Stopping Serial Killer: Catching the Next Strike

research.checkpoint.com/2021/stopping-serial-killer-catching-the-next-strike/amp

January 4, 2021

Brief

When we look at a prevalent malware family, we give credit to its authors regarding the established malicious infrastructure. New malicious activity is flowing smoothly, command-and-control servers appear, everything works like Swiss watch. Are there any weak points in such a construction?

To answer this question we may think about a race car. It's a masterpiece crafted for maximum speed, however, the more speed it has, the less chances it has to make a sharp turn. Malware infrastructure has the same weakness of inertia. When every joint works fine, you should have a strong reason to change something in it.

We can use it for our benefit just like movie detectives do. Take a city map, mark the spots of previous crimes — and you will likely understand the pattern and even get a probable place of next crime activity, it will likely follow the determined template. In this research we show how to transform these actions to the world of malware. We take one of the most prevalent contemporary botnets called Dridex, mark its previous crime scenes, build the map and draw conclusions helping us to catch the next strike. We show evidence of success of such an approach measured in strict numbers and explain how to use this idea in other real world cases.

Introduction

The Dridex Banking Trojan first appeared in 2014 and is still one of the most prevalent malware families. In March 2020, Dridex topped the list of most wanted malware.

Dridex was created by a cyber-crime group called "Evil Corp" which has caused an estimated damage of $100 million to the banking system worldwide. A lot of research has been issued already covering different aspects of the malware details and how the cyber-crime group functions.

In this article we provide a summary of key details known about Dridex to date. We explore pre-history of Dridex development, give an overview and show its key technical features and methods of spreading. We explain how we can intercept this malware at the earliest stages of the infection chain. We also provide graphs that show evidence of the success of our approach and how our customers are protected against this malware.

Background

Dridex has a famous lineage. Let's take a step back in history to find out more about the time period when its earliest version appeared.

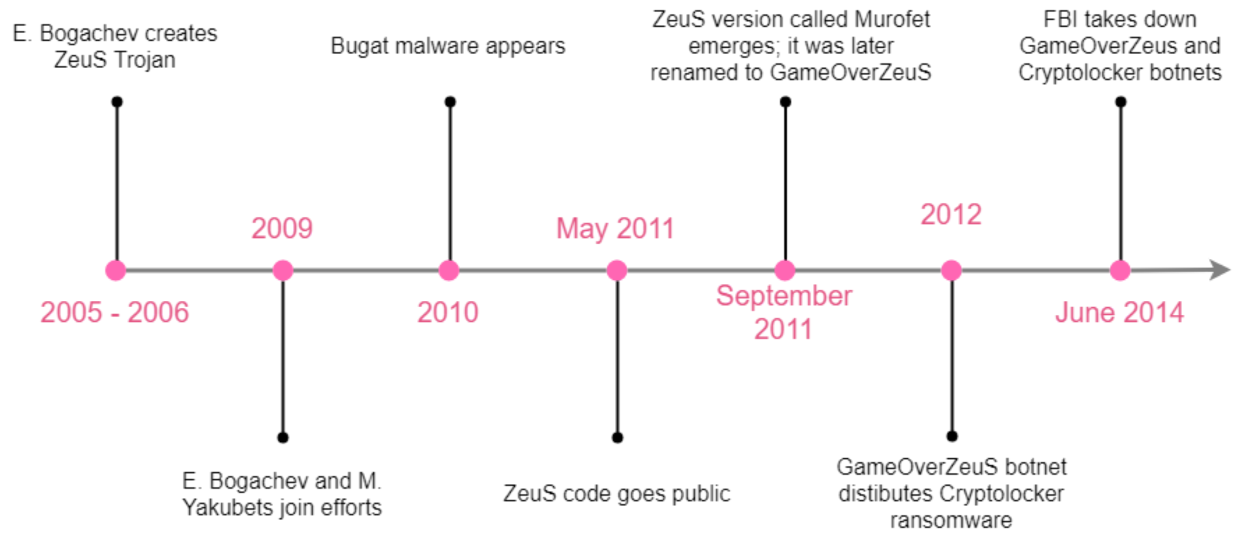
The key names in this story:

- **Evgeniy Bogachev —** Creator of the infamous ***ZeuS*** malware.
- **Maksim Yakubets —** Alleged leader of ***Evil Corp*** cyber-crime group which is responsible for Dridex operations.

Pre-Dridex era – It all starts with ZeuS

Zeus is a Trojan Horse malware. Its capabilities include turning an infected machine into a botnet node, stealing banking credentials, downloading and executing separate malicious modules. The members of cyber crime group attempted to steal around 220 million USD worldwide utilizing ZeuS according to FBI investigation.

The timeline below shows key points in ZeuS evolution:

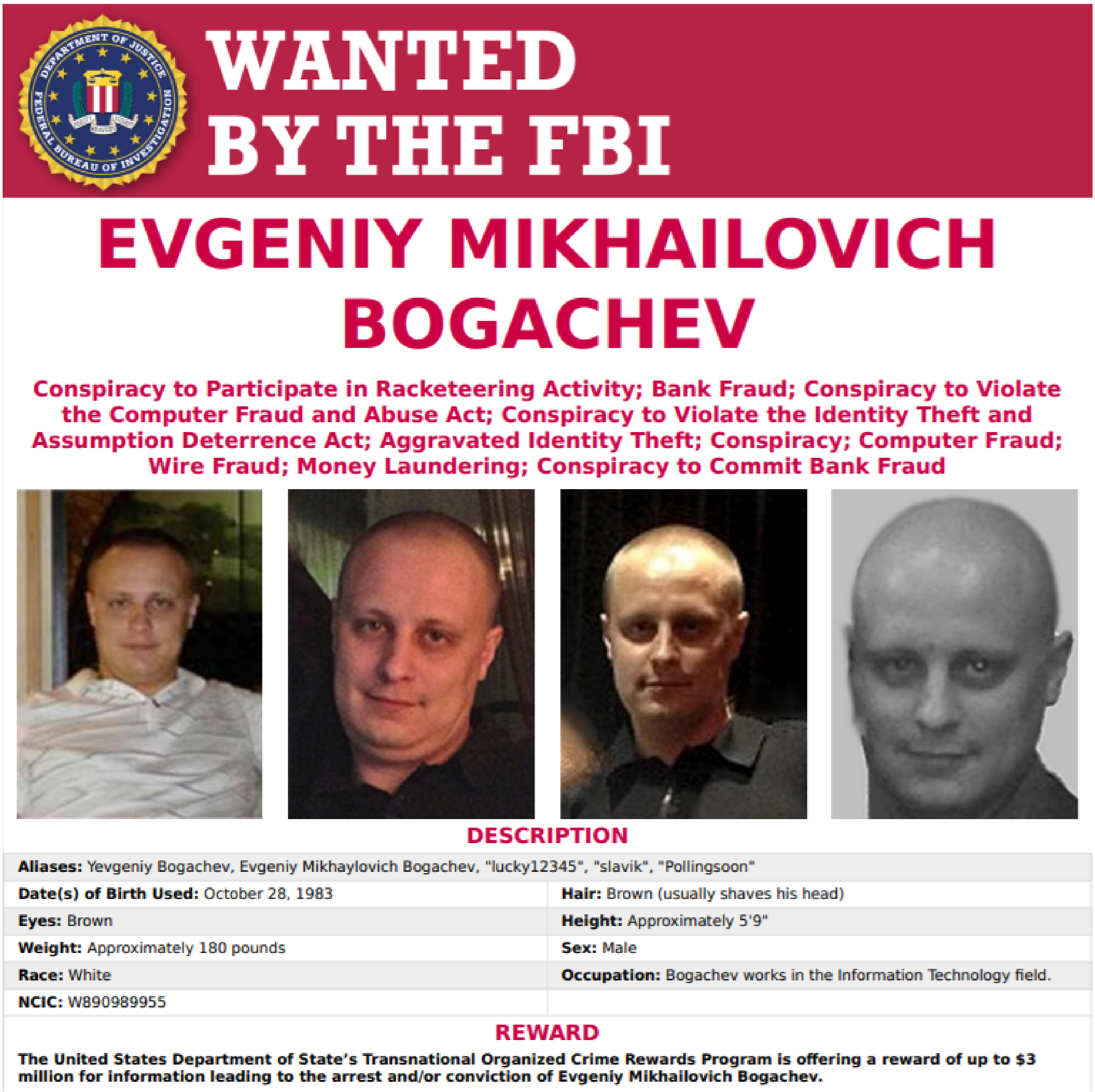


E. Bogachev creates ZeuS Trojan
2005 - 2006
2009
E. Bogachev and M. Yakubets join efforts
Bugat malware appears
2010
May 2011
ZeuS code goes public
ZeuS version called Murofet emerges; it was later renamed to GameOverZeuS
September 2011
2012
GameOverZeuS botnet distibutes Cryptolocker ransomware
FBI takes down GameOverZeus and Cryptolocker botnets
June 2014

Figure 1 – Chronology of ZeuS evolution.

When ZeuS source code was leaked in 2011, various branches of this malware started to appear. It was very popular malware and gave rise to lots of different malware branches. ZeuS versions may be in a ZeuS online museum. At the time of this writing, ZeuS was associated with 29 different malware families, featuring around 490 versions in total.

In May 2014, the FBI issued a bulletin with description of Evgeniy Bogachev and the promised reward of 3 million USD “for information leading to the arrest and/or conviction.”



