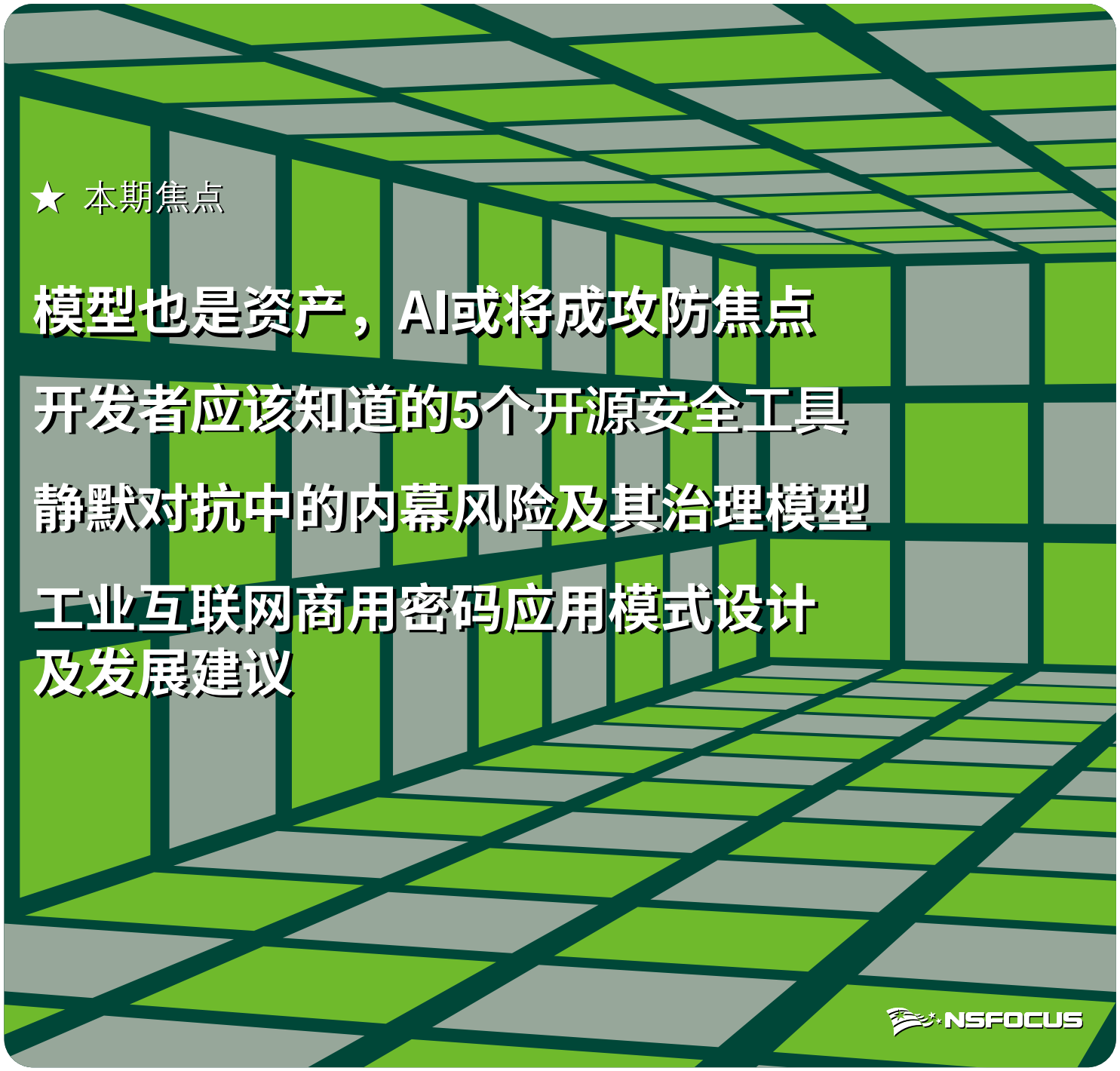
安全+
SECURITY
2023/07 总第 057
技术版 ▶▶ 与安全人士分享技术心得 Share technique experience with security professionals



★ 本期焦点

模型也是资产，AI或将成攻防焦点

开发者应该知道的5个开源安全工具

静默对抗中的内幕风险及其治理模型

工业互联网商用密码应用模式设计及发展建议

NSFOCUS

本期看点 HEADLINES

3 模型也是资产，AI或将成攻防焦点

6 开发者应该知道的5个开源安全工具

18 静默对抗中的内幕风险及其治理模型

38 工业互联网商用密码应用模式设计及发展建议

主办：绿盟科技
策划：《安全+》编委会
地址：北京市海淀区北洼路4号益泰大厦三层
邮编：100089
电话：(010)6843 8880-5462
传真：(010)6872 8708
网址：www.nsfocus.com

2023/07 总第 057

欢迎您来信nsmagazine@nsfocus.com 与我们交流，
分享您的建议和评论。（《安全+》部分图片来源于网络）

安全+ SECURITY

目录 CONTENTS

卷首语 叶晓虎 2

RSAC 3-17

模型也是资产，AI 或将成攻防焦点 刘文懋 3

开发者应该知道的 5 个开源安全工具 皮靖 6

僵尸网络威胁态势观察 果鹏 10

混合式办公中的十大隐私挑战 顾奇 14

安全趋势 18-37

静默对抗中的内幕风险及其治理模型 张睿 18

5G+ 医疗的安全风险与防护方向 覃达键 陈鸣昊 23

云原生 API 安全：背景、态势与风险防护 浦明 26

浅谈 5G 智慧港口网络安全防护 张铮 庞彬彬 34

能力构建 38-56

工业互联网商用密码应用模式设计及发展建议 杨博 38

公有云攻防系列：云凭证的泄露与利用 李来冰 45

Rilide：基于社工学的恶意软件 黄硕麒 49

SCARLETEEL：一起利用 Terraform、Kubernetes 和 AWS 的数据窃取事件 李来冰 52

政策解读 57-60

网络安全政策导读（2023 年 4-5 月） 林涛 张文辉 57

网络安全智能化的发展，正随着多维度感知智能技术的演进，向认知智能和决策智能化方向演进。特别是随着以ChatGPT等大语言模型为代表的大模型技术或基础模型技术的爆炸式发展，形成人-机器-环境协同的新交互范式，已为世界展示了实现通用人工智能技术的可能性。

作为全球规模最大的网络安全盛会之一，于2023年4月27日落幕的RSA大会从行业趋势、细分领域发展、技术与应用展现了安全世界全新视角：生成式AI已成为最受关注的热潮，持续输出着创新、商机与威胁。

本期《安全+》将继续立足网络安全发展，从前沿技术发展、安全理念应用等视角出发，探索网络安全新发展所需的整体脉络和发展路径。

当下，人工智能技术已经被应用于网络空间安全领域，在应对数字化转型过程中的各类安全难题上发挥着巨大潜力。大语言模型正在极大推动安全运营的发展进程。事实上，安全运营的自动化与智能化水平，已成为网络空间对抗成败的关键因素。大模型技术在知识容量、逻辑推理、人机交互等方面的绝对优势，全面提升智能安全运营场景下数据感知、推理认知、行动决策等多场景、多步骤、多目标任务的智能分析与交互水平，在大幅降低安全运营资源投入的同时，有效应对安全运营中海量日志告警、溯源路径爆炸、高水平研判人员缺失、处置决策冗长等诸多挑战。

在安全研究方面，绿盟科技持续致力于安全攻防研究及前沿技术的研究，开展类ChatGPT技术在安全领域应用的尝试，旨在实现对安全运营的智能化支撑，进一步提升安全运营服务效能。

技术爆炸不断定义变革，人工智能正立潮头，驶向新的“大航海时代”。

叶晓虎

模型也是资产，AI或将成攻防焦点

绿盟科技 创新研究院 刘文懋

美国旧金山时间 4 月 24 日下午，RSA Conference 2023 正式公布创新沙盒本年度冠军，人工智能安全厂商 HiddenLayer 一举夺魁。本文将从创新沙盒冠军 HiddenLayer 出发，进一步解读探讨 AI 安全。

1. 背景

人工智能安全厂商 HiddenLayer 成为最后的获胜者，不禁让笔者想到 2018 年的 Big ID，场景是如此相似。

2018 年 4 月 15 日 RSA 大会开幕，而一个月后的 5 月 25 日，通用数据保护条例 GDPR 将要生效，数据合规大棒将要落下，所有企业对数据安全的需求非常迫切，而主打帮助客户满足数据合规的 BigID 就成为呼声最高的决赛选手，而 BigID 当年也不负众望夺冠。今年 OpenAI 基于大语言模型的 ChatCPT 和 GPT-4 吸引了全世界各个行业的关注，人工智能达到了前所未有的期望高度，在一些赛前的投票中，听闻主打 AI 攻防的 HiddenLayer 关注最多，此次夺冠也可谓是情理之中。

表 1 历年创新沙盒冠军

时间	获胜者	方向
2005	Sourcefire	IPS
2006	Imperva	Web安全
2009	Alert Enterprise	物理及逻辑安全整合服务
2010	Altor	云安全
2011	Invincea	高级终端威胁检测服务
2012	Appthority	APP风险管理
2013	Remotium	BYOD移动安全
2014	Red Owl Analytics	风险监督
2015	Waratek	RASP/WAF
2016	Phantom	SOAR
2017	UnifyID	身份认证
2018	Big ID	数据安全
2019	Axonius	资产管理
2020	Securiti.ai	数据安全
2021	Apiiro	DevSecOps
2022	Talon	浏览器安全
2023	HiddenLayer	AI安全

2. AI 安全将成为新的赛道

安全行业向来以细分赛道多而著称，网络安全、终端安全、应用安全、云计算安全、物联网安全，等等。而本次创新沙盒花落 HiddenLayer，也是 RSAC 创新沙盒第一次把冠军颁发给 AI 安全。这在印证一个趋势：AI 安全将会成为一个独立的赛道。而这个赛道的出现背后，则是人工智能平民化、产业化。

从过去来看，每次随着新技术的出现，安全同行会考虑两个问题，一是这种新技术的自身安全，二是如何使用新技术赋能安全。通常而言，人们往往会先考虑第一个问题，以解决其带来的新风险，再利用新技术的新特性来帮助安全企业自己提升能效。其中原因是直接、新增业务机会的吸引力大于降本增效。比如，云计算出现后，我们一定是先论证访问控制、入侵检测等机制如何应用于云环境，设计并实现虚拟化安全、云原生安全解决方案；然后考虑使用云计算敏捷弹性的特性去重构现有的安全原子能力。其他如区块链、SDWAN 等技术莫不如此。

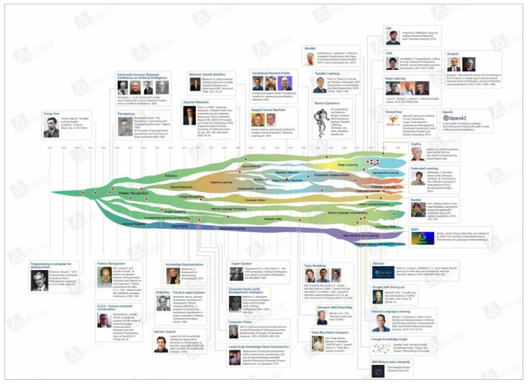


图 1 人工智能的发展

然而，人工智能却是例外，从二十世纪六十年代开始出现了三次起伏 [1]，有爆发期，也有人工智能之冬。但普遍意义的人工智能时代并没有到来，即便在 Google 的 AlphaGo 击败了围棋冠军，也只是说明了人工智能在特定领域具有超越人类的能力，但棋类运动、自然语言和图像识别等领域的成功并不能解决人类面临的所有问题，逻辑推理、领域知识、精确决策都不是彼时人工智能擅长之处。从落地角度来看，很多公司是看着图像和文本领域的效果不错就拍脑袋上 AI，而算法工程师的日常工作就是选模型、调参数，如何挖掘人工智能真正起作用的原理却很少思考，最后效果不好自然也就用不起来，因而很多领域的人工智能应用得到广泛应用，但实际效果一般。从结果来看，这些人工智能的模型价值并不高。

当然，人工智能的攻防一直是学术上的热点，如 2013 年就有研究通过对抗学习可以将一张增加了噪声的大熊猫照片骗过 AI，使其认为是长臂猿。绿盟科技也在 2022 年通过“CCF- 鲲鹏基金”资助了人工智能欺骗与防御的课题，有不错的成果。

尽管如此，AI 攻防在产业应用方面主要是在互联网巨头，独立产品的商业化落地还尚在早期，所以 HiddenLayer 宣称之前没有一家安全公司专注于模型安全。

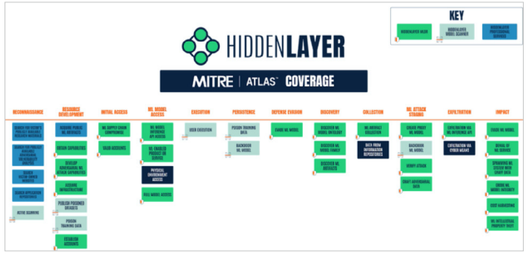
而 HiddenLayer 的夺冠，将会带动 AI 自身安全的产业。随着大语言模型和通用领域的人工智能产业爆发，之后必然还有大量的初创公司基于对现有 AI 模型的攻防推出自己的 AI 安全产品，这个细分赛道将会形成。

3. 人工智能安全也可利用既有攻防基础

从学术上看，人工智能攻防主要是站在机器学习的视角，通过对抗样本、对抗学习等技术欺骗模型或提高模型的健壮度、可解释性。似乎这些技术与传统攻防关系不大，对应的人工智能安全产品是一个内嵌于模型的紧耦合产物，所以其产品化本身难度就很大。但是 HiddenLayer 却独辟蹊径，从基础的安全理论和攻防技法入手，将高大上的 AI 安全讲解为以现有安全技术人员听得懂的形式。

例如，HiddenLayer 将模型和训练集也定义为企业中的一类资产，既然是资产就有脆弱性，也需要进行资产管理，更需要安全防护，所以从必要性上就能打动客户。其次，它在防护框架方面提出了 MLDR，复用了检测和响应的概念，这样模型的防护就能与 EDR、NDR、MDR 对等，甚至可以放置于 XDR 中，形成对企业 AI 资产的全生命周期防护。

做到了概念和框架上的自恰和兼容，具体战法上与传统攻防兼容是最不容易的。比如 AI 攻防在技术层面有成员推理、数据投毒、模型绕过、模型注入等，这些技术无论是从原理上还是从技术栈上跟传统安全攻防是不太一样的，如何能让客户理解并接受呢？幸运的是 Mitre ATT&CK 给出了针对机器学习的 ATLAS 矩阵 [3]，该矩阵枚举了诸多针对 AI 的攻击所使用的技战术，比较规范地给出了每种技术的使用场景和应对手段。而 HiddenLayer 则将其能力给出了 ATLAS 的覆盖度，以证明自己在 AI 攻防领域的全面、成熟和专业程度。



从企业 CISO 角度来看，HiddenLayer 能给出面向企业的 AI 资产梳理、风险发现和检测响应系统比较完整的方案，从防护理念、架构和产品来看都能兼容已建设的安全体系，也确实能解决企业上线 AI 引擎后知识产权保护、数据保护等一系列风险。

4. 总结

大语言模型热潮来临，人工智能已经像云计算一样被产业所认可，基于人工智能的通用性应用将无处不在。攻击者若想谋利，除了传统的网络攻防外，还会针对人工智能挖掘其弱点，对抗学习和对抗样本将会是攻击者手中武器库之一。未来人工智能的模型和训练集将会与 IT 系统、云主机一样，成为攻击者的目标。

HiddenLayer 本次夺冠，能看出传统企业对于上 AI 既迫切又担心，而 GPT 的成功也为 HiddenLayer 夺冠推了最大一把力。希望 HiddenLayer 能抓住 GPT 这波热潮，快速复制成功案例，将 AI 安全这个赛道走好、走宽。

而对于广大的安全从业者而言，除了学习网络攻防技术之外，人工智能技术和人工智能对抗技术恐怕也要是技能栈中基础之一。

国内公司也在做相关工作，比如绿盟科技天枢实验室一直从事可信人工智能（XAI）的研究，以提高模型的鲁棒性和可解释性，以抵御对抗机器学习的攻击。2022 年，“基于 XAI 的规则知识抽取引擎”获中国信通院 2022 可信 AI 案例和可信人工智能优秀实践案例。我们也会继续深入研究和孵化创新，如读者对此感兴趣，也可参与我们开源的可信人工智能项目 XAIGen。

参考文献

[1] 人工智能发展简史 ,https://www.aminer.cn/ai-history.

[2]「熊猫」变「长臂猿」,「乌龟」变「来复枪」，深度学习模型被攻击，破解之道有哪些 ,https://www.leiphone.com/category/academic/W4Wm5jfL19ZWbIbp.html.

[3] MITRE ATLAS ™ , https://atlas.mitre.org/.

开发者应该知道的5个开源安全工具

绿盟科技 安全平台技术部 皮靖

开发者在开发代码的过程中，都会担心代码、依赖、项目打包成的镜像是否存在安全问题。而 RSAC 2023 议题 5 *Open Source Security Tools All Developers Should Know About*，则推荐了 5 个开源的安全工具，覆盖代码扫描、依赖检查、基础设施扫描、容器扫描、运行时扫描 5 个方面。

在评估每种类别的安全工具时，列出了该类别下安全工具的候选集合，并综合多方面因素，最终评定出该类别下最优的安全工具。

在评估安全工具时，主要是从以下几方面进行综合裁决：

结果质量：开发视角下的结果准确度；

易用性：可以命令行使用也可以与各类 IDE 整合，速度快，结果易理解；

成熟度：社区支持情况、bug 修复情况、证书情况；

可扩展：工具容易被扩展，以适用于开发者。

每个类别推荐的工具如下：

表 1 每种类别推荐的开源工具

类别	工具名称	链接
代码扫描	Semgrep	https://github.com/returntocorp/semgrep
依赖检查	OSV-Scanner	https://github.com/google/osv-scanner
基础设施扫描	KICS	https://github.com/Checkmarx/kics
容器扫描	Trivy	https://github.com/aquasecurity/trivy
运行时扫描	ZAP	https://github.com/zaproxy/zaproxy

1. 代码扫描

代码扫描，主要用于发现代码中存在的脆弱性问题。通常包括：

OWASP 十大安全风险

CWE 25 个最常见漏洞

机密信息

自定义规则（如身份认证 / 授权信息等）

最终从如下候选工具集中，选出了 Semgrep。

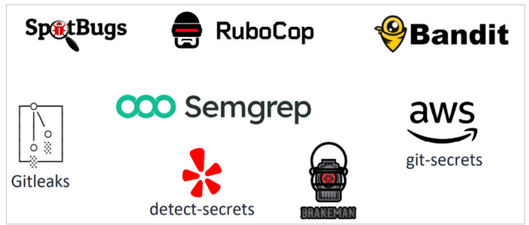


图 1 代码扫描工具候选集

Semgrep 的规则整合了很多的安全工具（如 Gitleaks，Findsecbugs, Gosec 等），而且还支持超过 30 种语言。从易用性方面看，它是无须编译的，而且可以运行在任何环境上（命令行、Docker、IDE），也是很容易扩展的，只需要编写规则就可以。Semgrep 有一个比较大的社区，贡献者也比较活跃。

Category	Languages
GA	C# · Go · Java · JavaScript · JSX · JSON · PHP · Python · Ruby · Scala · Terraform · TypeScript · TSX
Beta	Kotlin · Rust
Experimental	Bash · C · C++ · Clojure · Dart · Dockerfile · Elixir · HTML · Jsonnet · Lisp · Lua · OCaml · R · Scheme · Solidity · Swift · YAML · XML · Generic (ERB, Jinja, etc.)

