Bundesamt für
Verfassungsschutz

Cologne, 15 August 2024

BfV CYBER INSIGHT

The i-Soon-Leaks: Industrialization of Cyber Espionage

Part 3: Affected countries and specific targets of i-Soon

The i-Soon-Leaks: Industrialization of Cyber Espionage

Part 3: Affected countries and specific targets of i-Soon

Table of Contents

1. Introduction

On February 16th 2024 a data set was leaked on the GitHub[1] developer platform that provides a rare insight into China's methods of conducting hacking operations worldwide. The internal documents show the extent of cooperation between the Chinese cybersecurity company i-Soon and the Chinese government and intelligence services. In four consecutive reports BfV examines the leak in detail and describes the level of industrialization of cyber espionage activities by privately organized companies, who carry out cyber-attacks for state entities.

The leak includes over 570 files, images, and chat messages in Chinese, including:

- a presentation on the skills and services of i-Soon,
- lists of employees, product information/services, contract books and information on cyber operations and target entities,
- screenshots of presumably captured data and
- log files of compromised telecommunications service providers in Asia.

The leaked documents do not contain any indication of affected entities in Germany, however, the analysis offers an insight into the inner workings of private hacker companies and providers of malicious software and their close ties to the Chinese state. It also lays bare how APT[2] groups operate and how government agencies leverage them.[3]

[1] GitHub is an online software development and version management service for software projects.

[2] Advanced Persistent Threats (APT) denotes complex and targeted threats that target one or a specific group of victims. They are usually comprised of resource-intensive, government-controlled cyber-attacker groups. The attacks themselves are often elaborately prepared by the attackers, are sophisticated ("advanced") and can continue over a long period of time (“persistent”).

[3] For illustration purposes, various screenshots from the leak were translated and included in this report.

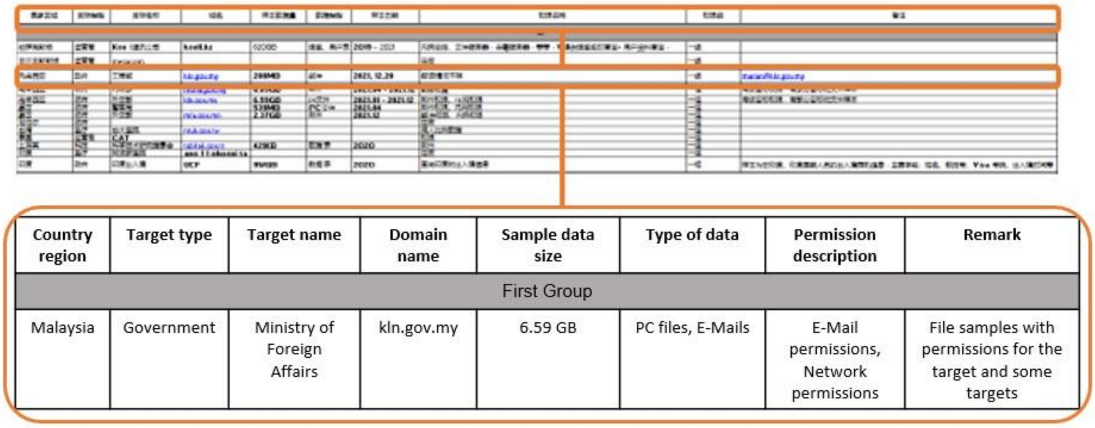
The BfV's evaluation of the leaked data is presented in a total of four reports, which are structured as follows:

- Organization and methods of i-Soon APT units (part 1),
- Connections of i-Soon to the Chinese security apparatus (part 2),
- **Affected countries and specific targets of i-Soon (part 3, this report),**
- Offered products and i-Soon customers (part 4).

Following part 1 (organization and methods of i-Soon APT groups and part 2 (connections of i-Soon to the Chinese security apparatus), part 3 is dedicated to the affected countries and specific targets of i-Soon.

2. Target regions and countries

The leaked data also contains a presentation on i-Soon's skills and offered services. By the company's own accord, its cyber operations focus on West Asia, Southeast Asia as well as Hong Kong, Taiwan, India, Nepal and Tibet. The cyber operations listed in the data leak confirm this concentration of activities. However, the leaked data also contains references to activities against EU institutions and member states. The entries show the state of running operations and give insight into the management of APT activities (see Figure 1).



