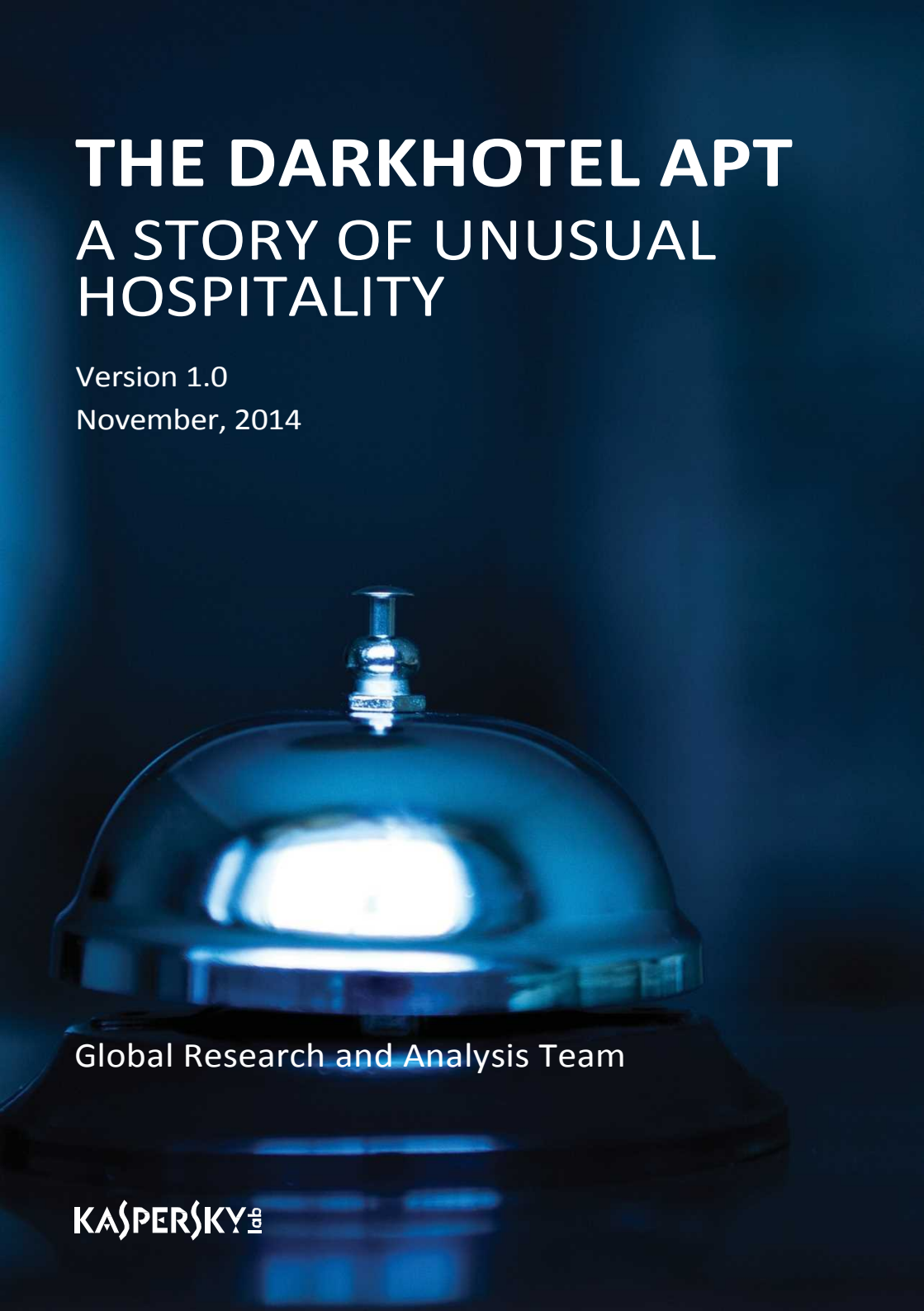
# THE DARKHOTEL APT

## A STORY OF UNUSUAL HOSPITALITY

Version 1.0

November, 2014



Global Research and Analysis Team

KASPERSKY lab

# 目次

# エグゼクティブサマリー

Darkhotelの標的型攻撃は、一見すると一貫性のない矛盾した特性を持つ攻撃で、高度な部分もあれば未熟な面もあります。10年近くも前から活動を続けており、Darkhotel攻撃者は今もなお活動中です。この攻撃者の活動は、特定のホテルやビジネスセンターのWi-Fiおよび有線接続に限定されています。また、一部はP2Pやファイル共有ネットワークにもつながっており、標的型攻撃メールを利用した攻撃を実行することも確認されています。Darkhotelのツールはいろいろありますが、「Tapaoux」「pioneer」「Karba」「Nemim」などの名前で検出されます。Darkhotelの攻撃には、以下のような特徴があります。

- 信頼できるグローバルスケールの商用ネットワークリソースに、何年間も戦略的な精度でアクセスし、侵入や悪用を果たしている運用の技能
- 高度な数学と暗号分析による攻撃機能を備え、認証局や PKIにまで拡大される信頼が損なわれることをいとわない
- 信頼できるリソースと信頼できないリソースを介して、地域は限定するが無差別にシステムに感染し、大規模なボットネットを構築、運用する
- 効果的かつ持続的なツールセットに組み込まれた巧妙な低水準のキーロガー
- 活動を通じ、一貫して特定の被害者カテゴリに特化し、それにタグ付けをする
- Apache Webサーバー、動的DNSレコード、暗号ライブラリ、PHP Webページで構成される大規模な動的インフラストラクチャ
- 日常的なゼロデイアクセス - Adobe Flashのゼロデイを利用するフィッシング攻撃が最近実行され、また頻度は低いながらその他のゼロデイリソースも、数年間に及ぶ大規模な攻撃活動の継続に利用されている

# はじめに

無防備な宿泊客がホテルでインターネットに接続しようすると、有名なソフトウェア（GoogleToolbar、Adobe flash、Windows Messenger など）のリリースに見せかけたトロイの木馬に感染することがあります。企業幹部やハイテクに強い起業家も例外ではありません。
マルウェアの最初の段階で、標的を確認することができ、重要な標的に対してはより高度なツールがダウンロードされ、実行されます。

