blackhat USA 2016

JULY 30 - AUGUST 4, 2016 / MANDALAY BAY / LAS VEGAS

Cunning with CNG: Soliciting Secrets from Schannel

"Black Hat Sound Bytes"

What you get out of this talk

□ Ability to decrypt Schannel TLS connections that use ephemeral key exchanges

Ability to decrypt and extract private certificate and session ticket key directly from memory

Public Cert/SNI to PID/Logon Session Mapping



Agenda

- □ A very short SSL/TLS Review
- □ A background on Schannel & CNG
- The Secret Data
- The Forensic Context
- Demo >.>

\Lambda black hat usa 2016

Disclaimer

This is NOT an exploit

- □ It's just the spec :D
- $\hfill\square$...and some implementation specific oddities

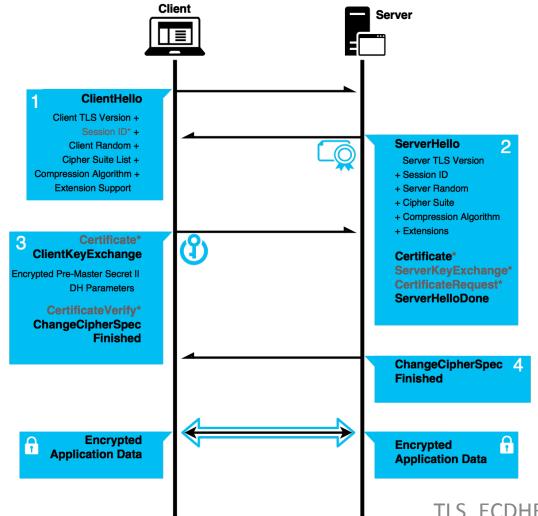
□ Microsoft has done nothing [especially] wrong

- □ To the contrary, their documentation was actually pretty great
- □ Windows doesn't track sessions for processes that load their own TLS libs
 - □ I'm looking at you Firefox and Chrome
- □ Windows doesn't track sessions for process that don't use TLS...
 - □ That'd be you TeamViewer...

Background

TLS, Schannel, and CNG

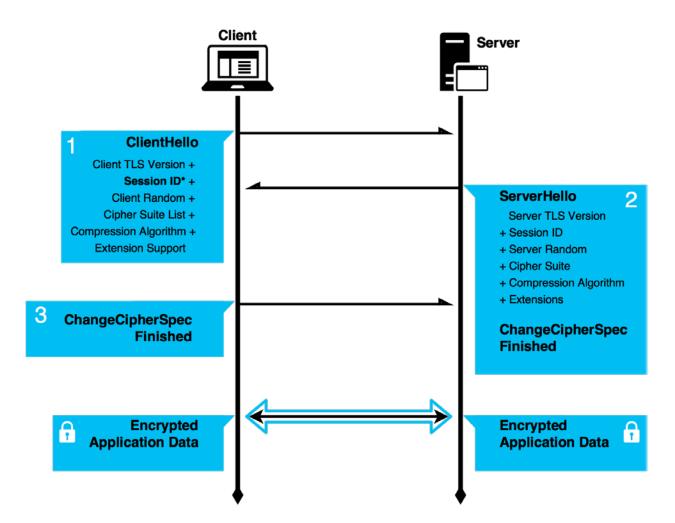
The infamous TLS Handshake



Initial Connection

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

The infamous TL&DR; Handshake



Session Resumption

Perfect Forward Secrecy

What we want to do

□ One time use keys, no sending secrets!

What TLS actually does

- □ Caches values to enable resumption
 - recommends `An upper limit of 24 hours is suggested for session ID lifetimes`
- □ When using session ticket extension, sends the encrypted state over the network
 - □ basically returning to the issue with RSA, but using a more ephemeral key...

What implementations *also* do

- □ Store symmetric key schedules (so you can find the otherwise random keys...)
- □ Cache ephemeral keys and reuse for a while...

\Lambda black hat usa 2016

Schannel & CNG

Secure Channel

- □ It's TLS -> the <u>Secure Channel</u> for Windows!
- A library that gets loaded into the "key isolation process" and the "client" process
 - □ Technically a Security Support Provider (SSP)

Spoiler: the Key Isolation process is LSASS

The CryptoAPI-Next Generation (CNG)

- □ Introduced in Vista (yes you read correctly)
- Provides Common Criteria compliance
- □ Used to store secrets and 'crypt them
 - □ Storage via the Key Storage Providers (KSPs)
 - Generic data encryption via DPAPI
 - Also brings modern ciphers to Windows (AES for example) and ECC
- Importantly, ncrypt gets called out as the "key storage router" and gateway to the CNG Key Isolation service

Schannel Prefered Cipher Suites

Administrator: C:\Windows\System32\cmd.exe	Administrator: C:\Windows\system32\cmd.exe	📾 Administrator: Command Prompt - powershell – 🗆 🗙
Microsoft Windows [Version 6.0.6002] Copyright <c> 2006 Microsoft Corporation. All rights reserved.</c>	Microsoft Windows [Version 6.1.7601] Copyright (c) 2009 Microsoft Corporation. All rights reserved.	Microsoft Windows [Version 10.0.10586] ^ (c) 2015 Microsoft Corporation. All rights reserved.
C:\Windows\system32>\Temp\ListCipherSuites.exe	C:\Windows\system32>\Temp\ListCipherSuites.exe	C:\Windows\system32>powershell
Sample Code from: https://msdn.microsoft.com/en-us/library/windo		Windows PowerShell
930.aspx	Sample Code from: https://msdn.microsoft.com/en-us/library/windo	Copyright (C) 2015 Microsoft Corporation. All rights reserved.
Listing Cipher Suites TLS RSA WITH AES 128 CBC SHA	930.aspx	
TLS_RSA_WITH_HES_T28_CBC_SHA	Listing Cipher Suites	PS C:\Windows\system32> \$(Get-TlsCipherSuite).Name
TLS_RSA_WITH_RC4_128_SHA TLS_RSA_WITH_3DES_EDE_CBC_SHA	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P256	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P256	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P384 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P521	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P384 TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P521	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P256	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P256	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P384	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P384 TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P521	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P521 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P256	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P284	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P521	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P521	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P256	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P384 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P521	TLS_ECDHE_RSH_WITH_HES_128_CBC_SHA_P304 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P521	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_DHE_DSS_WITH_AES_128_CBC_SHA TLS_DHE_DSS_WITH_AES_256_CBC_SHA	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
TLS_DHE_DSS_WITH_HES_Z56_CBC_SHH TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_RC4_128_MD5 SSL_CK_RC4_128_WITH_MD5	TLS_RSA_WITH_AES_256_GCM_SHA384 TLS_RSA_WITH_AES_128_GCM_SHA256	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
SSL_CK_DES_192_EDE3_CBC_WITH_MD5	TLS_RSA_WITH_AES_256_CBC_SHA256	TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_NULL_MD5 TLS_RSA_WITH_NULL_SHA Windows_Vista		TLS_DHE_RSA_WITH_AES_128_CBC_SHA
C:\lindous\sustam32\	TLS_RSA_WITH_AES_256_CBC_SHA	TLS_RSA_WITH_AES_256_GCM_SHA384
· · · · · · · · · · · · · · · · · · ·	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384_P384	TLS_RSA_WITH_AES_128_GCM_SHA256
	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384_P521 Windows 7	TLS_RSA_WITH_AES_256_CBC_SHA256
	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_P256	TLS_RSA_WITH_AES_128_CBC_SHA256
		TLS_RSA_WITH_AES_256_CBC_SHA
		TLS_RSA_WITH_AES_128_CBC_SHA

TLS RSA WITH 3DES EDE CBC SHA

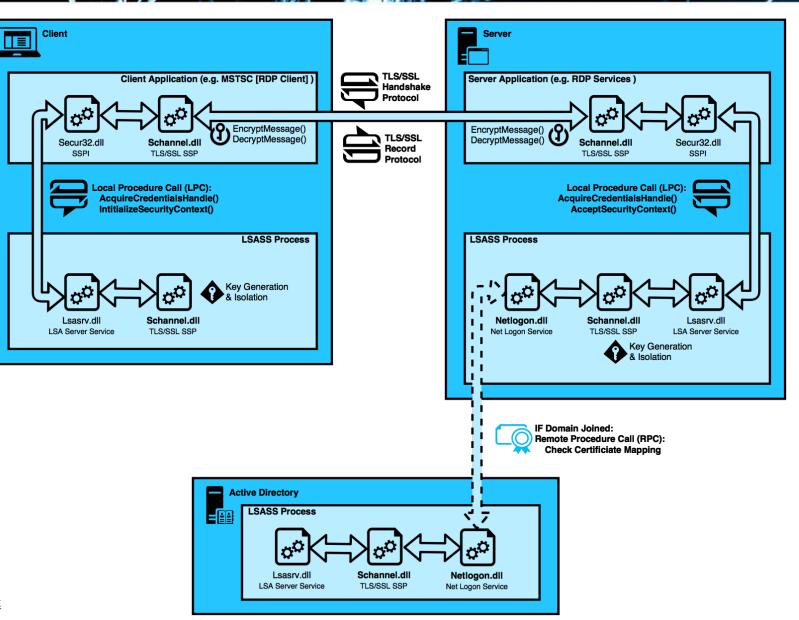
TLS_DHE_DSS_WITH_AES_256_CBC_SHA256

Windows 10

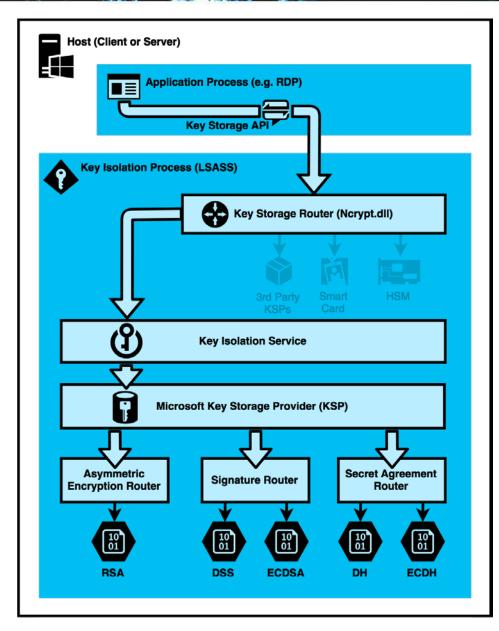
Microsoft's TLS/SSL Docs

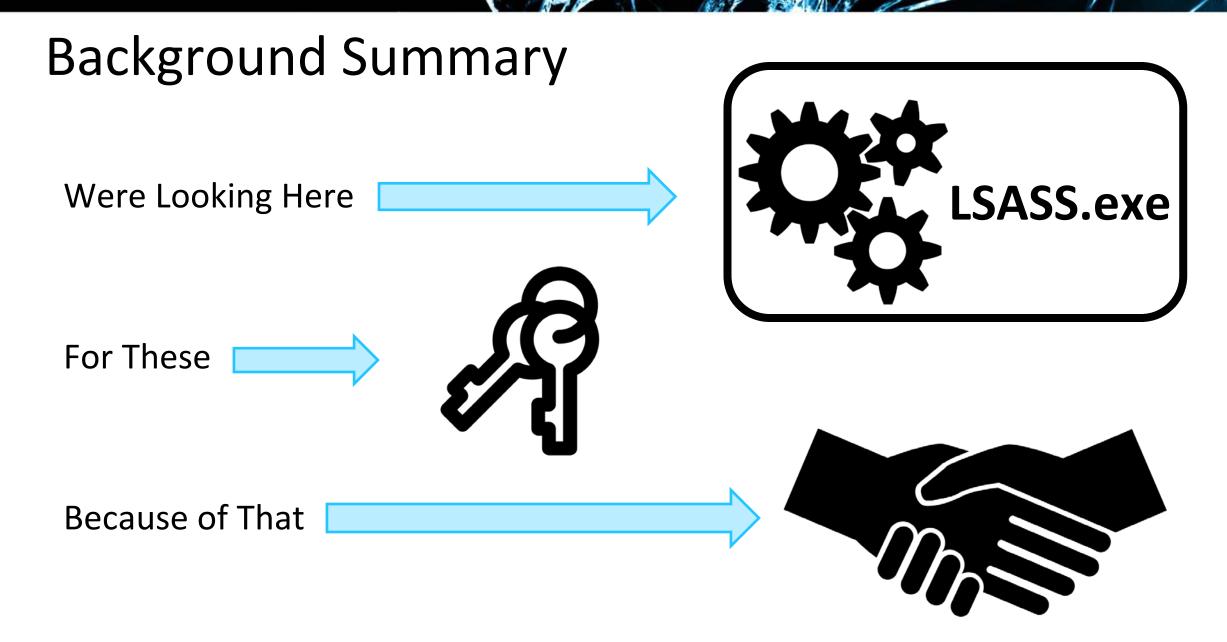
- □ ClientCacheTime: "The first time a client connects to a server through the Schannel SSP, a full TLS/SSL handshake is performed."
- When this is complete, the master secret, cipher suite, and certificates are stored in the session cache on the respective client and server."*
- ServerCacheTime: "...Increasing ServerCacheTime above the default values causes Lsass.exe to consume additional memory. Each session cache element typically requires 2 to 4 KB of memory"*
- □ MaximumCacheSize: "This entry controls the maximum number of cache elements. [...] The default value is 20,000 elements." *

Schannel Ops



CNG Key Isolation





What are we trying to accomplish?



We want to be able to see data that has been protected with TLS/SSL and subvert efforts at implementing Perfect Forward Secrecy



We want to gather any contextual information that we can use for forensic purposes, regardless of whether or not we can accomplish the above

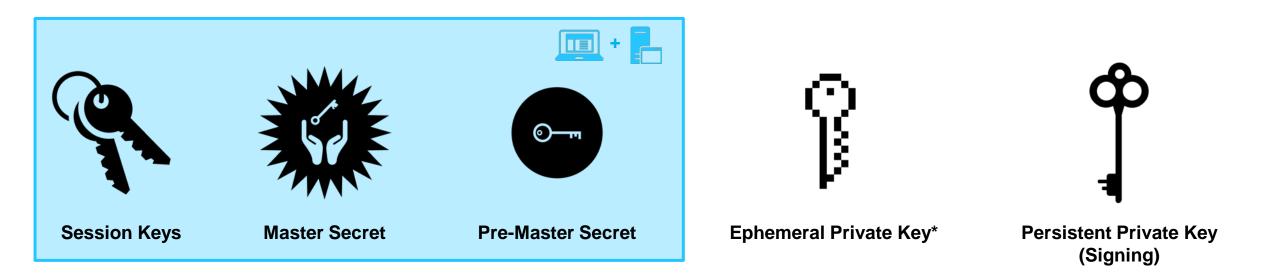


We (as an adversary) want to be able to get access to a single process address space and be able to dump out things that would enable us to monitor/modify future traffic, or possibly impersonate the target

□ We want to do this without touching disk

Secrets

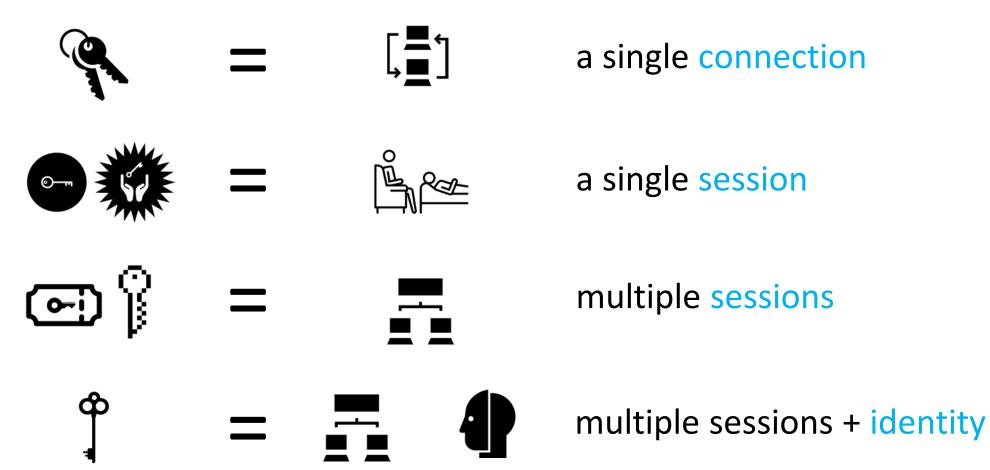
The Keys



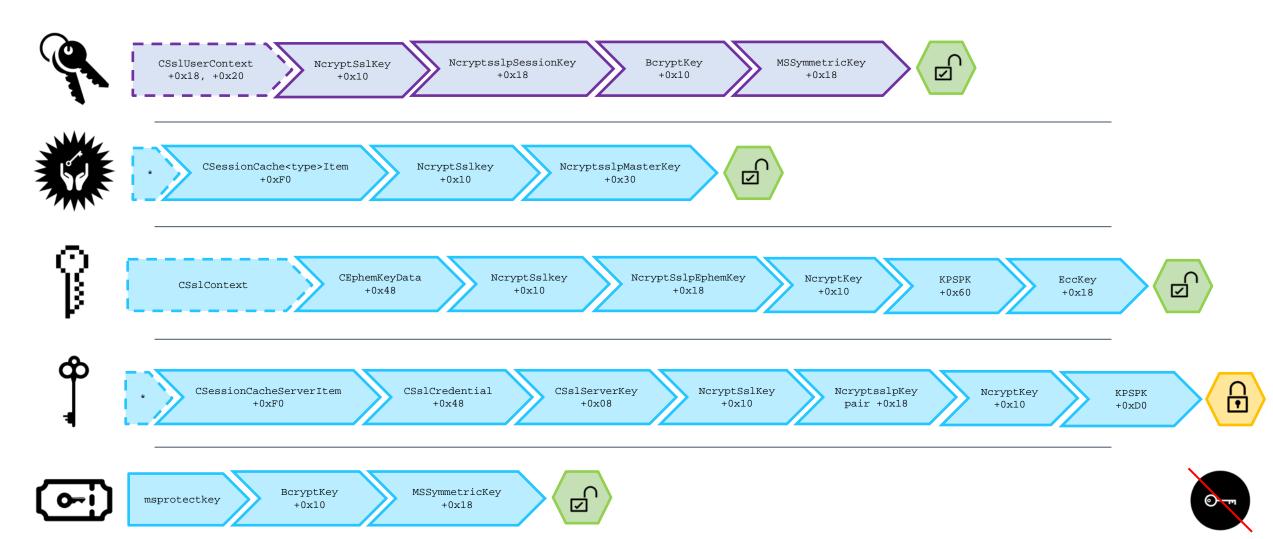


Session Ticket Key*

The Keys? What do they get us?



