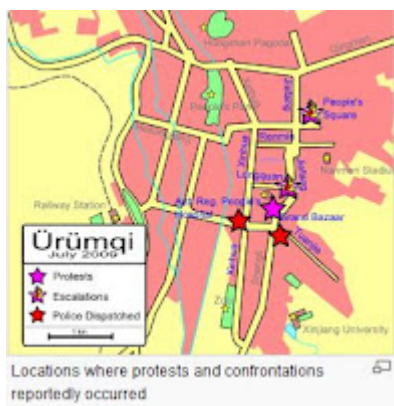


Jul 25 Mac Olyx backdoor + Gh0st Backdoor in RAR archive related to July 2009 Ürümqi riots in China (Samples included)

Archived: 2026-04-05 17:18:08 UTC

[Jul 25 Mac Olyx backdoor + Gh0st Backdoor in RAR archive related to July 2009 Ürümqi riots in China \(Samples included\)](#)

The recently discovered Backdoor for Mac Olyx ([Criminals gain control over Mac with BackDoor.Olyx](#)) was used for targeted attacks (or what it appears to be), which is not surprising. As [Microsoft pointed out](#), in addition to malware, the package contains an html page and photos from a Wikipedia page for events dated July 5, 2009, however it appears that all photos relate to one event - [July 2009 Ürümqi riots in China](#).



["Government censors"](#) disabled keyword searches for "Urumqi", and blocked access to Facebook and Twitter as well as local alternatives Fanfou and Youku. Chinese news sites mainly fed from Xinhua news service for updates about the rioting in Urumqi, comments features on websites were disabled on some stories to prevent negative posts about the lack of news. Internet connections in Urumqi were reportedly down. Many unauthorized postings on local sites and Google were said to have been "harmonised" by government censors, and emails containing terms related to the riots were blocked or edited to prevent discord."

Perhaps the trojans found in the package Ghostnet backdoor as [Backdoor:Win32/Remosh.A](#). and the new [Backdoor:MacOS_X/Olyx.A](#) were destined for a Chinese human rights activist, as he/she would be likely to be interested in this particular event update. In addition, it is known that many of the [Gh0stnet](#) targets were human rights activists.



