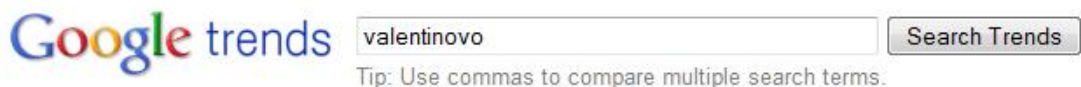




Previdni tudi na Valentinovo

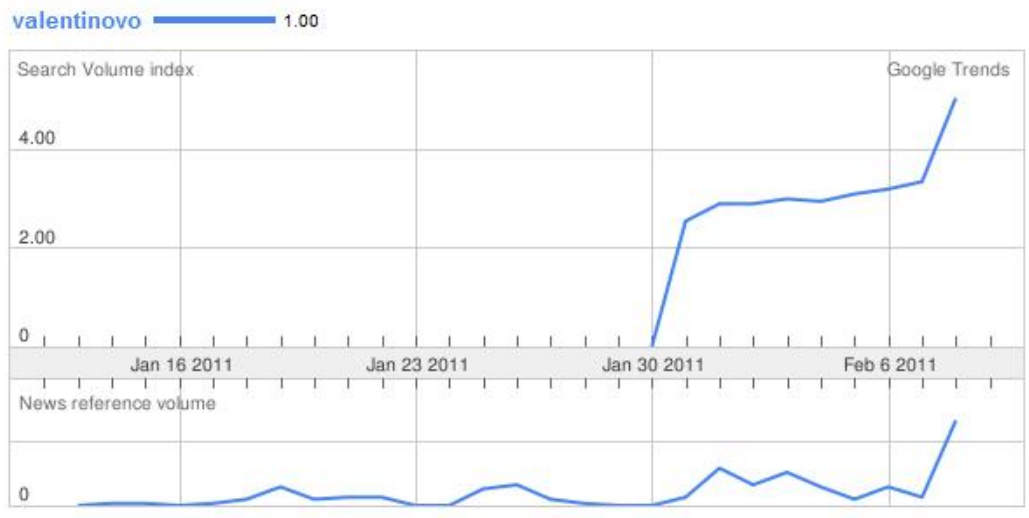
Čeprav je februar najkrajši mesec v letu, je, kar se širjenja in aktivnosti škodljive kode tiče, zelo aktiven. Eden od glavnih razlogov za to je Valentinovo, ki ga kiberkriminalci zaradi priljubljenosti po celem svetu s pridom izkoriščajo.

V preteklosti so kiberkriminalci svojo škodljivo kodo na Valentinovo širili predvsem s pomočjo elektronske pošte, danes pa se poslužujejo tudi naprednejših metod socialnega inženiringa na Facebooku, Twitterju in ostalih socialnih omrežij, s svojimi nevarnimi spletnimi stranmi pa se ob pomoči tehnik za optimizacijo v spletnih iskalnikih (SEO BlackHat) uvrščajo med prve zadetke pri iskanju vseh pojmov, ki so kakorkoli povezani z Valentinovim.



Searches Websites

Scale is based on the average traffic of **valentinovo** from Slovenia in the last 30 days. [Learn more](#)



Tudi v Sloveniji je Valentinovo od konca januarja vse pogostejši iskalni pojem.

Pet najpogostejših vzrokov za okužbo računalnika na Valentinovo:

