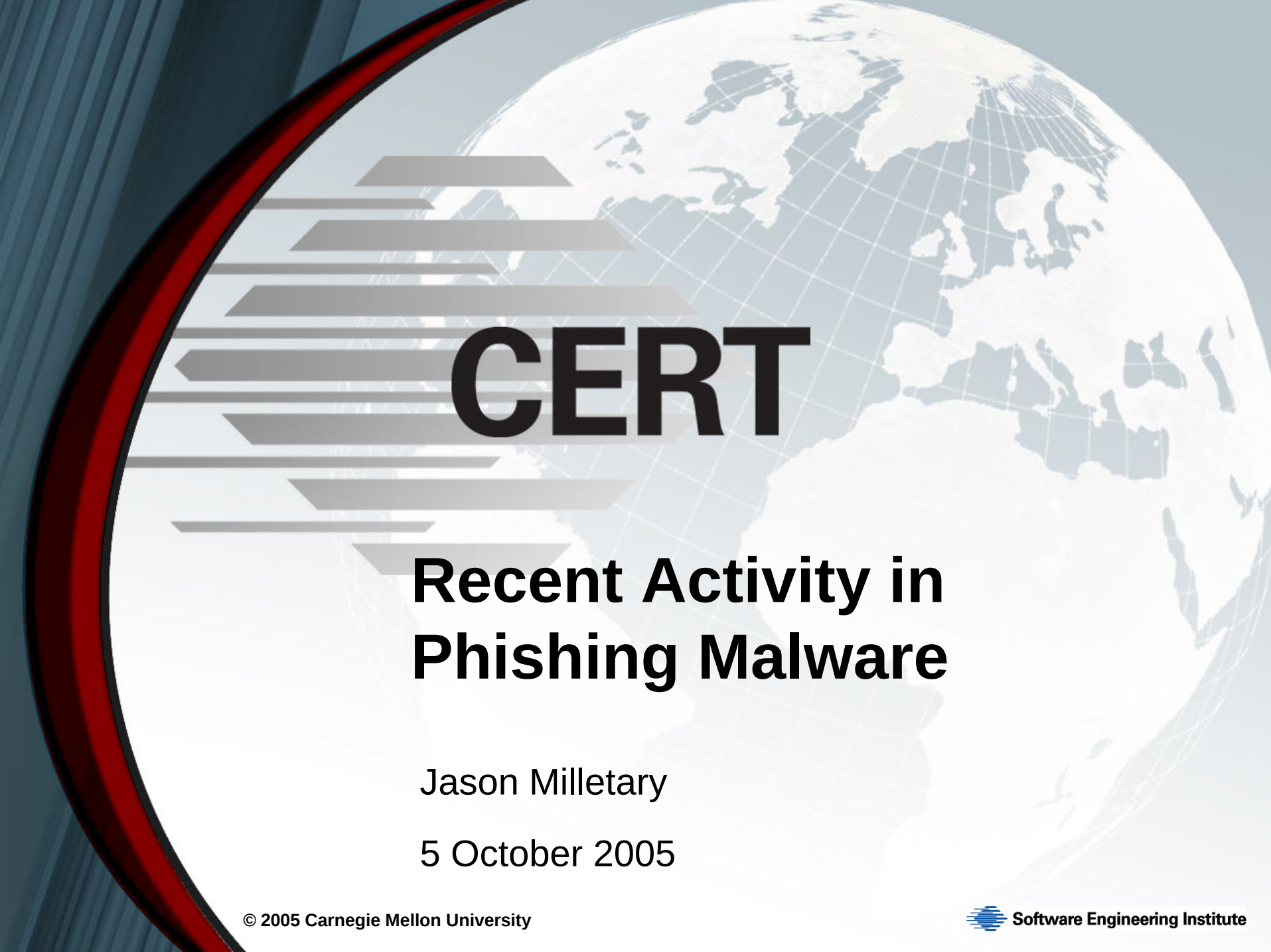




CERT

Recent Activity in Phishing Malware

Jason Milletary

5 October 2005

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!