General File Information

MD5: 93a9b55bb66d0ff80676232818d5952f

File Type: Mach-O I386

Malware: Backdoor.Olyx

MD5: f65fbeb945348ad2e1a123ef5cee65d3
















File Type: Windows PE EXE

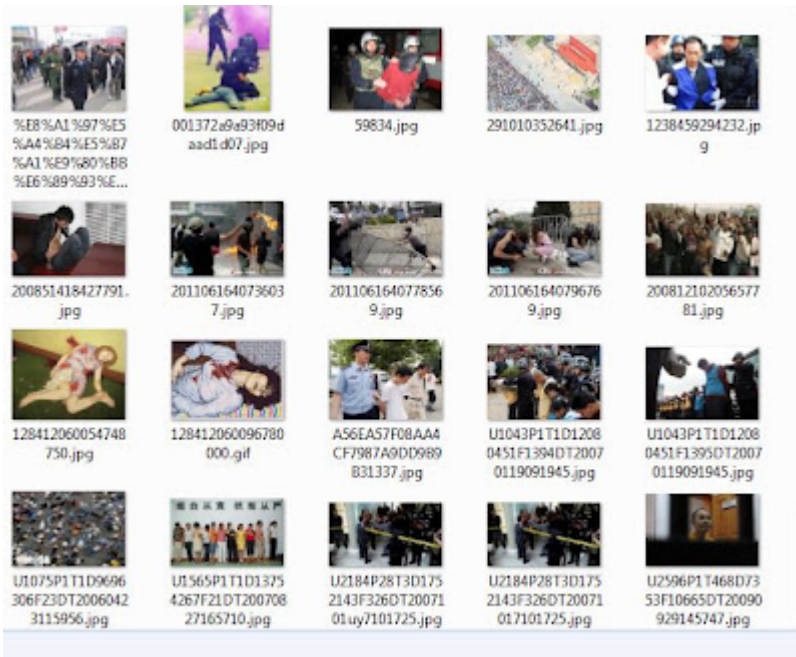
Malware: Ghostnet backdoor

Download



Additional information and Analysis links

Name	Date modified	Type	Size
 2011061640736037.jpg	6/16/2011 6:22 PM	Paint.NET Image	13 KB
 2011061640796769.jpg	6/16/2011 6:22 PM	Paint.NET Image	16 KB
 2011061640778569.jpg	6/16/2011 6:22 PM	Paint.NET Image	19 KB
 load(1).css	6/16/2011 5:10 PM	CSS Document	40 KB
 load.css	6/16/2011 5:10 PM	CSS Document	59 KB
 geoipllookup.wikimedia[1]	6/16/2011 4:45 PM	WIKIMEDIA[1] File	1 KB
 load(1).php	6/16/2011 4:45 PM	PHP File	12 KB
 index.php	6/16/2011 4:45 PM	PHP File	4 KB
 search-ltr.png	6/16/2011 4:45 PM	PNG image	1 KB
 load.php	6/16/2011 4:45 PM	PHP File	14 KB
 poweredby_mediawiki_88x31.png	6/16/2011 4:45 PM	PNG image	4 KB
 wikimedia-button.png	6/16/2011 4:45 PM	PNG image	3 KB
 MobileRedirect.js	6/16/2011 4:45 PM	JScript Script File	2 KB
 Current events 2009 July 5	6/16/2011 4:24 PM	File	50 KB
 Video-Current events 2009 July 5.exe	6/14/2011 11:29 PM	Application	201 KB



Microsoft Malware Protection center posted an excellent analysis with a lot of details, which you can find at the link below: [Backdoor Olyx - is it malware on a mission for Mac?](#)

Original report of Olyx backdoor by Dr.Web [Criminals gain control over Mac with BackDoor.Olyx](#)

MD5: 93a9b55bb66d0ff80676232818d5952f

File Type: Mach-O I386

Malware: Backdoor.Olyx

I am not a Mac or RE expert, I just made a few screenshots of the disassembled Mach-O file with Microsoft comments, which I thought were relevant. Please correct me if needed :)

```
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
  <key>Label</key>
  <string>com.google.com.tstartup 1.0</string>
  <key>ProgramArguments</key>
  <array>
    <string>/Library/Application Support/Google/startp</string>
  </array>
  <key>RunAtLoad</key>
  <true/>
  <key>LaunchOnlyOnce</key>
  <true/>
</dict>
</plist>
```

```

; Attributes: bp-based frame
_main proc near
var_41C= byte ptr -41Ch
var_1C= dword ptr -1Ch
arg_4= dword ptr 0Ch

push  ebp
mov   ebp, esp
push  edi
push  esi
push  ebx
sub   esp, 420h
mov   edi, [ebp+arg_4]
mov   eax, ds:___stack_chk_guard_ptr
mov   edx, [eax]
mov   [ebp+var_1C], edx
xor   edx, edx
mov   dword ptr [esp], offset a0000 ; char *
call  getenv
mov   esi, eax
mov   dword ptr [esp+4], 4FFh ; mode_t
mov   dword ptr [esp], offset a1library@aplica ; char *
call  _mkdir
mov   dword ptr [esp+4], 1E2Ch ; char a1library@aplica[]
mov   dword ptr [esp], 1E30h ; a1library@aplica db '/Library/Application Support/google'
call  _fopen$UNIX2003
mov   ebx, eax
mov   [esp+0Ch], eax
mov   dword ptr [esp+8], 9E5Ch
mov   dword ptr [esp+4], 1
mov   eax, ds:off_2024