The Keys? We got 'em...<u>all</u>.



Session Keys

- □ Smallest scope / most ephemeral
- **□** Required for symmetric encrypted comms
- □ Not going to be encrypted

Approach Premise:

- **Given Start with AES**
- □ AES keys are relatively small and pseudo-random
- AES key schedules are larger and deterministic
 - □ ... they are a "schedule" after all.
- □ Key schedules usually calculated once and stored*
- Let's scan for matching key schedules on both hosts

C:\Windows\system32\cmd.exe	-			×	
C:\TMP>findaes.exe rdp_mstsc.DMP					,
Searching rdp mstsc.DMP					
Found AES-256 key schedule at offset 0x3158ac:					
b9 f0 65 ef 0a 27 33 62 0d 92 3d 2a 1e ba 24 3b 9a 1d 94 a8 70 d4 b5 ab 08 18 d6	f8 (d8 04	1d	07	
Found AES-256 key schedule at offset 0x3162ac:					
b9 f0 65 ef 0a 27 33 62 0d 92 3d 2a 1e ba 24 3b 9a 1d 94 a8 70 d4 b5 ab 08 18 d6	f8	d8 04	. 1d	07	
Found AES-256 key schedule at offset 0xcd71dc:					
08 57 03 03 d2 71 5c bb 23 b1 69 1d b8 9a 2a ea 00 83 13 78 75 a5 84 a3 0f 21 af	5d	5c 4b	8c	f9	
Found AES-256 key schedule at offset 0xcd7bdc:					
08 57 03 03 d2 71 5c bb 23 b1 69 1d b8 9a 2a ea 00 83 13 78 75 a5 84 a3 0f 21 af	5d	5c 4b	8c	f9	
Found AES-256 key schedule at offset 0xcfeadc:					
b0 75 6f 15 5c 70 a5 ec 8e 4c e3 c9 f3 b3 ff 33 80 04 ed 43 d4 a6 36 b7 6e 41 8f	aa	d f 6c	e1	b9	
Found AES-256 key schedule at offset 0xcff4dc:					
b0 75 6f 15 5c 70 a5 ec 8e 4c e3 c9 f3 b3 ff 33 80 04 ed 43 d4 a6 36 b7 6e 41 8f	aa	df 6c	e1	b9	
Found AES-256 key schedule at offset 0x171571c:					
da 37 46 b4 a7 db e9 f5 b6 7f 27 ea a2 d3 26 c6 cc 65 30 42 f1 68 74 bb fb f5 c9	ef (64 f7	30	9c	
Found AES-256 key schedule at offset 0x171611c:					
da 37 46 b4 a7 db e9 f5 b6 7f 27 ea a2 d3 26 c6 cc 65 30 42 f1 68 74 bb fb f5 c9	ef	64 f7	30	9c	
C:\TMP>_					

Select C:\Windows\system32\cmd.exe	_	
C:\TMP>findaes.exe rdp_svchost.DMP		
Searching rdp_svchost.DMP		
Found AES-256 key schedule at offset 0x9bd7f50:		
o9 f0 65 ef 0a 27 33 62 0d 92 3d 2a 1e ba 24 3b 9a 1d 94 a8 70 d4 b5 ab 08 18 d6 f8	d8 0	04 1d 07
Found AES-256 key schedule at offset 0x9c9b1c0:		
o0 75 6f 15 5c 70 a5 ec 8e 4c e3 c9 f3 b3 ff 33 80 04 ed 43 d4 a6 36 b7 6e 41 8f aa	df 6	ic e1 b9
Found AES-256 key schedule at offset 0x9c9bbc0:		
p0 75 6f 15 5c 70 a5 ec 8e 4c e3 c9 f3 b3 ff 33 80 04 ed 43 d4 a6 36 b7 6e 41 8f aa	df 6	ic e1 b9
Found AES-256 key schedule at offset 0x9c9bf00:		
da 37 46 b4 a7 db e9 f5 b6 7f 27 ea a2 d3 26 c6 cc 65 30 42 f1 68 74 bb fb f5 c9 ef	64 f	7 30 9c
Found AES-256 key schedule at offset 0x9c9c900:		
da 37 46 b4 a7 db e9 f5 b6 7f 27 ea a2 d3 26 c6 cc 65 30 42 f1 68 74 bb fb f5 c9 ef	64 f	7 30 9c
Found AES-256 key schedule at offset 0x9ca8740:		
o9 f0 65 ef 0a 27 33 62 0d 92 3d 2a 1e ba 24 3b 9a 1d 94 a8 70 d4 b5 ab 08 18 d6 f8	d8 0	94 1d 07
Found AES-256 key schedule at offset 0x9ca9140:		
o9 f0 65 ef 0a 27 33 62 0d 92 3d 2a 1e ba 24 3b 9a 1d 94 a8 70 d4 b5 ab 08 18 d6 f8	d8 0	04 1d 07
Found AES-256 key schedule at offset 0x9cb97b0:		
08 57 03 03 d2 71 5c bb 23 b1 69 1d b8 9a 2a ea 00 83 13 78 75 a5 84 a3 0f 21 af 5d	5c 4	b 8c f9
Found AES-256 key schedule at offset 0x9cba1b0:		
38 57 03 03 d2 71 5c bb 23 b1 69 1d b8 9a 2a ea 00 83 13 78 75 a5 84 a3 0f 21 af 5d	5c 4	lb 8c f9
C:\TMP>		

Session Keys

_SSL_SES	SION_KEY	
4	cbStructLength	
4	dwMagic ["ssl3"]	
4	dwProtocolVersion	
4/8	pvCipherSuiteListEntry	
4	IsWriteKey	
4/8	pvBcryptKeyStruct	
		I

				-						
	+		4	cbStructLength						
			4	dwMagic ["UUUR"]						
		4	1/8	pvBcryptProvider						
		4	1/8	pvBcryptSymmKey						
					•					
	ms	_SYMM	ETRIC_P	CEY						
4	4	4 4/8 4/8 4/8 4/8 4/8 4/8 4/8 4/8 4/8 4/8 4/8 4 4 4 4 4 4 4 4 4 4 7		uctLength						
	4		dwMag	ic ["MSSK"]						
	4		dwKey	Туре						
		•								
	4		KeyLe	ngth						
	?		Symme	tricKey						
	?		SymmK	eySchedule						

BCRYPT KEY HANDLE

▶ Command - Dump					\	_		×
	y {s -[1w]a 0 L?800	000000000000000000000000000000000000000) 31ss}){	.echo *	** Ses	sion Ke	y ***;dd	\${ ^
*** Session Key **								
000000e1`7b047050								
000000e1`7b047054				3lss				
000000e1`7b047058								
	00007ffe`6fc11910	ncryptss]	lp!Cipher	SuiteLi	st+0x1	400		
000000e1`7b047068								
000000e1`7b047070	000000e1`7b0470c0	55555552	00000cbe					
000000e1`7b0470c0	00000cbe							
000000e1`7b0470c4	55555552			RUUU				
000000e1`7b0470c8	000000e1`784e3af0	55555551	00000130					
000000e1`7b0470d0	000000e1`7b0470e0	4d53534b	00000c80					
000000e1`7b0470d8	00000000,00000000							
*								
000000e1`7b0470e0								
000000e1`7b0470e4				KSSM				
000000e1`7b0470e8		00000010	00000001					
000000e1`7b0470f8								
000000e1`7b047100		4d535341	00000028					
000000e1`7b047118	00000020							
* AES Key:							_	
	b0 75 6f 15 5c 70						L	
000000e1 7604712c	80 04 ed 43 d4 a6	36 b7-6e	41 81 aa	di 6c	el b9	c	6.nA1	•••
ttt Consist Vou tt	•							
*** Session Key **)00000e1`7b047d90								
000000e1 76047d90				3155				
000000e1 7b047d94				3122				
	00007ffe`6fc11910	ncrynteel	IntCipher	SuiteLi	st+0v1	400		
000000e1`7b047da8		nerypessi	rp.orpher	Durceni	SCTUAL	100		
000000e1`7b047db0		55555552	00000cbe					
*		0000002	000000000					
000000e1`7b047e00	00000cbe							
000000e1`7b047e04				RUUU				
000000e1`7b047e08		55555551	00000130					
000000e1`7b047e10								
000000e1`7b047e18								
*								
000000e1`7b047e20	00000c80							
000000e1`7b047e24	4d53534b			KSSM				
000000e1`7b047e28	00010002 00000005	00000010	00000001					
000000e1`7b047e38	00000100 00000001							
000000e1`7b047e40	000000e1`784e83c0	4d535341	00000028					
000000e1`7b047e58	00000020							
* AES Key:								
	da 37 46 b4 a7 db					.7F	'	δ.
000000e1`7b047e6c	cc 65 30 42 fl 68	74 bb-fb	f5 c9 ef	64 f7	30 9c	.eOB.h	td.	0. 🗸
<								>
):000> \${kev}+1C L	1;r @\$t0 = \$p;.echd	> *;dd @\$t	.0 L1;dc	@\$t0+4	L1;dpp	@\$t0+8	L1;dpp	0
	echo *;r \$t0 = \$p;c				- L. L.		r r	0.0
St0+10 L2;	echo ~;r ştu = şb;d	1α @Ştu LJ	l;dc @ŞtO	+4 L1;c	ld @\$t0	+8 L6;d	pp @\$t0+	20
	30+\$ptrsize L1;.ech							

CSslUserContext

The Ncrypt SSL Provider (ncryptsslp.dll)

Х

Ncryptsslp Validation function Symbols

Command - Dump \\vmware-host\Share	
0:000> x /1 ncryptsslp!*Validate*	
ncryptsslp!SslpValidateEphemeralHandle	
ncryptsslp!SslpValidateMasterKeyHandle	
ncryptsslp!SslpValidateProvHandle	
ncryptsslp!SslpValidateHashHandle	
ncryptsslp!SslpValidateKeyPairHandle	

0:000>

These functions do three things:

□ Check the first dword for a size value

Check the second dword for a magic ID

□ Return the passed handle* if all is good

Ncryptsslp Validation function Symbols

0:000> uf ncryptsslp!SslpValidate ncryptsslp!SslpValidateMasterKeyH		еунапоте
00007fff`df75b5b8 4885c9	test	rcx, rcx
00007fff`df75b5bb 7412	je	ncryptsslp!SslpValidateMasterKeyHandle+0x17
0000/111 01/36366 /412	Je	herypessip:ssipvaridateMasterkeyhandie+0xi/
ncryptsslp!SslpValidateMasterKeyH	andle+0	x5:
00007fff`df75b5bd 833950	cmp	dword ptr [rcx],50h
00007fff`df75b5c0 720d	jb	ncryptsslp!SslpValidateMasterKeyHandle+0x17
ncryptsslp!SslpValidateMasterKeyH	andle+0	xa:
00007fff`df75b5c2 817904356c7373	cmp	dword ptr [rcx+4],73736C35h
00007fff`df75b5c9 7504	jne	ncryptsslp!SslpValidateMasterKeyHandle+0x17
ncryptsslp!SslpValidateMasterKeyH	andle+0	x13:
00007fff`df75b5cb 488bc1	mov	rax, rcx
00007fff`df75b5ce c3	ret	
ncryptsslp!SslpValidateMasterKeyH	andle+0	x17:
00007fff`df75b5cf 33c0	xor	eax,eax
00007fff`df75b5d1 c3	ret	
<		>

The Ncrypt SSL Provider (ncryptsslp.dll)

SSL Magic	Size (x86)	Size (x64)	Validation Functions
ssl1	0xE4	0x130	SslpValidateProvHandle
ssl2	0x24	0x30	SslpValidateHashHandle
ssl3	?	?	<none></none>
ssl4	0x18	0x20	SslpValidate KeyPair Handle
ssl5	0x48	0x50	SslpValidate MasterKey Handle
ssl6	0x18	0x20	SslpValidate Ephemeral Handle
ssl7	?	?	<none></none>

ssl3 was already discussed, appears in the following functions:

TlsGenerateSessionKeys+0x251 SPSslDecryptPacket+0x43 SPSslEncryptPacket+0x43 SPSslImportKey+0x19a SPSslExportKey+0x76 Ssl2GenerateSessionKeys+0x22c

Pre-Master Secret (PMS)

- □ The 'ss17' struct appears to be used specifically for the RSA PMS
- □ As advised by the RFC, it gets destroyed quickly, once the Master Secret (MS) has been derived
- Client generates random data, populates the ssl7 structure, and encrypts
- In ECC the PMS is x-coordinate of the shared secret derived (which is a point on the curve), so this doesn't /seem/ to get used in that case

Functions where ssl7 appears:

ncryptsslp!SPSslGenerateMasterKey+0x75 ncryptsslp!SPSslGenerateMasterKey+0x5595 ncryptsslp!SPSslGeneratePreMasterKey+0x15e ncryptsslp!TlsDecryptMasterKey+0x6b

Bottom line:

It's vestigial for our purposes - it doesn't do anything another secret can't



Master Secret

- Basically the Holy Grail for a given connection
 - □ It always exists
 - □ It's what gets cached and used to derive the session keys
- Structure for storage is simple - secret is unencrypted (as you'd expect)
- This + Unique ID = decryption, natively in tools like wireshark

So...how do we get there?

_SSL_MAS	STER_SECRET
4	cbStructLength
4	dwMagic ["ssl5"]
4	dwProtocolVersion
0/4	dwUnknown1* [alignment?]
4/8	pCipherSuiteListEntry
4	bIsClientCache
48	rgbMasterSecret
4	dwUnknown2 [reserved?]

Master Secret

_SSL_MASTE	R_SECRET
4	cbStructLength
4	dwMagic ["ssl5"]
4	dwProtocolVersion
0/4	dwUnknown1* [alignment?]
4/8	pCipherSuiteListEntry
4	bIsClientCache
48	rgbMasterSecret
4	dwUnknown2 [reserved?]

