ROYAUME DU MAROC
ADMINISTRATION
DE LA DEFENSE NATIONALE
Direction Générale de la Sécurité des Systèmes d'Information

المملكة المغربية
إدارة الدفاع الوطني
المديرية العامة لأمن نظم المعلومات

NOTE DE SECURITE

Titre	Meterpreter Malware
Numéro de Référence	58521411/25
Date de Publication	14 Novembre 2025
Risque	Critique
Impact	Critique

Meterpreter est un Malware qui fournit une console d'accès furtive et interactive sur une machine compromise. Il fonctionne entièrement en mémoire, évite l'écriture sur le disque, et offre des fonctions comme le contrôle du système, l'exécution de commandes, la capture d'écran, la récupération de fichiers et l'escalade de privilèges.

Ce malware reste un outil privilégié pour les groupes cybercriminels grâce à sa flexibilité, sa furtivité et ses capacités d'exploitation post-intrusion. La combinaison de campagnes ciblées, de vulnérabilités non corrigées et de mécanismes avancés de persistance en fait une menace majeure dans les infrastructures critiques.

Parmi les failles les plus fréquemment associées au déploiement du payload figurent CVE-2017-0143 (SMBv1 – EternalBlue) et CVE-2023-22527 (injection de templates Atlassian Confluence). D'autres vulnérabilités ont également été observées dans des campagnes transportant Meterpreter, notamment CVE-2024-27956, CVE-2018-7600 (Drupalgeddon 2), CVE-2021-26855 (ProxyLogon – Microsoft Exchange), CVE-2023-46604 (Apache ActiveMQ RCE), CVE-2022-47986 (IBM Aspera Faspex RCE), CVE-2023-27350 (PaperCut NG/MF RCE) ainsi que CVE-2018-7602 (Drupalgeddon 3). Toutes ces vulnérabilités sont utilisées par les attaquants comme une porte d'entrée directe dans les systèmes ciblés, rendant possible l'exécution de code malveillant et le déploiement ultérieur de Meterpreter pour la prise de contrôle du système compromis.

Direction Générale de la Sécurité des Systèmes d'Information,
Centre de Veille de Détection et de Réaction aux Attaques Informatiques, Méchouar Saïd,
B.P. 1048 Rabat – Tél : 05 37 57 21 47 – Fax : 05 37 57 20 53
Email : contact@macert.gov.ma

المديرية العامة لأمن نظم المعلومات ,مديرية تدبير مركز اليقظة والرصد والتصدي للهجمات المعلوماتية ، المشور السعيد، ص.ب. 1048 الرباط
هاتف: 47 21 57 37 05 – فاكس: 53 20 57 37 05
البريد الإلكتروني contact@macert.gov.ma

Le maCERT/DGSSI recommande d'intégrer les indicateurs de compromission (IOCs) ci-dessous au niveau des moyens de détection et d'alerter le maCERT/DGSSI en cas de détection d'une activité relative à ce malware.

Indicateurs de compromission (IOCs):

Hashs :