```

"It disguises itself as a Google application support file by creating a folder named 'google' in the /Library/Application Support directory"
- Microsoft Malware Protection Center

```

mov   [esp], ebx ; char *
call  _mkdir
mov   dword ptr [esp+8], 400h
mov   [esp+4], esi
mov   [esp], ebx
call  __strcpy_chk
mov   dword ptr [esp+8], 400h
mov   dword ptr [esp+4], 1E30h
mov   [esp], ebx
call  __strcpy_chk
mov   [esp+0], ebx ; char *
mov   dword ptr [esp], offset a1mpplst ; char *
call  _rename
call  _fork
test  eax, eax
jnz  short loc_10C2

loc_10C2:
mov   dword ptr [esp], offset a1mpgoogle_top
call  _remove
mov   dword ptr [esp+4], offset a1mpgoogle_top ; char *
mov   eax, [edi]
mov   [esp], eax ; char *
call  _rename

loc_10C0:
mov   [char a1library@aplica[]]
; a1library@aplica db '/Library/Application Support/google'
db '/start', 0

```

in the /Library/Application Support directory the backdoor installs as 'start'
- Microsoft Malware Protection Center

```

mov   ebx, [ebp+var_41C]
call  __strcpy_chk
mov   dword ptr [esp+8], 400h
mov   dword ptr [esp+4], 1E30h
mov   [esp], ebx
call  __strcpy_chk
mov   dword ptr [esp+8], 400h
mov   dword ptr [esp+4], 1E30h
mov   [esp], ebx
call  __strcpy_chk
mov   [esp+0], ebx ; char *
mov   dword ptr [esp], offset a1mpplst ; char *
call  _rename
call  _fork
test  eax, eax
jnz  short loc_10C0

loc_10C0:
mov   dword ptr [esp], offset a1mpgoogle_top
call  _remove
mov   dword ptr [esp+4], offset a1mpgoogle_top ; char *
mov   eax, [edi]
mov   [esp], ebx ; char *
call  _rename

loc_10C2:
mov   [char a1library@aplica[]]
; a1library@aplica db '/Library/Application Support/google'
db '/start', 0

```

"It also keeps a copy in the temporary folder as 'google.tmp'"
- Microsoft Malware Protection Center

