

## The Use of the Modern Social Web by Malicious Software

Lenny Zeltser

Senior Faculty Member, SANS Institute  
Incident Handler, Internet Storm Center  
<http://zeltser.com>

Malicious software thrives in the richness of the social web ecosystem, which incorporates mobile devices, reliable networks, powerful browsers and sociable users. Modern malware is programmed to take full advantage of these elements, which are especially potent in the context of social media and social networking websites. As the result, we're seeing malware exhibit the following characteristics:

- Using social networking sites to remotely direct malicious tools and attackers' actions
- Controlling social media site content to provide attackers with financial rewards
- Distributing links on websites with social capabilities to for autonomous malware propagation
- Defrauding participants of the social web by using chat bots and other techniques

Read this briefing to understand how malicious software makes use of these techniques to thrive on the social web and to offer lucrative benefits to malware authors and operators. Together, we can better understand such emerging threat vectors and devise defenses.

Social capabilities play a prominent role on the modern web ecosystem.



Social capabilities of modern websites and applications are changing how people communicate with each other and how businesses interact with customers. The social web incorporates sites that allow people to easily publish content and distribute public, private and semi-private messages. This includes traditional blogging platforms such as Blogger, micro blogs such as Tumblr, photo sharing sites such as Flickr and social networking sites such as Facebook.

We increasingly rely on the social web for both routine and crisis-related interactions. The attackers are also paying attention to this medium.

Malware takes advantage of social networking sites' capabilities and of the way that people use them.

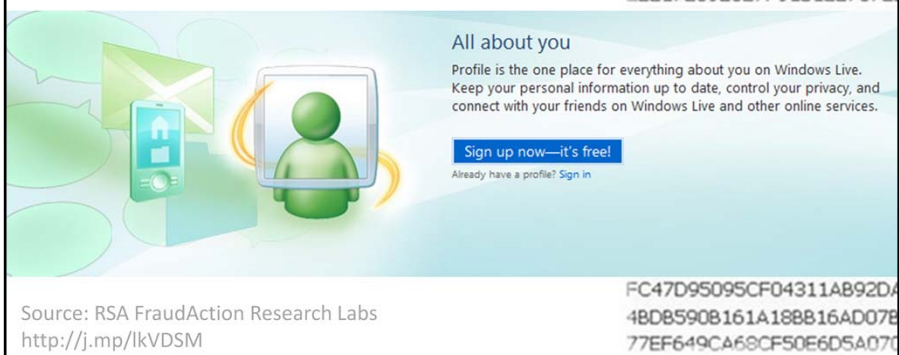


Authors and operators of malware are paying increasing attention to social media and social networking sites for conducting malicious activities. This isn't surprising. After all, such sites are designed to share information among friends, colleagues, and strangers looking for stories to read, pictures to admire, and videos to watch. Such sites are a powerful platform for spreading memes and holding conversations, both benign and malicious.

## Command and Control Through the Social Web

Let's begin our survey of how malware thrives on the social web by exploring how attackers have used social networking and similar sites for remotely controlling botnets.

## A banking trojan obtained instructions from a Windows Live profile.



The screenshot shows a Windows Live profile page for a user named "ana maria". The profile page includes a header with the name "ana maria wrote:" followed by a long alphanumeric string: "E1OWJJEFF7189829F9C8064C8389D37E8D67DE1E4AA088E488EC270DA73D30022DF589D768447C44CD05FB621852922217E89E027F9181EE767E". Below this is a section titled "All about you" with a description: "Profile is the one place for everything about you on Windows Live. Keep your personal information up to date, control your privacy, and connect with your friends on Windows Live and other online services." There are two buttons: "Sign up now—it's free!" and "Already have a profile? Sign in". The bottom of the page shows a source attribution: "Source: RSA FraudAction Research Labs http://j.mp/lkVDSM" and another long alphanumeric string: "FC47D95095CF04311A892DA48D85908161A188B16AD07B77EF649CA68CF50E6D5A070".

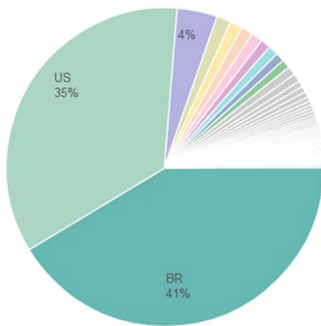
One example of a botnet making use of the social web was documented by RSA FraudAction Research Labs. The discovered a malicious program that used a profile displayed on the Windows Live website to obtain instructions from the attacker.

