POLICE NATIONALE

DIVISION DE L'ANTICIPATION ET DE L'ANALYSE

ALERTE

11 avril 2017

Direction Centrale de Police Judiciaire
Sous-Direction de la lutte contre la cybercriminalité

1. Résumé exécutif

Le cheval de Troie Dridex est opéré par des groupes de criminalité organisée russes spécialisés dans l'interception et le détournement des communications de banque en ligne. Ce code malveillant était très actif jusqu'à en 2014 et en 2015, causant de forts dommages financiers à ses victimes (plusieurs dizaines ou centaines de milliers de dollars par victime). Les campagnes d'infection de Dridex se sont taries après plusieurs actions de disruption par les forces de l'ordre fin 2015, mais les groupes organisés opérant Dridex n'ont pas été mis hors d'état de nuire.

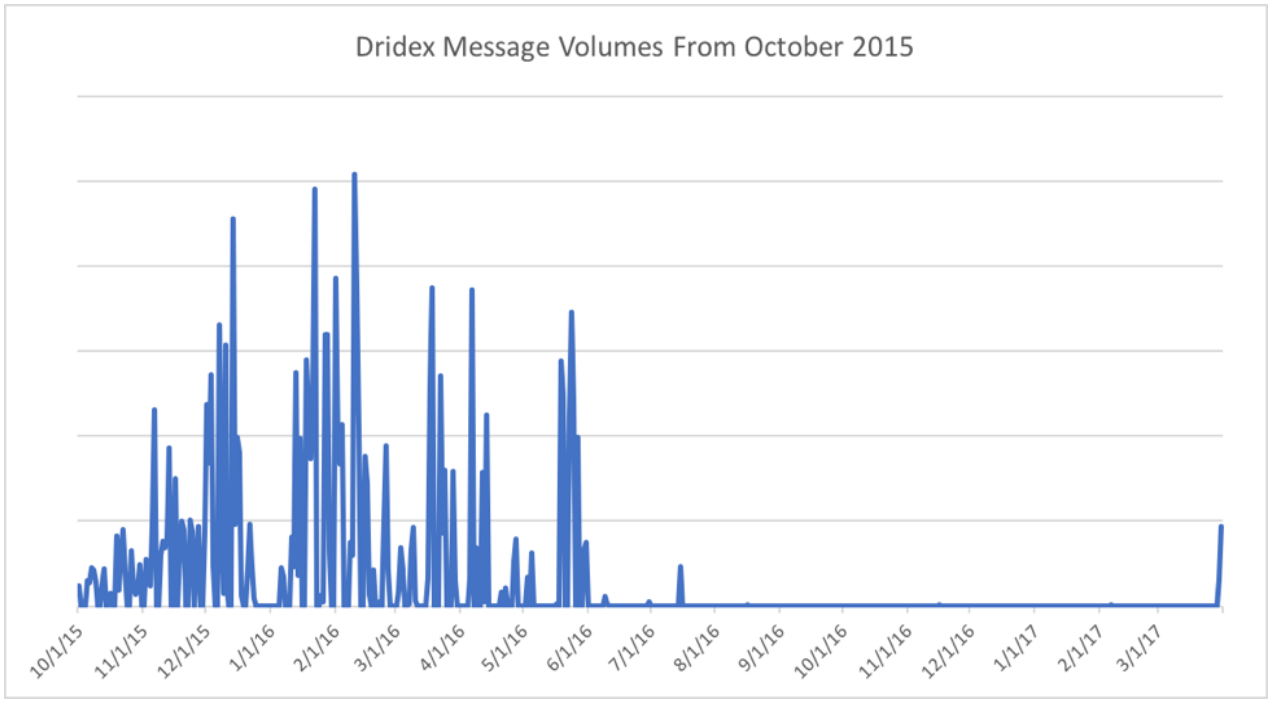
Le début de l'année 2017 a été marqué par la réapparition de Dridex. Une nouvelle version de ce code malveillant est apparue en février 2017 (version 4), introduisant de nouvelles techniques d'installation et de persistance. De courtes campagnes d'infection ont été observées, ciblant le Royaume-Uni, probablement à des fins de test. A partir de fin mars, les campagnes de spam visant à faire installer Dridex se sont intensifiées. Ces campagnes de spam ciblent pour l'instant toujours principalement des entreprises du Royaume-Uni, mais des fichiers de configuration interceptés indiquent que les banques australiennes sont également ciblées, ainsi que certaines cibles françaises non identifiées. La campagne de spam la plus récente exploite une faille 0-jour découverte dans Microsoft Office.

Ce regain d'activité signale les prémices de futures campagnes d'infections plus importantes et qui vont s'étende à d'autres pays.

2. Présentation de Dridex et des groupes opérant Dridex

Dridex est un code malveillant permettant de prendre le contrôle du PC qu'il infecte. Les fonctionnalités de ce code malveillant et les objectifs de ses opérateurs sont de détourner les communications bancaires en ligne afin d'effectuer des transferts d'argent frauduleux. Les cibles principales des groupes opérant Dridex sont les entreprises de toute taille. Lors des campagnes d'infection par Dridex en 2014/2015, le malware avait été distribué progressivement dans plusieurs pays: initialement au Royaume-Uni, suivi d'autres pays européens et d'Amérique du Nord, puis en Asie, suivie de l'Amérique du Sus, de l'Afrique et enfin de l'Australie.

Les opérateurs de Dridex sont des groupes expérimentés et très bien connectés au sein de la communauté de cybercriminalité bancaire russe. Ces groupes ont déjà causé des centaines de millions de dollars de dommages aux banques et entreprises qui en sont les victimes. Après l'action des forces de l'ordre contre Dridex en octobre 2015, les opérateurs de Dridex se sont tournés vers la distribution du ransomware Locky. Dridex continuait à être distribué en 2016, mais pour des campagnes de spam plus petites, plus occasionnelles, voir ciblées. Depuis mars 2017, les campagnes se sont faites plus fréquentes, et les dernières campagnes de spam ont ciblé des millions d'adresses email.

