Analysing a Widespread Microsoft 365 Credential Harvesting Campaign

bridewell.com/insights/blogs/detail/analysing-widespread-microsoft365-credential-harvesting-campaign

Bridewell Cyber Threat Intelligence (CTI) has identified a widespread ongoing credential harvesting campaign that has been ongoing since July.

The threat actors, believed to be connected to Storm-1575, are utilising the Dadsec platform to conduct widespread phishing of global organisations to steal Microsoft 365 credentials. The threat actors are using Cyber Panel, an open-source web development panel, hundreds of Domain Generated Algorithm (DGA) domains that are created daily to host credential harvesting pages.

DGA is a technique used by malicious actors to rapidly generate multiple domain names that can be used to host malicious content, such as malware, phishing sites, and command-and-control servers. It is used to evade detection and to ensure that their malicious content is not blocked by security controls.

The threat actors are using a variety of lures to redirect victims via services such as Bing, Google AMP and Microsoft Customer Voice before landing them on credential harvesting pages. The infrastructure associated with this activity is sat behind Cloudflare, a technique used to mask the origin of the malicious servers and evade detection by security tooling.

Our Cyber Threat Intelligence team has been working with our Security Operations Centre (SOC) on two incidents that began our initial investigations. After conducting research into this campaign, Bridewell CTI identified over 500 DGA domains, with up to 900 associated subdomains all generated since July daily as part of this activity. Utilising this information, we have been able to identify historical successful connections between other Bridewell customers which had gone unidentified by conventional security tooling. We have also ensured that affected customers had passwords reset to prevent account takeover.

We were also able to uncover additional infrastructure belonging to the Dadsec platform and threat actors utilising this toolset in campaigns. Based on the description provided by Microsoft and the findings in this report, **we assess with a high degree of confidence that this campaign matches the cluster of activity associated with Storm-1575.**

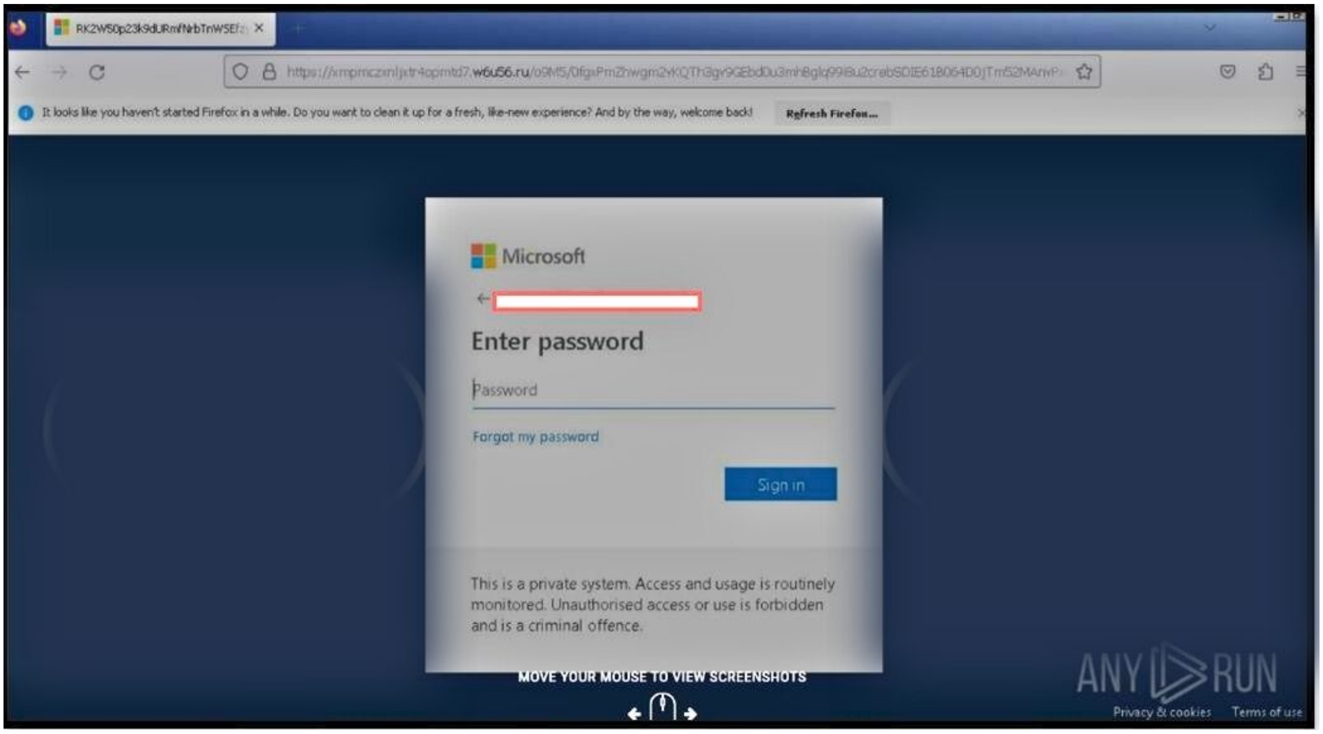
Whilst we attribute the campaign to the same cluster, it should be noted that any malicious threat actor with sufficient intent can purchase and run a campaign through the Dadsec platform for very little sophistication and financial investment.

The campaign is ongoing and we will share all identified IOCs in this report. Furthermore, we are sharing the process and analysis steps taken by our CTI team when supporting their IR teams on customer engagements. Additionally, CTI has worked closely with the teams at ANY.RUN, who collaborated with Bridewell to improve detection of this campaign within their platform as well as contribute to this report.

By consuming a threat intelligence service, you should expect that intrusion analysis is being performed by the threat intelligence team. This will ensure they are producing actionable insights and intelligence from attempted and successful attacks against your organisation. Bridewell CTI uses a blend of automated and manual analysis processes to keep you informed and protected against credible threats to your business and sector.

2. Initial Incidents

On the 28th and 29th of September 2023, we observed two of our customers, working in different sectors, receiving suspicious emails that ultimately directed users to fake Microsoft 365credential harvesting pages. In one instance, the organisation received over 500 emails with 25 being successfully delivered.



RK2WS0p23k9dURmfNrbTnWSEfz

https://xmpmczxnljxtr4opmtd7.w6u56.ru/o9M5/0fgxPmZhwgm2vKQTh3gv9GEbdDu3mh8glq99i8u2crebSDIE618064D0jTm52MAnvP

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

Refresh Firefox...

Microsoft

← [redacted]

Enter password

Password

Forgot my password

Sign in

This is a private system. Access and usage is routinely monitored. Unauthorised access or use is forbidden and is a criminal offence.

MOVE YOUR MOUSE TO VIEW SCREENSHOTS

Figure 1. Fake Microsoft 365 Credential Harvesting Page

2.1 Indicators

URL: 1e0yq0dnmzxs8ato15f0[.]15cl6[.]ru

URL: xmpmczxnljxtr4opmtd7[.]w6u56[.]ru

Based on the indicators from each incident, our Security Analysts assessed that the domains in both may be connected. Comparing the two indicators above, we noted the following traits:

- Both domains have a .RU TLD.
- The domains are 5 alphanumeric characters long.
- The subdomains 20 alphanumeric characters long.

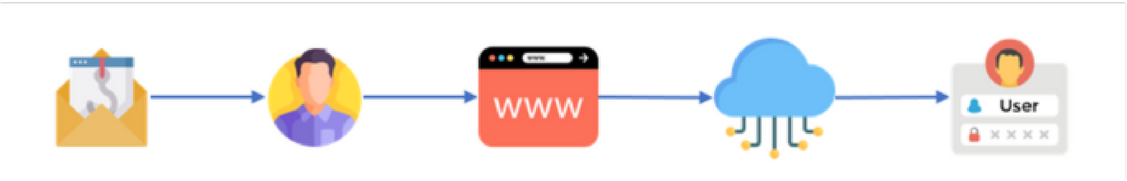


Figure 2.Example infection chain

1. User receives an email containing a variety of lures to share a file, which includes typically a HTML file attachment.

2. When the user clicks the link, the browser connects to a number of legitimate services abused for redirecting (e.g. Bing, Google AMP, Microsoft Customer Voice).
3. The user is redirected to the threat actor infrastructure hosted behind Cloudflare. The website presents the turnstile captcha to validate a user session.
4. The user is then presented with a fake Microsoft 365 page with user email pre-populated including their company logo.
5. The kit supports MFA and will run the user through the process, meanwhile an API acts as the user to middle man the challenge responses and issue user credentials to the threat actor via the web panel.

Example infection chains can be found here (note: whilst possible, no abuse of the Amazon r2.dev domain was observed during our research): https://twitter.com/anyrun_app/status/1709193919118844267

3. CTI Investigation

Types of questions the IR team wanted to understand:

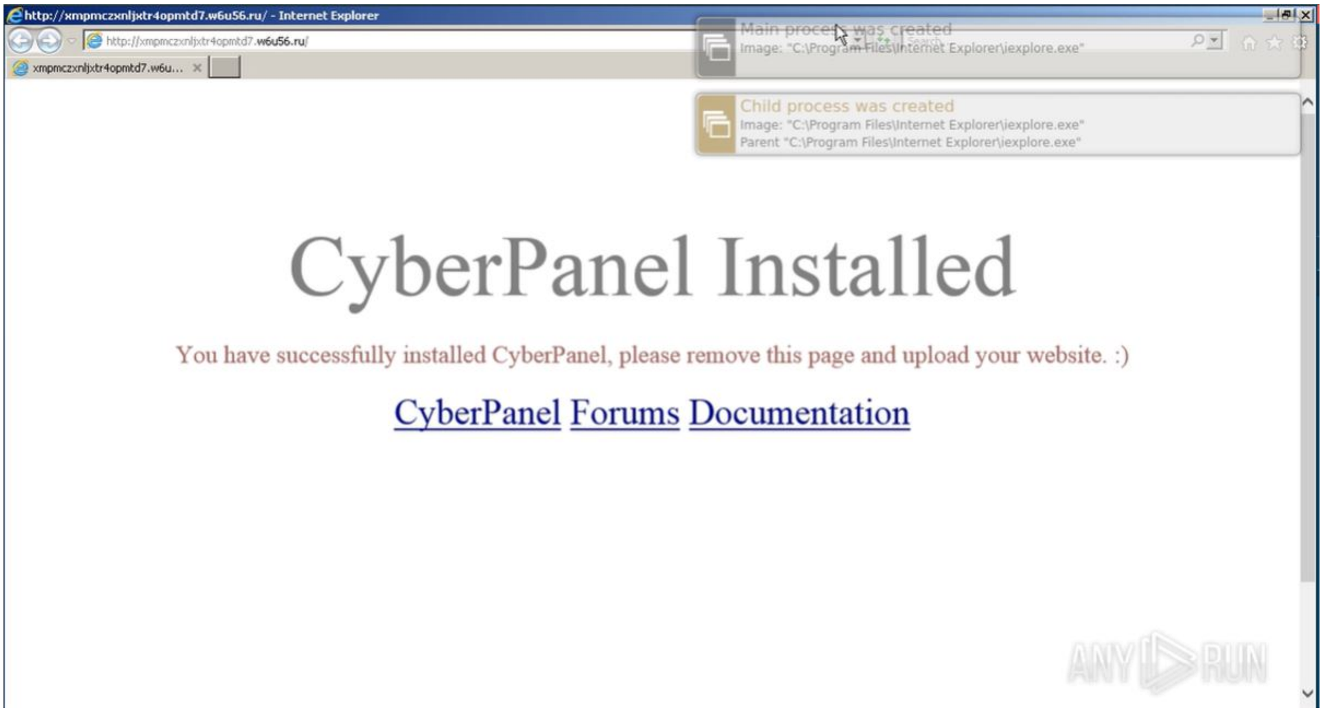
- Was there a connection between our customers?
- Were there other similar phishing emails delivered to our customers?
- Do we have any more information about this campaign?

