Comment anticiper la menace

L'exemple de Mustang Panda

ANSSI / CERT-FR

ANSSI/SDO/DCA

07/06/2023

Plan

Introduction (rapide) à l'analyse de la menace

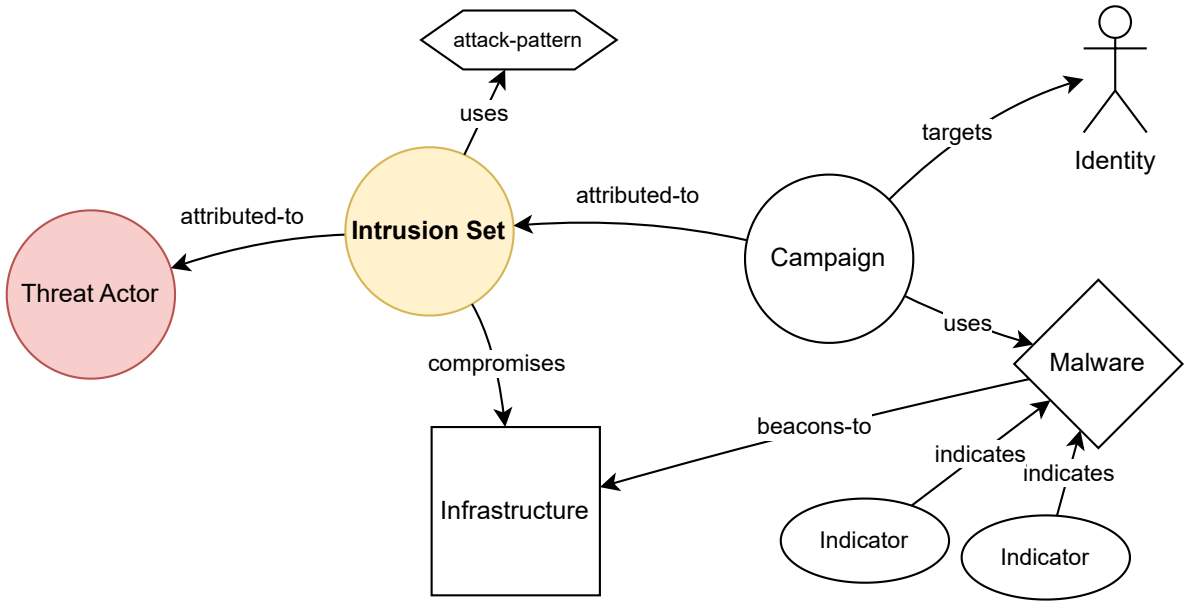
La menace ?

La menace est représentée par des **capacités** au service d'**intentions** cherchant à saisir des **opportunités** d'action sur une ou plusieurs cibles.

- L'analyse technique se concentre sur la compréhension des capacités adverses. Elle s'appuie sur nos propres capacités d'analyse ainsi que l'utilisation de nombreuses sources de données :
  - Bases de connaissances internes et externes ;
  - Plateformes d'analyse de fichiers en ligne ;
  - Moteurs de recherche indexant les résultats de balayage de ports ;
  - Bases de *passive DNS* et de *passive Whois* ;
  - etc.

Modélisation de la connaissance

- L'ANSSI s'appuie sur le modèle STIX 2.1 (*Structured Threat Information Expression*) [1] pour modéliser la menace.
  - **Groupe d'attaquants** (*Threat Actor*) : personnes physiques ou morales, opérant avec une intention malveillante ;
  - **Mode opératoire d'attaque** (MOA) (*Intrusion Set*) : ensemble cohérent de techniques, tactiques et procédures (TTP), de codes et d'infrastructures utilisés pour réaliser des attaques informatiques.



Représentation JSON (1/2)

```
{
    "type": "bundle",
    "id": "bundle--2a25c3c8-5d88-4ae9-862a-cc3396442317",
    "objects": [
        {
            "type": "indicator",
            "spec_version": "2.1",
            "id": "indicator--a932fcc6-e032-476c-826f-cb970a5a1ade",
            "created": "2014-02-20T09:16:08.989Z",
            "modified": "2014-02-20T09:16:08.989Z",
            "name": "File hash for Poison Ivy variant",
            "description": "This file hash indicates that a sample of Poison Ivy is present.",
            "indicator_types": [
                "malicious-activity"
            ],
            "pattern": "[file:hashes.'SHA-1' = '408d94384216f890ff7a0c3528e8bed1e0b01621']",
            "pattern_type": "stix",
            "valid_from": "2014-02-20T09:00:00Z"
        },
        // Suite page suivante
    ]
}
```