ホテルでインストールされるマルウェアは、標的とする個人を特定して配信されており、Darkhotelの攻撃者グループは、その個人が宿泊先の一流ホテルに滞在する日時をあらかじめ把握しているようです。攻撃者は狙った宿泊客がチェックインしてインターネットに接続するのを待ち伏せています。

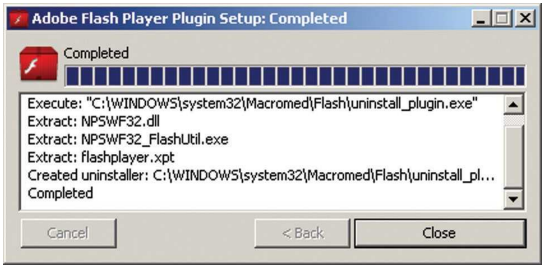
FBIは、ホテルで発生する同様の事案について注意勧告しており、オーストラリア政府からも、感染を確認したという類似の声明がありました。FBIは、海外のホテルにおいて宿泊客に対する攻撃が出現したのは 2012年5月だと発表していますが、収集したDarkhotelに関連する検体はそれより以前の 2007年にはすでに出回っていました。また、Darkhotelの攻撃者のサーバー内のログデータを分析したところ、2009年1月1日から継続して攻撃されていたという記録が残っていました。しかも、広く拡散しているマルウェアやゼロデイのスピアフィッシング攻撃をP2Pネットワークに広げていることから、Darkhotel APTは実行性のあるツールセットを保持したまま、宿泊客に対する歓迎を装って長期的に活動を続けていることが判明しています。

# 分析

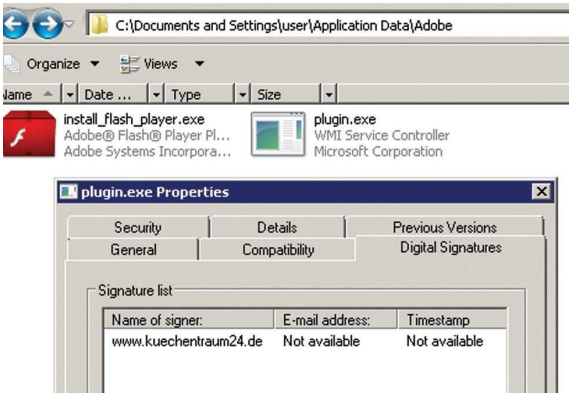
## 配信 - ホテルやビジネスセンター、無差別な拡散

### ホテルとビジネスセンターでの拡散

Darkhotel APTマルウェアの感染は、いくつかのホテルで、宿泊客がホテルのWi-Fiに接続すると、有名なソフトウェアパッケージのアップデートをインストールするよう求められる方法でした。




これらのパッケージは、実際にはバックドアを含むインストーラです。しかも、AdobeやGoogleの正規のインストーラに追加される形で感染しており、デジタル署名された Darkhotelのバックドアが、正規のパッケージと同時にインストールされ、感染します。




この感染手法で特に興味深い点は、Darkhotelのパッケージのインストール画面は特定の宿泊客に対してしか表示されない点です。宿泊客がホテルでインターネットを利用する際は、姓と部屋番号を使用してログインするのが一般的ですが、攻撃者側で標的を絞っている可能性が高いということです。例えば、同じホテルでカスペルスキーのハニーポット調査システムを動かしてもDarkhotelの攻撃を受けませんでした。このデータだけでは断定はできませんが、状況証拠から宿泊情報が攻撃に悪用されていた可能性が高いと言えるでしょう。

## ネットワークインフラストラクチャの悪用

Darkhotelの攻撃者は、ホテルのネットワークシステムに侵入する手段を確保しており、ホテルの宿泊者に対する攻撃を何年にもわたって繰り返していました。攻撃者は、攻撃を行う際に一流ホテルの宿泊者についてチェックイン/チェックアウト情報や身元情報を参照し、その情報を攻撃に利用している可能性が高いといえます。

継続的な調査の過程で、ホテルのログインページにiframeが埋め込まれていることも判明しました。このiframeによって、宿泊者がWebブラウザを使用してインターネットに接続しようとした際に、ソフトウェアの更新パッケージに偽装したマルウェアへと誘導されてしまうのです。攻撃者は、きわめて慎重にこのiframeや誘導先にマルウェアを設置しています。また、攻撃の成功時にこれらのツールの痕跡を完全に削除するという周到さも見せていました。現在、侵入経路はすでに調査と修正処理が完了しており、さらに今回の侵入経路に対する防衛処置が施されています。被害のあったホテルのネットワーク上で、カスペルスキーがこれらのインシデントの痕跡を確認したのは、2013年の終わりから2014年の初めにかけてでした。攻撃者は、こうした環境を整えたうえで、標的を絞り個人レベルで正確に攻撃しています。標的となっている宿泊者のホテルの滞在期間が終わると攻撃者は配置していたiframeとバックドアを含むマルウェアをホテルのネットワークから削除します。以前、別のホテルでも同様の攻撃を行っていましたが、その際にも痕跡を抹消しており、攻撃の手口は変わっていないと言えます。同じ活動に関する外部のレポートからも、同様に周到な活動を裏付けるデータが見つかっています。

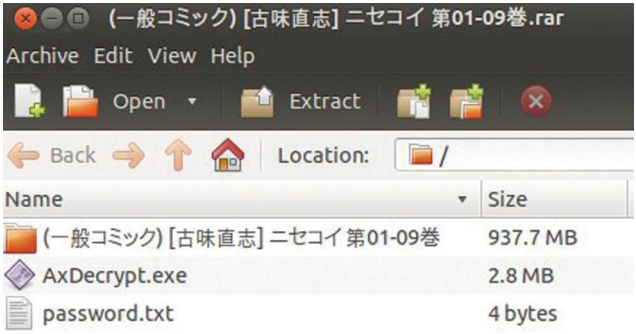
今回の攻撃の手口に関して、一般的なAPT攻撃にはある境界線が明確ではありません。きわめて不正確な「水飲み場型攻撃」すなわち「戦略的な Web侵害」とも、精度の高いスピアフィッシング型攻撃とも考えられます。Darkhotelの攻撃者は、被害者がホテルのWi-Fiまたは客室にある有線LANを使ってインターネットに接続するのを待ち伏せており、被害者がいずれかの方法で接続する確率は非常に高く、攻撃者はその確率に依存しているので、その点は水飲み場型攻撃に似ています。その一方、攻撃者は被害者のかなり正確な宿泊情報を入手しており、その上で標的とし選定しています。その点では、標的のメールアドレスや興味まで把握した上での標的型攻撃メールとも似ています。攻撃を準備する時点で、Darkhotelの攻撃者は標的の到着予定時刻や出発時刻、部屋番号、姓名といったデータまで知っているのです。こうしたデータを悪用して、攻撃者は悪意のあるiframe を用いて宿泊者の中から標的を厳選し、正確に攻撃を行うのです。以上のことから、この攻撃者については新たに独自の特徴が浮かび上がります。対象を広く特定し、きわめて正確に攻撃するアプローチという特徴です。

