CYBER DEFENSE AFRICA S.A.S.

# ALERTE DE SECURITE

## FASTCash 2.0
## « Le braqueur numérique de banques »

AS20-1202-1

CYBER DEFENSE AFRICA

# Informations du document

| Information | |
|---|---|
| **Projet** | ALERTE DE SECURITE |
| **ID** | AS20-1202-1 |
| **Titre** | FASTCash 2.0, le braqueur numérique de banques |
| **Sévérité** | Critique |
| **Cible** | Banques et institutions financières du Togo |
| **Rapporteur** | CDA |

| Version du document | Date | Nature des modifications |
|---|---|---|
| **1.0** | 02/12/2020 | Version originale |

CYBER DEFENSE AFRICA

# Table des matières



## Liste des tableaux et figures

# 1. Introduction

Le CISA (Cybersecurity and Infrastructure Security Agency), le Département du trésor (Treasury), Le FBI (Federal Bureau of Investigation) et le USCYBERCOM (U.S. Cyber Command) ont identifié un logiciel malveillant nommé FASTCASH 2.0. Ce malware est utilisé par une équipe nord-coréenne de cyber attaquant pour effectuer des retraits frauduleux dans les Guichets Automatiques de Banques (GAB). Le malware utilise plusieurs techniques pour rester invisible dans les systèmes d'information et rester actif malgré le redémarrage, changements de mots de passes, etc… (persistance).

D'après un rapport initialement publié le 26 Août 2020, Le Togo fait partie des pays impactés. Nous vous prions donc de vérifier si votre institution est victime de cette attaque à travers nos indications du chapitre 5 de ce document.

Dans le cas où votre institution serait victime, nous vous saurions gré de prendre contact avec Cyber Defense Africa S.A.S pour déclarer cet incident et obtenir un accompagnement pour la remédiation :

**Cyber Defense Africa S.A.S.**
Rue Abdoulaye Fadiga,
07 BP 13215, Lomé, Togo
csirt@cda.tg
(+228) 22 53 59 80
(+228) 70 54 93 24
(+228) 70 54 93 25
www.cda.tg

## 2. Les pays affectés par l'attaque

D'après le rapport, plusieurs institutions financières des pays suivants dont le Togo auraient été touché par cette attaque entre 2015 et 2020: Argentine, Brésil, Bangladesh, Bosnie-Herzégovine, Bulgarie, Chili, Costa Rica, Équateur, Ghana, Inde, Indonésie, Japon, Jordanie, Kenya, Koweït, Malaisie, Malte, Mexique, Mozambique, Népal, Nicaragua, Nigéria, Pakistan, Panama , Pérou, Philippines, Singapour, Afrique du Sud, Corée du Sud, Espagne, Taiwan, Tanzanie, Togo, Turquie, Ouganda, Uruguay, Vietnam, Zambie (figure 1).

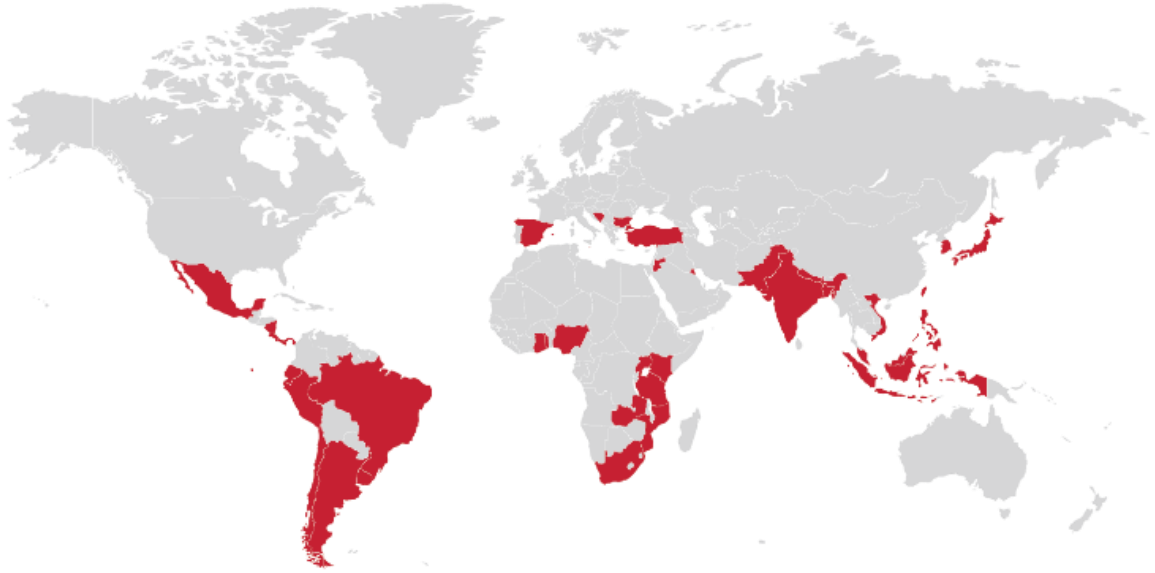

*Figure 1 : Pays affectés par l'attaque FASTCash 2.0 depuis 2015*

# 3. Anatomie d'une attaque de banque par FASTCash 2.0

La figure ci-dessous fournit une représentation graphique d'une attaque de banque par FASTCash 2.0.

