White Paper

Zero Hour Virus Outbreak Protection

A Key Layer in Complete Enterprise Email Security

Overview

Every enterprise has some form of anti-virus protection in place, yet malware penetration in the enterprise has become commonplace. Virus writers have identified the weak-point of traditional AV engines—the time it takes to develop protection for *new* viruses—and have exploited it to their advantage by flooding the Internet with thousands of new distinct virus variants simultaneously. These so-called server-side polymorphic viruses have caught enterprises unprotected, and can cause millions of dollars in damage and lost productivity.

This white paper introduces Commtouch Zero-Hour Virus Outbreak Protection (or Zero-Hour AV), an essential complement to traditional anti-virus protection, and now available as part of the Commtouch Enterprise Anti-Spam Gateway. Based on patented Recurrent Pattern Detection™ technology, Zero-Hour AV blocks hours and even days faster than traditional AV, closing the protection gap against new viruses and virus variants.

Email Under Siege

Email, one of the most important communication tools, is also the leading vector for viruses, accounting for 23% of all enterprise malware infections.[1] In fact, 84% of enterprise networks have been penetrated by email-borne viruses, worms or Trojans, according to Osterman Research.[2]

Securing email poses a particularly difficult challenge because allowing the free flow of messages is vital to business operations. Network administrators must balance between solid security and open flow of information, and costly compromises are commonplace. Most businesses cannot tolerate the risk that legitimate email will be misclassified as a virus and blocked. And yet, they are forced to take broad steps like blocking all executable files from entering the organization, because their AV solution is unable to recognize and block only the malicious attachments. This type of restrictive policy leads to blocking legitimate messages, or false positives, and frustration on the part of users.

Penetrations May Go Unnoticed at First

In the past, when virus-writers and virus-distributors were just “script kiddies” or hobby computer hackers seeking little more than notoriety amongst their peers, traditional anti-virus protection may have been sufficient. If a user became infected, it was obvious, since the computer disk might be formatted, or the virus would email itself out to the user’s contacts. The current reality is, however, that the majority of computer viruses today are virtually invisible to standard users. These stealthy malwares are designed to generate illicit revenue quietly for the malware underworld, without being detected. The potential for huge

profits has spurred the development of a more malicious breed of malware, capable of evading detection by common anti-virus solutions.

Most modern malware is designed to quietly go about its malicious activities without creating any noticeable symptoms. Keyloggers gather financial information and passwords; dialers can transmit sensitive information outside the organization; backdoors open up network connections for hackers to enter and send malware and spam directly from the enterprise network. All these activities are carried out in stealth-mode, without causing any noticeable interruption, allowing them to quietly continue their malicious activity.

Even more distressing is the fact that enterprises may believe themselves to be protected against these dangerous malwares. If IT managers go to the trouble of researching a particular virus on their AV provider's web site, they will likely come across dozens of entries of similar-sounding viruses against which the AV does in fact protect. However what they may not realize is that thousands of different variants with similar sounding names – each of which may require different protection capabilities – may be attacking their organization.

Traditional Anti-Virus: A Primer

In order to understand why traditional anti-virus cannot protect against today's malware, one must first understand how these conventional tools work. There are two basic technologies used in the established AV solutions: signatures and heuristics.

Signature-based anti-virus is the type we are most familiar with. As each new virus variant is identified, researchers at the AV company take the virus sample into their lab, pull apart the code, develop a signature or "scan-string" that identifies it, and then distribute that out to their users. This method has several drawbacks, among them that:

- Signatures are only good for known, identified viruses
- Signatures are typically only good for a single variant or small group of variants that shares a significant amount of code
- It takes time (a minimum of three hours, but it can often take days) to create and distribute signatures

The huge amount of time and effort involved in creating signatures has led some leading AV companies simply to ignore some threats, and not produce new signatures for them, even though the viruses themselves are reaching users' inboxes. As one leading AV company founder, Eugene Kaspersky remarked, "The anti-virus industry is slowly giving up because it is getting more and more difficult to resist the increasing number of the threats."[3]

Heuristic (rule-based) anti-virus engines were developed to partially automate AV defense and take a more pro-active approach to identifying unknown viruses. To create heuristics, AV labs still need to scan the virus code. However in this case, they are looking for virus-type commands in the code. They then build a series of rules based on each of the identified components; and incoming files are checked against these rules. The main benefit over signature-based AV is that heuristics can offer protection against some previously unknown viruses. However, several drawbacks remain. Heuristic AVs still:

- Take time to develop new heuristics, and distribute them to users
- Do not identify all virus variants

White Paper

So, just as in the famous fable "The Emperor's New Clothes," virus writers, AV vendors, and enterprise security managers may be satisfied, but in reality the traditional AV technologies are not able to adequately protect enterprises. AV vendors receive their quarterly seal of approval from testing labs, since the testing agencies use known "in the wild" viruses, and not the new unknown viruses which are the real threat today. Users do not necessarily notice that they are infected; they "feel" protected by signatures with the latest virus names without realizing that a single virus name may encompass tens of thousands of variants, against which the signature may not protect. And the bottom line is, of course, that the virus writers are able to continue carrying out their profitable attacks.

Today's Malware Evades Traditional AVs

At one point in time, traditional AV engines were effective, so let's examine how we reached the current situation. The earliest viruses were most often released in a single variant, in massive amounts. When a new virus was identified, IT managers could instruct their users not to open email messages with certain subjects or attachments. This was usually enough to protect users until the signature would come out a few hours or days later to protect against it.

Some early experimentation by virus writers showed that multiple virus variants could be used to evade signature-based anti-virus engines. A variant is a slightly altered version of malware code. While virus variants may perform basically the same malicious actions, the dissimilarity in the code fools signature-based AV engines that seek an exact match.

Based on the success of creating a handful of variants, virus-writers took the use of variants to the extreme and developed server-side polymorphic malware.[4] Server-side polymorphic malware refers to a technique of creating huge arsenals of slightly altered variants of malicious code and releasing them in quick bursts. The release of massive amounts of virus variants in just a few hours maximizes penetration by concentrating the outbreak into the brief period before signatures can be released.

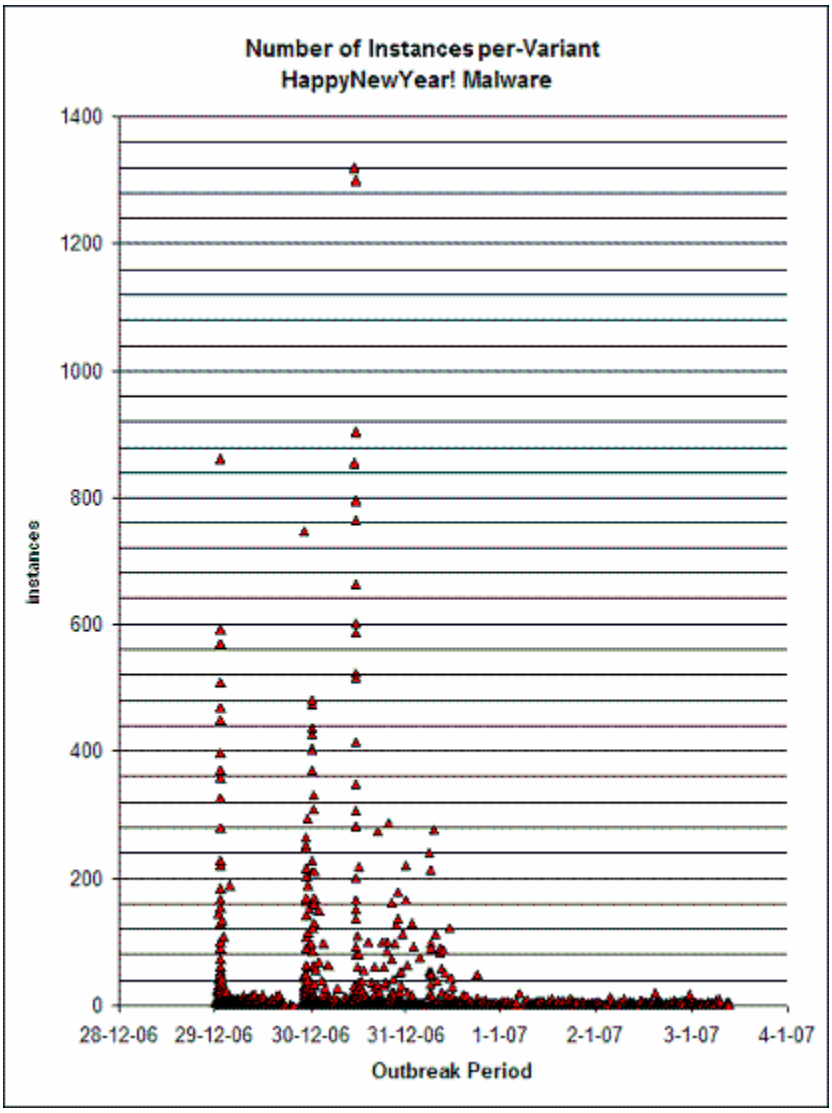
One early malware of this type was "Happy New Year," at the tail end of 2006/early 2007, followed closely by the Tibs/Zhelatin variants that appeared as the "Storm Worm," Valentine's Day greetings, various e-card scams, and so on. Even old-fashioned viruses like Bagle, more than three years old, which started out as a run-of-the-mill, single variant virus, is now a full-fledged server-side-polymorph, at times averaging over 600 new variants per day.

