MALWARE ANALYSIS REPORT

FROM

Notice

This document contains information which is the intellectual property of Network Intelligence (India) Pvt. Ltd. (also called NII Consulting). This document is received in confidence and its contents cannot be disclosed or copied without the prior written consent of NII.

Nothing in this document constitutes a guaranty, warranty, or license, expressed or implied. NII disclaims all liability for all such guaranties, warranties, and licenses, including but not limited to: Fitness for a particular purpose; merchantability; non infringement of intellectual property or other rights of any third party or of NII; indemnity; and all others. The reader is advised that third parties can have intellectual property rights that can be relevant to this document and the technologies discussed herein, and is advised to seek the advice of competent legal counsel, without obligation of NII.

NII retains the right to make changes to this document at any time without notice. NII Consulting makes no warranty for the use of this document and assumes no responsibility for any errors that can appear in the document nor does it make a commitment to update the information contained herein.

COPYRIGHT

TRADEMARKS

Other product and corporate names may be trademarks of other companies and are used only for explanation and to the owners' benefit, without intent to infringe.

NII INVESTIGATOR CONTACT DETAILS

Name	K. K. Mookhey
Title	Founder & Principal Consultant
Company	Network Intelligence (India) Pvt. Ltd.
Address	204 Ecospace, Off Old Nagardas Road, Andheri (East), Mumbai 400069
Tel. No	+91 22 40052628
E – Mail	kkmookhey@niiconsulting.com

1 Executive Summary

1.1 Summary

In early 2012, a client contacted us with suspicious-looking emails that he had received. There were two emails received by the client. While we completed the investigation and submitted the report to the customer at that time, we never took the case forward. However, when the Norman Hangover report was published it rang a few bells, and we decided to take a deeper look at the malware samples we had collected and do a more detailed analysis once again.

The following sections outline our analysis results.

2 Analysis:

The attachments received by our client were as shown below:

File name	File format	MD5 Hash value
Loop Mobile Bill Statement Date 08.11.2011	Pdf	4dc67b4647d81c2edc7db3cee97d64a4
Services	Doc	d0c2f4793239fba6d5c8aa0540a40e49
The Most wanted terrorist by delhi police	Doc	7bf74012ab520be300c21c01add3e537

2.1 Stage 1: Analysis Of the Attachments

All three files were self-extracting executables, which when double-clicked revealed a set of files as shown below:

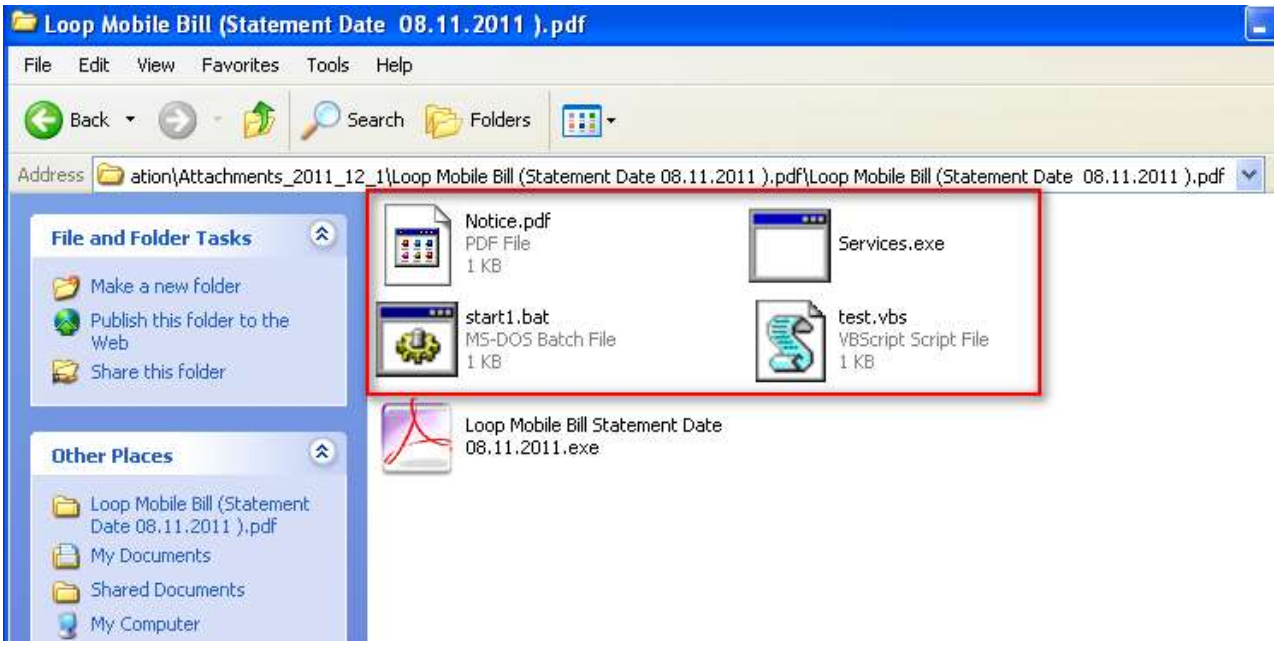
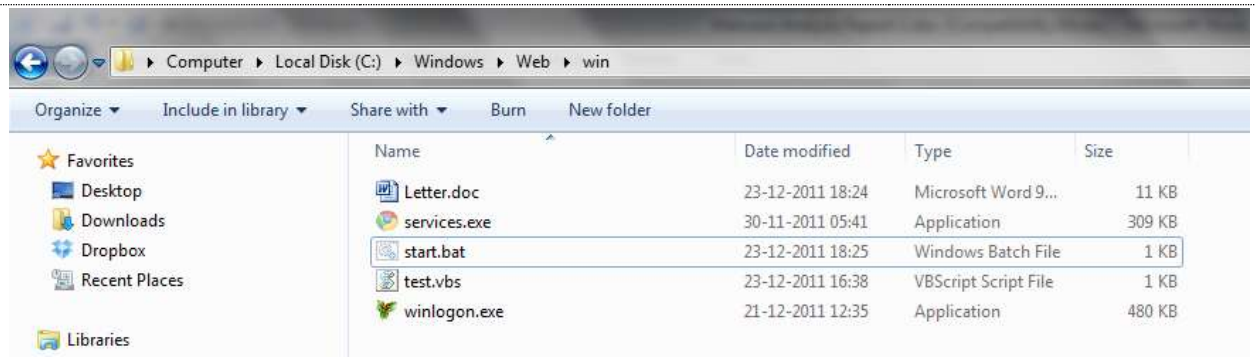


Figure 1 : Extracted Form Of Suspected File

In the normal course of execution, these files are extracted to a folder C:\Windows\web\win



As can be seen, this isn't exactly stealth mode.