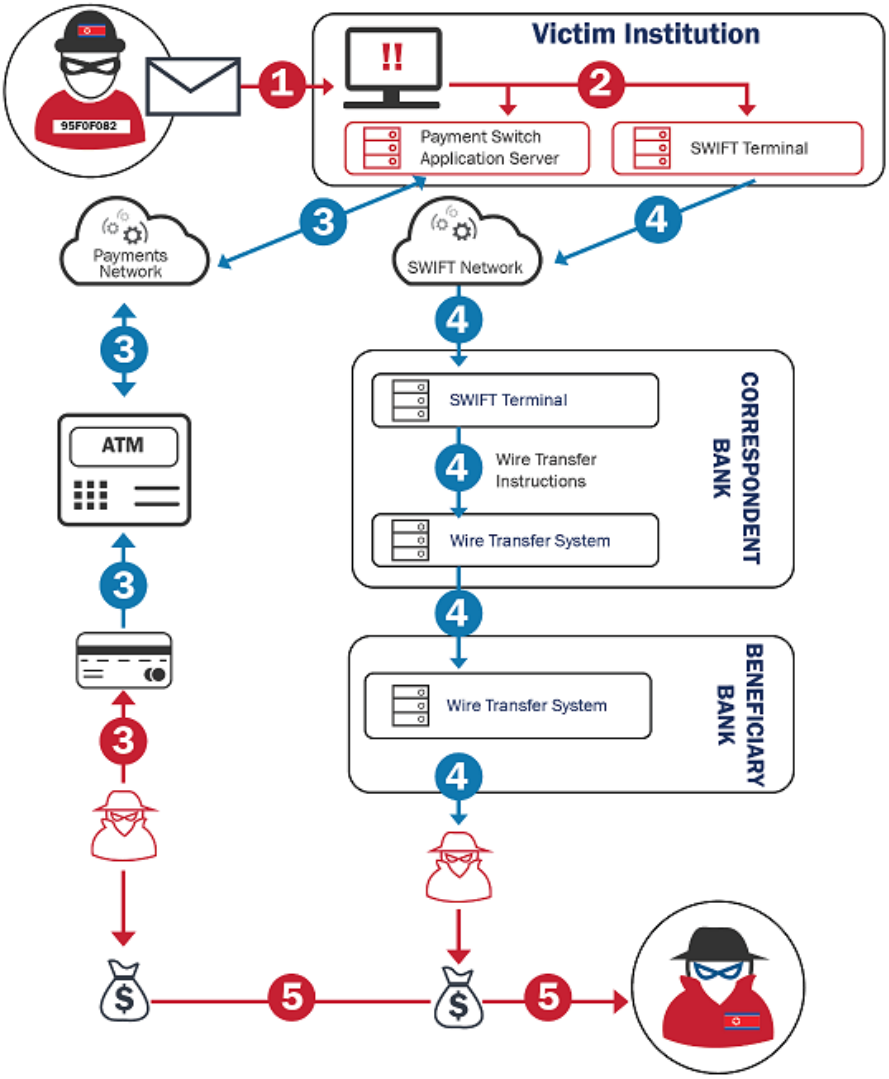


*Figure 2 : Présentation de l'attaque de FASTCash 2.0*

# 4 Analyse technique

## 4.1 Les vecteurs et méthodes d'attaques

Les attaquants derrière FASTCash utilisent une variété de techniques, telles que le spearphishing et le watering holes, pour permettre un accès initial aux institutions financières ciblées.

D'après le rapport, vers la fin de 2018 à 2019 et au début de 2020, ces attaquants ont démontré l'utilisation de tactiques d'ingénierie sociale en lançant des attaques de phishing sur le thème des applications métiers à l'aide des fichiers malveillants accessibles au public.

Les modes d'infection ou d'intrusion sont les suivants :

- Envoie par mail d'une pièce jointe contenant un logiciel malveillant à une personne, une entreprise ou une industrie ;
- Compromission d'un site Web visité par des utilisateurs d'une entreprise, des communautés, des industries ou des régions spécifiques ;
- Exploitation d'une faille (bug, pépin ou vulnérabilité de conception) dans un système informatique connecté à Internet (Serveur web, serveur de base de données, serveur d'application d'accès publique …) ;
- Vol des informations d'identification d'un utilisateur ou d'un compte de service spécifique pour contourner les contrôles d'accès et obtenir des privilèges élevés ;
- Compromission de partenaires qui ont accès à l'organisation prétendue victime et exploitent leur relation de confiance ;
- Utilisation des services à distance pour accéder initialement au réseau d'une victime et y rester.

## 4.2 L'exécution du malware

Ces attaquants utilisent une variété de techniques pour exécuter leur code sur les systèmes des victimes.

Les méthodes d'exécution du malware sont les suivants :

- Utilisation des interfaces de ligne de commande pour interagir avec les systèmes et exécuter d'autres logiciels ;
- Utilisation des scripts (exemple VBScript et PowerShell) pour accélérer les tâches opérationnelles, réduire le temps nécessaire pour accéder aux ressources critiques et contourner les mécanismes de surveillance des processus en interagissant directement avec le système d'exploitation (OS) au niveau de l'interface de programmation d'application (API) au lieu d'appeler d'autres programmes ;
- Appui sur des actions spécifiques de l'utilisateur, telles que l'ouverture d'une pièce jointe malveillante ;

- Exploitation des vulnérabilités logicielles pour exécuter du code sur un système ;

- Création de nouveaux services ou modification des services existants pour exécuter des exécutables, des commandes ou des scripts ;

- Utilisation de chargeur de module Windows pour charger des bibliothèques de liens dynamiques (DLL) à partir de chemins locaux arbitraires ou de chemins réseau arbitraires UNC (Universal Naming Convention) et exécuter du code arbitraire sur un système ;

- Utilisation de Windows API pour exécuter du code arbitraire sur le système de la victime ;

- Utilisation de planificateur de tâches pour exécuter des programmes au démarrage du système ou sur une base planifiée pour la persistance, effectuer une exécution à distance pour un mouvement latéral, obtenir des privilèges system pour l'escalade de privilèges ou exécuter un processus dans le contexte d'un compte spécifié ;

- Utilisation abusive de fichiers HTML (Hypertext Markup Language) compilés, couramment distribués comme partie intégrante du système d'aide HTML de Microsoft, pour dissimuler du code malveillant ;

- Utilisation de Windows rundll32.exe pour exécuter des binaires, des scripts et des fichiers d'éléments du panneau de configuration et exécuter du code via un proxy pour éviter de déclencher des outils de sécurité ;

- Exploitation de "cron" sous Linux pour créer des tâches d'arrière-plan préplanifiées et périodiques.

