THE DARKHOTEL APT
A STORY OF UNUSUAL HOSPITALITY

Version 1.1
November, 2014

Global Research and Analysis Team

KASPERSKY lab

Contents

Executive Summary

The Darkhotel APT is a threat actor possessing a seemingly inconsistent and contradictory set of characteristics, some advanced and some fairly rudimentary. Inhospitably operating for almost a decade, the threat actor is currently active. The actor's offensive activity can be tied to specific hotel and business center Wi-Fi and physical connections, some of it is also tied to p2p/file sharing networks, and they have been known to spear-phish targets as well. Darkhotel tools are detected as "Tapaoux", "Pioneer", "Karba", and "Nemim", among other names. The following list presents a set of characteristics for the crew:

- operational competence to compromise, mis-use, and maintain access to global scale, trusted commercial network resources with strategic precision for years
- advanced mathematical and crypto-analytical offensive capabilities, along with no regard for undermining the trust extended to the Certificate Authorities and the PKI
- indiscriminately infect systems with some regional clarity over trusted and untrusted resources to build and operate large botnets
- well-developed low level keyloggers within an effective and consistent toolset
- a focus throughout campaigns on specific victim categories and tagging them
- a larger, dynamic infrastructure built of apache webservers, dynamic dns records, crypto libraries, and php webapps
- regular 0-day access - recent deployment of an embedded Adobe Flash 0-day spear-phishing exploit, and infrequent deployment of other 0-day resources to sustain larger campaigns over several years

Introduction

When unsuspecting guests, including situationally aware corporate executives and high-tech entrepreneurs, travel to a variety of hotels and connect to the internet, they are infected with a rare APT Trojan posing as any one of several major software releases. These might be GoogleToolbar, Adobe Flash, Windows Messenger, etc. This first stage of malware helps the attackers to identify more significant victims, leading to the selective download of more advanced stealing tools.

At the hotels, these installs are selectively distributed to targeted individuals. This group of attackers seems to know in advance when these individuals will arrive and depart from their high-end hotels. So, the attackers lay in wait until these travelers arrive and connect to the Internet.

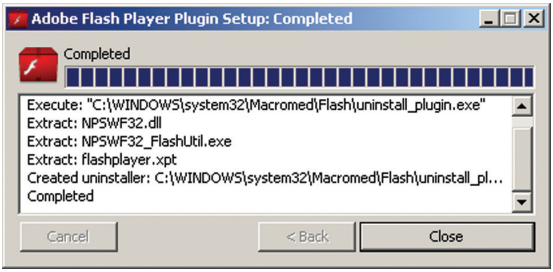
The FBI issued advisories about similar hotel incidents; Australian government officials produced similar, newsworthy accounts when they were infected. While an FBI announcement related to attacks on hotel guests overseas appeared in May 2012, related Darkhotel samples were already circulating back in 2007. And available Darkhotel server log data records connections as early as Jan 1, 2009. Additionally, seeding p2p networks with widely spread malware and 0-day spear-phishing attacks demonstrate that the Darkhotel APT maintains an effective toolset and a long-running operation behind the questionable hospitality it shows its guests.

Analysis

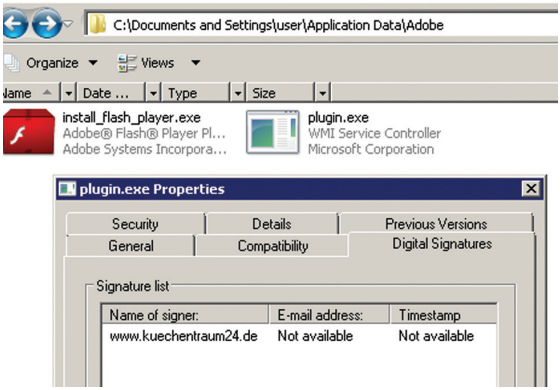
Delivery - Hotels/Business Centers and Indiscriminate Spread

Hotels and Business Centers Spread

The Darkhotel APT's precise malware spread was observed in several hotels' networks, where visitors connecting to the hotel's Wi-Fi were prompted to install software updates to popular software packages.



Of course, these packages were really installers for Darkhotel APT's backdoors, added to legitimate installers from Adobe and Google. Digitally signed Darkhotel backdoors were installed alongside the legitimate packages.



The most interesting thing about this delivery method is that the hotels require guests to use their last name and room number to login, yet only a few guests received the Darkhotel package. When visiting the same hotels, our honeypot research systems couldn't attract a Darkhotel attack. This data is inconclusive, but it points to misuse of check-in information.

Abusing Network Infrastructure

The Darkhotel actor maintained an effective intrusion set at hotel networks, providing ample access to unexpected points of attack over several years. These staging points also provide the attackers with access to check-in/check-out and identity information of visitors to high-end and luxury hotels.

As a part of an ongoing investigation, our research led us to embedded iframes within hotel networks that redirected individuals' web browsers to phony installers. The attackers were very careful with the placement of these iframes and executables on trusted resources - the hotels' network login portals themselves. The attackers were also very careful to immediately delete all traces of their tools as soon as an attack was carried out successfully. Those portals are now reviewed, cleaned and undergoing a further review and hardening process. We observed traces of a couple of these incidents in late 2013 and early 2014 on a victim hotel's network. The attackers set up the environment and hit their individual targets with precision. As soon as their target's stay was over and the attack-frame was closed, the attackers deleted their iframe placement and backdoored executables from the hotel network. The attackers successfully deleted traces of their work from earlier attacks in another hotel, but their offensive techniques were the same. Outside reports of the same activity at other hotels provide enough data to confirm the same careful operations there.

