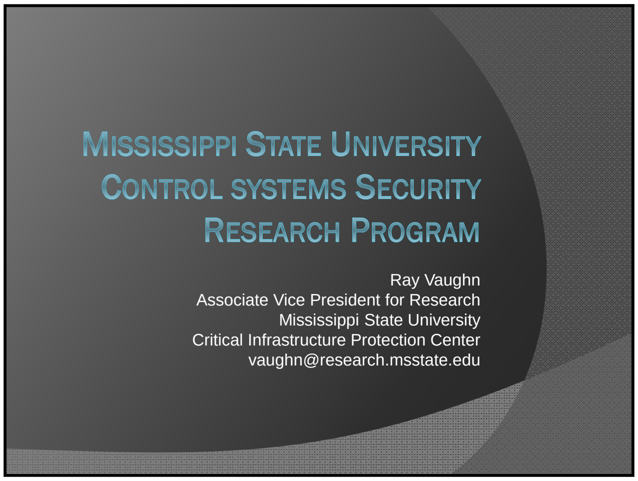
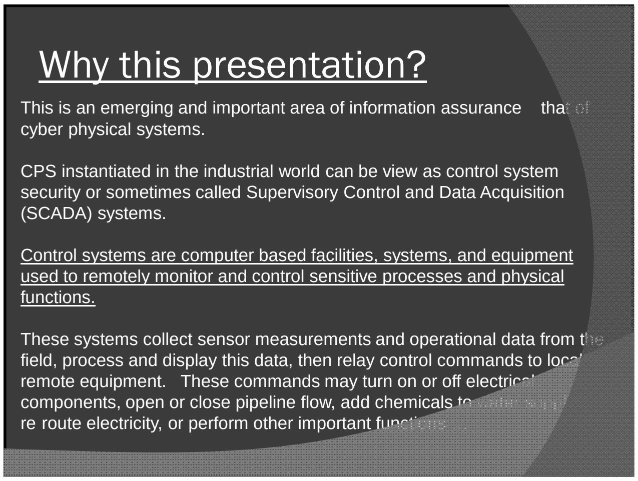


Mississippi State University Control systems Security Research Program

Ray Vaughn
Associate Vice President for Research
Mississippi State University
Critical Infrastructure Protection Center
vaughn@research.msstate.edu



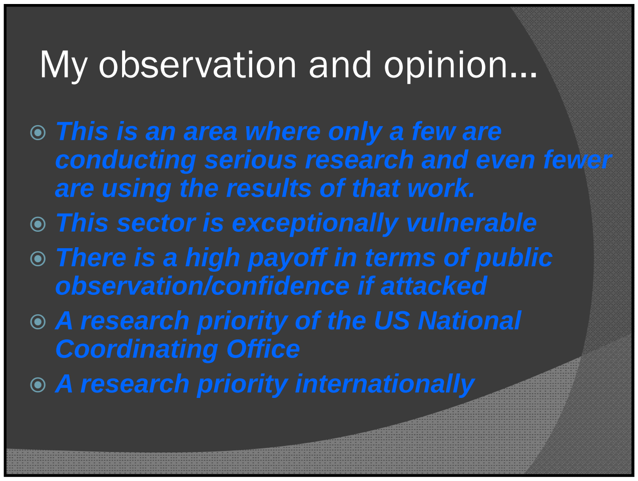
Why this presentation?

This is an emerging and important area of information assurance that of cyber physical systems.

CPS instantiated in the industrial world can be view as control system security or sometimes called Supervisory Control and Data Acquisition (SCADA) systems.

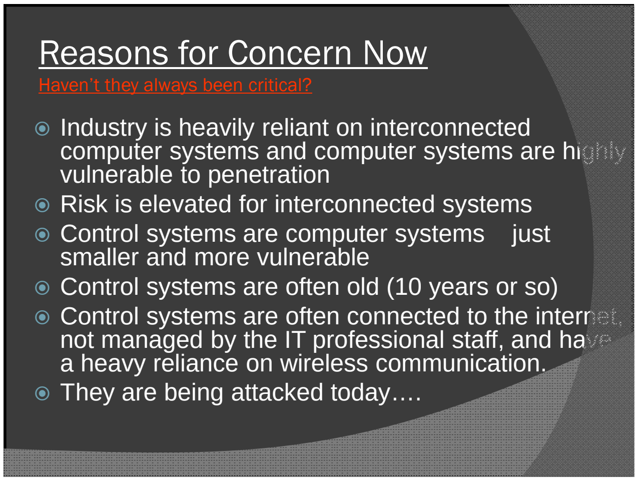
Control systems are computer based facilities, systems, and equipment used to remotely monitor and control sensitive processes and physical functions.

These systems collect sensor measurements and operational data from the field, process and display this data, then relay control commands to local remote equipment. These commands may turn on or off electrical components, open or close pipeline flow, add chemicals to water supply, re route electricity, or perform other important functions.



