• 10 Presentations
• 360 Seconds Each
• At 1 Minute Left – Warning
• At Bell –
  – Speaker Stops Speaking
  – Audience Erupts Into Applause
  – Next Speaker Takes Stage
Douglas Wilson

- Re-thinking Our Approach to Threat Intel Sharing
Rethinking Our Approach To Threat Intelligence Sharing

( in 360 seconds or less )

SANS CTI Summit 2/10/14
Doug Wilson
Manager
Mandiant, a FireEye Company
Adam Vincent

- The Business Side of Threat Intelligence
THE BUSINESS SIDE OF THREAT INTELLIGENCE

Adam Vincent
BUSINESS NEED

Every other part of the business has evolved to necessitate a platform to increase productivity and measure effectiveness. It’s your turn!
HOW DO YOU IMPROVE?

• Going beyond: “This Threat Intel stuff is a great idea!”:
  • AT&T, Bell Canada, Birmingham City University, cVidya, ThreatConnect, Edge Technologies, EMC/RSA, MITRE, Orange, Security Fabric Alliance, Symantec, Telecom New Zealand, Telstra, and the UK MOD’s Defence Science and Technology Laboratory (DSTL).

• You improve through understanding your processes and then measure, measure, measure…
ROI OF THREAT INTELLIGENCE

Threat Intelligence

Security Investment + Knowledge Assumptions = Cost
MODELING

Hourly Cost per Persona

Make Assumptions

Model & Measure

Potential Cost of Compromise

V1.0 contributed to TM Forum for incorporation to Fx13.5 release

© 2014 Cyber Squared Inc.
UNDERSTAND AND IMPROVE!

Prioritize

Understand Threats to Your Organization

Defend

Learn

Plan

© 2014 Cyber Squared Inc.
CONCLUSIONS

Download the calculator for free at

THANK YOU

Adam Vincent, CEO
Email: avincent@threatconnect.com
Web: www.threatconnect.com
• Employing Enterprise-wide Data to Mitigate the Insider Threat
Employing enterprise-wide data to mitigate the insider threat

Michael Gelles, Psy.D.

Deloitte Consulting LLP

February 2014
Insider Threat: A Call to Action

Recent years have seen a number of high profile insider threat incidents, ranging from unauthorized disclosure of classified information, to fraud, to workplace violence.

Bradley Manning

Manning released the largest set of restricted documents ever leaked to the public by leaking classified material to WikiLeaks during the summer of 2010.

- Gained access to information while assigned as an intelligence analyst to an army unit based near Baghdad, Iraq
- Was convicted in July 2013 of violations of the Espionage Act and other offenses
- Manning’s disclosures have been credited by the press as a catalyst for the Arab Spring

Edward Snowden

Snowden intentionally disclosed classified details of several top-secret US and British government mass surveillance programs to the press in May 2013.

- Gained access to information while working as a NSA Contractor for Booz Allen Hamilton (BAH)
- After three months of employment with BAH, Snowden leaked classified information
- Currently avoiding US prosecution by taking refuge in Russia
- Has been called a ‘traitor’ and ‘whistleblower’ by press

Aaron Alexis

Alexis was the sole gunman who killed twelve people at the Naval Sea Systems Command Building at the Navy Yard in September 2013.

- Gained access to the Navy Yard with his security clearance granted for his work as a civilian subcontractor for Hewlett-Packard Enterprise services
- Served in the Navy from 2007-2011 and was honorably discharged
- Was killed by security forces at the scene of the incident
Critical Concepts

Definition: A person who has the potential to harm an organization for which they have **inside knowledge or access**

<table>
<thead>
<tr>
<th>IT Sabotage</th>
<th>IP Theft</th>
<th>Fraud</th>
<th>Espionage</th>
<th>Workplace Violence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use of IT to direct specific harm at an organization or an individual</td>
<td>Use of insider access and knowledge to steal IP from an organization</td>
<td>Unauthorized modification or theft of organization’s data for personal gain</td>
<td>Use of insider access to obtain secret info for industrial or economic exploitation</td>
<td>Use of physical abuse or threats that creates a risk to the health and safety of organization’s workforce</td>
</tr>
</tbody>
</table>