图 2 Semgrep 支持的语言列表

如下图所示，便是用 Semgrep 来扫描代码，可以看到它的结果里显示 src/test.php 存在 eval($arg) 这行代码，而这行代码存在命令注入漏洞。

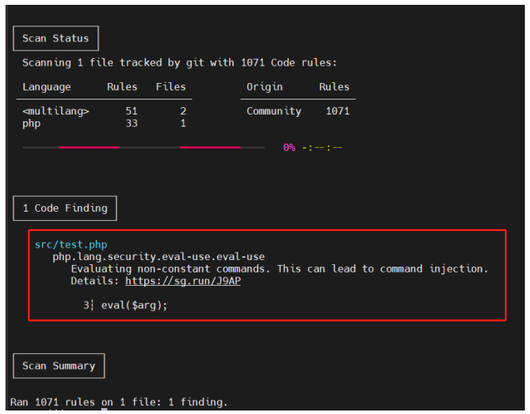


图 3 Semgrep 扫描结果

2. 依赖检查

依赖检查主要用于发现项目代码所依赖的具有漏洞的组件。主要步骤是，首先识别软件所使用的开源组件，然后与已知漏洞的数据库进行比较，从而检查出这些依赖是否存在任何公开披露的漏洞。这被称为 SCA，即软件组合分析（Software Composition Analysis）。

最终从如下工具候选集中，选出了 OSV-Scanner。

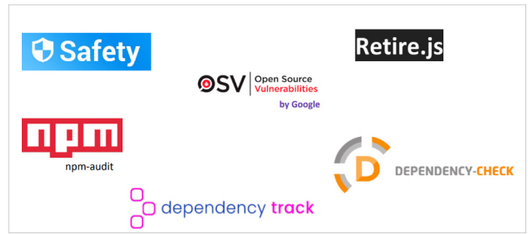


图 4 依赖检查工具候选集

OSV-Scanner 使用的是 Google 维护的 OSV 数据库（开源漏洞库），支持 13 种语言，可以扫描指定的 SBOM 和 lockfile 文件。OSV-Scanner 的受欢迎程度和社区支持度处于增长阶段见图 5

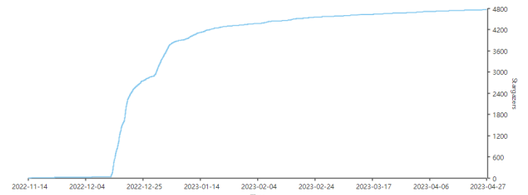


图 5 OSV-Scanner 随时间变化打星的趋势图

如图 6 所示，即为使用 OSV-Scanner 扫描 npm lockfile。它扫描了 1531 个软件包，并发现了一些安全问题。每个问题都有一个 OSV URL（安全漏洞的 ID）来提供有关漏洞的更多信息，同时还列出了与每个漏洞相关的软件包名称、版本号。

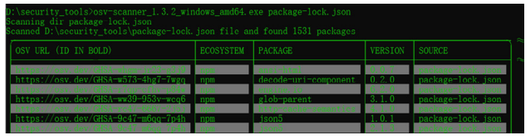


图 6 使用 OSV-Scanner 扫描 npm lockfile 的输出

3. 基础设施扫描

基础设施扫描，即将基础设施的配置和管理作为代码来处理，主要任务是在代码提交到云端之前检测出安全配置错误。这些错误可能包括：

缺少加密

宽泛的权限设置

缺少日志记录

默认设置

最终从如下工具候选集中，选出了 KICS。

图 7 基础设施扫描工具候选集

KICS 支持 18 种框架，并提供了 200 多种内置的修复方案，可以在任何地方运行 (IDE 插件、本地)。

如图 8 所示，是用 Terraform 创建了一个 EBS 卷。

```
resource "aws_ebs_volume" "web_host_storage" {
  # unencrypted volume
  #encrypted          = true
  availability_zone = "${var.region}a"
  size = 1
  tags = merge({
    Name = "${local.resource_prefix.value}-ebs"
    }, {
    git_commit           = "6e62522d2ab8f63740e53752b84a6e99cd65696a"
    git_file             = "terraform/aws/ec2.tf"
    git_last_modified_at = "2021-05-02 11:16:31"
    git_last_modified_by = "aviram@gmail.com"
    git_modifiers        = "aviram"
    git_org              = "myorg"
    git_repo             = "terragoat"
    yor_trace            = "c5509daf-10f0-46af-9e03-41989212521d"
  })
}
```

图 8 使用 Terraform 创建 EBS 卷

而 KICS 则可以扫描出其中存在的 2 个中危漏洞，一个是 IAM Access Analyzer 未定义，而另一个是 EBS 卷未启用加密 (见图 9)。

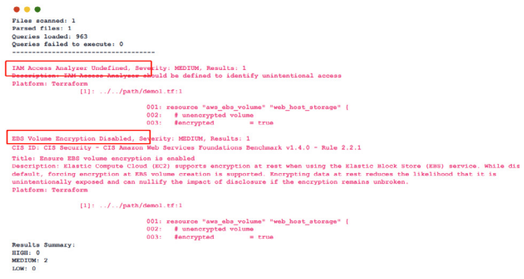


图 9 KICS 扫描结果

4. 容器扫描

容器扫描主要就是检测容器镜像中的漏洞和配置问题。最终从如下工具候选集中，选出了 Trivy。

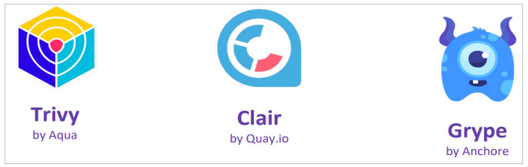


图 10 容器扫描工具候选集

Trivy 支持扫描容器镜像、文件系统、git 存储库、虚拟机等，还可以生成 SBOM。如图 11，展示了利用 Trivy 扫描 wordpress 镜像发现的漏洞情况，总共发现了 3 个漏洞，分别为 CVE-2021-33574、CVE-2022-23218、CVE-2022-23219。

libc-bin	CVE-2021-33574	CRITICAL	2.31-13+deb11u3	glibc: mq_notify does not handle separately allocated thread attributes https://avd.aquasec.com/nvd/cve-2021-33574
	CVE-2022-23218			glibc: Stack-based buffer overflow in svcunix_create via long pathnames https://avd.aquasec.com/nvd/cve-2022-23218
	CVE-2022-23219			glibc: Stack-based buffer overflow in sunrpc clnt_create via a long pathname https://avd.aquasec.com/nvd/cve-2022-23219

```
docker run aquasec/trivy image wordpress
```

图 11 Trivy 扫描 wordpress 镜像结果

5. 运行时扫描

运行时扫描，即在 Web 应用或者 API 运行时发现脆弱性问题。运行时扫描通常使用动态应用程序安全性测试 (DAST) 技术，模拟攻击并检测应用程序或 API 的漏洞。最终从如下工具候选集中，选出了 ZAP。

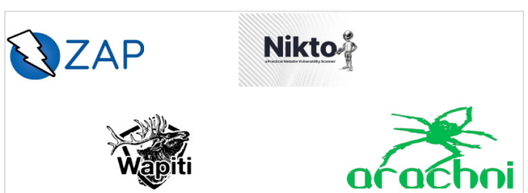


图 12 运行时扫描工具候选集

ZAP 可以检测 OWASP Top 10 风险，同时还包括 250 多个精选规则。同时 ZAP 也是 Github 排名前 1000 的项目之一，非常受欢迎，并拥有庞大的社区。如图 13 所示，即 ZAP 检测到了一个 XSS 漏洞，并给出了漏洞的描述、风险等级和可能的解决方案。此外，输出还包括有关漏洞的详细信息，如漏洞发现的位置、参数以及可以触发漏洞的参数值，这些信息可以帮助开发人员更好地理解和修复漏洞。最后，输出中还包括了参考链接，这些链接提供了有关漏洞的更多信息。

图 13 ZAP 扫描输出结果

公司通常都有相关工具和流程制度来进行代码审计、渗透测试，但是在开发的过程中也可以使用这些开源的安全工具进行自检，发现代码、依赖、配置、镜像里的各类安全问题，并及时进行修复。避免安全问题累积到较后阶段才暴露，提高项目的效率和整体安全性。

僵尸网络威胁态势观察

绿盟科技 抗拒绝服务产品部 果鹏

2023 年 4 月 24 日，网络安全行业年度盛会 RSA Conference 在旧金山隆重开幕。自 1995 年起，RSA Conference 每年都会围绕一个独特的主题展开交流和讨论。此次大会以 “Stronger Together” 为主题，议程主要包含安全研讨会、沙盒创新大赛、安全技术主题演讲等。大会主题切合当下不断升级、演变的网络威胁态势，各安全厂商只有携手共进、集思广益，才能够确保网络安全方案的多样化和有效性。值得一提的是，本次会议还引用了海伦 · 凯勒的一句名言对议题进行了升华—— “Alone we can do so little；together we can do so much.” 在针对 DDoS 攻击方向的研讨会中，诺基亚业务线的技术主管 Craig Labovitz 博士围绕近年来愈演愈烈的由企业僵尸网络造成的 DDoS 攻击展开了讨论。

如今，在云计算 、大数据、AI、在线直播等行业高速增长驱动下，DDoS 攻击态势也在不断变化和演进。在 2010 年到 2022 年这一区间，大多数 DDoS 攻击仍以围绕 IP 欺骗的技术手段为主，例如 NTP 放大攻击和 DNS 放大攻击等资源耗尽攻击。而自 2023 年起，这一 DDoS 攻击态势发生了根本性的变化，由企业僵尸网络生成的 DDoS 攻击比例超过了整体攻击比重的 50%，而该类型的攻击在 2021 年第二季度仅占整体比重的 10%，这一巨量增幅值得整个网络安全领域引起重视。

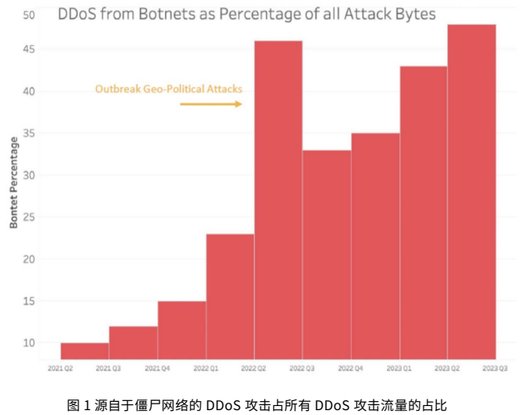


图 1 源自于僵尸网络的 DDoS 攻击占所有 DDoS 攻击流量的占比

而如今在企业、组织中大量应用的 IoT（物联网）设备正是造成这一变化的主要原因之一。根据市场洞察和战略商业情报提供商 IoT Analytics 的全球 IoT 市场预测，我们可以看到全球各种类型 IoT 设备的活跃数量正逐年递增。在各类组织、企业中，整合了 IoT 技术的摄像头、无线 AP（Access Point，即接入点）、HVAC 设备（Heating, Ventilation, and Air Conditioning，即采暖通风及空调系统）随处可见，大量部署的 IoT 设备为人们的生活和工作带来了诸多便利和可能，但一些潜在的风险也随之而来。

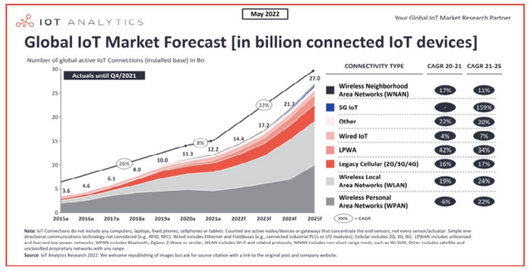


图 2 市场洞察和战略商业情报提供商 IoT Analytics 于 2023 年 5 月 24 日发布的全球 IOT 市场预测报告

截至 2022 年，由全球 IoT 设备构成的僵尸网络所带来的 DDoS 攻击其实并不算猛烈，这其实是由于 ISP（Internet Service Provider，网络服务供应商）对上行链路有着严格的限制，也正因如此，目前约 70% 的受控 IoT 设备实际上仅能产生不足 50Mbps 的 DDoS 攻击流量。

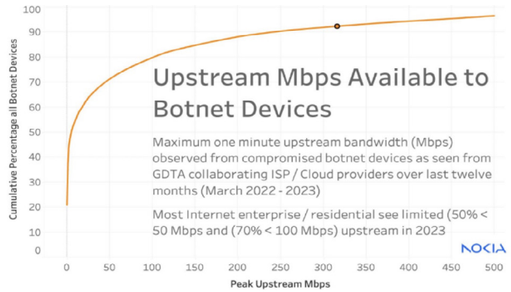


图 3 NOKIA 收集分析合作运营商 & 客户数据得出的僵尸网络上行流量趋势

图 4 运营商 Comcast 认为 GB 级别的上下行同步速率已成为可能

图 5 运营商 Verizon 已实现 1GBPS 的上行速率

但自 2023 年起，整个欧美地区的 ISP 行业竞争激烈，包括 Comcast、Verizon 在内的 ISP 厂商开始升级 1G 对称速率，也就是上行、下行链路均能实现 1Gbps 的速率。而这一网络升级的普及将对僵尸网络所产生的破坏力带来指数级的增长。

Craig Labovitz 博士针对僵尸网络进行了深入研究，通过分析诺基亚合作的 ISP、客户所共享的实时数据得到了一些值得分享的信息：

观测到的由 IoT 设备构成的僵尸网络的攻击峰值可以达到 1-2Tbps。

大多数僵尸网络的设备规模数量小于 5000 台，但仍有少数僵尸网络有着超过 60000 台的惊人规模。

从设备类型来看，CPE 设备（Customer Premise Equipment，即客户前置设备，包括但不限于电话机、无线路由器、防火墙、电脑、光猫、AP 等）的比重最多，约占 35%；摄像头类设备紧随其后，约占 30%；服务器类设备约占 20%；其他类型的设备均小于 10%。

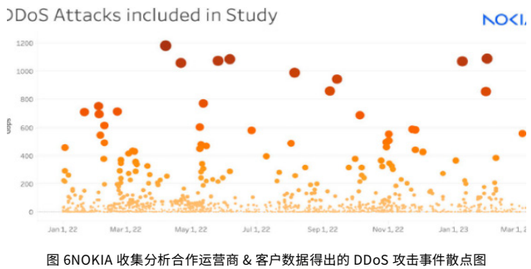


图 6NOKIA 收集分析合作运营商 & 客户数据得出的 DDoS 攻击事件散点图

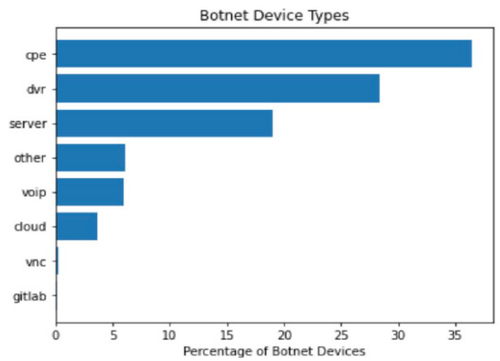


图 7 NOKIA 收集分析合作运营商 & 客户数据得出的僵尸网络中设备类型的占比图

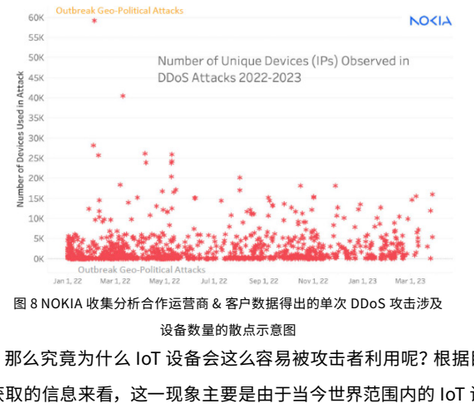


图 8 NOKIA 收集分析合作运营商 & 客户数据得出的单次 DDoS 攻击涉及设备数量的散点示意图

那么究竟为什么 IoT 设备会这么容易被攻击者利用呢？根据目前获取的信息来看，这一现象主要是由于当今世界范围内的 IoT 设备存在大量的管理缺陷。大多数已部署的 IoT 设备没有禁止向互联网开放管理权限，且管理员的密码复杂程度不够高，加之很多 IoT 设备部署后缺乏漏洞管理，没有或者无法及时更新官网补丁，而目前市面上传播的恶意软件又具备自我传播功能，这些原因最终导致 IoT 设备被 DDoS 攻击者大量滥用。

在实际操作上，物联网设备通常默默开启 telnet 远程登录功能，以便于运维人员进行远程管理。而攻击者可以利用这一问题，通过 IP 地址扫描来发现存活的物联网设备，然后进行端口扫描来判断该设备是否开启 telnet 服务。在这之后攻击者会尝试通过弱口令（如各厂商的出厂密码、admin/123456 等简单的用户名 / 密码组合）进行暴力破解，从而获得设备的绝对控制权。以图 9-10

为例，当攻击者发现物联网设备后，可以轻易地通过该设备的开放端口获取设备信息，然后通过各类搜索引擎轻易地获取该型号存在的漏洞问题以及漏洞代码，如果该设备没有及时更新补丁，则会轻易地被攻击者获取控制权限并加以利用，开展大规模的 DDoS 攻击，甚至衍生出黑色产业链，将 DDoS 攻击作为服务出售给不法分子，也就是臭名昭著的 DDoS as a service（DDoS 即服务）。而随着受控 IoT 设备僵尸网络的规模增长，发起 100Gbps 规模的 DDoS 攻击所需的成本也在骤降，由 2018 年的 1000 美元骤降至 2022 年的几十美元，这对于不法分子而言无疑是一场狂欢，而这一现象也为世界范围内的企业、组织带来了巨大的挑战。

Info	Refresh
Device ID	000000
Device Name	CVD-AF16S
Device Type	HY-DVR
Hardware Version	DM-245
Software Version	V7.1.0-20160603
IE Client Version	V2.0.0.277
IP Address	[redacted]
MAC Address	[redacted]
HDD Capacity	931G
Video Format	NTSC
Client Port	9000
HTTP Port	80
P2P ID	RSV1611018078580

图 9 攻击者通过 IoT 设备的开放端口获取设备硬件信息的示例图

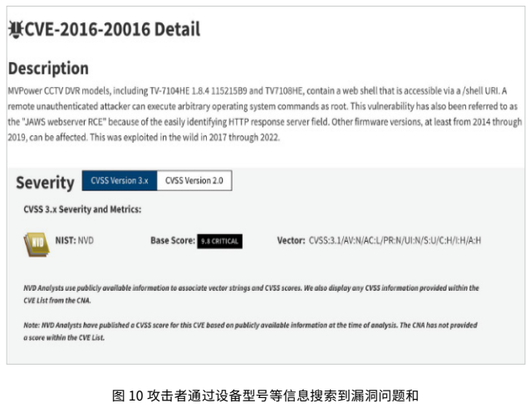


图 10 攻击者通过设备型号等信息搜索到漏洞问题和漏洞代码的示例

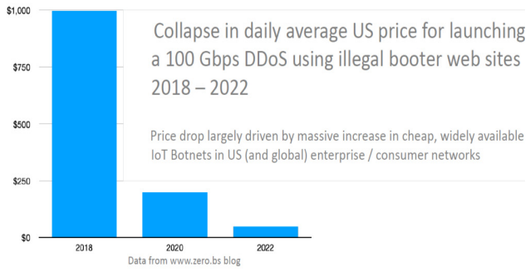


图 11 2018-2022 年通过非法网站发动 100Gbps 规模 DDoS 攻击的成本变化

混合式办公中的十大隐私挑战

绿盟科技 创新研究院 顾奇

2023 年的 RSA 大会上，来自 BH 咨询的首席运营官 Valerie Lyons 博士分享了议题“混合式办公中的十大隐私挑战”。该议题对混合式办公中的主要安全挑战与相应的解决方案进行了阐述，本文将梳理议题中所提及的各类挑战与方案。

1. 背景

在疫情等全球性事件的影响下，混合式办公日益普遍。所谓混合式办公（如图 1 所示），指的是除了传统的集体线下办公外，员工还采用多种工作模式，如线下优先、固定线上线下、灵活线上线下、完全线上等。据麦肯锡报告，只有 4% 的企业高管表示他们完全没有考虑推行混合式办公，然而也只有 11% 的高管承认他们已经开始实施混合办公模式。这表明，混合式办公的推广面临一系列挑战。RSAC 2023 议题 *Ten Key Privacy Challenges of the Hybrid Workforce* 对混合式办公中与个人隐私、企业数据安全等相关的十大挑战及解决方案进行了梳理。

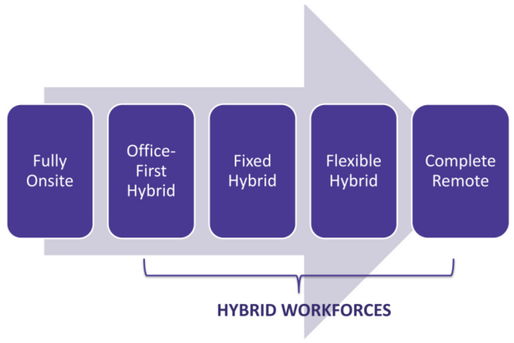


图 1 何谓混合式办公

2. 十大挑战与解决方案

挑战 1：技能集

在混合办公模式中，工作者需要兼顾其个人隐私、企业数据安全以及业务连续性。然而，根据对各企业的调查发现，实现这一目标的五大挑战包括：提高网络安全（35%）、良好的合作（29%）、拥有适当的技能（29%）、积极的工作氛围（28%）以及员工的数字化水平（26%）。这些挑战凸显了混合办公模式的复杂性，以及在实施过程中需要克服的困难。

解决方案

与首席信息安全官(CISO) 和业务连续性管理(BCM) 早期合作：在项目的早期阶段就与信息安全和业务连续性管理的专家合作，可以确保隐私和安全的问题得到充分考虑。

获取相关的专业认证，并参与专业协会：员工可以通过获取注册信息系统安全专业人员（CISSP）或注册信息安全管理师（CISM）等认证，以及参与信息系统安全协会（ISSA）、国际信息系统安全认证联盟（ISC2）、信息系统审计与控制协会（ISACA）等专业协会，来提高他们在信息安全和隐私保护方面的知识和技能。

遵循国际认可的标准和框架：遵循 NIST 网络安全、NIST 隐私框架、ISO27001/ISO27701 等国际认可的标准和框架，可以帮助企业提高他们的信息安全和隐私保护能力。

实施内部培训和技能提升计划：通过实施内部培训和技能提升计划，可以帮助员工提高他们在信息安全和隐私保护方面的知识和技能。

挑战 2&3：非工作环境

在混合办公模式中，非工作环境是一个重要的安全挑战。由于在企业外部传输或处理个人数据，绕过了基于策略的安全处理规则；同时在企业外部讨论敏感或机密的工作内容，这些本身就可能构成对企业的安全威胁。

解决方案

企业需要定期更新其安全和隐私政策，并确保所有员工都了解并遵守这些政策。此外，对于违反政策的行为，企业可以设定相应的处罚措施，以强化政策的执行力。

通过实施数据防泄露（DLP）和电子邮件监控 / 数据过滤技术，企业可以更有效地保护在非工作环境中传输或处理的个人数据。

在进行员工监控时，企业需要考虑进行数据保护影响评估（DPIA）和更新处理活动记录（ROPA），这些措施可以帮助企业更好地理解和管理数据处理活动的风险。

企业需要考虑如何有效地响应主体访问请求（SARs），以确保个人数据的透明度和可访问性。

挑战 4：移动式设备

由于不在集体线下环境，那么所有用于办公的设备都可看作是一种移动设备。这就需要企业的管理者清楚以下情况：

（1）企业管理的设备数量；

（2）这些设备上运行的应用程序；

（3）终端设备的可访问性以及它们传输数据的能力；

（4）是否能够远程擦除设备；

（5）对于分类信息的处理规则，是否符合企业的合规要求。

解决方案

修订移动设备策略：更新策略以反映混合工作的特点。这可能包括对设备使用、数据存储和传输以及远程访问等方面的规定。

实施或优化设备管理系统：如果还没有，那么应该实施以下的一种或多种设备管理系统：移动设备管理（MDM）、企业移动管理（EMM）、统一端点管理（UEM）。如果已经有了，那么应该进行检查和优化，确保它们能够有效地支持混合工作模式。

