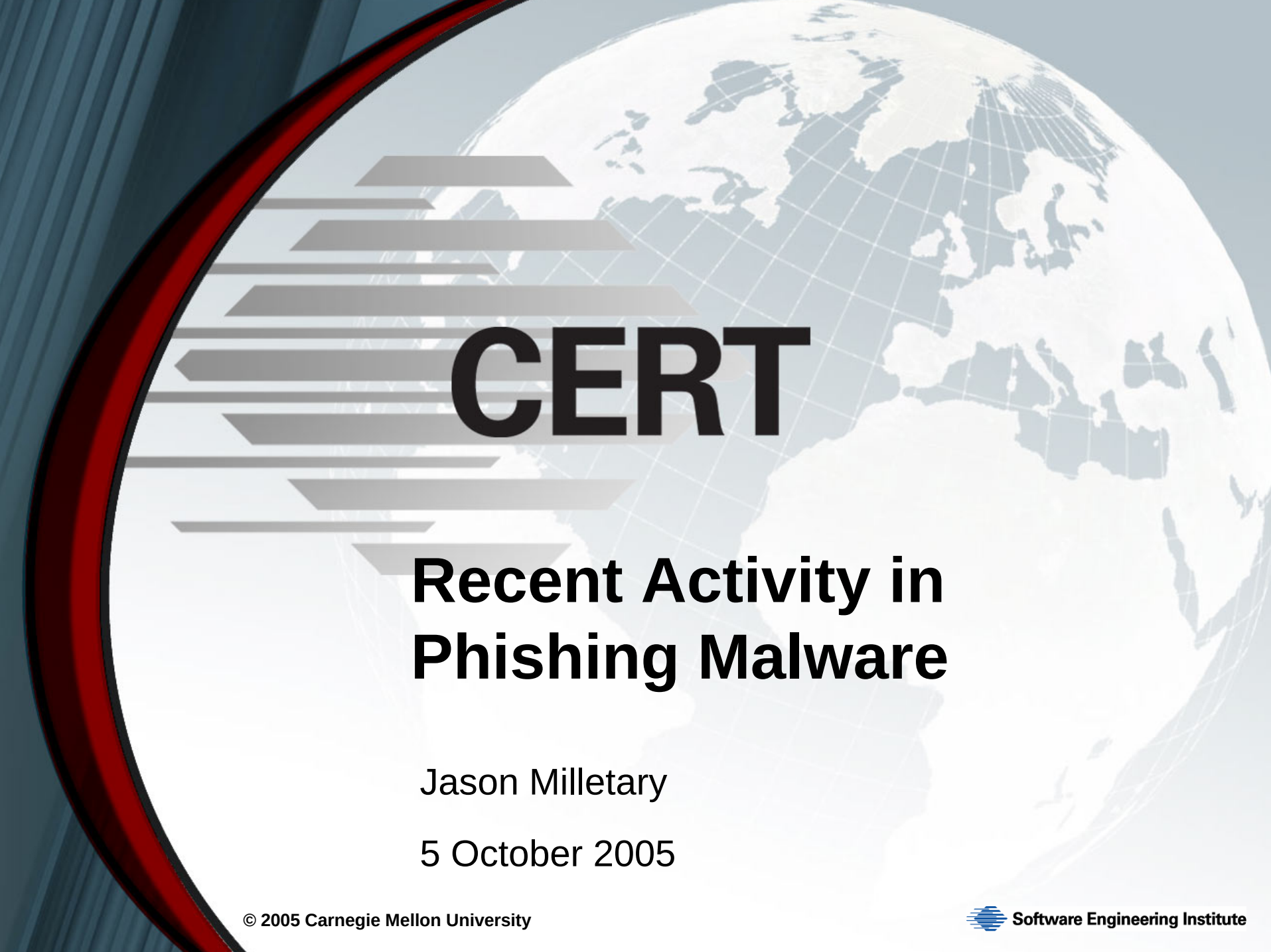


Recent Activity in Phishing Malware

Jason Milletary

5 October 2005

© 2005 Carnegie Mellon University

Overview

- Phishing perceptions
- Phishing malware
- Trends
- Examples

Phishing Perceptions

Phishing and related banking and identity theft crimes have manifested themselves differently across the globe (at least from our US-centric point of view)

- United States
  - Awareness has traditionally focused towards scam emails and sites
  - Increase in use of phishing malware
- Brazil
  - Phishing malware a major threat for the last few years
- Europe/Australia
  - Significant rise in phishing malware over the past year

Need help from you to fill in the gaps!