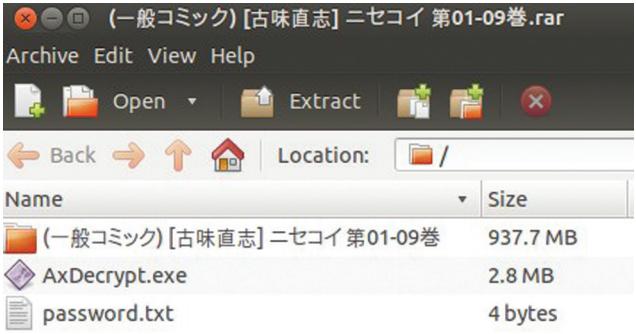
The attack technique blurs the line between a couple of common APT tactics; fairly inaccurate "watering holes" or "strategic web compromises" and more accurate spearphishing techniques. In this case, the Darkhotel attackers wait for their victim to connect to the Internet over the hotel Wi-Fi or the cable in their room. There is a very strong likelihood the targets will connect over these resources, and the attackers rely on that likelihood, much like at a watering hole. But the attackers also maintain truly precise targeting information over the victim's visit, much like they would know a victim's email address and content interests in a spearphishing attack. While setting up the attack, the Darkhotel attackers knew the target's expected arrival and departure times, room number, and full name, among other data. This data enables the attackers to present the malicious iframe precisely to that individual target. So, here we have yet another unique characteristic of this attacker - they employ a loosely certain but highly precise offensive approach.

Indiscriminate Spread

An example of the Darkhotel APT's indiscriminate malware spreading is demonstrated by the way it seeds Japanese p2p sharing sites, where the malware is delivered as a part of a large (approximately 900mb) rar archive. The archive is also spread over bittorrent, as detailed below. Darkhotel uses this method to distribute their Karba Trojan. These Japanese archives, translated for Chinese speaking viewers, appear to be sexual in nature, part of an anime sex/military comic scene, exposing the likely interests of potential targets.

This Darkhotel package was downloaded over 30,000 times in less than six months. The p2p bittorrent Darkhotel offering is listed here, posted on 2013.11.22. It was spread throughout 2014.

（一般コミック）［古味直志］ニセコイ 第01-09巻.rar



This torrent serves up an almost 900 mb file. The rar archive decompresses to a directory full of encrypted zips, the associated decryptor and a password file for decrypting the zips. But what looks like the AxDecrypt.exe decryptor is bound to both the true decryptor and the dropper for the Darkhotel Catch.exe Karba Trojan. When a user downloads the torrent and decrypts the zip files, the trojan surreptitiously is installed and run on the victim system.

Catch.exe, detected as Backdoor.Win32.Agent.dgrn, communicates with the following Darkhotel command and control servers:

microdelta.crabdance.com microyours.ignorelist.com micronames.jumpingcrab.com microchisk.mooo.com microalba.serveftp.com

Other examples of this Darkhotel backdoor bound within a shared torrent include adult content Japanese anime and more. There are tens of thousands of downloads of these individual torrents.

“torrent\[hgd资源组][漫画]comic1☆7漫画合集③+④+⑤+特典[5.08g][绅士向][总第四十三弹]（七夕节快乐！）\汉化\(comic1☆7) [莉零 (小鹿りな, 古代兵器)] 凌 -shinogi- (闪乱カグラ) [中文] “

and

“動漫\[hgd资源组][漫画]comic1☆7漫画合集③+④+⑤+特典[5.08g][绅士向][总第四十三弹]（七夕节快乐！）\汉化”）

The associated Darkhotel backdoor was hosted on bittorrent, emule, etc, under a variety of comic names. Examples include comics and anime offerings. Related Darkhotel command and control server domains include:

microblo5.mooo.com
microyours.ignorelist.com
micronames.jumpingcrab.com
microchisk.mooo.com
microalba.serveftp.com

Darkhotel Spear-phishing Campaigns

Darkhotel campaigns involving typical spear-phished Tapaoux implants publicly appeared in bits and pieces several times over the past five years. These subproject efforts targeted defense industrial base (DIB), government, and NGO organizations. Email content on topics like nuclear energy and weaponry capabilities was used as a lure. Early accounts were posted on contagio describing attacks on NGO organizations and government policy makers. This spear-phishing activity continues into 2014. The attacks follow the typical spear-phishing process and in the past couple of months, exploited systems retrieved downloader executables from web servers like hxxp://office-revision.com/update/files22/update.exe or hxxp://trade-inf.com/mt/duspr.exe

Over the past few years the group has emailed links that redirect targets’ browsers to Internet Explorer 0-day exploits. Sometimes the attachment itself includes an Adobe 0-day exploit.

Recent 0-day Deployment

This crew occasionally deploys 0-day exploits, but burns them when required. In the past few years, they deployed 0-day spear-phishing attacks targeting Adobe products and Microsoft Internet Explorer, including cve-2010-0188. In early 2014, our researchers exposed their use of cve-2014-0497, a Flash 0-day described on Securelist in early February.

