SOPHOS

Zeus Custom Builds

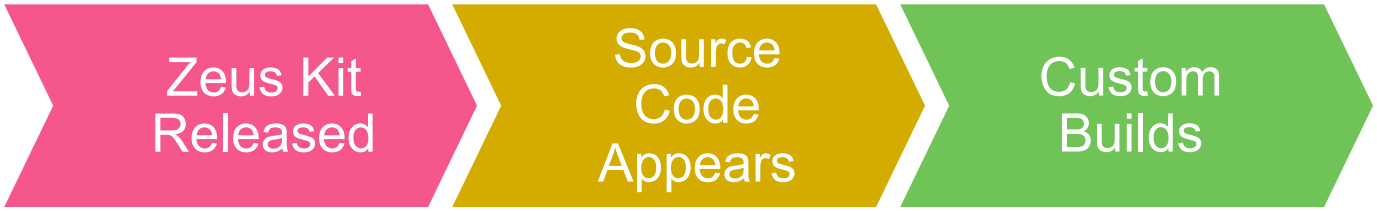
James Wyke

Agenda

- Introduction
- Overview of Source Code Use
- Functionality Modified/Added
- Kit Re-Branding
- Source Used in Other Malware Families
- Conclusions and Implications

Introduction

Introduction



- Rapidly gains popularity
- Several updates

- Slavik/Monstr announces retirement
- Harderman/ Gribodemon “takes over”
- Encrypted rar file appears
- Unencrypted rar file

- SpyEye updates
- Ice IX
- Citadel
- Gameover

Overview of Source Code Use

Overview of Source Code Use

No modification

- Unmodified 2.0.8.9 still prevalent

Modify/Add Functionality, Rebuild

- Encryption changes, C & C address obfuscation, Autorun

Kit Re-branding

- Minor modifications, change “look and feel”
- Major overhaul, significant new features, continuing development

Source Used in Other Malware Families

- Ramnit, SpyEye

Code Modifications

Code Modifications – Key Areas

C & C Address Hiding	• POST requests, P2P
Config File Contents Obfuscation	• New encryption algorithms
Additional Functionality	• Autorun, server side improvements, new bot commands

C & C Address Hiding

Increase the difficulty of tracking the botnet

Configuration File URL

- Harder to download the configuration file

Drop Zone Address

- Harder to find out where the stolen data is sent

C & C Address Hiding Example

Using POST Request Interplay

Config file is not served unless a specially crafted POST request is sent first

C & C Address Hiding Example

Post request has two parameters:

bn1=EXAMPLEPC-4_7875768F6522DF69

"Identifier" string

sk1=C2D72005A5EE8CC230859EFC684E2948

Hash of encrypted string, server performs same operation and compares values

C & C Address Hiding Example

Botnet is slightly harder to track

- Need to know encryption key, algorithm, hash algorithm
- More than just the URL
- Not very difficult for the determined

C & C Address Hiding Example

Using Peer-2-Peer

- Configuration data is obtained from other peers not from a centralized server
- Listens on high numbered UDP and TCP port
- Bot exe contains a bootstrap list of peers to connect to

C & C Address Hiding Example

Botnet is much harder to track

- Configuration data can be obtained, but we must speak the new protocol
- Drop zone now hidden somewhere in the P2P network
- Speculation that this is original author's work

Configuration File Contents Obfuscation

Increase difficulty of tracking botnet

Encryption Algorithm Changes

- AES
- Tweaked RC4

Tweaked RC4

Standard RC4

```
loc_408C70:                             ; CODE XREF: rc4_decryption
   inc     [ebp+i]                      ; i = i + 1
   movzx   esi, [ebp+i]
   mov     dl, [esi+eax]
   add     [ebp+j], dl                  ; j = (j + S[i])
   movzx   ecx, [ebp+j]
   mov     bl, [ecx+eax]
   mov     [esi+eax], bl
   mov     [ecx+eax], dl                ; swap(S[i], S[j])
   movzx   esi, byte ptr [esi+eax]
   mov     ecx, [ebp+data]
   movzx   edx, dl
   add     esi, edx
   and     esi, 0FFh
   mov     dl, [esi+eax]                ; S[(S[i] + S[j]) mod 256]
   xor     [ecx+edi], dl
   inc     edi
   cmp     edi, [ebp+size]
   jb      short loc_408C70
```

