Secrets of the Comfoo Masters

secureworks.com/research/secrets-of-the-comfoo-masters

Joe Stewart

- **Author:** Joe Stewart and Don Jackson, Dell SecureWorks Counter Threat Unit(TM) Threat Intelligence
- **Date:** 31 July 2013

Introduction

The details of organized cyber-espionage campaigns are becoming more public. So-called "Advanced Persistent Threat" (APT) attacks are common news as individuals and corporations discover the data on their hard drives is part of a country or competitor's "shopping list." The actors behind these attacks are generally well-equipped in terms of training, finances, and access to resources. The missions of APT threat actors are usually of strategic importance, and the actors exercise virtually unlimited patience in penetrating and persisting inside their specific target's network until they accomplish their goals.

One of the universal aspects of APT attacks is the use of malicious software tools that grant unauthorized backdoor access to computer systems inside the targeted network. Because maintaining a beachhead inside the network is often critical to mission success, threat actors must adapt to various network configurations and changes in defenses by choosing and deploying backdoors with specific functionality and features. It is difficult to be persistent without at least one backdoor. Threat actors often possess and use an arsenal of remote access trojans (RATs) to siphon data from their targets. Persistence requires malware, and the top cyber-espionage actors have hundreds of RATs at their disposal at any given time. Understanding the choice and usage of tools can be the keys to identifying and tracking APTs.

Dell SecureWorks researchers have identified and classified more than 200 distinct malware families used by various APT groups. Some malware is specially configured off-the-shelf software, and some malware is customized source code of an existing RAT. However, most malware families are proprietary, developed by the APT groups as weapons to be deployed against a variety of targets. Accurate identification and classification of this malware by antivirus (AV) companies is sparse. Shared code, the use of common tools, co-infections, and a history of generic or incorrect classification by multiple names make the automated tracking of these tools by AV companies difficult. This inaccuracy can be detrimental when designing defenses based on specific threat indicators. Tracking APTs requires a dedicated

malware intelligence effort. One way applied malware intelligence is used to discover new APT trojans is a recursive investigative method: Malware -> Infrastructure Touchpoints -> New Malware -> and so on.

Cyber-espionage actors often cycle through different RATs over a period of years. The Dell SecureWorks Counter Threat Unit™ (CTU) research team has tracked a RAT known as "Comfoo" that has been in continuous development since at least 2006. This RAT has maintained a fairly low profile, even though it was used as part of the RSA breach in 2010, when its code was first analyzed. Antivirus firm Trend Micro briefly mentioned its use in a 2012 paper titled "Luckycat Redux — Inside an APT Campaign with Multiple Targets in India and Japan." However, the disclosure of this trojan and some of its command and control (C2) infrastructure did not discourage its continued use by the threat actors responsible for it.

Comfoo characteristics

To maintain persistence on the system, Comfoo usually replaces the path to the DLL of an existing unused service rather than installing a new service. A new service is more likely to be noticed by system audits. Sometimes Comfoo is delivered with a rootkit that hides Comfoo's files on disk. Additionally, Comfoo starts the existing "ipnat" system service. This action causes remote inbound connections to the infected system to fail, blocking remote maintenance by the network administrator.

Network behavior

Comfoo's network traffic is encrypted and encapsulated in HTTP requests and responses, although some variants skip the encapsulation step. Payloads are encrypted by a 10-byte static XOR key that is hard-coded inside the Comfoo binary. Initial login data from the infected system (MAC address, internal IP address, campaign tag, and version data) is passed in the request URI and is additionally encrypted by a dynamic key, as shown in Figure 1.

