资产几何？现代组织的外部攻击面

工作来源

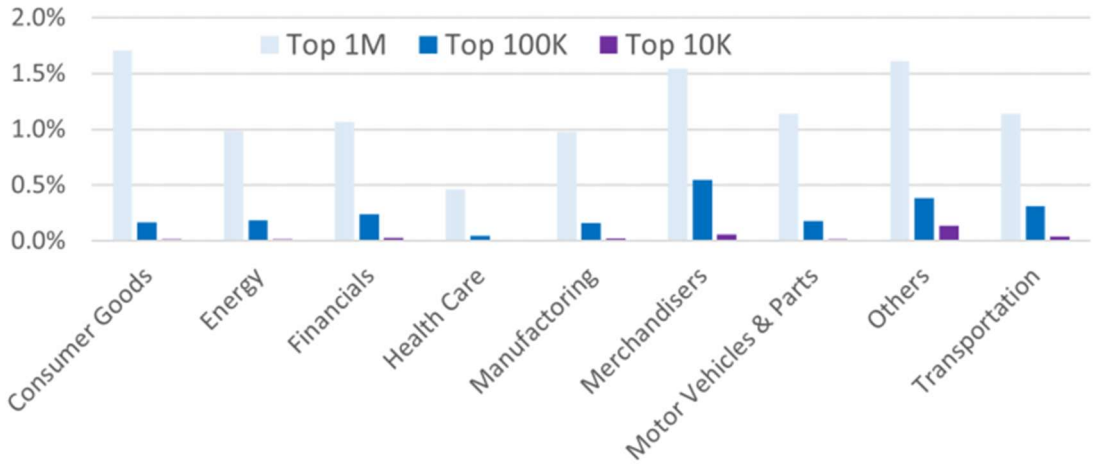
ASIA CCS 2024

工作背景

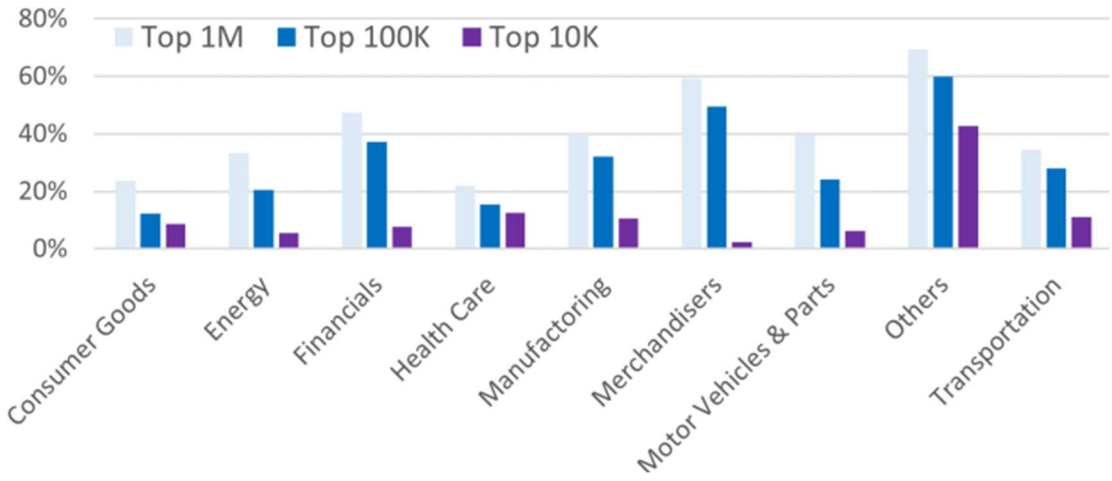
CISA 在 2022 年要求对政府的 IT 系统进行漏洞扫描，英国国家网络安全中心（NCSC）在 2022 年也计划扫描英国互联网连接的系统漏洞。由于混合云平台化以及外包等影响，获取组织完整的资产是极大的挑战，很多组织自己也不完全掌握资产情况。

由于 IPv4 地址空间有限，云服务厂商都对组织能够获得的 IP 地址做出了限制，如 Azure 每个区最多 10 个 IP、GCP 每个区最多 8 个 IP、AWS 每个区最多 5 个 IP。大量的共用现象存在，只扫描 IP 地址的前缀会遗漏掉 50% 的域名。

