Yui Kee Computing Ltd.

# Newsletter

April 2012

## Contents



## Attackers Target Sophos Partner Website

*<web-link for this article>*

Sophos has notified its distributors and resellers that suspicious activity was detected on the Sophos Partner Portal and, as a precautionary measure, the site has been shut down and a full security audit launched.

The suspicious activity was detected on Tuesday, 3rd April and reported to Sophos' business partners on 5th April. The attacker attempted to upload two attack tools, one to steal passwords, and the other to escalate privileges, but was blocked by Sophos Endpoint Security. Nevertheless, Sophos considered the attempt serious enough to take the portal offline and image the system for forensic analysis and to run copies in their secure lab to further understand the attack.

To reassure partners, Sophos emphasised that the database attacked was not designed to hold financial data, but they scanned for any banking details (credit cards, sorting codes, account numbers, etc.) lurking in the fields anyway, and found none. There will also be forced password resets when the system comes back online.

On 10th April, Sophos updated their report, saying that, following a hardware failure, misconfiguration of security settings on a standby server allowed the attacker to locate and exploit a vulnerability.

This incident again shows the value of defence in depth: a mistake or vulnerability in one system is covered by a complementary defence. Any security incident is hugely embarrassing for a security company, but it is only openness when an incident occurs that can give confidence that serious problems are not being swept under the carpet.

**More Information**

Security Notification for Sophos Partners
Sophos shutters partner portal after hack attack

# April Hong Kong Honeypot Report

*<web-link for this article>*

This is the fourth monthly report from West Coast Labs's honeypot in Hong Kong, providing some indication of the type and level of malware threat in Hong Kong, but it is only based on a single honeypot, so the conclusions should be treated with caution. The number of attacks has increased this month, and Taiwan tops the list of the commonest source for the first time, closely followed by Japan.

## Average Time To Infect: 10 hours 20 minutes

The average time to infect is an indication of how long it would be before a vulnerable computer connected to the internet in Hong Kong became infected. Two hours longer than previously.

## Summary

- Total number of attacks : 72
- 34 are brand new to this honeypot.
- 9 of these files have not been seen in other honeypots

## Source of Attacks

The following breaks down where these attacks have come from by use of IP geolocation.

| Number of attacks | Source |
|---|---|
| 25 | Taiwan |
| 24 | Japan |
| 6 | United_States |
| 4 | Canada |
| 3 | France |
| 2 | Spain |
| 2 | Iran |
| 1 | Brazil |
| 1 | Singapore |
| 1 | Turkey |
| 1 | South Korea |
| 1 | Malaysia |
| 1 | Poland |

## Malware List

| Checksum (md5) | This month | Previous count | Detection |
|---|---|---|---|
| e8fbf01a93eb2094b7939de960762f80 | 1 | 0 ***NEW | Y (W32/Trojan.MEX , Backdoor.Win32.Rbot.bni Virus.Win32.Virut.n , , ) |
| 8d0d86972040e17d4e00bd9481f4986d | 1 | 0 ***NEW | Y (w32/sdbot.aefv , Backdoor.Win32.Rbot.bni , , ) |
| 2fa0e36b36382b74e6e6a437ad664a80 | 1 | 0 ***NEW | Y (w32/backdoor.zzr W32/Trojan5.DCW , Backdoor.Win32.Rbot.aftu Backdoor.Win32.Rbot.yqj Backdoor.Win32.Rbot.yol Backdoor.Win32.Rbot.wjd Backdoor.Win32.Rbot.sds , , ) |