The attacker used the Windows Live profile named “ana maria” to publicly post encrypted content. Malware retrieved the profile’s contents, parsed and decrypted them, and used the results as its configuration file.

RSA observed that this method “allows the cybercriminal to issue encrypted commands without renting a dedicated, bulletproof server or registering a domain for the malware’s communication points.”

For additional details regarding this incident see: <http://blogs.rsa.com/rsafarl/cybercriminals-now-using-public-social-networks-to-give-command-and-control-orders-to-banking-trojans/>

## A botnet used Twitter, Jaiku and Tumblr to retrieve instructions.



Source: Jose Nazario, Arbor Networks  
<http://j.mp/kNe2xl>



Another incident that involved malware using the social web was documented by Jose Nazario from Arbor Networks. This bot was retrieving updates for a Twitter account “upd4t3” using the Twitter-generated RSS feed to obtain instructions from the botnet operator.

The use of Twitter allowed the attacker to control the botnet by merely posting encoded updates to the Twitter account, which could be done from a web browser or a mobile phone.

For more information regarding this malware see: <http://asert.arbornetworks.com/2009/08/twitter-based-botnet-command-channel/>

... the instructions on were base-64 encoded and pointed to malware.

```
aHR0cDovL2JpdC5seS9SN1NUViAgaHR0cDovL2JpdC5seS8yS29Ibw
```

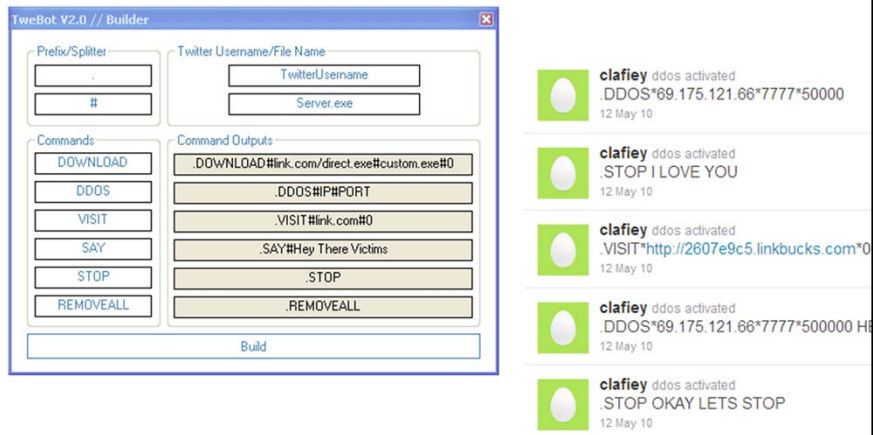


```
http: //bit.ly/ R6STV http:// bit.ly/ 2KoHo
```

The instructions distributed through Twitter for the botnet described on the previous page we encoded in base-65. If you decoded the text, you would see that it included URLs, such as the ones that you see on this slide.

The attacker appears to have used the popular URL shortening service Bitly for at least some of the link. This allowed both the attacker and malware researchers to see the statistics for how the URL was being accessed by the infected systems. In the case of one link, it was accessed 1,700 times. Also, according to Bitly's stats, the bots seemed to reside mostly in Brazil and USA.

## TwitterNET Builder made it easy to build a custom Twitter bot.



Another example of botnets that used Twitter for command and control (C&C) took the form of the TwitterNET Builder, which was a toolkit that allowed attackers to easily build custom bots. The bots had the ability to instruct the infected system to download and execute a program from a given URL, launch a distributed denial-of-service (DDoS) attack against the designated IP address, visit a specific URL (presumably for banner ad fraud), etc.

Each bot could be configured to keep an eye on the designated Twitter account to obtain instructions from the botnet operator.

The toolkit ran on Windows and provided the attacker with the ability to customize the bot before generating the malicious executable. The toolkit's user could customize the commands that the bots used, changing the default values such as "DOWNLOAD", "DDOS" and "VISIT".

The screenshot on the right side of this slide shows one such botnet being controlled by a Twitter account "clafiey".



## Torpig/Sinowal used Twitter trending topics for generating domain names of new attack sites.

**Current malicious domain**

**aghuvfcawe.com**

**Will be active soon**

**gfgytcggtwe.com  
oiajcmpotwe.com**

Source: Unmask Parasites Torpig  
Domain Generator <http://j.mp/lblggN>

In another example of the malicious use of the social web, the Torpig/Sinowal botnet possessed an algorithm for automatically generating new domain names where it would redirect victims for attacks. The bots relied Twitter API to obtain recent trending topics on Twitter, and used these topics as part of the seed for its pseudo-random name generator.

