

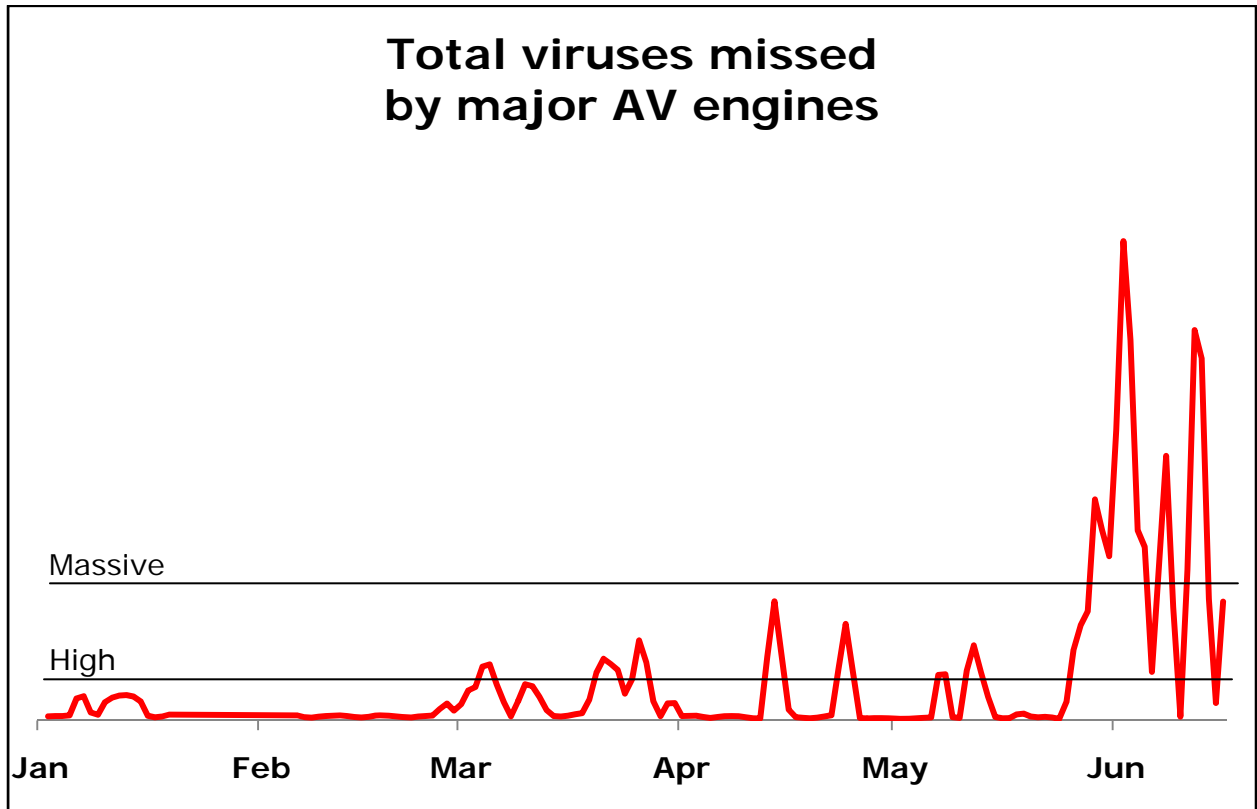


## Malware Outbreak Report

### June 2009

From late May through June, Commtouch Labs noted a sharp rise in the number of new viruses being circulated via email that were not caught by the major anti-virus engines. There were several malware outbreaks whose wide distribution caused malware numbers to temporarily and exponentially increase from the rather consistently low numbers we have seen during the past 18 months.

One explanation for the dramatic rise is the appearance of aggressive new variants of several different Trojans. With each new variant, there is a period of time during which anti-virus companies recognize it and then develop new signatures to protect their customers. The companies have tried blocking new variants with a dedicated signature per variant. This method proved inefficient, so security vendors have begun to develop generic signatures to block all variants of the same malware family. As demonstrated by this massive growth, the generic signatures have not proven to work against the recent variants.