在所有的 SaaS 和云应用上实施多因子认证（MFA）：多因子认证是一种安全措施，要求用户提供两种或更多种证明身份的方式，可以大大提高账户的安全性。

挑战 5：新员工

在混合办公模式中，新员工的隐私问题是一个重要的挑战。不同文化背景的员工对个人数据收集的接受程度可能会有所不同。此外，员工的隐私关注点可能会反映他们的政治观点。

解决方案

考虑不同的隐私法案是否适用于这些新员工：例如，欧盟的通用数据保护条例（GDPR）、加利福尼亚的消费者隐私法案（CCPA）和加利福尼亚的消费者隐私权法案（CPRA）等。

是否需要进行转移影响评估(TIAs) 或数据保护影响评估(DPIAs)：这些评估可以帮助企业更好地理解和管理数据处理活动的风险。

通过长期培训来统一隐私文化：定期的隐私培训可以帮助新员工理解和接受企业的隐私政策和实践。

需要高度私密 / 机密的企业，在候选人评估 / 员工调查的环节中将个人计算机（PC）规模列为考虑项。

挑战 6：电话录音

混合办公模式下，电话录音成为一大难题。据统计，语音交流占据了客户对话的 80%，但仅有不足 10% 被有效记录。对于金融机构，半数的客户对话发生在专门的呼叫中心之外。预计到 2025 年，将有 75% 的客户对话会被录音。

解决方案

理解并弥补员工和客户的电话录音需求差异：对需求进行深度分析，定位问题所在。

根据需要进行数据保护影响评估（DPIAs）和更新处理活动记录(ROPAs)：这些步骤有助于企业更好地管理电话录音活动的风险。

优化录音机制：针对不同类型的通信，如内部、外部、来电和去电，制定合理的记录策略；规范处理主体访问请求（SARs）的流程；梳理与在线协作工具的配合方式；并且，考虑移动电话与应用（如 WhatsApp，Snapchat 等）的录音需求与处理方法。

挑战 7：VPN

在混合办公模式中，虚拟专用网络（VPN）是一个重要的挑战。据 HP 2021 年的报告《2022 年及以后的混合工作场所的安全》显示，41% 的人依赖 VPN 技术，但他们关心的不仅仅是安全和隐私，75% 的人抱怨 VPN 的性能慢或者连接断开，影响了他们的工作效率。

解决方案

考虑零信任和远程桌面技术：零信任是一种安全模型，它假设内部网络和外部网络一样不可信，所有的网络请求都需要验证和授权。远程桌面技术则允许用户远程访问和控制另一台计算机（根据 HP 的报告，大多数受访者不打算以 VPN 作为主要身份验证方法，而是倾向于使用云和本地身份服务。大部分受访者计划实施零信任架构）。

挑战 8：监管问题

混合办公模式下，如何进行有效监控 / 监管是一大挑战。如果不通过 VPN 进行路由，那么如何进行监控？监控的合法依据是什么？合法的监控范围有多大？如何处理监控同意的复杂性？

解决方案

采用基于云的电子邮件（并使用多因素认证）：基于云的电子邮件既提供安全性也方便使用，多因素认证能进一步提高账户的安全性。

遵守 GDPR/CCPA/CPRA 等法规：需要确保员工知晓哪些个人身份信息（PII）被收集、处理、披露以及为什么。

根据需要进行数据保护影响评估（DPIA）：DPIA 能帮助企业更好地理解和管理数据处理活动的风险。

挑战 9：挑战过多

在混合办公模式中，挑战的多样性和复杂性本身就是一个重要的挑战。不同的问题可能会叠加在一起，产生新的、意想不到的困难。

解决方案

重组隐私和网络安全团队：例如，可以将这些团队重组为“数字风险保护部门”，以更好地应对混合办公模式中的各种挑战。

使用虚拟 / 外包服务：这可以帮助企业更有效地利用资源，应对各种挑战。

进行优先级排序：可以制作时间管理矩阵（按照是否紧急与是否重要划分，见图 2），帮助企业更好地管理时间和资源，以应对最重要的挑战。

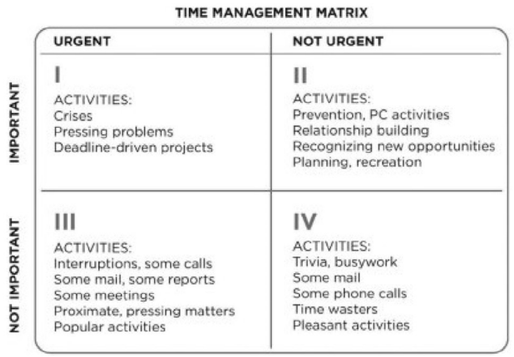


图 2 时间管理矩阵

挑战 10：隐私作为环境的一部分

在混合办公模式中，一个趋势是隐私正在被视为环境、社会、治理（ESG）议程的一部分。这是一个有趣的观察，因为我们通常会将隐私视为社会(S) 和治理(G) 议程的一部分（人权、数据保护法等），但如何更多地将隐私囊括在环境（E）议程中仍是一个待研究的问题。

解决方案

对于这个挑战，可以参考新的欧盟企业可持续性报告指令（Corporate Sustainability Reporting Directive，CSRD）。这个新的指令将于 2024 年 1 月开始实施，要求所有在欧盟内的大企业或在欧盟有重大活动的企业，以及营业额超过 1.5 亿欧元的企业，必须在其年度报告中包含关于其在 ESG 方面的表现和影响的信息；相应企业需要更加重视其数据处理和隐私保护的政策和实践，因为这些信息将被公开，并受到投资者、消费者和公众的关注。

3. 总结

本篇 RSAC 议题详细探讨了混合办公模式下的关键安全风险和挑战，这些挑战不仅仅存在于国外，国内的混合办公环境同样面临着这些问题。在可预见的短期内，我们需要依赖各种现有的安全技术，如数据防泄露、虚拟专用网络等，以减少无意中的信息泄露。然而，从长远来看，我们需要构建一个完整的隐私保护框架，从政策制定、技术应用到员工教育等多个方面提供全面的支持。我们坚信，在不久的将来，我们可以在享受混合办公模式带来的便利的同时，确保企业数据的安全以及个人隐私的保护。

静默对抗中的内幕风险及其治理模型

绿盟科技 总体技术部 张睿

摘要：以资产为核心的威胁发现在数据泄露事件不断、员工泄愤报复频发的背景下变得捉襟见肘，而对于只关注恶意员工与恶意行为的传统内部威胁管理模式，也无法应对当前诸如非恶意误操作高发、离职员工转移数据的新型风险场景。内幕风险管理的理念应运而生，其包容评价了不同主观意识状态下员工的行为风险，整合了管理流程，并通过持续安全意识教育保证闭环，引导并修正人员的行为，提出了围绕自然人主体威胁发现与风险管理更加普适的模型。

关键词：内幕风险 内部威胁 风险治理 主观罪过

根据 Forrester 于 2021 年 12 月发布的内幕风险报告以及 2022 年 RSA 大会公布的相关数据，59% 的组织关注外部威胁大于内部威胁，58% 的组织没有专门针对内部风险管理的团队，39% 的组织相关预算匮乏且 38% 的组织缺乏相关内部威胁管理的技术能力。与此同时，70% 的企业组织完全没有应对内幕风险的管理策略，而且 29% 的组织根本不认为内部人员威胁更大，可是现实是过去 12 个月内 59% 的安全事件均由企业内部人员引发。

安全已经不再像早年的网络安全充满了激烈的形式化攻击对抗，当前企业组织网络与数据安全防护的态势趋于静默环境下的资源和信息争夺的实质性对抗，其核心在于既定安全预算下如何保持合理的风险敞口以获得管理效率，既不能置安全于不顾，但又不能过度防护。当前很多企业的安全团队对组织的综合风险，尤其是全体内部员工的风险依然缺乏准确的把握，甚至很低的认知。组织内人力资源、法务、公共关系团队也往往无法从总体安全的角度把握员工在职期间、离职后的连续合规性，在数据泄露事件频发、员工泄愤报复事件不断的背景下，传统依赖围绕信息资产防护的思路，俨然难以应对围绕员工行为的各类风险。基于风险管理进行的安全活动，持续性监控、分析、处置相关风险，其综合了资产与安全，以保护相关业务与资产的价值处于受控状态。

而内幕风险管理正是在风险管理框架内，纳入安全领域涉及的威胁监测、漏洞发现、基线维护、应急响应，从内部人员这一关键角色出发，在包容传统资产威胁管理的基础上，将技术和管理于内幕风险的场景下进行了深度融合，其进一步整合了人力资源管理、公共关系管理、安全意识培训等要素，闭合了风险管理流程，解决了资源与风险错配的问题，以提升安全管理效率。

1. 内幕风险的定义

传统的内部威胁监控的思维是以资产为中心，通过叠加安全技术，不断搜集数据，进而分析安全问题。其客体上关注软、硬件以及应用等资产的脆弱性、异常参数，主体上聚焦发现特定的恶意人员及其恶意行为。在内部威胁方面，其关键功能在于发现我们经常提到的“内鬼”，即具有内部权限和优势信息，但尝试非法利用的合法员工。

而内幕风险管理的思维是以人为中心，在传统威胁监控的基础上，纳入监察的能力，通过融合安全技术与人员行为，关联人的背后动机，进而进行全体员工的行为分析和风险发现。所以其不但会分析发现主观恶意的人员，还会分析主观无恶意但是客观已攻陷，以及主观缺乏安全意识但客观误操作诱发风险的人员。从员工主体上，内幕风险拓展了对员工主观意识的分析和管理范围，综合合理地考虑了最广泛的合法员工的不安全、违规行为。而从逻辑上，正如 Gartner 和 Forrester 对内幕风险与内部威胁的定义一样，并非所有的内幕风险最终都会演变成内部威胁，但是所有的内部威胁绝对源于内幕风险，两者的对比如图 1 所示。

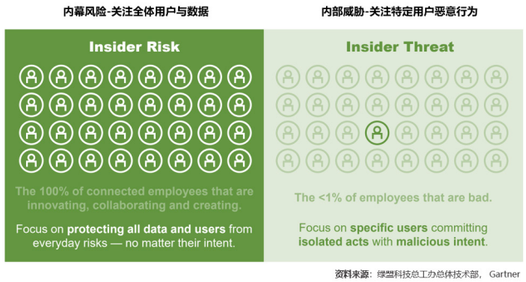


图 1 内幕风险与内部威胁对比

2. 内幕风险动机与威胁分类

Gartner 以及 Forrester 两家机构针对内幕风险的威胁源，以用户为基准参数，整体划分成粗心用户、恶意用户以及失陷用户三类。相关用户类型以及用户动机如图 2 所示。其中失陷用户是指在其主观未知的情况下，账户被窃权、控制，从而被攻击者利用，其定义与拒绝服务攻击（DOS 攻击）中的 Bot 即“肉鸡”较为类似，但不同之处是纳入用户作为“自然人”的主观因素，而超越 Bot 一般只针对受控终端的客观“物”的范围。值得注意的是，根据 Gartner 的数据，粗心用户因为缺乏安全意识以及偶然的误操作带来的安全事件概率高达 61%，远高于我们一般关注的外部攻击的失陷用户风险发生概率 14%，这也成为内幕风险管理必要性的关键，也是区分内幕风险与内部威胁的基础。

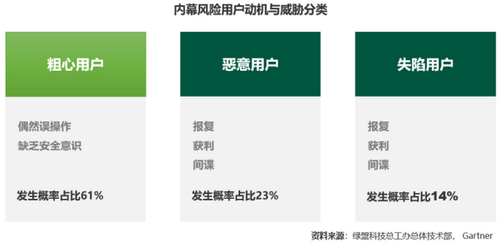


图 2 内幕风险用户动机与威胁分类

我们若单独以离职员工为例，其离职前可能带来的威胁包括数据破坏、泄露、越权复制和使用，甚至于系统植入逻辑炸弹，在离职后于条件满足时触发，其主观既可以基于恶意，也可能源于公司缺乏明确管理制度下的思维惯性。传统的内部威胁管理并不关注后者，尤其是针对数据复制的场景，很多员工主观虽然无恶意，但习惯性离职前拷贝既有数据，用以支持自己到新公司履职后工作

开展。匹配至员工角色，销售人员可能带走详细的公司客户名单以及合同，而软件开发人员会大批量复制代码和产品信息。所以公司应当明确管理规定，而且需要以可以明确获知、理解的方式事先约定相关行为的授权范围、合规性等问题。

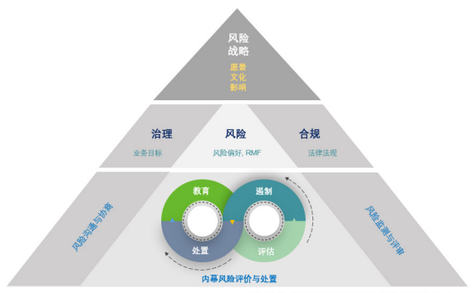
此外，传统的内部威胁管理更不跟踪员工离职后的行为，但是公司于此处存在两类非常高发的风险，一类为离职员工权限未及时全面解除，该离职员工还可以访问部分系统、数据，进行违规操作；另一类为员工故意规避保密、竞业履约责任，引发公司商业秘密泄露或技术竞争力与先进性，从而造成损失。后一类风险往往依赖公司人力资源管理和法务团队，但很多公司组织对于离职员工的履约行为跟踪能力和资源配备有限，更缺乏与安全部门技术团队的密切合作，成为内幕风险爆发的高危节点。

3. 内幕风险治理框架

在定义内幕风险的基础上，Gartner 于内幕风险管理方面提出了 C.A.R.E 模型，即 Contain（遏制）、Access（评估）、Resolve（处置）、Educate（教育）四步。

其中在遏制阶段，需要实现用户、设备、网络实体高危行为的监测，并于相关行为出现时，触发安全策略，可以通过限制准入、限制网络、禁用 USB 接口、锁定设备、停止应用与数据同步的方式防止过度风险暴露；在评估阶段，持续监测评估，关注数据泄露事件的指征，于此环节完成行为分析、风险评估、既往分析、基线建立；在处置阶段，启动数据泄露事件进行响应，并解决问题，实际涉及违规用户的关键必要操作，管理层和人类资源管理部门、法务部门的事件升级流程；而在教育环节，主要落实并培养员工安全意识，降低未来的暴露风险，所以实际工作包括指定用户定制化培训、政策与协议下发确认流程。内幕风险管理框架下的安全意识培训具有及时性和针对性，异于传统的安全意识培训，因为内幕风险管理基于人的行为，目的在于修正人的行为。

绿盟科技在 C.A.R.E 的基础上，纳入了 ISO 31000 风险管理框架，融合了风险监测于评审、风险沟通与协商的流程，保证风险管理流程的闭环。而鉴于内幕风险管理关注组织核心价值，既囊括了传统资产为核心的理念，也纳入了“人”的新的要素，所以在风险管理的基础上，我们进一步融合 GRC 框架，联合治理、合规要素，在考虑企业组织风险顶层战略要求下，关联组织愿景、文化、影响的要素，形成内幕风险治理框架，如图 3 所示。

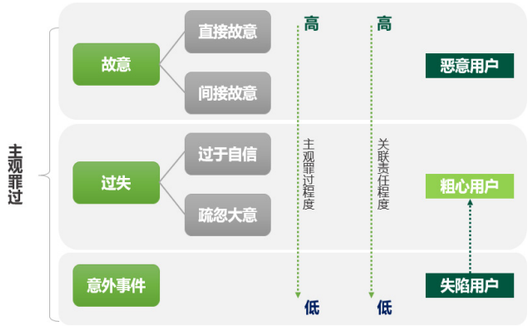


资料来源：绿盟科技总工办总体技术部，OECD，Gartner

图 3 内幕风险治理框架

此外，企业组织于内幕风险管理落地的过程中，鉴于员工主观的恶意与否，既会于技术层面影响实际用户画像的逻辑和效果呈现，又会于后续风险处置层面影响责任划分，所以为了保持公司组织对外举证司法流程衔接的效率，我们进一步将本文第二章节中涉及的粗心用户、恶意用户、失陷用户进行了主观罪过和关联责任的映射，以弥补 Gartner 在此方面的分析不足，如图 4 所示。其中，直接故意的主观罪过程度最高，而意外事件往往不涉及主观恶意。对应在经过客观方面评价后，确定承担责任或满足客观有罪要件的情况下，在主观罪过的评价过程中，主观罪过越高，对应的责任承担也会越高，而往往其企业组织要求证明相关员工的责任也会越重。

图 4 中，直接故意是指明知自己的行为会造成危害结果，仍积极采取行动，希望和追求该危害结果的发生的心理状态，如直接攻击、植入逻辑炸弹；间接故意是指明知自己的行为可能会造成危害结果，但放任结果的发生，有可能涉及不作为状态，如明知自己的账户口令被盗用，但离职不报任由情况恶化。粗心用户的责任介于中间，主要源于其职责潜在包含了保护、通报等义务，虽然其外在形式上往往较恶意用户的行为更不具有攻击特性，但并不意味着行为结果影响小，而且往往会被惩罚。此外，在责任层面，需要注意失陷用户有转化为粗心用户的通路，其主要源于该用户的工作职责涉及对应资产、数据的保护义务，虽然其在未知情况下被利用或被攻击，并不必然免责。



资料来源：绿盟科技总工办总体技术部

图 4 主观罪过与用户分类映射

4. 内幕风险检测处置与跨组织联动

根据内幕风险监测主体的特性，技术方面需要建立对员工行为的数据搜集和分析能力，完成风险分析并关联后续联动处置，相关内容如图 5 所示。依据数据流转结构，在靠近用户侧能够收集用户数据、建立行为基线，并不断训练形成行为风险模型。在此基础上，于中间层关联用户的行为，实现各类风险、威胁的元数据库匹配，全面分析本地、云端各类资产与此员工行为的风险关系。在风险管理的框架下，对于超越安全基线和阈值的行为进行告警，联动 SOAR（安全编排自动化响应）进行阻断，防止风险蔓延的事件影响扩大。

图 5 内幕风险检测处置流程

同样以离职员工为例，为保持内幕风险管理的有效性，除常规解除各类权限操作外，员工离职流程发起后，组织需要启动回溯离职前一段时间（数周或数月）内指定员工行为的审计流程，通过UEBA（用户和实体行为分析）关联身份、权限、操作，发现越权操作、数据外发、非公司业务必要的大规模拷贝、“蚂蚁搬家”式分批次全库复制等违规和异常行为。组织同时应该在员工离职后至少几周内继续监控其活动，在不侵犯离职员工隐私的情况下维持有效的风险管理，建立取证审计追踪的管理流程，并在合适的情况下，引入专业外部第三方资源，落实回溯审计的职能。

图 6 内幕风险管理联动

内幕风险管理除在技术层面建立完善的闭环检测响应系统外，在管理层面也需要设立职责分离、最小权限等流程，并在技术与管理结合的基础上，进一步纳入电子取证、证据链保全、法务支持等相关职能，确保有效地联动处置内幕风险引发的安全事件，如图 6 所示。

依然以离职员工为例，离职过程中，人力资源管理部门应尽力倡导维持透明、互信的沟通，离职面谈确保清晰沟通的同时评估员工的态度，降低因为分歧引发的不满甚至报复的概率。与此同时，员工离职后，需要持续针对员工履约行为进行监控，一般包括保密与竞业协议履约行为的跟踪，在合法取证的基础上，维护相关证据的完整性。所以一般依赖法务团队，或是选择专业外包团队，对于离职员工违约行为能够采取及时的沟通、警告，甚至发起司法救济流程，以维护企业自身合法权益。而针对可能引发仲裁、诉讼的员工，维持有效的公共关系和监管机构信息交换和互通，防止因为诸如“员工爆料”“实名举报”类似的负面事件或是不实信息等影响公司对外形象，造成股价、商誉的贬损。

参考文献

[1] Paul Furtado, A New Look at Insider Risk, Gartner,2022.

[2] Paul Furtado, Protection From the Risk Within—Managing Insider Risk, Gartner,2022.

[3] Randy Trzeciak Stop Chasing Insider Threats Start Managing Insider Risk, RSA Conference,2022.