## 無差別な拡散

Darkhotel APTがマルウェアを無差別に拡散している一例として、日本のP2P共有サイトにおける拡散の状況を見れば明らかです。マルウェアはサイズの大きい（約 900MB）RARアーカイブとして配布されているほか、bittorrentを介しても拡散されています。Darkhotelは、この手法を用いて「Karba」というトロイの木馬を拡散します。日本語から中国語に翻訳されているこれらのアーカイブは、マンガやアニメから抜粋されており、潜在的に標的の興味を引く内容に設定されていると考えられます。

以下に示す Darkhotelパッケージは、6か月足らずの間に 30,000回以上もダウンロードされています。マルウェア が仕掛けられているこのP2P bittorrentファイルは、2013年11月22日に投稿され、2014年に入ってからも継続して拡散されていました。

(一般コミック) [古味直志] ニセコイ 第0109巻.rar




この900MB近いRARアーカイブを解凍すると、暗号化されたZIPファイルが収納されたディレクトリ、復号化ツールと思われる実行ファイル、更に復号化に必要なパスワードを示したテキストファイルが展開されます。復号化ツールのように見える AxDecrypt.exeファイルには、本物の復号化ツールだけでなく、「Karba」というトロイの木馬であるDarkhotel Catch.exeを感染させる為のマルウェアも展開され、実行されます。ユーザーが このtorrentファイルをダウンロードして、復号化ツールを実行すると、その裏でトロイの木馬がインストールされ、感染します。

Catch.exe（Backdoor.Win32.Agent.dgrn として検出されます）は、以下のDarkhotelのC&Cサーバーと通信します。

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

torrentファイルに含まれるDarkhotelバックドアは、アダルトアニメや漫画などの例も確認されています。以下のようなtorrentファイルが、何万回もダウンロードされています。

“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] “

“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”)

このような Darkhotelバックドアは、さまざまなマンガのタイトルで配布されており、多くのマンガやアニメ作品が利用されています。関連するDarkhotelのC&Cサーバーのドメインは、次のとおりです。

| |
|---|
| microblo5.mooo.com<br>microyours.ignorelist.com<br>micronames.jumpingcrab.com<br>microchisk.mooo.com<br>microalba.serveftp.com |

## Darkhotelのスピアフィッシング攻撃活動

Darkhotelの攻撃活動のうち、典型的な標的型攻撃メールである「Tapaoux」は過去 5 年間に断続的に出現しました。こうした、いわばサブプロジェクト的な試みは防衛産業基盤（DIB）や政府、NGO組織を標的としており、原子力エネルギーや武器性能といったトピックを扱う内容のメールをエサとして使用しています。NGO組織と政府の政策決定機関に対する攻撃の解説が contagio に投稿されました。この標的型攻撃メールは、2014年に入っても続いています。この攻撃は典型的な標的型攻撃メール攻撃のプロセスを踏んでおり、過去数か月には hxxp://offi-revision.com/update/fite.exe または、hxxp://tradeinf.com/mt/ duspr.exe などの Webサーバーからシステムで取得されるダウンローダの実行可能ファイルが悪用されました。

過去数年間、このグループから標的型攻撃メールが送信されており、そのメールにはInternet Explorerのゼロデイが悪用されていました。また、添付ファイルとしてAdobeのゼロデイが含まれている場合もあります。

## 最近のゼロデイ攻撃

Darkhotelの攻撃者は、ゼロデイエクスプロイトを展開することがありますが、必要に応じてそれを削除します。過去数年の間に、Adobe製品とMicrosoft Internet Explorerのゼロデイがそれぞれ標的型攻撃メールとして使用され、その中にはCVE-2010-0188も含まれていました。2014年の前半にカスペルスキーのリサーチャーは、CVE-2014-0497が使用されていることについて報告し、2月の初めには公式ブログSecurelist上でFlashの脆弱性について発表しています。

攻撃者は、中国のISPを通じてインターネットに接続しているシステムを標的としてスピアフィッシングを仕掛け、ゼロデイエクスプロイトの中で、強化されたWindows 8.1システムを操作する機能を開発しました。興味深いのは、「list of the latest Japanese AV wind and how to use torrents.docx」という名前の韓国語の文書にFlashオブジェクトが埋め込まれている点です。Flashオブジェクト内に含まれているダウンローダ（d8137ded710d83e2339a97ee78494c34）は、以下にまとめた「情報窃取ツール」コンポーネントと似た不正な機能があります。（詳細は「Indicators of Compromise」Appendix D参照）

## デジタル証明書と認証局の信頼取り消し

Darkhotelの攻撃者は通常、何らかのデジタル証明書を使用してバックドアに署名しています。しかし、攻撃者が選んだオリジナルの証明書は、暗号鍵が脆弱であり、攻撃者によって悪用されている可能性がありました。Darkhotelの一般的に使用されている不正コードに署名した証明書のリストを以下に示します。現時点で、これらの鍵を因数分解するには高度な数学的機能が必要です。攻撃者グループが利用している証明書は、これだけではありません。ごく最近の活動から窃取した証明書を使用してコードに署名していることも確認されています。

| 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.m y 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 CA1 | Equifax Secure eBusiness CA1 | 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 | dlaitmiddleware@anthem.com sha1/RSA (512 bits) | invalid Sig | 4/22/2009 | 4/22/2010 |
| GTE CyberTrust | Cybertrust Educational CA | adidmapp.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<br>sha1/RSA (512 bits) | invalid Sig | 2/17/2009 | 2/17/2011 |