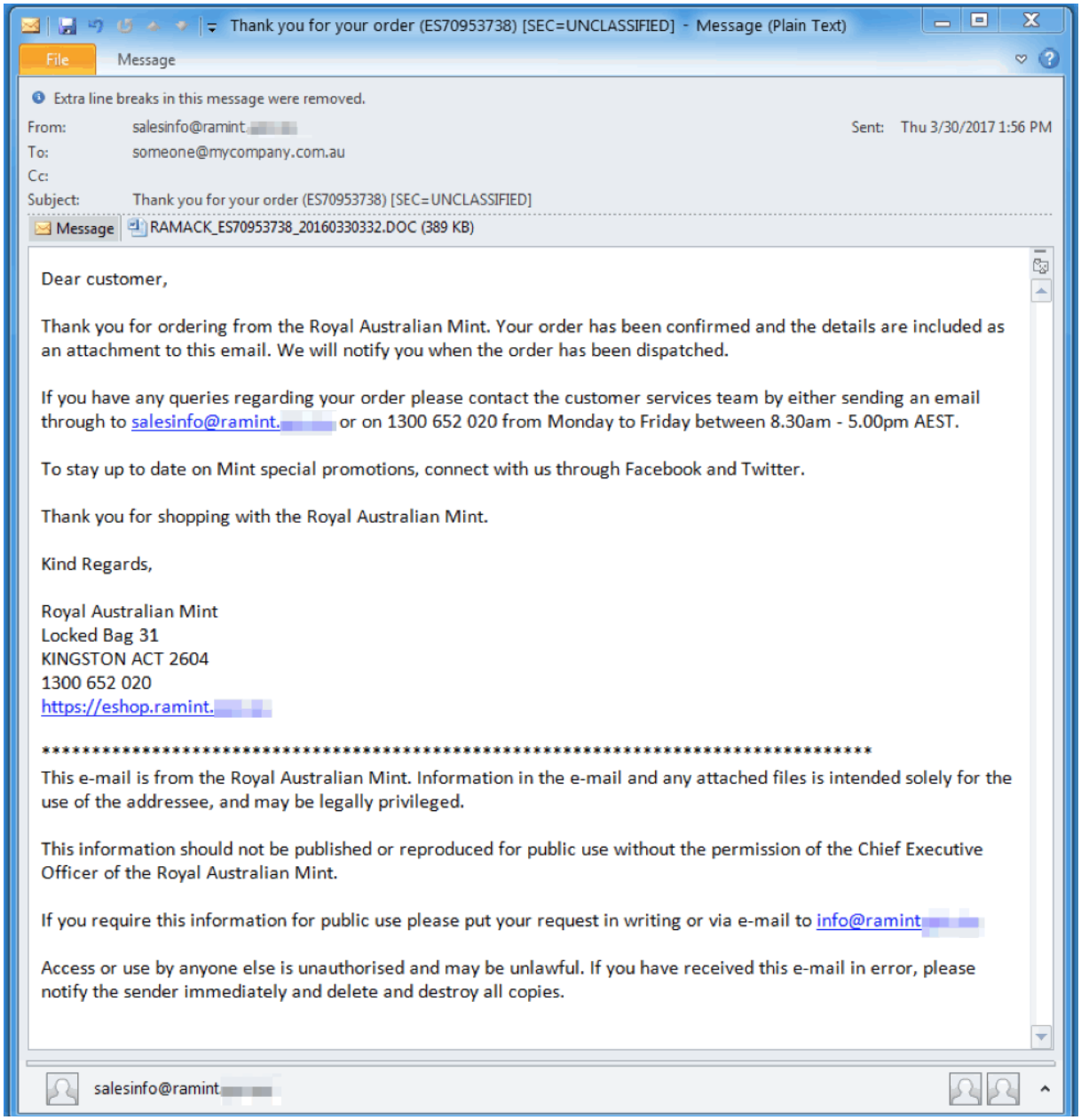


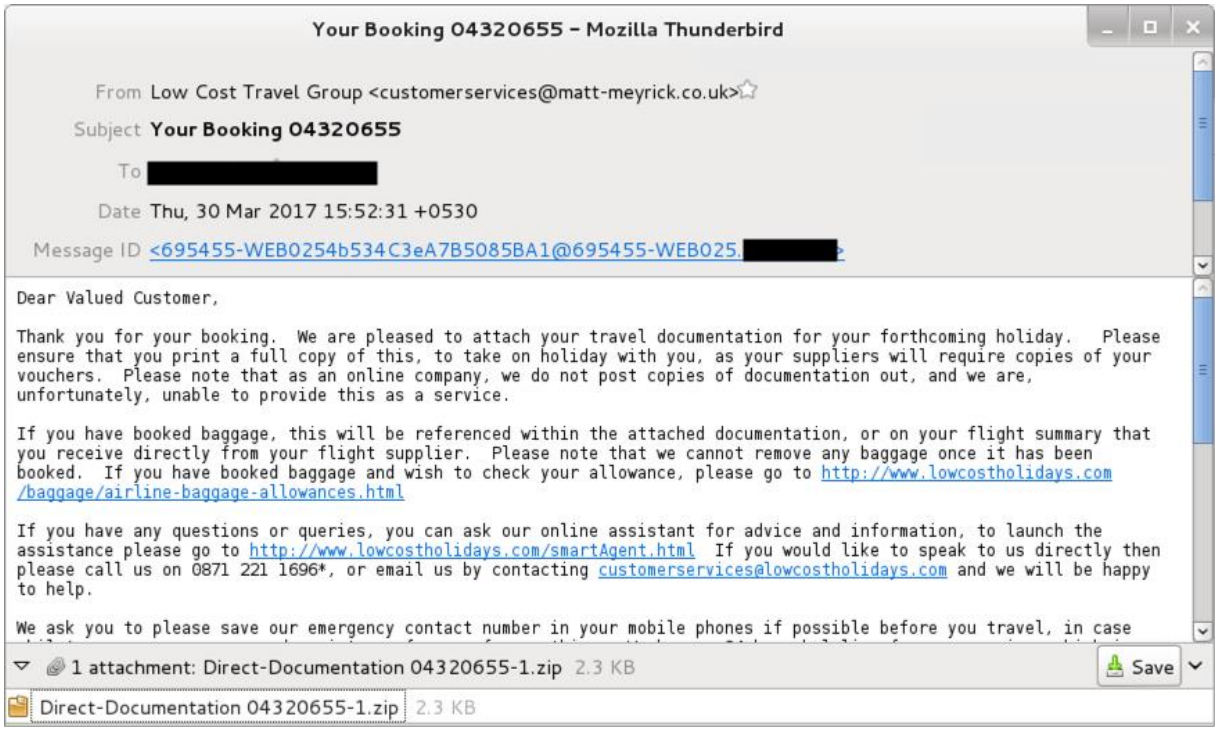
(source: Proofpoint)

