



网络空间威胁对抗防御技术研讨会
暨 第十届安天网络安全冬训营

浪海横流

执行体全量识别与精细管控

2022年网络安全威胁回顾

——安天2022年网络安全年报（预发布版）内容提要



安天 | 技术委员会常务副主任 李柏松



目 录

01 / 高级持续性威胁 (APT)

02 / 勒索攻击

03 / 挖矿木马

04 / 数据泄露 & 威胁泛化



网络空间威胁对抗防御技术研讨会
暨 第十届安天网络安全冬训营



01

高级持续性威胁 (APT)

全球APT攻击行动、组织归属地理位置分布图



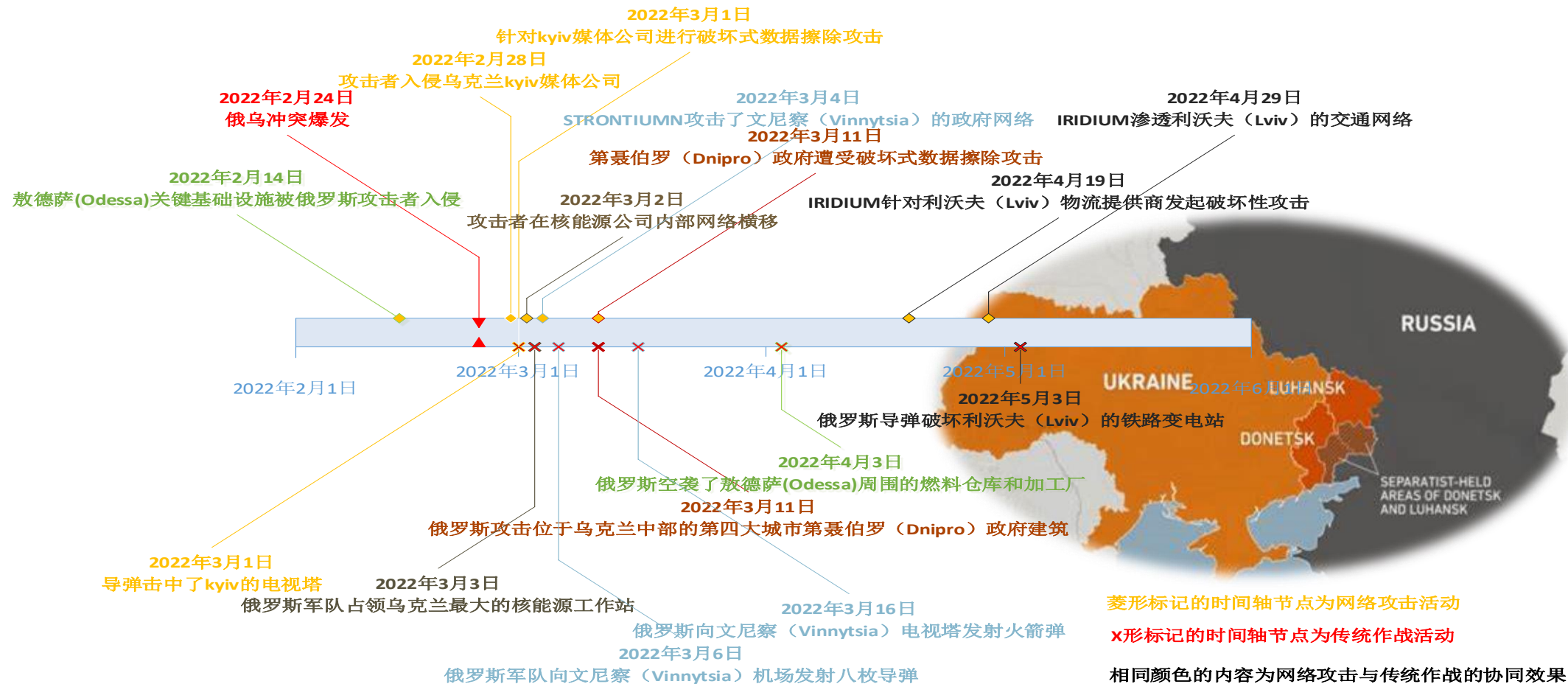
黄色的字是2022年活跃的攻击组织 ★ 星号代表2022年新增攻击组织 ● APT组织