The crew spear-phished a set of target systems connected to the Internet through Chinese ISPs, and developed capabilities within the 0-day exploits to handle hardened Windows 8.1 systems. It's interesting that the Flash objects were embedded in Korean documents titled "List of the latest Japanese AV wind and how to use torrents.docx" (loose English translation). The dropped downloader (d8137ded710d83e2339a97ee78494c34) delivered malcode similar to the "Information Stealer" component functionality summarized below, and detailed in Appendix D.

Digital Certificates and Delegitimizing Certificate Authority Trust

The Darkhotel actors typically sign their backdoors with digital certificates of one kind or another. However, the certificates originally chosen by this crew are very interesting because of their weak keys and likely abuse by attackers. Here is a listing of the certs that were commonly used to sign Darkhotel malcode, requiring advanced mathematical capabilities to factorize the keys at the time. They are not the only certificates used by the group. More recent activity suggests that the group has stolen certificates to sign their code.

CA Root	Subordinate CA/Issuer	Owner	Status	Valid From	Valid To
GTE CyberTrust	Digisign Server ID (Enrich)	flexicorp.jaring.my sha1/ RSA (512 bits)	Expired	12/17/2008	12/17/2010
GTE CyberTrust	Cybertrust SureServer CA	inpack.syniverse.my sha1/RSA (512 bits)	Revoked	2/13/2009	2/13/2011
GTE CyberTrust	Cybertrust SureServer CA	inpack.syniverse.com sha1/RSA (512 bits)	Revoked	2/13/2009	2/13/2011
GTE CyberTrust	Anthem Inc Certificate Auth	ahi.anthem.com sha1/ RSA (512 bits)	Invalid Sig.	1/13/2010	1/13/2011

CA Root	Subordinate CA/Issuer	Owner	Status	Valid From	Valid To
GlobalSign	Deutsche Telekom CA 5	www.kuechentraum24.de sha1/RSA (512 bits)	Revoked	10/20/2008	10/25/2009
GTE CyberTrust	Digisign Server ID (Enrich)	payments.bnm.gov.my sha1/RSA (512 bits)	Invalid Sig.	12/7/2009	12/7/2010
GTE CyberTrust	TaiCA Secure CA	esupplychain.com.tw sha1/RSA (512 bits)	Expired	7/2/2010	7/17/2011
GTE CyberTrust	Digisign Server ID (Enrich)	mcrs2.digicert.com. my sha1/RSA (512 bits)	Invalid Sig	3/28/2010	3/28/2012
GTE CyberTrust	Cybertrust SureServer CA	agreement.syniverse.com sha1/RSA (512 bits)	Invalid Sig	2/13/2009	2/13/2011
GTE CyberTrust	Cybertrust SureServer CA	ambermms.syniverse.com sha1/RSA (512 bits)	Invalid Sig.	2/16/2009	2/16/2011
Equifax Secure eBusiness CA-1	Equifax Secure eBusiness CA-1	secure.hotelreykjavik.i s md5/RSA (512 bits)	Invalid Sig	2/27/2005	3/30/2007
GTE CyberTrust	Cybertrust Educational CA	stfmail.ccn.ac.uk sha1/RSA (512 bits)	Invalid Sig.	11/12/2008	11/12/2011
GTE CyberTrust	Digisign Server ID (Enrich)	webmail.jaring.my sha1/RSA (512 bits)	Invalid Sig	6/1/2009	6/1/2011
GTE CyberTrust	Cybertrust Educational CA	skillsforge.londonmet.ac.uk sha1/RSA (512 bits)	Invalid Sig	1/16/2009	1/16/2012
GTE CyberTrust	Digisign Server ID (Enrich)	anjungnet.mardi.gov. my sha1/RSA (512 bits)	Invalid Sig	9/29/2009	9/29/2011
GTE CyberTrust	Anthem Inc Certificate Authority	dl-ait-middleware@anthem.com sha1/RSA (512 bits)	Invalid Sig	4/22/2009	4/22/2010
GTE CyberTrust	Cybertrust Educational CA	ad-idmapp.cityofbristol.ac.uk sha1/RSA (512 bits)	Invalid Sig	9/11/2008	9/11/2011
Verisign	Verisign Class 3 Secure OFX CA G3	secure2.eecu.com sha1/RSA (512 bits)	Invalid Sig	10/25/2009	10/26/2010
Root Agency	Root Agency	Microsoft md5/RSA (1024 bits)	Invalid Sig	6/9/2009	12/31/2039

CA Root	Subordinate CA/Issuer	Owner	Status	Valid From	Valid To
GTE Cybertrust	CyberTrust SureServer CA	trainingforms.syniverse.com sha1/RSA (512 bits)	Invalid Sig	2/17/2009	2/17/2011

All related cases of signed Darkhotel malware share the same Root Certificate Authority and Intermediate Certificate Authority that issued certificates with weak md5 keys (RSA 512 bits). We are confident that our Darkhotel threat actor fraudulently duplicated these certificates to sign its malware. These keys were not stolen. Many of the certificates were noted in a 2011 Fox-IT post "RSA-512 Certificates Abused in the Wild".