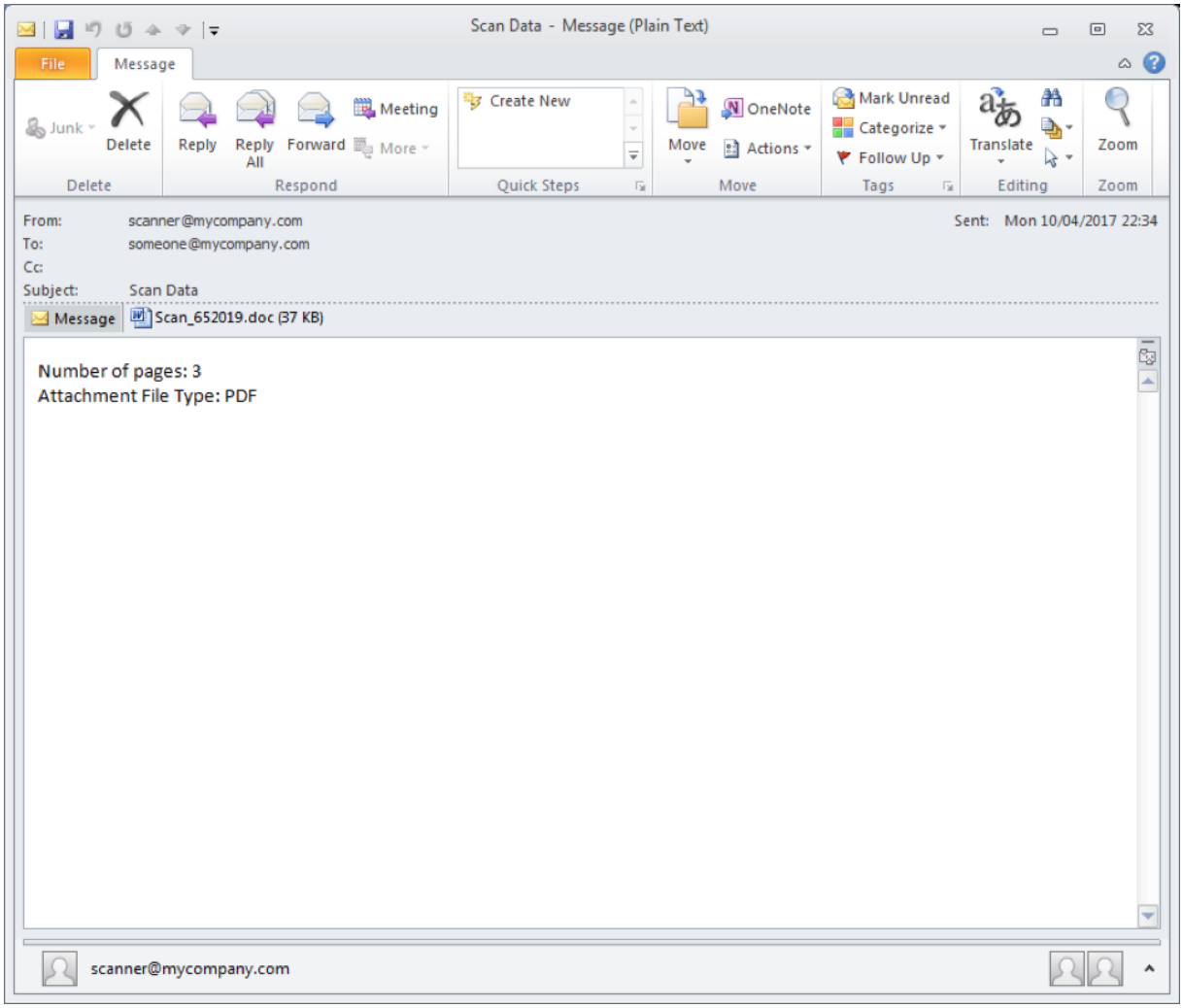
Ces groupes utilisent essentiellement des serveurs compromis afin de distribuer et de contrôler Dridex.

3. Infection par Dridex

Dridex est propagé par des campagnes de spam. Ces campagnes de spam sont très variées et ciblent un pays à la fois. Les emails usurpent des compagnies connues ou inconnues, ou des services d'envoi de scan. L'email de spam contient généralement un document malveillant. Cependant, dans le cas d'une campagne de spam ciblant des entreprises suisses en 2017, l'email incitait à télécharger un document malveillant.




Your Booking 04320655 – Mozilla Thunderbird
From Low Cost Travel Group <customerservices@matt-meyrick.co.uk>
Subject Your Booking 04320655
To [redacted]
Date Thu, 30 Mar 2017 15:52:31 +0530
Message ID <695455-WEB0254b534C3eA7B5085BA1@695455-WEB025[redacted]>
Dear Valued Customer,
Thank you for your booking. We are pleased to attach your travel documentation for your forthcoming holiday. Please ensure that you print a full copy of this, to take on holiday with you, as your suppliers will require copies of your vouchers. Please note that as an online company, we do not post copies of documentation out, and we are, unfortunately, unable to provide this as a service.
If you have booked baggage, this will be referenced within the attached documentation, or on your flight summary that you receive directly from your flight supplier. Please note that we cannot remove any baggage once it has been booked. If you have booked baggage and wish to check your allowance, please go to http://www.lowcostholidays.com /baggage/airline-baggage-allowances.html
If you have any questions or queries, you can ask our online assistant for advice and information, to launch the assistance please go to http://www.lowcostholidays.com/smartAgent.html If you would like to speak to us directly then please call us on 0871 221 1696*, or email us by contacting customerservices@lowcostholidays.com and we will be happy to help.
We ask you to please save our emergency contact number in your mobile phones if possible before you travel, in case
1 attachment: Direct-Documentation 04320655-1.zip 2.3 KB
Save
Direct-Documentation 04320655-1.zip 2.3 KB

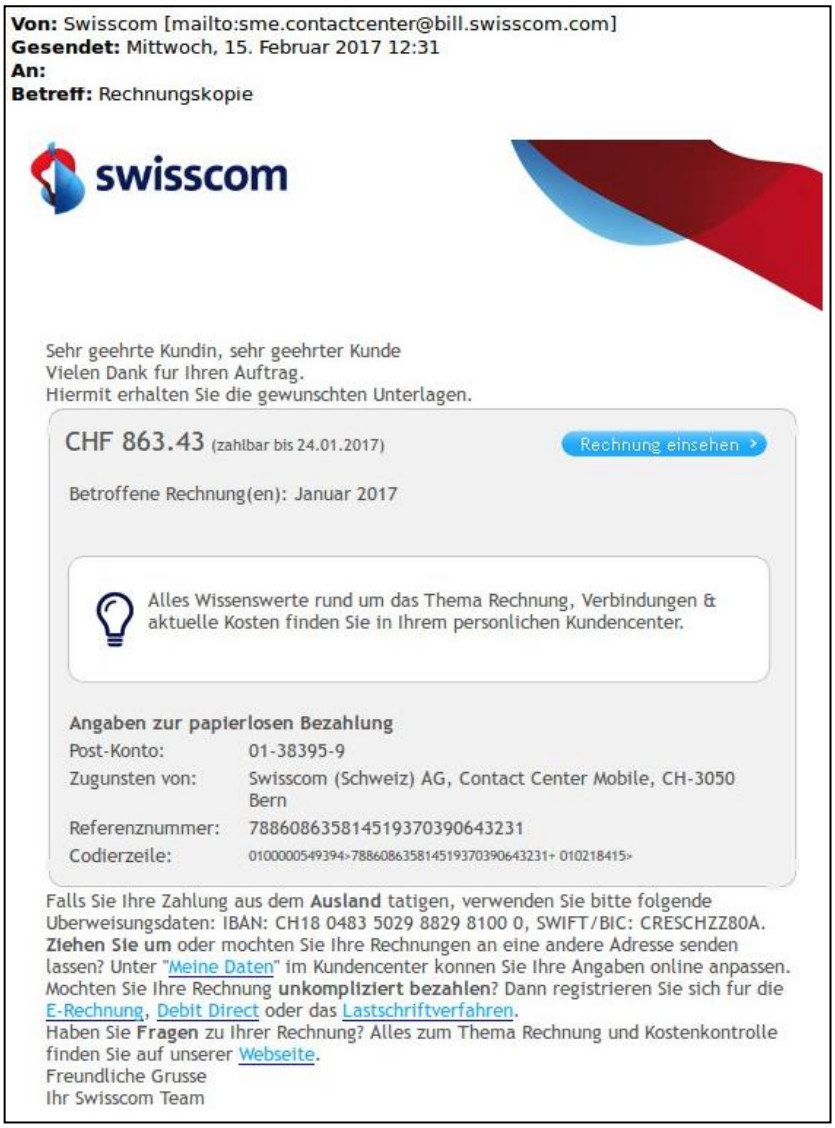


Exemples de sujets de message de spam ayant ciblé le Royaume-Uni en 2017:

- Your Booking [chiffres]
- Emailing: PIC[chiffres].JPG
- Your GB Energy Supply bill [chiffres]
- photos
- Your Telephone Bill Invoices & Reports (Client ID: (chiffres))
- copy invoice (chiffres)
- k_confirmation_ph[chiffres].pdf
- scan data
- CEF Documents
- (chiffres)_Invoice_(chiffres)
- [GameStop] Order No.(chiffres)
- Payment Request
- no reply
- thank you for your order (ES(chiffres))

Exemple de sujets de message de spam ayant ciblé la Suisse en 2017:

- Rechnungskopie



Von: Swisscom [mailto:sme.contactcenter@bill.swisscom.com]
Gesendet: Mittwoch, 15. Februar 2017 12:31
An:
Betreff: Rechnungskopie

swisscom

Sehr geehrte Kundin, sehr geehrter Kunde
Vielen Dank fur Ihren Auftrag.
Hiermit erhalten Sie die gewunschten Unterlagen.

