格物实验室
NSFOCUS GEWU LAB

NSFOCUS

2020
互联网安全事件观察报告

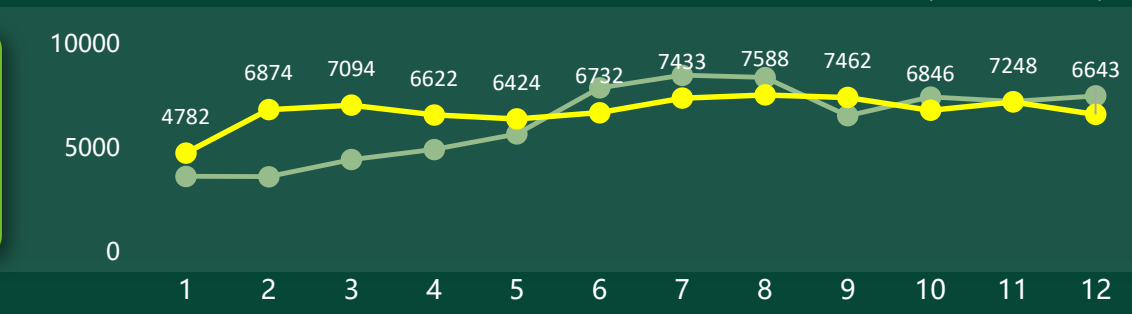
绿盟科技威胁响应中心

前提概要

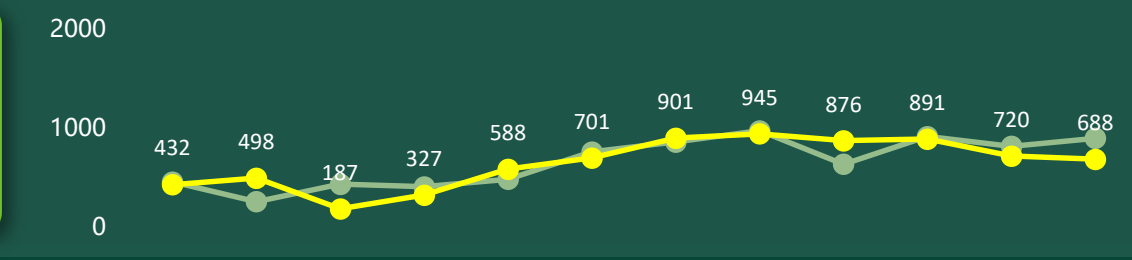
年度各类事件数量统计总览

以下数据为全年监测到的各类安全事件资讯逐月数量统计

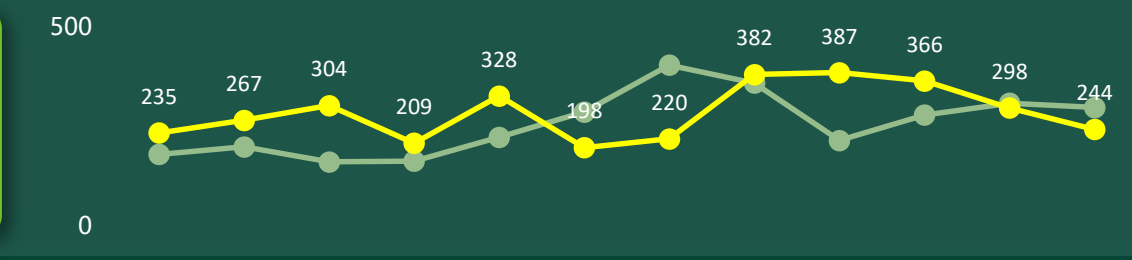
所有类别



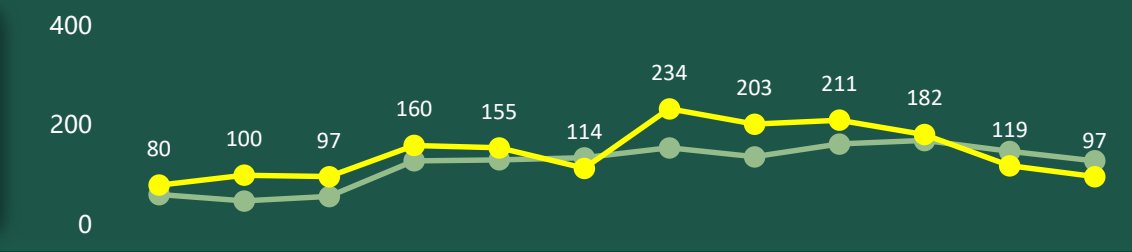
勒索软件



信息泄露



工控事件



8w+ 全年监测收集到的各类安全事件共计 81748，信息来源于各类漏洞库、国内外安全资讯网站、社交媒体等。

109 今年共发布安全通告109 篇，防护方案 11 篇。

分类 经观察全年安全事件主要有如下几类：漏洞类、勒索软件、信息泄露、工控、攻击事件及恶意软件。

年度重大安全事件 Top20

1月

- 2020 开年大洞，微软 Windows CryptoAPI 验证绕过漏洞 CVE-2020-0601
- 美天然气管道运营商遭勒索软件攻击
- 米高梅旗下酒店1070万住宿客户信息遭黑客散布
- Weblogic 多个远程代码执行漏洞
- SMBGhost，微软SMBv3远程代码执行漏洞
- Wi-Fi 漏洞 Kr00k 影响超十亿台设备
- 打着新冠疫情名义的钓鱼攻击、恶意软件传播、诈骗活动频发