Représentation JSON (2/2)

```
{
    [
        // Suite de la page précédente
        {
            "type": "malware",
            "spec_version": "2.1",
            "id": "malware--fdd60b30-b67c-41e3-b0b9-f01faf20d111",
            "created": "2014-02-20T09:16:08.989Z",
            "modified": "2014-02-20T09:16:08.989Z",
            "name": "Poison Ivy",
            "malware_types": [
                "remote-access-trojan"
            ],
            "is_family": false
        },
        {
            "type": "relationship",
            "spec_version": "2.1",
            "id": "relationship--29dcdf68-1b0c-4e16-94ed-bcc7a9572f69",
            "created": "2020-02-29T18:09:12.808Z",
            "modified": "2020-02-29T18:09:12.808Z",
            "relationship_type": "indicates",
            "source_ref": "indicator--a932fcc6-e032-476c-826f-cb970a5a1ade",
            "target_ref": "malware--fdd60b30-b67c-41e3-b0b9-f01faf20d111"
        }
    ]
}
```

Outillage

- STIX prend en compte la modélisation de la menace, mais aussi les indicateurs techniques.
- Il est possible de construire un modèle de données pour les investigations basé sur le modèle STIX (en Python par exemple [2]).
- Les outils internes d'investigation de l'ANSSI utilisent une implémentation du modèle STIX pour représenter les indicateurs techniques, offrant ainsi une interopérabilité native entre différents outils.

Vue d'ensemble

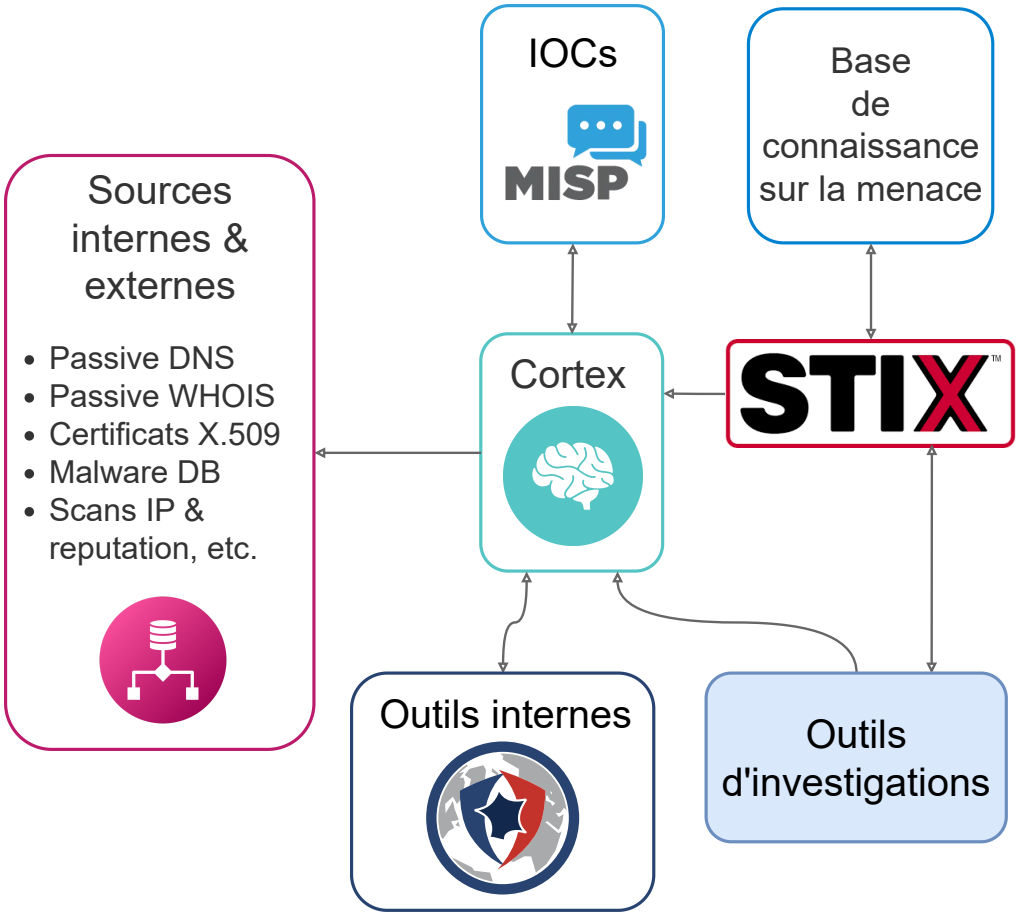


Figure – Infrastructure utilisée pour les investigations (vue partielle et simplifiée).