Country region	Target type	Target name	Domain name	Sample data size	Type of data	Permission description	Remark
First Group							
Malaysia	Government	Ministry of Foreign Affairs	kln.gov.my	6.59 GB	PC files, E-Mails	E-Mail permissions, Network permissions	File samples with permissions for the target and some targets

Figure 1: excerpt list of cyber operations

The listed targets show a focus of cyber operations against entities in Hong Kong, Thailand, Taiwan, Kazakhstan, Malaysia and Mongolia. Further nations affected by operations also include Kyrgyzstan, Nepal, Turkey, India, Pakistan, Egypt, France, Cambodia, Uganda, Rwanda, Indonesia, Vietnam, Philippines, South Korea, China, Nigeria, Afghanistan and Myanmar (see Figure 2).

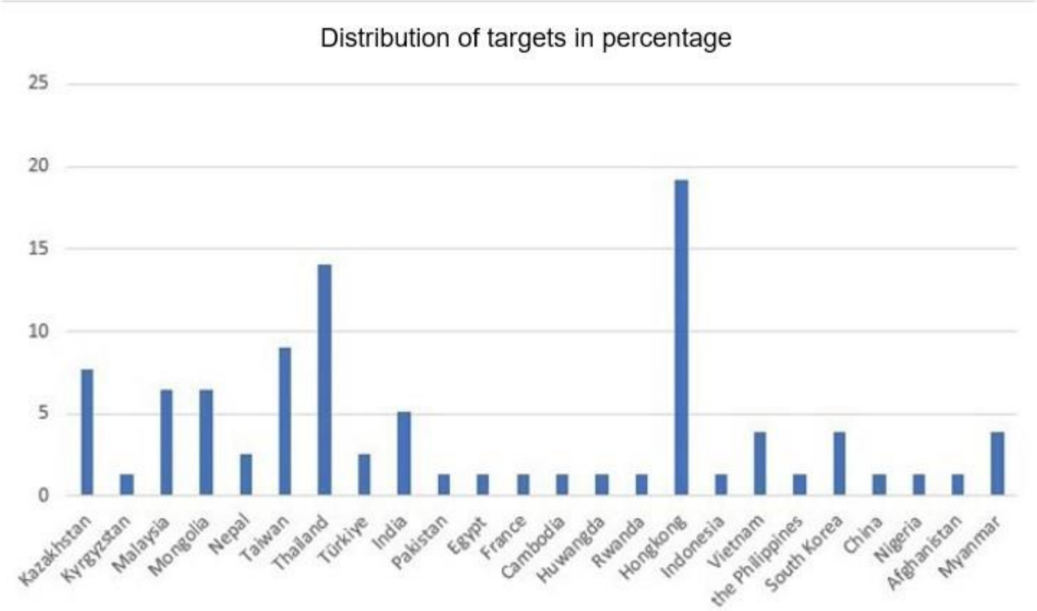


Figure 2: evaluation of affected countries (N = 78)

The leaked data contains no information on affected entities in Germany. However, there are indications that point towards compromises related to EU institutions, as well as attacks against European states and EU member states.

3. Specific targets

The leaked presentation of i-Soon's capabilities and services advertise the compromise of networks in the government, medical, transport, energy and telecommunications sector. This is supported by the leaked data covering specific cyber operations and targets against government institutions, telecommunications service providers, science and education institutions, medical institutions and data collections on demographics and religious institutions.

With a percentage of over 40 %, government institutions by far account for the largest proportion of affected sectors, followed by telecommunications service providers with almost 25 % (see Figure 3).