According to the Unmask Parasites blog, the bot requested trending topics from Twitter and then used “this information to generate a pseudo-random domain name of a currently active attack site on the fly.” It then injected a hidden iframe that attempted to load malware from that site.

For more details regarding this malware see:  
<http://blog.unmaskparasites.com/2009/12/09/twitter-api-still-attracts-hackers/>  
<http://www.cs.ucsb.edu/~seclab/projects/torpig>

C&C via social networking sites  
hides malware in plain sight.

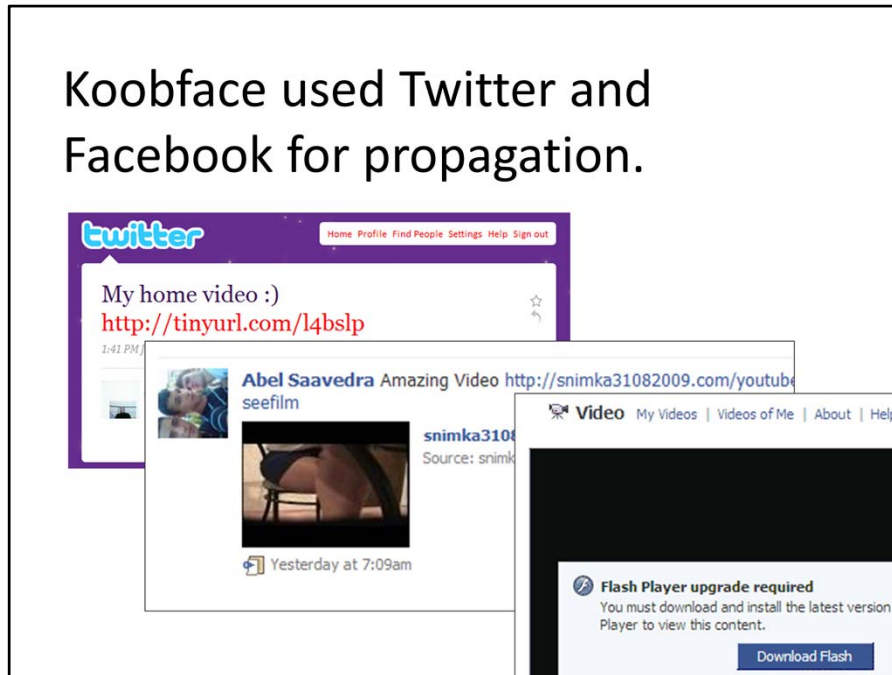


By using the social web for communicating with botnets, the authors and operators of malware are able to conceal their command-and-control traffic in plain sight. That's because such traffic mimics the routine activities in which computer users engage when they interact with websites. By using HTTP or HTTPS, which is plentiful on all networks, and by relying on the websites used by legitimate users, malware is often able to stay in touch with its operators undetected.

## Spreading Links Through Social Networks

Social networking websites are an attractive venue for spreading malicious links, because of the increasing amount of time people spend there. Moreover, these sites are becoming more effective for distributing links than email because of the relative sophistication of spam-fighting tools.

## Koobface used Twitter and Facebook for propagation.



Koobface is probably the best-known piece of malware that uses social networks, such as Facebook and Twitter, to propagate. When a person's system is infected with Koobface, the worm accesses the user social networking account and send a message to the victim's friends or followers with a link. When someone clicks the link, the person is directed to a website that attempts to infect the visitor with Koobface.

Koobface authors employ creative techniques to social-engineer people into clicking the link and to bypass security measures. For instance, Websense documented how Koobface might share a purposefully broken link to avoid Facebook's URL filters. In this scenario the attacker expects that the victim's desire to visit the destination will lead him to manually fix the link and paste the URL directly in the browser.

For more details on the Koobface use of purposefully broken URLs see:  
<http://community.websense.com/blogs/securitylabs/archive/2011/01/14/new-koobface-campaign-spreading-on-facebook.aspx>