- All behavior occurs in context
- From “bricks and mortar” to “bits and bytes”
- The path from an idea to action
- Interrupt forward motion
- Anomaly detection
- Mitigation
• Indicators: Not Just IP Addresses Anymore
Context & Actionable Indicators:

Not just IP Addresses anymore
Generating Context through the application of Knowledge allows for the creation of Intelligence that is actionable and specific to the organization that requested it.
**Behavioral Indicators**

- Poison Ivy Default Mutex Detected
- Process Created an Executable in a System Directory
- Process Modified an Executable File
- Process Modified a File in a System Directory
- A Document File Established Network Communications
- PDF Contains Embedded JavaScript Stream

This PDF Contains Embedded JavaScript. JavaScript embedded within a PDF is often obfuscated in order to conceal its intentions from analysts or in an attempt to bypass Intrusion Detection Systems. Attackers will use JavaScript to interact with dynamic elements that execute on a machine.

<table>
<thead>
<tr>
<th>Reference</th>
<th>File Type</th>
<th>Path</th>
<th>Artifact ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>stream</td>
<td>JavaScript</td>
<td>4f94b85d07114678df1601b572a232d.pdf:9</td>
<td>26</td>
</tr>
<tr>
<td>stream</td>
<td>JavaScript</td>
<td>\	empV4f94b85d07114678df1601b572a232d.pdf:9</td>
<td>31</td>
</tr>
</tbody>
</table>

- PDF Contains Embedded SWF Stream
- PDF Contains Suspicious Identifiers

The JavaScript embedded within the PDF contained one or more suspicious identifiers. On occasion attackers will assign meaningful variable names such as shellcode, or sc.

<table>
<thead>
<tr>
<th>Path</th>
<th>Identifier</th>
<th>Artifact ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>4f94b85d07114678df1601b572a232d.pdf:9</td>
<td>sc</td>
<td>26</td>
</tr>
<tr>
<td>\	empV4f94b85d07114678df1601b572a232d.pdf:9</td>
<td>sc</td>
<td>31</td>
</tr>
<tr>
<td>4f94b85d07114678df1601b572a232d.pdf:9</td>
<td>payLoadCode</td>
<td>31</td>
</tr>
<tr>
<td>\	empV4f94b85d07114678df1601b572a232d.pdf:9</td>
<td>payLoadCode</td>
<td>31</td>
</tr>
<tr>
<td>4f94b85d07114678df1601b572a232d.pdf:9</td>
<td>memory</td>
<td>26</td>
</tr>
<tr>
<td>\	empV4f94b85d07114678df1601b572a232d.pdf:9</td>
<td>memory</td>
<td>31</td>
</tr>
</tbody>
</table>

- PDF JavaScript Obfuscation Using "replace()" function

The replace method in JavaScript returns a copy of a string with text replaced using a regular expression or search string. If a particular antivirus application only looks for static artifacts within the file it deems indicative of shellcode then it may miss seemingly benign text that will later be transformed into usable code.

<table>
<thead>
<tr>
<th>Function</th>
<th>Path</th>
<th>Artifact ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>sc.replace</td>
<td>4f94b85d07114678df1601b572a232d.pdf:9</td>
<td>26</td>
</tr>
<tr>
<td>sc.replace</td>
<td>\tempV4f94b85d07114678df1601b572a232d.pdf:9</td>
<td>31</td>
</tr>
</tbody>
</table>

- Dynamic DNS Domain Detected
- Command Exe File Execution Detected
(define malware-zeroaccess-v2-variant-detected
 :title "Possible ZeroAccess Rootkit V2 Variant Detected"
 :description "ZeroAccess, also known as max++, is a kernel-mode rootkit that makes use of various advanced techniques to hide its presence on the system. It creates an encrypted hidden volume in the computer's file system where it stores ...".
 :category ["infection" "persistence"]
 :tags ["trojan" "host" "malware" "rootkit" "RAT" "fraud" "geoip" "ZeroAccess"]
 :severity 100
 :confidence 100
 :query
 ((fresh [Path])
 (artifact (ivar) "disk" Path (ivar) (ivar))
 (conde
  ((matches "\\RECYCLER\\S-1-5-18\\.*\\(L|U)\\.*\\.@" Path))
  ((matches "(?!)\\WINDOWS\\Installer\\.*\\(L|U)\\.*\\.@" Path))))
 (fresh [URL Method Network_Stream]
 (http-request Network_Stream (ivar) Method URL)
 (matches "GET" Method)
 (conde
  ((re-match "(?i).*promos\:fling\:com:\(80\)Vgeo\:txt\:city\:\.\?\.*" URL))
  ((re-match "(?i).*\:maxmind\:com:\(80\)Vapp\:geoiip\:js\:.\?\.*" URL))))
 (fresh [Port Network_Stream]
 (network-stream Network_Stream (ivar) (ivar) (ivar) Port)
 (conde
  (== Port 16464))
  (== Port 16465))
  (== Port 16470))
  (== Port 16471))))
A Holistic, Risk-Based Insider Threat Program