Command - Dump	\vmware-l	nost∖Sh	ared F	older	s\Doci	ume	nts\(Chal	lenc	ges\z	zzTn	np\			×
0:000> .foreach(ms	{s -[1]c	1 0 L?	80000	0000	00000) 's	ssl5	' })	{.€	chc) **	· *Ra	w Master	Secret	***
***Raw Master Secre															
000000c9`86d9e980														s	
00000c9`86d9e990															
000000c9`86d9e9a0 000000c9`86d9e9b0	22 83 50 a7 73 8a													-	
000000c9`86d9e9c0	44 0d fa													g.E., .%.Q	
Parsed Master Se	ecret														
000000c9`86d9e980	00000050														- 1
000000c9`86d9e984	73736c35								51	SS					
000000c9`86d9e988 000000c9`86d9e990	00000000				mt a a	1-10	1. mh	0.000		т.:	a+ 1	01	500		
* Secret:	00007ff1 00000000		Ialu	псту	puss.	LD ! C	, thu	ler:	uru	.егт	SL4	-0X1	500		
000000c9`86d9e99c	01 7b 37	90 2	2 83	5c 7	18-ca	16	f7	12	53	00	39	fb	. {7.".)	xS.	9.
000000c9`86d9e9ac	5d ea do														
00000c9`86d9e9bc	01 a3 25													.LE%.	
00000c9`86d9e9cc	00000000)													
Raw Master Secre	et														
000000c9`86d9f080	50 00 00	00 3	5 <mark>6</mark> c	73 7	/3-03	03	00	00	00	00	00	00	P51s	s	
000000c9`86d9f090															
000000c9`86d9f0a0														/B3i	
00000c9`86d9f0b0	60 5e 46													q2 z.?\$k	
000000c9`86d9f0c0	4a b4 84	lai	a 12	/a 1	0-31	24	60	dD	00	00	00	00	J	2.?\$K	•••
-										,		1.00			
0:000> .foreach(ms Secret***;dk	\${ms}-4	Ldwo	(\${ms	s}-4)	;.ech	10 ; .	ech	0 *	**E	ars	sed	Mas	ter Seci	:et***;d	
\${ms}-4 L1;c L1;.echo * \$ L1;.echo}															
							_								
Command - Dump	\\vmware-	າost∖Sh	ared F	olde	rs\Doc	ume	nts\	Cha	llen	ges\	zzTr	np			Х
0:000> r @\$t0 = 000	000c9`8	5d9e98	0;dc	@\$t() L2;	dp	@\$t()+1() L	1;.0	ech	o *;	dpu poi	(@\$t0+1)) L2
000000c9`86d9e980	00000050								Ρ	•••	51s	S			
000000c9`86d9e990 *	00007ff:	E`df76	1a10												
00007fff`df761a10	0000c030	0000	0c00												

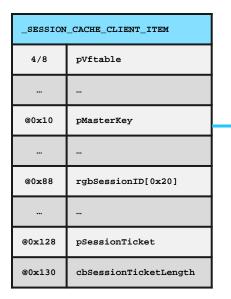
0:000>

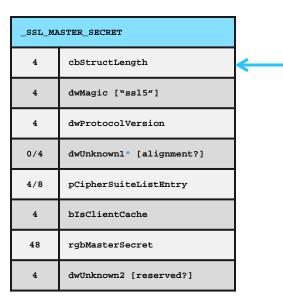


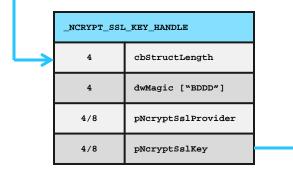
Master Secret Mapped to Unique Identifier

- The Master Key is linked back to a unique ID through an "NcryptSslKey"
- The NcryptSslKey is referenced by an "SessionCacheItem"
- The SessionCacheltem contains either the SessionID, or a pointer and length value for a SessionTicket
 - Instantiated as either client or server item

At this point, we can find cache items, and extract the Master Secret + Unique ID









Master Secret Mapped to Unique Identifier

Command - Dump				ost\	Shar	ed F	old	ers\Doci	ume	nts\	Cha	llen	ges\	_TS'	YS∖t			X
**** CLIENT CACHE	ITE	M * 1	* * *															^
* SessID *																		
000000d4`12bfdf28								ae-7a									.z.0>J5	
000000d4`12bfdf38	dc	a9	e8	39	eb	са	07	07-5b	1a	94	4d	8b	1b	71	f7	9	.[Mq.	
* Master Key *																		
000000d4`12b810fc								ea-db										
000000d4`12b8110c								fa-d0									K.d. <h< td=""><td></td></h<>	
000000d4`12b8111c	ce	db	9d	98	de	04	60	08-cd	e0	4a	40	97	79	5d	f2	`	J@.y].	
**** CLIENT CACHE	ITE	M *:	***															
* SessID *		_	_	_												_	_	
000000d4`12bfe098								cb-15									8 ı	
000000d4`12bfe0a8 Master Key *	le	d0	d5	39	57	89	01	dd-de	69	27	8d	bb	f9	73	8e	9W	i's.	
)00000d4`12b811fc	71	бa	1d	49	36	56	bf	53-4e	43	6f	fb	58	ff	2e	40	qj.16V.3	SNCo.X0	9
000000d4`12b8120c	00	05	16	b7	35	db	d5	df-af	f9	3f	37	b5	ac	90	ba	5	?7	
000000d4`12b8121c	1c	3a	25	ba	3e	15	05	b8-f3	aa	16	8a	65	7e	00	7b	.:%.>	e~.	I
**** CLIENT CACHE	ITE	M *:	* * *															
* Sess Ticket *																		
000000d4`12bda9f0	f8	0a	ee	e7	9a	1a	2f	64-1f	e7	9d	b6	da	af	8a	e1	/0	d	
* Master Key *																		
000000d4`12b808fc								5e-ac									^.G.mx.+.	
000000d4`12b8090c								0f-ad									!	
000000d4`12b8091c	39	ae	e0	09	88	72	cb	3c-9f	0d	4d	d6	20	£2	36	e4	9r.	<m6.< td=""><td></td></m6.<>	
**** CLIENT CACHE	ITE	M *;	* * *															
* SessID *				_	_				_	_				_	_			
000000d4`12bfe378								b9-fe									&.F^,	
000000d4`12bfe388	6C	C9	e5	9e	51	C6	71	4d-70	99	7e	63	b9	C6	fe	73	1Q.q1	Mp.~cs	3
* Master Key *		_			_									_				
000000d4`12b5607c								f0-a2									X.	
000000d4`12b5608c								3d-1f									='M.	
00000d4`12b5609c	76	e3	c7	72	17	7c	7d	04-62	af	ec	a5	7a	3d	9c	b2	vr. }	.bz=	
**** CLIENT CACHE	ITE	M *:	* * *															
* SessID *		10			~				~ ~	~		-						
000000d4`12bfe4e8								99-9a									i,.gJ	
000000d4`12bfe4f8	4b	2c	79	le	ce	2c	6d	16-21	af	95	e6	41	4e	c3	00	к,у,т	.!AN	
* Master Key *				~														
000000d4`12b3c27c								3b-60									;`.sQ	
000000d4`12b3c28c								cd-8c									••••••	
000000d4`12b3c29c	4f	6C	49	0d	5a	f3	df	88-1d	b5	85	e2	a1	0a	0a	ea	011.Z		
<			_	_	_	_	_		_		_	_						>
:000> .foreach(s																		
CSessionCa																		
(dwo(\${ses																	lse{.echo	* (
Sess Ticke										J};	.ecl	no 1	* Ma	aste	er K	ey *;db		
poi(poi(\${	sess	Iter	n}+:	10).	+10)	+10	c Li	30;.ecl	no}									

Wireshark SSL Log Format

RSA Session-

ID:97420000581679ae7a064f3e4a350682dca9e839ebca0 7075b1a944d8b1b71f7 Master-

Key: 897adf 533d0e87eadbc41bc1a13adb241251a56f0504 35fad0d54b1064f83c50cedb9d98de046008cde04a409779 5df2

RSA Session-

ID:f5350000be2cebcb15a38f38b99a20751ed0d53957890 1ddde69278dbbf9738e Master-

Key: 716a1d493656bf534e436ffb58ff2e40000516b735db d5dfaff93f37b5ac90ba1c3a25ba3e1505b8f3aa168a657e 007b

RSA Session-

ID:bcb3aff3581fccb9fe268d46f99f5e2c6cc9e59e51c67 14d70997e63b9c6fe73 Master-

Key:e45e18945197c2f0a2addb901a9558f194241d2b488c dc3d1f81e1271acb4dc776e3c772177c7d0462afeca57a3d 9cb2

RSA Session-

ID:c7d0f952fb3fc4999a692ce3674acb1a4b2c791ece2c6 d1621af95e6414ec3b0 Master-

Key:db93026b71e0323b60e2537f0eeebf4fc321094b8a9a 6ccd8cf0f50c7fa68c294f6c490d5af3df881db585e2a10a 0aea

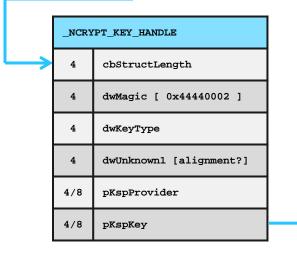
Ephemeral & Persistent Private Keys

Both share the same structure

- Both store secrets in a Key Storage Provider Key struct (KPSK)
- □ The "Key Type" is compared with different values
 - ssl6 gets compared with a list stored in bcryptprimitives
 - ssl4 gets compared with a list stored in NCRYPTPROV
- The Key Storage Provider Key (KPSK) is referenced indirectly through an "Ncrypt Key" struct*

SSL	KEY_PAIR
4	cbStructLength
4	dwMagic ["ssl4" "ssl6"]
4	dwKeyType
4	dwUnknown1 [alignment?]
4/8	pKspProvider
4/8	рКзрКеу

_KSP_KE	ζ.	
4	cbStructLength	←
4	dwMagic ["KSPK"]	
4	dwKeyType	
@0x60	PMSKY	
@0xD0	pDpapiBlob	
@0xD8	dwDpapiBlobLength	



Ephemeral Private Key

□ For performance, reused across connections

Given the public connection params, we can derive the PMS and subsequently MS

□ Stored unencrypted in a LE byte array

- □ Inside of MSKY struct
- □ The curve parameters are stored in the KPSK
 - Other parameters (A&B, etc) are stored in MSKY w/ the key

□ Verified by generating the Public & comparing

□ The Public Key is also stored in the first pointer of the CEphemData struct that points to "ssl6"

:000> .foreach(ek	{ S	-[]	1w](d 0	L?{	3000	000	000000	scl	nanr	nel	CEp	her	nKey	<i>i</i> Dat	a::`v	ftabl	e ' })	{.€
00000c9`86d2a000	000	007	fff	`ed2	23b1	L40	scł	nannel	!CEp	pher	nKey	ZDat	:a:	`vi	Etab	le'			
Public * 000000c9`86d9e688	f2	55	00	2h	06	02	51	3b-98	05	Q D	70	12	QF	1h	15	TT		ιт	v
00000c9`86d9e698								85-78									nx		
00000c9`86d9e6a8								ca-3c									u<		
00000c9`86d9e6b8								00-8d								-			
Curve *			~ ~		15.5	~ ~			~ ••										
00000c9`86d22fb0 * G(x)	000	000	0C9	860	15İ8	a00	"ni	istP25	6"										
00000c9`8698e71c	6b	17	d1	f2	e1	20	42	47-f8	bc	66	e5	63	a4	40	f2	k	.,BG.	C	ß
00000c9`8698e72c								a0-f4									3		
* G(y)	~	1 7	1-1	60	-	~		47 50		~	_	60			60				0
00000c9`8698e71c 00000c9`8698e72c								47-f8 a0-f4									.,BG. 3		
Private [LE!] *	//	03	7u	01	zu	eb	55	a0-14	aı	22	4J	uo	20	CΖ	90	w.}.		. 96.	• • •
00000c9`86d5fc80	d0	27	df	dd	c2	c6	78	5e-be	78	7e	70	94	c2	b7	1a		x^.	a∽x.	
00000c9`86d5fc90								f7-63									rc	-	
* * * *																			
00000c9`86d2cee0	001	007	fff	`od'	23h-	140	sch	nannel	I C Fr	hor	nKot	7Dat	• •	` v z f	Ftah	101			
Public *	000	007.		cu	200.	110	JCI	lanner	. СЦ	JIICI	uncy	Juan	.a.		Lub	16			
00000c9`86d9ff88	d6	35	6b	сс	81	66	c0	6e-74	86	f8	36	8c	be	с7	42	.5k.	.f.nt	6.	E
00000c9`86d9ff98	00	3e	6b	34	49	7f	95	1a-d5	e3	1f	6e	72	75	aa	77	.>k4	I	nr	u.v
00000c9`86d9ffa8	96	6d	93	0d	13	40	d3	f0-cd	f6	ac	30	16	01	7a	44	.m	.@	0.	.zI
00000c9`86d9ffb8	2b	са	16	ea	9d	fa	00	5d-63	f2	80	77	3d	23	1a	5d	+]c	w=	#•:
Curve *	0.01		0-0	0.0	100	- 10		-+	~ 11										
00000c9`86d231f0 * G(x)	000	000	009	860	160:	540	"n	istP25	6"										
00000c9`8698e93c	6b	17	d1	f2	e1	2c	42	47-f8	bc	e6	e5	63	a4	40	f2	k	.,BG.	c	. @
00000c9`8698e94c								a0-f4									3		
* G(y)																			
00000c9`8698e93c								47-f8									.,BG.		
00000c9`8698e94c	77	03	7d	81	2d	eb	33	a0-f4	a1	39	45	d8	98	c2	96	w.}.	3	.9E.	•••
Private [LE!] * 00000c9`86d602c0	cd	91	dh	f٩	f٥	68	hq	6e-05	8f	h6	70	f⊃	d 0	80	90		.h.n.	I.	
00000c9`86d602d0								32-0b									.\$B2.		
																			- , .
< Compared to the second secon																			
:000> .foreach(ek	10	Г ⁻	11	0 1	T.28	3000	2000	00000	scl	hanr	nel I	CEr	her	IKes	_{zDat}	a··`v	ftabl	011)	_

Private [LE!] *;db poi(poi(@\$t0+60)+10)+18) L20;.echo}

□ The RSA Key that is stored on disk

- Unique instance for each private RSA Key by default, the system has several
- **L** E.g. one for Terminal Services

□ RSA Keys are DPAPI protected

- □ Lots of research about protection / exporting
- □ Note the MK GUID highlighted from the Blob

□ The Key is linked to a given Server Cache Item

Verified by comparing the DPAPI blob in memory to protected certificate on disk

□ Also verified through decryption

📐 Command - Dump) \\vn	nwar	e-h	ost\:	Shar	ed F	old	ers\Docu	ume	nts∖	Cha	llen	ges\	zzTr	np\	— 🗆 X
0:000> .foreach(ke *** Private Key **		s -	[w1]]q (0x0	L ?(3000	000000	000	scł	nanr	nel	CSe	ess	ionC	acheServerItem::`v 🗚
000000c9`85d06630		00	00	00	40	0.0	04	df-01	15	41	11	00	7.0	00	a 0	z
000000c9`85d06640								00-66								0fhjJ
000000c9`85d06650								d1-04								····w(}\
000000c9`85d06660								00-74							00	C.r.y.p.t.o.A.P.
000000c9`85d06670		00		00				00-69						74	00	IP.r.i.v.a.t.
000000c9`85d06680								00-79						00	00	aK.e.yf
000000c9`85d06690		01	00	00		00		00-79 00-8a				f7		ec	£9	e
000000c9`85d066a0								3f-40						a3		70?@yeQ.u
000000c9`85d066b0		da		6f				d4-00					80	00	00	Zo
000000c9`85d066c0								00-d2						ce		2A
000000c9`85d066d0								f1-00					-		17	Q9T
000000c9`85d066e0	a7		c6					a3-50							ce	2
000000c9`85d066f0				f1				87-0c						5d		.??.xG`3]'
000000c9`85d06700								36-2a						69	8c]!.6*XVai.
000000c9`85d06710		11						dc-e9				~ ~		5e	31	>'\$=^1
000000c9`85d06720		56		de				ea-ea							34	.V^xR.p.4
000000c9`85d06730								d7-e5								1e
000000c9`85d06740		f1						98-ad							3e	![.4E.y.>
000000c9`85d06750								74-78							10)htxd
000000c9`85d06760		d0		£5				9a-97					76		7c	Bnv.
000000c9`85d06770								9e-a7							56	.g7./HvV
000000c9`85d06780		94						6e-dc					b2		26	%(nw&
000000c9`85d06790		-						9a-77						da		.32H.wG)
000000c9`85d067a0		21						27-6e			48		91		98	z!'n.\$H
000000c9`85d067b0		68						f7-6e								=h .H.X.n*.
000000c9`85d067c0		b3						d9-41							65	9.Q\$A.Qd*e
000000c9`85d067d0								a7-0a								bNF.F.K.
000000c9`85d067e0								86-1a							40	
000000c9`85d067f0								bc-b3							68	KGQG7.h
000000c9`85d06800								c5-c8							2a	U. (aU:*
000000c9`85d06810								c1-a4							a6	;&.ou5.
000000c9`85d06820	00			14				af-b9							d2	,w:Gm.
000000c9`85d06830								e4-95				4d			2e	
000000c9`85d06840								fb-e9								Bu&M.
000000c9`85d06850								53-80							47	.>N<.S.vG
000000c9`85d06860								15-0b								
000000c9`85d06870		00						8f-be						12].:Z9d.,
000000c9`85d06880								d7-6e								=qX.!.
000000c9`85d06890	ef							77-fe								
000000c9`85d068a0								e2-c8								He."
<	200	U.L	40	05	u.	66	az	02 00	60	36		Ja	aJ	va	au	e
				1 ~ 1	2	TO			0.00			1	Lac			
																acheServerItem::
																48))+8)+10)+18)+
10);.echo *		FLI	ate	e Ke	∍Y ,	~ ^ ~ ,	ap	bor (@:	20-	FDU)	ЪС	owr	(@\$1	LU+1	J8);	.ecno}

[†] Decrypting Persistent Key - DPAPI

	Can extract the blob from memory and decrypt w/ keys from disk	Command - Dump \\vmware-host\Shared Folders\Documents\Challenges\zzT C X 0:000> db lsasrv!InitializationVector L8;.echo 00007fff`edaec528 60 4a dd 90 31 45 80 97 `J1E
OR	DPAPIck / Mimikatz	0:000> r @\$t0 = poi(poi(lsasrv!h3DesKey)+10); db @\$t0+3c Ldwo(@\$t0+38);.echo 000000c9`85fb005c 3a 6a dd 76 0f 30 0b 7c-3d 43 f4 db e4 12 66 3a :j.v.0. =Cf: 000000c9`85fb006c 8c f2 b1 f0 a0 a5 5c e4
	_	000000c9`85d6a3b0 000000c9`85d5cd10 000000c9`85dbbdc0 000000c9`85d6a3c0 00000000`000003e7 000000c9`85d6a3c8 f96a6866 4ad11bd8 771afc85 d15c7d28
	 MasterKeys get cached in Memory On Win10 in: dpapisrv!g_MasterKeyCacheList 	000000c9`85d6a3d8 01d1cce0`db1e2d0c 000000c9`85d6a3e0 0000040 000000c9`85d6a3e4 e5 ce 98 a2 ff 50 0d 78-4a 8e 17 54 8f f1 fe b7P.xJT 000000c9`85d6a3f4 21 7e 17 70 2f 7d 52 aa-db cd 75 93 25 48 7a c2 !~.p/}Ru.%Hz. 000000c9`85d6a404 70 62 1a d9 5a e8 97 19-64 c6 62 a0 2a 75 66 9e pbZd.b.*uf.
	 See Mimilib for further details Even though symbols are sort of required, we could likely do without them 	000000c9`85d6a414 a5 c8 33 0c d7 af b6 b1-fb 38 ab 89 b7 d5 cf 1438 000000c9`85d6a424 0000000 000000c9`85d6a430 "C:\Windows\system32\Microsoft\Protect\S-1-5-18\"
	There are only two Bcrypt key pointers in Isasrv's .rdata section (plus one lock)	<pre></pre>
	Identifying the IV is more challenging	g_MasterKeyCacheList

