

Tracking and Trapping a Hacker

An Actual Takedown

Wesley McGrew

Ray Vaughn

Mississippi State University

Critical Infrastructure Protection Center

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

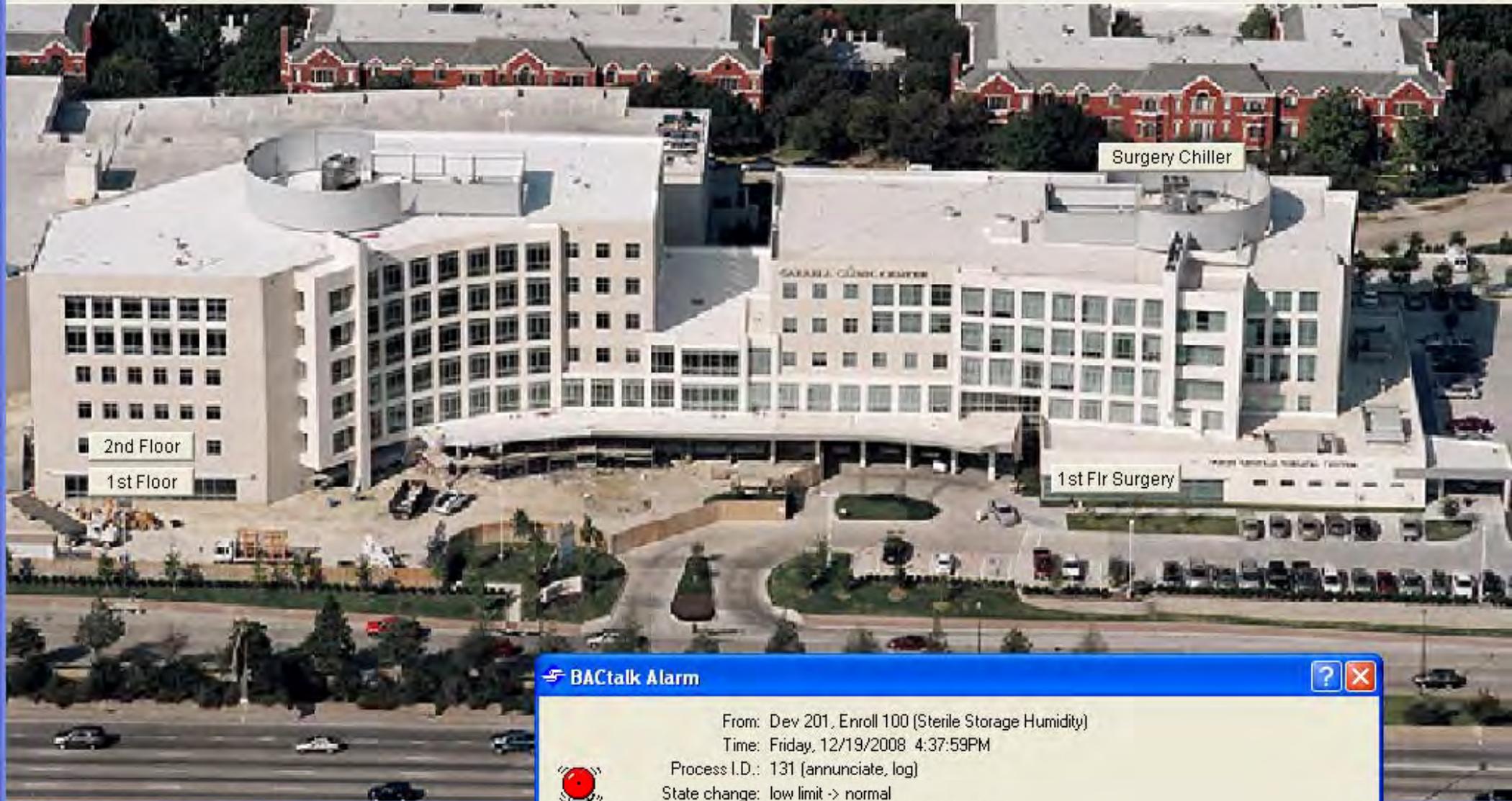
1. REPORT DATE APR 2010		2. REPORT TYPE		3. DATES COVERED 00-00-2010 to 00-00-2010	
4. TITLE AND SUBTITLE Tracking and Trapping a Hacker. An Actual Takedown				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Mississippi State University, Critical Infrastructure Protection Center, Mississippi State, MS, 39762				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution unlimited					
13. SUPPLEMENTARY NOTES Presented at the 22nd Systems and Software Technology Conference (SSTC), 26-29 April 2010, Salt Lake City, UT. Sponsored in part by the USAF. U.S. Government or Federal Rights License					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT Same as Report (SAR)	18. NUMBER OF PAGES 18	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			



