Overview

- CERT Insider Threat Center
- Insider Threats in the Cloud
- Protecting Against Cloud Insiders
- Future Research
What is CERT?

Center of Internet security expertise

Established in 1988 by the US Department of Defense on the heels of the Morris worm that created havoc on the ARPANET, the precursor to what is the Internet today

Part of the Software Engineering Institute (SEI)

- Federally Funded Research & Development Center (FFRDC)
- Operated by Carnegie Mellon University (Pittsburgh, Pennsylvania)
What is the CERT Insider Threat Center?

Center of insider threat expertise

Began working in this area in 2001 with the U.S. Secret Service

Our mission: The CERT Insider Threat Center conducts empirical research and analysis to develop & transition socio-technical solutions to combat insider cyber threats.
Who is a Malicious Insider?

Current or former employee, contractor, or other business partner who

- has or had authorized access to an organization’s network, system or data and
- intentionally exceeded or misused that access in a manner that
- negatively affected the confidentiality, integrity, or availability of the organization’s information or information systems.
Insider Threats in the Cloud

Identified by Cloud Security Alliance (CSA) “Top Threats to Cloud Computing, v 1.0”

- Malicious insider working for cloud provider

But there are other insider threats related to cloud computing…
Provider / Organization Relationship

Cloud Provider

Resources

Employee

Data

Victim Organization

Resources/Availability

Employee

Data
Cloud-Related Malicious Insider Threats

Malicious Cloud Provider Employee

• Rogue Administrator

Malicious Local Employee

• Attacking organization data in the cloud
• Using the cloud to attack the organization
Rogue Administrators

Hosting Company Administrators
- Update virtual machine drivers to compromise the hosted images
- Add instrumentation to the hosting software to monitor internal processes, memory calls, disks, etc.
- Network taps – they can perform man-in-the-middle attacks on all of their hosted systems, and do so completely transparently

Virtual Image Administrators
- Create alternate images that do not conform to the baseline, but report that they do.
- Copy virtual machines or disks
- Modify individual instances of a virtual machine in a cloud so that only some of the cloud behaves the wrong way.

System Administrators
- Traditional OS attacks – root compromises, Trojans, logic bombs, etc.
- Update virtual machine drivers to vulnerable instances

Application Administrators
- Virtual Machine aware attacks [Rutkowska 2006] that target known vulnerabilities in the VM drivers to gain control of the hosting platform.
- Malicious application configurations
- Copy all application data.
Malicious Local Employee

- Exploiting weaknesses of the Cloud
- Using the Cloud against you
Protecting Against Malicious Insiders

- Rogue Administrators
- Those that exploit weaknesses in the Cloud
- Those that use the Cloud against you
Future Research

- Socio-technical approach
- Predictive models
- Identifying cloud-based indicators
- Virtualization and hypervisors
- Awareness and reporting
- Normal user behavior analysis
- Policy integration
CERT Insider Threat Center Objective

Opportunities for prevention, detection, and response for an insider attack
Thank You!

Contact Info:

William R. Claycomb
claycomb@cert.org

Lead Research Scientist
CERT Insider Threat Research Center
Carnegie Mellon University