THE MALWARE DRIDEX: ORIGINS AND USES

17/07/2020

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION • ANSSI •

Sommaire

1 The malware Dridex

1.1 Changes in functionality since 2014

1.1.1 Functionality

Surfacing in June 2014, Dridex is the fifth variant of the banking trojan Bugat, active between 2010 and 2013 [1], enhanced with features specific to GameOverZeuS (GoZ) [2], which was active until 2014.

Its primary functionality is as a *stealer*, i.e. to steal online banking access codes[1], and enable threat actors to make fraudulent transfers from the compromised bank accounts. To that end, Dridex deploys at least three methods [3] :

- · Injection of an HTML script into the legitimate webpages of online banks that have previously been compromised, which displays malicious forms to customers asking them to provide their access codes;
- · Redirection towards a malicious page masquerading as the bank[2];
- · Interception of the server response from the bank's website and relay towards the threat actors' PHP server, which injects the code there.

1.1.2 Modularity

Dridex is made up of several modules, including:

- A *loader*, tasked with:
  - downloading a list of peers[3];
  - initial recognition within the information system (IS);
  - installing the payload;
  - downloading the additional modules.
- · A payload (also known as the *core module*, which contains the integrated functions and to which other modules may be added in order to expand its functionality.

The main functions integrated within Dridex's *core module* are as follows:

- A *keylogger*, which provides the threat actors with context about the victim (screenshots, keyboard input, etc.);
- Harvesting information and tampering with content on websites (web injection), via interaction with the Internet browsers. According to Bromium [4], Dridex is believed to have at least five *Web injection*[4] techniques.

This functionality can primarily be extended by the following modules:

- VNC: this module supplies *Virtual Network Computing* (VNC)[5] support for the threat actor's remote access to the victim's workstation;
- SOCKS: this gives Dridex a SOCKS proxy support[6];
- Pony: based on the Pony malware[7], this can steal access codes;

[1] As well as personal data and account balances.

[2] Technique previously leveraged by and most likely borrowed from the trojan Dyre.

[3] In the context of Dridex peer-to-peer pseudo-network operations.

[4] *DLL order hijacking, process hollowing, PE injection, thread execution hijacking* and *AtomBombing*.

[5] System for viewing and controlling the desktop environment of a remote computer, using the RFB protocol for communications.

[6] The network protocol *Secured over credential based kerberos* (SOCKS) enables a program to use the services of a firewall during an exchange with an external server

[7] Malware and controller of the botnet active since 2011, specialising in the theft of access codes and crypto-assets, but also in the distribution of malware, v1.9 of which leaked at the end of 2012 [5]. Pony has distributed such malware as GoZ, Necurs, Dyre, Vawtrak, Cryptolock and Cribit. In 2013, there were several Pony botnets.

- Kill OS: deployed across systems identified as belonging to researchers or automated malware analysis systems, it erases the *master boot record* (MBR) from the hard drive in a bid to sabotage the infected workstation;
- Spammer: this is harnessed to send spam emails;
- Email stealer: this is run to harvest the victim's emails.

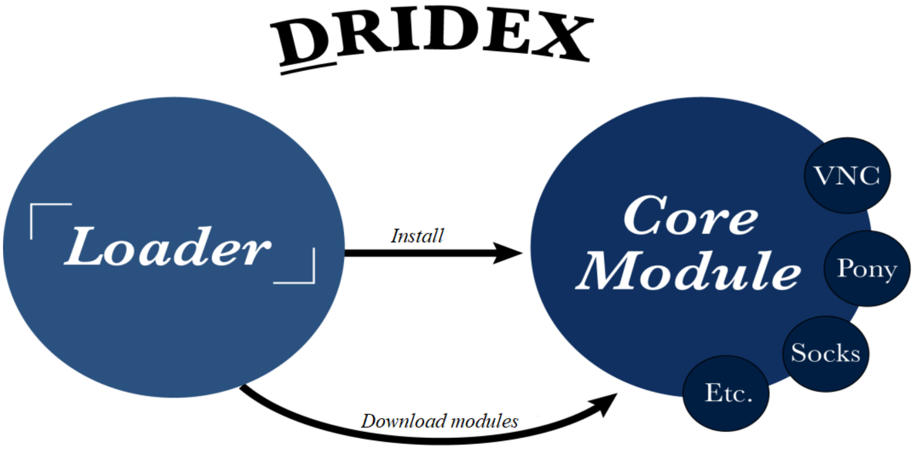


Fig. 1.1 : General composition

1.1.3 Development

Dridex is constantly being upgraded. Since 2014, its developers have added regular updates and patches. For example:

- In November 2014, Dridex embraced not only digital signature theft but also the P2P protocol [6].
- Dridex is the first known malware to have implemented, in February 2017, a new code injection technique discovered in October 2016, AtomBombing [4].
- Attack vectors are changing apace. Accordingly, the changeover from Dridex v3 to v4 in early 2017 came hand-in-hand with addition of the vulnerability 0-day MS Word (CVE-2017-0199)[8] [4, 7].

1.2 Botnet use

Dridex employs various Peer-to-Peer (P2P) botnets[9] [10] composed of workstations it compromises [9]. Their P2P architecture has three (*layers*), which makes the end *command and control (C2 backend)* machines more difficult to identify, so bolstering the infrastructure's resilience.

The *C2 backend*, otherwise known as the root infrastructure, contains the database and management logic of the botnet. It comprises around 24 servers [10]. It transmits new updates of the Pony, Kill OS, Spammer and Email Stealer modules to the *nodes*. The *C2 frontends* (*admin node*), which operate like *reverse proxies*, and comprise around 15 servers [10], communicate with the *nodes*, of which there are believed to be several hundred. These are composed of infected systems (bots) and represent the first communication layer in which the rest of the infected systems are in contact. They communicate together to maintain the network, extend it, distribute the VNC and SOCKS modules and transfer queries to the *C2 frontends*.

[8] Vulnerability enabling the concealment of malicious instructions in a document saved in .RTF format.

[9] For a clearer grasp of the notion of botnet, an assessment of the threat botnets pose can be found on the CERT-FR website [8].

[10] In botnets using this architecture, zombie machines do not communicate directly with the C2 infrastructure, but with other zombie machines defined in an updatable list of peers. As such, only a small number of machines are in contact with the C2 infrastructure run directly by the threat actor. These machines then relay the information transmitted by the C2 to the other infected machines featuring in their list, which will do the same.

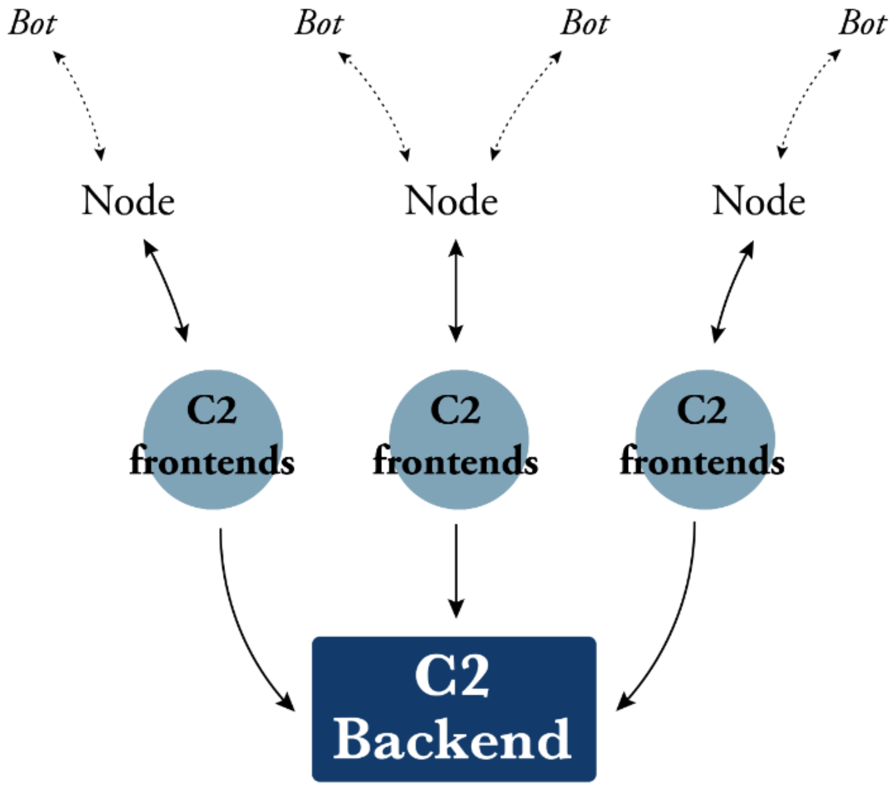


Fig. 1.2 : How the botnet Dridex works

Each bot (*peer*) can be identified within the P2P network via two IDs it generates: the bot ID identifies the infected user on a computer and the computer ID identifies the latter. In this way, multiple infections on the same computer can be detected. Moreover, each bot keeps a list of other *peers*, i.e. IP addresses and port numbers. In order to ensure this list remains active, the *peers* ask the *nodes* for updates at regular intervals.

