Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Identity Theft Made Easy

This paper discusses identity theft, made easy and "impersonal" with the use of the Internet and the development of shareware tools.

Copyright SANS Institute
Author Retains Full Rights

AD

Roy Reyes
GSEC
Version 1.2e
Original submission
Taking online certification

Identity Theft Made Easy

What's the one thing that we as individuals can claim to be our own from the moment we are born to even after our death?

Our identity.

…Or so we would think or at least hope. Identity theft is steadily on the rise[1] unknowingly to most of us; and, that is how the thieves would like to keep it. What was once done through what I would call "physical stealing" – starting off with stealing driver's license or some form of identification, then collecting more useful personal information and even doing some social engineering, identity theft is today made easy and "impersonal" with the use of the Internet and the development of shareware tools.

So what is identity theft? It is the inappropriate gathering of another's personal information/records for the purpose of unauthorized impersonation. More often it is done to basically steal money, but it can also be done to attack or deface an individual. Thieves would start out small so as not to make anything obvious; but the more they get away with their criminal activities, the more risks they will take. By the time a victim realizes what is going on, the perpetrator might have moved on to the next victim. The victim is not only left with monetary losses but also feelings of vulnerability and helplessness. There can even be some cases where the victim amasses a criminal record without having any clue about it.[2]

How to get started–

Like most cybercrimes, identity theft is considered a "white-collar" crime. It is a "faceless" crime which means the offender feels guilt-free not knowing who his victims are. The attacker would skillfully plan the attack, would be willing learn new techniques, and would to take the time to do research

[1] "Calls to the Federal Trade Commission's identity theft hotline have tripled in the past six months, and the Internet is partly to blame." – CNET News, 30 August 2000
[2] See www.ftc.gov/bcp/conline/pubs/credit/idtheft.htm#victim – IF YOU'RE A VICTIM: Criminal records/arrests.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

on a victim or for a victim. Ironically, in some cases his search is eased by the government itself:

> …The government may be giving out your home address, social security number and other personal information online:
>
> If you live in Ohio, anyone who types your name into a county database can learn your address and how much your house is worth. He can also inspect detailed floor plans of your house, showing placement of your windows, porches and balconies. Supporters of the state's online initiative call it a breakthrough for open access to government records. Critics have another way of describing it: a breaking-and-entering handbook.
>
> Governments around the country have been rushing to put property records online. Many jurisdictions have joined Ohio in creating databases searchable by name. If you go to the Brookline, Mass., website, you can find out where Michael Dukakis lives. Miami's will tell you Janet Reno's home address…
> *Time Magazine*, 2 July 2001

However, if the attacker does not reside in Ohio or in other such places, there are sites on the Internet where, for less than a hundred dollars, he can buy tools that would provide him with enough information to start an identity theft attack.

One such tool, *NetDetective2001* by Harris Digital Publishing, proclaims itself as "The Easiest Way to Discover the Truth about Anyone" and retails for only $49.50. *NetDetective2001* also claims on their site the following:

> NetDetective2001 is an amazing new tool that allows you to dig up facts about anyone. It is all completely legal, and you can use it in the privacy of your own home without anyone ever knowing. It's cheaper and faster than hiring a private investigator.
>
> NetDetective2001 is compatible with all Internet-related software (Windows 95/98 on AOL, Netscape, CompuServe, AT&T, or WebTV). Whether you're a computer beginner or a veteran computer use, it is simple and easy to use.
> www.netdetective2000.com

NetDetective2001 also offers a satisfaction guarantee and a two-year update. Certainly Harris Digital Publishing only had good intentions for selling this product, but who's to say that every

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

user have those same intentions. Just by saying that it can be used in the "privacy of your own home", they could be implying that they are not responsible for the actions of the individual user. Some of the information *NetDetective2001* can provide are:

- Email addresses
- Phone numbers
- Addresses
- Spoof your email address
- Driving records
- Criminal records
- Long lost loves
- Make untraceable phone calls