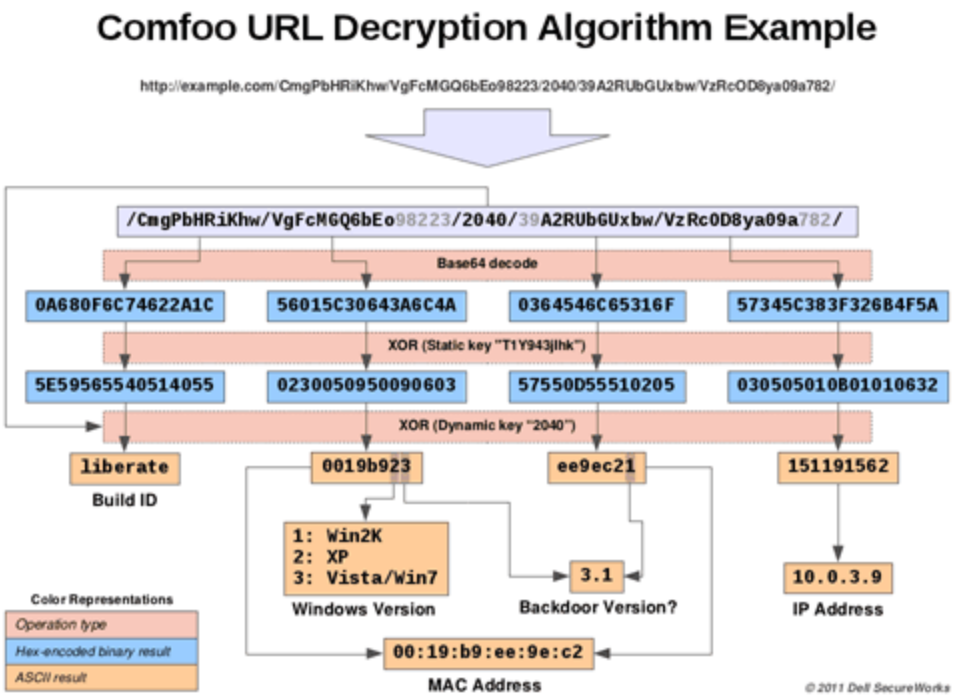

Figure 1. Comfoo URL decryption algorithm example. (Source: Dell SecureWorks)

Capabilities

The Comfoo RAT has the following features:

- System/network information gathering
- Keystroke logging
- Screenshots
- File upload/download/execute
- Command shell

Comfoo trojan C2 software discovery

By studying the network traffic of infected systems, CTU researchers determined that the server side of the Comfoo malware sends an HTTP server header identifying the server version as "Apache 2.0.50 (Unix)". However, the rest of the HTTP headers do not match the order or the formatting used by this version of Apache. This anomaly suggests that the C2 software was a standalone application instead of a series of scripts running under Apache. Searching for the specific server version string in the CTU malware repository produced a sample of the Comfoo server software, identified by the MD5 hash 2b29f0224b632fdd00d0a30527b795b7.

Analysis

The Comfoo C2 server turns out to be a rendezvous-type traffic relay program. This small binary can be deployed on rented or hacked Windows systems, where it passes traffic between Comfoo victims and the Comfoo master console operated by the threat actors (see Figure 2).

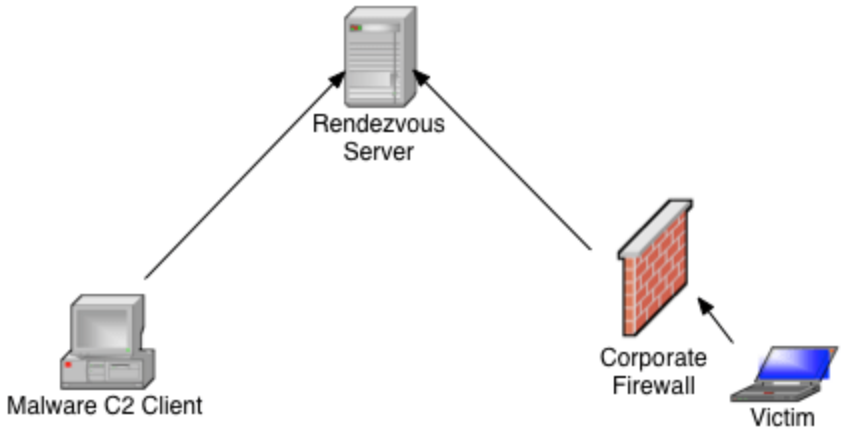

Figure 2. Organization of rendezvous-type traffic relay program. (Source: Dell SecureWorks)

Unlike "dumb" traffic relay servers such as HTran, the Comfoo relay server does not know the location of the master console. Instead, the master console program connects to the relay server on-demand, and any incoming victim data is passed to the master console connection. HTran is sometimes used to add an additional layer of untraceability to the victim connection. Likewise, the administrator can add other layers of proxies or VPN connections to the console connection side of the communication.