Further analysis of the scripts reveals that their role is to make the malicious program run in stealth mode, disable the Windows firewall and then execute the malicious executable (services.exe) which eventually establishes a rogue TCP connection to a remote Web Server.

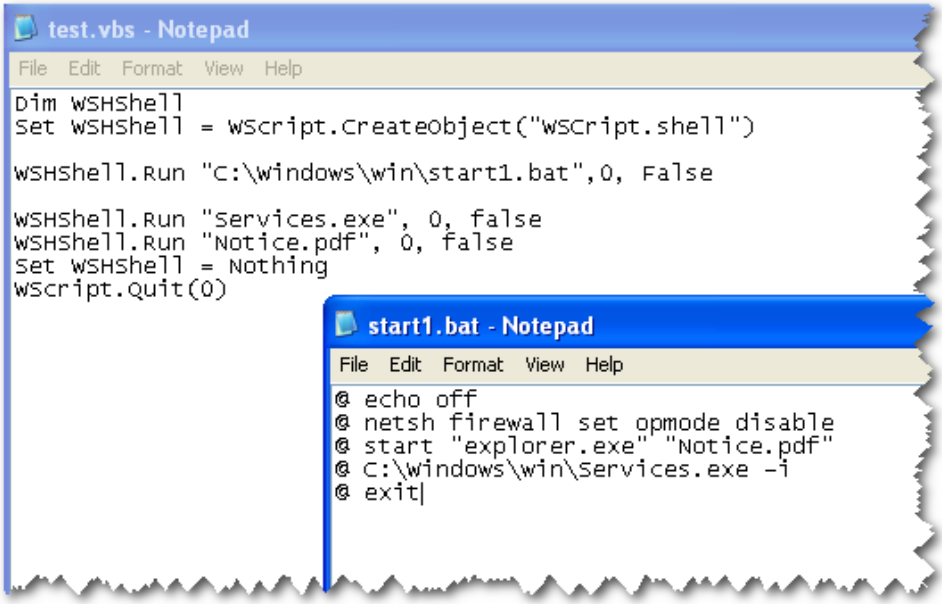


FIGURE 2 : CODES EXTRACTED

The self-extracting .exe also auto-launched the normal Word file, just to keep the guise going of it being a normal Word or PDF document. The services.exe will start in the background and establishes a TCP connection to the IP address 202.54.157.152.

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>netstat

Active Connections

  Proto  Local Address          Foreign Address        State

C:\Documents and Settings\Administrator>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    nii-c66e485c22a:1067   202.54.157.152:http    ESTABLISHED

C:\Documents and Settings\Administrator>
```

FIGURE 3 : TCP CONNECTION ESTABLISHED

A whois lookup showed the result that this IP address belongs to Tata Communications – an Indian ISP.

```
% [whois.apnic.net node-3]
% Whois data copyright terms    http://www.apnic.net/db/dbcopyright.html

inetnum:        202.54.0.0 - 202.54.255.255
netname:        TATACOMM-IN
descr:          Internet Service Provider
descr:          TATA Communications formerly VSNL is Leading ISP,
descr:          Data and Voice Carrier in India
admin-c:        TC651-AP
tech-c:         TC651-AP
country:        IN
remarks:        -+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
remarks:        This object can only be modified by APNIC hostmaster
remarks:        If you wish to modify this object details please
remarks:        send email to hostmaster@apnic.net with your organisation
remarks:        account name in the subject line.
remarks:        -+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
mnt-by:         APNIC-HM
mnt-lower:      MAINT-TATACOMM-IN
status:         ALLOCATED PORTABLE
changed:        hm-changed@apnic.net 20040319
changed:        hm-changed@apnic.net 20080826
changed:        hm-changed@apnic.net 20080827
source:         APNIC