- 特斯拉、波音等公司的零件制造商拒付赎金后，被窃机密遭泄露
- 委内瑞拉国家电网干线遭受攻击，造成全国大面积停电
- 视频会议软件 Zoom 重大漏洞导致数万私人视频被公开围观

6月

- Ripple20，Treck TCP/IP堆栈多个安全漏洞
- F5 BIG-IP TMUI 远程代码执行漏洞（CVE-2020-5902）
- SigRed ， Windows DNS服务器远程执行代码漏洞
- Bad Neighbor , Windows TCP/IP 远程代码执行漏洞
- Netlogon 超危提权漏洞（CVE-2020-1472）
- 工业物联网芯片制造商Advantech证实遭受勒索软件攻击，公司文件被窃。
- 超1600万巴西 COVID-19 患者个人和健康详细信息在网上暴露
- FireEye 遭网络攻击，红队工具被窃。
- 网络钓鱼活动目标锁定疫苗研发公司、新冠疫苗冷链组织
- 网络管理软件供应商 SolarWinds 遭供应链攻击，部分版本的 Orion Platform 更新文件中被植入后门

12.30

个人及企业对于高危漏洞的关注程度逐年增高，这些漏洞所能造成的直接影响已经较早些年大大降低。不过即便修复了漏洞也不能高枕无忧，有几类攻击也已活跃多年，他们产生的影响能渗透进生产生活的各个方面。

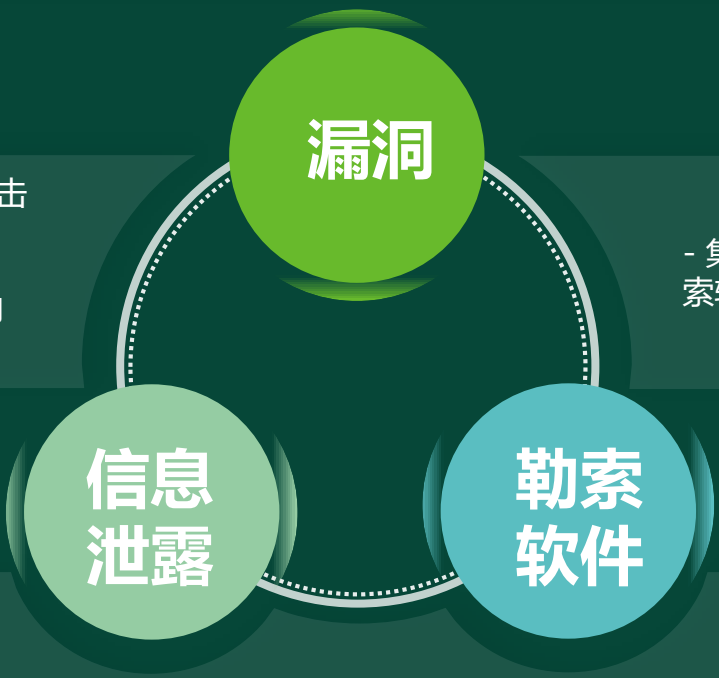
这些暗中操作，影响持久的攻击事件就是勒索软件攻击和信息泄露。

年度安全事件观察结果

“暗黑三兄弟”臭味相投、互相“扶持”