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

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

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

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

API Function Hooking

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

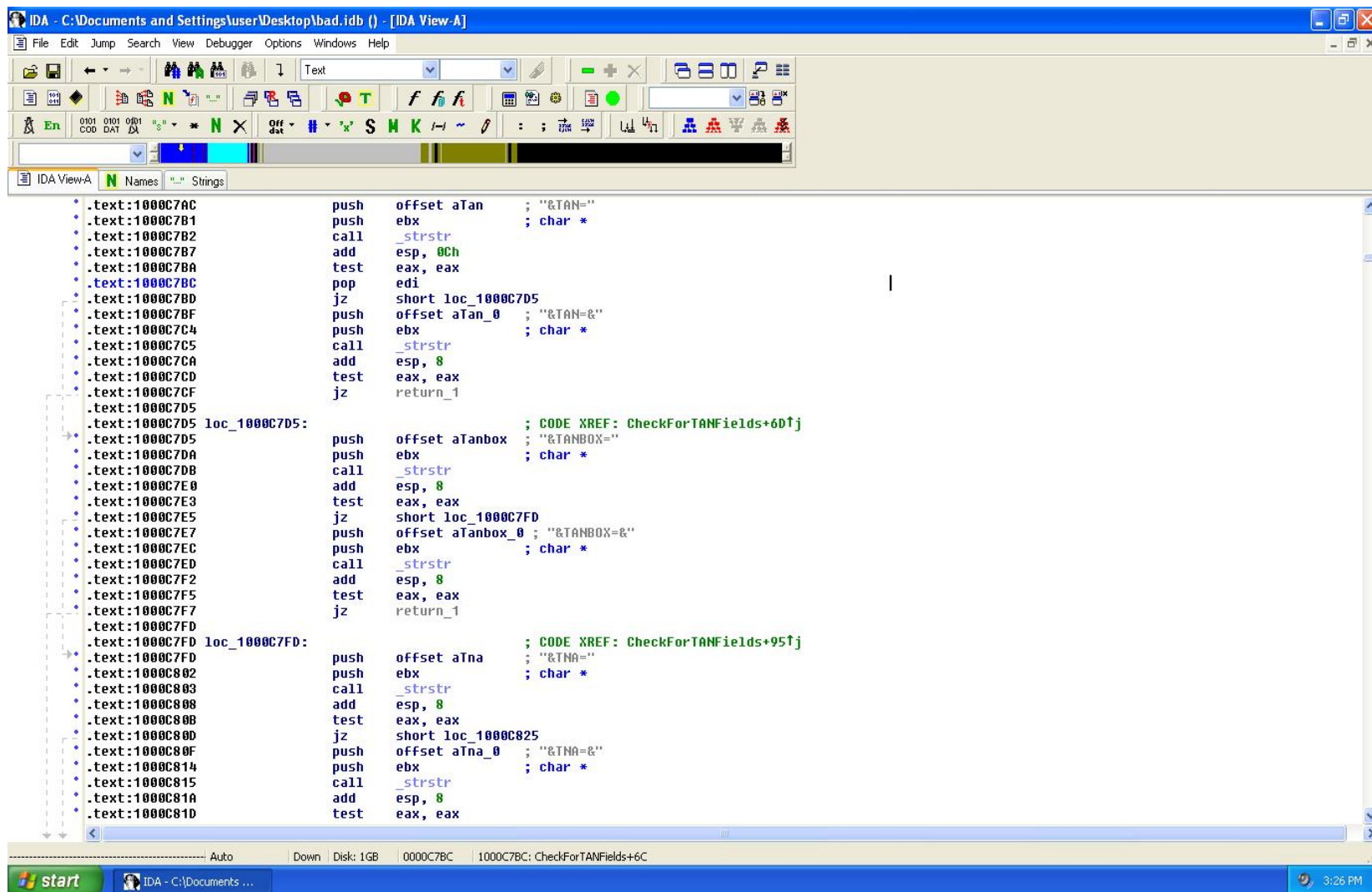
- Microsoft Windows provides API for HTTP
 - HttpSendRequestA
 - InternetCrackURLA
- Web browser process is tricked into calling a wrapper function that has access to parameters
 - URLs
 - POST data
- Attacks of this type could be browser-independent