消费品行业也只有不到 2%在 TOP 100 万列表中：



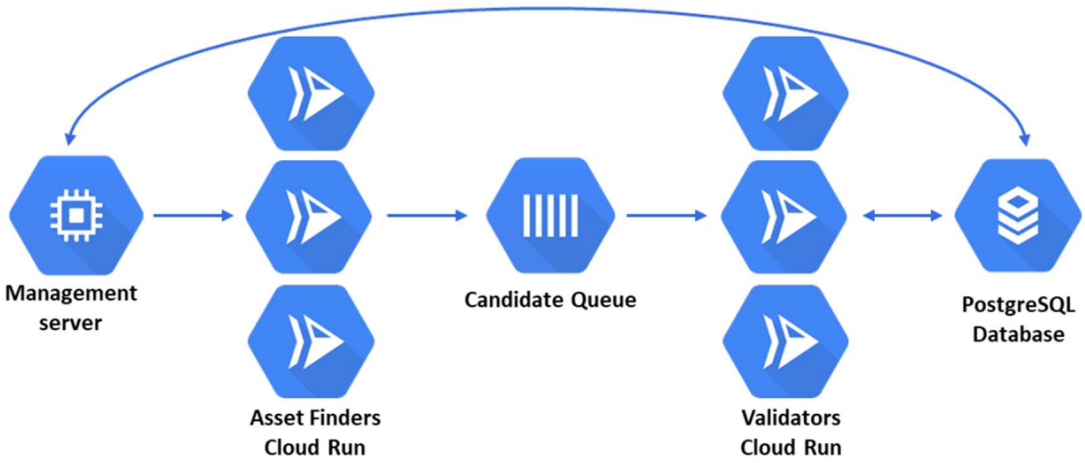
所有的 FQDN 只有大约 40% 顶级域名在 TOP 100 万列表中：



开源工具 OWASP AMASS2 依赖于精确的 whois 信息匹配，但 60.5% 的域名没有在 whois 记录中使用组织的电子邮件地址，37.3% 使用通用名称等。平均而言，一家公司为域名使用 86.8 个不同的组织名称。

工作设计

资产发现的架构如下所示：



IP 发现

查看 IP 块分配情况，与组织相关的电子邮件或者物理地址。每个组织的域名、子域名解析的 IP 前缀，检查这些 IP 块中是否存在其他非组织资产。

域名发现

多年跟踪新域名注册，创建可能与每个组织有关的域名数据库。通过计算域名特征（相关网页与应用程序、PKI、电子邮件、DNS、网络等），判断域名是否归属于该组织。例如以下三类：

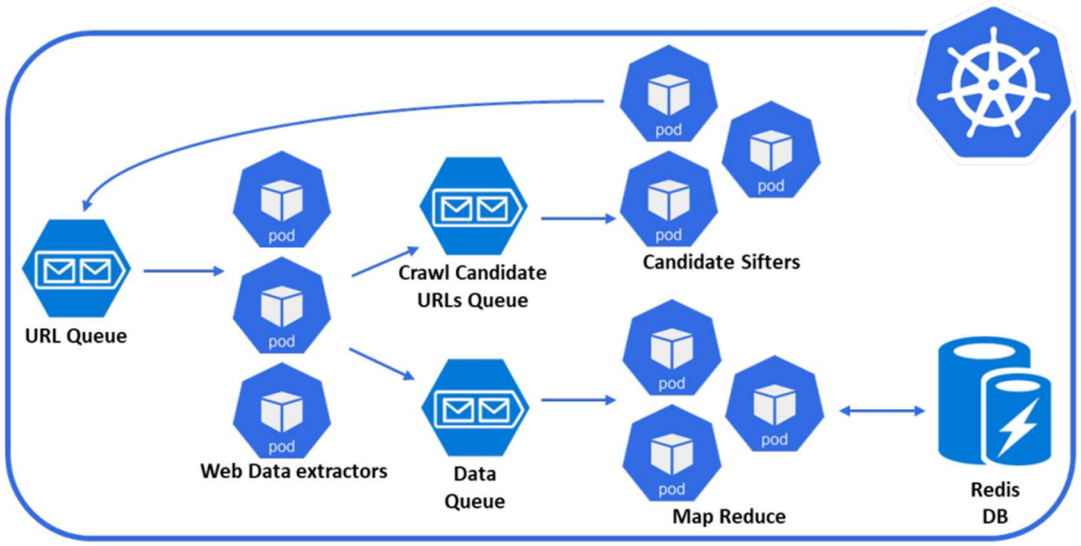
（1）直接相关。使用带有组织名称或组织徽标的证书、部署在组织的数据中心

（2）相似相关。共用相同的电子邮件服务器或者基础设施

（3）不相关。域名的电子邮件服务器未被其他已知的组织使用

子域名发现则是通用的模式，证书透明度日志、Passive DNS 日志、Web 历史日志、主动探测收集的证书和网页数据、搜索引擎数据、常用名称爆破等等。唯一需要注意的是，要避免通配符子域名的干扰。

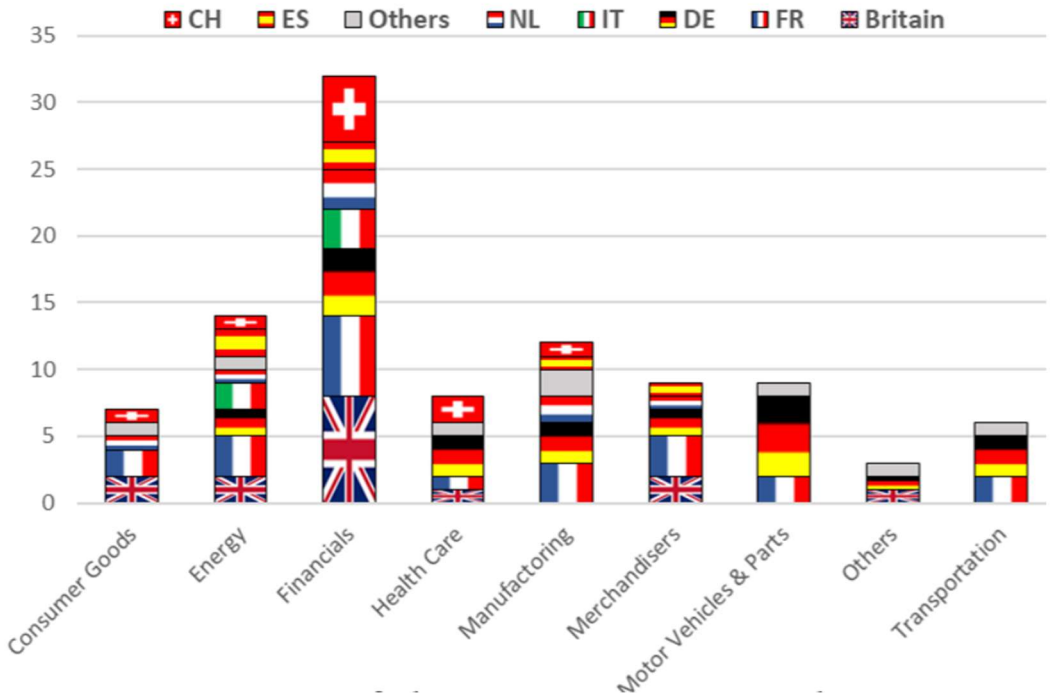
Web 爬虫的架构如下所示，分析内容安全策略（CSP）、Cookie 安全（HTTPOnly/Secure）、X-Content-Type-Options、HSTS 等。



