From: Dylan Kulesza [mailto:dylan.kulesza@yahoo.com]
Sent: Tuesday, December 14, 2010 8:56 PM
To: Caro, Armando
Subject: Re: Re:

I found one of the IRC servers he hangs out on. Very low amount of users (not a public server) and the channel is oriented for hackers. He isn't online presently.

Nothing I've seen puts him at a sophisticated level. But most people that do what he did aren't. Found a lot of info about him packetting / DDOS'ng. This would lead me to believe he got the credentials from a compromised machine that was keylogging, etc.

Did find lots of google info on tila.trb domain being catalogued (with our internal prod/test servers). Found out the password reset had a XSS vuln to it (but I can really just vuln myself - might be able to sucker help desk to click the link and XSS them). Had lots of time outs on server (username/login) so I'm gonna play with it later. Could be you guys doing LDAP queries.

From: "Caro, Armando" <acaro@tribune.com>
To: Dylan Kulesza <dylan.kulesza@yahoo.com>
Sent: Tue, December 14, 2010 6:53:58 PM
Subject: RE: Re:

Ngarcia

That account has been deleted

Armando Caro
Managing Director, Technology Architect
Tribune Technology
☎ (312) 222-2708

From: Dylan Kulesza [mailto:dylan.kulesza@yahoo.com]
Sent: Tuesday, December 14, 2010 6:53 PM
To: Caro, Armando
Subject: Re:

Can you send me the username that was used.

Going to do some googling with that to see if google leaked out info.

From: "Caro, Armando" <acaro@tribune.com>
To: "Dylan Kulesza (dylan.kulesza@yahoo.com)" <dylan.kulesza@yahoo.com>
Sent: Tue, December 14, 2010 6:38:41 PM
Subject:

http://nameless.pastebin.com/1iG0jCVx
http://skids.pastebin.com/2eTnZHkG
http://www.anonnews.org/?p=comments&c=press&i=34

From: Kulesza, Dylan
Sent: Wednesday, December 15, 2010 2:28 PM
To: Caro, Armando
Subject: RE: Final info on Chippy1337

I've seen the screen name used on Xbox 360 account (bungie) and a few other. With some sort of search warrant and cooperation, you could get the information. Other than that, it would take more time than it's worth. Have to become his friend online….sucker him to clicking a link to a website…etc…Basically reverse social engineer him.

From: Caro, Armando
Sent: Wednesday, December 15, 2010 2:14 PM
To: Kulesza, Dylan
Subject: RE: Final info on Chippy1337

Thanks for continuing to research this. I would imagine it would be difficult to discover his identity.

Armando Caro
Managing Director, Technology Architect
Tribune Technology
☎ (312) 222-2708

From: Kulesza, Dylan
Sent: Wednesday, December 15, 2010 2:04 PM
To: Caro, Armando
Subject: RE: Final info on Chippy1337

I guess so – I'm just idling on their chat server. A buddy of mine was talking to them as well.

I don't think it would be too hard to social either. When playing with it last night I got an error message to send out our internal help desk extension and phone number (with a lovely comment box to send a message). I sent a message with an XSS vulnerability – curious if there is an admin page that will render that. If it does – someone could target browser vulns through that system.

I'm still sitting in the chan recording everything. I'll let you know if I get any more details – these guys like to brag – status thing.

From: Caro, Armando
Sent: Wednesday, December 15, 2010 2:02 PM
To: Kulesza, Dylan
Subject: RE: Final info on Chippy1337

Good find. So he social engineered an admin password from someone.

Armando Caro
Managing Director, Technology Architect
Tribune Technology
☎ (312) 222-2708

From: Kulesza, Dylan
Sent: Wednesday, December 15, 2010 2:00 PM
To: Caro, Armando
Subject: Final info on Chippy1337

They said this on their private IRC server:

```
<&CalqCorn> lolwut
<&CalqCorn> sharpie
<&CalqCorn> chippys no 1 fan? rofl
<&sharpie> yeah
<&CalqCorn> r u hacking latimes?
<&Nikon> he did it
<&sharpie> social
<&Nikon> yday
<&sharpie> not hax
<&Nikon> he actually changed
<&Nikon> a full article lol
<&sharpie> http://imgur.com/ZhzUS.jpg
<~Xero> LOL
<&CalqCorn> xero
<&sharpie> It was just a test edit
<&sharpie> I was trying to do the full page
<&CalqCorn> i recovered an admin password for coldfusion 6.1
<&sharpie> *main page
<&CalqCorn> i cant decrypt it tho
<&sharpie> but got killed
<~Xero> uh
<&sharpie> before I could
<~Xero> werent you the
<~Xero> epic john guy
<~Xero> with the epic patched john
<~Xero> that cracked anything
<~Xero> or was that someone else
<&CalqCorn> no i have all those patches but
<&CalqCorn> from my internet scouring didnt see that mentions @_@
<&CalqCorn> mentioned*
<~Xero> nah
<~Xero> this guy
<~Xero> was like
<~Xero> EPIC
<~Xero> john
<~Xero> guy
<~Xero> he could crack any hash you could give him
```

```
<~Xero> cf, sql, triple sha-256
<~Xero> bbl
```

From: Kulesza, Dylan
Sent: Thursday, December 16, 2010 10:55 AM
To: Caro, Armando
Subject: FW: Logs of Veniusm

Logs – some from me and some from a buddy.

