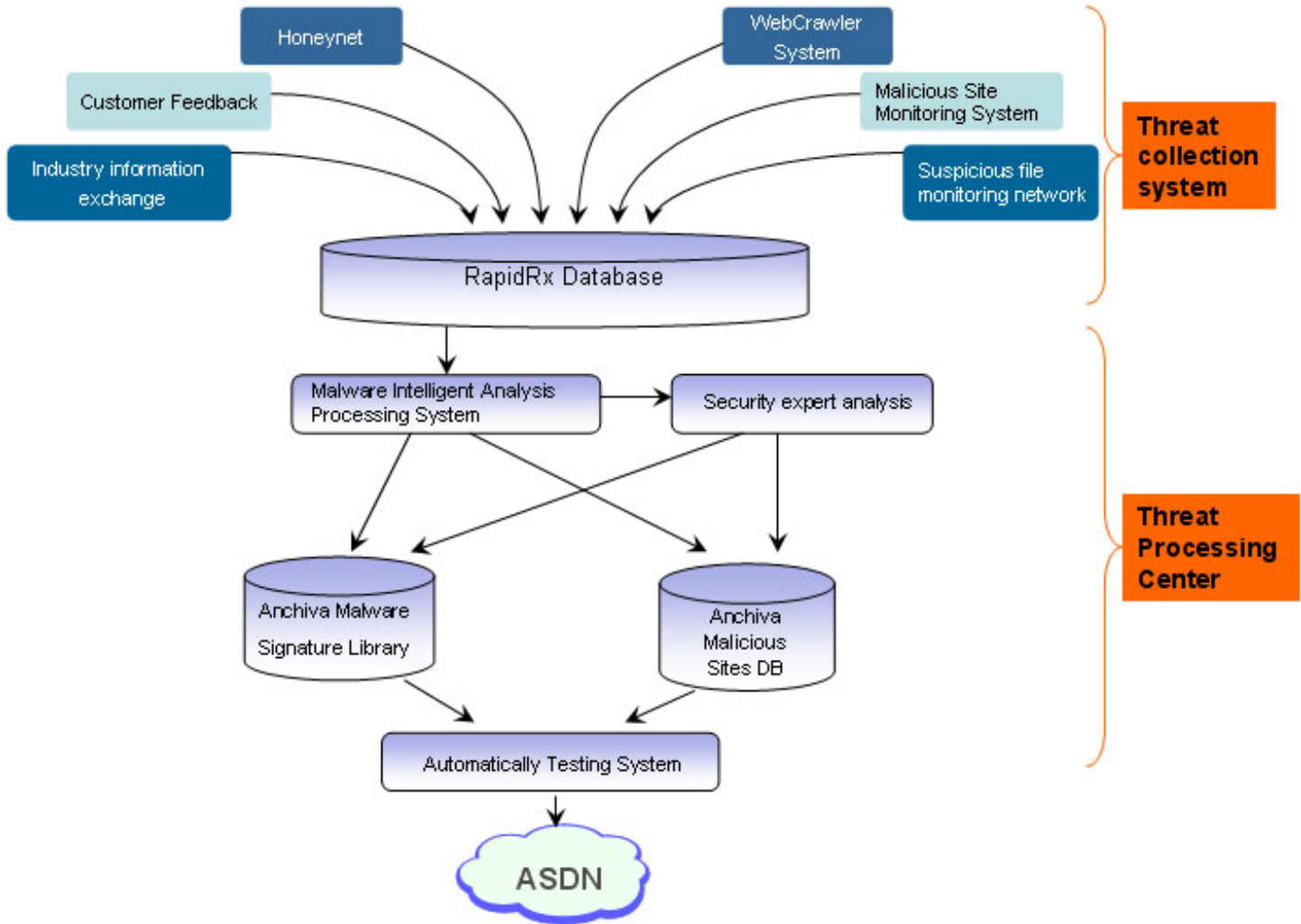