To further support this speculation please note the non-specific Microsoft Security Advisory below, the Mozilla advisory addressing the issue at the time, and the Entrust responses.

From Microsoft's security advisory from Thursday, November 10, 2011:

"Microsoft is aware that DigiCert Sdn. Bhd, a Malaysian subordinate certification authority (CA) under Entrust and GTE CyberTrust, has issued 22 certificates with weak 512 bit keys. These weak encryption keys, when broken, could allow an attacker to use the certificates fraudulently to spoof content, perform phishing attacks, or perform man-in-the-middle attacks against all Web browser users including users of Internet Explorer. While this is not a vulnerability in a Microsoft product, this issue affects all supported releases of Microsoft Windows.

There is no indication that any certificates were issued fraudulently. Instead, cryptographically weak keys have allowed some of the certificates to be duplicated and used in a fraudulent manner.

Microsoft is providing an update for all supported releases of Microsoft Windows that revokes the trust in DigiCert Sdn. Bhd. The update revokes the trust of the following two intermediate CA certificates: Digisign Server ID – (Enrich), issued by Entrust.net Certification Authority (2048) **Digisign Server ID (Enrich)**, issued by **GTE CyberTrust Global Root**"

From Mozilla's 2011 response:

"While there is n**o indication they were issued fraudulently, the weak keys have allowed the certificates to be compromised**. Furthermore, certificates from this CA contain several technical issues. They lack an EKU extension specifying their intended usage and they have been issued without revocation information."

From Entrust's response:

"There is no evidence that the Digicert Malaysia certificate authorities have been compromised."

Cracking the keys

Here are some notes on the costs and technical requirements of attacking these certificates.

The computing power required to crack and factor an RSA 512 bit key was $5000 and the period of time required was about 2 weeks. (see http://lukenotricks.blogspot.co.at/2010/03/rsa-512-factoring-service-two-weeks.html)

In October 2012, Tom Ritter reported that it would cost about $120-$150, perhaps even as little as $75.

Going even further back, there was much discussion about the technical methods of cracking these keys:
DJ Bernstein's 2001 paper on building a machine reducing the cost of integer factorization with Number Field Sieve techniques, breaking 1024 bit RSA keys.

RSA's reaction and 2002 statement on whether or not 1024 bit RSA keys are broken: "NIST offered a table of proposed key sizes for discussion at its key management workshop in November 2001 [7]. For data that needs to be protected no later than the year 2015, the table indicates that the RSA key size should be at least 1024 bits. For data that needs to be protected longer, the key size should be at least 2048 bits."

Other Tapaoux Certificates

Recent Tapaoux attacks and backdoors include malware signed with strong SHA1/RSA 2048 bit certificates, suggesting certificate theft.

CA Root	Subordinate CA/Issuer	Owner	Status	Valid From	Valid To
thawte	thawte Primary Root CA	Xuchang Hongguang Technology Co.,Ltd. sha1/RSA (2048bits)	Revoked	7/18/2013	7/16/2014
thawte	thawte Primary Root CA	Ningbo Gaoxinqu zhidian Electric Power Technology Co., Ltd. sha1/RSA (2048bits)	Revoked	11/5/2013	11/5/2014

Enhanced Keyloggers and Development

One of the most interesting components that we discovered as a part of this campaign was the use of a digitally-signed advanced keylogger. It is clean, well-written, kernel level malcode. The languages of its strings are a mix of English and Korean. It is signed with the familiar "belinda.jablonski@syniverse.com" digital certificate.

This keylogger is dropped by code running within svchost.exe on WinXP SP3, which maintains an interesting debug string:
d:\KerKey\KerKey(일반)\KerKey\release\KerKey.pdb

Note 일반 means "General" in Korean

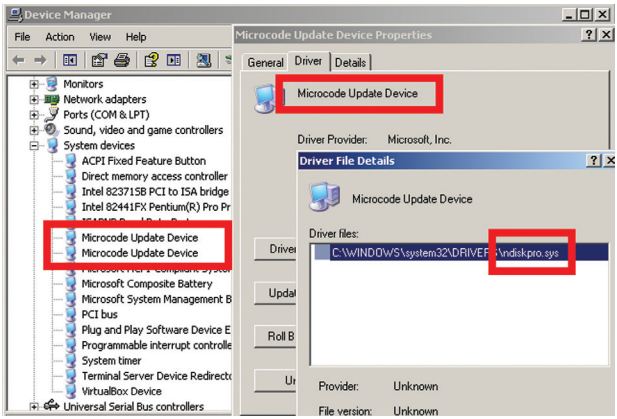
It probably was developed as a part of a mid-to-late 2009 project:
e:\project\2009\x\total_source\32bit\ndiskpro\src\ioman.c

Keylogger Code

This driver package is built to resemble a legitimate low-level Microsoft system device. It is installed as a system kernel driver "Ndiskpro" service, described as a "Microcode Update Device". It is slightly surprising that no rootkit functionality hides this service:

```
SERVICE_NAME: Ndiskpro
DISPLAY_NAME: Ndiskpro
        TYPE               : 1  KERNEL_DRIVER
        STATE              : 4  RUNNING
                                (STOPPABLE,NOT_PAUSABLE,IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0 ms
```

When loaded, the NDISKPRO.SYS driver hooks both INT 0x01 and INT 0xff, and retrieves keystroke data directly from port 0x60, the motherboard keyboard controller itself. It buffers, then communicates logged user data to the running user mode component. This component then encrypts and writes the retrieved values ondisk to a randomly named .tmp, file like ffffz07131101.tmp. This file is located in the same directory as the original dropper, which maintains persistence across reboots with a simple addition to the HKCU run key.