5G+医疗的安全风险与防护方向

绿盟科技 运营商售前技术部 覃达键 陈鸣昊

摘要：5G 作为新一代移动通信技术标准，不仅是实现万物互联的关键信息网络技术基础，也是经济社会数字化转型的重要驱动力量。5G 移动通信技术在造福社会、造福人民的同时，也对网络安全提出了更高要求，并面临诸多挑战。

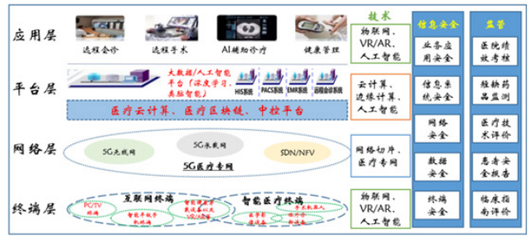
关键词：5G 医疗应用 网络安全 敏感信息

1. 概述

当前，第五代移动通信（5G）已成为全球热点，随着 5G 网络规模化商用以及迅速发展，5G 技术的大带宽 eMBB、低时延、高可靠 URLLC、大连接 mMTC 几大技术特点，将引领垂直行业新一轮的信息通信技术设施升级。

以医疗行业为例，5G 技术不断探索为智慧医疗的应用奠定了坚实基础。在第二届“一带一路”国际合作高峰论坛“共建 21 世纪数字丝绸之路”数字丝绸之路分论坛上，中国工程院院士邬贺铨表示，到 2035 年 5G 将增加全球产出 4.6%，即 12.3 万亿美元，其中为全球医疗领域提供超过 1 万亿美元的产品和服务。“以 5G 技术为基础的数字医疗将改进对医务人员的教学、培训、实习，提升医生的诊治水平，提供及时的远程救治指导，降低医疗成本和患者的负担，对实现医疗基本服务均等化有重要意义。”

本文从以 5G 技术为基础的数字医疗的场景出发，观察 5G 医疗应用市场，剖析真实痛点，共同寻找 5G、医疗、网络信息安全三方的结合点。



2. 市场调查

数字化时代，信息繁复、类型多样，带给人们方便的同时也带来了个人健康数据安全与隐私问题，智慧医疗可以通过相关技术手段，如医疗专网、智能标识解析体系和物联网等技术来提高效率，同时提升医院竞争力和诊治能力，但 5G 智慧医疗健康领域融合应用作为新兴事物，参与主体多、涉及领域广、安全风险高，在发展过程中也会遇到一些新情况、新问题。

一方面，缺乏统一的标准与评价体系。无线医疗和远程医疗应用场景众多，不同应用场景对于网络的需求差别较大，未建立完善的 5G 智慧医疗健康标准体系；5G 智慧医疗健康在创新型医疗器

械、终端设备接入方式、数据格式统一和应用数据传输等方面还存在许多规范问题需要结合医疗健康行业应用特点，推动面向医疗行业的 5G 标准体系的制定、实施和应用。

另一方面，在 CT 与 IT 的融合时代，数据的开放、流动和共享使得企业数据面临着前所未有的挑战，数据的保护难度也在增大。同时个性化定制、服务化转型涉及大量的用户信息使得用户隐私泄露风险也在不断增加。随着多接入边缘计算的大量部署，数据安全和隐私保护将被摆在更显眼的位置。

3. 痛点剖析

5G 时代的医疗行业应用，必须能够提供不低于传统专网的安全性与可靠性，才能够胜任高价值资产的承载，需要充分考虑 5G 网络以及围绕 5G 的医疗应用创新所带来的新技术与新能力的安全风险。在此情况下，需要有 5G 安全产品、5G 安全端到端解决方案、5G 安全服务等多种解决方案才能够满足一线市场的需求。

网络发展过程中将不可避免地出现安全问题，我国建立了一套完备的网络安全标准—— “等级保护 2.0”。但是，5G 环境下网络安全等级保护对象与传统信息系统相比差异显著，现有的网络安全等级保护并不能完全覆盖 5G 的方方面面。相比 4G、3G 网络，5G 采用的新空口技术、开放的服务能力给 5G 网络带来了诸多新的安全风险。5G 赋能垂直行业应用，导致 5G 网络环境下网络安全保护对象的安全职责划分界定难度增大。在原有的安全防护策略中，安全区域的设置是根据等级保护的对象划分的，但在 5G 网络环境下，网络物理资源可以通过 SDN 和 NFV 等技术实现资源虚拟化与切片化按需定制，不同的用户按照逻辑边界来共享和使用网络资源，导致传统的基于物理资源边界划分的方法不再适用。例如，5G 赋能智慧医疗主要通过网络切片技术建立端到端逻辑专网，在患者和医院、医院和医院之间搭建满足远程医疗等多种定制化网络服务的宽带低时延通信网络。然而，一旦 5G 网络遭受恶意攻击，医疗专网、医疗设备数据的传输质量和服务质量、医患敏感信息安全的保密都会受到不同程度的损害，甚至危及患者生命安全。

同时，随着《数据安全法》《个人信息保护法》以及《国家健康医疗大数据标准、安全和服务管理办法（试行）》等法律法规陆续出台，从多个视角对医疗卫生行业的数据处理和安全保护进行了规定。随着各类健康医疗数据采集变得更加立体，获取数据的渠道也越来越多，由单一的录入转变为群聚式收集。5G+ 互联网医疗应用数字化过程中产生的数据更全面、完整、精细，同时也意味着行业整体数据安全和个人信息保护面临着更大的威胁。

从数据的角度出发，医疗数据具有极强的隐私性，一旦泄露会对患者生活、工作带来负面影响。同时，大量医疗数据开始提供第三方开发测试使用，也容易造成个人隐私数据泄露。

另一方面，医疗行业的数字化不仅对数据的安全感知、安全存储、安全传输、安全处理等提出更大挑战，还对数据治理、服务平台、应用平台等带来新的安全需求。医疗行业关系国计民生，医疗数据一旦遭到篡改、破坏和泄露，势必会对医疗机构的声誉、医患双方的隐私及健康安全构成严重威胁，甚至影响社会的和谐稳定。

4. 未来方向

如何做到医疗数据的安全

国家针对数据安全已经出台了多项法规，如何有效防护医疗数据的安全和 5G 用户的个人信息安全，如何对鉴别信息数据、重要个人信息、数字衍生数据、重要业务数据做到针对性的监控与保护，使用户隐私数据在泄露前及时做出响应，避免因数据丢失造成的危害与损失，是网络信息安全行业未来需要考虑的实际问题。

如何让公众更信赖 5G+ 医疗

自新冠肺炎疫情发生以来，特殊时期的医疗需求让互联网医疗成为大众的 “应急选择”，很多消费者开始接触互联网医疗。在此背景下，如何在后疫情时代持续稳固大众的互联网医疗意识，建立大众对互联网医疗的信心并形成良好的消费互信关系是未来 5G 和医疗行业应用所需要考虑的重点问题。

5. 总结

本文结合 5G 移动通信技术特点与医疗行业属性，剖析了 5G 网络新环境下的网络安全防护的新痛点与未来工作构想，并提炼出 5G 环境下网络信息安全面临的安全问题与核心挑战。最后，提出了 5G 环境下网络信息安全的新思路与未来工作构想。

参考文献

[1] 沈昌祥，张焕国，冯登国，曹珍富，黄继武 . 信息安全综述 [J]. 中国科学：E 辑 ,2007,37(2):129-150.

[2] 张旭刚，谢宗晓 . 网络安全等级保护机器相关标准介绍 [J]. 中国质量与标准导报，2019(09)：12-15.

[3] 袁静，任卫红，赵泰 . 浅析 5G 环境下的网络安全等级保护工作思路 [C]. 公安部第三研究所 . 中国网 络安全等级保护和关键信息基础设施保护大会论文集 ,2019：4.

[4] IMT-2020（5G）推进组 . 5G 技术白皮书 [J]. 中国无线电，2015（05）：6.

[5] 王莉，王玥，田燕军 . 5G 移动通信网络关键技术的相关研究 [J]. 信息记录材料，2020，21（09）：191-192.

云原生API安全：背景、态势与风险防护

绿盟科技 创新研究院 浦明

摘要：全方位解读云原生 API 安全：安全态势、具体风险和防护思路大揭秘

关键词：API 安全 云原生安全

1. 概述

云原生技术的迅猛发展已经在全球各行各业产生积极的应用实践。根据 Gartner 在 2019 年的容器报告中预测，在 2020 年将有 50% 的传统老旧应用被云原生化改造，到 2022 年，全球 75% 的企业将会使用云原生的容器化应用。然而，由于应用架构的变革，在遵循面向微服务化的设计方式的前提下，功能组件化、服务 API 数量的激增，以及配置的复杂性等问题也随之而来。这些架构变化导致了传统 Web 请求 / 响应的服务交互模式向 API 请求 / 响应的服务交互模式的转变，如 RESTful/HTTP、gRPC、GraphQL 等。因此，在未来的云原生环境中，API 将作为主要的服务交互载体被大规模企业用户使用。

另一方面，从近年的安全事件来看，API 安全问题呈现上升的态势，严重威胁了用户的隐私和数据安全。一些典型的安全事件包括：2019 年 11 月，国外安全人员发现超过 2.67 亿条 Facebook ID、电话号码和姓名等信息被存储在某公开数据库中。相关研究显示，该数据库通过某未知 API 接口抓取，而非来自公开信息。2020 年 4 月，视频会议服务厂商 Zoom 被爆出多项安全漏洞，其中包括 Facebook Graph API 滥用导致隐私数据泄露问题。2021 年 4 月，Facebook 5 亿用户数据泄露，据暗网上公布的数据截图，涉及用户昵称、邮箱、电话等信息。2021 年 6 月，国外社交网络服务网站 LinkedIn 爆发大规模数据泄露事件，近 7 亿用户信息在暗网上被售卖，据相关研究人员证实，攻击者最终是利用 LinkedIn 的某一 API 获取到用户的敏感数据。据永安在线报道，2021 年 12 月，国内某证券公司的客户信息，包括用户姓名、手机号等敏感数据以每日 1 万条的量级在数据交易平台被售卖，经验证分析，证实为内部系统数据 API 管控疏忽导致。2022 年 4 月，WordPress 插件 Rank Math 爆出严重的 API 安全漏洞，借此漏洞可以直接修改用户数据库表信息。

根据云安全联盟（CSA）发布的云原生技术标准模型 [2]（如图 1 所示），我们可以看出横轴是开发运营安全的维度，涉及需求设计、开发、运营阶段，细分为需求、设计、编码、测试、集成、交付、防护、检测和响应阶段。纵轴则按照云原生系统和技术的层次进行划分，包括容器基础设施安全、容器编排平台安全、微服务安全、服务网格安全、无服务器计算安全五个部分。安全机制（蓝色标注部分）基本上覆盖了全生命周期的云原生安全要求。

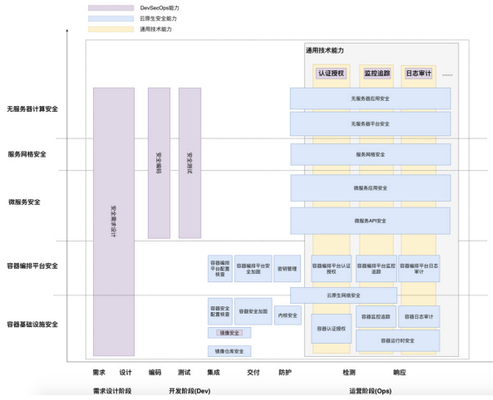


图 1 云安全联盟（CSA）发布的云原生技术标准模型

根据图 1 以及笔者的观察，容器安全产品在国内市场中，容器基础设施安全和容器编排平台安全的方案成熟度比较高，也得到广泛的应用和验证。而微服务安全、服务网格安全以及无服务器安全领域的成熟度则相对较低，这也是正常的，技术总是需要经历萌芽期、试探期、成熟期、衰败期等整个过程的。

未来，微服务间必然会使用大量 API 进行交互，这些 API 可能产生于 FaaS 函数、容器应用、Pod 等载体中。相应地，云原生 API 安全风险将随着云原生环境的进一步发展而不断增加，因此 API 安全的需求也将逐渐增多。在这种背景下，API 安全对于保护整个云原生环境的安全性至关重要，将成为云原生安全的下一个重要阶段。

本文将围绕云原生 API 所面临的安全风险以及相应的防护思路进行探讨，并介绍绿盟在云原生 API 安全防护上的一些思考与技术方案。希望这些内容能为各位读者带来一些启发与思考。

2. 云原生 API 安全风险

笔者认为云原生 API 安全风险应当从缺乏可见性、应用架构变化、东西向流量难以防护这几个方面去考虑。

2.1 缺乏可见性导致的风险

云原生环境中，由于微服务数量增多，每个微服务包含多个 API，因此微服务之间的 API 调用变得更加复杂。这种情况下，整个 API 系统的可见性变得缺乏，这可能导致以下几个问题：

首先，API 资产存在不可见性。当 API 资产受到黑客攻击时，很难及时定位入侵位置，从而错过最佳处理时间，增加安全风险。

其次，API 异常行为也缺乏可见性。例如，高频访问某 API 或利用 API 的未授权访问漏洞进行大量数据下载等异常行为，这些行为可能导致接口不稳定或敏感数据泄露的风险。

最后，随着微服务应用架构的普及，东西向流量交互增多导致 API 数量激增，API 权限管理变得更为复杂，由 API 调用链组合导致的权限绕过问题成为 API 业务安全的防护难题。

2.2 应用架构变化导致的风险

我们知道，新应用架构遵循微服务化的设计模式，通过应用的微服务化，我们能够构建容错性好、易于管理的松耦合系统。

与此同时，新应用架构的出现也会引入新的风险，本文笔者从数据泄露风险、未授权访问风险、被拒绝服务风险三方面进行介绍 [1]。

2.2.1 数据泄露风险

当单体应用被拆分为若干个服务后，这些服务会根据业务情况进行相互访问，API 访问范围变为服务到服务（Service to Service），若某服务因 API 漏洞导致攻击者有利可图，那么攻击者将会看到应用内部的流量，这无疑为攻击者提供了更多的攻击渠道，因而针对数据泄露的风险程度而言，微服务架构相比传统单体应用架构带来的风险更大。此外，随着服务数量达到一定规模，API 数量将不断递增，进而扩大了攻击面，增大了数据泄露的风险。

传统单体应用架构中，由于网络拓扑相对简单，且应用通信多基于 HTTP/HTTPS，因而造成的数据泄露风险多是因为采用了 HTTP 协议。微服务应用架构中，网络拓扑相对复杂，因遵循分布式的特点，应用间的通信不仅采用 HTTP/HTTPS 协议，还采用 gRPC 等协议，由于 gRPC 协议默认不加密，因而将会导致攻击面增多，为数据泄露带来了更多的风险。

2.2.2 未授权访问风险

在单体应用架构下，应用作为一个整体对用户进行认证授权，且应用的访问来源相对单一，基本为浏览器，因而风险是相对可控的，微服务应用架构下，其包含的所有服务均需对各自的访问进行授权，从而明确当前用户的访问控制权限。此外，服务的访问来源除了用户外还包含内部的其他服务，因而在微服务架构下，应用的认证授权机制更为复杂，为云原生应用带来了更多的攻击面。

微服务应用架构下，由于访问权限还需涉及服务对服务这一层面，因此将会导致权限映射关系变得更加复杂，相应的权限配置难度也在同步增加。例如，一个复杂应用被拆分为 100 个服务，运维人员需要精密地对每个服务赋予其应有的权限，如果因疏忽导致为某个服务配置了错误的权限，攻击者就有可能利用此缺陷对服务展开攻击，若该服务中包含漏洞，进而可能会导致单一漏洞扩展至整个应用的风险。所以如何对云原生应用的访问权限进行高效率管理成为一个较难的问题，这也是导致其风险的关键因素。

2.2.3 被拒绝服务风险

在微服务应用架构下，由于 API 数量会随着服务数量的递增而递增，因而可能将会导致单一请求生成数以万计的复杂中间层和后端服务调用，进而更容易引起被拒绝服务的风险。例如，若微服务应用的 API 设计未考虑太多因单个 API 调用引起的耗时问题，那么当外部访问量突增时，将会导致访问需求与资源能力不匹配的问题，使服务端无法对请求做出及时的响应，造成页面卡死的现象，进而会引起系统崩溃的风险。

2.3 东西向流量难以防护的风险

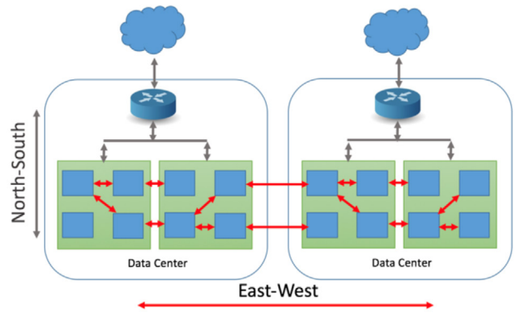


图 2 云原生环境下的东西向流量

云原生应用场景下的流量不仅包含传统基于边界的南北向流量，还包含集群节点间，微服务间访问的东西向流量，如果攻击者通过漏洞利用攻入集群内部，进而可能通过利用脆弱的认证机制横向移动入侵至其他微服务导致集群整体瘫痪。

2.4 其他风险

在云原生环境中，由于 API 的类型种类繁多，包括影子 API、僵尸 API、东西向 API、南北向 API、公共 API、内部 API 等，而且它们的迭代周期非常短，后端架构也更为复杂，因此管理起来更为困难。

此外，传统的安全设备很难适配 API 使用的其他协议，如 gRPC、SOAP、GraphQL 等。这些协议的出现使得云原生环境下的 API 安全风险进一步上升。

3. 云原生 API 安全防护思路

在讨论云原生 API 安全防护具体思路前，笔者想先提出云原生 API 安全防护的必要性，以下几个问题可能是读者普遍比较担忧的：

问题一：我的容器基础设施已有安全保护了，但业务部门运行的是微服务、服务网格和无服务，这些新的服务如何治理，安全性如何保证？

问题二：我有硬件、虚拟化或其他南北向的 WAF 了，但东西向的微服务安全怎么办？

问题三 :WAF 能解决所有的 API 问题吗？

带着以上问题，笔者梳理一些防护思路，下文将做具体介绍。

API 是微服务架构中通信的重要媒介，在云原生环境中，微服务通常以容器或 Pod 的形式出现，这些微服务在容器编排平台，如 Kubernetes 或 OpenShift 中运行，或者运行在服务网格（Service Mesh）中。因此，在云原生 API 安全防护方面，需要考虑容器编排平台和服务网格两种场景下的安全防护措施。

3.1 Kubernetes 场景

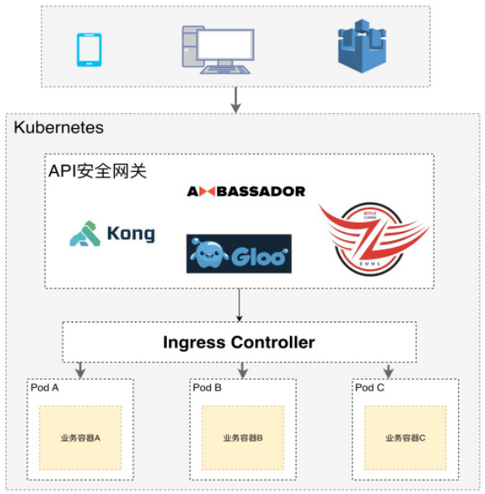


图 3 Kubernetes 场景防护方案

Kubernetes 场景中，常有的防护方案是在 Kubernetes Ingress Controller 前串行部署 API 安全网关用于处理恶意流量，此时，API 安全网关核心能力为 WAF 的能力，开源的 API 网关如 Ambassador、Gloo、Envoy Gateway 等虽然也集成了一部分的安全能力，但缺陷是集成的防护规则相对较弱，许多传统安全厂选择将其 WAF 产品容器化，并充分利用 K8S 的负载均衡和自动扩缩容能力提升高可用性。

然而，以上提出的方案实际也存在着一些问题，笔者认为主要有以下几方面。

首先，安全网关部署位置实际仍处于集群边界处，与传统安全网关部署位置相同，仅能对微服务的南北向流量进行防护，无法进行全向流量防护。

其次，采用 WAF 进行防护仅能处理 7 层恶意流量，并且无法覆盖 OWASP API Security Top 10 中的所有风险。在云原生环境中，微服务间通信协议还包括各类 RPC 调用，如 Google 的 gRPC、阿里的 Dubbo、Facebook 的 Thrift RPC 等，此外还存在 Graph-QL、SOAP 等通信协议，这些都是 WAF 无法进行防护的。

最后，云原生环境下，如果微服务访问采用加密流量，由于其数量可能会很多，传统 WAF 的证书卸载功能因为缺乏证书统一管理模块，因而并不一定适用于云原生场景，因此笔者认为该方案在某种程度上无法处理微服务加密流量。

3.2 Service Mesh 场景

3.2.1 安全能力容器化，通过引流将业务流量牵引至安全容器

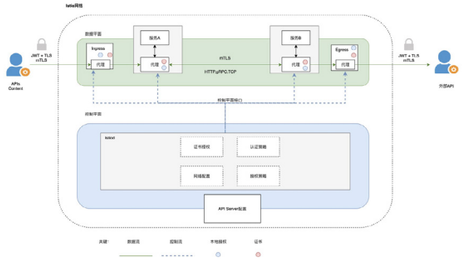


图 4 Istio 安全架构

图 4 为 Istio 的安全架构，我们知道 Istio 的数据平面主要通过 Envoy 代理容器实现流量管理、安全能力以及可观测性能力，安全方面主要提供以下机制：

1. 服务间及外部服务间多种认证授权机制；

2. 证书管理机制、加密流量卸载机制；

3.Envoy 提供 CSRF、外部授权服务器 (ext_auth filter，连接如 WAF 设备)、限流等 HTTP 安全过滤器。

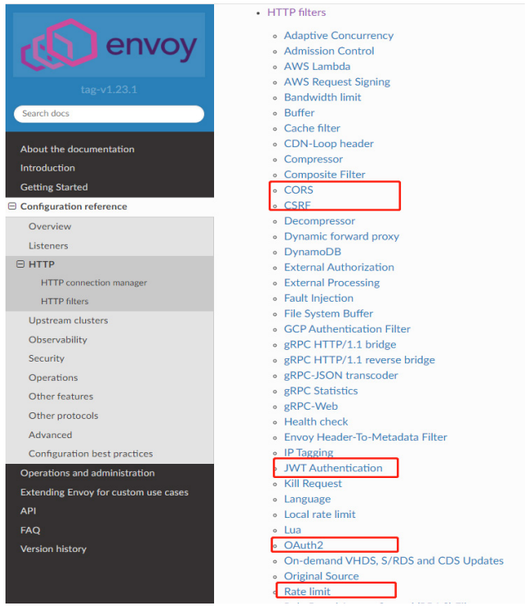


图 5 Envoy 安全类 filter

由图 5 我们可以看出 Envoy 自有的安全能力并不够，可行的一种方案是通过 Envoy 的引流 filter 引流到外部的安全容器，那么这个时候将传统的 WAF 容器化是一个较好的选择，WAF 也可以充分利用 K8S 的 LB 进行动态扩缩容。方案如图 6 所示。

