(http://digg.com/submit?url=https%3A%2F%2Ftechhelplist.com%2Fspam-list%2F930-re-purchase-order-harewood-trading-corp-malware&title=Re%3A%20Purchase%20Order%20-%20Harewood%20Trading%20Corp.%20-%20Malware) (http://www.facebook.com/sharer.php?u=https%3A%2F%2Ftechhelplist.com%2Fspam-list%2F930-re-purchase-order-harewood-trading-corp-malware&t=Re%3A%20Purchase%20Order%20-%20Harewood%20Trading%20Corp.%20-%20Malware) (https://plus.google.com/share?url=https%3A%2F%2Ftechhelplist.com%2Fspam-list%2F930-re-purchase-order-harewood-trading-corp-malware) (http://www.stumbleupon.com/submit?url=https%3A%2F%2Ftechhelplist.com%2Fspam-list%2F930-re-purchase-order-harewood-trading-corp-malware&title=Re%3A%20Purchase%20Order%20-%20Harewood%20Trading%20Corp.%20-%20Malware) (http://twitter.com/share?text=Re%3A%20Purchase%20Order%20-%20Harewood%20Trading%20Corp.%20-%20Malware via @techhelplistcom&url=https%3A%2F%2Ftechhelplist.com%2Fspam-list%2F930-re-purchase-order-harewood-trading-corp-malware)

Spam list

Re: Purchase Order - Harewood Trading Corp. - Malware

Details

Parent Category: Spam List (/spam-list/46-spam-list)

Published: 26 September 2015

Created: 26 September 2015

Last Updated: 26 September 2015

Harewood Trading (/component/tags/tag/239-harewood-trading)

Email:

Fake Harewood Trading Corp. malware spam emails claim they have a revised invoice for a purchase order attached.

Attached zip contains an executable virus or trojan horse.

These emails are not coming from Harewood Trading Corp. or harewoodtrading.com which doesn't even seem to exist.

Subject: Re: Purchase Order

```
Hello,

Please find the attached revised Invoice for purchase order, kindly look
through it and send me a price quote for the items listed in the attached.

Best Regards,

Chang Biming
(Asst. Manager)
Harewood Trading Corp.
Address. 14F, 86 Singde Road, San Chong Dist,
New Taipei City, Taiwan
Tel. +886-2-8871-3516
Fax. +886-2-8961-3517 | +886-2-8511-7118
Email. Chang.Biming@harewoodtrading.com
Skype. Chang.Biming
www.harewoodtrading.com

***************************************************************
Think environmentally and only print if absolutely necessary
***************************************************************
This email and any files transmitted with it are confidential and solely
for the  use of the intended recipient. If you have received this email in
error please delete this message and do not forward to any other party.

   purchase order.rar (968)
```

Header Examples:

24 September 2015

Spoofs gmail.com in From headers and Envelope headers (MAIL FROM connection string) but the IP address doesn't belong to Google. It DOES go to that domain, satam.eu .

```
Received: from satam.eu [62.73.5.77]
   X-Envelope-From: changbimingab1 @gmail.com
   Subject: Re: Purchase Order
   From: "Chang Bimling" <changbimingab1@gmail.com>
```

Malware

24 September 2015

Attachment : purchase order.rar containing purchase order.exe (DarkComet RAT)

This showed up in a real .rar file, not a .zip named as a .rar. So right off the bat you know this is interesting.

VirusTotal report
(https://www.virustotal.com/en/file/4ee0d69a96f8146dd16deceff174bc99211d1bad6acf633f981c71078eb01188/analysis/)

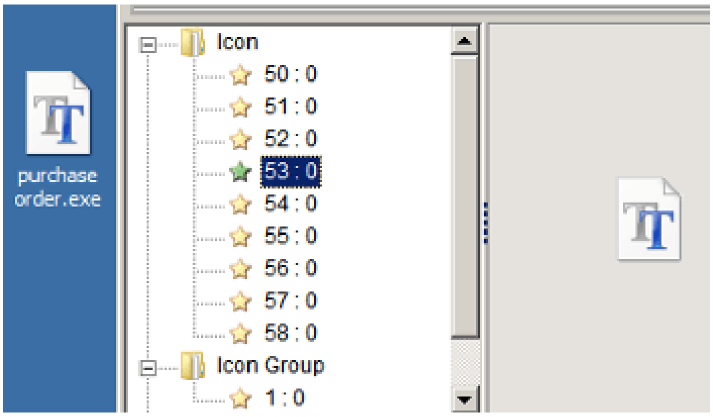
```
Kaspersky       Backdoor.Win32.DarkKomet.gbro
Microsoft       Backdoor:Win32/Fynloski.R
NANO-AV         Trojan.Win32.DarkKomet.dxiacs
```

Malwr.com report (https://malwr.com/analysis/OGViNzkwN2QzZmY4NDJmNTkxZDk1ZmNlN2JkMDJjZTE/)

```
Steals private information from local Internet browsers
Creates an Alternate Data Stream (ADS)
Installs itself for autorun at Windows startup
```

hybrid-analysis.com report (https://www.hybrid-analysis.com/sample/4ee0d69a96f8146dd16deceff174bc99211d1bad6acf633f981c71078eb01188?environmentId=3)

The executable wants to look like a TTF font file.