署名されたDarkhotelマルウェアはいずれも、同じルート認証局を共有しており、弱いMD5鍵（RSA 512 ビット）で証明書を発行した中間認証局も共通しています。Darkhotelの攻撃者が、これらの証明書を不正に複製してマルウェアに署名していることは間違いありません。ただし、鍵は盗まれたのではありませんでした。証明書の多くは、2011年のFoxITの投稿「RSA512 Certificates Abused in the Wild」で指摘されていました。

この推測をさらに裏づけるために、以下の一般的なMicrosoft Security Advisoryと、当時の問題に対処したMozillaの勧告、およびEntrustの対応も参照してください。

Microsoftによる2011年11月10日木曜日のセキュリティアドバイザリより:

「Microsoftは、マレーシアの下位認証局（CA）である、EntrustおよびGTE CyberTrust傘下のDigiCert Sdn. Bhdが、512ビットの脆弱な鍵で22件の証明書を発行していたことを確認しました。この脆弱な暗号鍵が破られた場合、攻撃者が証明書を悪用してコンテンツを偽装し、フィッシング攻撃を実行したり、Internet Explorerを含めたすべてのWebブラウザユーザーに対して中間者攻撃を実行したりする可能性があります。Microsoft製品の脆弱性ではありませんが、この問題はサポート対象であるすべてのMicrosoft製品に影響します。

どの証明書も不正に発行された兆候はありません。むしろ、暗号鍵に脆弱性があるために、証明書の一部が複製され、不正に利用されているようです。

Microsoftは、サポート対象の全リリースのMicrosoft Windowsについて、DigiCert Sdn. Bhdでの信頼を取り消すアップデートを提供しています。このアップデートを実行すると、Entrust.net 認証局発行（2048）のDigisign Server iD（Enrich）と、GTE CyberTrust Global Root発行のDigisign Server ID（Enrich）の2つの中間CA証明書の信頼が取り消されます。

Mozillaの2011年の対応より:

「不正に発行された兆候はありませんが、鍵が脆弱なために、証明書が危険な状態になっています。また、このCAからの証明書には複数の技術的な問題もあります。すなわち、本来の用途を示すEKU拡張がないことと、失効情報を持たずに発行されていることです」

Entrustの対応より:

「マレーシアDigicertの認証局が侵入を受けた証拠はありません」

## 暗号鍵のクラッキング

こうした証明書に対して攻撃を実行するコストと技術要件を紹介しておきましょう。

512ビットRSA暗号鍵のクラッキングと因数分解に必要な計算処理能力は 5,000ドルで、所要時間は約2週間でした（http://lukenotricks.blogspot.co.at/2010/03/rsa512factoringservicetwoweeks.htmlを参照）。

2012年10月に Tom Ritterが報告した試算によると、そのコストは120～150ドル、おそらくは75ドル足らずだということです。

さらにさかのぼると、暗号鍵のクラッキングに関する技術的な手法についても盛んに議論されていました。
数体ふるい法による整数因数分解でコストを削減したマシンを作成し、1024ビットのRSA鍵を破る方法に関する、DJ Bernsteinの2001年の論文。

1024ビットRAR鍵は破れるかどうかに関する、RASの回答の2002 年の声明:「NISTは2011年11月の鍵管理ワークショップで、暗号鍵のサイズに関する提案を話し合う場を設けました[7]。2015年まで保護が必要なデータについてはRSA鍵のサイズを1024ビット以上にするよう提案します。それより長く保護が必要なデータについては2048ビット以上を推奨します」

## その他のTapaoux証明書

Tapaouxによる最近の攻撃とバックドアでは、強力な2048ビットSHA1/RSA 暗号鍵で署名されたマルウェアも出現しており、証明書の窃取が疑われています。

| 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 |

## 強化されたキーロガーと開発

Darkhotelの攻撃活動で見つかったコンポーネントの中でも最も興味深いのは、デジタル署名された高度なキーロガーが使われていることです。これは適切な記述で異常のないカーネルレベルの不正コードです。文字列に使用されている言語は英語と韓国語が混在しており、署名には「belinda.jablonski@syniverse.com」という見慣れたデジタル証明書が使われています。

このキーロガーは、Windows XP SP3のsvchost.exe内で実行されるコードによってドロップされます。不正コード内には非常に重要なデバッグ用の文字列が含まれていました。
d:\KerKey\KerKey(일반)\KerKey\release\KerKey.pdb
「일반」は「一般」を表す韓国語です。

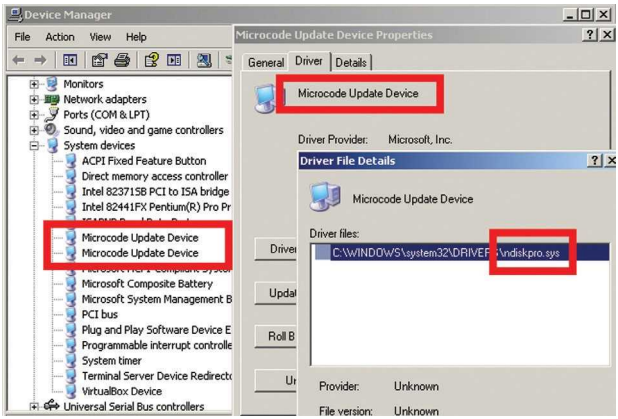
e:\project\2009\x\total_source\32bit\ndiskpro\src\ioman.cというパスから考えて、これは 2009年の中頃から後半のプロジェクトで開発されたようです。

## キーロガーのコード

このドライバパッケージは、正規のMicrosoftシステムデバイスを模倣するために作成されます。システムカーネルドライバのNdiskproサービスとしてインストールされ、「Microcode Update Device」という名前で表されます。このサービスを隠蔽するツールキット機能がないのは、いささか意外です。

```
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
```

