



FFR yarai analyzer活用事例 – Vawtrakの解析 –

株式会社 F F R I
<http://www.ffri.jp>

本資料の目的

- 弊社製品「FFR yarai analyzer」は従来セキュリティの専門家でなければ、解析が難しいとされてきたマルウェアの解析を自動化したシステムである。
- 本資料では「FFR yarai analyzer」を用いてマルウェアを解析していく手順や解析結果の活用方法を紹介することを目的としている。

解析対象

- 解析対象
 - 「Vawtrak.dat」
 - 今回解析対象としたマルウェアは通称「Vawtrak」と呼ばれており、オンラインバンキングユーザーを対象に攻撃する。
 - 2014年5月頃からその攻撃が多く報道されており、検出の約8割が日本国内をターゲットとしているとされている。
 - 「Vawtrak」は、従来より情報を詐取するマルウェアとして知られていたが、日本国内のオンラインバンキングユーザーへの攻撃に使用されたというのが他国では事例が少ないことから特徴的である。

解析手順

- 解析手順
 1. 解析対象をFFR yarai analyzer ver1.4のScanフォルダへコピー
 2. Crawler上にて解析開始を確認する
 - あらかじめCrawlerVMのデスクトップを表示しておく
 3. Crawler上にて、解析対象が実行されたら手動でInternet Explorerを起動する
 - IEはホームをwww.google.co.jpに設定してある
 4. 解析終了後、HTMLレポートを確認する

解析レポート (サマリ) の確認 (1/2)

- マルウェアとして検出されている
- 対象ファイルの実行方法が、rundll32.exe及びregsvr32.exeを使用した実行方法であることから、対象ファイルは「DLL形式」である



FFRI yarai analyzer プログラム解析レポート (サマリ)

システム情報

マシン名	XP1ANAL
OSバージョン	Windows XP Service Pack 3
搭載メモリ量	511M
実行ユーザ名	Administrator
解析日時	2014-11-25 21:26:49

解析ファイル概要

検査中にタイムアウトが発生しました

C:\YaraiAnalyzer\Scan\vawtrak.dat

SHA1 ハッシュ	b4cefb3148e9af37e0b7691e840719d4471d09fe
ファイルサイズ	286096
ゲスト側ファイル名	C:\YaraiAnalyzer\fsmon\webcrawler.exe\2012\2014-11-25-21-26-01-025_1.dat
結果	マルウェアが検出されました

脅威検出プロセスサマリ

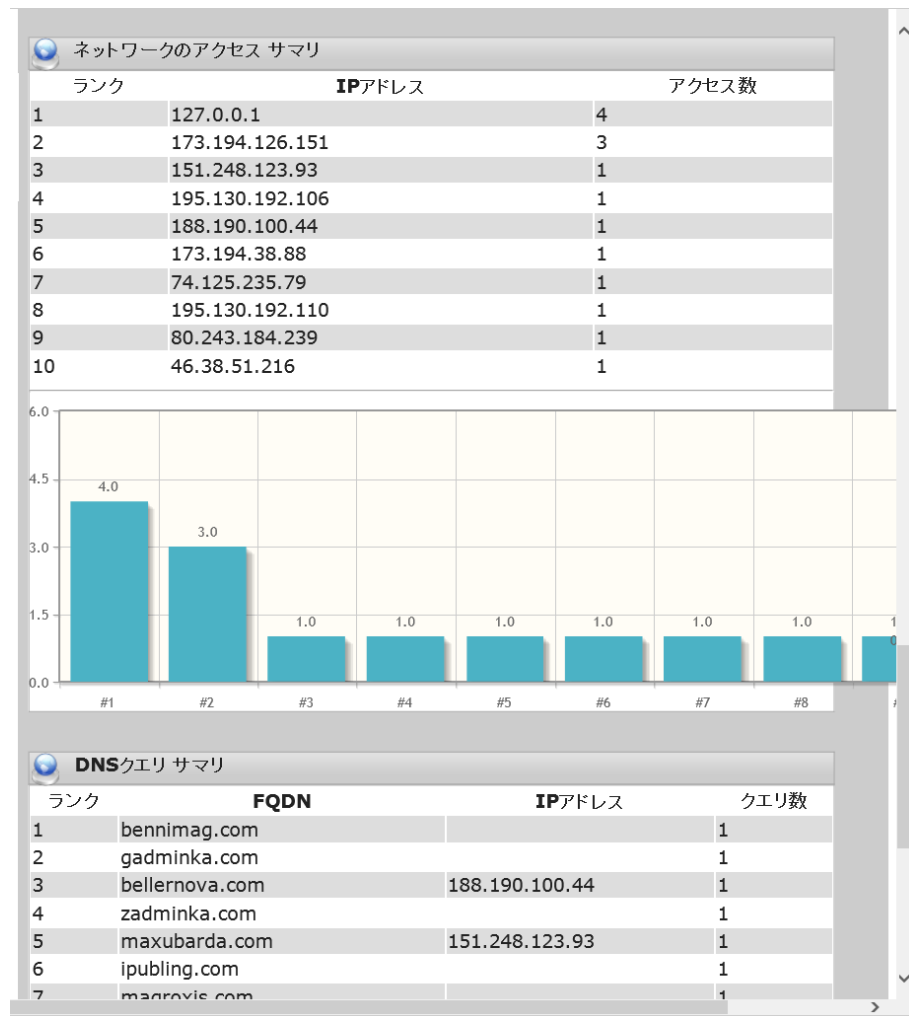
(548)C:\WINDOWS\system32\rundll32.exe	
脅威レベル	検出回数

