

CREDENTIAL HARVESTING

CAMPAIGNS, TARGETING UKRAINIAN ORGANIZATIONS

March 2023



The State Cyber Protection Centre of
the State Service of Special Communication and Information
Protection of Ukraine

<https://scpc.gov.ua/>

TLP:CLEAR

Executive Summary

Multiple variants of the same mass infostealing attack **targeting Ukrainian organizations of all forms of ownership** have been tracked by The Cyber Incidents Response Operational Centre of the State Cyber Protection Centre of Ukraine since the beginning of 2023.

All the detected emails as well as attached files are **composed in Russian language**, usually include **impersonation of the targeted entities** and **manipulate the password expiring theme**, luring the victims to update credentials as soon as possible in order to save account access.

The Cyber Incidents Response Operational Centre of the State Cyber Protection Centre of Ukraine has prepared the detailed analysis of the credential harvesting attack chains that are considered further in the report.

Table of Contents

Background Case Study	3
Initial Access	3
Phishing sites abusing GoDaddy platform	3
Attack Chain	5
Recent Credential Harvesting Case Study	6
Initial Access	6
Attack Chain	8
Attack Landscape and Infrastructure Analysis	8
Outlook	12
Indicators of Compromise	13
MITRE ATT&CK®Context	18

Background Case Study

Initial Access

On February, 14, 2023 the spear-phishing email targeted the user of Ukrainian email service "UKR.NET" (the general contact email of the organization that is registered and currently functioning in Ukraine). It was **the only discovered variant of such infostealing campaign where a .pdf file was distributed** as an attachment.

The email content states that the password for the targeted email account "expires today" and instructions from the attached file should be followed in order to save the current password and update the account.

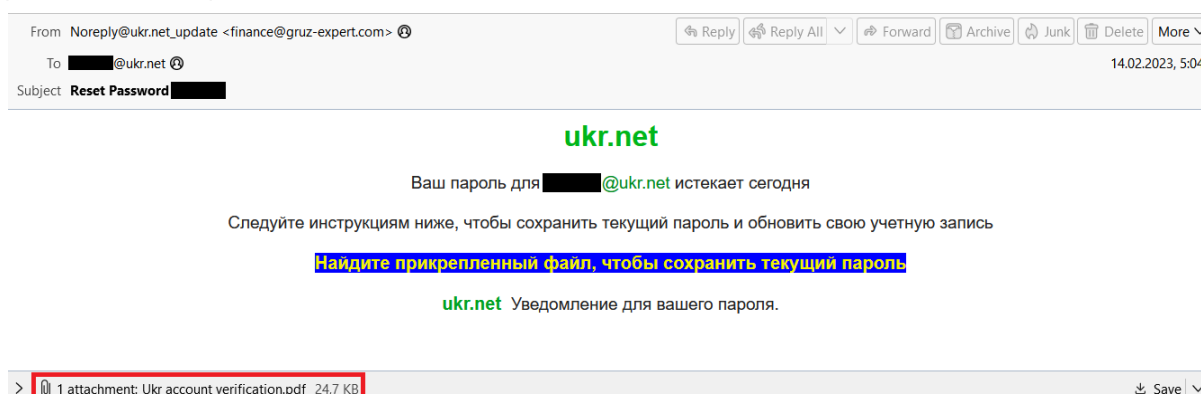


Fig1 - The spear-phishing email content

Phishing sites abusing GoDaddy platform

The content of the [.pdf file](#) named "Ukr account verification.pdf" lures the victim to click on "Нажмите здесь, чтобы подтвердить учетную запись" ("Click here to verify the account").



требуется проверка аккаунта

[Нажмите здесь, чтобы подтвердить учетную запись](#)

Примечание. Через 24 часа все неактивные учетные записи ukr.net будут деактивированы

Fig2 - The content of .pdf attachment

Strings, extracted from this .pdf file, contain the next links:

- [https://account_verification\[.\]godaddysites\[.\]com/updatemail](https://account_verification[.]godaddysites[.]com/updatemail)
- [https://notification9\[.\]godaddysites\[.\]com/login](https://notification9[.]godaddysites[.]com/login)
- [https://services194\[.\]godaddysites\[.\]com/login](https://services194[.]godaddysites[.]com/login)
- [https://account70\[.\]godaddysites\[.\]com/login](https://account70[.]godaddysites[.]com/login)
- [https://functionalities\[.\]godaddysites\[.\]com/temporarily](https://functionalities[.]godaddysites[.]com/temporarily)

The last one is resolved for the user redirection after clicking on the verification button.

