Security Driven Information Technology
U.S. accuses China of cyber spying on six American companies

WASHINGTON, May 19 (Reuters) - A U.S. grand jury has indicted five Chinese individuals with cyber espionage charges for allegedly targeting six American companies and stealing trade secrets, the U.S. Justice Department said, publicly accusing China of cyber spying for the first time.

The hackers targeted U.S. companies in the nuclear power, metals and solar products industries to steal information useful to competitors in China, the department said on Monday.

DOJ: Chinese military members stole U.S. trade secrets
Security Driven IT Services

Driving IT Value with People, Process & Technology
InterDev’s Leadership

• More than 30 years experience as a trusted source of IT advice, products and services

• Entrusted with sensitive IT missions for more than 30 government and public safety entities

• Managed IT and Security Services for over 100 commercial accounts

  – Microsoft Gold Certified Partner
  – Diamond Reseller for Barracuda Networks
  – Dell SecureWorks Partner
  – Netwrix, Qualys, Palo Alto, Imperva, Cisco, Symantec Partnerships
InterDev Services Menu

MANAGED SERVICES
• Managed IT
• Network Monitoring
• Disaster Recovery Planning
• Offsite Data Storage
• GIS Services

SECURITY SERVICES
• Vulnerability Assessment
• IT Auditing
• Penetration Testing
• Intrusion Prevention
• Data Loss Prevention
• Policy/Procedure Development
• Investigative IT Forensics

INFRASTRUCTURE
• Technology Consulting
• SAN Implementation
• High-Availability Solutions
• VoIP Solutions
• Voice/Data/Alarm Cabling
• Voice/Data/T1/SIP Circuits
• Data Center Solutions

BUSINESS SOLUTIONS
• Application Development
• Website Development
• SharePoint Development
Certifications and Memberships
Network:

– Organic growth – not Enterprise Design
  • Infrastructure needs enterprise level upgrades
  • Use of home-grade appliances for network connectivity and routing

– Lack of Documentation
  • Too much unshared knowledge resides with IT Supervisor only

– Departments reporting extended network latency and delays
Network (continued)

– Firewall
  • IT management “blind” to configurations and results – limited reporting, no logs or history
  • Multiple identified brute force security attacks/threats discovered on network
  • Expensive external hosted firewall solution
  • Leisure, Social Media and Peer-to-Peer traffic on network
– VPN access is not utilizing NAC (Network Access Control)
– Both VPN and terminal services access present concurrently
– No DMZ in network design – no buffer zone
Security

– Nature of your business raises the likelihood of a targeted attack
– Home/Small Business Class appliances - easy access points
– No encryption policy or procedures
  • Tapes, Notebooks, USB, emails, attachments, etc.
– Limited Systems logging, no Syslog server
– Too many Read/Write domain controllers
– Wireless functionality is extremely limited
  • negatively impacting productivity
  • Prompting workarounds
  • Rogue Wireless Access Points on LAN
– No IDS/IPS/DLP capability
Applications and Personnel

– Very clean – 0 virus and 0 malware detected.
  • Internal and External Qualys scans revealed only moderate issues
– Backup Systems are functioning well but may not be sustainable
  • Full backup and restore testing is not performed
  • Tape is functional but no longer the preferred enterprise solution
– Disaster Recovery Plan - limited and untested
– No Business Continuity Plan
Applications:

- ERP solution is home grown and vulnerable
- Catastrophic crash may not be recoverable
  - Security on SQL backend for ERP is suspect. Web front end to same application needs tighter security
  - Local client accessing via Internet using port 1433 directly to SQL

- Access to SQL data without a DMZ, VPN, Two Factor Authentication or Web Application Firewall is extremely risky
IT Department

– End user reluctance to work with IT department
  • User workarounds bypassing policy, filters and structure
– Need to address important technologies and security practices
  • Encryption and Two Factor Authentication
  • Logging and DLP
– Limited documentation of networks, infrastructure, policy and procedures
– Understaffed – need additional resources at multiple levels
Top High Risk Applications in Use

The high risk applications (risk rating of 4 or 5) sorted by category, subcategory and bytes consumed are shown below. The ability to view the application along with its respective category, subcategory and technology can be useful when discussing the business value and the potential risks that the applications pose with the respective users or groups of users.

Key observations on the 63 high risk applications:

**Activity Concealment:**
Proxy (1) and remote access (5) applications were found. IT savvy employees are using these applications with increasing frequency to conceal activity and in so doing, can expose Enercon to compliance and data loss risks.

**File transfer/data loss/copyright infringement:**
P2P applications (3) and browser-based file sharing applications (4) were found. These applications expose Enercon to data loss, possible copyright infringement, compliance risks and can act as a threat vector.

**Personal communications:**
A variety of applications that are commonly used for personal communications were found including instant messaging (3), webmail (5), and VoIP/video (2) conferencing. These types of applications expose Enercon to possible productivity loss, compliance and business continuity risks.