Tweaked version

```
loc_A38BA1:                             ; CODE XREF: rc4_decryption
   add     [ebp+i], 3                   ; i = i + 3
   movzx   esi, [ebp+i]
   mov     dl, [esi+eax]
   lea     ecx, [edx+7]                 ; j = (j + (S[i]+7))
   add     [ebp+j], cl
   movzx   ecx, [ebp+j]
   mov     bl, [ecx+eax]
   mov     [esi+eax], bl
   mov     [ecx+eax], dl                ; swap(S[i], S[j])
   movzx   esi, byte ptr [esi+eax]
   mov     ecx, [ebp+data]
   movzx   edx, dl
   add     edx, esi
   and     edx, 0FFh
   mov     dl, [edx+eax]                ; S[(S[i] + S[j]) mod 256]
   xor     [ecx+edi], dl
   inc     edi
   cmp     edi, [ebp+size]
   jb      short loc_A38BA1
```

Tweaked RC4

Very minor modifications

- Lookup stage changed to use i+3 rather than i+1 and S[i]+7 rather than S[i]
- Botnet trackers must update configuration file processing scripts
- Do modifications weaken algorithm? Biased output byte?

AES

Completely substitute RC4 for AES

- 128 bit key, ECB mode
- Several different variants
- Sometimes offered as additional “feature” at extra cost

Consequences

- Existing trackers cannot read configuration data, cannot track
- Botnet trackers must update their tools
- Remediation/Forensic tools need to be updated
- But that’s pretty much all…

Additional Functionality

Autorun

- Basic autorun functionality - exe copies itself to root of drives
- Common spreading mechanism, now added to Zbot
- Demonstrates how easily a new infection vector can be added

Additional Functionality

New Bot Commands

Standard 2.0.8.9

os_shutdown
os_reboot

bot_uninstall
bot_update

bot_bc_add
bot_bc_remove
bot_httpinject_disable
bot_httpinject_enable
fs_path_get
fs_search_add
fs_search_remove
user_destroy
user_logoff
user_execute
user_cookies_get
user_cookies_remove
user_certs_get
user_certs_remove
user_url_block
user_url_unblock
user_homepage_set
user_ftpclients_get
user_emailclients_get
user_flashplayer_get
user_flashplayer_remove

IceIX

os_shutdown
os_reboot

bot_uninstall
bot_update
bot_update_exe
bot_bc_add
bot_bc_remove
bot_httpinject_disable
bot_httpinject_enable
fs_path_get
fs_search_add
fs_search_remove
user_destroy
user_logoff
user_execute
user_cookies_get
user_cookies_remove
user_certs_get
user_certs_remove
user_url_block
user_url_unblock
user_homepage_set
user_ftpclients_get
user_emailclients_get
user_flashplayer_get
user_flashplayer_remove

P2P

os_shutdown
os_reboot

bot_uninstall

bot_bc_add
bot_bc_remove
bot_httpinject_disable
bot_httpinject_enable
fs_find_add_keywords
fs_find_execute

user_destroy
user_logoff
user_execute
user_cookies_get
user_cookies_remove
user_certs_get
user_certs_remove
user_url_block
user_url_unblock
user_homepage_set

user_emailclients_get
user_flashplayer_get
user_flashplayer_remove

Citadel

os_shutdown
os_reboot
url_open
bot_uninstall
bot_update

bot_bc_add
bot_bc_remove
bot_httpinject_disable
bot_httpinject_enable
fs_path_get
fs_search_add
fs_search_remove
user_destroy
user_logoff
user_execute
user_cookies_get
user_cookies_remove
user_certs_get
user_certs_remove
user_url_block
user_url_unblock
user_homepage_set
user_ftpclients_get
user_emailclients_get
user_flashplayer_get
user_flashplayer_remove

module_execute_enable
module_execute_disable
module_download_enable
module_download_disable
info_get_software
info_get_antivirus
info_get_firewall
dns_filter_add
dns_filter_remove

New Bot Commands

Minor

- bot_update_exe

Improvements

- fs_find_add_keywords
- fs_find_execute
- Now actually implemented

Brand New

- url_open
- module_*
- info_get_*

Additional Functionality

Server Side Improvements

- Cosmetic improvements to the interface
- Management improvements
- Plugins
- Security enhancements

Re-Branding The Zeus Kit

Kit Re-Branding

Modifications sold as new kit

Minor Mods

- Builder and control panel
- Some differentiating feature

Complete Overhaul

- Significant amounts of new code
- Some core functionality re-written/added
- Is this still Zeus?