ロードされると、NDISKPRO.SYSドライバはINT 0x01とINT 0xffを両方フックし、ポート0x60から直接キーストロークのデータを取得します。これは、マザーボードのキーボードコントローラそのものです。ドライバはログに記録されたユーザーデータをバッファし、実行中のユーザーモードコンポーネントに送信します。そして、取得した値を暗号化し、ランダムな名前のtmpファイル、たとえばffffz07131101.tmpとしてディスク上に書き込みます。このファイルは、元のドロッパーと同じディレクトリに設定されます。、また、レジストリーのキーに自身を追加することでWindowsのスタートアップとして登録することで再起動した際でも感染を維持します。




前述したように、キーロガーモジュールは収集したデータを暗号化してログファイルとして保存します。このときの暗号化アルゴリズムは、RC4と似ています。注目すべき点は、このモジュールがランダムに鍵を生成し、ログファイル名の中という予想外の場所にそれを格納することです。そのため、ファイル名のうち数字部分が擬似乱数を生成するための鍵データとして使用されます。異なるコンピューター上でも同じ結果が生成されるように、rand関数は静的にリンクされています。

# 重要なマルウェアコンポーネント

Darkhotelツールセットは複数のコンポーネントで構成されており、それが時間とともに少しずつ改変されています。これらのツールは、ホテルのネットワーク上で正規のソフトウェアインストーラに偽装し配布されていたドロッパーによって感染するか、torrentファイルの復号化ツールにバンドルされて、標的型攻撃メールのハイパーテキストリンクもしくは添付されているゼロデイによって感染します。

前述したキーロガーのような高度なツールは、これらのトロイの木馬によって後から被害システムにダウンロードされます。最近のケースでは、ゼロデイ脆弱性のあるFlashファイルを埋め込まれたWord文書が、バックドアを投下するか、リモートWebサーバーからバックドアをダウンロードして実行するものがありました。これらのツールがキーロガーをダウンロードし、システムから情報を窃取したり、他のツールをダウンロードしたりします。

- 小さいダウンローダ
- 情報窃取ツール
- トロイの木馬
- ドロッパーとセルフインジェクタ
- 選択的な感染ツール

これらのコンポーネントで特に需要な動作は、次のとおりです。

- きわめて特殊な条件下で、C&C通信が180日遅延する
- システムのデフォルトのコードページが韓国語に設定されている場合の自己停止ルーチン
- 強化されたMicrosoft Intelliform認証の盗難処理
- infostealerモジュールがInternet Explorer、Firefox、Chromeに対応
- 攻撃活動またはステージIDを維持
- 仮想マシン実行の感度
- マルウェアの拡散を組織内に集中させる選択的なウイルス感染ルーチン
- 署名された不正コード（前述）

## 小さいダウンローダ

このモジュールはサイズがきわめて小さく（24KB）、%AppDATA%\Microsoft\Crypto\DES64v7\msieckc.exeからモジュールをドロップして起動させるWinRar SFXファイルの一部です。このモジュールは、C&C サーバーで反復チェックを通じて悪意のあるコンポーネントを更新するほか、マルウェア本体に名前がハードコードされている古いコンポーネントを削除する機能も持っています。また、レジストリーの値を改竄し、システム起動時に自動起動できるようになります。

この実行可能ファイルで特に興味深いのは、異常な潜伏能力です。システムにある特別なファイルが存在すると、このモジュールはその特別ファイルが180日経過するまでC&C サーバーとの通信を開始しなくなります。したがって、その間に他の重要な不正コンポーネントが削除された場合は、現在のモジュールが6か月以内のシステムへのアクセスをバックアップしてリストアします。

このコンポーネントはシステム情報を収集し、それをDarkhotelのC&Cサーバーに送信します。(詳細は「Indicators of Compromise」Appendix D参照)

## 情報窃取ツール

このモジュールはサイズがきわめて小さく(24KB)、%AppDATA%\Microsoft\Crypto\DES64v7\msieckc.exeからモジュールを投下して起動させるWinRar SFXファイルの一部です。このモジュールの主な目的は、ローカルシステムに保存されている各種の機密情報を収集し、DarkhotelのC&Cサーバーにアップロードすることです。

- Internet Explorer 6、7、8、9 からキャッシュされたパスワード(Windows Protected Storage)
- Mozilla Firefoxに保存されている秘密情報(12.0 未満)
- Chromeに保存されている秘密情報
- Gmail Notifierの認証情報
- Intelliformで処理されるデータと以下の認証情報:
  - Twitter
  - facebook
  - yandex
  - Qip
  - Nifty
  - Mail.ru
  - 126.com email
  - Zapak
  - lavabit (暗号化されたメールサービスをシャットダウン)
  - Bigstring
  - Gmx
  - Sohu
  - Zoho
  - Sina
  - Care2
  - Mail.com

- fastmail
- inbox
- Gawab (中東のメールサービス)
- 163.com
- lycos
- lycos mail
- Aol login
- yahoo! logins
- yahoo! Japan logins
- Microsoft live logins
- Google login credentials

このモジュールは、システムのデフォルトのコードページが韓国語に設定されており、 Windows上で自分自身を停止することができるように設計されています。

### Trojan.Win32.Karba.e

このマルウェアのサイズは220KBです。MFCフレームワークのアプリケーションとして作成され、多くの外部呼び出しを実行するため、サンプルの解析が難しくなっています。GUIデスクトップアプリケーションを模倣しますが、可視のウィンドウやダイアログを生成してローカルユーザーと対話することはありません。Trojan.Win32.Karba.eは、システムとそこにインストールされているアンチマルウェアソフトウェアに関するデータを収集し、そのデータを DarkhotelのC&Cサーバーにアップロードします。（詳細は「Indicators of Compromise」Appendix D参照）

## トロイの木馬型のドロッパーとインジェクタ（正規のファイルに感染）

このマルウェアのサイズは63KBです。名前の異なる他のさまざまなソフトウェアパッケージにバインドされていますが、ホストパッケージは常に「Virus.Win32. pioneer.dx」という名前で検出されます。「選択的な感染ツール」コンポーネントであるigfxext.exeをディスクに投下し、実行します。

## 選択的な感染ツール

このコンポーネントはウイルスであり、USBまたはネットワーク共有を介して他のコンピューターに選択的に感染します。

このウイルスはまず、ディスク番号 4（D:\）からディスク番号 20（Z:\）までの間で使用可能なディスクをすべて見つけ出し、実行可能ファイルを検索してそれに感染します。コードは、マップされているリムーバブルドライブのリストを総当たりで検索するだけです。