CHF 863.43 (zahlbar bis 24.01.2017) Rechnung einsehen >

Betroffene Rechnung(en): Januar 2017

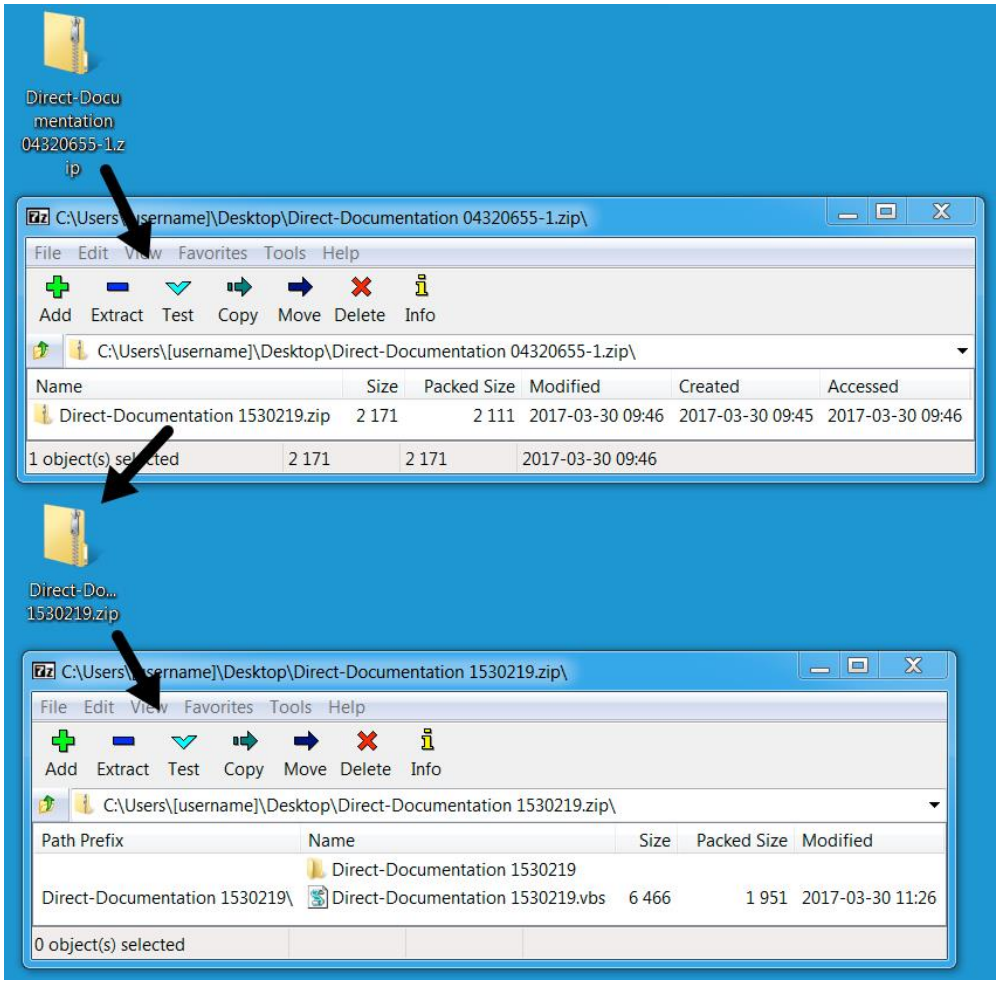
Alles Wissenswerte rund um das Thema Rechnung, Verbindungen & aktuelle Kosten finden Sie in Ihrem personlichen Kundencenter.

Angaben zur papierlosen Bezahlung

Post-Konto:	01-38395-9
Zugunsten von:	Swisscom (Schweiz) AG, Contact Center Mobile, CH-3050 Bern
Referenznummer:	788608635814519370390643231
Codierzeile:	0100000549394>788608635814519370390643231+ 010218415>

Falls Sie Ihre Zahlung aus dem **Ausland** tatigen, verwenden Sie bitte folgende Uberweisungsdaten: IBAN: CH18 0483 5029 8829 8100 0, SWIFT/BIC: CRESCHZZ80A.
Ziehen Sie um oder mochten Sie Ihre Rechnungen an eine andere Adresse senden lassen? Unter "Meine Daten" im Kundencenter konnen Sie Ihre Angaben online anpassen.
Mochten Sie Ihre Rechnung **unkompliziert bezahlen**? Dann registrieren Sie sich fur die E-Rechnung, Debit Direct oder das Lastschriftverfahren.
Haben Sie **Fragen** zu Ihrer Rechnung? Alles zum Thema Rechnung und Kostenkontrolle finden Sie auf unserer Webseite.
Freundliche Grusse
Ihr Swisscom Team

Les pièces jointes sont généralement des documents Office contenant une macro qui, si elle est exécutée, déclenche le téléchargement et l'installation de Dridex. Des fichiers ou des scripts exécutables (.exe, .js, .vbs, .hta, etc.) sont également envoyés par email. Ces fichiers malveillants sont contenus dans des archives zip ou rar, parfois eux-mêmes inclus dans une seconde archive zip. Dans quelques cas, le code malveillant QuantLoader était envoyé directement en pièce jointe, celui-ci se chargeant d'installer Dridex.



Les emails de spam peuvent avoir un champ SPF valide ou une signature DKIM valide. Dans le cas de la campagne de spam ciblant la Suisse, les emails de spam ont été envoyés via une plateforme d'envoi d'email professionnelle (SendGrid), généralement présente en liste blanche des filtres anti-spam, ou disposant d'une bonne réputation.

Enfin, la campagne de spam la plus récente (10 avril 2017, plusieurs millions d'adresses email impactées) utilisait une faille 0-jour récemment découverte dans Microsoft Office via l'envoi de fichier .rtf et ou .doc.

Une fois exécuté par la victime, la macro ou le script télécharge un fichier chiffré hébergé sur un serveur compromis. Ce fichier, qui représente le module Dridex Loader, est déchiffré par la macro ou le script et installé sur le poste infecté via l'utilisation de commandes powershell. Le Dridex Loader contacte ensuite un autre serveur compromis, afin de télécharger et d'installer un second module: le Dridex Worker.

