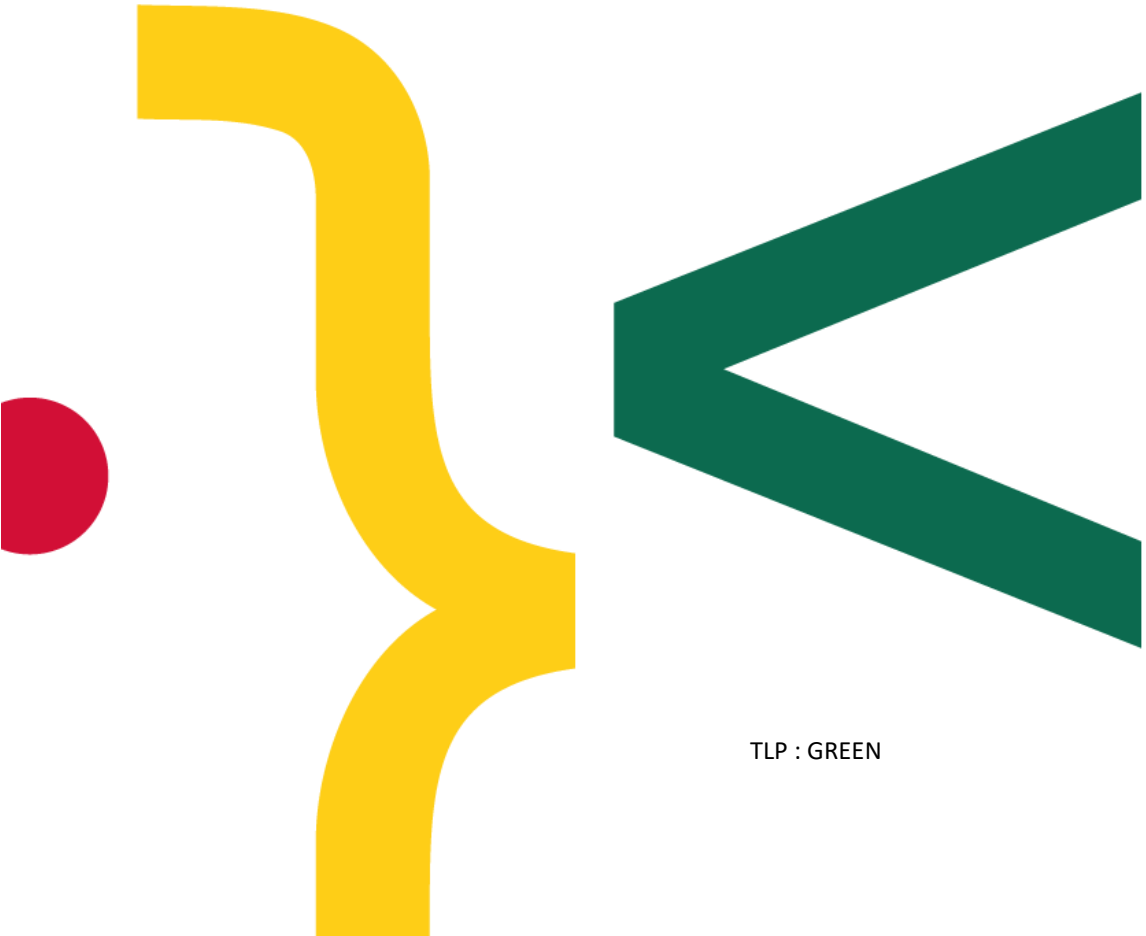
CERT.tg

CYBER DEFENSE AFRICA

Campagne de Phishing visant les institutions financières des pays d'Afrique francophone



TLP : GREEN

Informations du document

Information	
ID	AS01-0123
Titre	Campagne de Phishing visant les institutions financières des pays d'Afrique francophone
Sévérité	White
Destinataire	Institutions financières
Rapporteur	CERT.TG

Version du document	Date	Nature des modifications
1.0	10/01/2023	Version originale

Table des matières

Table des Figures

Listes des Tableaux

1. Sommaire

Le groupe cybercriminel Bluebottle, spécialisé dans les attaques ciblées contre le secteur financier, mène actuellement une campagne de phishing contre les institutions financières dans les pays de l'Afrique francophone.