WANTED
BY THE FBI

EVGENIY MIKHAILOVICH
BOGACHEV

Conspiracy to Participate in Racketeering Activity; Bank Fraud; Conspiracy to Violate the Computer Fraud and Abuse Act; Conspiracy to Violate the Identity Theft and Assumption Deterrence Act; Aggravated Identity Theft; Conspiracy; Computer Fraud; Wire Fraud; Money Laundering; Conspiracy to Commit Bank Fraud

DESCRIPTION

Aliases: Yevgeniy Bogachev, Evgeniy Mikhaylovich Bogachev, "lucky12345", "slavik", "Pollingsoon"	
Date(s) of Birth Used: October 28, 1983	**Hair:** Brown (usually shaves his head)
Eyes: Brown	**Height:** Approximately 5'9"
Weight: Approximately 180 pounds	**Sex:** Male
Race: White	**Occupation:** Bogachev works in the Information Technology field.
NCIC: W890989955	

REWARD

The United States Department of State's Transnational Organized Crime Rewards Program is offering a reward of up to $3 million for information leading to the arrest and/or conviction of Evgeniy Mikhailovich Bogachev.

Figure 2 – Description of Evgeniy Bogachev on the FBI site.

Dridex era

After the botnets of direct ZeuS successors were taken down, Dridex’s time came. This malware is a result of **Bugat** evolution (which appeared in 2010). Bugat v5 was recognized as Dridex in 2014.

More names appear on the stage at this time.

- Andrey Ghinkul (from Moldova) was allegedly one of the administrators behind Dridex botnets in 2015.
- Igor Turashev was allegedly one of the administrators behind Dridex botnets as well.
- Denis Gusev was one of the key investors behind EvilCorp.

More names connected to Dridex can be found in US treasury sanctions statement.

The timeline below shows some milestones in Dridex evolution:

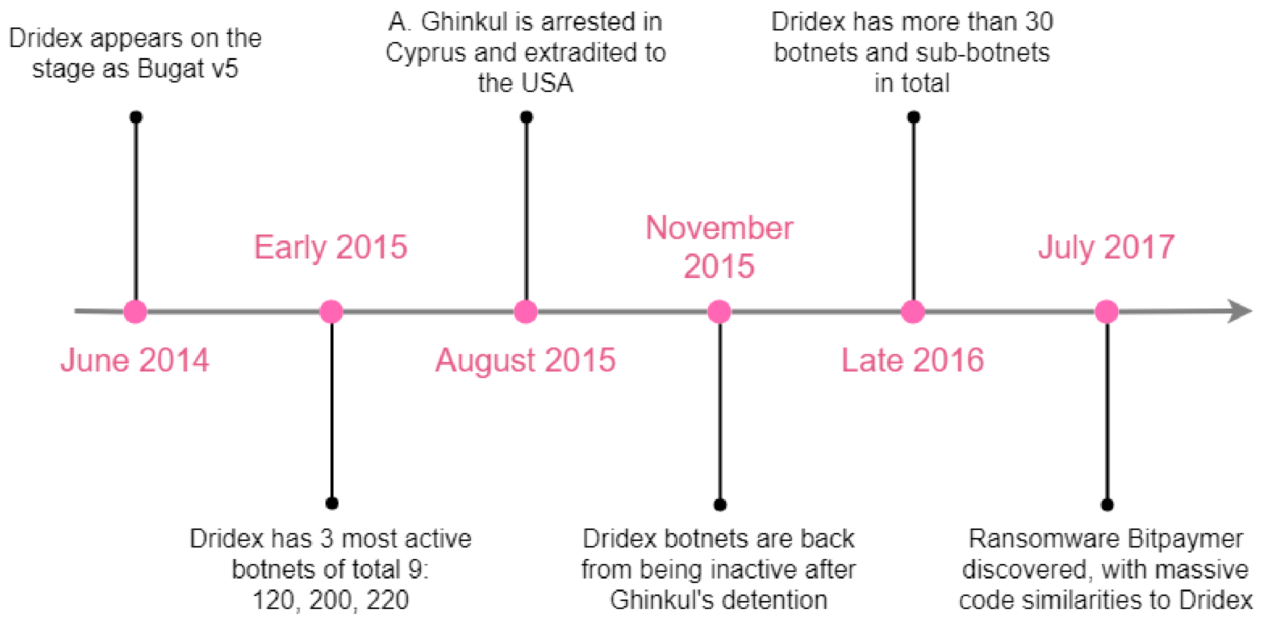

Dridex appears on the stage as Bugat v5
June 2014
Early 2015
Dridex has 3 most active botnets of total 9: 120, 200, 220
A. Ghinkul is arrested in Cyprus and extradited to the USA
August 2015
November 2015
Dridex botnets are back from being inactive after Ghinkul's detention
Dridex has more than 30 botnets and sub-botnets in total
Late 2016
July 2017
Ransomware Bitpaymer discovered, with massive code similarities to Dridex

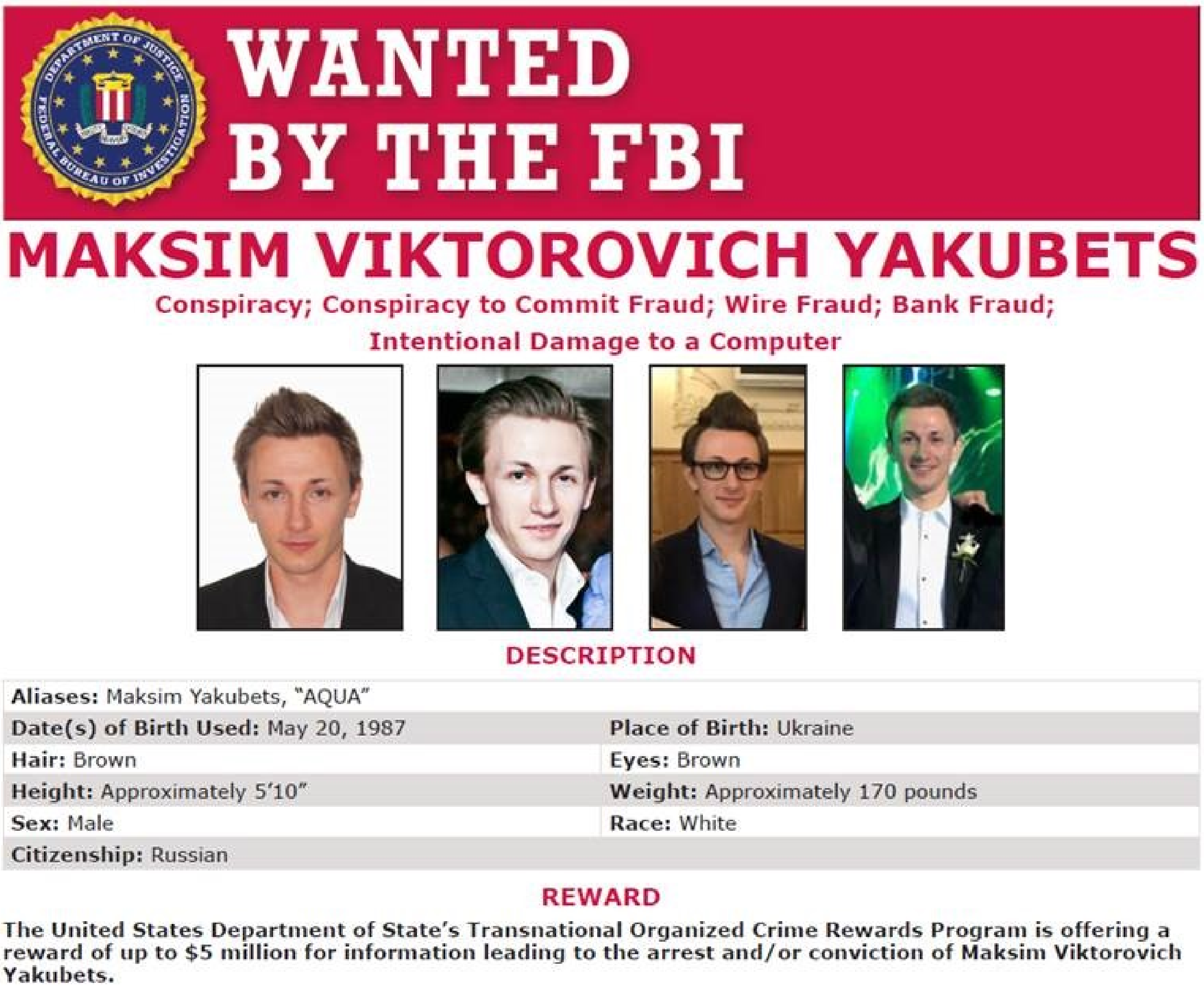
Figure 3 – Chronology of Dridex evolution.

Dridex in turn gave rise to a number of ransomwares starting with ***Bitpaymer*** in 2017. This branch continued with ***DoppelPaymer***, which was developed in 2019, and ***WastedLocker***, which was developed in 2020.

Recent past

In 2019, Dridex had at least 14 active botnets, some of which had already been spotted previously, and others newly developed. Botnets are differentiated by their ID numbers. These are among the most active at this time: 10111, 10222, 10444, 40200, 40300.

At the end of 2019, the FBI issued a bulletin with a description of the author of Dridex and a promised reward of 5 million USD (compared with 3 million USD previously for E. Bogachev).