Plan

Plan

Le cas du MOA Mustang Panda

- En 2022, de nombreux éditeurs de sécurité ont décrit les activités du MOA Mustang Panda (aussi connu sous les noms Earth Preta [3], Bronze President [4] ou RedDelta [5]).
- Réputé d'origine chinoise en source ouverte, cible majoritairement les entités gouvernementales et diplomatiques en Asie et en Europe à fins d'espionnage.
- L'ANSSI constate que depuis le mois de juin 2022, ce MOA est employé pour des campagnes d'hameçonnage ciblées, déployant les mêmes techniques, tactiques et procédures (*TTPs*).

TTPs du mode opératoire d'attaque

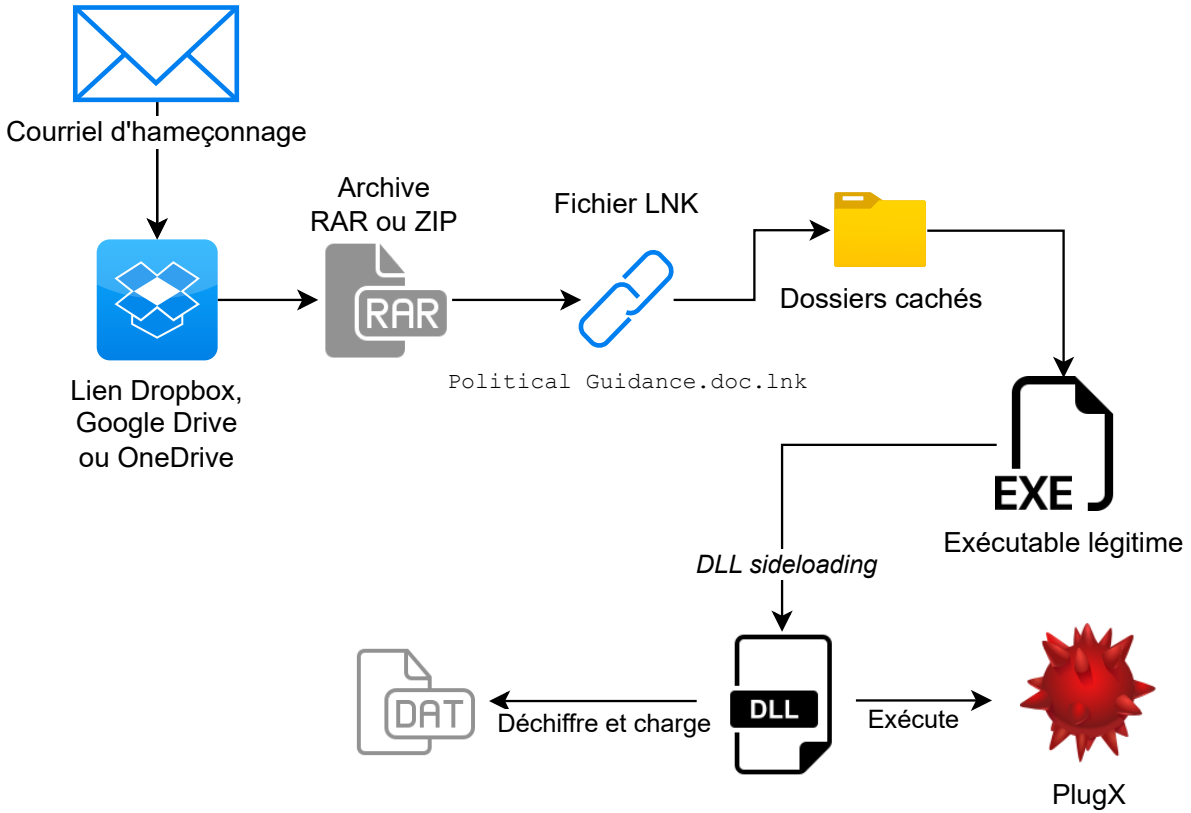
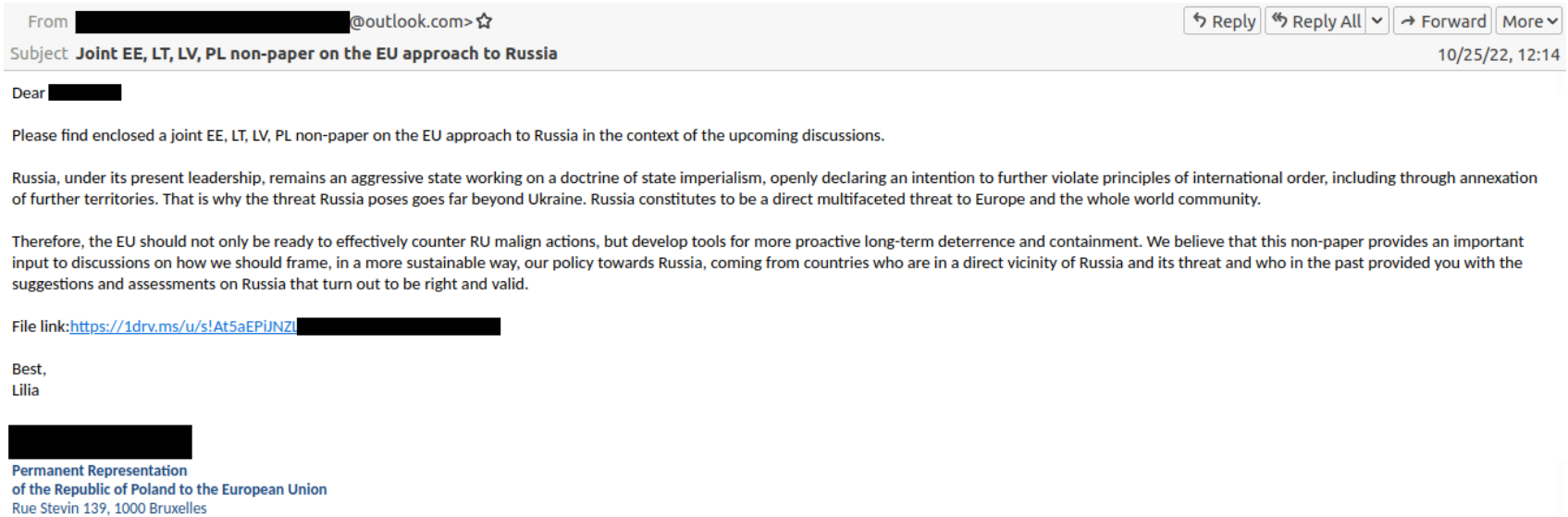