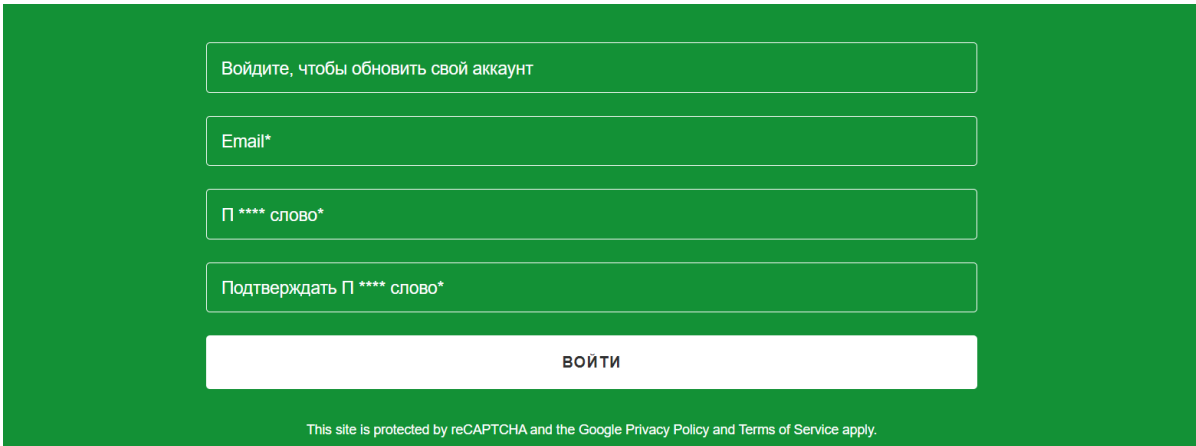
GoDaddy is a platform provider, hosting content on their own domain names on behalf of their users. [GoDaddy's website builder](#) is an online editing and publishing tool that allows quick website creation and hosting its content on GoDaddy's resources during a free trial period. This feature was used by the adversaries for creating phishing sites:

- **account_verification[.]godaddysites[.]com;**
- **notification9[.]godaddysites[.]com;**
- **services194[.]godaddysites[.]com;**
- **account70[.]godaddysites[.]com;**
- **functionalities[.]godaddysites[.]com** and in such a way abusing the GoDaddy platform.

```
13 0 obj<</S/URI/URI (https://account_verification.godaddysites.com/updatesmail-com)>>
14 0 obj<</S/URI/URI (https://notification9.godaddysites.com/login)>>
15 0 obj<</S/URI/URI (https://services194.godaddysites.com/login)>>
16 0 obj<</S/URI/URI (https://account70.godaddysites.com/login)>>
17 0 obj<</Type/Action/S/URI/URI (https://functionalities.godaddysites.com/temporarily)>>
```

Fig3 - Extracted strings

At the time of writing (March, 3, 2023), all the malicious subdomains of **godaddysites[.]com** mentioned above are inactive, but the [.html file](#) was discovered among the researched IoCs that are related to this activity and is considered to be the latest file downloaded from **hxxps://functionalities[.]godaddysites[.]com/temporarily** URL.



The image shows a login form on a green background. At the top, it says "Войдите, чтобы обновить свой аккаунт" (Log in to update your account). Below this are four input fields: "Email*", "П **** слово*" (Password **** word*), and "Подтверждать П **** слово*" (Confirm Password **** word*). At the bottom is a white button labeled "ВОЙТИ" (Log in). A small footer text reads: "This site is protected by reCAPTCHA and the Google Privacy Policy and Terms of Service apply."

Fig4 - The content of .html file

In this `.html` file `<script>` element points to an **external script file** (located at **hxxps://img1[.]wsimg[.]com/blobby/go/cd8014df-5cfb-40a3-a0ce-43dda9eb71c9/gpub/6984e83ccc84af61/script[.]js**) through the `src` attribute.

According to the script functionality, the submitted results are sent over HTTPS request to **hxxps://contact[.]apps-api[.]instantpage[.]secureserver[.]net** that is a legitimate URL used for processing feedback forms submissions within the GoDaddy Website Builder.

```

Core.utils.deferBootstrap({
  elId: 'bs-2',
  componentName: '@widget/CONTACT/bs-contact1-contact-form',
  props: JSON.parse('{"formTitle":"","formFields":[{"type":"SINGLE_LINE","label":"Войдите, чтобы обновить свой аккаунт","required":false,"keyName":"name"}, {"type":"EMAIL","label":"Email","validation":"email","required":true,"replyTo":true,"keyName":"email"}, {"type":"SINGLE_LINE","label":"[] **** слово","required":true,"keyName":"message"}, {"label":"Подтвердите [] **** слово","type":"SINGLE_LINE","required":true}, {"type":"ATTACHMENT","label":"Attachments","required":false}, {"type":"SUBMIT","label":"Войти","required":false}], "blankInfo":true, "formSubmitHost":"https://contact.apps-api.instantpage.secureserver.net", "showMap":false, "recaptchaEnabled":true, "recaptchaType":"V3", "domainName":"functionalities.godaddysites.com", "formSuccessMessage":{"blocks":[{"key":"djp2k"}, {"text":"https://mail.ukr.net/"}], "type":"unstyled", "depth":0, "inlineStyleRanges": [], "entityRanges": [], "data": {}, "entityMap": {}}, "formEnabled":true, "websiteId":"cd8014df-5cfb-40a3-abce-43dda9eb71c9", "pageId":"f4e053ff-f503-4643-afbc-64f9557ae96c", "accountId":"5d661098-9c86-11ed-82c6-3417eb7253b", "staticContent":{"today":"Today", "submitButtonLoadingLabel":"Sending", "contactFormResponseErrorMessage":"Something went wrong while sending your message, please try again later", "phoneValidationErrorMessage":"Please enter a valid phone number.", "defaultCancelButtonLabel":"Cancel", "byAppointment":"By Appointment", "defaultSubmitButtonLabel":"Send", "unsupportedFileType":"Unsupported file type", "maxFileCountLimit":"Only {0} files are allowed", "closed":"Closed", "attachments":"Attachments", "termsOfService":"Terms of Service", "attachFiles":"Attach Files", "recaptchaDisclosure":"This site is protected by reCAPTCHA and the Google {privacyPolicy} and {termsOfService} apply.", "emailValidationErrorMessage":"Please enter a valid email address.", "mapCTA":"Get directions", "privacyPolicyURL":"https://policies.google.com/privacy", "requiredValidationErrorMessage":"Please fill in this required field", "openToday":"Open today", "couldNotAttach":"Could not attach the following file(s)", "totalFileSizeLimit":"Total files would exceed {0} limit", "privacyPolicy":"Privacy Policy", "termsOfServiceURL":"https://policies.google.com/terms", "fileSizeLimit":"File exceeds {0} limit", "emailMaxCountValidationErrorMessage":"Your email address is too long"}, "emailOptInEnabled":false, "emailOptInMessage":"Sign up for our email list for updates, promotions, and more.", "emailConfirmationMessage":"We've sent you a confirmation email, please click the link to verify your address.", "widgetId":"c6614abf-dd03-4ce8-bc10-72c8133b7fc8", "section":"default", "category":"primary", "locale":"en-GB", "env":"production", "renderMode":"PUBLISH"}, context: JSON.parse('{"widgetId":"c6614abf-dd03-4ce8-bc10-72c8133b7fc8", "widgetType":"CONTACT", "widgetPreset":"contact1", "group":"Content", "groupType":"Default", "section":"default", "category":"primary", "fontSize":"medium", "fontFamily":"alternate", "websiteThemeOverrides": {}, "widgetThemeOverrides": {}}, contextKey: 'context-bs-2', radpack: '@widget/CONTACT/bs-contact1-contact-form', false);