Another site that an attacker can use is DOCUSEARCH.COM which supplies much of the same information as *NetDetective2001*; as well as one of the most personal data and a key information to identity theft – Social Security numbers. They have a variety of searches that range from $20 to $180, still pretty inexpensive considering all the information you can get. Their claim:

> DOCUSEARCH.COM is the place to find, locate & track down anybody! We offer locate searches, DMV driver & vehicle searches, telephone record searches, financial & bank searches, criminal & property records, plus hundreds of Free searches. www.docusearch.com

DOCUSEARCH.COM's director, Dan Cohn, denies the role that his company has played in the growing problem of identity theft since he believes Social Security numbers are "public" records.[3] Piecing this "public" information together with some of the other information the two sites present is enough for a thief to start a couple of credit cards under a false name.

So who, besides the government, provides for the providers? Other companies. Due to the shrinking economy, there is evidence that some folding dot-com companies sold off databases of customer information. The unethical and controversial practice was a last ditch effort to salvage any remaining assets.[4]

Gathering more data-

Getting credit cards is often not enough of a challenge to an ambitious attacker. He could try to gather more data about his victims by building a better profile of them. This is when spyware come in handy. Simply put, spyware are (sometimes free) tools available online that allow a user to spy on an innocent

[3] See www.infowar.com/class_1/00/class1_040400b_j.shtml – par.9
[4] "*Failed dot-coms may be selling your private information*" – CNET News, 29 June 2000

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

victim. Their capabilities range anywhere from seeing your internet activity to pretty much taking full control of your computer. Spyware are sometimes used by e-commerce websites to monitor who is viewing their pages. They use it to keep track of each visitor's interest so as to offer and show ads of other related items.[5]

To get these spyware running on their target computers, the attacker has a couple of options. If the attacker can some how get physical access to the victims' computer, he can simply bring with him a floppy and load an executable file that would run in the background; or, it could *sit* dormant in the victims' hard drive. The spyware will then be launched either when he opens up a particular application or when the attacker sends some remote command to that computer via email or network connections. If the attacker has no physical access, sending email(s) with a hidden Trojan file or an innocent looking webpage link attached to it would be the one of the more common methods. The mail message could be a very simple and generic ad about how to get FREE stuff online. Nothing hooks more people into downloading files or visiting malicious sites than the word "FREE".

A couple of spyware that are well-known not only in the hacker community but also in the White-Hat community are **Back Orifice2000** (by the hacker group *Cult of the Dead Cow*) and **NetBus** (written by a Swedish programmer, Carl-Fredrik Neikter). Both are several years old and have known signatures which mean that there are patches for them. However, this doesn't mean that every computer is immune from them. Patches are only effective if they are installed. From personal experience on a test network, NetBus is a powerful, fun, and at the same time, scary tool. It virtually allows you to take over the victim machine; from remotely opening the CD-ROM to getting screen shots to taking control of the mouse.

Other much newer tools which rival NetBus are **Spector** and **eBlaster**, both products of SpectorSoft. It sells for around $70 and claims to "record everything":

> …Install **Spector** on your PC and it will record EVERYTHING your spouse, kids and employees do on the Internet. Spector SECRETLY takes hundreds of screen snapshots every hour, very much like a surveillance camera. With Spector, you will be able to see

[5] See www.thebee.com/bweb/iinfo200.htm – par. 2

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

EVERY chat conversation, EVERY instant message, EVERY e-mail, EVERY web site visited and EVERY keystroke typed…

…Track Spouse, Children or Employee online activity by receiving email reports of everything they do online. **eBlaster** delivers detailed activity reports, including all web sites visited, all applications run, and all keystrokes typed, right to your e-mail address, as frequently as every 30 minutes…
www.spectorsoft.com

Once again, these tools were not created for malicious purposes but they can easily be used in that way.

GOTCHA!!!

Now the attacker has most of the information he needs to launch a full-on assault on victims' identities. He's has lots of vital information: addresses, phone numbers, email address, Social Security numbers, and even internet behavior of his victims. In addition, he is capable of monitoring their offline activities. He is now ready to "become" his victim.

