Goblin Panda changes the dropper and reuses the old infrastructure

M medium.com/@Sebdraven/goblin-panda-changes-the-dropper-and-reused-the-old-infrastructure-a35915f3e37a

Sebdraven

December 28, 2018

<u>Sebdraven</u> Dec 28, 2018 I found a new dropper



c580d77722d85238ed76689a17b0205b4d980c010bef9616b8611ffba21b142e with the same signature of others. But it changes the exploitation. Before, it uses the ole package to drop a 8.t file in %appdata% and decode two files, a legit file and an backdoor (PlugX, newcore rat, sysfader...).

Now it's a big object ole mapped in memory and one PE is used to drop the files.

RTF exploit

Now we have four object oles in the RTF.



this RTF exploits again the CVE-2017_1882 on eqnedt32.exe.

The biggest object is a new exe to overwritten the first eqnedt32.exe . This PE is decoded by the shellcode of the exploit and executes this PE.



It's the same algorithm of the exploit targeting Vietnam.

	0066C82A		B8 6	3 8E	F4	7B	mov eax,7BF48E63
	0066C82F		39 5				cmp dword ptr ss:[ebp-4],edx
	0066C832	~	7E 2				11e 66C856
·>●	0066C834		6A 0	7			push 7
	0066C836		5 F				pop edi
>®	0066C837		88 C	8			mov ecx,eax
	0066C839		C1 E	9 18			shr ecx,1B
•	0066C83C		33 C	8			xor ecx,eax
	0066C83E		C1 E	9 03			shr ecx,3
	0066C841		33 C	8			xor ecx,eax
•	0066C843		03 C	0			add eax,eax
	0066C845		83 E				and ecx,1
	0066C848		0B C	1			or eax,ecx
	0066C84A		4F				dec edi
L@	0066C84B	~	75 E				jne 66C837
→ •	0066C84D		30 C	4 1A			<pre>xor byte ptr ds:[edx+ebx],al</pre>
	Looccorol		4.5				inc of y

Т

Just the init key has changed.

Dropper

the PE creates a directory in %appdata% named IISWebClient

.text:004011B5	push	esi ; nSize
.text:004011B6	lea	eax, [ebp+Dst]
.text:004011BC	push	eax ; lpDst
.text:004011BD	push	offset Src ; "%appdata%"
.text:004011C2	call	ds:ExpandEnvironmentStringsA
.text:004011C8	mov	edi, ds:lstrcatA
.text:004011CE	lea	eax, [ebp+Dst]
.text:004011D4	push	eax ; 1pString2
.text:004011D5	lea	eax, [ebp+String1]
.text:004011DB	push	eax ; lpString1
.text:004011DC	call	edi ; lstrcatA
.text:004011DE	push	offset String2 ; "\\IISWebClient"
.text:004011E3	lea	eax, [ebp+String1]
.text:004011E9	push	eax ; lpString1
.text:004011EA	call	edi ; lstrcatA
.text:004011EC	push	ebx ; lpSecurityAttributes
.text:004011ED	lea	eax, [ebp+String1]
.text:004011F3	push	eax ; lpPathName
.text:004011F4	call	ds:CreateDirectoryA

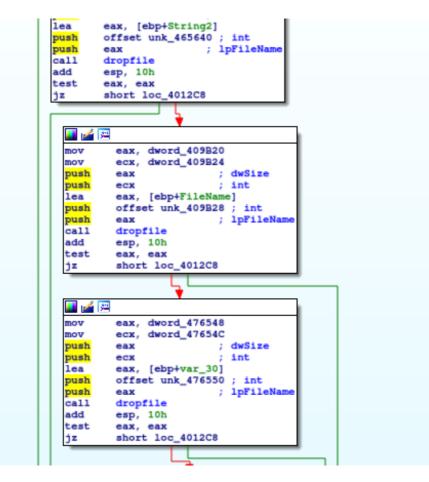
After, it decrypt a buffer in the address space of the executable with a xor.