- 774fae39540b1ff8e6c9fa1b7c47aa0bb40d189fc34815be2c71222d25638fbe
- 213474101c8faf1bd6053b37570bfb0d1d05adf6dda136d743966893a73ed80a
- d364cefb9cb8f33040947126ad616f98224df86f6c864205f8732f12d12fbc15
- d7aa72344ee9bfdc105a1fd9fed2a16743e656b3e671073e9b1a134298366956
- 798e8bca6ff558e2eab4b20ac4ad1437f641f099ce5d81b8ed8a890048423a13
- c1c3c4355773a0f90556200c5d074d1b4117554bba74293420b87e298b8fd1c8
- 26dce6a2cb385a3e3f9e70f60cb0769351629932b2aee20598f75041d1cb5e7a
- 020dc64fbbe5ff298ec3bd04488425005c1e81174ac6660d4aa84d3692ce0749
- 05a420b4c04e432cf0efc050e15fad162c17df38d1da09a59b8d4d714a72f421
- 57160f40696907c33ae008ea3834b89b486e1cb050f4ec9888c3a12ad3097bb0
- 5329c336a16e40e0e78f30bc1c685c1fc85990e66593e56eb48a7363c51b1474
- 750ebeb1ae03ea2def82b2f0b14a8b10fe4f26e98aa61e27fbdb5026ca1209d9
- 58bfca73fc9cb4ebc90130b5c3cd3b79afb42a6546a28c6dc5ab975937bf30c1
- f5333d0e5d643400823c74e0500688c8fd54efd543f2dbfb017e2ede523c7e15
- 59d3b0e85e84cfa45a16bdfac44043d542c44eea803ad2f2e45d22dc743c0e9e
- b828f4dedbd8f19b80a0a16e111ff4ae03d3d7f4ff321fbd4a762665beecd2e4
- 0222a89ed1fe51d7206f333647d11c0ecbbac4640c07d3904d02f9213a8ffa76
- 4e692e5a003f448eeb8b90aed18f71d34202531877043c928e2ac508c44ba25d
- e506e872abeff0b4122edf4b2e3cf35fd7c14dc83138062ae74a49dc0902eb46
- 3878987fb995bd7149e1e3707a6c07525939346cfd7a99a941c00da537cc106b
- e8efd41357ff1df25d0461bb4d10a694c7b78c2db794b2a1f01931678adff0a3
- c1b628312476130310115e09f9eb6697b5ba17e80bbc625911a892fe8178ac4a
- 07fe525b0076977f6a748b8db1a89fa06fc9b0653294d9ebbfd25db440e91f5e
- 6fb3ad101791cc281245eb7f99f7742a6fcff75d21fc9c5caf7a8b69608a56ad

Direction Générale de la Sécurité des Systèmes d'Information,
Centre de Veille de Détection et de Réaction aux Attaques Informatiques, Méchouar Saïd,
B.P. 1048 Rabat – Tél : 05 37 57 21 47 – Fax : 05 37 57 20 53
Email : contact@macert.gov.ma

المديرية العامة لأمن نظم المعلومات ,مديرية تدبير مركز اليقظة والرصد والتصدي للهجمات المعلوماتية ، المشور السعيد، ص.ب. 1048 الرباط
هاتف: 47 21 57 37 05 – فاكس: 53 20 57 37 05
البريد الإلكتروني contact@macert.gov.ma