CTI began the investigation with these questions in mind as we began two strands of work:

1. An initial internal hunt in our customer environments based on visible characteristics from known IOCs
2. Uncover additional infrastructure or domains based on open-source research to uncover more indicators and context

4. The Campaign

Based on the information provided by the IR team, we can use information about the domains, combined with observed technologies utilised by the threat actors to uncover additional infrastructure. By analysing the URLs within the ANY.RUN sandbox, we were able to identify the use of Cyber Panel, an open-source web hosting platform.



http://xmpmczxnljxtr4opmtd7.w6u56.ru/ - Internet Explorer

http://xmpmczxnljxtr4opmtd7.w6u56.ru/

xmpmczxnljxtr4opmtd7.w6u...

Main process was created
Image: "C:\Program Files\Internet Explorer\iexplore.exe"

Child process was created
Image: "C:\Program Files\Internet Explorer\iexplore.exe"
Parent "C:\Program Files\Internet Explorer\iexplore.exe"

CyberPanel Installed

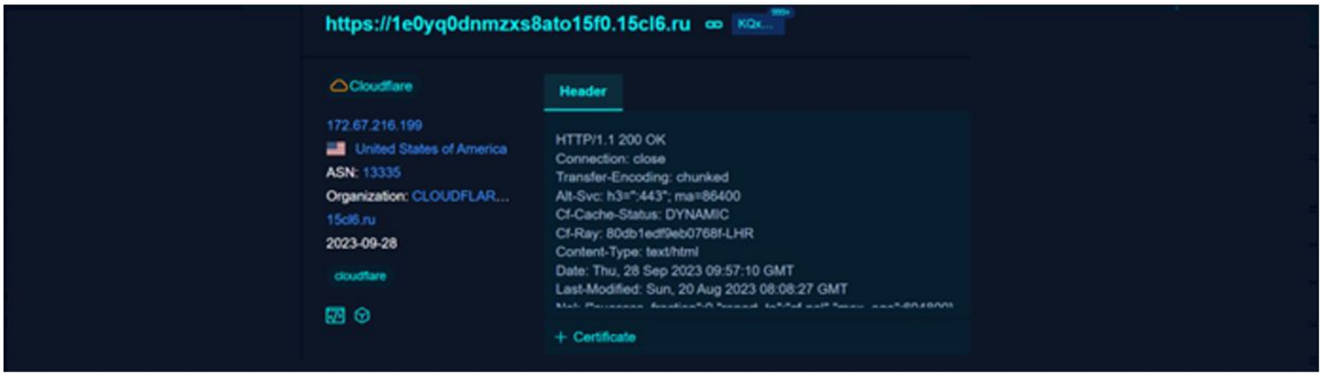
You have successfully installed CyberPanel, please remove this page and upload your website. :)

CyberPanel Forums Documentation

Figure 3. CyberPanel page on hosting infrastructure

4.1 Additional Infrastructure

Passive internet scanners are an incredibly good way of pivoting on identifiable characteristics for known bad infrastructure in order to identify servers based on these characteristics. We began by understanding what the known indicators from the incident looked like in the tool FOFA:



https://1e0yq0dnmzxs8ato15f0.15cl6.ru

Cloudflare

172.67.216.199

United States of America

ASN: 13335

Organization: CLOUDFLAR...

15cl6.ru

2023-09-28

cloudflare

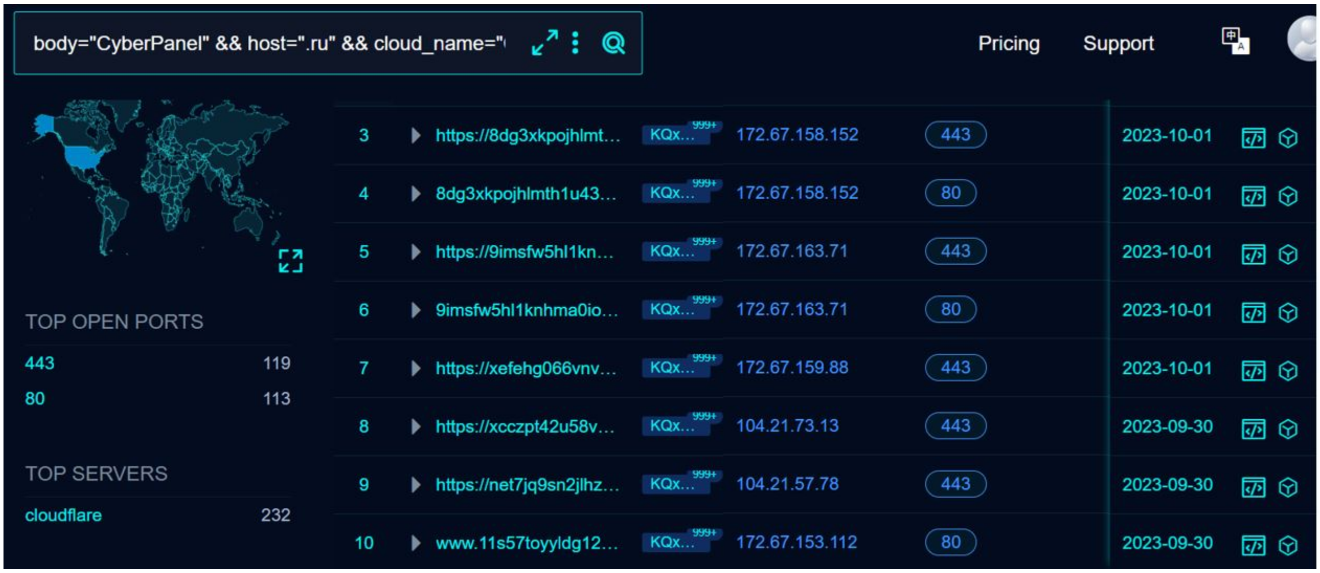
Header

```
HTTP/1.1 200 OK
Connection: close
Transfer-Encoding: chunked
Alt-Svc: h3=":443"; ma=86400
Cf-Cache-Status: DYNAMIC
Cf-Ray: 80db1edf9eb0768f-LHR
Content-Type: text/html
Date: Thu, 28 Sep 2023 09:57:10 GMT
Last-Modified: Sun, 20 Aug 2023 08:08:27 GMT
```

Figure 4. FOFA result for known indicator

Based on the known infection chain, we can see that the domains are sat behind Cloudflare. This can be problematic in that this is an effective mechanism for masking the true destination of the malicious infrastructure. However, we were able to observe the use of the open-source hosting framework, CyberPanel. This gives us an indication of the technologies potentially used by the threat actors.

Pivoting off known information regarding Cloudflare, CyberPanel and .RU TLD we can return additional infrastructure:



```
body="CyberPanel" && host=".ru" && cloud_name="
```

TOP OPEN PORTS

443	119
80	113

TOP SERVERS

cloudflare	232

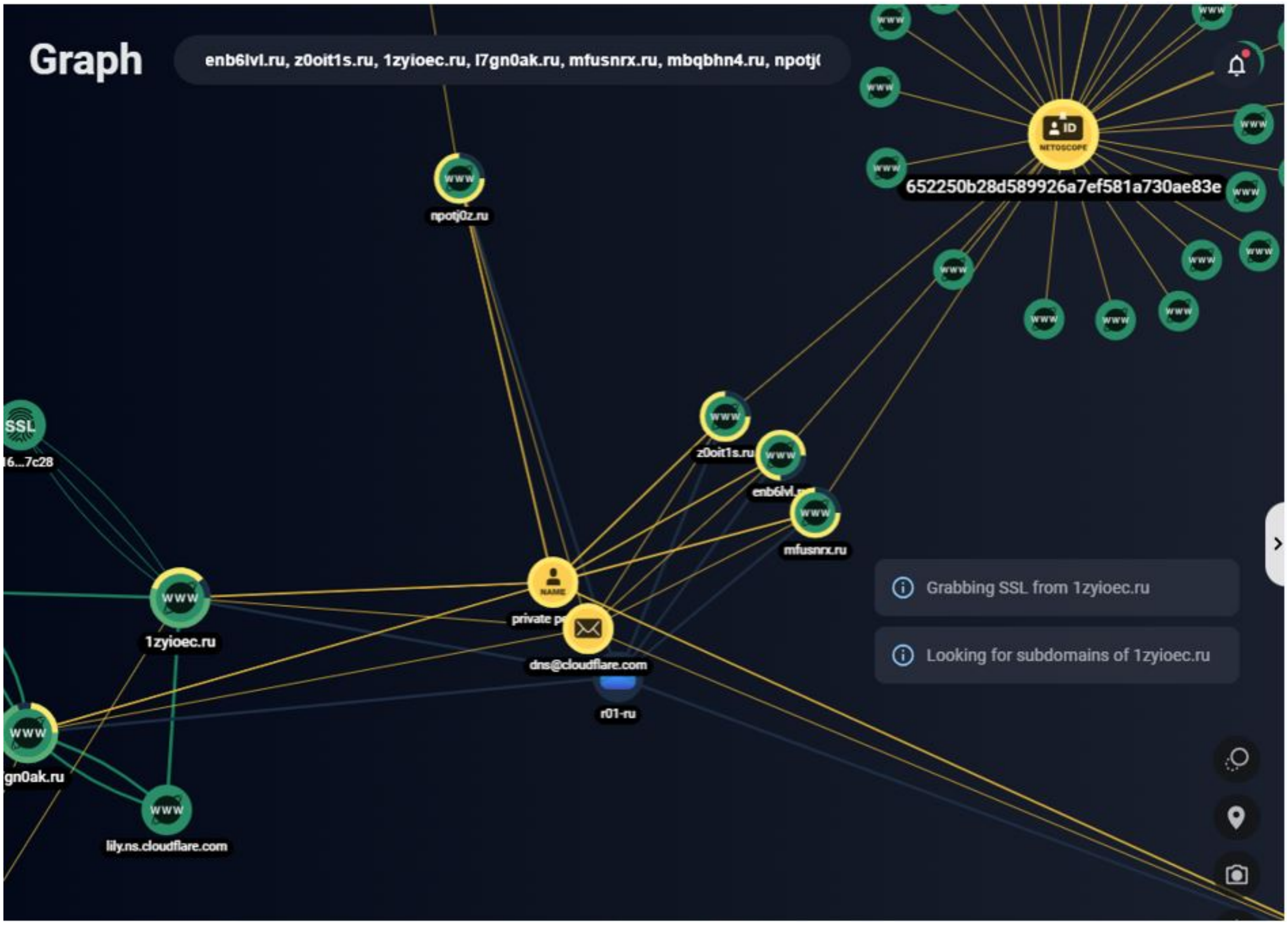
3	https://8dg3xkpojhlmt…	KQx… 999+	172.67.158.152	443	2023-10-01
4	8dg3xkpojhlmth1u43…	KQx… 999+	172.67.158.152	80	2023-10-01
5	https://9imsfw5hl1kn…	KQx… 999+	172.67.163.71	443	2023-10-01
6	9imsfw5hl1knhma0io…	KQx… 999+	172.67.163.71	80	2023-10-01
7	https://xefehg066vnv…	KQx… 999+	172.67.159.88	443	2023-10-01
8	https://xcczpt42u58v…	KQx… 999+	104.21.73.13	443	2023-09-30
9	https://net7jq9sn2jlhz…	KQx… 999+	104.21.57.78	443	2023-09-30
10	www.11s57toyyldg12…	KQx… 999+	172.67.153.112	80	2023-09-30