| | | | |
|---|---|---|---|
| 3d6fca9918d438c4eb9786f8af9ccb58 | 1 | 0 ***NEW | Y (w32/emailworm.amv , Net-Worm.Win32.Allaple.d , , ) |
| d1fb8b699d4f008b0e3a87b371439d5d | 1 | 0 ***NEW | Y (w32/rahack.a.gen!eldorado , Net-Worm.Win32.Allaple.b , , ) |
| bb39f29fad85db12d9cf7195da0e1bfe | 2 | 0 ***NEW | Y (w32/backdoor.zzr W32/Trojan5.DCW , Backdoor.Win32.Rbot.aftu Net-Worm.Win32.Kolabc.eia , , ) |
| f8815cdca238ad5ab566f05f5a6335a4 | 2 | 0 ***NEW | Y (w32/backdoor.zzr W32/Trojan5.DCW , Backdoor.Win32.Rbot.aftu Backdoor.Win32.Rbot.voe , , ) |
| 1bb4b25c0e5cb75905f97eafec333b8b | 1 | 0 ***NEW | Y (w32/threat-hlliye!eldorado , Net-Worm.Win32.Kolabc.hmn Net-Worm.Win32.Kolab.dgn , W32Kolab!I46 , ) |
| bbb5034e33568e100dd3dadabb5a57e9 | 3 | 1 | Y (w32/sdbot.otr , Net-Worm.Win32.Kolab.aefe Backdoor.Win32.Rbot.bqj , , ) |
| 94052374fdb3b2b41ea6c69c791e21e4 | 1 | 2 | Y (w32/genbl.94052374!olympus , HEUR:Trojan.Win32.Generic , , ) |
| 4f6f80f42364ef75ee76271ab3c3715d | 1 | 0 ***NEW | Y (w32/sdbot.aefv w32/virut.7116 , Backdoor.Win32.Rbot.adqd , , ) |
| f9dc3945bdd7406bd8db06a47963ec14 | 2 | 0 ***NEW | Y (W32/Sdbot.OTR , Net-Worm.Win32.Kolab.aefe Backdoor.Win32.Rbot.bqj , , ) |
| 70ec5c4b3ff662232eacb0192fae42ac | 1 | 0 ***NEW | Y (w32/ircbot.add , Backdoor.Win32.IRCBot.idc , W32Ircbot!I560 , ) |
| 15965bb88165d1eb06851d8f076130ba | 2 | 0 ***NEW | Y (w32/sdbot.otr , Net-Worm.Win32.Kolab.aefe Backdoor.Win32.Rbot.bqj , , ) |
| 3875b6257d4d21d51ec13247ee4c1cdb | 2 | 19 | Y (W32/Sdbot.AEFV W32/Malware!44f4 , Backdoor.Win32.Rbot.bni , W32Rbot!I2663 , ) |
| f5fbd1189db83db22d7e6cdb55eed193 | 1 | 1 | Y (w32/injector.a.gen!eldorado W32/Backdoor!d75d , Backdoor.Win32.Rbot.bni , , ) |
| c5ff7232868333107fa3efe895f12361 | 1 | 1 | Y (W32/Sdbot.OTR , Net-Worm.Win32.Kolab.aefe Backdoor.Win32.Rbot.bqj , , ) |
| 49cccd30a564410d1f9bbce89fa15890 | 1 | 0 ***NEW | Y (W32/Sdbot.AEFV , Backdoor.Win32.Rbot.adqd Backdoor.Win32.Rbot.bni , , ) |
| 925dabe1aa7a95811d363bf3441c74b4 | 3 | 0 ***NEW | Y (W32/Trojan5.DCW w32/backdoor.zzr , Backdoor.Win32.Rbot.xri Backdoor.Win32.Rbot.aftu , , ) |
| 99296c6c3d676ac0578dcaf0f7f1b927 | 2 | 0 ***NEW | Y (w32/genbl.99296c6c!olympus , Net-Worm.Win32.Kolab.bfzy not-a-virus:HEUR:Hoax.Win32.ArchSMS.gen , , ) |
| df51e3310ef609e908a6b487a28ac068 | 2 | 2 | Y (W32/Trojan5.DCW w32/backdoor.zzr , Backdoor.Win32.Rbot.rgk Backdoor.Win32.Rbot.aftu , , ) |
| 42c55cad12fc904f7d65c77c7ac76ecf | 1 | 0 ***NEW | Y (w32/emailworm.amu , Net-Worm.Win32.Allaple.a , , ) |
| f4a200f7818dfb166b9a3d238ac55a2d | 3 | 0 ***NEW | Y (W32/Trojan5.DCW w32/backdoor.zzr , Backdoor.Win32.Rbot.bqj Backdoor.Win32.Rbot.aftu Backdoor.Win32.DsBot.vd , , ) |
| 9019b23f2a5a51c33671739af2f30992 | 1 | 1 | Y (w32/sdbot.otr , Net-Worm.Win32.Kolab.aefe Backdoor.Win32.Rbot.bqj , , ) |
| 954919ad5661e1b44803092360ac5d82 | 1 | 0 ***NEW | Y (w32/trojan.mex , Backdoor.Win32.Rbot.bni Virus.Win32.Virut.n , , ) |
| 6ba3712b1b1ad63553d5521522ca07ba | 1 | 0 ***NEW | Y (w32/rahack.a.gen!eldorado , Net-Worm.Win32.Allaple.b , , ) |
| 1f8a826b2ae94daa78f6542ad4ef173b | 1 | 1 | Y (W32/Trojan5.DCW w32/backdoor.zzr , Backdoor.Win32.Rbot.aftu Backdoor.Win32.Rbot.phv Backdoor.Win32.Rbot.ion , , ) |
| 14a09a48ad23fe0ea5a180bee8cb750a | 2 | 1 | Y (W32/Trojan5.DCW w32/backdoor.zzr , Backdoor.Win32.Rbot.bqj Backdoor.Win32.Rbot.aftu Backdoor.Win32.DsBot.vd , , ) |
| cb576cca04946b3d0829703d108ae270 | 3 | 1 | Y (w32/sdbot.otr , Net-Worm.Win32.Kolab.aefe Backdoor.Win32.Rbot.bqj , , ) |
| 67804f7bbc3c3e5f2ca941d3c126a312 | 1 | 1 | Y (W32/Virut.7116 , Virus.Win32.Virut.av Net-Worm.Win32.Allaple.e , , ) |
| 80ad35cd27c0f9c2d6793d9a5e984956 | 1 | 0 ***NEW | Y (w32/rahack.a.gen!eldorado , Net-Worm.Win32.Allaple.b , , ) |
| ec513abb61c99fce74072789bb61bc72 | 1 | 0 ***NEW | Y (w32/genbl.ec513abb!olympus , , , ) |
| 7867de13bf22a7f3e3559044053e33e7 | 1 | 2 | Y (w32/susppack.cy.gen!eldorado , backdoor.win32.agent.aknp , , ) |
| 10980f4df2060b86a72eb5e533102980 | 1 | 0 ***NEW | Y (w32/backdoor2.dstk , |