My observation and opinion…

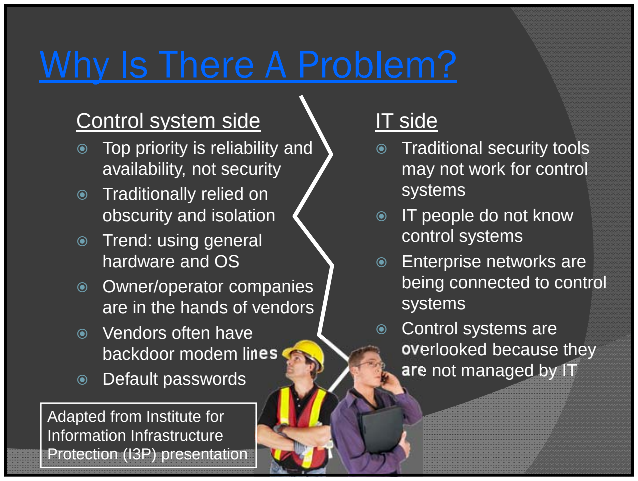
- ***This is an area where only a few are conducting serious research and even fewer are using the results of that work.***
- ***This sector is exceptionally vulnerable***
- ***There is a high payoff in terms of public observation/confidence if attacked***
- ***A research priority of the US National Coordinating Office***
- ***A research priority internationally***



Reasons for Concern Now

Haven't they always been critical?

- Industry is heavily reliant on interconnected computer systems and computer systems are highly vulnerable to penetration
- Risk is elevated for interconnected systems
- Control systems are computer systems just smaller and more vulnerable
- Control systems are often old (10 years or so)
- Control systems are often connected to the internet, not managed by the IT professional staff, and have a heavy reliance on wireless communication.
- They are being attacked today….



Why Is There A Problem?

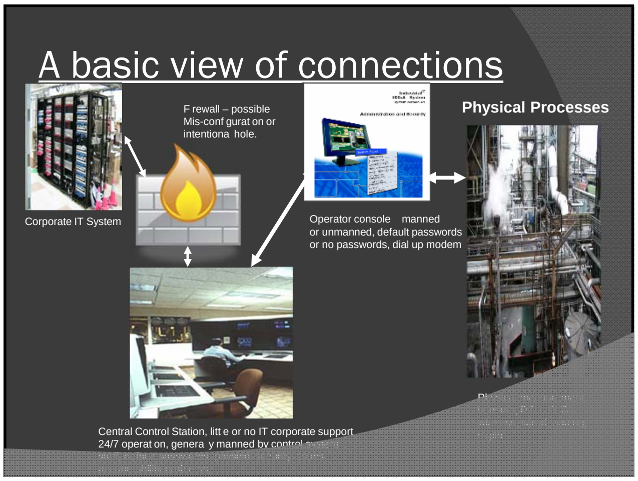
Control system side

- Top priority is reliability and availability, not security
- Traditionally relied on obscurity and isolation
- Trend: using general hardware and OS
- Owner/operator companies are in the hands of vendors
- Vendors often have backdoor modem lines
- Default passwords

IT side

- Traditional security tools may not work for control systems
- IT people do not know control systems
- Enterprise networks are being connected to control systems
- Control systems are overlooked because they are not managed by IT

Adapted from Institute for Information Infrastructure Protection (I3P) presentation



A basic view of connections

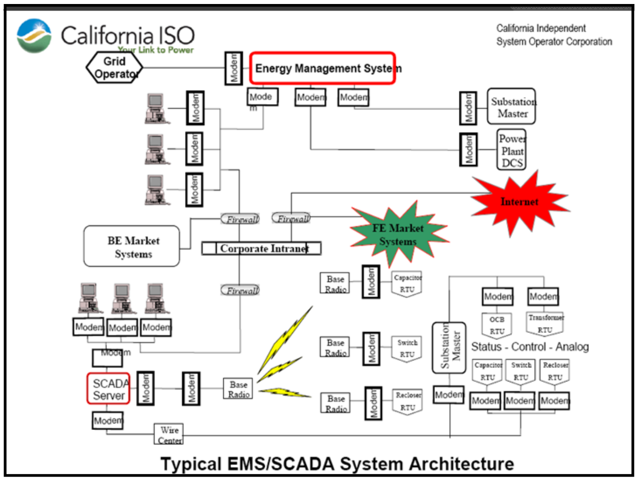
Corporate IT System

F rewall – possible Mis-conf gurat on or intentiona hole.

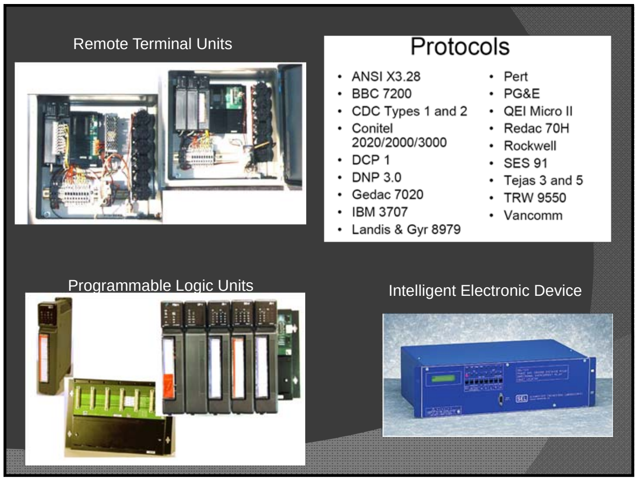
Operator console manned or unmanned, default passwords or no passwords, dial up modem

Physical Processes

Central Control Station, litt e or no IT corporate support 24/7 operat on, genera y manned by control [illegible]



Typical EMS/SCADA System Architecture



Remote Terminal Units

Protocols

- ANSI X3.28
- BBC 7200
- CDC Types 1 and 2
- Conitel 2020/2000/3000
- DCP 1
- DNP 3.0
- Gedac 7020
- IBM 3707
- Landis & Gyr 8979
- Pert
- PG&E
- QEI Micro II
- Redac 70H
- Rockwell
- SES 91
- Tejas 3 and 5
- TRW 9550
- Vancomm