The Comfoo relay server listens on up to three TCP ports at a time. The first port acts as a control and typically listens on port 1688. It performs the following tasks:

- Enables/disables the other ports
- Accepts new relay port configuration (stored in rlycfg.dll)
- Notifies master console that a new victim connection is available

The second port is the admin relay port, which typically listens on port 1689. It accepts connections from the master console to send commands to and receive data from victims' systems. The third port is the victim relay port, which listens on a configurable port number, usually port 80 or port 443. This port accepts connections from victims' systems to send data to and receive commands from the Comfoo administrator encapsulated in HTTP requests and responses. If there is no current connection between the victim and the Comfoo administrator, Comfoo logs the victim's connection and sends an idle response to the victim.

DNS resolution tactics

In addition to using rendezvous protocols and HTran forwarding servers, Comfoo operators create and maintain another layer of obfuscation to thwart analysis of their infrastructure. Like many other APT malware families, Comfoo reaches out to its masters based on DNS lookups of certain hostnames. The Comfoo operators commonly use dynamic DNS providers to micromanage the IP addresses to which Comfoo hostnames resolve. While Comfoo sleeps, its operators often set those IP addresses to common or bogus entries. When not being used to actively control Comfoo, the C2 domain name might resolve to the address of a popular search engine or a local loopback (127.0.0.1), private (10.1.1.1), or other special use (0.0.0.0) IP address. Domain names used in Comfoo operations only point to actual control infrastructure during very short time windows. Only during these time windows do alerts from a DNS monitoring tool inform researchers when it might be possible to locate an actual Comfoo server. Figure 3 maps IP addresses used in Comfoo campaigns.

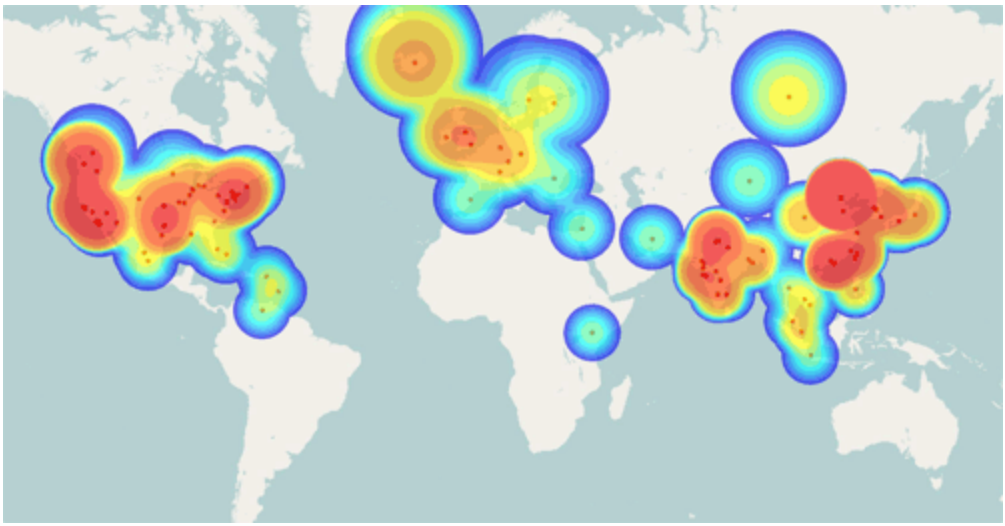

Figure 3. Geolocation plot of all public routable IP addresses resolved from a set of Comfoo C2 hostnames, including bogus distractors. (Source: Dell SecureWorks)

The map in Figure 4 shows only the IP addresses that actually speak Comfoo's protocol, illustrating how DNS tactics such as the distractor IP addresses can mask actual control infrastructure.