工作准备

在欧洲五百强中选出 TOP 100，来自于欧洲 13 个国家。德国、法国和英国占比最大，合计为 63 家公司。从行业来看，金融行业占到 32 家、能源行业占到

14 家、汽车行业占到 9 家。具体就不再这里一一列举，比如壳牌石油、英国石油、大众/奔驰/宝马/标致/雷诺/沃尔沃集团、西门子、雀巢、空客、巴斯夫、拜尔、联合利华、葛兰素史克等等。



使用 Common-Crawl 定期爬取公开网站，并且购买/收集了其他数据：

- 3 亿条 whois 记录
- IANA 分配的 1 千万个 IP 地址块注册信息
- PassiveDNS 数据
- 证书透明度数据

工作评估

现代组织的资产主要分布在三块：

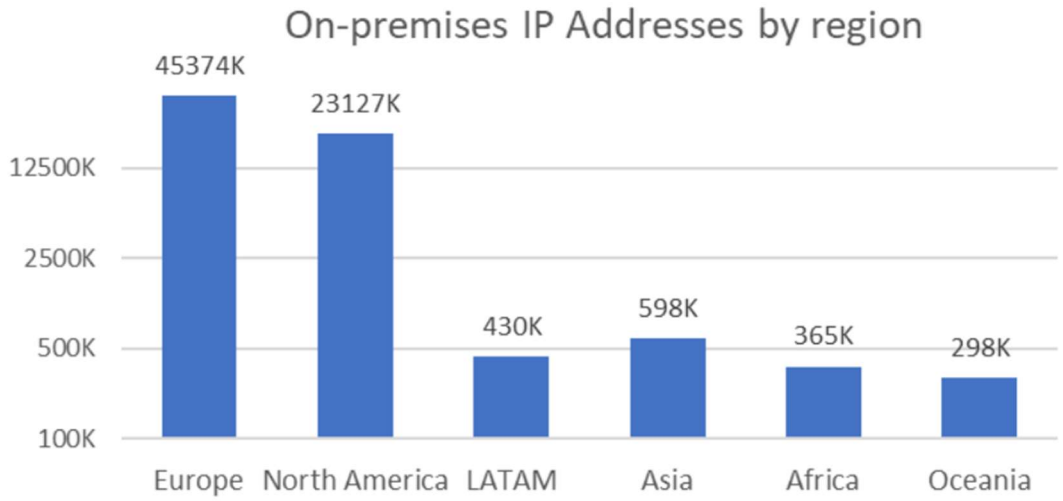
（1）直属。组织自行运营的资产，包含属于组织管理的 IP 地址。由于法规合规要求，欧洲的组织更喜欢直属资产。

（2）云上。云上资产的责任由组织和云服务商共同承担。

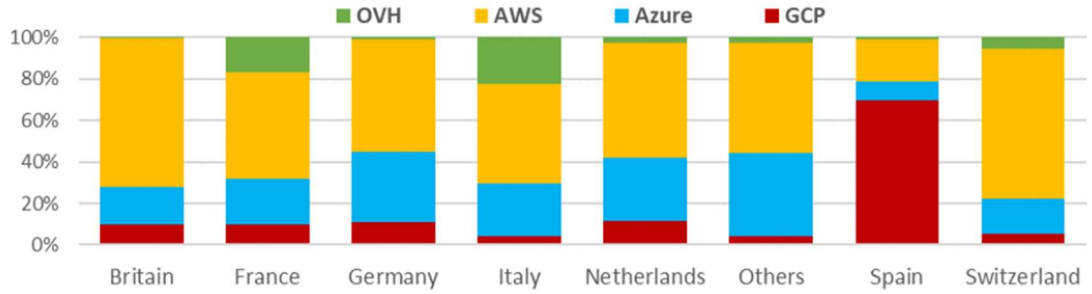
（3）外部。部署在外部非云服务商的资产，这也是分布最广的资产、攻击面最大的资产。

	Avg #Coun-tries	Avg #Net-works	#Ranked FQDNs (K)	#EU assets (K)	#North America assets (K)
On-prem/IP	20.27	190.56	129.3	45373.8	23126.8
On-prem/FQDN	6.84	18.04	129.3	157.9	37.7
External	31.28	274.5	194.2	193.9	200.1
Cloud	9.95	54.41	107.6	51.6	152.5

一共发现了 7020 万直属资产 IP 与 106 万域名，也有相当多的域名其实都未启用，只是为了品牌保护注册的。资产 IP 主要还是集中在欧洲和北美地区的：



使用的云服务商主要是 Amazon AWS（11.4 万域名）、Microsoft Azure（5.3 万域名）、Google Cloud Platform（2.6 万域名）、OVH（1 万域名）。其余云服务商，Digital Ocean 拥有 0.6 万域名、阿里云拥有 0.06 万域名。