Critical Infrastructure
Protection Center
At Mississippi State University

Recruitment

Thread / Author	Replies	Views	Rating	Last Post [asc]
 EverDesign Recruitment (Pages: 1 2) Matu EX	18	117	★★★★★	Today 12:52 PM Last Post: jebakumar1984
 WebHax Crew - Members read important news (Pages: 1 2 3 4 ... last) THE BOSS	153	1,823	★★★★☆	Today 12:36 PM Last Post: THE BOSS
 Poll: Stealers Group! (Pages: 1 2 3 4 ... last) 88power88	41	604	★★★★☆	Today 12:33 PM Last Post: i RaT YoU
 [NEW] Antimatter crew recruiting (Pages: 1 2 3 4 ... last) WhiteFlame	161	2,353	★★★★☆	Today 12:31 PM Last Post: i RaT YoU
 the Cash Crew (Pages: 1 2 3 4 ... last) Tomber	148	2,719	★★★★☆	Today 12:14 PM Last Post: Howell
 The Gamers - Recruitment (Pages: 1 2 3 4 ... last) Mendacious	297	3,655	★★★★☆	Today 12:06 PM Last Post: uzi94
 iHack (Pages: 1 2 3 4 ... last) Toxic Gangstar	41	495	★★★★☆	Today 11:55 AM Last Post: accountislocked
 The Wraith's back!!! (Pages: 1 2 3 4) Zammyslave	33	347	★★★★☆	Today 09:40 AM Last Post: i RaT YoU
 The Dark Side Co. - Recruitment OPEN AGAIN! (Pages: 1 2 3 4 ... last) ☺Yi n☺	346	4,524	★★★★☆	Today 09:29 AM Last Post: i RaT YoU
 [ETA] Recruiting White Hats ONLY [ETA] Dev//Null	7	103	★★★☆☆	Today 08:47 AM Last Post: Xon
 [Recruiting] The Wisemen (Pages: 1 2 3 4 ... last) [Comrade] Lucien Lachance	51	691	★★★★☆	Today 02:26 AM Last Post: Blacklisted™



BACtalk Alarm [?] [X]

From: Dev 201, Enroll 100 (Sterile Storage Humidity)
 Time: Friday, 12/19/2008 4:37:59PM
 Process I.D.: 131 (annunciate, log)
 State change: low limit -> normal
 Alarm message: Sterile Storage Humidity Normal
 Unit message: Sterile Storage Humidity

