

Present Danger : Top 10 Malware Threats

Contributed by Medianowonline Newsnetwork

Anti Malware Developer finds continued prevalence of Trojan horse programs

CLEARWATER, Fla., Feb. 3 - Sunbelt Software, a leading provider of Windows security software, today announced the top 10 most prevalent malware threats for the month of January 2010. The report, compiled from monthly scans performed by Sunbelt's award-winning anti-malware solution, VIPRE Antivirus + Antispyware, and its antispyware tool, CounterSpy, is a service of SunbeltLabs.

In January, the malware landscape remained remarkably similar to December, according to Sunbelt Software ThreatNet statistics. The top seven detections were the same as December, but in a slightly different order. In December and January, six of the top 10 detections were Trojan horse programs.

Trojan.Win32.Generic!BT - a generic detection for Trojans that comprised nearly one quarter (23.15 percent) of all the malware found. It remained in the top position for the third month in a row, growing by nearly 20 percent from 18.69 percent of all detections in December. It is a detection that includes many downloaders associated with scareware or rogue security products.

After holding the top spot on the list for most of 2009, the password-stealing Trojan-Spy.Win32.Zbot.gen held the second position on the list for the third consecutive month, decreasing from 6.23 to 4.91 percent of all detections.

"I think we can expect to see Trojan horse programs continue to be the top detections for the foreseeable future," said Michael St. Neitzel, Sunbelt Software vice president of Threat Research. "Trojans used to download and install a wide variety of other malware and those are the real moneymakers for the bad guys."

Other Trojans in the top 10 were:

- Trojan.Win32.Generic!SB.0
- Trojan.Win32.Malware
- Trojan.ASF.Wimad (v)
- Trojan.HTML.FakeAlert.a (v)

Meanwhile, three new detections moved onto this month's top 10 list. Virtumonde -- a generalized description of an adware program with many versions of pop up advertising -- constituted 1.23 percent of overall detections. Packed.Win32.TDSS.aa.3 (v) -- a sophisticated rootkit and Trojan that is used primarily to redirect search engine results -- made up 1.21 percent. Finally, Trojan.HTML.FakeAlert.a (v) -- a detection for an HTML file which replaces a desktop background and works with other rogue malware -- made up just under one percent of all detections.

The top 10 results represent the number of times a particular malware infection was detected during VIPRE and CounterSpy scans that report back to ThreatNet, Sunbelt's community of opt-in users. These threats are classified as moderate to severe based on method of installation among other criteria established by SunbeltLabs. The majority of

these threats propagate through stealth installations or social engineering.

The top 10 most prevalent malware threats for the month of January are:

1. Trojan.Win32.Generic!BT 23.15%
2. Trojan-Spy.Win32.Zbot.gen 4.91%
3. Exploit.PDF-JS.Gen (v) 4.55%
4. Trojan.Win32.Generic!SB.0 2.40%
5. Trojan.Win32.Malware 1.93%
6. Trojan.ASF.Wimad (v) 1.92%
7. INF.Autorun (v) 1.46%
8. Virtumonde 1.23%
9. Packed.Win32.TDSS.aa.3 (v) 1.21%
10. Trojan.HTML.FakeAlert.a (v) 0.98%

About SunbeltLabs

SunbeltLabs specializes in the discovery and analysis of dangerous vulnerabilities (i.e., security holes, bugs, maligned features or combination of operations) that could be exploited for Internet and email attacks. The research team actively researches new malware outbreaks, creating and testing new threat definitions on a constant basis.

About Sunbelt Software

Headquartered in Tampa Bay (Clearwater), Fla., Sunbelt Software was founded in 1994 and is a leading provider of Windows security software including enterprise antivirus, antispymware, email security, and malware analysis tools. Leading products include the VIPRE and CounterSpy® product lines, Sunbelt Exchange Archiver, CWSandbox, and ThreatTrack.