Even though AV vendors have improved their signature/heuristics delivery-time down to several hours in some cases, the newest viruses take advantage of those unprotected hours, and point all their ammunition to that vulnerability.

White Paper

White Paper

Server-Side Polymorphic Malware:
Hundreds of Overlapping Variants



Source: Commtouch Labs

Server-Side Polymorphic Malware Strategies

High velocity server-side polymorphic viruses use the following key strategies to bypass traditional AV defenses:

Vast Variant Quantity: These malwares distribute a vast number of variants; for example, Commtouch measured and blocked over 800 distinct "Happy New Year" variants in a single five-minute period. Storm-worm distributed over 7000 distinct variants on several days of that outbreak, and over 40,000 altogether during a 12-day period. Since each

variant or group of variants requires a different signature, it is impossible for anti-virus engines to keep up with this rapid-fire pace.

Brief Variant Lifetime: The fleeting lifetime of each variant is two to three hours on average, and each variant rarely makes a second appearance during the outbreak. Since it takes several hours to develop a new signature or heuristic, and up to several days to distribute to end-users, these short-lived variants are typically out of distribution by the time traditional anti-virus defenses are available.

Social Engineering: Multiple subject lines and attachment names are used, in order to confuse users; they can no longer be protected simply by avoiding email messages with known subjects or attachments. Topical subjects are designed to entice people to open the messages. For example, the "Storm-Worm" subject lines had a true irresistible tabloid quality to them.

Traditional Anti-Virus Engines Lag Behind the Zero Hour

The rapid release of virus variants, sometimes reaching a rate of hundreds per minute, takes advantage of the delay in traditional signature-based AV engines. A comparison put together using data from AV-Test.org shows that leading AV vendors release signatures hours, even days, after new virus variants have appeared across the Internet.

Variant MD5 checksum	Date & AV-Test.org ID	commtouch	CA eTrust	Kaspersky	McAfee	Microsoft	Panda	Sophos	Symantec	Trend Micro
7e9a27662faf6422a1ad83bf6429cf01	2007-06-25_21-04_0002			283:56						
dad26eeba40f0abdd060d266f8cc1ff7	2007-06-25_21-04_0002			8:55	115:48		118:56			32:31
29b9f1a1c38d2e78166767fef6c55cb1	2007-06-24_21-02_0004			39:17						
d571ad9595b1fb9e432f226c6b34fb37	2007-06-24_21-02_0004			38:00						
7b7b3354048d7bce3cc84fee669df442	2007-06-23_21-04_0002			12:15	65:04				64:51	53:37
a34568f365d143f14ac8b76525af342c	2007-06-22_12-46_0040			30:31			42:09			
266a6bf52fd2addc20af3a557d620bd5	2007-06-20_21-04_0004			22:17	74:51					
fb5a81f2fc80b470a61455e8a432c16a	2007-06-20_21-04_0004			50:31		15:03				71:29
96cd7cb47659e9c9b35ea2fc7831a196	2007-06-18_21-06_0001			99:34		45:50				89:48
629294802c709bffec3c72e2b478ddb6	2007-06-16_21-03_0001			3:27			138:30	42:22		26:22
168302a758121dfcbe883f9515b9ef08	2007-06-15_21-03_0002			21:18						
74c48d3a4fa68226de731d370d9978d5	2007-06-10_09-08_0005			40:13					48:55	34:47
27e1e3e4ebf000b9628cf445a4b71990	2007-06-10_09-08_0001			33:06		9:21				74:29
14f347f4c62e240dd74bf82c784ff885	2007-06-10_09-07_0002			13:02		8:57				
055a0a85900509700a94fce8831f5b23	2007-06-04_21-04_0002			8:57						