Figure 5. Wider search for known indicators using FOFA

Whilst not exhaustive, the above search gives us an indication of the size and scale of the potential campaign and provides our security team additional indicators in which to search for, building from the new information.

When we begin to analyse the domains we've collected further from FOFA, we can begin to identify additional characteristics of the domains involved in this campaign. The graphs below visualise some of those characteristics:

- The domains are registered with R01-RU and MAXNAME.
- The domains host a number of subdomains
- The sites are using both Let's Encrypt, R1 and Google Trust Services LLC certificates.



enb6lvl.ru, z0oit1s.ru, 1zyioec.ru, l7gn0ak.ru, mfusnrx.ru, mbqbhn4.ru, npotj(

Grabbing SSL from 1zyioec.ru

Looking for subdomains of 1zyioec.ru

Figure 6. Correlation between domains and WHOIS (Group-IB Threat Intelligence Platform)

Graph showing the connection between domain Registrars

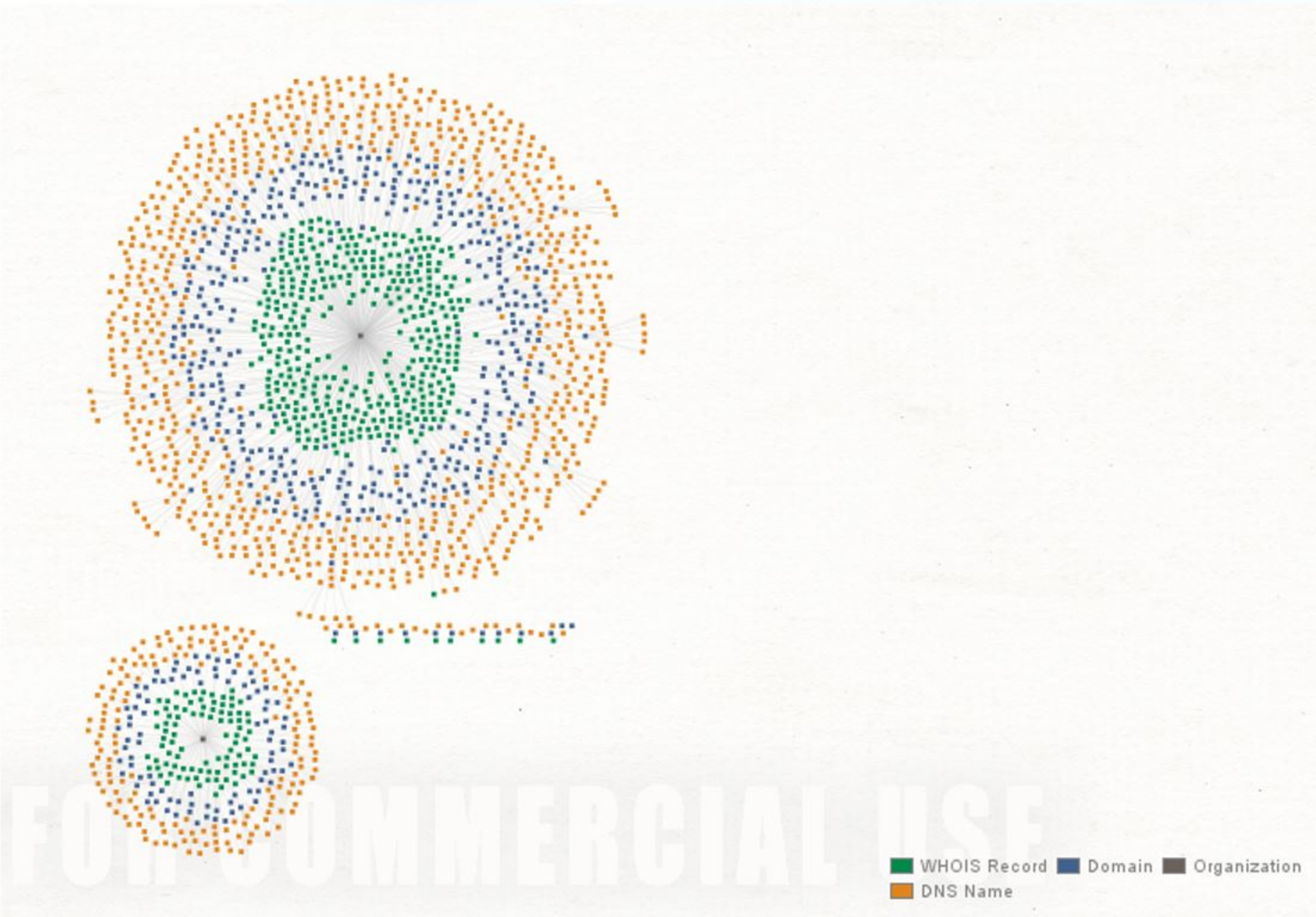


Figure 7. Correlation between WHOIS records and Registrars

When enriching our results further based on known features and passive DNS, we are able uncover additional domains. In total, at the time of analysis, we identified ~500 domains containing 900 subdomains believed to be linked with this campaign.

Based on WHOIS information, we can use the creation date of the domains to help understand when the campaign began and how active the ongoing campaign is:

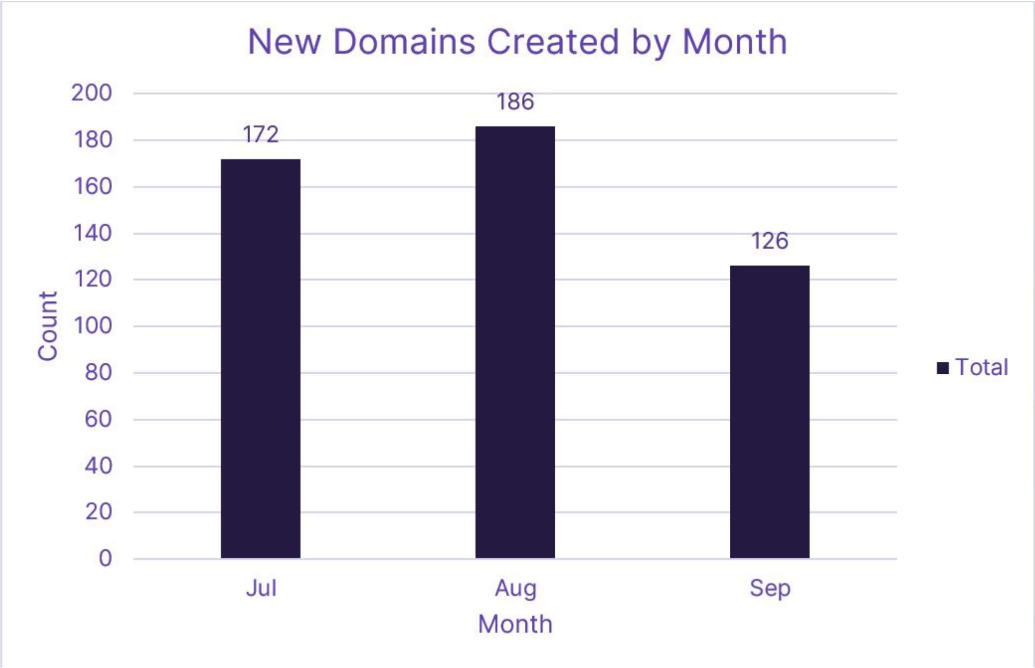


Figure 8. Timeline of new domain creation dates by month

The threat actor is actively generating hundreds of new domains every month to support his activity. A recent article by Infoblox details are new shift by threat actors to utilise RDGA's instead of DGA's. Whilst we get to grips with the new definitions, it appears that the frequent registration of new domains by threat actors to evade detection matches what we are seeing here and by other criminals such as malware authors. The goal of threat actors to utilise RDGA's is to ensure that each new domain is considered clean by security tooling as and when the threat actors deploy them in campaigns.

A full list of domains identified by Bridewell can be found at the following link: https://github.com/Bridewell-CTI/IOCs/blob/main/2023/10/Storm-1575.txt

4.2 Analysing known indicators

Going a step further, we decided to further enrich and analyse our known indicators to help understand more about the campaign, such as:

- What lures are the threat actors using?
- What file types are being used?
- How many samples are being submitted per day?
- What and how many targets have been affected?