		erry feebineerings?	
.text:00401223	push	eax ; lpF	athName
.text:00401224	call	ds:SetCurrentDirector	:yA
.text:0040122A	call	decrypt_loop	-

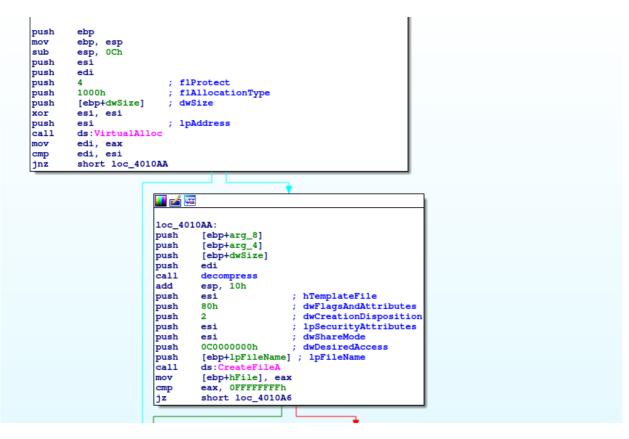


After the decoding, the PE decompresses and drops three files on the disk: iassvcs.exe developed and signed by Symantec, sqlite3.dll signed by the av 360 and RasTls.dll the backdoor.

The first step is to call dropfile

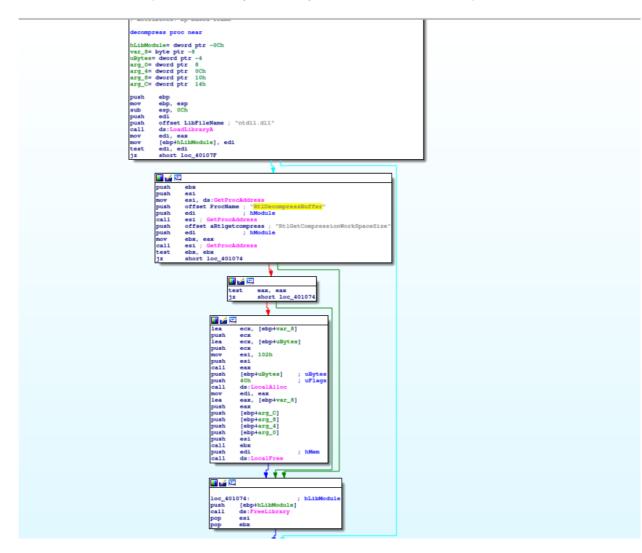


In this function the first step is to allocate at 0016000 a memory page and to decompress the file before writing on the disk.



push	edi
call	decompress
add	esp, 10h
push	esi ; hTemplateFile
push	80h ; dwFlagsAndAttributes
push	2 ; dwCreationDisposition
push	esi ; lpSecurityAttributes
push	esi ; dwShareMode
push	0C000000h ; dwDesiredAccess
push	[ebp+1pFileName] ; 1pFileName
call	ds:CreateFileA
mov	[ebp+hFile], eax
cmp	eax, 0FFFFFFFh
jz	short loc_4010A6
	mov eax, [ebp+dwSize]
	push ebx
	xor ebx, ebx
	<pre>mov [ebp+nNumberOfBytesToWrite], eax</pre>
	cmp eax, esi
	jbe short loc_40110F
	loc_4010E9: ; lpOverlapped
	push esi
	lea eax, [ebp+NumberOfBytesWritten]
	push eax ; 1pNumberOfBytesWritten
	<pre>push [ebp+nNumberOfBytesToWrite] ; nNumberOfBytesToWrite</pre>
	lea eax, [ebx+edi]
	push eax ; lpBuffer
	push [ebp+hFile] ; hFile
	call ds:WriteFile test eax, eax
	jz short loc_40112D