解析レポート（サマリ）の確認（2/2）

- 複数のIPアドレスにアクセスしている
- DNSクエリも多く出力されている
※IPアドレス、DNSには正規サイトも含まれる
- 出力されたDNSクエリをVirusTotalで検索すると、マルウェア配布サイトとなっていることがわかる

VirusTotal検索結果（抜粋）

ドメイン名	検索結果
bennimag.com	4/61
gadminka.com	3/61
maxubarda.com	6/62
ipubling.com	6/61
zadminka.com	4/61



対象ファイル実行プロセスの確認 (rundll32.exe)

- スタティック分析エンジンにてマルウェアとして検出
- rundll32.exeプロセス内ではファイル作成等の活動は行っていない

ファイルの更新情報				
結果	操作	ファイル名	検出エンジン	検出回数

アクセス権の設定情報			
ファイル名	種類	名前	アクセス許可

レジストリの更新情報				
操作	レジストリキー	エントリー	更新前	更新後

ネットワークアクセス情報	
IPアドレス	ポート番号

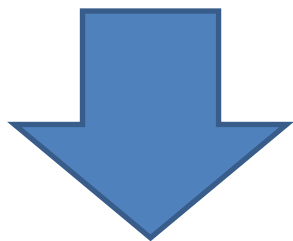
DNSクエリ情報	
FQDN	IPアドレス

プロセス概要	
プロセス名	rundll32.exe
プロセスID	548
親プロセスID	1312
プロセスパス	C:\WINDOWS\system32\rundll32.exe
コマンドライン	"C:\WINDOWS\system32\rundll32.exe "C:\YaraiAnalyzer\fsmon\webcrawler.exe\2012\2014-11-25-21-26-01-025_1.dat",DllEntryPoint"
結果	マルウェアが検出されました

検出した脅威	
検出脅威一覧	
	<ul style="list-style-type: none"> ● パッカーを検出しました。悪意あるコードが隠蔽されている可能性があります。 ● 不審なプログラム構造を検出しました。
脅威の内容	
パッカーを検出しました。悪意あるコードが隠蔽されている可能性があります。	
詳細説明	実行ファイル自身がパッカーによる圧縮もしくは暗号化されています。パッカーは、マルウェアがよく自身のコードを暗号化するために用います。これによりアンチウイルスベンダーは解析が困難になります。正常なプログラムがパッカーを使う強い理由はありません。
脅威レベル	高
検出エンジン	スタティック分析
不審なプログラム構造を検出しました。	
詳細説明	一般的なアプリケーションには見られないようなセクションの構造を検出しました。通常の開発環境からは生成されない実行ファイルの構造のため、マルウェアの可能性が疑われます。
脅威レベル	中
検出エンジン	スタティック分析

対象ファイル実行プロセスの確認 (regsvr32.exe)

- regsvr32.exeを使用した実行においても、ファイル作成等の活動は行われていない



- これにより、解析対象は別のプロセスに侵入し、悪意ある動作を行っていると推測される



Process details for regsvr32.exe:

- 名前: regsvr32.exe
- プロセスID: 552
- 親プロセスID: 1312
- プロセスパス: C:\WINDOWS\system32\regsvr32.exe
- コマンドライン: "C:\WINDOWS\system32\regsvr32.exe "C:\YaraiAnalyzer\fsmon\webcrawler.exe\2012\2014-11-25-21-26-01-025_1.dat""
- 結果: マルウェアは検出されませんでした

Security and file information sections are also visible but empty.