There are a number of building blocks required of a successful insider threat program that is capable of increasing the scrutiny on an organization’s highest-risk employees.

**Program Components**
- Pre-employ. Investigations Procedures
- Training & Security Awareness
- Personnel Management
- Security Capabilities
- Termination Procedures

**Program Stakeholders**
- HR
- Security
- General Counsel
- Policy
- Finance & Admin.
- Contracting

**Data Elements Monitored**
- Physical Security Access
- IT Security Access and Technical Controls
- Performance/Compliance/Finance/HR Data
- Personnel Behavioral Indicators
- Anomalous/Suspicious Network Activity

**Data Analytics Capability**
- Data Analysis & Reporting with Advanced Analytics Tool
- Active Monitoring*

**Key**
- Program Stakeholders
- Program Components
- Data Elements Monitored
- Data Analytics Capability

---

* Creates proactive awareness and potential for cross-disciplinary coordination, intervention, and resolution.

Risk mitigation efforts should focus on individuals perceived to be at an elevated risk to the organization.
Adam Meyers

• Intelligence-Driven Security
Unable to post slides
John Hultquist

- Distinguishing Cyber Espionage Activity to Prioritize Threats
Distinguishing Cyber Espionage to Prioritize Threats

10 February 2014
DEFINING AND DETERRING CYBER WAR

ctd@nsa.gov

U.S. Army War College, Carlisle Barracks, PA 17013-5050
December 2009

DEFINING AND DETERRING CYBER WAR

Since the advent of the Internet in the 1990s, not all users have acted in cyberspace for peaceful purposes. In fact, the threat and impact of attack in and through cyberspace has continuously grown to the extent that cyberspace has emerged as a setting for war on par with land, sea, air, and space, with increasing potential to damage the national security of states, as illustrated by attacks on Estonia and Georgia. Roughly a decade after the advent of the Internet, the international community still has no codified, sanctioned body of norms to govern state action in cyberspace. Such a body of norms, or regime, must be established to deter aggression in cyberspace. This project explores the potential for cyber attack to cause exceptionally grave damage to a state’s national security, and examines cyber attack as an act of war. The paper examines efforts to apply existing international norms to cyberspace and also assesses how traditional concepts of deterrence apply in cyberspace. The project concludes that cyber attack, under certain conditions, must be treated as an act of war, that deterrence works to dissuade cyber aggression, and provides recommendations to protect American national interests.

INFORMATION SUBJECT TO EXPORT CONTROL LAWS

Export of the attached information (which includes, in some circumstances, release to foreign nationals within the United States) without first obtaining approval or license from the Department of State for items controlled by the International Traffic in Arms Regulation (ITAR), or the Department of Commerce for items controlled by the Export Administration Regulation (EAR), may constitute a violation of law.

Download:
http://fcpra.org/language/CYBER.zip

or
http://rapidshare.com/files/318351062/CYBER.zip.html
http://braihavurah.org/language/CYBER.zip
When you can’t attribute...

- Nothing beats attributing activity to a known actor or campaign
- Instead of trying to prove/disprove something is espionage, identify the alternatives and judge which is most likely.
A few factors to consider...