```

Fig5 - The content of .html file

Attack Chain

The generalized attack chain scheme described above is shown in Fig6.

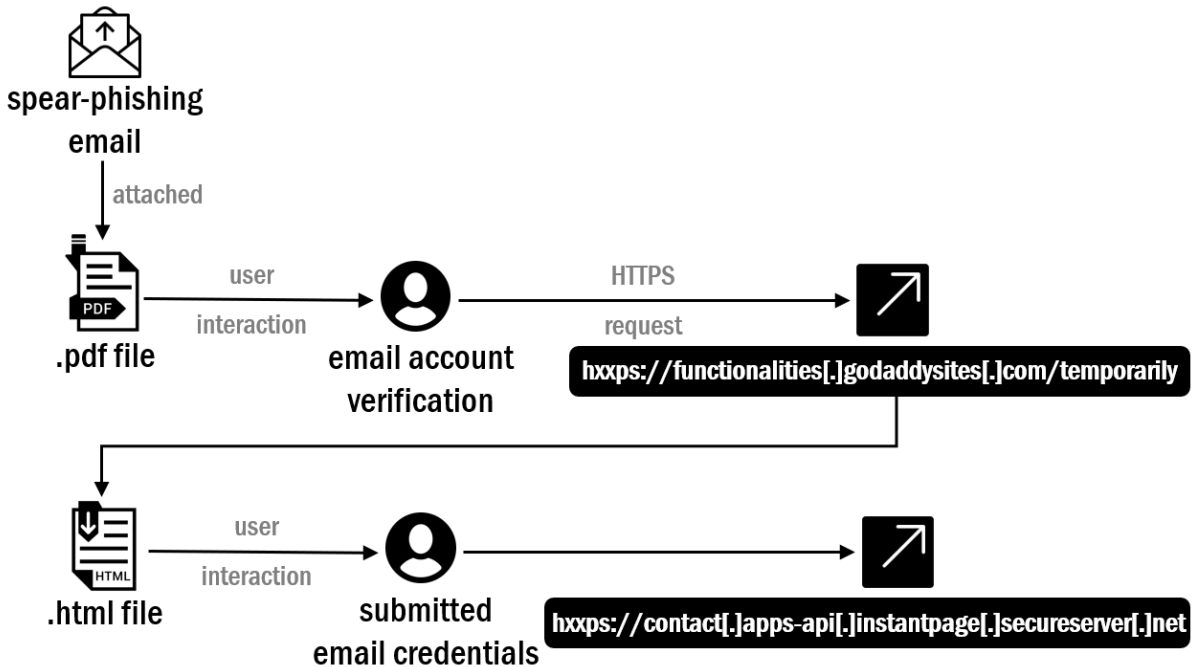


Fig6 - Attack chain overview

Newly discovered variants of infostealing campaigns that correspond to the same activity cluster are simplified through skipping the phase with the .pdf file and only .html/.shtml attachments have been disclosed in new credential harvesting campaigns.

Recent Credential Harvesting Case Study

Initial Access

On February, 24, 2023, the spear-phishing email was sent to the corporate email address of Region State Administration (one of the Ukrainian government organizations) as usually stating that the email account's password "expires today".