Figure – La charge finale délivre une variante du code malveillant **PlugX** [7, 6].

Hameçonnage ciblé



From [redacted]@outlook.com> ☆ Reply | Reply All | Forward | More

Subject **Joint EE, LT, LV, PL non-paper on the EU approach to Russia** 10/25/22, 12:14

Dear [redacted]

Please find enclosed a joint EE, LT, LV, PL non-paper on the EU approach to Russia in the context of the upcoming discussions.

Russia, under its present leadership, remains an aggressive state working on a doctrine of state imperialism, openly declaring an intention to further violate principles of international order, 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 actions, but develop tools for more proactive long-term deterrence and containment. We believe that this non-paper provides an important input to discussions on how we should frame, in a more sustainable way, our policy towards Russia, coming from countries who are in a direct vicinity of Russia and its threat and who in the past provided you with the suggestions and assessments on Russia that turn out to be right and valid.

File link:https://1drv.ms/u/s!At5aEPiJNZL[redacted]

Best,
Lilia

[redacted]
Permanent Representation
of the Republic of Poland to the European Union
Rue Stevin 139, 1000 Bruxelles

Figure – Exemple de courriel d'hameçonnage imputé au MOA Mustang Panda, détecté en propre.

Plan

Investigation

Investiguer, pourquoi faire ?

Les investigations permettent d'identifier des indicateurs de compromission (*IOC*) (système ou réseau) supplémentaires pour étendre la couverture de détection.

Les investigations se sont concentrées sur :

- les fichiers LNK utilisés par Mustang Panda dans ses courriels d'hameçonnage ;
- l'infrastructure de commande et contrôle (C2) des codes malveillants du MOA.

Fichiers LNK

Le fichier LNK :

- tente de lancer l'exécutable présent dans le dossier caché ;
- si échec, tente de dézipper l'archive RAR avec `7z` ou `Winrar` ;
- ...puis ré-essaye de lancer l'exécutable.

```
cmd.exe /c "_\___\_\___\_____\_____\__\test11.bpu||(forfiles /^P %USERPROFILE%\ /S /^M
↪  "Political Guidance for the new EU approach towards Russia.rar" /C "cmd /c
↪  (c:\progra~1\7-Zip\7z x -y -aoa @path||c:\progra~2\7-Zip\7z x -y -aoa
↪  @path||c:\progra~1\winrar\winrar x -id -o+ @path||c:\progra~2\winrar\winrar x -id -o+
↪  @path)&&_\___\_\___\_____\_____\__\test11.bpu")"
```

Listing – Exemple de fichier LNK utilisé par Mustang Panda.

Fichiers LNK

Les fichiers LNK utilisés dans les campagnes de Mustang Panda présentent des caractéristiques communes :

- Les commandes exécutées sont similaires (« `cmd.exe` », « `7z` », « `rar` »).
- Les noms de dossiers cachés sont marquants (« ' », « # », ...).
- Les métadonnées des fichiers LNK sont parfois identiques (date de création, nom de machine Windows).