Source: Commtouch Labs



## Top 10 Viruses Missed by Major AV engines: May 20 – June 29

	MD5 Checksum	Common Name
1	4be0d4b1dbc2d7ba92b6c920388ae4bb	Mal/WaledPak-A
2	fa5f6094f90a001d1fc742c7c036be7a	Mal/FakeVirPk-A
3	2c677cf98d1a4aa1f95ca456a6dfa18b	Troj/Agent-KBE
4	53d15dc652a2534572981bab1e2eddf3	Troj/Agent-JZY
5	c81ba436d85bba944adb74b86c90fae8	Mal/WaledPak-A
6	1396f9770b2702312c76987ca31e6866	Mal/WaledPak-A
7	7d06f4fc766b84faf02a91063946a96b	Mal/FakeVirPk-A
8	de90a24f3dfb5c1c8d4a0a3104f3dd4a	Mal/WaledPak-A
9	ad2b80463042d88056dc104c41e2a03e	Troj/Agent-KBJ
10	c17e6929f32dd05d718c83c2aae219bb	Troj/Dloadr-CMT

### Sample Viruses

Below is more detailed information about two of the Top 10 viruses – MD5 Checksum: c17e6929f32dd05d718c83c2aae219bb and MD5 Checksum: 2c677cf98d1a4aa1f95ca456a6dfa18b.

### MD Checksum: c17e6929f32dd05d718c83c2aae219bb

#### Sample Subject Lines

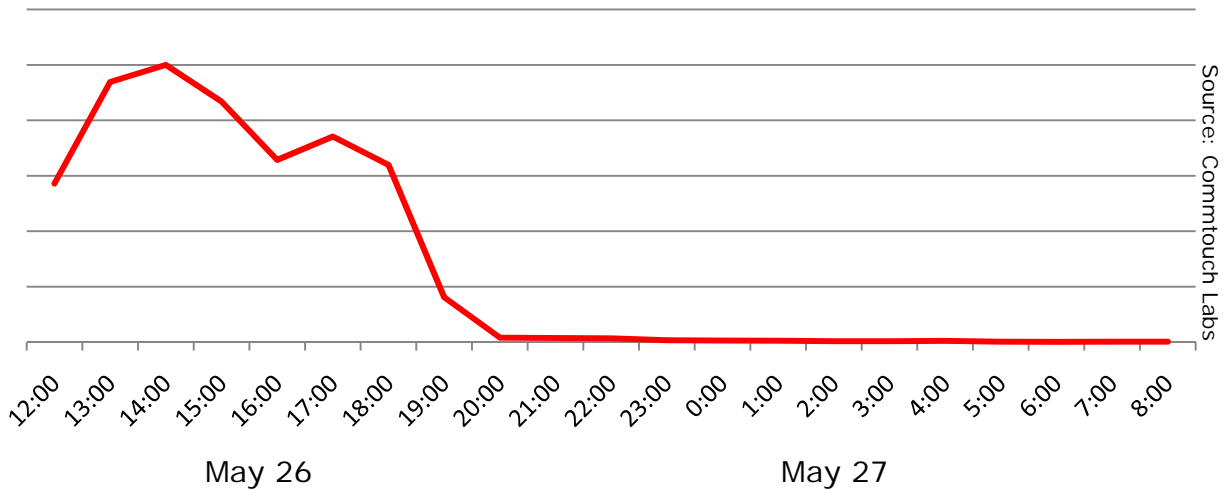
- see the transcript [failed(1)]
- past 4 hours
- delivery problems encountered
- please confirm your message
- email delivery error
- email policy violation
- western union transfer mtcn: 3475277661