上图采用国家测绘地理信息局标准地图服务系统，中图号为GS(2016)1666号的世界地图标注。

网空闪电战成为“俄乌冲突”先行军



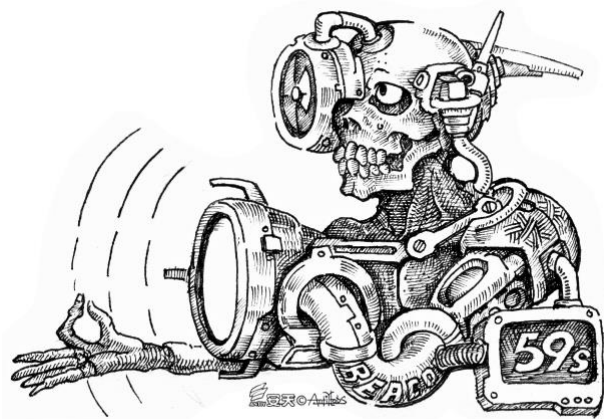
网空闪电战成为“俄乌冲突”先行军



“俄乌冲突”期间，网空/传统作战协同过程

值得警惕的不知名APT组织

- ✓商业木马
- ✓渗透测试工具
- ✓无文件实体技术
- ✓虚假标记



2022年安天观测到的新增APT组织

境外APT组织利用网络攻击栽赃构陷

STANDARD TIME ZONES OF THE WORLD

高级持续性威胁

Office文档、可执行程序
自解压文件等

Windows、Android

C++、Visual Basic

商业远控木马为主

CVE-2012-0158、CVE-2013-3906、CVE-2014-1761、CVE-2015-1641

组织
性质

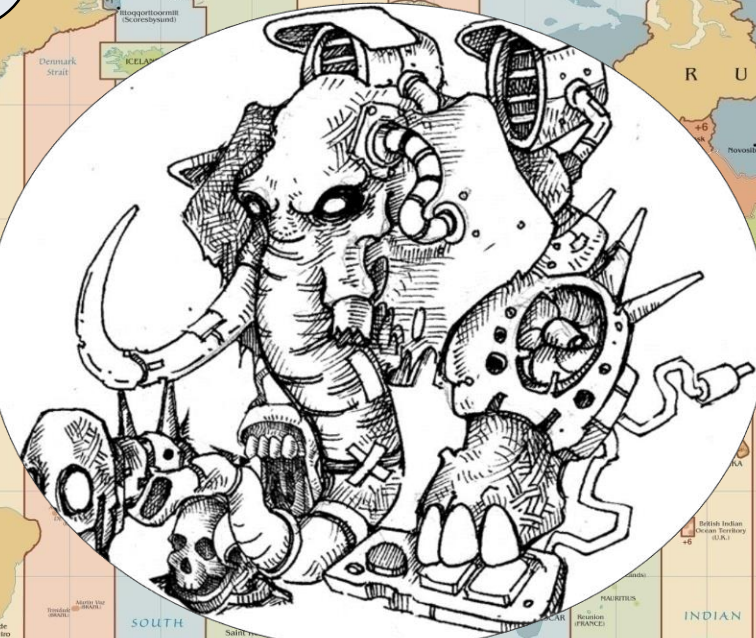
诱饵
类型

涉及
平台

开发
语言

武器
装备

使用
漏洞



疑似
来源

印度

活动
时间

最早可追溯到2012年

攻击
意图

窃取情报

攻击
手法

鱼叉邮件为主

攻击
技术

内存解密,内存注入,数字证书,时间戳篡改,文件体积填充

针对
目标

印度境内的社会活动人士, 及中国和巴基斯坦军事政治等目标。



网络空间威胁对抗防御技术研讨会
暨 第十届安天网络安全冬训营



02

勒索攻击

部分勒索攻击团伙开始运营挖矿木马

Bitcoin, ETH and BNB vs S&P 500 and Gold in 2022



破坏活动被伪装为勒索攻击

UKRAINE

RUSSIA



... vote! All your files, documents, photoes, videos, databases etc. have been successfully encrypted!