Grâce à ces informations, on peut créer une règle YARA qui permet d'identifier des fichiers similaires sur des plateformes d'analyses de codes (VirusTotal, HybridAnalysis, ...).

Fichiers LNK

MD5	Nom de l'archive	Date de soumission
3a94449d664033955012edac0161b2b8	Predlog termina zvanicne posjete zamjenice predsjedavajuceg Vijeca ministara i ministarke vanjskih poslova BiH.rar	2022-06-21
788cf16121782b4358dc8350012470ab	HU proposals to the draft EUCO conclusions.rar	2022-06-22
3277b31aa055bc149af8c37699019586	Embassy of the Republic of Suriname 2022-N-033.rar	2022-06-29
6814dbf5f182573d8b41483444f8949e	EL Non-Paper Pandemic Resilience final.rar	2022-07-21
1f47ba7fd131a1a6f7623d76b420d7e9	EL Non-Paper Pandemic Resilience final.rar	2022-07-14
5ba870c590e56ae0c70c4d7b3141fcde	State of play in EU trade policy.docx.rar	2022-08-09
93ea0e238a0968258753f7f0716027ca	SIAC SU - UA economy in a dire condition L INT.rar	2022-08-22
08ab54c515ac2ecbbe090a6ed48ba957	General background to the Red-White-Red Card.rar	2022-10-06
07e9c84bee28450b1ec24a6f06016802	NV 309-2022 HMA's departure.rar	2022-07-04
2d29e453749a6b6e18516015f6047f1a	Political Guidance for the new EU approach towards Russia.rar	2022-10-26
7162048537b87eede862446bbbdd2a8c	CTF Challenge.docx.lnk	2022-11-27
7fc81cb11b30d320f7c57efd80a91510	Written comments of Hungary.rar	2022-12-06

Table – Archives RAR malveillantes imputées au MOA Mustang Panda.

Infrastructure de commande et contrôle

Le code malveillant **PlugX** utilisé par Mustang Panda communique avec une infrastructure de commande et contrôle (C2) propre au mode opératoire.
Notamment, plusieurs serveurs ont présenté un même certificat TLS sur le service HTTPS :

```
Data:
    Version: 3 (0x2)
    Serial Number:
        93:2b:71:4e:d1:86:96:ee:d0:37:92:37:30:f2:d2:ce:11:07:4a:ec:da:9c:b0:55:37:a7:7a:a8:
        ↪  61:70:1a:ae
    Signature Algorithm: sha256WithRSAEncryption
    Issuer: CN = CTA Root CA, O = TEST TEST TEST , dnQualifier = XCyLBHpPeutyqKCD88faNw==
    Validity
        Not Before: Feb 23 11:24:19 2022 GMT
        Not After : Mar  3 11:24:19 2032 GMT
    Subject: CN = 45.134.83.29, O = File Transfer Service, OU = TLS Demo Cert, dnQualifier =
    ↪  mg3/mLPmK3YfX/MaJCs/mg==
```

Listing – Certificat TLS utilisé pour l'infrastructure C2 de Mustang Panda.

Infrastructure de commande et contrôle

Il est possible de chercher sur différents services les serveurs présentant ce certificat TLS :

