NOZOMI NETWORKS LABS

执行摘要

OT/IoT 安全报告

网络战洞察、威胁及趋势、建议

2022 年上半年回顾 | 2022 年 8 月

执行摘要

随着网络威胁模式的不断变化，理解网络威胁如何影响您的组织变得空前重要。过去六个月，网络攻击的频率和复杂性以及威胁主体对新战术的使用急剧增加。曾被视为不太可能的威胁突然变为常见操作。

例如，以往不是勒索软件目标的企业如今不断受到这类攻击。除了这种转变，威胁主体还继续模糊其恶意活动，以避开安全解决方案的检测。

为加强安全性、尽可能降低未来威胁，企业需要实时掌控其面对的网络风险，就如何以最优方式保护自身作出知情决定。

本报告：

- **回顾**网络安全的现状。
- **识别**威胁模式的新趋势，并提出应对解决方案。
- **概述**俄乌危机，介绍新的恶意工具和软件以及这场冲突如何让我们深入了解攻击者的能力。
- **提供**有关物联网僵尸网络、相应的失陷指标 (IoC) 以及威胁主体的战术、技术和程序 (TTP) 的洞察。
- **分享**建议和预测分析。

2022 年上半年威胁概况

自从俄罗斯于 2 月针对乌克兰发起特别军事行动，我们看到：

黑客活动

国家支持的 APT 及网络罪案

擦除器恶意软件

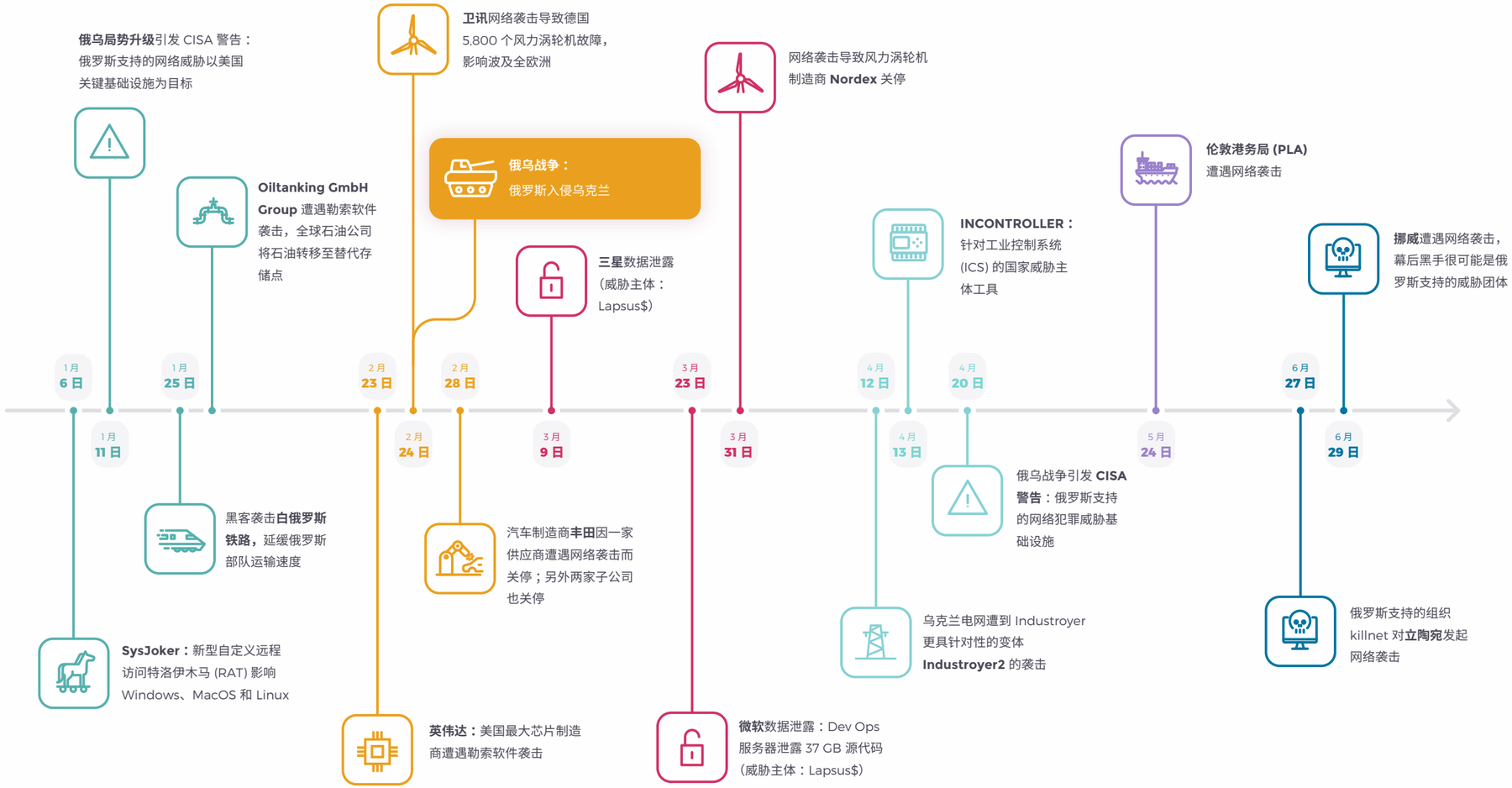
Industroyer2

2022 年上半年重要网络事件时间线

本页的时间线列出 2022 年 1 月至 6 月发生的主导当前网络威胁模式的重大网络事件。

自俄罗斯于 2022 年 2 月针对乌克兰发起特别军事行动，我们看到多种类型的威胁主体，包括黑客、国际支持的 APT 及网络罪案。

另外，擦除器恶意软件被大量使用，还开发出了攻击 IEC-104 协议的 Industroyer 变体（名为 Industryoyer2），此协议常用于工业环境。



物联网僵尸网络模式

Nozomi Networks Labs 的蜜罐收集数据，经分析后可就威胁主体活动提供有价值的洞察。2022 年上半年，我们观察到如下趋势：

- **主要攻击者国家 / 地区：**主要网络活动来自与中国和美国相关的 IP 地址。完善的技术和制造业很可能增大他们的攻击面。
- **涉及硬编码凭据的协议：**Mirai 这款流行的僵尸网络软件最初是利用 Telnet 进行攻击，但自从威胁主体公布源代码后，该软件经过修改，开始针对 SSH 和其他协议。
- **使用最多的凭据：**“root” 和 “admin” 显然是极有吸引力的目标，被多种攻击变体使用，因为它们可以让威胁主体访问所有系统命令和用户账户。
- **攻击者 IP 地址数量达到历史新高：**根据蜜罐收集到的与恶意活动相关的 IP 地址，4 月成为恶意活动最活跃的一个月，收集到的攻击者 IP 地址接近 5,000 个。
- **执行最多的命令：**我们总结了执行次数最多的 10 个命令，其中包括 `enable`、`shell`、`system` 和 `which Is`。每条命令约被 12,500 个自动程序执行过。

4 月
是僵尸网络最活跃的一个月，公布近

5,000 个
攻击者
IP 地址

阅读**完整报告**，进一步了解 2022 年上半年的物联网僵尸网络活动。

漏洞概况

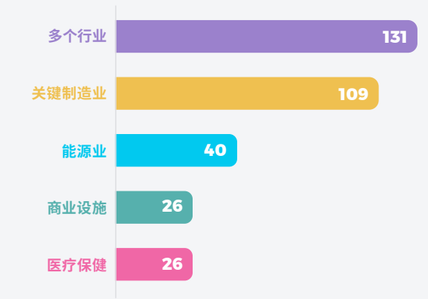