... computer has a special ID: [REDACTED]

... not try to decrypt then by yourself - it's impossible!

It's just a business and we care only about getting benefits. The only way to get your files back is to contact us and get further instructions.

To prove that we have a decryptor send us any encrypted file (less than 650 kbytes) and we'll send you it back being decrypted. This is our guarantee.

NOTE: Do not send file with sensitive content. In the email write us your computer's special ID (mentioned above).

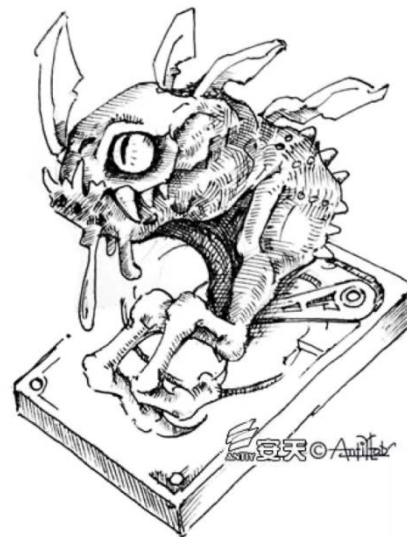
... you want to get your files back contact us:

...@protonmail.com

...@protonmail.com - if we don't answer you during 3 days

HermeticRansom 勒索信

```
18 if ( !wip_str )
19     return 0x57;
20 chunkPtr = wip_str->chunkPtr;
21 if ( !chunkPtr )
22     return 0x57;
23 disk_num = wip_str->diskNumber;
24 NumberOfBytesWritten = 0;
25 wnsprintfW(fileName, 260, L"\\\\\\\\.\\EPMNTDRV\\%u", disk_num); // EaseUS Partition Master
26 hndl = check_disk_geom_type(fileName, &dev_geom, 0);
27 hFile = hndl;
28 if ( !hndl || hndl == -1 )
29     goto finish;
30 lpBuffer = wip_str->randomBufToWrite;
31 LODWORD(nNumberOfBytesToWrite) = wip_str->sizeBuffer;
32 do
33 {
34     LowPart = chunkPtr->offset.LowPart; // retrieve the offset from the structure
35     HighPart = chunkPtr->offset.HighPart;
36     chunk_end = __PAIR64__(HighPart, LowPart) + chunkPtr->chunk_size;
37     HIDWORD(nNumberOfBytesToWrite) = HighPart;
38     if ( __SPAIR64__(HighPart, LowPart) < chunk_end )
39     {
40         do
41         {
42             NumberOfBytesWritten = 0;
43             if ( !SetFilePointerEx(hFile, __PAIR64__(HighPart, LowPart),
44
45             if ( !WriteFile(hFile, lpBuffer, nNumberOfBytesToWrite, &Numb
46                 GetLastError();
47             HighPart = (nNumberOfBytesToWrite + LowPart) >> 32;
48             LowPart += nNumberOfBytesToWrite;
49             next_offset = chunkPtr->offset.QuadPart + chunkPtr->chunk_siz
50             HIDWORD(nNumberOfBytesToWrite) = HighPart;
51         }
52         while ( __SPAIR64__(HighPart, LowPart) < next_offset );
53     }
54     chunkPtr = chunkPtr->fLink;
55 }
56 while ( chunkPtr != wip_str->chunkPtr );
57 if ( FlushFileBuffers(hFile) )
58     LastError = 0;
59 else
60 finish:
61     LastError = GetLastError();
62     if ( hFile )
63     {
64         if ( hFile != -1 )
65             CloseHandle(hFile);
66     }
67     return LastError;
68 }
```