Decrypting Persistent Key - DPAPI

File	Edit	Searcl	h V	iew	Ana	lysis	Ext	ras	Wind	dow	?							- 5	×
2.		Cant I		+ +	16	-	\sim	AN	SI		\sim	he	x	~	1				
		420 7					740			~ .		C 10	-	0.00	-				
1080a	асебу	42fb7f	r/cel	0231	212e	et4a4	-749	batd	3-01	31-40	ct/-b	009-	caso	IUC31	1929				
ffse	t (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	OD	0E	OF		^
0000	000	02	00	00	00	00	00	00	00	0D	00	00	00	00	00	00	00		
0000	010	00	00	00	00	1C	01	00	00	50	06	00	00	14	00	00	00	P	
0000	020	00	00	00	00	FC	00	00	00	54	53	53	65	63	4B	65	79	üTSSecKey	
0000																	00	Set1	
0000		00																	
0000		00			00									00			C7	ÿ.	
0000		94													-		OA	"ÒJDÆxp <pc÷•.< td=""><td></td></pc÷•.<>	
0000		57																WÊ.{. Œ^⊣'Đ.³]S⅓	
0000																		Þñ´N~VR—#É.ýcÜe;	
0000		7F																.?û=.€ha.1ÍP¦Bà.	
0000																		Ú-ÝÆ.Ia9<€¥	
0000		E6																æ.Äøú.tÆ+°−′Gø.¥	
0000																		r)ÉžôÀ.X,ñmYMà%*	
0000		AF																<pre>i ·AéÊ¥OU»#W"¾¿ë Å'"PÈÝIR(.ëÍ—±</pre>	
0000			_													-		A'"PEYIR(.eI—± .ŒËåÿ. íù‡ÏO.S•.	
0000		82															19 9B	,œEay. 10∓10.§•. ♡.ì´¨Ï."'ú:Òë),	<u>_</u>
0000		DE								_								<pre>y,1 1u:0e);; Páú`Raá.Äö∉>^â</pre>	
0000		45															0E	EŸâ.; '.v.NSPP».	
0000		45 F2																òcñèVž YA.d.ÌàS.	
0000		DO																Ð÷¯Ĵ¶'.ê9*>žÀ+.é	
0000		B2																YŸS£}41g.JæÁ	
0000				bo															
0000				7A														.@z.À0Â-ëfhi	
0000		F9																ùØ.ÑJü.w(}\Ñ	
0000				00														.,C.r.y.p.t.o	
0000				00													76	.A.P.IP.r.i.v	
0000	_			00													00	.a.t.eK.e.v	
0000				66														fŠ`@	
0000		B8				F9								3F			65	,÷Oìù7oÌ,æ?@ve	
0000			-	51			-										00	"Q£uZÚåo.%ÿÔ	
0000				80				02						00			1D	€ÒA.	
0000				F7														§<÷Î′Q¦9.Úñ.TÎ	
0000				A8													00	ç. "à.Ş.Æ"ßoï£P	
0000				9F														.+ŸpÎ.?ûñ?¦x‡.GÙ	
0000		BO																°`3]',]ë ·!*6*X¢	
0000		88			69			11						DC			FD	^VaiŒ>. ÿ'\$µÜé*ý	~
		0.0	-	~~		~ *	-				~ ~	2.0	-				~~	0644 TTAT 0 11 0	