### 4.3 La persistance dans votre environnement

Après compromission, les attaquants utilisent plusieurs tactiques pour maintenir l'accès sur le réseau.

Ces tactiques utilisées incluent la modification des informations du registre des systèmes, la programmation des actions à démarrer automatiquement à l'aide de **cron**, le vol des informations d'identification des comptes de service.

### 4.4 L'élévation des privilèges

Une fois que les attaquants s'infiltrent dans votre réseau, ils utilisent des méthodes d'élévation de privilèges en exploitant les comptes des administrateurs pour prendre le contrôle total de votre système d'information.

### 4.5 Furtivité

Les attaquants derrière FASTCash 2.0 utilisent des techniques anti détection très avancées, notamment le chiffrement et autres méthodes d'obfuscation avancées pour cacher leurs activités. Tout ceci rend la détection du malware très complexe.

### 4.6 Accès aux identifiants

Une fois vos systèmes compromis, les attaquants utilisent des logiciels de capture de claviers (keyloggers) très sophistiqués comme ECCENTRICBANDWAGON pour obtenir vos informations d'identification.

### 4.7 Découverte du réseau

Une fois à l'intérieur du réseau d'une institution financière, les attaquants de FASTCash 2.0 semblent rechercher deux systèmes spécifiques : le terminal SWIFT et le serveur hébergeant l'application de commutation de paiement de l'institution. Au fur et à mesure qu'ils progressent dans un réseau, ils découvrent les systèmes auxquels ils ont accédé afin de cartographier le réseau et d'accéder aux deux systèmes visés.

### 4.8 Déplacement latéral

Pour accéder au terminal SWIFT d'une institution financière compromise et au serveur hébergeant l'application de commutation de paiement de l'institution, FASTCash exploite les informations d'identification collectées et tire parti de l'accessibilité de ces systèmes critiques à partir d'autres systèmes du réseau d'entreprise de l'institution. Plus précisément, il est connu que FASTCash crée des exemptions de pare-feu sur des ports spécifiques, y compris les ports 443, 6443, 8443 et 9443.

### 4.9 Collecte d'informations

Les attaquants utilisent les techniques suivantes pour collecter des informations à partir des systèmes exploités :

- Utilisation des méthodes automatisées, telles que des scripts, pour collecter des données
- Capture des entrées de clavier de l'utilisateur pour obtenir des informations d'identification et collecter des informations
- Collecte des données des systèmes locaux à partir d'un système compromis
- Prise des captures d'écran du bureau des ordinateurs

- Collecte des données stockées dans le presse-papiers Windows auprès des utilisateurs

### 4.10 Command and Control

Pour faciliter l'exfiltration des données à distance, les attaquants de FASTCash 2.0 utilisent des protocoles C2 personnalisés et des systèmes de codage de données standard tels que l'American Standard Code for Information Interchange (ASCII), Unicode, Base64, les extensions de messagerie Internet polyvalentes et les systèmes de format de transformation Unicode 8 bits ou d'autres systèmes de codage binaire en texte et de caractères.

### 4.11 Exfiltration des données

Les attaquants de FASTCash 2.0 ne volent pas seulement de l'argent dans les institutions financières mais aussi utilisent ce malware pour exfiltrer des données hors des réseaux compromis.

Les techniques d'exfiltration de données souvent utilisées par les attaquants de FASTCash 2.0 sont les suivantes :

- Compressions et chiffrement des données collectées avant l'exfiltration pour minimiser la quantité de données envoyées sur le Web et les rendre portables, moins visibles et moins détectables.

- Collecte des données via des scripts (bien que cela puisse nécessiter d'autres techniques d'exfiltration).

- Exfiltration des données en utilisant le canal C2.

# 5 Listes des Indicateurs de Compromissions (IOCs) des activités malveillantes de FASTCash 2.0

Le tableau suivant liste les signatures uniques des fichiers indiquant la présence du logiciel malveillant FASTCash 2.0.

La version téléchargeable des IOCs en version STIX est disponible sur le lien suivant : https://us-cert.cisa.gov/sites/default/files/publications/MAR-10301706-1.v1.WHITE.stix.xml