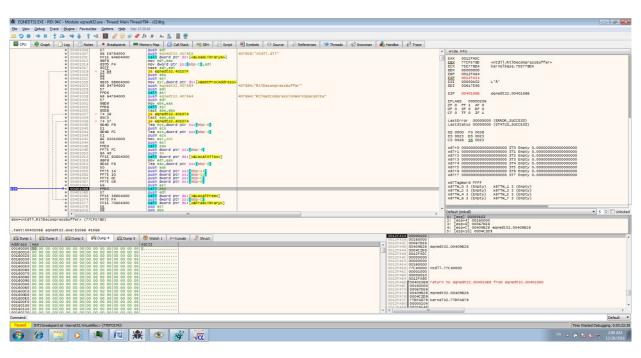
the function decompress loads dynamically the function RtIDecompressBuffer and use it.



In the debugger, theses steps are:

EQNEDT32.EXE - PID: 94C - Module: eqnedt32.exe - Thread				
View Debug Trace Plugins Favourites Options	Help Sep 13 2018			
		Symbols Source & References Threads & Snowman	La La La	
• 00401080 FF75 14	push dword ptr ss: [ebp+14]	Symbols Source & References Threads Showman		A Hide FPU
00401083 57 00401084 E8 47FF 00401089 83C4 10	FFFF call <eqnedt32.aboutmathtype></eqnedt32.aboutmathtype>			EAX 00000010
OO40108C 56 O040108D 68 8000	push est			EBX 00000000 ECX 77C9C74D ntdll.77C9C74D
e 004010C2 6A 02 e 004010C2 5A 02	push 2 push 2			EDX 77C40000 ntdll.77C40000 ESP 0012FA90
e 004010C5 56 e 004010C6 58 00000	push esi			ESP 0012FA6C FST 00000000
 004010CB FF75 08 004010CE FF15 14 	push dword ptr ss: ebo+5	[ebp+8]:"sqlite3.dll"		EDI 00160000
00401004 8945 F8 00401007 83F8 FF				EIP 00401089 eqnedt32.00401089
• 0040100A * 74 CA • 0040100C 8845 14	je egnedt32.4010A6 mov eax.dword ptr ss:[ebp+14]			EFLAG5 00000202 ZF 0 PF 0 AF 0
e 0040100F 53 e 004010E0 33DB e 004010E2 8945 FC	push ebx xor ebx,ebx mov dword ptr ss:[ebp-4],eax			OF 0 SF 0 DF 0 CF 0 TF 0 IF 1
004010E5 38C6	cmp eax,es1			Lasterror 00000000 (ERROR_SUCCESS)
	push esi lea eax,dword ptr ss:[ebp-C]			LastStatus 00000000 (STATUS_SUCCESS)
004010ED 50 004010EE FF75 FC	push eax push dword ptr ss: [ebp-4] lea eax,dword ptr ds:[ebx+edi]			GS 0000 FS 0038 ES 0023 DS 0023
e 004010F1 800438 e 004010F4 50	push eax			CS 0018 55 0023
004010F5 FF75 F8 004010F8 FF15 1C	504000 call dword ptr ds:[<swritefile>]</swritefile>			x87r0 000000000000000000 ST0 Empty 0.000000000000000000 x87r1 0000000000000000000 ST1 Empty 0.00000000000000000000000000000000000
004010FE 85C0 00401100 74 2B 00401102 8B45 F4	test eax, eax je eqnedt32,40112D mov eax, Aword ptr ss:[ebp-C]			x87r2 000000000000000000 ST2 Empty 0.00000000000000000 x87r3 00000000000000000 ST3 Empty 0.00000000000000000000000000000000000
2945 FC	sub dword ptr ss:[ebp-4],eax			x87r4 0000000000000000000 ST4 Empty 0.00000000000000000 x87r5 000000000000000000 ST5 Empty 0.0000000000000000000
00401108 0308 0040110A 3975 FC 00401100 77 DA	cmp dword ptr ss: ebp-4], esi			x87r6 00000000000000000 576 Empty 0.000000000000000000 x87r7 000000000000000000 ST7 Empty 0.0000000000000000000