Í 🛉

00000010 01 00 73 DA C7 94 D2 4A 44 14 20 15 C6 78 00000000 27 D0 17 B3 53 BD DE F1 B4 42 98 56 52 97 23 'D.']SHEAT'N'VR 00000000 C9 1A FD 63 DC 51 17 17 F3 F3 D1 90 66 61 15 'D.']SHEAT'N'VR 00000000 C9 1A FD 05 52 C7 23 'D.']SHEAT'N'VR 00000000 B0 20 A6 42 E0 2E DA 97 DC 61 54 93 C 'D'''''''''''''''''''''''''''''''''''	🕄 Eile I	Edit	Searc	h V	iew	Δna	lvsis	Evt	ras	Wind	wob	?								- 1
Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2				on I			.,						he			1				
Offset (h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 00000000 02 03 04 05 06 07 08 00 00 07 00 0						10		\sim	AN	21		~	ne	×	~	1				
00000000 $\beta 2 53 41 32 08 01 00 00 00 80 00 0F F 00 00 00 \beta 2 53 41 32 08 01 00 73 DA C7 94 D2 4A 44 14 20 15 C6 78 pcC^+. WÊ.(-T. 9) 0000000 070 01 70 35 D3 BD DF 1B 44 49 85 65 29 72 3' pcC^+. WÊ.(-T. 9) 0000000 070 D1 7B 55 D5 D5 DE F1 B4 49 85 65 29 72 3' pcC^+. WÊ.(-T. 9) 0000000 070 D1 7B 55 D5 DE F1 B4 49 85 65 29 72 3' pcC^+. WÊ.(-T. 9) 0000000 05 31 CD 50 A6 42 E0 2E DA 97 DD C6 15 49 61 39 30' 11^{2} PA 5' CS AC 00000000 B0 28 55 17 18 A5 E6 1F C4 F8 A0 A7 4 C6 2B c$	privRS	6A_de	c.bin																	
00000010 01 00 73 DA C7 94 D2 4A 44 14 20 15 C6 78 00000000 27 D0 17 B3 53 BD DE F1 B4 42 98 56 52 97 23 'D.']SHEAT'N'VR 00000000 C9 1A FD 63 DC 51 17 17 F3 F3 D1 90 66 61 15 'D.']SHEAT'N'VR 00000000 C9 1A FD 05 52 C7 23 'D.']SHEAT'N'VR 00000000 B0 20 A6 42 E0 2E DA 97 DC 61 54 93 C 'D'''''''''''''''''''''''''''''''''''	Offset	:(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	oc	OD	0E	OF		
00000000 70 3C 70 43 F7 95 0A 57 CA 1F 7B 9D AF 8C 5E AC p	000000	000	52	53	41	32	08	01	00	00	00	08	00	00	FF	00	00	00	RSA2.	ÿ
$\begin{array}{c} 0000030 & 27 \ D0 \ 17 \ B3 \ 5D \ 5S \ BD \ DE \ F1 \ B4 \ 4E \ 98 \ 56 \ 52 \ 97 \ 23 \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ $			01															-		
00000040 C9 1A FD 63 DC 65 A1 7F 3F FB 3D 19 80 68 61 15 É.ýCŮĘ;.?û=.€h 00000050 31 CD 50 A6 42 E0 2E DA 97 DD C6 15 49 61 39 3C 1ÍP Bà.Ú-Ý.E.Ia 00000060 80 02 85 85 17 18 A5 E6 1F C4 F8 FA 0A 74 C6 2B €¥æ.Äøú.t 00000070 B0 2D B4 47 F8 09 A5 72 29 C9 9E F4 C0 55 58 2C $^{\circ-}$ Gæ.Ye)źÉż. 00000080 F1 6D 59 4D E0 25 B2 AF 69 B7 41 E9 CA A5 4F 55 mmYMà* ⁼ 1·Å鞥 00000080 F1 6D 59 4D E0 25 B2 AF 69 B7 41 E9 CA A5 4F 55 mmYMà* ⁼ 1·Å鞥 00000080 F2 28 0C EB CD 97 B1 82 8C CB E5 FF 01 20 DF 9P R(.ĕí- \pm , Œšý. 00000000 B8 7 CF 30 19 A7 95 19 FF 88 ED 4A 8C F1 42 29 2 \pm 10.5°.ý, 1′ ⁻ 1. 00000000 16 C4 F6 A5 9B 88 E2 45 C2 9F E2 12 A1 B4 11 76 .Åö¥ $^{\circ}$ ážÅ'á; ' 00000000 16 C4 F6 A5 9B 88 E2 45 C2 9F E2 12 A1 B4 11 76 .Åö¥ $^{\circ}$ ážÅ'á; ' 00000000 16 C4 F6 C2 53 9D D0 F7 AF DB B6 27 14 EA 39 .d.ìAS $-^{\circ}$ Û¶. 00000000 12 0 44 18 CC E0 53 9D D0 F7 AF DB B6 27 14 EA 39 .d.ìAS $-^{\circ}$ Û¶. 00000010 B2 3E 9E C0 2B 1C E9 B2 DD 9F A7 A3 7D 34 6C 67 * $^{\circ}$ ŽÀ. $+é^{\circ}$ ÝÝS£1. 0000010 B2 3E 9E C0 2B 1C E9 B2 DD 9F A7 A3 7D 34 6C 67 * $^{\circ}$ ÄÅf > 0000010 B2 3E 9E C0 2B 1C E9 B2 DD 9F A7 B3 FB 8E 7. JæÁf > 0000010 B2 3E 9E C0 2B 1C E9 B2 DD 9F A7 B3 7B 4F C6 7 * ZÀ. $+é^{\circ}$ ÝÝS£1.ĕ 0000010 B2 3E 9E C0 2B 1C E9 B2 DD 9F A7 B3 7D 34 6C 67 * ZÀ. $+é^{\circ}$ ÝS£1.ĕ 0000010 B2 3E 9E C0 2B 1C E9 B2 DD 9F A7 B3 7D 34 6C 67 * ZÀ. $+é^{\circ}$ ÝS£. $^{\circ}$ J. $^{\circ}$ Å 00000120 4B FF 34 F5 05 5C 20 D4 B3 18 42 77 79 69 8F 0A KÝAČ. $^{\circ}$ J. $^{\circ}$ Bwy1 00000130 D6 73 46 64 54 E4 35 19 D8 39 A0 ED 1D EB 40 7E $^{\circ}$ SÅTÁ. $^{\circ}$ J. $^{\circ}$ J. $^{\circ}$ MW 00000140 E0 6A 0A 26 DC 8C D1 D0 1A D5 BA 8C 1D 1D 34 A3 $^{\circ}$ J. $^{\circ}$ ÚN $^{\circ}$ J. $^{\circ}$ MW 00000150 EC 58 CE DC 7A 97 8D 47 39 ED CB 88 40 58 17 FE $^{\circ}$ XÅUÅ $^{\circ}$ Ø [*] MU $^{\circ}$ M [*] 00000160 54 A3 E3 57 43 8A 2E EB 17 F7 B1 72 BB CC 9E C0 $^{\circ}$ QÅS(I. $^{\circ}$. $^{\circ}$ J. $^{\circ}$ MW 00000180 54 A3 E3 57 43 8A 2E EB 17 F7 B1 72 BB CC 9E CC $^{\circ}$ AŠA [*] LÅ [*] Q [*] J. $^{\circ}$ A [*] LÅ [*] Q [*] J. $^{\circ}$ A [*] LÅ [*] Q [*] Y [*] J. $^{\circ}$ A [*] LÅ [*] Q [*] S [*] J. $^{\circ}$ MU $^{\circ}$ M [*] J. $^{\circ}$ M [*] J. $^{\circ}$ M																				
$\begin{array}{cccccccccccccccccccccccccccccccccccc$																				
00000060 80 02 85 85 17 18 A5 E6 1F C4 F8 FA 0A 74 C6 2B $($																				
00000070 B0 2D B4 47 F8 09 A5 72 29 C9 9E F4 C0 05 58 2C $^{\circ}$ -'Gø.¥r)ÉžĉÅ. 0000080 F1 6D 59 4D E0 25 B2 AF 69 B7 41 E9 CA A5 4F 55 mWM&* [±] 1.AéÉ¥ 00000000 B2 35 77 93 BE BF EB C5 27 94 50 19 0D C8 D4 99 *#W*%¿ëÅ''P.Ě 00000000 52 28 0C EB CD 97 B1 82 8C CB E5 FF 10 20 ED F9 R(.čí±,cfžÅ;.P.Ě 00000000 FA 3A D2 EB 29 C5 9B DE E1 FA 60 2E 15 52 61 E1 ú:Ĉė)Å>báú'.R 00000000 16 C4 F6 A5 9B 88 E2 45 C2 9F E2 12 A1 B4 11 76 .ÅG¥>^áEÅYå;' 0000000F0 10 64 18 CC E0 53 9D D0 F7 AF DB B6 27 14 EA 99 .d.låS.D÷ ⁺ Û¥. 00000100 B2 3E 9E C0 2B 1C E9 B2 DD 9F A7 A3 7D 34 6C 67 *>ŽÅ+.é*ÝY\$£}4 00000100 B2 3E 9E C0 2B 1C E9 B2 DD 9F A7 A3 7D 34 6C 67 *>ŽÅ+.é*ÝY\$£}4 00000110 1A 4A E6 C1 00 00 00 00 00 00 00 83 9B 58 2F .JæÁf> 00000120 4B FF 34 F5 05 5C 20 D4 B3 18 42 77 79 69 8F 0A KŸ4ð.\ [°] .BWyi 00000130 D6 73 46 64 54 E4 35 19 D8 39 A0 ED 1D EB 40 7E 00000140 E0 6A 0A 26 DC 8C D1 D0 1A D5 BA 8C 1D 1D 34 A3 aj.sÜEŇĐ.Õ°C 00000150 1C B2 83 66 78 B4 62 08 22 82 43 F2 47 47 ED 7D .*ffx'b.",còGG 00000170 A3 F7 45 A5 94 D 4C E5 D2 67 E8 A9 24 93 FB 37 .±rtZMLÅOġB [°] 00000180 54 A3 E3 57 43 8A 2E EB 17 E7 B1 72 BB 0C 9E E0 1EÅWCŠ.ë.c;tr». 00000180 54 A3 E3 57 43 8A 2E EB 17 E7 B1 72 BB 0C 9E E0 1EÅWCŠ.ë.c;tr». 00000180 54 A3 E3 57 43 8A 2E EB 17 E7 B1 72 BB 0C 9E E0 1EÅWCŠ.ë.c;tr». 00000180 54 A3 E3 57 43 8A 2E EB 17 E7 B1 72 BB 0C 9E E0 1EÅWCŠ.ë.c;tr». 00000180 54 A3 E3 57 43 8A 2E EB 17 E7 B1 72 BB 0C 9E E0 1EÅWCŠ.ë.c;tr». 00000180 54 A3 E3 57 43 8A 2E EB 17 E7 B1 72 BB 0C 9E E0 1EÅWCŠ.ë.c;tr». 00000180 54 A3 E3 57 43 8A 2E EB 17 E7 B1 72 BB 0C 9E E0 1EÅWCŠ.ë.c;tr». 00000180 54 A3 E3 57 43 8A 2E EB 17 E7 B1 72 BB 0C 9E E0 1EÅWCŠ.ë.c;tr». 00000180 54 A3 E3 57 43 8A 2E EB 17 E7 B1 72 BB 0C 9E E0 1EÅWCŠ.ë.c;tr». 00000180 54 A3 E3 57 43 8A 2E EB 17 E7 B1 72 BB 0C 9E E0 1EÅWCŠ.ë.c;tr [†] .Å 00000180 54 A3 E3 57 43 8A 2E EB 17 E7 B1 72 BB 02 9E C0 3A .c,t [°] .Å 00000100 35 17 24 F2 1C 9D A3 E6 39 A6 03 62 C5 BC 09 C .s.,tw°! ÅLÅYÝ 00000210 35 17 24 F2 1C 9D A3 E6 39 A6 03 62 C5 B																				
00000080 F1 6D 59 4D E0 25 B2 AF 69 B7 41 E9 CA A5 4F 55 fmYMà* ⁼ 1.AéÊ¥ 0000090 BB 23 57 93 BE BF EB C5 27 94 50 19 0D C8 DD 49 $\#W^*X_{4}$ ÉÅ''P.É 00000000 52 28 0C EB CD 97 B1 82 8C CB E5 FF 01 20 ED F9 R(.čÍ-±, ŒĚÅY. 00000000 FA 3A D2 EB 29 C5 9B DE E1 FA 60 2E 15 52 61 E1 ú:Òė)Å>AúY. T 00000000 16 C4 F6 A5 9B 88 E2 45 C2 9F E2 12 A1 B4 11 76 .Åö¥> [*] áEÅYÅ;' 00000000 16 C4 F6 A5 9B 88 E2 45 C2 9F E2 12 A1 B4 11 76 .Åö¥> [*] áEÅYÅ;' 00000000 16 C4 18 CC E0 53 9D D0 F7 AF DB B6 27 14 EA 39 .d.ìÅS D- ⁻ ÖI'. 00000010 B2 3E 9E C0 2B 1C E9 B2 DD 9F A7 A3 7D 34 6C 67 [*] >ŽÀ+.é*ÝYŠ£I. 00000010 B2 3E 9E C0 2B 1C E9 B2 DD 9F A7 A3 7D 34 6C 67 [*] >ŽÀ+.é*ÝYŠ£I. 0000010 B2 3E 9E C0 2B 1C E9 B2 DD 9F A7 A3 7D 34 6C 67 [*] >ŽÀ+.é*ÝYŠ£I. 0000010 B2 3E 9E C0 2B 1C E9 B2 DD 9F A7 A3 7D 34 6C 67 [*] >ŽÀ+.é*ÝYŠ£I. 0000010 B2 3E 9E C0 2B 1C E9 B2 DD 9F A7 A3 7D 34 6C 67 [*] >ŽÀ+.é*ÝYŠ£I. 0000010 B2 3E 9E C0 2B 1C E9 B2 DD 9F A7 A3 7D 34 6C 67 [*] >ŽÀ+.é*ÝYŠ£I. 0000010 B2 3E 9E C0 2B 1C E9 B2 DD 9F A7 B3 7D 34 6C 67 [*] >ŽÀ+.é*ÝYŠ£I. 0000010 11 1A 4A E6 C1 00 00 00 00 00 00 00 83 9B 58 2F .JæÁf> 00000120 4B FF 34 F5 05 5C 20 D4 B3 18 42 77 79 69 8F 0A KÝAČ.\Ô'B.Wy1 00000130 D6 73 46 64 54 E4 35 19 D8 39 A0 ED 1D EB 40 7E ÖSFATTS.09 1. 00000140 E0 6A 0A 26 DC 8C D1 D0 1A D5 BA 8C 1D 1D 34 A3 àj.sÜCÑĐ.Õ°C. 00000140 E0 6A 0A 26 DC 8C D1 D0 1A D5 BA 8C 1D 1D 34 A3 àj.sÜCÑĐ.Õ°C. 00000160 1C B2 83 66 78 B4 62 08 22 82 43 F2 47 47 ED 7D .ffx'b.",CÒGG 00000170 A3 F7 74 5A 59 4D 4C E5 D2 67 E8 A9 24 93 FB 37 f±rZMÅOè@& [*] 00000180 54 A3 E3 57 43 8A 2E EB 17 F7 B1 72 BB 0C 9E E0 TÉÂWCŠ.ë.c‡Tx*. 00000180 54 A3 E3 57 43 8A 2E EB 17 F7 B1 72 BB 0C 9E E0 TÉÂWCŠ.ë.c‡TX*. 00000180 54 A3 E3 57 43 8A 2E EB 17 F7 B1 72 BB C5 9C 6C Q§ú[s.".f ¹ .¾A 00000180 54 A3 E3 57 43 8A 2E EB 17 E7 B1 72 BB C5 9C C6 Q§ú[s.".f ¹ .¾A 00000180 54 A3 E3 57 43 AA 2E EB 17 C7 B1 73 49 AB EF B1 iÒuQA)ÅX**4¥ 00000180 51 F2 A7 FA 5B 26 16 22 1F CE B3 12 BE C5 9C C6 Q§ú[s.".f ¹ .¾A 00000180 51 F2 A7 FA 5B 26 16 22 1F CE B3 12 BC C5 0C 05 7																				
$\begin{array}{cccccccccccccccccccccccccccccccccccc$																				
$\begin{array}{cccccccccccccccccccccccccccccccccccc$																				
000000B0 87 CF 30 19 A7 95 19 FF B8 EC B4 A8 CF 14 22 92 $\pm 10.5 \cdot 1^{-1}T$. 000000C0 FA 3A D2 EB 29 C5 9B DE E1 FA 60 2E 15 52 61 E1 $\pm 1^{\circ}Oe_{A}A_{P}A\dot{a}\dot{a}\dot{a}\dot{a}\dot{a}\dot{a}\dot{a}\dot{a}\dot{a}\dot{a}$																				
00000000 16 C4 F6 A5 9B 88 E2 45 C2 9F E2 12 A1 B4 11 76 .Äö¥>^â£ÂYâ.; 000000E0 13 4E 53 50 50 BB 0E F2 E7 F1 E8 56 9E 22 9F 41 .NSFP*.òçñèYž" 000000E0 10 64 18 CC E0 53 9D 0D F7 AF D8 B6 27 14 EA 39 .d.ìàS.D+¯ÛY. 00000100 B2 28 9E CO 28 1C E9 B2 DD 9F A7 A3 7D 34 6C 67 *>ZÅ+.éYŶSL4 00000110 1A 4A E6 C1 00 00 00 00 00 00 00 00 83 9B 58 2F .JæÁf> 00000120 4B FF 34 F5 05 5C 20 D4 B3 18 42 77 79 69 8F 0A Kÿ4ö.\ô'.Bwyi 00000130 D6 73 46 64 54 E4 35 19 D8 39 A0 ED 1D EB 40 7E ÖsFdTä5.Ø9 i.ë 00000140 E0 6A 0A 26 DC 8C D1 D0 1A D5 BA 8C 1D 1D 34 A3 àj.dŪCMD.Õ°C 00000150 EC 58 CE DC 7A 97 8D 47 39 ED CD 88 40 58 17 FE ìXÎÜZG9iî^8X 00000160 1C B2 83 66 78 B4 62 08 22 82 43 F2 47 47 ED 7D .ffx'b.", CÀGG 00000180 54 A3 E3 57 43 8A 2E EB 17 E7 B1 72 B8 0C 9E E0 T£ãWCŠ.e.etrx. 00000180 54 A3 E3 57 43 8A 2E EE 17 E7 B1 72 B8 02 9E C E2 Qá§ú[٤.".f ¹ .*Å 00000180 54 A3 E3 57 48 BA 2E A3 P4 D9 AD B8 E6 C0 05 7	000000	0B0	87	CF	30	19	A7	95	19	FF	B8	EC	B4	A8	CF	14	22	92		
000000E0 13 4E 53 50 50 BB 0E F2 E7 F1 E8 56 9E 22 9F 41 .NSPP*.dcfhěVŽ" 000000F0 10 64 18 CC E0 53 9D D0 F7 AF DB B6 27 14 EA 39 .d.hàs.p= $^{-1}$ 0°4'. 00000100 B2 3E 9E C0 2B 1C E9 B2 DD 9F A7 A3 7D 34 6C 67 *>ŽÀ+.é*ÝÝSL4 00000110 1A 4A E6 C1 00 00 00 00 00 00 00 83 9B 58 2F .JæÁ	000000	0C0	FA	ЗA	D2	EB	29	C5	9B	DE	E1	FA	60	2E	15	52	61	E1		
000000F0 10 64 18 CC E0 53 9D D0 F7 AF DB B6 27 14 EA 39 .d. $tas.b \div 0q^{\circ}$. 00000100 B2 3E 9E C0 2B 1C E9 B2 DD 9F A7 A3 7D 34 6C 67 *> $\lambda \pm A + \epsilon \pm \tilde{y} + \tilde{y} + \epsilon \pm \tilde{y} + \tilde{y} + \epsilon \pm \tilde{y} + \epsilon + \tilde{y} + \tilde{y} + \epsilon + \tilde{y} + \epsilon + \tilde{y} + \epsilon + \tilde{y} + y$	000000	DDO	16	C4	F6	A5	9B	88	E2	45	C2	9F	E2	12	A1	Β4	11	76	.Äö¥>^âI	£ÂŸâ.;′
00000100 B2 3E 9E C0 2B 1C E9 B2 DD 9F A7 A3 7D 34 6C 67 $*>\tilde{Z}A+.e^{\pm}\tilde{Y}\tilde{Y}\tilde{Y}s]_{4}$ 00000110 1A 4A E6 C1 00 00 00 00 00 00 00 83 9B 58 2F .JæÁf> 00000120 4B FF 34 F5 05 5C 20 D4 B3 18 42 77 79 69 8F 0A Kÿdč.\ô'.Bwyi 00000140 E0 6A 0A 26 DC 8C D1 D0 1A D5 BA 8C 1D 1D B4 07 E ÖsFdTač.99 i.e 00000140 E0 6A 0A 26 DC 8C D1 D0 1A D5 BA 8C 1D 1D 34 A3 àj.sÜCMD.Õ°C 00000150 EC 58 CE DC 7A 97 8D 47 39 ED CD 88 40 58 17 FE $\lambda \tilde{X}\tilde{U}zGsi^{-1}GX$ 00000170 A3 F7 45 A5 94 D4 CE 5D 26 7E 8A 92 493 FB 37 £+tZYMLÅOgèG*. 00000180 54 A3 E3 57 43 8A 2E EB 17 E7 B1 72 BB 0C 9E E0 TÉÄWCŠ.ë.ctr*. 00000180 54 A3 E3 57 43 8A 2E EB 17 E7 B1 72 BB 0C 9E E0 TÉÄWCŠ.ë.ctr*. 00000180 54 A3 E3 57 43 8A 2E EB 17 E7 B1 72 BB 0C 9E E0 TÉÄWCŠ.ë.ctr*. 00000180 51 E2 A7 FA 5B 26 16 22 1F CE B3 12 BE C5 9C 62 GåŠu[s.".Î ⁻ .ÅA 00000180 D9 29 26 CA BF D7 4B A5 FF 51 A8 53 50 1B FF 40 Û)sĉz×K¥ýQ°SP. 00000180 35 17 24 F2 1C 9D A3 E6 39 A6 03 62 C5 BC 0E 9C 5.\$o`.£æ9!.bÅ¥ 00000100 35 17 24 F2 1C 9D A3 E6 39 A6 03 62 C5 BC 0E 9C 5.\$o`.£æ9!.bÅ¥ 00000100 35 17 24 F2 1C 9D A3 E6 39 A6 03 62 C5 BC 0E 9C 5.\$o`.£æ9!.bÅ¥ 00000100 07 F5 4C D7 13 AD A0 96 23 1E 3F 3D D3 D2 CD 3A .čL× $=^{+}.=^{o}O$ 00000120 AD 95 B6 6D 3D CD 68 AF 8E 29 18 E5 64 F4 F2 F5 $^{gm=fn-Z}$).ådô 00000220 BD EB AA 46 B6 41 9B 2B C1 0C 3A D5 7F ED 4B $34^{o}\circ*!(gA)+Å.:Õ.$ 00000220 BD EB AA 46 B6 41 9B 2B C1 0C 3A D5 7F ED 4B $34^{o}\circ*!(gA)+Å.:Õ.$ 00000220 AD 95 B6 6D 3D CD 68 AF 8E 29 18 E5 64 F4 F2 F5 $^{gm=fn-Z}$).ådô 00000220 AD 95 B6 6D 3D CD 68 AF 8E 29 18 E5 64 F4 F2 F5 $^{gm=fn-Z}$).ådô 00000220 BD EB AA AA CD F6 CE 13 F 3A 63 8B 48 1F 2B 72 E2 43 -J-A&A1Å?:C.H.:*	000000	0E0	13	4E	53	50	50	BB	0E	F2	E7	F1	E8	56	9E	22	9F	41	.NSPP».	òçñèVž"
00000110 1A 4A E6 C1 00 00 00 00 00 00 00 00 83 9B 58 2F .JmÁf> 00000120 4B FF 34 F5 05 5C 20 D4 B3 18 42 77 79 69 8F 0A Kÿ4č.\Ô ³ .Bwyi 00000130 D6 73 46 64 54 E4 35 19 D8 39 A0 ED 1D EB 40 7E ÖsFdTä5.Ø9 i.ë 00000140 E0 6A 0A 26 DC 8C D1 D0 1A D5 BA 8C 1D 1D 34 A3 àj.dŪdND.Õ°C 00000150 EC 58 CE DC 7A 97 8D 47 39 ED CD 88 40 58 17 FE ìXÎÜzG9iî^8X 00000160 1C B2 83 66 78 B4 62 08 22 82 43 F2 47 47 ED 7D .ffx'b.",CòGG 00000170 A3 F7 74 5A 59 4D 4C E5 D2 67 E8 A9 24 93 FB 37 £+tZYMLÅÒgè@\$" 00000180 54 A3 E3 57 43 8A 2E EB 17 E7 B1 72 BB 0C 9E E0 T£&%ijc*,YÙ èq.IÒÉ 00000190 78 7F 82 9F D9 A0 E8 B6 0B CF D2 C9 00 00 00 00 x.,YÙ èq.IÒÉ 00000100 51 E2 A7 FA 5B 26 16 22 1F CE B3 12 BE C5 9C C6 Qá§úí(s.".î ¹ , MÅ 000001100 51 E2 A7 FA 5B 26 16 22 1F CE B3 10 B8 E6 C0 05 7 ^T , ^m m, ^m U." 000001100 51 72 4 F2 1C 9D A3 E6 39 A6 03 62 C5 BC 0E 9C 5.\$è£æ9!, bÅ+ 000001100 35 17 24 F2 1C 9D A3 E6 39 A6 03 62 C5 BC 0E 9C 5.\$è£æ9!, bÅ+ 000001100 75 4C D7 13 AD A0 96 23 1E 3F 3D D3 D2 CD 3A .dix#.?=ÓÒ 00000120 BD B BA A4 A6 B6 41 9B 2B C1 0C 3A D5 7F ED 4B H4×ifA>ÅÓ.	000000	OFO	10	64	18	CC	E0	53	9D	DO	F7	AF	DB	B6	27	14	EA	39	.d.ÌàS.H	÷ŤÛ¶'.
00000120 4B FF 34 F5 05 5C 20 D4 B3 18 42 77 79 69 8F 0A Kÿ4č.\ Ô ⁵ .Bwyi 00000130 D6 73 46 64 54 E4 35 19 D8 39 A0 ED 1D EB 40 7E ÖsFdTä5.Ø9 1.ë 00000140 E0 A0 A 26 DC 8C D1 D0 1A D5 BA 8C 1D 1D 34 A3 àj.GUCÑO.Õ°C 00000150 EC 58 CE DC 7A 97 8D 47 39 ED CD 88 40 58 17 FE ìXÎUzG911^0gX 00000160 1C B2 83 66 78 B4 62 08 22 82 43 F2 47 47 ED 7D .ffx'b.",CòcG 00000170 A3 F7 74 5A 59 4D 4C E5 D2 67 E8 A9 24 93 FB 37 £+t2YMLåÒgè@\$" 00000180 54 A3 E3 57 43 8A 2E EB 17 E7 B1 72 BB 0C 9E E0 T£äWCŠ.ë.etrx. 00000180 54 B2 7F 82 9F D9 A0 E8 B6 0B CF D2 C9 00 00 00 00 00 x., YÙ èq.IÒÉ yûştit.".f'.% 00000180 D9 29 26 CA BF D7 4B A5 FF 51 A8 53 50 1B FF 40 Ú) ĉ£ż.×K¥ŷQ`SF. 00000100 37 0C 4C 88 A8 71 6D 82 F9 94 D9 AD B8 E6 C0 05 7.L^~gm,ù'Ù.æ 00000100 35 17 24 F2 1C 9D A3 E6 39 A6 03 62 C5 BC 09 C 5.\$c£æ\$!.bÅ 000001100 35 17 24 F2 1C 9D A3 E6 39 A6 03 52 C5 BC 09 C4 5.\$c£æ\$!.bÅ 00000120 BD EB A 44 A6 B6 41 9B 2B C1 0C 3A D5 7F ED 4B `AL*\$c																				
00000130 D6 73 46 64 54 E4 35 19 D8 39 A0 ED 1D EB 40 7E ÖsFdTä5.09 1.e 00000140 E0 6A 0A 26 DC 8C D1 D0 1A D5 BA 8C 1D 1D 34 A3 àj.dDCMD.O°C 00000150 EC 58 CE DC 7A 97 8D 47 39 ED CD 88 40 58 17 FE ìXÎUzG9í°C 00000160 1C B2 83 66 78 B4 62 08 22 82 43 F2 47 47 ED 7D `ffx'b.",CòGG 00000170 A3 F7 74 5A 59 4D 4C E5 D2 67 E8 A9 24 93 FB 37 £+tZYMLåÓgè@S* 00000180 54 A3 E3 57 43 8A 2E EB 17 E7 B1 72 BB 0C 9E E0 TÉAWCŠ.ë.gtrx. 00000180 54 A3 E3 57 43 8A 2E EB 17 E7 B1 72 BB 0C 9E E0 TÉAWCŠ.ë.gtrx. 00000180 54 A3 E3 57 43 8A 2E EB 17 E7 B1 72 BB 0C 9E E0 Gású[s.".1 ² .*A 00000180 51 E2 A7 FA 5B 26 16 22 1F CE B3 12 BE C5 9C C6 Qású[s.".1 ² .*A 00000100 37 0C 4C 88 A8 71 6D 82 F9 94 D9 AD 88 E6 C0 05 7.L^~gm,ù'Ù.æ 00000100 35 17 24 F2 1C 9D A3 E6 39 A6 03 62 C5 BC 0E 9C 5.\$£æ\$!.bÅ 00000100 35 17 24 F2 1C 9D A3 E6 39 A6 03 62 C5 BC 0E 9C 5.\$£æ\$!.bÅ 00000100 35 17 24 F2 13 AD A0 96 23 1E 3F 3D D3 D2 CD 3Ac																_				
$\begin{array}{cccccccccccccccccccccccccccccccccccc$																			-	-
00000150 EC 58 CE DC 7A 97 8D 47 39 ED CD 88 40 58 17 FE iXîÜzG9iî^@X 00000160 1C B2 83 66 78 B4 62 08 22 82 43 F2 47 47 ED 7D .ffx'b.",CòGG 00000170 A3 F7 74 5A 59 4D 4C E5 D2 67 E8 A9 24 93 FB 37 £+tZYMLåÒgè@\$" 00000180 54 A3 E3 57 43 8A 2E EB 17 E7 B1 72 BB 0C 9E E0 T£āWCŠ.e.gtrw. 00000190 78 7F 82 9F D9 A0 E8 B6 0B CF D2 C9 00 00 00 00 x.,YÙ èq.IÒÉ 00000100 51 E2 A7 FA 5B 26 16 22 1F CE B3 12 BE C5 9C C6 Qá§úí[c.".î'.*A 000001100 51 E2 A7 FA 5B 26 16 22 1F CE B3 12 BE C5 9C C6 Qá§úí[c.".î'.*A 00000120 78 7F 24 F2 1C 9D A3 E6 39 A6 03 62 C5 BC 0E 9C 7.L^~@m, ù'Ù.æ 00000120 35 17 24 F2 1C 9D A3 E6 39 A6 03 62 C5 BC 0E 9C 5.\$ô£æ9; bÅ* 00000120 35 17 24 F2 1C 9D A3 E6 39 A6 03 62 C5 BC 0E 9C .ö.i×#.?=ôò 00000120 35 17 24 F2 1C 9D A3 E6 39 A6 03 62 C5 BC 0E 9C .ö.i×#.?=ôò 00000120 35 17 24 F2 1C 9D A3 E6 39 A6 03 62 C5 BC 0E 9C .ö.i×#.?=ôò 00000120 BD EB AA 46 B6 41 9B 2B C1 0C 3A D5 7F ED 4B .ö.i×#.?=ôò 00000210 AD 95 B6 6D 3D CD 68 AF 8E 29 18 E5 64 F4 F2 F5 gm=fn ⁻⁷ 2).ådô 00000220 BD DE BA A4 A6 B6 41 9B 22 L2 AE 13 FD 76 66 SA EE 3*.*.@výrf <td></td>																				
00000160 1C B2 83 66 78 B4 62 08 22 82 43 F2 47 47 ED 7D .*ffx'b.",CdGG 00000170 A3 F7 74 5A 59 4D 4C E5 D2 67 E8 A9 24 93 FB 37 £+tZXMLådgå@\$" 00000180 54 A3 E3 57 43 8A 2E EB 17 E7 B1 72 BB 0C 9E E0 TfāWCŠ.€.ctrw. 00000180 54 A3 E3 57 43 8A 2E EB 17 E7 B1 72 BB 0C 9E E0 TfāWCŠ.€.ctrw. 00000180 54 A3 E3 57 43 8A 2E EB 17 E7 B1 72 BB 0C 9E E0 TfāWCŠ.e.ctrw. 00000100 78 7F 82 9F D9 A0 E8 B6 0B CF D2 C9 00 00 00 00 x., YÙ èq.IČÉ 0000110 51 E2 A7 FA 5B 26 16 22 1F CE B3 12 BE C5 9C C6 Qâ\$ú[cî. ¹ . Å. 000001B0 D9 29 26 CA BF D7 4B A5 FF 51 A8 53 50 1B FF 40 Ú) &£¿¿×K¥ŷQ°SP. 000001C0 37 0C 4C 88 A8 71 6D 82 F9 94 D9 AD B8 E6 C0 05 7.L^~gm, ù'Ù.æ 000001D0 35 17 24 F2 1C 9D A3 E6 39 A6 03 62 C5 BC 09 C5 \$.c.`.£æ³; hÅ* 000001E0 DF 75 D8 FE 34 7D C3 58 68 D7 D7 34 9A BF 3B i0u004)ÅXh×*43 000001E0 DF 75 D8 FE 34 7D C3 58 68 D7 D7 34 9A D5 3E .c***																			-	
00000170 A3 F7 4 5A 59 4D 4C E5 D2 67 E8 A9 24 93 FB 37 £÷tZYMLåÒgè@\$" 00000180 54 A3 E3 57 43 8A 2E EB 17 F7 B1 72 BB 0C 9E E0 T£äWCŠ.€.g±rs. 00000190 78 7F 82 9F D9 A0 E8 B6 0B CF D2 C9 00 00 00 x., YÙ èq.ÍČÉ. 00000180 D9 29 26 CA BF D7 HB S FF S1 A8 S3 50 1B FF D ÅÉ KE MØ 00000100 37 0C 4C 88 87 16 82 F9 94 D9 AD B8 E6 C0 05 7.1.~~gm,ù~U`.æ 00000100 37 C4 C8 A8 71 60 82 F9 94 D9 AD B8 E6																				
00000180 54 A3 E3 57 43 8A 2E EB 17 E7 B1 72 BB 0C 9E E0 T£äWCŠ.ë.g±r». 00000190 78 7F 82 9F D9 A0 E8 B6 0B CF D2 C9 00 00 00 00 x., ŶD è1.ĨÒÉ 00000100 51 E2 A7 FA 5B 26 16 22 1F CE B3 12 BE C5 9C C6 Qâ\$ú[6.".Ĩ ² .¾Å 00000100 51 E2 A7 FA 5B 26 16 22 1F CE B3 12 BE C5 9C C6 Qâ\$ú[6.".Ĩ ² .¾Å 00000100 51 E2 A7 FA 5B 26 16 22 1F CE B3 12 BE C5 9C C6 Qâ\$ú[6.".Ĩ ² .¾Å 00000100 37 0C 4C 88 A8 71 6D 82 F9 94 D9 AD B8 E6 C0 05 7.L ⁻ gm, À'D., ¾ 00000100 35 17 24 F2 1C 9D A3 E6 39 A6 03 62 C5 BC 0E 9C 5.\$ò£æ9!.bÅ¥ 00000100 35 17 24 F2 1C 9D A3 E6 39 A6 03 62 C5 BC 0E 9C 5.\$ò£æ9!.bÅ¥ 00000100 7F 54 C D7 13 AD A0 96 23 1E 3F 3D D3 D2 CD 3A .čL×=4.?=?bÅ¥ 00000200 BD E BA A4 A6 B6 41 9B 2B C1 0C 3A D5 7F ED 4B ₩₽°×!(¶A>+Å.i.ö. 00000220 AD 95 B6 6D 3D CD 68 AF 8E 29 18 E5 64 F4 F2 F5 .·gm=ĺn ⁻ Ž).ådô 00000220 AD 95 B6 6D 3D CD 68 AF 8E 29 18 E5 64 F4 F2 F5 .·3 [*] .*.%ýÝT 00000220 E1 CD E2 25 4B FD 48 4B 9A 24 0A 3B CD ED 72 77 áláškýHŠ\$.;ĺ1 00000220 E1 CD E2 25 4B FD 48 4B 9A 24 0A 3B CD ED 72 77 áláškýHŠ\$.;ĺ1 00000220 64 AA CD F6 CE 11 3F 3A 63 8B 48 1F 2B 72 E2 43 3																				
$\begin{array}{cccccccccccccccccccccccccccccccccccc$																				
$\begin{array}{cccccccccccccccccccccccccccccccccccc$						-						_								
000001C0 37 0C 4C 88 A8 71 6D 82 F9 94 D9 AD B8 E6 C0 05 7.L^^gm,ù"Ù.æ 000001D0 35 17 24 F2 1C 9D A3 E6 39 A6 03 62 C5 BC 08 9C 5.\$ô£æ\$;.bÅ* 000001E0 ED F5 75 D8 FE 34 7D C3 58 68 D7 D7 34 9A BF 3B iõu@p4)ÅXh××4š 000001E0 FD F5 4C D7 13 AD A0 96 23 1E 3F 3D D3 D2 CD 3A .čLׇ.?=ôô 00000200 BD DE BA A4 A6 B6 41 9B 2B C1 0C 3A D5 7F ED 4B 'MP°¤(¶A>+Á.:õ. 00000210 AD 95 B6 6D 3D CD 68 AF 8E 29 18 E5 64 F4 F2 F5 .gm=îh¯Ž).ådô 00000220 D0 00 00 33 88 0D B2 2E AE 13 FD 76 66 5A EE 3^.f.@.ývf 00000220 E1 CD E2 25 4B FD 48 4B 9A 24 0A 3B CD ED 72 77 áfákýHK\$\$.;11 00000220 96 4A AC DF 6C E1 3F 3A 63 8B 48 1F 2B 72 E2 43 -J¬Blá?: <h.+ť< td=""></h.+ť<>	000001	1A0	51																	
000001D0 35 17 24 F2 1C 9D A3 E6 39 A6 03 62 C5 BC 0E 9C 5.\$è£m9; bÅ+ 000001E0 ED F5 75 D8 FE 34 7D C3 58 68 D7 D7 34 9A BF 3B iõup04)ÅXh×4š 000001F0 07 F5 4C D7 13 AD A0 96 23 1E 3F 3D D3 D2 CD 3A .ŏLׇ.?=ÓÒ 00000200 BD BA A4 A6 B6 41 9B 2B C1 0C 3A D5 7F ED 4B \%P`#!(A)+Å.iõ. 00000210 AD 95 B6 6D 3D CD 68 AF 8E 29 18 E5 64 F4 F2 F53*.*3*.*.@vyf 00000220 00 00 00 33 88 0D B2 2E AE 13 FD 76 66 5A EE3*.*.@vyf 00000230 E1 CD E2 25 4B FD 48 4B 9A 24 0A 3B CD ED 72 77 åfå&KyHK3\$.;11 00000240 96 4A AC DF 6C E1 3F 3A 63 8B 48 1F 2B 72 B2 43 -J~BåA?:<	000001	1B0	D9	29	26	CA	BF	D7	4B	A5	FF	51	A8	53	50	1B	FF	40	Ù)&Ê¿×K	fÿQ"SP.
000001E0 ED F5 75 D8 FE 34 7D C3 58 68 D7 D7 34 9A BF 3B iõu@p4)ãXh××4š 000001F0 07 F5 4C D7 13 AD A0 96 23 1E 3F 3D D2 CD 3A .õL×#.?=ÔÒ 00000200 BD BA A4 A6 B6 41 9B 2B C1 C2 3A .õL×#.?=ÔÒ 00000210 AD 95 B6 6D 3D CD 68 AF 8E 29 18 E5 64 F4 F2 F5 .fm=fh~Z) .ådô 000000220 00 00 03 88 0D B2 E 13 FD 76 A ##.f~Z .strime fh~Z) .ådô 3^* : .strim=fh~Z) <td< td=""><td>000001</td><td>1C0</td><td>37</td><td>0C</td><td>4C</td><td>88</td><td>A8</td><td>71</td><td>6D</td><td>82</td><td>F9</td><td>94</td><td>D9</td><td>AD</td><td>B8</td><td>E6</td><td>C0</td><td>05</td><td>7.L^"qm,</td><td>ù″Ù.,æi</td></td<>	000001	1C0	37	0C	4C	88	A8	71	6D	82	F9	94	D9	AD	B8	E6	C0	05	7.L^"qm,	ù″Ù.,æi
000001F0 07 F5 4C D7 13 AD A0 96 23 1E 3F 3D D3 D2 CD 3A .öL*#.?=ÓÒ 00000200 BD DE BA A4 A6 B6 41 9B 2B C1 0C 3A D5 7F ED 4B %F°#\\$A>+Å.:Õ. 00000210 AD 95 B6 6D 3D CD 68 AF 8E 29 18 E5 64 F4 F2 F5 .·¶m=fn ⁻ Ž).ådõ 00000220 00 00 00 33 88 0D B2 2E AE 13 FD 76 66 5A EE3°.*.⊗.ývf 00000230 E1 CD E2 25 4B FD 48 4B 9A 24 0A 3B CD ED 72 77 áfá≹kýHKŠ\$.;11 00000240 96 4A AC DF 6C E1 3F 3A 63 8B 48 1F 2B 72 B2 43 -J¬Blá?: <h.+t< td=""><td>000001</td><td>1D0</td><td>35</td><td>17</td><td>24</td><td>F2</td><td>1C</td><td>9D</td><td>A3</td><td>E6</td><td>39</td><td>A6</td><td>03</td><td>62</td><td>C5</td><td>BC</td><td>0E</td><td>9C</td><td></td><td></td></h.+t<>	000001	1D0	35	17	24	F2	1C	9D	A3	E6	39	A6	03	62	C5	BC	0E	9C		
00000200 BD DE BA A4 A6 B6 41 9B 2B C1 0C 3A D5 7F ED 4B ₩P°¤(¶A)+Á.:Ô. 00000210 AD 95 B6 6D 3D CD 68 AF 8E 29 18 E5 64 F4 F2 F5 .•¶m=ĺh¯Ž).ådô 00000220 00 00 00 03 38 80 DB 22 EAE 13 FD 76 66 5A EE3^.*.®.ývf 00000230 E1 CD E2 25 4B FD 48 4B 9A 24 0A 3B CD ED 72 77 áĺá&kýHKš\$.;ĺi 00000240 96 4A AC DF 6C E1 3F 3A 63 8B 48 1F 2B 72 B2 43 -J¬Blá?:c <h.+r< td=""><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></h.+r<>																				
00000210 AD 95 B6 6D 3D CD 68 AF 8E 29 18 E5 64 F4 F2 F5 .•¶m=fh ⁻ Ž).ådð 00000220 00 00 00 33 88 0D B2 2E AE 13 FD 76 66 5A EE3 [•] . [*] .⊗.ývf 00000230 E1 CD E2 25 4B FD 48 4B 9A 24 0A 3B CD ED 72 77 áÍâ%KýHKš\$.;Íí 00000240 96 4A AC DF 6C E1 3F 3A 63 8B 48 1F 2B 72 B2 43 -J¬ßlá?:c <h.+r< td=""><td></td><td></td><td></td><td></td><td></td><td>_</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></h.+r<>						_														
00000220 00 00 00 00 33 88 0D B2 2E AE 13 FD 76 66 5A EE3 [.] . ⁴ .⊗.ývf 00000230 E1 CD E2 25 4B FD 48 4B 9A 24 0A 3B CD ED 72 77 áÍâ\$KýHKš\$.;Íí 00000240 96 4A AC DF 6C E1 3F 3A 63 8B 48 1F 2B 72 B2 43 -J¬ßlá?:c <h.+r< td=""><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></h.+r<>																				
00000230 E1 CD E2 25 4B FD 48 4B 9A 24 0A 3B CD ED 72 77 áÍâ\$KýHKŠ\$.jĺi 00000240 96 4A AC DF 6C E1 3F 3A 63 8B 48 1F 2B 72 B2 43 -J-Blá?:c <h.+r< td=""><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>_</td><td></td><td></td><td></td><td></td><td></td><td></td><td>_</td><td></td><td></td></h.+r<>											_							_		
00000240 96 4A AC DF 6C E1 3F 3A 63 8B 48 1F 2B 72 B2 43 -J-Blá?:c <h.+r< td=""><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></h.+r<>																				
																			-	
	000002	240	30	AF	AC	DE	50	21	21	AC	03	20	10	11	20	22	52	10	-0-bia?	con.+r