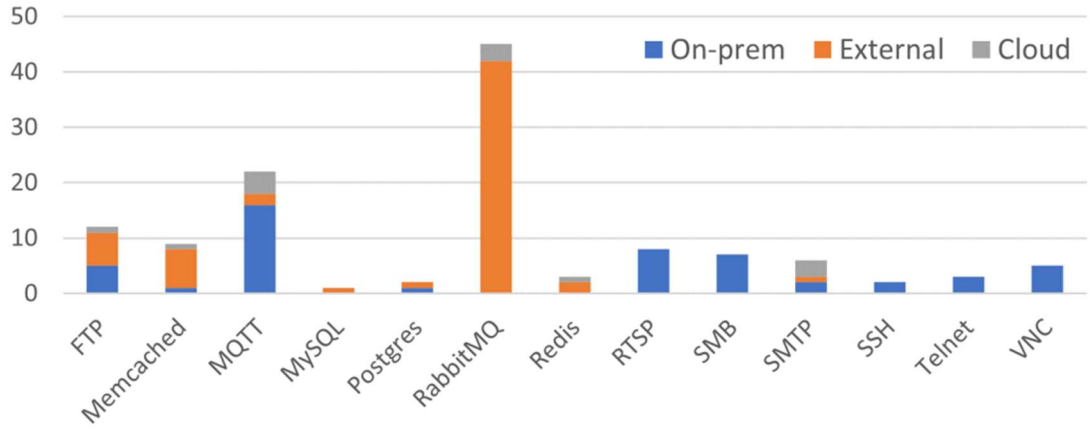
端口扫描

扫描 IP 的常见 400 端口并识别其服务，发现 35.9 万个 IP 上开放了 948.8

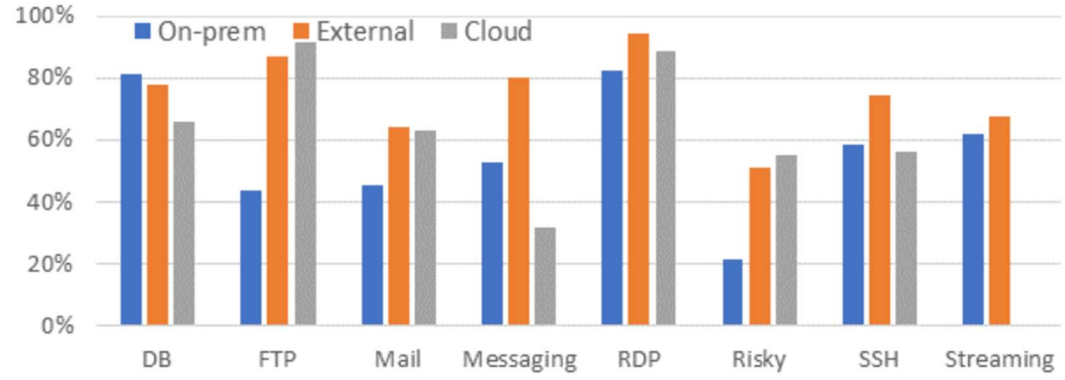
万个服务，其中 7.4 万个非 HTTP 服务。

	IPs discovered	Open ports	IPs with open ports	Active HTTP services	Active non-HTTP services	IPs with active services	% IPs with ports (/IPs)	% IPs with services (/IPs with open ports)	%HTTP services (/open ports)	%non-HTTP services (/open ports)	% active services (/open ports)
All	70412K	9488K	359K	307K	74K	212K	0.51%	59.13%	3.24%	0.78%	4.02%
External	129K	231K	45K	82K	31K	40K	35.12%	88.63%	35.56%	13.50%	49.06%
Cloud	91K	309K	43K	71K	8K	41K	47.42%	94.99%	23.04%	2.69%	25.73%
On-premise	70192K	8948K	271K	154K	35K	131K	0.39%	48.49%	1.72%	0.39%	2.11%
On-premise FQDNs	95K	397K	31K	34K	2K	24K	32.53%	76.46%	8.46%	0.40%	8.86%

一共 165 种非 HTTP 服务，如 SSH、远程桌面（RDP、VNC）、数据库（ES、Redis）、FTP、Risky（SMB、Telnet）、邮件（SMTP、IMAP、POP3）、IoT（RTSP）、消息传递（MQTT、RabbitMQ）。这些服务的弱口令情况如下所示：