WANTED BY THE FBI

MAKSIM VIKTOROVICH YAKUBETS

Conspiracy; Conspiracy to Commit Fraud; Wire Fraud; Bank Fraud; Intentional Damage to a Computer

DESCRIPTION

Aliases: Maksim Yakubets, "AQUA"	
Date(s) of Birth Used: May 20, 1987	**Place of Birth:** Ukraine
Hair: Brown	**Eyes:** Brown
Height: Approximately 5'10"	**Weight:** Approximately 170 pounds
Sex: Male	**Race:** White
Citizenship: Russian	

REWARD

The United States Department of State's Transnational Organized Crime Rewards Program is offering a reward of up to $5 million for information leading to the arrest and/or conviction of Maksim Viktorovich Yakubets.

Figure 4 – Description of Maksim Yakubets on the FBI site.

There is also evidence of Maksim's luxurious lifestyle, undoubtedly due to income from his malicious activities.

Figure 5 – Cars, girls, money; the luxurious lifestyle of Maksim Yakubets.

To date, Maksim Yakubets has not been apprehended by law enforcement.

As mentioned previously, in 2020, Dridex topped the lists of the most prevalent malware families in the world.

Infection chain

Before we start the analysis of Dridex samples themselves, we want to understand the infrastructure behind the malware. How is it delivered? What are the targets? What is the initial detection rate of supporting files? We will find the answers to all of these questions below.

Flow

When the operators want to spread Dridex, they use established spambots from different cyber-crime groups to send malicious documents attached to handily crafted e-mails. At different times of the Dridex lifecycle, ***Necurs***, ***Cutwail*** and ***Andromeda*** botnets have all been involved in spreading Dridex.

When a user downloads and opens such a document (it may be Word or Excel), the embedded macros are launched with the aim of downloading and executing the Dridex payload.

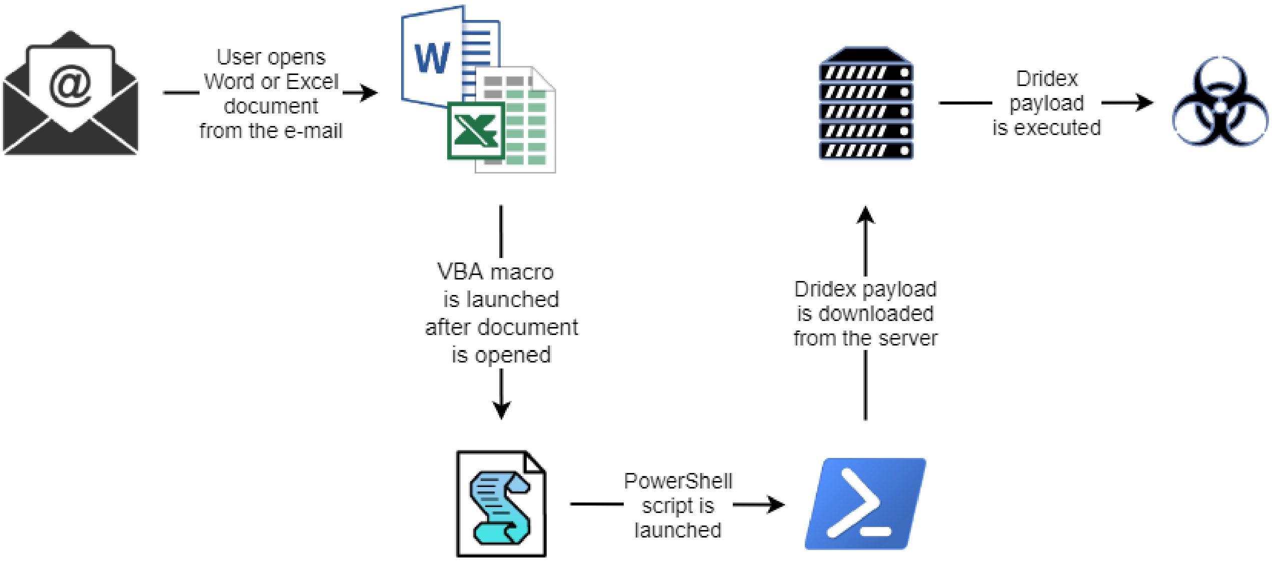

User opens Word or Excel document from the e-mail
VBA macro is launched after document is opened
PowerShell script is launched
Dridex payload is downloaded from the server
Dridex payload is executed

Figure 6 – Dridex infection chain execution flow.

Targets

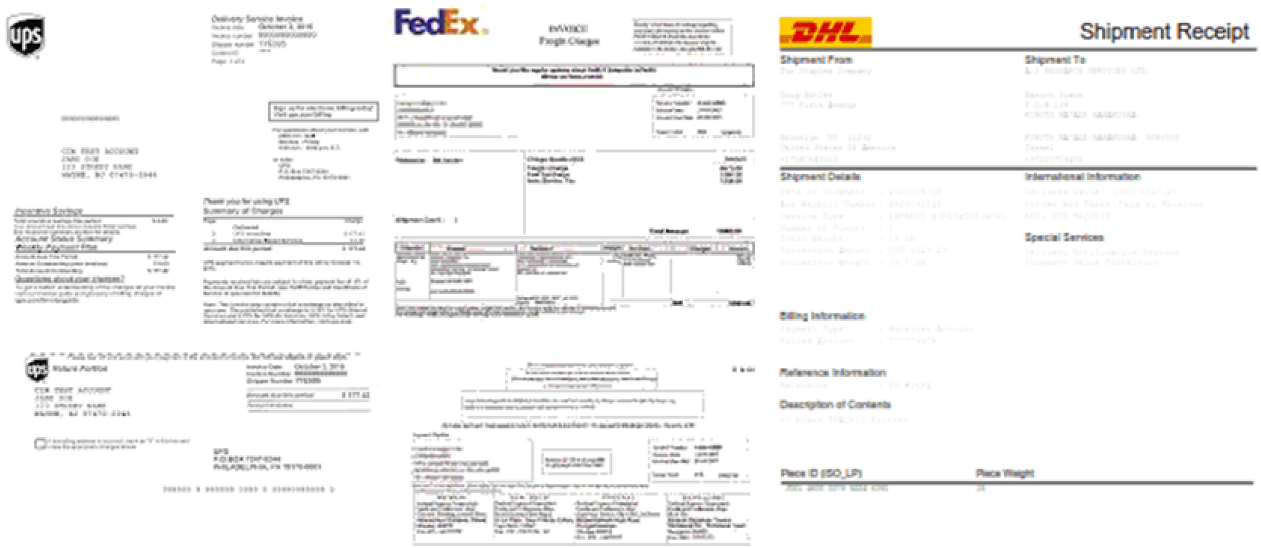
Dridex targets different high-profile entities from various parts of the world:

- U.S. bank accounts.
- U.S. credit card companies.
- U.S. financial investment corporations.
- European bank accounts.

- Governmental agencies in Saudi Arabia, Qatar, Oman.

Lures

To increase the successful rate at which Dridex is spread, malicious actors disguise their spam e-mails to look like legitimate ones. We can name examples of UPS, FedEx and DHL as companies whose logos and mailing style are used as bait in such e-mails.



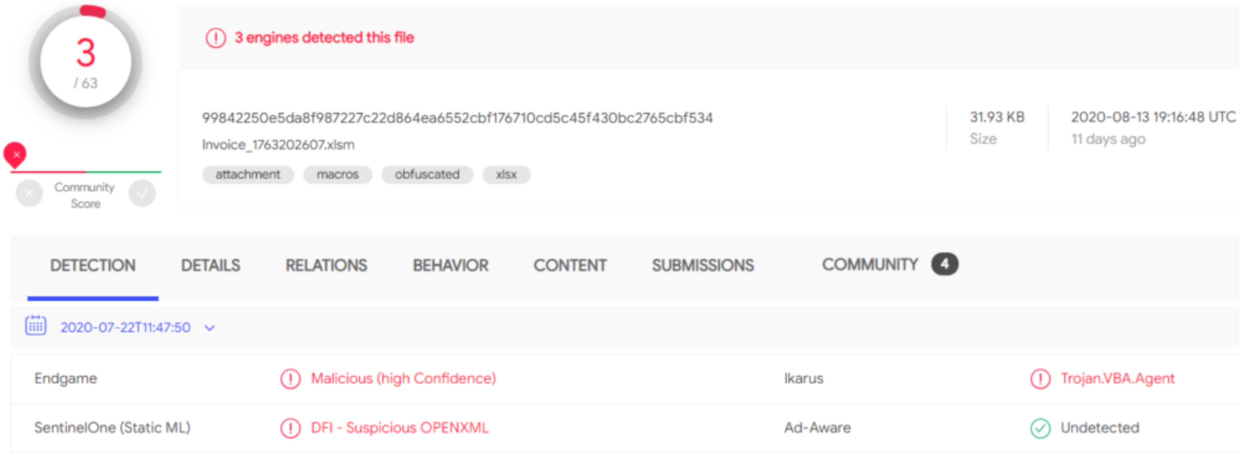
Delivery Service Invoice
Thank you for using UPS
Shipment Receipt
Shipment From
Shipment To
Shipment Details
International Information
Special Services
Billing Information
Reference Information
Description of Contents
Piece ID (ISO_LP)
Piece Weight

Figure 7 – Examples of lures.

When the victim clicks the link, either the archive with the malicious document or the malicious document itself is opened.

