August 2010

Feature Article: The Other Face of Facebook

Table of Contents

Feature Article: The Other Face of Facebook

Urban Schrott, IT Security & Cybercrime Analyst, ESET Ireland

In the last few years, social networks and Facebook in particular, as the most gigantic example of the breed (now exceeding 500 million users), have achieved what websites, portals and online forums have previously only dreamed of. That is, to have tens and hundreds of millions of people access them regularly, as their social lives have partially (or completely for some) shifted to this one place. A dream come true indeed for its founder and for advertisers, and also for all manners and forms of bad guys, who have gained a very lucrative platform for their endeavours as they trail behind like scavenging seabirds in the wake of a fishing boat.

The rapid growth of cybercriminal activities has brought with it further specialisation, targeting, and adaptation. Even for cybercrooks, the same old approaches to exploitation were no longer an option: collaborative efforts and diversification needed to be explored to generate results and profits. So imagine the co-operative mayhem and possible combinations of cybercriminal activities where spam mail leads to spyware, which steals passwords, which enable access to social networks, where other members are socially engineered into clicking links which do all kinds of other profitable damage such as proliferation of spam, malware, malicious URLs, pay per click scams, survey scams and so on.

So, let's take a look at some of the Facebook-related topics we've encountered so far.

The Book of Faces (& names, addresses, birthdates, etc)

The first and easiest abuse of Facebook dates back to its start, due to its lax security settings (which, despite frequent tweaking, continue to be a source of controversy to this day). Pretty much anyone could look up random people, and if they displayed their personal info there, it could have been collected. In a minority of cases for possible direct crime, such as burglaries when said user indicated they were absent from the listed address at a certain time. More often it was used for identity theft, password breaking (family and pet names, anyone?) and targeted (spear) phishing email attempts, which convinced the victim of their authenticity by using verifiable information. Most notorious among such scams were probably “Londoning” phishes where “friends” of victims claimed to have been mugged and needed some cash to get themselves sorted out (http://blog.eset.com/?s=Londoning). “Researcher” Ron Bowes garnered some publicity by scraping the data of 100 million or so Facebook users who’d been incautious about what information they revealed and assumed incorrectly that Facebook settings would protect them. Then he helpfully posted all that data to Pirate Bay so that it was available to anyone with the bandwidth to download it, so that even if they tightened up their settings, the information would be out there among the criminal fraternity forever and a day. (http://blog.eset.com/?s=bowes). Randy Abrams wrote an interesting blog recently about Who’s Downloading the Facebook Data, which lists interesting parties who could find the data useful. http://blog.eset.com/2010/08/04/who-is-downloading-the-facebook-data

Phishbook

One of the first abuses of Facebook came as email about “your password is out of order” or “additional security password” or similar phishes, where the victim was asked to kindly provide their existing password to a spoofed *Facebookalike* page. And in spite of continuous warnings from the security community, a shockingly large number of users actually did, and do. The list of phishing hoaxes and scams is a long one, and David Harley collected some examples (and some information resources) in his blog at http://chainmailcheck.wordpress.com/2010/08/06/facebook-hoaxes-and-scams/

Passwordbook

As it has been established that an overwhelming majority of people use one password across the board, not only was their Facebook account a target for abuse after having been phished, but the same password could also be tried at other locations associated with the same victim. And since their name, address, perhaps mother's maiden name even, and other info could easily be retrieved from their profile, it became much easier to get to victims' other assets.

Koobface

Koobface, an anagram of Facebook, is a family of threats that spread through social networking sites such as Facebook (of course), Bebo, MySpace, Twitter, and so on. This family has been active since 2008, spreading in its Facebook incarnation as a message sent to Facebook friends of the owner of an infected system. It enjoyed a resurgence this spring, in a version that came as an eye-catching link that claimed it needed a special codec to run the video. Randy Abrams wrote about it at http://blog.eset.com/2010/04/07/what-is-koobface, as did Aryeh Goretsky at http://blog.eset.com/2010/04/20/another-look-at-koobface. For a more comprehensive long-term view, try http://blog.eset.com/?s=koobface, and more technical descriptions of Koobface variants have been posted at http://www.eset.eu/encyclopaedia/win32-koobface-nbh-net-worm-bno-gen-g?lng=en and http://www.eset.eu/encyclopaedia/win32-koobface-ncf-net-worm-bjc-d-generic-dx-dsb?lng=en.

