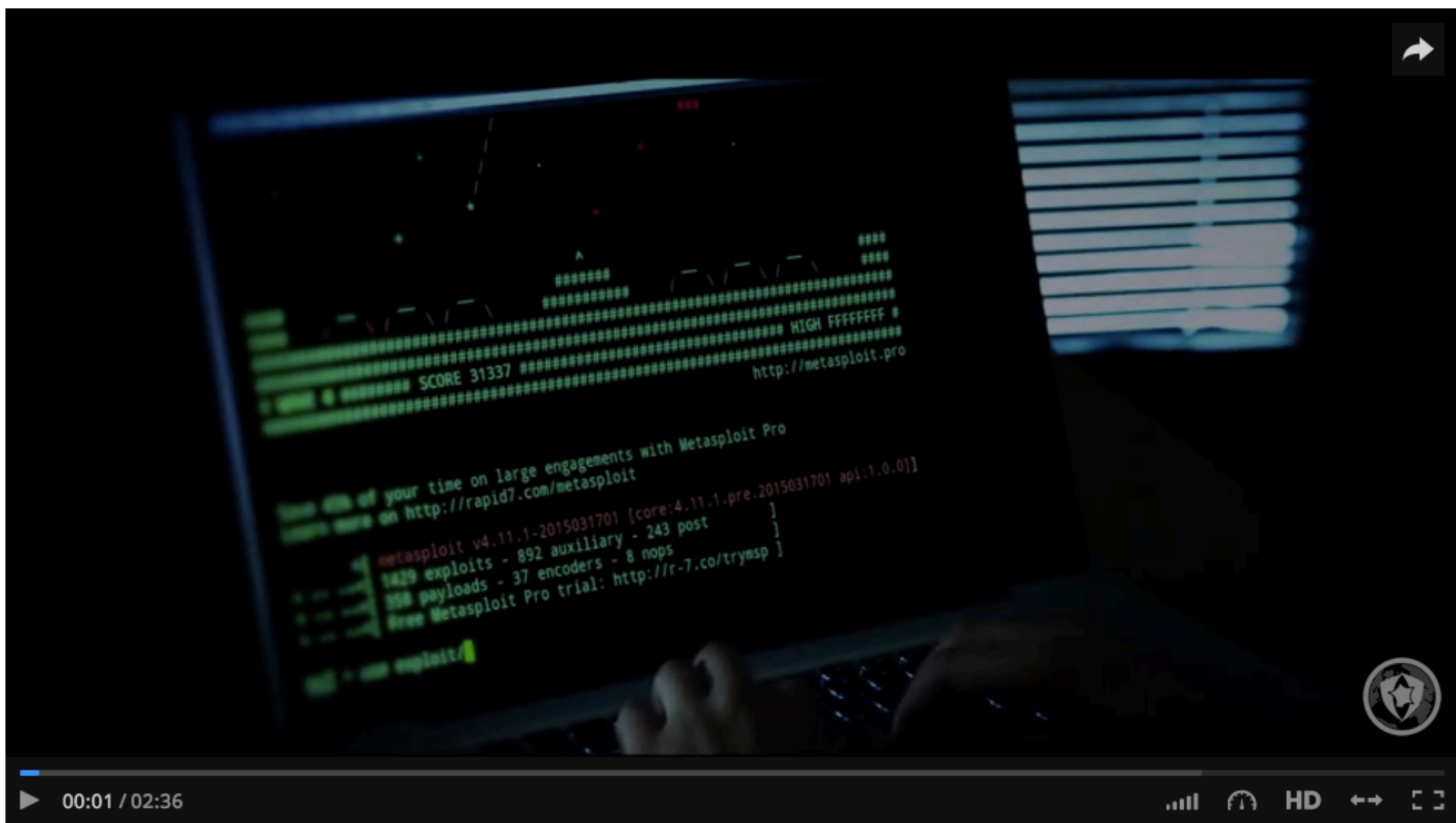


Le véritable challenge ANSSI

Un consultant indépendant



Découvrez l'action de l'ANSSI – une diversité de missions au service de la sécurité du numérique

