Advanced Persistent Threat: Evolution of the attacker

Joe Cummins, PCIP  
Founder, Principal Consultant  
Red Tiger Security – Canada

Jonathan Pollet, CAP, CISSP, PCIP  
Founder, Principal Consultant  
Red Tiger Security - USA
Presenter

- Joe Cummins, PCIP
  - Canadian Information Security practitioner
  - President and Principal Consultant of Red Tiger Security - Canada,
  - Provision of Threat and Vulnerability Assessments
  - SME in the areas of:
    - Critical Infrastructure,
    - Federal Readiness
- Speaker:
  - IEEE Boston, Mass
  - Canadian CIP Symposium
  - ISA Expo, Houston
  - SANS USA, SANS EURO
Jonathan Pollet – CISSP, PCIP, CAE

- 12 Years of Electrical Engineering, SCADA, Industrial Controls, and IT Experience
  - PLC Programming and SCADA System Design and Commissioning
  - Wireless RF and Telecommunications Design and Startup
  - Front-end Web Development for SCADA data
  - Backend Database design for SCADA data
  - Acting CIO for Seneca Oil Company for 2 years – Enterprise IT Management

- Last 8 Years Focused on SCADA and IT Security
  - Published White Papers on SCADA Security early in 2001
  - Focused research and standards development for SCADA Security since 2002
  - Conducted over 100 security assessments on Critical Infrastructure systems
  - Co-founded Critical Infrastructure Institute in 2004 and the PCIP certification
  - Developed security assessment methodology for SCADA Systems
APT - Overview

- Summary / Synopsis – Advanced Persistent Threat
- Anatomy
- Timeline – Threat Vector Evolution
- Tools – Malware, Bots
- Techniques – OSINT, Phishing
- Targets - Enterprise
- Case Studies
  - Project Aurora
  - Ghost Net
  - Georgia v. Russia
- Solutions / Safeguards
- Relevance to Pipeline Attack
- Horizon
Anatomy of APT

Signature and style of the evolved attack
APT - Anatomy

• Advanced:
  • Taking advantage of latest techniques
  • Application Stack
  • Protocols
  • Embedded Device Fuzzing

• Persistent
  • Intent dedication
  • Focused pattern
  • Patient / Latent ability

• Threat
  • Signatures
  • Vectors
APT - Signature

- Shift from enterprise (broad) scale attacks
- Focus on the dissection / comprehension of the Infrastructure
- Examination of the Corporate Infrastructure
- Pre-determined target / group
- Relentless approach
- Layered Focus
- Exfiltration of Data
Attack Timeline
Evolution of the Attacker
APT - Timeline of Attack

1970 - 1995 (Hackerz)

1995 - 2000 (Hobbyist Hacking)

2001 - 2005 (Hactivism)

2005 - 2009 (Hacker for Hire)

2009+
Evolution of the Attack

  - Objective:
    - Gain “unauthorized” Access
    - Usurp Control
    - Bypass common methods of control
  - Leveraging
    - Password Guessing
    - Early Trojans/viruses
    - Misconfigured networks
    - “Phreaking”
Evolution of the Attack

  • **Objective:**
    • Learn, exploration, Discovery
    • Exposure of flaws, weaknesses, poor workmanship
    • Defacement
    • Disruption
  • **Leveraging**
    • Email viruses,
    • BO2K
    • Early web attacks
Evolution of the Attack

  • Objective:
    • Capture Media attention
    • Publicity
    • Denial of Service
  
• Leveraging
  • Attracting attention through large-scale activities.
  • Motivation publicity and money
  • Methods: DoS, worms, rootkits, etc..
Evolution of the Attack

• “Hacker for hire” (2005 - 2009)
  • Objectives:
    • Identity theft
    • Information egress
    • DDOS
    • Financially motivated

• Leveraging:
  • Phishing/pharming
  • Targeted Spear-phishing
  • Redirected patching / AV
  • Bots / Botnets
Attack Landscape

Posture and Motivation of APT
APT - Defense / Threat Postures

Blue (Defender)
- Exposed
  - Information
  - Marketing
- Sluggish
  - Slow to adopt change
- Constrained
  - Underfunded
  - Personnel
  - Education