2005 Carnegie Mellon University

So what am I talking about?

The following terms have been used to refer to malware that targets online banking and related commerce systems

- Keystroke loggers
- Spyware
- Banking trojans
- Phishing malware

Advantages of Malware

Malware provides criminals with several advantages over scam emails and websites

- Increased ROI for attackers
  - Target multiple sites at once
  - Simple to modify existing malware
- Stealthier than email-based phishing
- Increased technical sophistication

Through its artifact analysis work, CERT/CC is working to understand the evolving capabilities of this class of malware

2005 Carnegie Mellon University

Malware Countermeasures

Currently, we are seeing various techniques to mitigate against malware that targets online banking and commerce information

- Virtual Keypads
  - Attempt to protect against keystroke loggers
- Dynamic credentials
  - Two-factor authentication
  - Some institutions provide an additional PIN, and will ask for a random selection of digits from this PIN at login
  - Also use personal questions
- Transaction Numbers (TANs)
  - Transaction-level authentication

Evolution of Malware

A significant trend we are observing is the continual evolution of malware capabilities that improve effectiveness and survivability

- Effectiveness of data capture
  - Keystroke logging
  - Targeted logging
  - Web form scraping
  - Screen captures
  - Fake web pages
- Survivability
  - Dynamic update
  - Anti-analysis
  - Obfuscation
  - Encryption

CERT

Keystroke Logging

A common term used when describing phishing malware

- Focus on web browser traffic
- Combination of generic and specific keywords to enable logging
- Generally do not record all keystrokes
- Dedicated or part of more complex malware (bots)

Mechanisms (Focus on Windows)

- Internet Explorer Automation
- API Function Hooking
- Keyboard Hooks

While “technically correct” in most cases, this term can understate the capability

Internet Explorer Automation

Automation

- Uses Common Object Model (COM)
  - Formerly known as OLE Automation
- Allows client applications to create and manipulate exposed objects from another application
- Internet Explorer provides robust interfaces for monitoring for specific events and controlling properties
  - DWebBrowserEvents
  - IWebBrowser2

CERT

Internet Explorer Automation

- Monitor for specific browser events
  - Before navigation
  - Change in menu bar
  - Page load completed
  - Browser exit
- Read and modify web page properties
  - Navigate to specific pages
  - Read contents of input elements
  - Replace specific elements within web pages
  - Automate user actions (e.g. form submit)
- Framework for different data theft techniques
  - URI/POST interception (“keystroke logging”)
  - Web form scraping
  - Web page/element overlays