Le groupe exploite les logiciels malveillants déjà connus et les outils à double usage (msf, cobaltstrike, etc) ; pour le moment aucun logiciel malveillant personnalisé n'a été déployé dans cette campagne.

La campagne de phishing aurait débuté entre **juillet** et **septembre 2022** (il est probable qu'une partie de l'activité aurait début déjà depuis mai 2022).

2. Mode opératoire

Le groupe cybercriminel utiliserait comme appâts des fichiers malveillants sur le thème des offres d'emploi ou de recrutement envoyés par spear-phishing où dans certains cas, le malware était nommé de manière à faire croire à l'utilisateur qu'il s'agissait d'un fichier PDF, par exemple :

- Fiche de poste.exe ("job description")
- Fiche de candidature.exe ("application form")
- Fiche de candidature.pdf.exe ("application form")

Dans de nombreux cas, le malware attaché au fichier est le logiciel malveillant GuLoader.

GuLoader est un téléchargeur basé sur un shellcode doté de fonctions anti-analyse qui va en plus déployer certains modules binaires légitimes comme diversion pour son activité malveillante. GuLoader a été distribué aux victimes dans un exécutable NSIS auto-extractible. Ce script NSIS déchiffre et injecte un shellcode obfusqué dans un autre processus. Le processus le plus souvent observé est **ieinstal.exe**, l'installateur de l'extension Internet Explorer, mais il comprend également **aspnet_regbrowsers.exe**, l'outil d'enregistrement du navigateur ASP.NET.

Le processus d'installation du module complémentaire d'Internet Explorer est probablement utilisé pour télécharger un téléchargeur .NET malveillant à partir d'URL telles que ***hxxp://178.73.192[.]15/ca1.exe***. Plusieurs téléchargeurs .NET ont été découverts, qui abusent du service de transfert de fichiers transfer[.]sh pour télécharger un fichier portant une extension RTF. Cette charge utile est inconnue, mais les téléchargeurs sont conçus pour la charger en tant que DLL .NET.

Après le déploiement de GuLoader et des chargeurs .NET, divers autres outils post-compromission ont été vus sur les réseaux des victimes. Il s'agit notamment du cheval de Troie d'accès à distance (RAT) **Netwire**, disponible publiquement, et du RAT open-source

Figure 4 Méthodes utilisées

Quasar. Les attaquants ont également utilisé l'outil commercial de post-intrusion **Cobalt Strike Beacon** (celle utilisée par Bluebottle emploie une technique « anti-forensic » afin d'entraver l'analyse).

3. Recommandations

Il est recommandé de :

- Vérifier la présence ou non dans les journaux d'évènement des serveurs mails des indicateurs de compromission mentionnés ci-dessous :
    - hxxp://files[.]ddrive[.]online:444/load
    - hxxp://85.239.34[.]152/download/XWO_UnBkJ213.bin
    - hxxps://transmissive-basin[.]000webhostapp[.]com
    - hxxps://udapte[.]adesy[.]in
    - banqueislamik[.]ddrive[.]online
    - hxxps://transfer[.]sh/get/mKwvWI/NHmZJu.rtf
    - hxxps://transfer[.]sh/get/RTPlqa/oISxUP.rtf
    - hxxp://files[.]ddrive[.]online:4448/a
    - hxxp://banqueislamik[.]ddrive[.]online:4448/ZPjH
    - hxxp://46.246.86[.]12/ca3.exe
    - hxxp://178.73.192[.]15/ca1.exe
    - personnel[.]bdm-sa[.]fr
    - 185.225.73[.]165

- Demander aux utilisateurs de signaler tous mails ou téléchargements suspects
- Effectuer une campagne de sensibilisation au phishing
- Effectuer une revue des règles sur les pares-feux c'est-à-dire limiter les trafics sortants uniquement aux ressources nécessaires, bloquer tous les autres trafics et limiter les trafics entrants aux ports, protocoles et aux ressources qui doivent y avoir accès
- Contacter le CERT.tg en cas d'activité suspecté liée à cette campagne.

Références

- https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/bluebottle-banks-targeted-africa
- https://www.crowdstrike.com/blog/guloader-dissection-reveals-new-anti-analysis-techniques-and-code-injection-redundancy/
- https://www.crowdstrike.com/blog/guloader-malware-analysis/