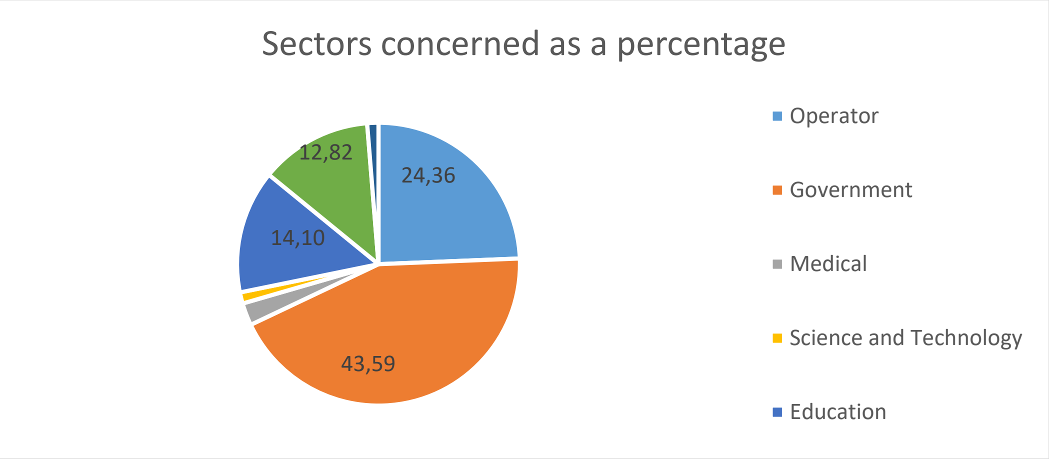
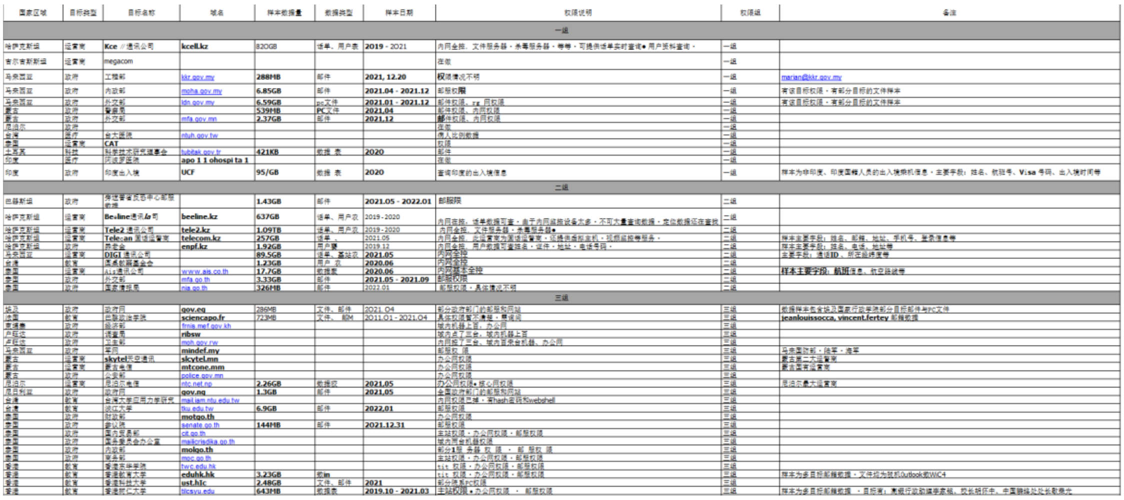


Figure 3: sectors affected by campaigns

The leaked information illustrates the professionalized approach of the hacking industry. The current progress of concrete attack operations is documented in ten columns (see Figure 4).