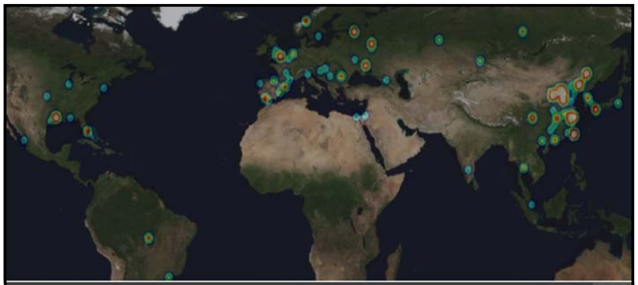
Programmable Logic Units

Intelligent Electronic Device

Things that concern us

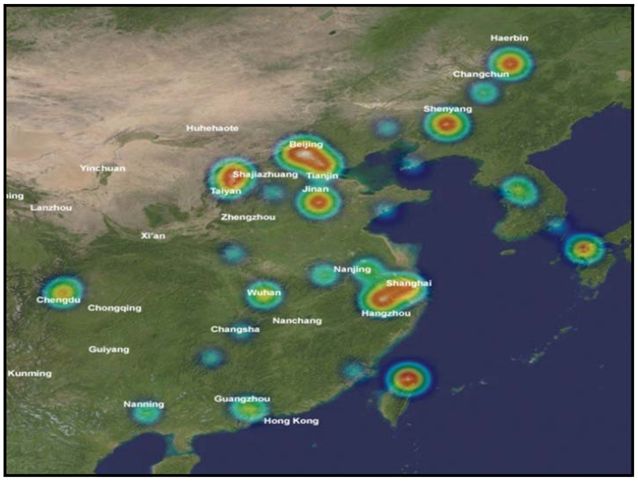
- Data is sent in clear text [redacted]
- Heavy use of wireless
- Protocols are not
- Data can be ch eated
- Connection e networks
- Unpatc improperly confi e, inadequate ph tion….

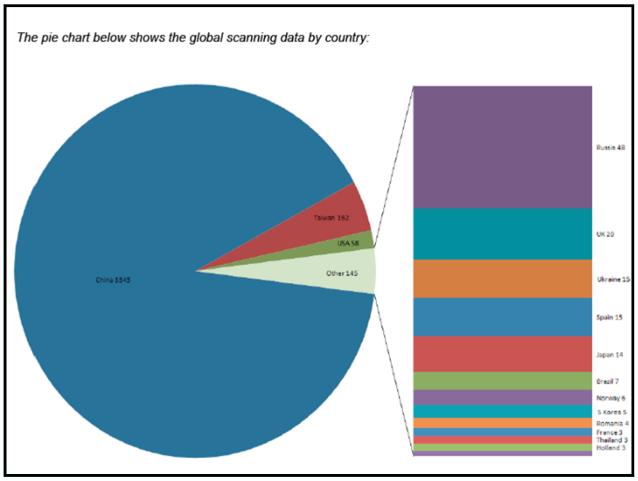
SIGNE
NUCLEAR WEAPONS ARE UNNECESSARY!
hack hack hack
hackety hack
WESTERN BANKS
U.S. POWER GRIDS
PENTAGON



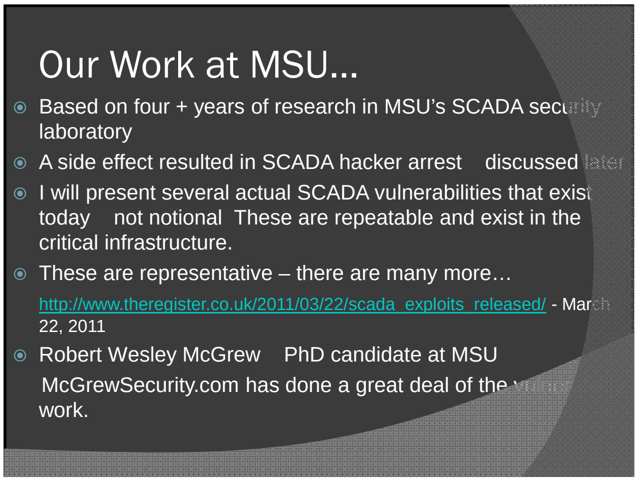
Who is looking for your SCADA infrastructure?

TEAM CYMRU





The pie chart below shows the global scanning data by country:

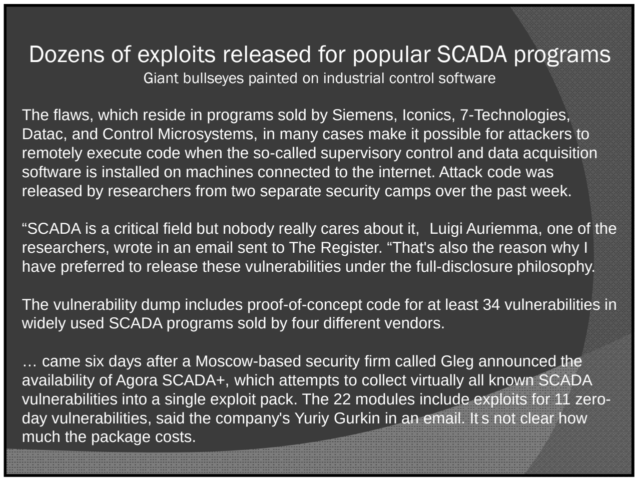


Our Work at MSU…

- Based on four + years of research in MSU's SCADA security laboratory
- A side effect resulted in SCADA hacker arrest discussed later
- I will present several actual SCADA vulnerabilities that exist today not notional These are repeatable and exist in the critical infrastructure.
- These are representative – there are many more…

  http://www.theregister.co.uk/2011/03/22/scada_exploits_released/ - March 22, 2011
- Robert Wesley McGrew PhD candidate at MSU

  McGrewSecurity.com has done a great deal of the vulner work.