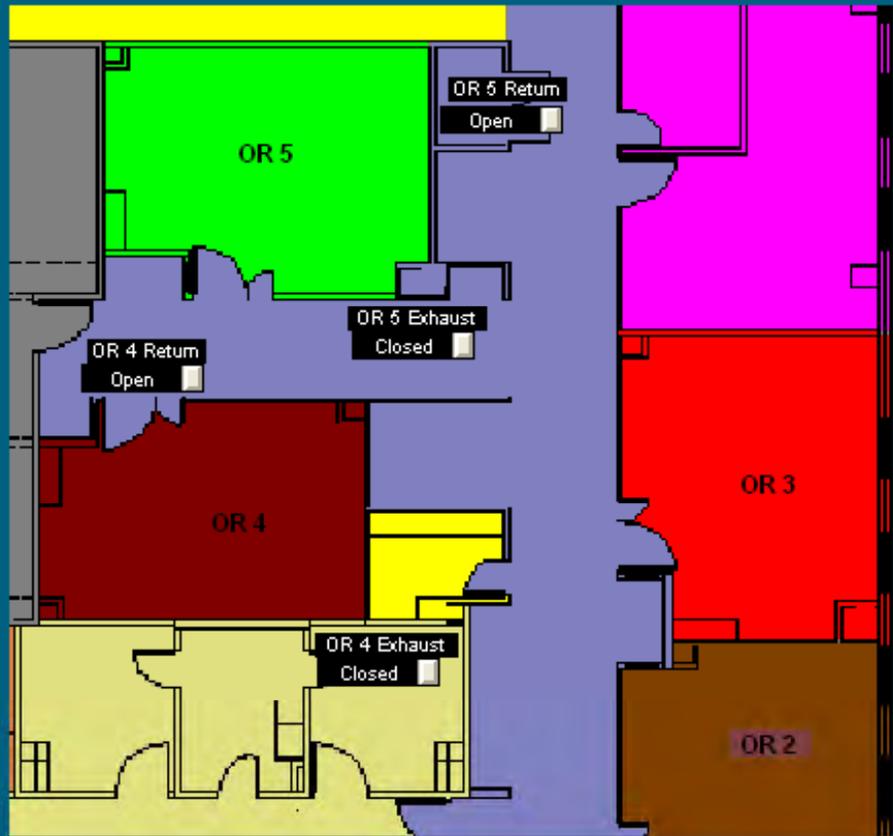


Acknowledge Acknowledge All Previous Next Options...



Previous

AHU 7 OR 4 Alarm	Normal
AHU 7 OR 5 Alarm	Normal
AHU 7 OA Alarm	Normal
AHU 4 OR Alarm	Normal
AHU 4 OA Alarm	Normal
AHU 7 RA Alarm	Normal
AHU 7 SA Alarm	Normal
AHU 4 RA Alarm	Normal
AHU 4 SA Alarm	Normal



SEF-1 Control	SEF-1 Status
Inactive	OFF
EF-1 Control	EF-1 Status
On	ON
EF-2 Control	EF-2 Status
On	ON

AHU 7 OA/RA Dampers
13.0 % Open

0% Open = O/A Closed _RA Open
100% Open = O/A Open _RA Closed

AHU 4 OA/RA Dampers
29.0 % Open

Envision for BACtalk - COHESIVE/CARRELL

BACtalk Edit View Tools Help



Previous



Surgery Freeze Protection Status	Off
Surgery Freeze Protection Setpoint	32.0
Surgery CHW Pump Ctrl	On
Surgery CHW Pump Status	Off
ChillerEnable	Enabled
UnitOFF	On
Surgery Chiller Setpoint	40.0
NetworkCoolTempSetpoint	40.0
ActiveLvgWaterTarget	40.0
LvgEvapWaterTempUnit	41.6
EntEvapWaterTemp	47.0
ChillerCapacity	38.6
AIWarningAlarm	0.0
AIProblemAlarm	33.0
AIFaultAlarm	0.0
AlarmDigitalOutput	Normal
ClearAlarm	Normal

Test Alarm Notification for Surgery Center

Inactive

Cohesive Automation, Inc.