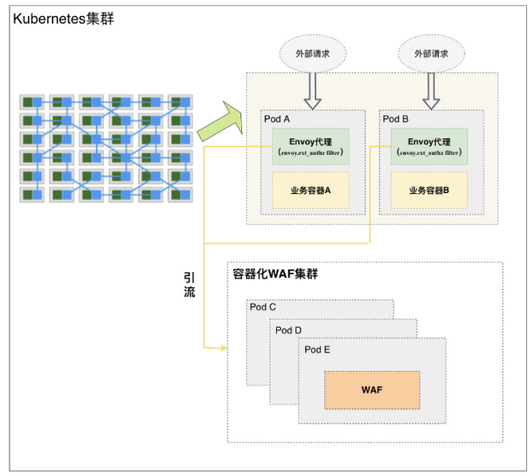


图 6 通过 Envoy 引流 filter 实现的方案

该方案通过 Envoy 容器进行流量牵引，使得所有集群服务的流量都经过了 WAF 的检测，具备了对东西向流量的检测优势。然而，这种方案也存在一些缺陷，其中最明显的就是 Envoy 引流插件的性能问题，即如何保证它能够承受大规模并发流量，并且防止服务宕机等问题。因此，针对这方面进行深入研究是非常有必要的。

3.2.2 安全能力集成至现有Sidecar容器

另一个思路是复用服务网格自身提供的扩展能力，如 Envoy 的扩展能力，实现将安全能力集成至现有的 Sidecar 容器，笔者将可以复用的 Envoy 扩展梳理为以下三种：

Envoy扩展	优势	不足	开源项目
Envoy custom filter	1. 更加原生化; 2. 执行效率高	1. 语言限制，只能使用c++进行扩展; 2. 部署运维成本高，每次更改需要重新编译Envoy; 3. 依赖性高，对Envoy版本强依赖性; 4. 开发灵活度低，需要适配Envoy自身的开发模式	envoy-filter-example(https://github.com/envoyproxy/envoy-filter-example)
Envoy lua filter	1. 插件式灵活嵌入Envoy，无须重新编译Envoy; 2. 默认支持对传输请求或响应流的操作	1. 语言限制，只能使用lua语言编写; 2. 执行效率相对较低; 3. 实验阶段	curiefense(https://github.com/curiefense/curiefense)
Envoy wasm filter	1. 不受语言限制（目前支持c++、Rust、AssemblyScript）; 2. 执行效率高; 3. 安全性高（密闭的沙箱环境，与Envoy隔离）; 4. 可靠性强（扩展崩溃不会影响Envoy运行）; 5. 敏捷性强（无须重新编译Envoy,可实现DevOps）; 6. 较为完善的SDK 官方指定SDK用于实现对传输请求的操作	版本限制 Istio 1.5以上的版本才可使用与wasm filter匹配的SDK	Wasm c++ sdk(https://github.com/proxy-wasm/proxy-wasm-cpp-sdk Wasm rust sdk (https://github.com/proxy-wasm/proxy-wasm-rust-sdk) Wasm AssemblyScript SDK (https://github.com/solo-io/proxy-runtime)

图 7 Envoy 扩展能力总结

3.2.3 安全能力Sidecar化

最后一种思路是将安全能力 Sidecar 化，我们知道 Istio 提供 Sidecar 自动注入能力，我们可以通过修改 Istio 注入模板，将安全能力作为 Sidecar 容器放置在现有 Service 数据平面中，如图 8 所示。

图 8 安全能力 Sidecar 化

上述思路，通过一定的策略管理，Service Mesh 可接管微服务的流量治理、监控及追踪甚至具备一定的基础防护能力，安全容器以轻量级安全伴生容器的方式透明注入至微服务中，并随着微服务资源的变化而变化，不仅可与现有服务网格治理框架高度兼容，也能进一步提升服务网格在流量侧的全向安全防护能力。此外，也能带来一些额外的优势，如：

1. 爆炸半径更小——爆炸半径仅限于一个微服务，即使安全容器因各种因素停止运行，由于安全容器于微服务内部运行，因而不会影响其他业务的正常运行。

2. 代理维护成本低——利用容器编排工具现有的滚动升级更新、灰度发布等机制，无须额外进行开发维护。

3. 安全边界更清晰—— 安全容器仅对位于同一微服务中的业务应用进行防护，与应用具有相同的 IP 地址。

4. 代理资源消耗依赖应用负载自身的变化—— 传统安全网关如 WAF 可能会存在不同站点流量抢夺的问题，即若有站点占用了较高的流量，消耗了 WAF 的所有资源，则其他站点流经的恶意流量将不会被处理，导致 WAF 无法正常工作，安全容器 Sidecar 化这种方式可通过配置微服务资源消耗占比有效应对此场景。

5. 容器级别的隔离防护—— 安全容器的方式可以让内核在容器级别执行所有的安全防护能力。

然而，该方案也存在一定的性能问题，比如高并发流量场景下，安全容器处理恶意流量会占用大量 CPU 和内存，导致超过节点承受最大阈值，即便安全网关容器不处理恶意流量也会占用一定内存和 CPU，引起不必要的性能消耗；此外，针对 Kubernetes 集群容器数量有一定限制的场景下，会影响正常业务的运行（如 100 个容器中，单安全容器就占用 50 个），再如这种方式将会导致请求链路增加，最终导致吞吐量降低和延迟升高。

4. 云原生 API 安全解决方案

技术实现上，我们提供了两种解决方案，分别支持 Kubernetes 以及 Service Mesh 场景，如图 9 所示。

图左为适配于 Service Mesh 的微 API 安全网关方案，安全能力采用轻量级的方式，无感知地接入每个微服务应用中，根据集群具体业务不同，可采用不同的 API 安全模块进行精准防护。此方案与 Service Mesh 配合使用，能够快速将微 API 安全网关注入至每个微服务应用中，同时对集群中的每个微 API 安全网关运行数据进行管理面上统一分析，并通过安全编排层进行服务策略编排，实现基于微服务粒度的全向安全防护能力。

图右为适配于 Kubernetes 的节点 API 安全网关方案，该方案采用 eBPF 技术将集群微服务引流从用户空间 offload 至内核层实现，降低系统 CPU 消耗的同时，提升了处理性能，也同时支持全向流量安全防护及灵活的策略编排。

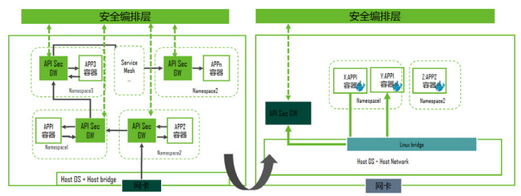


图 9 解决方案简要示意

5. 总结

Gartner 早在 2020 年 1 月提出了 CNAPP（Cloud Native Application Protection Platform，云原生应用防护平台）的术语，其集合了 CWPP 和 CSPM 的功能，重点强调了云应用安全防护的重要性。笔者认为，云原生 API 安全可有效针对微服务进行应用层面防护，是企业构建 CNAPP 过程的必经阶段，也是未来构建云原生应用安全（微服务安全、服务网格安全、FaaS 安全）必不可少的一环。此外，云原生 API 安全不应仅具备基于网络层面的威胁检测能力，还应集成 API 业务安全能力，以应对通过微服务业务逻辑漏洞对微服务进行攻击的风险，减少经济损失。最后，我们常说可见才可防，API 资产发现能力、分类分级能力和微服务可观测性等技术为 API 安全提供了有利的土壤，这些也是实现云原生 API 安全重要组成部分。

综上，本文较为系统地阐述了云原生 API 安全背景、态势、风险及防护思路，并介绍了绿盟在该领域的一些思考与实践，文章注重技术沟通，如有错误或不当之处，欢迎各位读者批评指正。

参考文献

[1] 云原生安全：攻防实践与体系构建 [M]. 机械工业出版社，2021.

[2]CSA 云原生安全技术规范，https://c-csa.cn/u_file/photo/20220316/c96467f1bf.pdf .

浅谈5G智慧港口网络安全防护

绿盟科技 解决方案销售中心 张铮 庞彬彬

摘要：近年来，港口业务应用逐步围绕智慧化、数字化方向进行变革，本文以集装箱码头为例，介绍 5G 技术在智慧港口的典型业务模式，剖析建设和运营阶段网络安全风险，探讨安全防护要点，为港口企业提供安全防护思路。

关键词：5G 智慧港口 集装箱码头 网络安全

随着我国交通强国战略稳步推进，交通行业新型基础设施建设有力支撑运输服务与业务开展。在航运领域，2022 年全球十大港口排名中，我国占据 8 个席位（见表 1）。当前港口领域业务建设正朝着智慧化和数字化方向发展。随着 5G、云计算等技术在港口领域大范围应用，其网络和数据安全防护的重要性日益凸显，网络安全持续建设和保障已成为港口企业用户的长期任务。

表 1 2022 年全球十大港口排名（数据来源：上海国际航运研究中心）

排名	港口	吞吐量（万吨）
1	宁波舟山港	122405
2	上海港	76970
3	唐山港	72240
4	青岛港	63029
5	广州港	63267
6	新加坡港	59964
7	苏州港	56590
8	德黑兰港	55327
9	日照港	54117
10	天津港	52954

1. 5G 智慧港口典型业务模式

传统港口的主要业务包括船靠泊管理、货物运输管理、车辆调度管理、港区管理等，其整个作业流程环节涉及非常复杂多样的应用场景。近年来，传统应用场景围绕智慧化、数字化发展方向进行变革，依托 5G 高速率、低时延和大连接等特点，实现港口领域人机物互联，在岸桥 / 场桥远控、港口无人集卡、智能理货、智能巡检等业务场景从试点示范逐步向大面积应用推进。

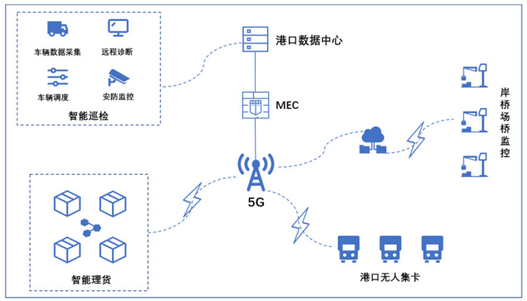


图 1 5G 智慧港口典型业务架构

5G 智慧港口典型业务架构如图 1 所示。在 5G 设施设备构成方面，港区内智能化设备（智能集卡、轮胎吊、拖船、摄像头等）通过如 CPE、5G 模组等终端接入 5G 行业虚拟专网中；5G MEC 存在垂直、水平多级部署方式，也存在基站节点后部署的场景；港口 5G MEC 不仅提供了业务处理、计算能力，同时也对港口内外数据进行分流，在保证高效处理能力和低时延之外，也进一步提高了港口数据的安全性；港口数据中心提供统一的综合业务平台，支撑港口多种业务。

在业务系统方面，5G MEC 平台通过标准化的北向接口给港口各项业务系统提供数据和服务；通常情况下，业务系统部署在临近此业务场景的 MEC 上，实现系统与场景在物理空间的紧耦合，在不同港口中，各项具体业务应用部署情况也根据港口运营规划、业务开展情况等因素进行灵活调整，如部署在港口的集中数据中心机房处，保证数据不出园区。

2. 5G 智慧港口网络安全风险

港口领域业务集中度高，风险暴露面大，攻击者可以以极低的成本对港口系统进行网络攻击，并造成大面积业务停摆。近年来，黑客针对港口的网络攻击越发频繁，印度、葡萄牙、挪威、丹麦、荷兰、南非等国家多个重要港口已先后成为攻击目标，而就在近期，欧洲最繁忙港口之一——葡萄牙里斯本港（Lisbon）也遭受网络攻击，直接冲击了该港的网站与内部计算机系统。港口网站在四天后仍处于离线状态，对港口业务正常运转造成巨大影响。

通过回溯分析，5G 智慧港口面临的风险主要包括港口领域信息系统固有风险隐患和 5G 技术应用带来的风险隐患，本文提炼出三点核心风险。

2.1 港口领域信息系统固有风险隐患

港口系统与协议存在先天风险。在集装箱码头控制系统中，大范围应用 OPC、CIP、EtherNet/IP、MODBUS 等工控标准化协议，以及西门子、施耐德、欧姆龙等设备供应商的私有工控协议，部分工控协议在设计阶段通常只考虑通信效率及稳定性，对通信安全考虑不足，存在仿冒认证、伪造授权、数据篡改和泄露等风险隐患。

港口领域专用控制系统漏洞利用逐年增多。在港口集装箱调度、监控等业务场景中集成了大量纯工业控制类系统，近年来工控系统漏洞被高频发现和利用，此类漏洞修复成本极高，部分港口企业宁愿承受外部系统风险，也不愿承担因漏洞修复造成的业务中断。

2.2 5G 技术应用带来的风险隐患

MEC 组网安全威胁。在内部组网方面，缺乏安全隔离可能导致恶意人员利用第三方应用发起攻击行为，攻击穿透 UPF，可影响核心网；在与核心网交互方面，存在信令和数据篡改、泄露等风险，可能对港口业务运行造成不良影响；与外部系统组网方面，连接互联网可能会使得系统开放，攻击者可以通过攻击第三方应用或管理 Portal 来攻击 UPF，进而攻击核心网。

MEC 边缘业务应用安全威胁。MEC 平台上的边缘业务应用存在多种安全威胁，包括恶意第三方 APP 接入网络提供非法服务、攻击者非法访问敏感数据、非法应用生命周期管理、恶意消耗系统资源等。

2.3 港口系统基础安全建设和运维管理不足

规划建设缺乏安全考量。港口领域业务线条众多，业务场景复杂，服务范围广泛，前期部分港口相关信息系统随用随建，缺少统一网络和安全规划，未充分遵循现行网络安全技术规范，造成智慧港口整体业务系统网络规范性、系统健壮性良莠不齐，存在先天安全风险。

安全运维管理手段不足。在部分港口的集装箱码头控制系统中，缺少防病毒、审计类功能设备，工控系统上位机较多使用 Windows XP/7 操作系统，缺乏进程管理、防病毒等有效的终端管控手段，对港口整体业务带来极大风险隐患。此外，港口企业网络安全专业管理和技术人员配备不足，运维管理未达成团队、工具、流程协同配套。

3. 5G 智慧港口网络安全防护思路

围绕《网络安全法》《数据安全法》和《关键信息基础设施保护条例》等国家政策法规，参照《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）及工业控制、港口领域技术标准，结合 5G 网络业务场景网络安全防护理论与案例，提出如下安全防护要点。

3.1 网络边界安全防护

引入 5G 边缘一体化安全 UPF，对智慧港口中各类业务场景进行网络边界安全防护。5G 边缘一体化安全 UPF 在传统数通能力基础上，强化安全能力构建，提供恶意流量检测、抗 DDOS 攻击、网络层访问控制、应用识别、数据隔离与防泄露、网络核心节点管控策略实施等安全能力，保障 5G 智慧港口各业务场景系统平稳运行。例如，在智能巡检（高清视频监控）场景中，依托 5G 边缘一体化安全 UPF 边界防护能力，在不同的网络边界设置不同的访问控制规则，实现细粒度安全访问控制，并对进出网络的信息内容进行过滤，使下级接入设备发起的恶意行为在 UPF 节点被控制，从而保障港口智能巡检等相关场景系统安全稳定。

3.2 MEC 安全防护

MEC 边缘计算安全防护

围绕基于流量的网络攻击溯源、MEC 主机安全防护和僵木蠕查杀等关键措施开展 MEC 边缘计算网络安全防护。通过对 MEC 网络流量和业务数据通信进行监测分析，实现风险预警和未知威胁检测分析，并通过资产梳理、准入认证和业务基线模型建立等方式管控 MEC 主机层风险，并对各类港口业务场景中的各类文件进行分析监测，依托沙箱技术对文件样本进行检测和还原，强化对僵木蠕的发现与病毒查杀能力的构建。

MEC 应用安全防护

对 MEC 应用安全威胁的防护手段包括加强认证鉴权和权限控制、针对开放接口 API 进行安全管控、保障通信安全和具备镜像安全保障机制等。具体措施包括使用白名单、证书等方式进行认证和鉴权，隔离管理权限，限制 API 接口访问，启用 TLS 加密传输，并对传输参数进行签名验证，启用镜像签名校验功能，对用户和镜像仓库进行组织管理等。

3.3 网络切片安全防护

安全隔离和数字证书、身份认证等技术保障切片隔离，并结合各场景业务实际进行明确、严格的防控控制策略制定与实施，确保用户或接入终端对每个网络切片拥有最小化访问权限，以保障智慧港口各类业务系统在网络切片层面安全稳定。此外，应综合判定具体场景中各类业务优先级，对高保障的业务服务和终端进行有限接入，以提高智慧港口各类场景系统业务连续性。

3.4 终端安全防护

依托运营商网络安全防护能力，实现对智慧港口场景中各类 5G 终端设备的多重认证与攻击防护，并通过 5G 电子围栏技术，实现对港口场区及港内 5G 终端设备的安全防控。

3.5 持续性网络安全运营

周期性网络安全检测评估

结合工业控制、业务服务等系统安全防护最佳实践，围绕业务保障需求，制定网络安全基线要求并进行周期性核查，对智慧港口各场景内网络设备、安全设备、应用系统、数据库、中间件、Web 应用系统进行漏洞扫描，并结合数据安全评估、渗透测试、实战攻防演练等方式降低各场景下业务系统脆弱性。

供应链安全保障

通过智慧港口企业自身供应链安全体系建设、供应商安全评估检查、产品技术能力建设以及漏洞应急能力建设这四方面能力建设，提高智慧港口供应链安全保障水平。如通过软件成分分析、软件静态 / 动态测试、容器安全检查、建立软件制品库等方式加强软件治理，并引入多源威胁情报，强化供应链漏洞发现和应急能力。

常态化监测预警与应急响应

建设智慧港口一体化网络安全运营中心，对港区内各类场景业务系统和港口对外服务系统开展安全网络和数据安全监测预警和态势感知，通过自动化编排技术，对设备、网络和系统等节点防护进行有效协同，提高安全运营效率。针对 APT 攻击、勒索病毒威胁开展攻防对抗，增强港口网络韧性。通过安全大数据分析、情报融合、威胁狩猎与应急响应，及时降低外部风险，构建全流程、全方位安全防护机制。

4. 总结

5G 技术的广泛应用有效提高了港口业务智慧化、数字化水平，岸桥 / 场桥远控、港口无人集卡、智能理货、智能巡检等新兴技术场景逐步替代传统业务模式。同时，在港口业务固有安全风险基础上，5G 技术的应用带来了新的风险隐患，港口企业用户需重点围绕 5G 网络和业务应用，强化网络安全纵深防御、主动防御能力，推动智慧港口常态化安全运营，不断提高网络安全防护水平，提升港口企业生产和经营核心竞争力。

参考文献

[1] 王信龙 , 王子萌 . 基于 5G 的智慧港口应用研究 [J]. 数据通信 ,2021(05):4-6.

[2] 薄明霞 , 白冰 .5G 智慧港口行业应用安全解决方案 [J]. 信息安全研究 ,2021,7(05):428-435.

[3] 王高欢 . 面向智慧港口的 5G 网络解决方案及应用 [J]. 中国新通信 ,2022,24(18):95-97.

[4] 刘强 . 港口生产业务系统网络安全技术研究 [J]. 信息安全研究 ,2019,5(08):746-751.

[5] DB4403/T XX—2022《5G 智慧港口网络建设规范（征求意见稿）》.