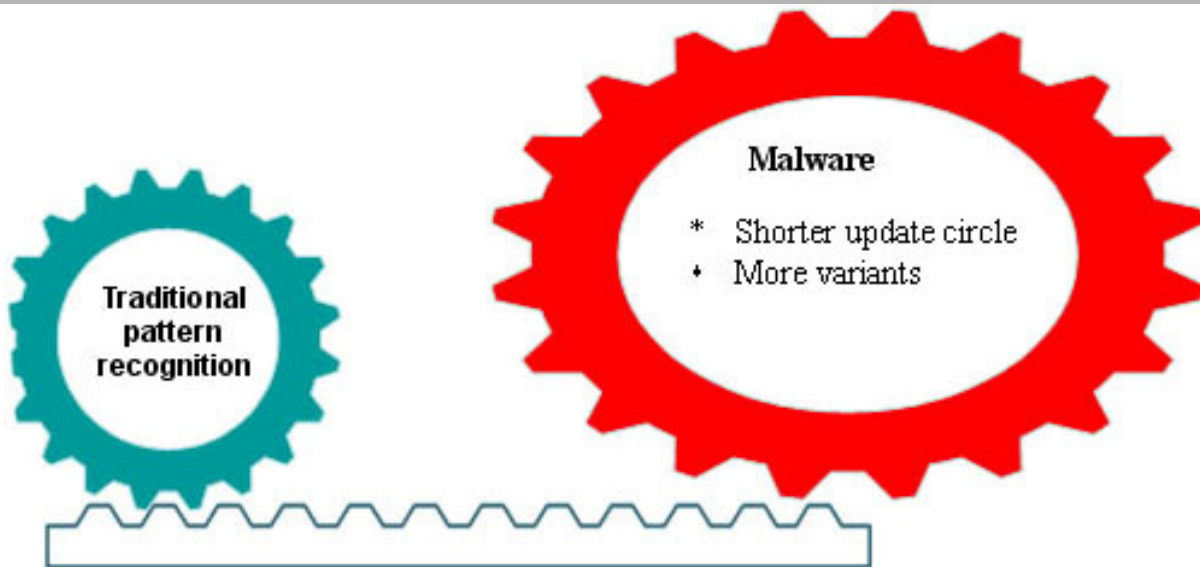