- **Actions on objective**
  - Persistence over time
  - Information collected
  - Destroying, disrupting, dumping, and defacing

- **Targeting**
  - Function/Role of Organization/Personnel
  - Source of Target Information
  - Social Engineering

- **Malcode**
  - Historical Use
  - Propagation and Access to Malcode
  - Functionality
## Analysis of Competing Hypothesis Method

<table>
<thead>
<tr>
<th>Evidence</th>
<th>Cyber Espionage</th>
<th>Cybercrime</th>
<th>Hacktivism</th>
</tr>
</thead>
<tbody>
<tr>
<td>No data dumping event</td>
<td>Consistent</td>
<td>Consistent</td>
<td>Inconsistent</td>
</tr>
<tr>
<td>Zeus malware available through marketplace</td>
<td>Neutral</td>
<td>Neutral</td>
<td>Neutral</td>
</tr>
<tr>
<td>Government social engineering</td>
<td>Highly Consistent</td>
<td>Inconsistent</td>
<td>Consistent</td>
</tr>
<tr>
<td>No specific targeting for fraud</td>
<td>Consistent</td>
<td>Inconsistent</td>
<td>Consistent</td>
</tr>
<tr>
<td>Multiple year duration</td>
<td>Consistent</td>
<td>Inconsistent</td>
<td>Consistent</td>
</tr>
<tr>
<td>Extra document exfiltration</td>
<td>Consistent</td>
<td>Inconsistent</td>
<td>Consistent</td>
</tr>
<tr>
<td>capability</td>
<td>Consistent</td>
<td>Inconsistent</td>
<td>Consistent</td>
</tr>
<tr>
<td>Targets acquired through Stratfor, TRC</td>
<td>Highly Consistent</td>
<td>Consistent</td>
<td>Consistent</td>
</tr>
</tbody>
</table>
• Insights for Executive: Cyber Media Analysis
More well-known U.S. retailers victims of cyber attacks

“Law enforcement sources have said they suspect the ring leaders are from Eastern Europe, which is where most big cyber crime cases have been hatched over the past decade.”

Jan 2014
Scan: What’s out there?

- Traditional news media
- Alternative news sites
- Blogs
- Social media
- Interviews
- Videos

Analyze: What does the conversation tell us?

Changes in language
Changes in referenced targets
Changes in strength
Changes in conversation volume
Changes in participation
Synthesize: There's an app for that

- Context
- Goals
- Methods
- Impact
- Recommendations

Unique human skills to put cybersecurity into uniquely human terms.
James Ulrich

- Placing a $ Value on a Cyber Risk
Key concepts behind CyberPoint’s patent-pending CyberV@R model for quantifying cyber-related risk

SANS CTI SUMMIT February 2014
Why might you want to place a $ value on risks associated to cyber attack?

• Consider the following exchange:

Mr. CFO, I’d like to spend $100K on IT security upgrades

Ms. CIO, with you the sky is always falling. What’s it going to cost me if don’t spend the money?

Um…I don’t know?

Come back when you know.
Investment bankers have figured out how to answer this question.

Stock A

‘s price changes are normally distributed with standard deviation $A$

Stock B

‘s price changes are normally distributed with standard deviation $B$

HISTORICAL DATA

HISTORICAL DATA says the prices changes of $A$ and $B$ are correlated as

Then the odds of losing more than $X$ in combined value of $A$ and $B$ are less than $P$, when $X$ satisfies

$$\frac{P}{100} = \frac{1}{\sqrt{2\pi}\sigma_{AB}} \int_{x=-\infty}^{x=X} e^{-x^2/(2\sigma_{AB})} dx.$$ (See Hull, “Options, Futures, and Other Derivatives, 4th ed)

where

$$\sigma_{AB} = \sigma_A^2 + \sigma_B^2 + 2\rho\sigma_A\sigma_B.$$
So can you carry this kind of modeling over to cyber?