各类攻击手法之间或多或少存在一种默契，相互“扶持”来使各自的攻击效果最大化。漏洞、信息泄露、勒索软件就颇有“臭味相投”的意思。

单独的一个高危漏洞已足以引起各路安全专家的注意，不过这才仅是个开始，一些漏洞被攻击者武器化后，通过掌握的泄露信息精准投放，入侵目标系统实施勒索，勒索时窃取到的信息又作为筹码被拿到黑市上交易，由此从中持续获利。观察近些年的网络攻击事件，发现这种模式已经被攻击者广泛利用。



- 被泄露的信息，被攻击者用来锁定目标系统，并尝试漏洞利用
- 利用漏洞攻入组织内部后又会窃取信息

- 集成了武器化漏洞的勒索软件杀伤力巨大

- 泄露的信息，有助于发起针对性社工或钓鱼攻击，并借此传播勒索软件
- 勒索成功后，再次窃取目标信息

肆虐虚拟网络空间的“暗黑三兄弟”在工控领域中也“大施拳脚”

工控系统是水利、电力、石油化工、制造、航空航天等诸多国家命脉行业的基础设施，因此在利益、政治等因素驱动下的攻击者也是对其虎视眈眈。工控系统软硬件更新更换困难的现状使得不少漏洞隐藏其中而得不到修复；勒索软件使工业生产停滞的代价更是迫使许多企业不得不满足攻击者的要求。

疫情大环境下的网络安全

今年由于疫情原因，有不少攻击者利用民众对于疫情的关注来进行攻击，加剧了信息泄露的风险和恶意软件的传播。

类似疫情这种大规模公共安全事件的发生也会影响到网络空间，不论是恶意APP还是不实谣言等都给管理网络空间安全带来了极大的挑战，网络安全不能完全脱离物理安全来考虑，应全方位的进行综合性评估，才能避免大规模的恶意攻击蔓延。

漏洞观察

近五年 CVE 数量统计

数据来源：https://nvd.nist.gov/general/visualizations/vulnerability-visualizations/cvss-severity-distribution-over-time#CVSSSeverityOverTime

CVE 总量连续四年创新高

自2017年CVE数量飙升超过1.4万，此后每年发布的CVE个数都再创新高。要论今年增长的原因，疫情影响应该算得上一个。

疫情时期，组织在快速将应用推向市场和维护代码安全性之间恐怕更倾向于前者。而且今年各国各地远程办公人数迅速增加，个人终端设备接入了公司网络，远程协作办公软件如视频会议、文档协作、虚拟专用网等自然也成为白帽黑客和攻击者的又一大目标。

老洞经久不衰，新洞层出不穷

据统计，漏洞具有平均七年的生命周期，2020 年遭频繁利用的漏洞几乎可以肯定将在2021年继续遭利用。能被反复利用的漏洞基本上已被武器化，或至少拥有公开/半公开可利用程序，且其目标多是广泛使用的操作系统、个人/企业常用软件、组件等。FireEye 被窃的红队工具包所涉及的漏洞能从侧面验证这一观点。

以下列举部分今年被广泛关注的常用软件漏洞：

Windows	**Bad Neighbor**	Windows TCP/IP远程代码执行漏洞 CVE-2020-16898
	SigRed	Windows DNS 服务器中具有蠕虫特性漏洞CVE-2020-1350
	SMBGhost	SMBv3 中具有蠕虫特性的 RCE 漏洞CVE-2020-0796
	Exchange	Exchange 远程代码执行漏洞CVE-2020-0688遭多个APT组织利用
Oracle	**Weblogic**	漏洞高产产品CVE-2020-2551/14882/14883
Apache	**Tomcat**	Apache Tomcat 文件包含漏洞CVE-2020-1938
浏览器	**IE 0day**	同 Firefox 0day(CVE-2019-17026)一起被 APT组织 Darkhotel 利用
	Chrome 0day	CVE-2020-15999 结合社工利用，野外发现攻击行为
	Firefox 0day	CVE-2020-6819/6820 Mozilla 提示发现了针对性的在野利用攻击
	IE 0day	CVE-2020-1380 在 Operation PowerFall 攻击活动中被发现
远程办公	**Zoom**	攻击者通过Zoom聊天功能进行远程代码执行，从而获得特权控制用户主机

