网络空间威胁对抗与防御技术研讨会
暨 第十一届安天网络安全冬训营

安天《威胁通缉令》年度更新介绍

安天安全研究与应急处理中心

执行体治理赋能与大模型辅助

01 安天《威胁通缉令》介绍

02 安天《威胁通缉令》年度更新解读

01 安天《威胁通缉令》介绍

什么是威胁通缉令?

扑克牌卡牌的形式

威胁通缉令是安天**自2011年**发起的一项安全知识科普活动。安天CERT工程师依托年度监测分析统计结果，每年年初对上一年度有代表性的安全威胁进行提炼总结——例如APT攻击中的恶意代码工具或利用的0day漏洞、有较大传播感染范围的恶意代码、有特殊技术特点的恶意代码等等，将其分类整理，并最后印刷在一套扑克牌上。

通缉令是扑克牌卡牌的形式，“**黑桃♠**”、“**红心♥**”、“**梅花♣**”、“**方块♦**”等4种花色分别对应上一年影响最大的4类威胁，同时每类威胁按照综合的评估原则，列出13个典型的具体威胁，**大小王为上一年度最值得关注的TOP1和TOP2威胁。**

十三年不懈的威胁追踪与持续更新

2011 2012 2013 2014 2015 2016 2017 2018 2019 2020 2021 2022 2023

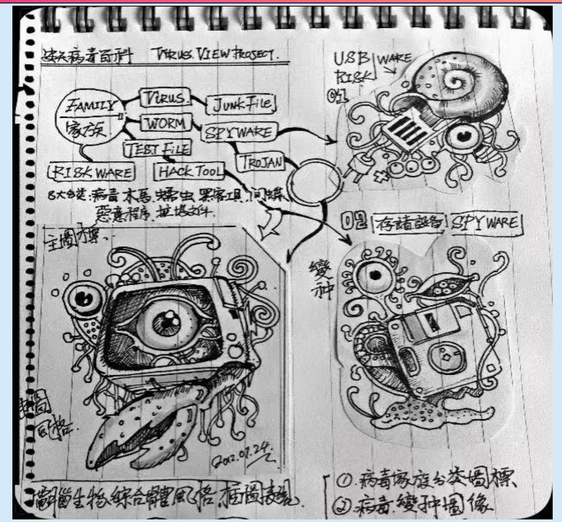
揭秘威胁通缉令的绘制过程

Mappy 文化创意工作室

Mappy文化创意工作室精心创作出了威胁通缉令系列扑克牌，以手绘的威胁可视化形象给大家揭露了隐藏在网络背后攻击者的丑陋面目。

安天工作者们以**威胁的名称、攻击手段、传播方式**等特征作为基础，对其进行可视化的设计，从而让人们直观的感受到抽象的“威胁”所带来的威胁，理解安全工作者所带来的价值。

从威胁可视化形象维度来看，安天以魔幻炫酷的克苏鲁风格作为这些**“凶残”的威胁形象**，这更能彰显我们安天引擎和CERT打败这些妖魔鬼怪的勇气和能力自信。



病毒形象设计手稿

威胁通缉令以独特的创意活跃在各大展会论坛

“**威胁通缉令**”扑克牌作为礼品在历届国家网络安全宣传周活动、中国网络安全年会、RSA大会、XCon安全焦点信息安全技术峰会、5G大会、数字中国建设峰会、大国工匠创新交流大会、高校数字校园高质量发展研讨会、华中地区高校网络安全专题交流会、大湾区数字化实践峰会等展会论坛活动赠送，宣传网络安全知识，提升公众网络安全防护技能。

哈工大活动现场

大国工匠展会现场

RSA大会现场

02

安天《威胁通缉令》年度更新解读

历年威胁通缉令威胁类型变更说明

年份\含义	黑桃♠	红心♥	梅花♣	方块♦	小王	大王
2011	木马与后门	蠕虫	感染式病毒	色情广告片	Rootkit	僵尸程序
2012	木马与后门	感染式病毒	蠕虫	移动威胁	Rootkit	僵尸程序
2013	木马与后门	感染式病毒	蠕虫	移动威胁	Rootkit	僵尸程序
2014	APT威胁	移动威胁	木马	蠕虫与感染式	Malware/Other（泛化）	APT
2015	APT威胁	移动威胁	木马	蠕虫与感染式	Malware/Other（泛化）	APT
2016	APT威胁	移动威胁	木马	蠕虫与感染式	商业军火	APT
2017	APT威胁	移动威胁	木马	蠕虫与感染式	勒索软件	APT
2018	APT威胁	移动威胁	木马	蠕虫与感染式	勒索软件	APT
2019	APT威胁	移动威胁	木马	蠕虫与感染式	勒索软件	APT
2020	APT威胁	移动威胁	木马	蠕虫与感染式	勒索软件	APT
2021	APT威胁	漏洞	木马	蠕虫与感染式	勒索软件	APT
2022	APT威胁	漏洞	木马	勒索	勒索软件	APT
2023	APT攻击装备	漏洞利用	木马	勒索攻击	APT	勒索即服务及定向勒索攻击

