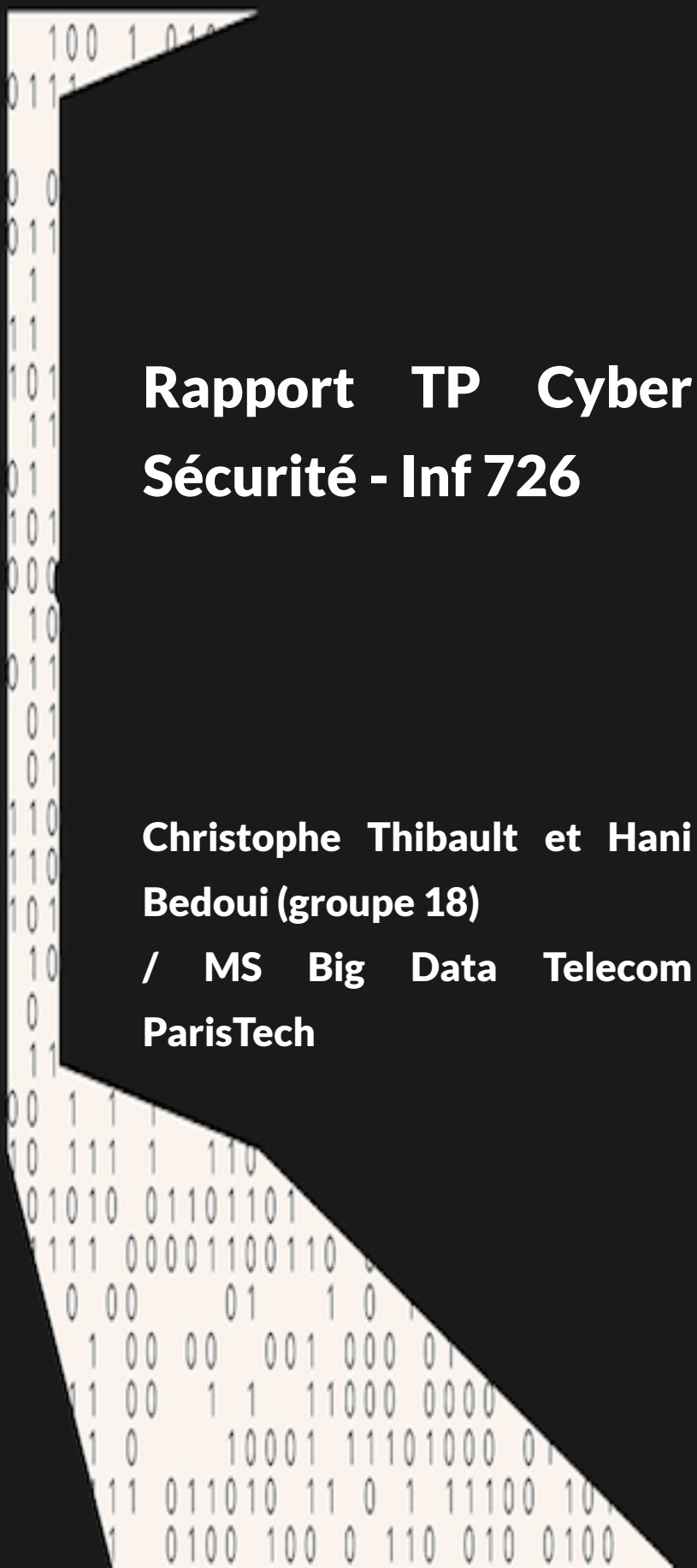

Rapport TP Cyber Sécurité - Inf 726

Christophe Thibault et Hani Bedoui (groupe 18)
/ MS Big Data Telecom ParisTech

Contents

1 CONTEXTE

1.1 INTRODUCTION

Nous sommes des analystes au sein d'un SOC (Security Operations Center) du ministère des armées. Le centre d'analyse et de lutte informatique défensive nous a envoyé par email un rapport d'analyse sur une campagne en cours : *Banacry*. En effet, depuis mars 2018, plusieurs fuites de données ont été attribuées au groupe Banet, implanté en Russie. Les secteurs ciblés sont ceux des télécommunications, de l'aéronautique et de la défense notamment de pays situés en zone Europe et membres de l'OTAN. Les techniques qui sont utilisées ne sont pas clairement identifiées mais des connexions à des serveurs C&C ont été repérées par des experts de McTersky. On a à notre disposition des url, des adresses IPs ainsi que des hashs de fichiers infectés.