Spambook

Facebook ads have at times been abused for linking to dodgy or outright malicious websites. As far as I know, some checking has been implemented since, and since it generally means some outgoing expense for the bad guys it's not a cybercriminal tactic of choice, but it is still not to be ruled out as an attack vector.

Appbook

Apps, however, are overall a festering wound. Anyone can make them, anyone can add them, and Facebook safely distances and disclaims itself against any possible damage they may cause, yet users still flock to them. Most apps require you to immediately surrender all your profile info to them, so there goes any trace of privacy out the window, your email address is posted to spammers' lists, your personal info sails away with the phishing fleet, your likes and interests to the social engineering department, and so on. And then there are direct links and invitations for you to conveniently expose yourself with your pants down to…well…just about anything.

Botbook

In recent times more and more accounts of unexpected and involuntary actions on the part of the user are being received. Such as app or link invites from and to random "friends" which they never actually sent: these may infect and replicate if you as much as open the Facebook message, without actually "liking" or adding the app. These prove that cybercriminals have gone about programming custom software that manipulates Facebook and its functions, in order to do their malicious bidding. The complex nature of the scam has been blogged about by Randy Abrams in http://blog.eset.com/2010/08/04/is-facebook-making-a-funny-face and http://blog.eset.com/2010/08/04/multi-level-cybercrime

Trustbook

Much of the trouble mentioned here comes from the fact that users trust Facebook, believing that they're safe, and that their data is visible only to themselves and those they chose to show it to. It seems that people hardly ever doubt that messages, links and apps coming from friends really came from those friends, or that they could possibly be anything but trustworthy. A supposed discussion between Mark Zuckerberg, Facebook's founder and a friend from the early days illustrates this (as well as providing a cultural insight into the organization that may have proved a salutary shock to some of Facebook's users):

Zuck: Yeah so if you ever need info about anyone at Harvard
Zuck: Just ask.
Zuck: I have over 4,000 emails, pictures, addresses, SNS
[Redacted Friend's Name]: What? How'd you manage that one?
Zuck: People just submitted it.
Zuck: I don't know why.
Zuck: They "trust me"
Zuck: Dumb f**ks

(According to an article in The Register at: http://www.theregister.co.uk/2010/05/14/facebook_trust_dumb/.)

But while we might be as dumb as Zuckerberg considers us to be for participating, it is also the way Facebook keeps changing its privacy settings that is constantly making fools out of us. IBM researcher Matt McKeon wrote an enlightening article about the evolution of Facebook privacy, which includes a progressive graph that illustrates in rather frightening detail the increasing accessibility of personal data: http://mattmckeon.com/facebook-privacy/

The ESET blog is a rich resource for further reading on Facebook related issues, with in-depth contributions from David Harley, Randy Abrams, Aryeh Goretsky, Charles Jeter and others http://blog.eset.com/category/facebook.

And because we at ESET Ireland are also on Facebook - http://www.facebook.com/eset.antivirus.ireland - here is the link to ESET's advice to staying safe on Facebook: ESET advises computer users how to keep safe on social networks.

Spanair Issue

According to a report published by the Spanish newspaper El Pais, a computer recording failures on Spanair planes was infected with malicious software at the moment of the accident with the flight JK 5022, which crashed two years ago in an accident where 154 people died. The system is responsible for flagging an alert when a plane registers three or more failures, but investigators suggest that it was infected by a Trojan, and not all faults were being recorded in a timely manner.

Although some media cover the issue as "a trojan brought down a plane", there is not enough information to confirm that the infection directly caused the accident. Nonetheless, it is a pretty good example of how critical systems can have the same malware problems as home computers, and companies can't afford risks involving critical computers. We often hear about infections affecting home users, or corporate user systems or servers. But critical systems can also be infected: computers that control electricity in a city, highly complex medical equipment or the present example of faults in aircraft control.