| N° | Nom des fichiers lies aux activités malveillantes de FASTCash | Signature unique (SHA-256) par ligne |
|---|---|---|
| **01** | FASTCash 2.0: North Korea's BeagleBoyz Robbing Banks | f12db45c32bda3108adb8ae7363c342fdd5f10342945b115d830701f95c54fa9<br>a1f06d69bd6379e310b10a364d689f21499953fa1118ec699a25072779de5d9b<br>0e3552c8232e007f421f241ea4188ea941f4d34eab311a5c2341488749d892c7<br>d48b211533f37e082a907d4ee3b0364e5a363f1da14f74a81b187e1ce19945a8<br>f9d29b21bb93004cea6431e79f7aa24b9cc419289ca04c0353d9e3db3c587930<br>16251b20e449d46e2b431c3aed229cd1f43f1ff18db67cc5a7fa7dd19673a9bc<br>d928b1c1096e636463afbd19f40a6b325e159196b4497895748c31535ea503dc |
| **02** | North Korean Remote Access Tool: ECCENTRICBANDWAGON | efd470cfa90b918e5d558e5c8c3821343af06eedfd484dfeb20c4605f9bdc30e<br>32a4de070ca005d35a885037171570b0dc3f2e8da76ffd618fca6563aec9c81f8<br>c6930e298bba86c01d0fe2c8262c46b4fce97c6c5037a193904cfc634246fbec<br>9ea5aa00e0a738b74066c61b1d35331170a9e0a84df1cc6cef58fd46a8ec5a2e |
| **03** | North Korean Remote Access Tool: VIVACIOUSGIFT | a917c1cc198cf36c0f2f6c24652e5c2e94e28d963b128d54f00144d216b2d118<br>aca598e2c619424077ef8043cb4284729045d296ce95414c83ed70985c892c83<br>f3ca8f15ca582dd486bd78fd57c2f4d7b958163542561606bebd250c827022de<br>9a776b895e93926e2a758c09e341accb9333edc1243d216a5e53f47c6043c852<br>70b494b0a8fdf054926829dcb3235fc7bd0346b6a19faf2a57891c71043b3b38<br>8cad61422d032119219f465331308c5a61e21c9a3a431b88e1f8b25129b7e2a1 |
| **04** | North Korean Remote Access Tool: FASTCASH for Windows | 129b8825eaf61dcc2321aad7b84632233fa4bbc7e24bdf123b507157353930f0<br>39cbad3b2aac6298537a85f0463453d54ab2660c913f4f35ba98fffeb0b15655<br>5cb7a352535b447609849e20aec18c84d8b58e377d9c6365eafb45cdb7ef949b |
| **05** | North Korean Remote Access Trojan: BLINDINGCAN | 586d012540ed1244572906e3733a0cb4bba90a320da82f853e5dfac82c5c663e<br>158ddb85611b4784b6f5ca7181936b86eb0ec9a3c67562b1d57badd7b7ec2d17<br>7933716892e0d6053057f5f2df0ccadf5b06dc739fea79ee533dd0cec98ca971<br>6a3446b8a47f0ab4f536015218b22653fff8b18c595fbc5b0c09d857eba7c7a1<br>d40ad4cd39350d718e189adf45703eb3a3935a7cf8062c20c663bc14d28f78c9<br>b70e66d387e42f5f04b69b9eb15306036702ab8a50b16f5403289b5388292db9<br>bdfd16dc53f5c63da0b68df71c6e61bad300e59fd5748991a6b6a3650f01f9a1<br>7d507281e2e21476ff1af492ad9f574b14cbf77eb4cda9b67e4256318c7c6bbd<br>0fc12e03ee93d19003b2dd7117a66a3da03bd6177ac6eb396ed52a40be913db6<br>d5186efd8502a3a99a66729cb847d3f4be8937a3fec1c2655b6ea81f57a314f5<br>58027c80c6502327863ddca28c31d352e5707f5903340b9e6ccc0997fcb9631d<br>8b53b519623b56ab746fdaf14d3eb402e6fa515cde2113a07f5a3b4050e98050 |
| **06** | North Korean Remote Access Tool: COPPERHEDGE | D8AF45210BF931BC5B03215ED30FB731E067E91F25EDA02A404BD55169E3E3C3<br>7985AF0A87780D27DC52C4F73C38DE44E5AD477CB78B2E8E89708168FBC4A882<br>E98991CDD9DDD30ADF490673C67A4F8241993F26810DA09B52D8748C6160A292<br>4838F85499E3C68415010D4F19E83E2C9E3F2302290138ABE79C380754F97324<br>E76B3FD3E906AC23218B1FBD66FD29C3945EE209A29E9462BBC46B07D1645DE2<br>1FAAA939087C3479441D9F9C83A80AC7EC9B929E626CB34A7417BE9FF0316FF7<br>3FF4EBAE6C255D4AE6B747A77F2821F2B619825C7789C7EE5338DA5ECB375395<br>C2F150DBE9A8EFB72DC46416CA29ACDBAE6FD4A2AF16B27F153EAABD4772A2A1<br>1678327C5F36074CF5F18D1A92C2D9FEA9BFAE6C245EAAD01640FD75AF4D6C11<br>C0EE19D7545F98FCD15725A3D9F0DBD0F35B2091E1C5B9CF4744F16E81A030C5 |