Red (Attacker)
- Agile
  - More than one target
  - More than one vector
- Mobile
  - Change in Strategy
  - Change in Tactics
- Hostile
  - Ruthless
  - Creative
  - Relentless
APT - Intentions

• DATA >> Competitiveness
  • Formulas,
  • Designs,
  • Schematics

• Information >> Knowledge
  • Agenda’s,
  • Itinerary,
  • Corporate Direction,
  • Mergers,
  • Acquisitions

• Advantage is the motivation
APT - Threat Vectors

External

- Internet
  - Email attachments
  - File sharing
  - Pirated Software
  - Spearphishing
  - DNS / Routing Modifications

- Physical
  - Infections of Media (USB, CD)
  - Infected Appliances
  - Malicious IT equipment

- External
  - Mass Vulnerability Exploits
  - Co-location Exploitation
  - Rogue Wifi AP

Internal

- Trusted Insider
  - Rogue Employee
  - Subcontractors
  - SOC-ENG
  - Break-In
  - Dual Use software

- Trusted Channel
  - Stolen VPN Credentials
  - Hijacked Cell Communications
  - P2P tapping
  - 3rd party breach
  - Un-trusted Devices
APT - Threat Vectors

- **Malware / Worms**
  - 2009 May – July
  - 1335 Unique variants and infections
    - Inclu. Conficker Worm / Conficker A, B, C, D and E
    - Malicious AV Advertisements/Products
    - Segmentation of the Network (ITSG-ITSB)

- **Mobile Devices**
  - USB drives
    - U3 Devices
  - Stolen or lost Laptops

- **Insecure Builds**
  - Devices that are mis-configured / unpatched before activation
APT - Threat Vectors (Con't)

• Information leakage
  • Exposure of sensitive media / material online
  • Small / Irrelevant

• Application Security
  • Fuzzing / Reverse Engineering
  • Overflows, Cross Site Scripting,

• Social Engineering
  • Spear phishing
  • Social Engineering Toolkit (SET) Framework
APT - Tools

- Open Sourced Information
- Search Aggregators
- Malware:
  - Botnets
  - Crimeware
  - Rootkits
  - Malicious Attachments
- Live DVD – Distributions
  - Backtrack
  - A.P.E.
APT - Overcoming Traditional Safeguards

• Anti-Virus
  • Signatures being obfuscated
  • Covert De-activation

• Patching
  • Servers being redirected
  • Popups

• Firewalls
  • Malicious attachments creating holes
  • USB devices circumvention
Symbiotic Progression

Cyber Crime

Cyber Espionage

Internet Web 0.0
Don’t take my word for it...

• **General Keith Alexander**
  - Head, US Cyber Command
  - On Operation Buckshot Yankee
  - "probed by unauthorized users approximately 250,000 times an hour, over six million times a day."

• **Richard A. Clark**
  - "It is the public, the civilian population of the United States and the publicly owned corporations that run our key national systems, that are likely to suffer in a cyber war."
• William J. Lynn III,
  • Deputy Secretary of Defense
  • "Computer-induced failures of U.S. power grids, transportation networks, or financial systems could cause massive physical damage and economic disruption"

• Jonathan Evans
  • Head MI-5
  • Both traditional and cyber espionage continue to pose a threat to British interests, with the commercial sector very much in the front line along with more traditional diplomatic and defence interests
Tools and Tradecraft

Skills and Methodology used in Construction of the APT
APT – Techniques / Tradecraft

• OSINT
• Social Engineering
• Targeted “Spear Phishing”
• Malicious Attachments
• USB devices
• Websites
Social Engineering

• Attack the 8th (Human) Level
• Contextual
• Implied / Explicit
• Leverages social interaction
• Forms emotional exchange
  • Anger
  • Surprise
  • Anticipation

• “Robyn Sage” Experiment
Targeted Spear Phishing

- Require in-depth knowledge of target
- Sophistication based on posted / known information
- Used to leverage people / groups
Malicious Attachments (Malware)

- **PDF**

- **MS Products**
  - Word, Excel, etc...