1.2 LES DONNÉES DISPONIBLES

Nous avons différentes bases de données à notre disposition:

- Bluecoat : proxy web
- cisco:esa : passerelle réseau
- fgttraffic : Firewall réseau
- linuxsecure : infos d'authentification Linux
- portcontrol : branchement support amovible
- streamysql : écoute réseau et interprétation protocol SQL
- winhostmon : infos de création de processus Windows

2 ANALYSE

En partant des adresses IPs (IOC) qui sont mises à notre disposition (par exemple les adresses 46.252.242.1 , 46.252.242.2 , 46.252.242.7), on a pu constater rapidement que deux machines ont été infectés. Les adresses sources des deux machines en question sont **10.11.36.115** et **10.11.36.93**. On peut le voir sur la figure 1 avec une requête sur l'adresse IP suivante : 81.94.12-.10

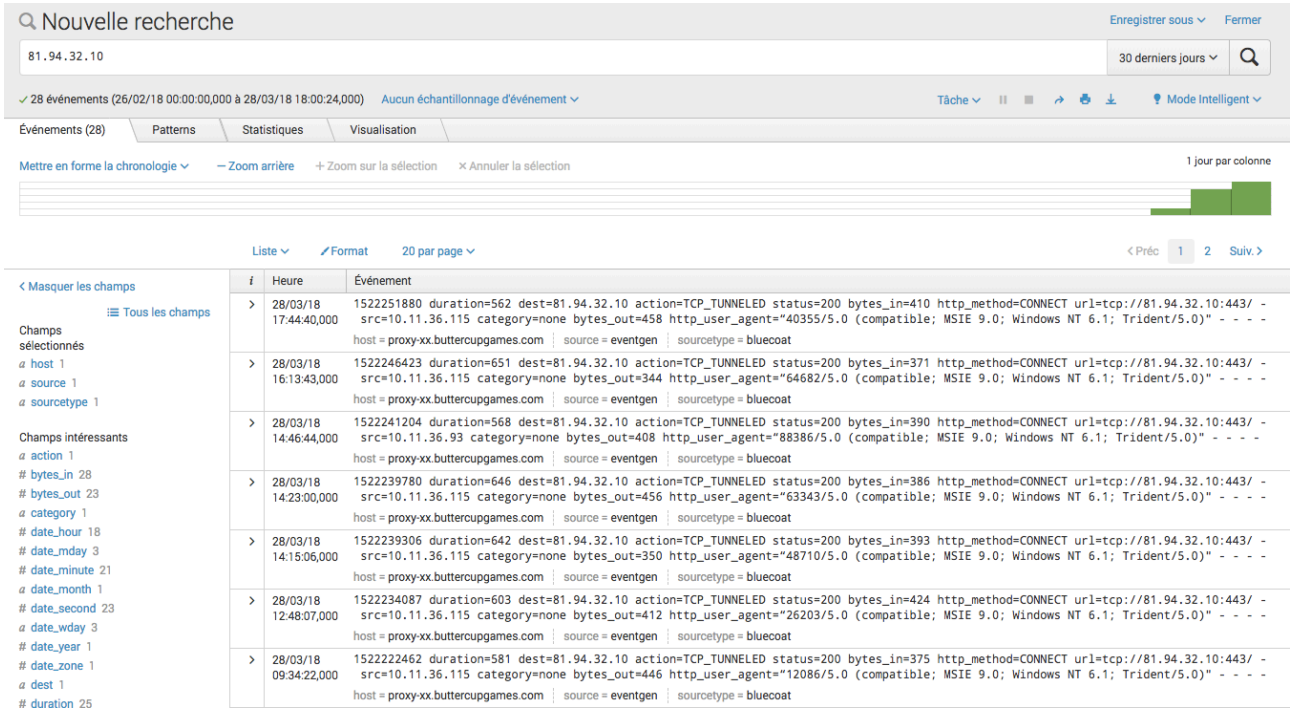

FIGURE 1: RÉSULTATS DES RECHERCHES POUR L'ADRESSE IP : 81.94.32.10

Sur la figure 2, nous avons requêté pour obtenir toutes les adresses IPs des machines qui se sont connectées sur les machines de notre réseau, les 10.11.36.115, et 10.11.36.93.