| | | |
|---|---|---|
| | | 9E4BD9676BB3460BE68BA4559A824940A393BDE7613850EDA9196259E453B9F3<br>EEE38C632C62CA95B5C66F8D39A18E23B9175845560AF84B6A2F69B7F9B6EC1C<br>F6E1A146543D2903146698DA5698B2A214201720C0BE756C6E8D2A2F27DCFAFF<br>37BB27F4EB40B8947E184AFDDBA019001C12F97588E7F596AB6BC07F7C152602<br>E6FC788B5FF7436DA4450191A003966A68E2A1913C83F1D3AEC78C65F3BA85CA<br>284BC471647F951C79E3E333B2B19AA37F84CC39B55441A82E2A5F7319131FAC<br>A1CDB784100906D0AC895297C5A0959AB21A9FB39C687BAF176324EE84095472<br>B4BF6322C67A23553D5A9AF6FCD9510EB613FFAC963A21E32A9CED83132A09BA<br>134B082B418129FFA390FBEE1568BD9510C54BFDD0E6B1F36BC7B8F867E56283<br>0A763DA26A67CB2B09A3AE6E1AC07828065EB980E452CE7D3354347976038E7E<br>1884DDC53EF66488CA8FC641B438895FCAADA77C15210118465377C63223B3BC<br>C24C322F4535DEF3F8D1579C39F2F9E323787D15B96E2EE457C38925EFFE2D39 |
| **06** | North Korean Trojan: TAINTEDSCRIBE | 106d915db61436b1a686b86980d4af16227776fc2048f2888995326db0541438<br>2057c0cf4617eab7c91b99975dfb1e259609c4fa512e9e08a311a9a2eb65a6cf<br>19f9a9f7a0c3e6ca72ea88c655b6500f7da203d46f38076e6e8de0d644a86e35 |
| **07** | North Korean Trojan: PEBBLEDASH | aab2868a6ebc6bdee5bd12104191db9fc1950b30bcf96eab99801624651e77b6 |
| **08** | North Korean Trojan: BISTROMATH | 04d70bb249206a006f83db39bbe49ff6e520ea329e5fbb9c758d426b1c8dec30<br>1ea6b3e99bbb67719c56ad07f5a12501855068a4a866f92db8dcdefaffa48a39<br>618a67048d0a9217317c1d1790ad5f6b044eaa58a433bd46ec2fb9f9ff563dc6<br>738ba44188a93de6b5ca7e0bf0a77f66f677a0dda2b2e9ef4b91b1c8257da790<br>b6811b42023524e691b517d19d0321f890f91f35ebbdf1c12cbb92cda5b6de32<br>133820ebac6e005737d5bb97a5db549490a9f210f4e95098bc9b0a7748f52d1f<br>43193c4efa8689ff6de3fb18e30607bb941b43abb21e8cee0cfd664c6f4ad97c |
| **09** | North Korean Trojan: SLICKSHOES | fdb87add07d3459c43cfa88744656f6c00effa6b7ec92cb7c8b911d233aeb4ac |
| **10** | North Korean Trojan: CROWDEDFLOUNDER | a2a77cefd2faa17e18843d74a8ad155a061a13da9bd548ded6437ef855c14442 |
| **11** | North Korean Trojan: HOTCROISSANT | 8ee7da59f68c691c9eca1ac70ff03155ed07808c7a66dee49886b51a59e00085 |
| **12** | North Korean Trojan: BUFFETLINE | 52f83cdaefd194fff3d387631d5693a709cd7b3a20a072e7827c4d4218d57695 |
| **13** | North Korean Trojan: HOPLIGHT | 05feed9762bc46b47a7dc5c469add9f163c16df4ddaafe81983a628da5714461<br>0608e411348905145a267a9beaf5cd3527f11f95c4afde4c45998f066f418571<br>084b21bc32ee19af98f85aee8204a148032ce7eabef668481b919195dd62b319<br>12480585e08855109c5972e85d99cda7701fe992bc1754f1a0736f1eebcb004d<br>1a01b8a4c505db70f9e199337ce7f497b3dd42f25ad06487e29385580bca3676<br>2151c1977b4555a1761c12f151969f8e853e26c396fa1a7b74ccbaf3a48f4525<br>32ec329301aa4547b4ef4800159940feb950785f1ab68d85a14d363e0ff2bc11<br>4a74a9fd40b63218f7504f806fce71dffefc1b1d6ca4bbaadd720b6a89d47761<br>4c372df691fc699552f81c3d3937729f1dde2a2393f36c92ccc2bd2a033a0818<br>70034b33f59c6698403293cdc28676c7daa8c49031089efa6eefce41e22dccb3<br>73dcb7639c1f81d3f7c4931d32787bdf07bd98550888c4b29b1058b2d5a7ca33<br>83228075a604e955d59edc760e4c4ed16eedabfc8f6ac291cf21b4fcbcd1f70a<br>8a1d57ee05d29a730864299376b830a7e127f089e500e148d96d0868b7c5b520<br>b05aae59b3c1d024b19c88448811debef1eada2f51761a5c41e70da3db7615a9<br>b9a26a569257fbe02c10d3735587f10ee58e4281dba43474dbdef4ace8ea7101<br>c66ef8652e15b579b409170658c95d35cfd6231c7ce030b172692f911e7dcff8<br>d77fdabe17cdba62a8e728cbe6c740e2c2e541072501f77988674e07a05dfb39<br>ddea408e178f0412ae78ff5d5adf2439251f68cad4fd853ee466a3c74649642d<br>f8f7720785f7e75bd6407ac2acd63f90ab6c2907d3619162dc41a8ffa40a5d03<br>fe43bc385b30796f5e2d94dfa720903c70e66bc91dfdcfb2f3986a1fea3fe8c5<br>44a93ea6e6796530bb3cf99555dfb3b1092ed8fb4336bb198ca15b2a21d32980<br>49757cf85657757704656c079785c072bbc233cab942418d99d1f63d43f28359<br>70902623c9cd0cccc8513850072b70732d02c266c7b7e96d2d5b2ed4f5edc289<br>823d255d3dc8cbc402527072a9220e4c38655de1a3e55a465db28b55d3ac1bf8<br>96a296d224f285c67bee93c30f8a309157f0daa35dc5b87e410b78630a09cfc7<br>ba80cb0a08908782f4b6e88aa15e2d306b19bc93e79bd8770bf8be904fd1bd09<br>cd5ff67ff773cc60c98c35f9e9d514b597cbd148789547ba152ba67bfc0fec8f |
| **14** | North Korean Proxy Malware: ELECTRICFISH | 7cf5d86cc75cd8f0e22e35213a9c051b740bd4667d9879a446f06277782bffd1<br>a1260fd3e9221d1bc5b9ece6e7a5a98669c79e124453f2ac58625085759ed3bb |
| **15** | North Korean Trojan: BADCALL | 4257bb11570ed15b8a15aa3fc051a580eab5d09c2f9d79e4b264b752c8e584fc<br>93e13ffd2a2f1a13fb9a09de1d98324f75b3f0f8e0c822857ed5ca3b73ee3672 |