~

Session Tickets

- Not seemingly in widespread use with IIS?
 Comes around w/ Server 2012 R2
 Documentation is lacking.
- Enabled via reg key + powershell cmdlets?
 Creates an "Administrator managed" session ticket key
- Schannel functions related to Session Tickets load the keyfile from disk
- Export-TlsSessionTicketKey :D

Administrator: C:\Windows\system32\cmd.exe - powershell –	х
PS C:\> mkdir \KeyConfig	^
Directory: C:\	
Node LastWriteTime Length Name	
d 7/24/2016 3:21 PM KeyConfig	
PS C:\> \$Password = Read-Host -AsSecureString	
<pre>PS C:\> New-TlsSessionTicketKey -Password \$Password -Path "C:\KeyConfig\TlsSessionTicketKey.config" PS C:\> Enable-TlsSessionTicketKey -Password \$Password -Path "C:\KeyConfig\TlsSessionTicketKey.config" -ServiceAccount ne "NetworkService" PS C:\> Enable-TlsSessionTicketKey -Password \$Password -Path "C:\KeyConfig\TlsSessionTicketKey.config" -ServiceAccount ne "System" PS C:\> New-ItemProperty -Path HKLM:\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL -Name EnableSession et -Value 1 -PropertyType DWORD</pre>	tNa
EnableSessionTicket : 1 PSPath : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Securi roviders\SCHANNEL PSParentPath : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Securi roviders PSChildName : SCHANNEL PSDrive : HKLM PSProvider : Microsoft.PowerShell.Core\Registry	-

Session Ticket Key

- Keyfile contains a DPAPI blob, preceded by a SessionTicketKey GUID + 8 byte value
- Key gets loaded via schannel
 - □ The heavy lifting (at least in Win10) is done via mskeyprotect
- AES key derived from decrypted blob via BCryptKeyDerivation()
- Key gets cached inside mskeyprotect!
 - No symbols for cache : /
 - □ No bother, we can just find the Key GUID that's cached with it :D

