blog.cloudflare.com /disrupting-flyingyeti-campaign-targeting-ukraine/

Disrupting FlyingYeti's campaign targeting Ukraine

⋮ 5/30/2024

05/30/2024

- Cloudforce One

15 min read

Cloudforce One is publishing the results of our investigation and real-time effort to detect, deny, degrade, disrupt, and delay threat activity by the Russia-aligned threat actor FlyingYeti during their latest phishing campaign targeting Ukraine. At the onset of Russia's invasion of Ukraine on February 24, 2022, Ukraine introduced a moratorium on evictions and termination of utility services for unpaid debt. The moratorium ended in January 2024, resulting in significant debt liability and increased financial stress for Ukrainian citizens. The FlyingYeti campaign capitalized on anxiety over the potential loss of access to housing and utilities by enticing targets to open malicious files via debt-themed lures. If opened, the files would result in infection with the PowerShell malware known as COOKBOX, allowing FlyingYeti to support follow-on objectives, such as installation of additional payloads and control over the victim's system.

Since April 26, 2024, Cloudforce One has taken measures to prevent FlyingYeti from launching their phishing campaign – a campaign involving the use of Cloudflare Workers and GitHub, as well as exploitation of the WinRAR vulnerability CVE-2023-38831. Our countermeasures included internal actions, such as detections and code takedowns, as well as external collaboration with third parties to remove the actor's cloud-hosted malware. Our effectiveness against this actor prolonged their operational timeline from days to weeks. For example, in a single instance, FlyingYeti spent almost eight hours debugging their code as a result of our mitigations. By employing proactive defense measures, we successfully stopped this determined threat actor from achieving their objectives.

Executive Summary

- On April 18, 2024, Cloudforce One detected the Russia-aligned threat actor FlyingYeti preparing to launch a phishing espionage campaign targeting individuals in Ukraine.
- We discovered the actor used similar tactics, techniques, and procedures (TTPs) as those detailed in Ukranian CERT's article on UAC-0149, a threat group that has primarily targeted Ukrainian defense entities with COOKBOX malware since at least the fall of 2023.

- From mid-April to mid-May, we observed FlyingYeti conduct reconnaissance activity, create lure content for use in their phishing campaign, and develop various iterations of their malware. We assessed that the threat actor intended to launch their campaign in early May, likely following Orthodox Easter.
- After several weeks of monitoring actor reconnaissance and weaponization activity (Cyber Kill Chain Stages 1 and 2), we successfully disrupted FlyingYeti's operation moments after the final COOKBOX payload was built.
- The payload included an exploit for the WinRAR vulnerability CVE-2023-38831, which FlyingYeti will likely continue to use in their phishing campaigns to infect targets with malware.
- We offer steps users can take to defend themselves against FlyingYeti phishing operations, and also provide recommendations, detections, and indicators of compromise.

Who is FlyingYeti?

FlyingYeti is the cryptonym given by Cloudforce One to the threat group behind this phishing campaign, which overlaps with UAC-0149 activity tracked by CERT-UA in February and April 2024. The threat actor uses dynamic DNS (DDNS) for their infrastructure and leverages cloud-based platforms for hosting malicious content and for malware command and control (C2). Our investigation of FlyingYeti TTPs suggests this is likely a Russia-aligned threat group. The actor appears to primarily focus on targeting Ukrainian military entities. Additionally, we observed Russian-language comments in FlyingYeti's code, and the actor's operational hours falling within the UTC+3 time zone.