| | | |
|---|---|---|
| | | d1f3b9372a6be9c02430b6e4526202974179a674ce94fe22028d7212ae6be9e7<br>edd2aff8fad0c76021adc74fe3cb3cb1a02913a839ad0f2cf31fdea8b5aa8195<br>91650e7b0833a34abc9e51bff53cc05ef333513c6be038df29929a0a55310d9c<br>da353b2845a354e1a3f671e4a12198e2c6f57a377d02dfaf90477869041a044f |
| **16** | HIDDEN COBRA FASTCash-Related Malware | 10ac312c8dd02e417dd24d53c99525c29d74dcbc84730351ad7a4e0a4b1a0eba<br>1f2cd2bc23556fb84a51467fedb89cbde7a5883f49e3cfd75a241a6f08a42d6d<br>3a5ba44f140821849de2d82d5a137c3bb5a736130dddb86b296d94e6b421594c<br>4a740227eeb82c20286d9c112ef95f0c1380d0e90ffb39fc75c8456db4f60756<br>820ca1903a30516263d630c7c08f2b95f7b65dffceb21129c51c9e21cf9551c6<br>9ddacbcd0700dc4b9babcd09ac1cebe23a0035099cb612e6c85ff4dffd087a26<br>a9bc09a17d55fc790568ac864e3885434a43c33834551e027adb1896a463aafc<br>ab88f12f0a30b4601dc26dbae57646efb77d5c6382fb25522c529437e5428629<br>ca9ab48d293cc84092e8db8f0ca99cb155b30c61d32a1da7cd3687de454fe86c<br>d465637518024262c063f4a82d799a4e40ff3381014972f24ea18bc23c3b27ee<br>e03dc5f1447f243cf1f305c58d95000ef4e7dbcc5c4e91154daa5acd83fea9a8<br>f3e521996c85c0cdb2bfb3a0fd91eb03e25ba6feef2ba3a1da844f1b17278dd2 |
| **17** | North Korean Trojan: KEYMARBLE | e23900b00ffd67cd8dfa3283d9ced691566df6d63d1d46c95b22569b49011f09 |
| **18** | North Korean Trojan: TYPEFRAME | 201c7cd10a2bd50dde0948d14c3c7a0732955c908a3392aee3d08b94470c9d33<br>20abb95114de946da7595438e9edf0bf39c85ba8512709db7d5532d37d73bd64<br>3c809a10106990ba93ec0ed3b63ec8558414c6680f6187066b1aacd4d8c58210<br>40ef57ca2a617f5d24ac624339ba2027b6cf301c28684bf8b2075fc7a2e95116<br>4bd7d801d7ce3fe9c2928dbc834b296e934473f5bbcc9a1fd18af5ebd43192cd<br>546dbd370a40c8e46f9b599a414f25000eec5ae6b3e046a035fe6e6cd5d874e1<br>675a35e04b19aab314bcbc4b1f2610e3dea4a80c277cc5188f1d1391a00dfdb1<br>8c3e0204f52200325ed36db9b12aba1c5e46984d415514538a5bf10783cacdf8<br>c9e3b83d77ce93cc1d70b22e967f049b13515c88572aa78e0a838103e5478777<br>d1d490866d4a4d29306f0d9300bffc1450c41bb8fd62371d29672bf9f747bf92<br>e69d6c2d3e9c4beebee7f3a4a3892e5fdc601beda7c3ec735f0dfba2b29418a7<br>089e49de61701004a5eff6de65476ed9c7632b6020c2c0f38bb5761bca897359<br>a71017302e1745c8a3d6e425187eb23c7531551bb6f547e47198563a78e933b6<br>e088c3a0b0f466df5329d9a66ff618de3d468d8a5981715303babb1452631eef |
| **19** | Joanap Backdoor Trojan and Brambul Server Message Block Worm | a1c483b0ee740291b91b11e18dd05f0a460127acfc19d47b446d11cd0e26d717<br>fe7d35d19af5f5ae2939457a06868754b8bdd022e1ff5bdbe4e7c135c48f9a16<br>077d9e0e12357d27f7f0c336239e961a7049971446f7a3f10268d9439ef67885<br>ea46ed5aed900cd9f01156a1cd446cbb3e10191f9f980e9f710ea1c20440c781<br>077d9e0e12357d27f7f0c336239e961a7049971446f7a3f10268d9439ef67885 |
| **20** | HIDDEN COBRA RAT/Worm | 077d9e0e12357d27f7f0c336239e961a7049971446f7a3f10268d9439ef67885<br>a1c483b0ee740291b91b11e18dd05f0a460127acfc19d47b446d11cd0e26d717<br>ea46ed5aed900cd9f01156a1cd446cbb3e10191f9f980e9f710ea1c20440c781<br>fe7d35d19af5f5ae2939457a06868754b8bdd022e1ff5bdbe4e7c135c48f9a16 |
| **21** | North Korean Trojan – HARDRAIN | ca057fd197fc99cfb60b7379cb64475e6bd206fdd4b019f1f70c2214115f3b83 |
| **22** | North Korean Trojan: BANKSHOT | 780a9da4b933d0eb457f71666a72f596163b6ef22756e760a7e222e920d0cf4b |
| **23** | North Korean Remote Administration Tool: FALLCHILL | a6067163550354d4a1ea0b15f3bee30aad41a2c32df28c2d468eafd18361d60d6<br>20abb95114de946da7595438e9edf0bf39c85ba8512709db7d5532d37d73bd64<br>0a118eb23399000d148186b9079fa59caf4c3faa7e7a8f91533e467ac9b6ff41 |
| **24** | North Korean Trojan: Volgmer | 9f177a6fb4ea5af876ef8a0bf954e37544917d9aaba04680a29303f24ca5c72c<br>e40a46e95ef792cf20d5c14a9ad0b3a95c6252f96654f392b4bc6180565b7b11<br>53e9bca505652ef23477e105e6985102a45d9a14e5316d140752df6f3ef43d2d<br>8fcd303e22b84d7d61768d4efa5308577a09cc45697f7f54be4e528bbb39435b<br>fee0081df5ca6a21953f3a633f2f64b7c0701977623d3a4ec36fff282ffe73b9<br>ff2eb800ff16745fc13c216ff6d5cc2de99466244393f67ab6ea6f8189ae01dd<br>eff3e37d0406c818e3430068d90e7ed2f594faa6bb146ab0a1c00a2f4a4809a5<br>6dae368eecbcc10266bba32776c40d9ffa5b50d7f6199a9b6c31d40dfe7877d1<br>1d0999ba3217cbdb0cc85403ef75587f747556a97dee7c2616e28866db932a0d<br>0281b2d1950a578aa41d1b2ec39abe09b9992e0846f5a503ce031f3f4f5e3c96<br>e79bbb45421320be05211a94ed507430cc9f6cf80d607d61a317af255733fcf2 |
| **25** | Analysis of Delta Charlie Attack Malware | 29a4ff6c133d433334d3a1762b6b7700ddcdcd02f63240d373689ae149ff90c3<br>aff73144a359020abbb4bde3f80858d822b840dd7171ba7946b77ba9b3487831 |
| **26** | North Korea's DDoS Botnet Infrastructure | 824d8b03e061ddd0d33ef9f03c669b13e7b6e339684009bd44d69178c45e2de1<br>60d82d0534c4cb8e1fe95e17e2dbdc3c02463723f1920e39c3ab3922d9cca866 |

