EMERGING THREATS & STRATEGIES FOR DEFENSE

Stephen Coty – Chief Security Evangelist
Industry Analysis – 2014 Data Breaches - Mandiant

Across the Cyber Threat Landscape

<table>
<thead>
<tr>
<th>Objective</th>
<th>NUISANCE</th>
<th>DATA THEFT</th>
<th>CYBER CRIME</th>
<th>HACKTIVISM</th>
<th>NETWORK ATTACK</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example</td>
<td>Botnets &amp; Spam</td>
<td>Intellectual Property Theft</td>
<td>Credit Card Theft</td>
<td>Website Defacements</td>
<td>Destroy Critical Infrastructure</td>
</tr>
<tr>
<td>Targeted</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Character</td>
<td>Automated</td>
<td>Persistent</td>
<td>Opportunistic</td>
<td>Conspicuous</td>
<td>Conflict Driven</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IRAN-BASED</th>
<th>CHINA-BASED</th>
</tr>
</thead>
<tbody>
<tr>
<td>Industries Targeted</td>
<td>Energy, state government agencies</td>
</tr>
<tr>
<td>Victim Selection</td>
<td>Limited based on vulnerabilities</td>
</tr>
<tr>
<td>Available Tools</td>
<td>Publicly available</td>
</tr>
<tr>
<td>Date of Initial Mandiant Observation</td>
<td>2012</td>
</tr>
<tr>
<td>Detected by Victim</td>
<td>75%</td>
</tr>
<tr>
<td>Average Time Spent in a Victim Organization</td>
<td>28 days</td>
</tr>
<tr>
<td>Re-Compromise After the Initial Security Incident</td>
<td>Not witnessed</td>
</tr>
</tbody>
</table>

Phishing Email Trends

- 93% of phishing emails were sent on weekdays
- 44% of observed phishing emails were IT related, often attempting to impersonate the targeted company’s IT department
- Median number of days that threat groups were present on a victim’s network before detection: 14 days less than 2012
- Longest Presence: 2,287 days

Time from Earliest Evidence of Compromise to Discovery of Compromise

- 33% of victims discovered the breach internally
- Down from 37% in 2012
October 2nd: The financial institution JP Morgan Chase discloses that hackers accessed contact information from 83 million accounts in a prolonged cyberattack, making it one of the biggest data breaches in history.

Chase.com online banking under extreme cyber attack for over 72 hours: website still down for...

@socengineerinc: Jpmorgan bracing for 'Spear Phishing' campaign: sources | Fox business http://t.co/ypbZq1mV3U via @foxbusiness.

@infosecurepci: HSBC acknowledges massive payment card breach http://t.co/NoeBW1Mh7 #databreach #pcidss.

Websites of fifth largest bank in U.S. (usbank.com) hacked by free syrian hackers.

@boolfifa: FBI is examining Morgan Stanley client data breach -source.
Industry Analysis - Energy

Just four men hacked into the U.S. military and Microsoft computer network and stole $100 million worth software. The stolen software is used to train Apache helicopter pilots as well as the source code and technical specifications related to Microsoft Xbox one gaming console and games including "call of duty: Modern Warfare 3".

Brazilian President Dilma Rousseff was angry on learning that the computer network of Petrobras, the state-run oil company, was hacked by...

Recent malware attacks on Saudi Aramco and Qatar’s RasGas have reinforced the urgency of securing businesses against this threat.

Bloomberg reported just last week that a group of Chinese hackers, whom U.S. intelligence agencies referred to as "Byzantine Candor," have stolen sensitive or classified information from 20 organizations, including Halliburton Inc., and a prominent Washington law firm, Wiley Rein LLP.

Though no specific company names were given, sources familiar with the matter claim that Calpine Corp., oil companies Saudi Aramco and Petróleos Mexicanos, Qatar Airlines and Korean Air were among the many companies targeted by the hackers.