Dridex' maximum infection rate is considered to have been reached over the 2015-2016 period. In 2015, the main countries to be targeted by Dridex were the UK, Italy and France, which had 1,804 bots. The United States was the next most common target [11].

1.3 Affiliate model

While some banking trojans are sold alone and deployed by the customer, Dridex operates according to an affiliate model. Each affiliate has access to a subset of bots [12], while the group Evil Corp controls the *C2 backends* of the different Dridex botnets.

According to the Western District of Pennsylvania Court indictment against members of Evil Corp, the affiliates apparently purchase Dridex use from the group (e.g. for USD 100,000 in the case of one British mule[11] who became an affiliate), then funnel half of the profits along with USD 50,000 per week to the group so as to retain the privilege of being able to use it. In return, Evil Corp is said to provide technical support [10].

The affiliates are distinguished by:

- their botnet ID, i.e. the number attributed to the Dridex version associated with the subset of bots they manage. With these botnet IDs, the activity of each of the affiliates can be distinguished and different botnet IDs can be associated with the same operator [13]. For example, in 2015 Dridex had nine botnets supporting

[11] Individual who transfers illegally acquired funds via different bank accounts in different countries.

its ecosystem, the three most active being botnets 120[12], 200[13] and 220[14];

- their targets, both in terms of sector and geography: for example, in 2015, the primary target of botnet ID 120 was banks, and France was particularly targeted by botnets 220, 120, 302, 125, 322, 225 and 228 in 2016 and botnet 1011 in 2019 [9, 15];
- the chosen infection vector.

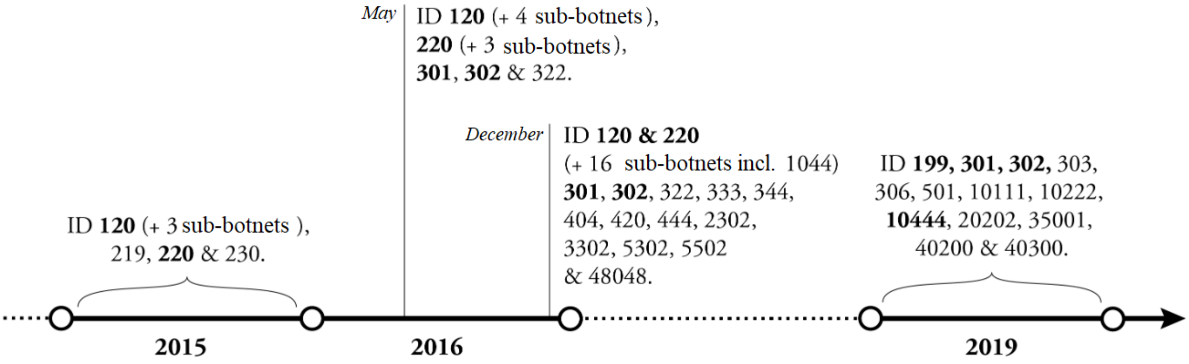


Fig. 1.3 : Main Dridex Botnet IDs from 2015 to today

[12] Which apparently contained 100,000 bots in May 2015 [10].
[13] Which apparently contained 750 bots in April 2015 [14].
[14] Which apparently contained 9,650 bots in April 2015 [14, 9].

2 Dridex' developers: Evil Corp

The names given in this chapter come from open sources and judicial documents that have been systematically referenced.

2.1 The group's origins: ZeuS, JabberZeuS and GameOverZeuS

In 2005-2006 or thereabouts, M. Bogachev (alias Slavik, lucky12345) created the trojan ZeuS (alias Zbot) (see Appendix 6.1). ZeuS was hired out as *malware-as-a-service* to other cybercriminal groups [16].

In early 2009, M. Bogachev began working with the cybercriminal group named "Business Club", allegedly led by M. Yakubets (alias Aqua) [17]. The group is thought to have called on Bogachev to collaborate on developing an enhanced version of Zeus capable of routing information to the threat actors on the compromised bank accounts, and particularly of notifying them when a victim signs in to their online bank account [18]. This version, enhanced by use of the XMPP (*Extensible messaging and presence protocol*) protocol, commonly dubbed Jabber [19], would be renamed JabberZeuS (see Appendix 6.2).

At the end of 2010, M. Bogachev claimed he was retiring, after reaping nearly USD 100m worth of profits during his five years in operation [20]. The FBI nevertheless published an indictment against M. Bogachev in June 2014, which would suggest that he continued his malicious operations.

In May 2011, Zeus' source code went public. To date, 447 variants of Zeus, associated with 27 families, have been identified [21].

In September 2011, a variant of ZeuS, Murofet (alias Licat), emerged, allegedly becoming the leading tool leveraged by members of the Business Club [17], and was soon after renamed GameOverZeuS (GoZ) (see Appendix **??**). In 2012, the botnet GoZ also distributed the ransomeware Cryptolocker.

In May 2014, the FBI-led Operation Tovar, supported by the Russian police [20], took down the infrastructure of GoZ and Cryptolocker, as well as the P2P network of the GoZ botnet. At the time, this included some 1 million bots, and was responsible for fraudulent transactions totalling tens of millions of dollars [18].

2.2 Evil Corp

2.2.1 2014: from JabberZeuS to Evil Corp

The banking trojan Dridex first appeared on the scene in June 2014[15]. Dridex is v5 of the malware Bugat, which surfaced in 2010, and is manifestly operated (perhaps even developed) by at least one member of the Business Club, Yakubets and Ghinkul, one of the operators of Troyak, the *bulletproof* hosting provider[16] (taken down in 2010) of Business Club [18].

A. Ghinkul (alias Smilex) [10], a Moldovan national, was arrested in August 2015 in Cyprus and extradited to the US [22], after Dell SecureWorks experts redirected the control points of the botnet Dridex towards a *sinkhole*[17] server, enabling the FBI to dismantle the associated infrastructure and pick him out from among 14 Dridex distributors. Ghinkul most likely belonged to the team administrating botnet ID 120.

[15] Two weeks after GOZ was taken down, the banking trojan Dyre also allegedly appeared. In addition to having the same developer as Gozi Neverquest, some attacks involving Dyre could be connected to the Business Club. It is quite possible, then, that the group branched out, harnessing Dyre to steal money from large business banking accounts, and Dridex to steal money from retail banking accounts. In November 2015, the arrest of Dyre's operators led to it becoming completely inactive [18].

[16] On the black market, criminals offer servers for hire that are remote from any jurisdiction. These are called *bulletproof* servers. Once hired out, a command centre can be installed in the server.

[17] *Sinkholing* involves redirecting data flow from zombie machines to a server outside the control of malicious operators.

Comment: it is interesting to note that, following Ghinkul's arrest, botnet ID 120 was not the only one to become temporarily inactive: botnet 220 associated with TA505 only resumed operations three months afterwards.

Despite this arrest, the Business Club, henceforth known as Evil Corporation (alias EvilCorp, Indrik Spider), headed up by Yakubets, has renewed its infrastructure and remained active.