国家区域	目标类型	目标名称	域名	样本数据量	数据类型	样本日期	权限说明	权限组	备注
一组									
哈萨克斯坦	运营商	Kce //通讯公司	kcell.kz	820GB	话单、用户表	2019 - 2021	内网全控、文件服务器・杀毒服务器・等等・可提供话单实时查询• 用户资料查询・	一组	
吉尔吉斯斯坦	运营商	megacom					在做	一组	
马来西亚	政府	工程部	kkr.gov.my	288MB	邮件	2021, 12.20	权限情况不明	一组	marian@kkr.gov.my
马来西亚	政府	内政部	moha.gov.my	6.85GB	邮件	2021.04 - 2021.12	邮服权限	一组	有该目标权限・有部分目标的文件样本
马来西亚	政府	外交部	kln.gov.my	6.59GB	pc文件	2021.01 - 2021.12	邮件权限、rg 网权限	一组	有该目标权限・有部分目标的文件样本
蒙古	政府	警察局		539MB	PC文件	2021.04	邮件权限、内网权限	一组	
蒙古	政府	外交部	mfa.gov.mn	2.37GB	邮件	2021.12	邮件权限、内网权限	一组	
尼泊尔	政府						在做	一组	
台湾	医疗	台大医院	ntuh.gov.tw				病人比例数据	一组	
泰国	运营商	CAT					权限	一组	
土耳其	科技	科学技术研究理事会	tubitak.gov.tr	421KB	数据 表	2020	邮件	一组	
印度	医疗	阿波罗医院	apo 1 1 ohospi ta 1				在做	一组	
印度	政府	印度出入境	UCF	95/GB	数据 表	2020	查询印度的出入境信息	一组	样本为非印度、印度国籍人员的出入境乘机信息・主要字段：姓名、航班号、Visa 号码、出入境时间等
二组									
巴基斯坦	政府	旁遮普省反恐中心邮服数据		1.43GB	邮件	2021.05 - 2022.01	邮服限	二组	
哈萨克斯坦	运营商	Beeline通讯公司	beeline.kz	637GB	话单、用户表	2019 - 2020	内网在控，话单数据可查・由于内网监控设备太多・不可大量查询数据・定位数据还在查找	二组	
哈萨克斯坦	运营商	Tele2 通讯公司	tele2.kz	1.09TB	话单、用户表	2019 - 2020	内网全控、文件服务器・杀毒服务器•	二组	
哈萨克斯坦	运营商	Telecan 国家运营商	telecom.kz	257GB	话单 、	2021.05	内网全控、此运营商为国家运营商・还提供虚拟主机・视频监控等服务・	二组	样本主要字段：姓名、邮箱、地址、手机号、登录信息等
哈萨克斯坦	政府	养老金	enpf.kz	1.92GB	用户表	2019.12	内网全控、用户数据可查姓名・证件・地址・电话号码・	二组	样本主要字段：姓名、电话、地址等
马来西亚	运营商	DIGI 通讯公司		89.5GB	话单、基站表	2021.05	内网全控	二组	主要字段：通话ID、所在经纬度等
台湾	教育	国系教育基金会		1.23GB	用户 表	2020.06	内网全控	二组	
泰国	运营商	Ais通讯公司	www.ais.co.th	17.7GB	数据表	2020.06	内网基本全控	二组	样本主要字段：航班信息、航空路线等
泰国	政府	外交部	mfa.go.th	3.33GB	邮件	2021.05 - 2021.09	邮服权限	二组	
泰国	政府	国家情报局	nia.go.th	326MB	邮件	2022.01	邮服权限・具体情况不明	二组	
三组									
埃及	政府	政府网	gov.eg	286MB	文件、邮件	2021.04	部分政府部门的邮服和网站	三组	数据样本包含埃及国家行政学院部分目标邮件与PC文件
法国	教育	巴黎政治学院	sciencapo.fr	723MB	文件、邮件	2011.01 - 2021.04	具体权限暂不清楚・需询问	三组	jeanlouissocca, vincent.fertey 邮箱数据
柬埔寨	政府	经济部	fmis.mef.gov.kh				域内机器上百，办公网	三组	
卢旺达	政府	调查局	ribsw				域内点了三台，域内机器上百	三组	
卢旺达	政府	卫生部	moh.gov.rw				内网控了三台、域内百来台机器、办公网	三组	
马来西亚	政府	军网	mindef.my				邮服权 限	三组	马来国防部・陆军・海军
蒙古	运营商	skytel天空通讯	skytel.mn				办公网权限	三组	蒙古第二大运营商
蒙古	运营商	蒙古电信	mtcone.mm				办公网权限	三组	蒙古国有运营商
蒙古	政府	公安部	police.gov.mn				办公网权限	三组	
尼泊尔	运营商	尼泊尔电信	ntc.net.np	2.26GB	数据表	2021.05	办公网权限• 核心网权限	三组	尼泊尔最大运营商
尼日利亚	政府	政府网	gov.ng	1.3GB	邮件	2021.05	全国政府部门的邮服和网站	三组	
台湾	教育	台湾大学应用力学研究	mail.iam.ntu.edu.tw				内网权限已掉・有hash密码和webshell	三组	
台湾	教育	淡江大学	tku.edu.tw	6.9GB	邮件	2022.01	邮服权限	三组	
泰国	政府	财政部	motgo.th				办公网权限	三组	
泰国	政府	参议院	senate.go.th	144MB	邮件	2021.12.31	邮服权限	三组	
泰国	政府	国内贸易部	cit.go.th				主站权限・办公网权限・邮服权限	三组	
泰国	政府	国务委员会办公室	mailcrisdika.go.th				域内两台机器权限	三组	
泰国	政府	内政部	molgo.th				部分1服 务器 权 限 ・ 邮 服权 限	三组	
泰国	政府	商务部	moc.go.th				主站权限・办公网权限・邮服权限	三组	
香港	教育	香港东华学院	twc.edu.hk				tit 权限・办公网权限・邮服权限	三组	
香港	教育	香港教育大学	eduhk.hk	3.23GB	数in		tit 权限・办公网权限・邮服权限	三组	样本为多目标邮箱数据・文件均为单机Outlook数据
香港	教育	香港科技大学	ust.hlc	2.48GB	文件、邮件	2021	部分体系pc权限	三组	
香港	教育	香港树仁大学	hksyu.edu	643MB	数据表	2019.10 - 2021.03	主站权限•办公网权限 ・ 邮服权限	三组	样本为多目标邮箱数据 ・目标有：高级行政助理李家裕、校长胡怀中、中国联络处处长歌泰光

