未来工厂的网络威胁分子综述

Discussion on Network Threat Molecules in Future Factories

孔博源

Boyuan Kong

中广电移动网络有限公司　中国·北京 140001

China Radio and Television Mobile Network Co., Ltd., Beijing, 140001, China

摘　要：第一，论文研究了不同的 CTA 列表，并识别了从政府机构到网络安全行业专家等多种组织类型的 CTA。第二，论文将类似的威胁行为者组合在一起，以减少行为者的重复。第三，将威胁分子及其能力映射到 FoF 环境的特征。第四，论文讨论了多少被礼貌地忽略的竞争对手的角色作为威胁的参与者和“黑客反击”的概念作为一个有争议的辩论防御机制。

Abstract: Firstly, this paper studied different CTA lists and identified various types of CTAs from government agencies to experts in the cybersecurity industry. Secondly, this paper combines similar threat actors together to reduce the repetition of actors. Thirdly, map threat molecules and their capabilities to the characteristics of the FoF environment. Finally, this paper discusses how many politely overlooked competitors act as threat participants and how the concept of "hacker counterattack" serves as a controversial debate defense mechanism.

关键词：未来工厂；网络安全；威胁分子

Keywords: future factory; network security; threatening elements

DOI: 10.12346/etr.v6i3.9221

1 引言

考虑到经济生态系统正变得越来越相互关联，尤其是未来工厂（FoF），本研究旨在提高对这一主题的认识。FoF 环境有望带来巨大的生产力收益和盈利商业策略的新可能性。然而，现实也表明，实现 FoF 环境所要求的这些各种条件，带来了严重的网络安全挑战。

2 未来工厂威胁分子态势

2.1 FoF 的定义

高度网络化的制造场景，跨系统的实时数据处理和相关的供应链是当今先进工业场景的特征。通用术语工业 4.0 包含了所有这些发展，作为一个概念，为工业景观的网络。这个词在 21 世纪 10 年代初出现在德国，此后引发了全球许多科技出版物。集成现有技术和工具，如嵌入式系统、传感器和其他工业硬件，以实现实时数据处理，反映了工业 4.0 生态系统。在这个生态系统中，CyberFactory No.1 项目（参见 https://www.cyberfactory-1.org/en/home/）旨在设计、开发、集成和演示许多关键能力，以增强 FoF 的优化和弹性。

增材制造、自主机器、协作机器人、机器学习、增强现实、大数据分析以及许多其他技术和数字方法 / 流程都与 FoF 的环境相连接。世界经济论坛发布的一份白皮书发现，那些能够超越试验这些新技术的工厂，是那些大规模包含三个关键要素的工厂，即连通性、智能和灵活的自动化。这些因素带来了网络安全方面的挑战，而这些挑战尚未得到过多讨论。

从网络安全的角度来看，高连通性的特点特别有趣。FoF 可以在许多点永久连接到 internet，云制造（CMfg）、工业物联网（IIoT）可以利用网状网络，IT 和运营技术（OT）系统可以互连。这些连接为传统的攻击模式创造了新的机会，当然也为 FoF 提供了新的攻击载体。

人们可以从两个角度来看待 FoF 的智能方面：一方面，机器学习或其他人工智能技术使自主机器人或能够在工厂车间与人类一起学习和工作的机器得以使用。另一方面，大数据决策可以帮助优化整个价值链的流程，从工程到客户服务。

【作者简介】孔博源（1986-），男，中国北京人，本科，工程师，从事通讯信息、工程建设研究。

灵活的自动化是通过 FoF 的连通性和智能来实现的。它允许对不寻常的情况快速和一致的反应，能够根据客户的需求定制产品，并减少时间和材料浪费。以灵活的方式制造产品的新方法包括增材制造（3D 打印）和云制造 [1]。

2.2 FoF 的威胁分子

协作、网络连接、情报和灵活的自动化也为威胁行为者提供了新的可能性。在本节中，我们将讨论已识别的 8 个威胁分子如何影响这些属性。FoF 系统的网络连通性带来了增加的攻击面。虽然网络防御不是一个新课题，但是使用多种无线和有线连接的资源之间复杂的互连要求使得环境非常具有挑战性。持续访问 Internet 是实现云资源高效使用的必要条件。在规划和操作这类系统时，必须考虑到保护物联网（IoT）设备所面临的挑战。这样一个具有挑战性的环境提供了一个广泛的攻击面，并将需要一个成熟的网络安全管理策略和更好的工具，以减少网络事件的可能性。虽然所有的 CTA 都能从一个更难保护的环境中获益，但最有可能从附加连接中获益的是民族国家行为者，他们拥有瞄准系统中任何组件的资源。此外，攻击者只需成功一次，而系统及其防御者必须不断地面对新的安全挑战。因此，在这种情况下，防守方总是处于压力之下，处于劣势。