別プロセスの確認 (explorer.exe)

- explorer.exeプロセスにて不審なレジストリ書込みが行われている（赤ハイライト部分）
- レジストリ書込みでは、自分自身をPC起動時に自動起動させるための書込みを実施
- 書込み内容より、実行には、regsvr32.exeを利用していることが判明

操作	レジストリキー	エントリ	更新前	更新後
新規	HKCU\S-1-5-21-507921405-823518204-6820033-30-500\Software\Microsoft\Internet Explorer\Main	TabProcGroup		DWORD 0
新規	HKCU\S-1-5-21-507921405-823518204-6820033-30-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3	2500		DWORD 3
新規	HKCU\S-1-5-21-507921405-823518204-6820033-30-500_CLASSES\CLSID\{261B4B5C-45D0-4A78-8861-53376C776D20}	#cert		Binary 0x31
新規	HKCU\S-1-5-21-507921405-823518204-6820033-30-500\Software\Microsoft\Windows\CurrentVersion\Run	2014-11-25-21-26-01-025_1		Sz regsvr...
新規	HKCU\S-1-5-21-507921405-823518204-6820033-30-500\Software\Microsoft\Windows\ShellNoRoam	regsvr32.exe "C:\YaraiAnalyzer\fsmon\webcrawler.exe"2012\2014-11-25-21-26-01-025_1.dat		Internet Explorer

書き込まれたレジストリエントリ

キー	HKCU\S-1-5-21-507921405-823518204-6820033-30-500\Software\Microsoft\Windows\CurrentVersion\Run
エントリ	2014-11-25-21-26-01-025_1
値	regsvr32.exe "C:\YaraiAnalyzer\fsmon\webcrawler.exe"2012\2014-11-25-21-26-01-025_1.dat

別プロセスの確認 (IEXPLORE.EXE)

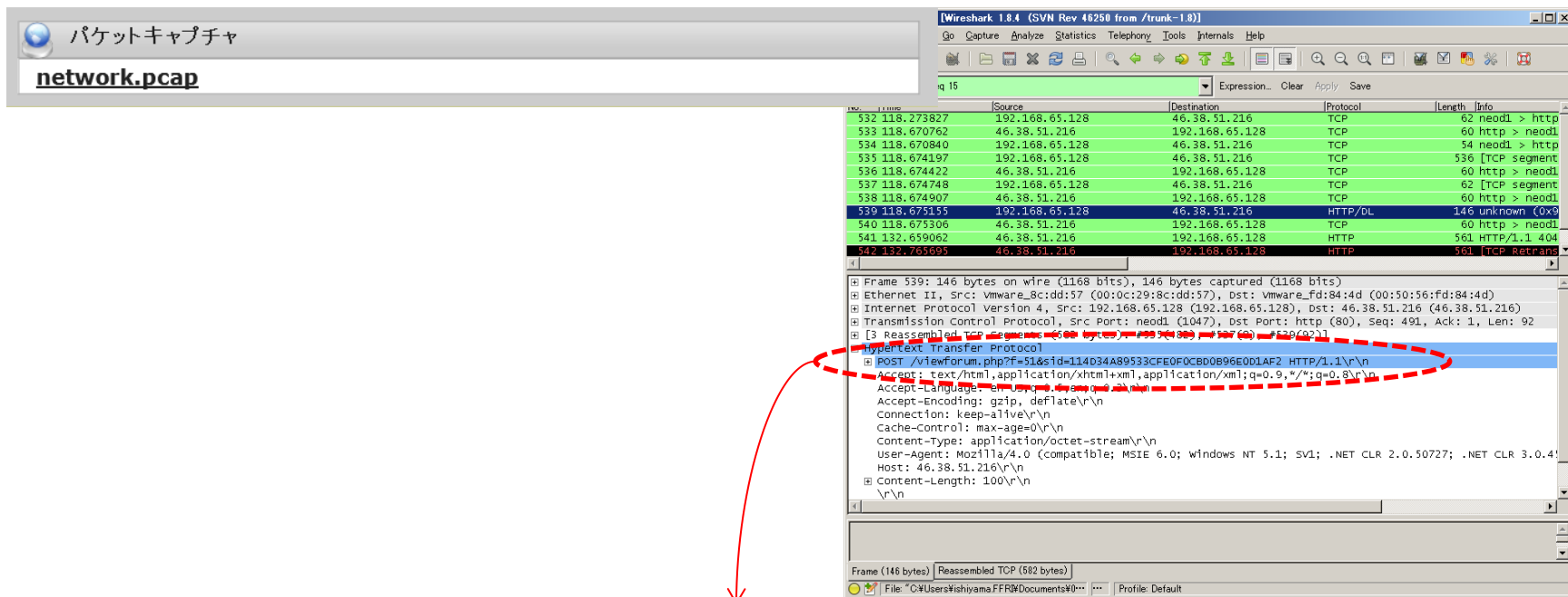
- IEプロセスからは、ホームに設定しているwww.google.co.jp以外のドメイン、IPアドレスにもアクセスを行っている
- 解析対象マルウェアがIEプロセスに侵入し、IEプロセスから通信していると考えられる