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



IDA - C:\Documents and Settings\user\Desktop\bad.idb () - [IDA View-A]

File Edit Jump Search View Debugger Options Windows Help

IDA View-A Names Strings

```
.text:1000C7AC      push     offset aTan      ; "&TAN="
.text:1000C7B1      push     ebx              ; char *
.text:1000C7B2      call    _strsr
.text:1000C7B7      add     esp, 0Ch
.text:1000C7BA      test    eax, eax
.text:1000C7BC      pop     edi
.text:1000C7BD      jz      short loc_1000C7D5
.text:1000C7BF      push    offset aTan_0    ; "&TAN=&"
.text:1000C7C4      push    ebx              ; char *
.text:1000C7C5      call    _strsr
.text:1000C7CA      add     esp, 8
.text:1000C7CD      test    eax, eax
.text:1000C7CF      jz      return_1
.text:1000C7D5      loc_1000C7D5:           ; CODE XREF: CheckForTANFields+60↑j
.text:1000C7D5      push    offset aTanbox   ; "&TANBOX="
.text:1000C7D8      push    ebx              ; char *
.text:1000C7DB      call    _strsr
.text:1000C7E0      add     esp, 8
.text:1000C7E3      test    eax, eax
.text:1000C7E5      jz      short loc_1000C7FD
.text:1000C7E7      push    offset aTanbox_0 ; "&TANBOX=&"
.text:1000C7EC      push    ebx              ; char *
.text:1000C7ED      call    _strsr
.text:1000C7F2      add     esp, 8
.text:1000C7F5      test    eax, eax
.text:1000C7F7      jz      return_1
.text:1000C7FD      loc_1000C7FD:           ; CODE XREF: CheckForTANFields+95↑j
.text:1000C7FD      push    offset aTna      ; "&TNA="
.text:1000C7FD      push    ebx              ; char *
.text:1000C802      call    _strsr
.text:1000C803      add     esp, 8
.text:1000C808      test    eax, eax
.text:1000C80D      jz      short loc_1000C825
.text:1000C80F      push    offset aTna_0    ; "&TNA=&"
.text:1000C814      push    ebx              ; char *
.text:1000C815      call    _strsr
.text:1000C81A      add     esp, 8
.text:1000C81D      test    eax, eax
```

start | IDA - C:\Documents and Settings\user\Desktop\bad.idb () - [IDA View-A]