| | | |
|---|---|---|
| **27** | Indicators Associated With WannaCry Ransomware | 4186675cb6706f9d51167fb0f14cd3f8fcfb0065093f62b10a15f7d9a6c8d982<br>c365ddaa345cfcaff3d629505572a484cff5221933d68e4a52130b8bb7badaf9<br>aee20f9188a5c3954623583c6b0e6623ec90d5cd3fdec4e1001646e27664002c<br>d5e0e8694ddc0548d8e6b87c83d50f4ab85c1debadb106d6a6a794c3e746f4fa<br>055c7760512c98c8d51e4427227fe2a7ea3b34ee63178fe78631fa8aa6d15622<br>97ebce49b14c46bebc9ec2448d00e1e397123b256e2be9eba5140688e7bc0ae6<br>40b37e7b80cf678d7dd302aaf41b88135ade6ddf44d89bdba19cf171564444bd<br>845d0e178aeebd6c7e2a2e9697b2bf6cf02028c50c288b3ba88fe2918ea2834a<br>5c7f6ad1ec4bc2c8e2c9c126633215daba7de731ac8b12be10ca157417c97f3a<br>3f33734b2d34cce83936ce99c3494cd845f1d2c02d7f6da31d42dfc1ca15a171<br>5afa4753afa048c6d6c39327ce674f27f5f6e5d3f2a060b7a8aed61725481150<br>a75bb44284b9db8d702692f84909a7e23f21141866adf3db888042e9109a1cb6<br>2c95bef914da6c50d7bdedec601e589fbb4fda24c4863a7260f4f72bd025799c<br>26fd072fda6e12f8c2d3292086ef0390785efa2c556e2a88bd4673102af703e5<br>d8489f8c16318e524b45de8b35d7e2c3cd8ed4821c136f12f5ef3c9fc3321324<br>1adfee058b98206cb4fbe1a46d3ed62a11e1dee2c7ff521c1eef7c706e6a700e<br>9bd38110e6523547aed50617ddc77d0920d408faeed2b7a21ab163fda22177bc<br>2adc900fafa9938d85ce53cb793271f37af40cf499bcc454f44975db533f0b61<br>e13cc9b13aa5074dc45d50379eceb17ee39a0c2531ab617d93800fe236758ca9<br>23e5e738aad10fb8ef89aa0285269aff728070080158fd3e7792fe9ed47c51f4<br>49f2c739e7d9745c0834dc817a71bf6676ccc24a4c28dcddf8844093aab3df07<br>7e491e7b48d6e34f916624c1cda9f024e86fcbec56acda35e27fa99d530d017e<br>552aa0f82f37c9601114974228d4fc54f7434fe3ae7a276ef1ae98a0f608f1d0<br>a0356696877f2d94d645ae2df6ce6b370bd5c0d6db3d36def44e714525de0536<br>cb5da96b3dfcf4394713623dbf3831b2a0b8be63987f563e1c32edeb74cb6c3a<br>519ad66009a6c127400c6c09e079903223bd82ecc18ad71b8e5cd79f5f9c053e<br>bd9f4b3aedf4f81f37ec0a028aabcb0e9a900e6b4de04e9271c8db81432e2a66<br>70c0f32ed379ae899e5ac975e20bbbacd295cf7cd50c36174d2602420c770ac1<br>02932052fafe97e6acaaf9f391738a3a826f5434b1a013abbfa7a6c1ade1e078<br>e64178e339c8e10eac17a236a67b892d0447eb67b1dcd149763dad6fd9f72729<br>72f20024b2f69b45a1391f0a6474e9f6349625ce329f5444aec7401fe31f8de1<br>146f61db72297c9c0facffd560487f8d6a2846ecec92ecc7db19c8d618dbc3a4<br>6db650836d64350bbde2ab324407b8e474fc041098c41ecac6fd77d632a36415<br>1f21838b244c80f8bed6f6977aa8a557b419cf22ba35b1fd4bf0f98989c5bdf8<br>402751fa49e0cb68fe052cb3db87b05e71c1d950984d339940cf6b29409f2a7c<br>4a468603fdcb7a2eb5770705898cf9ef37aade532a7964642ecd705a74794b79<br>2ca2d550e603d74dedda03156023135b38da3630cb014e3d00b1263358c5f00d<br>8b621c723619ac94f007a2809aeb6a0cf18e612c262f4ca3865445804f0470e3<br>389898c3dc62496f40760d988a930db34453e30a530c9a71ec7ad371a39025af<br>91062a4cc90a5edff95afbea94c1639dae3d044878c321b9ef11ee68b64b6a3d<br>b9c5d4339809e0ad9a00d4d3dd26fdf44a32819a54abf846bb9b560d81391c25<br>770df42900bd0a061d15c2b599cd4e171812bd9f12277f3d632ebbd0ad8edf5a<br>4186675cb6706f9d51167fb0f14cd3f8fcfb0065093f62b10a15f7d9a6c8d982<br>c365ddaa345cfcaff3d629505572a484cff5221933d68e4a52130b8bb7badaf9<br>aee20f9188a5c3954623583c6b0e6623ec90d5cd3fdec4e1001646e27664002c<br>d5e0e8694ddc0548d8e6b87c83d50f4ab85c1debadb106d6a6a794c3e746f4fa |

# 6 Comment savoir si vous êtes infecté ?

Les actions de détection de ce malware sont les suivantes :

1. Incorporer les IOCs identifiés dans vos systèmes de détection d'intrusion (IDS / IPS) pour détecter la présence de toute activité liée au FASTCash 2.0.
2. Vérifiez auprès de votre éditeur d'Anti-Virus, sa capacité à détecter FASTCash 2.0, mettre à jour votre système antivirus et lancer un scan complet du réseau.
3. Utiliser votre système de journalisation (SIEM) pour identifier toute activités liées aux IOCs identifiés.
4. Charger votre solution SIEM avec la liste des IOCs pour surveiller et détecter activement toutes activités liées à ce malware.