 J'aime

 Reposter



CHALLENGE ACCEPTED



▶ 00:13 / 02:36



melbourne, Flinders Street Station



Flinders Street Railway Station

4.0 ★★★★★ 91 reviews

Train Station

Directions



SAVE



NEARBY



SHARE

Iconic, domed railway and metro hub, opened in 1909, with a yellow facade and an arched entrance. - Google

Flinders St, Melbourne VIC 3000, Australia

ptv.vic.gov.au

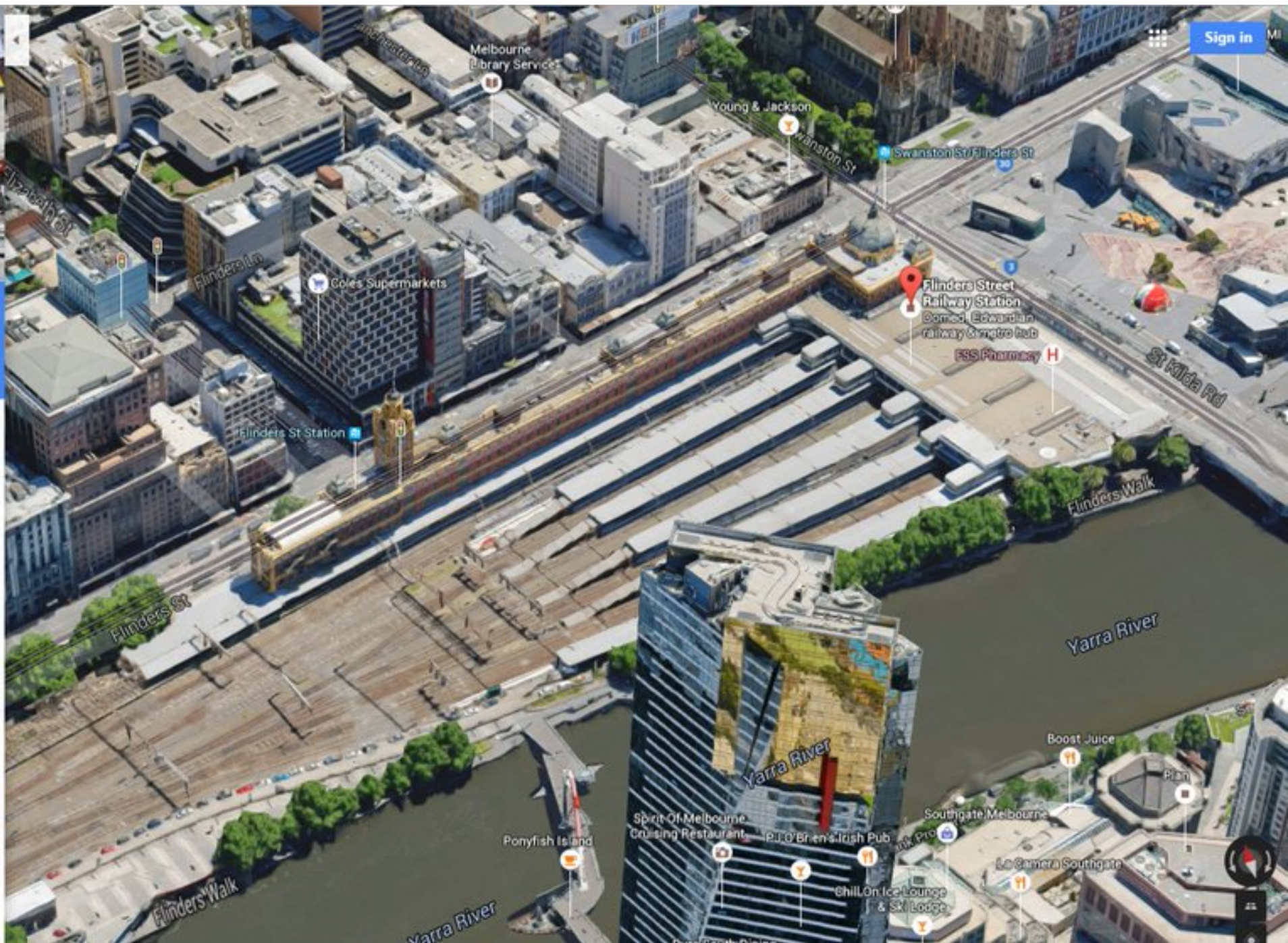
+61 3 9610 7476

Suggest an edit

yarratrams.com.au



Add a photo



Sign in





A problem has been detected and windows has been shut down to prevent damage to your computer.

The problem seems to be caused by the following file: SPCMDCON.SYS

PAGE_FAULT_IN_NONPAGED_AREA