Initial detection rate

When first seen in the wild, Dridex delivery files show a very low detection rate. In the screenshot below we see the initial detection rate of the Excel document which delivers Dridex:



3 / 63

Community Score

3 engines detected this file

99842250e5da8f987227c22d864ea6552cbf176710cd5c45f430bc2765cbf534
Invoice_1763202607.xlsm

attachment macros obfuscated xlsx

31.93 KB
Size

2020-08-13 19:16:48 UTC
11 days ago

2020-07-22T11:47:50

Endgame	Malicious (high Confidence)	Ikarus	Trojan.VBA.Agent
SentinelOne (Static ML)	DFI - Suspicious OPENXML	Ad-Aware	Undetected

Figure 8 – Initial detection rate of the Dridex delivery file.

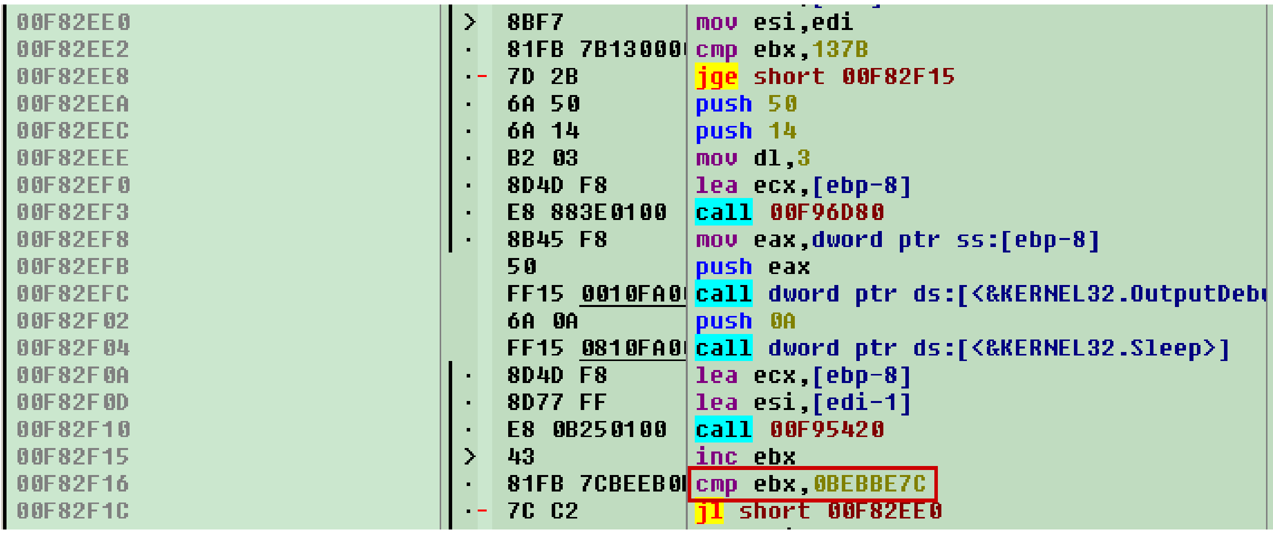
The same is true for other delivery files.

Loader and Payload

The Dridex sample consists of the loader and the payload. We discuss key points of each part below.

Anti-debug technique

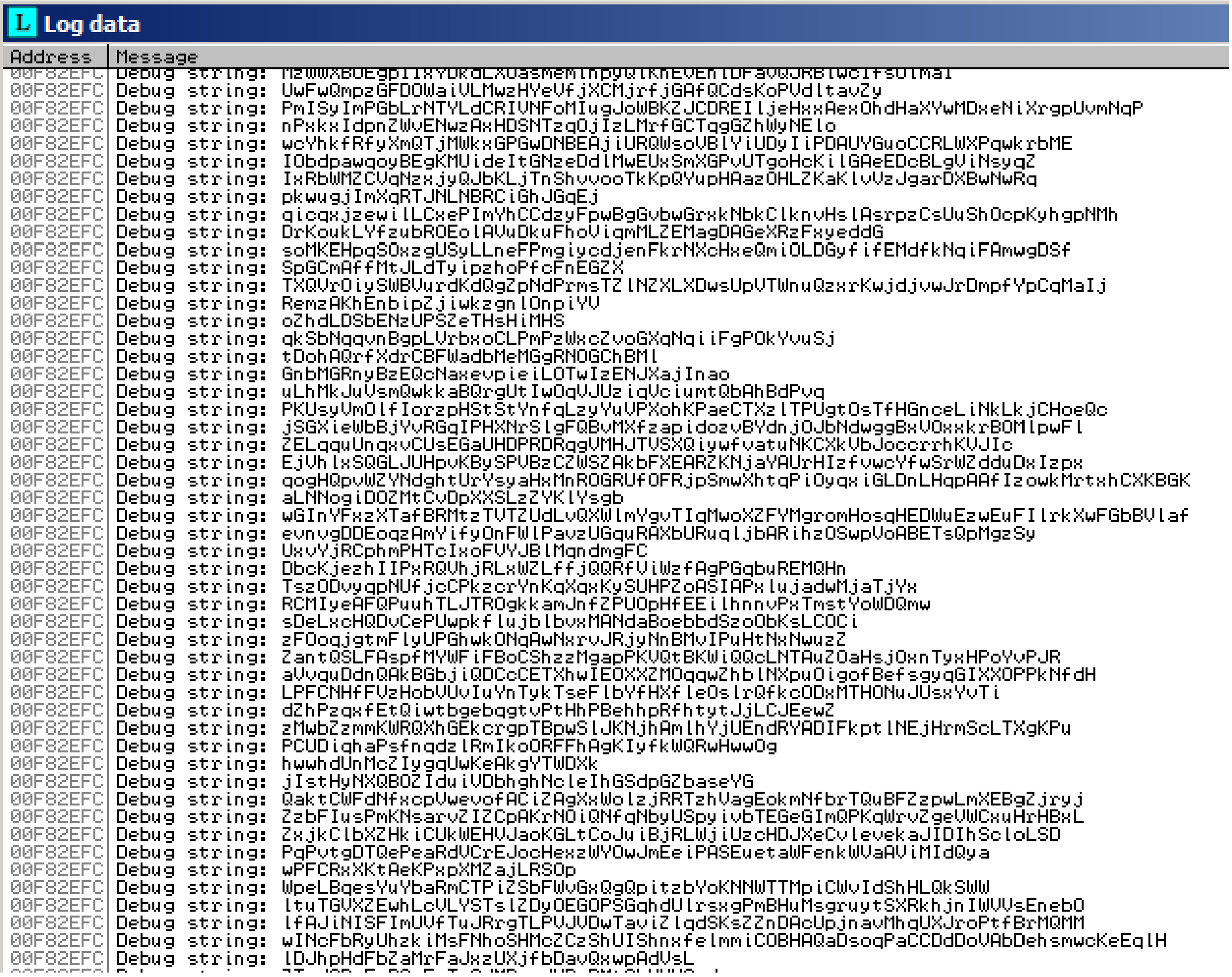
The Dridex loader utilizes the **OutputDebugStringW** function to make malware analysis more difficult. Different loaders produce different outputs (with the “Installing…” string being very popular) but the idea is the same everywhere: making a long loop that contains a lot of meaningless debug messages. In the figure below, we see the example of such a loop with an iteration of around 200 million:



```
00F82EE0    >  8BF7          mov esi,edi
00F82EE2    .  81FB 7B13000  cmp ebx,137B
00F82EE8    .- 7D 2B         jge short 00F82F15
00F82EEA    .  6A 50         push 50
00F82EEC    .  6A 14         push 14
00F82EEE    .  B2 03         mov dl,3
00F82EF0    .  8D4D F8       lea ecx,[ebp-8]
00F82EF3    .  E8 883E0100   call 00F96D80
00F82EF8    .  8B45 F8       mov eax,dword ptr ss:[ebp-8]
00F82EFB       50            push eax
00F82EFC       FF15 0010FA0  call dword ptr ds:[<&KERNEL32.OutputDeb
00F82F02       6A 0A         push 0A
00F82F04       FF15 0810FA0  call dword ptr ds:[<&KERNEL32.Sleep>]
00F82F0A    .  8D4D F8       lea ecx,[ebp-8]
00F82F0D    .  8D77 FF       lea esi,[edi-1]
00F82F10    .  E8 0B250100   call 00F95420
00F82F15    >  43            inc ebx
00F82F16    .  81FB 7CBEEB0  cmp ebx,0BEBBE7C
00F82F1C    .- 7C C2         jl short 00F82EE0
```

Figure 9 – Loop with 0xBEBBE7C (around 200 million) iterations calling ***OutputDebugStringW.***

The output looks like this in the log:

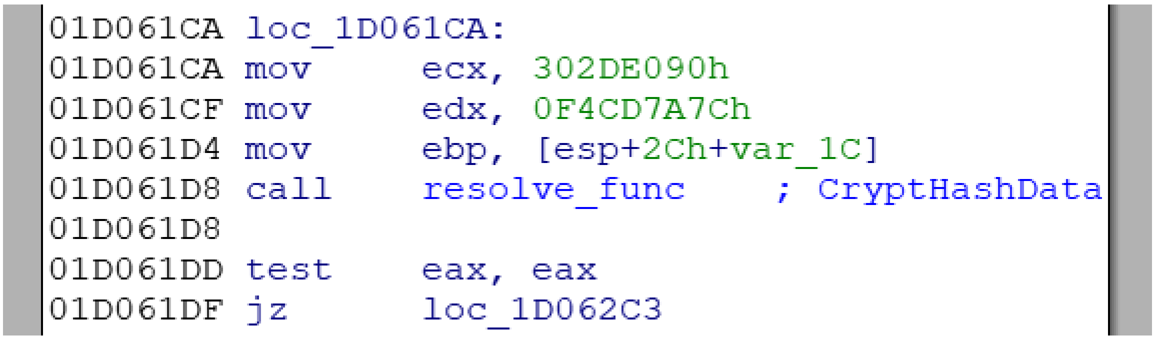


```
Address   Message
00F82EFC Debug string: UwFwQmpzGFDOWaiVLMwzHYeVfjXCMjrfjGAfQCdsKoPVdltavZy
00F82EFC Debug string: PmISyImPGbLrNTYLdCRIVNFoMIugJoWBKZJCDREIljeHxxAexOhdHaXYwMDxeNiXrgpUvmNqP
00F82EFC Debug string: nPxkxIdpnZWvENwzAxHDSNTzqOjIzLMrfGCTqgGZhWyNElo
00F82EFC Debug string: wcYhkfRfyXmQTjMWkxGPGwDNBEAjiURQWsoVBlYiUDyIiPDAUYGuoCCRLWXPqwkrbME
00F82EFC Debug string: IObdpawqoyBEgKMUideItGNzeDdlMwEUxSmXGPvUTgoHcKilGAeEDcBLgViNsyqZ
00F82EFC Debug string: IxRbWMZCVqNzxjyQJbKLjTnShvvooTkKpQYupHAazOHLZKaKlvVzJgarDXBwNwRq
00F82EFC Debug string: pkwugjImXqRTJNLNBRCiGhJGqEj
00F82EFC Debug string: qicqxjzewilLCxePImYhCCdzyFpwBgGvbwGrxkNbkClknvHslAsrpzCsUuShOcpKyhgpNMh
00F82EFC Debug string: DrKoukLYfzubROEolAVuDkuFhoViqmMLZEMagDAGeXRzFxyeddG
00F82EFC Debug string: soMKEHpqSOxzgUSyLLneFPmgiycdjenFkrNXcHxeQmiOLDGyfifEMdfkNqiFAmwgDSf
00F82EFC Debug string: SpGCmAffMtJLdTyipzhoPfcFnEGZX
00F82EFC Debug string: TXQVrOiySWBVurdKdQgZpNdPrmsTZlNZXLXDwsUpVTWnuQzxrKwjdjvwJrDmpfYpCqMaIj
00F82EFC Debug string: RemzAKhEnbipZjiwkzgnlOnpiYV
00F82EFC Debug string: oZhdLDSbENzUPSZeTHsHiMHS
00F82EFC Debug string: qkSbNqqvnBgpLVrbxoCLPmPzWxcZvoGXqNqiiFgPOkYvuSj
00F82EFC Debug string: tDohAQrfXdrCBFWadbMeMGgRNOGChBMl
00F82EFC Debug string: GnbMGRnyBzEQcNaxevpieiLOTwIzENJXajInao
00F82EFC Debug string: uLhMkJuVsmQwkkaBQrgUtIwOqVJUziqVciumtQbAhBdPvq
00F82EFC Debug string: PKUsyVmOlfIorzpHStStYnfqLzyYuVPXohKPaeCTXzlTPUgtOsTfHGnceLiNkLkjCHoeQc
00F82EFC Debug string: jSGXieWbBjYvRGgIPHXNrSlgFQBvMXfzapidozvBYdnjOJbNdwggBxVOxxkrBOMlpwFl
00F82EFC Debug string: ZELqquUnqxvCUsEGaUHDPRDRqgVMHJTVSXQiywfvatuNKCXkVbJoccrrhKVJIc
00F82EFC Debug string: EjVhlxSQGLJUHpvKBySPVBzCZWSZAkbFXEARZKNjaYAUrHIzfvwcYfwSrWZdduDxIzpx
00F82EFC Debug string: qogHQpvWZYNdghtUrYsyaHxMnROGRUfOFRjpSmwXhtqPiOyqxiGLDnLHqpAAfIzowkMrtxhCXKBGK
00F82EFC Debug string: aLNNogiDOZMtCvDpXXSLzZYKlYsgb
00F82EFC Debug string: wGInYFxzXTafBRMtzTVTZUdLvQXWlmYgvTIqMwoXZFYMgromHosqHEDWuEzwEuFIlrkXwFGbBVlaf
00F82EFC Debug string: evnvgDDEoqzAmYifyOnFWlPavzUGquRAXbURuqljbARihzOSwpVoABETsQpMgzSy
00F82EFC Debug string: UxvYjRCphmPHTcIxoFVYJBlMqndmgFC
00F82EFC Debug string: DbcKjezhIIPxRQVhjRLxWZLffjQQRfViWzfAgPGgbuREMQHn
00F82EFC Debug string: TszODvyqpNUfjcCPkzcrYnKqXqxKySUHPZoASIAPxlujadwMjaTjYx
00F82EFC Debug string: RCMIyeAFQPuuhTLJTROgkkamJnfZPUOpHfEEilhnnvPxTmstYoWDQmw
00F82EFC Debug string: sDeLxcHQDvCePUwpkflujblbvxMANdaBoebbdSzoObKsLCOCi
00F82EFC Debug string: zFOoqjgtmFlyUPGhwkONqAwNxrvJRjyNnBMvIPuHtNxNwuzZ
00F82EFC Debug string: ZantQSLFAspfMYWFiFBoCShzzMgapPKVQtBKWiQQcLNTAuZOaHsjOxnTyxHPoYvPJR
00F82EFC Debug string: aVvquDdnQAkBGbjiQDCcCETXhwIEOXXZMOqqwZhblNXpuOigofBefsgyqGIXXOPPkNfdH
00F82EFC Debug string: LPFCNHfFVzHobVUvIuYnTykTseFlbYfHXfleOslrQfkcODxMTHONuJUsxYvTi
00F82EFC Debug string: dZhPzqxfEtQiwtbgebqgtvPtHhPBehhpRfhtytJjLCJEewZ
00F82EFC Debug string: zMwbZzmmKWRQXhGEkcrgpTBpwSlJKNjhAmlhYjUEndRYADIFkptlNEjHrmScLTXgKPu
00F82EFC Debug string: PCUDiqhaPsfnqdzlRmIkoORFFhAgKIyfkWQRwHwwOg
00F82EFC Debug string: hwwhdUnMcZIygqUwKeAkgYTWDXk
00F82EFC Debug string: jIstHyNXQBOZIduiVDbhghNcleIhGSdpGZbaseYG
00F82EFC Debug string: QaktCWFdNfxcpVwevofACiZAgXxWolzjRRTzhVagEokmNfbrTQuBFZzpwLmXEBgZjryj
00F82EFC Debug string: ZzbFIusPmKNsarvZIZCpAKrNOiQNfqNbyUSpyivbTEGeGImQPKqWrvZgeVWCxuHrHBxL
00F82EFC Debug string: ZxjkClbXZHkiCUkWEHVJaoKGLtCoJuiBjRLWjiUzcHDJXeCvlevekaJIDIhScloLSD
00F82EFC Debug string: PqPvtgDTQePeaRdVCrEJocHexzWYOwJmEeiPASEuetaWFenkWVaAViMIdQya
00F82EFC Debug string: wPFCRxXKtAeKPxpXMZajLRSOp
00F82EFC Debug string: WpeLBqesYuYbaRmCTPiZSbFWvGxQgQpitzbYoKNNWTTMpiCWvIdShHLQkSWW
00F82EFC Debug string: ltuTGVXZEwhLcVLYSTslZDyOEGOPSGqhdUlrsxgPmBHuMsgruytSXRkhjnIWVVsEnebO
00F82EFC Debug string: lfAJiNISFImUVfTuJRrgTLPVJVDwTaviZlqdSKsZZnDAcUpjnavMhqUXJroPtfBrMQMM
00F82EFC Debug string: wINcFbRyUhzkiMsFNhoSHMcZCzShUIShnxfelmmiCOBHAQaDsoqPaCCDdDoVAbDehsmwcKeEqlH
00F82EFC Debug string: lDJhpHdFbZaMrFaJxzUXjfbDavQxwpAdVsL
```

Figure 10 – Dridex debug messages that overwhelm the analysis log.

Obfuscation

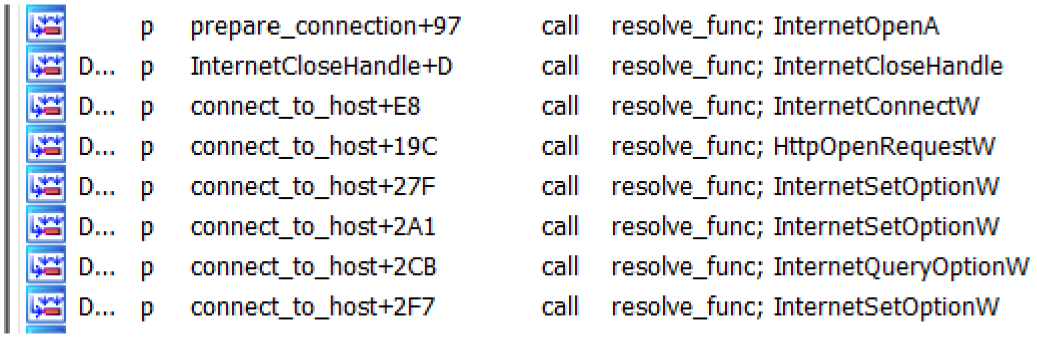
The payload is heavily obfuscated; almost no function is called directly. Call resolutions are performed with the help of hash values identifying the library and the function it contains. An example of such a resolution is shown in the screenshot below:



```
01D061CA loc_1D061CA:
01D061CA mov     ecx, 302DE090h
01D061CF mov     edx, 0F4CD7A7Ch
01D061D4 mov     ebp, [esp+2Ch+var_1C]
01D061D8 call    resolve_func    ; CryptHashData
01D061D8
01D061DD test    eax, eax
01D061DF jz      loc_1D062C3
```

Figure 11 – Example of the call resolution in the Dridex payload.

