Security Spotlight
February 4, 2011

Security Spotlight articles discuss recent noteworthy threats that users may encounter and should be aware of while surfing the Web.

CYBERCRIMINALS SPREAD LOVE VIA ONLINE THREATS

Cybercriminals frequently leverage important events and special occasions for social engineering opportunities. As TrendLabs^{SM} has noted over the years, Valentine's Day is one of cybercriminals' favorite occasions to target for malicious profit. From spammed messages serving malware to compromised sites, users must remain cautious of security threats that purport to spread love but actually do harm.

Valentine's Day Means More Business for Cybercriminals

What do Christmas, New Year, Halloween, and Valentine's Day have in common? Apart from being some of the most celebrated occasions worldwide, these also present cybercriminals with a lot of opportunities to spread malware. Cybercriminals leverage these occasions in their social engineering tactics to lure users into their scams.

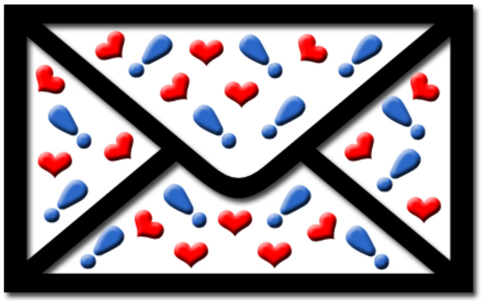
Valentine's Day presents a particularly lucrative opportunity for businesses. In fact, comScore found that February 2010 saw an increase in the number of consumer visits to dating, e-card, and gift sites in the United States. comScore noted that the number of visits to gift sites increased to 32.2 million while that to personal sites posted a 5 percent increase, reaching 24.2 million. E-card sites also became one of the top-ranking sites with a 7 percent increase in number of visits.

Valentine's Day is one of cybercriminals' favorite occasions to target for malicious profit. From spammed messages serving malware to compromised sites, users must remain cautious of security threats that purport to spread love but actually do harm.

Cybercriminals Love You

Given that special occasions are naturally lucrative for business, cybercriminals do not treat Valentine's Day as an exception. Valentine-themed spam and scams are just some of the attacks likely to plague users. These may lead to threats such as system infection as well as to information and financial theft.

Spam Entice Users



Spammed messages that offer special product discounts are already a staple in today's threat landscape. These become more effective, however, when tied to special occasions. Over the years, TrendLabs engineers have been coming across spam runs riding on Valentine's Day, including the following:

- Weeks before Valentine's Day 2009, TrendLabs engineers received a "dating spam" sample that claimed to come from Trend Micro. Upon analysis, we discovered that the message's *From* field has been tampered with. The spam was sent to random users. Responses to the message only served to validate the users' email addresses so they could be added to the spammers' future list of targets.

Please help us improve our reports by taking our quick survey.

- A few days after the above-mentioned incident, spammed messages supposedly from *Yahoo!* littered the Web. These contained links that looked like *Yahoo!* search results. Clicking the said links, however, led to sites that offered replica watches and other products at very low prices. A closer look revealed that the Web pages seemed to have been specifically created for the campaign using a single IP address.

- A few days after this second incident, TrendLabs engineers also received spam samples that posed as *iTunes Store* invoices. These also advertised a special Valentine's Day sale and had links that led to pharmaceutical sites. A similar campaign used jewelry instead of medicines/drugs and spoofed domains for the email addresses in the *From* field to evade detection.

- In February last year, a slew of spammed messages containing links that led to fake gift card promotional and replica watch advertising sites reached users' inboxes. Both campaigns leveraged the upcoming Valentine's Day to hook users to their malicious schemes.

- This year, days before Valentine's Day, TrendLabs engineers have already found spam samples that offer attractive flower delivery promos. The messages contain a link that leads users to a site that says the offer is no longer available. The spammed message contains "invisible" salad words that only turned up when the entire message is highlighted.

Spammers are not the only ones who prey on users on Valentine's Day. In fact, over the years, TrendLabs engineers have seen several malware variants target users on the lookout for Valentine gifts or e-cards.