The following image demonstrates the number of samples submitted to Virus Total that communicate with our known domains:

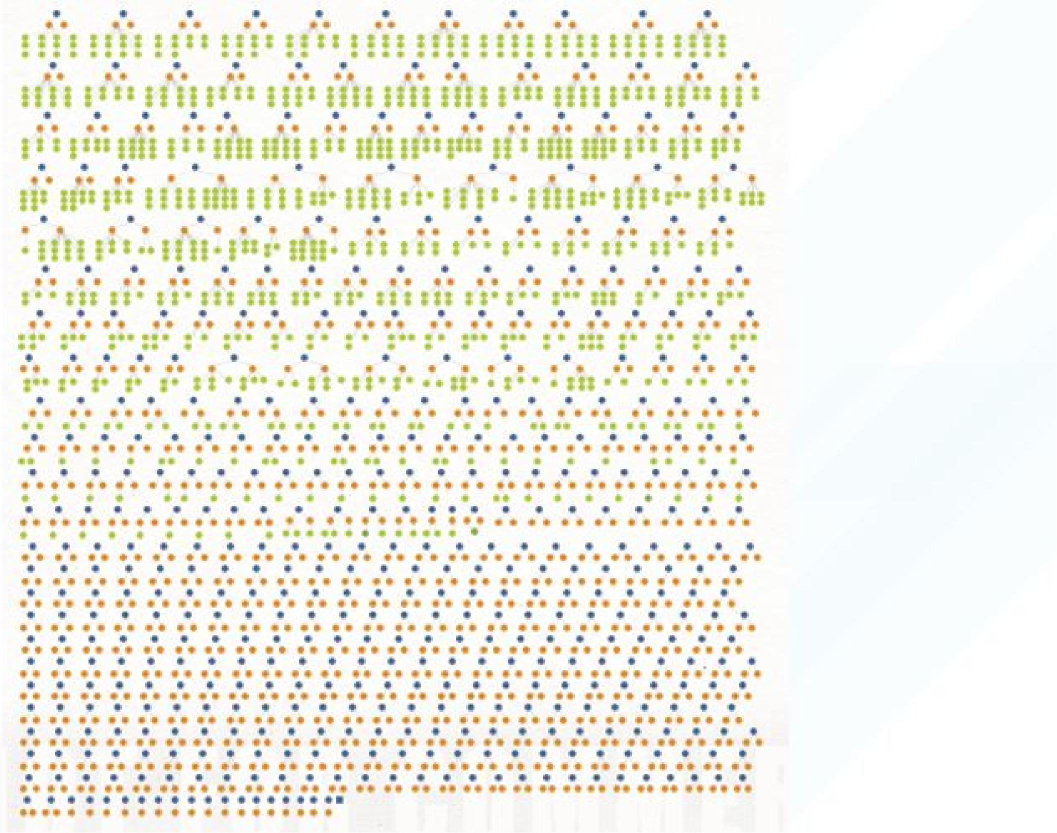


Figure 9. Graph showing VT file submissions by subdomain

Whilst this indicates that a number of the domains have been utilised in active campaigns, it shows that a number of the remaining domains either haven’t had samples submitted by victims/ targets, or, due to their young age, have yet to be utilised.

4.2.1 What lures are the threat actors using?

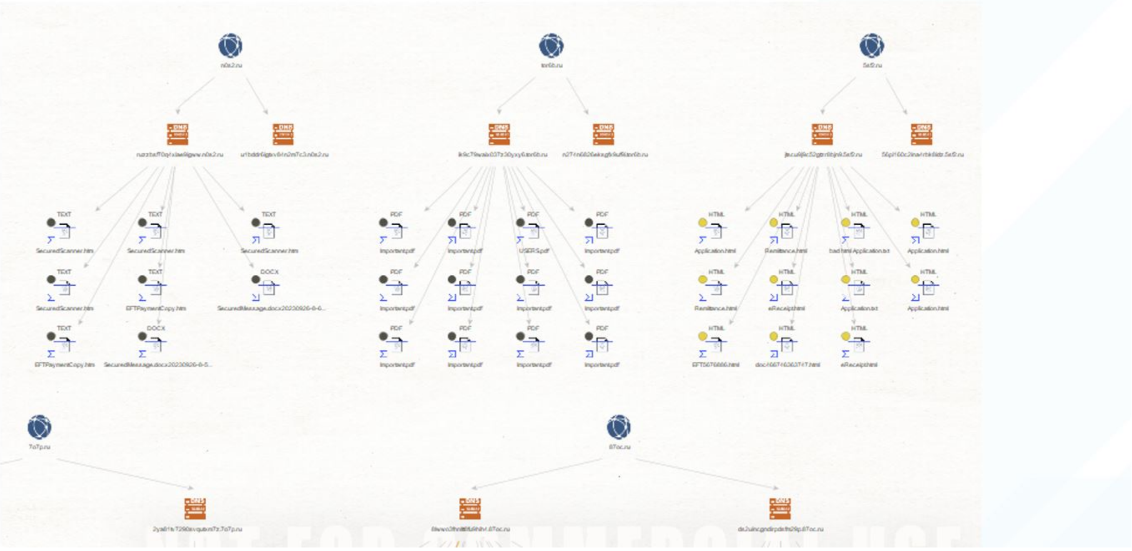


Figure 10. Closer inspection of VT submitted files with subdomains

By extracting the subject information, we are able to identify the types of lures that the threat actors are using in this campaign. By grouping on keywords we were able to identify the following themes:

- Advanced Payment or Payment Receipt/Confirmation
- Secure or Scanned Documents
- Invoices
- Employee Handbook ({Organisation})
- VM/Audio Recordings
- Important Updates
- 2FA or MFA setup/update

4.2.2 How long has the campaign been going on?

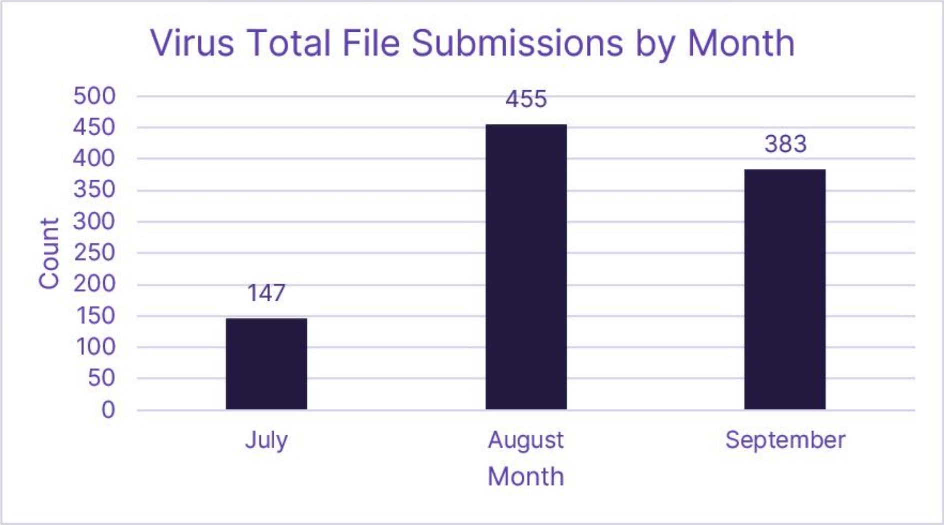


Figure 11. File submission dates by month

When comparing file submission dates, we can see that there is a slight delay between domain creation and the activity beginning and being submitted for analysis in Virus Total. Based on the current available information, it's clear that the campaign is ongoing.

4.2.3 What file types are they using?

By collecting this information from Virus Total, we can see that the majority of samples in this campaign contained some form of HTML attachment that was used to initiate the infection chain.

Attachment Type	Count
DOCX	9
HTML	800

JAVASCRIPT	15
PDF	144
TEXT	16

4.2.3 What sectors have been affected?

Based on analysis of the base64 encoded email addresses populated in the phishing URLs, CTI identified organisations operating in over 30 different sectors. The most common were **Financial Services, Manufacturing, Local Government and Energy**. Using the organisation head office information 27 organisations of the 54 countries identified were based in the **United States** and 7 were within the **United Kingdom**.

Based on this information, we can assess with a high degree of confidence that targeting is directed at Western countries. We can also assess with high confidence that targeting is not directed at a specific sector or victim profile.

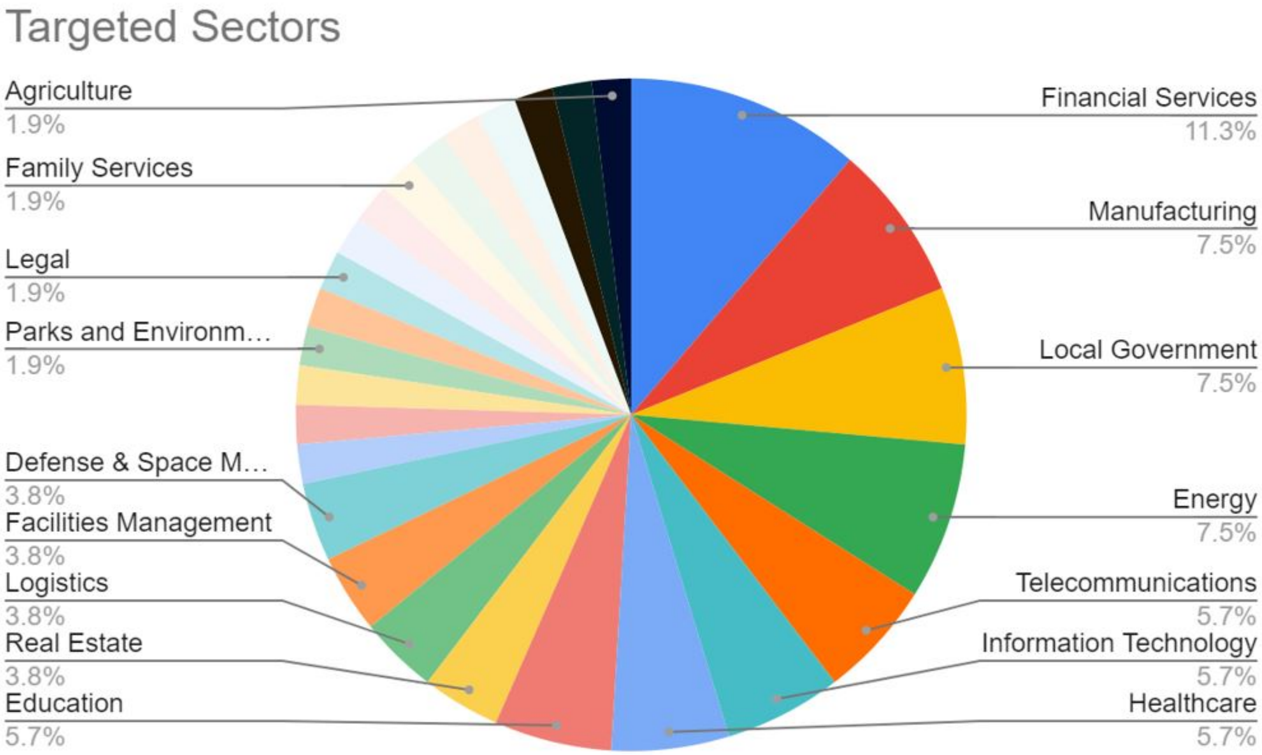


Figure 12. Pie Chart showing affected sectors

5. Attribution

Credential harvesting is nothing new and it's utilised by many threat actors. Fortunately, we were provided a key piece of information that was relevant and interesting to this campaign by our SOC. Microsoft Threat Intelligence linked an initial domain to activity conducted by Storm-1575.