This keylogger module encrypts and stores gathered data in a log file, as mentioned previously. Its encryption algorithm is similar to RC4. The interesting part is that the module randomly generates the key and stores it in an unexpected place: in the middle of the log file name. Hence, the numeric part of the filename is used as a seed for the pseudorandom number generator. The rand function is statically linked to ensure same results on different computers.

Interesting Malware Components

The Darkhotel toolset consists of multiple components that have been slightly modified over time. These tools are dropped by hotel installers spoofing legitimate software installers, bound within torrent bundles, or dropped by exploits or hypertext linked from spear-phishing emails.

More advanced tools, like the keylogger decribed above, are later downloaded to the victim system by one of these implants. In a recent case, word docs embedded with 0-day flash swf files either dropped these backdoors or downloaded and executed backdoors from remote web servers. These tools pull down the keylogger, steal information from the system, or download other tools.

- small downloader
- information stealer
- Trojan
- dropper and self-injector
- selective infector

The most interesting behaviors of these components include

- highly unusual conditional 180 day command and control communications delay
- self-kill routines when the system default codepage is set to Korean
- enhanced Microsoft IntelliForm authentication theft handling
- infostealer module Internet Explorer, Firefox, and Chrome support
- campaign or stage ID maintenance
- virtual machine execution sensitivity
- selective viral infection routines to focus the spread of malware within organizations
- signed malcode (previously noted)

Small Downloader

This module is quite small (27Kb) and comes as a part of WinRar SFX file that drops and starts the module from %APPDATA%\Microsoft\Crypto\DES64v7\msieckc.exe. This module is designed to update malicious components through recurring checks at the C&C server. It is also capable of removing some older components, the names of which are hardcoded in the body of the malware. The module adds autorun registry settings to enable an automatic start during system boot.

One of the most interesting functions of this executable is its unusual delay and persistence. If a special file exists on the system, the module will not start calling back to C&C server until the special file is 180 days old. So, if some other critical malicious component was removed during this period, current module backs up and restores access to the system within 6 months.

The component gathers system information and sends it to the Darkhotel command and control servers as detailed in Appendix D.

Information Stealer

This module is relatively large (455Kb) and comes as a part of a WinRar SFX file that drops and starts the module from %APPDATA%\Microsoft\Display\DmaUp3.exe. The main purpose of the module is to collect various secrets stored on a local system and upload them to Darkhotel command and control servers:

- Cached passwords from Internet Explorer 6/7/8/9 (Windows Protected Storage)
- Mozilla Firefox stored secrets (<12.0)
- Chrome stored secrets
- Gmail Notifier credentials
- Intelliform-handled data and credentials:
  - Twitter
  - Facebook
  - Yandex
  - Qip
  - Nifty
  - Mail.ru
  - 126.com email
  - Zapak
  - Lavabit (encrypted email service now shut down)
  - Bigstring
  - Gmx
  - Sohu
  - Zoho
  - Sina
  - Care2
  - Mail.com

- Fastmail
- Inbox
- Gawab (middle-eastern email service)
- 163.com
- Lycos
- Lycos mail
- Aol login
- Yahoo! logins
- Yahoo! Japan logins
- Microsoft Live logins
- Google login credentials

This module is designed to terminate itself on Windows with the system default codepage set to Korean.

Trojan.Win32.Karba.e

This malware is 220Kb in size. It was built as MFC framework application with a lot of extra calls that should have complicated the analysis of the sample. It mimics a GUI desktop application but it does not create any visible windows or dialogs to interact with local users. The Trojan collects data about the system and anti-malware software installed on it, and uploads that data to Darkhotel command and control servers. More technical details are provided in Appendix D.

Trojan-Dropper & Injector (infected legitimate files)

This malware is 63kb in size. It is bound to a variety of other software packages that vary in name, but the host package is consistently detected as “Virus.Win32.Pioneer.dx”. It drops the igfxext.exe “selective infector” component to disk and runs it.

Selective Infector

This component is a **virus**, and is used to selectively infiltrate into other computers via USB or network shares.

First, the virus retrieves all available disks and starting from disk number 4 (D:\) to disk number 20 (Z:\), finds executable files and infects them. The code simply brute forces the list of mapped removable drives.

During its infection routine, the infector changes the entrypoint of executable files, creates an .rdat section, and inserts a small loader in the section, then puts its main payload in the overlay. Every infected file has functionality described in Trojan-Dropper & Injector section, so it can collect information about the computer, send it to the C2 and download other Darkhotel components as commanded. Observed downloaded components are signed with a familiar expired certificate from www.esupplychain.com.tw, issued by Cybertrust SureServer CA.

Again, further technical details are provided in Appendix D.

