Webographie

Sécurité informatique et Malwares

Analyse des menaces et mise en oeuvre des contre-mesures (2e édition)

Auteur : Paul RASCAGNERES

Collection : Epsilon

Chapitre	Catégorie	Présentation	Langue	URL
1	site éditeur	Site proposant l'outil Windows Registry Recovery	EN	http://www.mitec.cz
1	site éditeur	Site proposant l'outil reglookup	EN	http://sentinelchicken.org
1	site éditeur	Site proposant l'outil ntfswalk	EN	http://www.tzworks.net
1	site éditeur	Site proposant l'outil disk2vhd	EN	http://technet.microsoft.com/en-us/sysinternals/ee656415.aspx
1	site éditeur	Site proposant l'outil Digitial Forensics Framework	EN	http://www.digital-forensic.org
1	site éditeur	Site proposant une suite d'outil lié à la réalisation d'image mémoire	EN	http://www.moonsols.com
1	site éditeur	Site proposant un outil de capture d'image mémoire	EN	https://github.com/carmaa/inception
1	site éditeur	Site proposant l'outil GMER	EN	http://www.gmer.net
2	site éditeur	Site proposant l'outil VirtualBox	EN	http://www.virtualbox.org
2	blog	Blog de Didier Stevens	EN	http://blog.didierstevens.com/
2	site éditeur	Site proposant l'outil JD-GUI	EN	http://java.decompiler.free.fr/?q=jdgui
2	site éditeur	Site proposant l'outil Exe2aut	EN	http://www.exe2aut.com
2	site éditeur	Site proposant l'outil .NET CodeReflect	EN	http://www.devextras.com/decompiler/
2	site éditeur	Site proposant l'outil Stud_PE	EN	http://www.cgsoftlabs.ro/studpe.html
2	site éditeur	Site proposant la librairie pefile	EN	http://code.google.com/p/pefile/
2	site éditeur	Site proposant Cuckoo Sandbox	EN	http://www.cuckoosandbox.org
2	site éditeur	Site proposant de scanner les fichiers par plusieurs antivirus	EN	http://www.virustotal.com
2	site éditeur	Site proposant un outil de sandbox en ligne	EN	http://anubis.iseclab.org
2	blog	Blog proposant des tutoriaux d'analyse de malware	EN	http://fumalwareanalysis.blogspot.fr
2	site éditeur	Site proposant des échantillons de malware et des analyses techniques	EN	http://www.malware.lu
2	blog	Blog proposant des échantillons de malware et des analyses techniques	EN	http://contagiodump.blogspot.fr
2	site éditeur	Site proposant des échantillons de malware	EN	http://openmalware.org
2	site éditeur	Site proposant des échantillons de malware	EN	http://virusshare.com
3	site éditeur	Site proposant l'outil WinDBG	EN	https://msdn.microsoft.com/en-us/library/windows/hardware/ff551063(v=vs.85).aspx
3	site éditeur	Site proposant l'outil Immunity Debugger	EN	http://www.immunityinc.com/products/debugger/index.html
3	site éditeur	Site proposant l'outil malwasm	EN	http://code.google.com/p/malwasm
3	infomation	Site de référence pour l'assembleur x86	EN	http://ref.x86asm.net
3	site éditeur	Site proposant l'outil IDA Pro	EN	http://www.hex-rays.com/products/ida/
4	site éditeur	Site proposant l'outil Cygwin	EN	http://www.cygwin.com
4	site éditeur	Site proposant l'outil metasm	EN	http://code.google.com/p/metasm
4	site éditeur	Site proposant l'outil LordPE	EN	http://www.woodmann.com/collaborative/tools/index.php/LordPE
4	site éditeur	Site proposant l'outil Peditor	EN	http://www.softpedia.com/get/Programming/File-Editors/Peditor.shtml
4	site éditeur	Site proposant l'outil ImpREC	EN	http://www.woodmann.com/collaborative/tools/index.php/ImpREC
5	site éditeur	Site proposant l'outil Squid	EN	http://www.squid-cache.org
5	site éditeur	Site proposant l'outil Snort	EN	http://www.snort.org/
5	site éditeur	Site proposant l'outil Suricata	EN	http://www.openinfosecfoundation.org/index.php/download-suricata

Webographie

Chapitre	Catégorie	Présentation	Langue	URL
5	site éditeur	Site proposant l'outil Yara	EN	http://code.google.com/p/yara-project/
5	site éditeur	Site proposant l'outil ssdeep	EN	http://ssdeep.sourceforge.net
5	site éditeur	Site proposant l'outil ClamAV	EN	http://www.clamav.net/
5	site éditeur	Site proposant l'outil OpenIOC	EN	http://www.openioc.org