role:           TATA Communications
nic-hdl:        TC651-AP
address:        6th Floor, LVSB, VSNL
address:        Kashinath Dhuru marg, Prabhadevi
address:        Dadar(W), Mumbai 400028
phone:          +91-22-56633503
fax-no:         +91-22-24320132
country:        IN
e-mail:         ip.admin@vsnl.co.in
admin-c:        IA15-AP
tech-c:         VT43-AP
mnt-by:         MAINT-TATACOMM-IN
changed:        hm-changed@apnic.net 20080826
changed:        hm-changed@apnic.net 20080827
source:         APNIC
```

FIGURE 4 : IP ADDRESS LOOKUP

Once the system got infected with the malicious program, it is also found that services.exe had automatically loaded into system start-up.

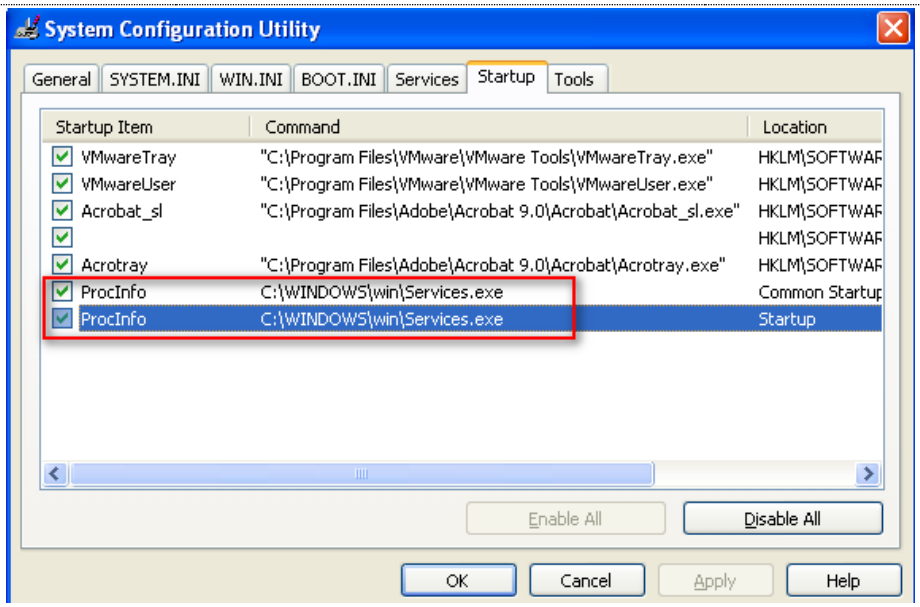


FIGURE 5 : SERVICES.EXE HAS LOADED INTO SYSTEM STARTUP

We did a very rudimentary check of services.exe on virustotal.org and it was found to be a Trojan with key-logging capability.

FIGURE 6 : TROJAN DETECTED

2.2 ANALYSIS OF SERVICES.DOC.EXE

Similar to the first self-executable, we have found services.exe file, which look like a Word document, but is wrapped up with multiple executables and scripts. These scripts are coded in a similar format, to launch the actual malware and hide its trail.

FIGURE 7 : FILE EXTRACTED

Taskmgr.exe is creating a backdoor in the victim's system, by establishing a backdoor connection to [IP address: 173.233.85.134].[1]

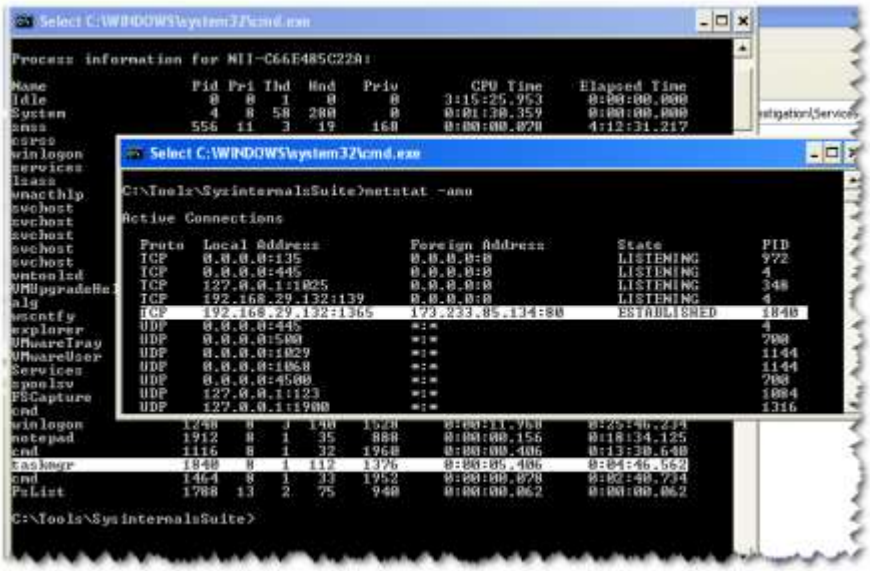


FIGURE 8 : TCP CONNECTION ESTABLISHED

Virustotal.org confirms the naughty nature of the various executable files in this case – called winlogon.exe.

[1] Note that this is our first common point with the Norman report. This IP address also appears in their Appendix

File name: winlogon.exe
Submission date: 2011-12-14 10:30:22 (UTC)
Current status: finished
Result: 6/ 43 (14.0%)

not reviewed
Safety score

Compact

Print results

http://www.virustotal.com - VirusTotal - Free Online Virus, Malware and URL Scanner

Table | Tabulated | CSV | HTML | BBCode | Show positives only

Antivirus	Version	Last update	Result
AhnLab-V3	2011.12.13.01	2011.12.14	Backdoor/Win32.Agent
AntiVir	7.11.19.103	2011.12.14	TR/Spy.Agent.AGK.1
AVG	10.0.0.1190	2011.12.13	PSW.Agent.ARMY
Emsisoft	5.1.0.11	2011.12.14	Trojan-PWS.Agent!IK
Ikarus	T3.1.1.109.0	2011.12.14	Trojan-PWS.Agent
K7AntiVirus	9.119.5671	2011.12.13	Riskware

MD5: 731adaf044f0f0fa35b99b4a60184b14
SHA1: 579b44535a1f627092349d35d550eb073d80d438
SHA256: e9f86117cc4c96966edb8fad6947f4a33652df3e94ecc8cab7ada45ae7f9f1c0
File size: 315904 bytes
Scan date: 2011-12-14 10:30:22 (UTC)

Antivirus: AhnLab-V3, AntiVir, Antiy-AVL, Avast, AVG, BitDefender, ByteHero, CAT-QuickHeal, ClamAV, Commtouch, Comodo, DrWeb, Emsisoft

FIGURE 9 : TROJAN BACKDOOR FOUND

We also analyzed that another executable (winlogon.exe) is modifying the Windows registry entries and taking screenshots of the infected system in the background and uploading this information to a website hosted at **(heritage-society.com[2])**

Base	Record	Name	IP	Reverse	Route	AS
www.heritage-society.com	a		173.233.85.134 United States	173-233-85-134.static.turnkeyinternet.net	173.233.64.0/19	AS40244 ?
heritage-society.com 9 minutes old	a		173.233.85.134 United States	173-233-85-134.static.turnkeyinternet.net		
	ns-soa	ns1.heritage-society.com 224 days old		(none)		?
	ns	ns1.heritage-society.com 224 days old		(none)		
		ns2.heritage-society.com 224 days old				
	mx	10 mail.heritage-society.com 224 days old	109.230.222.73 Germany	smtp10.trendsales1.com	109.230.208.0/20	AS3.435

com net turnkeyinternet.net static.turnkeyinternet.net trendsales1.com

FIGURE 10 : ROBTEX LOOKUP

The domain lookup of heritage-society:

[2] This is our second overlap with the Norman report. This domain name is one of the domain names discovered by them as well.