- b3a657094a82ed16fa86a23f806f86c622a16bbb8cc943b4ce6befdc763375fd
- edcf87c248b5fec451b48e8eec1e1ac237182250c052636910bbb41890636ff8
- 7c726fe15d97494ff8d866f989848378b337c5ecaf625c9cc86cd3e2fe274cba
- d3b937dee1f947c27df7a800c76f5c427d34b8600b5979000d0a0895f9ad8061
- f8a4ee6249cb3826cc33863b8a34fbc21c46eeec45db67e174c5b4591a810e78
- 8a7ec3317498b95a4dbc3b42983444658e605054e03be9d586765a6321ebe217
- 132d3a0165a60cc871ad3ab5209f37e09da3fcae288ad8f5fc739a96b610a4d1
- 40e3191da1524316f234c26738ae717730b75bacb9544943e6257794eba6deed
- e907ff03885e020ff925b4e67a219e3a2ccacb2f69c58779cac701e747d16e67
- cb733858674214a2d54233f379acbb18bbdceb8cc624faacf18bc7242d2ed82e
- a2b65c4abb1624e90e6fc19aa0410d36d2ba9cdda72583cf20cf0df7764e3baf
- d869c6f3cab6390fe866f11a2484795e0c74f3c98093251dc67b7ae78218a15c
- 6e9622db00279da2ddd0f01262dc892eb6674224cc1f8c0cbdc67ae831a68a6d
- 60fdd407121446dbe50b7ae9c96d8fef7fde181a40db893f381f7120c23afd56
- d42ccd041280603b2675e0baa74ac3f482bad611ed07b6ab548e7b41d068ac5c
- 03566b7c075cd5d0b720a019fcfb72bcc3f6bc236e0f727b28450b62454eddbb
- a613ec75636307b8b717d5c82c709dd90d67c2c27a531a2eba48f96c4a651b2a
- 37236e863fb47cd858498b3dc27fcfccbf49f02caf8f2e4d06fa7369f25930cf
- 836f25ca3c5dc85c51077d991c8966a147f579a6529225c4b719fcfd4bfc38e4
- 4f5aaf96c3a037b9fbb62f29723eba6d1bbfbf93d650634d172b551c0bb0e4f5
- 39139011c699adde61ef19bebca57b826cdfe94a39a8721ef3bcb45caf4ee4d9
- 2dc4fff0f3222ca6c48e402ab1a81d87814aeaf0196f357d180e5407c121c553
- a814c22692fa332be1635906d9826946a998bd7b10ee92280b85d58465665fd9
- 78d2b07e215f982dc92d54c2b960acb9eef8df8412c144d70c397e5afafcbb18
- 63438ed9d7dac6898021a77320b405ded9d819783d037ad156526ce95059da5d
- 03c3739a7337ab69e0efa13d936dc2b17d7192652661e787a2be0fe52962e0bf

Ip :

- 91.242.163.9 - 185.43.207.58 - 103.49.92.35 - 64.111.92.98 - 209.195.169.238 - 193.169.245.120 - 86.106.85.207 - 188.166.250.178 - 43.160.202.246 - 111.90.140.239 - 35.212.233.73 - 45.143.167.125 - 69.195.139.2 - 83.166.240.215 - 178.16.52.213 - 47.96.153.252 - 20.218.149.195 - 50.77.10.251 - 50.77.10.249 - 83.147.18.16 -

91.92.241.190 - 20.218.157.204 - 148.135.59.32 - 162.243.33.151 - 101.43.50.43 - 50.77.10.253 - 107.173.7.172 - 104.248.50.35 - 103.49.92.44 - 8.138.221.135 - 103.79.79.35 - 47.93.91.70 - 45.77.247.151 - 150.230.26.196 - 62.233.57.169 - 193.200.149.60 - 138.197.32.49 - 152.53.192.222 - 77.73.129.63 - 45.55.123.49 - 192.3.229.231 - 112.124.47.74 - 45.77.45.191

Signature malware:

- ✓ Gene.Win.Harmlet.6-6
- ✓ Win.Trojan.MSF_Shellcode-1
- ✓ Win64/HackTool.CobaltStrike.H8oAsywA
- ✓ Win64/HackTool.CobaltStrike.H8sA2NgA
- ✓ Trojan.Generic.bjrzd
- ✓ Trojan.Win64.CozyDuke.trLC
- ✓ Win.Malware.Meterpreter-9872014-0
- ✓ Trojan.Generic.uabj
- ✓ Win64/HackTool.CobaltStrike.H8sAXR0A
- ✓ Backdoor.Meterpreter.bo
- ✓ Win.Exploit.Meterpreter-10017195-0
- ✓ Win64/Trojan.ShellCode.H8oAA2oC
- ✓ Win64/HackTool.CobaltStrike.H8oAWF4A
- ✓ Win64/HackTool.CobaltStrike.HggAT7IA
- ✓ Win32/Trojan.Leivion.HxQBWBQB
- ✓ Win64/HackTool.CobaltStrike.H8sAQTkA
- ✓ Trojan.Generic.hqver
- ✓ Trojan.WinGo.Agent
- ✓ Trojan.Win32.Jorik.lrUS
- ✓ BackDoor.Meterpreter.227
- ✓ Win64/HackTool.CobaltStrike.HggAT7MA
- ✓ Trojan.Cometer.aww
- ✓ Trojan.Win32.Generic.4!c
- ✓ Win32/HackTool.Meterpreter.HgIAT6IA
- ✓ Trojan.Swrort.10
- ✓ Win64/HackTool.CobaltStrike.H8oAUwMA
- ✓ Trojan.Win64.Meterpreter
- ✓ Win64/HackTool.CobaltStrike.H8sATD0A
- ✓ Gene.Win.Harmlet.50738-0
- ✓ Win64/HackTool.CobaltStrike.H8oAYJUA
- ✓ Win.Trojan.MSShellcode-10042643-0
- ✓ Trojan.Win32.Shellcode.4!c
- ✓ Win32/Trojan.ShellCode.HgkAT7IA