## Another Facebook worm employed clickjacking to spread.

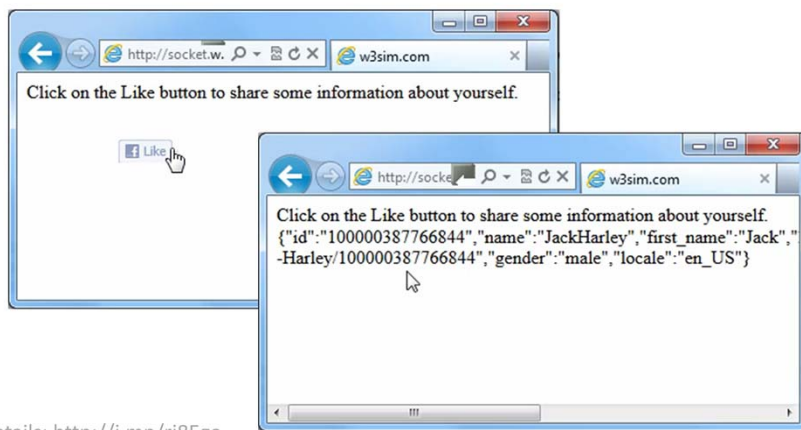


Clickjacking—the practice of deceptively directing a website visitor’s clicks to an undesired element of another site— has been surprisingly effective for propagating malicious links on Facebook.

In a classic clickjacking scenario, an attacker establishes a malicious website that invisibly embeds the Facebook Like or Share button in a transparent iframe. The iframe floats over a page element that the victim is likely to click on; alternatively, the invisible iframe follows the mouse cursor. When the victim clicks within the malicious site, the click is directed to the invisible Like or Share button.

In the example illustrated on this slide, the potential victim notices a link to an enticing video that has been shared by the person’s Facebook friend. Clicking the link brings the person to a website that appears to embed a video. However, the person doesn’t see the Like buttons that I captured on this screenshot. By attempting to play this video, the victim will actually press the Like button, increasing this site’s visibility on Facebook.

## Proof-of-concept code showed how to de-anonymize site visitors.



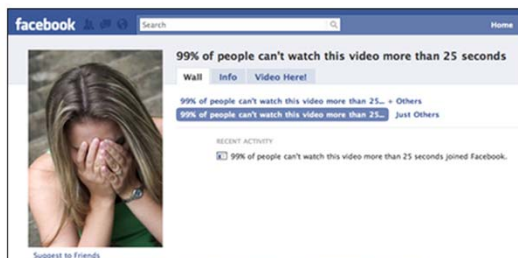
Details: <http://j.mp/rj8Ego>

In a paper *Clickjacking Attacks Unresolved*, Lin-Shung Huang and Collin Jackson document more insidious variations of clickjacking attacks. For instance, they provide a proof-of-concept demonstration how an attacker can determine the identity of the visitor to the malicious website by asking Facebook for this information.

The screenshot on this slide shows the Facebook Like button following the victim's mouse cursor; in a real attack, the button would be invisible. When the person inadvertently clicks the Like button, he or she becomes a fan of the attacker's Facebook page. Then, according to the researchers, "The attacker's web page is notified when the victim clicks on the Like button via `FB.Event.subscribe('edge.create', ...)`, triggering the attacker's server to pull the fan list from his Facebook page and identify the newly added fan. The attacker's server queries the user's public profile via Facebook Graph API, and then removes the user from the fan list."

For details about this threat vector see:  
[https://docs.google.com/document/pub?id=1hVcxPeCidZrM5acFH9ZoTYzg1D0VjkG3BDW\\_oUdn5qc](https://docs.google.com/document/pub?id=1hVcxPeCidZrM5acFH9ZoTYzg1D0VjkG3BDW_oUdn5qc)

## Another Facebook worm persuaded victims to copy-and-paste JavaScript.



Copy the code below, paste it into your browser's address bar and press enter to load this video..Plz wait 7-8 secs for processing!!!

Source: Roger Thompson, AVG  
<http://j.mp/pQDv9G>

In another example of malicious links spreading through Facebook, malware dared victims to click the link to get them hooked. It then asked the person to copy and paste JavaScript—this action hijacked the person's Facebook session and used it to spread this malware to the person's Facebook friends.

According to AVG's Roger Thompson, "you are taken to a page which automatically tells all your friends that you like the app, and it posts that link to your status."

As you can see, sometimes it is more effective to social-engineer the person to bypass the web browser's security by copying and pasting malicious code than attempt to exploit a technological vulnerability.

For more details regarding this incident see:  
<http://thompson.blog.avg.com/2010/07/remote-control-facebook.html>



Image source: Wikipedia, Portrait of René Descartes  
<http://j.mp/nNirPB>

Malware spreads with ease on social networks, because people frequently use them for sharing links to websites, articles, videos and stories that they like. Since the links are seen as being distributed by a friend, many people click on them.

We used to advise caution when opening email attachments. That wasn't very helpful advice, because people exchange email with strangers quite often. Moreover, attackers began sending malicious attachments from email accounts familiar to the recipient.