Upon execution it moves itself to :

```
...\AppData\Roaming\Microsoft\Windows\nasmon.exe
```

and then drops a small executable to:

```
...\AppData\Roaming\Microsoft\Windows\scsiwind.exe
```

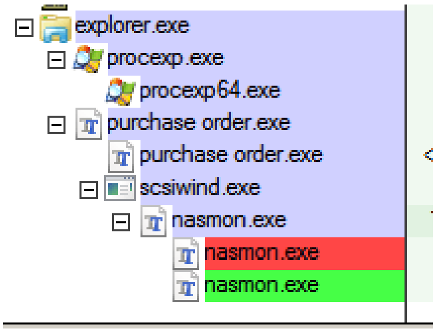
then creates 2 startups:

```
HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows\Load
  /c File not found: /c

HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows\Load
...\AppData\Roaming\Microsoft\Windows\scsiwind.exe
```

... the first of which looks like an error.

Processes looked this initially. The manually-ran executable was *purchase order.exe* and the smaller dropped *scsiwind.exe* was the parent of the moved *nasmon.exe* (the moved copy of *purchase order.exe*) After reboot, the original *purchase order.exe* processes are no longer running, but *scsiwind.exe* has a startup and runs *nasmon.exe*.



```
explorer.exe
  procexp.exe
    procexp64.exe
  purchase order.exe
    purchase order.exe
    scsiwind.exe
      nasmon.exe
        nasmon.exe
        nasmon.exe
```

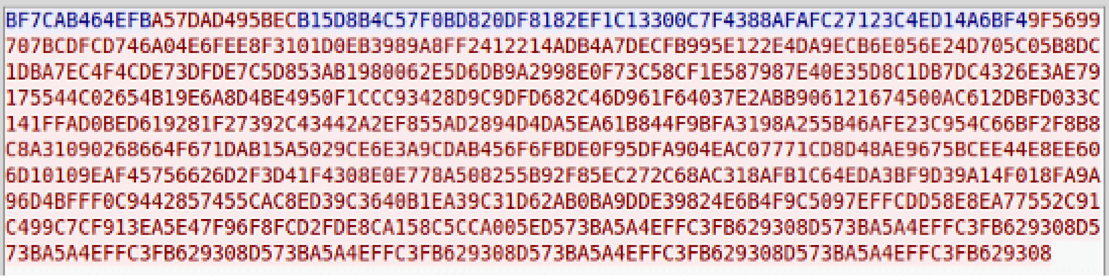
A DNS lookup is performed for :

```
123cooper.no-ip.biz
```

Which at the time of testing it, returned IP address :

```
178.175.138.224
```

A TCP conversation then ensued with 178.175.138.224:123

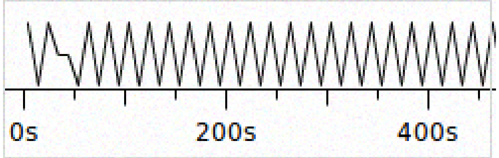


```
BF7CAB464EFBA57DAD495BECB15D8B4C57F0BD820DF8182EF1C13300C7F4388AFAFC27123C4ED14A6BF49F5699
707BCDFCD746A04E6FEE8F3101D0EB3989A8FF2412214ADB4A7DECFB995E122E4DA9ECB6E056E24D705C05B8DC
1DBA7EC4F4CDE73DFDE7C5D853AB1980062E5D6DB9A2998E0F73C58CF1E587987E40E35D8C1DB7DC4326E3AE79
175544C02654B19E6A8D4BE4950F1CCC93428D9C9DFD682C46D961F64037E2ABB906121674500AC612DBFD033C
141FFAD0BED619281F27392C43442A2EF855AD2894D4DA5EA61B844F9BFA3198A255B46AFE23C954C66BF2F8B8
C8A31090268664F671DAB15A5029CE6E3A9CDAB456F6FBDE0F95DFA904EAC07771CD8D48AE9675BCEE44E8EE60
6D10109EAF45756626D2F3D41F4308E0E778A508255B92F85EC272C68AC318AFB1C64EDA3BF9D39A14F018FA9A
96D4BFFF0C9442857455CAC8ED39C3640B1EA39C31D62AB0BA9DDE39824E6B4F9C5097EFFCDD58E8EA77552C91
C499C7CF913EA5E47F96F8FCD2FDE8CA158C5CCA005ED573BA5A4EFFC3FB629308D573BA5A4EFFC3FB629308D5
73BA5A4EFFC3FB629308D573BA5A4EFFC3FB629308D573BA5A4EFFC3FB629308D573BA5A4EFFC3FB629308
```