MD5: f65fbeb945348ad2e1a123ef5cee65d3

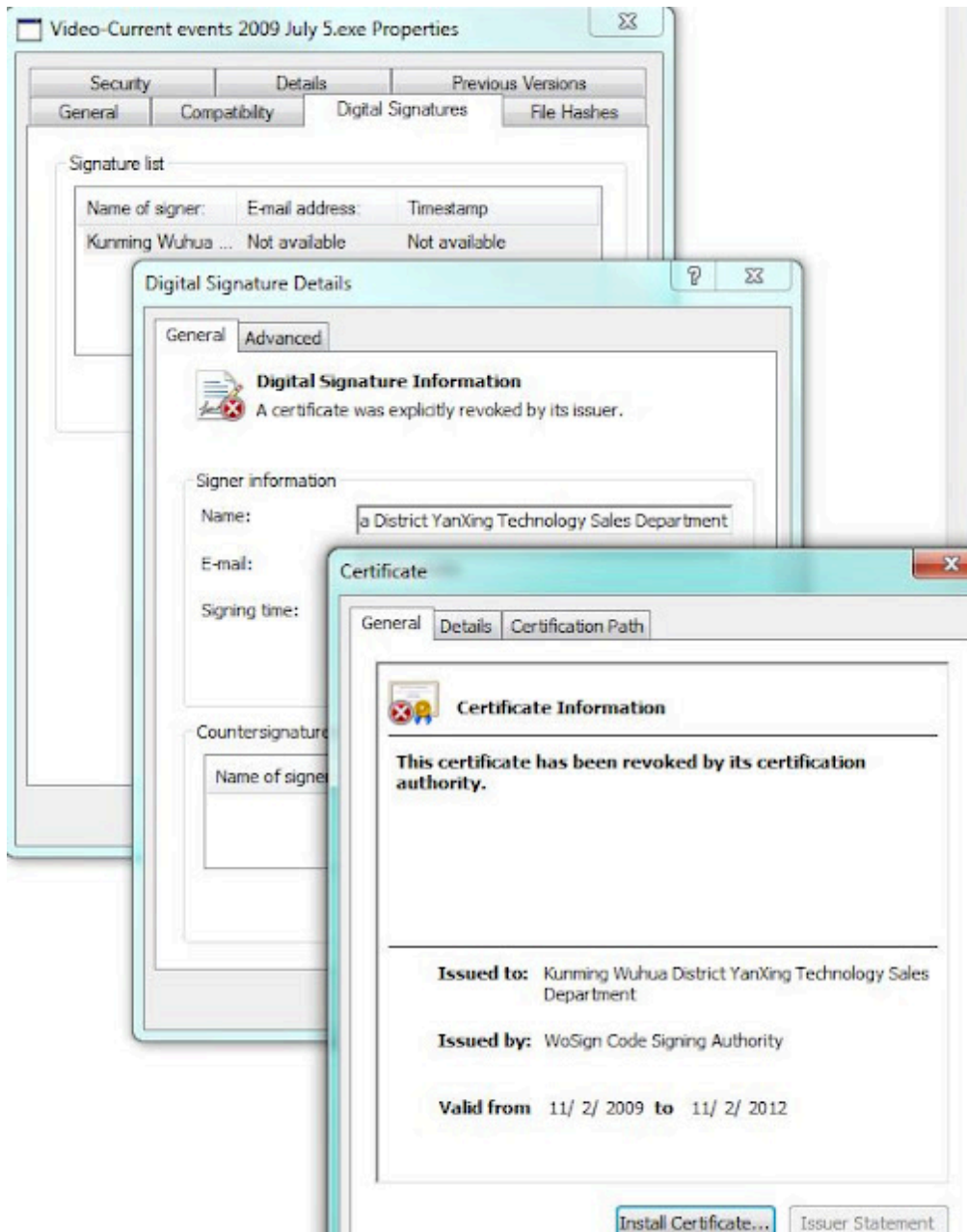
File Type: Windows PE EXE

Malware: Ghostnet backdoor

Anubis Analysis <http://anubis.iseclab.org/>

http://anubis.iseclab.org/?action=result&task_id=1ae9dcbf36d882e541d8fa26d533a9d39&format=html