Fig1: Anchiva RapidRx Threat Detection Network

Intelligent Pattern Recognition Technology

Statistics from the RapidRx labs collection centers is showing spikes in malware activity, with thousands of new malware samples collected daily. To keep pace with analyzing these large volumes of samples, traditional human analysis which may generate 20 signatures per man simply cannot scale to provide timely analysis and generate signatures, and have to face the reality that new variants come out before their features are released.



Disadvantages: man-made, inefficiency, always behind malware outbreak, narrow applicability.

Fig2: Traditional Malware Signature

To effectively solve the disadvantages of traditional pattern recognition and raise the adaptability of signature libraries, Anchiva researchers work diligently to make The IPR system accelerates and accurately performs malicious code analysis by breaking down and analyzing the files program structure, file content, behavior features (for example embedded registry or browser modification routines) and embedded evasion techniques. by using three classification libraries — program structure modeling library, application behavior modeling library, evasion technology modeling library — to identify the potential behavior of the code and newly active malware variants as well as provide zero-day protection.

By analyzing and associating the results of the three libraries, Anchiva RapidRx researchers are able to automate the classification process with a very high degree of accuracy. The result is an automated system that scales to analyze, classify and distribute tens of thousand malware samples a day.

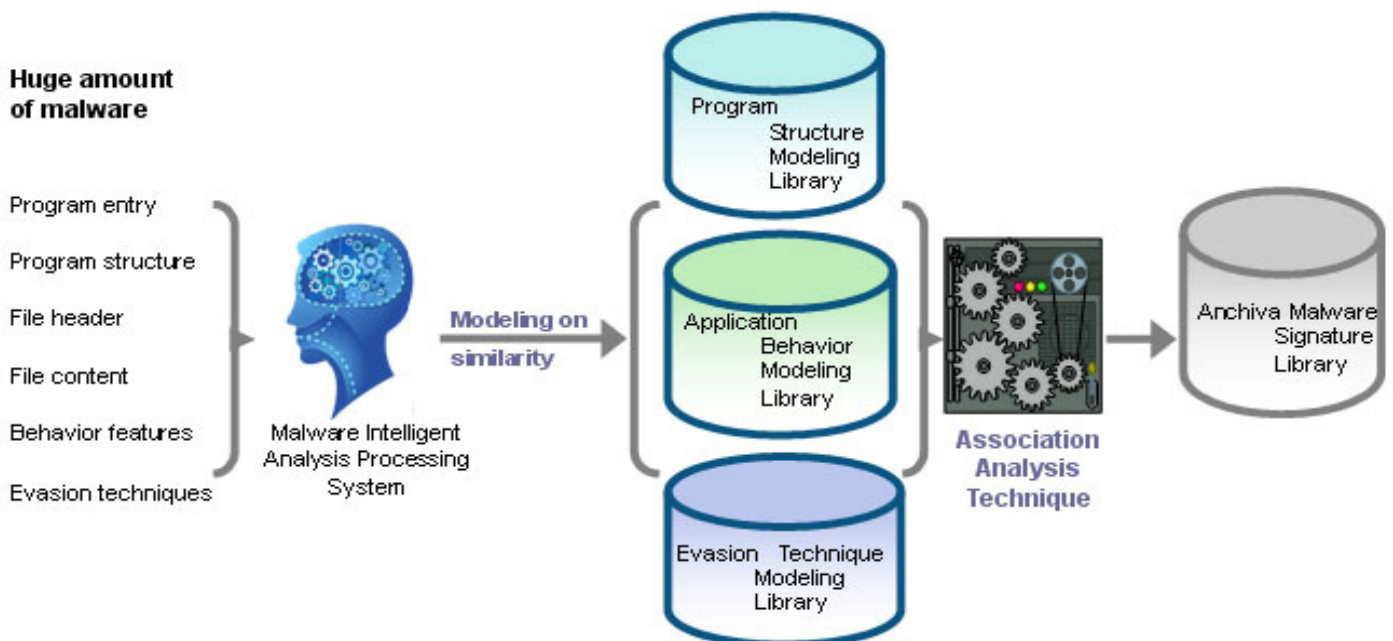


Fig3: Anchiva malware signature

Advantages:

- Meet exponentially increasing malware.
- Detection of polymorphic variants
- Provides zero-day protection against the latest malware

As recognition to the RapidRx's proactive research and classification efforts, the monthly reports from the Wildlist clearly shows Anchiva's ongoing contribution of being first to identify a considerable number of new malwares, malware that were analyzed and classified using both human and the IPR technology.