Dozens of exploits released for popular SCADA programs

Giant bullseyes painted on industrial control software

The flaws, which reside in programs sold by Siemens, Iconics, 7-Technologies, Datac, and Control Microsystems, in many cases make it possible for attackers to remotely execute code when the so-called supervisory control and data acquisition software is installed on machines connected to the internet. Attack code was released by researchers from two separate security camps over the past week.

"SCADA is a critical field but nobody really cares about it, Luigi Auriemma, one of the researchers, wrote in an email sent to The Register. "That's also the reason why I have preferred to release these vulnerabilities under the full-disclosure philosophy.

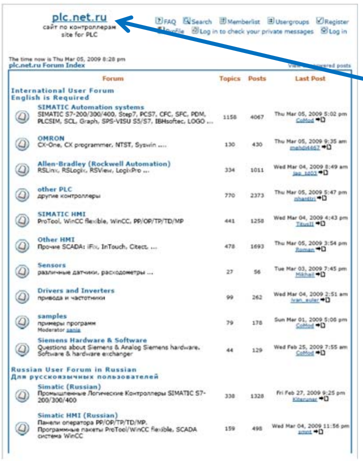
The vulnerability dump includes proof-of-concept code for at least 34 vulnerabilities in widely used SCADA programs sold by four different vendors.

… came six days after a Moscow-based security firm called Gleg announced the availability of Agora SCADA+, which attempts to collect virtually all known SCADA vulnerabilities into a single exploit pack. The 22 modules include exploits for 11 zero-day vulnerabilities, said the company's Yuriy Gurkin in an email. It s not clear how much the package costs.

SCADA Security Lab

Vulnerabilities in HMI Software

- GE Fanuc Proficy iFIX 4.5/5.0
- Insecure storage of passwords
- Authentication bypass
- Allows those with access to escalate privileges on the SCADA system
  - Lower-level personnel with physical access
  - Remote attackers with access via other/mainstream exploits



plc.net.ru
сайт по контроллерам
site for PLC

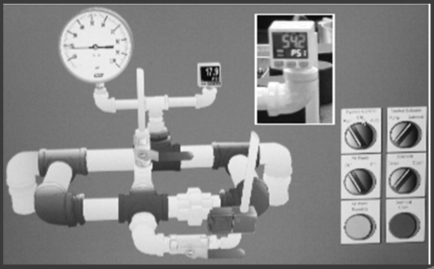
The time now is Thu Mar 05, 2009 8:28 pm
plc.net.ru Forum Index

Forum	Topics	Posts	Last Post
International User Forum English is Required			
SIMATIC Automation systems SIMATIC S7-200/300/400, Step7, PCS7, CFC, SFC, PDM, PLCSIM, SCL, Graph, SPS-VISU S5/S7, IBHsoftec, LOGO ...	1158	4067	Thu Mar 05, 2009 5:02 pm CoMod
OMRON CX-One, CX programmer, NTST, Syswin	130	430	Thu Mar 05, 2009 9:35 am mehdi4467
Allen-Bradley (Rockwell Automation) RSLinx, RSLogix, RSView, LogixPro ...	334	1011	Wed Mar 04, 2009 8:49 am jan_1603
other PLC другие контроллеры	770	2373	Thu Mar 05, 2009 5:47 pm nhanttri
SIMATIC HMI ProTool, WinCC flexible, WinCC, PP/OP/TP/TD/MP	441	1258	Wed Mar 04, 2009 4:43 pm Titus11
Other HMI Прочие SCADA: iFix, InTouch, Citect, ...	478	1693	Thu Mar 05, 2009 3:54 pm Roman
Sensors различные датчики, расходометры ...	27	56	Tue Mar 03, 2009 7:45 pm Mikhail
Drivers and Inverters привода и частотники	99	262	Wed Mar 04, 2009 2:51 am ivan_euler
samples примеры программ Moderator sania	79	178	Sun Mar 01, 2009 5:06 pm CoMod
Siemens Hardware & Software Questions about Siemens & Analog Siemens hardware, Software & hardware exchanger	44	129	Wed Feb 25, 2009 7:55 am CoMod
Russian User Forum in Russian Для русскоязычных пользователей			
Simatic (Russian) Промышленные Логические Контроллеры SIMATIC S7-200/300/400	338	1328	Fri Feb 27, 2009 9:25 pm Kitaruner
Simatic HMI (Russian) Панели оператора PP/OP/TP/TD/MP. Программные пакеты ProTool/WinCC flexible, SCADA система WinCC	159	498	Wed Mar 04, 2009 11:56 pm smmt

http://plcforum.uz.ua/

Sample Site where control system code is available and cracks are shared.

