

Sécurité et mobilité Windows 8

pour les utilisateurs nomades

UEFI • BitLocker et AppLocker • DirectAccess • VPN
• SmartScreen • Windows Defender...

Arnaud Jumelet
Stanislas Quastana
Pascal Saulière

Préface de Bernard Ourghanlian



Index

A

- accès à distance 146, 165
 - adresse IP 180
 - authentification forte 144
 - bureau à distance 165
 - conformité du poste 144, 145
 - connectivité applicative 142
 - connectivité réseau 142
 - connexion VPN 183
 - DirectAccess. *Voir* DirectAccess
 - fichier RDP 167
 - flux RSS 168
 - Forefront UAG 148
 - gestion des accès 154
 - IKEv2 (Internet Key Exchange) 173, 175, 182
 - kit de connexion 186
 - L2TP (Layer Tunneling Protocol) 173, 175
 - limitation des accès autorisés 144
 - passerelle bureau à distance 146, 152, 153, 154, 155, 157
 - PPTP (Point to Point Tunneling Protocol) 173, 175
 - protocole de connexion Bureau à distance 151
 - RD Gateway 152, 155
 - RDP (Remote Desktop Protocol) 151, 152, 153, 167
 - RD Web 166
 - RemoteApp 151, 165
 - Remote Desktop 151
 - réseau privé virtuel. *Voir* VPN
 - Resource Group 154
 - RRAS (Remote and Routing Access Server) 146, 173, 178, 182
 - service VPN 183
 - SSTP (Secure Sockets Tunneling Protocol) 173, 175
 - stratégie CAP (Connection Access Policies) 154, 161
 - stratégie d'autorisation d'accès aux ressources 154
 - stratégie d'autorisation de connexion 154
 - stratégie RAP (Resource Access Policies) 154, 163
 - surveillance 144
 - technologie 142
 - VPN Reconnect 173
 - VPN (Virtual Private Network) 152, 173, 175, 183, 206, 211
- accès physique à l'ordinateur 112
- access token. *Voir* jeton d'accès
- ACL (Access Control List) 66
 - ACE (Access Control Entry) 66
 - DACL (Discretionary ACL) 66
 - DACL (Discretionary ACL) 133
 - SACL (System ACL) 67, 133
- Active Directory 27, 28, 48, 58, 117, 121, 133, 134, 138, 154, 169
 - classification des fichiers 135
- anti-malware 78
 - aide à la décision 80
 - analyse de signature 79
 - détection comportementale 79
 - émulation 79
 - KIDS (Kernel Intrusion Detection System) 80
 - MAPS (Microsoft Active Protection Services) 78, 80
 - MMPC (Microsoft Malware Protection Center) 79, 80
- antivirus 15, 77, 202
- application
 - App 92
 - contrôle. *Voir* AppLocker

- de bureau 91
- distante 5
- gérée/non gérée 6
- locale 5
- SaaS 7
- virtualisée 5
- application Windows 8 72
 - isolation 71
- AppLocker 102
 - App 106
 - AppIDsvc 103
 - cmdlet 107
 - fonctionnement 103
 - identité du fichier 103
 - journal d'événements 109
 - liste blanche 104
 - message 108
 - règle 103, 104, 106
- Authenticode 35, 82
- authentification 43, 64
 - forte 57
 - jeton OTP 144
 - serveur Radius 181
- autorisation 64
 - admin approval mode 68
 - debug 64
 - élévation par approbation 68

B

- bac à sable 71
- base de signatures 34
 - base DB 34, 35, 36
 - base DBX 34, 35, 36
 - base des images connues 34
 - base des images révoquées 34
 - base KEK 34, 35, 36
- BCD (Boot Configuration Data) 23
- bcdedit.exe 23
- BitLocker 30, 111
 - activation avant installation de Windows 113
 - Active Directory 117, 121
 - agent de récupération 120
 - certificat autosigné 120
 - chiffrement de volume 118
 - clé de démarrage 119
 - clé de récupération 118, 119
 - clé en clair 121
 - clé externe 120
 - déverrouillage réseau 116, 120

- disque auto-chiffrant 116
- explorateur de fichiers 126
- fonctionnement 118
- Key Recovery Package 131
- ligne de commande 130
- MBAM (Microsoft BitLocker Administration and Monitoring) 130
- mot de passe 114
- mot de passe de déverrouillage 121
- mot de passe de récupération 120, 122
- package de clés 131
- Panneau de configuration 128
- PIN 119, 122, 123
- PowerShell 131
- préparer le disque 125
- protecteur 113, 119
- protection de support amovible 125
- protection du système d'exploitation 123
- récupération en ligne 117
- SID 121
- statut de protection 129
- To Go 112, 125, 127
- TPM (Trusted Platform Module) 119, 123
- UsedSpaceOnly 114
- utilisation 126
- Windows To Go 223
- WipeFreeSpace 114
- boot code. *Voir* code de démarrage
- boot device. *Voir* périphérique de démarrage
- boot loader. *Voir* Winload.exe
- Boot Manager 18, 20, 37
 - configuration 22
- bootmgfw.efi 21
- boot order list 20
- boot sector. *Voir* secteur de démarrage
- BYOD (Bring Your Own Device) 225

