The Emerging Cyber Threat Landscape

GFIRST

Strategic Objectives

- **Enable** informed risk management by members and partners through effective cyber information sharing and analysis.

- **Improve** security incident response through trusted analysis, collaboration and coordination.

- **Drive** informed decision making by policymakers and industry as a trusted sector-wide advisor on IT sector security response and cyber information sharing issues.

Membership

As of August 1, 2012

Foundation Members

BAE Systems, IT
CA Technologies
Cargill, Inc.
CSC
eBay
HP
Intel Corporation
Oracle USA, Inc.
Symantec Corp.
VeriSign, Inc.

Silver Members

Afilias, USA
Cisco Systems, Inc.
Juniper Networks
NeuStar
Trend Micro

Bronze Members

AT&T
GE
IBM
Microsoft Corp.
Lockheed Martin Corporation
Prescient Solutions
SAP Labs

Biography

Threat Indicator Special Interest Group

The IT-ISAC Threat Indicators Special Interest Group (SIG) facilitates trusted information sharing and collaborative analysis among IT-ISAC members and the IT-ISAC Operations Center to better enable members to identify attack, incident and threat indicators on their networks. The SIG is focused on, but not limited to, examining indicators from persistent adversaries who use multiple attack vectors to achieve their goals.

Biography

Sean McCracken brings 16 years of information systems and security experience to his current role as the Infrastructure & Engineering Supervisor at Blue Glacier Management Group, serving as the Technical Program Manager for the Information Technology - Information Sharing and Analysis Center (IT-ISAC). Sean has a diverse skillset acquired during professional involvements in software engineering, application development, security policy, and technical operations management. His current position utilizes past work experience and his Masters of Science in Computer and Information Systems aids his work with IT-ISAC membership comprised of leaders in the cyber security community.

Biography

Jeff Boerio has a Bachelor of Science Degree in Computer Science from Purdue University and has been with Intel since graduating in 1993. He is a Senior Information Security Specialist in the Intel Information Risk and Security Group's Threat Management Team and leads the team's cyber incident response efforts, including investigating suspected intrusions and conducting malware analysis. Jeff represents Intel's interests in cyber incident response to industry organizations including IT-ISAC, FIRST, and ICASI. He currently serves as the chairperson for the IT-ISAC Threat Indicator SIG.

Agenda

Overview

- Historical Threat
- Modern Threat
- Emerging Threat
- Conclusion/Questions

The Emerging Cyber Threat Landscape

The Historical Threat

- Morris Worm attack in 1988
  - Intentions not malicious
  - Caused DoS Attacks
  - Initiated on host to copy itself to other hosts
  - Remote execution of code – severe damage

- Code Red
  - Did not rely on user's contact list
  - Performed network scanning
  - Used IP of host a vector for propagation

- Nimda
  - 4 different propagation vectors
    - Websites, LAN, Emails, Executables

- Attacks were seen as venues for promotion of skill.

The Emerging Cyber Threat Landscape

Traditional Defensive Measures

- Digital Equipment Corporation (DEC)
  - Developed the packet filter firewall.
  - Allowed a host to inspect individual packets with the ability to establish unique rule sets whereby the firewall could accept, drop, or reject attempts to communicate with the host machine from a foreign source.
  - Provided a necessary layer of security, but only inspected packets individually and was unable to detect packets position within the data stream.

- Second Generation Packet Inspection Firewalls
  - Included the capability to identify a packet's place in a given connection (transport layer 4).
  - Able to determine application and protocol references embedded in the packet.
  - This technology does not stand alone; Has the ability to share deep packet inspection analysis with an Intrusion Prevention System (IPS).
  - Behavioral components to the technology
    - Organizational policies operate from a whitelist as opposed to establishing a blacklist for pre-identified unwanted traffic.
    - Instead all traffic is considered unwanted unless its deep packet inspection meets established criteria, allowing for a more secure perimeter.

The Historical Threat

- Malicious Signed Malware Growth
  - Symantec Global Security Report 2010 – Malware Doubled year-to year between 2006 and 2008
  - Symantec Internet Security Report 2012 – 403 million new unique variants in the wild compared to 286 million in 2010
  - McAfee and others show same trend
- Malware is Changing
  - More complex, sophisticated, and harder to detect
  - Easily accessible
  - Easy to Use (little technical experience needed)
  - Therefore functional for the common user

The Modern Threat

- Changes in the Landscape
- Socially Engineered Attacks
- Congestion with the Growth of Hacktivism
- Growth of Nation Sponsored Attacks

The Modern Threat

- Changes in the Landscape
  - Attackers' Goal
    - Bypass perimeter defenses while minimizing/erasing their footprint from IDPS systems inside the network.
  - Modern threat has moved beyond pure technical wisdom of launching attacks to include the exploitation of human behavior.

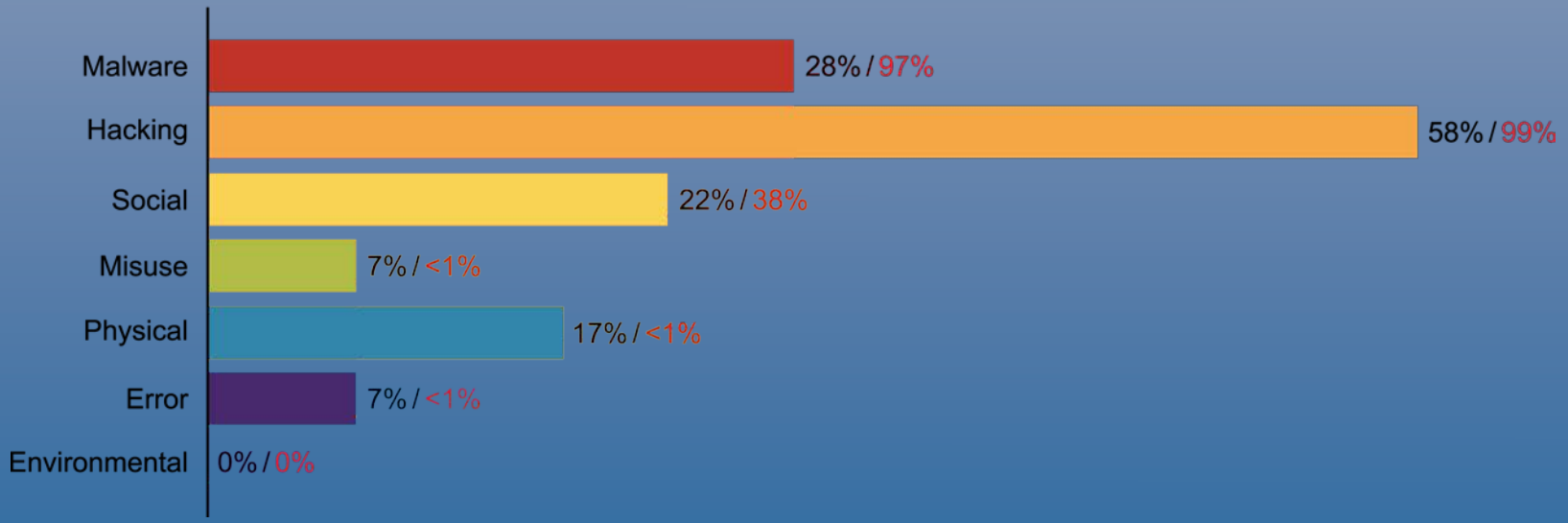
- Social Engineering
  - Attacker after specific information, intellectual property or customer information
  - Once Attacker has rights to a valid user's credentials, attacker can work under the radar operations (viewing, manipulating, destroying data).
  - Attackers attempt to exfiltrate targeted information
    - Can appear to be legitimate SSL traffic
  - Utilize split tunnel VPN
    - Target host system traveling with its owner onto unsecure and unmonitored home networks

The Emerging Cyber Threat Landscape

The Modern Threat

- Growth of Hacktivism
  - Verizon Data Breach Report of 2012:
    - Cyber criminals represent 83% of data breaches world-wide (however)
    - 58% of data stolen world-wide was the result of hacktivist activity.

Figure 18. Threat action categories by percent of breaches and percent of records – LARGER ORGS



The Emerging Cyber Threat Landscape

The Modern Threat

- Motive Behind Hacktivism
  - "Socio-Economic" Motivators
  - Cyber Intelligence Sharing and Protection Act (CISPA)
    - Perceived infringement on Constitutional Rights
  - DDoS Attacks
    - Most fail to overload a server
    - Time Consuming, creates commotion allowing cyber criminals to execute their attacks
    - Negatively impacts corporate brand reputation

- Nation-State Attacks
  - Government developed cyber weapons
  - FLAME Virus
    - Linked to Stuxnet attack of 2010.
    - Highly developed Malware (weeks to months of production) is accessible to be restructured and executed back into the wild by average users
  - Steal military secrets and Intellectual Property

The Emerging Threat

- Mobile Security (BYOD)
- Cloud-Based Services
- Attackers Moving Forward
- Attacker Mobilization & Targeted Attacks
- Countering the Emerging Threat

The Emerging Threat

- Mobile Security
  - According to Symantec[1]:
    - 71% Businesses polled are Planning Custom Mobile Applications
    - 41% of IT professionals polled ranked mobility as top risk
- Bring Your Own Devices
  - Increased attack surface
  - High area of concern for organizations who do not own devices they are charged with defending
  - Corporate Policies and Legal Precedents Evolve slower than affected technology
  - Mobile Security Defenses require significant resource allocation.
- Cloud-Based Services
  - Attackers will always go where the data is
  - Cloud advances make it easier for an attacker (more data in one location)
  - Balance between business efficiency in terms of continuity costs vs. the ability to directly manage risk in their data

The Emerging Threat

- Attackers Moving Forward
  - Focused on smaller organizations to carry out attacks.
  - Fewer resources devoted to IT Security
  - Less technical and human capabilities

- Small Organizations Tie to Larger Partners (Spear Phishing)
  - Remains the attacks ultimate target
  - Attacker uses traditional methods of exploit
    - Drive-by-download
    - Attacks on un-patched Common Vulnerability and Exposure (CVE) to gain access to network
    - Attacker can then monitor communication waiting for the opportune time to send a specifically crafted malicious email
    - If successful, larger partner is now infected

The Emerging Threat

- Attacker Mobilization
  - Attackers focused on research, social engineering, exploitation, lateral movement and exfiltration to obtain user credentials as a lunching point for exploitation
  - Attackers are more focused on collaboration, pooling resources and leveraging their capabilities to make attacks more effective
  - Attackers have evolved into a vast information-sharing network with communities, re-use of code, and common/shared techniques of exploit
- Targeted Attacks
  - Firewalls, IPS, and web-gateways are becoming increasingly vulnerable to zero-day exploits
  - Google Chrome Breach "Pwn2Own" – CanSecWest Conference Vancouver, BC:
    - Researcher used multiple exploits to achieve access to the system
    - Dubbed "Vulnerability Chaining" will continue to develop
    - IT-Managers employ heavy scrutiny on their patch cycles
    - Consider implications of leaving seemingly low risk vulnerabilities unpatched for a length of time

The Emerging Cyber Threat Landscape

Countering The Emerging Threat

- Engage With Peers
  - Leveraging formal and informal information sharing relationships with peer companies is vital in preventing, identifying and mitigating attacks.

- Industry – Industry Sharing
  - ISACs Provide Trusted, Confidential Information Sharing and Collaborative Analysis.
  - Bilateral communication w/ other companies or multilaterally w/ trusted peers.
  - National Council of ISACs.

- Industry – Government Sharing
  - National Cybersecurity and Communications Integration Center (NCCIC).
  - National Council of ISACs.

The Emerging Cyber Threat Landscape

Countering The Emerging Threat

- Global Communication
  - Forum for Incident Response and Security Teams (FIRST)
  - Corporations and Governments need to build a global capacity which enables them to best secure their individual networks when threats emerge from elsewhere

- Prioritizing Data
  - Organizations should have in place a data-centric protection strategy
  - Protection of most valuable assets first with more rigor than non critical assets

Conclusion

- Implement a risk management strategy which uses multiple layers of security that cost a potential attacker additional resources when attempting to target.
- Utilize controls in areas such as identity management, access management, and DLP technologies.
- Be aware of trending attack techniques and the profile of the attacker to identify the subtle changes that may indicate an emerging threat.
- Strategically reallocating defense assets as the threat landscape changes will equate to your organization remaining as close to the current threat as possible. When a new attack is witnessed it should serve as an indicator of attacks to come.

Reference

Symantec Corporation. 2012 State of Mobility Survey. Rep. N.p., 2012. Web. <http://www.symantec.com/content/en/us/about/media/pdfs/b-state_of_mobility_survey_2012_infographic.en-us.pdf>.

Contact Information

Sean McCracken
Sean.McCracken@ops.it-isac.org

Jeff Boerio
jeff.boerio@intel.com

Questions/Comments