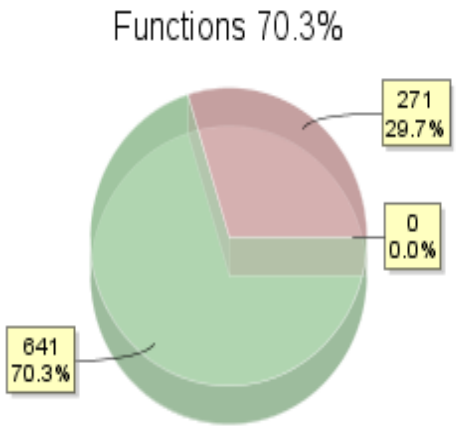
Kit Re-Brand Example

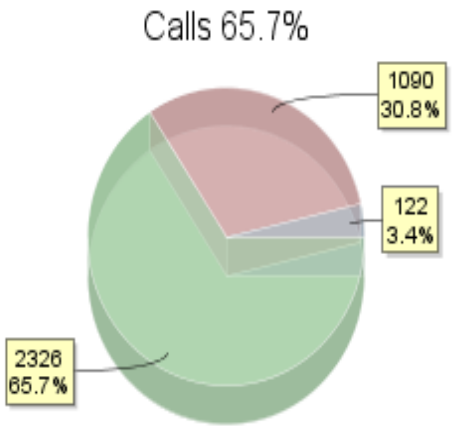
Ice IX

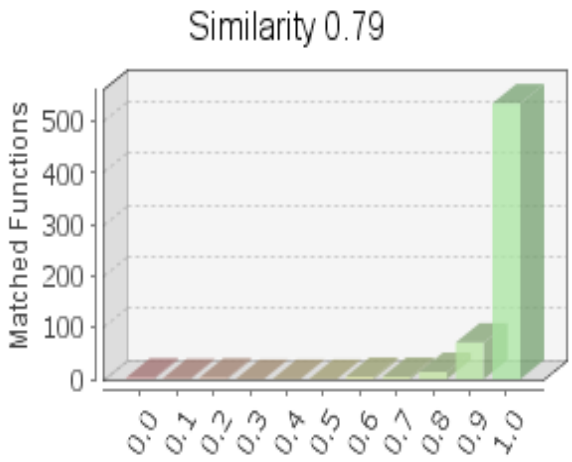
- One of the earliest new kits based on Zeus code
- Advertised as Zeus with “enhancements”
- Only significant modification – POST interplay to retrieve config file
- “Tracker protection”