在应对全年以万计数的漏洞时，应首先及时修复那些已被或易被武器化的漏洞，通过合理定级做取舍！

漏洞处置三部曲

一、事先预防

- 资产梳理
- 系统、软件、组件梳理
- 跟踪关注更新
- 自主挖掘安全隐患

梳理各类业务常用的系统、组件等。密切关注官方及第三方安全通告，确保在第一时间了解新漏洞情况。

同时自行挖掘某些关键组件的安全隐患，早发现早解决。

二、漏洞评估定级

并非每个漏洞都很“急”

漏洞大体可以从 4 个方面综合评估：

1，漏洞基本面

是否可以远程触发、是否需要特定权限、是否需要用户交互、是否需要额外配置

2、可利用程度

是否是 0day 漏洞、是否已有公开的 PoC 、是否已有公开的 Exp

3、影响范围

是否核心组件受影响、是否通用组件受影响、受影响组件在线暴露量是否较多

4、补丁情况

官方是否已提供补丁、官方是否给出缓解措施、如果没有官方补丁和缓解措施，是否有常规防护措施

三、应急处置

- 技术分析
- 影响统计
- 检测防护产品
- 整体方案

确认漏洞的威胁等级后，进行相应的应急处置。

通过分析漏洞的成因和攻击链，准备检测和防护措施。统计具体的影响面，形成完整的防护方案。

勒索事件观察

攻击事件爆炸增加 勒索手法频出花样
索要赎金节节攀升 不幸中招伤财伤人

殃及行业 Top 5

市政及公共部门
制造业
学术教育
医疗卫生
工控

活跃勒索软件 Top 10

Sodinokibi/REvil
Maze
SNAKE/EKANS
Ryuk
Nemty
Nephilim
NetWalker
DoppelPaymer
CLOP
Tycoon

针对国家 Top 5

美国
澳大利亚
加拿大
英国
德国

勒索软件趋势及特点

勒索软件事件占全年网络攻击 1/4

最高赎金超 4000万 美金

勒索软件即服务 RaaS 盛行

企业比个人金额高 20-40 倍

绝大部分利用 钓鱼邮件 传播

加密前会 窃取 敏感信息

不付赎金 公开拍卖 敏感数据

持续时间一般为 7 天左右

遭遇勒索后的常见情况:

- 勒索软件影响面超出预期可控范围
- 某些业务中断付出的代价远高于赎金
- 勒索软件进化后大范围的解密更困难

备份恢复 or 支付赎金？

技术恢复 + 支付赎金

在对先前一些公开的勒索事件做回顾后发现，在某些情况下，详细咨询过专家并谨慎评估风险后，支付赎金或许也可被纳入决策考虑之一。这些情况通常是通过技术手段也并不能完全恢复核心业务，或是业务中断付出代价远高于支付赎金。