CERT

API Function Hooking

Some malware will leverage the use of established API calls used by web browsers

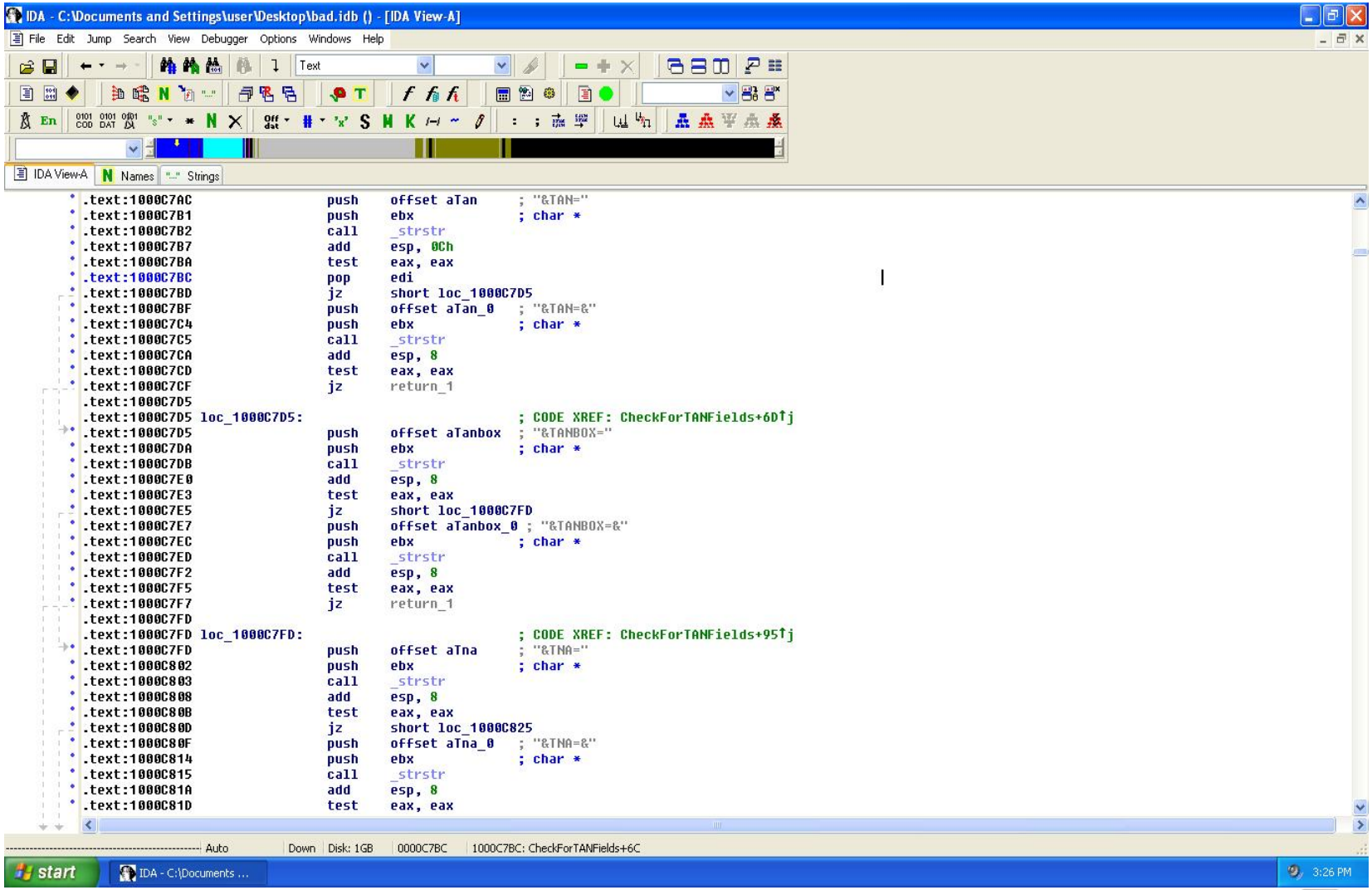
- Microsoft Windows provides API for HTTP
  - HttpSendRequestA
  - InternetCrackURLA
- Web browser process is tricked into calling a wrapper function that has access to parameters
  - URLs
  - POST data
- Attacks of this type could be browser-independent

Targeted Logging

In addition to targeting specific sites, we are observing malware that will target special authentication fields

- We are observing malware attempting to recover TANs (transaction numbers)
- Also observing malware that will attempt to block access to site after a TAN is stolen to increase the time window stolen data is useful