5.1 Who are Storm-1575?

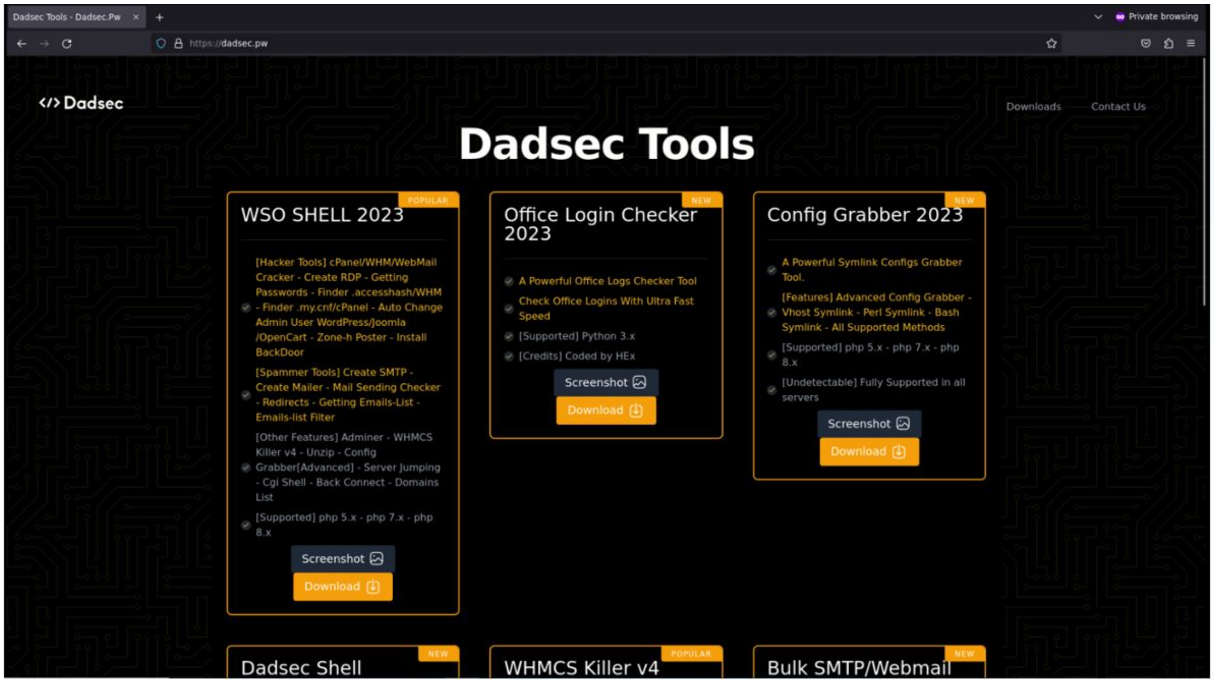
According to Microsoft:

“Microsoft has identified Storm-1575 as a cluster of activity using known infrastructure for several Phishing as a Service (PhaaS) campaigns on the Dadsec platform. The Dadsec platform allows cybercriminals to launch phishing campaigns without developing the phishing websites themselves. These websites are designed to look like legitimate web portals and are used to harvest user credentials and authentication tokens. This alert triggers upon a network connection to a domain affiliated with a Dadsec phishing page managed by a developer that Microsoft tracks as Storm-1575.**”**

Based on the description provided by Microsoft and the findings in this report, **Bridewell assess with a high degree of confidence that this campaign matches the cluster of activity associated with Storm-1575.** Whilst we attribute the campaign to the same cluster, it should be noted that any malicious threat actor with sufficient intent can purchase and run a campaign through the Dadsec platform for very little sophistication and financial investment.

5.2 What is Dadsec?

As Microsoft describes, the Dadsec platform provides threat actors with the tools to conduct phishing campaigns. CTI first discovered the site dadsec[.]pw which lists a number of tools for download, however, only the “Office Login Checker 2023” file is available for download.



Dadsec Tools

WSO SHELL 2023 POPULAR

- [Hacker Tools] cPanel/WHM/WebMail Cracker - Create RDP - Getting Passwords - Finder .accesshash/WHM - Finder .my.cnf/cPanel - Auto Change Admin User WordPress/Joomla /OpenCart - Zone-h Poster - Install BackDoor
- [Spammer Tools] Create SMTP - Create Mailer - Mail Sending Checker - Redirects - Getting Emails-List - Emails-list Filter
- [Other Features] Adminer - WHMCS Killer v4 - Unzip - Config Grabber[Advanced] - Server Jumping - Cgi Shell - Back Connect - Domains List
- [Supported] php 5.x - php 7.x - php 8.x

Office Login Checker 2023 NEW

- A Powerful Office Logs Checker Tool
- Check Office Logins With Ultra Fast Speed
- [Supported] Python 3.x
- [Credits] Coded by HEx

Config Grabber 2023 NEW

- A Powerful Symlink Configs Grabber Tool.
- [Features] Advanced Config Grabber - Vhost Symlink - Perl Symlink - Bash Symlink - All Supported Methods
- [Supported] php 5.x - php 7.x - php 8.x
- [Undetectable] Fully Supported in all servers

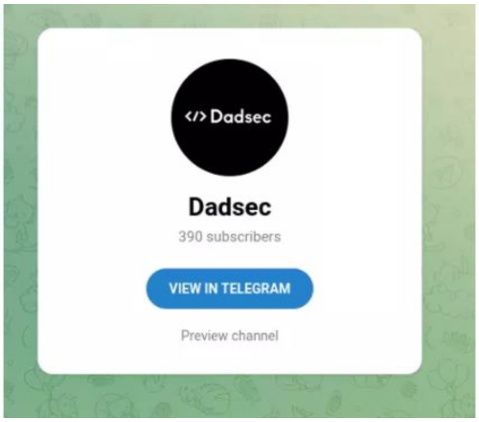
Dadsec Shell NEW

WHMCS Killer v4 POPULAR

Bulk SMTP/Webmail NEW

Figure 13. Dadsec webpage

Per the following Telegram channel “dadsec_pw”, this tool is made freely available by the developer. The Dadsec channel was first created in January 2023 and provides users with updates to the platform.

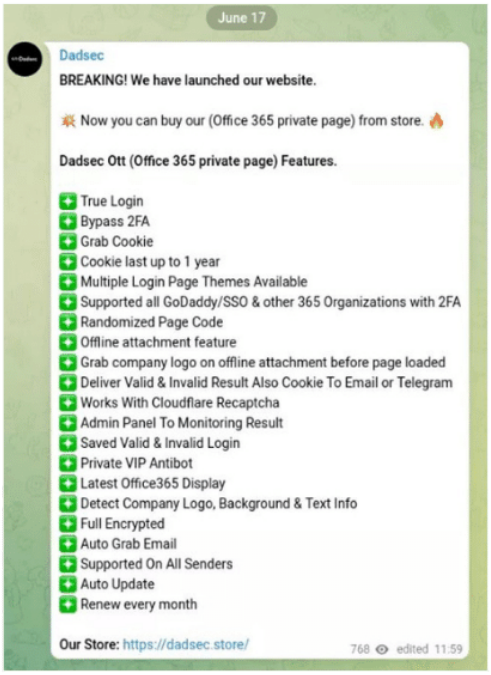


Dadsec

390 subscribers

Figure 14. Dadsec Telegram channel

On June 17th, the developers posted that they have launched their new website, dadsec[.]store, whereby users can purchase the “Office 365 private page” from their store. The also released a new Telegram channel on 8th August to support customers of the new store. This developer activity coincides with our assessment that the campaign began in July, just after this development.



June 17

Dadsec

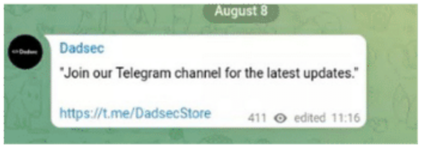
BREAKING! We have launched our website.

💥 Now you can buy our (Office 365 private page) from store. 🔥

Dadsec Ott (Office 365 private page) Features.

- ➕ True Login
- ➕ Bypass 2FA
- ➕ Grab Cookie
- ➕ Cookie last up to 1 year
- ➕ Multiple Login Page Themes Available
- ➕ Supported all GoDaddy/SSO & other 365 Organizations with 2FA
- ➕ Randomized Page Code
- ➕ Offline attachment feature
- ➕ Grab company logo on offline attachment before page loaded
- ➕ Deliver Valid & Invalid Result Also Cookie To Email or Telegram
- ➕ Works With Cloudflare Recaptcha
- ➕ Admin Panel To Monitoring Result
- ➕ Saved Valid & Invalid Login
- ➕ Private VIP Antibot
- ➕ Latest Office365 Display
- ➕ Detect Company Logo, Background & Text Info
- ➕ Full Encrypted
- ➕ Auto Grab Email
- ➕ Supported On All Senders
- ➕ Auto Update
- ➕ Renew every month

Our Store: https://dadsec.store/ 768 edited 11:59

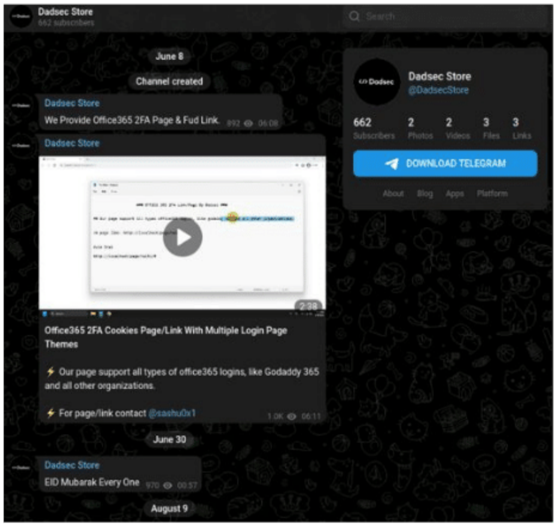


August 8

Dadsec

"Join our Telegram channel for the latest updates."

https://t.me/DadsecStore 411 edited 11:16



Dadsec Store
662 subscribers

June 8

Channel created

Dadsec Store
We Provide Office365 2FA Page & Fud Link. 892 06:08

Dadsec Store

Office365 2FA Cookies Page/Link With Multiple Login Page Themes

⚡ Our page support all types of office365 logins, like Godaddy 365 and all other organizations.