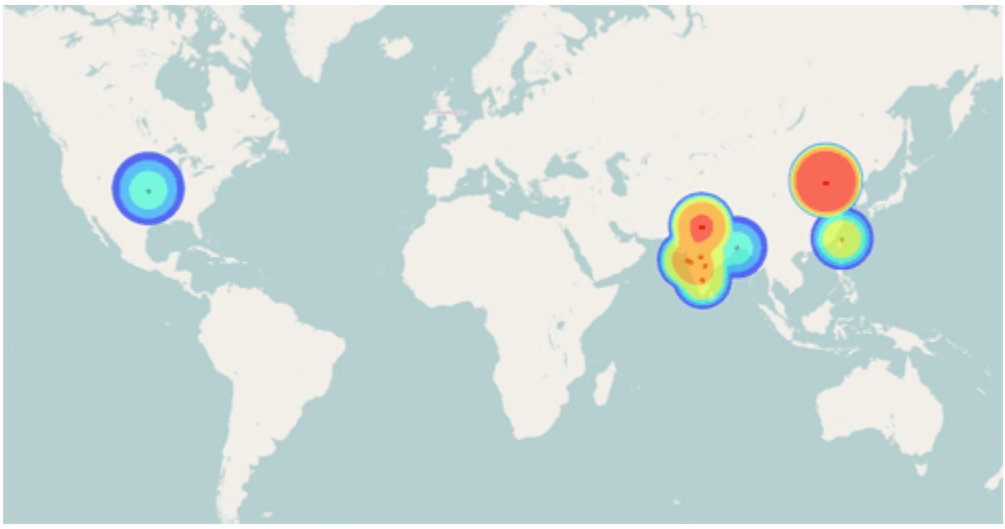

Figure 4. Geolocation plot of actual IP addresses used for Comfoo C2 servers. (Source: Dell SecureWorks)

Taking control

The unauthenticated nature of the Comfoo relay server's administrative connections makes it possible to take control of the C2 server and all victims' systems, armed only with knowledge of the protocol, the encryption method, and the static encryption key hard-coded into every Comfoo binary. Researchers can passively monitor victims' logins to the relay servers (sending no commands) by connecting to the correct port on the correct IP address at the right time. This technique is analogous to viewing webserver log data stored in a publicly accessible directory on a C2 server.

To help identify and notify victims of Comfoo-based espionage, CTU researchers set up a passive monitoring system for dozens of active Comfoo C2 relays and have been running this system since January 2012. Connections from the monitoring system are periodic, so not all victim logins are observed. Only the initial connection data is logged, and it is not possible to see data being exfiltrated from victims' networks using this method.

Passive monitoring results

While monitoring Comfoo, CTU researchers detected more than 200 variants of the trojan and 64 different campaign tags used by the threat actors to organize their campaigns. Numerous government entities and private companies based in the United States, Europe, and Asia Pacific had Comfoo-infected computers phoning home to the Comfoo C2 infrastructure (see Figure 5).

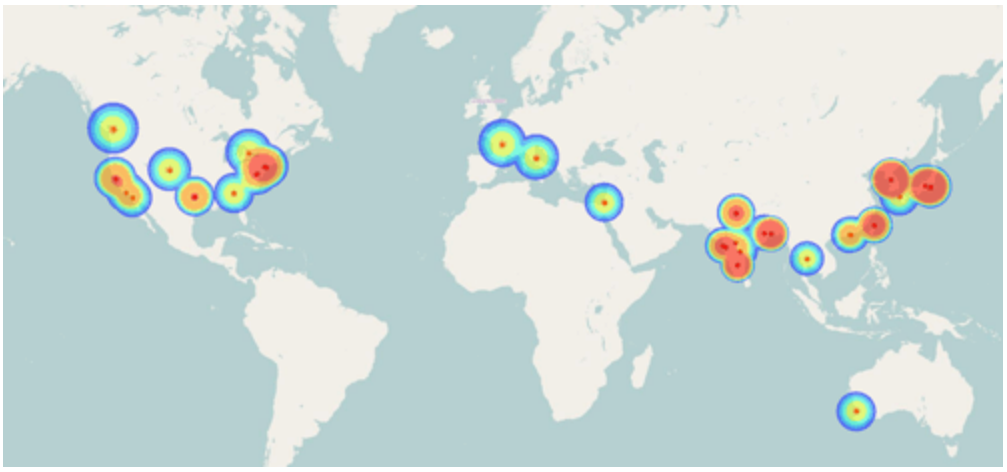

Figure 5. Geographic location of Comfoo victim organizations. (Source: Dell SecureWorks)

Much of the traffic emanated from multiple Japanese and Indian government ministries. CTU researchers outlined the Japanese attack campaign in a previous analysis entitled Chasing APT. The following industries were also targeted:

- Education
- Energy
- Mineral exploration
- News media
- Semiconductors
- Steel manufacturing
- Think tanks
- Telecommunications
- Trade organizations
- Audio and videoconferencing products

The targeting of audio and videoconferencing products is unusual. CTU researchers speculate that the threat actors might be looking for intellectual property relating to audio and videoconferencing. Another possibility is that it could be a clever and stealthy way of listening and watching activities of both commercial and government organizations.