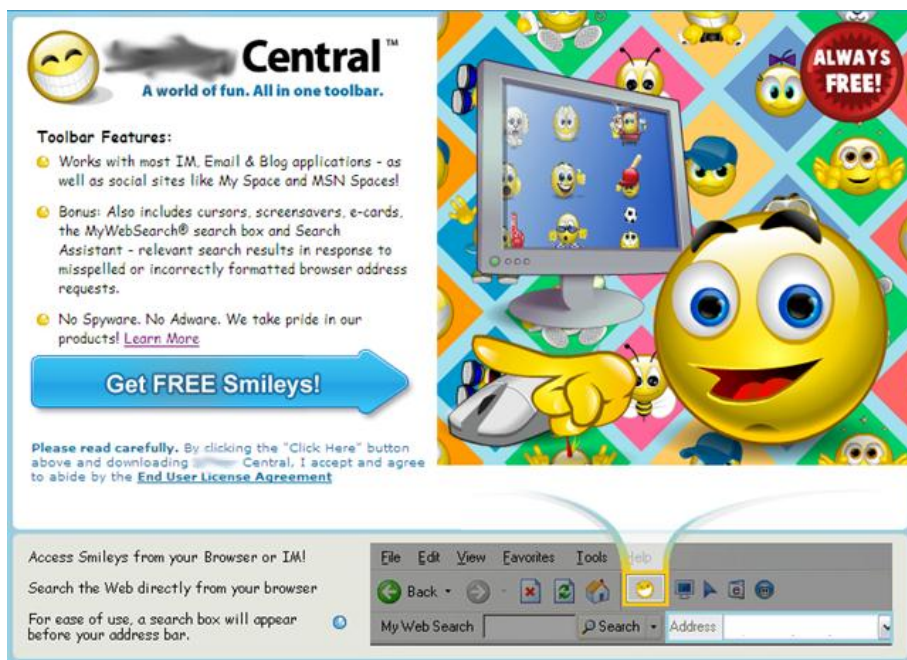
1. Socialna omrežja

Na prevare, ki izrabljajo Valentinovo še zdaleč niso odporna niti socialna omrežja. Spodaj je eden od primerov sporočila, ki se širijo v omrežju Twitter:



Sporočila pogosto oglašujejo brezplačne izdelke ali storitve, povezave v njih pa so skrajšane s pomočjo spletnih storitev Bit.ly ipd.

Uporabniki, ki kliknejo na povezavo v zgornjem sporočilu, so preusmerjeni na spletno stran, ki gostuje škodljive programe, v našem primeru gre za orodno vrstico (ESETovi protivirusni programi škodljivo datoteko prepoznajo kot oglaševalni programi):



Po kliku na povezavo v Twitter sporočilu je uporabnik preusmerjen na posebno podstran, ki so jo avtorji ustvarili posebej za Valentinovo:

Time	Type	URL
0.522	Redirect to: http://www.giveaway.org/gift-cards/celebrate-valentines-day-	http://bit.ly/frC...
1.199	text/html (NS_BINDING_ABORTED)	http://www.givea...
0.015	image/x-icon	http://www.givea...
0.961	text/html (NS_BINDING_ABORTED)	http://www.givea...
0.013	image/x-icon	http://www.givea...
4.163	Redirect to: http://x.azj.com/4bmRW	http://www.givea...
0.507	Redirect to: http://www.smiley.com/dl/index.html?spu=true&partner=.	http://x.azj.com/4b...
0.615	text/html	http://www.smileyce...
0.006	text/javascript	http://www.smileyce...
0.388	text/javascript	http://www.smileyce...
0.065	image/jpeg	http://ak.irgibson.co...
0.822	application/javascript	http://litem...

Po namestitvi orodne vrstice na žrtev računalnika se v registru operacijskega sistema Windows ustvari sedem novih zapisov v registru, poleg tega pa se v brskalniku Internet Explorer pojavi nova ikona, ki prikazuje oglasna sporočila:

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	MyWebSearch	MyWebSearch.com	c:\archivos de programa\mywebsearch\bar\1.bin\mwbar.dll
MyWebSearch	MyWebSearch Plugin Loader	MyWebSearch.com	c:\archivos de programa\mywebsearch\bar\1.bin\mwsoemon.exe
HKCU\Software\Microsoft\Windows\CurrentVersion\Run	MyWebSearch	MyWebSearch.com	c:\archivos de programa\mywebsearch\bar\1.bin\mwsoemon.exe
HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects	MyWebSearch	MyWebSearch.com	c:\archivos de programa\mywebsearch\bar\1.bin\mwbar.dll
MyWebSearch	MyWebSearch Search Assistant	MyWebSearch.com	c:\archivos de programa\mywebsearch\bar\1.bin\mwscas.dll
HKCU\Software\Microsoft\Internet Explorer\UriSearchHooks	MyWebSearch	MyWebSearch.com	c:\archivos de programa\mywebsearch\bar\1.bin\mwscas.dll
MyWebSearch	MyWebSearch Search Assistant	MyWebSearch.com	c:\archivos de programa\mywebsearch\bar\1.bin\mwscas.dll
HKLM\System\CurrentControlSet\Services	MyWebSearch	MyWebSearch.com	c:\archivos de programa\mywebsearch\bar\1.bin\mwsvc.exe

2. SEO BlackHat

Decembra smo lahko v najpriljubljenejšem spletnem iskalniku na temo Valentinovega zabeležili nekaj več kot milijon zadetkov, od takrat pa se je na spletu pojavilo še 600.000 novih spletnih strani, velik odstotek le-teh pa kiberkriminalci uporabljajo za širjenje svojih programov. S pomočjo tehnik za optimizacijo v spletnih iskalnikih (SEO BlackHat) se spletne strani kiberkriminalcev uvrščajo med prve zadetke pri iskanju vseh pojmov, ki so kakorkoli povezani z Valentinovim.



3. Lažne e-voščilnice

Elektronske voščilnice so na Valentinovo zelo priljubljene, česar se zavedajo tudi kiberkriminalci. V ta namen ustvarijo spletne strani s pomočjo katerih širijo svoje škodljive programe:



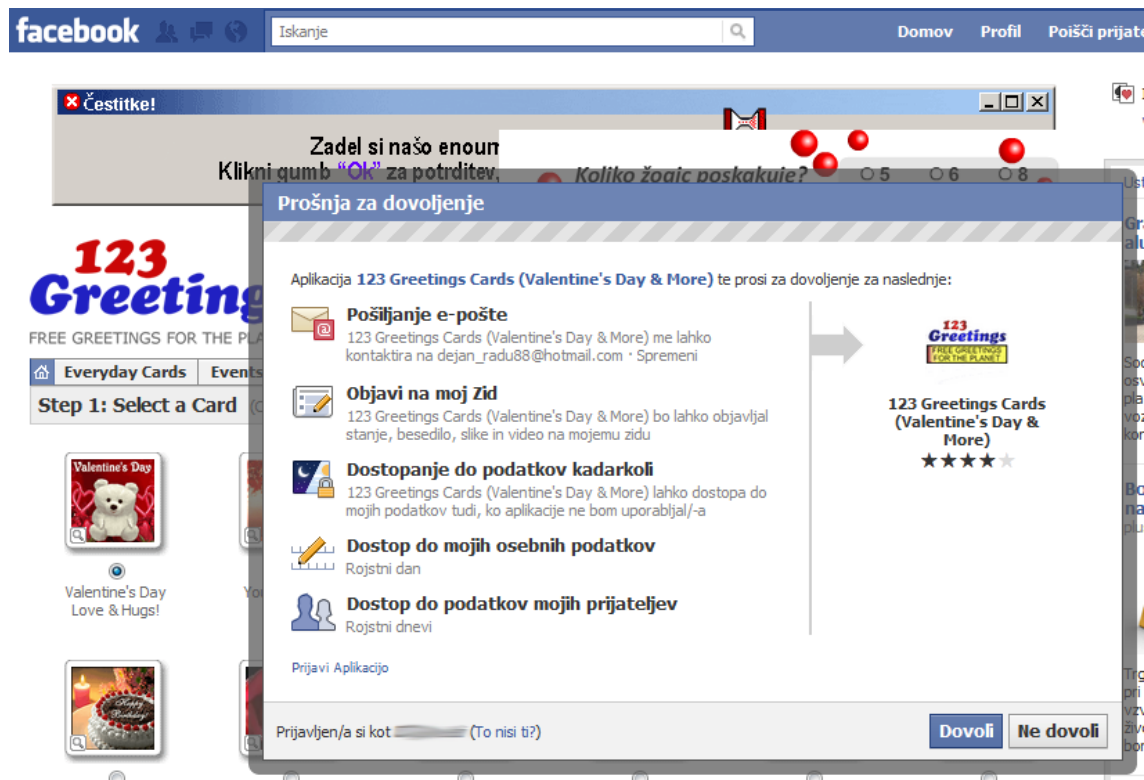
Klasična spletna stran z nevarnimi e-voščilnicami.