- **The usual suffixes**...
  - mp3, exe, lnk, dll, mov, com, mp4, bat, cmd, reg, rar, emf, shs, js, vb, yourcompany.com.zip, cab, mda, zip, mdb, scr, aiff, mde, cpl, msi, vbs, aif, m4p, msp, fdf, mdt, sys, wmf, hlp, hta, pif, jse, qef, scf, chm, <#>.txt, wsf, fli, vbe
APT – Targeted Attacks (2009)

Malware (Con’t)

General Attacks

- Malware: 66.8%
- Other: 11.8%
- Phishing: 7.7%
- Physical Loss: 8.6%
- Denial of Service: 3.1%
- Unauthorized Access Attempt: 0.2%
- Inappropriate Use: 1.8%
Malware Kits

• **Proliferation of cheap and easy to use**
  • Free (Webattacker)
  • Torrents, P2P

• **Complex $7,000 kits**
  • 12+ kits available every 3-4 months
    • Zeus (ZBOT)
    • GHOSTNET (GHOSTRAT)
    • MUMBA (Zeus v3)
    • Mariposa
ZEUS (ZBOT)

• Professional Crime-ware toolkit
• Versions: v.1 – v3 +
• Targets banks, banking systems
  • Harvests client data
  • Accounts
Zeus (ZBOT) Server location
Command and Control (C&C)

• Leverages communication systems to relay messages

• Command Vectors
  • Twitter
  • IRC
  • Facebook
  • Google Groups
Staged attack

- Series of weeks/months to fully compromise a system
- Incremental uploads/downloads/xchanges
- Results are fully “rooted” devices
- Random “radio” silence
  - Remain hidden,
Hardware backdoor

• Provision of devices/ equipments that have “malware” already
  • Projectors
  • Printers
  • Photocopiers
    • Flash memory
  • W32 Spybot worm

APT - Targets

- Intellectual Property
  - Code
  - Applications
  - Protocols

- Designs
  - Schematics
  - Drawings
  - Illustrations

- Chemical / Biological
  - Formula’s
  - Equations
  - Chemical Compounds
APT - Case Studies

- Stuxnet – 2010 - Present
- Ghostnet: 2009 – 2010
- Operation Aurora: June 2009 – January 2010
- Estonia vs Russia: 2007
Russia – Georgia Conflict (July – August 2007)

• Objective:
  • Precursor to the South Ossetia War
  • Destabilization / PsyOps support / Mis-Information

• Targeted:
  • 7 August: Georgian servers and the Internet traffic were seized and placed under external control;
  • 8 August, country wide cyber attack. Alleged connections to “Russian Business Network”;
  • 9 August, Defacement of Georgian MFA, MIA, MOD. DDOS National bank of Georgia as well as news portals;
  • 12 August, President Saakashvili’s website, Georgian TV websites were attacked;
  • 12-13 August, the Georgian MOD website suffered direct attack as well as compromise.
Operation Aurora

- **Objective**
  - Dubbed “Operation Aurora” based on a filename in the malicious payload traced to one of the hackers
  - Leveraged a Windows Internet Explorer browser vulnerability (CVE-2010-0249)

- **Targeted:**
  - Intellectual property,
  - Software configuration management (SCM) systems
  - Gmail e-mail accounts of Chinese human rights activists and three dozen large enterprises.
  - Google, IBM, Juniper, +28 others
  - STILL IN THE WILD
Operation Aurora (Con’t)

- **Stages of infection**
  - A targeted user received a link in email or instant message from a “trusted” source.
  - The user clicked on the link which caused them to visit a website hosted in Taiwan that also contained a malicious JavaScript payload.
  - The user’s browser downloaded and executed the malicious JavaScript, which included a zero-day Internet Explorer exploit.
  - The exploit downloaded a binary disguised as an image from Taiwan servers and executed the malicious payload.
  - The payload set up a backdoor and connected to command and control servers in Taiwan.
  - As a result, attackers had complete access to internal systems.
GhostNet (Ghostrat)

- **Objective**
  - Infection and Exfiltration

- **Targeted**
  - over 1,2000 infected in over 100 countries.