Example of TAN Harvesting



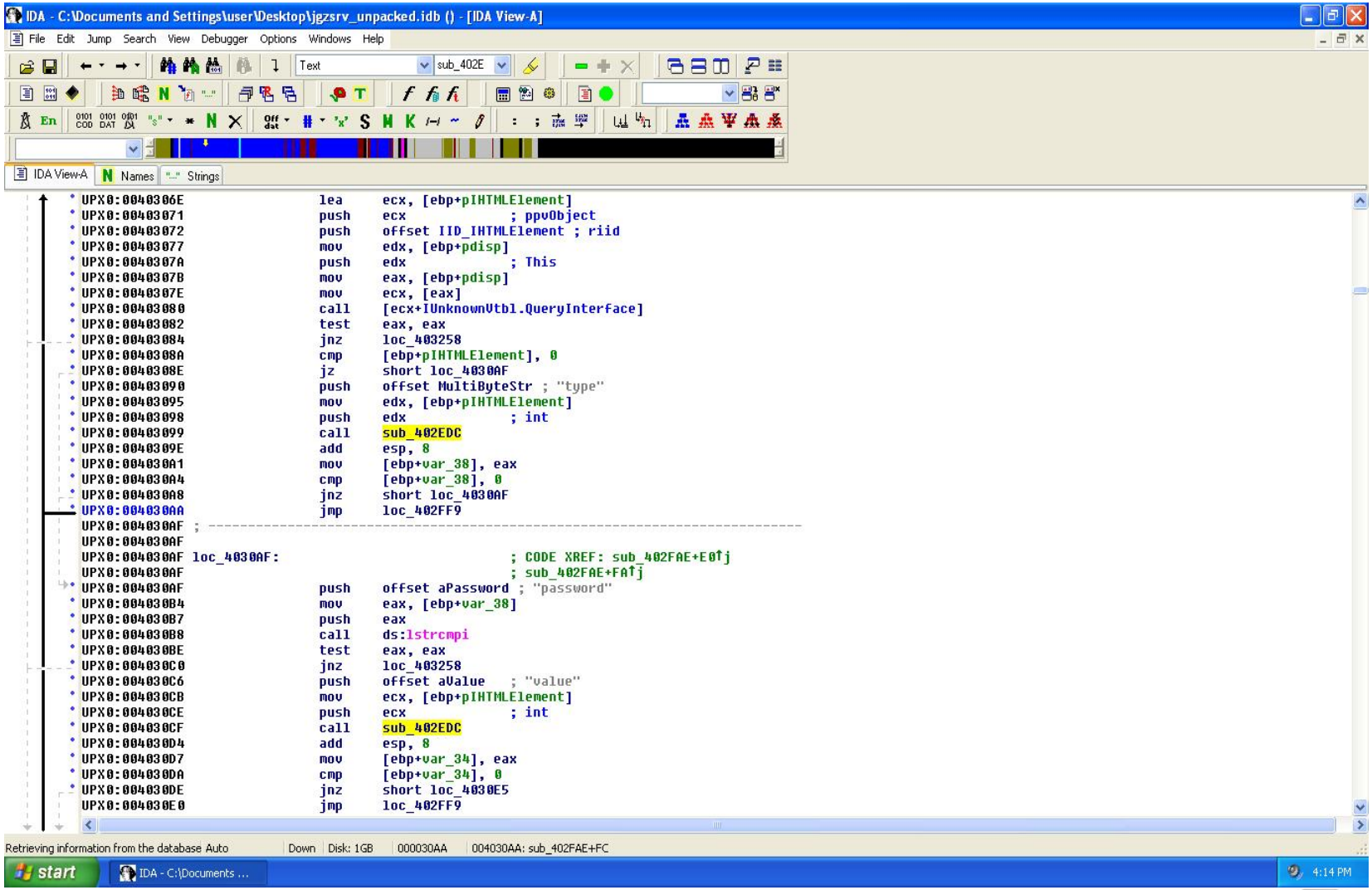
Web Form Scraping

Malware is able to leverage Microsoft Internet Explorer's COM interfaces to "scrape" values from a web form

- IHTMLDocument2 interface provides programmatic access to all elements within a web page in Internet Explorer
- This technique uses often-used or known field names (e.g. "password")
- Can also be used against some virtual keypad implementations