Campaign background

In the days leading up to the start of the campaign, Cloudforce One observed FlyingYeti conducting reconnaissance on payment processes for Ukrainian communal housing and utility services:

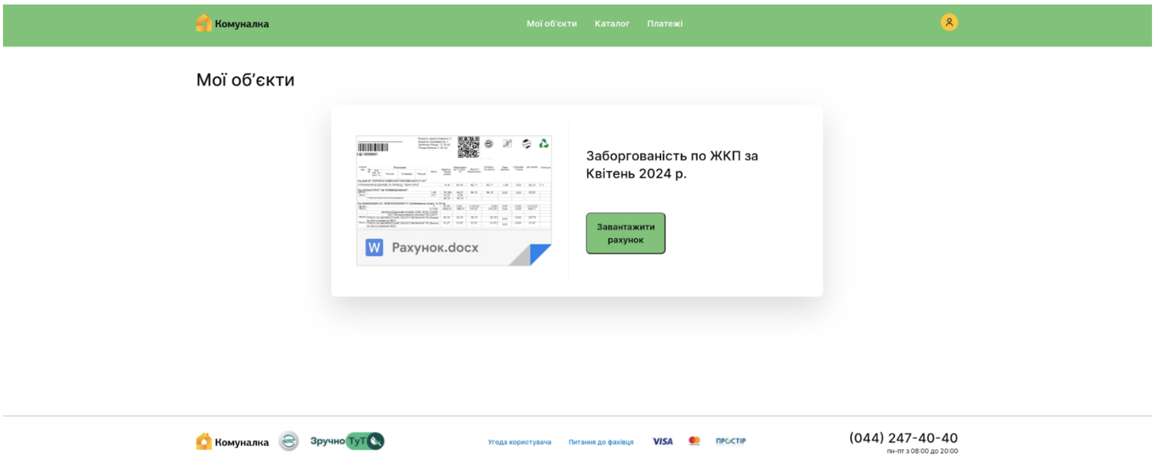
- April 22, 2024 – research into changes made in 2016 that introduced the use of QR codes in payment notices
- April 22, 2024 – research on current developments concerning housing and utility debt in Ukraine
- April 25, 2024 – research on the legal basis for restructuring housing debt in Ukraine as well as debt involving utilities, such as gas and electricity

Cloudforce One judges that the observed reconnaissance is likely due to the Ukrainian government's payment moratorium introduced at the start of the full-fledged invasion in February 2022. Under this moratorium, outstanding debt would not lead to evictions or termination of provision of utility services. However, on January 9, 2024, the government lifted this ban, resulting in increased pressure on Ukrainian citizens with outstanding debt. FlyingYeti sought to capitalize on that pressure, leveraging debt restructuring and payment-related lures in an attempt to increase their chances of successfully targeting Ukrainian individuals.

Analysis of the Komunalka-themed phishing site

The disrupted phishing campaign would have directed FlyingYeti targets to an actor-controlled GitHub page at hxxps[:]//komunalka[.]github[.]io, which is a spoofed version of the Kyiv Komunalka communal housing site https://www.komunalka.ua. Komunalka functions as a payment processor for residents in the Kyiv region and allows for payment of utilities, such as gas, electricity, telephone, and Internet. Additionally, users can pay other fees and fines, and even donate to Ukraine's defense forces.

Based on past FlyingYeti operations, targets may be directed to the actor's Github page via a link in a phishing email or an encrypted Signal message. If a target accesses the spoofed Komunalka platform at hxxps[:]//komunalka[.]github[.]io, the page displays a large green button with a prompt to download the document "Рахунок.docx" ("Invoice.docx"), as shown in Figure 1. This button masquerades as a link to an overdue payment invoice but actually results in the download of the malicious archive "Заборгованість по ЖКП.rar" ("Debt for housing and utility services.rar").



Мої об’єкти

Заборгованість по ЖКП за Квітень 2024 р.