Similarly, people will continue clicking on links shared on social networking sites, even as we become increasingly aware of the risks. It's in our nature to be curious.

Perhaps if Descartes were alive today, he might proclaim: *Clicco ergo sum*—I click, therefore I am—rather than *Cogito ergo sum*—I think, therefore I am.



## Defrauding Social Network Participants

On-line scammers use various venues to social-engineer their victims into compliance. Email has been the most popular platform for such interactions. As people increasingly turn to social networking sites for their interactions, so do the scammers.

Scammers increasingly rely on the richness and popularity of the on-line social networks conduct fraudulent activities. They often employ malware, designed thrive in the social networking ecosystem, in support of these efforts.

## Fraudsters used Facebook chat for the “stuck in London” scam.



Source: Jason Cupp  
<http://j.mp/k9JFf9>

Attackers have been conducting the “stuck in London” scam for several years. Early campaigns were relying on compromised webmail accounts to reach potential victims through email. In an example recently documented by Rakesh Agrawal, this classic scam was conducted via Facebook chat.

The scammer used a compromised Facebook account in an attempt to solicit emergency funds from the victim’s friend. The screenshot on this slide shows an excerpt from the chat transcript.

With low-cost labor available throughout the world, scammers can employ humans for chatting with victims while keeping their costs relatively low. The scammer was using Matt’s Facebook account and, as far as I can tell, was a human being. However, such interactions could have easily been automated using a chat bot.

For details regarding this Facebook chat scam see: <http://rake.sh/blog/2009/01/20/facebook-fraud-a-transcript/>

## Some chats are automated via bots.

friend: hey  
victim: yo  
victim: brb  
friend: what ya up to  
victim: not much  
victim: i got minecraft!  
friend: you have to see this best buy is giving away giftcards still for a couple of days  
victim: i live in germany  
friend: if you hurry you can still get one i just signed up for mine its awesome look at this  
http: // bestuygiveaway. co. tv

Source: <http://j.mp/nMvWuJ>

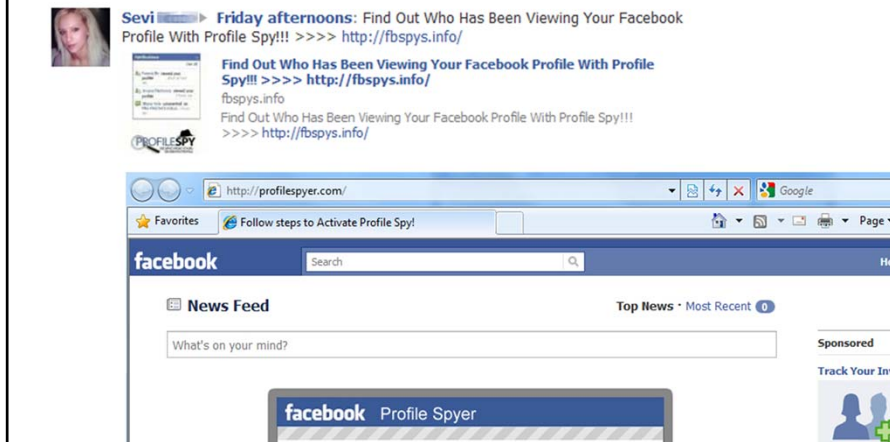
The idea of chat bots is an old one, dating back to early implementations of ELIZA. According to Wikipedia, its most famous implementation was DOCTOR, which simulated human-like interactions with a psychotherapist. A scammer could use similar software to automate the bot's chat interactions with victims.

For instance, a SANS Internet Storm Center reader reported receiving a Facebook chat message from a friend that started with "Hey [Name] you got a second?". When the person responded, the bot replied with "I can't score higher than 600 on the quiz, do you think you can?" and provided a link to a suspicious site.

Along these lines, this slide includes an example of an AOL Instant Messenger bot that is a bit more advanced in its chatting abilities. The bot seems to be using a compromised AOL Instant Messenger account of the victim's friend to social-engineer the person into visiting a fraudulent website.

For details regarding the Facebook chat example see <http://isc.sans.edu/diary.html?storyid=10039>

## Victims voluntarily spread links to the Profile Spyer app on Facebook.



Consider a scam that promises Facebook users to find out who has been viewing their Facebook profile. The implication is that the user can get access to these details (that feed the narcissist in all of us) by installing the Profile Spy application.

The scam attempts to trick the victim into revealing personal details, including a mobile phone number. The malicious site shows a fake Facebook page in the background, to make victims think they are within the “walled garden” of Facebook...



