

## HTran and the Advanced Persistent Threat

- **URL:** <http://www.secureworks.com/research/threats/htran/>
- **Date:** August 3, 2011
- **Author:** Joe Stewart, Director of Malware Research, Dell SecureWorks Counter Threat Unit Research Team

While researching one of the malware families involved in the RSA breach disclosed in March 2011, Dell SecureWorks CTU observed an interesting pattern in the network traffic of a related sample (MD5:53ba6845f57f8e9ef600ef166be3be14). When the sample under analysis attempted to connect to the C2 server at my.amazingrm.com (203.92.45.2), the server returned a succinct plain-text error message instead of the expected HTTP-formatted response:

```
[SERVER]connection to funn
```

Although the message was seemingly truncated, this pattern was enough to correlate the error string to a known (and fairly old) program called "HUC Packet Transmit Tool", or "HTran", for which source code can be readily found on the Internet: [http://read.pudn.com/downloads199/sourcecode/windows/935255/htran.cpp\\_.htm](http://read.pudn.com/downloads199/sourcecode/windows/935255/htran.cpp_.htm)

HTran is a rudimentary connection bouncer, designed to redirect TCP traffic destined for one host to an alternate host. The source code copyright notice indicates that HTran was authored by "lion", a well-known Chinese hacker and member of "HUC", the [Honker Union of China](#). The purpose of this type of tool is to disguise either the true source or destination of Internet traffic in the course of hacking activity.

HTran contains several debugging messages throughout the source code that are sent to the console or to the connecting client in order to diagnose connection issues. The part of the HTran source code that generated the error message seen in the trojan C2 response is shown below:

```
if(client_connect(sockfd2,host,port2)==0)
{
  closesocket(sockfd2);
  sprintf(buffer,"[SERVER]connection to %s:%d error\r\n", host, port2);
  send(sockfd1,buffer,strlen(buffer),0);
}
```

The code is written so that if the connection bouncer is unable to connect to the hidden destination in order to relay the incoming traffic, the formatted error message containing the target host and port parameters will be sent to the connecting client. As long as there are no connection issues, HTran might be a useful tool to hide a trojan C2's true location - but, in the case of any connection downtime between the HTran host and the hidden C2, HTran will betray the location of the hidden C2 host.

Instances of HTran on multiple hosts could theoretically be chained together in order to add extra layers of obfuscation. However, in case of the final endpoint C2 being unavailable for any reason, the last link in the HTran chain will still pass its connection failure message up the chain, rendering all of the other layers of obfuscation useless. This tiny bit of error debugging code left in by the author can be quite useful if one wants to track HTran-bounced hacking activity to its source.

### HTran Survey

Armed with the knowledge of HTran's transient error message formatting, Dell SecureWorks CTU was able to locate TCP packet captures containing HTran connection errors in response to traffic from other APT-related malware that had been previously executed in our sandnet. The following Snort signatures can be used by other organizations to search for HTran connection error messages in transit on their networks:

```
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"HTran Connection Redirect Failure Message"; flow:established,from_server; dsize:<80; content:"|5b|SERVER|5d|connection|20|to|20|"; depth:22; reference:url,www.secureworks.com/research/threats/htran/; sid:111111111; )
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"HTran Connection Redirect Failure Message (Unicode)"; flow:established,from_server; dsize:<160; content:"|5b00|S|00|E|00|R|00|V|00|E|00|R|005d00|c|00|o|00|n|00|n|00|e|00|c|00|t|00|i|00|o|00|n|002000|t|00|o|002000|"; depth:44; reference:url,www.secureworks.com/research/threats/htran/; sid:111111112; )
```