Figure 1: Prompt to download malicious archive “Заборгованість по ЖКП.rar”

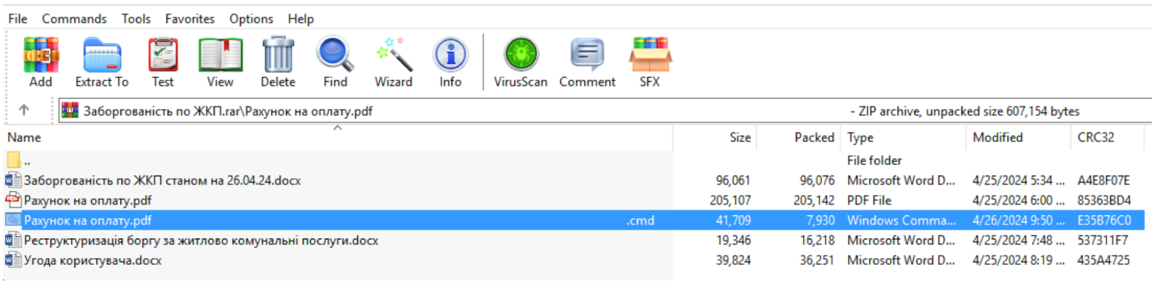
A series of steps must take place for the download to successfully occur:

- The target clicks the green button on the actor’s GitHub page hxxps[:]//komunalka.github[.]io
- The target’s device sends an HTTP POST request to the Cloudflare Worker worker-polished-union-f396[.]vqu89698[.]workers[.]dev with the HTTP request body set to “user=Iahhdr”
- The Cloudflare Worker processes the request and evaluates the HTTP request body
- If the request conditions are met, the Worker fetches the RAR file from hxxps[:]//raw[.]githubusercontent[.]com/kudoc8989/project/main/Заборгованість по ЖКП.rar, which is then downloaded on the target’s device

Cloudforce One identified the infrastructure responsible for facilitating the download of the malicious RAR file and remediated the actor-associated Worker, preventing FlyingYeti from delivering its malicious tooling. In an effort to circumvent Cloudforce One's mitigation measures, FlyingYeti later changed their malware delivery method. Instead of the Workers domain fetching the malicious RAR file, it was loaded directly from GitHub.

Analysis of the malicious RAR file

During remediation, Cloudforce One recovered the RAR file “Заборгованість по ЖКП.rar” and performed analysis of the malicious payload. The downloaded RAR archive contains multiple files, including a file with a name that contains the unicode character “U+201F”. This character appears as whitespace on Windows devices and can be used to “hide” file extensions by adding excessive whitespace between the filename and the file extension. As highlighted in blue in Figure 2, this cleverly named file within the RAR archive appears to be a PDF document but is actually a malicious CMD file (“Рахунок на оплату.pdf[unicode character U+201F].cmd”).



Заборгованість по ЖКП.rar\Рахунок на оплату.pdf - ZIP archive, unpacked size 607,154 bytes

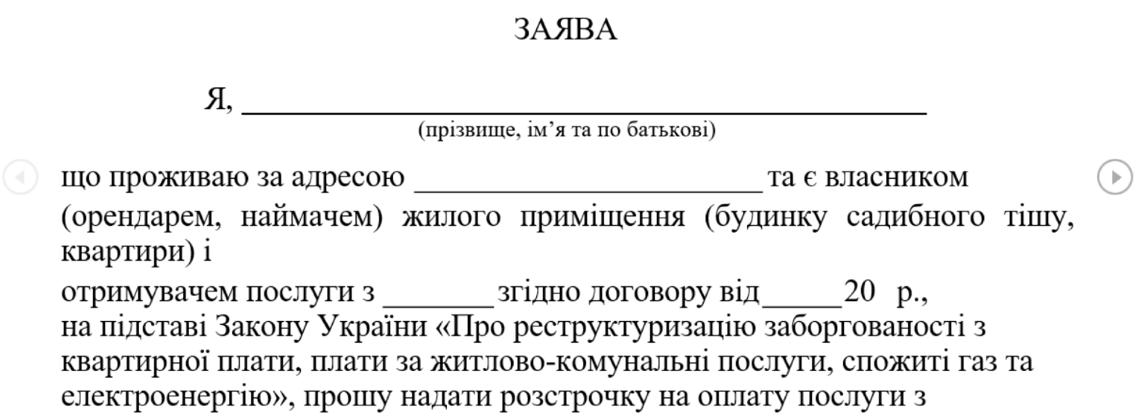
Name		Size	Packed	Type	Modified	CRC32
..				File folder		
Заборгованість по ЖКП станом на 26.04.24.docx		96,061	96,076	Microsoft Word D...	4/25/2024 5:34 ...	A4E8F07E
Рахунок на оплату.pdf		205,107	205,142	PDF File	4/25/2024 6:00 ...	85363BD4
Рахунок на оплату.pdf	.cmd	41,709	7,930	Windows Comma...	4/26/2024 9:50 ...	E35B76C0
Реструктуризація боргу за житлово комунальні послуги.docx		19,346	16,218	Microsoft Word D...	4/25/2024 7:48 ...	537311F7
Угода користувача.docx		39,824	36,251	Microsoft Word D...	4/25/2024 8:19 ...	435A4725