截图引自HermeticWiper: A detailed analysis of the destructive Malware that targeted Ukraine



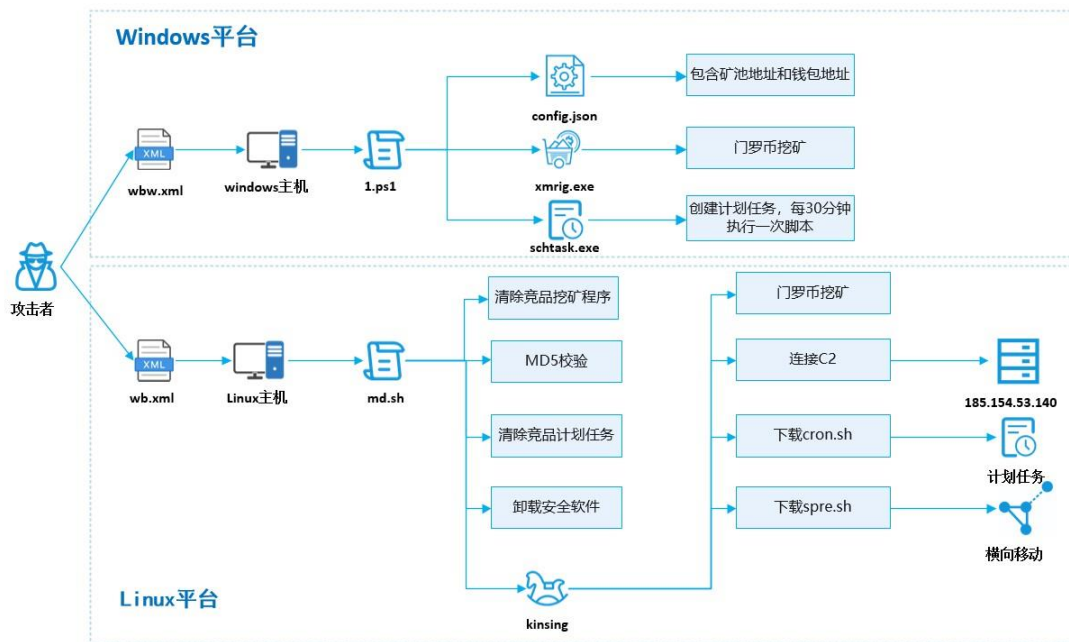
网络空间威胁对抗防御技术研讨会
暨 第十届安天网络安全冬训营