Auparavant, le mécanisme de persistance de Dridex fonctionnait ainsi: une valeur de registre permettait de démarrer Dridex lors du démarrage du PC:

HKCU\Software\Microsoft\Windows\CurrentVersion\Run

Après démarrage, Dridex effaçait cette valeur (cette clé n'était donc détectable que si l'ordinateur démarrait en mode sans échec). Lorsque Dridex détectait l'extinction du PC, Dridex réécrivait cette valeur, assurant son redémarrage. Dans la version 4 de Dridex apparue en février 2017, ce mécanisme a été abandonné pour une méthode de DLL hijacking. Les outils de détection de Dridex qui se basent sur ce mécanisme ne sont donc plus fiables.

La version 4 de Dridex inclut également un nouveau mécanisme d'injection de code nommé Atom Bombing, probablement afin de mieux contourner les logiciels antivirus.

4. Action de Dridex et de ses opérateurs

Chaque échantillon de Dridex appartient à un botnet identifiable par un numéro. Ces botnets ciblent un pays spécifique et possèdent un fichier de configuration qui leur est propre. Ce fichier de configuration leur indique leur comportement en fonction des informations rencontrées sur le poste infecté. Le fichier de configuration est téléchargé sur un serveur de commande et contrôle (C&C). Les informations qu'il contient nous renseignent sur les cibles potentielles de Dridex.

Pour l'instant deux botnets ont été identifiés dans les campagnes de spam de 2017: le botnet 7200 et le botnet 7500. Le fichier de configuration du botnet 7500 indique que plusieurs organismes de banques en ligne australiens sont ciblés par ce botnet. D'après la société Proofpoint, le botnet 7200 aurait été envoyé à des cibles du Royaume-Uni et de France. Le botnet 2144 est connu pour cibler des entreprises suisses, mais la campagne de spam de février 2017 contre les entreprises suisse n'a pas été rattachée avec certitude à ce botnet.

Lorsqu'une communication avec une des banques en ligne ciblée est détectée, Dridex intercepte et altère cette communication. Dridex est ainsi capable d'injecter du code à la volée dans les pages web de ses victimes afin de modifier les pages originales et de requérir et collecter des informations sensibles supplémentaires. Ces informations sont transmises au C&C et permettent aux opérateurs faire des tentatives de transactions frauduleuses en temps réél et en contournant les systèmes d'authentification à deux facteurs, en faisant intervenir la victime à son insu.

Dridex est également connu pour rechercher sur l'ordinateur infecté des informations liées aux programmes de gestion de banque en ligne, aux logiciels de paiement hors ligne, aux applications bancaires, aux lecteurs de carte à puce, et aux logiciels de gestion de points de vente. Les botnet 1234 et 2144 par exemple recherchent les traces de ce genre de logiciels. Les postes infectés qui utilisent ces logiciels sont ensuite isolés du botnet et confié à des opérateurs spécialisés dont le but est d'observer les usages et habitudes des entreprises infectées. Dridex permet de télécharger et d'installer d'autres codes malveillants. Ces opérateurs vont installer des outils d'administration à distance (Remote Access Tools) ou des outils d'intrusion afin d'espionner leur cible et/ou de dérober des mots de passe. D'autres codes malveillants adaptés à la cible peuvent être utilisés (les opérateurs de Dridex ont accès à un marché de code malveillants important). Enfin, des stratagèmes comme des fausses mises à jour sont utilisés afin de dérober des jetons d'indentification permettant de créer des ordres de virement frauduleux. Les opérateurs peuvent aller jusqu'à contourner des mécanismes de contrôle des ordres de virement (fax, impression, appel téléphonique, etc.). Des ordres de virement allant de $20 000 à plus de $2 000 000 ont été réalisés lors des campagnes précédentes.

Cibles du botnet 1234:

crealogix,multiversa,abacus,ebics,agro-office,cashcomm,softcrew,coconet,macrogram,mammut,omikron,multicash,quatersoft,alphasys,wineur,epsitec,myaccessweb,bellin,financesuite,moneta,softcash,trinity,financesuite,abrantix,starmoney,sfirm,migrosbank,migros bank,online banking,star money,multibit,bitgo,bither,blockchain,copay,msigna,armory,electrum,coinbase,magnr,keepkey,coinsbank,coolwallet,bitoex,xapo,changetip,coinapult,blocktrail,breadwallet,luxstack,airbitz,schildbach,ledger nano,mycelium,trezor,coinomi,bitcore

WinBacs,albacs,Albany.EFT.Corporate.Client,wpc,eSigner,StartStarMoney,StarMoney,acsagent,accrdsub,aceevents,acCOMpkcs,jp2launcher,sllauncher,cspregtool,RegisterTool,OEBMCC32,sfirm,Bbm24win,wip,paypen,mammut_tb,telelink,translink,deltaworks,dfsvc,bitcoin-qt,multibit,BacscomIP2,runclient,paycentre,accesspay,PaymentStudio,DiasClient,SynIntegrationClient,QuestLauncher,RemoteAdminServer,SymForm2App,plink,launch,PaygateWpfClient,terminal,Telelink,EBsec,ftrskr,Suite Entreprise,rbpmain2,rbpmain,tkc,ecbl-nxbp,sagedirect,turbo_teletransmission,cedripack,cedrisend,QikDesktop,QikDesktopCitrix,ConfigurationEditor,InteractFastConfig,otscm-client,ecb-sg,crs1,GbpSV,pstw32,MopaMaes,ldcptv10,gslshmsrvc,launcher,tokensharesrv,universe,ifrun60,roiwin31,guawin32,intwin31,kb_pcb,spawin31,cziwin31,czawin31,sta2gpc,etsr,tellerlauncher,prowin32,dirclt32,PLT1751,PLT1151,cegidebics,CCS3,CCMPS3,ComSX,keepass,c_agent,transac,relaisbtp,telebanking,ewallet,mstsc,cardentry,TPComplianceManager,TPWorkstation,BancLine 2.0,MS000000,BancLine 3.0,BancLine 4.0,BancLine 5.0,SFW,ptw1151,fedcomp,sfmain,VRNetWorld,KDS,Kasir,ICS,mpkds,pspooler,ipspool,POS-CFG,callerIdserver,EftTray,dpseftxc,EFTSERV,QBPOS,APRINT6,POSCONFG,jRestaurant,AFR38,rmpos,roi,AxUpdatePortal,Firefly,InitEpp,SM22,xfsExplorer,XFSSimulator,WosaXFSTest,kiosk,CRE2004,aspnet_wp,javav,XChrgSrv,rpccEngine,PTService,Rpro8,UTG2Svc,Active-Charge,javaw,DDCDSRV1,alohaedc,dbstpssvc,XPS,Transnet,posw,NCRLoader,PSTTransfer,TSTSolutions,wndaudit,TSTAdmin,TellerDR,merapplauncher,contact manager,goldtllr32,goldtrakpc,farm42phyton,fx4cash,bpcssm,vp-ebanking,LLB Online Banking,efix,iberclear,AMBCN,SGO,SQLpnr,vmware-view,banktelapk,SynJhaIntService,uniservice,client32,CanaraCustMaintenance,legaclt,pcsfe,pcscmenu,cwbtf,srvview,pcsmc2vb,cwb3uic,trcgui,cwbsvstr,rtopcb,cwbujcnv,cwbujbld,cwbuisxe,pcsws,cwbsvd,cwblog,cwbdsk,securID,jhaintexec,appupdate,SGNavigatorApp,dbr,WINTRV,bsaadmin,encompass,eautomate,link,adminconsole,commandclientplugin,commandclientplugin_gui,mfmanager,verex director-server manager,verex director-communication manager,notes,nlnotes,notes2,sacmonitor,netterm,fspnet,bridgerinside,cardserver,si,dais.ebank.client.offlineclient,BGFWIN31,BGDWIN31,BGXWIN31,bocusertool,CLXReader,UBSPay,Migros_Bank_E-Banking,Banklinth Online Banking,java,abastart,abamenu,abajvm,sage200.finanz.gui,vpxclient,htmlshell,mmc,e3K.Main,QOPT,cresus,wineur,abaeb,efinance,GestionPE,BCN-Netkey,Sage 30,ISL_light_client,msaccess,proffix.v4,pxShowThread,grpwise,mammut private,CashCommv5,winbiz