#### Sample Executable File Names

- westernunion\_tr0002212.exe



**MD5 Checksum:  
c17e6929f32dd05d718c83c2aae219bb  
Lifespan**



**MD5 Checksum: 2c677cf98d1a4aa1f95ca456a6dfa18b**

Sample Subject Lines

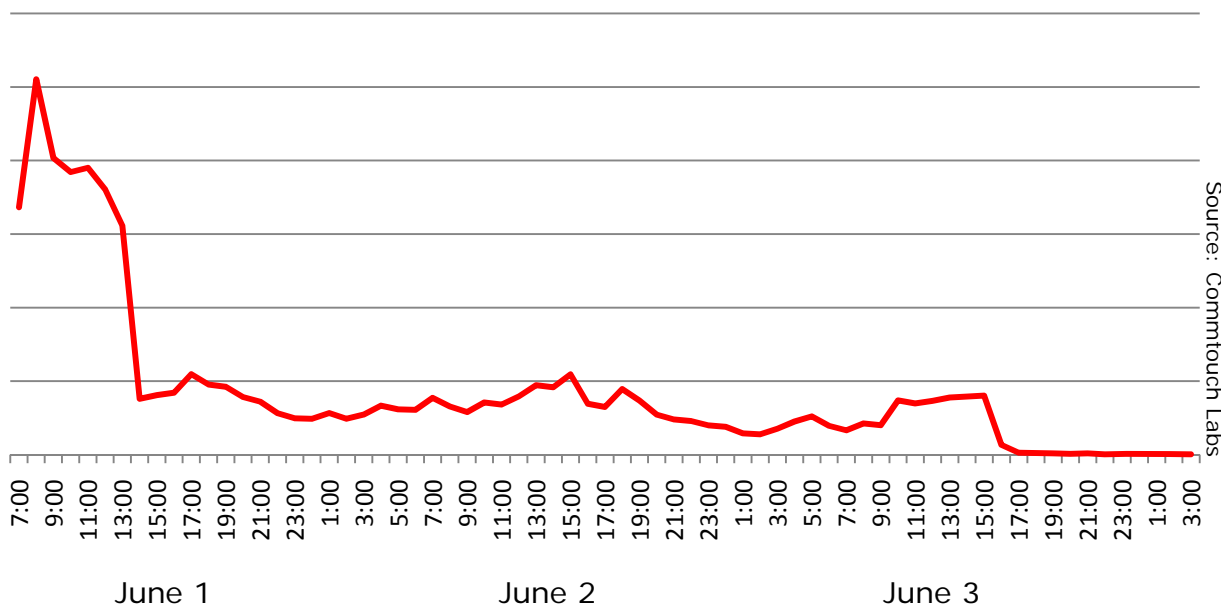
- apm-n de estado de entrega (error)
- past 4 hours
- delivery problems encountered
- tycqenk2yagqgnfl-(+wtgnjq-)
- uloqxnlayuuqgnfl- (+wflvw-)
- aok-tat de remise (+aok-chec)
- vdcy7a- +wmhq3a- +xuy5va-(+wuttka-)
- see the transcript [failed(1)]

Sample Executable File Names

- upsnr\_976120012.exe



**MD5 checksum:  
2c677cf98d1a4aa1f95ca456a6dfa18b  
Lifespan**



## Anti-Virus Engine Lag Time

### Methodology

Commtouch proactively scans vast amounts of email traffic circulating the Internet. Commtouch’s Recurrent Pattern Detection™-based detection engine analyzes the traffic as it is circulating and identifies massive virus outbreaks as soon as they emerge. The table below compares the Commtouch detection time to that of leading AV vendors, on average, for the two sample viruses detected by Commtouch at the time of publishing. These figures were calculated using AV engine detection times as reported by AV-Test.org and comparing them to detection times retrieved from the Commtouch RPD™ database.

### Definitions:

**Time difference from Commtouch:** The difference in signature release time per-AV engine, as reported by AV-Test.org, and Commtouch detection time as retrieved from the Commtouch RPD™ database.



**Zero-hour detection:** Indicates detection and blockage of the malware within the earliest moments of its outbreak.

**No detection during analysis period:** Indicates that the AV engine did not release a signature by the time this was posted to the web site; however it is possible that the AV engine released a signature after that time. Lately, most unique virus/malware attacks take place over the course of several hours, so a combination of pro-active Zero-Hour virus outbreak protection and traditional signature-based AV is the recommended defense.

### Virus Details:

Malware Characteristics		
MD5 checksum:	c17e6929f32dd05d718c83c2aae219bb	
Commtouch detect time [GMT]:	5/26/2009 12:17:00 PM	
Parent archive files(s):	westernunion_tr0002212.zip	
File name(s):	westernunion_tr0002212.exe	
Comparative Data		
This report generated 80.67 hrs. after Commtouch detect time		
Based on AV-Test.org Submission-ID: 2009-05-29_20-57_0001		<b>Time Difference From Commtouch</b> Source: Commtouch Software, Ltd.
Source: AV-Test.org		
AV Engine	Malware Name	
AVG	PSW.Generic7.JQF (Trojan horse)	10.52 hrs.
CA-AV	Win32/Bredolab.HW	20.70 hrs.
ClamAV	-	<b>No detection during analysis period</b>
Fortinet	PossibleThreat	14.03 hrs.
ISS VPS	-	<b>No detection during analysis period</b>
Kaspersky	Trojan.Win32.Agent.cjef	7.58 hrs.
McAfee	Spy-Agent.bw (trojan)	26.88 hrs.
Sophos	Troj/Dloadr-CMT	4.50 hrs.
Symantec	Trojan Horse	27.22 hrs.
Trend Micro	TROJ_BREDOLAB.BB	64.12 hrs.