Zero-hour detection

Blocked some of the attack

No detection during analysis period

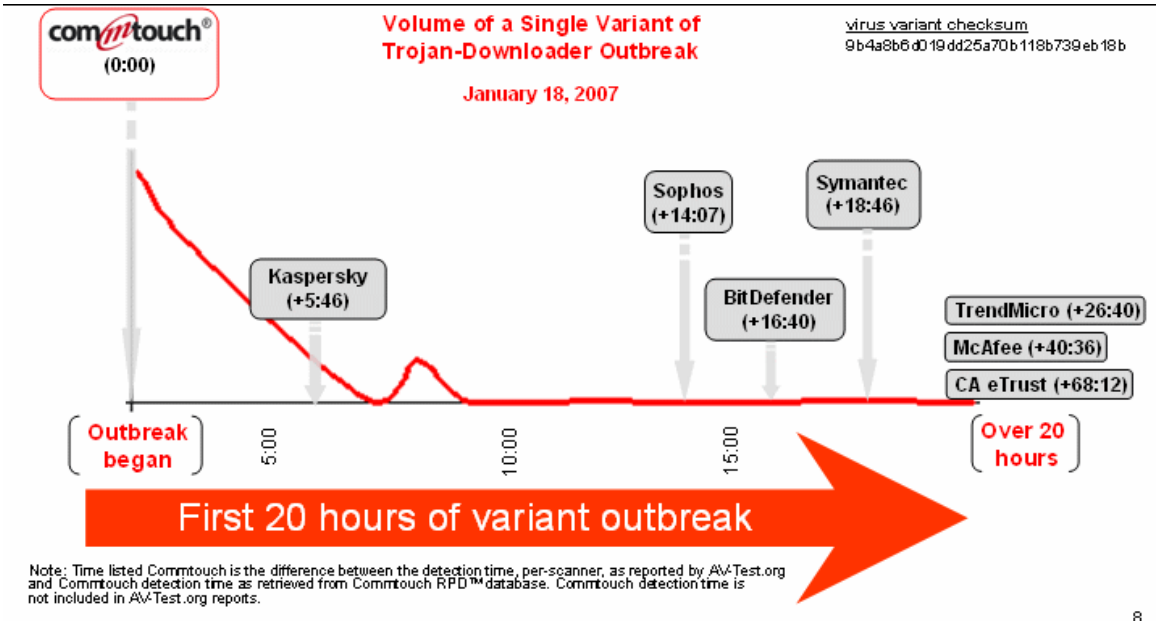
Note: Time listed is the difference between the detection time, per-scanner, as reported by AV-Test.org and Commtouch detection time as retrieved from Commtouch RPD™ database. Commtouch detection time is not included in AV-Test.org reports.

AV vendors are aware of their zero-hour vulnerability, and invest considerable efforts to release signatures and heuristics as quickly as they can. However, this approach depends on human analysis, and as such will always be subject to delays. Even the fastest AV engines leave customers exposed for several hours during the signature-update window.

Zero-Hour Virus Outbreak Protection

Commtouch Zero-Hour Virus Outbreak Protection takes a different approach to malware defense. Instead of focusing on hunting for new viruses and racing to catch them with a signature or heuristic, Commtouch monitors billions of messages each week across the globe, in order to identify and block new malware outbreaks the very moment they emerge. Based on patented Recurrent Pattern Detection (RPD™), Zero-Hour AV identifies and blocks email-borne malware in real-time, providing immediate protection against new variants, in the first critical hours of an outbreak.

Zero-Hour Comparison



Patent #6-330-590

As rapidly-changing malware techniques continue to develop, real-time virus outbreak detection has proven an effective defense against new outbreaks. Zero-Hour AV complements traditional AV solutions by adding an extra layer of Zero-Hour outbreak defense. Commtouch Enterprise Anti-Spam Gateway, now including Zero-Hour AV, delivers spam and virus outbreak protection, making Commtouch the complete email security solution for the enterprise.

White Paper

[1] *The 2007 Malware Report*, Computer Economics, p. 14

[2]Messaging Security Market Trends, 2006-2009, Osterman Research, p. 11

[3]SearchSecurity "SecurityWire Weekly, Episode 7, Eugene Kaspersky"

http://media.techtarget.com/searchSecurity/downloads/Security_Wire_Weekly_RSA_Kaspersky_02_08_2007.mp3

[4] Polymorphic malware is malware that self-mutates upon replication, thus making it more difficult for anti-virus engines to catch. *Server-side* polymorphic malware refers to the fact that the multiple variants are developed on the server-side, that is, before it is distributed to the targets.

White Paper