Nous nous apercevons aussi que les deux utilisateurs des machines ayant pour IPs 10.11.36.115 et 10.11.36.93 ont reçu un fichier pdf (reconversion_2017.pdf) à 22h04 le 27 mars 2018 puis quelques secondes plus tard, un exécutable (stuxbar.exe) se lance (voir sur la figure 3 pour le cas d'Eloise Jodor). Quatre personnes ont reçu un email provenant de liste@marinemobilite.com avec un fichier joint (reconversion_2017.com) comme nous pouvons le voir sur la figure 4.

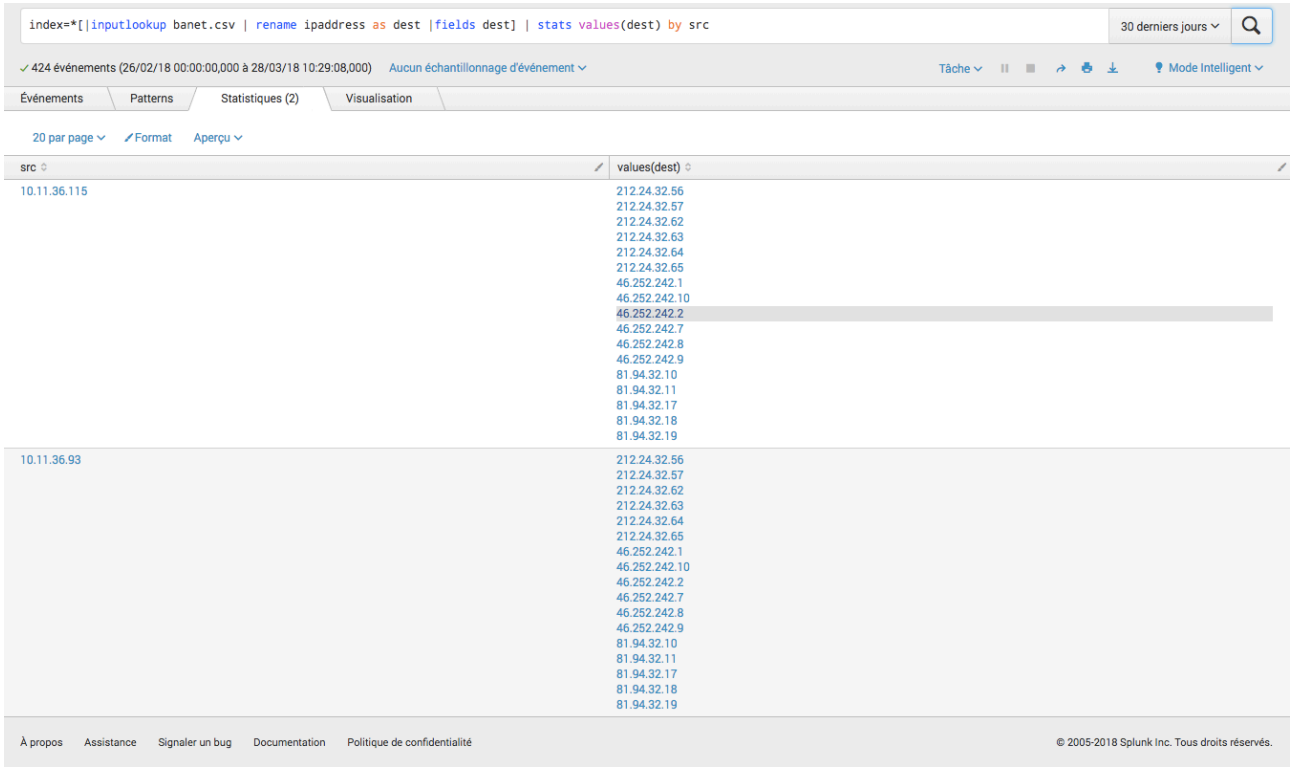

FIGURE 2: MACHINES APPARTEMENT AU RÉSEAU QUI SE SONT CONNECTÉES AVEC DES C&C SUSPECTS : 10.11.36.115 ET 10.11.36.93

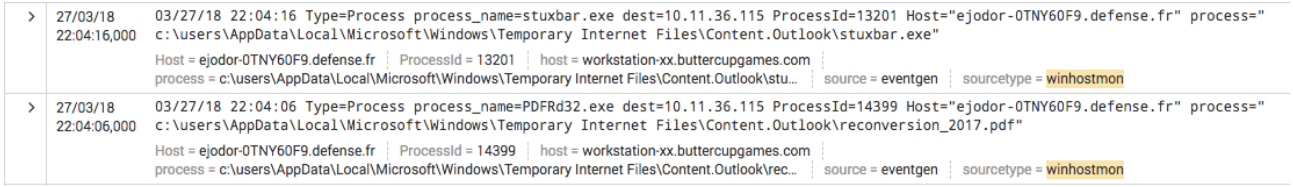

FIGURE 3: RÉSULTATS D'UNE REQUÊTE POUR ELOISE JODOR

On remarque que ce pdf a été envoyé par l'adresse liste@marinemobilite.com depuis l'adresse **212.53.36.199** aux personnes suivantes :