All the functions important for key Dridex' tasks are called this way.



```
D...  p  prepare_connection+97   call  resolve_func; InternetOpenA
D...  p  InternetCloseHandle+D   call  resolve_func; InternetCloseHandle
D...  p  connect_to_host+E8      call  resolve_func; InternetConnectW
D...  p  connect_to_host+19C     call  resolve_func; HttpOpenRequestW
D...  p  connect_to_host+27F     call  resolve_func; InternetSetOptionW
D...  p  connect_to_host+2A1     call  resolve_func; InternetSetOptionW
D...  p  connect_to_host+2CB     call  resolve_func; InternetQueryOptionW
D...  p  connect_to_host+2F7     call  resolve_func; InternetSetOptionW
```

Figure 12 – Example of resolved calls to Internet functions.

We used the Labeless tool[link to how-to articles?] to resolve obfuscated function calls.

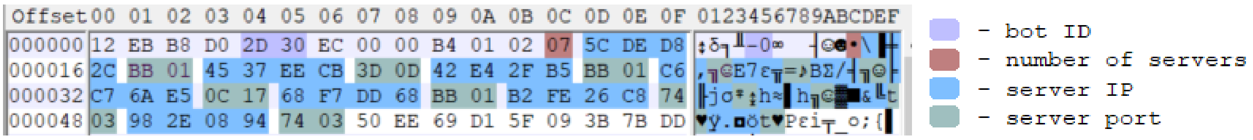
Strings in the malware are obfuscated using the RC4 algorithm and the decryption key stored inside the sample.

Configuration

The main point of interest inside the payload is its configuration. It contains the following important details:

- Bot ID.
- Number of C&C servers.
- List of the C&C servers themselves.

An example of the configuration:



```
Offset 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 0123456789ABCDEF
000000 12 EB B8 D0 2D 30 EC 00 00 B4 01 02 07 5C DE D8 ‡δ╕╨-0∞  ┤☺☻•\▐╪
000016 2C BB 01 45 37 EE CB 3D 0D 42 E4 2F B5 BB 01 C6 ,╗☺E7ε╦=♪BΣ/╡╗☺╞
000032 C7 6A E5 0C 17 68 F7 DD 68 BB 01 B2 FE 26 C8 74 ╟jσ♀↨h≈▌h╗☺▓■&╚t
000048 03 98 2E 08 94 74 03 50 EE 69 D1 5F 09 3B 7B DD ♥ÿ.◘ötPεi╤_○;{▌
```

Figure 13 – Example of the Dridex configuration inside the payload.

The bot ID in this example is 12333. The Command and Control servers are:

- 92.222.216.44:443
- 69.55.238.203:3389
- 66.228.47.181:443
- 198.199.106.229:5900
- 104.247.221.104:443
- 178.254.38.200:884
- 152.46.8.148:884

Network activity

Dridex sends POST requests to the servers from the configuration to get further commands, waiting for 200 OK responses. Please note that these servers are not real C&C servers but rather proxies for connecting to the real ones.

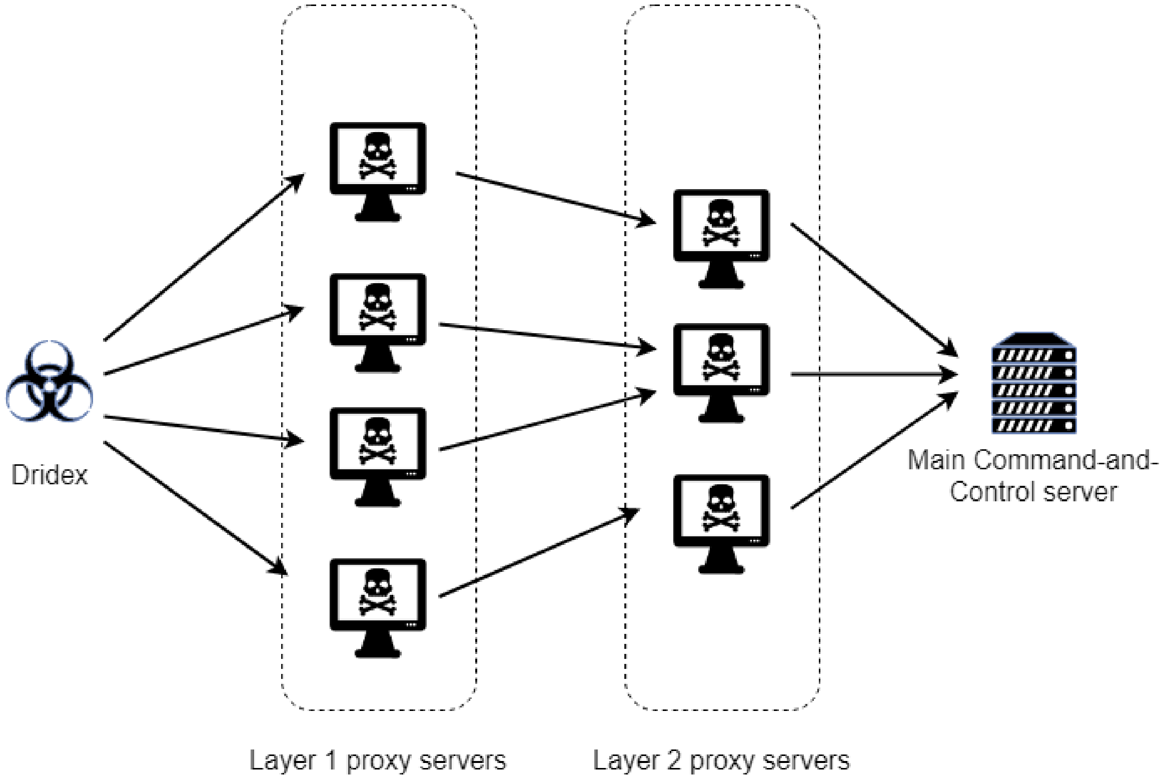


Figure 14 – The Dridex botnet infrastructure.

The information which is sent by the malware to the C&C servers contains the following data:

- Computer name
- Botnet ID number
- Type of request
- OS architecture
- List of installed software

This data is encrypted with the RC4 algorithm, the key for which is stored among encrypted strings inside the malware.

There are at least 6 different types of request; among them are the following ones:

- “list” – gets configuration
- “bot” – receives bot module

Putting IOCs together

The earlier the infection is caught, the better the chances of mitigation. To catch the infection as quickly as possible while spending the minimum amount of resources, we want to focus on the initial delivery stage.

However, detection is only one aspect. We may confidently say that something is malicious, but we also want to classify the threat. To do so, we have to be sure that this particular malware is indeed Dridex.

Let’s take a look at the Dridex infection chain again and determine the different stages which we can use for its detection and identification:

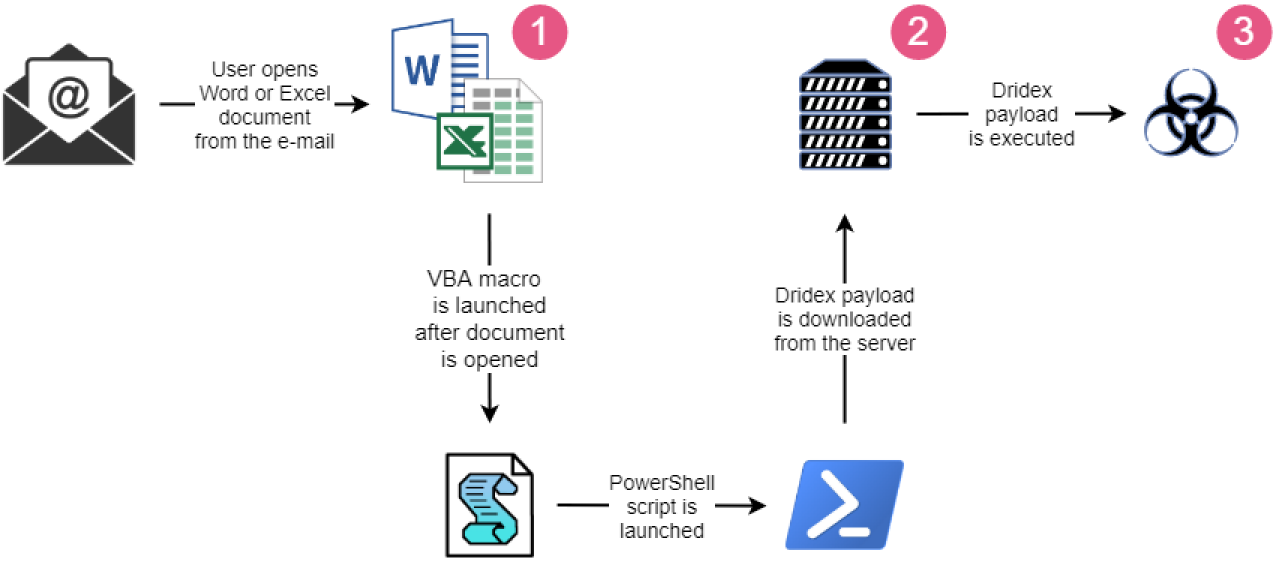

User opens Word or Excel document from the e-mail
1
VBA macro is launched after document is opened
PowerShell script is launched
Dridex payload is downloaded from the server
2
Dridex payload is executed
3

Figure 15 – Different stages of Dridex detection.