Also they setup a chippy1337@gmail.com account. I don't think Chippy1337 is a person, rather than an entity that this group (or a few users) use for hacking purposes. Two individuals might be utilizing this name...

My buddy said they have some root accounts and credit cards too in the log.... Might spark more interest in FBI with other illegal activity involved.

From: Ben Floyd [mailto:dataplex@gmail.com]
Sent: Thursday, December 16, 2010 9:59 AM
To: Kulesza, Dylan
Subject: Logs of Veniusm

Dylan,

Here are the logs of the IRC channel with enough information to begin an investigation. I take no responsibility for the contents on these log files nor will I use any information gathered for malicious or illegal purposes. I will delete the log files after this email has been received by you and confirmed.

- Ben

From: Kulesza, Dylan
Sent: Thursday, December 16, 2010 1:12 PM
To: Caro, Armando
Subject: Chippy1337 Incident

IRC Server:
irc.skidsr.us (6667)

Found using google for Chippy1337: http://venuism.pastebin.com/3iEDUjxa

Channel: #thegibson

My username: [M|RAGE]
Idle'd since the beginning

Another account a buddy (Ben Floyd) has used to capture info: hiccup
He is actively talking

Recently they've talked about using FiSH to encrypt traffic – haven't acted on yet.

From: Kulesza, Dylan
Sent: Thursday, December 16, 2010 1:36 PM
To: Caro, Armando
Subject: Consolidated Chippy1337 Notes

Updated with my latest logs.. They are encrypting some public stuff now.....Using FiSH: http://fish.secure.la/

IRC Server:
irc.skidsr.us (6667)

Found using google for Chippy1337: http://venuism.pastebin.com/3iEDUjxa

Channel: #thegibson

My username: [M|RAGE]
Idle'd since the beginning (Just recently 12/16/10 started to communicate)

Another account a buddy (Ben Floyd) has used to capture info: hiccup
He is actively talking

Recently they've talked about using FiSH to encrypt traffic – haven't acted on yet.

They said this on their private IRC server:

```
<&CalqCorn> lolwut
<&CalqCorn> sharpie
<&CalqCorn> chippys no 1 fan? rofl
<&sharpie> yeah
<&CalqCorn> r u hacking latimes?
<&Nikon> he did it
<&sharpie> social
<&Nikon> yday
<&sharpie> not hax
<&Nikon> he actually changed
<&Nikon> a full article lol
<&sharpie> http://imgur.com/ZhzUS.jpg
<~Xero> LOL
<&CalqCorn> xero
<&sharpie> It was just a test edit
<&sharpie> I was trying to do the full page
<&CalqCorn> i recovered an admin password for coldfusion 6.1
```

```
<&sharpie> *main page
<&CalqCorn> i cant decrypt it tho
<&sharpie> but got killed
<~Xero> uh
<&sharpie> before I could
<~Xero> werent you the
<~Xero> epic john guy
<~Xero> with the epic patched john
<~Xero> that cracked anything
<~Xero> or was that someone else
<&CalqCorn> no i have all those patches but
<&CalqCorn> from my internet scouring didnt see that mentions @_@
<&CalqCorn> mentioned*
<~Xero> nah
<~Xero> this guy
<~Xero> was like
<~Xero> EPIC
<~Xero> john
<~Xero> guy
<~Xero> he could crack any hash you could give him
<~Xero> cf, sql, triple sha-256
<~Xero> bbl
```

From: Kulesza, Dylan
Sent: Thursday, December 16, 2010 10:55 AM
To: Caro, Armando
Subject: FW: Logs of Veniusm

Logs – some from me and some from a buddy.

Also they setup a chippy1337@gmail.com account. I don't think Chippy1337 is a person, rather than an entity that this group (or a few users) use for hacking purposes. Two individuals might be utilizing this name...

My buddy said they have some root accounts and credit cards too in the log.... Might spark more interest in FBI with other illegal activity involved.

From: Ben Floyd [mailto:dataplex@gmail.com]
Sent: Thursday, December 16, 2010 9:59 AM
To: Kulesza, Dylan
Subject: Logs of Veniusm

Dylan,

Here are the logs of the IRC channel with enough information to begin an investigation. I take no responsibility for the contents on these log files nor will I use any information gathered for malicious or illegal purposes. I will delete the log files after this email has been received by you and confirmed.

- Ben