Malware Hone in on Hearts' Day

Spammers are, however, not the only ones who prey on users on Valentine's Day. In fact, over the years, TrendLabs engineers have seen several malware variants target users on the lookout for Valentine gifts or e-cards.

One such worm detected by Trend Micro as WORM_BAGLE.EW spread via spammed messages bearing subjects like "Will you be my valentine?" and "Love you with all my heart!" These messages enticed users with romantic poems and Valentine-themed backgrounds in an effort to convince them to open a malicious attachment. Once executed, the worm deletes the registry keys of antivirus and security applications to evade detection. It also propagates via peer-to-peer (P2P) networks and downloads other files from several malicious sites.

The following are some of the other malware that we discovered in relation to Valentine's Day over the years:

Detection Name	Routine	Payload
VBS_VALENTIN.A	Modifies registry entries to make a specific URL the affected user's default *Internet Explorer (IE)* home page; sends out spam	Renames the affected user's files in the *C:* drive; attempts to send a copy of itself to other users via Internet Relay Chat (IRC) messaging systems
VBS_NUMGAME.A	Displays message prompts; drops copies of itself; deletes files and subfolders; deletes registry entries	Drops the file *GuessGame.bat*
TROJ_CUPIDCARD.A	Creates registry entries, files, and folders	
WORM_KIPIS.E	Gathers email addresses; creates registry entries; drops copies of itself onto specific folders	
WORM_NUWAR.AAI	Drops files onto specific folders; modifies registry entries to disable Internet Connection Sharing (ICS) and *Windows* Firewall; propagates via email messages; creates a mutex	Terminates processes related to antivirus and security programs

TrendLabs also saw an increase in the number of malware detected a week after Valentine's Day last year. The number of detections increased by 21 percent, which indicated that users were more susceptible to threats on this occasion.

TrendLabs saw an increase in the number of malware detected as week after Valentine's Day last year. The number of detections increased by 21 percent, which indicated that users were more susceptible to threats on this occasion.

WALEDAC Spreads Love

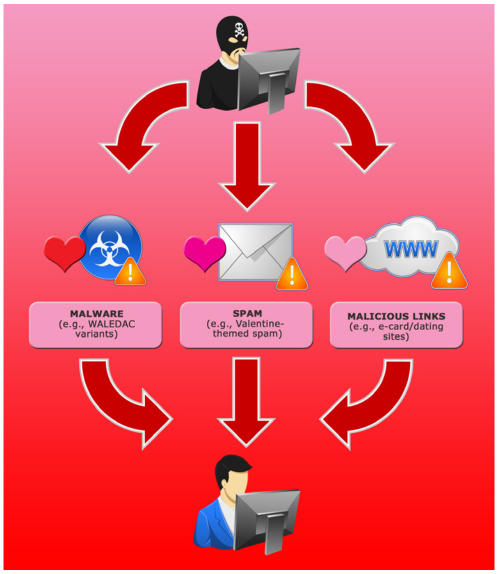
Possibly one of the most notorious malware that took advantage of Valentine's Day is WALEDAC. Primarily known for its spamming techniques, WALEDAC also acted as a means to introduce other malware variants to users' systems. Dubbed as the "new" Storm, WALEDAC used a similar technique and business model to Storm. However, it used an HTTP POST command-and-control (C&C) server, which was more common than Storm's Overnet P2P server, which made it more difficult for security researchers and analysts to track and block WALEDAC-related C&C traffic.

The following are some of the WALEDAC variants related to Valentine's Day that TrendLabs engineers discovered last year:

- Weeks before Valentine's Day, we found several spam samples that contained a link to a Valentine-themed site. When accessed, the user saw a prompt to download a file that Trend Micro detects as WORM_WALEDAC.AR. This worm gathers email addresses stored in the infected system. These addresses are then encrypted and stored in an .HTML or .PNG file, which is then sent to numerous IP addresses via HTTP POST.

- WORM_WALEDAC.BG was also discovered in relation to a slew of spammed messages that contained a link to another Valentine-themed site. Like the above-mentioned WALEDAC variant, this worm also gathers email addresses stored in the infected system and sends these to a remote user via HTTP POST.

