

Turla PNG Dropper is back

22 November 2018

By [Matt Lewis](#)



◆ Research ◆ Research ◆ Reverse Engineering ◆ Vulnerability ◆ Threat Intelligence

This is a short blog post on the PNG Dropper malware that has been developed and used by the Turla Group [1]. The PNG Dropper was first discovered back in August 2017 by Carbon Black researchers. Back in 2017 it was being used to distribute Snake, but recently NCC Group researchers have uncovered samples with a new payload that we have internally named RegRunnerSvc.

It's worth noting at this point that there are other components to this infection that we have not managed to obtain. There will be a first stage dropper that will drop and install the PNG Dropper/RegRunnerSvc. Nevertheless, we think that this it is worth documenting this new use of the PNG Dropper.

PNG Dropper

The PNG Dropper component has already been well documented by the research team at Carbon Black [1], but for the purpose of clarity we will now give a quick summary of what it is and how it works.



mon. 10/1/04

This website makes use of cookies.

This website uses cookies to ensure you get the best experience on our website. Some of these cookies are essential for the site to function, whilst others are useful to help us to analyse our traffic and collect statistics on how and when the site is being used and how it can be improved. We also share information about your use of our site with our analytics partners.

By clicking "Accept All," you consent to the storing of cookies on your device to enhance site navigation, analyse site usage, and assist in measuring the success of our marketing efforts.

Manage your preferences at any time, on the cookie preference tool at the bottom of the screen, or if you want to learn more, please go to our [Cookie policy](#)

Accept all cookies

Reject all cookies

Necessary cookies

Necessary cookies enable core functionality as you browse our website such as session management and remembering your cookie preferences. The website cannot function properly without these cookies and can only be disabled by changing your browser preferences.

Analytical Cookies

Analytical cookies help us to improve our website by collecting and reporting information on its usage.

Off

5 files.
 source
 ewed
 an

This
 GB value
 for a
 ;.

```

.text:000000013F700D26 8B D0      mov     edx, eax      ; dwSize
.text:000000013F700D28 49 89 17    mov     [r15], rdx
.text:000000013F700D2B 33 C9      xor     ecx, ecx      ; lpAddress
.text:000000013F700D2D 44 8D 49 40 lea     r9d, [rcx+40h] ; flProtect
.text:000000013F700D31 41 88 00 10 00 00 mov     r8d, 1000h    ; flAllocationType
.text:000000013F700D37 FF 15 CB 06 FF FF call    cs:VirtualAlloc
.text:000000013F700D3D 4C 8B 6D 6F mov     r13, [rbp+57h+arg_8]
.text:000000013F700D41 49 89 45 00 mov     [r13+0], rax
.text:000000013F700D45 48 85 C0    test    rax, rax
.text:000000013F700D48 0F 84 EC 00 00 00 jz      loc_13F700E3A
.text:000000013F700D4E 48 89 45 FF mov     [rbp+57h+var_58], rax
.text:000000013F700D52 48 8D 45 FF lea     rax, [rbp+57h+var_60]

```

This website makes use of cookies.

This website uses cookies to ensure you get the best experience on our website. Some of these cookies are essential for the site to function, whilst others are useful to help us to analyse our traffic and collect statistics on how and when the site is being used and how it can be improved. We also share information about your use of our site with our analytics partners.

By clicking "Accept All," you consent to the storing of cookies on your device to enhance site navigation, analyse site usage, and assist in measuring the success of our marketing efforts.

Manage your preferences at any time, on the cookie preference tool at the bottom of the screen, or if you want to learn more, please go to our [Cookie policy](#)

Each PNG
together
the PE file
executed

ally load
int is

```

.text:0000
.text:0000
.text:0000
.text:0000
.text:0000
.text:0000
.text:0000
.text:0000
.text:0000
.text:0000

```

Necessary cookies

Necessary cookies enable core functionality as you browse our website such as session management and remembering your cookie preferences. The website cannot function properly without these cookies and can only be disabled by changing your browser preferences.

RegF

The PNG
RegRunn

then run it. It is a stage dropper (which we have not managed to obtain, will have already installed it as a service and performed a few additional setup operations.