The table below shows the new malware submitted on November 2008, which were all detected by Anchiva's unique IPR pattern recognition technology. Conversely, the other two vendors need several different signatures to detect these malware.

Wildlist sample	AV Vendor1	AV Vendor2	Anchiva
ITW#66	Trojan.Win32.Vaklik.ced	TROJ_VAKLIK.GY	Trojan/XPack.gen
ITW#65	Trojan.Win32.Vaklik.cce	TROJ_VAKLIK.HU	Trojan/XPack.gen
ITW#64	Trojan.Win32.Vaklik.bop	WORM_ONLINEG.EWO	Trojan/XPack.gen
ITW#63	Trojan.Win32.Vaklik.bwc	WORM_TATERF.AF	Trojan/XPack.gen
ITW#606	Trojan-GameThief.Win32.OnLineGames.tob	WORM_LINEAGE.AZ	Trojan/XPack.gen
ITW#605	Trojan-PSW.Win32.OnLineGames.aptk	WORM_GAMMIMA.T	Trojan/XPack.gen
ITW#604	Trojan-GameThief.Win32.OnLineGames.sbo	Mal_NSAnti-1	Trojan/XPack.gen
ITW#602	Trojan-PSW.Win32.OnLineGames.ahvd	TSPY_ONLINEG.QYI	Trojan/XPack.gen
ITW#600	Trojan-GameThief.Win32.OnLineGames.sbwk	TROJ_GAMETHI.ER	Trojan/XPack.gen
ITW#597	Trojan.Win32.Vaklik.cms	TSPY_ONLINEG.PPX	Trojan/XPack.gen
ITW#596	Trojan.Win32.Vaklik.asm	WORM_ONLINEG.EWH	Trojan/XPack.gen
ITW#499	Worm.Win32.AutoRun.elj	WORM_AUTORUN.BEN	Trojan/XPack.gen
ITW#498	Worm.Win32.AutoRun.ekz	WORM_AUTORUN.AAF	Trojan/XPack.gen
ITW#487	Worm.Win32.AutoRun.dki	WORM_ONLINEG.EVW	Trojan/XPack.gen
ITW#442	Trojan-PSW.Win32.OnLineGames.adsy	WORM_AUTORUN.BZH	Trojan/XPack.gen
ITW#437	Trojan.Win32.Vaklik.ajx	WORM_ONLINEG.EWJ	Trojan/XPack.gen
ITW#361	Trojan-PSW.Win32.OnLineGames.acgu	WORM_ONLINEG.SYM	Trojan/XPack.gen
ITW#336	Trojan-GameThief.Win32.OnLineGames.zex	TSPY_ONLINEG.KTP	Trojan/XPack.gen
ITW#279	Trojan-GameThief.Win32.OnLineGames.ywy	TSPY_ONLINEG.MI	Trojan/XPack.gen
ITW#260	Worm.Win32.AutoRun.clb	WORM_ONLINEG.EVT	Trojan/XPack.gen
ITW#259	Trojan-GameThief.Win32.OnLineGames.zll	WORM_ONLINEG.SAY	Trojan/XPack.gen
ITW#253	Trojan-PSW.Win32.OnLineGames.acdy	TSPY_ONLINEG.IQR	Trojan/XPack.gen
ITW#243	Trojan-PSW.Win32.OnLineGames.acas	TSPY_ONLINEG.THF	Trojan/XPack.gen
ITW#167	Packed.Win32.PolyCrypt.h	WORM_ONLINEG.EWD	Trojan/XPack.gen
ITW#149	Trojan-GameThief.Win32.OnLineGames.ubg	WORM_ONLINEG.EWM	Trojan/XPack.gen