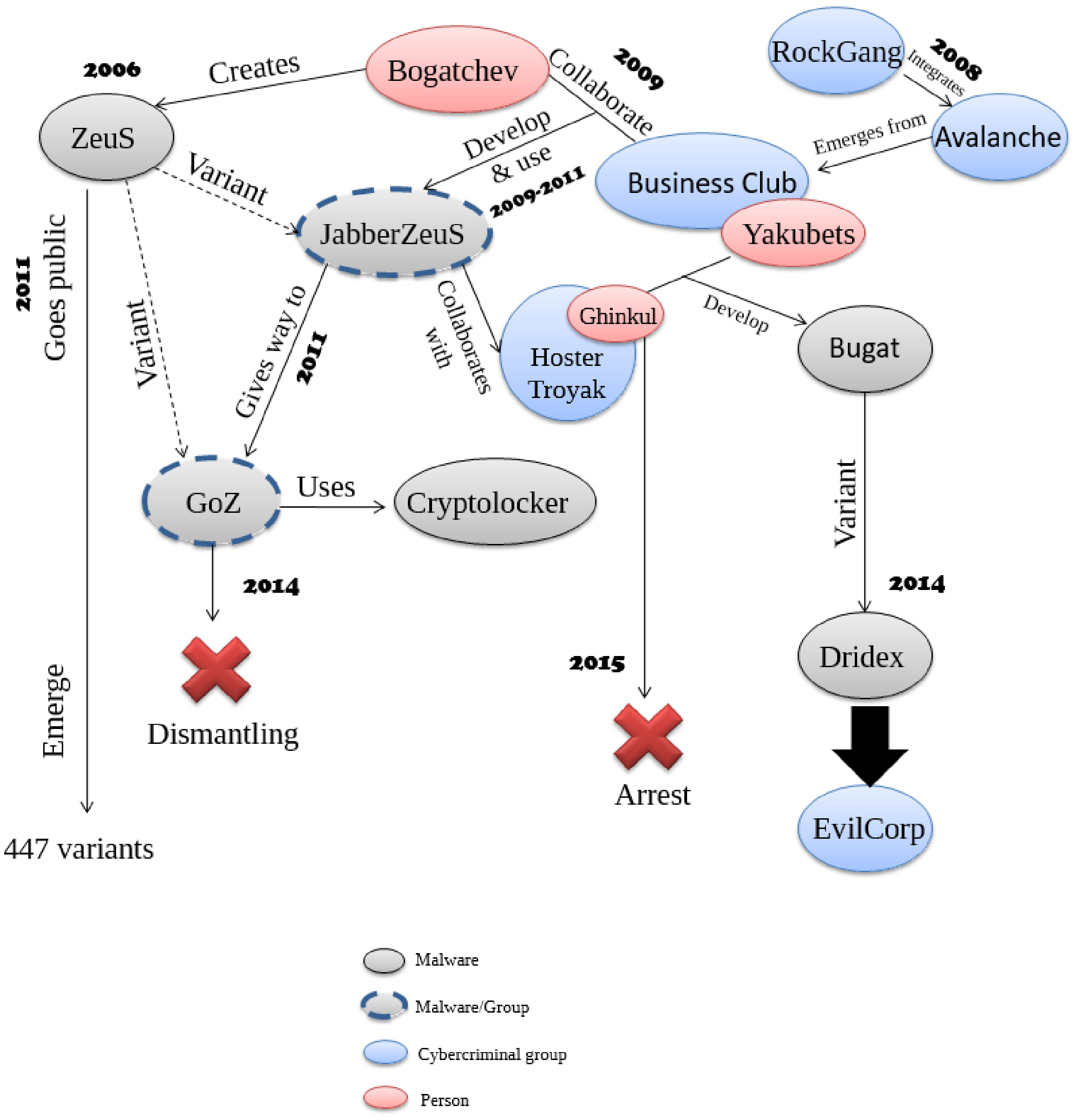


Fig. 2.1 : Mapping of links between Russian-speaking cybercriminal groups, from ZeuS to Evil Corp

In a joint indictment dated 5 December 2019, the US Department of Justice and Britain's National Crime Agency identified nine members of the group Evil Corp. In addition to M. Yakubets:

- I. Turashev allegedly acted as administrator of the malware Dridex and lent technical assistance to its operators;
- D. Gusev is accused of having materially and financially facilitated Evil Corp, with six Russian-based companies for which he was the General Director receiving sanctions on the part of the US Treasury [23];

- The six main remaining members of Evil Corp[18] have particularly been identified through posts on social media [24], most flaunting lavish spending sprees including luxury cars with “BOP” in the number plate (pronounced “VOR”, which means “thief” in Russian).

In addition to Dridex, Blueliv alleges that Evil Corp has also distributed other trojans including (*POS malware*) [25], as well as Carbanak[19] [26]. Evil Corp is most likely made up of two operational teams, each with *spammers*, i.e. individuals specialising in the distribution of phishing campaigns not only on behalf of Evil Corp but also other threat actor groups [27].

2.2.2 Evil Corp's development since 2017

The ransomware BitPaymer

Discovered in July 2017 [28], the ransomware Bitpaymer (alias FriedEx) first hit the headlines following its attack against Britain’s National Health Service (NHS), at a Scottish hospital, in August 2017.

Bitpaymer is a binary file, which means it cannot be distributed or log in to a C2 server of its own accord. Its operators therefore execute it manually. It has many code similarities with Dridex [28]. Moreover, a lot of attacks leading to encryption by the ransomware Bitpaymer have involved prior compromising by Dridex. Such connections suggest that Bitpaymer has been developed and operated by Evil Corp.

Bitpaymer represents a change in tactics on the part of Evil Corp, with precedence now given to a small number of highly profitable targeted attacks (*Big Game Hunting*) rather than its massive Dridex schemes run since 2014. In 2019, it appears that Evil Corp is now using Dridex no longer to commit bank fraud but to conduct recce operations on the ISs it compromises so as to determine whether or not it is worth distributing Bibpaymer on them [25]. Bitpaymer’s typical infection chain involving Dridex is as follows:

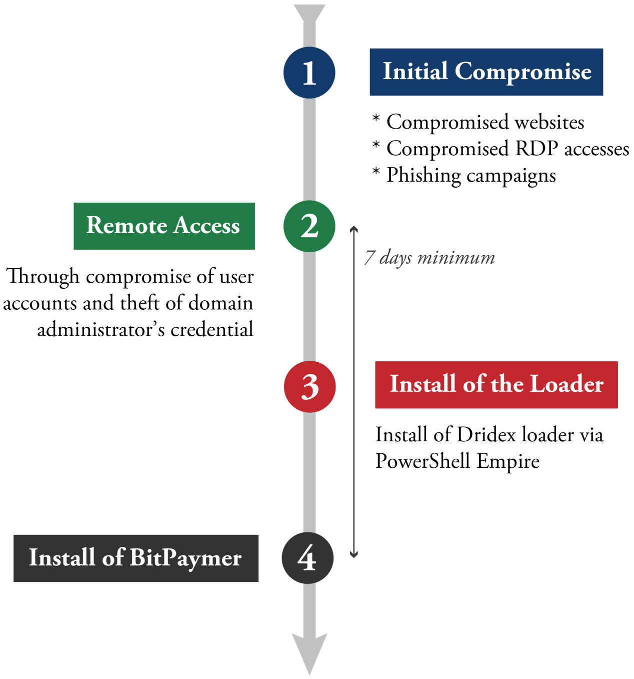

1
Initial Compromise
* Compromised websites
* Compromised RDP accesses
* Phishing campaigns
Remote Access
2
Through compromise of user accounts and theft of domain administrator’s credential
7 days minimum
3
Install of the Loader
Install of Dridex loader via PowerShell Empire
Install of BitPaymer
4

Fig. 2.2 : Bitpaymer’s infection chain involving Dridex

That said, Bitpaymer can also apparently be distributed by Emotet rather than Dridex (which is itself sometimes distributed by Emotet) [29, 30].

[18] Dmitry Smirnov, Artyom Yakubets, Ivan Tuchkov, Andrey Plotnitsky, Dmitry Slobodskoy and Kirill Slobodskoy.
[19] In 2016, there are even reports that Carbanak was sometimes downloaded by *Dridex loader* within infected ISs.

The indictment against Yakubets and other members of Evil Corp, published in early December 2019, does not seem to have dented the cybercriminal group's activities much, given the ongoing BitPaymer campaigns.

Split within Evil Corp

In April 2019, Evil Corp is thought to have split into two groups: Indrik Spider and Doppel Spider[20] [31]. While Indrik Spider allegedly ran the malware Dridex and Bitpaymer, as had been done since 2018, Doppel Spider purportedly executed a modified version of Dridex, DoppelDridex, as well as a variant of the ransomware BitPaymer, DoppelPaymer. In this way, it not only deployed banking fraud campaigns via DoppelDridex only, but also ransomware campaigns via DoppelPaymer.

Given that:

- the malware FakeUpdates distributed Dridex in October 2019, and that Dridex deployed either BitPaymer or DoppelPaymer within the victims' ISs [32],
- during a DoppelPaymer incident, FireEye detected the downloading of Dridex v4 botnet ID 501 (associated with Evil Corp), then of Dridex v2 botnet ID 12333 in a bid to deploy DoppelPaymer (associated with Doppel Spider) [32];
- Doppel Spider uses the services of Emotet [31], as does Evil Corp,

It would appear that the two groups are continuing to collaborate, or perhaps even that Doppel Spider is a subgroup of Evil Corp.

