CYBER DEFENSE AFRICA : ANNONCE DE SÉCURITÉ **Date** : 26/07/2024

Type de Contenu	Description
Titre	***Exploitation de la panne « Windows- CrowdStrike » pour des cyberattaques multiples***
ID	*202407/AS/08*
Code TLP	*Green*
Niveau de Risque	***Critique***
Application et service affectés	***Applications et services WINDOWS***
Version / Edition	Toutes les versions
Plateforme	***Microsoft WINDOWS***
Mise à jour	*N/A*
Résumé	*Les cybercriminels ont saisi l'occasion pour exploiter « la mise à jour ratée de CrowdStrike » et ciblent actuellement les utilisateurs concernés avec des escroqueries par hameçonnage et des logiciels malveillants via l'utilisation de plusieurs faux domaines et de mails CrowdStrike ».*
Impacts	- ***Exécution des attaques par phishing ou hameçonnage*** - ***Exécution des attaques d'injection SQL programmées*** - ***Exfiltration des informations sensibles de la base de données*** - ***Violation de données importantes, entraînant la fuite d'informations sensibles*** - ***Chiffrement de données et blocage des systèmes***
Description Détaillée	*La récente mise à jour effectuée par CrowdStrike le 18 juillet 2024 a entraîné une panne mondiale, causant d'importantes perturbations pour les utilisateurs qui se sont retrouvés avec des écrans bleus de la mort (BSOD) sur leurs appareils. Cette panne est actuellement exploitée par les cybercriminels pour leurs attaques.* *Les cybercriminels ont saisi cette occasion pour cibler les utilisateurs concernés avec des escroqueries par hameçonnage et des logiciels malveillants via l'utilisation de plusieurs faux domaines et mails CrowdStrike.*
Recommandations	• ***Tester si possible les mises à jour en environnement avant de les déployer en production ou le cas non échéant vérifier minutieusement toute mise à jour ou correctif avant de l'installer.*** • ***Suivre les étapes de remédiation proposées sur les liens officiels de CrowdStrike et de Windows.*** • ***Effectuer toujours des mises des systèmes uniquement depuis les sources officielles des fournisseurs.***
Indicateurs de Compromission	*Consulter la liste et les détails sur les IOCS en* ***Annexes***

Liens pour plus de détails	*https://any.run/cybersecurity-blog/crowdstrike-outage-abuse/?utm_source=malware_analysis&utm_medium=email&utm_campaign=crowdstrike-analyzing_20240725bsn&utm_content=crowdstrike-outage-abuse*

Annexes :

1. **Liste des faux domaines « CrowdStrike » collectés jusqu'à présent :**

crowdstrike-bsod[.]co	crowdstrike-bsod[.]com	crowdstrike-fix[.]zip	crowdstrike-helpdesk[.]com	crowdstrike-out[.]com
crowdstrike[.]blue	crowdstrike[.]bot	crowdstrike[.]cam	crowdstrike[.]ee	crowdstrike[.]es
crowdstrike[.]fail	crowdstrike0day[.]com	crowdstrikebluescreen[.]com	crowdstrikebsod[.]co	crowdstrikebsod[.]com
crowdstrikebug[.]com	crowdstrikeclaim[.]com	crowdstrikeclaims[.]com	crowdstrikeclassaction[.]com	crowdstrikecure[.]com
crowdstrikedoomsday[.]com	crowdstrikedown[.]com	crowdstrikedown[.]site	crowdstrikefail[.]com	crowdstrikefix[.]co
crowdstrikefix[.]com	crowdstrikefix[.]in	crowdstrikefix[.]zip	crowdstrikeglitch[.]com	crowdstrikehelp[.]com
crowdstrikelawsuit[.]com	crowdstrikemedaddy[.]com	crowdstrikeold[.]com	crowdstrikeoops[.]com	crowdstrikeoopsie[.]com
crowdstrikeoopsies[.]com	crowdstrikeout[.]com	crowdstrikeoutage[.]com	crowdstrikeoutage[.]info	crowdstrikepatch[.]com
crowdstrikeplatform[.]com	crowdstrikeplatform[.]info	crowdstrikerecovery[.]com	crowdstrikereport[.]com	crowdstrikesettlement[.]com
crowdstrikesuporte[.]com	crowdstrikesupport[.]info	crowdstriketoken[.]com	crowdstrikeupdate[.]com	crowdstrikeyou[.]xyz
crowdstrikezeroday[.]com	fix-crowdstrike-apocalypse[.]com	fix-crowdstrike-bsod[.]com	fix-crowdstrike[.]com	fixcrowdstrike[.]com
fixmycrowdstrike[.]com	fuckcrowdstrike[.]com	howtofixcrowdstrikeissue[.]com	iscrowdstrikedown[.]com	iscrowdstrikefixed[.]com
iscrowdstrikestilldown[.]com	isitcrowdstrike[.]com	microsoftcrowdstrike[.]com	microsoftoutagescrowdstrike[.]com	secure-crowdstrike[.]com
suportecrowdstrike[.]com	whatiscrowdstrike[.]com			