Figure 2: Files contained in the malicious RAR archive “Заборгованість по ЖКП.rar” (“Housing Debt.rar”)

FlyingYeti included a benign PDF in the archive with the same name as the CMD file but without the unicode character, “Рахунок на оплату.pdf” (“Invoice for payment.pdf”). Additionally, the directory name for the archive once decompressed also contained the name “Рахунок на оплату.pdf”. This overlap in names of the benign PDF and the directory allows the actor to exploit the WinRAR vulnerability CVE-2023-38831. More specifically, when an archive includes a benign file with the same name as the directory, the entire contents of the directory are opened by the WinRAR application, resulting in the execution of the malicious CMD. In other words, when the target believes they are opening the benign PDF “Рахунок на оплату.pdf”, the malicious CMD file is executed.

The CMD file contains the FlyingYeti PowerShell malware known as COOKBOX. The malware is designed to persist on a host, serving as a foothold in the infected device. Once installed, this variant of COOKBOX will make requests to the DDNS domain postdock[.]serveftp[.]com for C2, awaiting PowerShell cmdlets that the malware will subsequently run.

Alongside COOKBOX, several decoy documents are opened, which contain hidden tracking links using the Canary Tokens service. The first document, shown in Figure 3 below, poses as an agreement under which debt for housing and utility services will be restructured.



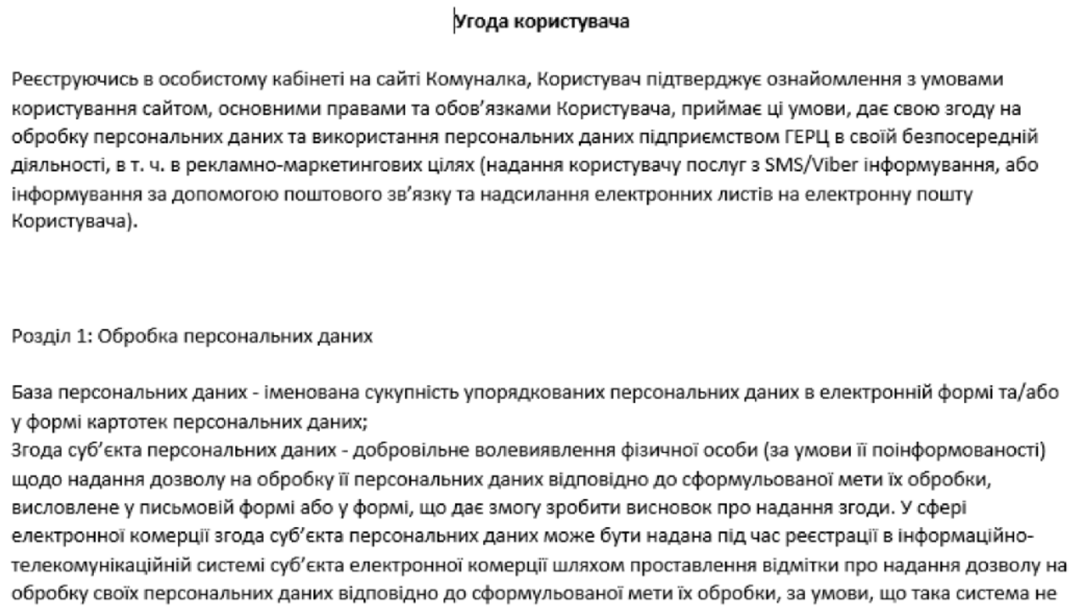
ЗАЯВА

Я, ____
(прізвище, ім’я та по батькові)