Beware of "Love" Scammers


WWW
MALWARE (e.g., WALEDAC variants)
SPAM (e.g., Valentine-themed spam)
MALICIOUS LINKS (e.g., e-card/dating sites)

Apart from the usual concerns related to malware infection and spamming, "love" scammers also target dating/personal and social networking sites to part users from their hard-earned money. As such, the Federal Trade Commission (FTC) came up with a list of telltale signs indicating that the strangers you meet online may just be interested in your money. These signs include the following:

- Wanting to immediately leave the dating site and use personal email or instant-messaging (IM) accounts instead

- Claiming instant feelings of love

- Claiming to be from the United States but is currently overseas

- Planning to visit though unable to do so because of a tragic event

- Asking for money to pay for travel, visas or other travel documents, medication, a child or another relative's hospital bills, recovery from a temporary financial setback, or expenses incurred while waiting for a big business deal to come through

- Making multiple requests for more money

The telltale signs that indicate that the strangers you meet online may just be interested in your money include:

- Wanting to immediately leave the dating site and use personal email or instant-messaging (IM) accounts instead
- Claiming instant feelings of love
- Claiming to be from the United States but is currently overseas
- Planning to visit though unable to do so because of a tragic event
- Asking for money to pay for travel, visas or other travel documents, medication, a child or another relative's hospital bills, recovery from a temporary financial setback, or expenses incurred while waiting for a big business deal to come through
- Making multiple requests for more money

Spread Love, Not Malware

The above-mentioned attacks pose grave threats to users but can be easily avoided with proper vigilance and education. Since most Valentine-themed attacks arrive via spam, users should be cautious of opening email messages that offer huge discounts or that advertise unbelievable promos. As much as possible, shop online via legitimate vendors' sites.

To stay safe online, keep the following tips in mind:

- Review a site's terms and conditions before purchasing an item from it. Verify important details such as overall cost, shipping date, order cancellation, and return policies.
- Make sure to check out the seller's physical address and phone number in case processing or delivery problems arise.
- Use credit instead of debit cards, as most banks offer credit protection policies to limit financial losses should theft occur. Using debit cards may expose personal bank accounts to greater risk and may not have the same mitigation advantages as using credit cards.
- Never input personal information into a pop-up screen. Hackers can use these to intercept your online sessions. Legitimate sites do not use pop-up messages to request for personal information.
- Before entering credit card information, look for *https://* in the address bar, as this is an indicator of a secure session. Some sites also display a closed padlock or an unbroken key icon at the bottom-right corner of your browser.

For the best protection, install a security solution that prevents spam from even reaching your inbox, that blocks access to malicious sites, and that prevents the download and execution of malicious files. Such a measure prevents system infection from the start, resulting in a pleasurable online experience not just on Valentine's Day but on any special occasion or holiday.

References:

- Argie Gallego. (February 13, 2009). *TrendLabs Malware Blog.* "WALEDAC Spreads More Malware Love." http://blog.trendmicro.com/waledac-spreads-more-malware-love/ (Retrieved February 2011).
- Argie Gallego. (January 27, 2009). *TrendLabs Malware Blog.* "Just Got Unlucky: Part 3." http://blog.trendmicro.com/just-got-unlucky-part-3/ (Retrieved February 2011).

To stay safe online, keep the following tips in mind:

- Review a site's terms and conditions before purchasing an item from it.
- Make sure to check out the seller's physical address and phone number in case processing or delivery problems arise.
- Use credit instead of debit cards, as most banks offer credit protection policies to limit financial losses should theft occur.
- Never input personal information into a pop-up screen.
- Before entering credit card information, look for *https://* in the address bar, as this is an indicator of a secure session.

Please help us improve our reports by taking our quick survey.

- comScore, Inc. (March 19, 2010). *comScore.* “comScore Media Metrix Ranks Top-Growing Properties and Site Categories for February 2010.” http://www.comscore.com/Press_Events/Press_Releases/2010/3/comScore_Media_Metrix_Ranks_Top-Growing_Properties_and_Site_Categories_for_February_2010 (Retrieved February 2011).