- emmanuel.coraidh@defense.fr
- capucine.palaci@defense.fr
- eloise.jodor@defense.fr
- pierre.dence@defense.fr

Deux personnes ont ouvert ce pdf : Pierre Dence et Eloise Jodor, ce qui correspond aux deux machines infectées et identifiées au début. Les deux autres destinataires n'ont pas ouvert le fichier (puisque l'exécutable stuxbar.exe n'apparaît pas dans les logs).

Comme nous l'avons décrit au début du rapport, le pays concerné semble être la Russie. Ce processus malveillant effectue donc des requêtes vers des serveurs de ce pays. La plupart de ces serveurs ont déjà été signalés pendant la campagne *Banacry*, et de nouvelles adresses liées à cette campagne ont été identifiées (voir la figure 5 de la partie Indices de compromission).

i	Heure	Événement
>	27/03/18 22:03:26,000	Mon Mar 27 22:03:26 2018 orig_dest=204.118.100.129 orig_recipient=liste@marinemobilite.com orig_src=212.53.36.199 protocol=SMTP recipient=emmanuel.coraidh@defense.fr subject="Opportunite reconversion" file_name=reconversion_2017.pdf host = sfo-resources-12.it.buttercupgames.com source = eventgen sourcetype = cisco:esa subject = Opportunite reconversion
>	27/03/18 22:03:26,000	Mon Mar 27 22:03:26 2018 orig_dest=204.118.100.129 orig_recipient=liste@marinemobilite.com orig_src=212.53.36.199 protocol=SMTP recipient=capucine.palaci@defense.fr subject="Opportunite reconversion" file_name=reconversion_2017.pdf host = sfo-resources-12.it.buttercupgames.com source = eventgen sourcetype = cisco:esa subject = Opportunite reconversion
>	27/03/18 22:03:26,000	Mon Mar 27 22:03:26 2018 orig_dest=204.118.100.129 orig_recipient=liste@marinemobilite.com orig_src=212.53.36.199 protocol=SMTP recipient=eloise.jodor@defense.fr subject="Opportunite reconversion" file_name=reconversion_2017.pdf host = sfo-resources-12.it.buttercupgames.com source = eventgen sourcetype = cisco:esa subject = Opportunite reconversion
>	27/03/18 22:03:26,000	Mon Mar 27 22:03:26 2018 orig_dest=204.118.100.129 orig_recipient=liste@marinemobilite.com orig_src=212.53.36.199 protocol=SMTP recipient=pierre.dence@defense.fr subject="Opportunite reconversion" file_name=reconversion_2017.pdf host = sfo-resources-12.it.buttercupgames.com source = eventgen sourcetype = cisco:esa subject = Opportunite reconversion

FIGURE 4: LISTE DES PERSONNES AYANT REÇU UN EMAIL DE LA PART LISTE@MARINEMOBILITE.COM AVEC COMME FICHIER JOINT RECONVERSION_2017.PDF

3 CONCLUSION

L'attaque par ameçonnage ciblé repose généralement sur une usurpation de l'identité de l'expéditeur, et procède par ingénierie sociale forte afin de lier l'objet de l'email et le corps du message à l'activité de la personne ou de l'organisation ciblée. Généralement, l'email usurpe l'identité d'une personne morale ou physique dans le but de duper le destinataire qu'il invite à ouvrir une pièce jointe malveillante ou à suivre un lien vers un site Web malveillant. Une fois cette première machine contaminée, l'attaquant en prend le contrôle pour manœuvrer au sein du système d'information de l'organisation constituant la véritable cible.

En conclusion, cette simulation d'attaque de Banet était très intéressante et nous a permis d'avoir un aperçu du métier dans un Service Operations Center. Nous nous sommes rendus compte qu'il n'y avait pas de procédure unique, et qu'il fallait y aller à tâtons dans notre démarche. L'analyste doit chercher en partant du peu d'informations reçues en entrée et essayer de remonter vers la source de l'attaque. L'expérience de l'analyste et la connaissance du comportement type des attaques est donc essentielle.