e 0040110F FF75 F8	504000 call dword ptr ds: [calloseHandles]			x87Tagword FFFF
00401118 68 0080 00401110 <u>56</u>	00 <u>00</u> push 8000 push es1			x87TW_0 3 (Empty) x87TW_1 3 (Empty) x87TW_2 3 (Empty) x87TW_3 3 (Empty)
0040111E 5Z 0040111F FF15 18 00401125 53C0	504000 push edi call dword ptr ds:[<&VirtualFreex] xor eax,eax			x87TW_4 3 (Empty) x87TW_5 3 (Empty) x87TW_6 3 (Empty) x87TW_7 3 (Empty)
e 00401127 40 e 00401128 58	inc eax			
• 00401129 5F	000 ed1			Default (stdcal)
rd ptr [00406014 <eqnedt32.&createfilea>]=<</eqnedt32.&createfilea>	cernelsz.CreateFileA>			1: [esp+4] 00067DE8 2: [esp+8] 00409828 eqnedt32.00409828
xt:004010CE egnedt32.exe:\$10CE #10CE				3: [esp+C] 0004C2D9 4: [esp+10] 770FA879 <kernel32.lstrcat> 5: [esp+14] 00000104</kernel32.lstrcat>
Dump 1 8 Dump 2 8 Dump 3 8 Dump 4	🖽 Dump 5 🔗 Weatch 1 Istellionals 🛞 Struct		0012FA6C 00160000 0012FA70 00067DE8	[3. [csp+14] 0000104
Iress Hex	ASCII		 0012FA70 00067DE8 0012FA74 00409B28 eqner 0012FA78 0004C2D9 	dt32.00409628
60000 HD 5A 90 00 03 00 00 00 04 00 00 00 FI 60010 B5 00 00 00 00 00 00 00 00 40 00 00 00			0012FA7C 77DFA879 kern 0012FA80 00000104	el32.77DFA879
60020 00 00 00 00 00 00 00 00 00 00 00 00	0 00 00 00		0012FA84 0001A548 0012FA88 00000070	
60060 69 73 20 70 72 6F 67 72 61 60 20 63 62 60060 74 20 62 65 20 72 75 6E 20 69 65 20 4			0012FA8C 00000000 0012FA90 0012FF40	
			0012FA94 0040126C retur 0012FA98 0012FF00 "sql	rn to eqnedt32.0040126C from eqnedt32.00401085 ites.d]]"
60040 52 04 07 25 16 68 51 06 17 68 51 06 18 60 06 16 66 51 06 16 66 50 06 17 66 51 06 51 06 17 66 51 06 51 06 17 66 51 06 17 66 51 06 17 66 51 06 17 66 51 06 17 66 51 06 51	8 68 51 8C .w_N.kQMyt[N.kQN 5 68 51 8C vtUS.kQN.c.S.kQN		0012FA9C 00409B28 eqner 0012FAA0 0004C2D9 0012FAA4 00067DE8	dt32.00409828
60080 16 68 50 8C 54 68 51 8C 20 4D 58 8C 5 600C0 20 4D 5A 8C 15 68 51 8C D1 6D 57 8C 1	9 68 51 8C .kPATKOA M[AYKOA 7 68 51 8C NZA.KOARMA4.KOA		0012FAA4 00067DE8 0012FAA8 00000000 0012FAAC 00000000	
600E0 00 00 00 00 00 00 00 00 00 00 00 00	5 65 51 BC EKUN. KONKICH. KON		0012FAB0 7FFDD000	rn to ntdll.77C958D0 from ntdll.77C958DC
600F0 00 00 00 00 00 00 00 00 00 50 45 00 00 46 60100 68 8A 91 4C 00 00 00 00 00 00 00 00 00 00 8			0012FABS 00000440 0012FABC 00000458	
60110 08 01 06 00 00 30 05 00 00 20 01 00 00 60120 28 37 05 00 00 10 00 00 00 00 40 05 00 00	00 00 10 17 8		v <	
and: 				Defau Time Wasted Debugging: 0:0
	🗉 🌟 💿 💣 🛴 🗹			FR - (# 1% de 🙂 12000