Malware Characteristics		
MD5 checksum:	2c677cf98d1a4aa1f95ca456a6dfa18b	
Commtouch detect time [GMT]:	06-01-09 07:24	
Parent archive files(s):	upsnr_976120012.zip	
File name(s):	upsnr_976120012.exe	
Comparative Data		
This report generated 85.62 hrs. after Commtouch detect time		
Based on AV-Test.org Submission-ID: 2009-06-04_21-01_0002		<b>Time Difference From Commtouch</b> Source: Commtouch Software, Ltd.
Source: AV-Test.org		
AV Engine	Malware Name	
AVG	Pakes.DRC (Trojan horse)	13.08 hrs.
CA-AV	Win32/Donloz.OA	38.43 hrs.
ClamAV	Trojan.Agent-115743	3.87 hrs.
Fortinet	PossibleThreat	7.93 hrs.
ISS VPS	-	<b>No detection during analysis period</b>
Kaspersky	Trojan.Win32.Inject.accz	5.97 hrs.
McAfee	Spy-Agent.bw (trojan)	31.15 hrs.
Sophos	Troj/Agent-KBE	4.30 hrs.
Trend Micro	TSPY_ZBOT.AWF	21.13 hrs.

The data on these pages consists of samples of email-borne malware that Commtouch Zero Hour™ Virus Outbreak Protection solution, based on Recurrent Pattern Detection (RPD™) technology recently detected and blocked. The pages are updated approximately twice daily, and therefore are not intended to be a real-time alert service for new malware incidents. Data is often published after the outbreak has ended, in order to provide a comprehensive overview of the detection performance of Commtouch and other popular AV scanners. Data about other AV solutions is based on tests made by an independent third-party, AV-Test.org. Other Commtouch data, including comparisons with other AV scanners, is based on Commtouch Virus Outbreak Detection research labs.



## Commtouch Zero-Hour™ Virus Outbreak Protection: OEM Solution

Today's viruses, worms and Trojan downloaders target the primary weakness in anti-virus technology: the time it takes for new signatures or heuristics to be developed and distributed.

Commtouch Zero-Hour Virus Outbreak Protection provides a complementary shield to conventional AV technology, protecting in the earliest moments of malware outbreaks, and right through as each new variant emerges.

### About Commtouch

Commtouch® (NASDAQ: CTCH) provides proven messaging and Web security technology to more than 100 security companies and service providers for integration into their solutions. Commtouch's patented Recurrent Pattern Detection™ (RPD™) and GlobalView™ technologies are founded on a unique cloud-based approach, and work together in a comprehensive feedback loop to protect effectively in all languages and formats. Commtouch technology automatically analyzes billions of Internet transactions in real-time in its global data centers to identify new threats as they are initiated, protecting email infrastructures and enabling safe, compliant browsing. The company's expertise in building efficient, massive-scale security services has resulted in mitigating Internet threats for thousands of organizations and hundreds of millions of users in 190 countries. Commtouch was founded in 1991, is headquartered in Netanya, Israel, and has a subsidiary in Sunnyvale, Calif. Stay abreast of the latest messaging and Web threat trends all quarter long at the Commtouch Café: <http://blog.commtouch.com>. For more information about enhancing security offerings with Commtouch technology, see <http://www.commtouch.com> or write [info@commtouch.com](mailto:info@commtouch.com). Recurrent Pattern Detection, RPD, Zero-Hour and GlobalView are trademarks, and Commtouch is a registered trademark, of Commtouch Software Ltd. U.S. Patent No. 6,330,590 is owned by Commtouch.

### About Halon

About Halon Security Halon Security, headquartered in Gothenburg, Sweden, develops and manufactures IT security products with hardware firewalls as their specialty. Standard with each firewall is BSD, the market's safest operating system. Advanced functionality for antispam and antivirus, Quality of Service, the ability to schedule every services, hardware failure avoidance, and Internet provider switching enables Halon Security firewall users to get maximum IT security and performance. Today, Halon Security's firewalls are available in Europe, Asia, and the Americas. For more information go to: <http://www.halonsecurity.com>.

-----  
© Copyright 2009 Commtouch Software Ltd. All Rights Reserved. Recurrent Pattern Detection, RPD, Zero-Hour and GlobalView are trademarks, and Commtouch is a registered trademark, of Commtouch Software Ltd. U.S. Patent No. 6,330,590 is owned by Commtouch.