工业互联网商用密码应用模式设计及发展建议

绿盟科技 总体技术部 杨博

摘要：《商用密码管理条例》修订版于 2023 年 7 月 1 日施行，工业互联网企业的网络安全建设迎来新的合规要求，关保、等保、密评的衔接将更加紧密。密评成为工业互联网领域关基、等保三级系统上线、运行的前提条件之一。本文通过介绍商用密码在工业互联网场景下的应用模式以及构建认证信任服务体系的技术实现方式，为工业互联网企业开展商用密码应用建设提供了借鉴。

关键词：工业互联网 身份认证 信任体系 数据安全 商用密码

1. 引言

信息技术广泛应用和网络空间飞速发展，极大地促进了经济社会繁荣进步，同时也带来了新的网络安全风险和挑战。国家高度重视网络安全工作，自 2015 年《国家安全法》首次从法律的高度提出“实现网络和信息核心技术、关键基础设施和重要领域信息系统及数据的安全可控”以来，我国相继出台《网络安全法》《密码法》《数据安全法》《个人信息保护法》《关键信息基础设施安全保护条例》《网络安全》《商用密码管理条例》（2023 年 4 月国务院令第 760 号修订，以下简称《条例》）等法律法规，明确了对关键信息基础设施、等级保护三级系统、重要数据和个人信息采用密码技术实现重点防护的总体要求。法律法规中对关键信息基础设施、等保三级系统应用密码技术实施保护的具体要求如图 1 所示。

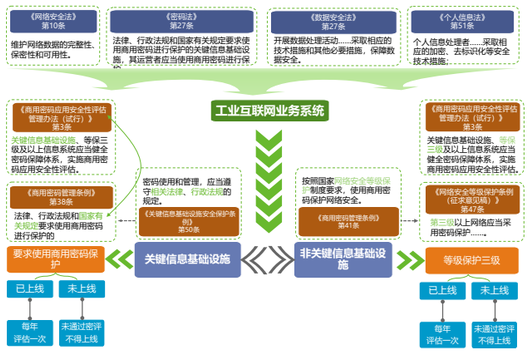


图 1 工业互联网商用密码应用合规性要求索引

《条例》中第 38 条“法律、行政法规和国家有关规定要求使用商用密码进行保护的关键信息基础设施，其运营者应当使用商用密码进行保护”和第 41 条“网络运营者应当按照国家网络安全等级保护制度要求，使用商用密码保护网络安全”都将国家密码管理局颁布的《商用密码应用安全性评估管理办法（试行）》作为工业互联网业务系统应用商用密码进行安全保障的指引，即关键信息基础设施、等保三级及以上信息系统应当健全密码保障体系。随着《条例》在 2023 年 7 月 1 日正式施行，工业互联网领域的商用密码应用也将从推荐性要求变为强制性合规要求。

2. 工业互联网商用密码应用的必要性

电力、交通、水利、石油、石油化工等行业中基于工业互联网的关键基础设施的稳定运行离不开工业互联网的安全。随着数字化转型逐步深入，工业互联网为数字世界与物理世界搭建起融合的桥梁，工业技术体系也由封闭逐步走向开放。基于工业互联网云—管—端三层典型架构，一方面，互联网技术引入工业生产，构建了工业数字化、网络化、智能化发展的基础；另一方面，工业网络互联互通性逐渐增强，为各生产过程的人、机、料、法、环构建数据传输的网络通路。我们在享受工业互联网带来的工业降本增效、高质量发展红利的同时，也面临着严峻的网络安全挑战。需要基于商用密码保障体系实现安全拓展，实现工业互联网全场景、全生态安全可控，保障用户、工业企业实现安全广泛连接。

2.1 端：工业智能设备接入安全性

数量、种类繁多的工业智能设备以多种方式接入工业网络，由于工业智能设备的开放化与标准化的技术架构不可避免地会产生安全漏洞，通信与计算资源不足限制了自身的网络安全功能，从而降低了针对工业互联网的网络攻击门槛，将信息世界的网络安全威胁引入到物理世界，加剧了国家关键基础设施遭受网络攻击造成的后果，轻则导致工业生产线宕机停摆带来经济损失，重则导致生产安全事故带来人员伤亡，甚至危害国家安全、动摇执政根基。数量庞大的工业智能终端和传感设备处于无人值守状态，有必要对接入设备实现认证。

2.2 管：数据传输安全性

数据是工业互联网蓬勃发展的“血液”，保障工业互联网敏感数据跨设备、跨平台、跨行业传输安全，对工业互联网企业正常运转、安全运营、稳定生产等方面具有重要的现实意义和应用价值，有必要对数据传输过程中的机密性、完整性、不可否认性进行保护，确保工业互联网通信过程安全、可靠、可控。

2.3 云：数据访问的可控性与存储安全性

工业互联网的发展正对传统工业生产模式进行优化、改造和重新定义。工业互联网平台实现了工业网络向用户侧延伸，逐步扩展了安全边界。管理端、生产端、消费端等多个层面的新业务系统用户大量增加，权限、数据、操作等安全风险不断扩大。工业生产模式由工业企业内部闭环运行转变为向社会公众开放，使得工业

互联网平台业务规模庞大，有必要在数据交互频繁，用户需求多元的场景下实现身份可信任和访问权限可控制。

工业互联网平台为分散在各个工业生产环节数据的汇聚提供了便利，客户信息、产量数据、图纸配方、流程参数等集中存储一方面可以利用多源信息融合技术处理、分析、挖掘数据中蕴藏的价值，另一方面给这些高价值数据的存储安全带来高要求，一旦这些数据发生泄露、篡改、丢失，将会给企业带来巨大的利益损失，有必要对此类数据存储进行敏感性分类、分级，并采取不同类别、级别的数据加密措施。

3. 商用密码在工业互联网中的应用模式

密码作为国之重器，是保障网络空间安全的核心技术，在网络空间中身份识别、安全隔离、信息加密、完整性保护和抗抵赖等方面具有不可替代的重要作用，可实现数据的机密性、真实性、完整性和行为的不可否认性。相对于其他类型的安全手段，如设备加固、物理隔离、防火墙技术等，密码技术是保障网络与信息安全最有效、最可靠、最经济的手段，是构建网络信任体系的基础支撑，是信息系统内置的免疫基因。

3.1 全场景身份识别与数据安全防护

工业互联网中接入对象具有设备多、数据大、区域广、体系复杂、类型多样的特点，基于单一类型的数字证书类型无法满足平台、设备、数据对身份识别和接入认证的需求，需要实现多态多类型的数字证书体系构建，融合多种认证证书类型，根据认证需求选择适合的认证体系，支撑工业互联网需求，提升认证能力和认证效率。工业互联网场景下的数字证书类型如图 2 所示。

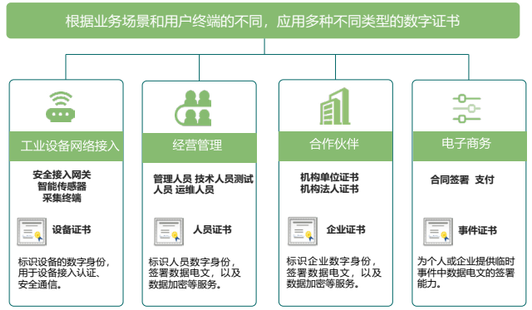


图 2 工业互联网数字证书类别

以数字证书为核心的加密技术 (加密传输、数字签名、数字信封等安全技术) 可以对网络上传输的信息进行加密和解密、数字签名和签名验证，确保网上传递信息的机密性、完整性及交易的不可抵赖性。通过对工业互联网应用的分析，各类型证书的应用场景如表 1 所示。

表 1 工业互联网数字证书应用场景

编号	应用分类	应用场景	证书类型
1	身份认证	使用数字证书登录工业互联网相关业务系统 （1）电子招投标系统； （2）研发设计协同系统； （3）生产制造执行系统； （4）其他业务系统	个人证书 机构证书
		使用数字证书登录工业互联网相关硬件设备。	个人证书 机构证书 设备证书
		标识工业互联网Web系统域名，有效识别钓鱼网站	应用/系统证书
2	数字签名	识别签名人身份并表明签名人认可其中内容的数据，防篡改、抗抵赖： （1）电子订单； （2）电子支付； （3）审计流程； （4）业务关键数据签名	个人证书 机构证书 设备证书
		代表一次性事件行为的有效性、不可否认性，私钥临时生成，使用完立即销毁： （1）电子合同； （2）其他一次性事件签名	事件证书
3	数据加密	即对原始的或未加密的数据，通过数字信封或对称加密算法对其进行加密，保障数据的机密性： （1）订单内容； （2）支付金额； （3）业务关键数据加密	个人证书 机构证书 设备证书

3.1.1 工业生产控制安全应用

基于数字证书、可信认证、国产算法为核心的密码技术，解决终端层工业智能设备非法接入、控制指令篡改、采集数据截获等痛点，实现工业生产控制在不同层级间的身份认证以及数据机密性、完整性保护，提升控制指令下达、采集数据上报等流程业务的安全等级，基于数字证书的工业生产控制环节应用方案如图 3 所示。

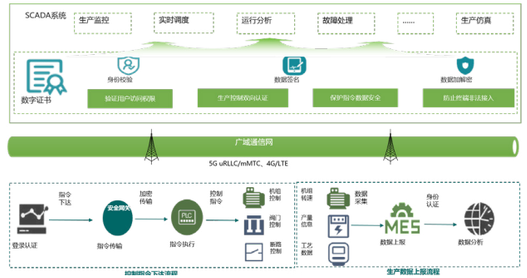


图 3 工业生产控制数字证书应用方案

3.1.2 工业互联网经营交易安全

工业互联网平台为工业生产制造企业、原材料供应企业、储运企业、终端消费者构建了交易渠道。随着工业互联网进程的不断推

进，以及数字证书在全行业的推广，数字证书的安全性与可信性已经得到充分认可，越来越多系统已经将数字证书作为首选身份认证方式，通过将客户管理、合同管理、产品管理、产能发布、撮合成交等应用的参与者身份与数字证书融合，实现身份认证，并为交易价格、交易量和电子合同生成等提供时间戳、行为抗抵赖、数据加密、数据追溯、数据完整性保护，解决工业互联网交易双方信息不对称导致的信任缺失问题，打造了公平公开的市场化交易环境。基于数字证书的工业互联网经营交易环节应用模式如图 4 所示。

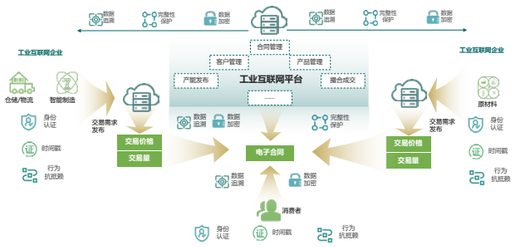


图 4 工业互联网经营交易数字证书应用方案

3.2 工业互联网认证信任服务支撑应用

工业互联网认证信任是实现工业互联网互联互通的前提和保障，能够有效支撑跨行业、跨企业间互信互认，打破现有认证体系壁垒，打通上下游产业链，从身份认证和数据加密两个方面进行安全保护，有效解决工业互联网中身份伪造、信息泄密、数据篡改的安全问题。但由于历史原因或者技术限制，一张数字证书往往仅仅能在一个应用或者一个行业（企业）使用，无法在其他系统使用，即未实现数字证书的互认互通，已经成为工业互联网互联互通的重大瓶颈。实现证书认证信任服务支撑架构如图 5 所示。

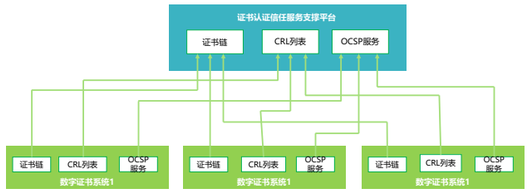


图 5 数字证书认证信任服务支撑架构

如图 5 所示，各个数字证书系统把自己的证书链、CRL 列表、OCSP 上传到证书认证信任服务支撑平台，由平台对请求进行身份认证的证书解析其颁发者，并根据颁发者匹配对应 CA 机构的证书链、CRL 以及 OCSP 服务，然后进一步验证数字证书的状态，并返回验证结果给请求方；从而实现各数字证书系统颁发证书的互认互通。数字证书用户登录应用系统的认证信任时序如图 6 所示。

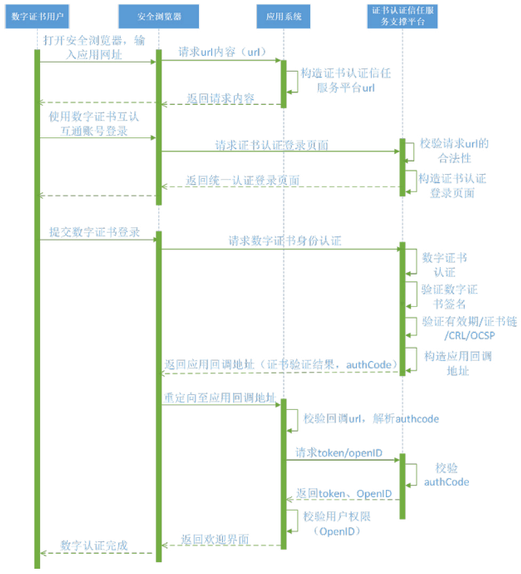


图 6 数字证书认证信任服务时序

依托证书认证信任服务支撑平台采用的统一认证，数字证书系统只需要接入到平台一次，平台下的应用便都能使用或支持该数字证书机构颁发的数字证书，从而实现工业互联网跨行业、跨行政区划、跨企业的互认互通。

4. 工业互联网企业建设商用密码保障体系建议

随着工业互联网建设步入发展快车道，对商用密码的使用需求急剧扩大，工业互联网企业应始终保持密码应用工作的初心，积极响应国家法律法规和政策要求，通过先行探索开拓，推动和促进国产商用密码技术与工业互联网业务加速融合。

4.1 设立商用密码应用管理机构

成立企业商用密码应用管理机构，负责落实国家和行业密码应用政策，加强对密码应用的管理，确保业务系统与密码应用同步规划、同步建设、同步投入使用，充分发挥商用密码保障工业互联网生产经营安全的重要作用。

4.2 制订商用密码体系顶层规划

工业互联网企业需要制订和落实商用密码应用发展规划，全面筹划各类业务系统的密码应用方案，逐步完善密码应用管理体系和应用模式，推动探索行业引领示范成效，打造工业互联网密码应用品牌效应。

4.3 开展统一密码服务平台集约建设

建设统一密码服务平台，提供身份认证、电子签名验签、数据

加解密等“一体化”密码服务，实现密码的使用规范化、管理科学化、应用大众化，简化业务系统使用密码服务的复杂度，满足业务需求持续变化对密码应用模式的复杂多样，遵循统一标准体系，实施统一安全防护，构建一体化的密码应用支撑体系。

4.4 打造以密码技术为核心的立体防御体系

改变“建围墙”式的网络安全防护模式，构建密码技术与网络安全技术相融合的立体防御体系。平台服务层采用密码资源池，网络层打造安全传输通道，终端层采用安全芯片、软件密码模块，最终形成“软硬兼施、刚柔并济”的全方位立体防御体系。

5. 结束语

工业革命的大背景下，随着工业互联网建设进程的不断深化，工业互联网平台的数量持续增加，工业互联网规模迅速扩大，工业互联网的安全状况以及所面临的攻击威胁日益严重，工业互联网密码应用对我国工业互联网网络安全体系的长远发展战略将起到重要的支撑和推动作用，有利于规范工业互联网产业的安全有序、健康发展。

参考文献

[1] 国家互联网信息办公室 . 国家网络空间安全战略 [EB/OL].(2016-12-27) http://www.cac.gov.cn/2016-12/27/c_1120195926.htm.

[2] 张飞，郭子梦，孙晓辉，习佳 . 工业互联网安全及评测综述 [J]. 科技视界 , 2019(25): 120-121.

[3] 杨博 . 工业企业两化融合网络安全保障模型研究与应用 [J]. 信息安全研究 . 2021,7(08): 773-778.

[4] 杨博 , 王振东 , 彭磊 . 工业互联网数据安全监测平台建设实践探索 [J]. 工业信息安全 . 2022(02): 90-95.

[5] 吉林省密码管理局 . 密码知识科普读本 [M]. 北京：人民出版社，2018.

公有云攻防系列：云凭证的泄露与利用

绿盟科技 创新研究院 李来冰

摘要：本文通过梳理云上数据泄露事件，总结了云上数据泄露的原因，说明了其中云凭证泄露的危害与利用手段，最后提出了一些防止凭证泄露的思路。

1. 引言

在文章《公有云攻防系列——云服务利用篇》[1] 中，我们向大家介绍了一些利用公有云厂商提供的云服务来进行攻击的案例，说明了公有云在给用户提供便利的同时，也有可能带来新的风险。本文则从近几年的一些云上数据泄露事件出发，梳理了发生数据泄露的常见原因，重点介绍了其中一个重要原因——云凭证的泄露与利用，最后站在防御的角度给出一些防止凭证泄露的方案。

文中涉及的技术仅供教学、研究使用，禁止用于非法用途。

2. 云上数据泄露事件

要关注云上数据安全，需要先从实际的安全事件中出发，总结安全事件涉及的技术关键词。云计算的部署模式多种多样，包括公有云、私有云、混合云和社区云，以下梳理了近几年发生在这些云上的一些数据泄露事件（见下表）。

从表格中可知，云上数据泄露的原因多且杂，尤其涉及人的原因，可被影响的因素较多。

随着应用程序的不断完善以及各种安全防护产品的诞生，网络安全防御系统也在不断升级加强，但人员仍是系统中最薄弱的环节。相比于利用漏洞进行网络攻击的高门槛，针对人员因素的攻击门槛更低，或是在使用复杂云服务时访问控制配置不当，或是由于意识薄弱而误点击钓鱼邮件，或是在技术社区意外泄露了重要凭证，种种因素都有可能被攻击者利用，造成数据泄露。下文主要介绍其中一个因素：云凭证的泄露。

时间	事件	技术关键词
2020 年 7 月	美国开放银行 Dave 的 750 万名用户的数据被泄露，原因是前合作伙伴 Waydev 拥有 Dave 在 Github 和 Gitlab 上的 OAuth token，Waydev 由于漏洞被黑客入侵，导致 token 泄露，黑客从 Dave 的 Github 项目中发现明文密码，成功访问 Dave 的系统并窃取了数据。	SaaS、第三方服务、Github、明文密码、凭证泄露
2017 年 8 月	知名云服务供应商 BroadSoft 未妥善保护时代华纳托管在亚马逊存储服务器的数据，导致逾 400 万名客户的信息在线泄露[2]，原因是管理人员因配置错误未关闭服务器公共访问权限，导致任意用户均可匿名访问。	AWS、错误配置
2021 年 8 月	VpnMentor 的研究团队发现 B2B 营销公司 OneMoreLead 将其存储数据库设置为公开访问，数据库中包含至少 6300 万条用户数据。	私有云、错误配置
2021 年 8 月	T-Mobile 被曝泄露近 4900 万条用户数据，原因是黑客通过网络攻击入侵其测试环境，然后进入其内部网络，成功窃取数据。	私有云、测试环境对外访问、漏洞攻击
2021 年 11 月	电子交易平台 Robinhood 披露，未经授权的有关方通过电话冒充员工，访问了其客户支持系统，成功窃取了约 700 万条用户数据。	私有云、用户冒充、社工欺骗
2021 年 12 月	在线预订服务平台 FlexBooker 超 370 万个账户数据遭泄露，原因是攻击者获取了 AWS 基础设施中一个被泄露的账户，从而入侵 AWS 云存储系统，导致数据泄露	AWS、账户泄露、凭证泄露
2022 年 2 月	美国的一家提供在线电子邮件营销工具的公司 Beetle Eye 发生重大数据泄露，此次事件是由于 AWS S3 存储桶未进行任何加密且配置错误造成的，该漏洞导致 Amazon S3 存储桶处于打开状态，泄露了大约 700 万人的敏感数据	AWS、S3 存储桶、错误配置
2022 年 4 月	美国知名投资公司 Cash App Investing 的 820 万名客户的数据被泄露，由一名前员工下载了公司内部的一份报告引起，泄露的信息包含客户的全名和经济账号等	私有云、离职员工、账户管理
2022 年 8 月	SpiderSilk 公司发现了微软的员工在 Github 上暴露了公司在线基础设施的敏感登录凭据，其中 7 个暴露点都是 Azure 服务器的凭证	Azure、员工误泄露、凭证泄露、Github
2022 年 9 月	网络安全商 SOCRadar 披露，微软由于“一个配置错误的数据桶”导致分布在全球 111 个国家和地区的超过 65000 家企业受到影响	Azure、存储桶、错误配置

3. 常见凭证泄露途径

云厂商在提供云服务时，为了方便用户在多种场景下（如在业务代码中调用云服务功能或引入云上数据资源时）使用，大部分都支持 API 调用的方式，此时便涉及访问控制的问题。

用户使用云厂商生成的凭证（如图 1 所示）可成功访问该凭证对应权限下的云服务资源。

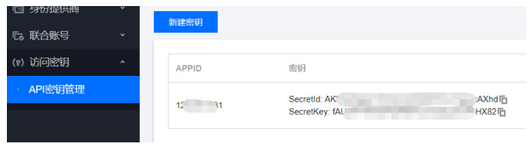


图 1 某云厂商 API 密钥

凭证格式主要分为 SecretId 和 SecretKey，其中 SecretId 用于标识 API 调用者身份，SecretKey 用于验证 API 调用者身份。

在实际调用云服务 API 时，部分开发者会将凭证以硬编码的形式保存在代码中，但这无疑增加了额外的风险。这些凭证可能会因为人员的失误通过各种途径泄露出去，最终导致相关数据受到损害。以下梳理了云凭证常见的泄露途径。

3.1 代码托管平台

Github 是深受众多开发者喜爱的代码托管平台，开发者常常将个人代码或公司代码推送至私有仓库或公共仓库，但在推送代码的过程中可能会因为审计工作不足导致代码中的硬编码凭证泄露出去。据 GitGuardian 报告 [3] 指出，“2021 年检测超过 600 万个泄露的硬编码凭证被推送到 Github 上，比 2020 年翻了一倍”。报告所指的另一个问题也需要关注，“私有仓库比公共仓库隐藏的硬编码凭证要多得多”，由于私有仓库不对外公开访问的原因，许多开发者便“心安”地将凭证直接推送至私有仓库中，但一旦 Github 的 Access Token 发生泄露，私有仓库也将变得不再私有。

除了 Github，还有 Gitee、Gitea、Gogs 和 Gitblit 平台也可能发生同样的情况。如开源项目 Gitlab，被不少企业用来管理内部代码，但 Gitlab 漏洞频出，一旦内部 Gitlab 代码平台存在漏洞且对外可访问，恶意攻击者可利用相关漏洞攻陷代码服务器，窃取源代码。在绿盟科技先前发布的文章《DevOps 风险测绘之代码篇》[4] 中表明，源代码泄露风险不可小觑，感兴趣的可以详细阅读。

3.2 公共镜像仓库

随着容器技术的火热发展和快速落地，Docker Hub 成了另一个开发者喜爱的平台。据报告 [3] 指出，Docker Hub 上存储了 800 多万可用的公共镜像，GitGuardian 通过抽样扫描其中一万数量的镜像，得出“4.62% 的镜像至少暴露了一个 secret”的结论，可见公共镜像仓库也成为凭证泄露的又一大平台。

3.3 技术社区

2020 年，在中国最大的程序员技术博客平台上，曾有一名用户分享如何把数据备份到阿里云上，不慎将硬编码的阿里云凭证泄露 [5]。

参与系统开发的人员在个人层面发布相关博客时，并不能按照公司级别严格的流程，可能会由于审核不足误将敏感信息泄露。

3.4 应用程序漏洞

利用 Spring Boot 信息泄露获取凭证

Spring Boot 是用来简化 Spring 应用开发流程的框架，采用 JAVA 语言编写。Actuator 是其中用来监控的功能模块，当 Actuator 启用时，如果没有做好权限控制，可导致用户未授权访问某些执行器端点（如 /heapdump）来获取应用系统中的监控信息。Heap dump 是堆转储文件，是一个 JAVA 进程在某个时间点的内存快照。当 /heapdump 未授权访问时，可利用工具 [6] 从 heapdump 文件中查找凭证，如图 2 所示。

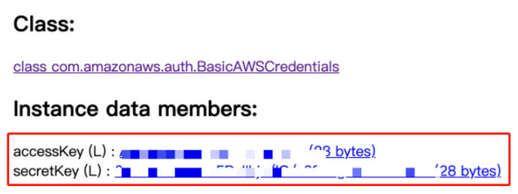


图 2 匹配到 aws 凭证 [7]

由 Swagger 引发的 OSS AccessKey 泄露 [8]

Swagger 是一个规范和完整的框架，用于生成、描述、调用和可视化 RESTful 风格的 Web 服务。当可访问 Swagger 接口文档时，可测试接口是否存在注入、越权等漏洞，若存在未授权访问，则有可能从敏感接口获取到凭证信息。

4. 云凭证的利用

当通过各种途径获取到云凭证时，该如何利用呢？如前文所说，云厂商在提供 API 调用的形式时，也提供了相关的文档说明和实例演示，以腾讯云为例：

1. 访问 https://console.cloud.tencent.com/api/explorer 可查看相关操作对应的 API。

2. 选择 Python 语言，点击“调试 SDK 示例代码”可进入 Cloudshell 界面，如图 3 所示。

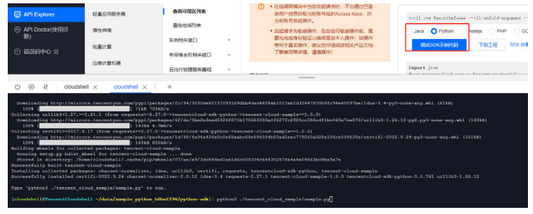


图 3 Cloudshell 界面

3. 进入相关 python 文件，修改“cloud_secret_id”和“cloud_secret_key”值（如图 4 所示）为发现的凭证，然后运行 python 文件即可利用该凭证进行操作。

图 4 修改 python 文件

除上述官方方式外，也可利用现有的工具，以下是调研的一些凭证利用工具。

项目名称	项目地址	项目功能
Pacu	https://github.com/RhinoSecurityLabs/pacu	AWS 攻击利用框架，包括用户权限提升、IAM 用户的后门、攻击易受攻击的 Lambda 函数等
CF	https://github.com/teamssix/cf	针对阿里云、腾讯云、aws 的 AK 凭证进行利用
aws-cli	https://github.com/aws/aws-cli	命令行操作 AWS 云服务的官方客户端
gcloud CLI	https://cloud.google.com/sdk/docs/install#linux	命令行操作 Google 云服务的官方客户端
alicloud-tools	https://github.com/iiiusky/alicloud-tools	辅助使用阿里云 API 操作 ECS 以及策略组的小工具

5. 如何防止凭证泄露

在了解到云凭证的泄露途径之后，便需要思考对应的防御对策。以下是总结的一些可供参考的方案和建议。

严格的代码审计

个人、公司代码在提交至公开代码仓库或公共镜像仓库时，应对代码或镜像进行严格的审计，避免出现硬编码的凭证。

凭证安全管理和保护

使用专业的凭证管理工具存储凭证，避免使用硬编码，在需要使用凭证时调用工具获取值即可。同时定期更换凭证，即使凭证泄露也有可能失效。

定期检查代码仓库漏洞

若公司自建代码管理平台，需定期检查平台的脆弱性，同时禁止对外公开访问。

漏洞评估

对于调用云服务资源的应用程序定期进行漏洞评估，防止出现因为漏洞导致的凭证泄露。

员工安全意识培训

加强对员工的安全意识培训，严格禁止公司内部代码私自上传、拍照行为。

参考文献

[1] https://mp.weixin.qq.com/s/zw9nGP9-czU2aPrpVa6wkg.

