CAUTHEN, JOHN M. (SC) (FBI)

From: CALDERON, CHRISTOPHER A. (SF) (FBI)
Sent: Thursday, February 10, 2011 2:52 PM
To: CAUTHEN, JOHN M. (SC) (FBI)
Subject: RE: Chippy1337

Hey John,

Sorry for the delay in getting back to you. It would definitely be best if you cut a lead and then we can search everything we have and provide you with all the info. Just send it to squad CY-2 in the San Jose RA.

Let me know if you need any other info.

-Chris

From: CAUTHEN, JOHN M. (SC) (FBI)
Sent: Thursday, February 10, 2011 6:45 AM
To: CALDERON, CHRISTOPHER A. (SF) (FBI)
Subject: RE: Chippy1337

I have the hack coming from IP 188.165.6.178 on Dec 14 2010 between about 2 and 5 pm (GMT). I am really interested in this IP.

If you have anything on that date, for IP 188.165.6.178 , I'd like to know.

Also, I'd like to get any IP's associated with sharpie.

I also have a list of IP's the subject used to send e-mails taunting the victim, I'd like to search in the logs to see if they are associated with anyone? They are :

178.73.198.66 on 12/1/2010

212.82.108.124 (Dublin Ireland), on 12/2/2010
189.1.169.40 (Brazil)
98.208.49.74 - (Comcast)
85.17.155.83, (Italy)
81.218.235.170, (Israel)
212.82.109.128, (Yahoo server located in Dublin Ireland)
91.205.175.34, (Germany)
212.82.108.243, (Yahoo server located in Dublin Ireland)
212.82.108.116, (Yahoo server located in Dublin Ireland)
212.82.108.246, (Yahoo server located in Dublin Ireland)
78.46.93.184, (Germany)
80.74.135.87, (Switzerland)
91.214.168.172, (Switzerland)
213.229.110.98, (England)
213.229.110.97, (England)

91.214.168.172 - on 12/6/2010

I hope I am not tasking you with a lot of work that you don't really have time to work on. Should I send an ec with a lead? Should I request a copy of the logs and search it myself? What can I do to minimize the impact on you folks?

Again, thanks for your help!

John Cauthen
UNCLASS
NON RECORD

From: CALDERON, CHRISTOPHER A. (SF) (FBI)
Sent: Wednesday, February 09, 2011 6:00 PM
To: CAUTHEN, JOHN M. (SC) (FBI)
Subject: RE: Chippy1337

Sharpie is definitely in our logs. I took a really quick look and he's in there a lot. I saw a few IPs and they were mostly in Europe. Let myself or Melanie Adams know if you want more information on what we have.

-Chris

From: CAUTHEN, JOHN M. (SC) (FBI)
Sent: Wednesday, February 09, 2011 5:18 PM
To: CALDERON, CHRISTOPHER A. (SF) (FBI)
Subject: RE: Chippy1337

I'm just doing a little more research on ACS and comparing it to my notes. It seems after the hack, the victim, on his own, got on an IRC channel called "thegibson" which is reference in 288A-SF-147136. On this IRC, the victim got involved in a chat with sharpie, Xero, and others. It appears the moniker "sharpie" actually did the hack. Both sharpie and xero and featured in 288A-SF-147136 and 288A-WF-242710. Do you guys have anything on sharpie?

From: CALDERON, CHRISTOPHER A. (SF) (FBI)
Sent: Wednesday, February 09, 2011 5:14 PM
To: CAUTHEN, JOHN M. (SC) (FBI)
Subject: RE: Chippy1337

Hey John,

I took a look in our logs, but no luck. He doesn't show up. On a side note ... while we were working this thing, I was educated as to what "1337" means. Apparently "1337" spells "leet", as in elite. Those who use 1337 in their name are supposed to be "elite hackers".

Wish I had more info for you. Sorry.

-Chris

From: CAUTHEN, JOHN M. (SC) (FBI)
Sent: Wednesday, February 09, 2011 3:47 PM
To: CALDERON, CHRISTOPHER A. (SF) (FBI)
Subject: Chippy1337

Chippy1337 is my subject. It looks like he has some level of access to the Tribune Media Server in Los Angeles.

Thanks!

SA John M. Cauthen
Telephone 916-416-6714
NON RECORD
UNCLASS