@shell_news_Shell Data Leak May Compromise Safety Of Staff – Emails - Royal Dutch Shell plc.com #RoyalDutchShell http://t.co/NPw8DBHILC.
Different Cells
New Groups Emerging
Tools of the Trade
Black Shades RAT
HOW DO WE DEFEND AGAINST THESE ATTACKS
Security Architecture

Network
- Firewall/ACL
- Intrusion Detection
- Deep Packet Forensics
- Netflow Analysis
- NAC
- DDOS
- Scanner

Server/App
- Vulnerabilities
- Log Mgmt
- SDLC
- Patch Mgmt
- Mail/Web Filter
- Scanner
- Backup

Host
- Anti-Virus
- Encryption
- GPG/PGP
- FIM
- Anti Malware
- IAM
- Central Storage

http://aws.amazon.com/security/security-resources/
Data Correlation is the Key
NGX SIEM Operations

- 8.2 Million Per Day
- 40,000 Per Month

FIG. D

INCIDENT IDENTIFICATION APPROACH

- THREAT IDENTIFICATION
  - Malware
  - Network Scans
  - Botnets
  - Worms
  - Trojans
  - Unauthorized Access

AUTOMATED EXPERT SYSTEM ANALYSIS

1. Attacker Reputation
2. Nature of Exploit
3. Attacker Behavior
4. Target Asset Vulnerability
5. Target Asset Value
6. Global Threat Trends
7. Attacker Confirmation

CERTIFIED ANALYST REVIEW

INCIDENTS
Enterprise Cyber Security Teams

- Monitor and Maintain non-managed hardware deployment uptime
- Collect and Maintain content for all non-managed devices
- Operational Implementation of all security infrastructure
- Network and Application Penetration Testing and Audit Team

Cyber Security Awareness Program

Incident Response Team
24x7 Security Operations Center

- Monitor intrusion detection and vulnerability scan activity
- Respond to incidents and provide ongoing tuning services as new threats appear
- Provide guidance on remediation when incidents are identified
- Detect Zero-Day and APT attacks
- Proactively monitor web application firewall
- Analyze incidents and escalate according to custom requirements
- Identify and implement required policy changes
Honeypot Findings

- Highest volume of attacks occurred in Europe
- Attacks against Microsoft DS accounted for over 51% of the overall attack vectors
- Database services have been a consistent target
- 14% of the malware loaded on the Honeypots was considered undetectable by AV
- Underscores the importance of a defense in depth strategy for the need to secure your enterprise and cloud infrastructure
Samples of Malware detected

If an attacker were using the collected malware to launch an attack against an individual or an enterprise it would be theoretically run in this order.

1. Ping Sweep
2. Port Reconnaissance
3. Exploit a Vulnerability
4. Check for Shares or Networked Drives
5. Load Malware
6. Load Worm
7. Load Remote Access Trojan for full Control
Partnering with other Researchers
Information Sharing Model

Cybersecurity information types

- **Incidents**: Details of attempted and successful attacks that may include a description of information lost, techniques used, intent, and impact. The severity of an incident could range from a successfully blocked attack to a serious national security situation.

- **Threats**: Yet-to-be-understood issues with potentially serious implications; indicators of compromise, such as malicious files, stolen email addresses, impacted IP addresses, or malware samples; or information about threat actors. Threat information can help operators detect or deter incidents, learn from attacks, and create solutions that can better protect their own systems and those of others.

- **Vulnerabilities**: Vulnerabilities in software, hardware, or business processes that can be exploited for malicious purposes.

Key actors

- Government
- Private critical infrastructure
- Business enterprises
- IT companies
- IT security firms
- Security researchers

Exchange

- **Mechanisms of exchange**: Person to person, machine to machine
- **Methods of exchange**: Formalized, Trust-based, Security clearance-based, Ad hoc

Mitigations

Methods for remedying vulnerabilities, containing or blocking threats, and responding to and recovering from incidents. Common forms of such information include patches to plug vulnerabilities, antivirus updates to stop exploitation, and directions for purging malicious actors from networks.

Situational awareness

Information that enables decision-makers to respond to an incident and that may require real-time telemetry of exploited vulnerabilities, active threats, and attacks. It could also contain information about the targets of attacks and the state of critical public or private networks.

Best practices

Information related to how software and services are developed and delivered, such as security controls, development and incident response practices, and software patching or effectiveness metrics.

Strategic analysis

Gathering, distilling, and analyzing many types of information to build metrics, trends, and projections. It is often blended with projections of potential scenarios to prepare government or private sector decision-makers for future risks.
Jan 2014: "In January of this year, the cyber security firm CrowdStrike...Havex Trojan From Russia?"

Mar 2014: "Since March 2014 the group has targeted the energy grid, major electricity firms and petroleum pipeline operators using a number of attack vectors, including the Havex Trojan which has infected industrial control systems, according to a report by Symantec Corp. /quotes/z/n/qm/78622/delayed /quotes/nls/symc SYMC +0.57% on Monday."