GhostExodus

Ghost Exodus



Join Date: May 2009

Location: inside your source code

Posts: 37

Thanked: 5 times

Marketplace Tools

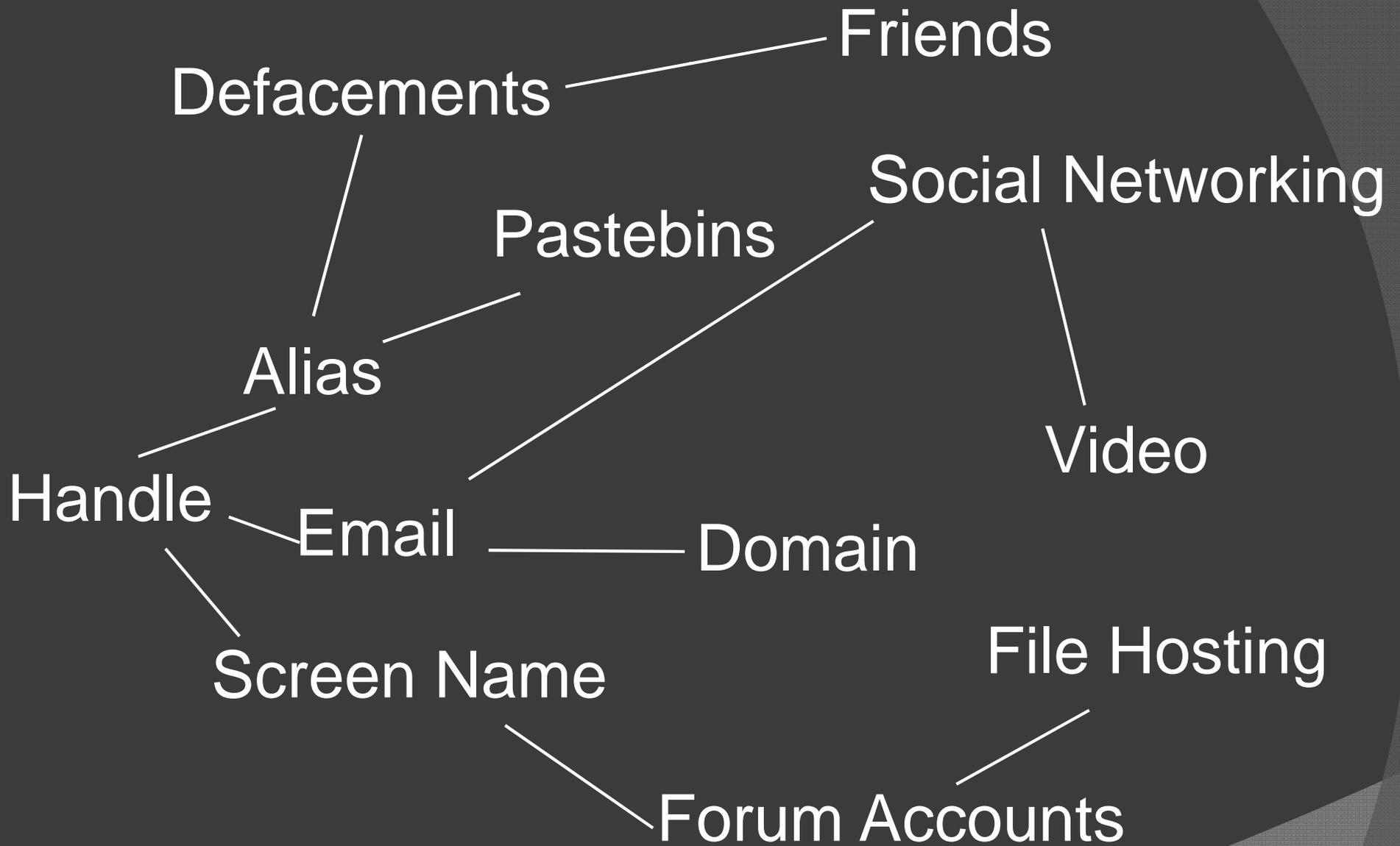
Trust Rating: (0) (Info)

HVAC Server Hacked! - 05-24-2009, 06:06 AM

Spreading botnets is boring. But sometimes you get a hefty prize for all your hard work and labor. Like this you see below. An HVAC server. An HVAC is: HVAC (pronounced either "H-V-A-C" or "H-vak") is an initialism or acronym that stands for "heating, ventlating, and air conditioning". HVAC is sometimes referred to as climate control and is particularly important in the design of medium to large industrial and office buildings such as skyscrapers and in marine environments yay for wiki

This image has been resized. Click this bar to view the full image. The original image is sized 1024x768.