许多 ICS 软件和硬件产品的安全防线都因为某些漏洞形同虚设，而这些漏洞也基本被安全研究人员发现。2022 年上半年，美国工业控制系统网络应急响应小组 (ICS-CERT) 发布了 560 个常见漏洞和风险 (CVE)，其中 303 个是 2022 年新宣布的。与 2021 年下半年相比，报告的 CVE 数量减少 14%。

其中 131 个 CVE 影响多个行业。关键制造业是受到直接影响最大的领域，有 109 个 CVE。能源业位列第二，有 40 个 CVE；医疗保健和商业设施并列第三，均有 26 个 CV。另外，CVE 警报中提到 60 家供应商，涉及 172 款产品。受影响的供应商比 2021 年下半年增加 27%，受影响的产品增加 19%。

ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

560 个
CVE

受影响最大的行业



建议

可由组织内不同人员实施的主动安全措施越来越受到追捧。这些人员包括可能从不同角度看待安全问题的 IT 团队、合规人员和风险经理。首要的安全做法应当包括：

- 备存准确的资产目录
- 安装最新的 VPN 补丁
- 权限访问管理
- 使用不容易遭受语音钓鱼或 SIM 调换攻击的高强度多因素验证 (MFA)
- 经常更换密码；以及
- 加强对员工进行语音钓鱼和整体社交工程防范培训

其他缓解措施：

- **备份：**为确保勒索软件或擦除器恶意软件攻击不会造成全面数据丢失，务必定期备份数据、测试备份系统并确保将备份存放在场外，而非运行服务器的同一网络上。
- **威胁情报：**网络威胁情报指收集、分析和传播有关网络威胁的信息，帮助组织保护系统和数据。这些信息可以包括恶意软件签名、攻击向量和失陷指标 (IoC)。
- **云安全：**确保云提供商声誉良好，符合 ISO 27001 或 ISO 1/2/3 认证等行业标准，加密存储或传输的数据，并使用 2FA 和身份管理工具。
- **威胁检测：**威胁检测用于实时检测和响应潜在威胁，并为未来事件提供警报。在威胁检测中，系统监视网络中的可疑活动，例如来自一个 IP 地址的异常流量或者通往特定服务的大量连接。具体操作包括扫描异常活动或网络中的已知漏洞。
- **软件物料清单 (SBOM)：**SBOM 可让您了解每个组件存在多少版本以及这些版本的使用位置，以便跟踪版本变化，确保它们不会与其他组件产生冲突。SBOM 还有助于您了解哪些组件的风险更大或漏洞更多，以及如何缓解这些漏洞。虽然 SBOM 尚未被广泛使用，但有必要关注这项技术的发展。

增强安全性的主要威胁缓解措施

预测

根据最新分析，我们预计 2022 年下半年将出现如下主要网络安全趋势。

- 更多 ICS 相关攻击
- 勒索软件威胁主体将继续针对关键基础设施企业
- 针对大型企业的攻击增加
- 盗窃科技源代码
- 随着今年早前发起的私人 / 政府倡议的成型，网络政策和治理有所增加

下载 OT/IoT 安全报告

Nozomi Networks Labs 分析当前威胁模式并分享：

- 近期的勒索软件与 IoT 僵尸网络攻击
- ICS、OT/IoT 设备漏洞和利用趋势
- 加强网络威胁缓解战略的步骤

下载

NOZOMI NETWORKS

Nozomi Networks

OT 和 IoT 安全与可见性领先解决方案

Nozomi Networks 保护世界的关键基础设施、工业和政府组织免受网络威胁，从而加速数字转型。我们的解决方案交付卓越网络和资产可视化、威胁检测能力以及对 OT 和物联网环境的洞察。顾客依托我们降低风险和复杂性，同时最大化运营韧性。

NN-SEC-RP-ES-SC-2022-1H-001

nozominetworks.com