If this is the first time you've seen this stop error screen, restart your computer. If this screen appears again, follow these steps:

Check to make sure any new hardware or software is properly installed. If this is a new installation, ask your hardware or software manufacturer for any windows updates you might need.

If problems continue, disable or remove any newly installed hardware or software. Disable BIOS memory options such as caching or shadowing. If you need to use safe mode to remove or disable components, restart your computer, press F8 to select Advanced Startup options, and then select Safe Mode.

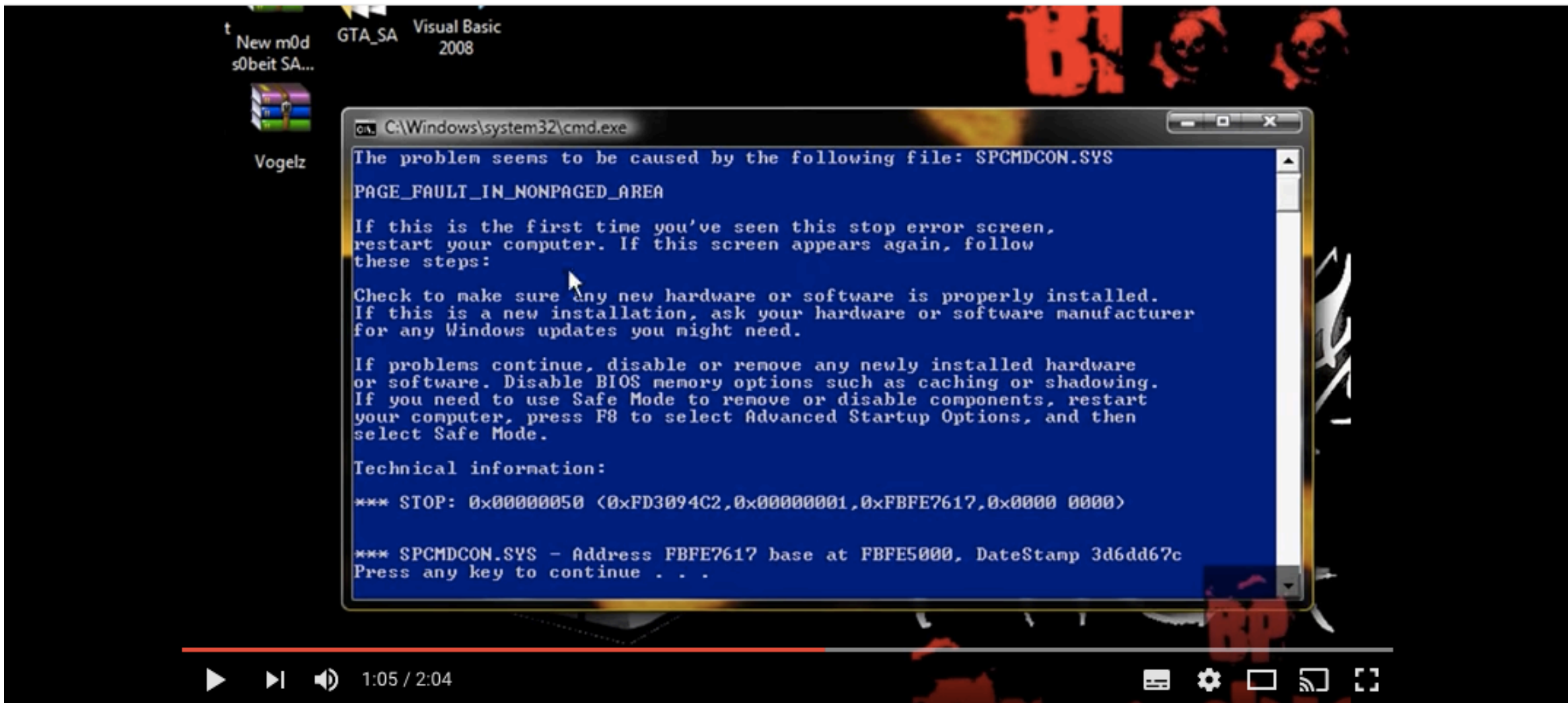
Technical information:

*** STOP: 0x00000050 (0xF03094C2, 0x00000000, 0x00000000, 0x00000000)

*** SPCMDCON.SYS - Address FBFE7017 base at FBFE1000, hexadecimal 70170000

SPCMDCON.SYS





1:05 / 2:04 ⏮ ⏪ 🔊 ⏩ ⏭ ⚙️ 📺 📶 🗑️

How to make a bsod in a notepad!



BloodyPirania

S'abonner 78

42 802 vues

À suivre

Lecture automatique



BSOD in Funny Places

EquinoxDavid
40 625 vues

2:00



71768 ?



00:33 / 02:36

HD



L'Hôtel National des Invalides accueille la direction et la sous-direction Relations extérieures et coordination (RELEC) de l'ANSSI

Courrier postal :

Agence nationale de la sécurité des systèmes d'information
Secrétariat général de la défense et de la sécurité nationale
51, boulevard de La Tour-Maubourg
75700 Paris 07 SP

Téléphone : +33 (0)1 71 75 84 05 ou +33 (0)1 71 75 84 06

Télécopie : +33 (0)1 71 75 84 00

Courrier électronique :

- Écrire à la direction : [secretariat.anssi \[at\] ssi.gouv.fr](mailto:secretariat.anssi@ssi.gouv.fr)
- Question d'ordre général : [communication \[at\] ssi.gouv.fr](mailto:communication@ssi.gouv.fr)



ESCROQUERIE EN LIGNE PORTANT LE LOGO DE L'ANSSI

Numéro d'urgence : 01 71 76 85 98

Un message décrit la marche à suivre en cas de compromission.