₩0 HxD	- [C:\F	Progra	mDa	ta∖M	licro	soft\	Сгур	to\T	lsSes	sion	Ticke	etKey	/s\S-	1-5-2	20\Se	ssio	nTick	:etK — □ >	<
📓 File	Edit	Searc	h V	iew	Ana	lysis	Ext	ras	Wind	dow	?							_ 8	x
🗋 🙆	-	Sum (3	+ +	16		\sim	AN	SI		\sim	he	x	~	-				
📓 Sessi	ionTic	ketKey	/.key																
Offse	t (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	OD	0E	OF		^
00000	0000	01	00	00	00	BE	E4	Α4	E0	F9	E 5	D1	01	9E	81	06	07	%ä¤àùåÑ.ž	
00000	0010	6F	A8	89	4F	BB	0C	E5	СВ	35	Β7	9B	36	06	01	00	00	o¨‰O».åË5∙>6	
00000	0020	01	00	00	00	DO	8C	9D	DF	01	15	D1	11	8C	7A	00	CO	ÐŒ.ßÑ.Œz.À	
00000	0030	4 F	C2	97	EΒ	01	00	00	00	D4	C1	60	18	2D	9F	CC	47	O—ëÔÁ`.−ŸÌG	
00000	0040	A1	6B	00	66	8B	4E	C4	10	04	00	00	00	02	00	00	00	;k.f <nä< th=""><th></th></nä<>	
00000	0050	00	00	10	66	00	00	00	01	00	00	20	00	00	00	03	56	fV	
00000		FD	BD	75	FD	E9	FE	29	Α9	8B	FD	81	F4	09	8F	57	BA	ý‱uýéþ)©ký.ôW°	
00000		AC	1D	A 0	32	E7	17	3C	59	5A	02	D1	C7	7A	C8	00	00	¬. 2ç.≺YZ.ÑÇzÈ	
00000		00	00	0E	80	00	00	00	02	00	00	20	00	00	00			€ \«	
00000		EB	D7	EC	61	73	91	Α4	2F	FA	C8	AO	73	03	59	4B	1A	ë×ìas`¤∕úÈ́s.YK.	
00000		32	D3	0E	28	EB	A 8	9E	2F	14	8E	B5	45	4B	В1	30	00	2Ó.(먞/.޵EK±0.	
00000		00	00	A2	DA	10	24	AD	C7	30	BF	45	A1	CA		27	2C	¢Ú.\$.Ç0¿E;Ê.',	
00000		18	A5	2D	FO	E4	33	E9	В9	64	DO	42	Β4	DO		E8	AA	.¥-ðä3é'dÐB'Ðìè*	
00000		AF	88	BB	89	A5	D1	47	6B	02	99	87	0C	A 8			85	_^»‰¥ÑGk.™‡.¨¬Z…	
00000		D4	24	40	00	00	00	F5	F4	3C	D8	55	FC	FO	AC		70	Ô\$@õô<ØUüð¬Ýp	
00000		39	C4	AA	8A	BB	В4	72	55	27	B8	4B	BD	F1		42	5C	9İŠ≫´rU',K∿≦ñ.B∖	
00000		A9	D1	29	84	FC	6C	0C	5A	BB	E3	E2	E1	F4		16	В1	©Ñ)"ül.Z»ãâáô±	
00000		10	B9	1D	9E	40		A 8	F7	53	83	9A	E3	32	92	97	30	.¹.ž@¨÷Sfšã2′—0	
00000	0120	FA	OF	F7	96	E9	D4											ú.÷-éÔ	Υ.
Offset: 0																		Overwrite	.:



Possibly Salt or MAC?

Session Ticket Key GUID



Size of ensuing DPAPI Blob

DPAPI Blob (contains it's own fields)

Decrypting Session Tickets

- □ Session Ticket structure pretty much follows the RFC (5077), except:
 - MAC & Encrypted State are flipped (makes a lot of sense)
- □ After extracting/deriving the Symm key, it's just straight AES 256
- □ Contents of the State are what you'd expect:
 - □ Timestamp
 - □ Protocol/Ciphersuite info
 - □ MS struct

🛃 *Local Area Connection (ip host 172.25.20.63)																	
<u>F</u> ile	<u>E</u> dit	<u>V</u> iew	<u>G</u> o	<u>C</u> aptu	ure <u>A</u>	nalyze	<u>S</u> tati	stics	Telep	hony	<u>W</u> ireless	<u>T</u> ools	<u>H</u> elp				
	٥	0	010	X	9	<pre> </pre>	€ 🖻	1	J. 📃		\odot \odot	Q 🎹					
ssl.handshake.session_ticket																	
No.	т	ime		Source				Des	tination	1		Protoco	ol	Length	Info		
1	21 0	.17504	10	172.2	25.20	.63		172	.25.2	20.72		TLSv1	.2	38	0 New 3	Session	Ticke.
	23 0	.18393	76	172.2	25.20	.63		172	.25.2	20.72		TLSv1	2	38	0 New 1	Session	Ticke.
 Transmission Control Protocol, Src Port: 443 (443), Dst Port: 35093 (35093), Seq: 1160, Ack: 667, Lt Secure Sockets Layer TLSv1.2 Record Layer: Handshake Protocol: New Session Ticket Content Type: Handshake (22) 																	
Version: TLS 1.2 (0x0303) Length: 270																	
•			. 270														÷.
0020	14	48 01	bb 8	9 15 9	91 e7	9b 1	2 8f	5b 93	3 d1 9	50 18	.н		.[P.				
0030		fe e9							0 01 0			· · · · · ·					- 1
0040 0050		8c a0 bb 0c							76fa F212					K	ey Gl	JID	
0060		84 e5				- 20 4 ed e		40 di				.5 6J ((0			11.7		
0070		58 81				5e 6				03 3d		^i			IV		J
0080	9c	84 5a	21 a	e 1a	dc cc	37 d	e c1	3f f9	9 32 6	6f 43	z!		.?.200		MAG	~	л I
0090	f2	f0 e1			a7 99	6d a	a 14	be 74	1 2a e	e2 d7							-
00a0	67			e fa		b4 1				ee e6			~	1			
00b0 00c0	са 86			0 1b 1 4 b0		06 5		e1 00		e3 69		0WI		:			
00d0	ea			4 00. 5 ec 1		05 8 75 1		d7 83 06 b0		14 0d 65 ee		0 u.		ι Ε	ncryp	ted	
00e0	a7			8 55		f7 f		f5 80		d8 4f		KU					¦
00f0		77 bf							1 79 4			< m.		-	TLS		¦
0100	bd	73 6d	53 4	2 0d	69 aa	cd 0	6 06	de f@	5 1 e 1	17 25		8.i			State	е	; L
0110	b7	c1 ad	9c a	5 87	32 71	a7 4	9 b5	60 8a	a 43 8	8b d9		2q .I		-	-		1
0120	c5		80 8		39 2b	c6 7			7 b5 (9+ .z		-			i i
0130		05 58							9 99 a			4.		!		· ·	_i
0140	93	74 fb	9f f	4 0b :	35 c2	1e 1	4 03	03 00	0 01 0	01 16	.t	5 <mark>.</mark>					
🔴 🝸 New Session Ticket (ssl.handshake.session_ticket), 260 bytes 🛛 Packets: 184537 · Displayed: 2 (0.0%)																	

Decrypting Session Tickets

						(hex)	dec13ff9326f43f2f0e1db13ffa7996daa14be742ae2d7673f735f0efa99b6b4107bf73e9feee6cac2 30bc401b9005065746e100ede3698644ce5040b30a4058e2d78386140dea57714d85ecf487514d0 06b04d65eea76bd0c45855c691f7fda0f58cd8d84f0377bf864b808206da8a58f51794e5dbd736d53
🧃 *Local Area C	Connection (ip host 172.25.20.63)						420d69aacd0606def61e1725b7c1ad9ca5873271a749b5608a438bd9c51e99808d03392bc67ab8b157 h56cr3fh0558h3h7ahr19934f180f24999arc99374fh9ff40h35c21e
	ew <u>G</u> o <u>C</u> apture <u>A</u> nalyze <u>S</u>						Plaintext Hex Autodetect: ON OFF
🧉 📕 🙋 🏵]]. 🛅 🗙 🛅 🍳 👄 🔿	😤 🗿 🖢 🚍 🚍 🔍	ର୍ ବ୍ 🎹			Function:	AES *
ssl.handshake	e.session_ticket			Expression +		Mode:	CBC (cipher block chaining)
No. Time		Destination	Protocol	Length Info			
21 0.17		172.25.20.72	TLSv1.2	380 New Session Ticket, Change Cipher Spec, Hello Req		Key: (hex)	6f 6d 75 1d 89 3a 87 51 eb dc 6d 27-de d0 41 68 ba fc bd 1c ab 5c 5f 60 d7 97 4e 99-f6 06 5c 79
23 0.18	33976 172.25.20.63	172.25.20.72	TLSv1.2	380 New Session Ticket, Change Cipher Spec, Hello Req			Plaintext Hex
	380 bytes on wire (3040 b					Init. vector:	4a b5 46 af 21 2e ce b9 84 e5 27 28 28 51 0f ed
▷ Internet P	II, Src: Vmware_df:02:a2 (Protocol Version 4, Src: 1	172.25.20.63, Dst: 172	2.25.20.72	E			> Encrypt! > Decrypt!
Iransmissi 4 Secure Soc		Port: 443 (443), Dst	Port: 35093 (3509	3), Seq: 1160, Ack: 667, Len: 326			
	2 Record Layer: Handshake tent Type: Handshake (22)	Protocol: New Session	Ticket			Initialization vect	ctor:
Vers	sion: TLS 1.2 (0x0303) gth: 270					4ab546af212ece	ceb984e5272828510fed (256 bits)
	01 bb 89 15 91 e7 9b 12					Decrypted text:	
	e9 85 00 00 16 03 03 01		НР.	Command - Dump C:\Users\jkambic\Downloads_DEFCON-BH\session	Ticket for decrypt Isass,DMP		
	a0 01 04 00 00 00 00 9e	81 06 07 6f a8 89	·····	0:000> s -b 0 L?80000000000000 9e 81 06 07 6f;.e		00000000 0	00 00 00 00 20 00 00 00 80 00 00 25 03 09 80
	0c e5 cb 35 b7 9b 36 4a e5 27 28 28 51 0f ed e2)5 6J.F.!	00007ffb`adacf9a0 9e 81 06 07 6f a8 89 4f-bb 0c e		0000010 a	a0 00 00 14 00 00 0c 34 4c c5 06 e6 d1 01 Ü4LÅ.æÑ.
	81 f3 d2 af c7 c1 5e 69		X ^i=	0:000> dpp 00007ffb`adacf9a0-20 L60/\$ptrsize;.echo		0000020 0	00 00 00 00 ff 00 00 00 34 00 00 00 4c 00 00 00ÿ4L
	5a 21 ae 1a dc cc 37 de	c1 3f f9 32 6f 43 .	.Z! 7?.2oC	00007ffb`adacf980 0000218`120155d0 0050005c`003a	0043	0000030 8	80 00 00 00 00 00 00 00 00 00 00 00 00 0
	e1 db 13 ff a7 99 6d aa		t*	00007ffb`adacf988 00000000`0000000		00000040 0	00 04 00 00 30 c0 00 00 1d 00 00 00 1d 21 c1 d80À
	73 5f 0e fa 99 b6 b4 10 30 bc 40 1b 90 05 06 57		;?s{.≻i .0.@WFi	00007ffb`adacf990 0000000`0000f10 00007ffb`adacf998 00000218`12882ca0 0000000`0000	0000	00000050 2	22 bb b9 18 4c 00 00 03 5 6c 73 73 03 03 00 00 "» ¹ . L 5 1 s s
	ce 5c 04 b0 30 a4 05 8e		D.\0.	00007ffb`adacf9a0_4f89a86f`0706819e		0000060 3	30 c0 00 00 00 00 00 00 00 00 00 00 00 00
	71 4d 85 ec f4 87 75 14	d0 06 b0 4d 65 ee .	WqM uMe.	00007ffb`adacf9a8 369bb735`cbe50cbb 00007ffb`adacf9b0 01d1e5f9`e0a4e4be			66 e7 41 8c dd 24 d9 e4 7e f8 98 f2 e0 75 dd 8d fçA.Ý\$Ùä-øòàuÝ
	d0 c4 58 55 c6 91 f7 fd		kXU0	00007ffb`adacf9b8 00000000`00000020		00000080 e	e9 d0 a3 06 f4 ad 6b 46 17 71 54 29 9d e3 c4 20 éĐ£.ô.k, f.qT) ãÄ
	bf 86 4b 80 82 02 6d a8		wK mQyN]	00007ffb`adacf9c0 00000218`1288aa00 4d693532`3bc6			08 3d 9e 6e 9d 0a 46 74 b3 91 b9 f6 17 1a be 14 . = . n . Ft ³ ¹ ö K.
	6d 53 42 0d 69 aa cd 06 ad 9c a5 87 32 71 a7 49		smSB.i%	00007ffb`adacf9c8 00000218`1200c770 55555552`0000 00007ffb`adacf9d0 0000000`00000020	0020	[Download as a l	a binary file] [Show more] [Show all] [?] Privacy & Cookies Policy Inactive
	99 80 8d 03 39 2b c6 7a			00007ffb`adacf9d8 00000218`1288a580 857a5754`9123	f91d	4	
0130 fb 05	58 b3 b7 ab c1 99 34 f1	80 f2 49 99 ac c9 .	.X 4I		-		
0140 <mark>93 74</mark>	fb 9f f4 0b 35 c2 1e 14	03 03 00 01 01 16	t5 <mark></mark>	0:000> db pci(00000218'1200c770+10) 00000218'1200c790 6e 02 00 00 4b 53 53 4d-02 00 0	1 00 01 00 00 00 m	KSSM	
🔴 🏹 New S	Session Ticket (ssl.handshake.session	ticket), 260 bytes		00000218`1200c7a0 10 00 00 00 10 00 00 00-00 01 0	0 00 00 00 00 00 .		
					0 00 00 00 00 00 00 0 0 00 6f 6d 75 1d		
				00000218`1200c7d0 89 3a 87 51 eb dc 6d 27-de d0 4	1 68 ba fc bd 1c .	.Q. m'. Ah	
				00000218`1200c7e0 ab 5c 5f 60 d7 97 4e 99-f6 06 5	⊂ 79 00 00 00 00 .	N. N.	
				00000218`1200c7f0 6f 6d 75 1d 89 3a 87 51-eb dc 6 00000218`1200c800 ba fc bd 1c ab 5c 5f 60-d7 97 4	a 27 de dU 41 68 or e 99 f6 06 5c 79	u	
				0:000>			

- • ×

Ŧ

☆ 🗠 🕄

😂 💿 AES Encryption – Easily en 🗙 📃

Text

aes.online-domain-tools.com

dec13ff9326f43f2f0e1db13ffa7996daa14be742ae2d7673f735f0efa99b6b4107bf73e9feee6cac2

C $\leftarrow \rightarrow$

Input type:

Input text:

Secrets are cool and all...

But Jake, what if I don't have a packet capture? (And I don't care about future connections?)