що проживаю за адресою ______________________ та є власником (орендарем, наймачем) жилого приміщення (будинку садибного тішу, квартири) і
отримувачем послуги з _______згідно договору від_____20 р.,
на підставі Закону України «Про реструктуризацію заборгованості з квартирної плати, плати за житлово-комунальні послуги, спожиті газ та електроенергію», прошу надати розстрочку на оплату послуги з

Figure 3: Decoy document Реструктуризація боргу за житлово комунальні послуги.docx

The second document (Figure 4) is a user agreement outlining the terms and conditions for the usage of the payment platform komunalka[.]ua.



Угода користувача

Реєструючись в особистому кабінеті на сайті Комуналка, Користувач підтверджує ознайомлення з умовами користування сайтом, основними правами та обов’язками Користувача, приймає ці умови, дає свою згоду на обробку персональних даних та використання персональних даних підприємством ГЕРЦ в своїй безпосередній діяльності, в т. ч. в рекламно-маркетингових цілях (надання користувачу послуг з SMS/Viber інформування, або інформування за допомогою поштового зв’язку та надсилання електронних листів на електронну пошту Користувача).

Розділ 1: Обробка персональних даних

База персональних даних - іменована сукупність упорядкованих персональних даних в електронній формі та/або у формі картотек персональних даних;
Згода суб’єкта персональних даних - добровільне волевиявлення фізичної особи (за умови її поінформованості) щодо надання дозволу на обробку її персональних даних відповідно до сформульованої мети їх обробки, висловлене у письмовій формі або у формі, що дає змогу зробити висновок про надання згоди. У сфері електронної комерції згода суб’єкта персональних даних може бути надана під час реєстрації в інформаційно-телекомунікаційній системі суб’єкта електронної комерції шляхом проставлення відмітки про надання дозволу на обробку своїх персональних даних відповідно до сформульованої мети їх обробки, за умови, що така система не

Figure 4: Decoy document Угода користувача.docx *(User Agreement.docx)*

The use of relevant decoy documents as part of the phishing and delivery activity are likely an effort by FlyingYeti operators to increase the appearance of legitimacy of their activities.

The phishing theme we identified in this campaign is likely one of many themes leveraged by this actor in a larger operation to target Ukrainian entities, in particular their defense forces. In fact, the threat activity we detailed in this blog uses many of the same techniques outlined in a recent FlyingYeti campaign disclosed by CERT-UA in mid-April 2024, where the actor leveraged United Nations-themed lures involving Peace Support Operations to target Ukraine’s military. Due to Cloudforce One’s defensive actions covered in the next section, this latest FlyingYeti campaign was prevented as of the time of publication.

Mitigating FlyingYeti activity

Cloudforce One mitigated FlyingYeti's campaign through a series of actions. Each action was taken to increase the actor's cost of continuing their operations. When assessing which action to take and why, we carefully weighed the pros and cons in order to provide an effective active defense strategy against this actor. Our general goal was to increase the amount of time the threat actor spent trying to develop and weaponize their campaign.

We were able to successfully extend the timeline of the threat actor's operations from hours to weeks. At each interdiction point, we assessed the impact of our mitigation to ensure the actor would spend more time attempting to launch their campaign. Our mitigation measures disrupted the actor's activity, in one instance resulting in eight additional hours spent on debugging code.