In addition to locating historical packet captures containing evidence of HTran connection failures, Dell SecureWorks CTU

implemented a scanning system which checks for the HTtran error message in responses from active probing of more than a thousand IP addresses known to be associated with APT trojan activity currently or in the past. The results of this survey can be seen in the following table:

| Malware C2 IP/Port                      | Associated Hostnames  | Host-Related Malware Hashes  | Hidden Destination IP/Port   |
|---|---|--|--|
| 12.38.236.41:443                        | epod.businessconsults.net<br>happy2010.lflinkup.net<br>info.businessconsults.net<br>pop.businessconsults.net<br>ssa.businessconsults.net<br>sys.businessconsults.net  | 3493fc0e4a76b9d12b68afc46cab7f34<br>fd4a4ac08f5a7271fbd9b8157d30244e<br>51744d77fc8f874934d2715656e1a2df                                     | 112.65.87.58:443<br>58.247.25.108:443  |
| 173.244.209.196:443                     | bbs.india-videoer.com<br>ititupdated.dyndns.info<br>news.india-videoer.com<br>www.india-videoer.com   | 1daa3e392d1fea79badfbc86d765d32<br>855cea7939936e86016a0aedee1d2c24  | 123.120.102.251:443  |
| 204.45.228.140:80<br>204.45.228.140:443 | create301.dyndns.info   | 00b9619613bc82f5fe117c2ca394a328   | 123.120.106.136:8080<br>123.120.117.98:9000<br>123.120.126.73:8080<br>123.120.127.146:9000 |
| 207.225.36.69:443                       | leets.hugesoft.org<br>rouji.freepirit.acmetoy.com<br>slnoa.newsonet.net<br>sos.businessconsults.net<br>trb.arrowservice.net<br>ug-aa.hugesoft.org<br>www.optimizon.com  | cca75af9786d7364866f40b80ddcc5c  | 58.247.240.91:80   |
| 212.125.200.197:443                     | inter.earthsolution.org<br>quick.earthsolution.org  | 3a3bf6cab9702d0835e8425f4e9d7a9c   | 223.167.5.10:8000<br>223.167.5.250:8000<br>223.167.5.254:8000                              |
| 212.125.200.204:443                     | bah001.blackcake.net<br>caci2.infosupports.com<br>doa.bigdepression.net<br>lucy2.businessconsults.net<br>lucy2.infosupports.com<br>lucy.blackcake.net<br>lucy.businessconsults.net<br>mantech.blackcake.net<br>news.businessconsults.net  | 03557c3e5c87e6a121c58f664b0ebf18<br>8a873136b6e4dd70ff9470288ff99d93<br>bbf4212f979c32eb6bc43bd8ba5996f9                                     | 112.64.214.174:443   |
| 220.110.70.51:443                       | qiao1.bigdepression.net<br>qiao2.bigdepression.net<br>qiao3.bigdepression.net<br>qiao4.bigdepression.net<br>qiao5.bigdepression.net<br>qiao6.bigdepression.net<br>sports.businessconsults.net<br>srs.infosupports.com   | c9067c06bb9e8a5304b93687c59e4e15   | 125.215.189.114:40781  |
| 60.249.150.162:443                      | nsweb.hostent.org<br>argentina.faqserv.com<br>epaserver.toythieves.com<br>mailserver.instanthq.com<br>mailserver.sendsmtp.com<br>moiserver.myftp.info<br>mosfdns.ddns.ms<br>office.lflink.com<br>san.www1.biz<br>seoulsummit.ddns.ms<br>songs.longmusic.com<br>sysinfo.mynumber.org<br>timeforbeat.ns01.us<br>www.cpear.ddns.us<br>yahoo2.epac.to<br>aar.bigdepression.net<br>conn.gxdet.com<br>db.billten.net<br>dobb.gxdet.com<br>info.billten.net<br>info.dcfrr.com<br>info.helpngr.net<br>info.new-soho.com |  | 121.229.201.158:10009<br>121.229.201.238:10009   |
| 64.255.101.100                          | info.scitence.net<br>mail.new-soho.com<br>mailsrv.scitence.net  | 056310138cb5ed295f0df17ac591173d<br>45a66ae3537488f7d63622ded64461e0<br>92e28cec1c82f5d82cbd80c64050c5ca<br>ec4d34c742d2d5714c600517f05c2253 | 112.64.213.249:443   |