We can try a map along the following lines:

<table>
<thead>
<tr>
<th>Financial risk model component</th>
<th>Analogous CyberV@R model component</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial portfolio.</td>
<td>Networked computing infrastructure and the assets (IP, PII) housed there.</td>
</tr>
<tr>
<td>Market fluctuations.</td>
<td>Threats to which the network is exposed, with incidence rates.</td>
</tr>
<tr>
<td>Hedging strategies (buy more A? sell more B?).</td>
<td>Alternative security mitigations.</td>
</tr>
<tr>
<td>Asset prices given by Brownian motion with drifts, based on historical data.</td>
<td>Probabilistic threat evolution modeled by Bayesian networks constructed from pre-defined attack trees.</td>
</tr>
</tbody>
</table>

Threats + Network + Security Controls + Information Assets = $ on attack risk
Yes, if we can simulate how a threat moves through our network, stealing assets. For example:

Trojan.taidoor exploits WinOS vulnerabilities in PDFs, such as BID47314. Drops a backdoor that attaches to services.exe, svchost.exe, communicates with a C&C server. Used to target think tanks involved in U.S./Taiwan relations & policy formulation. -Symantec, 2012.
And that model is converted to a probabilistic graphical model, yielding a probability distribution.

Each threat stage has a probability of occurring.

Each security control (e.g. 1 of the SANS 20) has a probability of thwarting the stage.

Add proposed controls to see how $ valuation of risk changes.

The entire graph defines a joint probability distribution.

Monte Carlo simulations over the joint distribution yield a distribution on asset losses, and hence “$ value X such that odds of losing more than $X over time window T are less than P %”
Some other useful ingredients:

- Automated threat feeds by type, industry
- Good languages / tools for threat model construction
- Understanding of efficacy of security mitigations such as SANS 20 Critical Controls, for various threat types, and levels of implementation (via survey-based data, say)
Thank you,

have a great day! For more info, see

http://www.cyberpointllc.com/cyberpoint_labs.html
• Introducing the Concept of a Core IDS
Next Generation
Behavioral-Based
Data Protection

Bob DeWolfe
Regional VP
bob.dewolfe@dbnetworks.com
(978) 317-8197
"There are two kinds of companies in the world. Those who have been breached and know it, and those who have been breached and don't know it."

"Most of what we do is about prevention, prevention, prevention. Great. Just know it won't work."

"Signature detection just doesn't work anymore. The threats are so overwhelming. We have no choice but to move to behavior,"
What is SQL / SQL Injection?

- SQL – Structured Query Language
  Structured Query Language is a programming language designed for managing data in relational database management systems. (RDBMS)

- SQL Injection / SQL Injection Attack
  SQL injection is a hacking technique allows the introduction of unintended SQL commands to a database:

  ```
  Username: bob' or "1"="1" --
  Password: 
  ```
1. Injection (SQL)
   - The Money Shot: More data stolen than all other attacks combined!
   - Easy, Effective and **INVISIBLE WHEN SUCCESSFUL**!

2. Broken Authentication and Session Management (was formerly 2010-A3)
3. Cross-Site Scripting (XSS) (was formerly 2010-A2)
4. Insecure Direct Object References
5. Security Misconfiguration (was formerly 2010-A6)
6. Sensitive Data Exposure (2010-A7 Insecure Cryptographic Storage and 2010-A9 Insufficient Transport Layer Protection were merged to form 2013-A6)
7. Missing Function Level Access Control (renamed/broadened from 2010-A8 Failure to Restrict URL Access)
8. Cross-Site Request Forgery (CSRF) (was formerly 2010-A5)
9. Using Components with Known Vulnerabilities (new but was part of 2010-A6 – Security Misconfiguration)
10. Unvalidated Redirects and Forwards
When SQL Injection reaches the Database Tier there is nothing to alert you!

**SQL Injection**

- Code Scanning + Application Vulnerability Scanning

**Database Tier**

- Network IDS
- Web Application Firewall
- Application Server
- IDS 6300

**WHITELIST** **BLACKLIST**
Introducing Core IDS

Perimeter
- Network F/W
- Network DoS
- Network IDS
- WAF
- NAC
- VPN
- Reverse Firewall
- Load Balancer
- Web / Application Servers

Core
- Critical Asset Protection
- Database Servers
- IDS-6300

SIGNATURES

Multi-Dimensional Behavioral Analysis
If you stop the SQL Injection, you stop the attack!

www.dbnetworks.com

Bob DeWolfe
Regional VP
bob.dewolfe@dbnetworks.com
(978) 317-8197
Curt Shaffer

- Pragmatic Intelligence
Curt Shaffer

Curt Shaffer has been in the IT field for 15 years. His experience is diverse across the IT field from ISP network design and installation, to server engineering for small and medium business as well as a number of local and US federal international agencies as well as intrusion analysis, incident response and malware reverse engineering. His change over the past 5 years has been his security focus. A majority of his security work most recently has been building internal threat intelligence for federal agencies and in his current position as the Owner of and Sr. Threat Researcher, for Symbiotic Network Technologies, LLC he analyzes current and new trends in that attack landscape in order to provide organizations with a realistic view of how they are being attacked and what can be done about it.