信息收集 & 评估

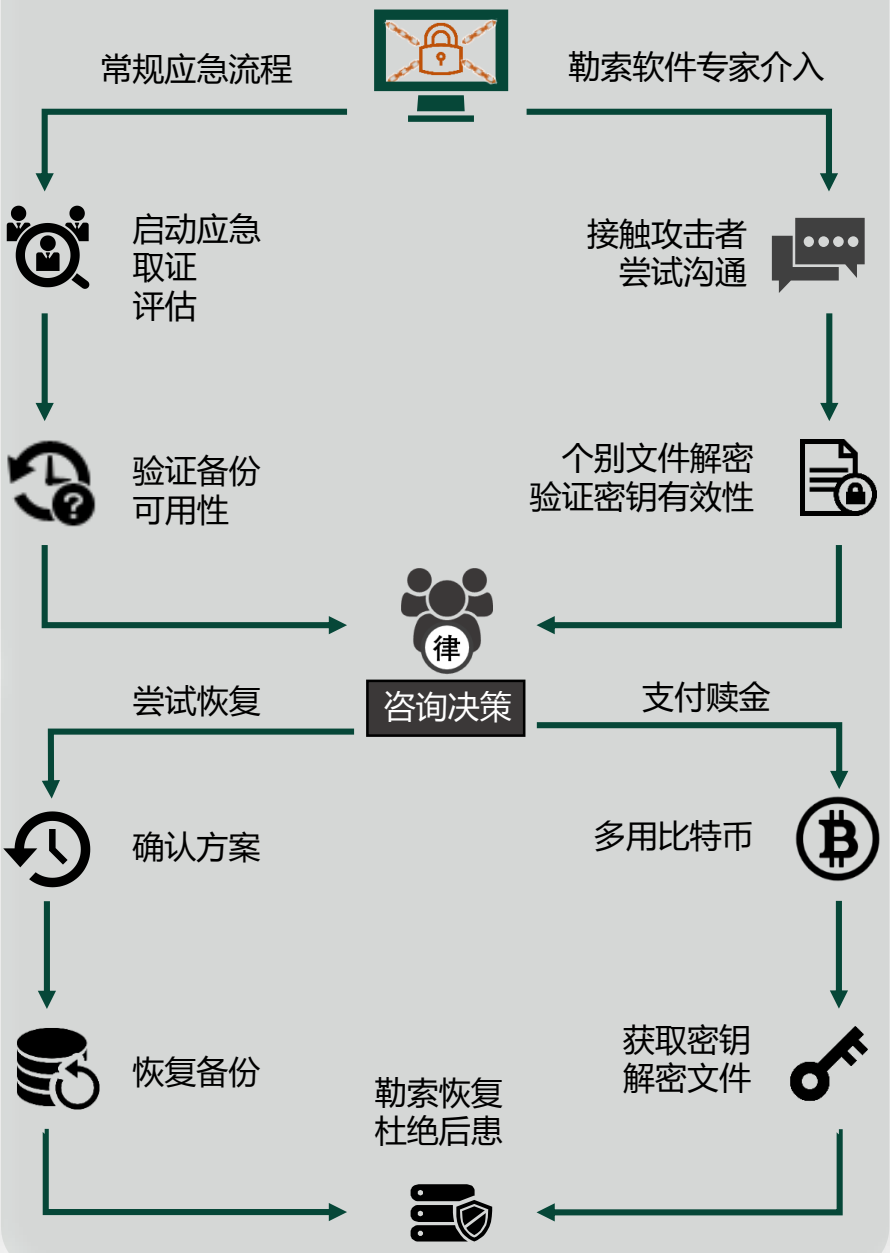
遭受攻击后，应第一时间隔离受感染系统、确认受影响范围、评估受损程度并验证备份可用性。