その感染ルーチンで、感染ツールは実行可能ファイルのエントリポイントを変更してrdatセクションを作成し、そのセクションに小さいローダを挿入してから、メインのペイロードをオーバーレイに配置します。感染したファイルのそれぞれが、「トロイの木馬型のドロッパーとインジェクタ」の項で説明した機能を持っているため、コンピューターに関する情報を収集し、それをC&Cサーバーに送信して、コマンドに従ってDarkhotelの他のコンポーネントをダウンロードすることができます。ダウンロードが確認されているコンポーネントは、Cybertrust SureServer CAによって発行されるwww.esupplychain.com.twからの証明書で署名されていますが、この証明書は失効しています。

これについても、技術的な詳細は「Indicators of Compromise」Appendix Dを参照してください。

## 攻撃活動コード

このマルウェアのバックドアはほぼすべて、内部の攻撃活動コードすなわちIDを保持しており、それが前述した最初のC&Cサーバーとの通信に使用されます。一部のIDは、地理的な情報と関連しているようですが、他のIDについては不明です。Darkhotelの攻撃で確認されたIDのリストを以下に示します。これらのコンポーネントでは内部IDとC&Cリソースが重複しており、コネクトバックリソースに応じた分布のパターンはありません。ほとんどのIDは「DEXT87」です。

| | |
|---|---|
| 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 |

## インフラストラクチャと被害者

Darkhotelのインフラストラクチャチームは、攻撃活動と比べるとそれほど高度なスキルは持ち合わせていないようです。管理されているサーバーの設定は脆弱であり、監視や防御対応も限られており、単純なミスさえ見られます。とは言え、完全に利用可能なインフラストラクチャを保持し、既存の感染と新たな感染に対応するという点では実行性の高い機能を備えています。

全体的に、カスペルスキーのシンクホールログとKaspersky Security Network（KSN）のデータでは全世界に分布が見られますが、大多数は日本、台湾、中国、ロシア、韓国、香港に集中しています。

## シンクホールのドメイン

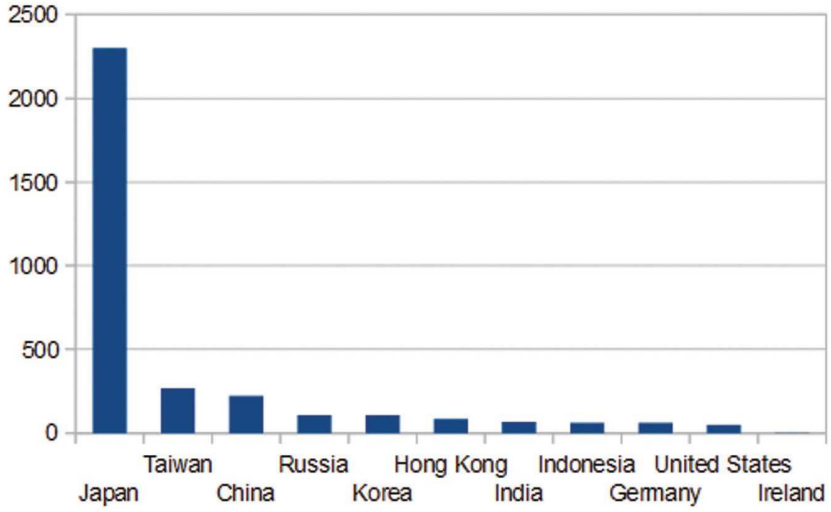
シンクホールで捕捉され、カスペルスキーのシンクホールサーバーにリダイレクトされたC&Cドメインは、以下のとおりです。

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
supportforum.org
updatewifis.dyndns-wiki.com

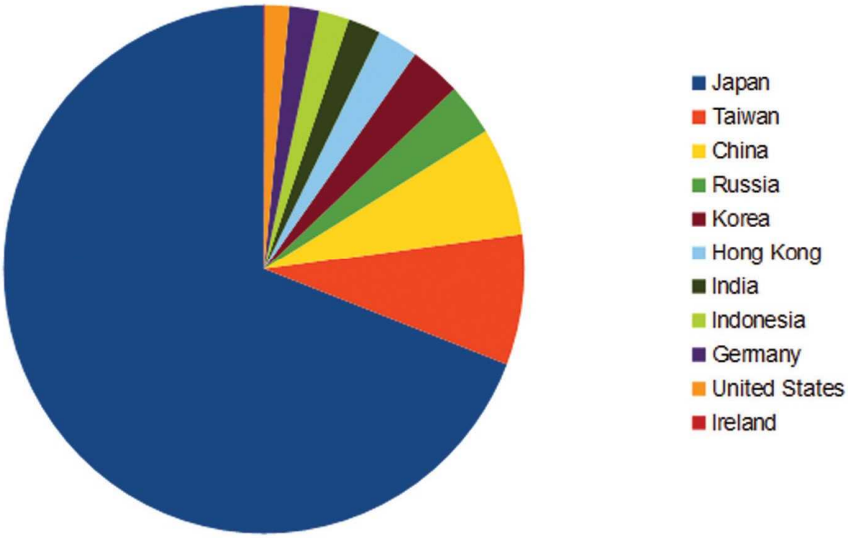
## 被害者の地理的な分布 - KSNおよびシンクホールのデータから

### KSNデータ

Kaspersky Security Network（KSN）は、数千台に及ぶコンピューターから Darkhotelの攻撃を検知しました。そのほとんどは、DarkhotelのP2P攻撃に関連するものです。このデータから地理的な分布を推測すれば、Darkhotelの攻撃がどこで発生しているかを最も正確に把握できます。