PHowever, since the first quarter of 2020, what distinguishes the operators behind DoppelPaymer from Bitpaymer's operators is that the former have started to publish the data exfiltrated from the IS of their victims (on the website www.doppleshare[.]top/), in the same way as operators of other ransomware (Maze, Sodinokibi, Clop and Nemty in particular) [33].

[20] Indrik Spider and Doppel Spider are two alias established by Crowdstrike.

3 Distribution of Dridex by the main affiliates

The infection vector comes across as the most discriminating characteristic of the different botnet IDs, and therefore of the different affiliates. That said, there is a risk of confusing the affiliate and the distributor chosen by the latter. For example, the operator of a botnet distributing the Dridex of a specific botnet ID must not be confused with the affiliate of the botnet ID in question.

3.1 Phishing emails

3.1.1 The botnet CraP2P (alias Necurs)

Active from 2012 to 2020, CraP2P is a botnet specialising in the distribution of phishing campaigns and malware, on behalf of various threat actor groups. Over this time, the number of bots making it up has risen to nine million. Any one of these bots was capable of sending out several million spam emails in the space of a few dozen days [34]. CraP2P was, for example, used by its operators to distribute GoZ in 2013, Cryptolocker in 2014 and Dridex from at least 2015 [35].

Over the 2015-2016 period, CraP2P was behind phishing campaigns particularly delivering Dridex botnets, ID 120, 122, 123, 220, 223 and 301. Whereas botnet ID 120 was associated with A. Ghinkhul until the middle of 2015, botnets 220 and 223 have been associated with TA505 [36].

According to Proofpoint [37], the cybercriminal group TA505 began using Dridex in July 2014, so a month after it was designed (June 2014). TA505 made fairly intermittent use of Dridex until June 2016 then completely stopped using it in June 2017. The botnet IDs used by TA505 between 2014 and 2015 to deploy Dridex are most likely 125, 220 (targeting the UK, France and Australia) and 223 (targeting Germany and Austria). TA505 reportedly then used botnets, ID 7200 and 7500 (probably in 2017).

Comment: Because TA505 used one of the three most active botnet IDs of the Dridex network (ID 220), it could have been confused with Evil Corp, whereas it was ultimately no more than a particularly engaged affiliate of the P2P network, and therefore, in effect, in close collaboration with Evil Corp.

It thus appears that the operators of CraP2P were working closely with Evil Corp and some of its affiliates in terms of distribution, which resulted from past collaboration with GoZ.

Comment: Some sources indicate that Evil Corp could be the operator of the CraP2P botnet, while others claim that this could be TA505. Without further evidence, it is only possible to confirm a close relationship between these different groups.

3.1.2 The botnet Cutwail

TA544 (alias Narwhal Spider) is a cybercriminal service provider believed to make the botnet Cutwail available for hire on Russian-speaking underground forums[21] [38].

Over the period it was active, GoZ rented access to part of the infrastructure of the botnet Cutwail to distribute phishing emails [39]. Its supposed successor, Evil Corp, is also thought to have called on the services of TA544 [40].

In 2019, the botnet Cutwail was distributing Dridex ID 1044 via phishing campaigns [41], primarily targeted at the United States, Canada and Australia. At least once in November 2019, the infection chain purportedly did not stop at Dridex, since the latter propagated the ransomware Hermès [22] [15].

Comment: It is not easy to tell whether TA544 is an affiliate of Dridex, or whether part of the botnet it operates is used by Evil Corp or one of its affiliates to distribute Dridex, making TA544 a distributor only.

[21] Botnet founded in 2007: GameOver ZeuS was apparently a customer in 2012.

[22] Used by Lazarus during the attack against the Far Eastern International Bank, Hermès is a ransomware that can be purchased on the Dark Web.

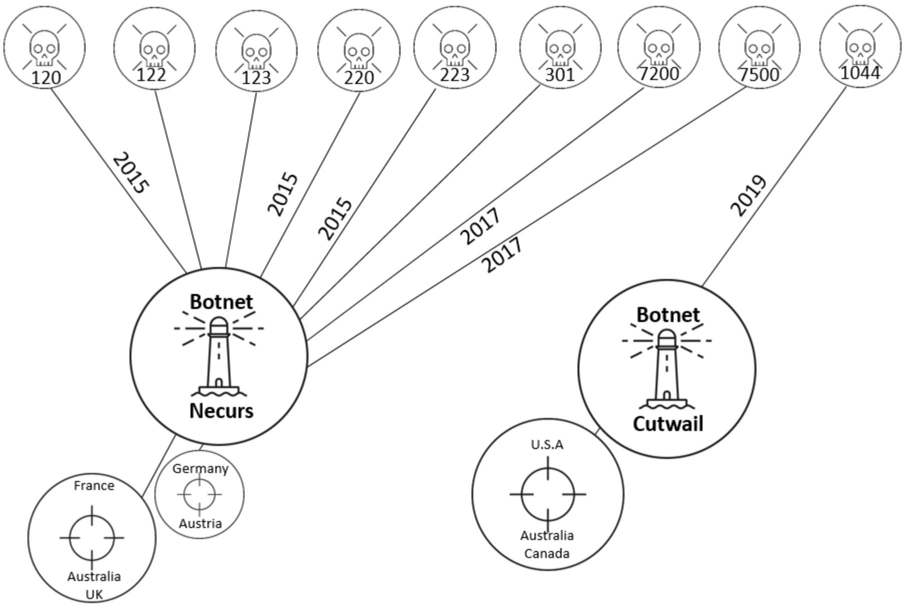


Fig. 3.1 : Distribution of Dridex via the botnets CraP2P and Cutwail

3.1.3 The botnet Andromeda

Before it was taken down in 2017, the botnet Andromeda (alias Gamarue) was tasked with distributing Dridex, particularly with the UK as a target in 2016 [13].

3.2 As a second payload

By Trend Micro's reckoning, the operators of Emotet, Gozi ISFB (alias Ursnif)[23] and Dridex likely share the same PE[24] *loader*[25], provider, and perhaps even exchange resources [29].

Emotet[26] has been able to propagate Dridex since at least 2017 [43]. Emotet has even been known to distribute Bitpaymer, the ransomware exclusively used by Evil Corp. The first connections between Emotet and the operators of Dridex, Evil Corp, were found in April 2017 [44].

Comment: Evil Corp appears to call on the operators of Emotet (Mummy Spider, Mealybug, TA542) to deliver Dridex as a second payload within the IS that they have already compromised. The operators of TrickBot (Wizard Spider) have the same modus operandi.

Regarding Gozi ISFB, TA551 (alias Shathak) used its loader RM3[45] to distribute Dridex botnets, ID 301, 302, 303, 3101 and 35001, in 2018 and 2019 [15, 46] across the US, Canada and Italy. During these same infection chains, Gozi v2 RM3 has sometimes been accompanied by the credential-stealing malware Predator the Thief [27] or ransomware GandCrab (occurrences in December 2018)[28].

[23] The original banking trojan horse Gozi was developed in 2006 as a competitor of the trojan horse ZeuS. The source code for Gozi leaked in 2010 and was co-opted by other cybercriminal groups to create other trojans, including Gozi ISFB, Vawtrak (Neverquest) and GozNim, a combination of Gozi IFSB and Nymain [16]. Version 2.13.24.1 of Gozi ISFB leaked in February 2015.

[24] Format of executable files and libraries on Windows operating systems, including .EXE (for programs) and .DLL (for libraries).

[25] The PE loader enables Windows to perform the instructions of a PE file.

[26] Banking trojan horse that surfaced in 2014, and became a *loader* of such malware families as TrickBot, Gootkit and IcedID from 2017. The operators of Emotet allow other cybercriminal groups to rent access to the workstations they have infected [42, 29].

[27] Malware sold on the Dark Web in June 2018.

[28] GandCrab may well have also been deployed at the end of 2018 during infection chains involving Dridex botnet ID 10202 and TA547, identified by Proofpoint as the operator of the banking trojan Danabot [47].