Due to our proactive defense efforts, FlyingYeti operators adapted their tactics multiple times in their attempts to launch the campaign. The actor originally intended to have the Cloudflare Worker fetch the malicious RAR file from GitHub. After Cloudforce One interdiction of the Worker, the actor attempted to create additional Workers via a new account. In response, we disabled all Workers, leading the actor to load the RAR file directly from GitHub. Cloudforce One notified GitHub, resulting in the takedown of the RAR file, the GitHub project, and suspension of the account used to host the RAR file. In return, FlyingYeti began testing the option to host the RAR file on the file sharing sites pixeldrain and Filemail, where we observed the actor alternating the link on the Komunalka phishing site between the following:

- hxxps://pixeldrain[.]com/api/file/ZAJxwFFX?download=one
- hxxps://1014.filemail[.]com/api/file/get?filekey=e_8S1HEnM5Rzhy_jpN6nL-GF4UAP533VrXzgXjxH1GzbVQZvmpFzrFA&pk_vid=a3d82455433c8ad11715865826cf18f6

We notified GitHub of the actor's evolving tactics, and in response GitHub removed the Komunalka phishing site. After analyzing the files hosted on pixeldrain and Filemail, we determined the actor uploaded dummy payloads, likely to monitor access to their phishing infrastructure (FileMail logs IP addresses, and both file hosting sites provide view and download counts). At the time of publication, we did not observe FlyingYeti upload the malicious RAR file to either file hosting site, nor did we identify the use of alternative phishing or malware delivery methods.

A timeline of FlyingYeti's activity and our corresponding mitigations can be found below.

Event timeline

Date	Event Description
2024-04-18 12:18	Threat Actor (TA) creates a Worker to handle requests from a phishing site
2024-04-18 14:16	TA creates phishing site komunalka[.]github[.]io on GitHub
2024-04-25 12:25	TA creates a GitHub repo to host a RAR file
2024-04-26 07:46	TA updates the first Worker to handle requests from users visiting komunalka[.]github[.]io
2024-04-26 08:24	TA uploads a benign test RAR to the GitHub repo
2024-04-26 13:38	Cloudforce One identifies a Worker receiving requests from users visiting komunalka[.]github[.]io, observes its use as a phishing page
2024-04-26 13:46	Cloudforce One identifies that the Worker fetches a RAR file from GitHub (the malicious RAR payload is not yet hosted on the site)
2024-04-26 19:22	Cloudforce One creates a detection to identify the Worker that fetches the RAR
2024-04-26 21:13	Cloudforce One deploys real-time monitoring of the RAR file on GitHub
2024-05-02 06:35	TA deploys a weaponized RAR (CVE-2023-38831) to GitHub with their COOKBOX malware packaged in the archive
2024-05-06 10:03	TA attempts to update the Worker with link to weaponized RAR, the Worker is immediately blocked
2024-05-06 10:38	TA creates a new Worker, the Worker is immediately blocked
2024-05-06 11:04	TA creates a new account (#2) on Cloudflare
2024-05-06 11:06	TA creates a new Worker on account #2 (blocked)
2024-05-06 11:50	TA creates a new Worker on account #2 (blocked)

Date	Event Description
2024-05-06 12:22	TA creates a new modified Worker on account #2
2024-05-06 16:05	Cloudforce One disables the running Worker on account #2
2024-05-07 22:16	TA notices the Worker is blocked, ceases all operations
2024-05-07 22:18	TA deletes original Worker first created to fetch the RAR file from the GitHub phishing page
2024-05-09 19:28	Cloudforce One adds phishing page komunalka[.]github[.]io to real-time monitoring
2024-05-13 07:36	TA updates the github.io phishing site to point directly to the GitHub RAR link
2024-05-13 17:47	Cloudforce One adds COOKBOX C2 postdock[.]serveftp[.]com to real-time monitoring for DNS resolution
2024-05-14 00:04	Cloudforce One notifies GitHub to take down the RAR file
2024-05-15 09:00	GitHub user, project, and link for RAR are no longer accessible
2024-05-21 08:23	TA updates Komunalka phishing site on github.io to link to pixeldrain URL for dummy payload (pixeldrain only tracks view and download counts)
2024-05-21 08:25	TA updates Komunalka phishing site to link to FileMail URL for dummy payload (FileMail tracks not only view and download counts, but also IP addresses)
2024-05-21 12:21	Cloudforce One downloads PixelDrain document to evaluate payload
2024-05-21 12:47	Cloudforce One downloads FileMail document to evaluate payload
2024-05-29 23:59	GitHub takes down Komunalka phishing site
2024-05-30 13:00	Cloudforce One publishes the results of this investigation