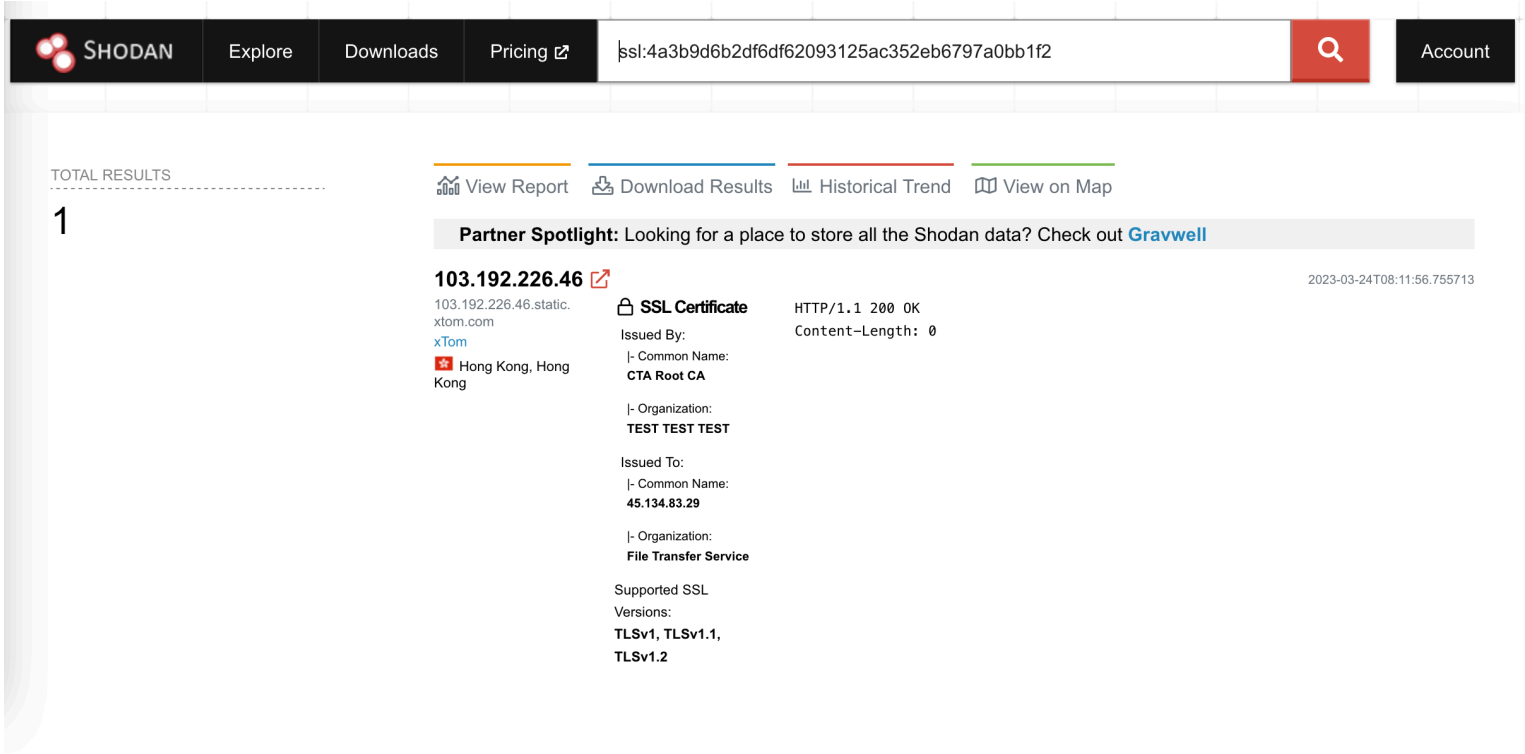


Figure – Exemple de requête SHODAN permettant d'identifier les serveurs utilisant ce certificat TLS.

Infrastructure de commande et contrôle

Un suivi automatique a permis de remonter plusieurs éléments de l'infrastructure C2 du MOA :

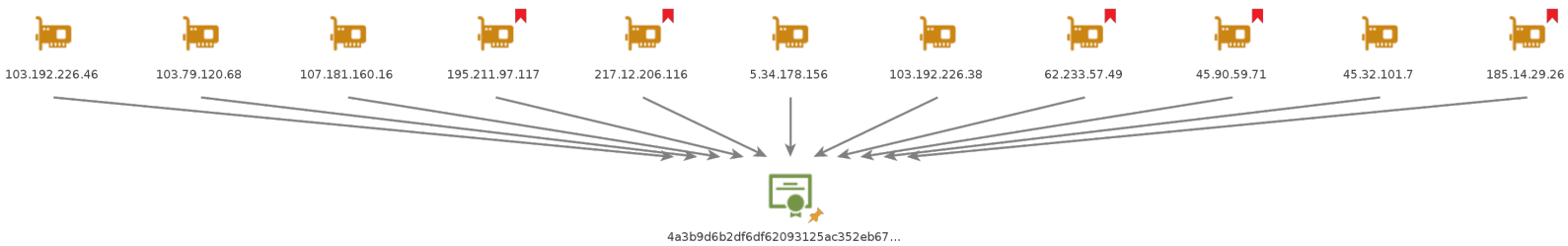


Figure – Schéma partiel de infrastructure identifiée grâce au certificat TLS. Les nouveaux serveurs identifiés ont été tagués en rouge.

Infrastructure de commande et contrôle

Les serveurs C2 présentent aussi d'autres caractéristiques marquantes :

- la réponse HTTP est particulièrement lacunaire (pas d'en-tête « `Server` » ni de contenu) ;

```
HTTP/1.1 200 OK
Content-Length: 0
```

Listing – Réponse HTTP retournée

- l'empreinte JARM [8] des serveurs est identique.

Infrastructure de commande et contrôle

Ces caractéristiques ont permis d'identifier une autre ramification de l'infrastructure du mode opératoire.

```
Data:
Version: 3 (0x2)
Serial Number:
c0:5b:ce:14:96:c7:54:8b
Signature Algorithm: sha256WithRSAEncryption
Issuer: C = US, ST = Washington, L = Seattle,
↪  O = "TrustAsia Technologies, Inc." , OU =
↪  Domain Validated SSL, CN = Root
CA, emailAddress = admin@admin.com
Validity
Not Before: Sep 1 08:41:15 2022 GMT
Not After : Sep 1 08:41:15 2023 GMT
Subject: C = US, ST = Washington, L = Seattle,
↪  O = "TrustAsia Technologies, Inc.", OU =
↪  Domain Validated SSL, CN = Root
CA, emailAddress = admin@admin.com
```

Listing – Exemple de certificat auto-signé utilisé par Mustang Panda.