- **Stages of Infections**
  - infected host downloads trojans that give the attacker control of actions made on host computer.
  - the trojan attacks the computer by downloading files and activating the host’s webcams and microphones.
APT – GhostNet by distinct IP

Infected IP / Country

- Vietnam
  - 53 infected IPs

- Other countries:
  - India: 225
  - Vietnam: 130
  - Others: 113, 65, 92, 148
Signed Code abuse

- STUXNET
- Took advantage of Jmicron / Realtek private keys to hack drivers that were signed by these companies
- Legitimate signatures.
- Cyber-sabotage
Valid Certificates ?!?!
Certificates – Con’t

Confirm this is the correct certificate before performing any functions with it.

Verify Certificate

Common Name: JMicron Technology Corp.
Status: Valid
Class: Digital ID Class 3 - Software Validation Renewal
Organization: JMicron Technology Corp.
Organizational Unit: Digital ID Class 3 - Microsoft Software Validation v2 System Design
State: Taiwan
City/Location: Hsinchu
Country: TW
Serial Number: 476f49f4c959f656e9aa1eb87fc529bb
Issuer Digest: 4e302eae92e9d99951ec2be99ec85757
Stuxnet - Dissected

- **Certificate**
  - Jmicron
  - Realtek

- **USB**
  - Initial infection vector
  - USB replication (x3)

- **Windows 0day**
  - 4 unique Vulns
  - Each found on most MS 2003

- **Rogue PLC logic**
  - Discovers PLC Device
  - Pushes new logic
Stuxnet - Process

Step7

s7otbxdx.dll

PLC: s7/315-2

Step7

s7otbxsx.dll

PLC: s7/315-2
Stuxnet – 0day

- **2 Privileges Escalation Vulnerabilities**
  - SMB – MS08-067

- **Print Spooler**
  - CVE-2010-2729
  - MS10-061

- **USB Proliferation Vulnerability**
  - BID 41732 +
    - ~WTR4141.tmp
    - ~WTR4132.tmp
APT – Steps to compromise
APT – Phased Compromise

First Contact

Initiation

Command & Control

Discovery

Spread

Orders

Data

Exfiltration / Propagation

Hosts / Devices

0Day / Vuln

Radio Silence

Infect

Collect

Transmit
Mitigation Strategy
Real world solutions to combat the APT Threat
Education and Awareness

- **Half Day:**
  - Executive Briefing
  - High Level / Consumable

- **Full Day:**
  - More Detailed
  - Focus on Sector Specific requirements

- **3 Day Intermediate:**
  - Intensive Review
  - Split of Theory / Practical

- **5 Day:**
  - Hands On
  - Advanced Defence / Tradecraft
R & D: Security/Automation Lab

• **Active / Functional**
  - Replication of actual processes in the Field
  - Scaled Automation network

• **Focus:**
  - Patching
  - Testing Signatures (AV / IDS)
  - More robust DCS Environment

• Technology is available and cost effective
Compliance ≠ Security

• Back to Basics
  • “you can’t buy security; You have to get security”

• Product Panacea
  • Configuration
  • Inspection
  • Dissection

• Standards
  • Jump Off point
  • Security Conversation
  • What works for you / others
  • One size fits none
Defence Strategy

• Conduct External/Internal Security Assessments
  • What you don’t know can STILL hurt you
  • Assessments from External / Internal perspective

• Education / Awareness
  • Training
  • Regular Briefings
  • Foster environment of Security / Communication
    • INTRA Departmental

• Security Bulletins
  • Weekly reminders
  • Trends

• Advanced Persistent Diligence
  • Truth, but Verify
APT meet APD

Advanced Persistent Diligence

• Testing patches before pushing
  • Development of a lab environment
  • Functional
  • Compressed version of ACTUAL devices and configuration

• SOCNET
  • Truth, and Verify

• Cyber Security Awareness
  • Employees are the best security barometer
Event Horizon

What do we see on the way
The Horizon

• **Mutating Bots / Command & Control**
  - Quiet installation
  - Obfuscated Exfiltration (HTTP, DNS, Masked)

• **Directed Social Engineering**
  - Staggered Attack
  - Combined with other styles
  - Building relationships over time

• **Leverage of Social Networks (SOCNET)**
  - Facebook is not your friend
  - Twitter or Linkedin aren’t too fond of you either...