The blue being the server and the pink being the client / malware. For a while, the client simply sent:

```
D573BA5A4EFFC3FB629308
```

every 20 seconds like clockwork.

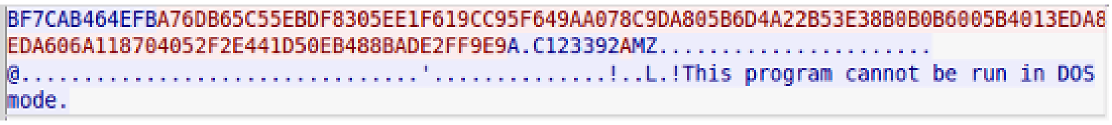


The traffic triggered these NSM / IDS rules :

```
ETPRO TROJAN DarkComet-RAT activity
ETPRO TROJAN DarkComet-RAT init connection 2
ETPRO TROJAN Backdoor.Win32.DarkKomet Keep-Alive
ETPRO TROJAN DarkComet-RAT server join acknowledgement 2
```

Which made me question if I should call it Komet or Comet. Anyway...

After a while, my infected computer downloaded another executable :



```
BF7CAB464EFBA76DB65C55EBDF8305EE1F619CC95F649AA078C9DA805B6D4A22B53E38B0B0B6005B4013EDA8
EDA606A118704052F2E441D50EB488BADE2FF9E9A.C123392AMZ......................
@................................'..............!..L.!This program cannot be run in DOS
mode.
```

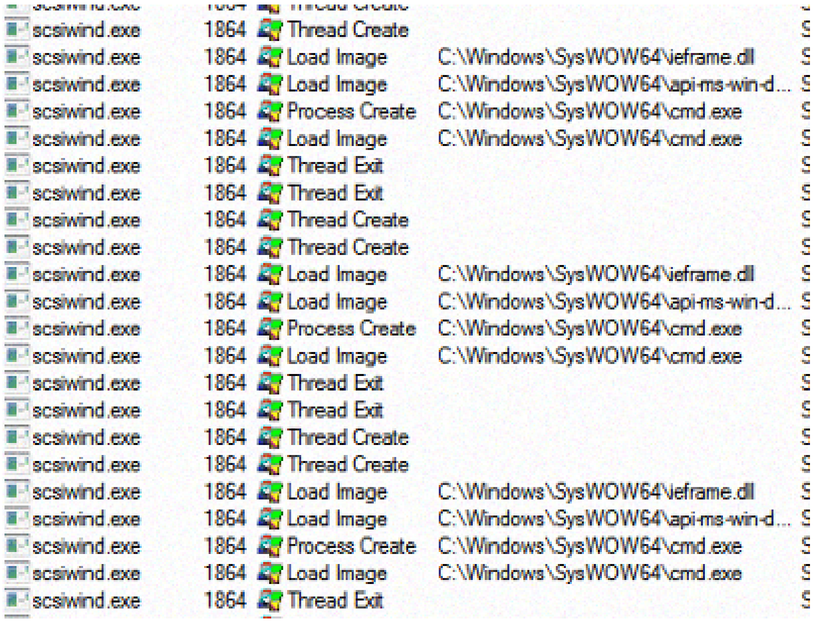
This executable was dropped to :

```
...\AppData\Roaming\purchase..exe
```

Dropped executable : scsiwind.exe (from initial Dark Comet)

VirusTotal report (https://www.virustotal.com/en/file/52f4e33c5539fc19c070a9f5bfc2044a2dc33c1b3e593eaa6e440c647ef94252/analysis/) | Malwr.com report (https://malwr.com/analysis/ZGMwYTg1NmEyMGZmNDM5OGE0MjQ5NDYzODQ5ODg3M2E/) | hybrid-analysis.com report (https://www.hybrid-analysis.com/sample/52f4e33c5539fc19c070a9f5bfc2044a2dc33c1b3e593eaa6e440c647ef94252?environmentId=1)