Jun 2014: "The department said last week it was investigating whether the Havex Trojan software had been involved in previous compromises of energy infrastructure."
Monitoring the Social Media Accounts
Following IRC and Forums

Athena IRC Bot

An IRC (Internet Relay Chat) bot that could steal file information, flood your network (DDOS) or any target sites with your zombie bots. The amount of Athena IRC bot is around $100 pre-configured Bot per customer’s request. $10 for rebuild and another $15 IRC setup via TeamViewer, join.me and PuTTY. In addition to that the bin settings has a capability or has a tool that could convert the encrypting the actual IP. The ability to download binaries (hosted elsewhere) and take over a target client to gain access/privileges.

The following PCAP sample triggered our IDS system to one of our customers.

JOIN #chatroom
.MODE #chatroom
+w!fCVa...
NICK n[USA][U][D][W]
IN786[2c]ozzww xu...
 n[USA][U][D][WIN7]
x86[2c]ozzwwwu“ mrrMommmj@brama.g
oogle.com J01
N #chatroom...
irc-private-life.biz 353 n[USA][U]
D[WIN7]x86[2c]lzcz
zuwcom @ #chatro
om: n[USA]
oljgavw@brama.g
oogle.com J01
N #chatroom...l
irc-private-life.
biz 353 _

What was identified:
- JOIN (command use to join a channel)
- #chatroom (exsiting chatroom)
- n[USA][U][D][WIN7]x86[2c]ozzwwwu“ mrrMommmj@brama.google.com (is possible target brute-forcing its way to the machine)
• He is a guy from a European country/ (Russia)
• His handle or nick is madd3
• Using ICQ 416417 as a tool of communication (illegal transaction)
• A simple /whois command to the nick provided us with good information
  85.17.139.13 (Leaseweb)
• ircname: John Smith
• channels: #chatroom
• server: irc.private-life.biz [Life Server]
• Check this out user has another room. #attackroom4
• We can confirm that Athena version 2.3.5 is being use to attack other sites.
• 2,300 infected Users
• Cracked Software is available in forums
• As of today 1 BTC to $618.00 or £361.66
Forums to Follow – Exploit.in

A US court on Friday sentenced a hacker from Estonia Sergey Churikov to imprisonment for 11 years for breaking into RBS WorldPay. Churikov convicted of cyber fraud and stealing $9.4 million from a bank branch Royal Bank of Scotland in Atlanta in 2008. Churikov sentenced to 11 years in prison and ordered to pay $8.4 million. The Government of Estonia in early May 2010 decided to give Churikova US authorities. In co-operation of the State Prosecutor’s Office and the Estonian Central Criminal Police, US law enforcement May 6, 2009 were arrested members of a group of international computer fraud. As found out a consequence, Churikov in early November 2008 hacked into the database of the company operator debit cards RBS WorldPay one of the US banks. These data Churikov gave his partner Igor Grudievu, whose task was to record dumps resulting from burglary, on cards and then cash in ATMs. Just for one day Ronald and Evelyn Choi, and Michael Evgenov removed from the accounts of different persons over 3.5 million CZK 10 000 Estonian kronor at a time in Tallinn. In the future, money from ATMs worldwide and received numerous other hired drops. - presided resident of Tallinn, while 25-year-old Sergey Churikov, a resident of St. Petersburg Victor Pleschuk and resident Oleg cowelline Chaisase. The fourth key figure of the group took place on court documents as “Hacker 3”. Igor chest was accused of repeated forgery of means of payment for the purpose of use, the use of counterfeit payment instruments and computer fraud. He is sentenced to 3 years imprisonment with a probation period of 5 years. Eugene and Evelyn Choi charged with computer fraud and fraudulent use of payment instruments in a large scale, Evelyn Choi was sentenced to 3 years imprisonment with a probation period of 3 years, Eugene - to 2 years imprisonment with a probation period of 2 years.

In November 2008, 12 hours more than 2100 ATMs in 280 cities around the world were received US $ 9 million. Crime seized the US, Estonia, Russia, Ukraine, Italy, Hong Kong, Japan and Canada. Withdraw money previously hired drops.
Stay Informed of the Latest Vulnerabilities

• Websites to follow
  - http://www.securityfocus.com
  - http://www.exploit-db.com
  - http://seclists.org/fulldisclosure/
  - http://www.securitybloggersnetwork.com/
To Follow our Research

• Twitter:
  - @AlertLogic
  - @StephenCoty

• Blog:
  - https://www.alertlogic.com/resources/blog

• Newsletter:

• Cloud Security Report

• Zero Day Magazine
  - http://www.alertlogic.com/zerodaymagazine/
Thank you.