Figure 4: list of on-going cyber operations

Columns contain information on

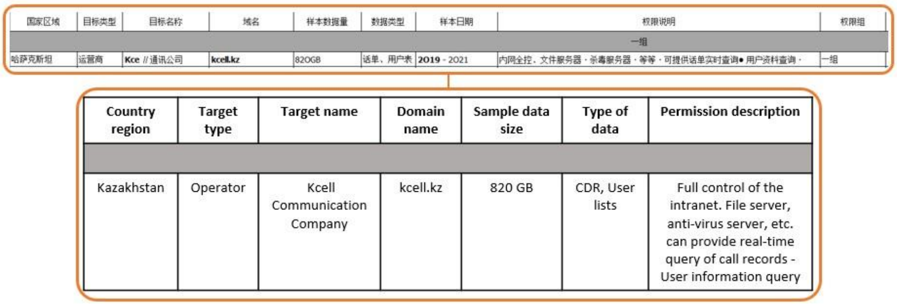
- country of destination,
- target type,
- target name,

- domain,
- file sample size,
- date of sampling,
- type of data;
- access options,
- rights group; and
- comments regarding the listed entity.

The data covers a period of up to two years in which i-Soon is believed to have gained access to the affected networks. Leaked chat logs show that listed samples are sent to customers for evaluation. In case of approval by the customer, a complete data set is provided by i-Soon; in case of refusal, other data is acquired.

In its entirety, the leaked data provides decisive insight into the actual extent of cyber operations. It shows that compromises not only lasted a long time, but were also often far-reaching in terms of access to information and obtained administrative rights. Customers were given comprehensive powers in the infiltrated networks with which it was possible to gain a deep understanding of internal structures of the compromised organizations.

One example of the scope of activities is the case of a Kazakh telecommunications company. To give possible clients a first impression, i-Soon offered a total of 820 GB of exfiltrated company data as a sample. Offered services included the full control over the intranet including file servers, anti-virus servers, etc. as well as the possibility of real-time queries on users' call records (see Figure 5).



国家区域	目标类型	目标名称	域名	样本数据量	数据类型	样本日期	权限说明	权限组
一组								
哈萨克斯坦	运营商	Kce //通讯公司	kcell.kz	820GB	话单、用户表	2019 - 2021	内网全控，文件服务器，杀毒服务器，等等，可提供话单实时查询● 用户资料查询，	一组

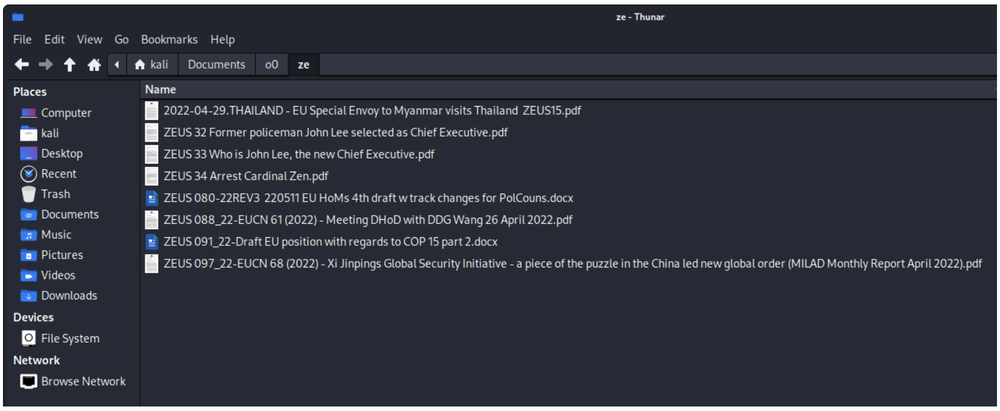
Country region	Target type	Target name	Domain name	Sample data size	Type of data	Permission description
Kazakhstan	Operator	Kcell Communication Company	kcell.kz	820 GB	CDR, User lists	Full control of the intranet. File server, anti-virus server, etc. can provide real-time query of call records - User information query

Figure 5: data example of Kazakh telecommunications company[4]

[4] The table is shortened for a better overview. Entries for the date of the operation and the rights group are not included.