- ✓ Trojan.Packed.bjp
- ✓ Trojan.Win32.Injuke.16!c
- ✓ HackTool.Win32.Meterpreter
- ✓ Win.Trojan.CobaltStrike-7899872-1
- ✓ Win64/Trojan.Generic.HggAT6MA
- ✓ Win64/HackTool.CobaltStrike.H8oATWkA
- ✓ Safe
- ✓ Win64/Trojan.ShellCode.H8sAUA0B
- ✓ Hacktool.Win32.Meterpreter.3!c
- ✓ Trojan.Win32.Beacon.4!c
- ✓ BackDoor.Meterpreter.1419
- ✓ Gene.Win.Harmlet.16341-0
- ✓ Trojan.CobaltStrike.sz
- ✓ Trojan.Win32.CobaltStrike.tsgn
- ✓ Win32/HackTool.Meterpreter.HxMBAQkC
- ✓ Trojan.Win32.CobaltStrike
- ✓ Win.Exploit.D388a-9756522-0
- ✓ BackDoor.Siggen2.247
- ✓ Trojan.Win64.Injector
- ✓ win/malicious
- ✓ Suspicious
- ✓ Win64/HackTool.CobaltStrike.H8oAXDYA
- ✓ Win64/HackTool.CobaltStrike.H8oAXkkA
- ✓ PUA.RiskWare.Meterpreter
- ✓ Trojan.Win32.Rozena.hpcmlv
- ✓ Win64/HackTool.Meterpreter.H8sASH0A
- ✓ Malicious
- ✓ Trojan.Zenpak.kyw
- ✓ Win32/Trojan.Generic.HxMBBPYC
- ✓ HEUR/QVM20.1.4FD3.Malware.Gen
- ✓ Win64/HackTool.CobaltStrike.H8sASloA
- ✓ Trojan.Generic.garbz
- ✓ Trojan.Generic.gdijr
- ✓ Win64/HackTool.CobaltStrike.H8sAxWAA
- ✓ Trojan.Win64.Rozena
- ✓ Trojan.Win32.Meterpreter
- ✓ Gene.Win.Harmlet.4-6
- ✓ Win64/HackTool.CobaltStrike.HggAT7QA
- ✓ Win32/Trojan.Generic.HgkAT6QA
- ✓ Trojan.Win64.Agent
- ✓ Win64/HackTool.CobaltStrike.H8sATR4A
- ✓ Win64/HackTool.CobaltStrike.HggAT7UA
- ✓ Trojan.Win32.Marte.4!c

- ✓ Trojan.Win32.Meterpreter.ktjmmp
- ✓ Trojan.Win32.Swrort.eratya
- ✓ Trojan.Win32.Meterpreter.4!c
- ✓ Win32/HackTool.Meterpreter.HgkAT7AA
- ✓ Win.Exploit.Meterpreter-9777172-0
- ✓ Trojan.Win32.Veil.4!c
- ✓ Trojan.Win32.Meterpreter.m!c
- ✓ Win32/Trojan.ShellCode.Hx4CABkC

Ports susceptibles:

- 2222
- 4444
- 5555