# 7 Que faire si vous êtes infecté ?

Contacter immédiatement le CERT TG ou Cyber Defense Africa S.A.S concernant toutes activités identifiées liées à FASTCash.

**Cyber Defense Africa S.A.S.**
Rue Abdoulaye Fadiga,
07 BP 13215, Lomé, Togo
csirt@cda.tg
(+228) 22 53 59 80
(+228) 70 54 93 24
(+228) 70 54 93 25
www.cda.tg

# 8 Recommandations générales

Les utilisateurs et les administrateurs doivent utiliser les meilleures pratiques suivantes pour renforcer la sécurité des systèmes de votre organisation :

- Maintenir à jour les signatures et les moteurs antivirus.
- Garder les correctifs du système d'exploitation à jour.
- Désactiver les services de partage de fichiers et d'imprimantes. Si ces services sont requis, utiliser des mots de passe forts ou une authentification Active Directory.
- Restreindre la capacité (autorisations) des utilisateurs à installer et exécuter des applications logicielles indésirables. N'ajoutez pas d'utilisateurs au groupe des administrateurs locaux. Si des exceptions sont requises, elles doivent être surveillés de près.
- Appliquer une politique de mot de passe fort et exiger des changements de mot de passe réguliers.
- Être prudent lorsque vous ouvrez des pièces jointes à un e-mail, même si la pièce jointe est attendue et que l'expéditeur semble connu.
- Activer un pare-feu personnel sur les postes de travail de l'agence et configurez-le pour refuser les demandes de connexion non sollicitées.
- Désactiver les services inutiles sur les postes de travail et les serveurs des agences.
- Rechercher et supprimer les pièces jointes suspectes ; assurez-vous avant d'ouvrir que la pièce jointe et son type correspondent (c'est-à-dire que l'extension correspond à l'en-tête du fichier).
- Surveiller les habitudes de navigation Web des utilisateurs ; restreindre l'accès aux sites dont le contenu est défavorable.
- Être prudent lorsque vous utilisez des supports amovibles (par exemple, clés USB, lecteurs externes, CD).
- Scanner tous les logiciels téléchargés sur Internet avant de les exécuter.
- Garder une conscience situationnelle des dernières menaces.
- Mettre en place des listes de contrôle d'accès appropriées.
- Surveiller activement votre système d'information avec un SIEM

# 9 Recommandations pour les institutions dotées de systèmes de paiement marchants

Les utilisateurs et les administrateurs doivent utiliser les meilleures pratiques suivantes pour renforcer la sécurité des systèmes de votre organisation :

1. Mettre en œuvre les exigences de la norme PCI DSS
2. Valider le cryptogramme de la puce et du numéro d'identification personnel (PIN) :

    - Mettre en œuvre les exigences en matière de puce et de code PIN pour les cartes de débit.

    - Valider les cryptogrammes de demande d'autorisation générés par la carte.

    - Utiliser les cryptogrammes de réponse d'autorisation générés par l'émetteur pour les messages de réponse.

    - Exiger la validation du cryptogramme de réponse d'autorisation générée par carte pour vérifier les messages de réponse légitimes.

    - Vérifier que les contrôles de sécurité du périmètre empêchent les hôtes Internet d'accéder à l'infrastructure du réseau privé desservant votre serveur d'applications de commutation de paiement.

3. Isoler l'infrastructure du système de paiement

    - Exiger une authentification multi facteur pour tout utilisateur pour accéder au serveur d'applications du commutateur.

    - Confirmer que les contrôles de sécurité du périmètre empêchent tous les hôtes en dehors des points de terminaison autorisés d'accéder à votre système, en particulier si votre serveur d'applications de commutation de paiement est accessible sur Internet.

4. Ségréguer logiquement votre environnement d'exploitation

    - Utiliser des pares-feux pour diviser votre environnement d'exploitation en enclaves ;

    - Utiliser des listes de contrôle d'accès pour autoriser / empêcher un trafic spécifique de circuler entre ces enclaves ;

    - Accorder une attention particulière à la séparation des enclaves contenant des informations sensibles (par exemple, les systèmes de gestion de cartes) des enclaves nécessitant une connectivité Internet (par exemple, le courrier électronique).

5. Chiffrer les données en transit

   - Sécuriser tous les liens vers les moteurs du système de paiement avec un mécanisme basé sur des certificats, tel que Mutual Transport Layer Security, pour tout le trafic externe et interne externe ;

   - Limiter le nombre de certificats pouvant être utilisés sur le serveur de production et limiter l'accès à ces certificats.

6. Surveiller les comportements anormaux dans le cadre de la mise en place de la défense en profondeur (defense in depth)

   - Configurer le serveur d'applications du commutateur pour consigner les transactions et auditer régulièrement les transactions et les journaux système ;

   - Développer une base de référence des logiciels, des utilisateurs et des ouvertures de session attendus et surveillez les serveurs d'applications de commutation pour les installations logicielles inhabituelles, les mises à jour, les changements de compte ou d'autres activités en dehors du comportement attendu ;

   - Élaborer une base de référence des participants à la transaction attendus, des montants, de la fréquence et du calendrier Surveiller et signaler les transactions anormales pour une activité frauduleuse suspectée.

# 10 Recommandations pour les organisations dotées de GAB ou d'appareils de point de vente

Valider les réponses des émetteurs aux messages de demande financière :

- Mettre en œuvre les exigences de la norme PCI DSS
- Mettre en œuvre les exigences en matière de puce et de code PIN pour les cartes de débit.
- Exiger et vérifier les codes d'authentification des messages sur les messages de réponse aux demandes financières de l'émetteur.
- Effectuer la validation du cryptogramme de réponse d'autorisation pour les transactions par puce et PIN.

# 11 Références

| Référence | URL |
|---|---|
| CERT US | https://us-cert.cisa.gov/ncas/alerts/aa20-239a |
| CERT US | https://us-cert.cisa.gov/ncas/analysis-reports/ar20-239a |