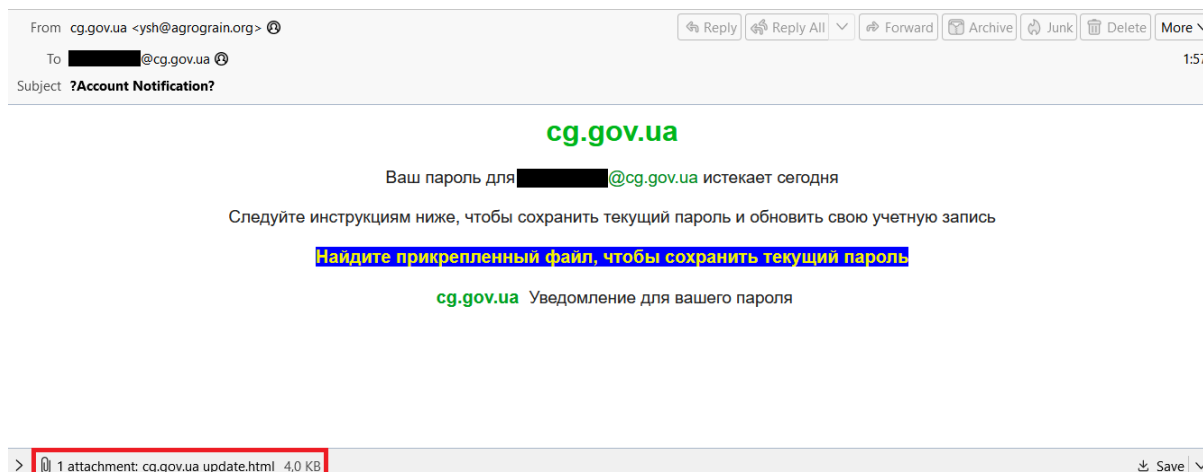


Fig7 - The spear-phishing email content

HTML code inside .html attachment contains **<form>** tag for creating an HTML form for user input with the **hardcoded "email" field** that corresponds to the targeted user.

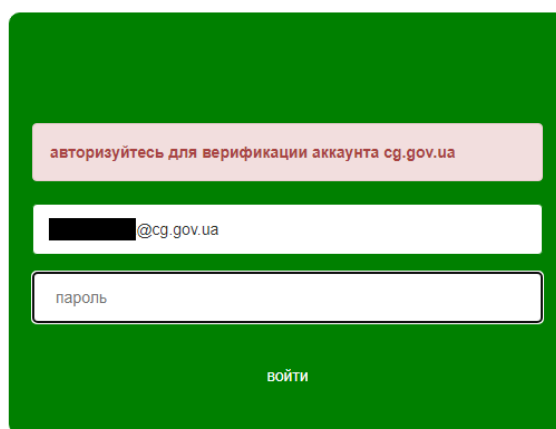


Fig8 - Phishing .html form

The **<form>** element includes the **action attribute** that specifies the submitted form-data is sent to **hxxps://aerotrustsystems[.]com/n/vk..php** via HTTPS POST request.

No.	Source	Destination	Protocol	Length	Info
	[redacted]	192.185.171.241	HTTP2	588	HEADERS[1]: POST /n/vk..php
	[redacted]	192.185.171.241	HTTP2	127	DATA[1] (application/x-www-form-urlencoded)

> Frame 310: 127 bytes on wire (1016 bits), 127 bytes captured (1016 bits) on interface intf0, id 0

> Ethernet II, Src: [redacted], Dst: ba:b7:a6:d4:a4:ff (ba:b7:a6:d4:a4:ff)

> Internet Protocol Version 4, Src: [redacted], Dst: 192.185.171.241

> Transmission Control Protocol, Src Port: 49783, Dst Port: 443, Seq: 1230, Ack: 4624, Len: 73

> Transport Layer Security

> HyperText Transfer Protocol 2

> Stream: DATA, Stream ID: 1, Length 42

> HTML Form URL Encoded: application/x-www-form-urlencoded

- > Form item: "Email" = "[redacted]@cg.gov.ua"
- > Form item: "Password" = "[redacted]"

Fig9 - Network capture of sending the submitted data over the HTTPS POST request

Attack Chain

The generalized attack chain scheme described above is shown in Fig12.

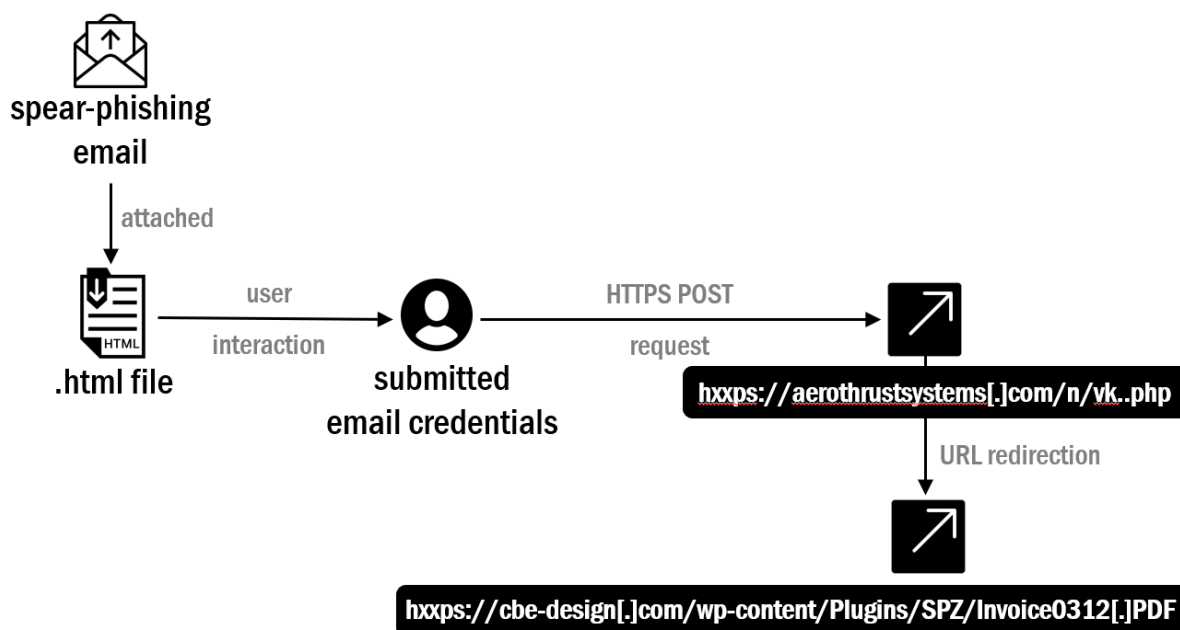


Fig12 - Attack chain overview

Attack Landscape and Infrastructure Analysis

Taking into account the specificity of emails and the variety of domains from which the spear-phishing emails are sent, it is possible to assume that these email accounts have been previously compromised in the same way in order to leverage them to conduct further phishing operations.