2. **Fichiers archive malveillant avec Remcos :**

Le fichier malveillant, nommé «crowdstrike-hotfix», a été distribué à partir de **hxxps://portalintranetgrupobbva[.]com.** Après son exécution, il transmettait Remcos au système infecté.

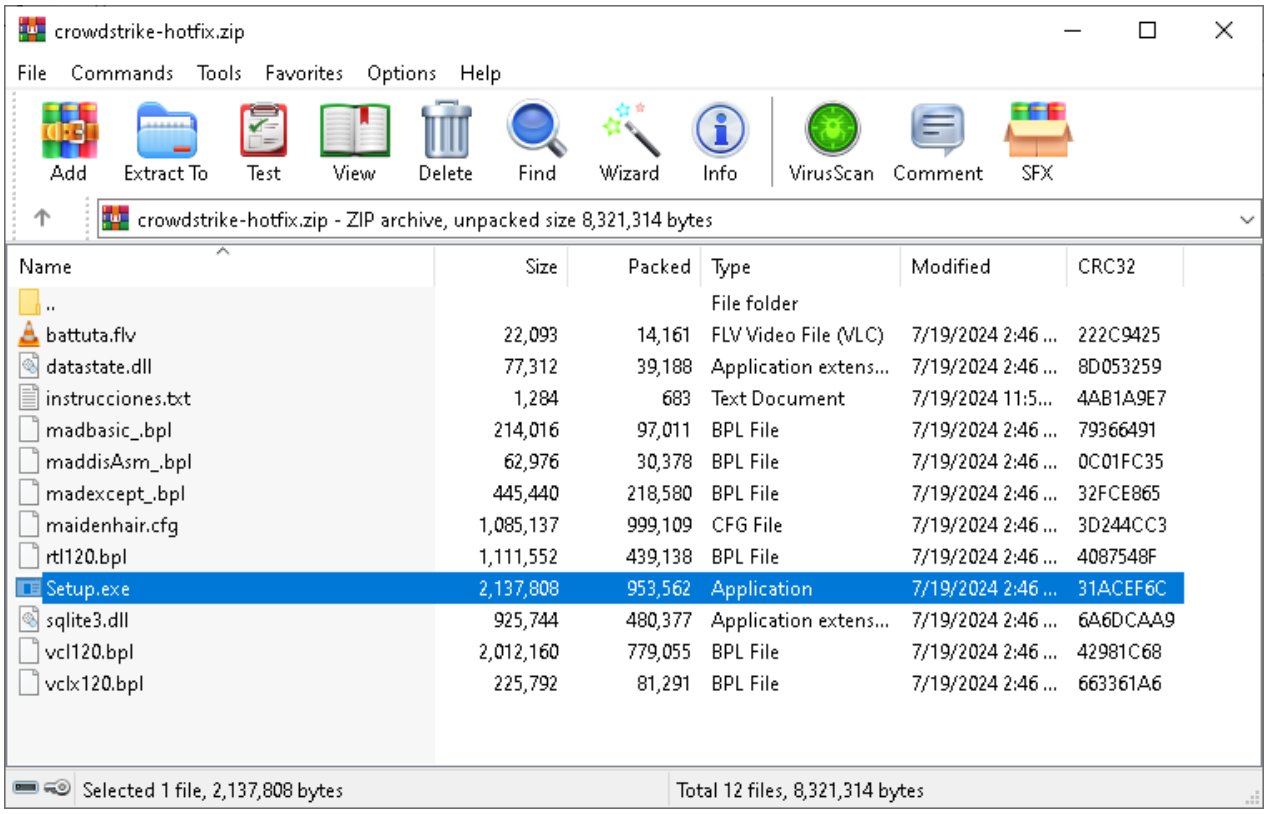

Figure 1: Image de l'archive malveillant avec Remcos

Liste des IOCS du fichier archive «crowdstrike-hotfix».