“Post[sic] July 4th Infiltration”



Experienced Ethical Hacker/ PC Repair (Arlington)

Reply to: ghostexodus@gmail.com [Errors when replying to ads?]

Date: 2009-06-13, 4:17AM CDT

name and other contact information available upon request.

Objective: To invest my talents and skills in an area that others may benefit from them

April, 2007 - April 2008 Allied Baron Security Services Fortworth, TX

Security Officer

Responsibilities include the following: data entry, telephone etiquette, customer service, making copies, handling difficult situations, communicating with EMS and police.

April 2008 - May 2008 Triple D Armored Services Dallas, TX

Armored Car Driver

Daily interaction with customers, delivery, telephone etiquette, navigation, loading and unloading, auditing coin and cash.

October 2008 - present United Protective Services Dallas, TX

Customer service, telephone etiquette, monitoring and securing infrastructure, making copies, logging events.

please [flag](#) with care:

[miscategorized](#)

[prohibited](#)

[spam/overpost](#)

[best of craigslist](#)

- Called FBI and Texas DA's office on Monday
- FBI agent from Jackson drove up that afternoon to get the evidence
- Briefed agents on findings and notified them of new developments over the next few days
- Arrested as he arrived to work that Friday evening

4. There is probable cause to believe that **JESSE WILLIAM MCGRAW** has violated the provisions of 18 U.S.C. §1030(a)(5)(A) and §1030(c)(4)(B)(iv).

1030(a)(5)(A) Whoever . . . knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer..

1030(c)(4)(B)(i) the punishment for an offense under subsection (a) . . . of this section is - a fine under this title, imprisonment for not more than 10 years, or both, in the case of - an offense under subsection (a)(5)(A) which does not occur after a conviction for another offense under this section, if the offense cause . . . a harm provided in subclauses (I) through (VI) of subparagraph (A)(iv), [that being **(iv)**], a threat to public health or safety;

15. On 6/24/2009. SAs Lynd and Singh spoke to the apartment manager at **2801 TRINITY OAKS DR, ARLINGTON, TX, 76001**, who confirmed that **JESSE WILLIAM MCGRAW** lives in apartment 328 based on his lease and that he and his wife had two vehicles on the lease, including a Nissan Altima. The apartment manager also provided a floor plan of apartment 328 and a verbal description of the apartment. The apartment manager also stated there was a camera over the door of apartment 328. It is Affiant's experience that computer hackers who believe that they are under surveillance or in danger of being arrested use cameras to see who is at their doors in order to destroy evidence and / or flee if law enforcement or a rival hacker come to their residence. The manager stated that apartment 328 was in the first set of apartments on the right facing Trinity Oaks Drive and across the first breezeway and up one flight of stairs on the left side of the landing.

19. SA Singh was also told that a review of the HVAC computers had identified a malicious program on it which allowed unauthorized users to assume remote control of the system. Property management also noted that the HVAC system was continuing to experience problems, including a one hour outage of all five units controlled by the HVAC computer on 6/25/2009, which appeared to originate with the software controlling the HVAC system as none of the alarms which should have gone off did. They further noted that prior to the intrusion they have never experienced an incident where more than one or two units had problems at the same time.

Other Acts:

21. SAs Lynd and Singh also reviewed the documents provided by LT Hilbolt which CW-1 had collected. Included in these documents was what appeared to be a compromise of the City of Dallas computer system by ETA, **MCGRAW**'s hacker group. Based on the naming of this system it appeared to be a computer used by Dallas Police Department's

Page 16 of 18

Case 3:09-mj-00207-BD Document 1 Filed 06/26/2009 Page 18 of 19

(DPD) aviation unit. Detective Bill Cox, a DPD officer working with the FBI in a task force role, confirmed that the computer was an aviation unit computer located at or near Love Field and that it was already known by DPD to have been compromised by an unauthorized individual. Other documents indicated that **MCGRAW** had also compromised computers used by the National Aeronautic and Space Administration (NASA).