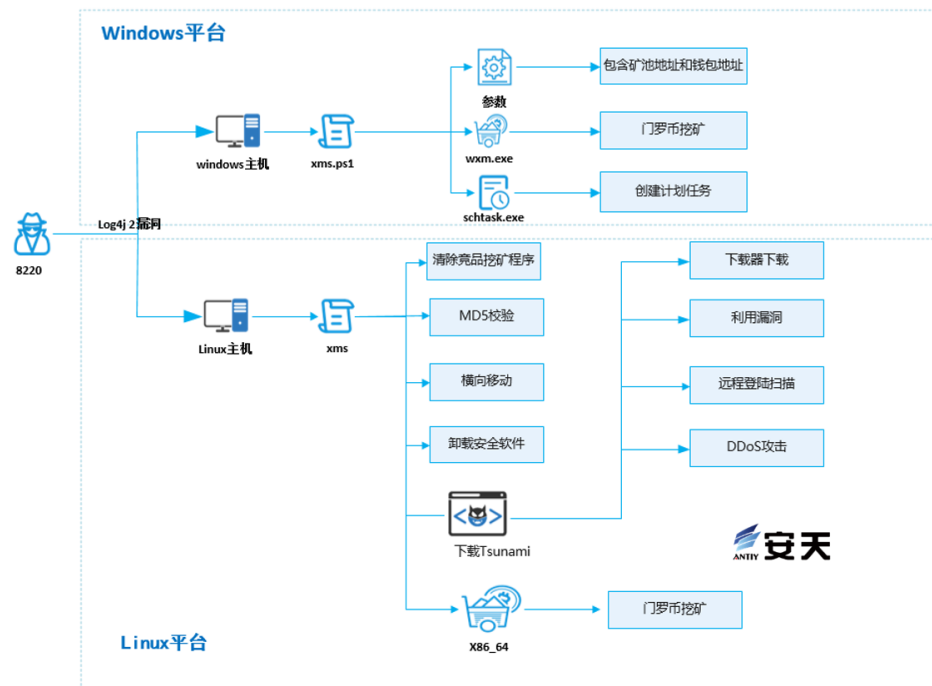
03

挖矿木马

挖矿木马团伙快速利用漏洞开展攻击行动

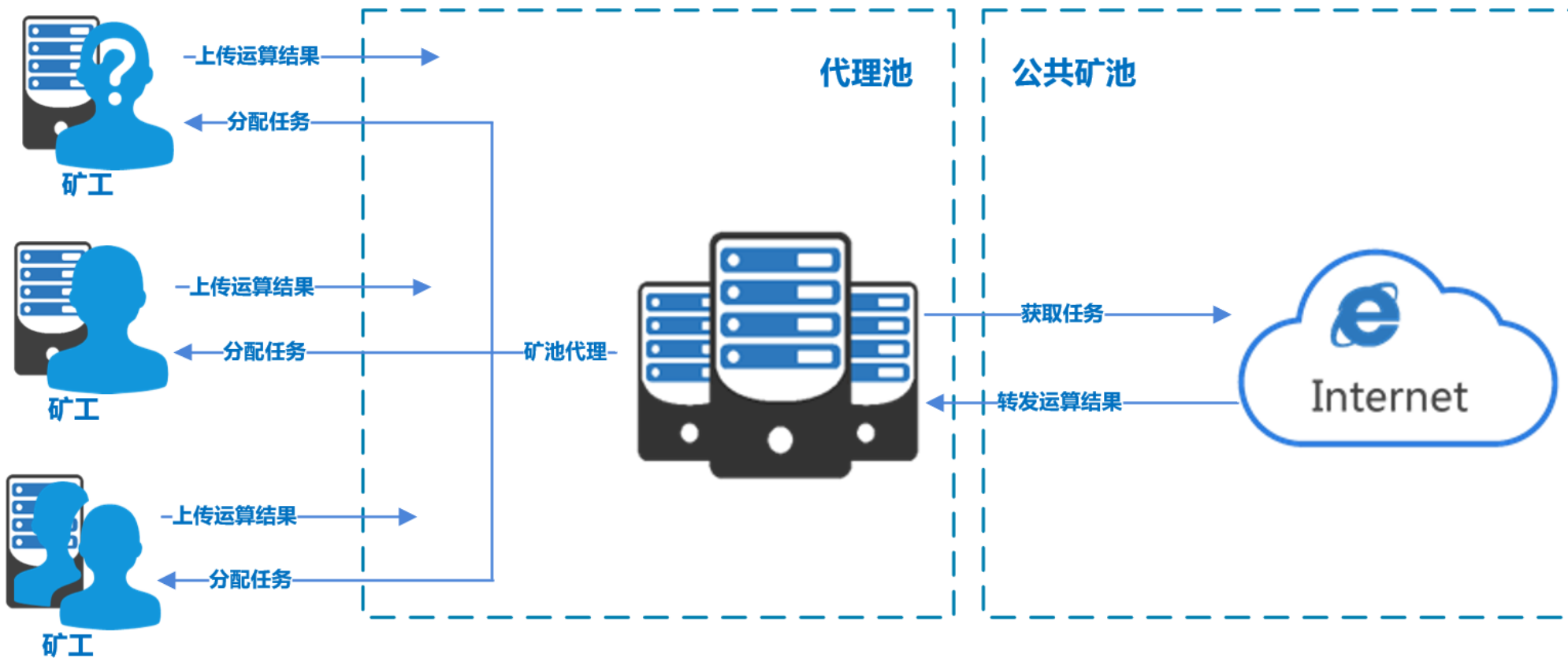


H2Miner挖矿组织攻击活动



8220挖矿组织攻击活动