与此同时，咨询勒索软件专家，并尝试与攻击者谈判，验证其解密能力。

采取行动 & 事后总结

确认技术方案的可行性，如有可用备份，则直接用相关备份恢复业务。否则在咨询过专家并衡量风险后，确定支付方案，通过支付赎金来恢复数据。

勒索攻击双管齐下响应流程



预防优于补救

提高员工安全意识，避免被钓鱼、社工攻击
完善合理的备份系统和关键业务的应急方案
通过技术手段增强内部恶意软件的检测能力

信息泄露事件观察

医疗保健
成本最高的行业

~70%
泄露信息中包含电子邮箱

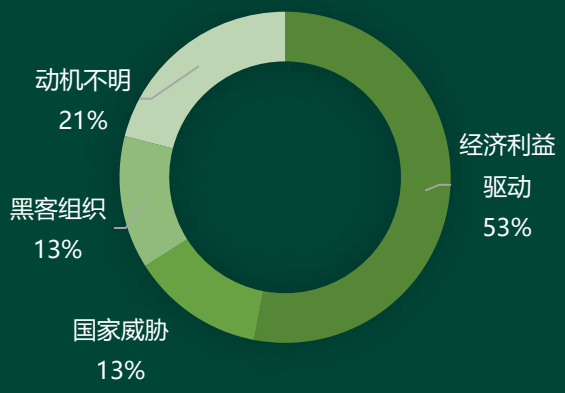
~200天
发现和控制所需的平均时间

~80%
泄露信息中包含客户个人可识别信息

远程办公
疫情环境下远程办公增加了泄露风险

~50%
恶意攻击在泄露原因中占比最高

恶意攻击威胁向量



受影响行业分析

住宿 & 交通运输 & 医疗卫生行业
酒店、航空、医院等均需实名认证，这类数据有较大的交易、利用价值，是攻击的主要目标之一。

互联网行业：
如社交网站、招聘网站、电商网站等，其中的数据不仅有用户的个人信息还能体现出用户的关系图谱。

政府及公共服务单位：
因为除了掌握着大量公民信息外，还涉及一些机密信息，因此也备受关注。

目标案例

酒店	万豪酒店数据泄露，影响 520 万客人
政府	490万格鲁吉亚选民信息被公开
医疗	明尼苏达医院遭黑客入侵，泄露5万患者信息
IT	FireEye 遭黑客组织入侵，红队攻击工具被窃
社交媒体	2.67 亿条 Facebook 记录在黑客论坛上售价 600 美元

利益驱动下，隐私信息已成为获利的一大目标。被泄信息可能被用于倒卖、诈骗、勒索、社工等。

随着自媒体发展，个人敏感信息在网上暴露情况也越发常见，某些生物信息的采集，甚至在不知情或非自愿情况下进行。

隐私信息的安全，需要个人意识、企业责任、法律法规共同守护。

信息泄露发生时

泄露原因

- 恶意攻击：
蓄意攻击，针对性强，目标数据在非法交易中有较高价值，这也是促使攻击发生的主要原因之一。
- 暗藏内鬼：
内部有权限接触敏感数据的人员获取数据后，对外出售。
- 系统故障、人为失误
- 不规范网站、平台、APP 对信息过度采集和诱导采集。海量数据在传输、存储过程中未被妥善处理，便成为“黑色产业链”中的交易对象。

泄露数据类型 TOP3

- 公民信息：
各类公民个人信息，包括基本身份信息、个人征信、银行账户信息等。
- 账号数据：
网站和APP账号中有大部分虚构信息，但是账号密码常被用来撞库，影响范围会被层层扩大。
- 商业敏感信息：
包括员工私人信息，以及账单、合同、交易、客户相关的各类机密信息。牵连范围较大，社会影响恶劣。

信息泄露发生后

造成影响

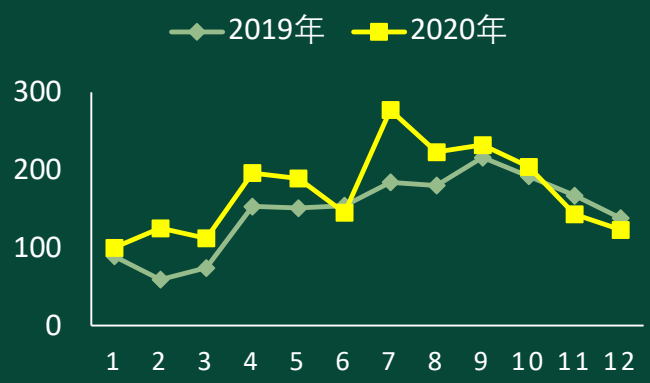
- 经济损失：
攻击者拿着被泄数据向网络运营者索要钱财，对受影响个人进行诈骗。
- 名誉受损：
无论是未能满足攻击者的勒索要求被公开了信息，还是信息被泄后遭遇倒卖。信息来源方和信息主体的名誉都将严重受损。
- 影响持久：
信息泄露造成的影响是持久的，可能持续很多年。它无法随着单一事件的公开、解决而完全根除。更像是后遗症一样，在不确定的时期可能又会被恶意攻击者利用。

建议

《网络安全法》规定：
- 任何个人和组织有权对危害网络安全的行为向网信、电信、公安等部门举报。
- 个人发现网络运营者违反法律、行政法规的规定或者双方的约定收集、使用其个人信息的，有权要求网络运营者删除其个人信息。- 任何个人和组织不得窃取或者以其他非法方式获取个人信息，不得非法出售或者非法向他人提供个人信息。
- 提高信息保护意识，在受到危害时借助法律寻求帮助！