Here is a screenshot of the certificate, which was revoked and some strings from the binary



```

00404324: 5SZ00404324_RegOpenKeyExA 'RegOpenKeyExA',0
00404334: 5SZ00404334_RegQueryInfoKeyA 'RegQueryInfoKeyA',0
00404348: 5SZ00404348_RegQueryValueExA 'RegQueryValueExA',0
0040435C: 5SZ0040435C_RegSetValueExA 'RegSetValueExA',0
0040436C: 5SZ0040436C_RegCreateKeyA 'RegCreateKeyA',0
0040437C: 5SZ0040437C_RegEnumKeyA 'RegEnumKeyA',0
00404388: 5SZ00404388_Kernel32_dll 'Kernel32.dll',0
00404398: 5SZ00404398_CopyFileA 'CopyFileA',0
004043A4: 5SZ004043A4_DeviceIoControl 'DeviceIoControl',0
004043B4: 5SZ004043B4_FindResourceA 'FindResourceA',0
004043C4: 5SZ004043C4_LoadResource 'LoadResource',0
004043D4: 5SZ004043D4_SizeofResource 'SizeofResource',0
004043E4: 5SZ004043E4_LockResource 'LockResource',0
004043F4: 5SZ004043F4_shell32_dll 'shell32.dll',0
00404400: 5SZ00404400_ShellExecuteA 'ShellExecuteA',0
0040470C: 5SZ0040470C_shell32_dll 'shell32.dll',0
00404718: 5SZ00404718_SHGetSpecialFolderLocation 'SHGetSpecialFolderLocation',0
00404734: 5SZ00404734_SHGetPathFromIDListA 'SHGetPathFromIDListA',0
00404EE4: 5SZ00404EE4_APPDATA 'APPDATA',0
00404EF4: 5SZ00404EF4_Environment 'Environment',0
00405010: 5SZ00405010_Users_Public 'Users\Public',0
00405028: 5SZ00405028_APAFBE2EE_837C_4EA5_B933_998F94A 'APAFAFBE2EE-837C-4EA5-B933-998F94AEC654',0
00405058: 5SZ00405058_ProgramData 'ProgramData',0
00405070: 5SZ00405070_TEMP_TEMP 'TEMP\TEMP',0
00405084: 5SZ00405084_TEMP 'TEMP',0
004054EC: 5SZ004054EC_notepad_exe 'notepad.exe',0
00405AF0: 5SZ00405AF0_shell32_dll 'shell32.dll',0
00405AFC: 5SZ00405AFC_IsUserAnAdmin 'IsUserAnAdmin',0
00406094: 5SZ00406094_nls 'nls',0
00406E78: 5SZ00406E78_AD18BB45B27C8946AD19A0768E749458 'AD18BB45B27C8946AD19A0768E749458AE29A05BB2478847AF82A15A8D778E46AC
00408120: 5SZ00408120_PackedCatalogItem 'PackedCatalogItem',0
004081F4: 5SZ004081F4_SYSTEM_CurrentControlSet_Service 'SYSTEM\CurrentControlSet\Services\MinSock2\Parameters\Protocol_Cat
004082F4: 5SZ004082F4_PathName 'PathName',0
004086D0: 5SZ004086D0_SOFTWARE_Microsoft_Windows_Curre 'SOFTWARE\Microsoft\Windows\CurrentVersion\Run',0
00408708: 5SZ00408708_Kernel_Fault_Check 'Kernel Fault Check',0
0040871C: 5SZ0040871C_Kernel_Fault_Check 'Kernel Fault Check',0
004088B0: 5SZ004088B0_dumprep_exe 'dumprep.exe',0
004088C0: 5SZ004088C0_open 'open',0
00408A54: 5SZ00408A54_b758_tbl 'b758.tbl',0
00408A80: 5SZ00408A80_SYSTEM_CurrentControlSet_Service 'SYSTEM\CurrentControlSet\Services\MinSock2\mssock32',0
00408B80: 5SZ00408B80_dxdiag_exe 'dxdiag.exe',0
00408D8C: 5SZ00408D8C_Global '\\.\Global',0
00408DA0: 5SZ00408DA0 '\\.\',0
00408DBC: 5SZ00408DBC_port 'port',0
00408FE0: 5SZ00408FE0_SysFader 'SysFader',0
00409054: 5SZ00409054_Error 'Error',0
0040905C: 5SZ0040905C_Runtime_error_at_00000000 'Runtime error at 00000000',0
00409208: 5SZ00409208_UCL_data_compression_library_0Dh.00h.00h.'UCL data compression library.',00h.'$Copyright: UCL <<
00409348: 5SZ00409348_1_03 '1.03',0
0040934F: 5SZ0040934F_Jul_20_2004 'Jul 20 2004',0

```



Automated Scans

Current events 2009 July 5

Submission date:2011-07-27 05:07:51 (UTC)

Result:19 /43 (44.2%)

<http://www.virustotal.com/file-scan/report.html?>

[id=a5c1b89b26007f4672409e0e7a3ab85135a0ffc01c74c4b6d49084da7fe9def5-1311743271](http://www.virustotal.com/file-scan/report.html?id=a5c1b89b26007f4672409e0e7a3ab85135a0ffc01c74c4b6d49084da7fe9def5-1311743271)

AhnLab-V3	2011.07.27.00	2011.07.27	MacOS_X/Olyx
Avast	4.8.1351.0	2011.07.26	MacOS:Olyx [Trj]
Avast5	5.0.677.0	2011.07.26	MacOS:Olyx [Trj]
BitDefender	7.2	2011.07.27	MAC.OSX.Backdoor.Olyx.A
Comodo	9524	2011.07.27	UnclassifiedMalware
DrWeb	5.0.2.03300	2011.07.27	BackDoor.Olyx.1
Emsisoft	5.1.0.8	2011.07.27	Backdoor.OSX.Olyx.IK
F-Secure	9.0.16440.0	2011.07.27	Backdoor:OSX/Olyx.A
GData	22	2011.07.27	MAC.OSX.Backdoor.Olyx.A
Ikarus	T3.1.1.104.0	2011.07.27	Backdoor.OSX.Olyx
Kaspersky	9.0.0.837	2011.07.27	Backdoor.OSX.Olyx.a