crowdstrike-hotfix.zip	c44506fe6e1ede5a104008755abf5b6ace51f1a84ad656a2dccc7f2c39c0eca2
Setup.exe	5ae3838d77c2102766538f783d0a4b4205e7d2cdba4e0ad2ab332dc8ab32fea9
maddisAsm_.bpl	52019f47f96ca868fa4e747c3b99cba1b7aa57317bf8ebf9fcbf09aa576fe006
battuta.flv	be074196291ccf74b3c4c8bd292f92da99ec37a25dc8af651bd0ba3f0d020349
sqlite3.dll	02f37a8e3d1790ac90c04bc50de73cd1a93e27caf833a1e1211b9cc6294ecee5
vclx120.bpl	2bdf023c439010ce0a786ec75d943a80a8f01363712bbf69afc29d3e2b5306ed
rtl120.bpl	b1fcb0339b9ef4860bb1ed1e5ba0e148321be64696af64f3b1643d1311028cb3
maidenhair.cfg	931308cfe733376e19d6cd2401e27f8b2945cec0b9c696aebe7029ea76d45bf6
datastate.dll	6010e2147a0f51a7bfa2f942a5a9eaad9a294f463f717963b486ed3f53d305c2

madexcept_.bpl	835f1141ece59c36b18e76927572d229136aeb12eff44cb4ba98d7808257c299
vcl120.bpl	b6f321a48812dc922b26953020c9a60949ec429a921033cfaf1e9f7d088ee628
madbasic_.bpl	d6d5ff8e9dc6d2b195a6715280c2f1ba471048a7ce68d256040672b801fda0ea
instrucciones.txt	4f450abaa4daf72d974a830b16f91deed77ba62412804dca41a6d42a7d8b6fd0
Domain:	hxxps://portalintranetgrupobbva[.]com/
C2	213.5.130.58:443
URLs:	mail.zoomfilms-cz[.]com discussiowardder[.]website wxt82[.]xyz

3. Mail de Phishing (hameçonnage)

Cela a commencé par un courriel d'hameçonnage sur le thème de CrowdStrike (logo, police,) et une pièce jointe au format PDF, qui comprenait à son tour un lien pour le téléchargement d'un fichier ZIP.

Download The Updater

CrowdStrike is actively working with customers impacted by a defect found in a single content update for Windows hosts. Mac and Linux hosts are not impacted. This was not a cyberattack.

The issue has been identified, isolated and a fix has been deployed.

We are referring customers to update their Windows servers as soon as possible through through the tool to avoid disruptions!

We further recommend organizations ensure they're communicating with CrowdStrike representatives through official channels.

Our team is fully mobilized to ensure the security and stability of CrowdStrike customers.

We understand the gravity of the situation and are deeply sorry for the inconvenience and disruption. We are working with all impacted customers to ensure that systems are back up and they can deliver the services their customers are counting on.

Obviously, the consequences of any failure to update the system and disruption will be the responsibility of the organization's IT manager.

Figure 2: Image du Mail de Phishing pdf

IOCs sur le courriel de phishing ou hameçonnage

update2.pdf	1bbb795ce19f4dcc4ac9f8e8c12f3452f1f07c68a53ef631c76e392e1d06ea43
update.zip	96dec6e07229201a02f538310815c695cf6147c548ff1c6a0def2fe38f3dcbc8
CrowdStrike.exe	4491901eff338ab52c85a77a3fbd3ce80fda738046ee3b7da7be468da5b331a3
URL	hxxps://link.storjshare[.]io/s/jwyite7mez2ilyvm2esxw2jq3apq/crowdstrikeisrael/update.zip?download=1

4. Document malveillant avec des programmeurs voleurs de données

Les attaquants ont également utilisé d'autres moyens pour inciter des victimes peu méfiantes à exécuter des logiciels malveillants.

L'image ci-dessous montre un document nuisible qui prétend fournir des instructions sur la manière de résoudre le problème. Pourtant, lorsqu'il est ouvert, il utilise un mauvais script VBS (Visual Basic Script) pour lancer une série d'outils sur l'ordinateur infecté.