Ven 6 nov

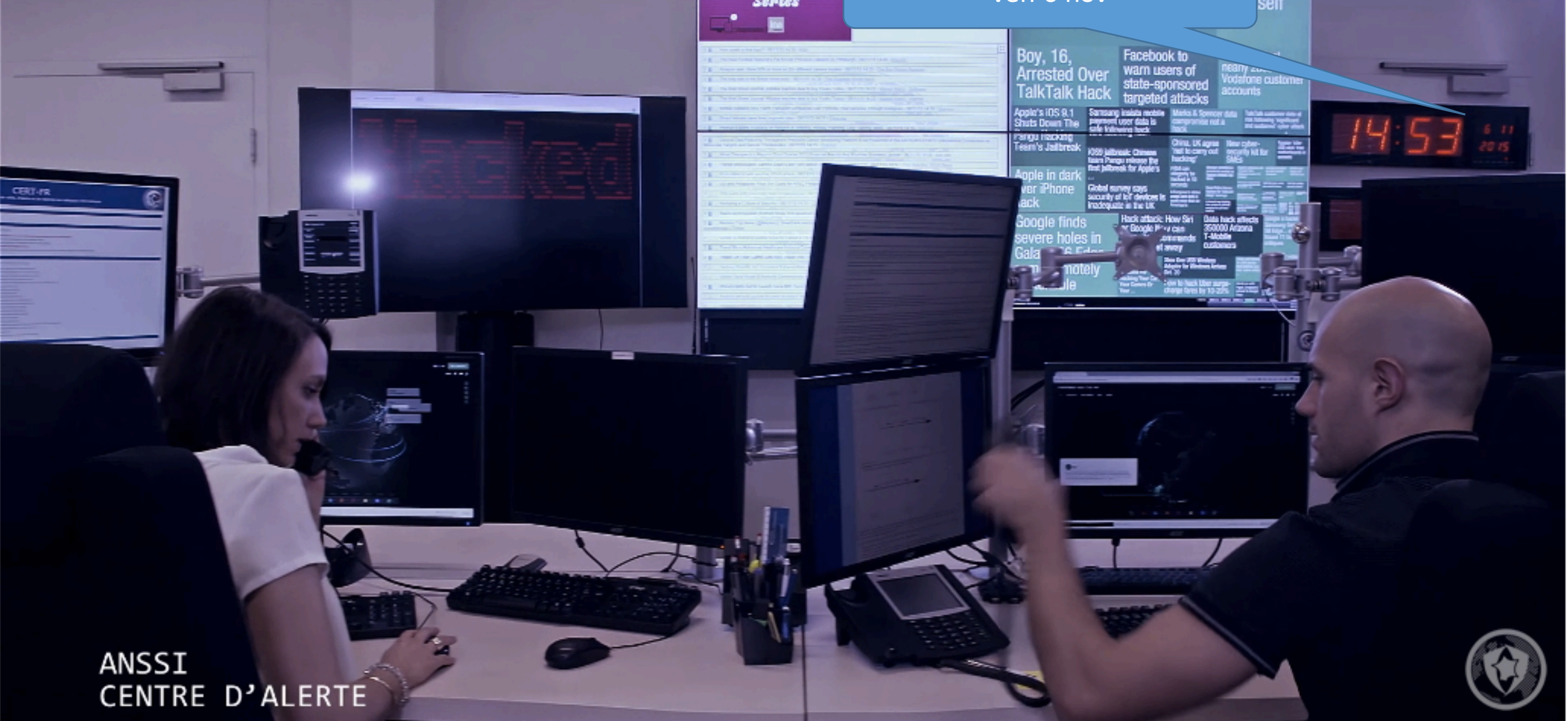


00:34 / 02:36

HD



Ven 6 nov



ANSSI
CENTRE D'ALERTE



00:38 / 02:36

HD



```
2012-10-30 14:40:44 UTC+00:00 1320 svchost.exe ** * 172.16.2.15:442
2012-10-30 14:40:44 UTC+00:00 1320 svchost.exe ** * 127.0.0.1:62660
2012-10-30 12:26:26 UTC+00:00 864 svchost.exe ** * 0.0.0.0:0
2012-10-30 12:26:26 UTC+00:00 864 svchost.exe ** * 0:0:0:0:0:0:0:0
2012-11-05 02:12:22 UTC+00:00 1076 svchost.exe ** * 0.0.0.0:0:28219
2012-11-05 02:12:22 UTC+00:00 1076 svchost.exe ** * 0:28219:0:0:0:0:0:0
2012-10-30 14:28:26 UTC+00:00 4 System ** * 172.16.2.15:138
2012-10-30 14:28:26 UTC+00:00 4 System ** * 172.16.2.15:137
2012-11-05 02:12:22 UTC+00:00 792 LISTENING 0.0.0.0:49154 TCPv4 0.0.0.0:49154
2012-11-05 02:12:22 UTC+00:00 792 LISTENING 0:0:0:0:0:0:0:0 TCPv6 0:0:0:0:0:0:0:0
2012-11-05 02:12:22 UTC+00:00 792 LISTENING 0.0.0.0:0:49154 TCPv4 0.0.0.0:49154
2012-11-05 02:12:22 UTC+00:00 524 LISTENING 0.0.0.0:0:49156 TCPv4 0.0.0.0:49156
2012-11-05 02:12:22 UTC+00:00 524 LISTENING 0:0:0:0:0:0:0:0 TCPv6 0:0:0:0:0:0:0:0
2012-11-05 02:12:22 UTC+00:00 524 LISTENING 0.0.0.0:0:49156 TCPv4 0.0.0.0:49156
2012-11-05 02:12:22 UTC+00:00 660 LISTENING 0.0.0.0:0:132 TCPv4 0.0.0.0:132
2012-11-05 02:12:22 UTC+00:00 660 LISTENING 0:0:0:0:0:0:0:0 TCPv6 0:0:0:0:0:0:0:0