CERT

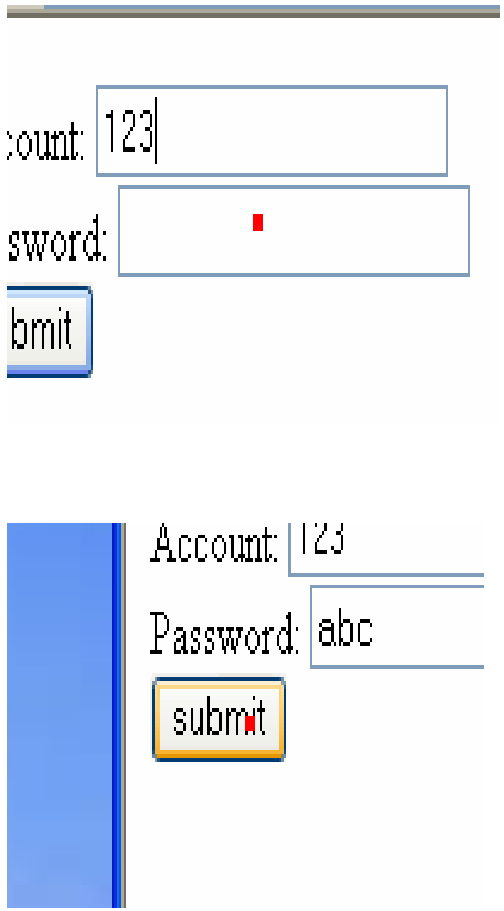
Example of Form Scraping



Screen Captures

Several different varieties of malware have the capability of captures screen shots

- Virtual keypads
  - Take screen shot at every mouse click on a specific screen
- Account Information
  - Take screen shot on specific screens to capture account details (e.g. balance, passwords)



Survivability

Malware authors are taking more steps to protect their code and data from analysis by the security industry and their competition

- PE packers/protectors
  - Thwarts casual identification via strings
  - Bypass AV detection
- String obfuscation
  - Targeted sites
  - Drop sites
- Debugger/Virtual Machine detection
- Encryption
  - Occasionally used to protect stolen information

Dynamic Updates

Malware is adding capabilities to be updated dynamically

- Downloading and executing new malware is a common and well-established capability
- Bots
  - Can be configured from command and control
- Phishing malware
  - Configuration data can be configured dynamically
    - Drop sites
    - Malware to download

Examples

Examples of banking malware that utilizes these capabilities

- Bancos
- Grams
- BankAsh

Bancos

A common name for malware that targets Brazilian banks

- Numerous variants active for over 2 years
- Some versions will generate a fake web browser that mimics a banks login screen
- Some versions have screen capture ability
- Most versions have their own SMTP engine for emailing stolen data
- Versions written in Visual Basic and Delphi

Grams

Grams represented a unique threat vector

- Account siphoner targeting Internet Explorer users of an online funds transfer site
- Use Automation to control Internet Explorer instance for an already authenticated session
  - Transferred funds to another account
- Would not be prevented by two-factor authentication