Often, "he" (as I've referred to through out my paper) is more than one person. *HE* consists of two or more people and sometimes a big group of people varying in ages who have a knack for pushing things to the limit to see what they can get away with; seeing every obstacle such as firewalls as a challenge. While some in the group hack only for fun without cruel intents others have mischievous agendas.

Conclusion

Of course the purpose of my paper is not to encourage identity theft but to bring awareness. The first thing anyone should do to protect themselves is to be more aware of identity theft and that it can happen to anyone. When using the Internet, pay close attention to what information you are providing the website you are in. If there is any doubt on its legitimacy, do not provide pertinent and personal info. Don't be naïve.

Also, there are many ways to make the Internet work for you so as to safeguard yourself. For one, apply or install patches to your software. Keep up to date with what vulnerabilities are out there. Know your rights that the government has established for you such as the Gramm-Leach-Bliley Act,[6] which protects your

[6] Privacy: The Act requires all financial institutions, regardless of whether they form an FHC, to disclose to customers their policies and practices for protecting the privacy of non-public personal information. The disclosure

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

privacy; or "California… has a law that permits police to release arrest data to reporters while withholding it from businesses that would use it for commercial purposes. Privacy advocates say more jurisdictions should follow California's lead…"[7]

In addition, there are private non-profit companies like *Privacy Rights Clearinghouse* that help people become more aware of how to protect their privacy. So, hope is not all lost. There are ways to prevent identity theft, it just takes a little proactive approach.

© SANS Institute 2002, Author retains full rights.

which customers would receive at the time of establishing the relationship and at least annually thereafter would allow customers to "opt-out" of information sharing arrangements to non-affiliated third-parties. The Act permits financial institutions to share personal customer information with affiliates within the holding company. Effective immediately, it is a criminal offense for any person (including firm employees) to obtain or attempt to attain customer information relating to another person from any financial institution by making a false or fraudulent statement to an employee of that financial institution. Regulators have six months after the date of enactment to adopt final rules implementing the privacy provisions. - www.sia.com/gramm_leach_bliley

[7] Time Mag, July 2, 01 - http://www.time.com/time/covers/1101010702/index.html

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Reference:

Ard, Scott. "Back Orifice 2000 makes its debut." *CNET NETWORKS*. 10 July 1999. URL: news.cnet.com/news/0-1003-200-344651.html

Barnes, Cecily. "Internet contributes to rise of identity theft, FTC says." *CNET NETWORKS*. 30 August 2000. URL: news.cnet.com/news/0-1005-200-2654832.html

Brand, Bob. "Spyware." *Internet Info For Real People*. 7 April 200. URL:www.thebee.com/bweb/iinfo200.htm

Cohen, Adam. "Internet Insecurity." *Time Magazine*. 2 July 2001. URL:www.time.com/time/covers/1101010702/index.html (2 July 2001)

Docusearch.com™. Boca Raton, FL. URL:www.docusearch.com

Federal Trade Commission. "ID Theft: When Bad Things Happen To Your Good Name." February 2001. URL:www.ftc.gov/bcp/conline/pubs/credit/idtheft.htm

"NetBus - Backdoor For Win 95/98 and Win NT." 2 April 2001. URL: http://home.t-online.de/home/TschiTschi/netbus_eng.htm

"NetBus -- BO's Older Cousin." 13 October 1998. URL: http://www.nwinternet.com/~pchelp/nb/netbus.htm

NetDetective2001. Harris Digital Publishing, Deland, FL. URL:www.netdetective2000.com

O'Brien, Timothy L. "Aided By Internet, Identity Theft Soars." *The New York Times News Service*. 4 March 2000. URL:www.infowar.com/class_1/00/class1_040400b_j.shtml (4 April 2000)

Privacy Rights Clearinghouse. 16 July 2001. URL: http://www.privacyrights.org

Sandoval, Greg. "Failed dot-coms may be selling your private information." *CNET NETWORKS*. 29 June 2000. URL: http://news.cnet.com/news/0-1007-200-2176430.html

"Securities Industry Association: Gramm-Leach-Bliley Act". URL: www.sia.com/gramm_leach_bliley

SpectorSoft. URL: http://www.spectorsoft.com/

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 21st, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced