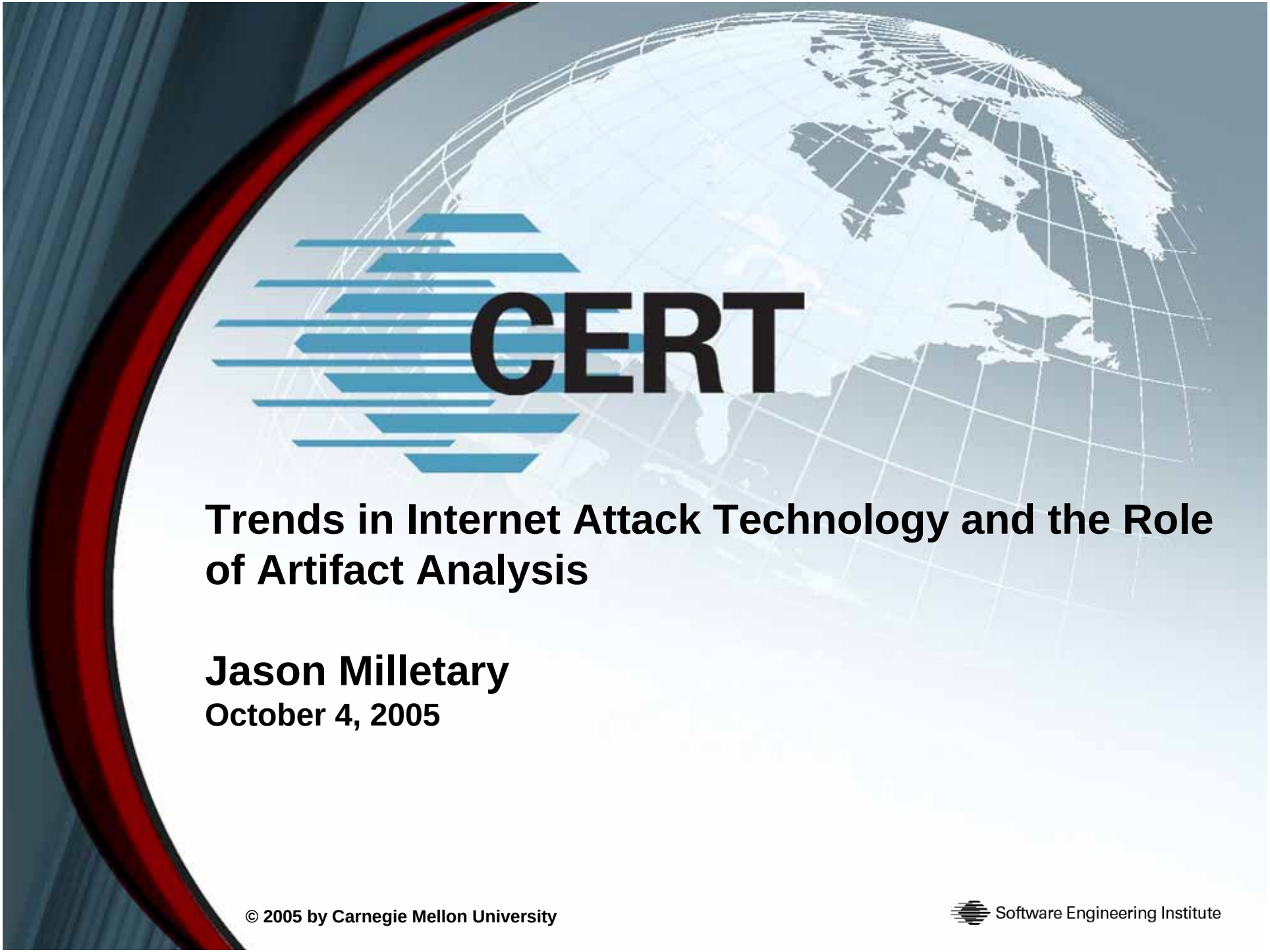



# Trends in Internet Attack Technology and the Role of Artifact Analysis

**Jason Milletary**

**October 4, 2005**

# Overview

- Attack Trends
- Role of Artifact Analysis Capabilities
- Typical Artifact Analysis Capabilities

# Attack Trends

A high level review of the major attacks trends that we have observed at CERT

- Focus on end-user attacks
- Emphasis on use of compromised resources
- Maturation of economic incentive

# End-User Attacks

The rapid increase of phishing and spyware incidents demonstrate a shift towards end-user attacks

- Applications vs. Infrastructure
  - Web browsers
  - Instant Messaging clients
  - Email clients
  - Peer-to-peer clients
- Attack vectors remain the same
  - Vulnerability exploitation
  - Social engineering

# Use of Compromised Resources

2003: Focus on propogation

- Email attachments (e.g., SoBig)
- Worms (e.g., Blaster, Slammer)

2004: Focus on use of resources

- Information stealing
- DDoS agents
- Services
- Remote control
- Survivability

# Information Stealing

Evolving mechanisms

- Keystroke loggers
- Web form scraping
- Screen captures
- HTTP URI interception
- Microsoft Protected Store enumeration

Information of Value

- Authentication credentials
  - Online banking sites
  - Financial services sites
  - Payment system sites
  - E-government
- Email addresses
- Documents (PDF, Word, Excel, etc.)

# Distributed Denial of Service (DDoS)

DDoS Agents

- Technology is not new
- Refining command and control
- Refining modus operandi

Use of DDoS

- Extortion
- Corporate sabotage

# Services

## Email Gateways

- Deployment of email delivery infrastructure
- SPAM, Phishing, malware delivery
- Distributed and disposable
- Track and trace becomes difficult

## Servers

- Websites for phishing and/or malware distribution
- Proxy services
- FTP server for “warez” or collection of stolen data

# Remote Control

Botnets

- Integration of functionality
- Predominantly IRC-based command and control
  - Emergence of other protocols (HTTP,P2P,IM)
- Mobile, adaptable, distributed

# Survivability

Attack chaining

- Combinations of social engineering and vulnerability exploitation
- Multiple components, one goal (money)

"Secure" compromised resources

- Disable anti-virus, personal firewalls, etc
- Disable other malware
- Secure system (patch, disable services)
- Hide malware presence (e.g., rootkits)

# Economic Incentive

The use of malware as tools for crime has promoted the development of a sophisticated economic system

- Follow the money
  - Financial gain is growing incentive for attacks
  - Low risk of legal repercussions
  - Legal and law enforcement environments critical
- Skills specialization
  - Malware authoring
  - Resource acquisition / malware deployment
  - Attack execution
  - Data recovery

# What is Artifact Analysis?

The study of Internet attack technology, otherwise known as malicious code, or “malware”

- Viruses
- Worms
- Trojan horses
- Rootkits
- Botnets
- Denial-of-service tools
- Vulnerability exploits

# Who does Artifact Analysis?

Artifact analysts include

- Computer Security Incident Response Teams
- Security product vendors (AV, IDS/IPS, etc.)
- Managed Security Service Providers
- Software vendors
- Enterprises / organizations
- Governments, law enforcement
- Attackers

# Roles of Artifact Analysis

- Incident response
- Vulnerability analysis
- Attack technology trends
- Threat assessment
- Capability assessment
- Law enforcement / forensics
- Signature generation
- Attacker competition

# Role: Incident Response

One of the roots of artifact analysis can be found in the incident response process

- Malicious code often involved in security incidents
- Need to understand attack methods used in incident in order to respond
- Communicate threats, impact, and protective measures to constituency

# Role: Vulnerability Analysis

Artifact analysis can provide insight into the mechanics and lifecycle of vulnerability exploitation

- Exploits for vulnerabilities are developed, improved, and re-used
  - Scope of vulnerability can change
- Existence of working exploit can escalate response to a vulnerability
- Understanding an exploit can expand understanding of vulnerabilities
  - Current remediation may be insufficient

# Role: Attack Technology Trends

Artifact analysis provides insight to the constantly evolving nature of internet attacks

- Effective attack techniques are re-used
- Attack techniques evolve
  - New targets of opportunity
  - Resist countermeasures
- New classes of attack techniques can present challenges for extended periods of time
- Understanding enables focus on classes of security issues

# Role: Threat Assessment

Artifact analysis can help direct incident response policy by helping to determine threat

- Determining current threat posture requires, in part, understanding of attack technology
- Which malware threats require drop-everything action? Which require long-term analysis? Which require no action?
- What is the threat assessment for potential or anticipated malware capabilities?

# Role: Capability Assessment

Understand the capabilities of the attacker community provides insight to those designing and implementing security mechanisms

- Malware varies in complexity and capability
- Classes of attack techniques vary in maturity of available attack tools
- Development and deployment of attack tools require different skill sets
- Assessing capability requires understanding and contrasting attack technology and methodology

# Role: Law Enforcement / Forensics

Artifact analysis can add value to law enforcement and forensics investigations

- Malware analysis may provide evidence of crime
  - Compromised financial information
- Collection of known malware used as comparison set for forensics discovery
- Forensics recovers artifacts, artifact analysis discovers functionality of recovered artifacts
  - Additional evidence for investigation or prosecution

# Role: Signature Generation

Security product vendors rely on artifact analysis to provide timely and accurate detection/prevention

- Intrusion Detection / Prevention
  - Signatures based on classes of attacks
  - Classes of attacks evolve
  - Produce signature targets
  - Aid understanding of triggered signatures
- Anti-Virus / Spyware detection
  - Signatures generated through artifact analysis

# Role: Attacker Competition

In addition to countering responses from the security community, intruders are driven by competition with each other

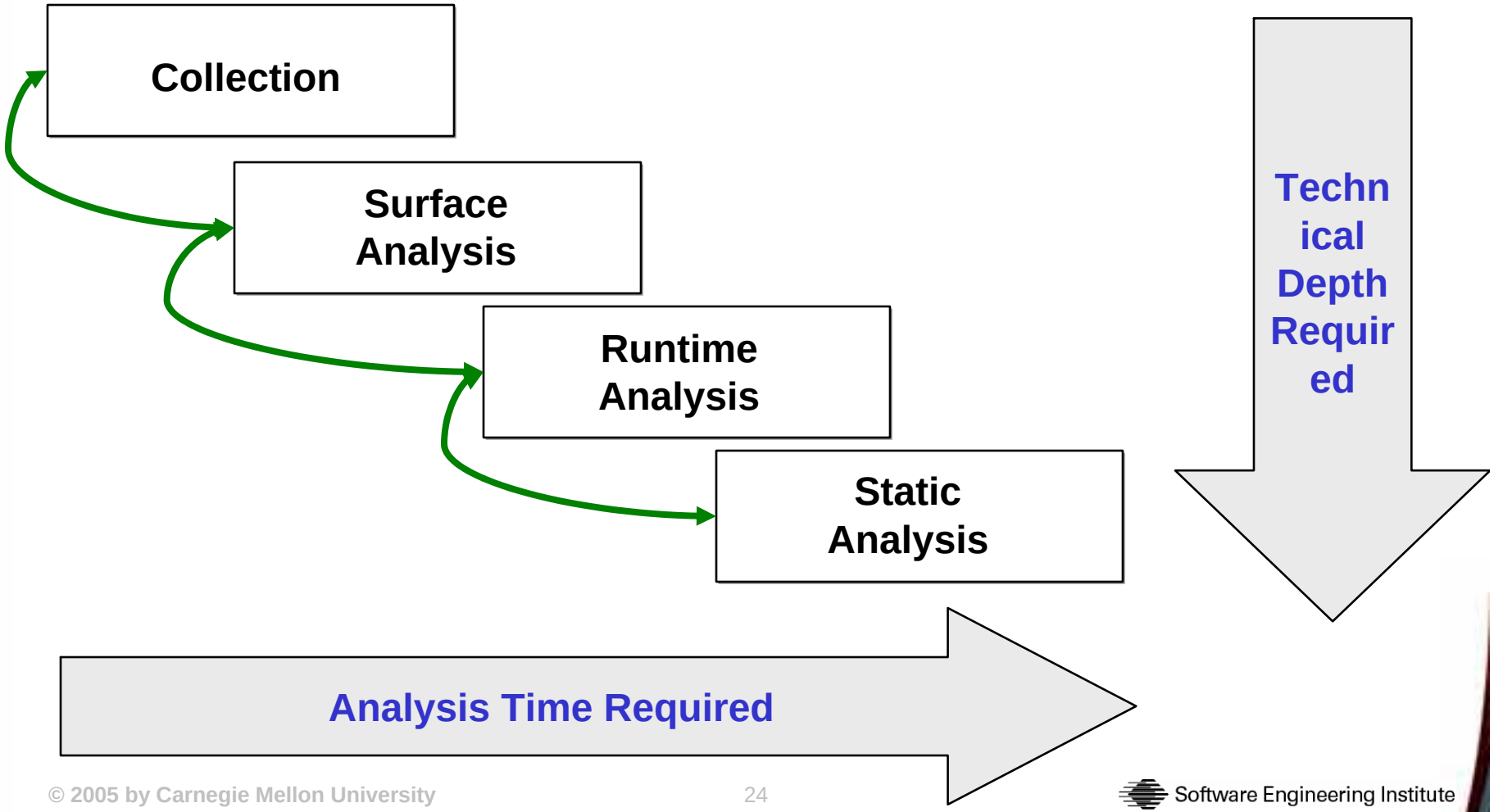
- Exploiting deployed malware
  - "Stealing" compromised resources
    - Netsky vs. Mydoom
    - Botnet hijacking
  - Adaptation of functionality
- Competition for resources
  - SMTP relay and proxy for SPAM/Phishing
  - Denial-of-service agents
  - Proxies
  - Malware launch points
  - Compromised resources / information

# Degrees of Analysis / Trust

Artifact analysis produces understanding and insights

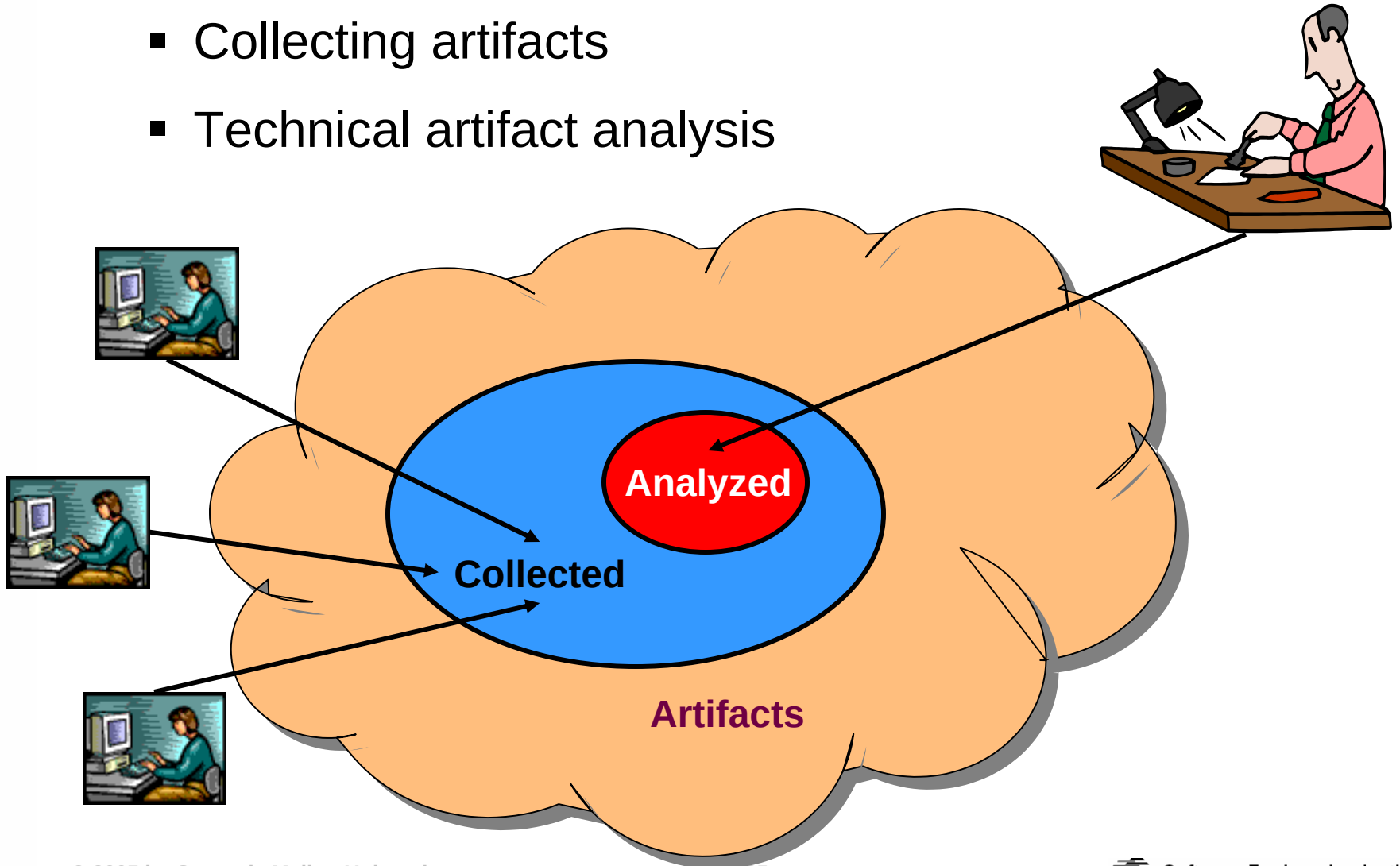
- Degrees of required understanding vary
  - Answering specific questions
  - Authoritatively describing complete functionality
- Consumers must trust analysis
- Artifact analysis capability is a way to create targeted trusted information