**Bandwidth hogging:**
Applications that are known to consume excessive bandwidth including photo/video (13), audio (1) and social networking (5) were detected. These types of applications represent an employee productivity drain and can consume excessive amounts of bandwidth and can act as potential threat vectors.
Application Vulnerabilities Discovered

The increased visibility into the applications on the network, regardless of port hopping, tunneling or other evasive tactics that may be used, extends into vulnerability exploit protection to ensure that the threat is detected and blocked. The application vulnerabilities discovered on the network, ranked by severity and count are shown in the table below.

<table>
<thead>
<tr>
<th>Threat Name</th>
<th>Application</th>
<th>Category</th>
<th>Severity</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>MS-RDP Brute-force Attempt</td>
<td>ms-rdp</td>
<td>brute-force</td>
<td>High</td>
<td>115</td>
</tr>
<tr>
<td>HTTP: User Authentication Brute-force Attempt</td>
<td>sharepoint-base</td>
<td>brute-force</td>
<td>High</td>
<td>5</td>
</tr>
<tr>
<td>HTTP Unauthorized Brute-force Attack</td>
<td>sharepoint-base</td>
<td>brute-force</td>
<td>High</td>
<td>5</td>
</tr>
<tr>
<td>Microsoft SQL Server User Authentication Brute-force Attempt</td>
<td>mssql-db</td>
<td>brute-force</td>
<td>High</td>
<td>4</td>
</tr>
<tr>
<td>SMB Fragment Packet Found</td>
<td>ms-ds-smb</td>
<td>info-leak</td>
<td>Medium</td>
<td>4</td>
</tr>
<tr>
<td>Buffer overflow in the On-Access Scanner in McAfee VirusScan</td>
<td>eset-update</td>
<td>code-execution</td>
<td>Medium</td>
<td>1</td>
</tr>
<tr>
<td>Microsoft Windows Registry Read Attempt</td>
<td>msrpc</td>
<td>info-leak</td>
<td>Low</td>
<td>1,255</td>
</tr>
</tbody>
</table>
Qualys External Scan

Summary of Vulnerabilities

<table>
<thead>
<tr>
<th>Severity Level</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Severity 5</td>
<td>1</td>
</tr>
<tr>
<td>Severity 4</td>
<td>0</td>
</tr>
<tr>
<td>Severity 3</td>
<td>4</td>
</tr>
<tr>
<td>Severity 2</td>
<td>2</td>
</tr>
<tr>
<td>Severity 1</td>
<td>1</td>
</tr>
</tbody>
</table>

Total: 7

<table>
<thead>
<tr>
<th>Vulnerabilities Total</th>
<th>19</th>
<th>Security Risk (Avg)</th>
<th>3.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>by Severity</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Severity</td>
<td>Confirmed</td>
<td>Potential</td>
<td>Information Gathered</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>4</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>12</td>
</tr>
<tr>
<td>Total</td>
<td>7</td>
<td>0</td>
<td>12</td>
</tr>
</tbody>
</table>

INTERDEV
Managed IT Security
Qualys Internal Scan

### Summary of Vulnerabilities

<table>
<thead>
<tr>
<th>Vulnerabilities Total</th>
<th>557</th>
<th>Security Risk (Avg)</th>
<th>3.6</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>by Severity</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Severity</strong></td>
<td><strong>Confirmed</strong></td>
<td><strong>Potential</strong></td>
<td><strong>Information Gathered</strong></td>
</tr>
<tr>
<td>5</td>
<td>2</td>
<td>10</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>6</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>33</td>
<td>16</td>
<td>40</td>
</tr>
<tr>
<td>2</td>
<td>28</td>
<td>9</td>
<td>58</td>
</tr>
<tr>
<td>1</td>
<td>10</td>
<td>0</td>
<td>344</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>74</td>
<td>41</td>
<td>442</td>
</tr>
</tbody>
</table>

### 5 Biggest Categories

<table>
<thead>
<tr>
<th>Category</th>
<th><strong>Confirmed</strong></th>
<th><strong>Potential</strong></th>
<th><strong>Information Gathered</strong></th>
<th><strong>Total</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP/IP</td>
<td>1</td>
<td>0</td>
<td>94</td>
<td>94</td>
</tr>
<tr>
<td>Information gathering</td>
<td>0</td>
<td>0</td>
<td>94</td>
<td>94</td>
</tr>
<tr>
<td>General remote services</td>
<td>26</td>
<td>2</td>
<td>65</td>
<td>93</td>
</tr>
<tr>
<td>Windows</td>
<td>15</td>
<td>27</td>
<td>27</td>
<td>69</td>
</tr>
<tr>
<td>SMB / NETBIOS</td>
<td>20</td>
<td>0</td>
<td>48</td>
<td>68</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>62</td>
<td>29</td>
<td>327</td>
<td>418</td>
</tr>
</tbody>
</table>
Summary

- Enterprise Class Infrastructure Upgrades
- ERP Upgrade (Security and Stability)
- Security - Plans, Policies, Technologies
- Fully Developed and Tested DR and BC Plans
- Increased IT Staff and Service Levels