CreateFile



Decompress

🗰 EQNEDT32.EXE - PID: 94C - Module: kerneB2.dll - Thread: Main Thread F94 - x32dbg	
File View Debug Trace Plugins Favourities Options Help Sep 13 2018	
S = S = I → E S → W → I S → A E Ø Ø ⊗ Ø A fx # A ₁ ≤ E E	
📓 CPU 🌻 Graph 🛛 Log 🖒 Notes 🔹 Brealipoints 🛲 Memory Nap 🚺 Call Stack 🧠 SBH 💿 Script 🐏 Symbols 🗢 Source 🔑 References 😒 Threads 😴 Snowman 📥 Handles 🕫 Trace	
Image: Construction Image: Construction	Initia F FM KK 0000001 KK Verofi base.7877700 KK KK 0000001 KK Verofi base.7877700 KK KK 0000001 KK Verofi base.7877700 KK KK 0000001 KK Verofi base.7877700 KK KK 0000000 KK Verofi base.7877700 KK KK 0000000 KK Verofi base.7877700 KK Lattery 0000000 KK Verofi base.2787700 KK Lattery 00000000 KK Verofi base.2787700 KK Lattery 00000000 KK Verofi base.2787700 KK Lattery 0000000000000 KK Verofi base.2787700 KK Lattery 000000000000000 KK Verofi base.2787700 KK Lattery 000000000000000000000000000000000000
ebp=00127A3C	1: [esp+4] 004010FE eqnedt32.004010FE 2: [esp+8] 00000070
.text:77605664 kernel32.dll:555654 #55654	3: [esp+C] 00160000 4: [esp+10] 0001A548
0012FA90	5: [esp+14] 0012FA84
Add/res Het Add/res Ad	ned132.00465640
Command:	Default 🔻
Paced Dump: 00160000 -> 00160000 (xx00000001 bytes)	Time Wasted Debugging: 0:00:11:05
🚯 😥 🚆 🔍 🖳 🛣 👁 💕 📆	FR - 🔐 🔀 地 🙂 1:37 AM 12/28/2018

Write the buffer on the disk after decompressing

🚱 🕞 👻 🐌 Computer → Windows7 (C:) → Users → IEUser → AppData → Roaming → IISWebClient									
Organize 👻 Include in	library - Share with - New fol	der							
4 🚖 Favorites	Name	Date modified	Туре	Size					
🧮 Desktop	😗 iassvcs.exe	12/28/2018 1:38 AM	Application	106 KB					
😹 Downloads	🚳 RasTIs.dll	12/28/2018 2:54 AM	Application extens	18 KB					
Recent Places	sqlite3.dll	12/28/2018 2:54 AM	Application extens	416 KB					

And the dropper execute the iassvcs.exe to make a side loading and make the persistence.