暴力破解情况如下所示：



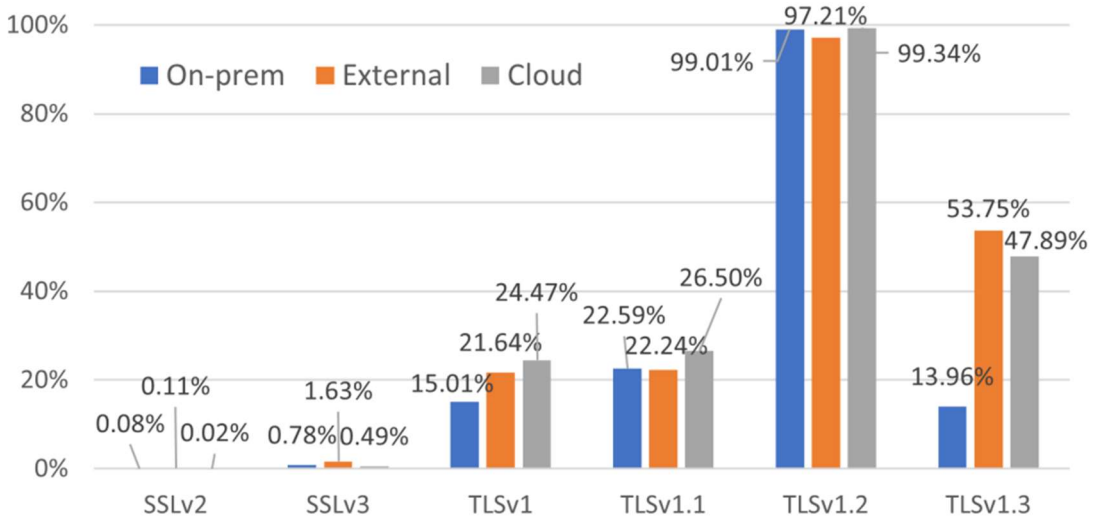
直属资产 IP 地址大多没有绑定域名，绑定的只占 0.13%。绑定域名解析的，更有可能存在开放服务。HTTP 服务更有可能使用域名，HTTP 服务中存在解析的占比 21.84%，相比非 HTTP 服务 4.54% 高得多。

PKI 验证

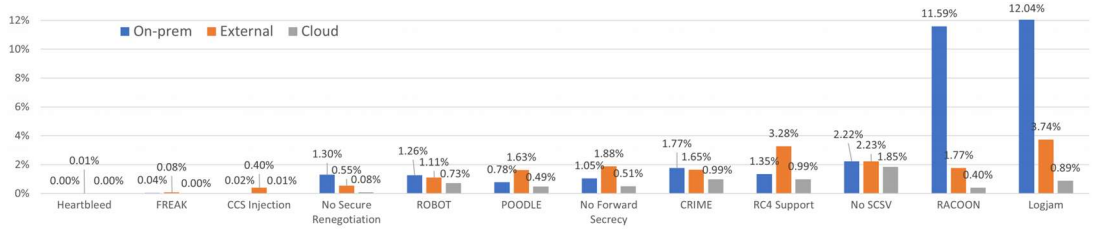
对 106 万域名都进行了握手和证书分析，查看是否会受到典型漏洞（CRIME、

FREAK、Logjam、POODLE、RACOON、CCS 注入、Heartbleed 等) 的影响。

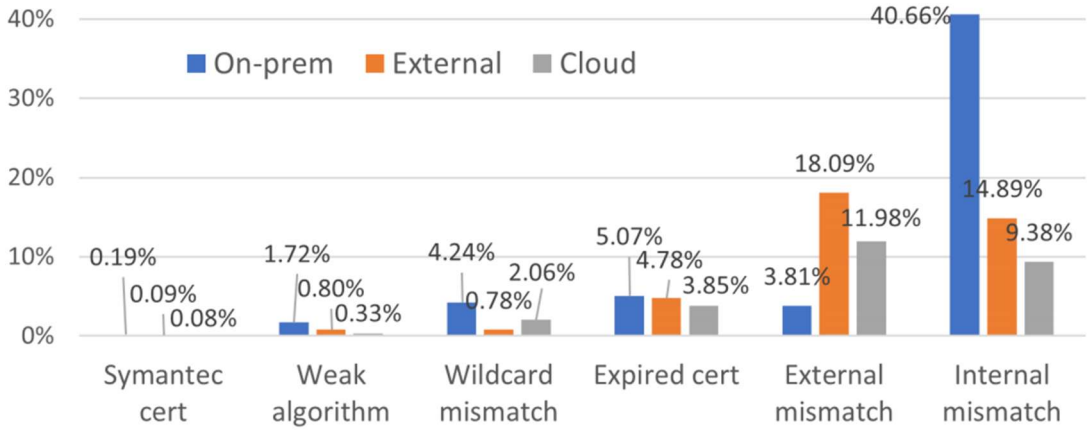
证书的上下文，包括弱算法、过期证书、域名不匹配等，也包含在考虑范围内。



可以看到，被弃用的 TLS 1.0 与 1.1 版本仍然被广泛使用中。当然，这有可能是外部服务提供商和云服务提供商都要支持旧服务和旧设备，毕竟无法强制要求客户使用新版本。



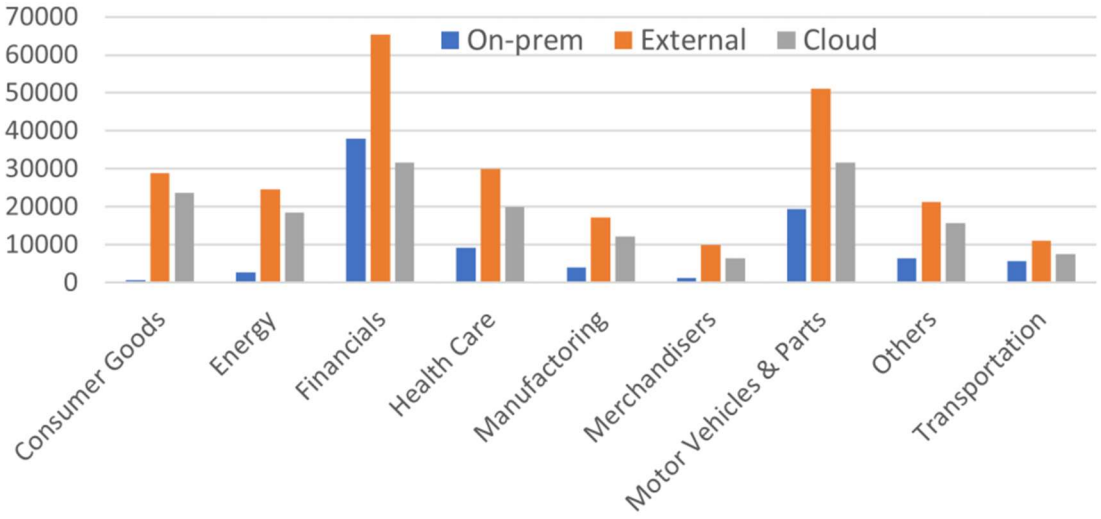
云环境中 PKI 安全状态明显要更好，易受攻击的比例较低。对于不可利用的漏洞，组织缺乏修复或缓解的动力。