Malicious Sites Filtering Technology

Effective protection against malware infections requires multiple layers of defenses including deep content inspection and URL reputation filtering. As many malware infections occur from unfiltered web browsing, URL filtering can be used as a first line of defense to prevent infections by blocking user access or redirection to known malicious sites known to house and distribute malware. Anchiva's SWS provide two levels of URL reputation services: the RapidRx maintained Malicious Sites databases and integration with Google's Safe Browsing filtering library. Both databases can effectively prevent users from visiting websites that may be acting as Phishing websites or hacked and infected webpage that can automatically download and silently install malware on a user computer.

As with the threat database, the SWG can automatically update both the malicious sites and Google safe browsing databases based on recurring schedules that require no administrator intervention after initial configuration.

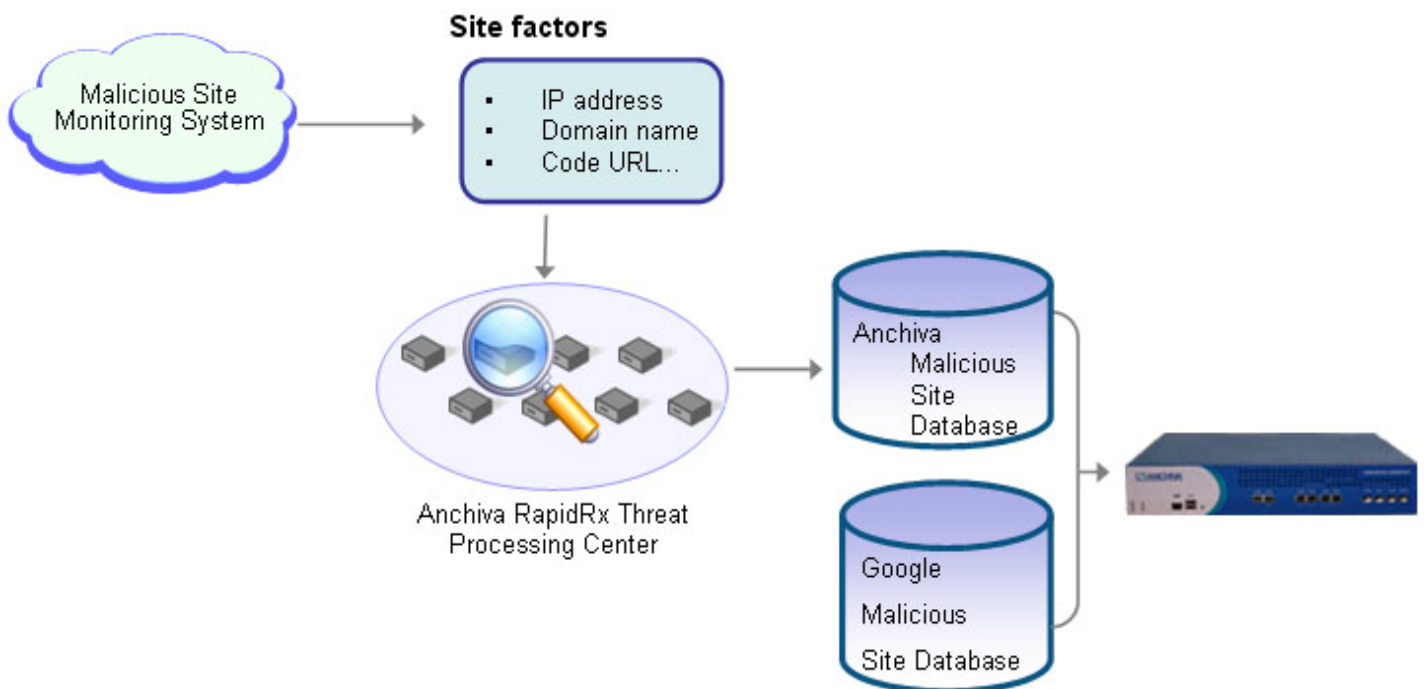


Fig4: Anchiva Malicious Sites Filtering Protection Architecture

Heuristic Behavior Association Analysis Technology

To detect yet unclassified and unidentified malware, a great deal of research and analysis on malicious programs has been conducted by Anchiva's malware experts. File characteristics studied include file structure analysis, source of origin, means of transmission and other embedded malicious routines. These characteristics were then used to develop Anchiva's heuristic analysis technology which uses multiple file scoring methods to determine if a file may or may not have malicious content with a very high level of accuracy.

Continuous tuning of the heuristic engine is performed by feeding in new samples received daily from customer sites and the honey pot network. With the users consent, the SWG can automatically flag and upload suspicious files to Anchiva's collection servers for further analysis. For files found to have malicious content a signature will automatically be generated and placed in the update file for download by the SWG systems in the field.

All the above process, including first heuristic checking of suspicious files, defining a malware and releasing signatures, can be done within two hours. This enables Anchiva's products the ability to provide in-time and forward zero-day protection of Internet application threats.