Analytical Cookies

☐ Off

se of
and

Figure 5 shows the entry point for RegRunnerSvc. Here we can see the call to StartServiceCtrlDispatcher. In this case the name of the service is WerFaultSvc, obviously chosen in an attempt to seem like a legitimate part of the Windows Error Reporting service. The service also serves as a persistence mechanism for the malware.

```
push rbx
sub rsp,40
mov rbx,rcx
mov ecx,8007
call qword ptr ds:[<&SetErrorMode>]
cmp byte ptr ds:[1400040FF],0
mov qword ptr ds:[140004138],rbx
lea r8,qword ptr ds:[140004080]
je 6e.140001BA2
mov rcx,r8
mov edx,20
movzx eax,byte ptr ds:[rcx-80]
add rcx,4
xor byte ptr ds:[rcx-4],al
movzx eax,byte ptr ds:[rcx-4]
xor byte ptr ds:[rcx-4],eax
movzx eax,byte ptr ds:[rcx-4]
xor byte ptr ds:[rcx-4],eax
movzx eax,byte ptr ds:[rcx-4]
xor byte ptr ds:[rcx-4],eax
sub rdx,1
jne 6e.140001BA2
lea rax,qword ptr ds:[140004080]
lea rcx,qword ptr ds:[140004080]
mov qword ptr ds:[140004080],rax
xor eax,eax
mov qword ptr ds:[140004080],eax
mov qword ptr ds:[140004080],eax
call qword ptr ds:[140004080]
xor eax,eax
add rsp,40
pop rbx
ret
```

EntryPoint

```
rcx:&"WerFaultSvc"
ecx:&"WerFaultSvc"
```

```
r8:"WerFaultSvc", 0000000140004080:"WerFaultSvc"
```


```
rcx:&"WerFaultSvc", r8:"WerFaultSvc"
20:' '
```

```
rcx:&"WerFaultSvc"
```

This website makes use of cookies.

This website uses cookies to ensure you get the best experience on our website. Some of these cookies are essential for the site to function, whilst others are useful to help us to analyse our traffic and collect statistics on how and when the site is being used and how it can be improved. We also share information about your use of our site with our analytics partners.

By clicking "Accept All," you consent to the storing of cookies on your device to enhance site navigation, analyse site usage, and assist in measuring the success of our marketing efforts.

Manage your preferences at any time, on the cookie preference tool at the bottom of the screen, or if you want to learn more, please go to our [Cookie policy](#) 

After the
Generally
string wit
are enun
starts at
either th
detail (sh
the size c
as the de
its setup
importar

stry.
ated)
values
ation
rch until
tation
d is that
st seem
formed
more

Necessary cookies

Necessary cookies enable core functionality as you browse our website such as session management and remembering your cookie preferences. The website cannot function properly without these cookies and can only be disabled by changing your browser preferences.

Analytical Cookies

Analytical cookies help us to improve our website by collecting and reporting information on its usage.




```
cmp    eax, ERROR_NO_MORE_ITEMS
mov    ebx, eax
jz     loc_14000193F
```

```
db     66h, 66h
xchg   ax, ax
```

This website makes use of cookies.

This website uses cookies to ensure you get the best experience on our website. Some of these cookies are essential for the site to function, whilst others are useful to help us to analyse our traffic and collect statistics on how and when the site is being used and how it can be improved. We also share information about your use of our site with our analytics partners.

By clicking "Accept All," you consent to the storing of cookies on your device to enhance site navigation, analyse site usage, and assist in measuring the success of our marketing efforts.

Manage your preferences at any time, on the cookie preference tool at the bottom of the screen, or if you want to learn more, please go to our [Cookie policy](#) 

The data doesn't contain any sensitive data, however, the first system data block contains the first 200 bytes of the header.

Necessary cookies

Necessary cookies enable core functionality as you browse our website such as session management and remembering your cookie preferences. The website cannot function properly without these cookies and can only be disabled by changing your browser preferences.

Analytical Cookies

Analytical cookies help us to improve our website by collecting and reporting information on its usage.



it. It key. This ypt*). re ovider". d the he first at cription

Offset	Description
0x00	Offset to secret data – used in call to the BCryptGenerateSymmetricKey() function
0x08	Size of secret data

0x10	Offset to IV
0x18	IV size
0x20	Offset to AES encrypted data
0x28	Encrypted data size

Now the payload is the BCrypt created. The payload is (it checks the header). The point is c

This website makes use of cookies.

This website uses cookies to ensure you get the best experience on our website. Some of these cookies are essential for the site to function, whilst others are useful to help us to analyse our traffic and collect statistics on how and when the site is being used and how it can be improved. We also share information about your use of our site with our analytics partners.