Cibles du botnet 2144:

Abacus
Abrantix
Alphasys
Argo-Office
Bellin
Cashcomm
CoCoNet
Crealogix
Epsitec
financesuite
Financesuite
Macrogram
Mammut
Mmulticash
Moneta
Multiversa
Myaccessweb
Omikron
Quatersoft
Softcash
Softcrew
Starmoney
Trinity

Cibles du botnet 7500

hxxp://ebank\[.]australianmilitarybank\[.]com\[.]au/[.]+/SignOn/[.]ogin\[.]aspx
hxxp://www2\[.]my\[.]commbiz\[.]commbank\[.]com\[.]au/logon/usermaintenance/
hxxp://bankwithfriends\[.]hicu\[.]com\[.]au/mvpheritageisle/[.]ogin\[.]as[.]*
hxxp://secure\[.]amp\[.]com\[.]au/wps/portal/sec/login/!ut/p/a1/[.]*/dl5/d5/L2dBISEvZ0FBIS9nQSEh/
hxxp://bizpermonline\[.]newcastlepermanent\[.]com\[.]au/NPBSBusines[.]*
hxxp://internetbanking\[.]mycreditunion\[.]com\[.]au/mvprcu/login[.]as[.]*
hxxp://internetbanking\[.]scu\[.]net\[.]au/mvpscu/[.]ign[.]n/[.]ogin\[.]asp[.]*
hxxp://secure\[.]regionalaustraliabank\[.]com\[.]au/banking/[.]ign[.]n/[.]ogin\[.]asp[.]*
hxxp://ebanking\[.]customsbank\[.]com\[.]au/ibank/[.]ign[.]n/[.]ogin\[.]asp[.]*
hxxp://ibank\[.]gcmutualbank\[.]com\[.]au/mvpgcm/[.]ign[.]n/[.]ogin\[.]asp[.]*
hxxp://bankwithfriends\[.]hicu\[.]com\[.]au/mvpheritageisle/[.]ogin\[.]as[.]*
hxxp://internetbanking\[.]imb\[.]com\[.]au/[.]ersonal/[.]ank[.]ast-[.]sername-[.]ogo[.]*
hxxp://ibanking\[.]unitybank\[.]com\[.]au/mvpunitybank/[.]ignon/[.]ogin\[.]asp[.]*
hxxp://internetbanking\[.]firstoptioncu\[.]com\[.]au/mvptab/signon/login\[.]asp[.]*
hxxp://bizpermonline\[.]newcastlepermanent\[.]com\[.]au/NPBSBusines[.]*

^http://[.]+\:3496/[.]*
^http://[.]+/flows/ebanking/
^http://[.]*citrix
^http://sisesrv1/
^http://shv-09
^http://[.]+winbacs/
^http://srvesmad04:8080/
^http://synfo/
^http://[.]+\:81/[.]*
^http://[.]+\:8888/[.]*
^http://[.]+\:8090/[.]*
^http://[.]+\:8084/[.]*
^http://127\[.]0\[.]0\[.]1:3495
^http://[.]+/MULTIVERSA
^http://[.]+/workbench/
^http://dtsgui\[.]cbhi\[.]local/
^http://srvaweb01/
^http://cujc-arcu/
^http://[.]*/sapphire/
^http://192\[.]168\[.]161\[.]23
^http://[.]+/mscmain
^http://intersection
^http://[.]+\:3495/[.]*
^http://[.]+\:9000/[.]*
^http://core-web/
^http://10\[.]118\[.]32\[.]33/
^http://core-syn/
^http://r-space/
^http://170\[.]209\[.]0\[.](3|2)
^http://webmail\[.]
^http://[.]*/flows/banking/
^http://dtsacquire2011
^http://arta2/
^http://dtsap:70/
^http://nmain/
^http://[.]*/b2b/faces/login/
^http://[.]*ingbusinessonline
hxxp://[.]*\[.]liverail\[.]com
^http://[.]*multiversa
^http://[.]*multiweb
hxxp://[.]+\[.]services\[.]mozilla\[.]com/
^http://bankway[.]*/
^http://ebanking
^http://[.]*office-wings
^http://[.]+/login\[.]aspx

hxxp://urs\[.]microsoft\[.]com/
hxxp://self-repair\[.]mozilla\[.]org/api/
hxxp://localhost[.]*/skypectoc/
hxxp://[.]*\[.]skype\[.]com/api/
hxxp://syndication\[.]twitter\[.]com/
hxxp://incoming\[.]telemetry\[.]mozilla\[.]org/
hxxp://geo\[.]query\[.]yahoo\[.]com/
hxxp://www\[.]bing\[.]com/
cashproonline-[.]+\[.]bankofamerica\[.]com
www3\[.]bankline\[.]
pioneer\[.]co-operativebank\[.]
hxxp://ibank\[.]b-e\[.]com\[.]au/ibank/SignOn/[.]ogin\[.]asp[.]
hxxp://[.]*\[.]cdfonline\[.]org\[.]au/[.]risbane/[.]ign[.]n/[.]ogin\[.]asp[.]*
hxxp://[.]*\[.]cdfonline\[.]org\[.]au/canberra/[.]ign[.]n/[.]ogin\[.]asp[.]*
hxxp://[.]*\[.]cdfonline\[.]org\[.]au/melbourne/[.]ign[.]n/[.]ogin\[.]asp[.]*
hxxp://ibank\[.]humebank\[.]com\[.]au/mvp/signon/login\[.]asp[.]*
hxxp://ibank\[.]humebank\[.]com\[.]au/mvp-resp/[.]ignon/[.]ogin\[.]asp[.]*
hxxp://netbank\[.]secul\[.]com\[.]au/mvpesb/signon/login\[.]asp[.]*
hxxp://permonline\[.]newcastlepermanent\[.]com\[.]au/NPBSPersona[.]*
hxxp://online\[.]arabbank\[.]com\[.]au/login/
hxxp://inetbnkp[.]adelaidebank[.]com[.]au/OnlineBanking/
hxxp://transtasman\[.]online\[.]anz\[.]com/client/
hxxp://bbo\[.]stgeorge\[.]com\[.]au/
hxxp://bbo\[.]bankofmelbourne\[.]com\[.]au/
hxxp://www\[.]bendigobank\[.]com\[.]au/eai/Logon/
hxxp://www\[.]ib\[.]boq\[.]com\[.]au/
hxxp://secure\[.]boqspecialist\[.]com\[.]au/BOQ/
hxxp://www\[.]hsbc\[.]com\[.]au/1/2/!ut/p/c5/[.]*\!/
hxxp://ibs\[.]bankwest\[.]com\[.]au/BWLogin/
hxxp://online\[.]beyondbank\[.]com\[.]au/
hxxp://secure\[.]macquarie\[.]com\[.]au/sepas/
hxxp://nabconnect2\[.]nab\[.]com\[.]au/auth/nabclogin/
hxxp://ib\[.]greater\[.]com\[.]au/OnlineBanking/
hxxp://netaccess3\[.]qtmb\[.]com\[.]au/QTMB/NetTeller/
hxxp://ribs\[.]rabobank\[.]com\[.]au/RIBSAU/
hxxp://internetbanking\[.]suncorpbank\[.]com\[.]au/
hxxp://banking\[.]westpac\[.]com\[.]au/wbc/banking/
hxxp://online\[.]corp\[.]westpac\[.]com\[.]au/
hxxp://secure\[.]rabodirect\[.]com\[.]au/exp/policyenforcer/pages/
hxxp://www\[.]amp\[.]com\[.]au
hxxp://ibank\[.]b-e\[.]com\[.]au/ibank/SignOn/[.]ogin\[.]asp[.]
hxxp://ib\[.]bankvic\[.]com\[.]au/bvib/signon/[.]ogin\[.]asp[.]
hxxp://mvp\[.]bigsky\[.]net\[.]au/mvpbscu/[.]ign[.]n/[.]ogin\[.]asp[.]
hxxp://[.]*\[.]cdfonline\[.]org\[.]au/[.]risbane/[.]ign[.]n/[.]ogin\[.]asp[.]*
hxxp://[.]*\[.]cdfonline\[.]org\[.]au/canberra/[.]ign[.]n/[.]ogin\[.]asp[.]*