Les certificats TLS sont aussi marquants :

- ils sont auto-signés ;
- ils imitent des certificats TLS légitimes délivrés par TrustAsia Technologies ;
- les adresses courriels présentes dans les certificats ne correspondent pas à celles des certificats TLS légitimes.

Infrastructure de commande et contrôle

censys | Hosts | services.jarm.fingerprint: 07d0bd16d21d21d07c07d0bd07d21dd7fc4c7c6ef19b7 | Search

Results | Report

Host Filters

Labels:

5 remote-access
4 network-administration
1 file-sharing

Autonomous System:

1 GREENFLOID-AS
1 ITL-BG
1 ITL-LV
1 ITLDC-NL
1 UCLOUD-HK-AS-AP UCLOUD INFORMATION TECHNOLOGY HK LIMITED

Location:

1 Bulgaria
1 Hong Kong
1 Latvia
1 Netherlands
1 Singapore

Service Filters

Hosts

Results: 5 Time: 0.34s

195.123.211.59 (vds1099164.hosted-by-itldc.com)
ITL-LV (50979) Riga, Latvia
443/HTTP 3389/RDP 5000/UNKNOWN 5985/HTTP 47001/HTTP

5.34.176.204 (vds1099249.hosted-by-itldc.com)
GREENFLOID-AS (204957) Singapore
22/SSH 443/HTTP

185.82.216.184 (vds-989443.hosted-by-itldc.com)
ITL-BG (59729) Sofia-Capital, Bulgaria
137/NETBIOS 139/NETBIOS 443/HTTP 445/SMB 3389/RDP
5000/UNKNOWN 5010/UNKNOWN 5985/HTTP 47001/HTTP

185.14.30.182 (vds-1003600.hosted-by-itldc.com)
ITLDC-NL (21100) Drenthe, Netherlands
443/HTTP 3389/RDP 5000/UNKNOWN 5010/UNKNOWN 5985/HTTP

152.32.225.186
UCLOUD-HK-AS-AP UCLOUD INFORMATION TECHNOLOGY HK LIMITED (135377) Central and Western, Hong Kong

Figure – Exemple de requête Censys prenant en compte les caractéristiques marquantes identifiées.