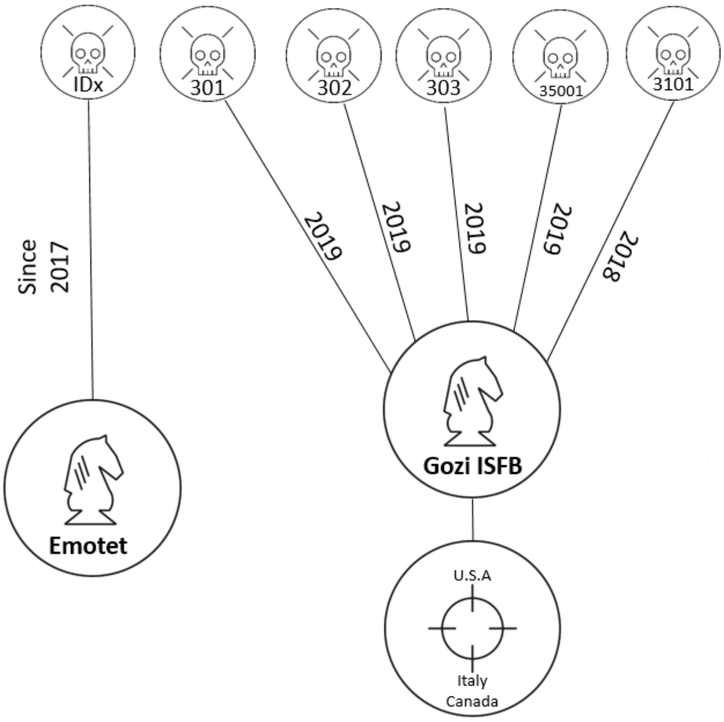


Fig. 3.2 : Distribution of Dridex as a second payload of Emotet and Gozi ISFB

3.3 Watering hole

Since 2019, Dridex v4 botnets, ID 199 and 501, are thought to be distributed via FakeUpdates (alias SocGholish)[29]. Watering hole attacks, or phishing emails pointing to a malicious URL, entail the display of a false browser update where the malware FakeUpdates would be installed followed by the propagation of Dridex and BitPaymer or DoppelPaymer [32]. Spanish IT service provider Everis System fell victim to one of these attacks in November 2019 [25]. In the case of DoppelPaymer, Dridex ID 12333 was reportedly downloaded on the IS after the latter was infected by Dridex v4 botnets, ID 199 or 501.

<u>Comment:</u> Logically, Dridex ID 12333 would thus be associated with Doppel Spider. Such would also be case for Dridex ID 40300.

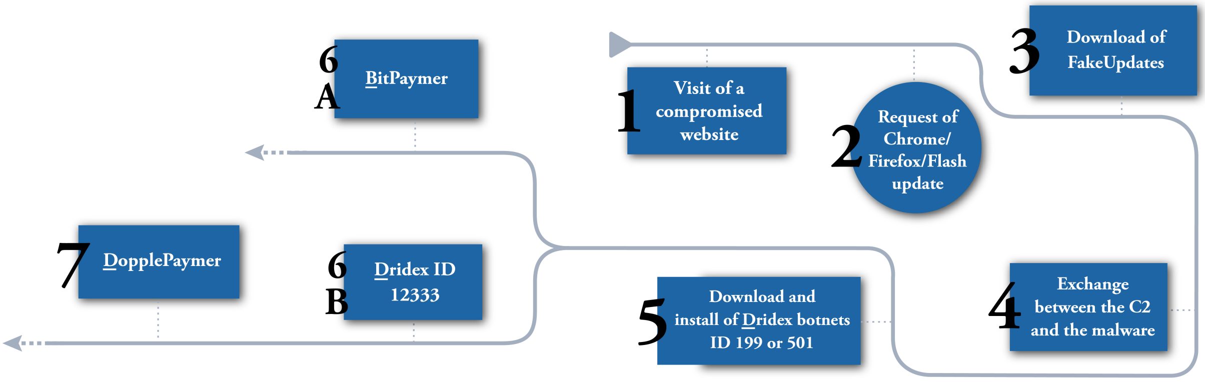

1
Visit of a compromised website
2
Request of Chrome/ Firefox/Flash update
3
Download of FakeUpdates
4
Exchange between the C2 and the malware
5
Download and install of Dridex botnets ID 199 or 501
6 A
BitPaymer
6 B
Dridex ID 12333
7
DopplePaymer

Fig. 3.3 : Dridex infection chain via FakeUpdates

[29] Dridex botnet ID 11122 was purportedly distributed in the same way in 2018.

These campaigns deliver, in turn, Dridex v4 botnets, ID 199 or 501, AZORult, Chthonic[30] and NetSupport RAT[31], illustrating the fact that Evil Corp calls on the operator of FakeUpdates, in the same way as other cybercriminal groups, in order to distribute Dridex then BitPaymer.

3.4 Exploit kits

In June 2019, the exploit kit Spelevo[32] delivered Dridex, as well as between September and November, concomitantly with the exploit kit Fallout [15], via compromised websites [52].

The exploit kit Fallout is thought to be the favourite infection vector of the affiliate corresponding to the botnet ID 10111, while the botnet ID 30102 tends to use the exploit kit Spelevo.

[30] Banking trojan resulting from the trojan ZeusVM, itself a variant of ZeuS, whose *builder* binary code leaked in June 2015 [48, 49], and itself based on the malware Zeus, whose source code leaked in 2011. Chthonic has been designed similar to Dridex with a module-based architecture, and shares three of its modules (Pony, SOCKS and VNC) [50].

[31] Legitimate remote access tool [51].

[32] This exploit kit is also known to have distributed the ransomware Maze.

4 Conclusion

The malware Dridex illustrates just how complicated it is to attribute attacks on account of the plethora of interconnected groups inhabiting the Russian-speaking cybercriminal ecosystem (providers, customers, botnet operators, etc.). Dridex has a manifold background (Bugat, GoZ), operators from myriad groups (Rock Gang, Avalanche, JabberZeuS), just like its affiliates, and is distributed via many different infection vectors, against a wide array of targets all over the world.

However, the string of indictments that have built up over the past decade against members of Evil Corp has helped to better pinpoint the group's activities, connecting individuals to cyberattacks and malware.

Be that as it may, Dridex remains a threat in the hands of Evil Corp, Doppel Spider and their current affiliates in particular, in the context of more targeted campaigns aimed at spreading ransomware.

5 Methods of detection

The compromise indicators indicated below may be blocked and looked for on an information system to prevent or detect attacks involving the malware Dridex.

IOC	Type	Comment
admin@belpay.by	Adresse courriel	Campagne Dridex
faber@imaba.nl	Adresse courriel	Campagne Dridex
s.palani@itifsl.co.in	Adresse courriel	Campagne Dridex
yportocarrero@elevenca.com	Adresse courriel	Campagne Dridex
tom@blackburnpowerltd.co.uk	Adresse courriel	Campagne Dridex
pranab@pdrassocs.com	Adresse courriel	Campagne Dridex
admin@sevpazarlama.com	Adresse courriel	Campagne Dridex
farid@abc-telecom.az	Adresse courriel	Campagne Dridex
bounce@bestvaluestore.org	Adresse courriel	Campagne Dridex
web1587p16@mail.flw-buero.at	Adresse courriel	Campagne Dridex
fabianurquiza@correo.dalvear.com.ar	Adresse courriel	Campagne Dridex
info@melvale.co.uk	Adresse courriel	Campagne Dridex
faturamento@sidestecaminhoes.com.br	Adresse courriel	Campagne Dridex
cariola72@teletu.it	Adresse courriel	Campagne Dridex
info@golfprogroup.com	Adresse courriel	Campagne Dridex
info@antonioscognamiglio.it	Adresse courriel	Campagne Dridex
http://owenti.com/fprl.exe	Domaine	Dridex
http://tamboe.net/frap.exe	Domaine	Dridex
http://owenti.com/fprl.bin	Domaine	Dridex
http://saitepy.com/glps.exe	Domaine	Dridex
http://klerber.com/glps.exe	Domaine	Dridex
http://fdistus.com/glps.exe	Domaine	Dridex
http://uprevoy.com/opxe.exe	Domaine	Dridex
http://typrer.com/qrpt.exe	Domaine	Dridex
http://urefere.org/opxe.exe	Domaine	Dridex
http://inesmoreira.pt/img/galeria/beloura/123.bin	Domaine	Dridex
https://masteronare.com/function.php?3b3988df-c05b-4fca-93cc-8f82af0e3d2b	Domaine	Dridex
urefere.org/opxe.exe	Domaine	Dridex
hxxp://bienvenidosnewyork.com/app.php	Domaine	Dridex
hxxp://photoflip.co.in/lndex.php	Domaine	Dridex
hxxp://everestedu.org/lndex.php	Domaine	Dridex
https://thinkunicorn.com/wp-admin/css/colors/fish/HraXJHWvJbyTvdLwdaAu/0ev7Bg.bin	Domaine	DoppelDridex (botnet ID 40300)
https://unfocusedprints.co.kr/HraXJHWvJbyTvdLwdaAu/0ev7Bg.bin	Domaine	DoppelDridex (botnet ID 40300)
62.149.158.252	Adresse IP	Dridex
177.34.32.109	Adresse IP	Dridex
2.138.111.86	Adresse IP	Dridex
122.172.96.18	Adresse IP	Dridex
69.93.243.5	Adresse IP	Dridex
200.43.183.102	Adresse IP	Dridex
79.124.76.30	Adresse IP	Dridex
188.125.166.114	Adresse IP	Dridex
37.59.52.64	Adresse IP	Dridex
50.28.35.36	Adresse IP	Dridex
154.70.39.158	Adresse IP	Dridex
108.29.37.11	Adresse IP	Dridex
65.112.218.2	Adresse IP	Dridex
47.254.236.15	Adresse IP	Dridex
194.99.22.193	Adresse IP	Dridex
194.99.22.193	Adresse IP	Dridex
178.63.67.20	Adresse IP	Dridex
5.127.14.171	Adresse IP	Dridex
34.213.221.29	Adresse IP	Dridex