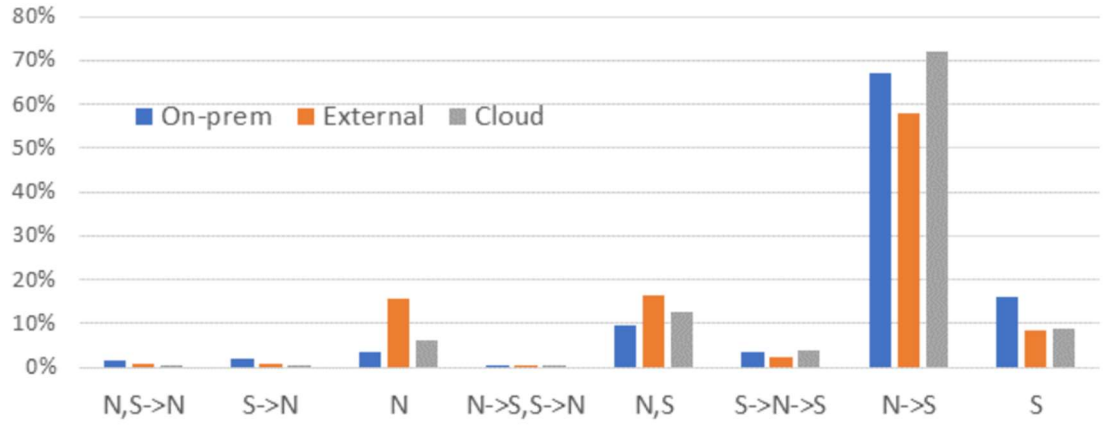
无效证书中，直属资产中也存在外部域名不匹配（3.81%）的情况。分析发现主要在金融和汽车行业，大多是在内部使用合作伙伴或者供应商的服务。云上资产相比外部资产问题更小的原因，估计是外部资产的服务往往老旧，而云上资产的服务相对较新。

Web 安全

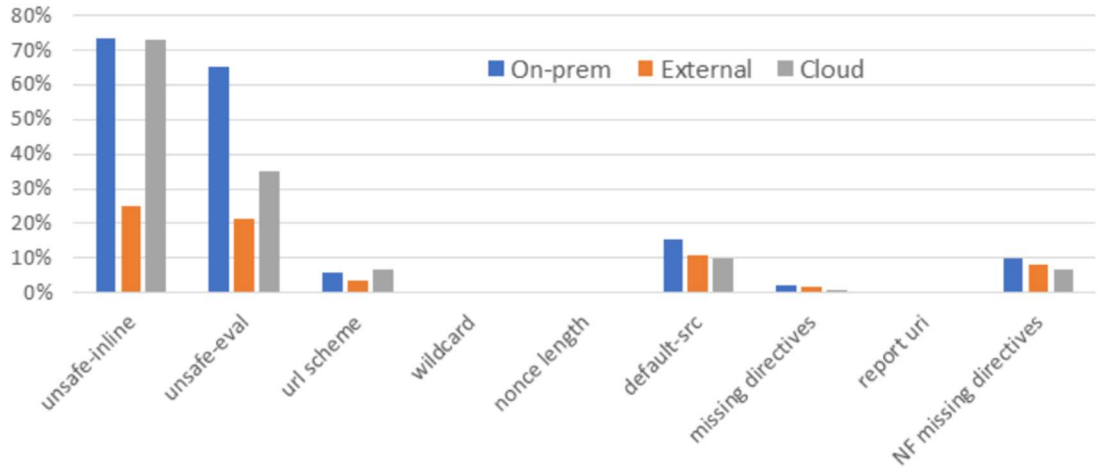
一共发现了 51.4 万个 HTTP 服务，各行业的使用依赖情况并不相同。平均直属资产有 17%，但具体到消费行业只有 1.1%，而金融行业又有 28.1%。金融行业是唯一一个直属资产多于云资产的行业，这也受到历史积累与法律法规的影响。