Coordinating our FlyingYeti response

Cloudforce One leveraged industry relationships to provide advanced warning and to mitigate the actor's activity. To further protect the intended targets from this phishing threat, Cloudforce One notified and collaborated closely with GitHub's Threat Intelligence and Trust and Safety Teams. We also notified CERT-UA and Cloudflare industry partners such as CrowdStrike, Mandiant/Google Threat Intelligence, and Microsoft Threat Intelligence.

Hunting FlyingYeti operations

There are several ways to hunt FlyingYeti in your environment. These include using PowerShell to hunt for WinRAR files, deploying Microsoft Sentinel analytics rules, and running Splunk scripts as detailed below. Note that these detections may identify activity related to this threat, but may also trigger unrelated threat activity.

PowerShell hunting

Consider running a PowerShell script such as this one in your environment to identify exploitation of CVE-2023-38831. This script will interrogate WinRAR files for evidence of the exploit.

```
CVE-2023-38831
Description:winrar exploit detection
open suspios (.tar / .zip / .rar) and run this script to check it

function winrar-exploit-detect(){
$targetExtensions = @(".cmd" , ".ps1" , ".bat")
$tempDir = [System.Environment]::GetEnvironmentVariable("TEMP")
$dirsToCheck = Get-ChildItem -Path $tempDir -Directory -Filter "Rar*"
foreach ($dir in $dirsToCheck) {
    $files = Get-ChildItem -Path $dir.FullName -File
    foreach ($file in $files) {
        $fileName = $file.Name
        $fileExtension = [System.IO.Path]::GetExtension($fileName)
        if ($targetExtensions -contains $fileExtension) {
            $fileWithoutExtension =
[System.IO.Path]::GetFileNameWithoutExtension($fileName); $filename.TrimEnd() -
replace '\.
```

```
$cmdFileName = "$fileWithoutExtension" $secondFile = Join-Path -Path $dir.FullName -
ChildPath $cmdFileName if (Test-Path $secondFile -PathType Leaf) { Write-Host "[!]
Suspicious pair detected " Write-Host "[*] Original File:$($secondFile)" -
ForegroundColor Green Write-Host "[*] Suspicious File:$($file.FullName)" -
ForegroundColor Red # Read and display the content of the command file $cmdFileContent
= Get-Content -Path $($file.FullName) Write-Host "[+] Command File
Content:$cmdFileContent" } } } } } winrar-exploit-detect
```

Microsoft Sentinel

In Microsoft Sentinel, consider deploying the rule provided below, which identifies WinRAR execution via cmd.exe. Results generated by this rule may be indicative of attack activity on the endpoint and should be analyzed.

```
DeviceProcessEvents
| where InitiatingProcessParentFileName has @"winrar.exe"
| where InitiatingProcessFileName has @"cmd.exe"
| project Timestamp, DeviceName, FileName, FolderPath, ProcessCommandLine,
AccountName
| sort by Timestamp desc
```

Splunk

Consider using this script in your Splunk environment to look for WinRAR CVE-2023-38831 execution on your Microsoft endpoints. Results generated by this script may be indicative of attack activity on the endpoint and should be analyzed.

```
| tstats `security_content_summariesonly` count min(_time) as firstTime max(_time)
as lastTime from datamodel=Endpoint.Processes where
Processes.parent_process_name=winrar.exe `windows_shells` OR Processes.process_name
IN ("certutil.exe","mshta.exe","bitsadmin.exe") by Processes.dest Processes.user
Processes.parent_process_name Processes.parent_process Processes.process_name
Processes.process Processes.process_id Processes.parent_process_id
| `drop_dm_object_name(Processes)`
| `security_content_ctime(firstTime)`
| `security_content_ctime(lastTime)`
| `winrar_spawning_shell_application_filter`
```

Cloudflare product detections

Cloudflare Email Security

Cloudflare Email Security (CES) customers can identify FlyingYeti threat activity with the following detections.

