

Ankur De

Securus Technical Support

Securus Technologies, Inc.
3000 Kellway, Suite 150
Carrollton, Texas 75006

Office: (972) 277-040
Mobile: (817) 703-705
www.securustech.net

From: John Mr
Sent: Monday, July 21, 2014 2:07 PM
To: Ankur De
Subject: FW: Adams Co, NE / Port locations

MANAGEMENT LEVEL

Suffolk County Jail, MA >> All Sites

Recording Audit Log Search

Access Date/Time	Recording Usage	First Name	Last Name	Acct Number	PIN	Cal Dat	
07/18/2014 14:56:46	PLAYBACK	AARON	HERNANDEZ	147230	1472303791	07-18-201	
07/18/2014 14:49:44	PLAYBACK	AARON	HERNANDEZ	147230	1472303791	07-11-201	
07/18/2014 14:43:21	PLAYBACK	AARON	HERNANDEZ	147230	1472303791	07-10-201	
install@SECUR.TX	Installation Team	64.251.160.49	Administrator	Successful Login	07/18/2014 14:37:49	07/18/2014 21:57:23	440
install@SECUR.TX	Installation Team	50.123.222.186	Administrator	Successful Login	07/18/2014 09:08:57	07/18/2014 10:02:59	54
install@SECUR.TX	Installation Team	50.123.222.186	Administrator	Successful Login	07/18/2014 09:08:41	07/18/2014 09:08:41	0

<http://www.iplocation.net/index.php>

IP Address	Country	Region	City	Postal Code	Area Code
64.251.160.49	United States	SD	Rapid City		605

From:

Sent: Tuesday, July 22, 2014 9:56 AM

Subject: IP trace

Importance: High

Below is a trace I ran on the IP address that was used to access calls in Suffolk, MA. It is not a Securus IP and it originates from *Golden West Telecom* in Rapid City, South Dakota.

While there are no facilities in the immediate vicinity, it's still possible that this IP belongs to a facility somewhere in SD. There was a generic account used to access the calls, that is typically used by Field technicians for conducting installations which has since been disabled.

We had originally suspected [redacted] who lives in [redacted] but we have not been able to tie this IP back to him. After having him provide his IP identity we found that he was using a different service provider and the IP was not a match. Although, there is no telling what computer or location he might have accessed the calls from - or even if he was the person responsible. From my perspective, there is really no way to tell for sure.

There are really only two things that we can do:

Option 1 is to prevent this IP from accessing SGate and see if someone calls Tech Support to report the outage. It might help pinpoint the person responsible. The Network Team would have to block it at the firewall. In doing so, there is a possibility that we prevent legitimate users from accessing resources (see message from Bruce P: [redacted] below). If it comes back as a facility, we would obviously want to work with them to try and identify who used the computer to access the calls. I believe that since there is potential for an outage to a customer with this option, the decision needs to come from the executive level and be executed on change control.

Option 2 is getting a subpoena for Golden West Telecom to request the owner of the IP address. This would only be useful if the IP is directly tied back to someone's house and we get the name, or to one of our facilities that we can alert to the breach and work with to identify the responsible party. It's entirely possible that it comes back as a public library or even a Starbucks.

Additionally, D [redacted] is requesting some sort of official response to this situation to give the site in Suffolk, MA.

Sent: Wednesday, July 23, 2014 9:12 AM

To:

Subject: RE: Recordings Access - DT Hernandez

Re request that like this: AND PLEASE STICK TO THIS SCRIPT

- We recognize the calls were accessed and "played back" but not downloaded
 - Someone has illegally accessed the system using an "install" username/password that was inactive for a couple of years and which we believed was deactivated (it has now been deactivated)
 - We have noted the IP address from which the calls were accessed
 - These are your recordings that were illegally accessed, and if you want to issue a subpoena to get the exact address from which the access was obtained, we will support you in that effort
 - All inquires have been researched, and no other inactive accounts exist
 - We've done our own internal investigation, and we do not believe the way done by a vendor's employee
 - We don't have a subpoena on hand
-

From: E

Sent: Monday, July 21, 2014 3:08 PM

To: D

Subject: RE: IP trace

I don't believe blocking the IP is the correct way to address this. Is the customer in South Dakota? If so then this may be a facility IP with multiple users accessing S-Gate and blocking the IP may block legitimate users. If it is not a site and we block the address the suspected user can simply go to another location with a different IP address and gain access again.

Can we disable the generic account that was used for access? Then the user is blocked no matter where they attempt access from.

Trish Aug <taug@securustech.net> wrote:

OMG.....this is not good! The company will be called to task for this if someone got in there that shouldn't have been. I have to let Matt R know. We are mtg. with the command staff on Weds. and will be questioned on this if that is the case

From: Debbie C
Sent: Monday, July 21, 2014 1:58 PM
To: Trish Aug
Subject: RE: Recordings Access - DT Hernandez

Looks like it came from Wall, South Dakota. Ankur is contacting the FSM in that area. I don't think we are going to be able to get an actual name. More to come.

Debbie C
Director Technical Support
Securus Technologies, Inc.
14651 Dallas Parkway, Suite 600
Dallas, Texas 75254-8815

Office: (972) 277-031
Mobile: (817) 688-432
www.securustech.net

From: Debbie C
Sent: Monday, July 21, 2014 12:55 PM
To: Trish Aug
Subject: RE: Recordings Access - DT Hernandez

I'll call IT now...Ankur can't get in touch with anyone.

Debbie C
Director Technical Support
Securus Technologies, Inc.
14651 Dallas Parkway, Suite 600
Dallas, Texas 75254-8815

Office: (972) 277-03

From: Debbie C
Sent: Monday, July 21, 2014 12:10 PM
To: Trish Aug
Subject: RE: Recordings Access - DT Hernandez

He found the IP address...he is asking IT who it is...


Debbie C:
Director Technical Support
Securus Technologies, Inc.
14651 Dallas Parkway, Suite 600
Dallas, Texas 75254-8815

Office: (972) 277-031
Mobile: (817) 688-432
www.securustech.net

From: Trish Aug
Sent: Monday, July 21, 2014 11:10 AM
To: Debbie C
Subject: Fwd: Recordings Access - DT Hernandez

Anything?

----- Original message -----



From: Trish Au
Sent: Monday, July 21, 2014 2:04 PM
To: Matt R
Subject: FW: Recordings Access - DT Hernandez
Importance: High

FYI – potential problem in Suffolk..... ☺

From: Debbie C
Sent: Monday, July 21, 2014 2:02 PM
To: Trish Aug
Subject: RE: Recordings Access - DT Hernandez

Still working on it...

Sent via the Samsung Galaxy S4 Mini, an AT&T LTE smartphone

----- Original message -----

From: Debbie Ca
Date: 07/21/2014 1:56 PM (GMT-06:00)
To: David Bel
Subject: FW: Need some help

From: Ankur De
Sent: Monday, July 21, 2014 11:06 AM
To: Bruce Patte
Subject: Need some help

Bruce.

I was wondering if your team may be able to help me. I have an IP Address and I need to know if you can trace back to who used it on Friday July 18th?

The IP Address is 64.251.160.49

I need to know if your team can look at this asap as this is a hot issue for me.

Thanks,

Ankur De

Securus Technologies, Inc.
3000 Kellway, Suite 150
Carrollton, Texas 75006

Office: (972) 277-0400
Mobile: (817) 703-705
www.securustech.net