- Cristina Buenviaje. (February 2, 2011). *TrendLabs Malware Blog.* “Valentine’s Day Spam Now Arriving.” http://blog.trendmicro.com/valentines-day-spam-now-arriving/ (Retrieved February 2011).

- Federal Trade Commission. (November 23, 2010). *Federal Trade Commission.* “FTC Warns Consumers About Online Dating Scams.” http://www.ftc.gov/opa/2010/11/onlinedating.shtm (Retrieved February 2011).

- Florabel Baetiong. (January 26, 2009). *TrendLabs Malware Blog.* “WALEDAC Loves (to Spam) You.” http://blog.trendmicro.com/waledac-loves-to-spam-you/ (Retrieved February 2011).

- Jonell Baltazar, Joey Costoya, and Ryan Flores. (June 2009). *TrendWatch.* “Infiltrating WALEDAC Botnet’s Covert Operations.” http://us.trendmicro.com/imperia/md/content/us/pdf/threats/securitylibrary/infiltrating_the_waledac_botnet_v2.pdf (Retrieved February 2011).

- Maria Alarcon. (February 2, 2010). *TrendLabs Malware Blog.* “Early Hearts’ Day Presents from Spammers.” http://blog.trendmicro.com/early-hearts-day-presents-from-spammers/ (Retrieved February 2011).

- Maria Alarcon. (February 6, 2009). *TrendLabs Malware Blog. “iTunes* Invoices and Valentine’s Ads Conceal Pharma Spam.” http://blog.trendmicro.com/itunes-invoices-and-valentines-ads-conceal-pharma-spam/ (Retrieved February 2011).

- Mary Ermitano. (January 25, 2009). *TrendLabs Malware Blog.* “‘Dating Spam’ Gone Wrong.” http://blog.trendmicro.com/dating-spam-gone-wrong/ (Retrieved February 2011).

- Robert McArdle. (January 17, 2008). *TrendLabs Malware Blog.* “P.S. I Love You.” http://blog.trendmicro.com/ps-i-love-you/ (Retrieved February 2011).

- Trend Micro, Incorporated. (2009). *Threat Encyclopedia.* “WORM_WALEDAC.AR.” http://about-threats.trendmicro.com/ArchiveMalware.aspx?language=us&name=WORM_WALEDAC.AR (Retrieved February 2011).

- Trend Micro, Incorporated. (2009). *Threat Encyclopedia.* “WORM_WALEDAC.BG.” http://about-threats.trendmicro.com/ArchiveMalware.aspx?language=us&name=WORM_WALEDAC.BG (Retrieved February 2011).

- Trend Micro, Incorporated. (2008). *Threat Encyclopedia.* “WORM_BAGLE.EW.” http://about-threats.trendmicro.com/ArchiveMalware.aspx?language=us&name=WORM_BAGLE.EW (Retrieved February 2011).

- Trend Micro, Incorporated. (2005). *Threat Encyclopedia.* "WORM_KIPIS.E." http://about-threats.trendmicro.com/ArchiveMalware.aspx?language=us&name=WORM_KIPIS.E (Retrieved February 2011).
- Trend Micro, Incorporated. (2003). *Threat Encyclopedia.* "TROJ_CUPIDCARD.A." http://about-threats.trendmicro.com/ArchiveMalware.aspx?language=us&name=TROJ_CUPIDCARD.A (Retrieved February 2011).
- Trend Micro, Incorporated. (2002). *Threat Encyclopedia.* "VBS_NUMGAME.A." http://about-threats.trendmicro.com/ArchiveMalware.aspx?language=us&name=VBS_NUMGAME.A (Retrieved February 2011).
- Trend Micro, Incorporated. (2001). *Threat Encyclopedia.* "VBS_VALENTIN.A." http://about-threats.trendmicro.com/ArchiveMalware.aspx?language=us&name=VBS_VALENTIN.A (Retrieved February 2011).
- United States Computer Emergency Readiness Team. (December 3, 2007). *US-CERT.* "Quarterly Trends and Analysis Report." http://www.us-cert.gov/press_room/trendsanalysisQ407.pdf (Retrieved February 2011).