Denial of Service



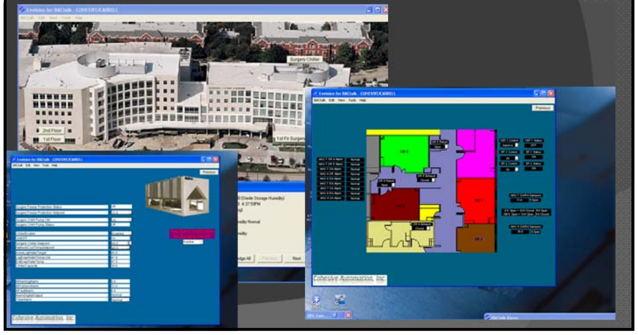
An Actual Takedown

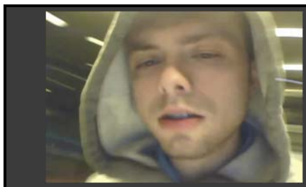
Tracking and Trapping a Hacker

Wesley McGrew & Ray Vaughn
Mississippi State University
Critical Infrastructure Protection Center

Real-World HMI Security Incident

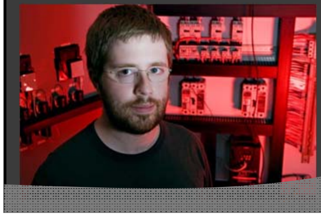
Texas Hospital Control System Incident – late June to early July 2009



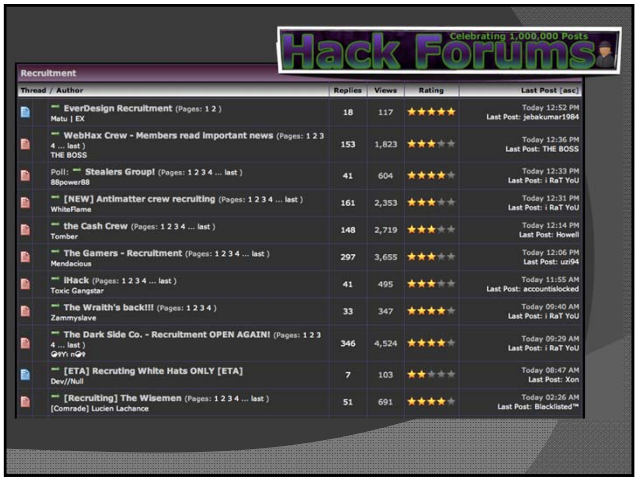


Evidence of criminal activity scattered around the internet (YouTube, Myspace, Forums, etc.)

Plans were made for a 4th of July coordinated DDOS attack by the ETA

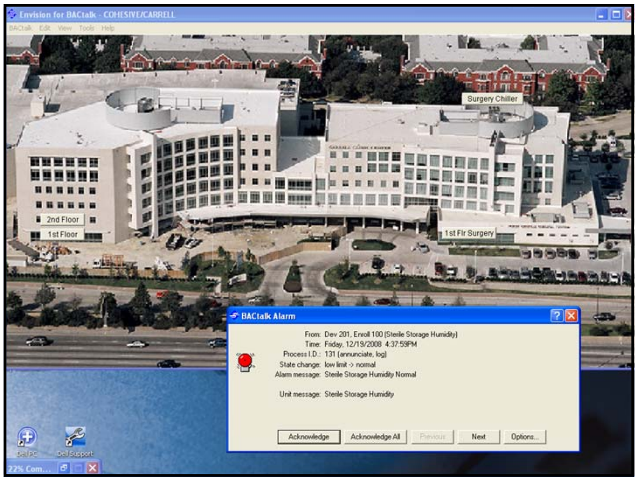


Suspect arrested by the FBI a week before the planned attacks, with evidence gathered by and analyzed at the MSU CIPC



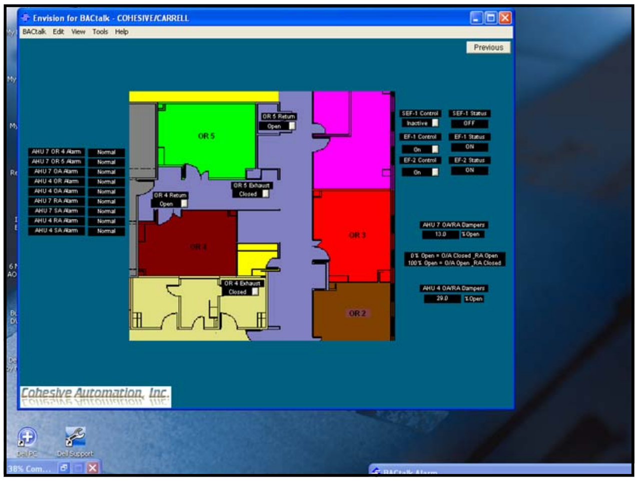
Recruitment

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) [illegible]	346	4,524	★★★★☆	Today 09:29 AM Last Post: i RaT YoU
[ETA] Recruting 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™



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


Envision for BACtalk - COHESIVE/CARRELL
BACtalk Edit View Tools Help
Previous
OR 5
OR 4
OR 3
OR 2
Cohesive Automation, Inc.
Dell PC
Dell Support
38% Com...
BACtalk Alarm

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

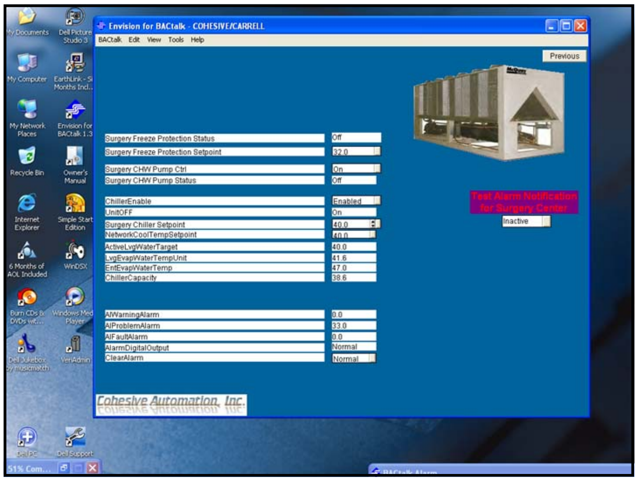
OR 5 Return: Open
OR 5 Exhaust: Closed
OR 4 Return: Open
OR 4 Exhaust: Closed