Probably it will never be known the real situation about this incident, but there obviously are scenarios where malware could have caused loss of life, and it probably has happened.

More information at:

http://www.elpais.com/articulo/espana/ordenador/Spanair/anotaba/fallos/aviones/tenia/virus/elpepunac/20100820elpepinac_11/Tes

http://www.zdnet.com/blog/bott/fact-check-malware-did-not-bring-down-a-passenger-jet/2354

http://www.theregister.co.uk/2010/08/20/spanair_malware/

Stuxnet: summary of a 0-day attack

The part played by malware in the Spanair disaster, if any, could be described as accidental, or collateral damage. July and August saw an instance of a very specific attack on critical systems, based on a vulnerability in the Windows Shell. Microsoft Security Advisory 2286198 explains how the operating system incorrectly parses shortcuts files (.LNK). Several malware families subsequently attempted to make use of this vulnerability. Here is a brief timeline of coverage, especially ESET's, of the incident, with some links to more information relating to each stage of the problem. Stuxnet includes code that attempts to exploit SCADA systems that may use particular control software (Siemens WinCC and PCS7 Products – of course, not all Siemens control software is affected, not all SCADA sites use the targeted products, and even on those that are using them won't necessarily be vulnerable to infection on all or any systems, being protected by access controls, good patching practice, security software and so on.

July 17th.: 0-day vulnerability becomes general knowledge:
http://blog.eset.com/2010/07/17/windows-shellshocked-or-why-win32stuxnet-sux

July 20th.: Win32/Stuxnet is still spreading, with high rate of infections
http://blog.eset.com/2010/07/19/yet-more-on-win32stuxnet
http://blog.eset.com/2010/07/21/win32stuxnet-more-news-and-resources

July 21st.: Microsoft updated advisory with a workaround to lower the risk.

July 23rd.: More malware families spread exploiting the vulnerability
http://blog.eset.com/2010/07/22/new-malicious-lnks-here-we-go

July 27th.: New samples of Sality started to exploit the same vulnerability
http://blog.eset.com/2010/07/27/more-lnk-exploits-by-jove

July 30th.: Microsoft announces an out of cycle patch would be released.
http://www.microsoft.com/technet/security/bulletin/ms10-aug.mspx

August 2nd.: Microsoft patch MS10-046 is published, addressing the bug for supported systems.
http://www.microsoft.com/technet/security/bulletin/MS10-046.mspx

More information at http://blog.eset.com/2010/08/02/save-your-work-microsoft-releases-critical-security-patch

While the patch will, if applied, fix the .LNK problem on systems that are still supported by Microsoft (i.e. Windows XP SP3 and later), users of earlier versions of XP and Windows 2000 will have to update their systems or look for other ways to address the issue. (ESET products do have detection for the exploit as well as for specific malware.) Apart from our ongoing research into the actual malware, we are also working with a number of agencies and stakeholders to address the problem for users of systems that can't be updated.

Zeus

Zeus is a crimeware pack for botnet administration: botnets are networks of zombie computers used to perform various types of computer attacks: phishing, DDoS, spamming, etc. Zeus is specially designed to create trojans for baking and finance information stealing.

Zeus has many versions, which are being seld on the black virtual market by values between 3000 and 4000 dollars in their private versions. As we've received several enquiries from journalists about it, here is a brief note about the versioning evolution of the package:

The first and second generations (1.1.x and 1.2.x) are not in use now. The third and the fourth generations (1.3.x and 1.4.x) – the last published during 2010 – include a new feature to generate a serial number related to a hardware ID, to hamper analysis of the malware, because it will then only run on the hardware on which it was first executed.

Also, there are a lot of unofficial versions in the virtual market: these are cheaper than the private ones, but frequently include backdoors, so bad guys are cheating bad guys.