hxxp://[.]*\[.]cdfonline\[.]org\[.]au/canberra/[.]ign[.]n/[.]ogin\[.]asp[.]*
hxxp://mvp\[.]capecu\[.]com\[.]au/mvpcape/[.]ogin\[.]asp[.]*
hxxp://ibank\[.]humebank\[.]com\[.]au/mvp/signon/login\[.]asp[.]*
hxxp://ibank\[.]humebank\[.]com\[.]au/mvp-resp/[.]ignon/[.]ogin\[.]asp[.]*
hxxp://[.]*\[.]cdfonline\[.]org\[.]au/melbourne/[.]ign[.]n/[.]ogin\[.]asp[.]*
hxxp://ib\[.]cwcu\[.]com\[.]au/mvpcwcul/[.]ign[.]n/[.]ogin\[.]asp[.]*
hxxp://netbank\[.]secul\[.]com\[.]au/mvpesb/signon/login\[.]asp[.]*
hxxp://ib\[.]fmbank\[.]com\[.]au/[.]*/[.]ignon/[.]ogin\[.]asp[.]*
hxxp://permonline\[.]newcastlepermanent\[.]com\[.]au/NPBSPersona[.]*
hxxp://banking\[.]mymove\[.]com\[.]au/myMOVE/SignOn/Login\[.]asp[.]*
hxxp://ib\[.]tmbank\[.]com\[.]au/[.]*/[.]ignon/[.]ogin\[.]asp[.]*
hxxp://internetbanking\[.]scu\[.]net\[.]au/mvpscu/[.]ign[.]n/[.]ogin\[.]asp[.]*
hxxp://onlinebanking\[.]themaccu\[.]com\[.]au/mvpmacu/signon/login\[.]asp[.]*
hxxp?://(ya|yandex)\[.]ru

5. Ressources et Indicateurs

Tracker de C&C Dridex: https://feodotracker.abuse.ch/

Dridex C&C:
195.88.209.221
217.197.39.1
91.219.28.55
178.32.255.130
208.87.225.248
104.236.252.178
83.141.2.155
64.250.115.129
59.125.50.132
192.3.165.10
205.186.129.254
194.190.161.63
23.94.38.151

QuantLoader C&C:
hxxp://justjohnwilhertthet[.]ws/m/
hxxp://jusevengwassresbet[.]ws/q/index.php
hxxp://sinmanarattot[.]ws/q/index.php

Download URLs:
palmcoastcondo.net/de3f3
shadowdalestorage.com/de3f3
lpntornbook.com/de3f3

precisioncut.com.au/de3f3
golongboard.pl/b723dd?
taddboxers.com/b723dd?
dfl210.ru/b723dd?
naturalcode-thailand.com/b723dd?
http://ricgemmell.com/t76b6r4v?eGoTyOyavv=MqolVeiGcn
http://birchwoodplaza.com/54gf3f
hxxp://solucionesfenix[.]net/33f3v3.exe
hxxp://nzhat[.]net/9jgtyft6
hxxp://meyermuehltal[.]de/0h656jk
hxxp://technologyservice[.]eu/0h656jk
hxxp://tspars[.]com/0h656jk
hxxp://thaipowertools[.]com/0h656jk
hxxp://www[.]movimentodiesel[.]gr/0h656jk
hxxp://lhgarden[.]org/0h656jk
hxxp://www[.]soulcube[.]com/0h656jk
hxxp://roylgrafix[.]com/76gbce?
hxxp://signwaves[.]net/76gbce?
hxxp://testsite[.]prosun[.]com/76gbce?
hxxp://omurongen[.]com/76gbce?
hxxp://pastasmolinero[.]es/76gf33
hxxp://nzhat[.]net/9jgtyft6

211shap.ru - GET /874hv
anticon.net - GET /874hv
cardoso1.com - GET /874hv
centralsecuritybureau.com - GET /874hv
decadd.com - GET /874hv
designbyli.com - GET /874hv
hiddencreek.comcastbiz.net - GET /874hv
jheroen.nl - GET /874hv
kapil.50webs.com - GET /874hv
kpwc.comcastbiz.net - GET /874hv
marinusjanssen.nl - GET /874hv
ncdive.com - GET /874hv
produlav.com.br - GET /874hv
RussellYermal.com - GET /874hv
solucionesfenix.net - GET /874hv
super-marv.com - GET /874hv
trans-atm.com - GET /874hv
tserv.su - GET /874hv
usawaterproofing.com - GET /874hv
www.mdfond.ru - GET /874hv

