medium.com /walmartglobaltech/diavol-resurfaces-91dd93c7d922

Diavol resurfaces

Jason Reaves :: 9/30/2022

By: Jason Reaves and Jonathan McCay



We previously walked through the Diavol ransomware variants file encryption[1] which has been linked to the TrickBot group[2]. After the recent breakup[3,4], Diavol all but seemed to have disappeared. Curiously, we began to notice an uptick in samples submitted to VirusTotal. While investigating the more recent samples, we were able to determine that it uses a mix of RSA encryption and XOR encoding for files. In some instances, file recovery is still possible.

The following samples were identified on VirusTotal:

```
SHA256: aac969e36686f8f8517c111d30f8fb3b527988ebd31b3b762aec8d46e860eb9d
Creation Time 2022-09-05 20:01:56 UTC
First Submission 2022-09-09 21:06:06 UTC
Last Submission 2022-09-13 15:50:00 UTC
Last Analysis 2022-09-13 15:50:00 UTC
```

SHA256: fb5ee29b98446d34520bf04a82996eefec3b5692710c5631458da63ef7e44fe4 Creation Time 2022-09-05 20:04:30 UTC First Submission 2022-09-11 20:30:20 UTC Last Submission 2022-09-11 20:30:20 UTC Last Analysis 2022-09-11 20:30:20 UTC

SHA256: 708806f5e2e8bfa3dle911e391ff2ccf1edcac05cc1df80439b8b867253423dfCreation Time 2022-08-25 16:12:58 UTCFirst Submission 2022-08-29 19:49:08 UTC Last Submission 2022-09-03 15:40:44 UTC Last Analysis 2022-09-03 15:40:44 UTC

The samples are now 64 bit but function similarly. For the purposes of this report we will be going through the 7088 sample above. For the purposes of this report, we will be going through the 7088 sample above.

group=testfile_ext=.bullynote_filename=WARNING.txt

File encryption still involves the use of a 2048 byte XOR key which is randomly generated in the GENBOTID piece of the main bot. The key is then stored in the main bot and reused later in the file encryption code. Then a loop will sit reading chunks of 2048 bytes unless the amount of data to be encoded is less than 2048:

The first part of the file encryption is the aforementioned usage of the 2048 byte XOR key. For most files, the amount of bytes that will be XOR encoded is based on the overall file size divided by 10. Then a loop will sit reading chunks of 2048 bytes unless the amount of data to be encoded is less than 2048:



A similar XOR loop has been implemented, which can be seen in the previous version of Diavol[1]. The loop will handle XOR encoding the chunk of data that was read before writing it back to the file:

	💵 🗹 🖭					
loc 310:						
	mov e	ax. Erso	+168h+var 881			
	CMD [rsp+168h	+var 881. rax			
inb short loc 379						
	•		•			
🔲 ⊿ 🖼) 🚺 🔏 🕻				
mou	rax $[rax+20h]$	1 nc 37	70 -			
mou	r_{CX} , [r_{SD+168b+uar 88]	mou_01	rax. [rsn+168h+uar_A0]			
mouzx	eax, bute ptr [rax+rcx]	mov	rcx. [rsp+168h+var 98]			
mov	rcx. [rsp+168h+var 881	sub	rcx. rax			
mov	rdx, [rsp+168h+var_B0]	mov	v rax. rcx			
add	rdx, rcx	mov	mov [rsp+168h+var 110], rax			
mov	rcx, rdx	xor r9d, r9d				
movzx	ecx, byte ptr [rcx]	xor	xor r8d, r8d			
xor	ecx, eax	mov	mov rdx, [rsp+168h+var_110]			
mov	eax, ecx	mov rcx, [rsp+168h+var 118]				
mov	rcx, [rsp+168h+var_88]	call	all large qword ptr cs:8DDh ; SetFilePointerEx			
mov	rdx, [rsp+168h+var_B0]	mov	nov [rsp+168h+var_90], 0			
add	rdx, rcx	mov	[rsp+168h+var_148], 0			
mov	rcx, rdx	lea	a r9, [rsp+168h+var_90]			
mov	[rcx], al	mov	mov r8d, [rsp+168h+var_B8]			
jmp	short loc_309	mov	iov rdx, [rsp+168h+var_B0]			
		mov	rcx, [rsp+168h+var_118]			
		call	large qword ptr cs:8FDh ; WriteFile			
		mov	eax, [rsp+168h+var_B8]			
		mov	rcx, [rsp+168h+var_A0]			
		sub	rcx, rax			
		mov	rax, rcx			
		mov	[rsp+168h+var_A0], rax			
		jmp	1oc_28C			

After XOR encoding the file, the RSA encrypted XOR key is written to the end of the file followed by the number of encoded bytes:

```
[rsp+168h+var_148], 0
r9, [rsp+168h+var_48]
r8d, 900h
rax, [rsp+168h+var_100]
rdx, [rax+28h] ; Encrypted XOR key
rcx, [rsp+168h+var_118]
large qword ptr cs:8FDh ; WriteFile
[rsp+168h+var_148], 0
r9, [rsp+168h+var_48]
r8d, 8
rdx, [rsp+168h+var 981 ; enceded but

mov
lea
mov
mov
mov
mov
call
mov
lea
mou
                          r80, 8
rdx, [rsp+168h+var_98] ; encoded bytes
rcx, [rsp+168h+var_118]
large qword ptr cs:8FDh ; WriteFile
[rsp+168h+var_80], 0
lea
mov
call
mov
jmp
                           short loc_4BC
```

Next the bot single XOR encodes the number of encoded bytes and writes that to the end of the file:



After XOR encoding and writing the appropriate data to the end of the file, the bot goes back to the beginning of the file and begins reading in chunks of 0x75 bytes. It will RSA encrypt them and the encrypted bytes are then written back to the file but without the padding bytes. In this way, 0x75 * 10 or 1170 bytes at the beginning of the file will be RSA encrypted after getting XOR encoded.

	cmp [rsp+168h+var_60], 0Ah		
	jge loc_7	10	
🔲 🄏 📴			
mou	eav [rcn+168h+uar 68]	-1	
imul	cax, [isp://oon/var_00]	- 1	100 710
cdae	eax, 750	- 1	100_710.
DOU	[PCD+1695+U3P 118] P3V	- 1	yor ody ody
NOR	20d 20d	- 1	mou rev [rep+169b]
NOF	r9d r9d	- 1	coll lorge gword of
mou	rdy [rcn+168h+uar 110]	- 1	cmp [rsp+168b+uar
mou	rev [rep+168h+uar 118]	- 1	iz short loc 745
call	large gword ofr cs:800b · SetEilePointer	E V	Jz 50010 100_745
mou	Fren+168h+uar 1/81 0	-	
100	r0 [rcn+168b+uar 78]	- 1	
Tea	r9, [r5p+1001+var_r0]	- 1	
mou	rou, 750 , u	- 1	
mou	rev [rep+168h+uar 118]	- 1	
ep11	large gword ofr cc.9555 - PoadEile	- 1	
DOU	dword ptr Except60bruce 1201 - 00b - 101	- 1	
102	$uworu per [rsp+100n+var_100], 00n , g$	- 1	
TEG	Tax, [TSP+100H+Var_70] [MCD+16054H2M 100] M2M	- 1	
mou	[[S]+100 *Vdr_140], rdx	- 1	
mou	rax, [rsp+1000+var_00]	- 1	
NOV	[[Sp+100 +Var_140], rax	- 1	
XUP	ryu, ryu w0d d	- 1	
1100	rou, i	- 1	
XUP	eux, eux	- 1	
0011	TCX, [rsp+100H+Var_70]	- 1	
	Targe quoru per es:9000 ; eryptenerypt	- 1	
100	eax, [rsp+1000+var_00]	- 1	
1001	eax, 750	- 1	
cuye	Feca-1605-024 1101 424		
NON	[[SPT100170dF_110], FdX		
XUF	гуц, гуц 40d - 40d	- 1	
AUF DOU	rou, rou edu [ecol160bluce 110]		
mov	rux, [rsp*100 *Vdr_110]		
000	lawan awawd atw ac:000b : SatEilaDaistaw	. I	
COLL	Terpet460bauge 1001 0	C X	
102	[[SPT10017VdF_140], 0 M0 [Mcp+160b+upm 70]		
TEG	ry, [rsp+1000+var_70]		
MOV BOU	rou, 770 ; U Mdy Fycoul605000 601		
MOV BOU	rux, [rsp+100 *Vdr_00]	- 1	
0.011	lawaa awawd atw ac.950b , WwitaFila		
LGII	Targe yworu pir US:0rDH ; WriteFile		
MOV BOU	[[SP+1000+VdF_110], 0		
NUV	ryu, z	- 1	

A quick test can be performed to validate our findings, using a file of NULLs and a large MSI file. First, we validate the end data that was added to the file, which should be 110+0x900+16 bytes from the end:

>>> data = open('test_data.txt.bully', 'rb').read()>>> 110+0x900+16 2430>>> end =
data[-2430:]

Skipping over the RSA encrypted XOR key should show the two 8 byte values with the second being XOR encoded with 0xFF

>>>

Since the file is NULLs, the clear XOR key should be the first 2048 bytes after we skip over the 1170 RSA encrypted bytes at the beginning:

>>> key = bytearray(data[1170:1170+2048])

We can test this against another file, in this case an MSI:

So it is possible to recover most of each file trivially, after you recover the XOR key. The next step is to just rebuild the first 1170 bytes.

IOCs

Endpoint:

WARNING.txtwarning.txt.bully4eb5bea255c0308b296f5aa259f6862688b41ba2d6b7cca40118de9007cf64a0e5cc9710aacs

Ransom Note:

You've been hacked. All your corporate network servers and workstations are encrypted.Your company is a victim of double extortion ransomware attack.\rhat is it? Basically it means that not only your data is encrypted, but it's also have been exfiltrated from your network.Double Extortion attack explained in details :https://www.zscaler.com/resources/security-terms-glossary/what-is-double-extortionransomware\r=== What now? =====If you want your network to be fully operational again and if you want us not to publish all files we've taken :1. Download Tor Browser from original site : https://torproject.org\r. Open this url in Tor Browser and visit this website : https://Typnbv3snejqmgce4kbewwym4cm5j6lkzf2hra2hyhtsvwjaxwipkyd.onion/\r. Enter this key : 57C0E-4C543-DCABB-EBF0C-2EDCA-A9FC4If you've done everything correctly - now you are able to contact us and take a chance to leave this all behind for a reasonable fee.\rOTE : If TOR network is unavailable by any reason - you can use any VPN service to solve it.

Network:

hxxps://7ypnbv3snejqmgce4kbewwvym4cm5j6lkzf2hra2hyhtsvwjaxwipkyd[.]onion173.232[.]146[.]118

References

1: https://medium.com/walmartglobaltech/diavol-the-enigma-of-ransomware-1fd78ffda648

2: https://www.bleepingcomputer.com/news/security/fbi-links-diavol-ransomware-to-the-trickbot-cybercrime-group/

3: https://www.advintel.io/post/the-trickbot-saga-s-finale-has-aired-but-a-spinoff-is-already-in-the-works

4: https://www.bleepingcomputer.com/news/security/conti-ransomware-shuts-down-operation-rebrands-into-smallerunits/