⚡ For page/link contact @sashu0x1 1.0K 06:11

June 30

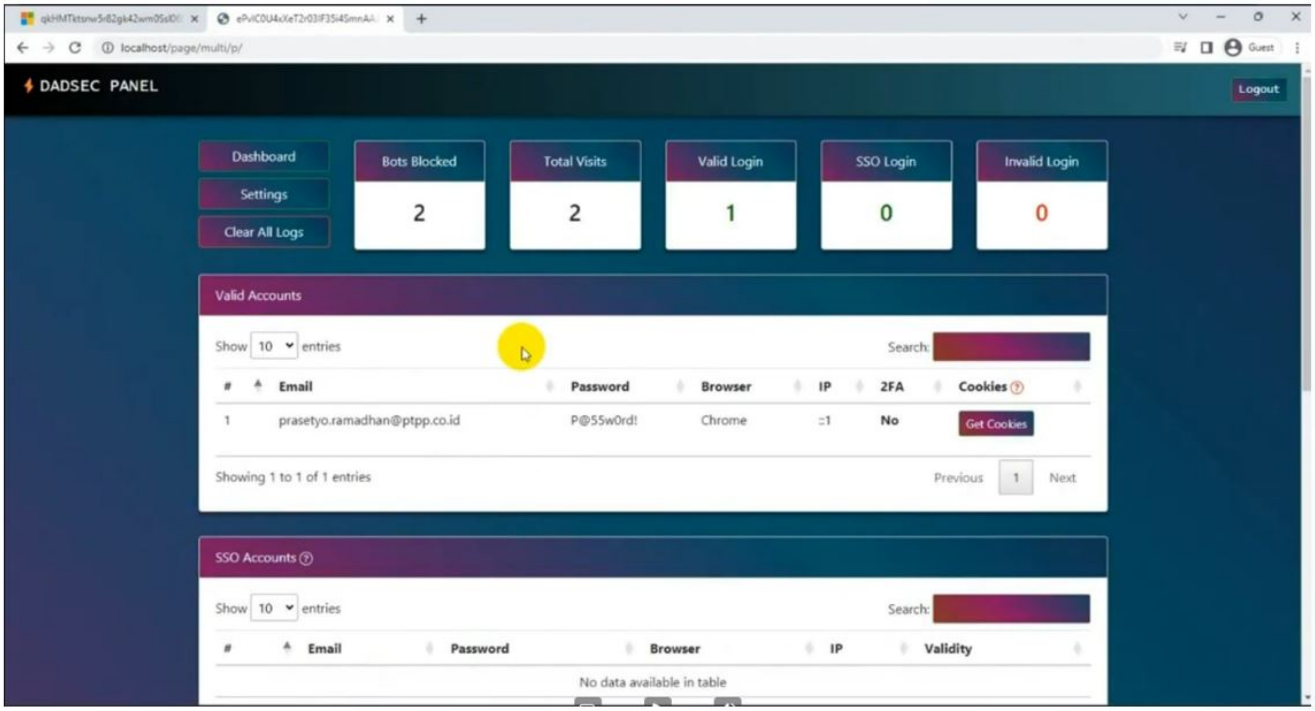
Dadsec Store
EID Mubarak Every One 970 00:57

August 9

Dadsec Store
@DadsecStore

662 Subscribers 2 Photos 2 Videos 3 Files 3 Links

On the Dadsec store Telegram channel the developer takes users through how the phishing kit works, including grabbing and using Cookies to login in to compromised Microsoft 365 accounts, examples of the different themes as well as access and management to the phishing panels:



⚡ DADSEC PANEL

Bots Blocked	Total Visits	Valid Login	SSO Login	Invalid Login
2	2	1	0	0

Valid Accounts

Show 10 entries Search:

#	Email	Password	Browser	IP	2FA	Cookies
1	prasetyo.ramadhan@ptpp.co.id	P@55w0rd!	Chrome	::1	No	Get Cookies

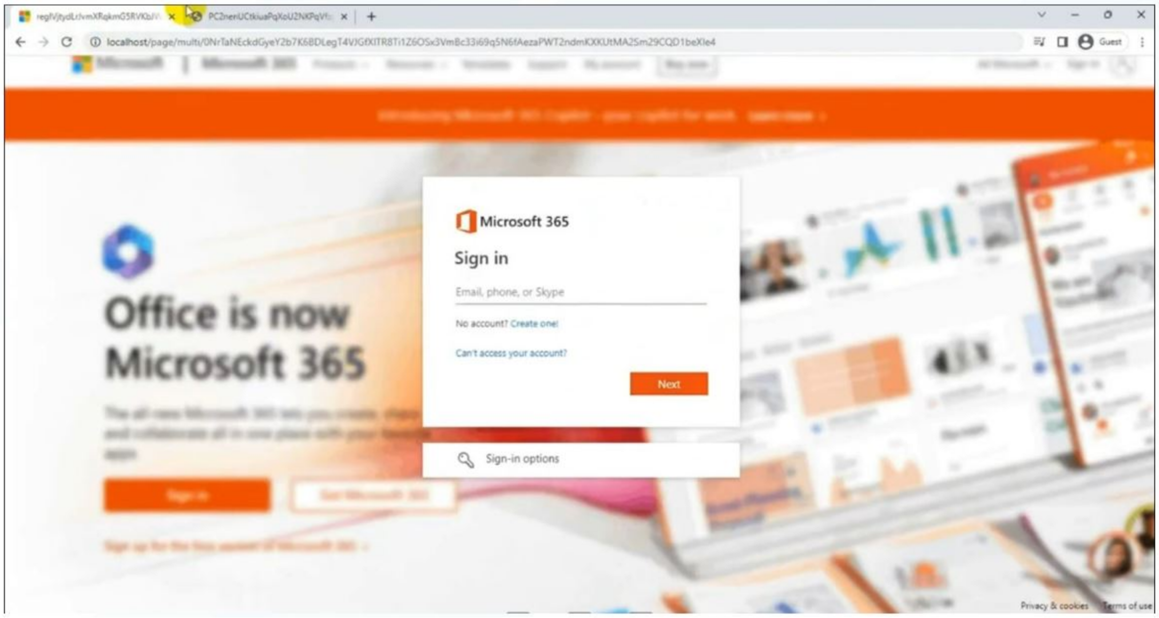
Showing 1 to 1 of 1 entries

SSO Accounts

Show 10 entries Search:

#	Email	Password	Browser	IP	Validity
No data available in table					

Figure 16. Dadsec Panel


localhost/page/multi/0NrTaNEckdGyeY2b7K6BDLegT4VJGfXITR8Ti1Z6OSx3VmBc33i69q5N6fAezaPWT2ndmKXKUtMA2Sm29CQD1beXle4

Microsoft 365

Sign in

Email, phone, or Skype

No account? Create one!

Can't access your account?

Next

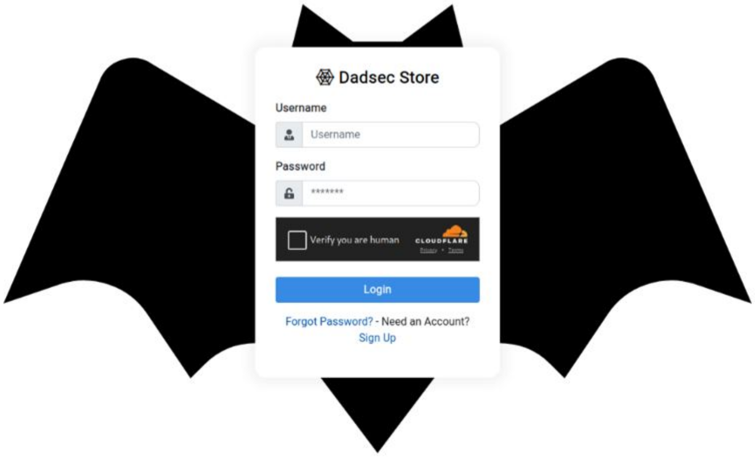
Sign-in options

Office is now Microsoft 365

Figure 17. Dadsec harvesting page example

5.2.1 Dadsec Store

The new Dadsec store website, **dadsec[.]store**, is hosted on Namecheap in the US and is also protected by Cloudflare captcha on the login portal.


Dadsec Store

Username: Username

Password: *******

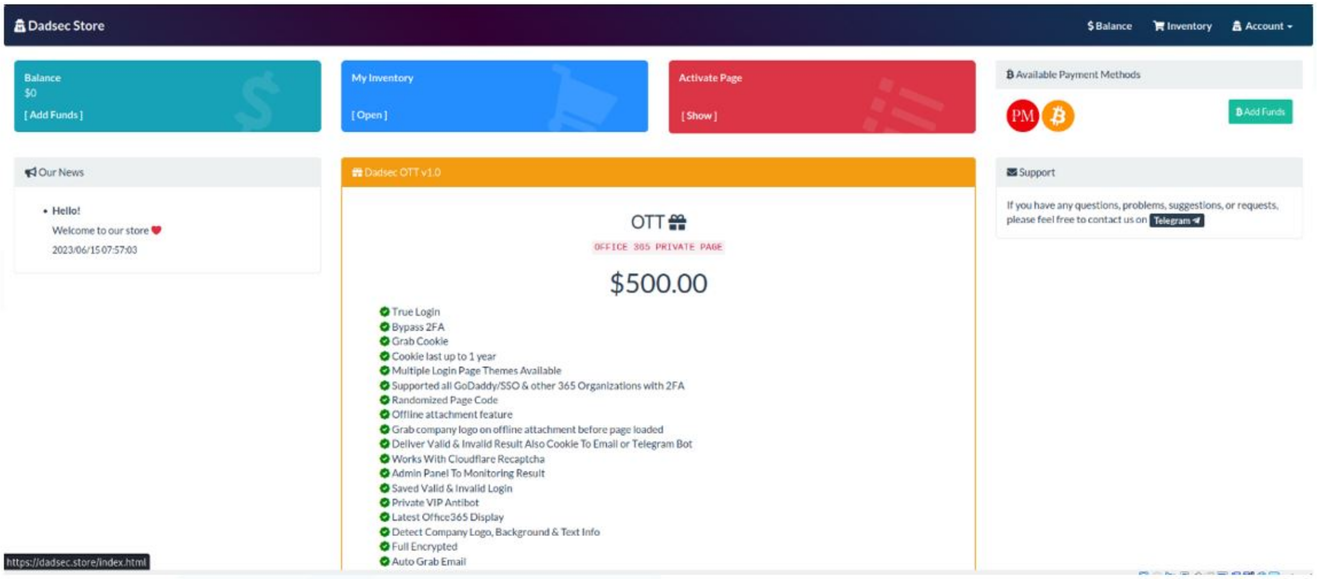
□ Verify you are human

Login

Forgot Password? - Need an Account? Sign Up

Figure 18. Dadsec Store login panel

Once you've logged in to the portal, you are met with the following dashboard:



Dadsec Store

$ Balance · Inventory · Account ▾

Balance
$0
[Add Funds]