Dridex MD5

0014171a1d36d19db8bfd0b33c2e1adf
00596a10403e5e6fbde84fab8d34d5aa
0069e7e9213c8a1e1ae26877c7271d18
007295b6d9ec6863a4802e66d70d93c4
0074ec2a1b8ff59f12893ea40788d3f9
00d461f4692731e3119ff60b14872fb1
01115718bf610bd45629d4baa20b8bb0
0117a759fb6c8f4262260fe844f29f68
0121e8fe5076d07dce7bc5da5331ed48
0181a54e65f6e820f157521ceb79d48d
0196f16a6d56a22fa9e148bea9aefae4
01b5fd091df56cfd483a4ed7b1dc8b36
0243c9bb903d6f89d7eeadae882cf591
026222a1bbabfbadf35cdf6cb13d1d0f
02aa65b8cb868a93b4ac07eb6d157931
0355c8248e65335b576caa8c84e2bd24
036ee7143e7d708769212dd40d297494
0374bbb66fb38a550709d41f83e6eb9a
038ca495563bb39213a88240c5f23091
039d966f382bec0bd84d7bdb9b14e901
03b4e8d71f7b79ed21f91aee6b6a8f7c
03c85ddb26fac3699acfe06a99e9bbea
04117c25c082670aa88412fb7178c112
0438d8d201fade69a545e91f48c67599
043be1a96ce13531753963678bfbc710
044302f964684e71ef0ea90db2385a37
04c4a14ab16656f33d21cdab835e6921
0522d3e0d34aa35b2dd3bdb70ad981e1
0530807ad5f7d4ef7a7cfb6a1b3c25d4
0562791c2721eeb440cbe5f2aeecbc67
05686ffd966366a84e1389e925b3ed00
056dcb753ee067aa716bc0db8f85fb2e
05b69466691ed7957be7e02a26b5c8a7
05c7abc4eb1da8e116e86a801f297d18
0639c6cf4594c3188d5aa0489f345e8c
066004128cfb361304e809496afa1c53
068977def5e2ac64cfc3f0677b45bfb4
06c2aeaee9091593dbdfc4c41cfe2327
06f8a4ec64ed0b0947cbb9b66cd5d33d
0702ddd6599d4a9ce73b7670fd737685
070ad2426cff1c5006be896d6a0cf0bc
07ce6d5360d615c6f6d4dc450d5ec268
08302a89347cbfcde24a9eca8115913a
08474f3474d0104663ddb0328465332c
084bd7f6854c41fc93c36c8fa07cae10

0966afb4bf769b433ca6dc8d32506e7d
09761918ca5064b9d2042eb86994997b
098198486ce3d9b397dc64f927bc3103
09c64d212a85bba46c6fdd62b08bbcf0
09cdd86743a636c5e73306ec06e1cda2
09d5837ff64f460a09d33c18f38104b8
0a353d59a85c0305fbaa3b61ab0bb884
0a6eacd0345160f027c4061258176d14
0a77f6654820c8a04cfa07d730914279
0a88383bea1b71fb0f5e33994dbf40c7
0a89ee13686a4652a8d7805fd63665b4
0a970b5bcb1d098d0bcac72eca2f797d
0ab8203c936e62fb7682f160ed048169
0ae18ef72e6a5d6ffc551b87acb405c4
0ae3bff08972439a30cdb2f23397b5e2
0af2f0f440d85b7f724171c1994cedb6
0b1a93fb94891f0f88b9fbb5dca2d1ab
0b2507b4df00118b40dd2b11c0cfe255
0b4c27dc77cce3c6b1b9cd4d54fa3056
0b5e8f65777e8b48943d7a29aa262c31
0b98b81e62140b6c4bac098858a5fd17
0bbd3a2eaa66a78d4276e442ea19325e
0bbed74f5ebd70f10d523c642fed756a
0c02c2d8176f46114d815b3bd5249ea8
0c070e9370f3c97d5f40f16882925eea
0c309e4da1d89a17890f42ba282b94d0
0c3489a889120d09b85b9dd0bbe6e824
0c3acd0c97b29b35cb648948abf51e67
0c435c043b84001a9e1b3159ea328f34
0cb3d0456c73b78128285b1fa1c6059f
0cdf9419e32d50300e11cc6caf17a44a
0d52d9cb5027e40ac4ef9f1000954e8a
0d60d682eecebd43f4c25481c069c545
0dc6d55c8a96919d54d8b01603802fa7
0de75ef4fec5bc6996f37238cbf126f0
0e2d2ae8af3b942a988d525b7b6ceec4
0eb1e46b144c1e7b70a7549a0729b3c9
0ed9a8cf04868fb2dba9d6698f303333
0f0ca333ee3bdc6747104b86ef027698
0f13d9045c1fc3e202a548c4c5904351
0f8741d37a13b2a60ad3b6089718bd8c
0fe49b37f0d9a74df9c14fa17f3b9ec6
100e4f9c1ec83fc3e92506fa37cac56b
110ca3c4224dbc68e886b2d8de67fb4d
1184bae378cbf4a1363dfe696d9bcaac
12c05bc27820b74c5d2be6c8ac03e41a

13902606d0ca0aedca132cb2d61ff6b4
1398dcf9f7ae29f0157bb47ca7c574d2
13ec1d31426fef220eff60f2c51af841
14598da3a97fbea440bdc6ebf87316bb
3ede7214e1fe848aefd67e8d11beec00
41a5b1d50947452adb663abcb6ecb829
c738746c751e3f4465cdf20959ed7115
e50522bf1817a8f5698b740e5225c34f
f4e11acef79702561dea6070d4dbba45

4. Références

https://www.proofpoint.com/us/threat-insight/post/dridex-campaigns-millions-recipients-unpatched-microsoft-zero-day
https://www.proofpoint.com/us/threat-insight/post/high-volume-dridex-campaigns-return
https://myonlinesecurity.co.uk/emailing-pic9744891-jpg-malspam-delivers-dridex/
https://isc.sans.edu/forums/diary/Dridex+malspam+seen+on+Monday+20170410/22280/
https://securityintelligence.com/dridexs-cold-war-enter-atombombing/
https://labsblog.f-secure.com/2017/03/31/dridex-spam-runs-targeting-uk/
https://www.govcert.admin.ch/blog/28/the-rise-of-dridex-and-the-role-of-esps
http://www.malware-traffic-analysis.net/2017/03/30/index2.html
https://myonlinesecurity.co.uk/payment-request-malspam-spoofing-hedley-ellis-ltd-delivers-dridex/
https://myonlinesecurity.co.uk/spoofed-gamestop-co-uk-help-gamestop-order-no-327609-malspam-delivers-malware/
https://myonlinesecurity.co.uk/confirmation-letter-enclosed-please-see-attachment-malspam-delivers-malware/
https://myonlinesecurity.co.uk/scan-as-reqested-malspam-delivers-dridex/
https://myonlinesecurity.co.uk/photos-from-georgia-delivers-dridex-banking-trojan/
https://myonlinesecurity.co.uk/spoofed-your-gb-energy-supply-bill-00077334-is-attached-delivers-dridex-banking-trojan/
https://myonlinesecurity.co.uk/your-telephone-bill-invoices-reports-client-id62331521-malspam-delivers-dridex-banking-trojan/
https://myonlinesecurity.co.uk/attached-is-the-copy-of-your-payment-receipt-malspam-delivers-malware/
https://myonlinesecurity.co.uk/copy-invoice-581652-spoofed-onehotcookiefranchise-com-delivers-dridex-banking-trojan/
https://myonlinesecurity.co.uk/fw-to-all-employees-malspam-delivers-dridex/

Conduite à tenir :

Dans le cas où vous seriez infecté, vous pouvez communiquer ces éléments à la Sous-Direction de la Lutte contre la Cybercriminalité :

- Entête du mail et mail à l'origine de l'infection au format EML
  (mode opératoire de récupération de l'entête)
  Ne pas transférer l'email original, nous ne pourrons pas récupérer l'entête lors du transfert.
  Enregistrer l'email sur votre bureau et zippez l'archive que vous aurez cryptée avec un mot de passe.

- La charge utile (pièce jointe du mail)

- Logs serveur ou postes (journaux d'évènements)

Adresser votre mail à csirt-pj@interieur.gouv.fr