| | | | |
|---|---|---|---|
| | | | Backdoor.Win32.IRCBot.jwy<br>Worm.Win32.AutoRun.tet , W32Ircbot!I484 , ) |
| 74473505ef968e2f8cd764d9af12adb2 | 1 | 0 ***NEW | Y (W32/Allaple.H ,<br>Net-Worm.Win32.Allaple.e , , ) |
| 8a5ce07df6a5357dafa84f5317aaad35 | 2 | 0 ***NEW | Y (w32/sdbot.otr , Net-Worm.Win32.Kolab.aefe<br>Backdoor.Win32.Rbot.bqj , , ) |
| ced2ed2358f1fb56051d50f97229bfca | 1 | 1 | Y (w32/virut.7205 , Virus.Win32.Virut.bl<br>Net-Worm.Win32.Allaple.e , , ) |
| 977a6cbbd0c43fcd9b55eaa9e134bbdb | 1 | 0 ***NEW | Y (w32/rahack.a.gen!eldorado ,<br>Net-Worm.Win32.Allaple.e , , ) |
| 94109e9b3f2b045350db9a5cb592b178 | 1 | 0 ***NEW | Y (w32/sdbot.otr , Net-Worm.Win32.Kolab.aefe<br>Backdoor.Win32.Rbot.bqj , , ) |
| 4ed217391b897fc2d46ec9ce8af282cf | 1 | 2 | Y (W32/Virut.AG , Backdoor.Win32.Rbot.adqd , , ) |
| 1d419d615dbe5a238bbaa569b3829a23 | 1 | 1 | Y (W32/Trojan5.DCW w32/backdoor.zzr ,<br>Backdoor.Win32.Rbot.bqj<br>Backdoor.Win32.Rbot.aftu<br>Backdoor.Win32.DsBot.vd , , ) |
| 809fe9b32845edf5c09b871e0e68f227 | 1 | 1 | Y (w32/sdbot.otr , Net-Worm.Win32.Kolab.aefe<br>Backdoor.Win32.Rbot.bqj , , ) |
| 865915650a85e7c27cdd11850a13f86e | 1 | 0 ***NEW | Y (w32/sdbot.otr , Net-Worm.Win32.Kolab.aefe<br>Backdoor.Win32.Rbot.bqj , , ) |
| 952098cf3c65cfcb52282d8959ddffd3 | 1 | 2 | Y (W32/Allaple.H , Trojan.Win32.Genome.rioo<br>Net-Worm.Win32.Allaple.e , , ) |
| baaeaf7bb0d1319789047dd56ec17c45 | 1 | 0 ***NEW | Y (w32/emailworm.hqk ,<br>Net-Worm.Win32.Allaple.e , , ) |
| f783dc2353fa692beab90057318b859c | 1 | 0 ***NEW | Y (, Trojan.Win32.Yakes.acev , , ) |
| f61ba933ea990e83a84c2cc9cbd6dc32 | 2 | 0 ***NEW | Y (, Net-Worm.Win32.Kolab.bgcs , , ) |
| 5b174cefdc4322a9a9d2ff90a9b2fbc7 | 1 | 0 ***NEW | Y (W32/Trojan.MEX ,<br>Backdoor.Win32.Rbot.bni , , ) |
| c3d2e3026f0d69689df95c06802d82bc | 1 | 0 ***NEW | Y (w32/virut.7116 ,<br>Backdoor.Win32.Rbot.adqd , , ) |
| 1d53fb866c27a421f7557e3cda0592ac | 4 | 0 ***NEW | N (, , , ) |
| 0d085a46de34df53c75f9ea8d5ad3a86 | 1 | 0 ***NEW | Y (w32/emailworm.hqk ,<br>Net-Worm.Win32.Allaple.e , , ) |

Four of these files have been in the Wildlist.