By clicking "Accept All," you consent to the storing of cookies on your device to enhance site navigation, analyse site usage, and assist in measuring the success of our marketing efforts.

Manage your preferences at any time, on the cookie preference tool at the bottom of the screen, or if you want to learn more, please go to our [Cookie policy](#)

he main
assed to
g
the
lid PE file
in the PE
entry

```
memcpy(v12, &v10, 0x10);
memcpy(v12, &v10, 0x10);
v12 = aesi_encrypt(v12, v10, v10);

free(Src);
Src = 0;
if ( !v12 || !v10 || !v10 )
{
    v18 = 0;
    v19 = 0;
    v20 = 0;
    v21 = 0;
    v6 = 1;
    free(p);
    p_decrypt(v12, v10, v10);
    if ( !v6 )
        break;
}
```

Necessary cookies

Necessary cookies enable core functionality as you browse our website such as session management and remembering your cookie preferences. The website cannot function properly without these cookies and can only be disabled by changing your browser preferences.

Analytical Cookies

Analytical cookies help us to improve our website by collecting and reporting information on its usage.

☐ Off

18);

Figure 7

Summary

In this blog post we have had a quick look at a new use of the PNG Dropper by the Turla Group. The group is now using it with a new component: RegRunnerSvc, which extracts and encrypted

PE file from the registry, decrypts it and runs it. It seems that the group is taking ideas from fileless malware, such as Poweliks or Kovter. The group is ensuring that it is leaving as little information as possible in the binary files, i.e. not hardcoding the name of the registry key containing the encrypted data. This means that that it is not possible to extract useful IOCs for threat hunting.

Thankfully all is not lost and we can at least detect the usage of the PNG dropper using the Yara rules below

As part of our research we have decided to share this here: <http://www.nccgroup.com/us/research-blog/turla-png-dropper-is-back/>

Yara


This website makes use of cookies.

oper. We

This website uses cookies to ensure you get the best experience on our website. Some of these cookies are essential for the site to function, whilst others are useful to help us to analyse our traffic and collect statistics on how and when the site is being used and how it can be improved. We also share information about your use of our site with our analytics partners.

order.

By clicking "Accept All," you consent to the storing of cookies on your device to enhance site navigation, analyse site usage, and assist in measuring the success of our marketing efforts.

Manage your preferences at any time, on the cookie preference tool at the bottom of the screen, or if you want to learn more, please go to our [Cookie policy](#) 

Necessary cookies

Necessary cookies enable core functionality as you browse our website such as session management and remembering your cookie preferences. The website cannot function properly without these cookies and can only be disabled by changing your browser preferences.

Analytical Cookies



Analytical cookies help us to improve our website by collecting and reporting information on its usage.


```
rule turla_png_dropper {
  meta:
    author = "Ben Humphrey"
    description = "Detects the PNG Dropper used by the Turla group"
    sha256 =
"6ed939
```

st

This website makes use of cookies.

This website uses cookies to ensure you get the best experience on our website. Some of these cookies are essential for the site to function, whilst others are useful to help us to analyse our traffic and collect statistics on how and when the site is being used and how it can be improved. We also share information about your use of our site with our analytics partners.

By clicking "Accept All," you consent to the storing of cookies on your device to enhance site navigation, analyse site usage, and assist in measuring the success of our marketing efforts.

Manage your preferences at any time, on the cookie preference tool at the bottom of the screen, or if you want to learn more, please go to our [Cookie policy](#) 

Necessary cookies

Necessary cookies enable core functionality as you browse our website such as session management and remembering your cookie preferences. The website cannot function properly without these cookies and can only be disabled by changing your browser preferences.

Analytical Cookies



Analytical cookies help us to improve our website by collecting and reporting information on its usage.

```
48 63 43 3C          // movsxd rax, dword ptr [rbx+3Ch]
B9 0B 01 00 00       // mov ecx, 10Bh
BA AF BE AD DE       // mov edx, 0DEADBEAFh
66 39 4C 18 18       // cmp [rax+rbx+18h], cx
8B 44 18 28          // mov eax, [rax+rbx+28h]
45 33 C9             // xor r9d, r9d
44 8B C2             // mov r8d, edx
```



```
48 8B CB          // mov rcx, rbx
48 03 C3          // add rax, rbx
FF D0            // call rax
}
```


condition:

```
(uint16(0) == 0x544D and uint16(uint32(0x3c)) == 0x4550) and
```

This website makes use of cookies.