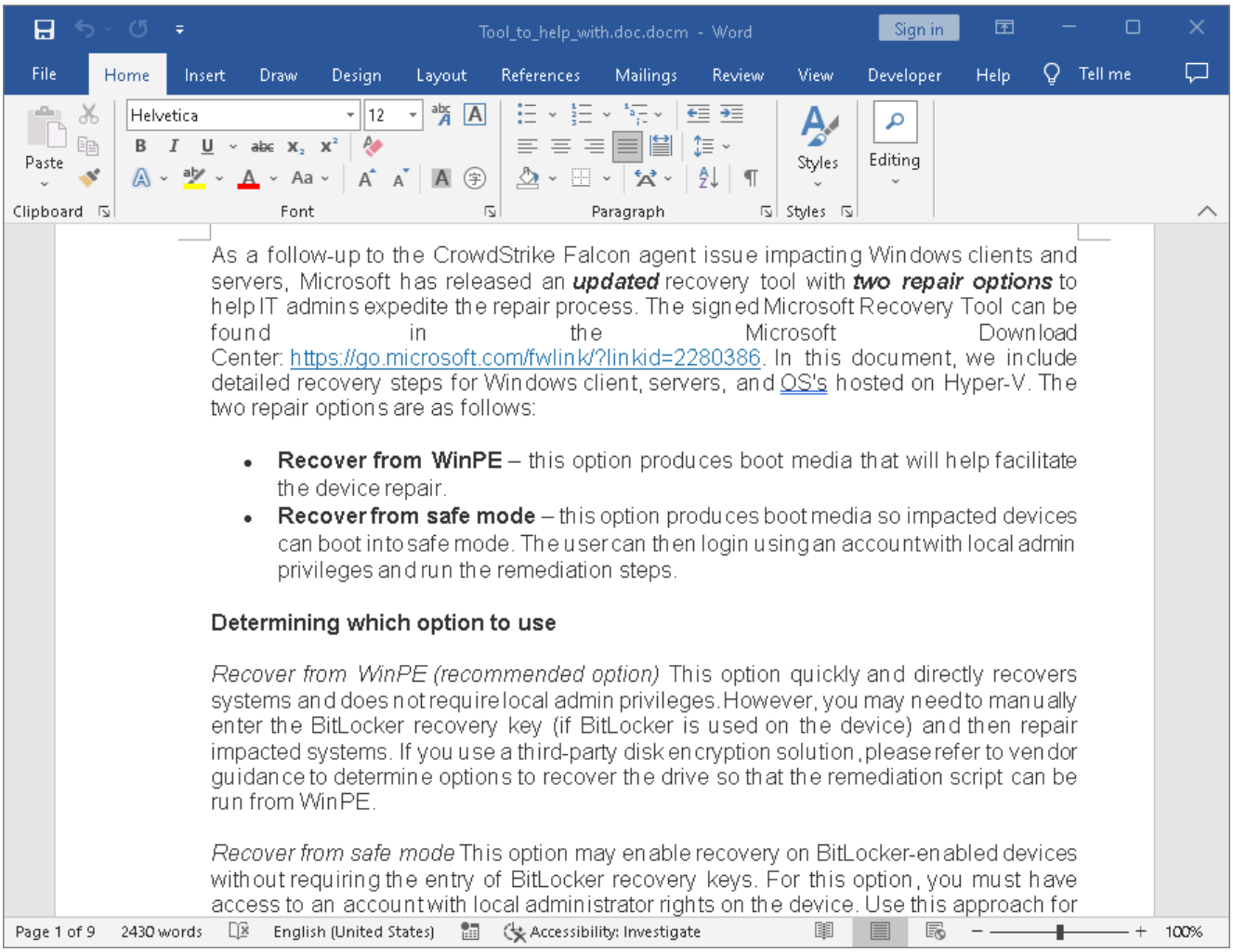

Figure 3: Image du fichier .docm malveillant qui lance le logiciel malveillant

IOCs du document malveillant

Name	New_Recovery_Tool_to_help_with_CrowdStrike_issue_impacting_Windows.docm
Hash sum	803727ccdf441e49096f3fd48107a5fe55c56c080f46773cd649c9e55ec1be61
URL	hxxp[://]172.104.160[.]126:8099/payload2[.]txt

IOCs du programme malveillant utilisé pour voler et extraire les données sur les machines victimes

Hash sum	4ad9845e691dd415420e0c253ba452772495c0b971f48294b54631e79a22644a
URL	172.104.160.126:5000