**Note**

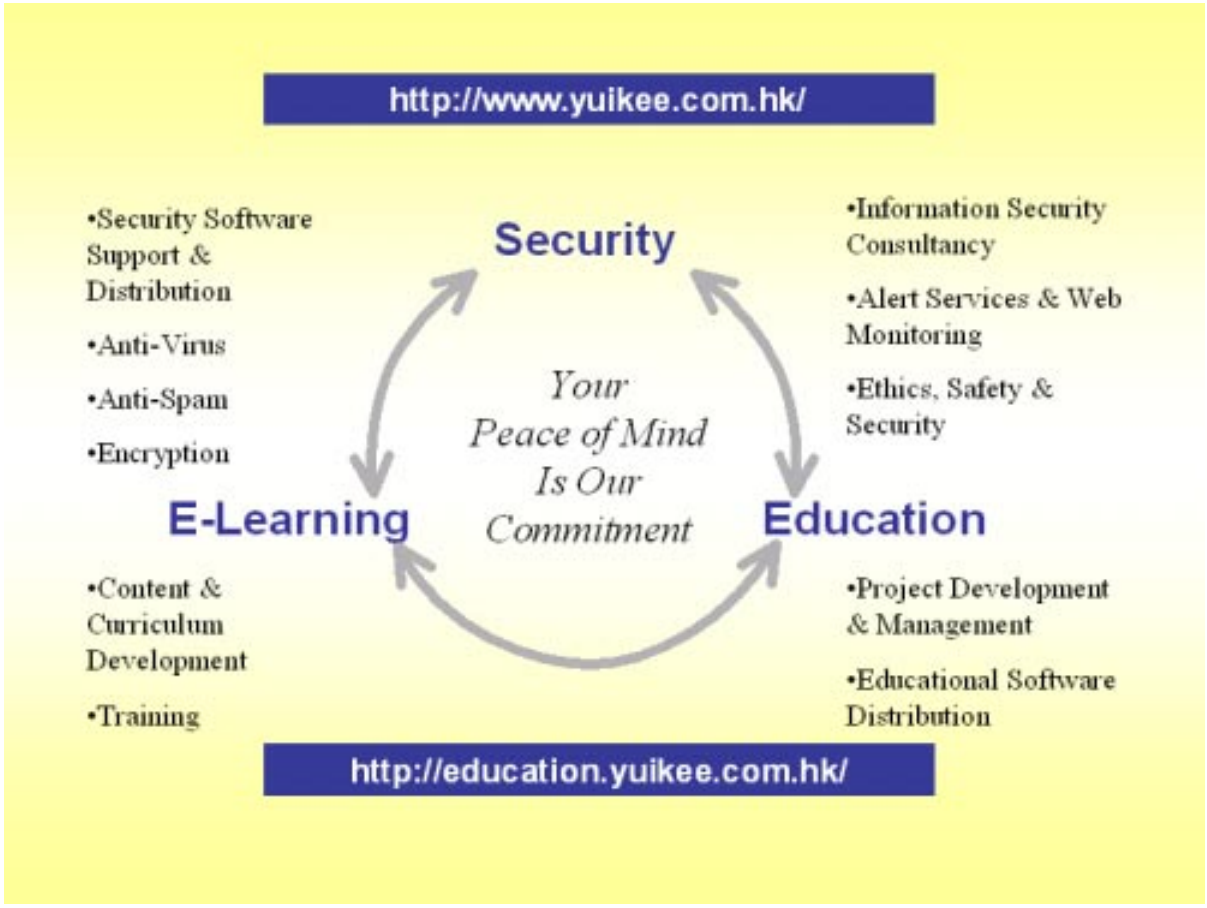
The parameter 'Detection' here relates to whether one or more scanners was able to associate a name with this checksum.

**More Information**

[January Hong Kong Honeypot Report]
[West Coast Labs]


YUI KEE 銳基電腦顧問有限公司
Anti-Virus, Network Security & Education

Suite C & D, 8/F, Yally Industrial Building
6 Yip Fat Street, Wong Chuk Hang, Hong Kong
Tel: 2870 8550 Fax: 2870 8563
E-mail: info@yuikee.com.hk
http://www.yuikee.com.hk/


http://www.yuikee.com.hk/
Security
•Security Software Support & Distribution
•Anti-Virus
•Anti-Spam
•Encryption
•Information Security Consultancy
•Alert Services & Web Monitoring
•Ethics, Safety & Security
Your Peace of Mind Is Our Commitment
E-Learning
Education
•Content & Curriculum Development
•Training
•Project Development & Management
•Educational Software Distribution
http://education.yuikee.com.hk/