Campaign Codes

Almost every backdoor in this set maintains an internal campaign code or id, used in initial c2 communications as described above. Some IDs appear to be related to geographic interests, others do not seem obvious. We gathered a list of Darkhotel campaign IDs shown below. Internal IDs and c2 resources overlap across these components, there is no pattern of distribution according to connectback resources. The most common id is “DEXT87”:

DEXT87	NKstep2-auto
step2-auto	PANA(AMB)-auto
dome1-auto	PANA#MERA
step2-down	SOYA#2-auto
Java5.22	step2-down-u
C@RNUL-auto	(ULT)Q5SS@E.S-down
dome-down	VER1.5.1
M1Q84K3H	VICTORY
NKEX#V1.Q-auto	WINM#V1.Q

Infrastructure and Victims

This infrastructure team appears to employ a lesser skillset than top notch campaigns, maintaining weak server configurations with limited monitoring and defensive reactions, and making some simple mistakes. However, they are effective at maintaining a fully available infrastructure to support new and existing infections.

Overall, victims in our sinkhole logs and KSN data were found across the globe, with the majority in Japan, Taiwan, China, Russia, Korea and Hong Kong.

Sinkhole Domains

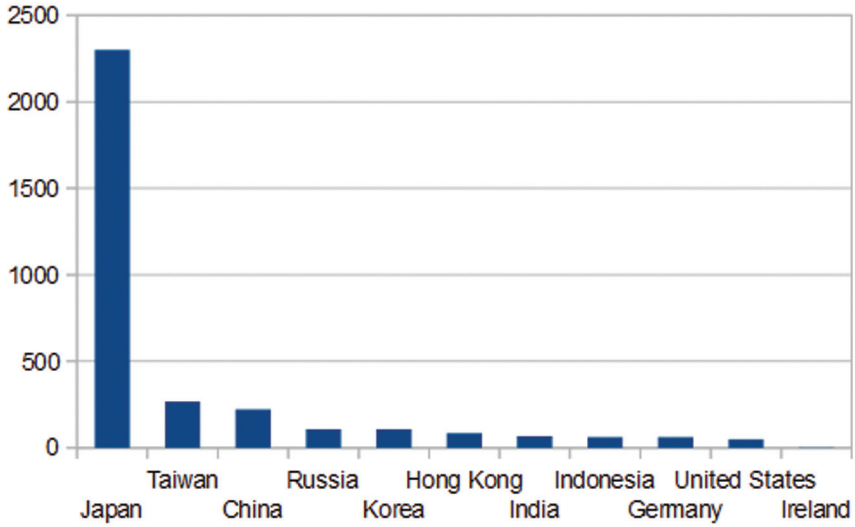
The following C&C domains have been sinkholed and redirected to the Kaspersky Sinkhole Server

42world.net
academyhouse.us
adobeplugs.net
amanity50.biz
autocashhh.hostmefree.org
autochecker.myftp.biz
autoshop.hostmefree.org
autoupdatfreeee.coolwwweb.com
checkingvirusscan.com
dailyissue.net
dailypatch-rnr2008.net
fenraw.northgeremy.info
generalemountina.com
goathoney.biz
jpnspts.biz
jpqueen.biz
mechanicalcomfort.net
micromacs.org
ncnbroadcasting.reportinside.net
neao.biz
private.neao.biz
reportinside.net
self-makeups.com
self-makingups.com
sourcecodecenter.org
support-forum.org
updatewifis.dyndns-wiki.com

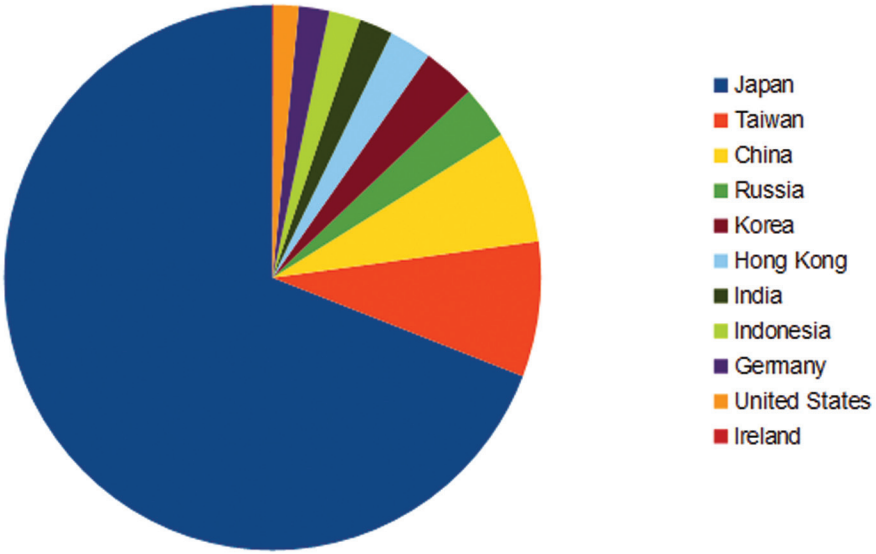
Victim Locations - KSN and Sinkhole Data

KSN Data

Our Kaspersky Security Network detected Darkhotel infections across thousands of machines, mostly related to the Darkhotel p2p campaigns. These geolocation estimates probably provide the most accurate picture of where Darkhotel activity is occurring.