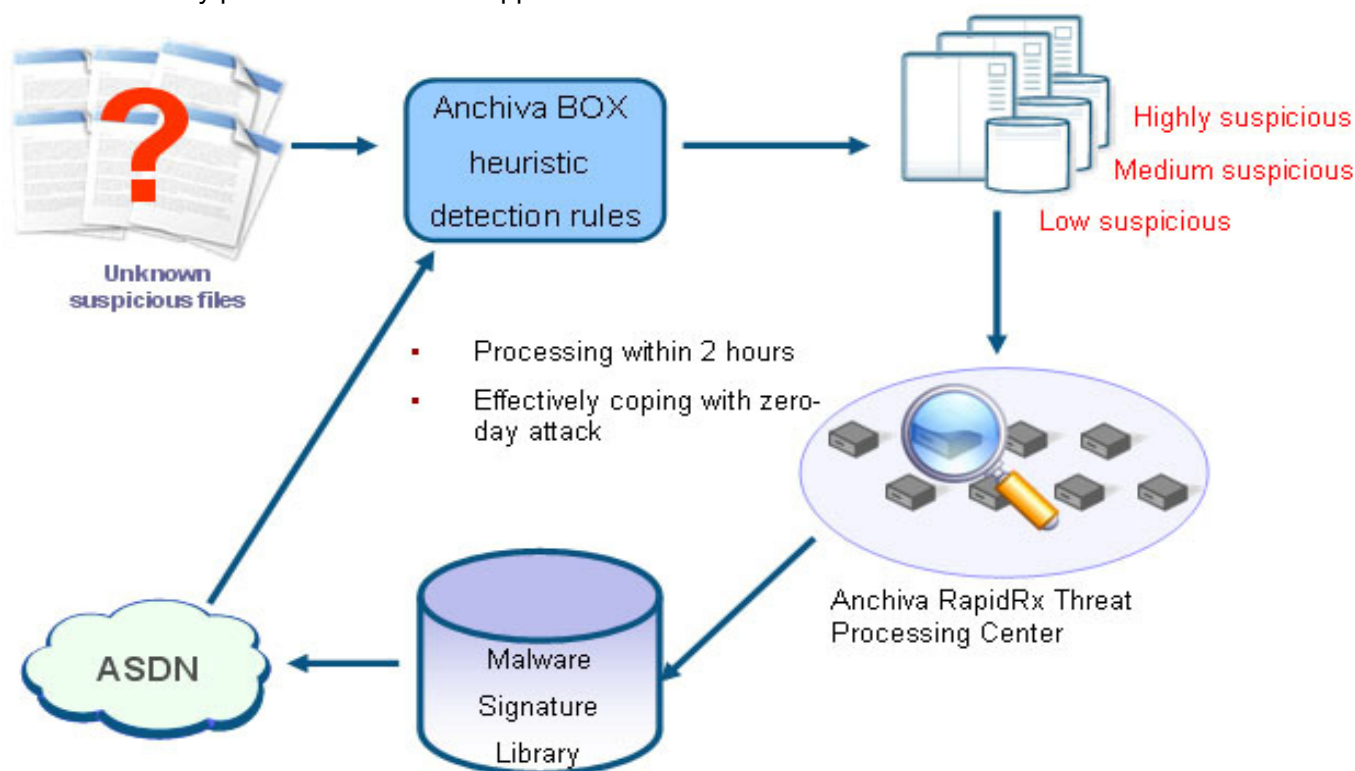


Fig5: Heuristic Behavior Association Analysis Technology

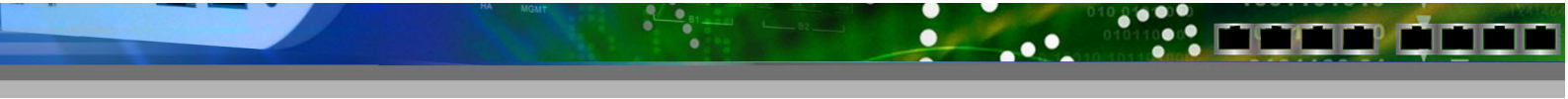
Web Server Protection

Hackers are targeting unsecured websites to plant and distribute their malware. In the past, hackers targeted smaller and little known domains that had very few daily visitors, resulting in only a small number of users becoming infected from the planted malware. Utilizing new attacks such as cross site scripting and SQL injections that allow hackers to exploit vulnerable web server code, hackers can now target the larger websites from the more popular domains, allowing the hackers to infect thousands if not millions of users daily with various types of malware.

To prevent these types of attacks and protect the brand reputation of the website owner, the SWG filters input from the clients, inspecting for malicious content such as cross site scripting and SQL injection exploit attempts, while HTTP POST uploads are also inspected for malware. To prevent interference of a websites service, the filtering process is ASIC accelerated to provide low latency processing.

Internet Application or Content Analysis and Control Technology

Non-approved application use in the workplace is greatly affecting employee productivity and draining internet bandwidth from critical applications such as VOIP, CRM and email. To enforce rouge application use, Anchiva's SWG provides controls to detect and block, log and/or bandwidth limit non-supported applications such as online gambling, stock trading, stream media applications and many others. The RapidRx team constantly adds new applications from customer requests and also from active monitoring of internet activities from Anchiva's trusted ISP and university partners who allow Anchiva's RapidRx teams to remotely monitor systems to collect valuable information.



Conclusion

Protecting against today's internet threats that are designed with cloaking and obfuscation routines to evade traditional firewall and intrusion prevention (IPS) systems requires a new approach. Anchiva's advanced Secure Web Gateways look at the traffic at the application layer, accurately identifying legitimate from malicious traffic, and allowing the use of business critical applications without interference and without the system becoming a network bottleneck.

All information referred in this document may be updated at any time, and Anchiva will not notify especially.
Copyright@2005-2009 Anchiva System Ltd. All rights reserved.
AnchivaOS and Anchiva are registered trademarks.
The names of actual companies and products mentioned herein may be the trademarks of their respective owners.