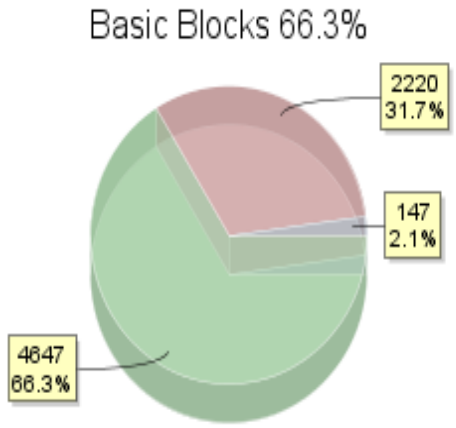
Ice IX

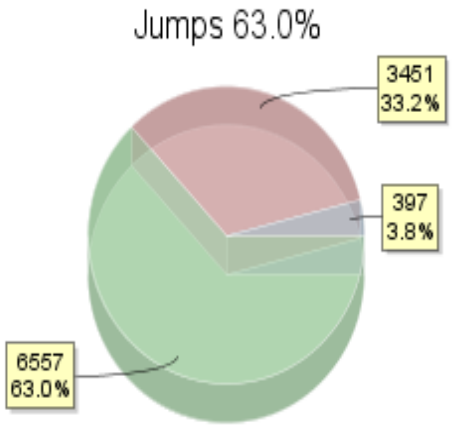
Code Comparison

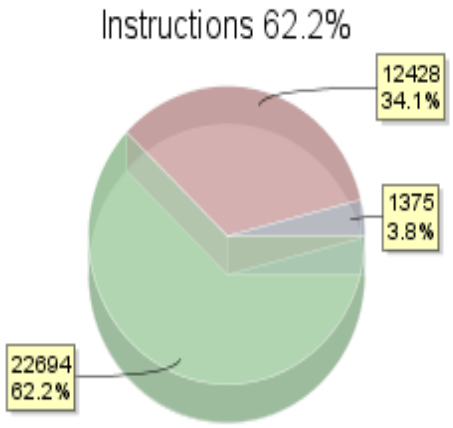












SOPHOS

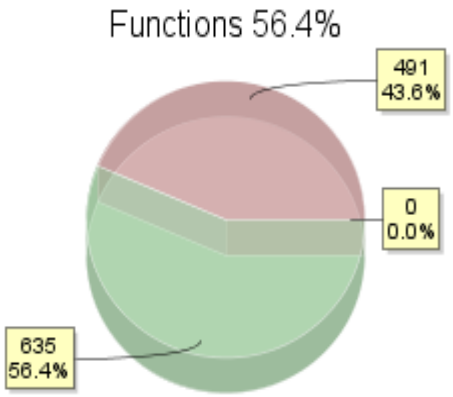
Kit Re-Brand Example

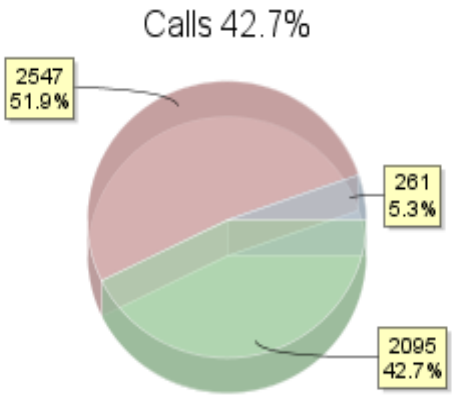
Citadel

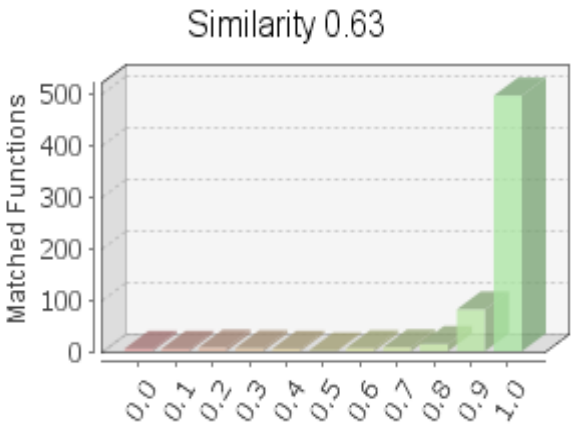
- Significant code modifications
- New functionality – DNS redirects, video grabbing
- Module loading framework
- Information on installed software
- Zeus code genuinely used as a “base”

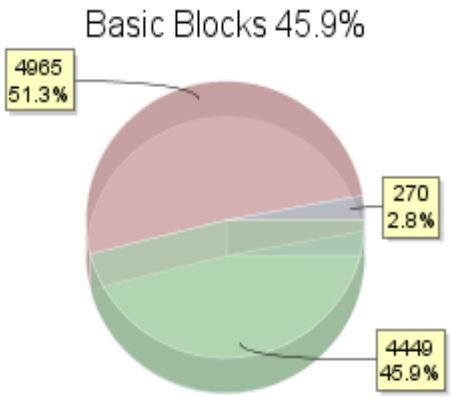
Citadel

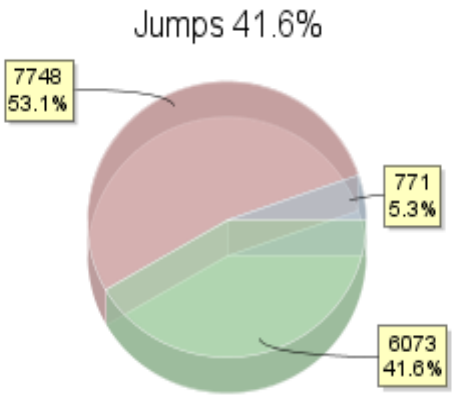
Code Comparison

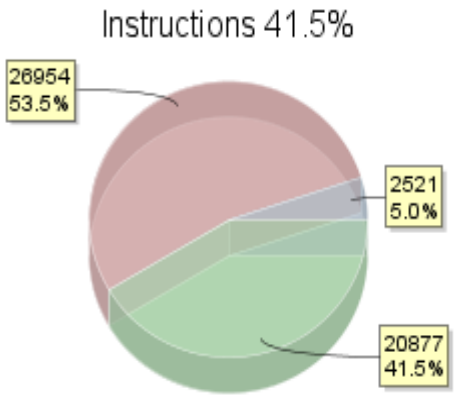












SOPHOS

Source Code In Other Families

Source Code In Other Families

Ramnit

- Form grabber code taken from Zeus

SpyEye

- Mostly control panel changes - SpyZeus

Conclusions and Implications

Pros and Cons

Pro

- Zeus as we knew it is dead

Con

- Several new families instead of one

Pros and Cons

Pro

- Multiple families using common code base, source code available for analysis
- Many areas of code remain untouched

Con

- Active development for multiple divergent code bases
- Functionality of other families improved by Zeus code

Will We See This Again?

Why Did it Happen?

- Fear of capture/prosecution
- Retirement smokescreen?

Who Does it Benefit?

- Malware community
- **Not** the author

Conclusion

- Plenty of Zeus that was good is still being used
- Players taking up the Zeus position in the market and improving on it
- Modifications tend to be in specific key areas
- Code has proliferated through the malware ecosystem
- More Zeus based malware than before

Zeus Custom Builds
CARO 2012

SOPHOS