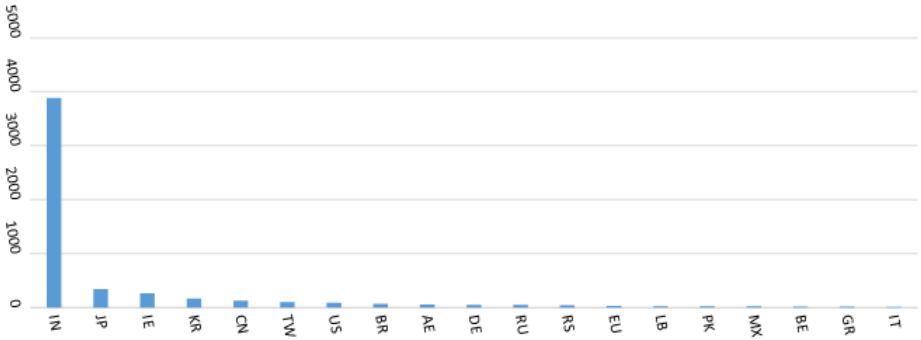


Here is a pie chart to better visualize the proportions of attack activity throughout the world. As you can see, over 90% of it occurs in the top five countries: Japan, followed by Taiwan, China, Russia and Korea.



Sinkhole Data

Because the operators very actively build up new command and control servers, it is difficult to sinkhole enough domains to get an accurate overall picture of victim system location based on this data. Also, many researcher systems are connected to the sinkholed domains. However, this graph of current sinkhole callbacks presents a low confidence distribution of victim geolocation, with India, Japan, Ireland, Korea, China and Taiwan in the top slots. Removing India and Ireland, the set more closely matches our KSN data.



Available ddrlog Victim Data

Many of these c2s maintain a common directory path that serves a ddrlog. The ddrlogs appear to maintain callback data that the attackers want to set aside in error logs. Many of the callback URLs have errors, many are from unwanted IP ranges, and others are clearly unwanted researcher sandbox system callbacks.

A description of the detailed connectback URL values and their xor/base64 encoding scheme is included in the “Interesting Malware Trojan.Win32.Karba.e” technical notes in Appendix D.

The Darkhotel c2 maintain these directory structures to store and serve ddrlog content:

- /bin/error/ddrlog
- /patch/error/ddrlog

The following structures appear to be common across servers, but do not produce ddrlog and do not maintain an /error/ directory:

- /u2/
- /u3/
- /patch2/
- /major/
- inor/
- /asp/
- /update3/

Two ddrlog files report entries starting January 1, 2009 at 9:16 a.m.

- autozone.000space.com
- genuinsman.phpnet.us

All of the logs maintain a significant number of entries, almost 50,000, with a simple stamp “B” or “L”. Those records are formatted in the following manner:

```
2009.01.01 09:16:00 150.70.xxx.xx --> B
2009.01.01 09:16:33 150.70.xxx.xx --> B
2009.01.01 09:14:52 220.108.x.xxx --> L
2009.01.01 09:16:04 112.70.xx.xx --> L
```

Only 120 IP addresses perform the “B” checkin, and 90% of these are from the range 150.70.97.x. This entire range is owned by Trend Micro in Tokyo, JP.

A handful of the remaining addresses, like 222.150.70.228, appear to come from other ranges owned by Trend Micro in JP. One outlier comes from an El Salvadoran ISP, and another is connected to a Japanese ISP. Approximately 20,000 IP addresses perform the “L” checkin.

Other ddrlogs may include “A” tags as well.

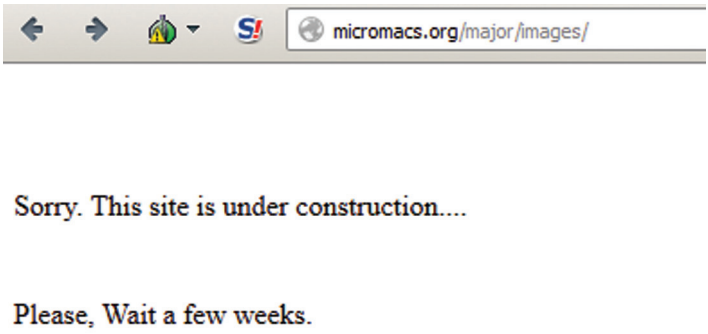
The “A” tag labels unwanted checkins from untargeted locations, like Hungary and Italy. The “B” tag labels unwanted checkins from Trend Micro IP ranges.

The “L” tag labels unwanted checkins from a variety of ranges, but includes odd IP like the loopback address, 127.0.0.1, clearly an error.

Entries in these logs include callback URLs that have spaces and unusual characters that do not conform to the required base64 character dictionary.