M Registry Editor			
File Edit View Favorites Help			
Speech SQMClient	^ Name	Туре	Dete
5 JystemCertificates	(Default)	REG_SZ	(value not set)
WAB	M DebugOptions	REG_SZ	2048
Web Service Providers	evice 🚵	REG_SZ	Microsoft XPS Document Writer, winspool, Ne00:
Þ 🍶 wfs	A Documents	REG_SZ	
> Windows	and DosPrint	REG_SZ	no
> - Windows Mail	🚵 Load	REG_SZ	C:\Users\IEUser\AppData\Roaming\IIISWEB-1\iassvcs.exe
Windows Media	📣 NetMessage	REG_SZ	no
Windows NT	MullPort 👏	REG_SZ	None
- CurrentVersion	Programs	REG_SZ	com exe bat pif cmd
AppCompatFlags	UserSelectedDef.	_ REG_DWORD	0-0000000 (0)
Devices			
DEFS			
MsiCorruptedFileRecovery			
Network			
- B PeerNet			
TaskManager			
Windows Script			
Windows Script Host			
Windows Search			
Windows Sidebar			
b 🍶 Wisp			
Netscape			
DOBC			
Policies			
>			
>			
System System Volatile Environment			
A B HKEY_LOCAL_MACHINE			
> BCD0000000			
HARDWARE			
SAM			
SECURITY			
SOFTWARE			
ATI Technologies			
> Classes			
D- Clients			
Cygnus Solutions			
Cygwin			
👂 🏭 Intel			
Microsoft			
DOBC	-		
Computer\HKEY_CURRENT_USER\Software\Microsoft\Windo	ws NT\CurrentVersion\Wind		
📀 ∂ 📇 💽 🗶 🛙	🖭 🇶 💿	💣 🖡	77 - (P 10 4. 10 308 AM 01
	- 7K 🔍		

at each executable or cmd line, the executable is reloaded.

囊 EQNEDT32.EXE - PID: 94C - Module eqnedb2.exe - Thread: Main Thread F94 - x32dbg	- \$ -							
File View Debug Trace Plugne Fevourities Options Help Sep 13.2018								
Image: Construction								
00401291 85C0 Test eax, eax								
All Store Figs Store Figs Store Image: Store	0 0 0 0 0							
0001312 C74F # \$480000 mov dhord ptr :sifest@:distance 0001312 C74F # \$48000 mov dhord 0001312 C	▼ 5 🔄 🗍 Unlocked							
4 m , Detrad (uda)	• 5 💽 🗋 Unlocked							
dword ptr [0040632 <equed132.46he]1xxcutetxa> 21 epsia 0000000 21 epsia 0000000 21 epsia 0000000</equed132.46he]1xxcutetxa>								
.text:00401333 eqned132.exe:1313 #1313 # [*69-C] 70700000 5 [*69-V] 70700000								
I blow I blow<	, v Joefsuk v							
Paced [Int] Breeligionit at deerel32.GenetFiel/by (720FEAE5) Tree Wasted Debugging: 0.00.455.35								
	# 😼 🌜 🙄 3:02 AM							

In a second part, I'll analysed the backdoor.

Threat Intelligence

the backdoor contacts hxxps://skylineqaz.crabdance.com/

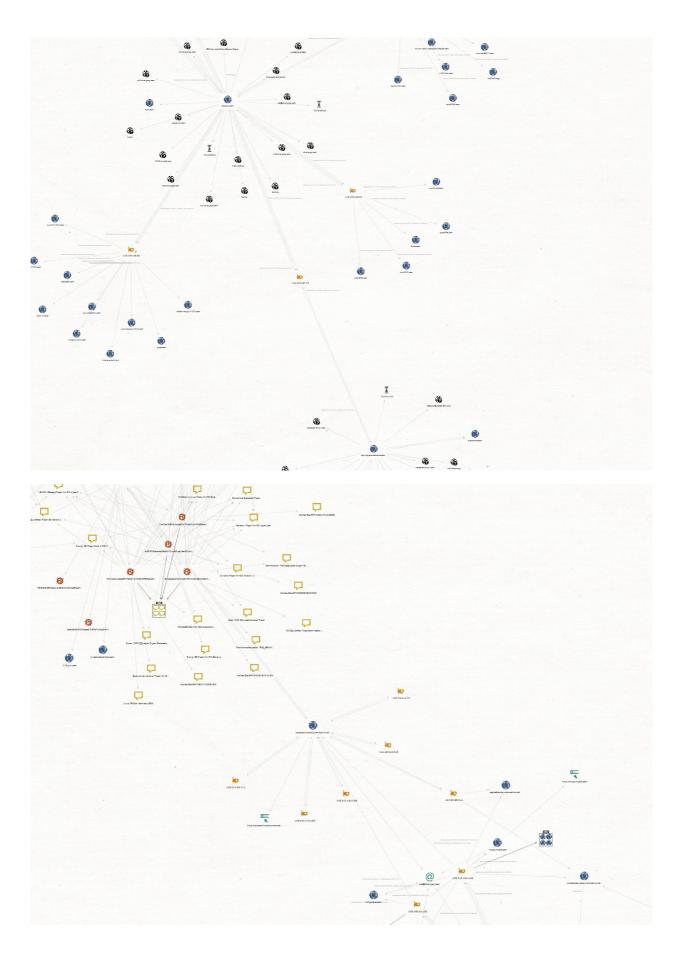
the domain resolves 154.223.167.20. This IP is very interesting because it connects with tele.zyns.com and old infrastructures used by chinese APT or DDOS Chinese team against the ancient soviet republics.