Further findings on concrete i-Soon targets were obtained by the evaluation of leaked screenshots of captured data. Amongst other things, they contain chat histories and folder directories with victim data and imply activities against targets including EU institutions and member states. Although there is no further information on the individual attack operations, the screenshots indicate the extent to which i-Soon is able to compromise the internal networks of government organizations.

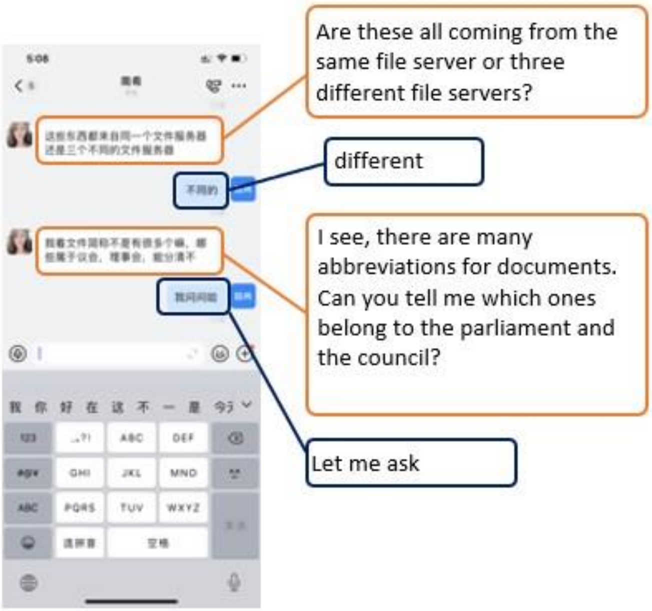
For example, one screenshot of a folder directory shows files that appear to originate from a French entity. The list of classified EU documents contain the keyword ZEUS (see Figure 6). This stands for "ZED! For European Union Security" and is an encryption standard developed by the French company Prim'X Technologies. ZED! is used by EU institutions and member states to send classified files. The procedure is also used for classified NATO files.



2022-04-29.THAILAND - EU Special Envoy to Myanmar visits Thailand ZEUS15.pdf
ZEUS 32 Former policeman John Lee selected as Chief Executive.pdf
ZEUS 33 Who is John Lee, the new Chief Executive.pdf
ZEUS 34 Arrest Cardinal Zen.pdf
ZEUS 080-22REV3 220511 EU HoMs 4th draft w track changes for PolCouns.docx
ZEUS 088_22-EUCN 61 (2022) - Meeting DHoD with DDG Wang 26 April 2022.pdf
ZEUS 091_22-Draft EU position with regards to COP 15 part 2.docx
ZEUS 097_22-EUCN 68 (2022) - Xi Jinpings Global Security Initiative - a piece of the puzzle in the China led new global order (MILAD Monthly Report April 2022).pdf

Figure 6: EU-related victim files

The screenshots of exfiltrated data demonstrate a continued interest in information in EU matters. In addition, they reveal how flexible the methods of private hacker companies and malicious software providers are in their pursuit for information. For example, one chat discussed if (exploited) documents contained abbreviations for "the (European) Parliament" or "the (European) Council" (see Figure 7).



5:08

这些东西都来自同一个文件服务器
还是三个不同的文件服务器

不同的

我看文件简称不是有很多个嘛，哪些属于议会，理事会，能分清不

我问问哈

Are these all coming from the same file server or three different file servers?