|                  |   |  |                   |
|------------------|---|--|-------------------|
|                  | news.billten.net<br>news.scitence.net<br>pop.dnsweb.org<br>techniq.whandjg.net<br>webmail.dcfrr.com<br>webmail.whandjg.net<br>gee.safalife.com<br>ghma.earthsolution.org<br>hav.earthsolution.org<br>java.earthsolution.org<br>quiet.earthsolution.org<br>special.earthsolution.org<br>visual.earthsolution.org<br>vop.earthsolution.org<br>vope.purpledaily.com<br>catalog.earthsolution.org<br>ou2.infosupports.com<br>ou3.infosupports.com |  |                   |
| 68.96.31.136     |   | 3a3bf6cab9702d0835e8425f4e9d7a9c<br>7cb055ac3acbf53e07e20b65ec9126a1 | 223.167.5.10:8000 |
| 72.167.34.54:443 | ou7.infosupports.com<br>www2.wikaba.com<br>yang1.infosupports.com<br>yang2.infosupports.com   | 47a76cf2e60960405a492bc7f41b0483                                     | 58.247.27.232:443 |

### *HTran Survey Results*

The hostnames in the table were gathered using passive DNS records showing that at one point in time they pointed to the IP address in question. The hostnames may currently be pointed at different IP addresses than shown, as they are rotated frequently. The domains involved are all known to be connected to a variety of different Advanced Persistent Threat (APT) trojans. In cases where a related sample has been analyzed by Dell SecureWorks CTU, the MD5 hash of the sample is provided.

The survey of HTran traffic shows a clear pattern that can be seen by analyzing the Autonomous System Number (ASN) owner of each hidden IP address:

```

17621 | 112.64.213.249 | CNCGROUP-SH China Unicom Shanghai network
17621 | 112.64.214.174 | CNCGROUP-SH China Unicom Shanghai network
17621 | 112.65.87.58 | CNCGROUP-SH China Unicom Shanghai network
4134 | 121.229.201.158 | CHINANET-BACKBONE No.31,Jin-rong Street
4134 | 121.229.201.238 | CHINANET-BACKBONE No.31,Jin-rong Street
4808 | 123.120.106.136 | CHINA169-BJ CNCGROUP IP network China169 Beijing Province Network
4808 | 123.120.117.98 | CHINA169-BJ CNCGROUP IP network China169 Beijing Province Network
4808 | 123.120.126.73 | CHINA169-BJ CNCGROUP IP network China169 Beijing Province Network
4808 | 123.120.127.146 | CHINA169-BJ CNCGROUP IP network China169 Beijing Province Network
4515 | 125.215.189.114 | ERX-STAR PCCW IMSBiz
60055 | 223.167.5.10 | CNCGROUP-SH China Unicom Shanghai network
60055 | 223.167.5.250 | CNCGROUP-SH China Unicom Shanghai network
60055 | 223.167.5.254 | CNCGROUP-SH China Unicom Shanghai network
17621 | 58.247.240.91 | CNCGROUP-SH China Unicom Shanghai network
17621 | 58.247.25.108 | CNCGROUP-SH China Unicom Shanghai network
17621 | 58.247.27.232 | CNCGROUP-SH China Unicom Shanghai network

```

### *Autonomous System Owner By HTran IP Address*

Every hidden IP address observed in the HTran error messages captured during our survey is located on just a few different networks in the People's Republic of China (PRC). In almost every case, the observable C2 is in a different country, most likely the same country in which the victim institution is located.



It's not surprising that hackers using a Chinese hacking tool might be operating from IP addresses in the PRC. Most of the Chinese destination IPs belong to large ISPs, making further attribution of the hacking activity difficult or impossible without the cooperation of the PRC government.

### Conclusion

Over the past ten years, we have seen dozens of families of trojans that have been implicated in the theft of documents, email and computer source code from governments, industry and activists. Typically when hacking or malware traffic is reported on the Internet, the location of the source IP is not a reliable indicator of the true origin of the activity, due to the wide variety of programs designed to tunnel IP traffic through other computers. However, occasionally we get a chance to peek behind the curtain, either by advanced analysis of the traffic and/or its contents, or due to simple programmer/user error. This is one of those cases where we were lucky enough to observe a transient event that showed a deliberate attempt to hide the true origin of an APT. This particular hole in the operational security of a certain group of APT actors may soon be closed, however it is impossible for them to erase the evidence gathered before that time. It is our hope that every institution potentially impacted by APT activity will make haste to search out signs of this activity for themselves before the window of opportunity closes.