挖矿木马使用矿池代理规避检测





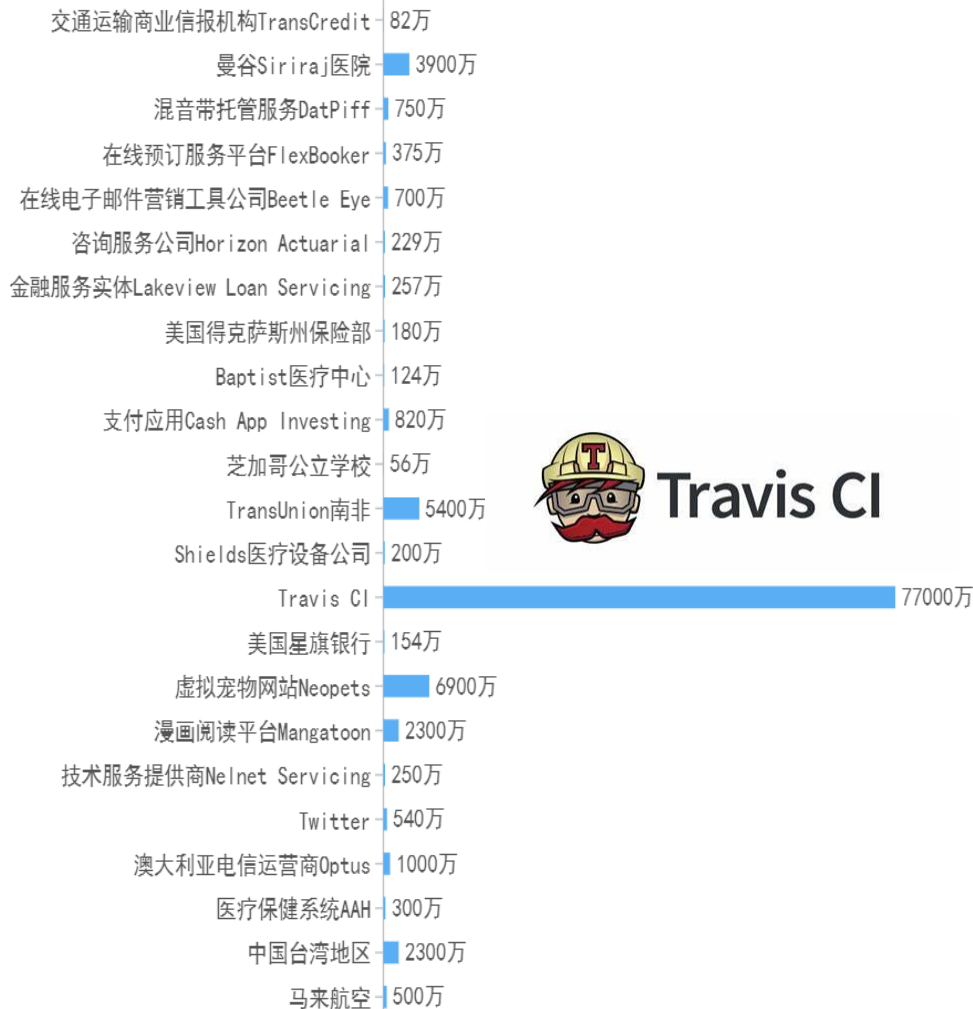
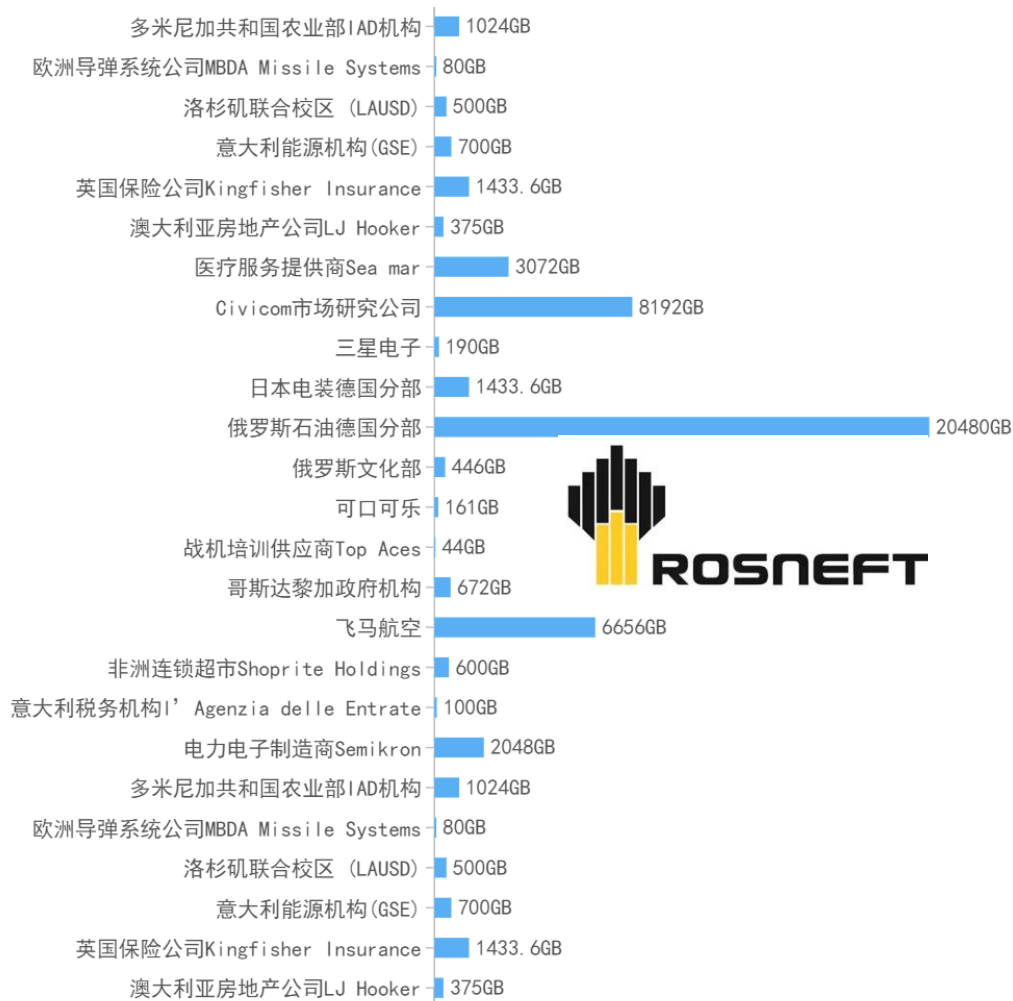
网络空间威胁对抗防御技术研讨会
暨 第十届安天网络安全冬训营



04

数据泄露 & 威胁泛化

2022年影响较大的数据泄露事件



威胁正在加速泛化



2015年



2017年



2019年



2021年

2016年



2018年



2020年



征求意见稿





网络空间威胁对抗防御技术研讨会
暨 第十届安天网络安全冬训营

浪海横流

感谢大家的关注



安天冬训营 wtc.antiy.cn