Microsoft 1.7104 2011.07.26 Backdoor:MacOS_X/Olyx.A
NOD32 6327 2011.07.27 OSX/Olyx.A
PCTools 8.0.0.5 2011.07.27 Backdoor.Olyx
Sophos 4.67.0 2011.07.27 OSX/Bckdr-RID
Symantec 20111.1.0.186 2011.07.27 Backdoor.Olyx
TrendMicro-HouseCall 9.200.0.1012 2011.07.27 OSX_OLYX.WA
VBA32 3.12.16.4 2011.07.26 BackDoor.OSX.Generic
VirusBuster 14.0.140.0 2011.07.26 Backdoor.OSX.Olyx.A

Additional information

Show all

MD5 : 93a9b55bb66d0ff80676232818d5952f

Video-Current events 2009 July 5.exe - WINDOWS BINARY Submission date:2011-07-27 05:00:39 (UTC)

Result:19/ 43 (44.2%)

<http://www.virustotal.com/file-scan/report.html?>

[id=d2f45192f22ef62a694facd0604b12c8c748ac94a6d8a2913f4beec7f04be1c1-1311742839](http://www.virustotal.com/file-scan/report.html?id=d2f45192f22ef62a694facd0604b12c8c748ac94a6d8a2913f4beec7f04be1c1-1311742839)

AhnLab-V3 2011.07.27.00 2011.07.27 Win-Trojan/Olyx.205480
AntiVir 7.11.12.130 2011.07.27 BDS/Olyx.A
BitDefender 7.2 2011.07.27 Backdoor.Wolyx.A
Comodo 9524 2011.07.27 TrojWare.Win32.Magania.~AD
DrWeb 5.0.2.03300 2011.07.27 Trojan.PWS.Multi.228
Emsisoft 5.1.0.8 2011.07.27 Trojan-PWS.Win32.Hangame.cl!IK
eSafe 7.0.17.0 2011.07.26 Win32.Backdoor.Troja
GData 22 2011.07.27 Backdoor.Wolyx.A
Ikarus T3.1.1.104.0 2011.07.27 Trojan-PWS.Win32.Hangame.cl
McAfee 5.400.0.1158 2011.07.27 Artemis!F65FBEB94534
McAfee-GW-Edition 2010.1D 2011.07.26 Heuristic.BehavesLike.Win32.AdSpyware.A
Microsoft 1.7104 2011.07.26 Backdoor:Win32/Wolyx.A
NOD32 6327 2011.07.27 Win32/Delf.OBY
Panda 10.0.3.5 2011.07.26 Suspicious file
PCTools 8.0.0.5 2011.07.27 Backdoor.Trojan
Symantec 20111.1.0.186 2011.07.27 Backdoor.Trojan
TrendMicro-HouseCall 9.200.0.1012 2011.07.27 BKDR_WOLYX.WA
VIPRE 9978 2011.07.27 Trojan.Win32.Generic.pak!cobra
VirusBuster 14.0.140.0 2011.07.26 Backdoor.Wolyx!YVAf5CV8Y34

MD5 : f65fbeb945348ad2e1a123ef5cee65d3

Anubis Analysis

http://anubis.iseclab.org/?action=result&task_id=1ae9dcfb36d882e541d8fa26d533a9d39&format=html

Traffic

121.254.173.57

Host reachable, 234 ms. average

121.254.128.0 - 121.254.255.255

Korea Internet Data Center Inc.

Korea, Republic of

Yunmi Lee

ip@kidc.net

KIDC Bldg, 261-1, Nonhyun-dong, Kangnam-ku, Seoul

phone: +82-2-6440-2925

fax: +82-2-6440-2909



Source: <http://contagiodump.blogspot.com/2011/07/jul-25-mac-olyx-gh0st-backdoor-in-rar.html>