ネットワークアクセス情報	
IPアドレス	ポート番号
127.0.0.1	5152
127.0.0.1	1034
80.243.184.239	80 (www)
173.194.126.151	80 (www)
173.194.126.151	443 (https)
74.125.235.79	443 (https)
173.194.38.88	443 (https)
151.248.123.93	80 (www)
195.130.192.106	80 (www)
188.190.100.44	80 (www)
195.130.192.110	80 (www)
46.38.51.216	80 (www)

DNSクエリ情報	
FQDN	IPアドレス
www.google.co.jp	173.194.126.151
clients1.google.co.jp	74.125.235.79
ssl.gstatic.com	173.194.38.88
magroxis.com	
ipubling.com	
maxubarda.com	151.248.123.93
zadminka.com	
bellernova.com	188.190.100.44
gadminka.com	
bennimag.com	

パケットキャプチャの確認

- 解析レポート（サマリ）ページの下部からパケットキャプチャファイルをダウンロードし、Wiresharkで確認
- 接続が成功したIPアドレスのURLのパスを確認



network.pcap

No.	Time	Source	Destination	Protocol	Length	Info
532	118.273827	192.168.65.128	46.38.51.216	TCP	62	neod1 > http
533	118.670762	46.38.51.216	192.168.65.128	TCP	60	http > neod1
534	118.670840	192.168.65.128	46.38.51.216	TCP	54	neod1 > http
535	118.674197	192.168.65.128	46.38.51.216	TCP	536	[TCP segment
536	118.674422	46.38.51.216	192.168.65.128	TCP	60	http > neod1
537	118.674748	192.168.65.128	46.38.51.216	TCP	62	[TCP segment
538	118.674907	46.38.51.216	192.168.65.128	TCP	60	http > neod1
539	118.675155	192.168.65.128	46.38.51.216	HTTP/DL	146	unknown (0x8
540	118.675306	46.38.51.216	192.168.65.128	TCP	60	http > neod1
541	132.659062	46.38.51.216	192.168.65.128	HTTP	561	HTTP/1.1 404
542	132.765695	46.38.51.216	192.168.65.128	HTTP	561	[TCP Retrans

```
POST /viewforum.php?f=51&sid=114D34A89533CFE0F0CBD0B96E0D1AF2 HTTP/1.1\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
Accept-Language: en-US\r\n
Accept-Encoding: gzip, deflate\r\n
Connection: keep-alive\r\n
Cache-Control: max-age=0\r\n
Content-Type: application/octet-stream\r\n
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2)\r\n
Host: 46.38.51.216\r\n
Content-Length: 100\r\n
\r\n
```

POST /viewforum.php?f=51&sid=114D34A89533CFE0F0CBD0B96E0D1AF2 HTTP/1.1

解析レポートまとめ

- 対象マルウェアはDLL形式のマルウェア
- 別プロセスに侵入し、別プロセス内で悪意ある行動を行う
- レジストリの自動起動設定を利用してPC起動時に起動するようにしている
- Internet Explorerプロセス内からC&Cサーバへの接続を行っている

補足

- 解析対象実行後のInternet Explorerの起動について
 - 今回、手動にて解析実施時にInternet Explorerを起動したが、設定ファイルを編集することで、解析実行時にInternet Explorerを起動させることが可能
 - 編集対象ファイル
 - C:¥YaraiAnalyzer¥Config¥Crawler¥findexec.conf
 - 編集内容
 - 赤枠部分を追記する

```
# Execute DLL file with rundll32 or regsvr32
FILTER_RULE
    dllfilter
    sha1chk
    execute          C:¥WINDOWS¥system32¥rundll32.exe "%p", DllEntryPoint
    execute          C:¥WINDOWS¥system32¥regsvr32.exe "%p"
    execute          "C:¥Program Files¥Internet Explorer¥IEXPLORE.EXE"
    print
```