EXHIBIT 20

THREAT ENCYCLOPEDIA

WORM_DORKBOT

Publish date: October 09, 2012

ANALYSIS BY

Karl Dominguez

PLATFORM: Windows 2000, Windows XP, Windows Server 2003

OVERALL RISK RATING:
DAMAGE POTENTIAL:
DISTRIBUTION POTENTIAL:
REPORTED INFECTION:

Low Medium High Critical

Threat Type:Worm

Destructiveness:No

Encrypted: Yes

In the wild: Yes

OVERVIEW

Infection Channel: Propagates via flashdrives, Propagates via instant messaging applications

This description is based on a compiled analysis of several variants of WORM_DORKBOT. Note that specific data such as file names and registry values may vary for each variant.

This worm arrives via removable drives. It may be downloaded by other malware/grayware/spyware from remote sites. It may be dropped by other malware. It may be unknowingly downloaded by a user while visiting malicious websites.

It drops an AUTORUN.INF file to automatically execute the copies it drops when a user accesses the drives of an affected system.

It also has rootkit capabilities, which enables it to hide its processes and files from the user.

It deletes the initially executed copy of itself.

TECHNICAL DETAILS

File Size: Varies

File Type: EXE

Memory Resident: Yes

Initial Samples Received Date: 10 Mar 2011

Payload: Drops files, Connects to URLs/IPs

Arrival Details

This worm arrives via removable drives.

It may be downloaded by other malware/grayware/spyware from remote sites.

It may be dropped by other malware.

It may be unknowingly downloaded by a user while visiting malicious websites.

Autostart Technique

This worm adds the following registry entries to enable its automatic execution at every system startup:

```
HKEY_CURRENT_USER\Software\Microsoft\
Windows\CurrentVersion\Run
{malware file name} = "%User Profile%\Application Data\{malware file name}.exe"
```

Propagation

This worm creates the following folders in all removable drives:

{drive letter}:\RECYCLER

It drops the following copy(ies) of itself in all removable drives:

{drive letter}:\RECYCLER\{random characters}.exe

It drops an AUTORUN.INF file to automatically execute the copies it drops when a user accesses the drives of an affected system.

The said .INF file contains the following strings:

```
[AutoRun]
;{garbage characters}
shellexecute=RECYCLER\{malware file name}.exe
;{garbage characters}
icon=shell32.dll,7
;{garbage characters}
shell\open\command=RECYCLER\{malware file name}.exe
;{garbage characters}
action=Open folder to view files
;{garbage characters}
shell\explore\command=RECYCLER\{malware file name}.exe
;{garbage characters}
useautoplay=1
```

It sends messages that contain links to sites hosting remote copies of itself using the following instant-messaging (IM) applications:

- Windows Live Communicator
- MSN Messenger
- Pidgin
- Xchat
- mIRC

Backdoor Routine

This worm connects to the following URL(s) to send and receive commands from a remote malicious user:

- {BLOCKED}ebsite.com
- {BLOCKED}rebitch.com
- {BLOCKED}ney.biz
- {BLOCKED}ousez11.com
- {BLOCKED}g.{BLOCKED}oan.com
- {BLOCKED}g.{BLOCKED}opperz11.com
- {BLOCKED}g.{BLOCKED}ousez11.com

{BLOCKED}g.{BLOCKED}allone.com

{BLOCKED}g.{BLOCKED}ketbaby.com

{BLOCKED}s.com

{BLOCKED}ussy.info

{BLOCKED}ctronix.com

{BLOCKED}enial.com

{BLOCKED}m.{BLOCKED}ch.ru

{BLOCKED}g.{BLOCKED}ousez11.com

Rootkit Capabilities

This worm also has rootkit capabilities, which enables it to hide its processes and files from the user.

Other Details

This worm connects to the following URL(s) to get the affected system's IP address:

http://api.wipmania.com/

It deletes the initially executed copy of itself

NOTES:

This worm monitors the Internet activities of the infected system to steal user credentials if the user visits websites with the following strings:

&Password=

&txtPassword=

.alertpay./*login.aspx

.moneybookers./*login.pl

1and1.com/xml/config

4shared.com/login

:2083/login

:2086/login

alertpay.com/login

aol./*login.psp*

*bcointernacional*login*

bigstring./*index.php*

depositfiles./*/login*

*dotster.com/*login*

dyndns/account*

enom.com/login

facebook./login.php*

fastmail./mail/*

fileserv.com/login

fileserve./login*

*filesonic.com/*login*

FLN-Password=

freakshare.com/login

gmx./*FormLogin*

godaddy.com/login

google./*ServiceLoginAuth*

hackforums./member.php

hotfile.com/login

letitbit.net

login.live./*post.srf*

login.yahoo./*login*

login_password=

loginUserPassword=

*mediafire.com/*login*

megaupload./*login

megaupload./*login*

members.iknowthatgirl*/members*

members.brazzers.com

*moniker.com/*Login*

*namecheap.com/*login*

*netflix.com/*ogin*

netload.in/index

no-ip/login*

*officebanking.cl/*login.asp*

oron.com/login

pass=

passwd=

password=

password]=

paypal./webscr?cmd=_login-submit*

runescape/*weblogin*

screenname.aol./login.psp*

secure.logmein./*logincheck*

sendspace.com/login

service=youtube

*signin.ebay*SignIn

sms4file.com//signin-do*

speedyshare.com/login

steampowered/login*

TextfieldPassword=

thepiratebay.org/login

*torrentleech.org/*login*

*twitter.com/sessions

*uploaded.to/*login*

*uploading.com/*login*

vip-file.com//signin-do*

*webnames.ru/*user_login*

what.cd/login

youporn./login*

Email

EmailName

FLN-Password

FLN-UserName

login

login_email

login_password

loginId

loginUserName

loginUserPassword

Passwd

Password

quick_password

quick_username

screenname

session[password]

session[username_or_email]

TextfieldEmail

TextfieldPassword

txtEmail

txtPassword

username

It attempts to steal user credentials used in the following websites:

AlertPay

AOL

BigString

DynDNS

Facebook

Fastmail

FileServe

Gmail

GMX

Hackforums

LogMeIn

Megaupload

Moneybookers

No-IP

NoIP

OfficeBanking

PayPal

Runescape

Steam

Twitter

Windows Live

Yahoo

Yahoo!

YouTube

It has the following backdoor capabilities:

Block DNS

Create processes

Download other files

Insert iframe tags into HTML files

Join an IRC channel

Log in to FTP sites

Perfrom Slowloris, UDP, and SYN flooding

Run Reverse Socks4 proxy server

Send MSN Messenger messages

Steal login credentials

Update Itself

Visit a Web Site

It may also prevent the user from using the following applications:

cmd.exe

ipconfig.exe

regedit.exe

regsvr32.exe

rundll32.exe

verclsid.exe

It blocks users from accessing websites with the following strings:

avast.

avg.

avira.

bitdefender.

bullguard.

clamav.

comodo.

emsisoft.

eset.

fortinet.

f-secure.

garyshood.

gdatasoftware.

heck.tc

iseclab.

jotti.

kaspersky.

lavasoft.

malwarebytes.

mcafee.

norman.

norton.

novirusthanks.

onecare.live.

onlinemalwarescanner.

pandasecurity.

precisesecurity.

sophos.

sunbeltsoftware.

symantec

threatexpert.

trendmicro.

virscan.

virus.

virusbuster.nprotect.

viruschief.

virustotal.

webroot.

It hooks the following API to hide itself and to aid its routines.

CopyFileA

CopyFileW

CreateFileA

CreateFileW

DeleteFileA

DeleteFileW

DnsQuery_A

DnsQuery_W

GetAddrInfoW

HttpSendRequestA

HttpSendRequestW

InternetWriteFile

LdrEnumerateLoadedModules

LdrGetDllHandle

LdrGetProcedureAddress

LdrLoadDll

MoveFileA

MoveFileW

NtEnumerateValueKey

NtQueryDirectoryFile

NtQueryInformationProcess

NtQueryInformationThread

NtQuerySystemInformation

NtQueryVirtualMemory

PR_Write

RegCreateKeyExA

RegCreateKeyExW

RtlAnsiStringToUnicodeString

URLDownloadToFileA

URLDownloadToFileW

It drops shortcut files pointing to the copy of itself in removable drives. These dropped .LNK files use the names of the folders located on the said drives for their file names. It then sets the attributes of the original folders to Hidden to trick the user into clicking the .LNK files.

This description is based on a compiled analysis of several variants of WORM_DORKBOT. Note that specific data such as file names and registry values may vary for each variant.

Featured Stories

HP Pulls Out of Hacking Contest, Citing Changes to Wassenaar Arrangement

Spear Phishing 101: What is Spear Phishing?

Q&A: The Deep Web, Anonymity, and Law Enforcement

EXPERT INSIGHT: Ransomware Today

↑ Top of page

CONNECT WITH US ON