My Inventory
[Open]

Activate Page
[Show]

Available Payment Methods

PM ₿ · Add Funds

Our News

- **Hello!**
  Welcome to our store ❤
  2023/06/15 07:57:03

Dadsec OTT v1.0

OTT

OFFICE 365 PRIVATE PAGE

$500.00

- ✓ True Login
- ✓ Bypass 2FA
- ✓ Grab Cookie
- ✓ Cookie last up to 1 year
- ✓ Multiple Login Page Themes Available
- ✓ Supported all GoDaddy/SSO & other 365 Organizations with 2FA
- ✓ Randomized Page Code
- ✓ Offline attachment feature
- ✓ Grab company logo on offline attachment before page loaded
- ✓ Deliver Valid & Invalid Result Also Cookie To Email or Telegram Bot
- ✓ Works With Cloudflare Recaptcha
- ✓ Admin Panel To Monitoring Result
- ✓ Saved Valid & Invalid Login
- ✓ Private VIP Antibot
- ✓ Latest Office365 Display
- ✓ Detect Company Logo, Background & Text Info
- ✓ Full Encrypted
- ✓ Auto Grab Email

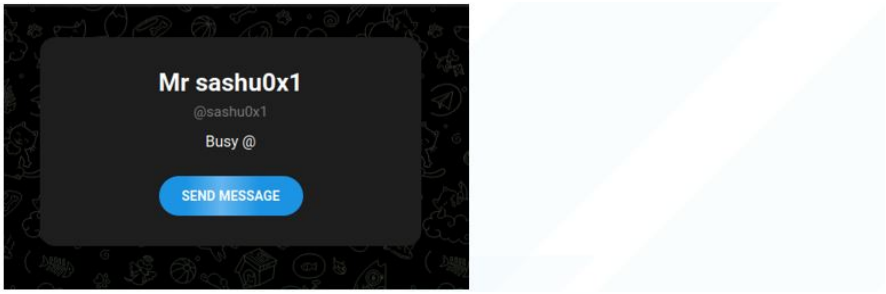
Support

If you have any questions, problems, suggestions, or requests, please feel free to contact us on Telegram

https://dadsec.store/index.html

Figure 19. Dadsec store page

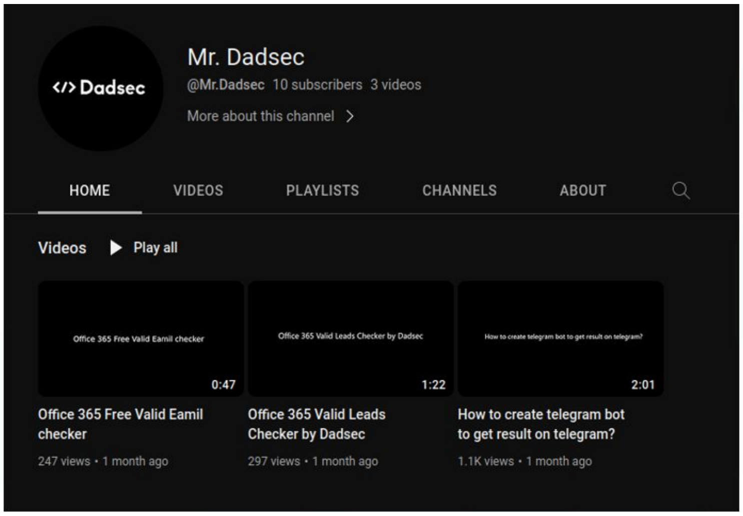
The only item that can be purchased is the “OTT” Office 365 tool which can be activated once purchased for $500. Payment can be made via Bitcoin and PerfectMoney. The support provided on the platform takes you to the Telegram account “Mr sashu0x1”, which differs from the Telegram account “Dadsec Store”:



Mr sashu0x1
@sashu0x1
Busy @

Figure 20. Telegram account for “Mr sashu0x1”

Additionally, the developer behind Dadsec also created a YouTube account on June 8th with other instruction videos:



</> Dadsec
HOME
VIDEOS
PLAYLISTS
CHANNELS
ABOUT
Videos
Play all
Office 365 Free Valid Eamil checker
Office 365 Valid Leads Checker by Dadsec
How to create telegram bot to get result on telegram?
0:47
1:22
2:01

Mr. Dadsec

@Mr.Dadsec 10 subscribers 3 videos

More about this channel

Office 365 Free Valid Eamil checker
247 views • 1 month ago

Office 365 Valid Leads Checker by Dadsec
297 views • 1 month ago

How to create telegram bot to get result on telegram?
1.1K views • 1 month ago

Figure 21. Dadsec YouTube Channel

5.3 Linking Campaign infrastructure to Dadsec

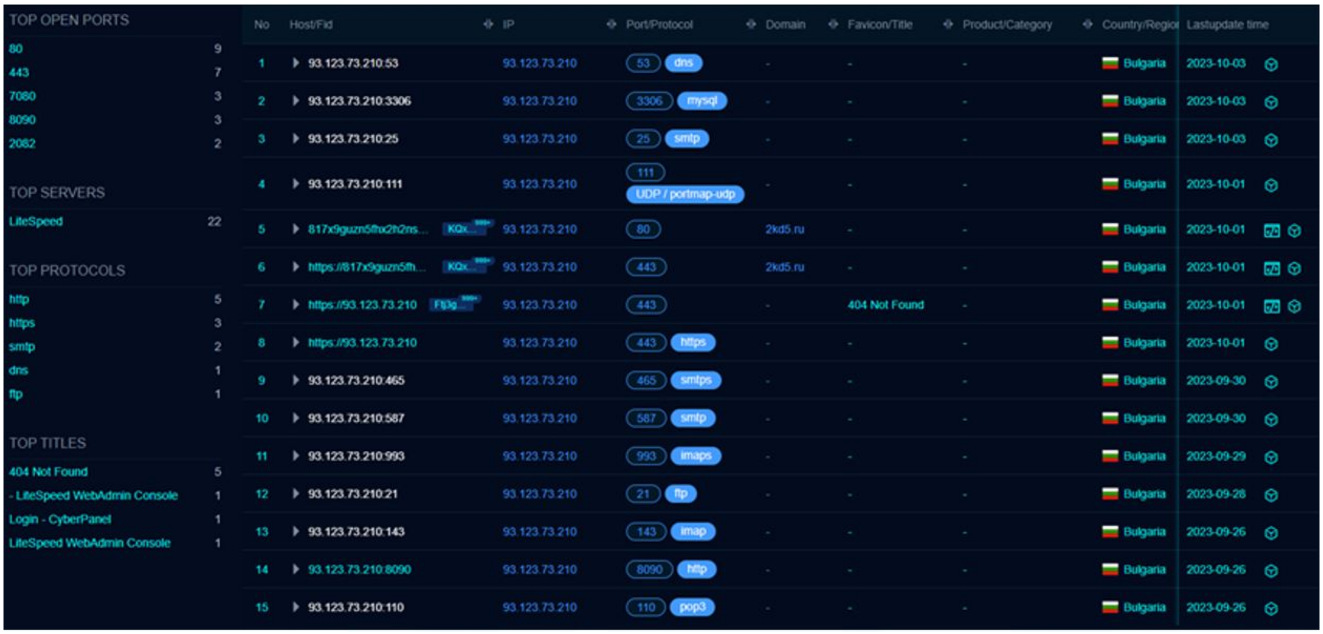
During analysis, we were able to single out backend infrastructure that hosted credential pages from domains linked to this campaign.

The following IP addresses are involved in this campaign:

- 95.216.158[.]157
- 93.123.73[.]210

Country	IP Address	Host	Organisation
FI	95.216.158[.]157	www.6gdta4cfx7iibgg960im.7heob05.ru	Hetzner Online GmbH
BG	93.123.73[.]210	https://k68w0vrsnw3suiun72v9.zaq3.ru	Verdina Ltd.
BG	93.123.73[.]210	https://817x9guzn5fhx2h2nsze.2kd5.ru	Verdina Ltd.
BG	93.123.73.210	https://www.h6thcl5jiwvvx030mvxk.f3u1.ru	Verdina Ltd.

5.3.1 Analysing the backend servers



TOP OPEN PORTS	
80	9
443	7
7080	3
8090	3
2082	2

TOP SERVERS	
LiteSpeed	22

TOP PROTOCOLS	
http	5
https	3
smtp	2
dns	1
ftp	1

TOP TITLES	
404 Not Found	5
- LiteSpeed WebAdmin Console	1
Login - CyberPanel	1
LiteSpeed WebAdmin Console	1

No	Host/Fid	IP	Port/Protocol	Domain	Favicon/Title	Product/Category	Country/Regior	Lastupdate time
1	93.123.73.210:53	93.123.73.210	53 dns	-	-	-	Bulgaria	2023-10-03
2	93.123.73.210:3306	93.123.73.210	3306 mysql	-	-	-	Bulgaria	2023-10-03
3	93.123.73.210:25	93.123.73.210	25 smtp	-	-	-	Bulgaria	2023-10-03
4	93.123.73.210:111	93.123.73.210	111 UDP / portmap-udp	-	-	-	Bulgaria	2023-10-01
5	817x9guzn5fhx2h2ns... KQx... 999+	93.123.73.210	80	2kd5.ru	-	-	Bulgaria	2023-10-01
6	https://817x9guzn5fh... KQx... 999+	93.123.73.210	443	2kd5.ru	-	-	Bulgaria	2023-10-01
7	https://93.123.73.210 Ftj3g... 999+	93.123.73.210	443	-	404 Not Found	-	Bulgaria	2023-10-01
8	https://93.123.73.210	93.123.73.210	443 https	-	-	-	Bulgaria	2023-10-01
9	93.123.73.210:465	93.123.73.210	465 smtps	-	-	-	Bulgaria	2023-09-30
10	93.123.73.210:587	93.123.73.210	587 smtp	-	-	-	Bulgaria	2023-09-30
11	93.123.73.210:993	93.123.73.210	993 imaps	-	-	-	Bulgaria	2023-09-29
12	93.123.73.210:21	93.123.73.210	21 ftp	-	-	-	Bulgaria	2023-09-28
13	93.123.73.210:143	93.123.73.210	143 imap	-	-	-	Bulgaria	2023-09-26
14	93.123.73.210:8090	93.123.73.210	8090 http	-	-	-	Bulgaria	2023-09-26
15	93.123.73.210:110	93.123.73.210	110 pop3	-	-	-	Bulgaria	2023-09-26

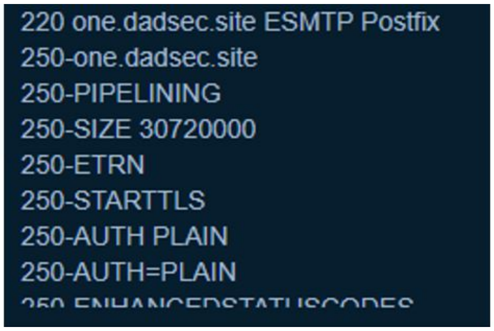
Figure 22. Inspecting the backend servers for open services

By analysing the open ports and banners for these IP addresses we can gather additional information.