Based on the recent activity, the [.html file](#) was identified targeting [ysh@agrograin\[.\]org](mailto:ysh@agrograin[.]org) email account, from which the spear-phishing email was recently sent (described in [Recent Credential Harvesting Case Study](#) section), that confirms this hypothesis.

Following the tracked history of URLs from where the file **Invoice0312.PDF** has been downloaded and analyzing the domains related to these webpages, it can be concluded that **the phishing emails** attributed to the same activity cluster have been **distributed to the Ukrainian corporate email addresses since May, 2022**.

In May, 2022 the first related .html file with the hardcoded corporate email address targeting Ukrainian Joint Stock Bank Ukrgasbank (see Fig. 13,14) was discovered.



Fig13 - The content of .html file



Fig14 - The content of .html file after clicking "посмотреть файл" ("view file")

Overall, **48 phishing forms** of such sample targeting Ukrainian organizations have been distributed via .html, .shtml or .pdf email attachments since May, 2022.

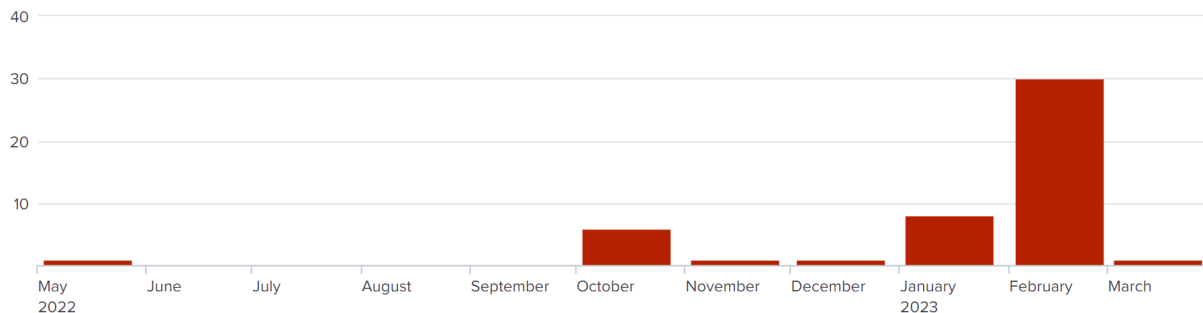


Fig15 - Timechart of the described phishing activity cluster, targeting Ukraine since May, 2022

The initial review highlights that the described phishing activity is **focused more on mass distribution rather than on accuracy** based on the prevalence of general contact emails, that can be easily retrieved from the official website contact page, **among the targeted corporate email addresses** and the variety of the targeted economy sectors.

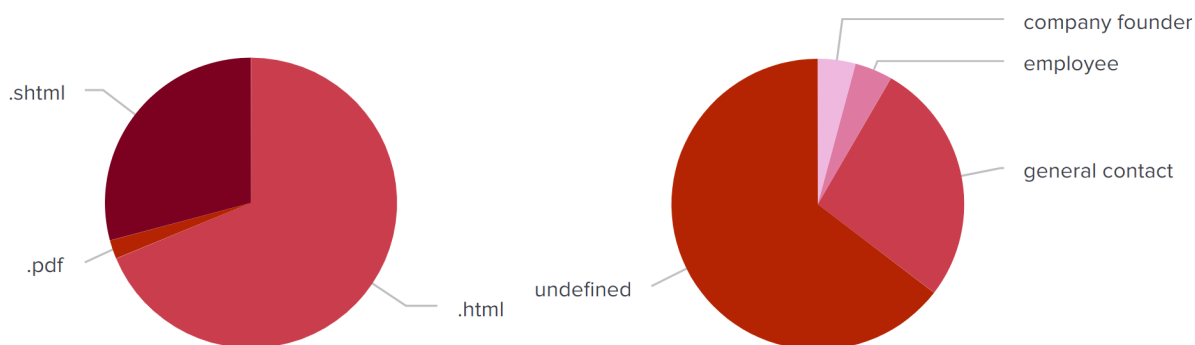


Fig16 - The proportionality of the distributed attachments by their extension

Fig17 - The proportionality of the distributed attachments by the categories of the targeted individuals (their relation to the targeted entity) the phishing emails were addressed to

According to the ratio of the distributed attachments by the form of ownership of the targeted entities, the **Commercial Facilities sector predominates**.