- CVE-2023-38831
- FLYINGYETI.COOKBOX
- FLYINGYETI.COOKBOX.Launcher
- FLYINGYETI.Rar

Recommendations

Cloudflare recommends taking the following steps to mitigate this type of activity:

- Implement Zero Trust architecture foundations:
- Deploy Cloud Email Security to ensure that email services are protected against phishing, BEC and other threats
- Leverage browser isolation to separate messaging applications like LinkedIn, email, and Signal from your main network
- Scan, monitor and/or enforce controls on specific or sensitive data moving through your network environment with data loss prevention policies
- Ensure your systems have the latest WinRAR and Microsoft security updates installed
- Consider preventing WinRAR files from entering your environment, both at your Cloud Email Security solution and your Internet Traffic Gateway
- Run an Endpoint Detection and Response (EDR) tool such as CrowdStrike or Microsoft Defender for Endpoint to get visibility into binary execution on hosts
- Search your environment for the FlyingYeti indicators of compromise (IOCs) shown below to identify potential actor activity within your network.

If you're looking to uncover additional Threat Intelligence insights for your organization or need bespoke Threat Intelligence information for an incident, consider engaging with Cloudforce One by contacting your Customer Success manager or filling out this form.

Indicators of Compromise

Filename	SHA256 Hash	De
Заборгованість по ЖКП.rar	a0a294f85c8a19be048ffcc05ede6fd5a7ac5e2f0032a3ca0050dc1ae960c314	RA ar
Рахунок на оплату.pdf .cmd	0cca8f795c7a81d33d36d5204fcd9bc73bdc2af7de315c1449cbc3551ef4fb59	CO Sa (co in ar
Реструктуризація боргу за житлово комунальні послуги.docx	915721b94e3dffa6cef3664532b586be6cf989fec923b26c62fdaf201ee81d2c	Be W Do wi Tr Lin (co in ar
Угода користувача.docx	79a9740f5e5ea4aa2157d9d96df34ee49a32e2d386fe55fedfd1aa33e151c06d	Be W Do wi Tr Lin (co in ar
Рахунок на оплату.pdf	19e25456c2996ded3e29577b609de54a2bef90dad8f868cdad795c18df05a79b	Ra Bin (co in ar
Заборгованість по ЖКП станом на 26.04.24.docx	e0d65e2d36afd3db1b603f10e0488cee3f58ade24d8abc6bee240314d8696708	Ra Bin (co in ar

Domain / URL	Description
komunalka[.]github[.]io	Phishing page
hxxps[:]//github[.]com/komunalka/komunalka[.]github[.]io	Phishing page
hxxps[:]//worker-polished-union-f396[.]vqu89698[.]workers[.]dev	Worker that fetches malicious RAR file

Domain / URL	Description
hxxps[:]//raw[.]githubusercontent[.]com/kudoc8989/project/main/Заборгованість по ЖКП.rar	Delivery of malicious RAR file
hxxps[:]//1014[.]filemail[.]com/api/file/get?filekey=e_8S1HEnM5Rzhy_jpN6nL-GF4UAP533VrXzgXjxH1GzbVQZvmpFzrFA&pk_vid=a3d82455433c8ad11715865826cf18f6	Dummy payload
hxxps[:]//pixeldrain[.]com/api/file/ZAJxwFFX?download=	Dummy payload
hxxp[:]//canarytokens[.]com/stuff/tags/ni1cknk2yq3xfcw2al3efs37m/payments.js	Tracking link
hxxp[:]//canarytokens[.]com/stuff/terms/images/k22r2dnjrvjsme8680ojf5ccs/index.html	Tracking link
postdock[.]serveftp[.]com	COOKBOX C2