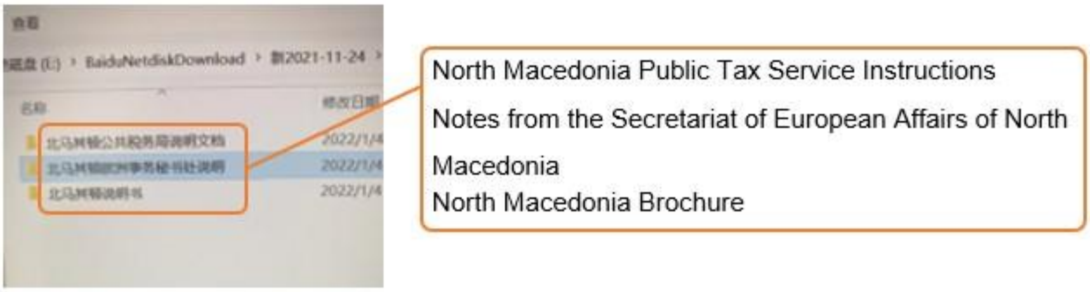
different

I see, there are many abbreviations for documents. Can you tell me which ones belong to the parliament and the council?

Let me ask

Figure 7: chat on presumably exfiltrated EU documents

Further screenshots of victim files indicate compromises in North Macedonia (see Figure 8). A folder named "Notes of the Secretariat for European Affairs of North Macedonia" may imply that attackers were interested in gaining information on the accession negotiations of North Macedonia with the EU. Furthermore, the machine-translated filename "North Macedonia Public Guidance on Tax Services" points towards a greater interest in North Macedonian public institutions.



查看

磁盘 (E:) › BaiduNetdiskDownload › 新2021-11-24 ›

名称	修改日期
北马其顿公共税务局说明文档	2022/1/4
北马其顿欧洲事务秘书处说明	2022/1/4
北马其顿说明书	2022/1/4

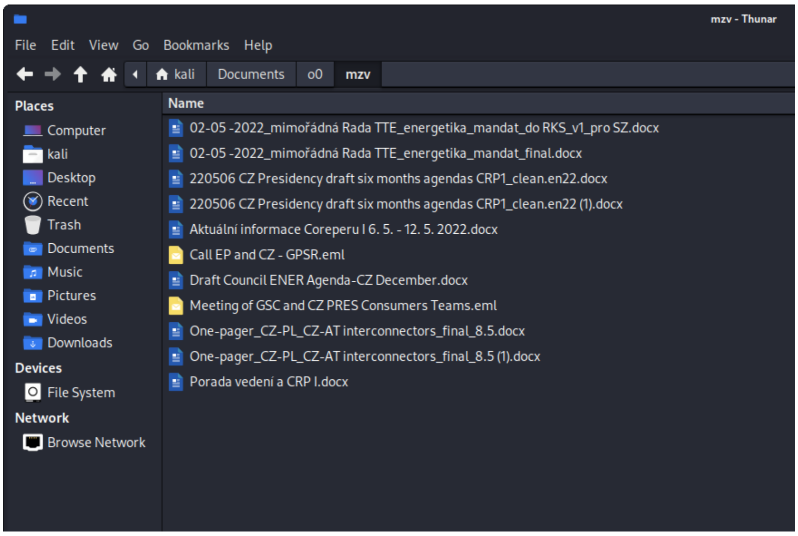
North Macedonia Public Tax Service Instructions

Notes from the Secretariat of European Affairs of North Macedonia

North Macedonia Brochure

Figure 8: folder concerning North Macedonia

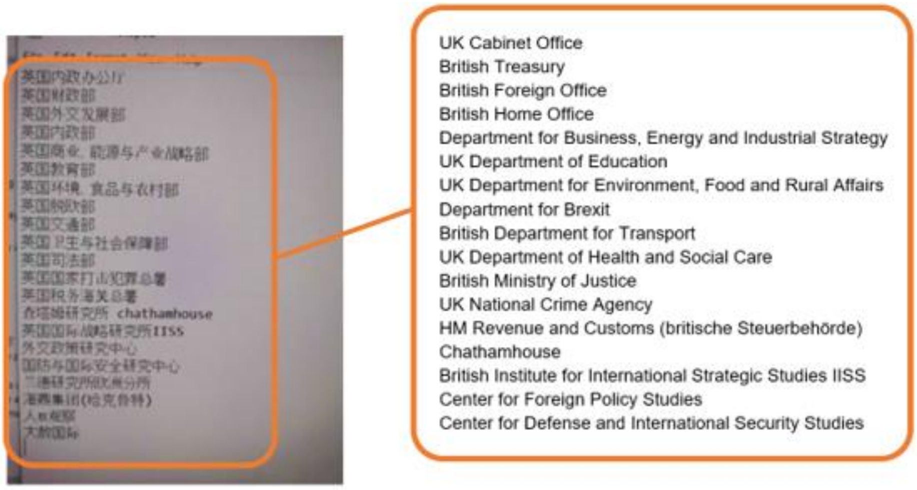
There is more evidence that marks the attacker's interest in EU topics. One leaked screenshot contains the abbreviation "mvz" in the directory path, which may stand for Ministry of Foreign Affairs of the Czech Republic (Ministerstva zahranicnich veci). The documents refer to the rotating Presidency of the Council of the EU for the second half of 2022 (see Figure 9).