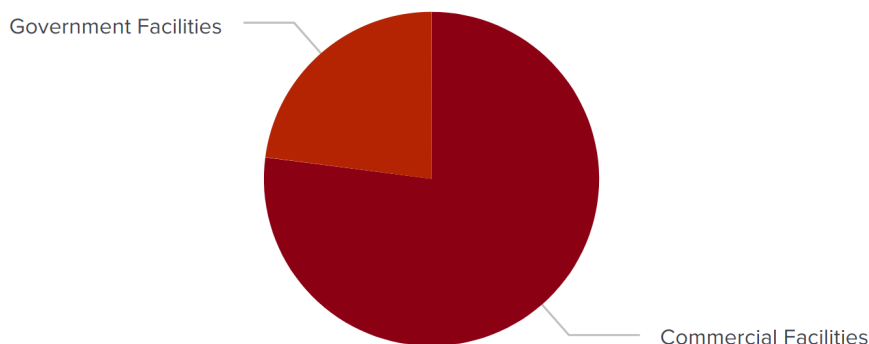


Fig18 - The proportionality of the distributed attachments by the property type of the targeted entities

Fig. 19, 20 display the proportionality of the distributed attachments across the targeted entities by economy sectors in which they operate.

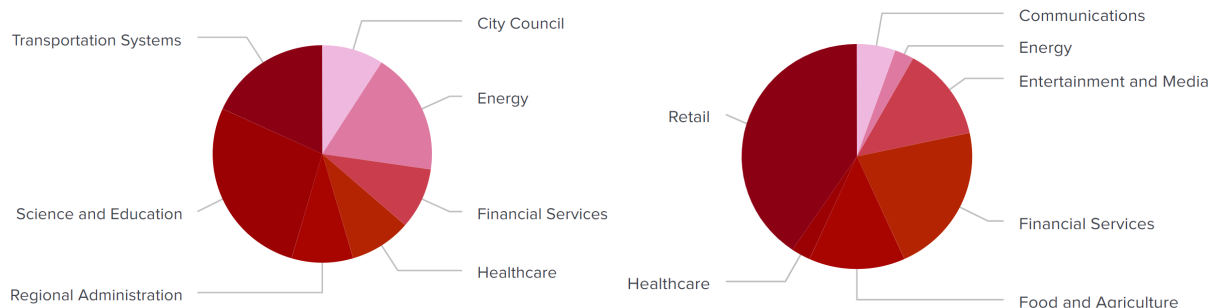


Fig19 - The proportionality of the distributed attachments across targeted entities (Government Facilities) by economy sectors to which they belong

Fig20 - The proportionality of the distributed attachments across targeted entities (Commercial Facilities) by economy sectors to which they belong

Fig. 21 displays the proportionality of DNS zones of the targeted domains that represent Ukrainian organizations.

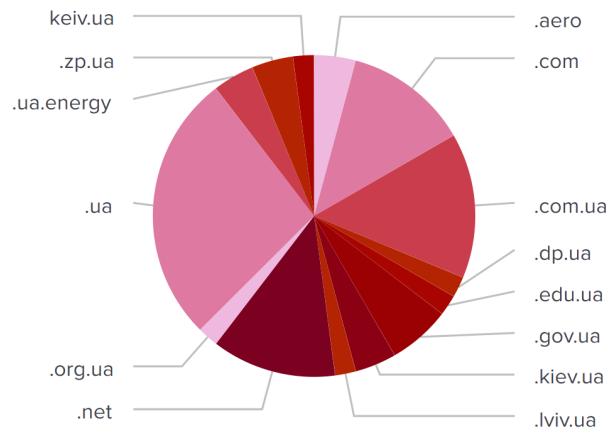


Fig21 - The proportionality of the targeted domain zones

Table1 provides information about all the discovered malicious domains identified during the analysis of the phishing forms distributed via email attachments to the corporate email addresses, the domains of which represent Ukrainian organizations.

domain	IP address	Registrar	Creation Date	Notes
aerothrustersystems[.]com	192.185.171.241	Instra Corporation Pty Ltd.	2022-09-02	Represents the company Aero Thrust System (ATS) located at Islamabad, Pakistan that manufactures industrial grade, aerial robotics and turn-key unmanned aerial system (UAS).
tyutta[.]com	162.241.219.188	FastDomain Inc.	2020-05-13	-
mangal-pab[.]vn[.]ua	31.41.216.90 31.41.217.90 5.9.177.94 195.248.235.241	ua.bestname	2019-12-02	-
rojowska[.]pl	195.78.66.225	Cyber_Folks S.A.	2020-07-06	-
thevetlounge[.]com[.]au	103.27.35.250	SYNERGY WHOLESALE PTY LTD	-	-

Table2 provides information about IP addresses of the domains mentioned in Table1.

IP	AS	AS name	Company name
192.185.171.241	AS19871	Network Solutions, LLC	WEBSITEWELCOME.COM
162.241.219.188	AS46606	Unified Layer	Unified Layer
31.41.216.90 31.41.217.90 195.248.235.241	AS42655	ON-LINE Ltd	ON-LINE Ltd
5.9.177.94	AS24940	Hetzner Online GmbH	Hetzner Online GmbH
195.78.66.225	AS41079	Cyber_Folks S.A.	Cyber_Folks S.A.
103.27.35.250	AS45638	SYNERGY WHOLESALE PTY LTD	SYNERGY WHOLESALE PTY LTD

Taking into account the history of URLs from where the redirection to [https://cbe-design\[.\]com/wp-content/Plugins/SPZ/Invoice0312\[.\]PDF](https://cbe-design[.]com/wp-content/Plugins/SPZ/Invoice0312[.]PDF) webpage was tracked and following the domains of such webpages, we can determine that **the phishing activity described in the report** (including attacks targeting the other countries) **started in August, 2021**.