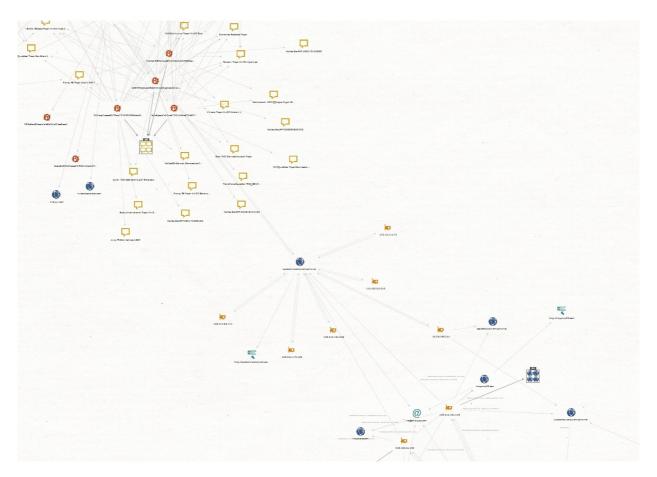
Also, the name of domains show the targets is energy and telecom sectors.

they find uzwatersource.dynamic-dns.net used by Icefog connected by the 150.129.80.184 to tele.zyns.com

uzwatersource.dynamic-dns.net connects to tajikstantravel.dynamic-dns.net by 45.252.63.244.

The domain tajikstantravel.dynamic-dns.net connected to ddos infrastructure chinese.





Another thing is the dropper what has submitted by an ID coming of the Kazakhstan. So Goblin Panda targets it ?

IOCs

the dropper:

dropper "c580d77722d85238ed76689a17b0205b4d980c010bef9616b8611ffba21b142e" sha256 c580d77722d85238ed76689a17b0205b4d980c010bef9616b8611ffba21b142e sha1 398fb04ce9b2e30bce932590e0b86b594c8a97ea md5 30528dc0c1e123dff51f40301cc03204 Dropped executable file sha256 C:\Users\admin\AppData\Roaming\IISWebClient\RasTIs.dll eb0b848f18d8002aaf59faca18b28941df67dc46891868b96fa4daf03018d148 sha256 C:\Users\admin\AppData\Roaming\IISWebClient\iassvcs.exe f9ebf6aeb3f0fb0c29bd8f3d652476cd1fe8bd9a0c11cb15c43de33bbce0bf68 sha256 C:\Users\admin\AppData\Roaming\IISWebClient\sglite3.dll e342eefb43249a3a1b62b8622f7c94fc391c0488bdae7e1909e37cb125029f1c **DNS** requests domain skylinegaz.crabdance.com domain xn-ylineqaz-y25ja.crabdance.com Connections ip 154.223.167.20 HTTP/HTTPS requests url https://skylineqaz.crabdance.com/

tele.zyns.com 103.242.134.146 150.129.80.184 (Goblin Panda, Icefog)