```
Registration Service Provided By: DOMAIN REGISTRATION COMPANY
Contact: +011.9997591058

Domain Name: HERITAGE-SOCIETY.COM

Registrant:
    PrivacyProtect.org
    Domain Admin        (contact@privacyprotect.org )
    ID#10760, PO Box 16
    Note - All Postal Mails Rejected, visit Privacyprotect.org
    Nobby Beach
    null,QLD 4218
    AU
    Tel. +45.36946676

Creation Date: 25-Apr-2011
Expiration Date: 25-Apr-2012

Domain servers in listed order:
    ns1.heritage-society.com
    ns2.heritage-society.com

Administrative Contact:
    PrivacyProtect.org
    Domain Admin        (contact@privacyprotect.org )
    ID#10760, PO Box 16
    Note - All Postal Mails Rejected, visit Privacyprotect.org
    Nobby Beach
    null,QLD 4218
    AU
    Tel. +45.36946676
```

FIGURE 11 : WHOIS LOOKUP

Updated info: The whois information on heritage-society.com reveals the following address currently:
Registrant Contact Details:

N/A
Bhuvan Malik (heatman001@hotmail.com)
102, Indu. Area, Phase-IV, Panchkula
chandigarh
Chandigarh,160017
IN
Tel. +91.9823945434

Running Wireshark on the infected system when it is trying to send screenshots to heritage-society.com reveals the following type of behavior:

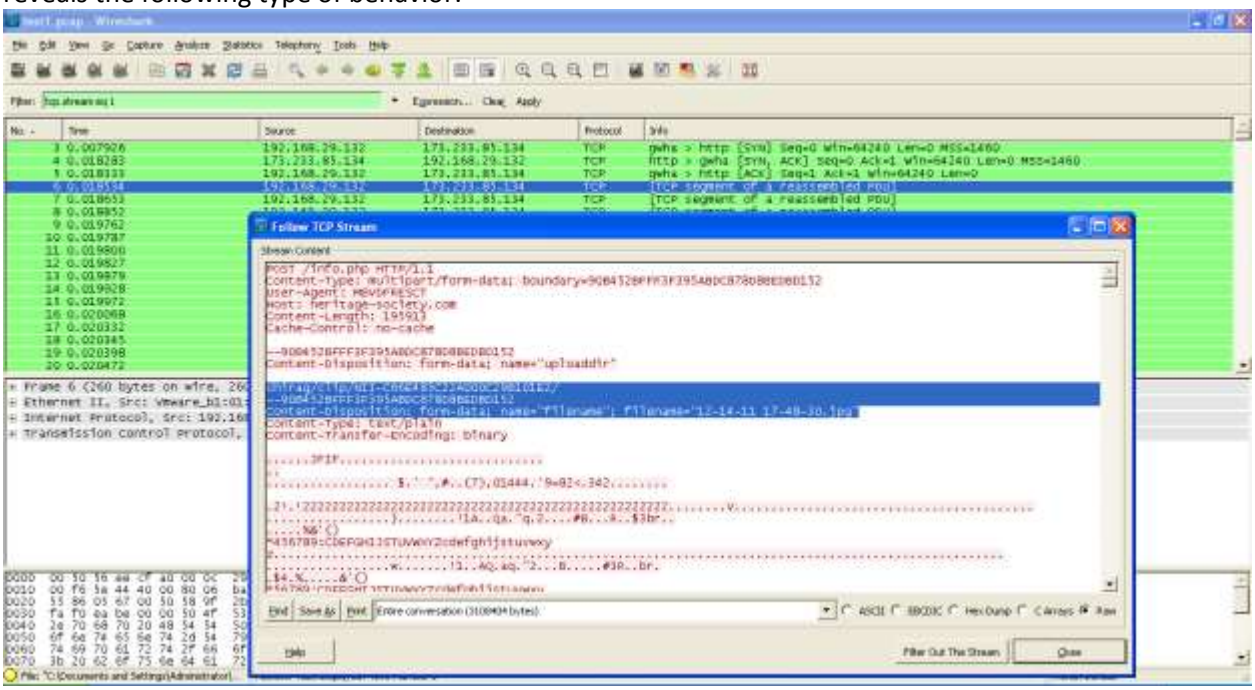


FIGURE 12 : PACKET CAPTURES OF SCREEN CAPTURE PROCESS USING WIRESHARK

Once we noted the path of the file upload, we simply navigated to the URL and noted our own system's screenshot being nicely saved as a jpg on the server.

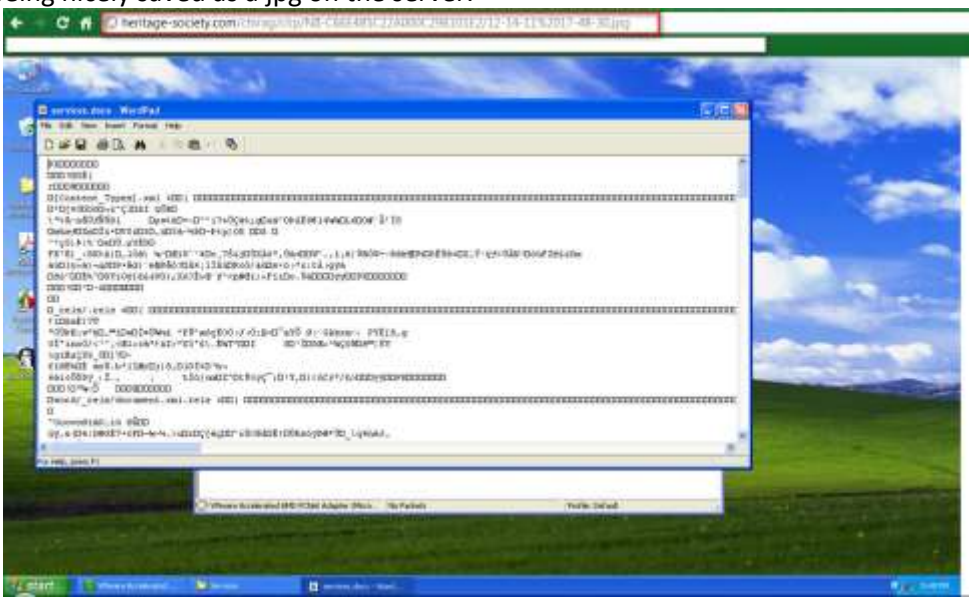


FIGURE 13 : BACKDOOR UPLOADING SCREEN CAPTURE TO ATTACKER'S DOMAIN

It is interesting to note that the malware author was uploading files to a folder called “chirag”. This is most surprising and slightly amateurish, unless of course it was someone else trying to implicate a person called “chirag”.

2.3 Analysis of “The Most Wanted Terrorist by Delhi Police”

The third attachment in this saga behaves in exactly the same way, with only some changes in the names of the files and the scripts. This malware also connects to **heritage-society.com.**

Figure 14 : Files Extracted