ESET on the conference circuit

We remind our readers that in the next months ESET's team will be making presentations at various international conferences:

- At CFET (The 4th International Conference on Cybercrime Forensics Education & Training), held on the 2nd and 3rd of September at Canterbury Christ Church University, David Harley is presenting papers on " Antivirus Testing and AMTO: has anything changed?" and "SODDImy and the Trojan Defence" which will be available on the white paper's page at http://www.eset.com/documentation/white-papers shortly afterwards.
- At the 20th Virus Bulletin International Conference, between 29 September and 1 October in Vancouver, Canada, ESET will be presenting:
    - "Large-scale experiments malware, how and why so what?" By Joan Calvet, Jean-Yves Marion, Pierre-Marc Bureau and Jose M. Fernandez.
    - "AV Testing Exposed", by Peter Kosin, Juraj Malcha, Richard Marko and David Harley.
    - "Call of the WildList: last orders for WildCore-based testing?", By David Harley and Andrew Lee.
- On the 13th Association of Anti Virus Asia Researchers International Conference, from 17 to 19 of November, in Bali, David Harley, Lysa Myers and Eddy Willems are presenting "Files and Product Evaluation: the Case for and against Malware

Simulation".

The Top Ten Threats

Keen observers may notice that the top ten ranking, which is normally fairly static and even predictable, has changed this month. This is partly because the Virus Lab has introduced some changes in process which affect the way in which automated signatures are named. This change will enable us to identify reported threats more precisely and deal with customer support issues even more effectively. We've also taken the opportunity to optimize the implementation of ThreatSense.Net® data reporting and finer-grained statistical analysis. Again, this will make interpretation of the statistics easier and more accurate.

1. INF/Autorun

Previous Ranking: 2
Percentage Detected: 7.76%

This detection label is used to describe a variety of malware using the file autorun.inf as a way of compromising a PC. This file contains information on programs meant to run automatically when removable media (often USB flash drives and similar devices) are accessed by a Windows PC user. ESET security software heuristically identifies malware that installs or modifies autorun.inf files as INF/Autorun unless it is identified as a member of a specific malware family.

Removable devices are useful and very popular: of course, malware authors are well aware of this, as INF/Autorun's frequent return to the number one spot clearly indicates. Here's why it's a problem.

The default Autorun setting in Windows will automatically run a program listed in the autorun.inf file when you access many kinds of removable media. There are many types of malware that copy themselves to removable storage devices: while this isn't always the program's primary distribution mechanism, malware authors are always ready to build in a little extra "value" by including an additional infection technique.

While using this mechanism can make it easy to spot for a scanner that uses this heuristic, it's better, as Randy Abrams has suggested in our blog (http://www.eset.com/threat-center/blog/?p=94; http://www.eset.com/threat-center/blog/?p=828) to disable the Autorun function by default, rather than to rely on antivirus to detect it in every case. You may find Randy's blog at http://www.eset.com/threat-center/blog/2009/08/25/now-you-can-fix-autorun useful, too.

2. Win32/Conficker

Previous Ranking: 1
Percentage Detected: 4.89%

The Win32/Conficker threat is a network worm originally propagated by exploiting a recent vulnerability in the Windows operating system. This vulnerability is present in the RPC sub-system and can be remotely exploited by an attacker without valid user credentials. Depending on the variant, it may also spread via unsecured shared folders and by removable media, making use of the Autorun facility enabled at present by default in Windows (though not in Windows 7).

Win32/Conficker loads a DLL through the svchost process. This threat contacts web servers with pre-computed domain names to download additional malicious components. Fuller descriptions of Conficker variants are available at http://www.eset.eu/buxus/generate_page.php?page_id=279&lng=en.

While ESET has effective detection for Conficker, it's important for end users to ensure that their systems are updated with the Microsoft patch, which has been available since the third quarter of 2008, so as to avoid other threats using the same vulnerability. Information on the vulnerability itself is available at http://www.microsoft.com/technet/security/Bulletin/ms08-067.mspx. While later variants dropped the code for infecting via Autorun, it can't hurt to disable it: this will reduce the impact of the many threats we detect as INF/Autorun. The Research team in San Diego has blogged extensively on Conficker issues: http://www.eset.com/threat-center/blog/?cat=145

It's important to note that it's possible to avoid most Conficker infection risks generically, by practicing "safe hex": keep up-to-date with system patches, disable Autorun, and don't use unsecured shared folders. In view of all the publicity Conficker has received and its extensive use of a vulnerability that's been remediable for so many months, we'd expect Conficker infections to be in decline by now if people were taking these commonsense precautions. While the current ranking looks like a drop in Conficker prevalence, this figure is affected by the changes in naming and statistical measurement mentioned earlier: there's no indication of a significant drop in Conficker infections covering all variants.