This website uses cookies to ensure you get the best experience on our website. Some of these cookies are essential for the site to function, whilst others are useful to help us to analyse our traffic and collect statistics on how and when the site is being used and how it can be improved. We also share information about your use of our site with our analytics partners.

By clicking "Accept All," you consent to the storing of cookies on your device to enhance site navigation, analyse site usage, and assist in measuring the success of our marketing efforts.

Manage your preferences at any time, on the cookie preference tool at the bottom of the screen, or if you want to learn more, please go to our [Cookie policy](#) 

Necessary cookies

Necessary cookies enable core functionality as you browse our website such as session management and remembering your cookie preferences. The website cannot function properly without these cookies and can only be disabled by changing your browser preferences.

Analytical Cookies



Analytical cookies help us to improve our website by collecting and reporting information on its usage.


```
rule turla_png_reg_enum_payload {  
  meta:  
    author = "Ben Humphrey"  
    description = "Payload that has most recently been dropped by the  
Turla PNG Dropper"
```

"fea27c

This website makes use of cookies.

This website uses cookies to ensure you get the best experience on our website. Some of these cookies are essential for the site to function, whilst others are useful to help us to analyse our traffic and collect statistics on how and when the site is being used and how it can be improved. We also share information about your use of our site with our analytics partners.

By clicking "Accept All," you consent to the storing of cookies on your device to enhance site navigation, analyse site usage, and assist in measuring the success of our marketing efforts.

Manage your preferences at any time, on the cookie preference tool at the bottom of the screen, or if you want to learn more, please go to our [Cookie policy](#) 

Necessary cookies

Necessary cookies enable core functionality as you browse our website such as session management and remembering your cookie preferences. The website cannot function properly without these cookies and can only be disabled by changing your browser preferences.

Analytical Cookies



IOCs

Analytical cookies help us to improve our website by collecting and reporting information on its usage.

Sample Analysed

- 6ed939f59476fd31dc4d99e96136e928fbd88aec0d9c59846092c0e93a3c0e27 (PNG Dropper)
- fea27eb2e939e930c8617dcf64366d1649988f30555f6ee9cd09fe54e4bc22b3 (Payload contained in the PNG dropper)

Services

- WerFaultSvc

References

[1] <https://www.carbonblack.com/2017/08/18/threat-analysis-carbon-black-threat-research-dissects-png-dropper/>


Published date: 22 November 2018

Written by

This website makes use of cookies.

This website uses cookies to ensure you get the best experience on our website. Some of these cookies are essential for the site to function, whilst others are useful to help us to analyse our traffic and collect statistics on how and when the site is being used and how it can be improved. We also share information about your use of our site with our analytics partners.

By clicking "Accept All," you consent to the storing of cookies on your device to enhance site navigation, analyse site usage, and assist in measuring the success of our marketing efforts.

Manage your preferences at any time, on the cookie preference tool at the bottom of the screen, or if you want to learn more, please go to our [Cookie policy](#) 

Necessary cookies

Necessary cookies enable core functionality as you browse our website such as session management and remembering your cookie preferences. The website cannot function properly without these cookies and can only be disabled by changing your browser preferences.

Analytical Cookies

Analytical cookies help us to improve our website by collecting and reporting information on its usage.



Terms and

Privacy Policy

Contact Us

Consulting & Implementation

Managed Services

Incident Response

Threat Intelligence

+1-(415)-268-9300

24/7 Incident Response Hotline

+1-(855)-684-1212


or cirt@nccgroup.com

© NCC Group 2024. All rights reserved.

This website makes use of cookies.

This website uses cookies to ensure you get the best experience on our website. Some of these cookies are essential for the site to function, whilst others are useful to help us to analyse our traffic and collect statistics on how and when the site is being used and how it can be improved. We also share information about your use of our site with our analytics partners.

By clicking "Accept All," you consent to the storing of cookies on your device to enhance site navigation, analyse site usage, and assist in measuring the success of our marketing efforts.

Manage your preferences at any time, on the cookie preference tool at the bottom of the screen, or if you want to learn more, please go to our [Cookie policy](#) 

Necessary cookies

Necessary cookies enable core functionality as you browse our website such as session management and remembering your cookie preferences. The website cannot function properly without these cookies and can only be disabled by changing your browser preferences.

Analytical Cookies



Analytical cookies help us to improve our website by collecting and reporting information on its usage.