C

- carte à puce 57
 - virtuelle 57, 58
- certificat SSL 156, 159, 182, 202
- chargeur de démarrage. *Voir* Winload.exe
- claims 134
- classification des fichiers 135
- clé de chiffrement
 - AIK (Attestation Identity Key) 27, 28, 30
 - EK (Endorsement Key) 27
 - KDF (Key Derivation Function) 125
 - KEK (Key-Exchange Key) 34

- PK (Platform Key) 34, 37
- SRK (Storage Root Key) 25, 28, 30
- cloud. *Voir* stockage d'information/nuage
- cmdlet 27, 38, 88, 94, 107, 131
- code de démarrage 19
- Code Integrity 22, 40, 41
- commande PowerShell. *Voir* cmdlet
- compte utilisateur
 - Microsoft 117
- consommation 1
- contrôle d'accès 64
- contrôle d'accès dynamique. *Voir* DAC (Dynamic Access Control)
- contrôle de compte 67, 71
- courrier électronique 15
- CRL (Certification Revocation List) 191
- CRTM (Core Root of Trust for Measurement) 26
- Ctrl+Alt+Suppr 45

D

- DAC (Dynamic Access Control) 132, 133
 - fonctionnement 134
 - mise en œuvre 139
 - politique d'accès centralisée 138
 - règle de classification 136
 - stratégie d'accès centralisée 139
- démarrage du système
 - étapes 18
 - plate-forme BIOS 19
 - plate-forme UEFI 20
- démarrage sécurisé. *Voir* Secure Boot
- descripteur de sécurité 65, 66
- DirectAccess 147
 - 6to4 193
 - administration 220
 - architecture 190
 - client 191, 209, 218
 - configuration 205, 208, 218
 - construction d'adresse IP 197
 - installation 205
 - IP-HTTPS 193, 194, 211, 220
 - IPsec 191, 199
 - IPsec-AH (IP Authentication Header) 200
 - IPsec-ESP (IP Encapsulating Security Payload) 201
 - IPv4 192, 193, 194
 - IPv6 191, 192, 197
 - ISATAP 193, 195, 196, 197
 - mode simplifié 205, 208

- NAT64/DNS64 193, 195, 197
- serveur 191, 211
- serveur d'applications 215
- serveur d'autorité de certification 191
- serveur de liste de révocation de certificats 191
- serveur de localisation réseau 191
- serveur d'emplacement réseau 202
- serveur de politique réseau 192
- serveur d'infrastructure 191, 202, 213
- surveillance du serveur 216
- Teredo 193, 194, 220
- topologie de déploiement 203
- transition IPv4-IPv6 192
- transition IPv6-IPv4 198
- Traversée latérale 220

E

- écran de verrouillage 44
- écran d'ouverture de session 44, 47
- ELAM (Early-Launch of Anti-Malware) 22, 39, 40, 78
- Endpoint Protection 87, 89
- environnement de préinstallation. *Voir* Windows PE
- environnement de récupération. *Voir* WinRE
- extension ECU (Enhanced Key Usage) 41, 83

F

- filtrage 15
- firmware 17, 35, 36, 122, 123, 231
 - BIOS 18, 19, 23, 125
 - UEFI 18, 23, 123, 125
- firmware boot manager 20

G

- gestionnaire de démarrage. *Voir* Boot Manager

H

- hameçonnage. *Voir* risque/vol d'identité
- HIPS (Host-based Intrusion Prevention System) 89

I

- identifiant de zone. *Voir* Zone.Identifier
- identification 64
- image UEFI 20, 21, 34, 36
 - liste blanche 35
 - liste noire 35
 - validation 35

Internet Explorer 10 86
IPsec 133
IPv6 192
isolation d'application 71
 AppContainer 72, 73
 isolation des fenêtres 73
 isolation des informations d'identification 73
 isolation des périphériques 73
 isolation des processus 72
 isolation du réseau 73
 isolation du système de fichiers 73

J

jeton d'accès 65, 133
jeton OTP 144

K

Kerberos 134, 212
KMCS (Kernel Mode Code Signing) 41

L

lock screen. *Voir* écran de verrouillage
logo Windows 8 24
lsass 65

M

Measured Boot 32
mise à jour 11
 affichage 99
 Apps 100
 BITS (Background Intelligent Transfer Service) 94
 BranchCache 95
 configuration 96
 en ligne 95
 facultative 94
 importante 93
 Microsoft Update 95
 période de maintenance 98
 recommandée 93
 redémarrage de l'ordinateur 99
 Windows Update 92, 93, 95
 WSUS (Windows Server Update Service) 102
mot de passe
 code confidentiel 55
 image 53
 standard 52
mot de passe de propriétaire 27, 30, 123