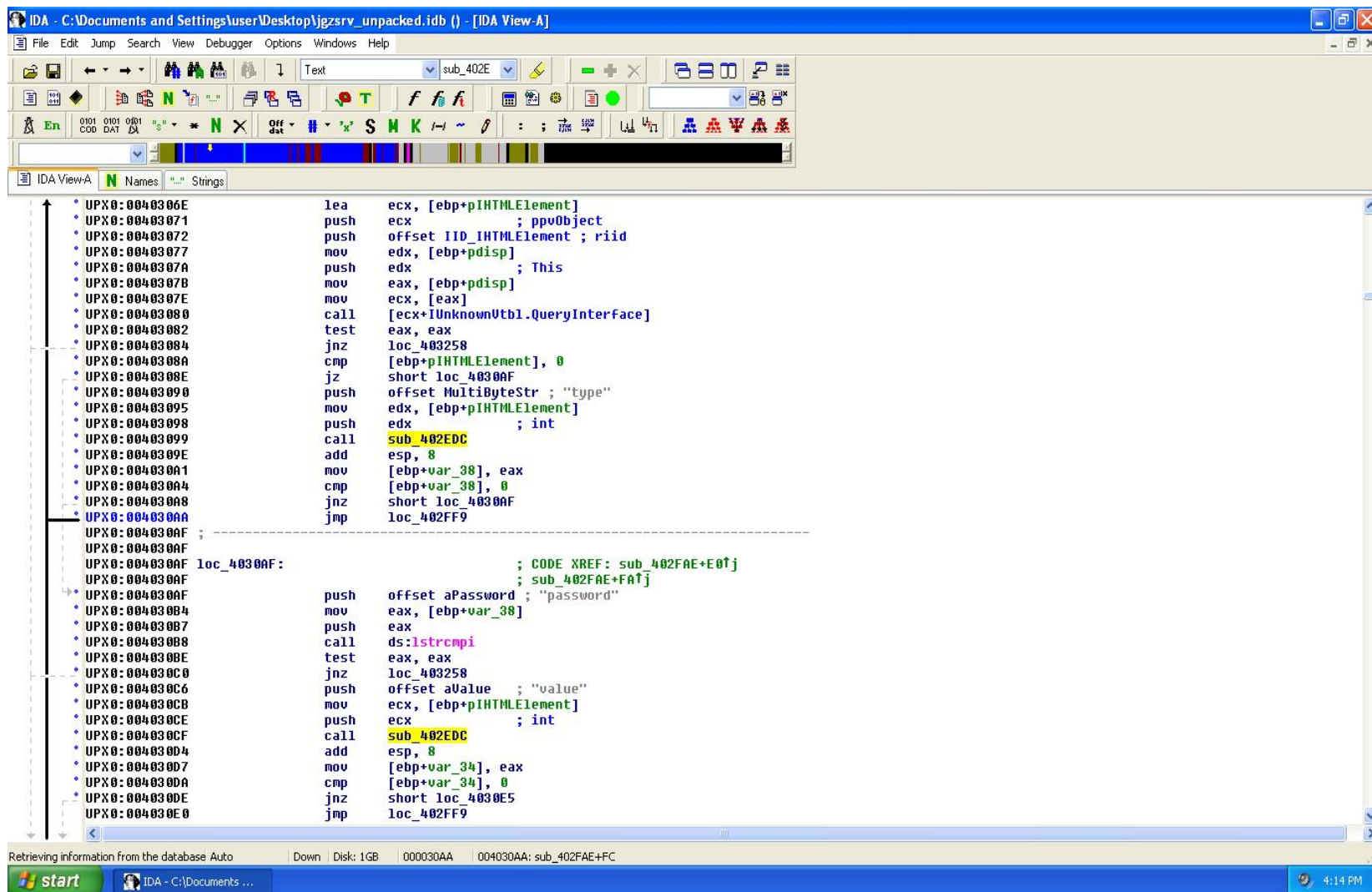
Auto | Down | Disk: 1GB | 0000C7BC | 1000C7BC: CheckForTANFields+6C | 3:26 PM

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

Example of Form Scrapping



The screenshot displays the IDA Pro interface with the assembly view of a function named `sub_402E`. The code is written in x86 assembly and includes comments in English. The routine appears to be a form scraper, as evidenced by the use of `ds:strcmpi` to compare a password and the retrieval of a value from a form. The code is organized into blocks, with a jump to `loc_4030AF` after a series of initial setup and comparison instructions.