3. Win32/PSW.OnLineGames

Previous Ranking: 4
Percentage Detected: 3.82%

This is a family of Trojans used in phishing attacks aimed specifically at game-players: this type of Trojan comes with keylogging and (sometimes) rootkit capabilities which gather information relating to online games and credentials for participating. Characteristically, the information is sent to a remote intruder's PC.

These Trojans are still found in very high volumes, and game players need to remain alert. While there have always been unpleasant people who will steal another gamer's credentials just for the heck of it, trading in virtual cash, treasure, avatars and so on is now a major source of illegal income for cybercriminals. It's also important that participants in MMORPGs (Massively Multi-player Online Role Playing Games) like Lineage and World of Warcraft, as well as "metaverses" like Second Life, continue to be aware of the range of other threats like griefing ranged against them. The ESET Research team considered gaming malware in detail in the ESET 2008 Year End Global Threat Report, which can be found at http://www.eset.com/threat-center/threat_trends/EsetGlobalThreatReport(Jan2009).pdf

4. Win32/Tifaut

Previous Ranking: 20
Percentage Detected: 2.56%

The Tifaut malware is based on the Autoit scripting language. This malware spreads between computers by copying itself to removable storage devices and by creating an Autorun.inf file to start automatically.

The autorun.inf file is generated with junk comments to make it harder to identify by security solutions. This malware was created to steal information from infected computers.

See INF/Autorun above for discussion of the implications of software that spreads using Autorun.inf as a vector.

5. INF/Conficker

Previous Ranking: 7
Percentage Detected: 1.61%

INF/Conficker is related to the INF/Autorun detection: the detection label is applied to a version of the file autorun.inf used to spread later variants of the Conficker worm.

As far as the end user is concerned, this malware provides one more good reason for disabling the Autorun facility: see the section on INF/Autorun above.

6. Win32/Agent

Previous Ranking: 3
Percentage Detected: 1.25%

ESET NOD32 describes this detection of malicious code as generic, as it describes members of a broad malware family capable of stealing user information from infected PCs.

To achieve this, the malware usually copies itself into temporary locations and adds keys to the registry which refers to this file or similar ones created randomly in other operating system's folders, which will let the process run at every system startup.

This label covers such a range of threats, using a wide range of infection vectors that it's not really possible to prescribe a single approach to avoiding the malware it includes. Use good anti-malware (we can suggest a good product ☺), good patching practice, disable Autorun, and think before you click.

7. JS/TrojanClicker.Agent.NAZ

Previous Ranking: 18
Percentage Detected: 1.20%

This malware is a Trojan horse that does not generate copies of itself, but is usually part of other malware.

It contains a list of web addresses to which to send requests, used to simulate clicking on advertisements for financial gain (click fraud).

8. HTML/ScrInject.B

Previous Ranking: 6
Percentage Detected: 1.12%

Generic detection of HTML web pages containing script obfuscated or iframe tags that that automatically redirect to the malware download.

Malicious scripts and malicious iframes are a major cause of infection, and it's a good idea to disable scripting by default where possible, not only in browsers but in PDF readers. NoScript is a useful open source extension for Firefox that allows selective disabling/enabling of Javascript and other potential attack vectors.

9. Win32/AutoRun.IRCBot.CX

Previous Ranking: 29
Percentage Detected: 0.87%

Win32/AutoRun.IRCBot.CX is a worm that spreads via removable media. It can be controlled remotely as part of a botnet. It uses techniques common for rootkits.
The worm sends data and commands from a remote computer to Internet using IRC protocol. The implications for the user in terms of infection are similar to those of other malicious programs that use Autorun as a vector. Use caution in what files you access and apply countermeasures against autorun infection. An infected computer will behave in ways associated with botnet activity. However, these activities will not necessarily be obvious to the system user.