N

NAP (Network Access Protection) 154, 192
NAT (Network Address Translator) 194, 207, 211
navigation Internet 11
NIS (Network Inspection System) 89
NLS (Network Location Server) 191, 213
noyau du système. *Voir* Ntoskrnl.exe
NPS (Network Policy Server) 192
Ntoskrnl.exe 18, 22, 40

O

ouverture de session 43, 64

P

partitionnement
 GPT 18, 22
 MBR 18, 19, 22
 partition de démarrage 125
 partition OS 125
 partition système 125
partition système 125
 ESP 21
périphérique de démarrage
 priorité 18
phishing. *Voir* risque/vol d'identité
pile réseau 194, 195
pilote de périphérique 20
PKI (Public Key Infrastructure) 191
poste de travail
 d'entreprise 1
 mise à jour 11
 mobile 3, 7
 pare-feu 14
 périphérique connecté 3
 personnel 1
PowerShell 187, 205
programme malveillant 39, 78, 87
 détection 80, 89
 protection de l'entreprise 87
protection des données. *Voir* BitLocker
psexec.exe 50

R

regedit.exe 50
réputation 81, 86
revendications. *Voir* claims

risque

- APT (infection persistante avancée) 10
- attaque par le réseau 13
- courrier électronique 15
- exécution automatique 14
- intelligence économique 10
- navigation Internet 11
- périphérique amovible 14
- perte d'information 7
- vol d'identité 9, 10
- vol d'information 7

S

- SAM (Security Account Manager) 48, 50. *Voir* type de compte/compte local
- SAS (Secure Attention Sequence).
Voir Ctrl+Alt+Supr
- SCCM (System Center Configuration Manager) 87
- SD (Security Descriptor) 133
- secteur de démarrage 19
- Secure Boot 18, 22, 32, 123
 - administrer 38
 - désactiver 33
 - fonctionnement 33
 - Setup Mode 33
 - User Mode 33
- security descriptor. *Voir* descripteur de sécurité
- séquence de démarrage 112
- serveur Radius 192
- SERVICE_BOOT_START 20, 22
- Services.exe 20, 22
- SERVICE_SYSTEM_START 20, 22
- SharePoint 48
- SID (Security Identifier) 65, 67, 73, 121
- signature numérique 82
 - Authenticode 82
- sign-in screen. *Voir* écran d'ouverture de session
- signtool.exe 83
- SkyDrive 5, 48, 51, 113, 117
- Smss.exe 20, 22
- spear phishing.
- stockage d'information
 - cloud 4, 48
 - externe 4
 - interne 4
 - système d'information 4
- stratégie de groupe 117, 137, 169, 233
- système de fichiers
 - FAT 21, 126

NTFS 125

- système d'information
 - cloisonnement 6

T

- TCG (Trusted Computing Group) 24
- tpm.msc 59
- TPM (Trusted Platform Module) 24, 27, 58, 112, 119, 121, 123, 224
 - configuration 28
 - mot de passe de propriétaire 123
 - PCR (Platform Configuration Register) 25, 28, 123
 - prendre possession 30
 - préparer le module 29
 - unité fonctionnelle 25
 - version 1.2 31
 - version 2.0 31
- type de compte 48
 - compte de domaine 48, 51
 - compte local 48
 - compte Microsoft 48, 50, 51

U

- UAC (User Account Control). *Voir* contrôle de compte

V

- VDI (Virtual Desktop Infrastructure) 154
- VPN (Virtual Private Network) 146

W

- Windows 7 46, 71
- Windows 8
 - historique 46
- Windows boot manager 22
- Windows Defender 39, 77, 78
 - Malware Protection 78
 - mise à jour 80
 - planification des analyses 80
 - type d'analyse 80
- Windows Installer 91, 92
- Windows NT 46
- Windows PE 114, 126
- Windows SmartScreen 77, 80
 - configuration 83
 - filtre Internet 86
 - téléchargement de programme 85
- Windows Store 48, 63, 71, 92, 100, 225, 233

Windows To Go 17, 18, 124
administration 227
BitLocker 223
cas d'utilisation 225
configuration matérielle 226
création du support 227
données utilisateur 227
firmware 231
fonctionnement 223
premier démarrage 223
vs installation classique 224
Windows Update 37
Windows Vista 46, 71

Windows XP 46
Wininit.exe 20, 22
Winload.exe 18, 20, 40, 41
Winlogon 46, 65
Winlogon.exe 20, 22
WinRE 126
emplacement 126
lancer 126
WSUS (Windows Server Update Services) 88

Z

Zone.Identifier 85