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

AHU 7 OA/RA Dampers: 13.0 %Open

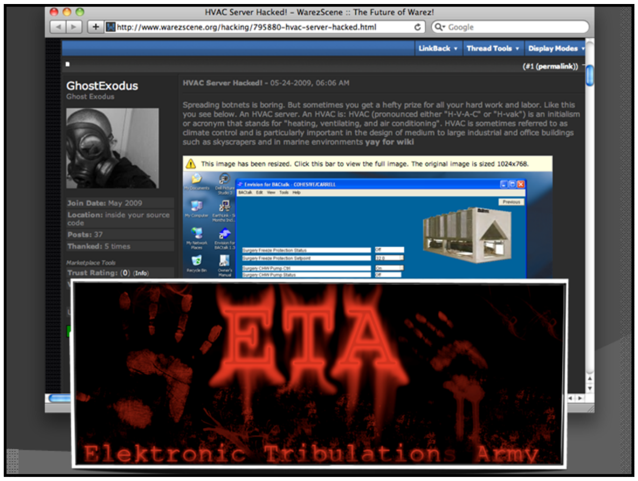
0% Open = O/A Closed _RA Open
100% Open = O/A Open _RA Closed

AHU 4 OA/RA Dampers: 29.0 %Open



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


HVAC Server Hacked! – WarezScene :: The Future of Warez!
http://www.warezscene.org/hacking/795880-hvac-server-hacked.html
Google
LinkBack
Thread Tools
Display Modes
(#1 (permalink))
ETA
Elektronic Tribulation Army

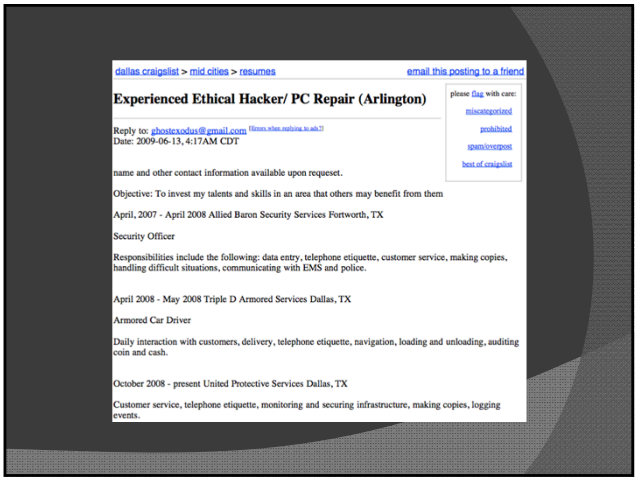
GhostExodus
Ghost Exodus

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, ventilating, 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.


dallas craigslist > mid cities > resumes   email this posting to a friend

Experienced Ethical Hacker/ PC Repair (Arlington)

please flag with care:
miscategorized
prohibited
spam/overpost
best of craigslist

Reply to: ghostexodus@gmail.com [Errors when replying to ads?]
Date: 2009-06-13, 4:17AM CDT

name and other contact information available upon requeset.

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

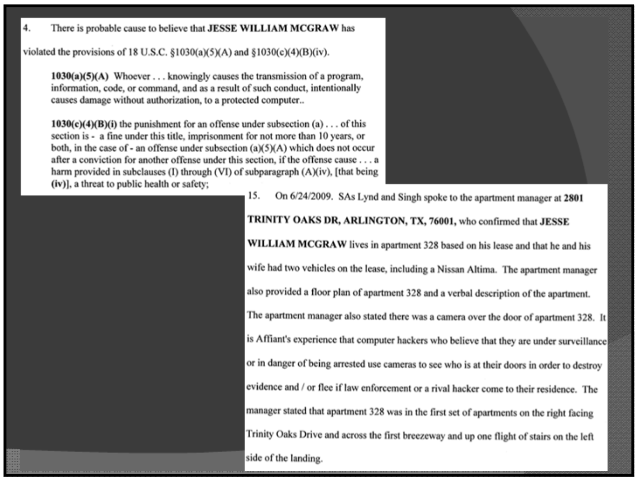
Armored Car Driver

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.

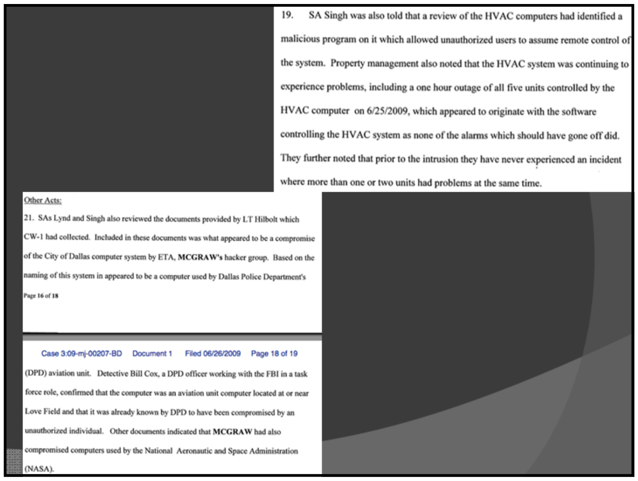
- Called FBI and Texas DA’s office on Monday
- FBI agent from Jackson drove up that afternoon to get the evidence
- Briefed agents on findings and notified them of new developments over the next few days
- Arrested as he arrived to work that Friday evening



