Government of Mauritius

Gregg Gerber
Strategic Engagement, Emerging Markets
Japan's top weapons maker has confirmed it was the victim of a cyber attack reportedly targeting data on missiles, submarines and nuclear power plants.

Mitsubishi Heavy Industries (MHI) said viruses were found on more than 80 of its servers and computers last month.

The government said it was not aware of any

---

Valve's online game service
by hackers

The Steam video game service, used by 35 million people, has been hacked.

Its owner and operator, Valve, said all emails were accessed and data stolen.

It is the latest in a string of attacks on Steam, which have included a DDoS attack.

---

Anonymous claims credit for crashing FBI
DOJ sites

The site of the FBI and the Department of Justice have been crashed.

It is not clear whether this is related to the attacks on Steam.

---

Cyber attack takes Qatar's RasGas offline

RasGas, the second largest producer of Qatar LNG after Qatar Petroleum, has been hit by an "unknown virus" which has taken the company offline.

A RasGas spokesperson confirmed that "an unknown virus has affected its office computer systems," said the company.

The virus was discovered on Monday and has caused the company to shut down its operations.

---

Threat to Its Security Franchise

The company is now investigating the cause of the virus and working to restore normal operation.

---

Nitro' targeted mass hit chemical comp

Symantec has traced the attacks that hit a region in China.

The goal of the attackers appears to be to collect intellectual property such as design documents, formulas, and manufacturing processes.

The attacks, dubbed Nitro, combine social engineering and remote access Trojans to infect targeted Windows computers.

From Symantec's report (PDF):
<table>
<thead>
<tr>
<th>APT</th>
<th>Attacker (Malicious Outsider)</th>
<th>Insider (Malicious and Non-malicious)</th>
<th>Hack-tivist</th>
<th>Cyber Criminals</th>
<th>State Nation</th>
</tr>
</thead>
<tbody>
<tr>
<td>RECON</td>
<td>Free Scanners</td>
<td>Insider Knowledge</td>
<td>Social Networks / Google</td>
<td>Data Mining</td>
<td>Espionage / Collusion</td>
</tr>
<tr>
<td>INCURSION</td>
<td>Basic Scripts / MetaSploit</td>
<td>Privileged Access</td>
<td>Social Engineering</td>
<td>Attack Kits / Malcode / Bots / Affiliates</td>
<td>Tailored Malcode / 0-Day</td>
</tr>
<tr>
<td>DISCOVERY</td>
<td>Random Targeting</td>
<td>Asset Awareness</td>
<td>Targets of Chance</td>
<td>Targets of Chance / Choice</td>
<td>Targets of Choice</td>
</tr>
<tr>
<td>CAPTURE</td>
<td>Visible / Low Value</td>
<td>Critical Assets</td>
<td>Media Worthy Asset or Access</td>
<td>Monetized Assets</td>
<td>High Value IP / Government Secrets</td>
</tr>
<tr>
<td>EXFILTRATE</td>
<td>Tagging and Damage</td>
<td>Theft and Damage</td>
<td>DDoS, Theft and Damage</td>
<td>Fraud and Financial Gain</td>
<td>Gain / Maintain Strategic Advantage</td>
</tr>
</tbody>
</table>
Strategy Rethink: Anatomy of an attack

1. Research
2. Incursion
3. Discovery
4. Capture
5. Exfiltrate

Risk Posture and Policies

- Reconnaissance
- Weaponization
- Delivery
- Exploitation
- C2
- Exfiltration
IT Security pressures – changing world

User demands
- Social Networking
- Fav technology

Information
- Supply chain
- De-perimeterisation

Governance
Compliance

Time
- to enable
- to respond

Reduce costs

New Tech adoption

Threats
- Volume
- Type

Security Complexity
(More controls)
Where Does Your Threat Intelligence Reside?

**Internal**

**Targeted Attacks**
Are meant specific organizations – They’re not seen at a global level, Symantec can provide researcher-level tools & local assistance to help you detect and prevent these types of attacks

**Global Intelligence Network**
Like-minded organizations can share intelligence to help peers, some industries and agencies are not able to for National Security Reasons

**External**
Symantec Cyber Threat Intelligence

**Cyber Awareness**
- Cyber Briefing Center
- Strategist Advisories
- Cyber Risk Assessments
- Cyber Training
- Cyber Readiness Assessments

**Cyber Preparedness**
- Security Base lining
- Threat Intelligence Reports
- Reputation Analysis
- Business Risk Modeling

**Cyber Forensics**
- Security Base lining
- Incident & Event Management
- Threat Analysis & Response
- Threat Impact Assessment

**Cyber Response**
- Product & Threat Analysis Support
- Cyber Incident Advice
- Cyber Threat Response
- Scribe
What Makes Symantec Unique?