2012-11-05 02:12:22 UTC+00:00 660 LISTENING 0.0.0.0:0:132 TCPv4 0.0.0.0:132
2012-11-05 02:12:22 UTC+00:00 436 LISTENING 0.0.0.0:0:49152 TCPv4 0.0.0.0:49152
2012-11-05 02:12:22 UTC+00:00 436 LISTENING 0.0.0.0:0:49152 TCPv4 0.0.0.0:49152
2012-11-05 02:12:22 UTC+00:00 436 LISTENING 0:0:0:0:0:0:0:0 TCPv6 0:0:0:0:0:0:0:0
2012-11-05 02:12:22 UTC+00:00 724 LISTENING 0.0.0.0:0:49123 TCPv4 0.0.0.0:49123
2012-11-05 02:12:22 UTC+00:00 724 LISTENING 0.0.0.0:0:49123 TCPv4 0.0.0.0:49123
2012-11-05 02:12:22 UTC+00:00 724 LISTENING 0:0:0:0:0:0:0:0 TCPv6 0:0:0:0:0:0:0:0
2012-11-05 02:12:22 UTC+00:00 4 LISTENING 0.0.0.0:0:139 TCPv4 172.16.2.15:139
2012-11-05 02:12:22 UTC+00:00 4 LISTENING 0:0:0:0:0:0:0:0 TCPv6 0:0:0:0:0:0:0:0
2012-11-05 18:00:34 UTC+00:00 1076 svchost.exe ** * 172.16.2.15:139
2012-11-05 18:00:34 UTC+00:00 1076 svchost.exe ** * 172.16.2.15:139
2012-11-05 17:06:10 UTC+00:00 724 svchost.exe ** * 172.16.2.15:139
2012-10-30 12:26:26 UTC+00:00 864 svchost.exe ** * 0.0.0.0:123
2012-10-30 12:26:26 UTC+00:00 864 svchost.exe ** * 0.0.0.0:0
2012-10-30 14:40:44 UTC+00:00 1320 svchost.exe ** * 172.16.2.15:1900
2012-10-30 14:40:44 UTC+00:00 1320 svchost.exe ** * 172.16.2.15:442
----- ESTABLISHED -----
----- ESTABLISHED -----
```