Technique has not been knowingly reproduced

- Technically complex
- Current methods are adequate

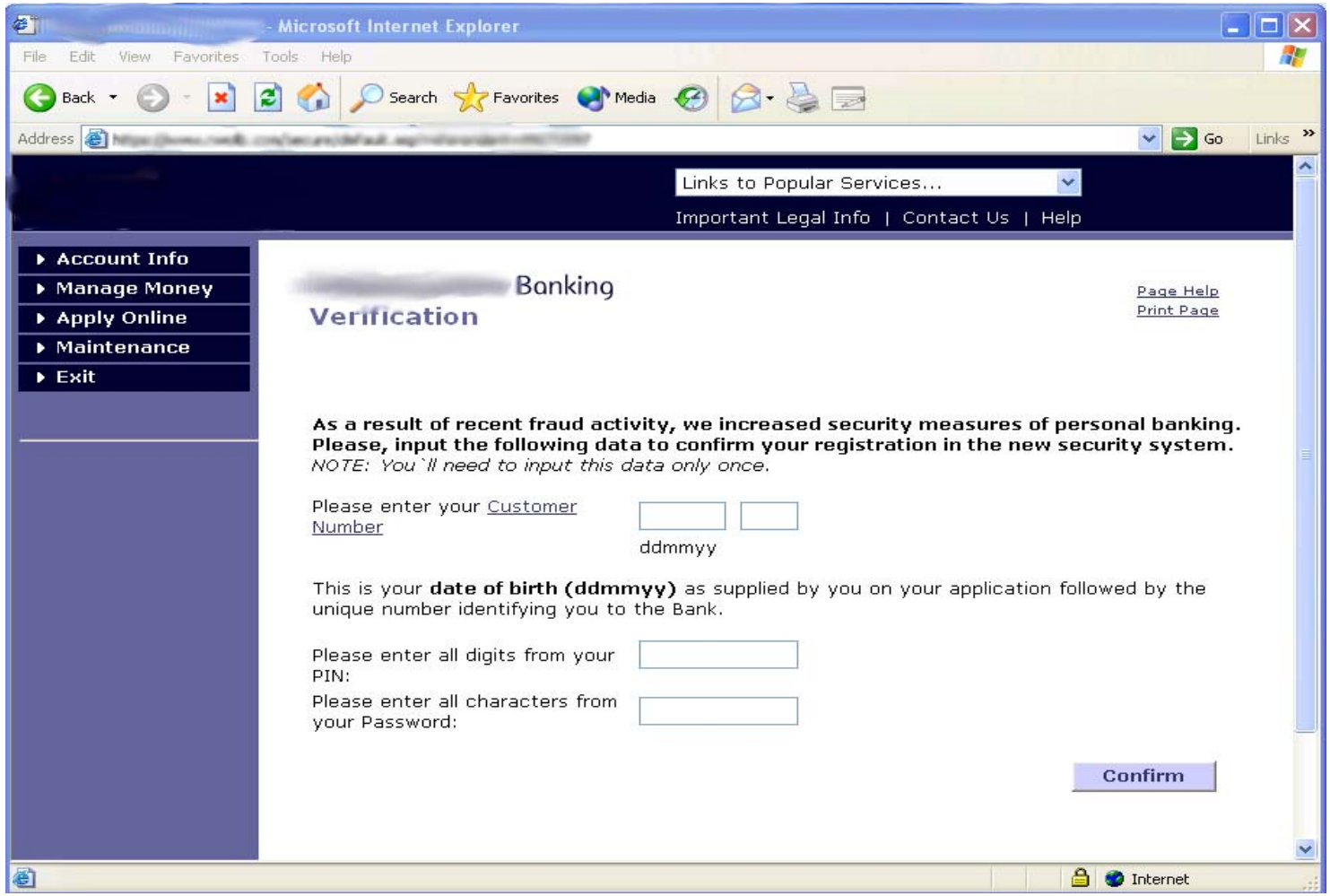
2005 Carnegie Mellon University

BankAsh

Implemented as a COM object to receive events from Internet Explorer

- Targets banks in several countries
- Attempts to steal POST data during SSL sessions
- Looks for banks and URL characteristics that may indicate an online bank that uses TANs
  - Specially tag the stolen data
  - Attempt to block user access to web site
- Uses embedded HTML and Automation to overlay login pages with phish page as another information capture mechanism
  - Targets banks that use a dynamic representation of credentials
- Contains blacklist of sites not to log POST data for
- Attempting to disable AV, firewalls, anti-spyware

Real or Phish ????



What are the lessons?

- Malware is becoming a global problem for phishing/identity theft
- Malware quickly evolves as countermeasures are developed
- Financial institutions should be aware of potential threats even when they are not actively targeted
- Avoid focusing narrowly on these tools when developing policies (security and legislative) and security countermeasures

Questions? Feedback?

CERT