209.40.205.12	Adresse IP	DoppelDridex (botnet ID 40300)
79.143.178.194	Adresse IP	DoppelDridex (botnet ID 40300)
188.165.247.187	Adresse IP	DoppelDridex (botnet ID 40300)
185.234.52.170	Adresse IP	DoppelDridex (botnet ID 40300)
107.152.33. 15	Adresse IP	DoppelDridex (botnet ID 40300)
199.101.86.6	Adresse IP	DoppelDridex (botnet ID 40300)
188.165.247.187	Adresse IP	DoppelDridex (botnet ID 40300)
176.10.250.88	Adresse IP	DoppelDridex (botnet ID 40300)
7239da273d3a3bfd8d169119670bb745	MD5	Dridex (botnet ID 199 ou 501)
72fe19810a9089cd1ec3ac5ddda22d3f	MD5	Dridex (botnet ID 199 ou 501)
07b0ce2dd0370392eedb0fc161c99dc7	MD5	Dridex (botnet ID 199 ou 501)
c8bb08283e55aed151417a9ad1bc7ad9	MD5	Dridex (botnet ID 199 ou 501)
6e05e84c7a993880409d7a0324c10e74	MD5	Dridex (botnet ID 199 ou 501)
63d4834f453ffd63336f0851a9d4c632	MD5	Dridex (botnet ID 199 ou 501)
0ef5c94779cd7861b5e872cd5e922311	MD5	Dridex (botnet ID 199 ou 501)
9aa3089af134627ef48b178db606268a	MD5	DoppelDridex (botnet ID 40300)
e614a69d706913376ab2bb20a703dcf5	MD5	Dridex
1d778359ab155cb190b9f2a7086c3bcb4082aa195ff8f754dae2d665fd20aa05	SHA256	Dridex (botnet ID 199)
abf99a028dae6812f6f0ca633d7424ce9272dfcfbebf6b518c1e6c97f872f3e7	SHA256	Dridex
6712500bb0de148a99ec940160d3d61850e2ce3803adca8f39e9fa8621b8ea6f	SHA256	Dridex
86bcfce2dd342e9a1c04cfc65731d40ed1c397a4ec47bd9f5b41771297d81100	SHA256	Dridex
005e77a55b8f1bf4049d6231c2349a01d019b46f47b6930103458a2aadd1bfa6	SHA256	Dridex
a1388cb3e6ae68a6130ae12f9db4881238c97718875a3362b6bc5788e61c6663	SHA256	Dridex
ca087f46f97cd465f46e4ccb04181e6eae7b2c751ae7fd9e262191b979728ccc	SHA256	Dridex
4ad0998882a3fbd3412f0c740faebb8ef78bec4c3e566650424c40a878e6a23a	SHA256	Dridex

Since Dridex is likely to download the ransomware BitPaymer and DoppelPaymer as a second payload, it may be worth focusing detection efforts on these codes in the event Dridex has been identified on the information system.

Because Dridex is also likely to be distributed as a second payload by malware families FakeUpdates, Emotet, Gozi ISFB , there may be equal merit in focusing detection efforts on these codes so as to stop the attack in its tracks.

6 Appendices

6.1 Appendix 1: Characteristics of the malware package ZeuS

ZeuS serves two key purposes:

- it turns its victims into zombie machines of the botnet bearing the same name;
- it can tell when its victim is signed into a bank's website and harvests the latter's account access codes. This enables its operators to transfer money from the victims' accounts to the accounts controlled by mules.

Its main functions are as follows [53] :

- targeted information theft: for example, in 2007 ZeuS stole information from the US Department of Transportation (the United States is its number one target [54];
- remote access via the VNC protocol;
- program downloading and running[33];
- deletion of key components for the functioning of the operating system in a bid to destroy the infected machine.

  Comment: The trojan Zeus would thus have been capable of sabotaging ISs, in the same way as Dridex through its module KillOS.

6.2 Appendix 2: JabberZeuS

The Business Club all began with the cybercriminal group Rock Gang, which operated from 2004 to 2008, and whose members were of Ukrainian, Russian, Romanian and Moldovan nationality [18]. In 2008, lots of Rock Gang's members reportedly began to use Avalanche, an extensive global network hosting infrastructure harnessed by different groups of cybercriminals [55]. Among them, some, united within the Business Club, allegedly called on M. Bogachev to help develop an enhanced version of ZeuS: JabberZeuS.

The new group formed around JabberZeuS includes some fifty individuals, whose privileges stem from their seniority and who work across several activities:

- fraud: to participate in fraud activities, membership fees must be paid and a profit-sharing agreement signed;
- recruitment of mules: some mules were located in two Chinese cities, adjacent to the Russian border, north of Vladivostok [17]. In September 2010, the network of British JabberZeuS mules was arrested during Operation Trident breACH[34] [18];
- technical support;
- provision of services: the group sold access to ZeuS (for USD 3,000 or 4,000 [20], not including modules) and to other trojans. Accordingly, in October 2010, the FBI, collaborating with its British and Ukrainian counterparts, dismantled a network of a dozen or so cybercriminals which had leveraged the malware Zeus to target US bank accounts and siphoned around USD 70m off them [56, 57].

Identified group members include M. Bogachev, M. Yakubets (particularly in charge of recruiting mules), Y. Penchukov (alias tank), I. Klepikov (alias petr0vich), A. Bron (alias thehead), Y. Kulibaba (alias jonni), Y. Konovalenko (alias jtk0) and A. Tikonov (alias kusanagi) [58]. The latter is believed to have developed Leprechaun, a system for automating fraudulent transactions on Internet banking platforms, used by JabberZeuS. This system particularly

[33] Function generally used by affiliates of the botnet ZeuS, which also propagated other malware as a second payload in order to ramp up their earnings.

[34] ACH refers to unauthorised fund transfers occurring in bank accounts.

makes it possible to alter a victim's banking transactions in real time [18]. Brian Krebs35 has identified disagreements within the group between M. Yakubets and M. Bogachev[35] [59].

6.3 Appendix 3: GameOverZeuS

The group built a structure of botnets operating in P2P, via GameOverZeuS and modelled on the ZeuS botnet. This structure had 27 botnets, whose *C2 backends* were each controlled by a different person or group, operating alongside other malware. Most of these botnets already existed and simply migrated towards the P2P of GoZ when it was designed. In this way, GoZ infiltrated computers that had already been infected by JabberZeuS [18].

GoZ included an automated fund transfer system, similar to Leprechaun, called *The World Bank Center* [18].

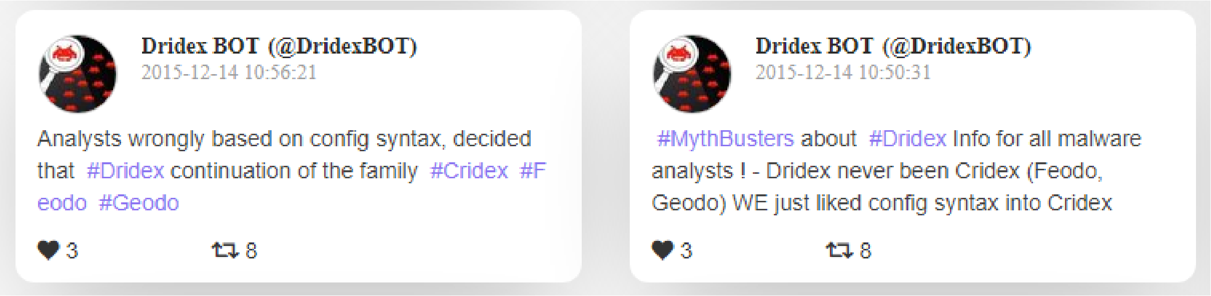
Not only that, but the threat actor group was a customer of the same *bullet proof hoster* (Troyak) for server use as the Rock Gang and operators of Avalanche and Gozi, and rented access to part of the infrastructure of the botnet Cutwail to distribute phishing emails. They also used the exploit kit BlackHole[36] which distributed Pony Loader so as to install the payload GameOver ZeuS, as well as the kit Dirt Jumper in a bid to launch DDoS attacks on banks' websites and so create a diversion from their fraudulent transfer operations [39].