30 octobre 2015

```
anssi@anssi: ~$ volatility -F vm-win8-x86.raw --profile=Win8SP0x86 pslist
Volatility Foundation Volatility Framework 2.4
Offset(V) Name PID PPID Thds Hnds Sess Wow64 Start
-----
0x830041c0 System 4 0 79 0 0 0 2015-10-30 14:28:08 UTC+0000
0x84a7b1c0 smss.exe 268 4 2 0 0 0 2015-10-30 14:28:08 UTC+0000
0x8479d8c0 csrss.exe 372 364 8 0 0 0 2015-10-30 14:28:23 UTC+0000
0x83927040 smss.exe 428 268 0 0 1 0 2015-10-30 14:28:23 UTC+0000
0x83929000 wininit.exe 436 364 2 0 0 0 2015-10-30 14:28:23 UTC+0000
0x839098c0 csrss.exe 444 428 9 0 1 0 2015-10-30 14:28:23 UTC+0000
0x838638c0 winlogon.exe 484 428 3 0 1 0 2015-10-30 14:28:23 UTC+0000
0x838ef400 services.exe 508 436 12 0 0 0 2015-10-30 14:28:23 UTC+0000
0x838ff040 lsass.exe 524 436 8 0 0 0 2015-10-30 14:28:24 UTC+0000
0x84c9f840 svchost.exe 616 508 6 0 0 0 2015-10-30 14:28:24 UTC+0000
0x84c953c0 svchost.exe 660 508 10 0 0 0 2015-10-30 14:28:24 UTC+0000
0x84798540 svchost.exe 724 508 18 0 0 0 2015-10-30 14:28:24 UTC+0000
0x84d63c40 LogonUI.exe 732 484 0 0 1 0 2015-10-30 14:28:24 UTC+0000
0x84d66bcc0 dwm.exe 744 484 7 0 1 0 2015-10-30 14:28:24 UTC+0000
0x84d81040 svchost.exe 792 508 33 0 0 0 2015-10-30 14:28:24 UTC+0000
0x84d98100 svchost.exe 864 508 18 0 0 0 2015-10-30 14:28:24 UTC+0000
```



SRU-Monitor.exe

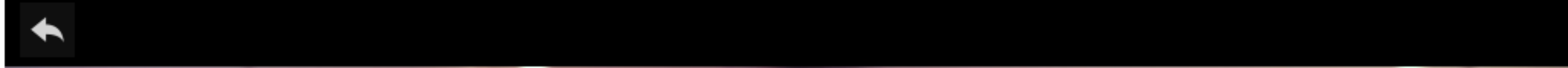


The screenshot displays the SRU-Monitor.exe application interface. On the left, there are several panels: 'Événements' (Events) with a table showing 'Accès à un point d'arrêt' at 0:02 s; 'Utilisation de la mémoire' (Memory usage) with a graph; 'Utilisation du processeur' (CPU usage) with a graph; and 'Outils de diagnostic' (Diagnostic tools) with a 'Zoom avant' (Zoom in) button. The main area on the right is a code editor showing C# code for SRU-Monitor, including methods like 'Encode', 'Decode', and 'LPTSTR_to_string'. A video player overlay is visible in the center, showing a man's face.

02:10 / 02:36

Video player controls including a progress bar, play/pause button, volume icon, HD logo, and window management icons.

Wait



```

Code Machine | Source.cpp | (Portée globale)
...hSurDLL=LoadLibraryEx(TEXT("srumapi.dll"),NULL,LOAD_LIBRARY_SEARCH_SYSTEM32);
..._SruQueryStats=(tSruQueryStats)GetProcAddress(hSurDLL,"SruQueryStats");
...Encode(szText,'sText');//szText is probably an URL...

```

Encode(szText,'sText');//szText is probably an URL...

```

...psruresult=psruresults->results;
...for(DWORD i=0;i<psruResults->dwResultCount;i++)
...{
...LPTSTR szSid=NULL;
...PSRU_ELEMENT sruElement;
...if((psruResult->sruSid.pSid)&&(psruResult->sruSid.sSize))
...{
...Encode(
..._In_reads_bytes_(sInput)LPCTSTR szInput,
..._In_size_t sInput

```

Outils de diagnostic | Variables locales | Automatique | Registres | Threads | Modules

Sélectionner les outils

- Utilisation de la mémoire des (2 ms sélectionnées)
- Utilisation de l'UC 40ms | 5ms | 60ms
- Événements

Événement	Heure	Durée	Thread
Accès à un point d'arrêt	0,05 s	2 ms	[8568]

27 45 40 4d 26 75 08 62 16 08): '#s]]).
f1 6c b0 79 45 18 00 00 00 00 d6 7RP1MM\$uy