He holds a number of industry standard certifications including CISSP, SANS:GREM, GCIA, GCIH, GPEN, GSEC and a number of CompTIA and Microsoft certifications.
The Process

- **Reconnaissance**
- **Weaponization and Delivery**
- **SIEM**
- **C2**
- **IDS/IPS/DLP**
- **Exploitation**

Diagram showing the process flow.
Not all intel is good intel
Event Overview

Weaponization: Attacker creates Java payload with exploit code and “publishes” the malware into an ad system for delivery

Delivery: Regex HTTP URI for \/[a-z]{8}\./php\?[a-z]{8}=[0-9]{6}$

Exploitation JAR:

• HTTP Request Method = GET

• Content-Type = application/x-java-archive

• Regex HTTP URI for \/[a-z]{8}\./jar$

Successful Infection

• will call home for further instructions

Actionable Intel

• **Delivery:** IDS/IPS rule to match the URL pattern or web content filter rule of the delivery of weaponized malware

• **Exploitation:** Yara or IDS/IPS rule for keywords or pattern of the JAR payload and code exploiting CVE-2012-1723

• **C2:** IDS/IPS/DLP rule to match known C2 call back URI pattern.
Actionable Intel vs Informative Intel

- Redirection URL is identified
- The JAR delivery - identified and would be labeled as related, but with an additional label of exploitation
- Aspects of the JAR - indicating the client in fact downloaded C2 is recognized - related and additionally labeled as C2
- Corroborating evidence the target is infected
<table>
<thead>
<tr>
<th>Severity</th>
<th>AlertID</th>
<th>Summary</th>
<th>Time</th>
<th>With Malware</th>
<th>Kill Chain Phase</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>10027</td>
<td>Known Impact Exploit Kit Landing Page</td>
<td>6/22/13 8:00</td>
<td>Yes</td>
<td>Delivery</td>
</tr>
<tr>
<td>High</td>
<td>10028</td>
<td>Impact EK Payload Content-type = application/x-java-archive</td>
<td>6/22/13 8:01</td>
<td>No</td>
<td>Delivery</td>
</tr>
<tr>
<td>High</td>
<td>10029</td>
<td>JAR file matching CVE-201201723</td>
<td>6/22/13 8:03</td>
<td>Yes</td>
<td>Exploitation</td>
</tr>
<tr>
<td>High</td>
<td>10030</td>
<td>Impact EK C2 URI detected</td>
<td>6/22/13 8:10</td>
<td>No</td>
<td>C2</td>
</tr>
</tbody>
</table>
Main Incident Takeaways (by most management)

- How fast was the behavior detected?
- How fast did the team respond to the event?
- How long did it take to be fixed?

- We aim to be able to assist the analysts with providing good news to all of these factors.
<table>
<thead>
<tr>
<th>Kill Chain Phase</th>
<th>Observed Action</th>
<th>Mitigation Actions</th>
<th>Indicator</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delivery</td>
<td>File Identification in IDS/IPS</td>
<td>Create IDS/IPS to alert or prevent.</td>
<td>alert tcp $EXTERNAL_NET $HTTP_PORTS -&gt; $HOME_NET any (msg:&quot;ET CURRENT_EVENT S Impact Exploit Kit Landing Page&quot;; flow:established,from_server; pcre:&quot;/[a-z]{8}.[a-z]{8}=[0-9]{6;classtype:trojan-activity;sid:99999999;rev:1;}&quot;)</td>
</tr>
<tr>
<td>Kill Chain Phase</td>
<td>Observed Action</td>
<td>Reason for success</td>
<td>Mitigation Actions</td>
</tr>
<tr>
<td>------------------</td>
<td>----------------</td>
<td>--------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>Delivery</td>
<td>Known Impact Exploit Kit Landing Page</td>
<td>Lack of previous IDS/IPS rule</td>
<td>IDS/IPS rule for identification</td>
</tr>
<tr>
<td>Delivery</td>
<td>Impact EK Payload Content-type = application/x-java-archive</td>
<td>Lack of previous IDS/IPS rule</td>
<td>IDS/IPS rule for identification</td>
</tr>
</tbody>
</table>
Exploit: Indicator