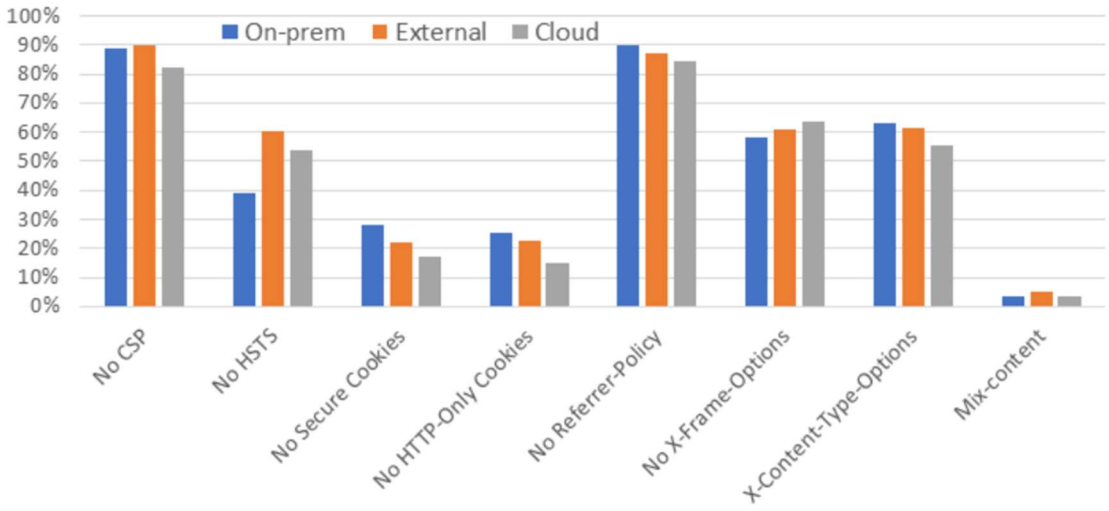
15.6% 的外部资产只能通过 HTTP 加载，可能有些资产短时间用过后就被遗忘了：



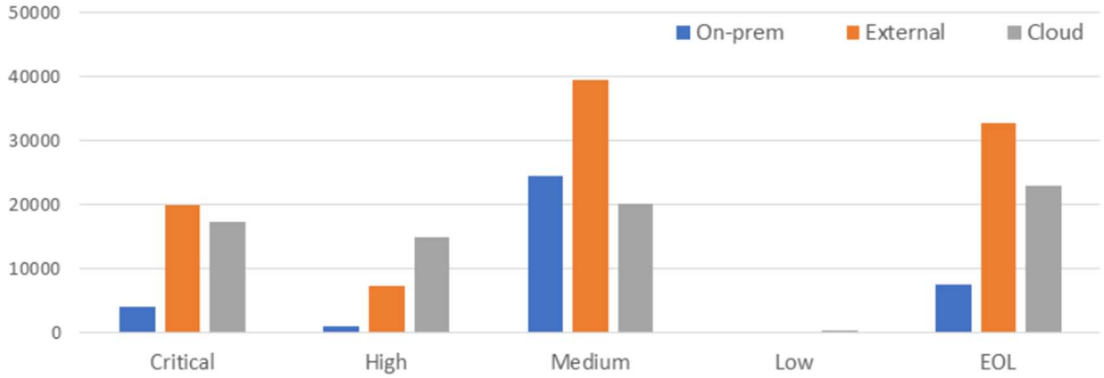
直属资产中存在大量 CSP 错误配置，云上资产也遑不多让。外部资产表现这么好的情况，可能是由于运行时间短、复杂度低，往往不需要更改。



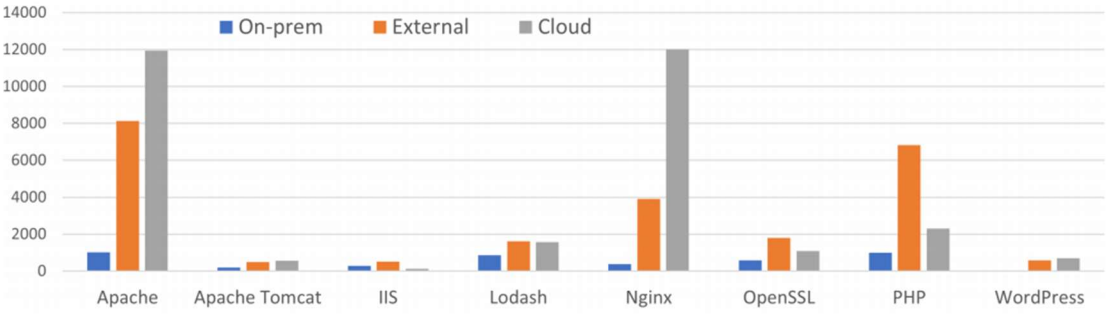
各类资产最佳实践的分布情况如下所示。需要用户主动操作的最佳实践，云上资产差距往往较大。



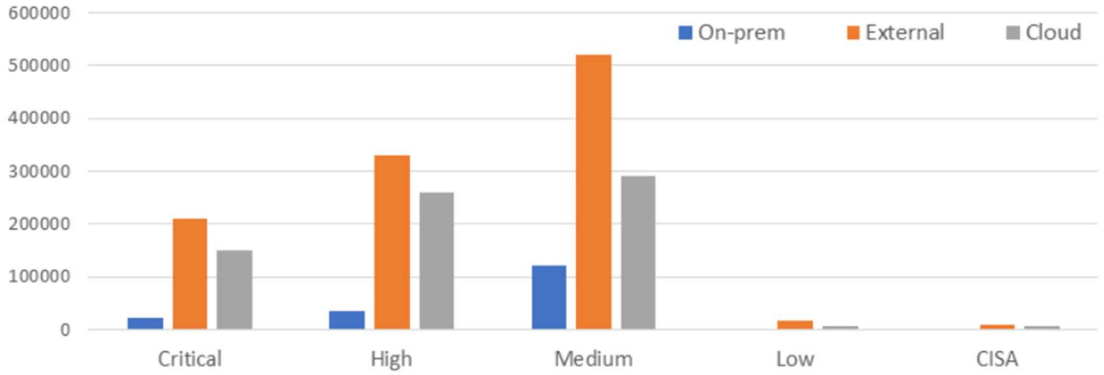
根据软件版本查看服务存在漏洞情况，外部资产和云上资产的漏洞要比直属资产多得多。直属资产可能更被安全团队所重视，投入了更多资源与精力。