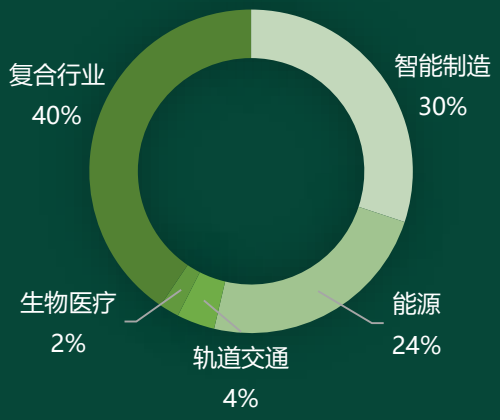
工控安全事件观察

年度工控事件总览



上图为年度工控漏洞及工控事件(事件资讯、研究等)数量的统计。
年初因为疫情原因，整体关注度较全年略低，但在年中开始稳步提升，年末有所回落。

工控相关事件涉及行业



上图为年度工控事件相关行业的分布图。智能制造是最受攻击者青睐的行业，此外由于工控设备通常能在多种行业内使用，所以攻击大多涉及复合行业。

典型事件

Ripple20 (供应链风险)
- Treck TCP/IP 协议栈漏洞
- 影响全球物联网和工业互联网供应链安全

委内瑞拉全国大面积停电 (黑客攻击)
- 时隔10月，国家电网干线再遭重创
- 国家关键基础设施是政治博弈的一大目标

欧洲能源巨头EDP遭遇勒索 (勒索软件)
- 利用 10TB 敏感数据索要千万美金
- 巨头厂商更易成为攻击者的摇钱树

现状

70% 工控漏洞 70% 以上属于高危漏洞普遍危害大。

Nday 被利用的大多是 Nday 这和工控漏洞修复难度大有密切关系

DDoS 漏洞造成影响 DDoS 居多 相比其他行业，DDoS 对工控行业的影响更为致命

工控威胁现状观察

威胁主要来源

具有破坏工业流程能力的勒索软件是对工业生产最大的威胁。生产线被迫关停、索要高昂赎金、核心制造工艺等敏感信息被盗都是勒索软件所到之处能造成的危害。

2020年针对以色列水利基础设施的网络入侵就是缘于暴露在互联网上的PLC。暴露的每一台设备都为攻击者打开了通往企业核心的一扇大门。

有的钓鱼邮件会作为恶意软件的载体，诱导员工点击链接或下载附件从而释放恶意软件。有的钓鱼邮件则通过社工手法，直接索取内部敏感信息以进行下一步攻击。

上游攻破一点，下游影响一片。供应链任一环节中存在的漏洞都有可能逐层传递，扩散范围巨大。最终受影响产品修复难度大，修复周期长。比如今年的 Ripple20、AMNESIA33

攻击趋势

越来越多国家级高级攻击组织在瞄准工控系统，这些组织对目标系统的研究程度更深，因此其开发使用的恶意工具对工控设备及生产线的打击也更具针对性和致命性。

比如 ELECTRUM 组织，曾利用专门针对工控系统的恶意软件 Industroyer 导致乌克兰大面积停电。还有专门针对西门子 SCADA 设备的恶意软件 IRONGATE。

委内瑞拉大停电、瞄准以色列水利设施的网络攻击等足以证实这一点。

IT 安全 vs ICS 安全

- 保护传统 IT 系统时，更注重保护的是信息（机密性），而对于 ICS 系统时，更注重保护的是过程（可用性）。
- 介于 ICS 系统必须保证系统运行的连续性，所以其中存在很多未修复的已知漏洞，因此打补丁及时更新系统这种解决方案在现实中并不适用于ICS系统。
- ICS 系统中，系统组件和设备可能分布在数百公里外（如管道、电网等），这使得物理安全也要尤为关注，因为远程现场也极有可能成为攻击者进入 ICS 的入口。

建议

- 应对资产暴露：定期进行资产梳理，对于暴露在外的资产进行严格管控，如因业务需要对外开放的，一定要配置认证，并且进行安全评估。
- 应对钓鱼邮件：通过培训和演练提高人员安全意识、辨别及处置能力。
- 引入各类检测防护产品，比如使用工控入侵检测系统对工控的攻击行为进行检测、通过工业防火墙等防护设备对工控网络安全区域之间进行逻辑隔离等 。
- 定期进行备份，同时也要注意验证备份有效性。

绿盟科技格物实验室

绿盟科技格物实验室专注于工业互联网、物联网和车联网三大业务场景的安全研究。实验室以“格物致知”的问学态度，致力于以智能设备为中心的漏洞挖掘和安全分析，提供基于业务场景的安全解决方案。积极与各方共建万物互联的安全生态，为企业和社会的数字化转型安全护航。