Thus, additional indicators can also be extracted (under [Indicators of Compromise](#) section):

 [medium level of confidence] the indicator, related to:

- URL forwarding to [https://cbe-design\[.\]com/wp-content/Plugins/SPZ/Invoice0312\[.\]PDF](https://cbe-design[.]com/wp-content/Plugins/SPZ/Invoice0312[.]PDF)

 [high level of confidence] the indicator, related to:

- URL forwarding to [https://cbe-design\[.\]com/wp-content/Plugins/SPZ/Invoice0312\[.\]PDF](https://cbe-design[.]com/wp-content/Plugins/SPZ/Invoice0312[.]PDF);
- **.html**, **.shtml** or **.pdf** files that are distributed as email attachments and have the exact same contents.

Outlook

Social engineering threats remain popular for gaining an initial foothold in an organization or achieving other individual goals due to the impact that can be caused through the materialization of these threats.

Despite using unsophisticated phishing techniques that can be easily identified and avoided without specialized technical background, the described analysis of previous and recent credential harvesting campaigns clearly demonstrates that adversaries elaborate their attack scheme and work on enhancing their capabilities.

Thus it is important to follow basic cyber hygiene and cybersecurity guidelines as well as stay informed about the latest threats in order to be able to recognize and avoid phishing scams, especially in corporate environments.

Indicators of Compromise

URLs

URL	Security Context
https://aerotrustersystems[.]com/n/vk..php	webpage, to which the submitted data from the phishing form is sent
https://aerotrustersystems[.]com/v/ukr[.]php	
https://aerotrustersystems[.]com/ju/vk..php	
http://aerotrustersystems[.]com/ju/vk..php	
https://aerotrustersystems[.]com/v/vk..php	
http://tyutta[.]com/vi/g[.]php	
http://test[.]javidhatami[.]com/vn/code[.]php	
http://mangal-pab[.]vn[.]ua/wp-content/vd454/ukr[.]php	
http://mangal-pab[.]vn[.]ua/wp-content/vd454/1[.]php	
http://mangal-pab[.]vn[.]ua/wp-content/vd454/2[.]php	
http://mangal-pab[.]vn[.]ua/wp-content/vd454/3[.]php	
https://thetelounge[.]com[.]au/wp-content/plugins/mail/kach[.]php	
https://thetelounge[.]com[.]au/wp-content/plugins/mail/ukr[.]php	
https://thetelounge[.]com[.]au/wp-content/plugins/mail/f[.]php	
http://thetelounge[.]com[.]au/wp-content/plugins/mail/g[.]php	
https://generaljantz[.]com/ho/Excel[.]php	
http://prelanders[.]lemaleadmachine[.]nl/well-known/leks[.]php	
http://rojowska[.]pl/wp-includes/js/crop/g/j[.]php	
http://rojowska[.]pl/wp-includes/js/jcrop/g/b[.]php	
http://rojowska[.]pl/wp-includes/js/jcrop/g/v[.]php	
http://rojowska[.]pl/wp-includes/js/crop/g/h/w[.]php	
http://rojowska[.]pl/wp-includes/js/crop/g/sender[.]php	
http://rojowska.pl/wp-includes/js/crop/g/leks[.]php	
http://rojowska[.]pl/wp-includes/js/crop/g/y/contact[.]php	

hxxp://chemoogle[.]de/wp-content/mu-plugins-old/g[.]php	
hxxp://chemoogle[.]de/wp-content/mu-plugins-old/chi[.]php	
hxxp://chemoogle[.]de/wp-content/mu-plugins-old/chiff[.]php	
hxxps://gaiapoint[.]com[.]br/lol/chi[.]php	
hxxp://gaiapoint[.]com[.]br/lol/china[.]php	
hxxp://gaiapoint[.]com[.]br/lol/hide[.]php	
hxxp://gaiapoint[.]com[.]br/lol/mine[.]php	
hxxps://gaiapoint[.]com[.]br/lol/mine[.]php	
hxxps://arslonbigsh[.]com/k/Sp_Pdf[.]php	
hxxp://wangnan[.]wang/wp-content/themes/twentyseventeen/wlma/mail[.]php	
hxxp://wangnan[.]wang/wp-content/themes/twentyseventeen/wlma/m[.]php	
hxxp://wangnan[.]wang/wp-content/themes/twentyseventeen/wlma/g[.]php	
hxxps://escentinstitute[.]com/wp-admin/h/m/mail[.]php	
hxxp://escentinstitute[.]com/wp-admin/h/m/mail[.]php	
hxxp://escentinstitute[.]com/wp-admin/h/g[.]php	
hxxps://bildungsangebot[.]de/wp-content/plugins/cdofkgqnqu/n/kachi[.]php	
hxxps://bildungsangebot[.]de/wp-content/plugins/cdofkgqnqu/hold/r[.]php	
hxxps://bildungsangebot[.]de/wp-content/plugins/cdofkgqnqu/kr/kr[.]php	
hxxps://pairviewtraining[.]com/Gohard/xxl2[.]php	
hxxps://pairviewtraining[.]com/brall/ection[.]php	
hxxps://pairviewtraining[.]com/brall/pdf[.]php	
hxxp://pairviewtraining[.]com/brall/p[.]php	
hxxp://pairviewtraining[.]com/brall/pdf[.]php	
hxxps://pairviewtraining[.]com/brall/dnx[.]php	
hxxps://pairviewtraining[.]com/brall/p[.]php	
hxxps://mailh[.]000webhostapp[.]com/wp-includes/link/send[.]php	
hxxp://www[.]sakurasora[.]com/zSp_Pdf[.]php	