This executable is pretty small. It seems like its main job is just to be a persistence mechanism that starts things. Every few seconds it would go though a cycle like:



```
scsiwind.exe    1864  Thread Create
scsiwind.exe    1864  Thread Create
scsiwind.exe    1864  Load Image      C:\Windows\SysWOW64\ieframe.dll
scsiwind.exe    1864  Load Image      C:\Windows\SysWOW64\api-ms-win-d...
scsiwind.exe    1864  Process Create  C:\Windows\SysWOW64\cmd.exe
scsiwind.exe    1864  Load Image      C:\Windows\SysWOW64\cmd.exe
scsiwind.exe    1864  Thread Exit
scsiwind.exe    1864  Thread Exit
scsiwind.exe    1864  Thread Create
scsiwind.exe    1864  Thread Create
scsiwind.exe    1864  Load Image      C:\Windows\SysWOW64\ieframe.dll
scsiwind.exe    1864  Load Image      C:\Windows\SysWOW64\api-ms-win-d...
scsiwind.exe    1864  Process Create  C:\Windows\SysWOW64\cmd.exe
scsiwind.exe    1864  Load Image      C:\Windows\SysWOW64\cmd.exe
scsiwind.exe    1864  Thread Exit
scsiwind.exe    1864  Thread Exit
scsiwind.exe    1864  Thread Create
scsiwind.exe    1864  Thread Create
scsiwind.exe    1864  Load Image      C:\Windows\SysWOW64\ieframe.dll
scsiwind.exe    1864  Load Image      C:\Windows\SysWOW64\api-ms-win-d...
scsiwind.exe    1864  Process Create  C:\Windows\SysWOW64\cmd.exe
scsiwind.exe    1864  Load Image      C:\Windows\SysWOW64\cmd.exe
scsiwind.exe    1864  Thread Exit
```

The Process Create action was :

```
"C:\Windows\System32\cmd.exe" /c
  reg add "HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows"
  /v "Load" /d "cmd /c C:\Users\jimmy\Desktop\scsiwind.exe" /f
```

This sample above was run in isolation without the DarkComet executable. So the startup from the main *purchase order.exe* shown above was actually created by this little dropped runner.

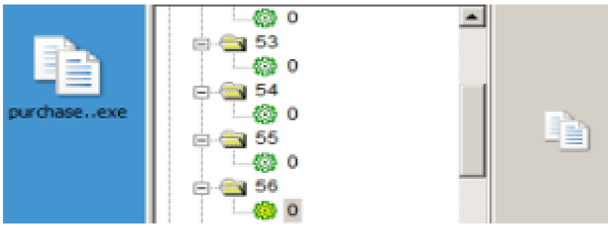
Downloaded executable : purchase..exe (NetWire RAT)

Somewhere in here is a NetWire RAT but with a little something different.

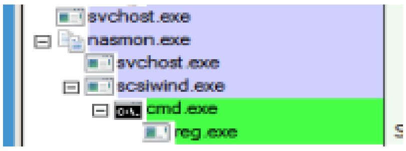
VirusTotal report (https://www.virustotal.com/en/file/9ada5f16e6ef81bbb49e3df778204360af7aee8537b8656da708c2ae2dfcf561/analysis/) | Malwr.com report (https://malwr.com/analysis/ODQzMjA2ZmQyM2EwNGZkZWI4OWE3Mzc4M2I2OWU0MTc/) | hybrid-analysis.com report (https://www.hybrid-analysis.com/sample/9ada5f16e6ef81bbb49e3df778204360af7aee8537b8656da708c2ae2dfcf561?environmentId=6)

Interestingly, this malware maintained a 0 score on VT for over 5 hours. However, the Invincea Cynomix system had identified it as belonging to a cluster of other RAT executables (http://cynomix3.appspot.com/sample/f2303c25c50f3c3502976ed7a69cba3793be2042) from the first time I uploaded during hour 0.

The icon looks like this thanks to icon grapical resources:



Upon execution, I get a familiar-looking setup :



```
svchost.exe
nasmon.exe
  svchost.exe
  scsiwind.exe
    cmd.exe
      reg.exe
```

The *purchase..exe* executable created process *svchost.exe* which moved the original exe to :

```
...\AppData\Roaming\Microsoft\Windows\nasmon.exe
```

and then drops a small executable to:

```
...\AppData\Roaming\Microsoft\Windows\scsiwind.exe
```