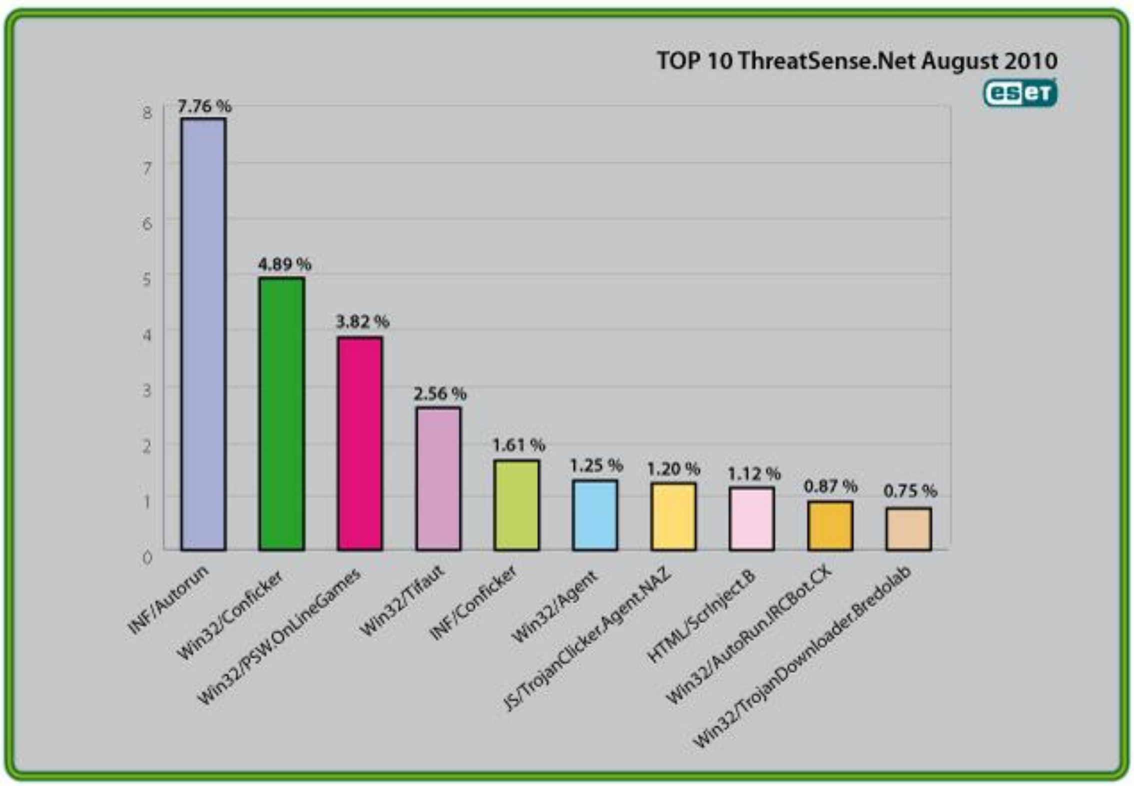
10. Win32/TrojanDownloader.Bredolab

Previous Ranking: n/a
Percentage Detected: 0.75%

This Trojan is designed to establish a clandestine connection to different domains through instructions embedded in code, which will automatically download and run other pieces of malware to the infected computer. This malware does not generate copies of itself. Bredolab variants are associated with the downloading of a wide range of other malicious programs with a wide range of payloads and secondary infection mechanisms

Top Ten Threats at a Glance (graph)

Analysis of ESET's ThreatSense.Net®, a sophisticated malware reporting and tracking system, shows that the highest number of detections this month, with almost 7.76% of the total, was scored by the INF/Autorun class of threat.



About ESET

ESET is a global provider of security software. The ESET NOD32® Antivirus and ESET Smart Security products are consistently recognized among the most comprehensive and effective security solutions available today.

Additional resources

Keeping your knowledge up to date is as important as keeping your AV updated. For these and other suggested resources please visit the ESET Threat Center to view the latest:

- ESET White Papers
- ESET Blog
- ESET Podcasts
- Independent Benchmark Test Results
- Anti-Malware Testing and Evaluation