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:

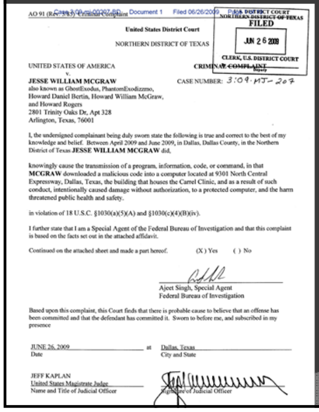
21. SAs Lynd and Singh also reviewed the documents provided by LT Hilbolt which CW-1 had collected. Included in these documents was what appeared to be a compromise of the City of Dallas computer system by ETA, **MCGRAW's** hacker group. Based on the naming of this system in appeared to be a computer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

Arrest and Indictment



AO 91 (Rev. 5/85) Criminal Complaint Case 3:09-mj-00207-BD Document 1 Filed 06/26/2009 Page 1 of 19

U.S. DISTRICT COURT
NORTHERN DISTRICT OF TEXAS
FILED
JUN 26 2009
CLERK, U.S. DISTRICT COURT
By Deputy

United States District Court

NORTHERN DISTRICT OF TEXAS

UNITED STATES OF AMERICA
v.
JESSE WILLIAM MCGRAW
also known as GhostExodus, PhantomExodizzmo,
Howard Daniel Bertin, Howard William McGraw,
and Howard Rogers
2801 Trinity Oaks Dr, Apt 328
Arlington, Texas, 76001

CRIMINAL COMPLAINT

CASE NUMBER: 3:09-MJ-207

I, the undersigned complainant being duly sworn state the following is true and correct to the best of my knowledge and belief. Between April 2009 and June 2009, in Dallas, Dallas County, in the Northern District of Texas **JESSE WILLIAM MCGRAW** did,

knowingly cause the transmission of a program, information, code, or command, in that **MCGRAW** downloaded a malicious code into a computer located at 9301 North Central Expressway, Dallas, Texas, the building that houses the Carrel Clinic, and as a result of such conduct, intentionally caused damage without authorization, to a protected computer, and the harm threatened public health and safety.

in violation of 18 U.S.C. §1030(a)(5)(A) and §1030(c)(4)(B)(iv).

I further state that I am a Special Agent of the Federal Bureau of Investigation and that this complaint is based on the facts set out in the attached affidavit.

Continued on the attached sheet and made a part hereof. (X) Yes ( ) No

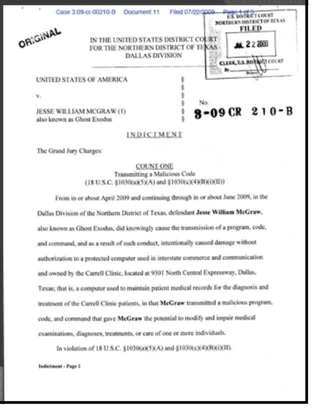
Ajeet Singh, Special Agent
Federal Bureau of Investigation

Based upon this complaint, this Court finds that there is probable cause to believe that an offense has been committed and that the defendant has committed it. Sworn to before me, and subscribed in my presence

JUNE 26, 2009 at Dallas, Texas
Date City and State

JEFF KAPLAN
United States Magistrate Judge
Name and Title of Judicial Officer

Signature of Judicial Officer



Case 3:09-cr-00210-B Document 11 Filed 07/22/2009 Page 1 of 5

ORIGINAL

U.S. DISTRICT COURT
NORTHERN DISTRICT OF TEXAS
FILED
JUL 22 2009
CLERK, U.S. DISTRICT COURT
By Deputy

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

UNITED STATES OF AMERICA §
§
v. §
§ No.
JESSE WILLIAM MCGRAW (1) § **3-09 CR 210-B**
also known as Ghost Exodus §

INDICTMENT

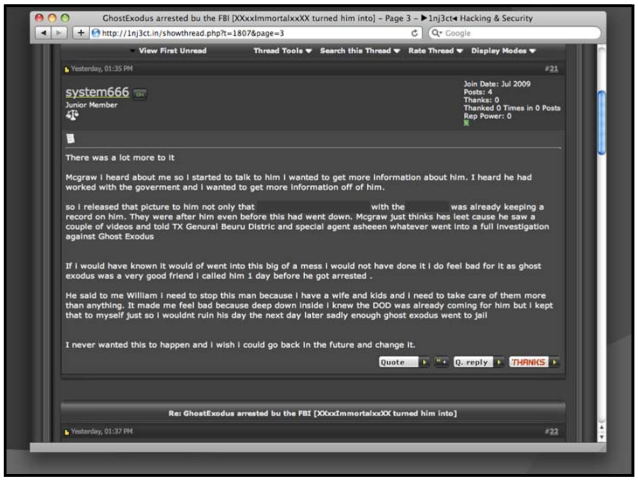
The Grand Jury Charges:

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

From in or about April 2009 and continuing through in or about June 2009, in the Dallas Division of the Northern District of Texas, defendant **Jesse William McGraw**, also known as Ghost Exodus, did knowingly cause the transmission of a program, code, and command, and as a result of such conduct, intentionally caused damage without authorization to a protected computer used in interstate commerce and communication and owned by the Carrell Clinic, located at 9301 North Central Expressway, Dallas, Texas; that is, a computer used to maintain patient medical records for the diagnosis and treatment of the Carrell Clinic patients, in that **McGraw** transmitted a malicious program, code, and command that gave **McGraw** the potential to modify and impair medical examinations, diagnoses, treatments, or care of one or more individuals.