This one does something a little more interesting: once the malware gets infected, it will steal the hard-coded password (saved password of applications like Firefox, email client applications, etc) and upload the same to the attacker’s domain (also heritage-society.com)

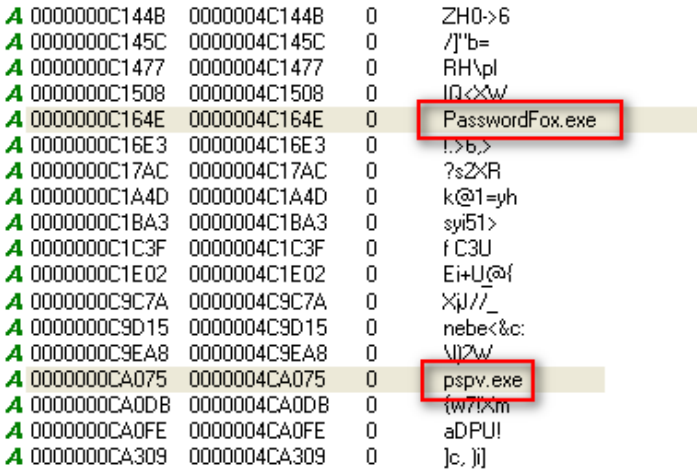


Figure 15 : Password Stealers Found

We analysed the behaviour of the malware by capturing the packets during the infection and concluded that it is hijacking stored passwords of various client applications.

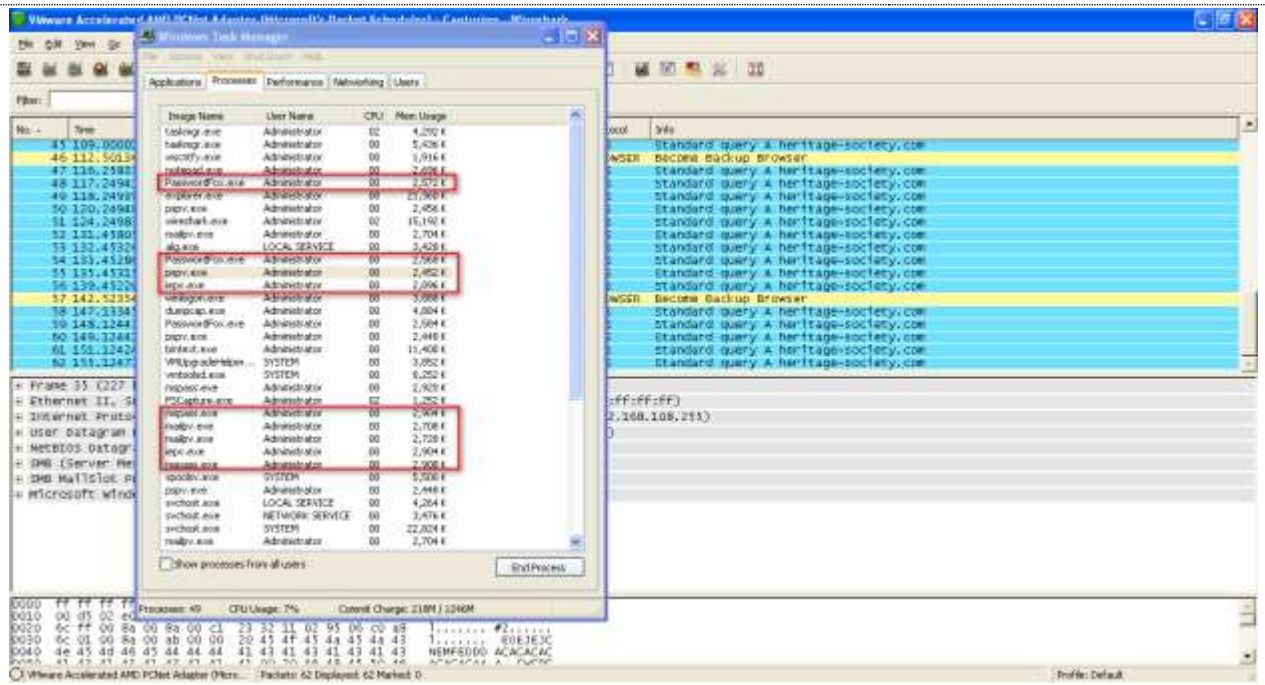


FIGURE 16 : PASSWORD STEALERS RUNNING DURING INFECTION

2.4 Compromised Entities

Under the folder "chirag", we found 3 more sub-folders, "clip", "drop", and "water". We are not sure what the meaning of these names is, but within these folders, we found another number of sub-folders. The names and structured of these sub-folders shows that these are the names of systems compromised, the IP address of the compromised system, and each of them contains text files called as "keylog.txt", which are captured passwords and other keyphrases. We are not revealing the details here, as we believe these are systems that have been made victims. A quick whois lookup of these IP addresses reveals them to be all Indian entities. This is a strong case for Indian law-enforcement agencies to investigate this further, as it is an attack on Indian enterprises

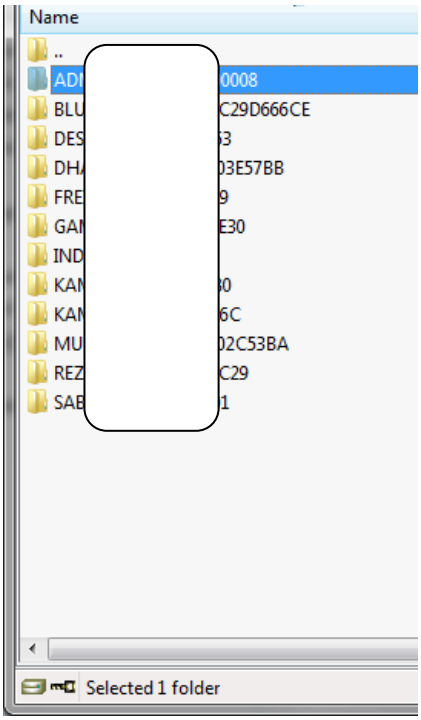


Figure 17 : Folders under the folder "CLIP" under "CHIRAG"

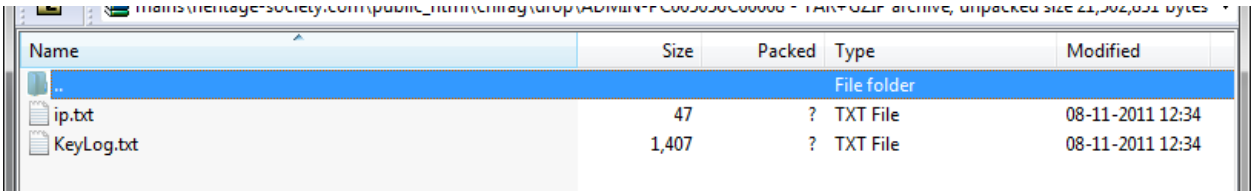


Figure 18 : Text files under each of the numerous sub-folders

Based on the information in the text files, we have reason to believe that the following entities have been compromised:

1. A hospital in Goa. The information in the log file contains patient data, in clear violation of the Indian IT Act
2. An agency helping migrant workers
3. A Tax/Accounts Consultant

4. Medical centre in Lucknow, Uttar Pradesh
5. At least 3 other entities, whom we are unable to determine the identities of

2.5 Things get interesting

At this stage, we decided to surf around on heritage-society.com and determine what sort of heritage they were protecting. We found that the site had a number of directory listing vulnerabilities. By listing the files and downloading what we could, things began to take an interesting turn:

calc(1).exe *	114,688	42,304
asa.wav *	4,746	672
aswwew.pdf *	2,714	2,464
application.doc *	779	608
aMiner_Installation_Step_by_Step.doc *	193,024	128,416
appin1.pdf *	2,714	2,464
appin(2).doc *	778	608
appin(1).doc *	778	608
aMatrix.doc *	303,118	38,384
appin.doc *	0	16
AdobeID20060816083920(4).pdf *	82,070	75,152
AdobeID20060816083920(3).pdf *	82,070	75,152
AdobeID20060816083920.pdf *	82,070	75,152

Another directory listing output is given below:

./win7
./win7/exploit.html
./win7/Exploit.jar
./win7/Exploit.class
./moneytime
./moneytime/abc
./moneytime/abc/dsfd.pdf
./moneytime/report.php
./moneytime/aaaa
./moneytime/aaaa/decr.exe
./moneytime/Aminer
./moneytime/Aminer/Utility_installation_step_by_step.doc
./moneytime/Aminer/aMiner2.0.iso
./moneytime/Aminer/aMiner_Installation_Step_by_Step.doc
./moneytime/Aminer/utilities.iso
./moneytime/Appin
./moneytime/Appin/appin.doc

./moneytime/Appin/appin1.pdf
./moneytime/email list.txt
./moneytime/WinXpcr.py
./moneytime/main.png
./moneytime/demor
./moneytime/demor/application.doc
./moneytime/key
./moneytime/key/conhost.exe
./moneytime/key/smse.exe

The files appin1.pdf, appin.doc, appin(1).doc and appin(2).doc download a file called http://heritage-society.com/moneytime/ABC/decr.exe onto the system where they are executed.

We had downloaded this file earlier, but not analysed it. After the Norman report, when we took a look at it, we could see that it is a VB executable. We analysed it for strings, and these ones caught our attention:

File Position	String
000000004DF3	Q*\AD:\YASH\PRO\MY\DELIVERED\RAT\Dragon-Eye\LATEST-DE-B\ServerZ\Server.vbp[3]
000000009D78	N30M4tr1X
000000009D90	M4tr1Xn30

It is possible that someone is trying to implicate Appin by creating files with these names.

The other filenames that caught our attention were:

Name	Size	Packed
..		
aMatrix.rar *	124,352,115	124,653,040
AVs.rar *	1,013,065,294	1,014,488,6...
Codejock.Xtreme.Suite.Pro.ActiveX.v13.2.1.Retail.Incl.Keymake...	58,375,418	58,486,048
CRRedist2008_x86.zip *	16,128,677	16,134,688
Data.rar *	372,357	369,920