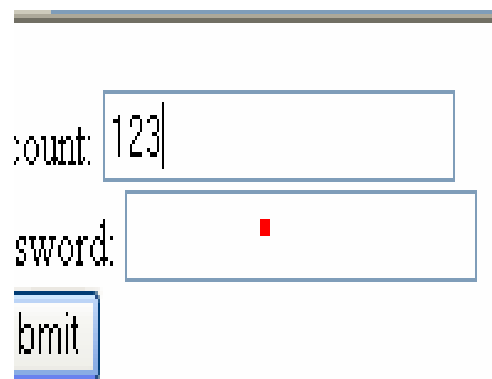
```
UPX0:0040306E lea ecx, [ebp+pIHTMLElement]
UPX0:00403071 push ecx ; ppvObject
UPX0:00403072 push offset IID_IHTMLElement ; riid
UPX0:00403077 mov edx, [ebp+pdisp]
UPX0:0040307A push edx ; This
UPX0:0040307B mov eax, [ebp+pdisp]
UPX0:0040307E mov ecx, [eax]
UPX0:00403080 call [ecx+IUnknownVtbl.QueryInterface]
UPX0:00403082 test eax, eax
UPX0:00403084 jnz loc_403258
UPX0:0040308A cmp [ebp+pIHTMLElement], 0
UPX0:0040308E jz short loc_4030AF
UPX0:00403090 push offset MultiByteStr ; "type"
UPX0:00403095 mov edx, [ebp+pIHTMLElement]
UPX0:00403098 push edx ; int
UPX0:00403099 call sub_402EDC
UPX0:0040309E add esp, 8
UPX0:004030A1 mov [ebp+var_38], eax
UPX0:004030A4 cmp [ebp+var_38], 0
UPX0:004030A8 jnz short loc_4030AF
UPX0:004030AA jmp loc_402FF9

UPX0:004030AF ; CODE XREF: sub_402FAE+E0fj
UPX0:004030AF ; sub_402FAE+FAfj
UPX0:004030AF push offset aPassword ; "password"
UPX0:004030B4 mov eax, [ebp+var_38]
UPX0:004030B7 push eax
UPX0:004030B8 call ds:strcmpi
UPX0:004030BE test eax, eax
UPX0:004030C0 jnz loc_403258
UPX0:004030C6 push offset aValue ; "value"
UPX0:004030CB mov ecx, [ebp+pIHTMLElement]
UPX0:004030CE push ecx ; int
UPX0:004030CF call sub_402EDC
UPX0:004030D4 add esp, 8
UPX0:004030D7 mov [ebp+var_34], eax
UPX0:004030DA cmp [ebp+var_34], 0
UPX0:004030DE jnz short loc_4030E5
UPX0:004030E0 jmp loc_402FF9
```

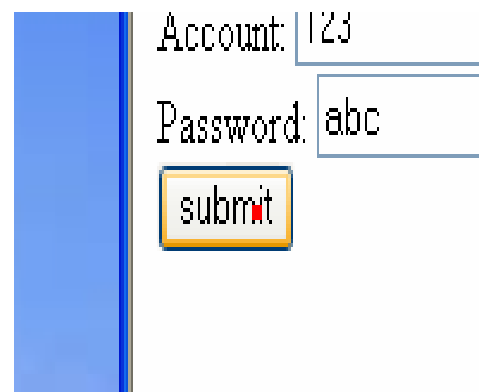
Screen Captures

Several different varieties of malware have the capability of capturing 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)



A screenshot of a web form. At the top is a horizontal progress bar. Below it, the text "count:" is followed by a text input field containing "123". Below that, the text "sword:" is followed by a text input field containing a red square. At the bottom left is a button labeled "bmit".



A screenshot of a web form. On the left is a vertical blue bar. To its right, the text "Account:" is followed by a text input field containing "123". Below that, the text "Password:" is followed by a text input field containing "abc". At the bottom is a button labeled "submit".

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

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 ????

Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Media Print Mail

Address <https://www.webb.com/secure/default.asp?showorder=0011000> Go Links

Links to Popular Services... Important Legal Info | Contact Us | Help

Account Info
Manage Money
Apply Online
Maintenance
Exit

Banking

Page Help
Print Page

Verification

As a result of recent fraud activity, we increased security measures of personal banking. Please, input the following data to confirm your registration in the new security system.
NOTE: You'll need to input this data only once.

Please enter your Customer Number
ddmmyy

This is your **date of birth (ddmmyy)** as supplied by you on your application followed by the unique number identifying you to the Bank.

Please enter all digits from your
PIN:

Please enter all characters from
your Password:

Confirm

Internet

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?