rule cf_jar_cve_2013_0422
{
    meta:
        description = "Java Applet JMX Remote Code Execution"
        cve = "CVE-2013-0422"
        ref = "http://pastebin.com/JVedyrCe"
        author = "adnan.shukor@gmail.com"
        date = "12-Jan-2013"
        version = "1"
        impact = 4
        hide = false

    strings:
        $0422_1 = "com/sun/jmx/mbeanserver/JmxMBeanServer" fullword
        $0422_2 = "com/sun/jmx/mbeanserver/JmxMBeanServerBuilder" fullword
        $0422_3 = "com/sun/jmx/mbeanserver/MBeanInstantiator" fullword
        $0422_4 = "findClass" fullword
        $0422_5 = "publicLookup" fullword
        $class = /sun\org\mozilla\javascript\internal\.(Context|GeneratedClassLoader)/

    condition:
        (all of ($0422_*)) or (all of them)
}
<table>
<thead>
<tr>
<th>Kill Chain Phase</th>
<th>Observed Action</th>
<th>Mitigating Action</th>
<th>Indicator</th>
</tr>
</thead>
</table>
classtype:trojan-activity; sid:9999999; rev:4;) |
Key Benefits!

• Provides clear and concise ability to analyze events to ascertain if they are just events or incidents as rapidly as possible.
• Provides the analyst quality feedback.
• IR teams for action plans
• Lessons learned meetings
<table>
<thead>
<tr>
<th>Kill Chain Phase</th>
<th>What happened</th>
<th>Why our controls failed</th>
<th>Mitigation Plan</th>
<th>IOC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delivery</td>
<td>EK URL Access</td>
<td>No blocking rule in IDS/IPS or web filtering</td>
<td>Create signature for the URL for block</td>
<td>IDS/IPS/DLP signature or blacklist in web filter</td>
</tr>
<tr>
<td>Delivery</td>
<td>JAR with known bad characterizes delivered</td>
<td>No blocking rule in IDS/IPS or web filtering</td>
<td>Create signature for the URL for block</td>
<td>IDS/IPS/DLP signature or blacklist in web filter</td>
</tr>
<tr>
<td>Exploitation</td>
<td>JAR with CVE-2012-1723</td>
<td>Workstation s not patched for this CVE</td>
<td>Deploy the patch to all systems</td>
<td>AV or Yara Signature</td>
</tr>
<tr>
<td>C2</td>
<td>EK C2 URI Access</td>
<td>No blocking rule in IDS/IPS or web filtering</td>
<td>Create signature for the URL for block</td>
<td>IDS/IPS/DLP signature or blacklist in web filter</td>
</tr>
</tbody>
</table>
Questions?
Shameless Plug

I’m happy to announce the beginning of a collaborative vetted threat intelligence group

• Not ANOTHER GROUP!
• Vetting is a bit different:
  • *Sponsor/community references
  • *Email address
  • *Voice telephone #
  • *A short description of why you would like access to CyberIntel.com
What’s Different?

OSINT out the wazoo!!

But you just told us to practice pragmatic intelligence!

Good catch. We strive to have attributable work so it can be tracked and followed up on. We make OSINT and make actionable indicators that members can then use pragmatically.

Utilizing the extension of the XORCISM framework our goal is to ingest or product indicators in a format ready for action for you!
What’s Different?

• Ticket tracking for members analyzing data
• Custom Correlation Rules to increase intel confidence
• Use of patent pending dynamic malware analysis and research lab
• Web interface for API configuration self service
• Web search/filter/analyze/Trend graphs etc
• Cloud Nein* style collab with mind mapping
We Want You!

Interested in helping out with this new crowd sourced community? Follow the requirements set out on http://cyberintel.com
We are accepting a limited number of beta members until we consider the product really prime time for the collaboration.
• Thank you for attending!

• Please fill out speaker evaluations on your way out.