hxxps://quizzical-cannon[.]165-22-245-176[.]plesk[.]page/PO/zSp_Pdf[.]php	
hxxps://bl-draft-commercial-invoice[.]000webhostapp[.]com/zSp_Pdf[.]php	
hxxps://www[.]bemardistribuidora[.]com[.]jar/wp-content/plugins/Bck/Sp_Pdf[.]php	
hxxps://ganeshfounders[.]com/spf[.]php	
hxxps://ganeshfounders[.]com/sp/new-po[.]php	
hxxps://vinodavani[.]jorg/Sp_Pdf[.]php	
hxxps://hariomtincontainers[.]in/cl22/Sp_Pdf[.]php	
hxxps://worktutorial[.]com/wp-content/Spz/gb/Sp_Pdf[.]php	
hxxps://bnpr[.]t[.]feip[.]co/cache/gen/Sp_Pdf[.]php	
hxxp://factoryrider[.]com/Sp_Pdf[.]php	
hxxp://factoryrider[.]com/skin/zcannoauto[.]php	
hxxps://worktutorial[.]com/wp-content/Spz/Uch/Sp_Pdf[.]php	
hxxp://worktutorial[.]com/wp-content/Spz/Uch/Sp_Pdf[.]php	
hxxps://josuegoncalves[.]com[.]br/wp-content/plugins/lzzykyqksh/jay/Sp_Pdf[.]php	
hxxps://czczcxvvsbbw[.]isasecret[.]com/zlx/pdf/Sp_Pdf[.]php	
hxxps://petrolpumpservice[.]in/404/Sp_Pdf[.]php	
hxxps://josuegoncalves[.]com[.]br/wp-content/plugins/lzzykyqksh/upload/Sp_Pdf[.]php	
hxxps://cbe-design[.]com/wp-content/Plugins/SPZ/edu/Sp_Pdf[.]php	
hxxps://blkindustries[.]co[.]za/Excel[.]php	

Domains

Domain	Security Context
aerotrustersystems[.]com	Domain of the webpage, mentioned in URL section
tyutta[.]com	
javidhatami[.]com	
mangal-pab[.]vn[.]ua	
thevetlounge[.]com[.]au	
generaljantz[.]com	

lemaleadmachine[.]nl
rojowska[.]pl
chemoogle[.]de
gaiapoint[.]com[.]br
wangnan[.]wang
escentinstitute[.]com
bildungsangebot[.]de
pairviewtraining[.]com
sakurasora[.]com
000webhostapp[.]com
bemardistribuidora[.]com[.]ar
ganeshfounders[.]com
vinodavani[.]org
hariomtincontainers[.]in
worktutorial[.]com
feip[.]co
factoryrider[.]com
josuegoncalves[.]com[.]br
cbe-design[.]com

IP Addresses

IP address	Security Context
192.185.171.241	IP address of the domain aerotrustersystems[.]com
162.241.219.188	IP address of the domain tyutta[.]com
66.33.196.232	IP address of the domain javidhatami[.]com
31.41.216.90 31.41.217.90 5.9.177.94 195.248.235.241	IP address of the domain mangal-pab[.]vn[.]ua
103.27.35.250	IP address of the domain thevetlounge[.]com[.]au

192.254.186.185	IP address of the domain generaljantz[.]com
37.97.143.19	IP address of the domain lemaleadmachine[.]nl
195.78.66.225	IP address of the domain rojowska[.]pl
46.242.233.147	IP address of the domain chemoogle[.]de
148.72.144.232	IP address of the domain gaiapoint[.]com[.]br
101.42.222.102	IP address of the domain wangnan[.]wang
139.59.75.162	IP address of the domain escentinstitute[.]com
135.181.101.225	IP address of the domain bildungsangebot[.]de
104.21.39.217 172.67.148.232	IP address of the domain pairviewtraining[.]com
153.92.0.100	IP address of the domain 000webhostapp[.]com
160.251.151.158	IP address of the domain sakurasora[.]com
200.58.112.68	IP address of the domain bemardistribuidora[.]com[.]ar
162.214.202.31	IP address of the domain ganeshfounders[.]com
188.114.96.0 188.114.97.0	IP address of the domain vinodavani[.]org
162.214.202.31	IP address of the domain hariomtincontainers[.]in
74.220.199.6	IP address of the domain worktutorial[.]com
84.201.147.148	IP address of the domain feip[.]co
185.160.180.120	IP address of the domain factoryrider[.]com
104.21.11.199 172.67.167.55	IP address of the domain josuegoncalves[.]com[.]br
160.153.91.196	IP address of the domain cbe-design[.]com

MITRE ATT&CK®Context

Reconnaissance TA0043	Gather Victim Identity Information T1589	Email Addresses T1589.002
	Search Open Websites/Domains T1593	Social Media T1593.001
		Search Engines T1593.002
Search Victim-Owned Websites T1594		
Resource Development TA0042	Acquire Infrastructure T1583	Domains T1583.001
		Server T1583.004
	Stage Capabilities T1608	Link Target T1608.005
Initial Access TA0001	Phishing T1566	Spearphishing Attachment T1566.001
Execution TA0002	User Execution T1204	Malicious Link T1204.001
		Malicious File T1204.002
Command and Control TA0011	Application Layer Protocol T1071	Web Protocols T1071.001
	Encrypted Channel T1573	Asymmetric Cryptography T1573.002