6.4 Appendix 4: On the links between Dridex and Cridex

The similarity in names and behaviour between the malware families Dridex and Cridex has long led to the belief that they could have been designed by the same developers. This does not seem to be the case in reality, however.

On 10 December 2015, the account DridexBOT appeared on the Twitter network [60], most likely registered using the email address dridex[@]mail.ru created specifically for the occasion.

Although this account behaves like a bot, its tweets are actually written by one or more individuals as can be inferred from its many interactions with accounts of users close to the world of cybersecurity, particularly the blog MalwareTech, which would authenticate the account on 4 April 2016 [61]. Between December 2015 and 14 April 2017, the date of its last tweet, DridexBOT posted 153 messages, frequently aimed at demonstrating the non-existence of links between its source code and those of the Cridex family (Feodo, Geodo, etc.) [62, 63, 64].



Dridex BOT (@DridexBOT)
2015-12-14 10:56:21

Analysts wrongly based on config syntax, decided that #Dridex continuation of the family #Cridex #Feodo #Geodo

♥ 3 ⮔ 8

Dridex BOT (@DridexBOT)
2015-12-14 10:50:31

#MythBusters about #Dridex Info for all malware analysts ! - Dridex never been Cridex (Feodo, Geodo) WE just liked config syntax into Cridex

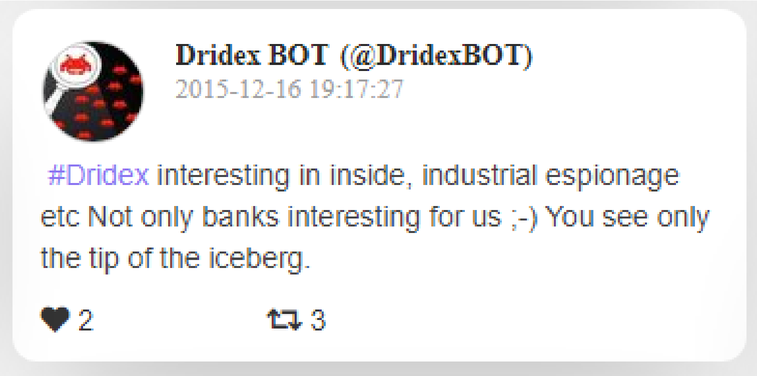
♥ 3 ⮔ 8

Fig. 6.1 : Tweets by DridexBOT

Finally, it was keen to underline Dridex' interest for sectors other than banking, not least industrial espionage [65].

[35] During a chat, M. Yakubets agreed with these words from one of the members of JabberZeuS about M. Bogachev: "he, fucker, annoyed the hell out of everyone, doesn't want to write bypass of interactives and trojan penetration 35-40%, bitch".

[36] Also used to deploy the variants of ZeuS Bugat, Feodo and Cridex, as well as the banking trojan horses Mebroot and Torpig.



Dridex BOT (@DridexBOT)
2015-12-16 19:17:27

#Dridex interesting in inside, industrial espionage etc Not only banks interesting for us ;-) You see only the tip of the iceberg.

♥ 2 3

Fig. 6.2 : Tweet de DridexBOT

7 Bibliographie

[1] ASSISTE. *Botnet Dridex*. 9 avr. 2020. URL : https://assiste.com/Botnet_Dridex.html.

[2] SECURITY INTELLIGENCE. *New Variant of Bugat Malware Uses Lucrative Gameover Zeus Techniques*. 14 août 2014. URL : https://securityintelligence.com/new-variant-of-bugat-malware-borrows-lucrative-gameover-zeus-techniques/.

[3] DEVCENTRAL. *Dridex BOTnet 220 Campaign DevCentral*. 25 fév. 2016. URL : https://devcentral.f5.com/s/articles/dridex-botnet-220-campaign-17873.

[4] BROMIUM. *Dridex Threat Analysis : Masquerading and Code Injection Techniques*. 29 juil. 2019. URL : https://www.bromium.com/dridex-threat-analysis-july-2019-variant/.

[5] ACUNETIX. *Pony : A Breakdown of the Most Popular Malware in Credential Theft*. 25 sept. 2018. URL : https://www.acunetix.com/blog/articles/pony-malware-credential-theft/.

[6] KASPERSKY. *Dridex : A History of Evolution*. 27 jan. 2020. URL : https://securelist.com/dridex-a-history-of-evolution/78531/.

[7] PROOFPOINT. *Dridex Campaigns Hitting Millions of Recipients Using Unpatched Microsoft Zero-Day*. 10 avr. 2017. URL : https://www.proofpoint.com/us/threat-insight/post/dridex-campaigns-millions-recipients-unpatched-microsoft-zero-day.

[8] CERT-FR. *Etat de La Menace Liée Aux Botnets*. 4 nov. 2019.

[9] BIT SIGHT. *Dridex Botnets*. 24 jan. 2017. URL : https://www.bitsight.com/blog/dridex-botnets.

[10] UNITED STATES DISTRICT FOR THE WESTERN DISTRICT OF PENNSYLVANIA. *Declaration of Special Agent Brian Stevens in Support of Application for an Emergency Temporary Restraining Order and Order to Show Cause Re Preliminary Injunction*. 8 oct. 2015.

[11] FIREEYE. *Evolution of Dridex*. 18 juin 2015. URL : https://www.fireeye.com/blog/threat-research/2015/06/evolution_of_dridex.html.

[12] TREND MICRO. *Dealing with the Mess of DRIDEX*. 6 déc. 2014. URL : https://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/3147/dealing-with-the-mess-of-dridex.

[13] BOTCONF 2020. *Dridex Gone Phishing*. 25 sept. 2016. URL : https://www.botconf.eu/2016/dridex-gone-phishing/.

[14] BIT SIGHT. *Dridex. Chasing a Botnet from the Inside*. 2015.

[15] TWITTER. *@Kafeine*. 5 déc. 2019. URL : https://twitter.com/kafeine/status/1202684242905448448.

[16] ZDNET. *10 ans de malwares : les pires botnets des années 2010*. 11 déc. 2019. URL : https://www.zdnet.fr/actualites/10-ans-de-malwares-les-pires-botnets-des-annees-2010-39895641.htm.

[17] FOX-IT. “Backgrounds on the Badguys and the Backends”. 2015. In : (2015).

[18] SECURE WORKS. *Evolution of the GOLD EVERGREEN Threat Group*. 15 mai 2017. URL : https://www.secureworks.com/research/evolution-of-the-gold-evergreen-threat-group.

[19] XAKER.RU. *Le solitaire contre la ”société du mal”. Comment Brian Krebs s’est battu contre les pirates russes d’Evil Corp*. 31 jan. 2020. URL : https://xakep.ru/2020/01/31/evil-corp-vs-brian-krebs/.

[20] INSTITUT PANDORE. *On décortique Zeus, le malware le plus hardcore jamais découvert*. 23 jan. 2020. URL : https://www.institut-pandore.com/hacking/analyse-malware-zeus/.

[21] *Zeus Museum*. 9 avr. 2020. URL : https://zeusmuseum.com/.

[22] CNEWS. *Un Ressortissant de La Communauté Des Etats Indépendants Sera Incarcéré 15 Ans Pour Le Piratage Informatique d’écoles et d’une Entreprise Pétrolière*. 15 fév. 2017. URL : https://safe.cnews.ru/news/top/2017-02-15_vyhodets_iz_sng_syadet_v_tyurmu_na_15_let_za_vzlom.

[23] U.S. DEPARTMENT OF THE TREASURY. *Treasury Sanctions Evil Corp, the Russia-Based Cybercriminal Group Behind Dridex Malware*. 5 déc. 2019. URL : https://home.treasury.gov/news/press-releases/sm845.

[24] NATIONAL CRIME AGENCY. *International Law Enforcement Operation Exposes the World’s Most Harmful Cyber Crime Group*. 5 déc. 2019. URL : https://www.nationalcrimeagency.gov.uk/news/international-law-enforcement-operation-exposes-the-world-s-most-harmful-cyber-crime-group.