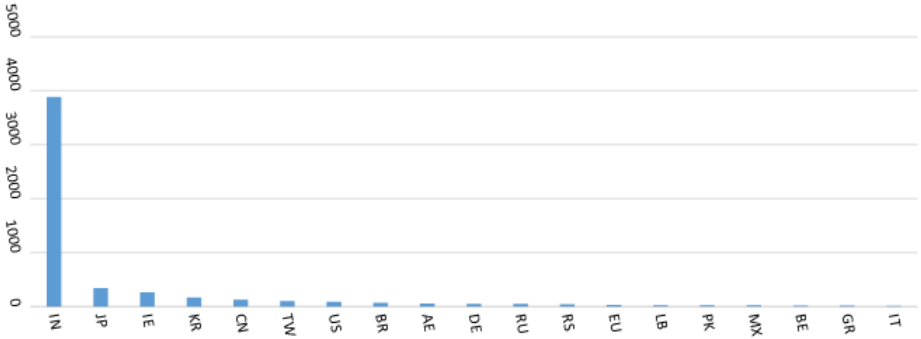


世界的な攻撃分布の比率をさらに見やすく円グラフにしてみました。これで分かるとおり、検知の90%以上は5か国に集中しています。日本がトップで、台湾、中国、ロシア、韓国がそれに続いています。



## シンクホールデータ

攻撃者は新しいC&Cサーバーを次々と構築していくため、十分な数のドメインをシンクホールに捕捉して、そのデータから被害システムの所在の正確な状況を把握することは困難です。また、シンクホール対象のドメインには多くの研究システムも接続されています。それでも、現在のシンクホールに接続のあった通信元を示したこのグラフを見ると、信頼性は低いながらも、被害者の所在が見えてきます。インド、日本、アイルランド、韓国、中国、台湾が上位に並んでいます。インドとアイルランドを除くと、KSNデータに近い状況になります。




## 被害者に関して利用可能なddrlogデータ

C&Cサーバーの多くでは、ddrlogとして特定のディレクトリパスに設置されています。ddrlogには、攻撃者がエラーログから切り分けたいコールバックデータが記録されているようですコールバックURLの多くにはエラーがつきもので、また多くは不要なIP範囲から発信されています。また、それ以外も研究者のサンドボックスシステムのコールバックであり、明らかに無関係です。

詳細なコネクトバックURL値に関する説明と、そのxor/base64エンコード方式は、「Indicators of Compromise」Appendix Dのテクニカルノート、「interesting Malware Trojan.Win32.Karba.e（注意すべきマルウェア Trojan.Win32.Karba.e）」に記載されています。

DarkhotelのC&Cサーバーでは、ddrlogの内容を保持して提供するために、以下のようなディレクトリ構造に設定されています。

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

以下の構造は、サーバー間で共通のように見えますが、ddrlogを生成せず、/error/ディレクトリも管理されません。

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

2009年1月1日午前9:16から始まるエントリは、次の2つのddrlogファイルでレポートされています。

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

すべてのログには約50,000件のエントリが記録されており、「B」または「I」というシンプルなスタンプが付いてます。これらのレコードは、以下のような書式です。

```
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 > I
2009.01.01 09:16:04 112.70.xx.xx > I
```

「B」チェックインを実行しているIPアドレスは120件だけで、残り90% は150.70.97.xの範囲に属しています。このIP範囲はすべて、東京のTrend Microのものです。

222.150.70.228など、残りのごく一部は日本のTrend Microが所有する他の範囲のもので、例外的に1つだけがエルサルバドルのISPからの IP、もう1つが日本のISPに接続しているIPです。およそ20,000件のIPアドレスが「I」チェックインを実行しています。

他のddrlogsには、「A」というタグも含まれている場合があります。

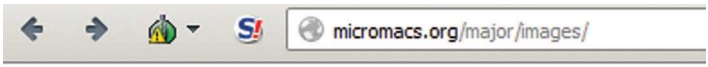
「A」タグは、ハンガリーやイタリアなど、標的以外の拠点に由来する無関係なチェックインを示すものです。「B」タグは、Trend MicroのIP範囲に由来する無関係なチェックインを示しています。

「I」は、さまざまな範囲に由来する無関係なチェックインを表しますが、ループバックアドレスである127.0.0.1などの異常IPは、明らかなエラーとして含まれています。

これらのログのエントリには、base64のキャラクタ辞書の要件に準拠していない空白や特殊文字を含むコールバックURLも含まれています。

## C&Cサーバーの通信と構造

一般的なメインページは次のとおりです。




Sorry. This site is under construction....

Please, Wait a few weeks.

auto2116.phpnet.us の場合、ディレクトリ構造は以下のようになります。

/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
    - 窃取されて暗号化された被害システムの内容
    **/l**
    /f

auto2116.phpnet.usの場合、ディレクトリ構造は以下のようになります。

/patch
    chkupdate.php（メインのコマンドと制御スクリプト）
/patch/error
    ddrlog

攻撃者グループは、サーバー上にある被害者のデータを暗号化しますが、複数の被害者に対してもユーザー/パスキーの組み合わせは1つだけです。被害者を管理するためのDarkhotel Webインターフェイスに不正なユーザーがアクセスを試みた場合、パスキーが正しくなければHTMLページとテーブルレイアウトが正しく表示されますが、そのページ上のすべての値が文字化けした暗号テキストとして返されます。

## 被害者の管理

新しい被害者は、システム上で判定します。攻撃者は、新たな被害者を判定するためのシステムをWebインターフェイス越しに管理しています。攻撃者はまず最優先に、最新のコマンドアンドコントロールサーバーのチェックインに従って被害者をリスト化し、並べ替えます。収集されたデータはほとんどの場合、重要性の順に表示されます。

1. ユーザーのログオン名
2. システムのCPUとOS
3. 「ping sec」、すなわち被害システムとC&Cサーバーとの距離
4. 「in」、すなわち攻撃者のDLLコードが実行されるプロセス
5. Vac：??
6. システムのLAN IP
7. ネットワークのWAN IP

管理Webページの一例を以下に示します。

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

## 調査活動

研究者のサンドボックスツールを使用しての自動分析が、ログの中にも大量に含まれていることは間違いありません。2013年6月から2014年4月まで（約11か月間）に、わずか15のddrlogファイルでも研究用サンドボックスシステムからの接続がほぼ7,000件確認されています。ネットワーク接続では、QEMUベースのサンドボックスを識別するためにa1=からa3=の値が設定され、すべてはわずか485のWAN IPアドレスに集約されます。30個のLAN IPが記録されており、そのすべてが同じ172.16.2.14126の範囲です。このシステムでは、「Dave」というユーザーアカウントと「HoMEoffD5f0AC」というWindowsシステム名が使われています。