Infrastructure de commande et contrôle

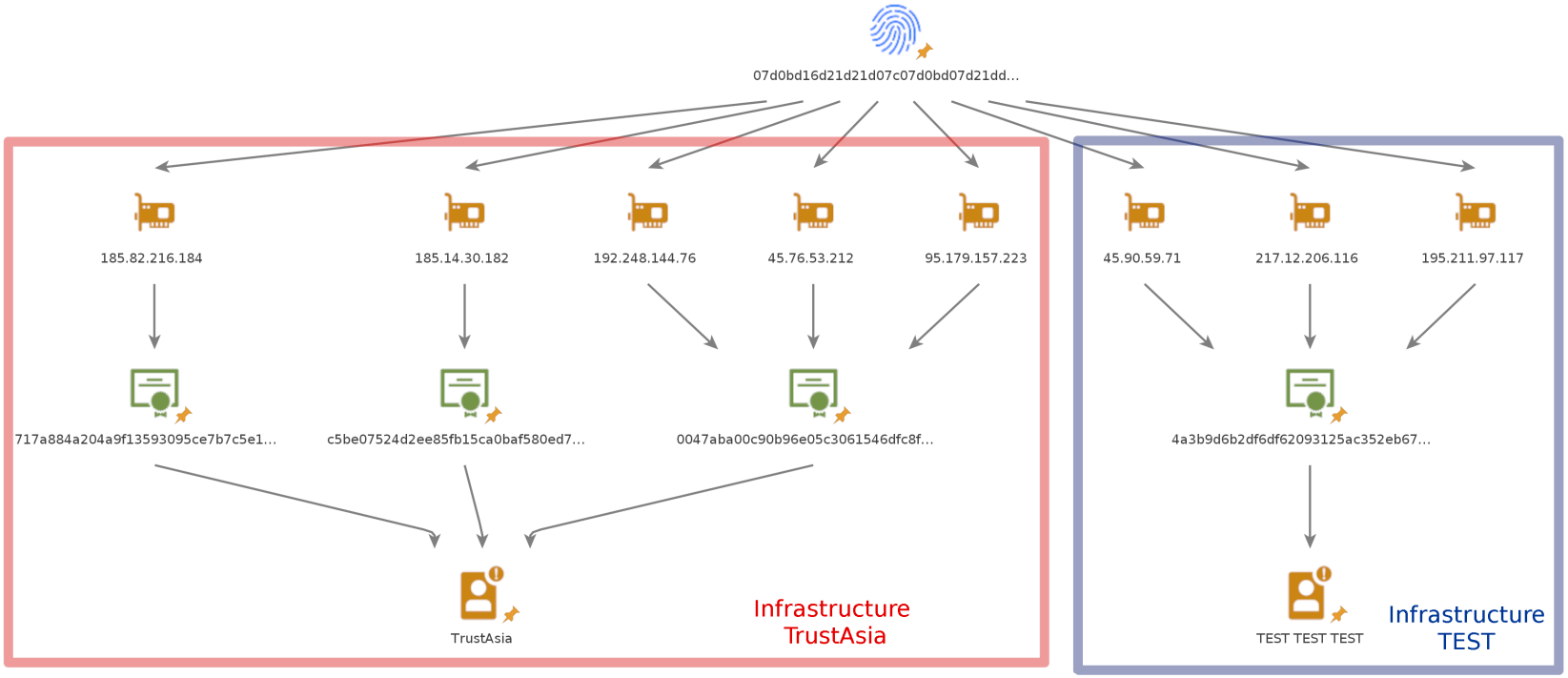


Figure – Schéma partiel des infrastructures identifiées liées à Mustang Panda. Les deux parties d'infrastructure partagent la même empreinte JARM.

Infrastructure de commande et contrôle

- Au total, une vingtaine de serveurs a été identifiée.
- Plusieurs de ces serveurs ont effectivement été utilisés comme serveurs C2 de **PlugX**.
- D'autres caractéristiques marquantes des serveurs ont pu être identifiées (nom de machine Windows, réutilisation d'hébergeurs, ...) :
  - Par exemple les noms de machine suivantes : « `WIN-9ACKK6OQFVF` » et « `XS15594200214` »

Plan

Entrave réussie

- Le CERT-FR a réussi à anticiper la menace en mettant en détection des indicateurs de compromission (*IOC*) jusqu'alors inconnus.
- Il est possible de rejouer l'investigation à l'aide de nombreux outils en ligne (e.g. SHODAN, ONYPHE, CENSYS), comme illustré précédemment.
- En développant ses propres outils afin d'automatiser ces recherches, notamment en s'appuyant sur Cortex [1], il est possible de suivre une infrastructure d'attaque.
- Cette mise en détection précoce a permis d'entraver l'attaque en effectuant un signalement vers une victime potentielle qui a su réagir rapidement.

1. `https://github.com/TheHive-Project/Cortex`

En savoir plus

- Nos rapports sur la menace
  - `cert.ssi.gouv.fr/cti/`
- Notre flux MISP public
  - `https://misp.cert.ssi.gouv.fr/feed-misp/` [2]

2. Politique de partage et d'utilisation : `https://www.cert.ssi.gouv.fr/csirt/politique-partage/`

Bibliographie I

[1] OASIS Cyber Threat Intelligence Technical Committee. *STIX Version 2.1*. https://docs.oasis-open.org/cti/stix/v2.1/os/stix-v2.1-os.html. 2021.

[2] *Bibliothèque Python STIX*. https://pypi.org/project/stix2/. Sept. 2021.

[3] TrendMicro. *Earth Preta Spear-Phishing Government worldwide*. https://www.trendmicro.com/en_us/research/22/k/earth-preta-spear-phishing-governments-worldwide.html. Nov. 2022.

[4] SecureWorks. *Bronze President targets government officials*. https://www.secureworks.com/blog/bronze-president-targets-government-officials. Sept. 2022.

[5] Recorded Future. *Chinese State-Sponsored Group 'RedDelta' Targets the Vatican and Catholic Organizations*. https://www.recordedfuture.com/reddelta-targets-catholic-organizations. 28 juill. 2022.

[6] Kienmanowar. *Diving into a PlugX sample of Mustang Panda group*. https://kienmanowar.wordpress.com/2022/12/27/diving-into-a-plugx-sample-of-mustang-panda-group/. Déc. 2022.

[7] ESET. *Mustang Panda's Hodur : Vieux trucs, nouvelle variante de Korplug*. https://www.welivesecurity.com/fr/2022/03/25/mustang-pandas-hodur-nouveau-korplug/. Mars 2022.

[8] Salesforce. *Easily Identify Malicious Servers on the Internet with JARM*. https://engineering.salesforce.com/easily-identify-malicious-servers-on-the-internet-with-jarm-e095edac525a/. Nov. 2020.