93.123.73[.]210 is running a number of open ports and services. Based on the following screenshot we can see from the Cyber Panel that the server is running LiteSpeed and also has SMTP, DNS and FTP ports open. Additionally, we see the domains and subdomains on ports 80 and 443 as well as portmapper on port 111.

The same ports and services were running on however, the SMTP banner was slightly different and didn't reference Dadsec, instead the following string was observed "three.enb6lvl.site".

Looking at the SMTP port 25, we can check the banner information. The notable observation is the reference to Dadsec, allowing us to connect this back to the Dadsec platform. This information is also visible on port 465 for SMTPS:



```
220 one.dadsec.site ESMTP Postfix
250-one.dadsec.site
250-PIPELINING
250-SIZE 30720000
250-ETRN
250-STARTTLS
250-AUTH PLAIN
250-AUTH=PLAIN
250-ENHANCEDSTATUSCODES
```

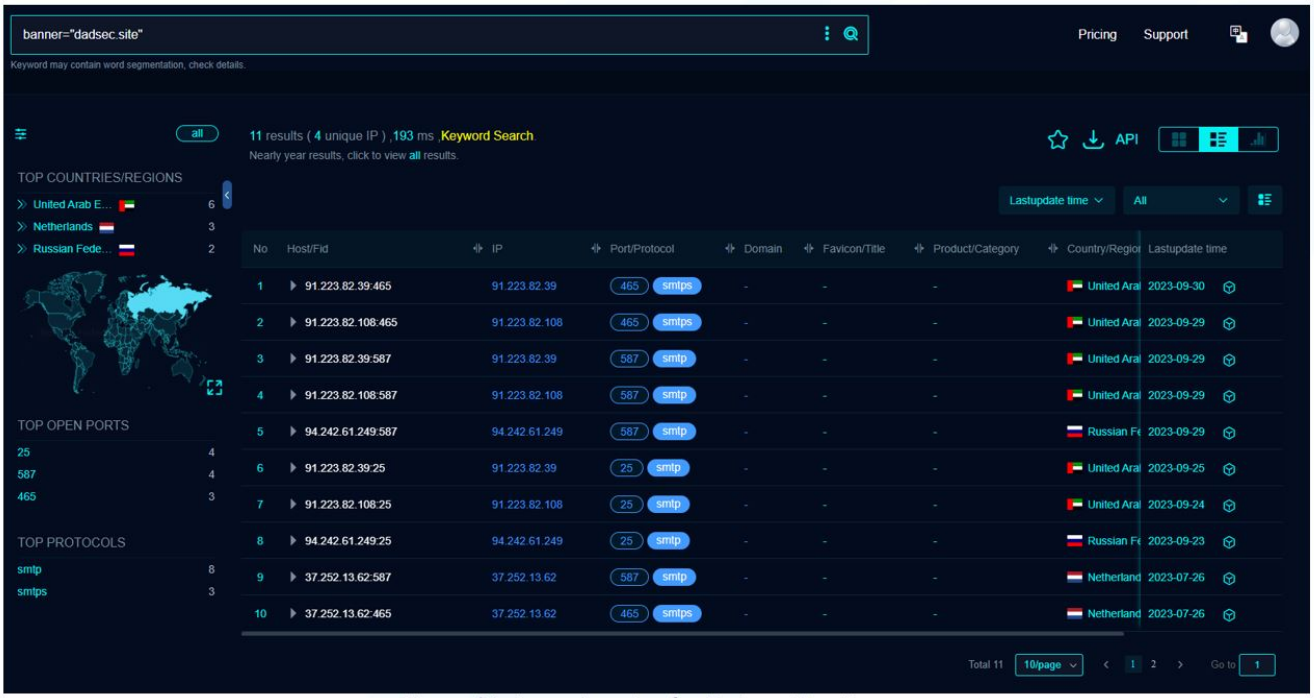
Figure 23. SMTP service banner

5.3.2 Hosting providers

Hetzner Online GmbH and Verdina Ltd. appear to be two hosting providers of choice for the threat actors. These hosting providers provide automated deployment of tools such as Cyber Panel, making them an obvious choice for the threat actors.

5.3.3 Hunting for Dadsec

Now that we know some SMTP mail servers reference Dadsec, we can use this information to uncover other potential mail servers utilised by the threat actors in this campaign:



banner="dadsec.site"

Keyword may contain word segmentation, check details.

11 results (4 unique IP) ,193 ms ,Keyword Search.
Nearly year results, click to view all results.

TOP COUNTRIES/REGIONS

United Arab E...	6
Netherlands	3
Russian Fede...	2

TOP OPEN PORTS

25	4
587	4
465	3

TOP PROTOCOLS

smtp	8
smtps	3

No	Host/Fid	IP	Port/Protocol	Domain	Favicon/Title	Product/Category	Country/Regioi	Lastupdate time
1	91.223.82.39:465	91.223.82.39	465 smtps	-	-	-	United Aral	2023-09-30
2	91.223.82.108:465	91.223.82.108	465 smtps	-	-	-	United Aral	2023-09-29
3	91.223.82.39:587	91.223.82.39	587 smtp	-	-	-	United Aral	2023-09-29
4	91.223.82.108:587	91.223.82.108	587 smtp	-	-	-	United Aral	2023-09-29
5	94.242.61.249:587	94.242.61.249	587 smtp	-	-	-	Russian Fe	2023-09-29
6	91.223.82.39:25	91.223.82.39	25 smtp	-	-	-	United Aral	2023-09-25
7	91.223.82.108:25	91.223.82.108	25 smtp	-	-	-	United Aral	2023-09-24
8	94.242.61.249:25	94.242.61.249	25 smtp	-	-	-	Russian Fe	2023-09-23
9	37.252.13.62:587	37.252.13.62	587 smtp	-	-	-	Netherland	2023-07-26
10	37.252.13.62:465	37.252.13.62	465 smtps	-	-	-	Netherland	2023-07-26

Total 11 10/page < 1 2 > Go to 1

Figure 24. Image hunting for Dadsec IP addresses

AS_Organisation	IP	Port	Country
Iws Networks LLC	91.223.82[.]108	25	AE
Iws Networks LLC	91.223.82[.]39	465	AE
Iws Networks LLC	91.223.82[.]108	465	AE
Iws Networks LLC	91.223.82[.]39	587	AE
Iws Networks LLC	91.223.82[.]108	587	AE
SIA VEESP	94.242.61[.]249	587	RU
Iws Networks LLC	91.223.82[.]39	25	AE
SIA VEESP	94.242.61[.]249	25	RU

AS_Organisation	IP	Port	Country
Scalaxy B.V.	37.252.13[.]62	587	NL
Scalaxy B.V.	37.252.13[.]62	465	NL
Scalaxy B.V.	37.252.13[.]62	25	NL

The search above identifies other infrastructure utilising the Dadsec platform and may be linked to this campaign.

6. Collaborating with ANY.RUN

During our research, CTI identified a post by a security researcher working at ANY.RUN, highlighting a regular expression query to capture phishing domains that matched the domains that we had observed. We reached out to them in order to share findings and collaborate to understand the extent of this campaign.

ANY.RUN had the following comments:

"After analyzing the structure of the phishing campaign domains that you provided, we hypothesized that an automated domain name generation system was being used, similar to Domain Generation Algorithms (DGAs), which we sometimes see in malware examined by our analytics department. This was confirmed by the uniform frequency distribution of the alphabet characters that make up domain names.

Despite this challenge, we were determined to protect our customers. To that end, we created network rules for the Suricata IDS (Intruder Detection System), a system for detecting unwanted network activity used in http://ANY.RUN. These rules rely on regular expressions to distinguish suspicious sequences of domain name characters from the domain names generated by ordinary users. In this case, the "letter-digit-letter" and "digit-letter-digit" character combinations, as well as the lengths of domains and subdomains, played an important role.

By implementing these rules in our service, we were able to enhance its detection capabilities and discover the significant scale of the malicious campaign. As a result, we increased the visibility of phishing public submissions to our users by about 2x, identifying approximately 650 phishing alerts across the samples submitted by our users per day."

A number of examples are provided below:

https://app.any.run/tasks/60c8ef7a-c89f-435d-96cc-f6a1832a4095/

https://app.any.run/tasks/8fc0327e-2122-442a-a7b1-becce5b39fe0/

https://app.any.run/tasks/f3330f01-65cd-4353-8af5-e4f14b013d6f/

Many thanks to Jane for collaborating with us on this research and providing insight and support, including the generation of new detection content through the ANY.RUN platform.

7. Action Taken

By uncovering this dataset and information, we were able to:

- Provide technical intelligence back to the SOC for retrospective searches within the timescale of the campaign in our customer environments. This uncovered additional successful connection network events from two more of our customers, allowing us to reset user accounts. This allowed us to identify missed alerts from security tooling.
- Create analytics for our security tooling to alert on connections to new infrastructure linked to this platform and campaign, further protecting our customers in real-time.

After conducting our analysis we are able to answer a number of the questions posed by our IR teams at the beginning of the incident:

7.1 Was there a connection between our customers?

We don't believe there was any direct connection between Bridewell's customers, a broad spectrum of sectors are affected by this campaign.

7.2 Were there other similar phishing emails delivered to our customers?

Yes, other customers were affected by this campaign. At the time of receiving the phishing emails, no security products were detecting the links as phishing however, no compromise was detected, and user accounts were reset as a precaution.

7.3 Do we have any more information about this campaign?

We now know this campaign is utilising the Dadsec platform and can potentially be linked to a threat actor called Storm-1575 by Microsoft. The campaign is ongoing and generating new domains and VT submissions every month. CTI has enabled the SOC to conduct retro hunts and generate new detections moving forward.

8. Takeaway

Intrusion analysis is a valuable tool for any security team focused on threat intelligence. Intrusion analysis models allow those tasked with generating cyber threat intelligence to quickly analyse large amounts of incoming data and establish clear linkages between various pieces of threat information. The outcome for your security teams is a better understanding of adversary intents and strategies, which enables your business to develop proactive countermeasures against new and emerging cyber threats.

By consuming a threat intelligence service, you should expect that intrusion analysis is being performed by the threat intelligence team. This will ensure they are producing actionable insights and intelligence from attempted and successful attacks against your organisation. Bridewell CTI uses a blend of automated and manual analysis processes to keep you informed and protected against credible threats to your business and sector.

Author

Joshua Penny

Senior Threat Intelligence Analyst

Linkedin