# Increased Understanding Requires Increased Resource



# Scope of work

- Collecting artifacts
- Technical artifact analysis



# Prioritization (Deciding What to Analyze)

- Organizational Mission (Qualitative)
- Numeric Weights (Quantitative)
  - Scope – How widespread is the artifact
    - # of reported incidents
    - # of sites
  - Propagation
    - Does the artifact spread, if so, is it automated spread or does it require human intervention (ex. Emailing to other users)?
  - Damage Potential
    - Is the malware destructive to data or availability of resources?
    - Does the malware collect data that could potentially damage the target (ex. Bank account related info of the users)?
  - Impact
  - Difficulty of Remediation
  - Other Areas of Interest to your Organization

# Surface Analysis

Surface analysis includes:

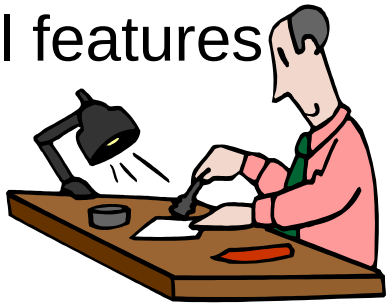
- Quick checks to identify and characterize an artifact
  - File type, MD5 checksum, file size, filename
- Public source analysis
  - Internet searches, mailing lists, AV reports, etc.
- Easily identifiable contents
  - Review of text files
  - Review of source code (if available)
  - Review of strings output
- Comparative analysis against already obtained artifacts
  - String comparisons
  - Comparisons of file sets with similar attributes

Automation, automation, automation…

# Runtime Analysis

Derive artifact function from lab testing

- Starting point based on surface analysis
- Sometimes difficult to uncover and test all features



Rapidly deployable test environments

- In-office virtual labs for easy access
- Sharable image library for multiple platforms
- Undoable disk images - always a fresh install
- Virtual network with DHCP, DNS, SMTP, HTTP, FTP, IRC, packet mangling capabilities, etc.
- Repository of vulnerable software

# Static Analysis

Determine specific or full functionality of an artifact

- When source code is available, interpreting it is the fastest path to complete understanding
- When only binary executables are available, disassembly and reverse engineering are required
- Comprises several steps
  - Disassembly of an executable binary
  - Understanding the assembly
  - Decompilation – rewriting as source code
- Provides a complete picture of an artifact
  - Time intensive
  - Requires great technical depth
  - There are no secrets when complete

# Conclusions

- Internet attacks continue to evolve in the fact of countermeasures and to meet new targets of opportunity
- Artifact analysis can be valuable for those organizations who need to produce insight on the functionality of malicious code
- Artifact analysis capability should be customized to fit an organization's mission and resources

# CERT® Contact Information

CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
4500 Fifth Avenue
Pittsburgh PA 15213-3890
USA

Hotline: +1 412 268 7090

CERT personnel answer 8:00 a.m. — 5:00 p.m. EST(GMT-5) / EDT(GMT-4), and are on call for emergencies during other hours.

Fax: +1 412 268 6989

Web: http://www.cert.org/

Email: cert@cert.org

# Questions? Feedback?