02-05 -2022_mimořádná Rada TTE_energetika_mandat_do RKS_v1_pro SZ.docx
02-05 -2022_mimořádná Rada TTE_energetika_mandat_final.docx
220506 CZ Presidency draft six months agendas CRP1_clean.en22.docx
220506 CZ Presidency draft six months agendas CRP1_clean.en22 (1).docx
Aktuální informace Coreperu I 6. 5. - 12. 5. 2022.docx
Call EP and CZ - GPSR.eml
Draft Council ENER Agenda-CZ December.docx
Meeting of GSC and CZ PRES Consumers Teams.eml
One-pager_CZ-PL_CZ-AT interconnectors_final_8.5.docx
One-pager_CZ-PL_CZ-AT interconnectors_final_8.5 (1).docx
Porada vedení a CRP I.docx

Figure 9: files related to the Czech Republic

Another screenshot shows a possible target selection for cyber campaigns in the United Kingdom (UK) (see Figure 10). Here, numerous entities in the context of foreign policy are listed. In addition, there are other institutions that appear to have been randomly listed. One possible explanation is that the attackers presume that these potentially less-secured networks provide an entry-point through which more highly secured targets can be accessed.



英国内政办公厅
英国财政部
英国外交发展部
英国内政部
英国商业、能源与产业战略部
英国教育部
英国环境、食品与农村部
英国脱欧部
英国交通部
英国卫生与社会保障部
英国司法部
英国国家打击犯罪总署
英国税务海关总署
查塔姆研究所 chathamhouse
英国国际战略研究所IISS
外交政策研究中心
国防与国际安全研究中心
兰德研究所欧洲分所
[illegible]集团(哈克[illegible])
人[illegible]
大[illegible]国际

UK Cabinet Office
British Treasury
British Foreign Office
British Home Office
Department for Business, Energy and Industrial Strategy
UK Department of Education
UK Department for Environment, Food and Rural Affairs
Department for Brexit
British Department for Transport
UK Department of Health and Social Care
British Ministry of Justice
UK National Crime Agency
HM Revenue and Customs (britische Steuerbehörde)
Chathamhouse
British Institute for International Strategic Studies IISS
Center for Foreign Policy Studies
Center for Defense and International Security Studies

Figure 10: possible targets in the UK[5]

[5] Due to poor readability, some lines were not translated.

4. Targeting in line with China’s geopolitical interests

The i-Soon-leaks provide a rare insight into the activities of a single medium-sized company. Just based on the leaked information of this one Chinese company alone, it can be assumed that there are many more companies, who carry out similar operations. Thus, it is extremely likely that there is a large number of successful cyberattacks worldwide that are hitherto undetected.

Both the target countries exposed in the leak and the targeted information show a focal targeting on political topics by i-Soon. The regional focus on Hong Kong, Thailand, Taiwan, Kazakhstan, Malaysia and Mongolia, as well as the numerous attacks on government institutions and telecommunications providers, coincide with China's geopolitical interests. The aforementioned countries are relevant targets for obtaining political information.

The final report on i-Soon covers offered products and customers (part 4). The previous reporting on the i-Soon-leaks exposes the organization and methods of i-Soon APT units (part 1) and examines i-Soon’s links to the Chinese security apparatus (part 2).

Publication information

Published by
Bundesamt für Verfassungsschutz
Abteilung 4
Merianstraße 100
50765 Köln
poststelle@bfv.bund.de
www.verfassungsschutz.de
Tel.: +49 (0) 228/99 792-0
Fax: +49 (0) 228/99 792-2600

Image credits
cover: BfV, ai-generated

Date of Information
July 2024