Detecting Comfoo in the enterprise

The presence of Comfoo on a network or computer can be detected in a variety of ways, even if AV engines lack detection for the latest variants. Analysts can search for known Comfoo threat indicators in network traffic, on hard drives, in memory, or in the Windows registry.

Network detection

A typical Comfoo HTTP phone-home request looks like the following:

```
GET /CWoNaJLBo/VTNeWw11212/12664/12VTNfNmM1aQ/UTWOqVQ132/ HTTP/1.1Accept: image/gif,
image/x-xbitmap, image/jpeg, image/pjpeg, */*Accept-Language: en-enUser-Agent:
Mozilla/4.0 (compatible; MSIE 6.0;Windows NT 5.1)Host:
smtp.dynamiclink.ddns.usConnection: Keep-AliveCache-Control: no-cache
```

An active C2 server responds with headers similar to the following:

```
HTTP/1.1 200 OKDate: Mon, 29 Jul 2013 19:26:15 GMTServer: Apache/2.0.50
(Unix)Content-Length: 10Keep-Alive: timeout=15, max=90
```

Disk/memory/registry detection

The unique string T1Y943jIhk can be found in the Comfoo binary. Offline forensic analysis may be required to search for this string if a rootkit is in play.

These additional strings can be searched but are not guaranteed to be unique to Comfoo:

- CPUSpeed:%d.%dGHz
- CPUNameString:%s
- CPUVendorIdentifier:%s
- CPUIdentifier:%s
- No %d CPU Information:
- SystemCurrent Time:
- systemBoot Time:
- IE BHO Name:%s
- 11. IE BHO Information!
- 10. IE Version Information!
- 9. InstallApp Information!
- 8. NETBIOS Information!
- 7. Protocol Information!
- 6. NET Information!
- 5. Disk Information!
- 4. Account Information!
- 3. System Time!
- 2. CPU Type!
- Can not get this information, error code is %d.
- Windows Version Information!

Additionally, Comfoo uses the SetEvent Windows API and registers an event that frequently contains the word "GAME". The following are example Comfoo event names:

- exclusiveinstance12
- THIS324NEWGAME
- MYGAMEHAVESTART

- MYGAMEHAVEstarted
- MYGAMEHAVESTARTEd
- MYGAMEHAVESTARTED
- thisisanewfirstrun
- THISISASUPERNEWGAMENOWBEGIN
- thisisnewtrofor024

To persist without adding new registry entries, Comfoo edits an unused system service configuration, replacing the DLL path and setting it to auto-start on boot. For example, a system service registry key entry changed by Comfoo might resemble the following:

system\CurrentControlSet\Services\Netman\Parameters

- Original: "ServiceDll" => "%SystemRoot%\System32\netman.dll"
- Modified: "ServiceDll" => "C:\WINDOWS\system32\tabcteng.dll"

system\CurrentControlSet\Services\Netman

- Original: "Start" => "3"
- Modified: "Start" => "2"

Comfoo hijacks service settings for some legitimate service DLLs:

- netman.dll
- rasauto.dll
- sens.dll

The following are DLL names commonly used by Comfoo:

- cmmos.dll
- jacpet.dll
- javadb.dll
- mszlobm.dll
- netfram.dll
- netman.dll
- ntdapie.dll
- ntdelu.dll
- ntobm.dll
- odbm.dll
- senss.dll

- suddec.dll
- tabcteng.dll
- vmmreg32.dll
- wininete.dll

If Comfoo successfully connects to the relay server and receives commands from the master console, then it creates a file named "mstemp.temp" on the infected system to store the output of the last shell command.