- Leaders in Threat Research & Technology
- The Biggest Organisations Trust our People & Services
- Provide Risk-Based Perspective
- Market Validation
Symantec Cyber Threat Intelligence Summary

**Government Engagement**
- Participation in National Cyber Strategies

**Security Intelligence Group**
- Our Global Intelligence Network and Reputation Feeds add Threat Context to YOUR Infrastructure

**Highly Targeted Threat Analysis**
- The Symantec's Threat Analysis Tools Used by Our Researchers Are Also Available to You to Analyze Highly Targeted Attacks

**Leverage Existing Investments**
- Our Modular Approach means we can Leverage Investments in Your Existing Security Controls, and Demonstrate Where to allocate resources With Risk Modeling

**Cyber Readiness Programs**
- We Help you understand YOUR risks and Prepare for Cyber Threats
Attack Scenarios

- Economically motivated
- Steal money/info to resell
- 17th century privateering and modern cybercrime
- Link between crime and national security actors
Targets - Depend on the objective of the attacker

Government
Economic / Intel / Warfare / Political

Large Business
IPR / Economic / Espionage

Defense
Intel / Warfare / Political

CII Operators
Economic / Intel / Warfare / Political

Consumers
Trusted

Small Business
Stepping Stone / Economic
Modus operandi

My Money went to NIGERIA and all I got was this lousy T-Shirt

Because there is no patch for stupidity
Modus operandi

$ with info
- $ without
  value

Smart Grid
Jumping the Air Gap
Zero-Day Vulnerabilities
OS Intelligence
Value of Information
SCADA
Specifically on defense

5th Domain of Warfare

Land  Sea  Air  Space  Cyber

Merge of EW and SIGINT with cyber
Specifically on defense
Makes sense from a military point of view

VS.

Sensors, communications and robotics technologies dominating future battlefield
Specifically on defense

Historically listen to information & deny access to information

New paradigms include modifying information to create a false operational picture and damage the infrastructure, or remotely control it.
Cyber Awareness

Strategist Cyber Advisories
Summary business reports defining best practices for mitigating the attack

Cyber Training
Cyber threat detection and incident response course (10 day)

Cyber Briefing Center
Briefing on the latest threats, understand the processes and techniques required to deal with today's cyber attacks

Cyber Risk Assessments
Information risk assessments, cyber security policy assessments

Cyber Readiness
Join Symantec's Cyber war games to test and develop your skills and capability
Cyber Preparedness

Security Base Lining

Define/validate the state of your environment & security controls

CCS Vulnerability Mgr.
Altiris
SEP/CSP
Cyber V Assessments
Enterprise Security Assessment

CCS Vulnerability Mgr.
DeepSight Feeds
Reputation Feeds
Threat Analyst service
Vulnerability assessment

CCS Risk Manager
SPC
Business Continuity Planning service *
Cyber Response

Business Critical Services

Product and threat analysis support

24x7 Access
Personalized
Scribe

Priority Access to Strategists

Trusted Partner Ecosystem

24x7 Access

Priority Access to Strategists

Trusted Partner Ecosystem
**Cyber Forensics – In-Progress & Post Incident**

### Security Base Lining

- **(Re)** Define/validate the state of your environment & security controls

### CCS Policy/Assessment Mgr.
- Altiris
- SEP/CSP
- Cyber V Assessments
- Enterprise Security Assessment

### Managed Security Services
- SSIM
- DeepSight Feeds
- SIM design & optimization
- Threat Analyst

### Non-classified
- Reputation Feeds
- STAR
- BCS - Scribe
- Threat Analyst

### Classified
- Smart Harness
- Threat Expert
- Security cleared Threat Analysis

### Non-classified
- Reputation Feeds
- DeepSight Feeds
- Data Cache

### Classified
- Reputation Feeds
- DeepSight Feeds
- Security cleared Threat Analyst
Thank You

Gregg Gerber
Gregg_gerber@symantec.com
@gregg_gerber