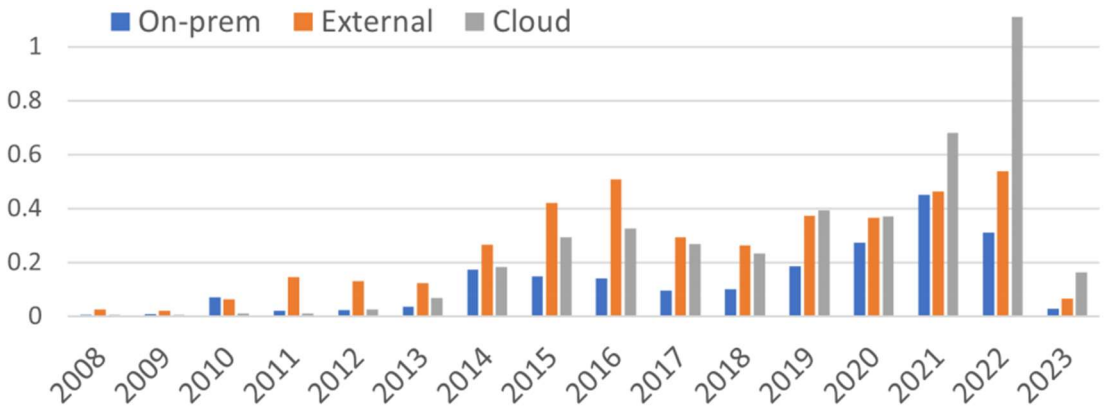
毫不意外，Apache、Nginx 与 PHP 的高危漏洞数量是最多的。



尽管看起来漏洞那么多，但被 CISA 标记为已知易受攻击的漏洞却很少。尤其是直属资产，此类漏洞几乎不存在。

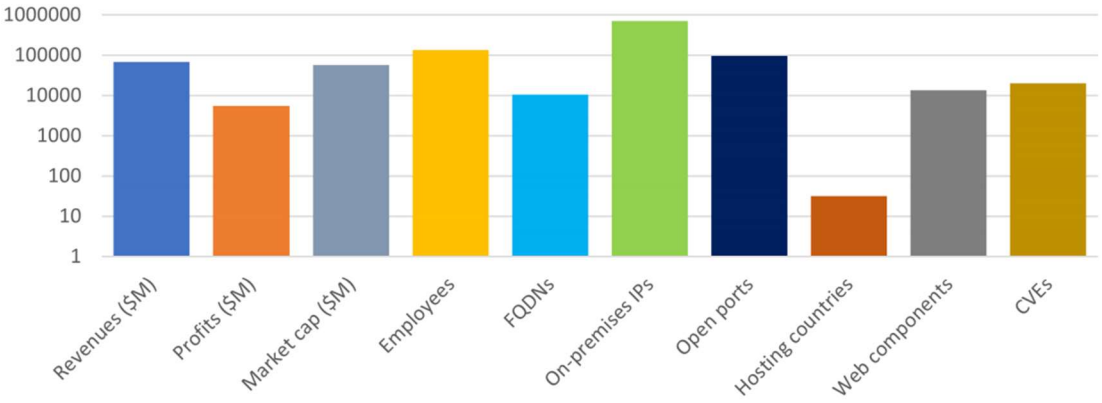


云上资产往往使用的软件版本更新，外部资产使用的软件版本是最老的：



工作思考

欧洲一百强的平均营收接近 1000 亿美元、平均利润接近 100 亿美元、平均市值接近 1000 亿美元。平均每个公司拥有 10 万个员工、1 万个域名、100 万个 IP、10 万个开放端口、1 万个 Web 组件、1 万个漏洞。



对不同行业来说，问题如下所示。在医疗和能源行业，云上资产是最薄弱的地方。在制造业等其他行业，通常都是直属资产最脆弱。

行业	直属资产	外部资产	云上资产
消费	旧组件存在漏洞，特别是 CISA 列表中的漏洞	※大量开放非 HTTP 服务	旧的/被遗忘的/无人管理的 PKI
能源	SSL/TLS 协议与漏洞	大量开放非 HTTP 服务	※大量开放非 HTTP 服务，且许多组件存在高危漏洞
金融	※大量开放 FTP/SSH 服务，以及旧的/被遗忘的/无人管理的 PKI	旧的/被遗忘的/无人管理的 PKI/HTTP	许多组件存在高危漏洞
医疗	旧的/被遗忘的/无人管理的 PKI	不安全的 HTTP 访问	※许多组件存在高危漏洞，特别是 CISA 列表中的漏洞
制造	※大量开放非 HTTP 服务	大量开放非 HTTP 服务	大量开放非 HTTP 服务
贸易	TLS 版本太旧，存在漏洞较多	※大量开放非 HTTP 服务，不安全的 HTTP 访问	旧的/被遗忘的/无人管理的 PKI
汽车	旧的/被遗忘的/无人管理的 PKI	※大量开放非 HTTP 服务，旧的/被遗忘的/无人管理的 PKI/HTTP	大量开放非 HTTP 服务
运输	开放 IoT 等流服务	※许多组件存在高危漏洞，特别是 CISA 列表中的漏洞	

随着我国综合国力的提高，世界五百强中公司数量已经达到了世界第一。与这个

工作类似的，中国一百强的外部攻击面情况如何？组织自己能完全掌握自己资产的情况吗？