Conclusion

Comfoo is the tip of an iceberg. The CTU research team notified many Comfoo victims, either directly or through the computer security incident response teams (CSIRTs) in their respective country. Analysis was also shared with law enforcement. Based on the number of campaign tags observed in malware samples versus those seen in live monitoring by the CTU research team, there are likely hundreds more unidentified victims.

Most businesses will never see a Comfoo infection. However, evaluating whether an organization is a potential target of cyber-espionage is important in any risk evaluation. Chief information security officers should maintain awareness of any reported cyber-espionage threats in their business sector. If one player in an industry is targeted, it is likely all major players (or newcomers with interesting technology) in that industry will be targets at some point.

Organizations compromised by Comfoo (or most types of APT malware) likely face a major forensic and eradication effort. This effort should be followed by a major investment in security measures to keep cyber-espionage actors out of the network. Many in-house security teams do not have the APT expertise to respond to a persistent threat that requires a persistent, active, and layered defense model spanning the entire attack surface of an organization. As a result, the organization might need outside expertise to effectively mitigate these types of threats.

Appendix: Comfoo hostnames for blacklisting consideration

accounts . ddns . info
active . googleupdate . hk
active . nifty-user . com
addr . googleupdate . hk
ahn06 . myfw . us
allroot80 . 4pu . com
apf . googleupdate . hk
aptlkxqm . 25u . com
back . agfire . com
back . winsupdate . com
my . amazingrm . com
my . officebeautyclub . com
myweb . wwwcrazy . com
nevruz . mrface . com
news . mcesign . com
news . rumorse . com
news . win . dnset . com
news . wintersunshine . net
night . mefound . com
nikimen . etowns . net

bbs . dynssl . com
bbs . gladallinone . com
bigdog . winself . com
billgates . itsaol . com
bjllgvtms . effers . com
blizzcon . sexidude . com
blizzcon . sexxxy . biz
buffet80 . bigmoney . biz
buffet80 . itsaol . com
buffet . bbsindex . com
bxpudqx . otzo . com
cart . itsaol . com
catawarm . gicp . net
cell . missingthegirl . com
cmart . iownyour . org
config . microupdata . com
copyright . imwork . net
cpt . csinfos . net
crsky . systemsupdata . com
database . googleupdate . hk
davidcat . yick . lflink . com
daviddog . gicp . net
db . themmdance . com
ddns . yourturbe . org
deminich . gicp . net
deminich . jungleheart . com
demi . yick . lflink . com
dgoil . 3322 . org
dns . google-login . com
do . centr-info . com
dolaamen . xicp . net
domain . centr-info . com
domain . nifty-user . com
download . yourturbe . org
dunya . 8800 . org
et . stoneqwer . com
eudge . 3322 . org
eudge . redirect . hm
european . pass . as
eurowizard . byinter . net
facebook . nifty-japan . com
fact . winsupdate . com
fbook . google-login . com
fish . windwarp . uicp . net
football . deminich . jungleheart . com
football . dynamiclink . ddns . us
foxpart . oicp . net
free3w . lflinkup . org
fr . washbart . com
ftp . alvinton . jetos . com
ftp . lucky . ddns . ms
ftpserver . 3-a . net
nslsa . microupdata . com
nsser . systemsupdata . com
nsservic . googleupdate . hk
nunok . ninth . biz
oct . clawsnare . com
offer . eosboxster . com
okkou . 9966 . org
park006 . myfw . us
pazar . vicp . net
pcnews . rr . nu
pcpc . helpngr . net
pcuser . ikwb . com
podding . newsinsky . com
poft . yahoo-user . com
pofuyer . 4pu . com
polly . jwt . ourhobby . com
polly . slyip . com
poly . jwt . ourhobby . com
pop3 . freemail . mrface . com
pop . microupdata . com
pop . peroillion . com
prc . deminich . jungleheart . com
prc . dynamiclink . ddns . us
pure . mypop3 . org
record . yick . lflink . com
rember . clawsnare . com
reserve . trickip . net
rouji . king . proxydns . com
s0ft . noorno . com
sapudy . dns2 . us
server . epac . to
server . nifty-login . com
server . universityexp . com
services . google-config . com
shift . 8866 . org
sinagame . 2288 . org
singes . organiccrap . com
singngh . gicp . net
slll . pbfsnet . com
smell . gotgeek . com
smtp . deminich . jungleheart . com
smtp . travelexpolorer . com
soft . yahoo-user . com
sollysly . servegame . com
sonam . goodnews007 . com
sports . wintersunshine . net
srv911 . yahoo-user . com
srv91 . googleupdate . hk
srv91 . yahoo-user . com
sscdtt . phmail . us
stone . king . proxydns . com
superaround . ns02 . biz