U.S. DISTRICT COURT
NORTHERN DISTRICT OF TEXAS
FILED

Jul 22 2009

CLERK, U.S. DISTRICT COURT

By [Signature]

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

UNITED STATES OF AMERICA

v.

JESSE WILLIAM MCGRAW (1)

3-09 CR-210-B

INDICTMENT

18 U.S.C. § 1030(a)(5)(A) and § 1030(c)(4)(B)(i)(II)
Transmitting a Malicious Code

18 U.S.C. 1030(a)(5)(A) and § 1030(c)(4)(B)(i)(II) and (IV)
Transmitting a Malicious Code

2 Counts

A true bill rendered:

[Signature]

DALLAS

FOREPERSON

Filed in open court this _____ day of _____, A.D. 2009.

Clerk

JESSE WILLIAM MCGRAW - In Custody (Seagoville)

UNITED STATES ~~DISTRICT~~ MAGISTRATE JUDGE

[Signature]
7/22/09

Criminal Complaint 3:09-MJ-207

Magistrate Case No. 3:09-207-MJ

View First Unread Thread Tools Search this Thread Rate Thread Display Modes

Yesterday, 01:35 PM

#21

system666 DH

Junior Member



Join Date: Jul 2009
Posts: 4
Thanks: 0
Thanked 0 Times in 0 Posts
Rep Power: 0



There was a lot more to it

Mcgraw I heard about me so I started to talk to him I wanted to get more information about him. I heard he had worked with the government and I wanted to get more information off of him.

so I released that picture to him not only that with the was already keeping a record on him. They were after him even before this had went down. Mcgraw just thinks hes leet cause he saw a couple of videos and told TX Genural Beuru Distric and special agent asheen whatever went into a full investigation against Ghost Exodus

If I would have known it would of went into this big of a mess I would not have done it I do feel bad for it as ghost exodus was a very good friend I called him 1 day before he got arrested .

He said to me William I need to stop this man because I have a wife and kids and I need to take care of them more than anything. It made me feel bad because deep down inside I knew the DOD was already coming for him but I kept that to myself just so I wouldnt ruin his day the next day later sadly enough ghost exodus went to jail

I never wanted this to happen and I wish I could go back in the future and change it.

Quote + Q. reply THANKS

Re: GhostExodus arrested bu the FBI [XXxxImmortalxxXX turned him into]

Yesterday, 01:37 PM

#22

site hacked

Rate This News 23 Views

Your [Security](#) Has Been Breached By Wesley Mcgrew If you Want Me To Fix This Issue
[contact Me](http://www.mcgrewsecurity.com) At <http://www.mcgrewsecurity.com>

Rate This News 23 Views

HackServer.org > Hacking > Hacked Sites
mcgrew a hacker?

Post Reply

View First Unread

Thread Tools

Display Modes

Today, 07:00 PM

#1

MR^E Offline
Senior Member

Join Date: Sep 2009
Location: new zealand
Posts: 144



mcgrew a hacker?

<http://www.realtyverticals.com/NewsView.php?id=2600>

<http://www.danasoft.com/sig/MRE395154.jpg>

Quote

kingwifu

From: wesleymcgrew

<http://www.submedia.tv/>
stop servin your masters and join the resistance mcgrew

5:31 Tuesday, October 27, 2009

kingwifu 5:31
u [redacted]

6:10 Wednesday, November 4, 2009

kingwifu 6:10
[redacted]

10:16 Thursday, November 5, 2009

kingwifu 10:16
hey thar why u no answer your ims?
strap on your seatbelt and prepare for turbulance

kingwifu

Take-away

- ⦿ Low skill can lead to heavy consequences
- ⦿ Human-Machine Interface security
- ⦿ Physical security
 - Recommendations
- ⦿ Taking action on serious incidents that present themselves

Questions, Discussion