Under the promise of providing the magical Profile Spy application, the scammer’s website requests that the user click the Like button. This helps promote the Facebook page set up for the Profile Spy application, because the more people “liked” the page, the more legitimate it appears to future victims.

The site also requests that the person click the Share button. This shares the link to the Profile Spy website with the victim’s friends on Facebook.

Lastly, the person is asked to fill out some surveys that ask for contact information and other details to, presumably, sell that data to third parties. The promise of the Profile Spy application is never fulfilled, sorry.

For more perspectives on the Profile Spy scam see <http://blog.zeltser.com/post/1137736287/profile-spy-scams-on-facebook>

Social networks' participants can't avoid the social frame of mind.



Scams are propagating on social networking sites because the participants of such sites are in the social frame of mind. They are there to share links and interact with people with whom they might have only weak ties. In this environment, people cannot help but expose themselves to potential interactions with scammers and their tools.

Moreover, it's becoming less practical to social networking sites as standalone entities. Social media is getting infused into all interactions. The web as we knew it is ceasing to exist and is turning into the social web. As the result, the manner of online interactions combines many characteristics that until recently haven't coexisted in a single communication platform. These include:

- Instant one-to-one and group communications
- Hard-to-control channel (HTTP and HTTPS)
- Public archives of interactions
- Real-time and delayed conversations
- Video and audio, not just text
- Support for strong and weak relationships
- Accessible on the move (mobile)

## Using Malware to Control Content on the Social Web

People increasingly turn to social websites for consuming content, be it the use of a Facebook Connect plugin by CNN.com or the reliance on Twitter to determine which articles are worth reading. As the result, attackers have an incentive to find a way of controlling the popularity and distribution of content shared through or published on the social web. Malicious code can assist them in this quest.

“Import your created/hacked Twitter accounts and hit start, they will then follow your Twitter page which will give you more trust and will help you spread your server/virus with ease.”



One of the ways in which social media participants gain power for distributing content is by increasing their popularity, which is often linked to greater influence. This provides an incentive to inflate the number of people who pay attention the person’s social media presence. For instance, attackers have been known to obtain logon credentials of Twitter accounts—either by purchasing such credentials or by obtaining them through phishing campaigns. The attackers then direct the compromised accounts to follow the attacker’s Twitter account, thereby increasing the attacker’s popularity.

This slide presents a screenshot of a tool that aims at assisting attackers with this process. It allows the scammer to import a list of compromised Twitter credentials, and will then automatically direct these accounts to follow the designated account to “create an army of 1000’s of followers!”



## Bots on LiveJournal tricked victims into befriending them.

nov 12th: [ptiknui](#), [vhahtroeautosau](#), [vandewouwaufqtu](#), [porfiriogarry](#), [gewwalfib](#)  
nov 5th: [mcluskie3mahh2](#), [samijmodnyj](#), [pwifwe](#), [abramsuvulotomy](#), [pinnaehrosbe](#), [t](#)  
oct 24th: [vloneuhowwily0](#), [heintzitemitran](#), [cvazasrefofarre](#), [plusninety](#)  
oct 19th: [alisa69sex](#), [patehescoors](#)  
oct 17: found and reported 2211 more. (grand total found: 9089!)  
17: [marissa\\_jacobs](#), [brinybergeron](#), [orlyhisko](#), [chiyin\\_pilip](#)  
15: [cordeliesandifo](#), [billzisu](#), [jaclyn\\_mcallist](#), [stephan\\_lockard](#), [lisha\\_bezdel](#), [ran](#)  
[bunnypic](#), [maribelle\\_nou](#), [randie\\_kirady](#), [ynezboulais](#), [birmingham\\_clif](#), [mista\\_4](#),   
[mista\\_5](#), [mista\\_6](#), [mista\\_7](#), [mista\\_8](#), [mista\\_9](#), [mista\\_10](#), [mista\\_11](#), [mista\\_12](#), [r](#)  
[mista\\_16](#), [mista\\_17](#), [mista\\_18](#), [mista\\_19](#), [mista\\_20](#), [mista\\_24](#), [mista\\_22](#), [mista\\_23](#)  
14: [eblancheg](#)  
13: [jeffery\\_lawther](#), [isabell\\_oslund](#), [jamaha](#), [wallacestasyszy](#), [ivan\\_kochis](#), [bonnie\\_stins](#)

Listing source: nympholept  
<http://j.mp/iL5LhW>

In another example of malware preparing to control social media content, Irene Michlin at Sophos provided an insightful look into automated bot activities on LiveJournal—a site especially popular in the Russian-speaking community—which includes blogging and social networking features. Irine describes the complicated logic built into LiveJournal bots for spreading spam content on the site.