2023年威胁通缉令各花色更新详解

2023年威胁通缉令								
	黑桃♠		红心♥		梅花♣		方块♦	
牌号	APT攻击装备	同比变化	漏洞利用	评分	特洛伊木马	同比变化	勒索攻击	同比变化
A	方程式	-	curl缓冲区溢出(CVE-2023-38545)	9.8	AgentTesla	-	LockBit	-
K	白象	↑1	ICMP远程代码执行（CVE-2023-23415）	9.8	H2Miner	新上榜	Clop	↑5
Q	孔夫子	新上榜	Apache Shiro身份认证绕过（CVE-2023-34478）	9.8	Redline	-	BlackCat	↓1
J	苦象	↑1	RocketMQ远程命令执行（CVE-2023-37582）	9.8	SwimSnake	新上榜	BlackBasta	新上榜
10	Kimsuky	新上榜	WinRAR远程代码执行（CVE-2023-38831）	7.8	GuLoader	新上榜	Akira	新上榜
9	奇幻熊	-	WPS Office软件代码执行	暂无	Sysrv-Hello	新上榜	8Base	新上榜
8	响尾蛇	新上榜	Coremail远程代码执行	暂无	RecordBreaker	新上榜	Play	新上榜
7	Konni	新上榜	Chrome任意代码执行（CVE-2023-3216）	8.8	TeamTNT	新上榜	BianLian	新上榜
6	DarkPink	新上榜	GitLab命令执行（CVE-2023-23946）	7.5	Formbook	新上榜	Royal	新上榜
5	CNC	↑2	GitLab文件包含（CVE-2023-22490）	5.5	WatchDog	新上榜	BlackByte	↑2
4	灵猫	新上榜	Outlook权限提升（CVE-2023-23397）	9.8	Qbot	↑1	Rhysida	新上榜
3	透明部落	新上榜	Windows权限提升（CVE-2023-21746）	7.8	Gh0st	↓1	NoEscape	新上榜
2	双尾蝎	新上榜	Linux Kernel权限提升（CVE-2023-32233）	7.8	ObserverStealer	新上榜	Medusa	新上榜

2023年度最值得关注的TOP1和TOP2威胁

依托RaaS的定向勒索攻击行为已经形成了窃取数据、瘫痪系统和业务、贩卖数据和曝光数据的组合作业。其最大化风险不只是系统和业务瘫痪无法恢复，而且同时面临被攻击企业的用户信息、关键数据、文档、资料、代码等核心资产被倒卖，被公开的风险，从而带来更大的连锁反应。

大王

勒索即服务及定向勒索攻击（RaaS+APT+Ransomware）

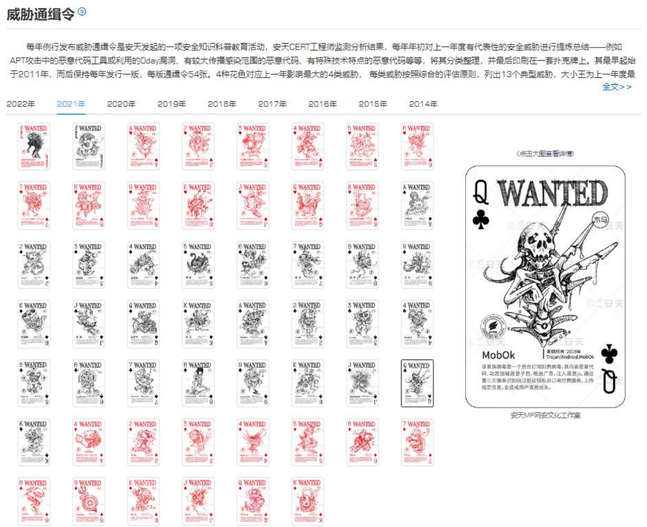
小王

高级持续性威胁（APT）

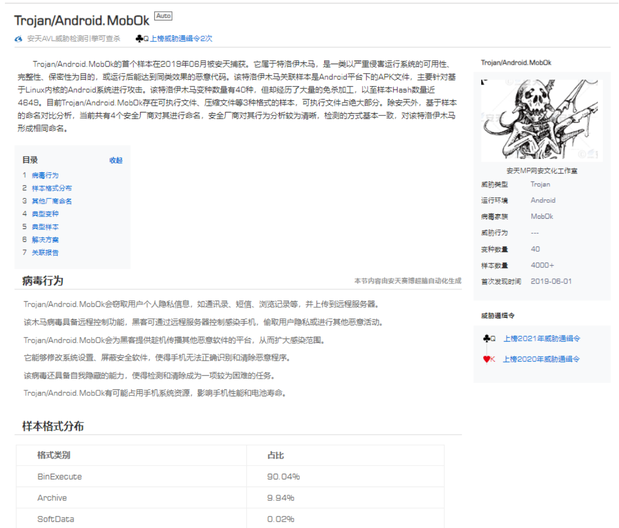
2023年全球高级持续性威胁（APT）活动的整体形势依然非常严峻。基于安天持续监测的内部和外部的情报来源，2023年全球公开安全研究报告数量696篇，其中披露的安全报告涉及162个APT组织，其中包括2023年新增的66个APT组织。

威胁通缉令现已上线计算机病毒百科

受限于卡片的数量、更新频率、卡片版面的大小，感兴趣的用户很难深入了解威胁的行为机理、防御方案等信息。因此我们选择将威胁通缉令上线计算病毒百科，用户在浏览威胁通缉令专题的时候，可以查看关联的威胁词条，进一步了解威胁的详细信息。



病毒百科上的历年威胁通缉令



病毒家族详细信息（样本行为、样本格式分布、解决方案等）

扫描二维码查看威胁通缉令详细信息

网络空间威胁对抗与防御技术研讨会
暨 第十一届安天网络安全冬训营

了解网络威胁，提高防范意识

安天冬训营 wtc.antiy.cn

执行体治理赋能与大模型辅助

北向守望