[25] BLUELIV. *Spanish Consultancy Everis Suffers BitPaymer Ransomware Attack : A Brief Analysis*. 6 nov. 2019. URL : https://www.blueliv.com/cyber-security-and-cyber-threat-intelligence-blog-blueliv/research/everis-bitpaymer-ransomware-attack-analysis-dridex/.

[26] MALWAREBYTES. *The Forgotten Domain : Exploring a Link between Magecart Group 5 and the Carbanak APT*. 22 oct. 2019. URL : https://blog.malwarebytes.com/threat-analysis/2019/10/the-forgotten-domain-exploring-a-link-between-magecart-group-5-and-the-carbanak-apt/.

[27] Dell Secure WORKS. "Banking Botnets Persists despite Takedowns". 2015. In : (2015).

[28] ESET. *FriedEx : BitPaymer, nouveau rançongiciel des auteurs de Dridex*. 31 jan. 2018. URL : https://www.welivesecurity.com/fr/2018/01/31/friedex-bitpaymer-dridex/.

[29] TREND MICRO. *URSNIF, EMOTET, DRIDEX and BitPaymer Gangs Linked by a Similar Loader*. 18 déc. 2018. URL : https://blog.trendmicro.com/trendlabs-security-intelligence/ursnif-emotet-dridex-and-bitpaymer-gangs-linked-by-a-similar-loader/.

[30] MICROSOFT. *Human-Operated Ransomware Attacks : A Preventable Disaster*. 5 mar. 2020. URL : https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/.

[31] CROWDSTRIKE. *CrowdStrike Discovers New DoppelPaymer Ransomware & Dridex Variant*. 12 juil. 2019. URL : https://www.crowdstrike.com/blog/doppelpaymer-ransomware-and-dridex-2/.

[32] FIREEYE. *Head Fake : Tackling Disruptive Ransomware Attacks*. 1er oct. 2019. URL : https://www.fireeye.com/blog/threat-research/2019/10/head-fake-tackling-disruptive-ransomware-attacks.html.

[33] BLEEPING COMPUTER. *Three More Ransomware Families Create Sites to Leak Stolen Data*. 24 mar. 2020. URL : https://www.bleepingcomputer.com/news/security/three-more-ransomware-families-create-sites-to-leak-stolen-data/.

[34] UNITED STATES DISTRICT COURT EASTERN DISTRICT OF NEW-YORK. *Complaint*. 5 mar. 2020.

[35] CYWARE. *The Many Faces and Activities of Ever-Evolving Necurs Botnet*. 29 déc. 2019. URL : https://cyware.com/news/the-many-faces-and-activities-of-ever-evolving-necurs-botnet-1e8d2734.

[36] PROOF POINT. *Locky Ransomware : Dridex Actors Get In The Game*. 6 avr. 2016. URL : https://www.proofpoint.com/us/threat-insight/post/dridex-actors-get-in-ransomware-with-locky.

[37] PROOF POINT. *Threat Actor Profile : TA505, From Dridex to GlobeImposter*. 27 sept. 2017. URL : https://www.proofpoint.com/us/threat-insight/post/threat-actor-profile-ta505-dridex-globeimposter.

[38] SECURE WORKS. *Cutwail Spam Swapping Blackhole for Magnitude Exploit Kit*. 18 oct. 2013. URL : https://www.secureworks.com/blog/cutwail-spam-swapping-blackhole-for-magnitude-exploit-kit.

[39] SECURE WORKS. *The Lifecycle of Peer to Peer (Gameover) ZeuS*. 23 juil. 2012. URL : https://www.secureworks.com/research/the-lifecycle-of-peer-to-peer-gameover-zeus.

[40] MALPEDIA. *NARWHAL SPIDER*. Mar. 2020. URL : https://malpedia.caad.fkie.fraunhofer.de/actor/narwhal_spider.

[41] TWITTER. *@FaLconIntel*. 16 avr. 2020. URL : https://twitter.com/FaLconIntel/status/1247689506410475520.

[42] ZDNET. *Meet the White-Hat Group Fighting Emotet, the World's Most Dangerous Malware*. 29 fév. 2020. URL : https://www.zdnet.com/article/meet-the-white-hat-group-fighting-emotet-the-worlds-most-dangerous-malware/.

[43] NAKED SECURITY. *Emotet's Goal : Drop Dridex Malware on as Many Endpoints as Possible*. 10 août 2017. URL : https://nakedsecurity.sophos.com/2017/08/10/watch-out-for-emotet-the-trojan-thats-nearly-a-worm/.

[44] PROOFPOINT. *Threat Actor Profile : TA542, From Banker to Malware Distribution Service*. 15 mai 2019. URL : https://www.proofpoint.com/us/threat-insight/post/threat-actor-profile-ta542-banker-malware-distribution-service.

[45] TWITTER. "@Vitali Kremez". 11 déc. 2019. In : (11 déc. 2019).

[46] TWITTER. "@Vitali Kremez". 17 nov. 2018. In : (17 nov. 2018).

[47] PROOFPOINT. *DanaBot - A New Banking Trojan Surfaces Down Under*. 31 mai 2018. URL : https://www.proofpoint.com/us/threat-insight/post/danabot-new-banking-trojan-surfaces-down-under-0.

[48] Computer World. *Leak of ZeusVM Malware Building Tool Might Cause Botnet Surge*. 6 juil. 2015. URL : https://www.computerworld.com/article/2944041/leak-of-zeusvm-malware-building-tool-might-cause-botnet-surge.amp.html.

[49] MalwareMustDie. *MMD-0036-2015 - KINS (or ZeusVM) v2.0.0.0 Tookit (Builder & Panel Source Code) Leaked.* 5 juil. 2015. URL : https://blog.malwaremustdie.org/2015/07/mmd-0036-2015-kins-or-zeusvm-v2000.html.

[50] Kaspersky. *Trojan-Banker.Win32.Chthonic*. Mar. 2016. URL : https://threats.kaspersky.com/fr/threat/Trojan-Banker.Win32.Chthonic/.

[51] FireEye. *Fake Software Update Abuses NetSupport Remote Access Tool*. 5 avr. 2018. URL : https://www.fireeye.com/blog/threat-research/2018/04/fake-software-update-abuses-netsupport-remote-access-tool.html.

[52] SocPrime. *Spelevo Exploit Kit Spreads IcedID and Dridex Trojans*. 1^er^ juil. 2019. URL : https://socprime.com/en/news/spelevo-exploit-kit-spreads-icedid-and-dridex-trojans/.

[53] Le pouvoir claPratique. “Inside a ZeuS botnet”. 2015. In : *Le pouvoir claPratique* (2015).

[54] Comodo. *What Is Zeus Malware ?* 31 juil. 2018. URL : https://enterprise.comodo.com/blog/what-is-zeus-malware/.

[55] US Cert. *Avalanche (Crimeware-as-a-Service Infrastructure)*. 1er déc. 2016. URL : https://www.us-cert.gov/ncas/alerts/TA16-336A.

[56] LeMondeInformatique. *Forte montée des attaques ciblées via le malware Zeus*. 27 mai 2013. URL : https://www.lemondeinformatique.fr/actualites/lire-forte-montee-des-attaques-ciblees-via-le-malware-zeus-53727.html.

[57] Reuters. “Analysis : Top Hacker ”Retires”; Experts Brace for His Return”. 29 oct. 2010. In : *Reuters* (29 oct. 2010).

[58] United States District Court for the District of Nebraska. *Criminal Complaint*. 13 juil. 2012.

[59] Krebs on Security. *Inside ‘Evil Corp,’ a $100M Cybercrime Menace*. 16 déc. 2019. URL : https://krebsonsecurity.com/2019/12/inside-evil-corp-a-100m-cybercrime-menace/.

[60] Twitter. *@Dridex BOT*. 10 déc. 2015. URL : http://archive.vn/SoHYv.

[61] Twitter. *@MalwareTech*. 4 avr. 2016. URL : http://archive.vn/Zw5MD.

[62] Twitter. *@Dridex BOT*. 17 déc. 2015. URL : https://twitter.com/dridexbot/status/677561943171952641.

[63] Twitter. *@Dridex BOT*. 14 déc. 2015. URL : https://twitter.com/dridexbot/status/676353569180774400.

[64] Twitter. *@Dridex BOT*. 14 déc. 2015. URL : https://twitter.com/dridexbot/status/676355038441299968.

[65] Twitter. *@Dridex BOT*. 16 déc. 2015. URL : https://twitter.com/dridexbot/status/677205919630024704.

- 17/07/2020

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

ANSSI - 51 boulevard de la Tour-Maubourg, 75700 PARIS 07 SP
www.cert.ssi.gouv.fr / cert-fr.cossi@ssi.gouv.fr

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
SGDSN