In violation of 18 U.S.C. §1030(a)(5)(A) and §1030(c)(4)(B)(i)(II).

Indictment - Page 1



GhostExodus arrested bu the FBI [XXxxImmortalxxXX turned him into] - Page 3 - ▶1nj3ct◀ Hacking & Security

http://1nj3ct.in/showthread.php?t=1807&page=3

Yesterday, 01:35 PM #21

system666
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 goverment and i wanted to get more information off of him.

so i released that picture to him not only that [redacted] with the [redacted] 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 asheeen whatever went into a full investigation against Ghost Exodus

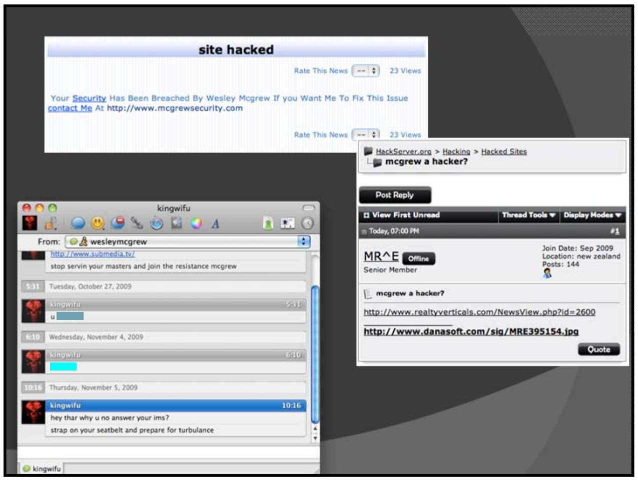
If i would have known it would of went into this big of a mess i would not have done it i do feel bad for it as ghost exodus was a very good friend i called him 1 day before he got arrested .

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.

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 At http://www.mcgrewsecurity.com

Rate This News -- 23 Views

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

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

Today, 07:00 PM #1

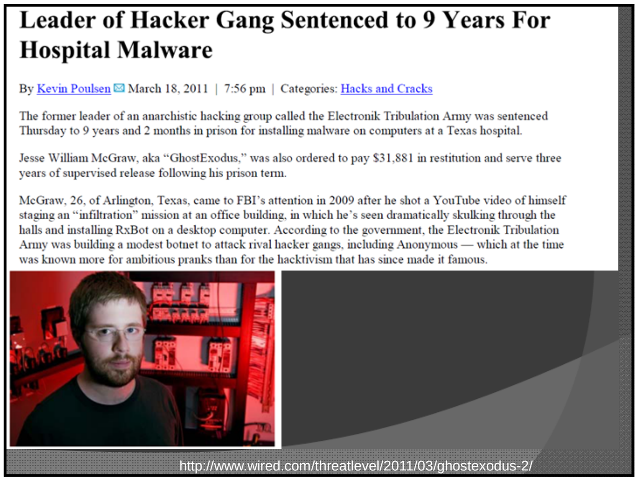
MR^E Offline
Senior Member

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



Leader of Hacker Gang Sentenced to 9 Years For Hospital Malware

By Kevin Poulsen ✉ March 18, 2011 | 7:56 pm | Categories: Hacks and Cracks

The former leader of an anarchistic hacking group called the Electronik Tribulation Army was sentenced Thursday to 9 years and 2 months in prison for installing malware on computers at a Texas hospital.

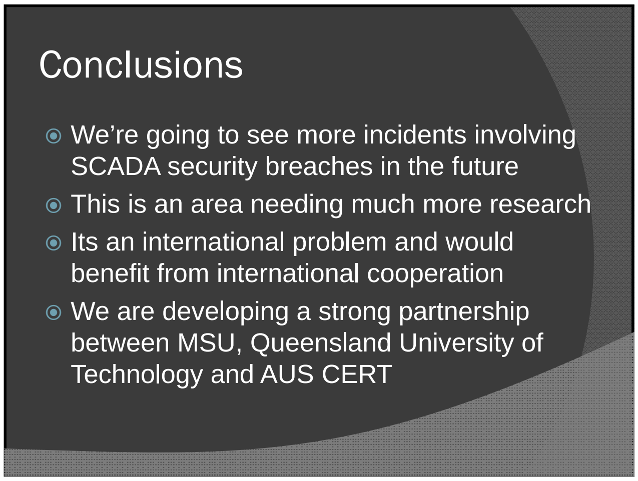
Jesse William McGraw, aka "GhostExodus," was also ordered to pay $31,881 in restitution and serve three years of supervised release following his prison term.

McGraw, 26, of Arlington, Texas, came to FBI's attention in 2009 after he shot a YouTube video of himself staging an "infiltration" mission at an office building, in which he's seen dramatically skulking through the halls and installing RxBot on a desktop computer. According to the government, the Electronik Tribulation Army was building a modest botnet to attack rival hacker gangs, including Anonymous — which at the time was known more for ambitious pranks than for the hacktivism that has since made it famous.

http://www.wired.com/threatlevel/2011/03/ghostexodus-2/

Take-away

- Low skill can lead to heavy consequences in SCADA attacks
- Human-Machine Interface security is important and flawed today
- Physical security can be the Achilles heal
- Taking action on serious incidents that present themselves is important
- Vendors of SCADA hardware and software need to consider security during the design phase



Conclusions

- We’re going to see more incidents involving SCADA security breaches in the future
- This is an area needing much more research
- Its an international problem and would benefit from international cooperation
- We are developing a strong partnership between MSU, Queensland University of Technology and AUS CERT