[2] https://www.cnbc.com/2017/09/01/around-4-million-time-warner-personal-records-exposed-in-data-leak.html.

[3] https://res.cloudinary.com/da8kiytlc/image/upload/v1646148528/GitGuardian_StateOfSecretsSprawl2022.pdf.

[4] https://mp.weixin.qq.com/s/s-y0T_L5rP0WkGyvJsFd6g.

[5] https://archive.ph/mP3bh#selection-10187.2-10189.435.

[6] https://github.com/wyzxxz/heapdump_tool.

[7] https://zhuanlan.zhihu.com/p/372985944.

[8] https://www.yuque.com/corgi/fw01x2/ds00tf.

Rilide：基于社工学的恶意软件

绿盟科技 售前技术部 黄硕麒

摘要：Rilide 是一种针对 Chromium 体系的恶意软件，通过恶意文件、网络木马、钓鱼网站重定向等方式进行传播。一旦触发 Rilide，用户浏览器活动将被持续监控并且 Rilide 将伺机窃取用户的重要数据资产。Rilide 利用了社会工程学的理念，利用人类思维惯性绕过双因子认证系统，从而实现资产窃取。

关键词：Rilide 社会工程学 Chromium 体系 双因子认证绕过

1. 引言

Rilide 是一种伪装成合法 Google Drive 扩展程序的恶意软件，主要针对基于 Chromium 体系的浏览器，如 Google Chrome、Brave、Opera 和 Microsoft Edge。Rilide 通过恶意文件、网络木马、钓鱼网站重定向等方式进行传播。用户一旦安装后 Rilide 会立刻修改浏览器的快捷方式文件，后续用户每次启动浏览器时将会自动运行 Rilide。Rilide 将持续监控用户浏览器活动、随时截取屏幕截图并窃取用户的重要数据资产，如电子邮件账户密码、加密货币钱包地址、资产私钥以及其他敏感信息。

2. Rilide 的传播方式

目前由 Trustwave 的 Spider 实验室发现了两种可能的 Rilide 传播方式，如图 1 所示。

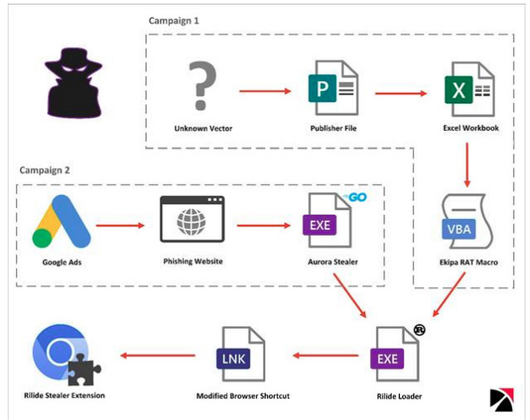


图 1 Rilide 的传播方式 [1]

第一种方法是通过 Microsoft Publisher 来传播，通过在

Publisher 文件里写入 Ekipa RAT 实现。Ekipa RAT 是一类远控木马 (RAT)，可获取用户电脑的关键信息如 IP 地址、硬件信息、文件目录等。此外，Ekipa RAT 还可以对受感染的电脑上传下载、删除、移动、重命名文件，远程运行代码。当用户打开 Publisher 文件时，会立刻执行 Ekipa RAT，Ekipa RAT 会远程连接到黑客所控制的远控服务器，进而从服务器下载、执行与安装 Rilide 到用户电脑上。

第二种方法是借由谷歌广告服务来诱导用户下载 Aurora，Aurora 是一种数据窃取程序，Aurora 能假冒 Team Viewer 或 Nvidia 驱动程序的安装程序来诱骗用户下载安装。Aurora 后续从远控服务器下载安装 Rilide。

Rilide 在用户电脑上安装后，如果检测到用户电脑上有 Chromium 体系的浏览器，Rilide 会通过模仿良性的 Google Drive 扩展程序，通过改变几个内置的 chrome 功能参数如 --load-extension 来修改快捷方式 (LNK)，从而保证用户点击浏览器时自动启动 Rilide。

3. Rilide 的工作原理

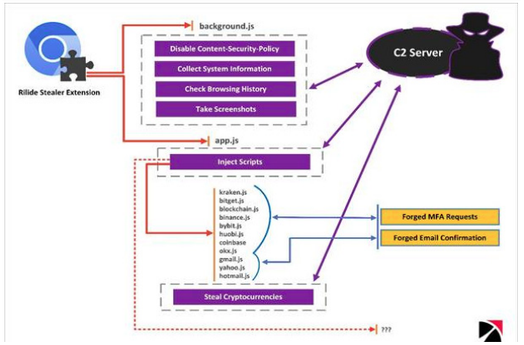


图 2 Rilide 的工作原理 [1]

Rilide 启动后会运行内部脚本在用户电脑上安装一个侦听器，侦听器会监控用户电脑上 Chromium 体系的浏览器何时切换选项卡、何时接收网站内容、何时网页加载完成。此外，Rilide 还会检查当前站点是否与远控 (C2) 服务器提供的目标列表相匹配。如果匹配 Rilide 会加载 SQL 注入脚本，从用户电脑上窃取用户数据资产。

Rilide 会定期扫描浏览历史记录，以确定此用户是否具备数据窃取价值，此外还可以实时捕获屏幕截图并发送到远控服务器上，从而方便黑客及时调试脚本。

Rilide 的核心功能是它的双因子认证绕过系统，即通过使用伪造的身份认证来欺骗用户主动通过双因子认证。当用户向网站提交取款申请时，如果站点和 Rilide 内置的目标网站匹配，Rilide 的绕过脚本将被激活，此时用户的页面将会被替换成和源网站类似的身份验证界面，诱使用户通过双因子认证。此外，如果网站属于使用邮件来进行身份认证的形式，只要用户仍然使用相同的 Web 浏览器输入邮箱，那么确认邮件将会被 Rilide 及时截获，从而拿到用户的授权码。同时 Rilide 会发送一封虚假的授权邮件，原始邮件中的授权码将被自动提取并填写在虚假的授权邮件内，从而使用户认为自己收到了真实的授权邮件。Rilide 绕过了双因子认证后，此时用户的数据基本就不设防了，此时通过远控服务器收到消息的黑客将对此用户的数据为所欲为。

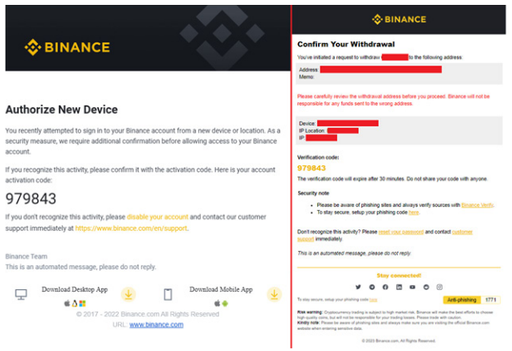


图 3 Rilide 邮件伪造示例 [1]

4. 从 Rilide 看社会工程学

Rilide 不是第一个恶意浏览器扩展软件，它能做到的事情看起来和普通远控木马没有太大的出入，拆开来看无非就是传统利用 XSS 诱骗用户下载木马，通过包装成浏览器扩展程序木马篡改系统权限，然后远程连接服务器那一套远控流程，但 Rilide 的最关键点就在于它利用了社会工程学伪造网站身份验证来欺骗用户通过双因子认证。双因子认证近年来在全世界范围内流行普及，尤其是在中国，双因子认证几乎成为公认的网站身份验证方式，就连国家法律如“等保 2.0”里双因子认证也作为必需项来向全国推行。

双因子认证是一种采用时间同步技术的系统，传统的双因子认证采用了基于时间、事件和密钥三变量而产生的临时动态密码来代替传统的静态密码。每个动态密码都有一个唯一密钥，该密钥同时存放在用户及服务器端，每次认证时动态密码卡与服务器分别根据同样的密钥，同样的随机参数（时间、事件）和同样的算法进行计算从而确保双边密码的一致性，从而实现用户认证。双因子认证为什么被认为安全，其原因就在于其每次认证时的随机参数不同，产生的动态密码也不同，通过每次计算时参数的随机性保证了每次密码的不同，也就导致了双因子认证的破解难度大。

既然双因子认证从外部强行破解的难度大，那么能不能从内部破解？黑客不需要强行破解认证，只要用户自己帮我通过双因子认证就行。听上去很荒谬，但社会工程学就是这样利用人类的心理弱点化不可能为可能，而 Rilide 就是社会工程学的一次经典复刻。从一开始通过伪造成 Microsoft Publisher 文件或者通过谷歌的广告服务来诱导用户下载木马载体，到利用用户对于双因子认证的默认放心，说白了和之前曝光的某地商场某著名运动品牌店真假混卖的事情是同一原理，都是利用用户对于品牌或者社会共识的认同来达到欺骗目的。

对所有组织（单位）而言，人都是安全防范措施里最薄弱的一环，也是整个安全防护最脆弱的层面。人是社会的产物，人的本性就是社会性，所以人具有社会学方面的弱点，容易遭受社会工程学攻击。精通社会工程学的攻击者通常会利用社会工程学手段获取自己想要的信息，Rilide 只是把以往黑客或诈骗犯的社工学理念融入到自动化恶意程序中，这一步显著降低了黑客的破解成本。就和早些时候爆火的 ChatGPT 一样，只是在底座数据库转化为上层人机交互中加入了人工训练选择这一步，就使得人机交互准确性大幅提升。

对于 Rilide 的防范，本质上和防社工学一样，都需要靠人的安全意识提升才能解决。老生常谈的严防钓鱼邮件、拒绝访问不受信地址、拒绝打开可疑程序等防社工意识，如果人人都能具备，那么 Rilide 就会像其他常规的远控木马一样，随着技术的发展逐渐消失在历史长河中。

5. 结语

Rilide 是当下网络环境日益复杂所带来危险的典型示例，是社会工程学在恶意程序上的初步实现。未来随着攻击者对于人性的理解加深，Rilide 的演化将会越来越可怕，今日只能撬开你的网站账户，明日可能撬开你的网上银行。在这个信息爆炸的时代，繁杂的信息削弱了我们对事务的准确判断，使我们更容易遭受类似钓鱼邮件的网络攻击。就像零信任理念所倡导的一样，“永不可信，持续验证”不只是针对系统，也是针对我们每一个人。

参考文献

[1] Pawel Knapczyk, Wojciech Cieslak. Rilide: A New Malicious Browser Extension for Stealing Cryptocurrencies, 2023.

SCARLETEEL：一起利用Terraform、Kubernetes和AWS的数据窃取事件

绿盟科技 创新研究院 李来冰

摘要：本文介绍了云上攻击活动 SCARLETEEL 的攻击链和相关技术细节，带读者了解真实的云上攻击事件。

关键词：云安全 公有云攻防 云服务利用 AWS

1. 引言

根据 Sophos 安全公司在 *The Reality of SMB Cloud Security in 2022*[1] 中指出，在过去的一年里，发生在云上的网络攻击增加了 56%。在云端获得持久性、窃取敏感数据和创建资源进行恶意挖矿是几个最常见的动机，这些攻击活动不仅是利用云服务资源进行获利，还包括一些间谍活动。

本文主要解读了由 Sysdig 威胁研究团队公开的一起云上攻击活动 [2]，由于攻击过程复杂且较为典型，希望能够分享其中的技术细节，带大家了解真实的云上攻击事件。

文中涉及的技术仅供教学、研究使用，禁止用于非法用途。

2. 攻击链概述

该攻击活动发生在 Sysdig 的一个客户环境，被取名为 SCARLETEEL。攻击者利用一个容器化的工作负载获得初始访问权限，通过一些手段进行权限提升和横向移动，使得影响扩大至客户的 AWS 账户，大致攻击链如图 1 所示。

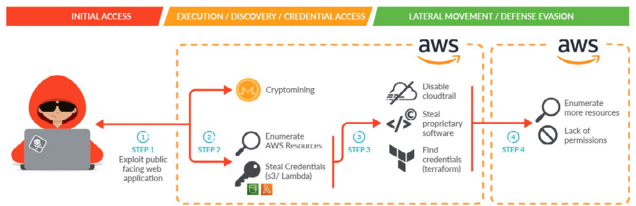


图 1 SCARLETEEL 攻击链

步骤 1：攻击者利用托管在 AWS 云账户中的 Kubernetes 集群获得初始访问权限。

步骤 2：获得集群 Pod 的访问权限后，攻击者可以进行以下两种操作：

a. 启动一个加密货币挖掘软件，以谋取利益。

b. 利用实例元数据服务获取临时凭证权限，利用集群角色权限收集信息。由于授予的权限过大，导致攻击者可以：

（a）枚举 AWS 资源；

（b）从 Lambda 和 S3 服务中获取其他 IAM 用户凭证。

步骤 3：利用步骤 2 中获取的凭证进行横向移动，可通过 AWS API 获取更多账户相关信息：

a. 停用 CloudTrail 日志以绕过检测；

b. 窃取专利数据；

c. 通过 S3 存储桶中的 Terraform 状态文件，寻找其他 IAM 用户凭证。

步骤 4：利用新的凭证重复步骤 3 中的横向移动行为，但因缺乏权限而尝试失败。

3. 技术分析

初始访问——攻击容器应用

攻击者利用暴露在公网上的服务获得初始访问权限，发现该业务运行在 Kubernetes 集群中。容器作为一个受限的隔离环境，并非攻击者的最终目的，攻击者在容器环境中进行了两个攻击操作。

1. 在当前环境中下载和启动挖币软件，但是挖币只是攻击者的最初目标或者作为窃取数据行为的“障眼法”，一旦可以继续扩大战果，攻击的目标也就随之改变。

2. 因此攻击者尝试利用 IMDS（Instance Metadata Service）服务进行权限提升。

IMDS 即实例元数据服务，它是 AWS 实例上的组件，在实例上进行编码，用于安全访问实例元数据。利用元数据服务获取临时凭据是一种常见的攻击思路，不同的云厂商所对应的元数据服务地址不同，其中 AWS 的元数据服务接口如下：

// 获取 IAM 信息

http://169.254.169.254/latest/meta-data/iam/info

// 获取 IAM 凭证信息，包括 AccessKeyId、SecretAccessKey 和临时令牌

http://169.254.169.254/latest/meta-data/iam/security-credentials/<rolename>

在获取凭证信息之后，可以使用 aws-cli 工具控制 AWS 云服务资源，但是利用 AWS API 的调用请求会在 AWS CloudTrail 服务上留下日志。AWS CloudTrail 是一项安全服务，能够记录、持续监控和保留与整个 AWS 网络服务基础设施行为有关的账户活动，包括 AWS 管理控制台、AWS SDK、命令行工具和其他 AWS 网络服务采取的行动。如图 2 所示，Sysdig 通过查看 CloudTrail 日志可了解攻击者的攻击操作。

Event name	Username	Event Source	Error code	Event type
CreateUser	i-054197bb12d401810	iam.amazonaws.com	AccessDenied	AwsApiCall
ListAttachedGroupPolicies	i-054197bb12d401810	iam.amazonaws.com	NoSuchEntityException	AwsApiCall
AttachGroupPolicy	i-054197bb12d401810	iam.amazonaws.com	AccessDenied	AwsApiCall
AttachGroupPolicy	i-054197bb12d401810	iam.amazonaws.com	AccessDenied	AwsApiCall
AttachGroupPolicy	i-054197bb12d401810	iam.amazonaws.com	AccessDenied	AwsApiCall
AttachGroupPolicy	i-054197bb12d401810	iam.amazonaws.com	AccessDenied	AwsApiCall
AttachGroupPolicy	i-054197bb12d401810	iam.amazonaws.com	AccessDenied	AwsApiCall
AttachGroupPolicy	i-054197bb12d401810	iam.amazonaws.com	AccessDenied	AwsApiCall
AttachGroupPolicy	i-054197bb12d401810	iam.amazonaws.com	AccessDenied	AwsApiCall
AttachGroupPolicy	i-054197bb12d401810	iam.amazonaws.com	AccessDenied	AwsApiCall
AttachGroupPolicy	i-054197bb12d401810	iam.amazonaws.com	AccessDenied	AwsApiCall
CreateGroup	i-054197bb12d401810	iam.amazonaws.com	AccessDenied	AwsApiCall
ListBuckets	i-054197bb12d401810	s3.amazonaws.com	-	AwsApiCall

图 2 CloudTrail 日志

由图 2 可知，由于 IAM 角色权限有限，类似“CreateGroup”“CreateUser”等敏感操作都被拒绝。AWS 的 IAM 权限模型采用的是 ABAC，即基于属性的访问控制（ABAC），它基于属性来定义权限。在实际操作中，这

些属性也叫作标签，通过在权限策略中添加标签字段，实现对资源的动态权限管理。但不论是 AWS 的 ABAC，还是 Azure 的 RBAC，一般云厂商的权限逻辑都认为拒绝操作优先于允许操作，因此合理分配 IAM 角色权限，可以很大程度地减小实例沦陷后的危害。

但不幸的是，此次事件中由于 IAM 角色配置不当，攻击者可以获取较多的信息。

发现——AWS

常见 AWS 云服务资源的信息收集思路，主要包括以下几种方式：

1. 在 Lambda 函数代码和环境变量中收集信息：函数代码和环境变量中可能包含其他 IAM 角色的凭证信息，使得攻击者获取更高权限。

2. 在 ECS Task Definitions 中收集信息：ECS Task Definition 中包含容器在启动时运行的命令信息、租户运行任务时使用的 IAM 角色信息等。

3. 在 S3 存储桶中收集信息：S3 是 AWS 的对象存储服务，从过去发生的一些 S3 存储桶数据泄露事件可知，用户可能会利用 S3 存储一些敏感信息，包括敏感凭证、日志文件等，都可能为攻击者提供辅助。

主要思路是在一切可存储数据、可查看配置的云服务资源中获取信息。

此次事件中攻击者利用了 Lambda 函数和 S3 存储桶服务。通过已有权限查看 Lambda 函数列表、下载函数代码，最终窃取了客户的专有软件代码以及专有密钥，造成了知识产权的损失。

针对 S3 存储桶需要说明的是：CloudTrail 并不记录存储在 S3 存储桶中的对象的数据事件，除非明确开启此类功能。在此次攻击事件中，该功能并没有开启，因此并没有记录下查看特定对象的请求信息，仅有列举存储桶列表的日志记录，如图 3 所示。

Event name	Username	Event Source	Error code	Event type
ListBuckets	i-03ca5b989cf8cc06a	s3.amazonaws.com	-	AwsApiCall
ListBuckets	i-03ca5b989cf8cc06a	s3.amazonaws.com	-	AwsApiCall
ListBuckets	i-03ca5b989cf8cc06a	s3.amazonaws.com	-	AwsApiCall
ListBuckets	i-03ca5b989cf8cc06a	s3.amazonaws.com	-	AwsApiCall