4 INDICES DE COMPROMISSION

- Processus malveillant : **stuxbar.exe**
- Fichier infecté : **reconversion_2017.pdf**

- Adresse email suspecte : **liste@marinemobilite.com**

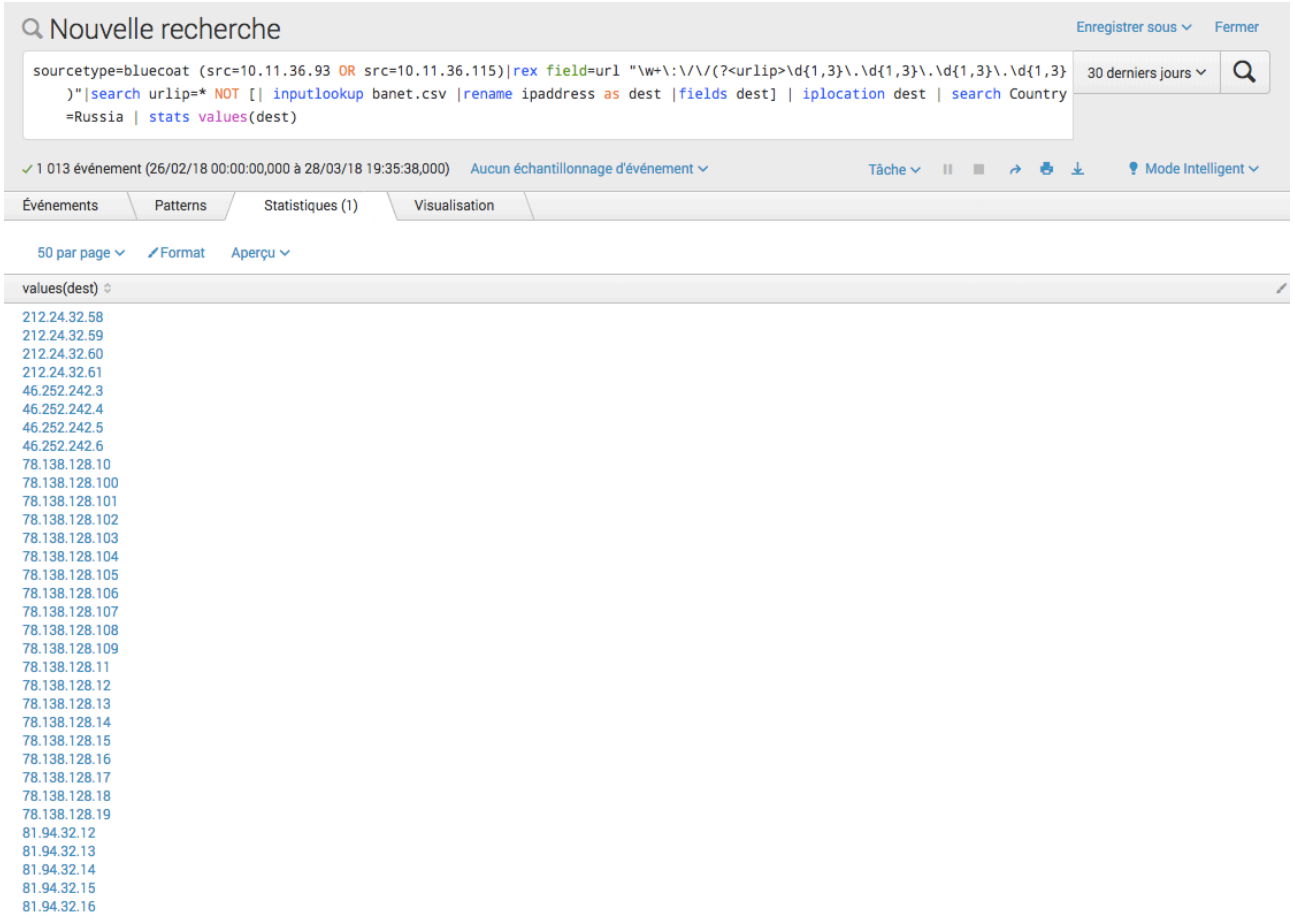

FIGURE 5: LISTE DES ADRESSES IP SUSPECTES, COMPLÉTANT CELLE FOURNI PAR MC-TERSKY