C2 Communications and Structure

Typical main page:



For begatrendstone.com, we have the following directory structure:

/bin
    -read_i.php (main C&C script)
    -login.php (unknown, replies “Wrong ID()”)
/bin/error (error logs stored here)
    -ddrlog
/bin/tmp
 /bin/SElhxxwiN3pxxiAPxxc9
    -all.gif
    /i
    - encrypted stolen victim system content
    /L
    /f

For auto2116.phpnet.us, we have the following directory structure:

/patch
    -chkupdate.php (main command and control script)
/patch/error
    -ddrlog

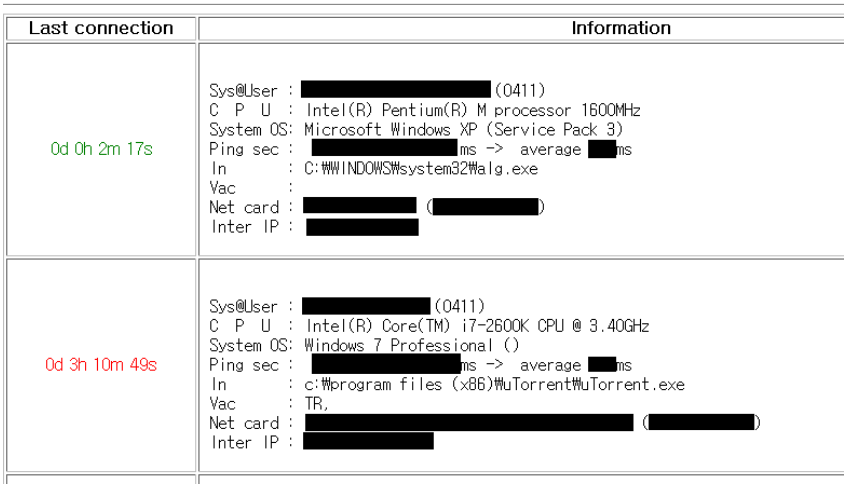
The group encrypts victim data on their servers with single user/passkey combinations across multiple victims. When an unauthorized user attempts to access a Darkhotel web interface for victim management without the correct passkey, the html page and table layout renders properly, but all the data values on the page are returned as garbled ciphertext.

Victim Management

New victim systems appear to be systematically vetted. The attackers maintain a web interface to vet these new victim systems. The attackers first and foremost list and sort victim systems according to their latest c2 check-in. Collected data probably is presented in order of importance:

1. user's logon name
2. system CPU and OS
3. "Ping sec", or how far the victim system is from the c2
4. "In", or the process that the attackers' dll code executes within
5. Vac: Antivirus Product identifier
6. system LAN IP
7. network WAN IP

Here is an example of one of these web pages:



Last connection	Information
0d 0h 2m 17s	Sys@User : [redacted] (0411) C P U : Intel(R) Pentium(R) M processor 1600MHz System OS: Microsoft Windows XP (Service Pack 3) Ping sec : [redacted]ms -> average [redacted]ms In : C:₩WINDOWS₩system32₩alg.exe Vac : Net card : [redacted] ([redacted]) Inter IP : [redacted]
0d 3h 10m 49s	Sys@User : [redacted] (0411) C P U : Intel(R) Core(TM) i7-2600K CPU @ 3.40GHz System OS: Windows 7 Professional () Ping sec : [redacted]ms -> average [redacted]ms In : c:₩program files (x86)₩uTorrent₩uTorrent.exe Vac : TR, Net card : [redacted] ([redacted]) Inter IP : [redacted]

Researcher Activity

Clearly, some automated analysis activity involving researchers' sandbox tools are filling up these logs. From June 2013 to April 2014 (approximately an 11 month period), in only 15 ddrlog files, we observe almost 7,000 connections from research sandbox systems. The network connections provide a1= through a3= values identifying a QEMU based sandbox, all sourced from only 485 WAN IP addresses. Under 30 lan IPs are recorded, all in the same 172.16.2.14-126 range. This system(s) uses a "Dave" user account and "HOME-OFF-D5F0AC" Windows system name.

These characteristics correspond with network activity generated by GFI Software's "CWsandbox" tools, now owned by "ThreatTrack Security".

Conclusions

For the past seven years, a strong threat actor named Darkhotel, also known as Tapaoux, has carried out a number of successful attacks against a wide range of victims from around the world. It employs methods and techniques which go well beyond typical cybercriminal behavior.

The Darkhotel crew's skillset allows it to launch interesting cryptographical attacks, for instance factoring 512 bit RSA keys. Its use of 0-days is another indicator of a strong threat actor.

The targeting of top executives from various large companies around the world during their stay at certain "Dark Hotels" is one of the most interesting aspects of this operation. The exact method of targeting is still unknown - for instance, why some people are targeted while others are not. The fact that most of the time the victims are top executives indicates the attackers have knowledge of their victims whereabouts, including name and place of stay. This paints a dark, dangerous web in which unsuspecting travelers can easily fall. While the exact reason why some hotels function as an attacker vector are unknown, certain suspicions exist, indicating possibly a much larger compromise. We are still investigating this aspect of the operation and will publish more information in the future.

A further interesting trait is the deployment of multiple types of campaigns, both targeted and botnet. This is becoming more and more common on the APT scene, where targeted attacks are used to compromise high profile victims and botnet style operations are used for massive surveillance or performing other tasks such as launching DDoS attacks on hostile parties or simply upgrading victims to more sophisticated espionage tools.

We expect the Darkhotel crew to continue their activities against DIB, Government and NGO sectors. The appendix released with this paper provides technical indicators of compromise which should help victims identify the malicious traffic and enable targets to protect themselves better against attack.

Kaspersky Lab HQ

39A/3 Leningradskoe Shosse
Moscow, 125212
Russian Federation

more contact details

Tel: +7-495-797-8700
Fax: +7-495-797-8709

E-mail: info@kaspersky.com
Website: www.kaspersky.com