These bots strive to appear to be full participants of the social network, building up friendships and reputation so that the spam comments and blog postings they create are seen by a wide audience. For details see <http://nakedsecurity.sophos.com/2010/11/15/bots-on-livejournal-explored/>

One LiveJournal user attempted to keep track of the accounts associated with bots on the site. The list, captured partially on this site, resides at: <http://writingbots.javaprogramming4u.info/making-livejournal-friends-on-autopilot-with-htmlunit-and-ljtoolkit/>

## Bots with many friends grow in LJ content-distribution power.



### ▼ Basic Info

Name: ylehinahina  
Birthdate: 03-18

### ▼ Bio

Я Русалочка...Не диснеевская , а та самая из сказки ГансаХристиана Андерсона , она совсем про меня...br br br br Сейчас , заполучив ноги взамен на 280 лет получить человеческую душу и чувствую себя очень одиноко в мире людей...

### ▼ Friends [View Entries]

#### ▼ Friends (64):

\_\_magnus\_\_, \_nqlbak\_fan\_, agent\_omally, aimeegonzo, alawi77, alisnazz, ameretto\_sour, ashleyxd, asriel16, aux\_et  
aznherbalkandy, blue\_\_\_angel, candiedapple73, christmasgirl09, craziaspccachic, crazyblondie094, daria090, dark\_he  
darkcinderella, darksf3ar, dimen03, doublepatch, elevin, ericahock, esli7223, evildjinn, feangolfean, flame\_avator,  
gabbiluvzgerard, gduquette, grimsarcat, grthebear, hacker\_rob, hattnickhero, ilovekristin709, kennyknox, lanitochka,  
lilbitch\_8703, malaki\_101, mermaidecho, mikemartin\_ifs, minamurray666, mishi782, mustbethistall, mybookclub,  
phoenixfirebird, pinkdolly777, ppaspaseln, prolapsusofsoul, quack13, r0ssi12, so\_dolly, soccergurl1467, softyslowly,  
stephybabii04, thelostone3, thuglove, twyzted75, vancemichael, vayn\_glory, waxroses, x\_nebel\_x, xkimxviolencex,  
yellowchicklet

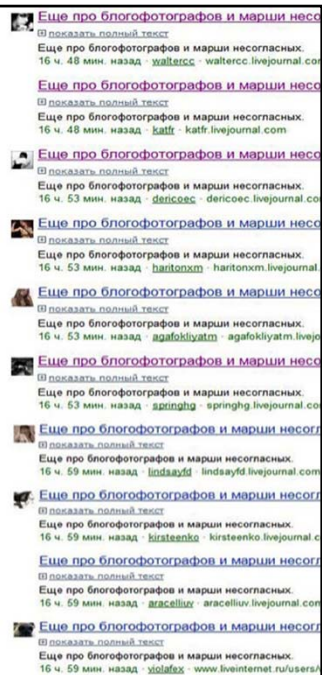
#### ▼ Friend of (9):

elevin, feangolfean, gisoymio, lanitochka, softyslowly, umtipa, vancemichael, vzgnvvey, xkimxviolencex

LiveJournal bots attempt to build up their LiveJournal profiles to make it hard for comment moderators to distinguish the bot from a human user. This involves building fake friendships. According to Irene Michlin, “bot control programs recognise which accounts are more promising in improving their reputation.” The bots can also mimic other users’ interests by copying features of their profiles into their own profiles.

Distinguishing between bots and human users can be hard. For instance, this slide presents a screenshot of a LiveJournal profile that I think belongs to a bot, but I’m not sure. One indicator that this might be a bot is based on the discrepancy between the profile’s photograph—representing a serious-looking male—and the bio that describes the person as a lonely mermaid from a fairytale. Though this might be a description of a real person, I found it strange that the same exact bio is used for several LiveJournal user profile that incorporated other indicators suggesting that they might be bots.

## LiveJournal bots drowned out political discussion with noise.



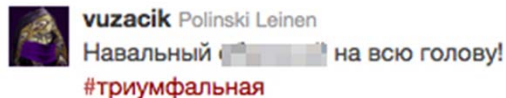
Source: Irene Michlin, Sophos  
<http://j.mp/joG98B>

Irene Michlin continued her discussion of malicious activities on LiveJournal by describing how bots drown out political discussion with spam and porn. In this example, bots appeared to seek out political content related to the controversial trial of Mikhail Khodorkovsky in Belarus.