Kiberkriminalci obiskovalce, ki kliknejo na voščilnico 'obdarijo' z nevarnim programom.

4. Kraja osebnih podatkov

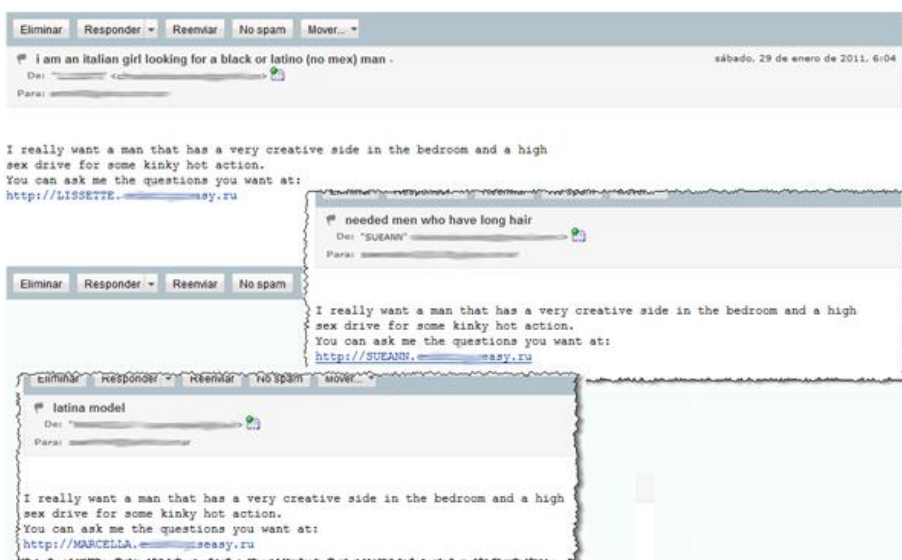
Navdušenje nad Valentinovim lahko izrabljajo tudi avtorji aplikacij v socialnih omrežjih (predvsem na Facebooku). Marsikateri uporabnik pri nameščanju takšnih aplikacij pozabi ali spregleda celo vrsto osebnih informacij, ki jih bo z avtorji delil po namestitvi.



Pred namestitvijo preverite katera dovoljenja aplikacija zahteva.

5. Lažne e-zmenkarije

Kiberkriminalci se zavedajo, da se na Valentinovo za zmenke na slepo pogosteje kot običajno dogovarjajo tudi samski. Pred Valentinovim se zaradi tega močno poveča količina neželene pošte na temo zmenkarij.



Gre za dobro znane prevare, ki največkrat izvirajo iz Rusije, avtorji pa z različnimi zvijačami od žrtev poskušajo pridobiti informacije, ki bi jih lahko kakorkoli zlorabili ali preprodali.

Nekaj nasvetov, kako se lahko izognete prevaram na Valentinovo:

- Ne odpirajte sporočil, ki vam jih pošljejo neznanci
- Izogibajte se odpiranju povezav in priponk v sporočilih
- Bodite pozorni na naslove sporočil, v kolikor vsebujejo besede Valentine's Day ipd., gre zelo verjetno za neželjeno sporočilo
- Prepričajte se, da na svojem računalniku uporabljate protivirusni program, ki ima tudi proaktivno zaščito in tako prepozna grožnje že takoj ob izbruhu
- Uporabljajte požarni zid, ki zna prepoznati nevarne prihodne in odhodne povezave iz vašega računalnika
- Posodablajte svoj operacijski sistem in vso ostalo programsko opremo