0x0000000060A630 29 3a 27 23 73 5d 4a 14 05 02 5a 16 32 27 7d 34 26 07 13 4d 14 07 5b 24 74 0d 12 6a 7a 4a 23 27 45 40 4d 26 75 08 62 16 08): '#s]]...Z.2')48..M..[{\$t..jz]# 'E@M&u.b..
0x00000000CFC9C6DA659 37 52 50 31 4d 4d 24 75 79 10 10 71 47 52 00 fd fd fd fd 00 00 00 00 07 00 00 00 00 00 00 00 00 00 f1 6c b0 79 45 18 00 00 00 d6 7RP1MM\$uy..qGR.ýýýý.....ñl'yE....ö


```
data_in = "29 3a 27 23 73 5d 4a 14 05 02 5a 16 32 27 7d 34  
26 07 13 4d 14 07 5b 24 74 0d 12 6a 7a 4a 23 27 45 40 4d 26  
75 08 62 16 08 37 52 50 31 4d 4d 24 75 79 10 10 71 47 52"
```

```
key = "ANSSIrecrute"
```

```
data_out = ""
```

```
i = 0
```

```
for c in data_in.split(" "):
```

```
    data_out += chr( int(c, 16) ^ ord(key[i % len(key)]) )
```

```
    i += 1
```

```
print data_out
```

<http://www.ssi.gouv.fr/A5CA938FD759C4F1EAE73C89A47CC857>

The Easy Way



A5CA938FD759C4F1EAE73C89A47CC857



Tous

Images

Maps

Vidéos

Actualités

Plus ▾

Outils de recherche


1 résultat (0,34 secondes)

Liens courts | Agence nationale de la sécurité des systèmes d ...

www.ssi.gouv.fr/liens-courts/ ▾

... /uploads/2012/09/ /A5CA938FD759C4F1EAE73C89A47CC857/, /recrutement/.

/fr/sigelec/igca/revocation/DEL/igca4096.crl/, /uploads/2014/11/ ...

/defense-profondeur/	/guide/70-la-defense-en-profondeur-appliquee-aux-systemes-dinformation/
/politique-filtrage-parefeu/	/guide/recommandations-pour-la-definition-dune-politique-de-filtrage-reseau-dun-pare-feu/
/attaque-idns/	/actualite/vulnerabilite-dns-critique-attaque-en-deni-de-service-par-recursion-infinie-affectant-bind-unbound-et-powerdns-recursor/
/block-dns-msg/	/agence/publication/demonstration-dun-detournement-possible-de-technologies-anti-deni-de-service-distribue-ddos/
/maturite-ssi/	/administration/guide/50-guide-relatif-a-la-maturite-ssi/
/ebios/	/guide/ebios-2010-expression-des-besoins-et-identification-des-objectifs-de-securite/
/javasec/	/agence/publication/securite-et-langage-java/
/tbssi/	/guide/30-tbssi-guide-delaboration-de-tableaux-de-bord-de-securite-des-systemes-dinformation/
/gissip/	/guide/40-gissip-guide-dintegration-de-la-securite-des-systemes-dinformation-dans-les-projets/
/profils-metiers-ssi/	/entreprise/formation/profils-metiers/
/passerelle-interconnexion/	/guide/definition-dune-architecture-de-passerelle-dinterconnexion-securisee/
/fr/produits-et-prestataires/	/entreprise/produits-certifies/
/emet/	/guide/deploiement-et-configuration-centralises-demet-pour-le-durcissement-des-postes-de-travail-et-des-serveurs-microsoft-windows/
/agence/cybersecurite/ozssi/	/agence/cybersecurite/action-territoriale/
/pris/	/administration/qualifications/prestataires-de-services-de-confiance-qualifies/prestataires-de-reponse-aux-incidents-de-securite-pris/
/pdis/	/administration/qualifications/prestataires-de-services-de-confiance-qualifies/prestataires-de-detection-dincidents-de-securite-pdis/
/uploads/IMG/pdf/NP_IPsec_NoteTech.pdf/	/uploads/2012/09/
/A5CA938FD759C4F1EAE73C89A47CC857/	/recrutement/ 
/fr/sigelec/igca/revocation/DEL/igca4096.crl/	/uploads/2014/11/