Malware was programmed to overwhelm such “undesirable” posts with numerous spam comments, making it harder for humans to participate in discussions related to the attacked post. Irene noted that “people might be deterred from opening such posts, fearful that they will be caught accessing pornographic content.” The bots also replicated some aspects of the attacked post in an attempt to pollute search results.

For details regarding this incident see <http://nakedsecurity.sophos.com/2011/01/12/livejournal-bots-drown-out-political-discussion-spam-porn/>

## Twitter bots drowned out anti-Kremlin tweets.



Source: Maxim Goncharov, TrendLabs  
<http://j.mp/GPMIzH>

Another similar situation arose on Twitter during December 2012 anti-Kremlin protests in Russia. TrendLabs' Maxim Goncharov reported Twitter bots posting "range of national slogans and crude language. With a rate of up to 10 messages per second, these bots succeeded in blocking the actual message feed with that hashtag." (See <http://blog.trendmicro.com/the-dark-side-of-social-media>)

Brian Krebs described additional Twitter bots activities around the same time frame and used for the same purpose. According to Brian, 2,000 Twitter accounts that seemed to belong to these bots were mostly "created at the beginning of July 2011, and have very few tweets other than those meant to counter the protesters, or to simply fill the hashtag feeds with meaningless garbage. Some of the bot messages include completely unrelated hashtags or keywords, seemingly to pollute the news stream for the protester hashtags." (See <http://krebsonsecurity.com/2011/12/twitter-bots-drown-out-anti-kremlin-tweets/>)

Online social media will play an increasingly critical role in our lives.

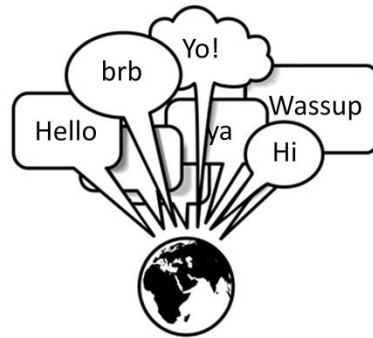


Online social media will play an increasingly important role in our lives, providing incentives for attackers to find a way to control the content on the social web to their advantage, be it to conduct blackhat Search Engine Optimization (SEO), to propagate scams, drown out legitimate conversations or pursue political goals. Malware can provide the automation necessary to conduct such activities on a large scale.

## Wrapping It Up

In these pages, I attempted to provide concrete examples of how scammers and other categories of attackers have used malware in the context of social media and social networking sites. My hope was to avoid presenting theoretical risks that make us worried about the use of the social web, so that we can make decisions based on facts, rather than theoretical possibilities and conjecture.

“Social” is the future of people’s online interactions. It’s the future of online criminal activities, too.



Given the way we’re embracing social features of websites and applications, it’s easy to envision the world where such interactions become essential to our daily lives. Since “social” appears to be a dominant trait of our web-based activities, criminals are likely to pay increasing attention to the social web.

Understand the threats to devise practical and relevant defenses.



Our use of the social web is evolving at a rapid pace. Yet, we're only now starting to understand the potential of social media and social networking sites. Similarly, we're only now starting to understand the likely threats that we may be exposed to through this medium. There's much we need to learn to understand the form that attacks are likely to take place on the social web. Similarly, much work remains to be done to find practical and relevant defenses against such threats. My hope is that surveying the current landscape of "social" malware can propel such discussions.



**Lenny Zeltser**

blog.zeltser.com

twitter.com/lennyzeltser

If you have any questions, comments or recommendations regarding this document, please get in touch with me! You can find me on Twitter at <http://twitter.com/lennyzeltser>. I also maintain a security-focused blog at <http://blog.zeltser.com>.

**Disclaimer:**

The views herein are those of the author and do not reflect any official opinion or position of the author's employer.

**About The Author:**

Lenny Zeltser is a seasoned information security professional with strong business background, most recently focusing on malware threats, incident response and cloud infrastructure security. He is a board of directors member at SANS Technology Institute, a SANS faculty member, and an incident handler at the Internet Storm Center.

Lenny frequently speaks on information security and related business topics at conferences and private events, writes articles, and has co-authored several books.

Lenny is one of the few individuals in the world who have earned the highly-regarded GIAC Security Expert (GSE) designation. He also holds the CISSP certification. Lenny has an MBA degree from MIT Sloan and a computer science degree from the University of Pennsylvania. For more information about his projects, see <http://zeltser.com>.