AdobeID20060816083920(3).pdf *	82,070	75,152
AdobeID20060816083920(4).pdf *	82,070	75,152
AdobeID20060816083920.pdf *	82,070	75,152
aMatrix Help.chm *	15,502,089	15,525,072
aMatrix.doc *	303,118	38,384
aMiner_Installation_Step_by_Step.doc *	193,024	128,416

A Google search for "aMiner_Installation_Step_by_Step.doc" revealed that it was a tool from Appin, with the same tool being available at:
http://www.eagle.appinonline.com/uploads/7/5/6/9/7569501/aminer_support.pdf

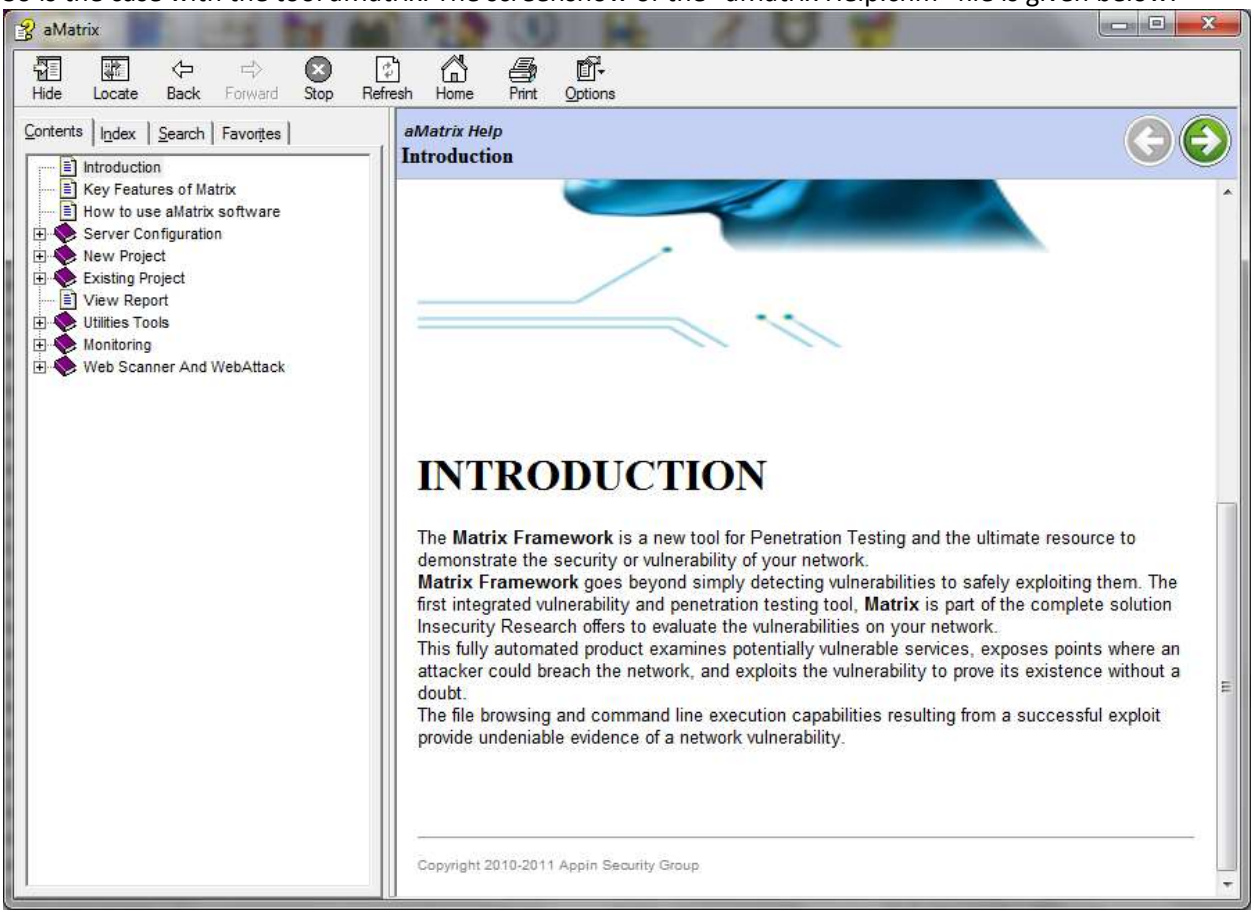
The tool aMiner on the Appin site is described as:

[3] These strings are identical to the ones identified in the Norman report

"aMiner Call Data Record Analyzer"

"aMiner" is an analytical tool which enables us to analyze, visualize and investigates to large amounts of disparate information and turn it into meaningful reports. This is achieved by providing a framework for information which helps the analyst quickly create a report of objects and relationships. This allows data to be collated and filtered such that the important relationships can be easily understood during the investigation.

So is the case with the tool aMatrix. The screenshow of the "aMatrix Help.chm" file is given below:



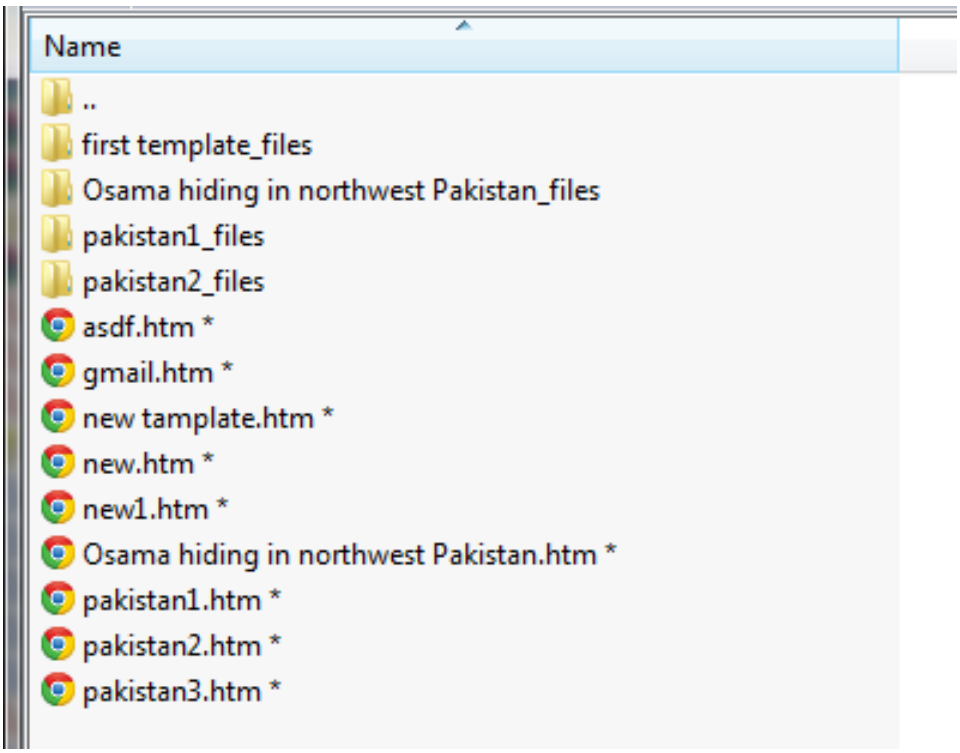
This tool is described as follows within the help file (site link http://www.appinonline.com/appin-amatrix-email-penetration-testing-tool.html):

Different Type of Attacks:

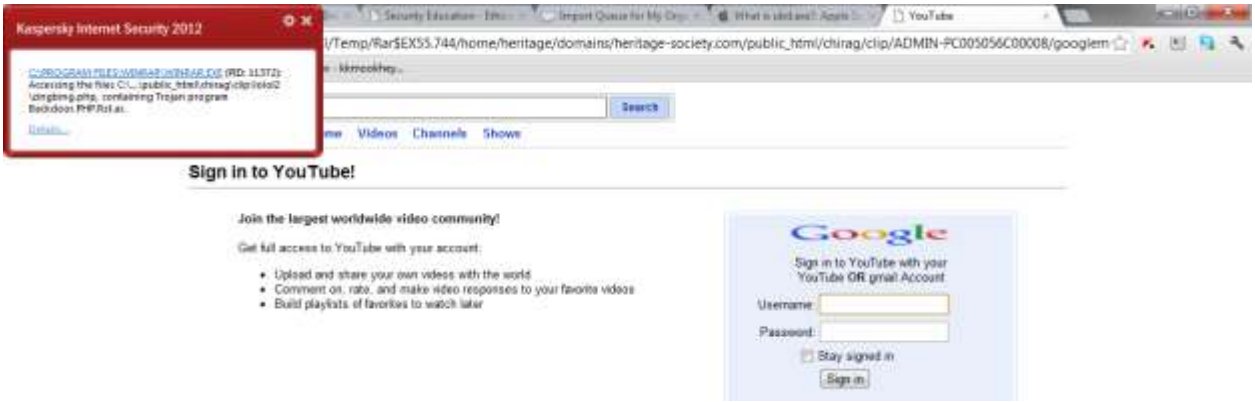
- Social Engineering Webpage (send as Link only).
- Exploits (sends either as Link or an attachment)
- Wrappers (sends either as Link or an attachment)

It is possible, that the attacker is a client of Appin or has got their hands on Appin tools and is using them.

Also, the folder of this tool on the server was in a password-protected RAR format, and we could only see the file listings. One of these matches with similar indicators in the Norman report, in that it builds an enticing Pakistan link:



The other files that we found of interest were HTML files that look like attempts at spear-phishing. These come with PHP backdoors as shown below:



2.6 EMAIL IDS DISCOVERED:

The PHP scripts contain this email ID: allmail.moniter@gmail.com

- Other email IDs we found were:
- rajuk058@gmail.com
- appins82@gmail.com
- demosoftware9@gmail.com
- just4u@gmail.com

3 Conclusion and Next Steps

From the above, we conclude that:

- We believe that this was malware written specifically from a corporate espionage perspective.
- The malware isn't really all that smart – says volumes for the general levels of security awareness given the number of people infected
- The affected entities discovered during our analysis are all Indian – hospital in Goa, visa facilitation agency in Bangalore, tax/account consultant, textile trading company, etc.
- The attacks also are Indian-flavoured (with attachment names of Loop Mobile Bill, Terrorists wanted by Delhi police, etc.).
- The attacks are targeted – my client did in fact use a mobile plan from Loop Mobile.
- One of the C&C IP addresses belongs to Tata Communications – an Indian ISP.
- Though the string "appin" occurs in the names of a number of files hosted on the C&C server as well as tools authored by Appin (aMatrix and aMiner), the link with Appin Security Group is not concrete. It is in Appin's best interest to cooperate with Indian Law Enforcement Agencies to investigate whether it is someone trying to malign their name or misusing their tools or ex-employees who have gone rogue.
- It is in the interest of Law Enforcement Agencies to take this ahead and investigate along the following lines:
    - Who had registered the IP address 202.54.157.152 (Tata Communications)
    - Who had registered the domain heritage-society.com
    - Who are "chirag" and "yash"? Maybe they should talk to Chirag Goyal (in.linkedin.com/pub/chirag-goyal/58/629/2bb)
    - Who owns the email ID allmail.moniter@gmail.com and others noted in the section above
    - Who are the Indian entities compromised - we have their public IP addresses, if not their names
    - Is this a one-off issue, or part of a larger corporate espionage exercise carried out by rogue group/organization?

We would be, of course willing to share all details we have in our possession with the responsible investigation officers.

---- END OF REPORT ----