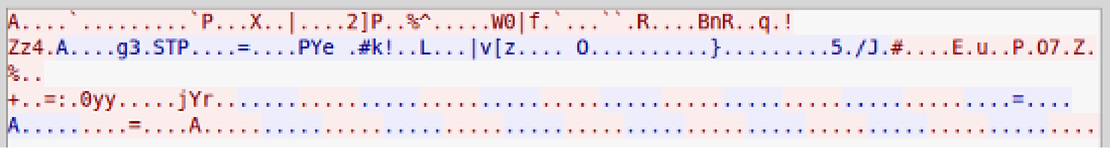
A DNS lookup is performed for :

```
123cooper.no-ip.biz ( same as above )
```

Which at the time of testing it, returned IP address :

```
178.175.138.224
```

A TCP conversation then ensued with 178.175.138.224:1221 which is a different port but same host as above.



```
A....`.........`P...X..|....2]P..%^.....W0|f.`...``.R....BnR..q.!
Zz4.A....g3.STP....=....PYe .#k!..L...|v[z.... O..........}.........5./J.#....E.u..P.07.Z.
%..
+..=:.0yy.....jYr...................................................................=....
A.........=....A.............................................................................
```

...which triggered NSM / IDS rules :

```
ET TROJAN Netwire RAT Client HeartBeat
ET TROJAN Possible Netwire RAT Client HeartBeat C2
ET TROJAN Netwire RAT Check-in
```

The little runner scsiwind.exe functions much the same but had a different hash than the one that came with the initial Dark Comet.

Dropped executable : scsiwind.exe (from secondary NetWire)

VirusTotal report (https://www.virustotal.com/en/file/43a3d2b2ab1edf7747b5df7e5d28fef7945999e2e5e3167329463291f1475821/analysis/) | Malwr.com report (https://malwr.com/analysis/NWEwNmRhZTdiMjNmNDczZTg2ZjFmZGNhNzkwMWMwZTk/) | hybrid-analysis.com report (https://www.hybrid-analysis.com/sample/43a3d2b2ab1edf7747b5df7e5d28fef7945999e2e5e3167329463291f1475821?environmentId=1)

Main Menu

Home (/)
Tech Tutorials (/tech-tutorials)
Spam list (/spam-list)
Pastes (/pastes)

Found something bad?

Do your part to clean it up!

Report malicious links to:

StopBadware.org (https://www.badwarebusters.org/community/submit)

Report phishing links to:

Google Safebrowsing - Phishing (http://www.google.com/safebrowsing/report_phish/)

Netcraft Anti-Phishing (http://toolbar.netcraft.com/report_url)

Send Virus Samples to:

Clam AV Database (http://www.clamav.net/report/report-malware.html)

Microsoft Anti-Malware DB (https://www.microsoft.com/security/portal/submission/submit.aspx)

But most importantly:

Follow THL on Twitter (https://twitter.com/Techhelplistcom)

Submitting an email to THL

Submissions welcome!

j (a-t) techhelplist (d-o-t) com

password zips with "slick-banana"

Some other GREAT resources

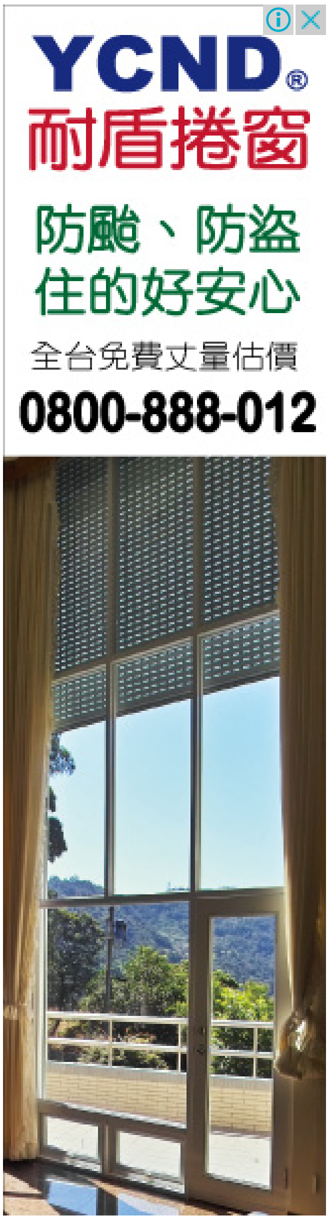
Malware Traffic Analysis (http://malware-traffic-analysis.net/)

StopMalvertising (http://stopmalvertising.com)

Dynamoo's Blog (http://blog.dynamoo.com)

MyOnlineSecurity (http://myonlinesecurity.co.uk)

THL Privacy Policy (https://techhelplist.com/index.php/670-privacy-policy)


YCND®
耐盾捲窗
防颱、防盜
住的好安心
全台免費丈量估價
0800-888-012

Back to Top