ftp . superaround . ns02 . biz
ftp . y3 . 3-a . net
funew . noorno . com
fun . marktie . com
funnygamea . vicp . net
games . jeepworker . com
games . noorno . com
googlemail . servehttp . com
googleupdate2009 . kmip . net
graymmy . longmusic . com
gws01 . microupdata . com
gws12 . microupdata . com
hanoihcm . phdns01 . com
havefuns . rkntils . 10dig . net
henryclub . 25u . com
hfwwpofuyer . 4pu . com
homehost . 3322 . org
https . port25 . biz
hyphen . dyndns . biz
hzg002 . mooo . com
image . google-login . com
image . qpoe . com
info . kembletech . com
info . rumorse . com
info . whandjg . net
insert . 51vip . biz
office-sevice . com
intrusion . post-horse . net
it . buglan . com
it . davyhop . com
it . pudnet . net
johnnees . rkntils . 10dig . net
kapa2000 . 3322 . org
kimomail . 3-a . net
korea001 . tribeman . com
korea1 . mooo . com
kx . davyhop . com
lanama . jkub . com
lcyma . jetos . com
li . noorno . com
livedoor . microupdata . com
login . yahoo-user . com
lovehill . 3d-game . com
lovehill . dyndns-blog . com
lovehill . xxuz . com
lsass . google-login . com
luck201202 . oicp . net
mail911 . nifty-login . com
mail911 . nifty-user . com
mail91 . nifty-login . com
mail91 . nifty-user . com
mail . carsystm . net
tech . bommow . com
terrys . rr . nu
test1 . dns1 . us
test1 . windwarp . uicp . net
thec . csinfos . net
timeout . myvnc . com
trans . helpngr . net
tttt . sundaynews . us
tw . pudnet . net
uncrisis . findhere . org
update . yourturbe . org
usstream . coyo . eu
venus . gr8domain . biz
vstar-2006 . vicp . net
wakawaka . servehttp . com
webdata . helpngr . net
web . nifty-login . com
web . nifty-user . com
web . yahoo-user . com
wetboy . vicp . hk
winhelp . yahoo-config . com
winserver . 3-a . net
wogawoga . sytes . net
worldwide . servehttp . com
wt . pudnet . net
wwmrus . gicp . net
www12 . sexidude . com
www . a1yac . net
www . avau . info
www . ayfd . info
www . butr . info
www . catholicstory . info
www . config . sendsmtp . com
www . drsc . in
www . firehorse . changeip . name
www . fsdr . info
www . google-login . com
www . greenhawthorn . com
www . grtk . info
www . hgtw . info
www . jeepworker . com
www . kkle . info
www . lconstruct . com
www . linejudge . net
www . microsoft . yourtrap . com
www . missingthegirl . com
www . nifty-japan . com
www . noorno . com
www . post-horse . net
www . search . wwwhost . biz
www . setinfor . proxydns . com
www . smtp2010 . googleupdate . hk

mail . lthreebox . com
mail . mariofreegame . net
mail . mgtfcayman . com
mail . mofa . zyns . com
mailsrv . mariofreegame . net
mail . systemsupdata . com
mail . xygong . com
manpower . 3322 . org
marhone . vicp . net
mdb . clawsnare . com
mf . tpznet . com
microsoft . redirect . hm
mil . winsupdate . com
msnsupport . servehttp . com
www . solarisc . com
www . superpowereye . com
www . swf . zyns . com
www . test1 . dns1 . us
www . tomdavid . dns04 . com
www . windows . dynamicdns . org . uk
www . wsdv . info
xmahone . 51vip . biz
xmahone . gicp . net
xmahone . suroot . com
yftpost . flnet . org
ynet . nifty-login . com
ynet . nifty-user . com
zp . amazingrm . com
zp . tpznet . com