The Context

Inherent Metadata TLS Provides

Core SSL/TLS functionality

- □ Timestamps
 - □ The random values *typically* start with a 4-byte timestamp (if you play by the RFCs)
- □ Identity / fingerprinting
 - Public Key

□ Session ID*

- □ Offered Cipher Suites / Extensions
- Session ID's are arbitrary, but are not always random -> Schannel is a perfect example
 - uses MaximumCacheEntries parameter when creating the first dword of the random, leading to a(n imperfect) fingerprint of two zero bytes in 3/4th byte*

TLS Extensions

- Server Name Indication (SNI)Virtual hosts
- Application-Layer Protocol Negotiation (ALPN)
 Limited, but what protocol comes next
 fingerprinting?
- Session Tickets
 - 🔲 Key GUID

Schannel Caching Parameters

Parameters:

- The following control upper-limit of cache time: m_dwClientLifespan m_dwServerLifespan m_dwSessionTicketLifespan
- ❑ All of which: are set to 0x02255100 (10hrs in ms)
- □ Also of Interest:
 - m_dwMaximumEntries (set to 0x4e20 or 20,000
 entries by default)
 - m_dwEnableSessionTicket COntrols use of
 session tickets (e.g. 0, 1, 2)
 - m_dwSessionCleanupIntervalInSeconds (Set
 to 0x012c or 300 seconds by default)

HOWEVER:

□ Schannel is the library, the *process* has control

□ Proc can purge its own cache at will

- □ For example, IIS reportedly* purges after around two hours
- Schannel maintains track of process, frees cache items after client proc terminates : <</p>
 - Haven't looked at the exact mechanism
 - As you'll see, the upside is that the Process ID is stored in the Cache

This is your Schannel Cache (x64)

' SSL SESSION CACHE CLIENT ITEM': [0x148, { '**Vftable**': [0x0, ['pointer64', ['void']]], `MasterKey': [0x10, ['pointer64', ['void']]], 'PublicCertificate': [0x18, ['pointer64', ['void']]], 'PublicKey': [0x28, ['pointer64', ['void']]], 'NcryptSslProv': [0x60, ['pointer64', ['void']]], 'SessionIdLen': [0x86, ['short short']], 'SessionId': [0x88, ['array', 0x20, ['unsigned char']]], 'ProcessId': [0xa8, ['unsigned long']], 'MaxLifeTime': [0xB0, ['unsigned long']], 'CertSerializedCertificateChain': [0xB0, ['pointer64', ['void']]], 'UnkList1Flink': [0xB8, ['pointer64', ['void']]], 'UnkList1Blink': [0xC0, ['pointer64', ['void']]], 'UnkCacheList2Flink': [0xC8, ['pointer64', ['void']]], 'UnkCacheList2Blink': [0xD0, ['pointer64', ['void']]], 'ServerName': [0x108, ['pointer64', ['void']]], 'LogonSessionUID': [0x110, ['pointer64', ['void']]], 'CSessCacheManager': [0x120, ['pointer64', ['void']]], 'SessionTicket': [0x138, ['pointer64', ['void']]], 'SessionTicketLen': [0x140, ['int']], }],

Command - Dump \\vmware-host\Shared Folders\Documents\Challenges_TSYS\tools\debug\lsass.... × *Client CACHE ITEM************ 000000d4`125878e0 00007ffa`1ceeal80 schannel!CSessionCacheClientItem::`vftable' Master Secret * 000000d4`125878f0 000000d4`12dd2320 44444442`00000020 Public Cert * 000000d4`12bac8f0 ad 06 00 00 30 82 06 a9-30 82 05 91 a0 03 02 010..... 000000d4`12bac900 02 02 10 0e cb 09 39 b2-b1 01 54 b8 95 70 c7 b29...T..p.. 000000d4`12bac910 2b 7a 47 30 0d 06 09 2a-86 48 86 f7 0d 01 01 0b +zG0...*.H..... 000000d4`12bac920 05 00 30 70 31 0b 30 09-06 03 55 04 06 13 02 55 ...0p1.0...U....U 000000d4`12bac930 53 31 15 30 13 06 03 55-04 0a 13 0c 44 69 67 69 s1.0...U....Digi 000000d4`12bac940 43 65 72 74 20 49 6e 63-31 19 30 17 06 03 55 04 Cert Incl.0...U. 000000d4`12bac950 0b 13 10 77 77 77 2e 64-69 67 69 63 65 72 74 2e ...www.digicert. 000000d4`12bac960 63 6f 6d 31 2f 30 2d 06-03 55 04 03 13 26 44 69 com1/0-..U...&Di * Session ID * Process ID * 000000d4`12587988 00000bc4 Server Name Indication* 000000d4`12e1b500 "www.facebook.com" Session Ticket * 000000d4`12b5ba90 3d e9 b5 6b da b7 a3 7b-6d 0a ff 68 56 b7 a9 9d =..k...{m..hV... 000000d4`12b5baa0 56 01 cb 2e fc 26 ef 76-67 2e 33 cf ed 35 b8 b5 V....&.vg.3..5.. Session Ticket Length * 000000d4`12587a10 00000c0 **Client CACHE ITEM************* 000000d4`12587a50 00007ffa`1ceea180 schannel!CSessionCacheClientItem::`vftable' Master Secret * 000000d4`12587a60 000000d4`12dd1830 44444442`00000020 Public Cert * 000000d4`12eb2850 5c 06 00 00 30 82 06 58-30 82 04 40 a0 03 02 01 \...0..X0..@.... 000000d4`12eb2860 02 02 13 5a 00 02 05 3a-c4 09 8a a2 3d bf fd 5e ...Z...:....=..^ 000000d4`12eb2870 00 01 00 02 05 3a 30 0d-06 09 2a 86 48 86 f7 0d:0...*.H... 000000d4`12eb2880 01 01 0b 05 00 30 81 8b-31 0b 30 09 06 03 55 040..1.0...U. 000000d4`12eb2890 06 13 02 55 53 31 13 30-11 06 03 55 04 08 13 0a ...US1.0...U.... 000000d4`12eb28a0 57 61 73 68 69 6e 67 74-6f 6e 31 10 30 0e 06 03 Washington1.0... 000000d4`12eb28b0 55 04 07 13 07 52 65 64-6d 6f 6e 64 31 1e 30 1c U....Redmond1.0. 000000d4`12eb28c0 06 03 55 04 0a 13 15 4d-69 63 72 6f 73 6f 66 74 ..U....Microsoft * Session ID * 000000d4`12587ad8 25 45 00 00 3f 95 34 ca-3b 79 6f 65 ea 5a 19 af %E..?.4.;yoe.Z.. 000000d4`12587ae8 e4 d1 a9 71 8d 2c c4 db-76 15 25 2b 74 b8 5e 30 ...g.,..v.%+t.^0 * Process ID * 000000d4`12587af8 00000bc4 * Server Name Indication* 000000d4`12dd1010 "pipe.skype.com" * Session Ticket * * Session Ticket Length * 000000d4`12587b80 00000000 0:000> .foreach(cCache (s -[w1]q 0x0 L280000000000 schannel!CSessionCacheClientItem::`vftable'}) (.echo **Client CACHE ITEM****************;dps cCache L1;.echo * Master Secret *;dpp \${cCache}+ 10 L1:.echo * Public Cert *:db poi(\${cCache}+18):.echo * Session ID *:db \${cCache}+88 L20; .echo * Process ID *;dd \${cCache}+a8 L1;.echo * Server Name Indication*;du /c ff poi(\${cCache}+f8);.echo * Session Ticket *;db poi(\${cCache}+128) L20;.echo * Session Ticket Length *;dd \${cCache}+130 L1}

This is your Schannel Cache (x64)

```
'_SSL_SESSION_CACHE_SERVER_ITEM': [ 0x110, {
    'Vftable': [0x0, ['pointer64', ['void']]],
    'NcryptKey': [0x10, ['pointer64', ['void']]],
    'NcryptSslProv': [0x60, ['pointer64', ['void']]],
    'SessionId': [0x88, ['array', 0x20, ['unsigned char']]],
    'ProcessId': [0x88, ['unsigned long']],
    'MaxLifeTime': [0xB0, ['unsigned long']],
    'LastError?': [0xE8, ['unsigned long']],
    'CSslCredential': [0xF0, ['pointer64', ['void']]],
}],
```

Command - Dump \\vmware-host\Shared Folders\Documents\Challenges\zzTmp\hostY\lsa... × 0:000> .foreach(sCache {s -[w1]q 0x0 L?80000000000 schannel!CSessionCacheServerItem::`vftal ~ **SERVER CACHE ITEM************ 000000c9`86d2flc0 00007fff`ed239f90 schannel!CSessionCacheServerItem::`vftable' Master Secret * 000000c9`86d2f1d0 000000c9`86d5f870 44444442`00000020 Session ID * 000000c9`86d2f248 5e 06 00 00 30 4b 18 77-32 15 9c 6a 53 56 75 b6 ^...0K.w2..jSVu. 000000c9`86d2f258 64 6c 63 c5 dd c4 53 3a-8d 0b 42 f5 b6 ef c9 76 dlc...s:..b...v * Process ID * 000000c9`86d2f268 000003b0 * Server Key * 000000c9'86d2f2b0 000000c9'85dbb040 00007fff'ed23b118 schannel!CSslCredential::'vftable' **SERVER CACHE ITEM************ 000000c9`86d2f6c0 00007fff`ed239f90 schannel!CSessionCacheServerItem::`vftable' * Master Secret * 000000c9`86d2f6d0 000000c9`86d60f40 44444442`00000020 * Session ID * 000000c9`86d2f758 3a 06 00 e9 9f b8 77 03-9f 82 c1 be ba 09 42 4a :.....BJ * Process ID * 000000c9`86d2f768 000003b0 Server Kev * 000000c9'86d2f7b0 000000c9'85d5e8e0 00007fff'ed23b118 schannel!CSslCredential::'vftable' **SERVER CACHE ITEM************ 000000c9`86d2f800 00007fff`ed239f90 schannel!CSessionCacheServerItem::`vftable' * Master Secret * 000000c9`86d2f810 000000c9`86d60270 44444442`00000020 * Session TD * 000000c9`86d2f888 a3 40 00 00 08 89 68 b2-a6 06 0f c0 52 b5 eb c4 .@...h....R... 000000c9`86d2f898 58 lb 4b f2 61 47 23 80-16 db 64 7d 34 ef a7 1a X.K.aG#...d}4... * Process ID * 000000c9`86d2f8a8 000003b0 * Server Key * 000000c9`86d2f8f0 000000c9`85dbb040 00007fff`ed23b118 schannel!CSslCredential::`vftable' **SERVER CACHE ITEM*********** 000000c9`86d2fa80 00007fff`ed239f90 schannel!CSessionCacheServerItem::`vftable' * Master Secret * 000000c9`86d2fa90 000000c9`86d60c20 44444442`00000020 * Session ID * 000000c9`86d2fb08 0b 2d 00 00 ab 80 7a 38-e4 9c 64 5c 42 2e 74 d2 .-...z8..d\B.t. 000000c9`86d2fb18 a2 d8 c3 b1 71 17 77 b8-48 f7 93 f8 16 ef 30 03g.w.H.....0. * Process ID * 0:000> .foreach(sCache {s -[w1]q 0x0 L?80000000000 schannel!CSessionCacheServerItem:: `vftable'}){.echo **SERVER CACHE ITEM************;dps sCache L1;.echo * Master Secret *;dpp \${sCache}+10 L1;.echo * Session ID *;db \${sCache}+88 L20; .echo * Process

ID *;dd \${sCache}+a8 L1;.echo * Server Key *;dpp \${sCache}+f0 L1;.echo }

This is your Schannel Cache on Drugs Vista

' SSL SESSION CACHE CLIENT ITEM': [0xf0, { 'Flink': [0x0, ['pointer', ['void']]], 'Blink': [0x4, ['pointer', ['void']]], 'ProcessId': [0x8, [['unsigned long']], 'MasterKey': [0x14, ['pointer', ['NcryptSslKey']]], 'CipherSuiteId': [0x1C, ['pointer', ['void']]], 'ECCurveParam': [0x20, ['pointer', ['void']]], 'NcryptSslProv': [0x28, ['pointer', ['void']]], 'PublicCertificate': [0x2C, ['pointer', ['void']]], 'PublicCert2': [0x34, ['pointer', ['void']]], 'PublicKeyStruct': [0x3C, ['pointer', ['void']]], 'PublicCertStruct3': [0x44, ['pointer', ['void']]], 'ServerName': [0x80, ['pointer', ['void']]], 'SessionIdSize': [0x94, ['short short']], 'SessionId': [0x98, ['array', 0x20, ['unsigned char']]], 'ErrorCode': [0xEC, ['pointer64', ['void']]], }],

Command - Dump \\vmware-host\Shared Folders\Documents\Challenge... X *** Cache Item *** * ProcId: 001d76f0 00000cf8 NcrypSslKey: 001d76fc 001dab40 00000018 * SNT: 001d7768 01f9e480 "live.sysinternals.com" * SessionID: 001d7780 59 19 00 00 07 4a 6c cc-d6 b0 e2 b2 5f cd d1 30 Y....J1..... ..0 001d7790 bf ee 06 bl ec 20 e3 57-e3 79 52 72 d7 f5 a5 41W.yRr...A *** Cache Item *** * ProcId: 001d7828 00000cf8 NcrypSslKey: 001d7834 001dabe0 00000018 * SNI: 001d78a0 01fa3cb8 "www.torproject.org" * SessionID: 001d78b8 ba ce 7b 7e ca 6d e8 15-92 e8 ae fb 08 bb 71 83 ...{~.m......q. 001d78c8 e7 87 ed 78 e5 12 f3 c0-24 a3 b6 0b e8 a2 43 b9 ...x...\$......\$....... *** Cache Item *** * ProcId: 001d7960 0000cf8 NcrypSslKey: 001d796c 01fa3f98 00000018 SNI: 001d79d8 01fa3d18 "urs.microsoft.com" * SessionID: 001d79f0 99 0e 00 00 d8 3f de 02-53 c3 68 49 59 89 c2 c0?..S.hIY... 001d7a00 71 ca bd 8f 5f 7b bd 59-08 6c df 44 8c a7 b7 7b g... {.Y.l.D...{ *** Cache Item *** ProcId: 001d7e40 00000cf8 * NcrypSslKey: 001d7e4c 01fa3ed8 00000018 * SNI: 001d7eb8 01f75d88 "login.live.com" SessionID: 001d7ed0 f6 07 00 00 5d 3d bc aa-f7 91 9a 5e f5 3e b7 10]=....^.>.. *** Cache Item *** * ProcId: 001d7bd0 0000cf8 NcrypSslKey: N14754- N16-2670 AAAAAA 0:000> !list -x ".echo *** Cache Item ***;.echo * ProcId:;dd @\$extret+8 L1;.echo * NcrypSslKey:;dpp @\$extret+14 L1;.echo * SNI:;dpu @\$extret+80 L1;.echo * SessionID:; db @\$extret+98 L20" 001d8ba0

Automating it

1

\Lambda black hat usa 2016

Volatility / Rekall

□ Plugins for both – by default (no args) they:

- □ Find LSASS
- Scan Writeable VADs / Heap for Master Key signature (Volatility) or directly for SessionCacheItems (Rekall)
- Dump out the wireshark format shown earlier
- Hoping to have functional powershell module or maybe incorporation into mimikatz? (Benjamin Delphy is kinda the man for LSASS)

% vol.py --plugins=./plugins --profile=Win10x64 -f ./Win10-Test-c2a4a77d.vm em lsasslkey

Volatility Foundation Volatility Framework 2.5

RSA Session-ID:b93c0000a110690b4ae9111bce5725c6c47a037b3c39c49c75ce51e1c2eb79ee M aster-Key:bc28467999b99fd3fdf3a24642c5d93b9ab43e51627f6e0145ef120ba98a1c3223f3dbe 0154e30d7869bdb7ab66f5318

RSA Session-ID:173300000f84a86aebb2c5de0af20e6d5c2cab95ab65043e14c6e19cee54ee17 M aster-Key:9dd750e12e6e4439b08326d4a1f9eba2d2fe65c2a26c2088e7cec22ce1d91e9f219b704 547a2b2eccb9a81d557d5ae1a

RSA Session-ID:3c2c000024b8f70dd2613d8b13d0c4ac4daaefbe53ab4b7cb9763e80feccb4f1 M aster-Key:2d119c64695ffc9c143c136471f5625d8cde92d35721f5f2849b92639603799a45e1e60 1786cbf89b00c186969d44983

RSA Session-ID:d4170000da09f8596739215e216c496568fa66e42ac32b974d440949dff33d2b M aster-Key:44b503bef7842ea9a416fbf8b63b932b23b7b687fbf5297b253eac427877c8e11595e14 c3f00c40bf2a0f4688de0b7aa

RSA Session-ID:432a0000bf4f622f0fc119974a0ef30cd838c3a025b83abbdcdbce7b2325d2d9 M aster-Key:552699d61e21d1b871af4b05a54003bf03eade60666dd1e54b94c3b5ec98f296db4ae99 baed4e23882175e5ffd88be31

RSA Session-ID:6f230000a021aac48d15544524c1454e4ec01d5adb305d8d9d57ab2b991dd597 M aster-Key:8bc9e9df653e3cbf533be84c6897787bd453b8cee9d5389e9c3659ebf997d9c8d0666aa dca5be2258f30b9251215a717

Limitations

□ We're working with internal, undocumented structures

- □ They change over time -- sometime around April 2016, an element appears to have been inserted in cache after the SessionID and before the SNI
 - Not a huge deal, except when differences amongst instances of same OS (e.g. ones that have and have not been updated)

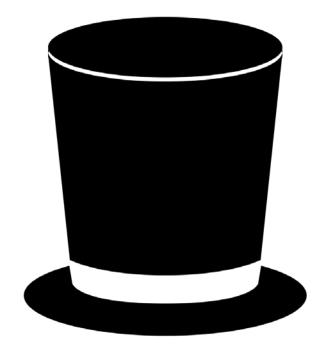
Relying on symbols for some of this

- □ MS giveth and can taketh away.
- □ Still, can be done without them, just slightly less efficiently.

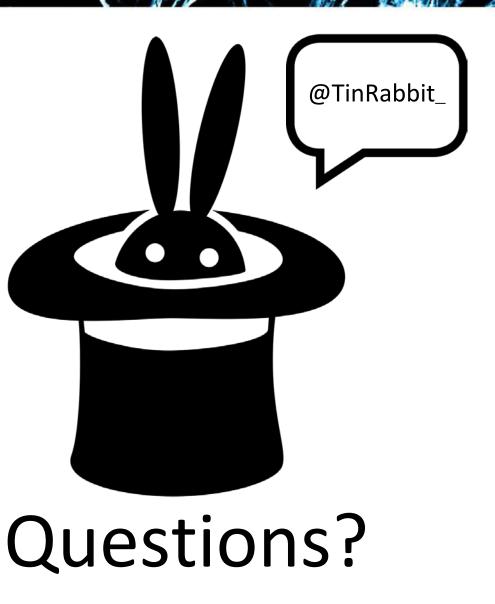
□ You need to be able to read LSASS memory

- □ Not a huge deal in 2016, but still merits mention -- you need to own the system
- □ If you own the system, you can already do bad stuff (keylog / tap net interface)
- □ This is why it's probably most useful in a forensic context

Demo



Fin.



.

Special Thanks

For general support, helpful comments, their time, and encouragement.

Áine Doyle - Badass Extraordinaire (OCSC)
Dr. John-Ross Wallrabenstein - Sypris Electronics
Dr. Marcus Rogers - Purdue Cyber Forensics Laboratory
Michael Hale Ligh (MHL) - Volexity
Tatiana Ringenberg - Sypris Electronics