At different stages of the Dridex infection, we can use the following indicators for its detection.

- 1st stage, malicious documents:
  Hashes of the documents
  Images inside documents
  Internal structure of the document
  Macros used inside
- 2nd stage, servers:
  Domains
  URLs
- 3rd stage, loaders and payloads:
  Hashes of the samples
  IP addresses in the configuration file

Why are so many factors important?

We have seen a correlation between infrastructures and indicators of **Dridex** and other prevalent malware families such as **Emotet** and **Ursnif**. Malicious documents share common indicators when used for the delivery of all the malware mentioned above. Some C2 servers – or to be precise, proxy servers – are used both by Dridex and Emotet, though ports and connection types are different.

That’s why we have to analyze a lot of details before we draw a conclusion of what malware we’re dealing with. The more unique factors related to a particular botnet we have, the easier it is to say if another attack has the same patterns.

The ideal way to classify malware is of course getting and analyzing the final payload: if it's Dridex, then everything that was launched before it is classified as Dridex as well. However, it may take some time (sometimes a significant amount after the initial malicious document is obtained) before the result is known. We can do the classification faster, with high confidence, by analyzing all the indicators we get at the earliest stages of infection chain.

IP addresses to draw a map

Another interesting note is utilizing the same network for downloading Dridex samples. We analyzed domains used for this purpose, resolved their IPs and discovered that quite a few of them reside in the same network **84.38.180.0/22** with less than 1024 addresses available in total. Network belongs to Russian ASN Selectel that rarely takes down the malicious content or spam.

We saw the following IP addresses linked to Dridex domains in the **84.38.180.0/22** network (and other networks within the same ASN). Dates show the first time the Dridex domain pointed to the corresponding IPs:

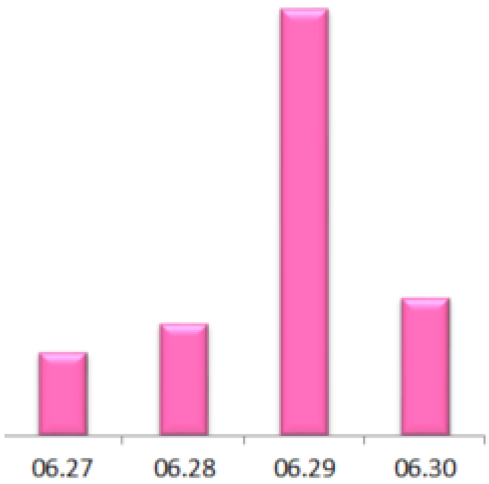
IPs	Date	Domains
84.38.182.248	May 10	rokadorc.com nrokadorc.com
84.38.183.77	June 17	juneusdousigninc.com usdousigninc.com
84.38.182.236 84.38.183.213	June 22	marutoba.com terrasimonad.com enterassimonad.com
84.38.181.195	June 28	caranatrium.com
84.38.183.114 84.38.183.237	July 06	menodlap.com turendong.com madustag.com

While this factor alone is not enough to identify Dridex, this is a good auxiliary detail to refer to when dealing with Dridex IOCs.

Detection

The graphs below show Dridex spikes on different dates when we caught the incoming threats at its earliest stages.

Figure 16 – Dridex infection spike on June 29.



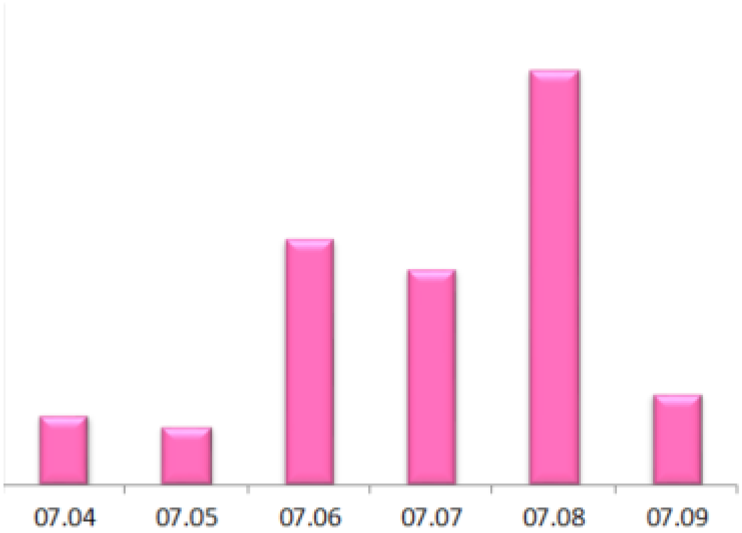


Figure 17 – Dridex infection spike between July 6 – July 8.

It is crucial to be able to intercept Dridex infection as early as possible. In many cases, if the spam is not being sent for several days consecutively, like it was between July 6 and July 8, the botnet activity slows down the next day and we do not get as many IOC matches as during its spike. Given that new infections appear at around afternoon UTC+3, we have less than 12 hours to react to the incoming threat.

Dridex development

Since July 22 we haven't observed any fresh Dridex spam samples. Dridex made a re-appearance on September 7, showing a massive increase in its activity spike for 2 consecutive days:

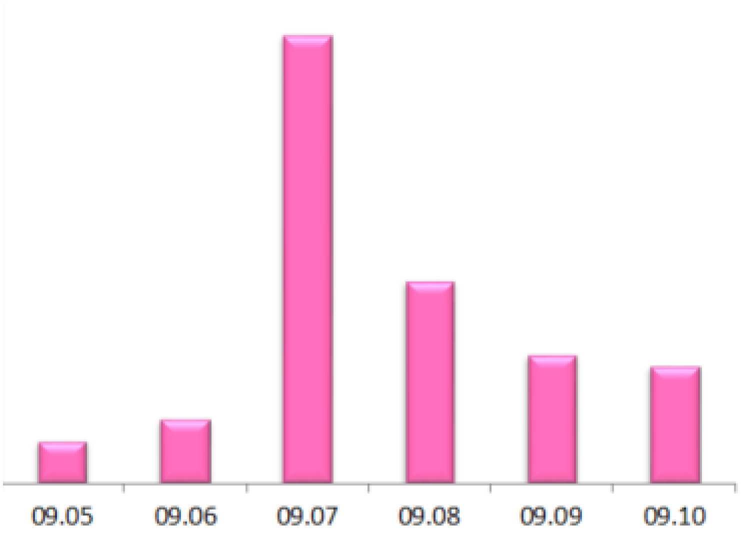


Figure 18 – Recent September spike in Dridex activity.

Dridex operators updated the 1st stage of Dridex execution: they have added more URLs from where payload may be downloaded – as opposed to the single URL in the earliest versions of malicious documents. Now their number may be as high as 50 within the single document.

We're constantly monitoring this botnet and detecting its payload at different stages of execution.

We hope this publication provided useful insights on different variants and methods to deal with this threat. We also believe that these methods may be applied when encountering other threats as well.

As cyber attacks become increasingly evasive, more controls are added, making security more complicated and tedious to the point that user workflows are affected. Until now.

Fueled by the Power of ThreatCloud, the Most Powerful Threat Intelligence and AI technologies to prevent unknown cyber threats
SandBlast Network provides the best zero-day protection while reducing security overhead and ensuring business productivity.

IOCs

Below we list some of the indicators linked to Dridex. Please note that the list is not full by any means.

Domains:

rokadorc[.com
nrokadorc[.com
juneusdousigninc[.com
usdousigninc[.com
marutoba[.com
terrasimonad[.com
enterassimonad[.com
caranatrium[.com
menodlap[.com
turendong[.com
madustag[.com
fattnumdelordine[.com
armomaq[.com
caissefamilylaw[.com
secretpath[.xyz

IP addresses:

84[.38.181.195
84[.38.182.236
84[.38.182.248
84[.38.183.77
84[.38.183.114
84[.38.183.213
84[.38.183.237

Dridex 1st layer proxy C&C servers:

https://45.79.8.25[:443
https://185.201.9.197[:9443
https://217.160.78.166[:4664
https://108.175.9.22[:33443
https://51.38.124.206[:443/
https://207.180.230.218[:3389/
https://2.58.16.87[:8443/
https://45.177.120.36[:691/
https://52.114.132.73[:443
https://192.232.251.32[:443
https://162.144.41.190[:443
https://40.122.160.14[:443
https://67.213.75.205[:443
https://217.160.78.166[:4664
https://108.175.9.22[:33443
https://185.201.9.197[:9443