これらの文字は、GFI Softwareの「CWsandbox」ツールによって生成されることを確認しており、その所有者は現在「ThreatTrack Security」です。

# まとめ

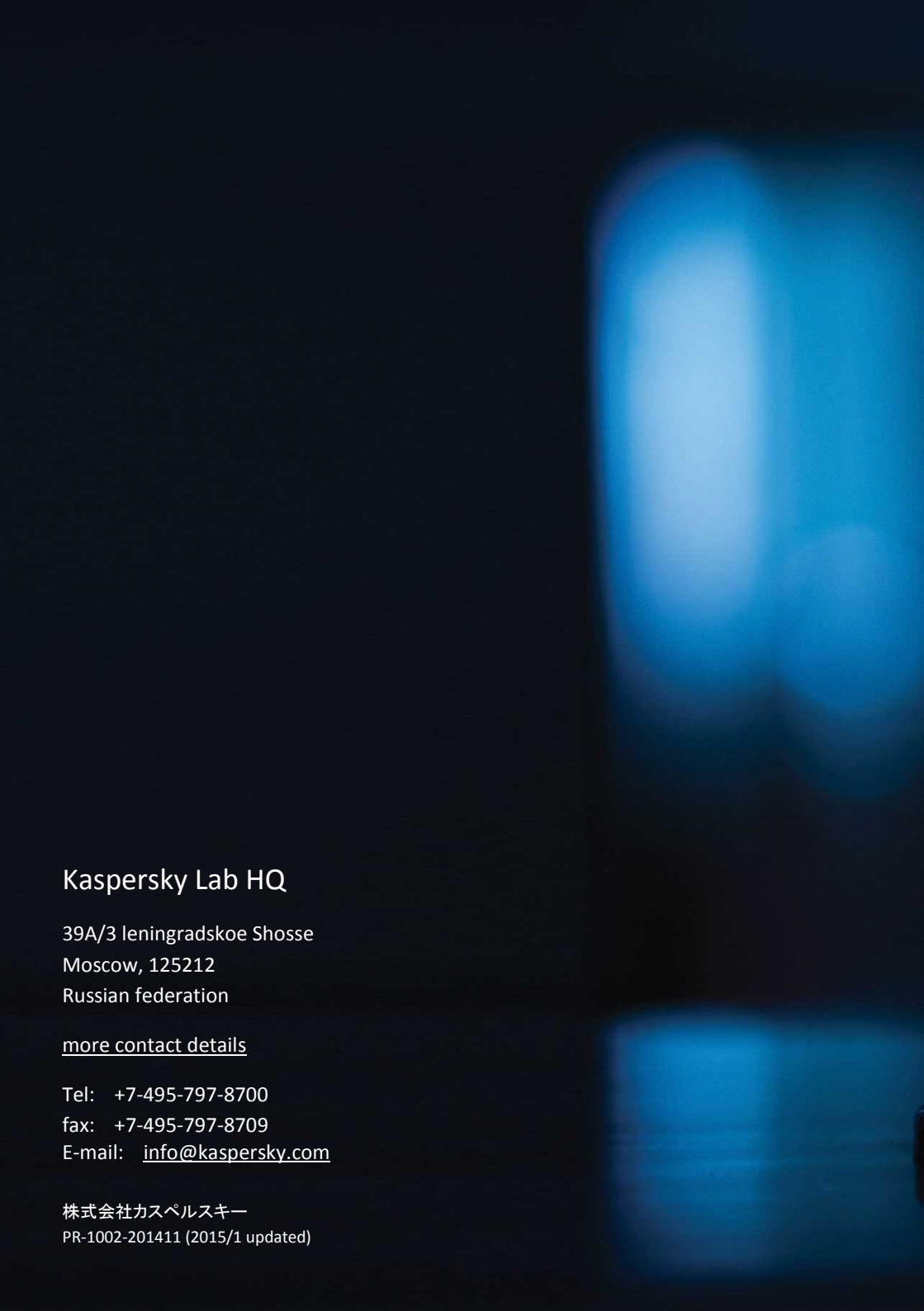
過去7年間にわたり、Darkhotelという強力な攻撃者（別名Tapaoux）が全世界のユーザーを対象に広範囲の攻撃を実行し、成功してきました。そこで使われている手法もテクニックも、一般的なサイバー犯罪者を大きく超えています。

Darkhotelの攻撃者は、512ビットRSA暗号鍵の因数分解など暗号化を利用した注目すべき攻撃を実行できるほどのスキルを有しています。また、ゼロデイを利用していることも、攻撃者の強大さを示しています。

世界各国の大規模企業の幹部が特定の「ダークホテル」に滞在している間を狙っていることが、この活動の最大の特徴です。標的を選定する正確な手法、たとえば標的とする宿泊者と標的としない宿泊者をどう見極めているのかは、まだ判明していません。ほとんどの場合、被害者が幹部クラスであるという事実から、攻撃者は被害者の所在地や名前、宿泊先もつかんでいると考えられます。このような攻撃者が描いた暗く危険な Web 上のワナに、無防備な宿泊客はまんまと捕らわれてしまうのです。特定のホテルだけが攻撃者経路として利用されている理由も正確には分かっていませんが、一定の疑惑は明らかに存在し、そこからさらに大きい被害も想定されます。この攻撃活動の真相については現在も調査中であり、今後も詳細をご報告する予定です。

もうひとつ注目に値する傾向は、標的型とボットネットを含めて複数タイプの攻撃が展開されているということです。これは、APT攻撃の世界でますます一般的になりつつある傾向です。まず標的型攻撃によって著名なユーザーに感染し、次にボットネットスタイルの攻撃で大規模な調査に乗り出す、あるいは敵対する相手にDDoS攻撃を仕掛けたり、被害者をさらに巧妙なスパイ活動のツールに仕立てたりという攻撃を実行するのです。

Darkhotelの攻撃者は、今後もDIBや政府機関、NGO組織に対する攻撃を続けると見られます。本書と同時に発行される付録（「Indicators of Compromise」）では、この攻撃の技術的な特徴について解説しています。悪意のあるトラフィックを特定し、標的となった場合でも攻撃に対する防御をとるヒントになるはずです。




## 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



株式会社カスペルスキー
PR-1002-201411 (2015/1 updated)