图 3 CloudTrail 日志中列出存储桶操作记录

但 Sysdig 断定攻击者遍历了存储桶用以寻找敏感数据，因为该存储桶中的 Terraform 相关文件信息在后续攻击步骤中被利用。

防御绕过——禁用 CloudTrail 日志

由于 CloudTrail 服务会记录下大部分 AWS 账户日志，因此在攻击 AWS 时攻击者往往会考虑绕过该服务的检测。在考虑如何规避 CloudTrail 时，需要先了解清楚该服务的运行详情。

通过查看 AWS 官方文档了解到，CloudTrail 服务是默认启用的，AWS 用户可以免费查看最近 90 天的事件记录。通过以下命令可以查看 CloudTrail 的监视范围，结果如图 4 所示。

aws cloudtrail describe-trails

```
{
    "trailList": [
        {
            "IncludeGlobalServiceEvents": true,
            "Name": "cloudgoat_trail",
            "S3KeyPrefix": "cloudtrail",
            "TrailARN": "arn:aws:cloudtrail:us-west-2:[redacted]:
trail/cloudgoat_trail",
            "LogFileValidationEnabled": true,
            "IsMultiRegionTrail": false,
            "HasCustomEventSelectors": false,
            "S3BucketName": "867817072204441829549121249332282322911
4175143969632541 8",
            "HomeRegion": "us-west-2"
        }
```

图 4 CloudTrail 监控配置

其中，“IsMultiRegionTrail”字段代表是否将监视所有区域，true 代表是，false 代表仅监视单区域；“S3BucketName”代表将 CloudTrail 日志写入 S3 存储桶。

然后了解到常见的绕过方式主要有以下两种 [3]：

1. 中止 CloudTrail 服务

使用以下命令中止日志记录：

aws cloudtrail stop-logging --name awscloudtrail-example

当完成攻击后，重新启动日志服务：

aws cloudtrail start-logging --name awscloudtrail-example

2. 删除 CloudTrail 服务

删除 trails 或者删除存储日志的存储桶：

aws cloudtrail delete-trail --name awscloudtrail-example

此种方法较为“高调”，会使 CloudTrail 服务处于宕机状态，同时删除存储桶后会在管理控制台弹窗提示，如图 5 所示。

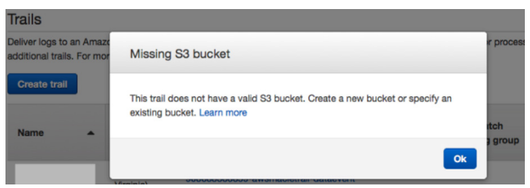


图 5 CloudTrail 控制台弹窗

同时 AWS 的另一个监控服务 GuardDuty 也会对 CloudTrail 服务的异常状态发出警报，因此并非攻击者的首选。

4. 区域绕过

当 CloudTrail 服务仅监视个别区域时，可以在监视区外的区域对实例进行操作，绕过监控；或者利用 include-global-service-events 标签关闭全球服务，命令如下：

aws cloudtrail update-trail --name my-trail --no-include-global-service-events

此次攻击活动中，攻击者采用了第一种方案进行规避，为调查取证提供了阻碍。在实际给应用程序分配 IAM 角色时，禁用或删除安全日志的权限对于程序来说是不必要的，因此说明了合理分配权限与权限审查的重要性。

凭据访问——Terraform 状态文件

Terraform 是一个开源的基础设施即代码（IaC）工具，用于部署、改变或创建云环境中的基础设施。

为了让 Terraform 知道哪些资源在其控制之下，以及何时更新和销毁它们，它默认使用一个名为 terraform.tfstate 的状态文件。当 Terraform 在持续集成 / 持续交付（CI/CD）管道中被集成和自动化时，该状态文件需要以适当的权限被访问。特别是，运行管道的服务主体需要能够访问保存状态文件的存储账户容器。这使得像 AWS S3 这样的共享存储成为保存状态文件的完美候选。

然而，Terraform 状态文件中可能包含凭证信息。

在上述攻击步骤中，攻击者有权限列出可用的存储桶并检索所有的数据。在事件调查期间，Sysdig 尝试用不同的工具来检索数据，

验证了在 S3 存储桶内的 terraform.tfstate 文件中可以找到明文 IAM 用户凭证信息，如图 6 所示。

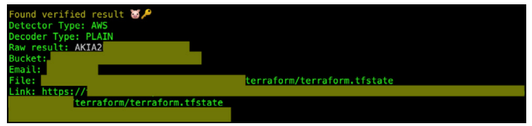


图 6 S3 存储桶中的 terraform.tfstate 文件

横向移动——AWS 账户

通过上述手段获得新凭证后，攻击者重复信息收集和横向移动操作，尝试以新凭证权限获得额外的资源。但后续的操作并没有主动规避 CloudTrail 服务的意识，导致 CloudTrail 记录了新凭证对应的可疑活动，如图 7 所示。

Event name	Event source	Error code	Event type
ListGroups	iam.amazonaws.com	AccessDenied	AwsApiCall
PutUserPolicy	iam.amazonaws.com	AccessDenied	AwsApiCall
AttachUserPolicy	iam.amazonaws.com	AccessDenied	AwsApiCall
ListUsers	iam.amazonaws.com	AccessDenied	AwsApiCall
ListUsers	iam.amazonaws.com	AccessDenied	AwsApiCall
ListUsers	iam.amazonaws.com	AccessDenied	AwsApiCall
GetUser	iam.amazonaws.com	AccessDenied	AwsApiCall
GetCallerIdentity	sts.amazonaws.com	-	AwsApiCall

图 7 CloudTrail 记录了新凭证的攻击行为

由图 7 可知，攻击者尝试了“ListGroups”“ListUsers”“AttachUserPolicy”等操作，但都因缺乏权限而失败。

5. 总结与思考

SCARLETEEL 事件始于一个易受攻击的 Pod，攻击者通过信息收集获取到了 AWS IAM 用户凭证信息，从而横向移动至 Lambda 服务、S3 存储桶服务，最终窃取了客户的专有软件。

从 Sysdig 调查分析的攻击行为来看，此次事件涉及的云上攻击者的攻击思路较为灵活，基本包括了常见的攻击技术并能够应用至攻击活动中，但在过程中也难免会“存在疏忽”导致留下更多痕迹。

该攻击活动真实地说明了网络安全是一项复杂的系统工程，每个环节都应做到最佳防护，防止出现“牵一发而动全身”的影响。尤其是此次攻击活动中最为突出的两个问题：最小权限原则和威胁检测机制。若在分配角色权限过程中能够遵循最小化原则并定期进行权限审查，攻击者难以横跨至云服务资源中从而获取更多信息，也难以绕过日志监控系统，可能会留下更多的攻击痕迹。而强大的威胁检测机制则可以在攻击者进一步深入之前给出警报信息，帮助客户及时止损。

参考文献

[1] https://news.sophos.com/en-us/2022/11/29/the-reality-of-smb-cloud-security-in-2022/.

[2] https://sysdig.com/blog/cloud-breach-terraform-data-theft/.

[3] https://rzepsky.medium.com/playing-with-cloudgoat-part-2-fooling-cloudtrail-and-getting-persistence-access-6a1257bb3f7c.

网络安全政策导读（2023年4-5月）

绿盟科技 总体技术部 林涛 张文辉

栏目说明：

本专栏基于绿盟科技团队在网络安全政策法规方面的日常跟踪，筛选国内外近期热点政策法规文件，并重点结合网络安全产业发展，对其内容和影响等进行分析。

本期选取并分析 2023 年 4—5 月国内外发布的热点政策法规。

限于篇幅，本栏目内容做了删减，如需全文请参阅绿盟科技和网安罗盘公众号。

国内篇

1. 国家互联网信息办公室就《生成式人工智能服务管理办法（征求意见稿）》公开征求意见，强化生成式 AI 监管

【内容概述】2023 年 4 月 11 日，国家互联网信息办公室发布关于《生成式人工智能服务管理办法（征求意见稿）》公开征求意见的通知（以下简称《征求意见稿》）。《征求意见稿》共 21 条，旨在促进生成式人工智能健康发展和规范应用。

【导读分析】本次发布的《征求意见稿》与此前人工智能相关规范文件相比，具有三个显著特点。一是规范对象的具体化，《征求意见稿》聚焦“生成式人工智能产品”这一特定对象提出了具体的监督管理举措，与此前的文件形成互补。二是突出保发展、促成长的主旨，这一特点充分体现在突出服务提供者主体义务、对法律责任做出原则性规定等方面。三是提出了“准入 + 义务 + 责任”的新型监管模式：在“准入”方面以“安全评估”“算法备案”为基本要求；在“义务”方面，提出了技术、服务、客户管理三类主要义务；在“责任”方面，主要明确了法律责任的依据。当然，《征求意见稿》对于生成式人工智能产品和服务管理的覆盖范围、关键环节、潜在风险等是否完善，仍是目前各界研究和讨论的热点。

2. 国家互联网信息办公室等五部门联合发布《关于调整网络安全专用产品安全管理有关事项的公告》，启动网络安全专用产品统一检测认证工作

【内容概述】2023 年 4 月 17 日，国家互联网信息办公室、工业和信息化部、公安部、财政部和国家认证认可监督管理委员会五部门联合发布《关于调整网络安全专用产品安全管理有关事项的公告》（以下简称《公告》）。《公告》旨在加强网络安全专用产品安全管理，推动安全认证和安全检测结果互认，避免重复认证、检测。

【导读分析】对于开展“网络安全专用产品”统一检测认证工作，《公告》做出的“破旧”“立新”两方面规定尤其值得关注。

在“破旧”方面。一是规定停止执行《关于调整信息安全产品强制性认证实施要求的公告》和《财政部 工业和信息化部 质检总局 认监委关于信息安全产品实施政府采购的通知》两个文件；二是规定停止颁发《计算机信息系统安全专用产品销售许可证》。

在“立新”方面。一是明确了实施统一检测认证的主要标准依据为《信息安全技术 网络安全专用产品安全技术要求》（该标准为国家强制标准，将于 2023 年 7 月 1 日正式生效）；二是明确了两

个重要目录 / 名录，即《网络关键设备和网络安全专用产品目录》《承担网络关键设备和网络安全专用产品安全认证和安全检测任务机构名录》。

3. 全国人大常委会印发《中华人民共和国反间谍法》，强化涉网管理和规范

【内容概述】2023 年 4 月 26 日，全国人民代表大会常务委员会正式通过修订后的《中华人民共和国反间谍法》（以下简称《反间谍法》），自 2023 年 7 月 1 日起施行。《反间谍法》共 6 章 71 条，旨在加强反间谍工作，防范、制止和惩治间谍行为，维护国家安全。

【导读分析】修订后的《反间谍法》增加了多项与网络安全相关的内容，包括以下三部分：一是该法新增“网络攻击、侵入、干扰、控制、破坏等活动”为间谍行为，表明网络安全已逐步成为影响国家安全的重要因素；二是该法将持有国家秘密的“文件、数据、资料、物品”等列为窃密对象和调查对象，表明数据或将成为未来各国争夺的重要战略资源；三是该法要求重点单位“加强对要害部门部位、网络设施、信息系统的反间谍技术防范”，并对“涉及间谍行为的网络信息内容或者网络攻击等风险”进行通报和处置，表明对重点单位的网络安全监管态势趋严。

4. 交通运输部发布《公路水路关键信息基础设施安全保护管理办法》，为我国首个行业级关基保护专项规章

【内容概述】2023 年 5 月 6 日，交通运输部发布《公路水路关键信息基础设施安全保护管理办法》（以下简称《管理办法》）。《管理办法》共 6 章 33 条，旨在保障公路水路关键信息基础设施安全，落实公路水路关键信息基础设施的安全保护和监督管理工作。

【导读分析】《管理办法》在《公路水路关键信息基础设施安全保护管理办法（征求意见稿）》的基础上，进一步完善了公路水路关键信息基础设施安全保护制度体系。修改完善之处主要包括三方面：一是关键基础设施分层保护制度，由交通运输部及省级人民政府交通运输主管部门分别对部级设施和省级设施承担保护责任；二是运营者的供应链安全保护制度，新增“鼓励运营者从已通过云计算服务安全评估的云计算服务平台中选择采购云计算服务”；三是运营者的个人信息和数据安全保护制度，要求运营者“将在我国境内运营中收集和产生的个人信息和重要数据存储在境内，确需向境外提供数据的，应当按照国家相关规定和标准进行安全评估”等。

5. 国务院印发《商用密码管理条例》，全面强化商密管理重要制度体系

【内容概述】2023 年 5 月 24 日，中华人民共和国国务院修订通过了《商用密码管理条例》（以下简称《条例》），自 2023 年 7 月 1 日起施行。《条例》共 9 章 67 条，旨在规范商用密码应用和管理，鼓励和促进商用密码产业发展。

【导读分析】从内容对比来看，《条例》主要有三方面修订。一是优化商用密码监管方式，包括由原《条例》规定的全面严格管控，调整为以重点制度强化对关键环节的重点把控，管理方式由重事前审批转为加强事前、事中、事后的全周期监管；二是强化商用密码检测认证，以此严守产品服务的“入口关”，包括推进商用密码检测认证体系建设、明确商用密码检测和认证机构资质规范、对使用网络关键设备和网络安全专用产品的商用密码服务等实行强制性检测认证制度等；三是加强商用密码进出口管理，包括明确商用密码实施进出口管理的范围、对商用密码实行进口许可清单和出口管制清单管理等。

6. 国家互联网信息办公室发布《个人信息出境标准合同备案指南（第一版）》，标志个人信息出境标准合同备案工作实际启动

【内容概述】2023 年 5 月 30 日，国家互联网信息办公室发布《个人信息出境标准合同备案指南（第一版）》（以下简称《备案指南》）。《备

案指南》旨在落实《个人信息出境标准合同办法》（以下简称《合同办法》），指导和帮助个人信息处理者规范、有序备案个人信息出境标准合同。

【导读分析】作为《合同办法》出台后的首个配套实操文件，从内容来看，《备案指南》对适用范围、申报材料等方面的细化规定，表明在个人信息出境的监管导向上，具有趋严的管理特征。

与此同时，《备案指南》的发布也预示着，个人信息出境标准合同备案工作已在监管侧及运营侧均准备就绪，相关管理工作已进入实际启动实施阶段。

国外篇

1. 美国 CISA 发布《零信任成熟度模型》（第二版），完善国土安全领域零信任实施规范

【内容概述】2023 年 4 月 11 日，美国网络安全与基础设施安全局（CISA）发布了《零信任成熟度模型》（第二版）（*Zero Trust Maturity Model Version 2.0*）（以下简称《零信任模型 2.0》）。《零信任模型 2.0》是支持美国联邦政府机构向零信任架构过渡的方式之一，旨在帮助美国联邦机构评估和改进其零信任安全策略和实践的水平，提高其安全防护能力和减轻可能面临的风险。

【导读分析】美国国土安全部发布的零信任相关政策战略和标准规范，在具体内容和实施方式上均有值得我们借鉴之处。例如，美国对零信任划分不同发展阶段，并以“功能支柱”的形式，对各阶段零信任发展目标水平做出明确分解，这种标准架构方式可以为我国零信任标准体系的构建提供参考。此外，该标准所提到的一些关键技术点，也可以成为我们开展零信任技术攻关、产品方案研发等工作可供参考的发展方向，如可见性分析、自动化和编排、网络弹性等。

2. 欧盟委员会发布《欧盟网络团结法案》，强化欧盟网络安全基本主张

【内容概述】2023 年 4 月 18 日，欧盟委员会提出了《欧盟网络团结法案》（*EU Cyber Solidarity Act*）（以下简称《团结法案》）提案，《团结法案》旨在加强欧盟对重大网络安全威胁和攻击的准备、检测和响应能力，同时加强现有的合作机制。

【导读分析】从本提案可以看出欧盟在对待网络安全方面的几个基本主张和态度。一是注重技术防御，从“网络盾”的设置和运营模式不难发现，欧盟在网络安全防护体系建设中，较强调先进技术在网络安全中的融合应用，如人工智能等。二是重视强调监管，尽管欧美一贯宣扬网络自由观念，但实际上也在持续部署各种监管和审查手段，如本次法案所提出的网络安全事件审查制度等。三是看重公私合作，这一点在创建欧盟网络安全后备军、强化网络安全应急机制等方面体现得淋漓尽致。四是开展集体防御，这可以视为欧洲集体防御政策在网络安全领域的延伸，以夯实成员国之间的协同，促进欧洲的区域网络安全防护体系不断走向健全。

3. 美国白宫发布《关键和新兴技术的国家标准战略》，巩固和加强技术竞争力

【内容概述】2023 年 5 月 4 日，美国白宫发布了《关键和新兴技术的国家标准战略》（*National Standards Strategy for Critical and Emerging Technology*）（以下简称《战略》）。《战略》旨在加强美国在对国家安全和经济发展至关重要的先进技术的领导地位，提升在国际标准制定中的竞争力。《战略》提出了需要重点关注的技术领域，如通信和网络技术、先进计算、半导体和微电子、人工智能、先进网络传感与签名管理、量子信息技术等。

【导读分析】从《战略》中，我们可以得到三个方面的思考启示。一是标准不仅是规范和促进技术发展的手段，更是开展技术竞争的重要阵地，技术标准领域的国际话语权，已经成为当前反映各国技术创新竞争力的核心指标之一。二是标准战略并非仅限于技术本身，而是涵盖与技术相关的诸多关键要素，并且这些要素对于标准的发展往往具有更加重要的决定作用，例如《战略》所强调的投资、合作、人才等。三是美国作为全球领先的技术强国，其技术

标准战略对我国有重要参考意义，如《战略》所提出的重点技术框架及其关键技术方向，包括半导体和微电子、人工智能等，已经或正在引领着全球技术创新和变革的方向。对此，我们不仅需要加强布局和储备，更可以从中寻求可以实现换道超车的潜在机会。

4. 美国白宫科技政策办公室发布 2023 版《国家人工智能研发战略计划》，优化 AI 研发方向

【内容简介】2023 年 5 月 23 日，美国白宫科技政策办公室（National Science and Technology Council）发布了 2023 版《国家人工智能研发战略计划》（*National Artificial Intelligence Research and Development Strategic Plan 2023 Update*）（以下简称 2023 版《战略计划》）。该计划旨在确保美国在开发和使用可信人工智能系统方面继续处于领先地位，并为整合所有联邦部门的 AI 系统进行人才储备，同时协调所有联邦机构正在进行的 AI 活动。2023 版《战略计划》还明确了人工智能领域主要的研究挑战，这些挑战或成为美国联邦政府重点协调和投资的方向。

【导读分析】美国此次发布的《建议指南》，对于我国健全漏洞管理标准规范而言，有两方面的参考意义。一是以“框架”的模式，推动加强网络产品和系统漏洞相关标准的体系化发展，提升标准间的衔接与协同；二是以指南建议的方式，加强对网络产品和系统漏洞的披露规范化，确保不同部门、行业间相关漏洞披露机制、披露信息的权威性、准确性和及时性。

5. 美国 NIST 发布《对联邦漏洞披露的建议指南》，推进漏洞披露体系化建设

【内容概述】2023 年 5 月 24 日，美国国家标准与技术研究院（NIST）发布《对联邦漏洞披露的建议指南》（*Recommendations for Federal Vulnerability Disclosure Guidelines*）（以下简称《建议指南》），《建议指南》为美国联邦政府机构管理内部信息系统的漏洞披露提供了指南，并定义了联邦漏洞披露框架（Federal Vulnerability Disclosure Framework）（以下简称“披露框架”），可供美国政府建立和维护统一的漏洞披露管理流程。

【导读分析】美国此次发布的《建议指南》，对于我国健全漏洞管理标准规范而言，有两方面的参考意义。一是以“披露框架”的模式，推动加强网络产品和系统漏洞相关标准的体系化发展，提升标准间的衔接与协同；二是以指南建议的方式，加强对网络产品和系统漏洞的披露规范化，确保不同部门、行业间相关漏洞披露机制、披露信息的权威性、准确性和及时性。

6. 美国国防部提交非公开版《2023 年国防部网络战略》，彰显“以攻为守”军事网络思想

【内容概述】2023 年 5 月 26 日，美国国防部向国会提交非公开版的《2023 年国防部网络战略》（*2023 DoD Cyber Strategy*）（以下简称《2023 网络战略》），该战略强调美军将继续利用网络能力在网络空间开展行动，主动打击对手构成的网络威胁，同时明确了美军新的网络空间重点任务，包括提高国家弹性、开展网络作战、加强国际合作以及强化网军建设等。

【导读分析】《2023 网络战略》对于美国防领域网络安全发展至少会产生以下两方面影响。一方面，进一步强化“以攻为守”的网络安全策略。《2023 网络战略》体现出更强的“进攻性防御”属性，后续或将对美国国防领域网络安全的监管方式、合作路径等方面产生影响。另一方面，对产业、外交等领域的溢出效应将持续显现。《2023 网络战略》所涉及的网络安全重点领域建设方向、管理思路等，也极有可能启发其他国家，而在网络安全建设管理模式、路线和重点等方面的趋同，反过来也会强化当前的网络空间生态，进而潜移默化地强化以美国为首的国防、技术、研究乃至外交领域同盟、联盟的发展。

绿盟数据保险箱助力数据安全流转

大幅降低内部人员泄露数据的风险“可用不可见”，计算服务方无法留存用户需要计算的数据

令攻击者“进不来、看不懂、改不了、拿不走、跑不掉”

THE EXPERT
BEHIND GIANTS
巨人背后的专家

多年以来，绿盟科技致力于安全攻防的研究，为政府、金融、运营商、能源、交通、科教文卫等行业用户和各类型企业用户，提供具有核心竞争力的安全产品及解决方案，帮助客户实现业务的安全顺畅运行。在这些巨人的后面，他们是备受信赖的专家。

客户支持热线：400-818-6868

NSFOCUS 绿盟科技