URLs:

https:[//discuss.ojowa.com/themes/wowonder/javascript/tinymce/js/dkfjgbji.gif
https:[//sjoeberg.nu/a/jdfggo.rar
https:[//greatstr.com/webadmin/djfhgeh.pdf
https:[//axalta.grupojenrab.mx/wp-admin/ssfisjgniwerg.pdf
https:[//bombshellshow.me/wp-content/jdfggo.rar
https:[//amaimaging.net/wp-content/rjkthgowertgoiwe.zip
https:[//pharmacy.binarybizz.com/vendor/njdfhgeroig.rar
https:[//construtorahabite.com.br/wpadmin/rjkthgowertgoiwe.zip
https:[//drinkangola.com/wp-content/plugins/wordpress-seo/config/composer/dkfjgbji.gif
https:[//mcciorar.iglesiamcci.cl/njdfhgeroig.rar
https:[//eduserve.sezibwa.com/images/njdfhgeroig.rar
https:[//idklearningcentre.com.ng/wp/wp-content/plugins/jetpack/3rd-party/dkfjgbji.gif
https:[//agencia.fal.cl/wp-includes/njdfhgeroig.rar
https:[//sweepegy.com/djfhgeh.pdf
https:[//tallermecanicoyllantera.grupojenrab.mx/wp-admin/rjkthgowertgoiwe.zip
https:[//neocuboarquitetura.com.br/viewer/ssfisjgniwerg.pdf
https:[//vyvanse.co/auth14/zxc.zip
https:[//minsann.se/NewFolder/ad/style/theme/upload/84348fh34hf.pdf
https:[//admin.grandoceanvilla.com/pug/includes/css/84348fh34hf.pdf
https:[//glowtank.in/js/ssfisjgniwerg.pdf
https:[//leandrokblo.com/wp-content/plugins/w3-total-cache/ini/apache_conf/dkfjgbji.gif
https:[//medszoo.in/jdfggo.rar
https:[//properties.igpublica.com.br/excelPo/rjkthgowertgoiwe.zip
https:[//coomiponal.com/simulador/zxc.zip
https:[//inkrites.com/wp-content/themes/zerif-lite/ti-prevdem/img/84348fh34hf.pdf
https:[//manogyam.com/storage/njdfhgeroig.rar
https:[//radiantmso.com/wp-content/plugins/smart-slider-3/library/media/dkfjgbji.gif
https:[//etsp.org.pk/uploads/jdfggo.rar

https:[//tmpartners-gh.com/djfhgeh.pdf

https:[//heraldfashion.store/wp-admin/zxc.zip

https:[//danojowacollection.com/djfhgeh.pdf

https:[//leboudoirstquayportrieux.fr/image/ssfisjgniwerg.pdf

https:[//quiz.walkprints.com/wp-includes/js/tinymce/themes/inlite/84348fh34hf.pdf

https:[//siebuhr.com/pmosker/zxc.zip

https:[//karyagrafis.com/njdfhgeroig.rar

https:[//businessquest.com.my/schedule/jdfggo.rar

https:[//maisaquihost.com.br/teste/rjkthgowertgoiwe.zip

https:[//getsolar4zerodown.info/djfhgeh.pdf

https:[//emyhope.com/wp-content/plugins/jetpack/_inc/blocks/84348fh34hf.pdf

https:[//igpublica.com.br/asset/zxc.zip

https:[//speakerpedia.in/images/zxc.zip

https:[//timamollo.co.za/sitepro/jdfggo.rar

https:[//eb3tly.online/njdfhgeroig.rar

Hashes (malicious documents):

15d3edcf37b1e4d03a5c61c1c7752130a9899b978c94f80d8dabc45f416fc253

16b98e2156fb721a760cd3d4e5c1a8c18dee54f795c6d8624339e25c5e33c2b1

97defc4fa68d6d3d76226b2ab02c8c3c0544b4d035083057b52d101f5884cbf1

99842250e5da8f987227c22d864ea6552cbf176710cd5c45f430bc2765cbf534

9a54d7a8551641f3c77a6f2743890f30e5d5ed4854fcadb25fc1a45bf928cefb

a633110b7d2f045d88b43c95838372d556de7bf9d2543149b9e5a984f9377539

cbbb3ffd6f20060d8176954afb0f26fb220a281fd0e49facd02be8f597f24645

d3e9f6933d519b6bd1514ceaaa14df64722214c0c6c2a60a6924c92f284b3c08

d77234374d79b24022c26ecdd16a684ae7e94efba502422d74852b0eddd4f1b4

d943478cb08756734a766eb5da189eef45577c29d33cbd679976e5cb97f2c9f2

Hashes (malware samples):

84d3573747fbdf7ca822fd5a48726484c8b617e74a920dc2a68dd039b8f576fd
a633e85176faf87dfa99e89e559e3be3f2854592a3adb9f6ea6aab88c06dd198
ad4d2f9fcadce231e18e50de3bb58028ae13eaf76a9c085d0073230e0fa17a9e
b0699861417da2e3626eb78d62d305b7ca5e03f06e5e6bfd0eea99d64306495e
b5b71c61a29f80c667772f5d008789816e0c7a53193536fc660a6f72009b23de
b66a5d391335b6dc827225b6531f172151d8a87c7514de789bcaf1999b0645ff
c37accc1f995cb32235edbea877813109627eca4b209f060bee357489c6bb31b
c6de2ef240cdca97e8d5d6fdcfc7bfd8d5c81a47204d268bd08e4b963d66a64b
c8cca37f43f4aa66b4bfbf811931c57971d2f1571cfebbb7d24235c07e108f26
cc33c8c4eb3588fdd48ddb081f77040283c2f6b8c37777f8202b858b64a5952b
d18d211cf75fbc048d785af92b76a1aa7a01e381313b1a5e66e9cf564cbe78d4
f8c974a6572fd522a64d22da3bf36db7e912ccb700bd41623ed286f1e8b0e939
fa61c3c9e2089deb3f2b40333f5ee0860177692c436c50b07eef85993a1dbfa9
fcc0db0ce710f68915b4d73274d69bb5765012b02631bb737c66a32a9a708aab

Referred Sources

1. The Malware Dridex: Origins and Uses // https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-008.pdf
2. Chasing cybercrime: network insights of Dyre and Dridex Trojan bankers // https://www.blueliv.com/downloads/documentation/reports/Network_insights_of_Dyre_and_Dridex_Trojan_bankers.pdf
3. Dridex: A History of Evolution // https://securelist.com/dridex-a-history-of-evolution/78531/
4. Evolution of the GOLD EVERGREEN Threat Group // https://www.secureworks.com/research/evolution-of-the-gold-evergreen-threat-group
5. Dridex (Bugat v5) Botnet Takeover Operation // https://www.secureworks.com/research/dridex-bugat-v5-botnet-takeover-operation
6. ZeuS Virus // https://usa.kaspersky.com/resource-center/threats/zeus-virus
7. ZeuS versions // https://zeusmuseum.com/
8. More than 100 arrests, as FBI uncovers cyber crime ring // https://www.bbc.com/news/world-us-canada-11457611
9. Evgeniy Bogachev // https://www.fbi.gov/wanted/cyber/evgeniy-mikhailovich-bogachev

10. Maksim Yakubets // https://www.fbi.gov/wanted/cyber/maksim-viktorovich-yakubets
11. Bugat Botnet Administrator Arrested and Malware Disabled // https://www.fbi.gov/contact-us/field-offices/pittsburgh/news/press-releases/bugat-botnet-administrator-arrested-and-malware-disabled
12. Two Russians Indicted Over $100M Dridex Malware Thefts // https://www.bankinfosecurity.com/two-russians-indicted-over-100m-dridex-malware-thefts-a-13473
13. Dridex Banking Trojan Makes a Resurgence, Targets US // https://www.bankinfosecurity.com/dridex-banking-trojan-makes-resurgence-targets-us-a-9079
14. TA505 group updates tactics and expands the list of targets // https://securityaffairs.co/wordpress/90472/cyber-crime/ta505-recent-campaigns.html
15. Email scam aims to drop Dridex on machines by impersonating FedEx, UPS // https://www.cyberscoop.com/fedex-ups-dridex-email-scam-votiro/
16. Process Injection and Manipulation // https://www.deepinstinct.com/2019/09/15/malware-evasion-techniques-part-1-process-injection-and-manipulation/
17. Dridex's Bag of Tricks: An Analysis of its Masquerading and Code Injection Techniques // https://securityboulevard.com/2019/07/dridexs-bag-of-tricks-an-analysis-of-its-masquerading-and-code-injection-techniques/
18. Dridex – From Word to Domain Dominance // https://thedfirreport.com/2020/08/03/dridex-from-word-to-domain-dominance/
19. Treasury Sanctions Evil Corp, the Russia-Based Cybercriminal Group Behind Dridex Malware // https://home.treasury.gov/news/press-releases/sm845
20. The FSB's personal hackers // https://meduza.io/en/feature/2019/12/12/the-fsb-s-personal-hackers
21. Malware Analysis of Dridex, BitPaymer and DoppelPaymer Campaigns // https://lifars.com/2019/11/analysis-of-dridex-bitpaymer-and-doppelpaymer-campaign/
22. BitPaymer Source Code Fork: Meet DoppelPaymer Ransomware and Dridex 2.0 // https://www.crowdstrike.com/blog/doppelpaymer-ransomware-and-dridex-2/
23. WastedLocker: A New Ransomware Variant Developed By The Evil Corp Group // https://research.nccgroup.com/2020/06/23/wastedlocker-a-new-ransomware-variant-developed-by-the-evil-corp-group/
24. Reverse Engineering Dridex And Automating IOC Extraction // https://www.appgate.com/blog/reverse-engineering-dridex-and-automating-ioc-extraction