2.3 为 FoF 评估威胁分子

预测是非常困难的，尤其是关于 FoF。然而，通过结合 FoF 环境所具有的特殊特征，我们可以估计最可能影响 FoF 环境的威胁分子。

FoF 环境可能是由车间内的工业网络与工业互联网和云资源结合而成。这对信息安全管理提出了挑战。

工业网络有部分具有高度专业化的设备，需要高度专业化的知识。然而，当实现访问时，网络通常很容易中断，因为高可用性需求阻止了安全增强技术的使用（如安全监控、加密）。

FoF 环境的联网方面通常在更健壮的安全管理策略下运行。然而，该环境是许多 CTA 的典型，这意味着尽管攻击任何安全云提供商都需要专业知识，但更熟练的攻击者可能已经拥有可用的工具。管理 FoF 使用的基础设施的新合作伙伴和事实上的内部人员将大大增加攻击面。新的工具和技术要求对安全的应用程序进行精确的信息安全管理。这与工业网络的软基础相结合，使得该系统对许多 CTA 非常有吸引力。

我们对 ENISA 2019 年报告中所列的观察到的威胁如何与威胁分子以及上述 FoF 的四个方面（网络连通性、协作、灵活自动化和智能）进行了评估。如果 CTA 是主要威胁，则威胁分子的权重为“1”，如果报告认为他们是次要威胁，则权重为“0.5”。这样就可以估计不同的 CTA 利用最常见威胁类型的差异有多大。FoF 中最可能受到此类威胁的特征的估计，并对其进行排序，以便最经常检测到的威胁位于顶部。值得注意的是，在相关报告中，合伙人和寻求刺激的 CTA 并没有出现。

显示了所有类别的威胁分子能够使用现有技术对 FoF 环境发起攻击。网络犯罪分子、民族国家行为者和竞争对手获得的分数尤其高。在这一分析中，竞争对手的威胁技术能力与国家和网络罪犯相匹配。

2.4 FoF 环境的不同 CTA 分析

网络犯罪分子是网络安全领域最活跃的威胁分子。他们的目标是广泛的行业，并有丰富的货币化技术可以利用。只要 FoF 系统有利可图且风险不高，它就有可能成为网络犯罪分子的攻击目标。他们可能会像以前一样，以一种创造性的方式采用传统方法进入新环境，并且极有可能成为 FoF 环境中事件的主要来源。这也反映在当前的威胁报告中，如表 1 所示。

表 1 2018 年观察到的对贸易协定的威胁

Top Threats 2018	Cyber Criminals	Nation-States	Competitors	Ideologues	Insiders	Affected FoF Aspect
Malware	1	1	1	0.5	-	Network Connectivity
Web Based Attacks	1	1	1	1	-	Network Connectivity
Web Application attacks	1	1	1	1	-	Network Connectivity
Denial of Service attacks	1	0.5	0.5	1	-	Network Connectivity
Botnets	1	1	1	1	-	Network Connectivity
Phishing	1	1	1	1	1	Network ConnectivityCollaboration
Spam	0.5	0.5	0.5	-	1	Collaboration
Ransomware	1	1	1	-	0.5	All
Insider Threat	1	0.5	1	0.5	-	All
Physical Manipulation/ Damage/Theft/Loss	1	1	1	0.5	1	Flexible automation
Exploit Kits	1	1	1	-	-	CollaborationNetwork Connectivity
Data Breach	1	1	1	1	1	Network Connectivity
Identity theft	1	1	1	1	1	Collaboration
Information leakage	1	1	1	0.5	0.5	All
Cyber espionage	-	0.5	0.5	-	0.5	CollaborationNetwork ConnectivityFlexible automation
Total	13.5	13	13.5	9	6.5	-

国家行为体感兴趣的是战略数据、间谍活动和经济间谍活动以及控制关键基础设施和破坏关键生产链的能力。他们还感兴趣的是是否有能力中断决策和干预竞争的国家领导人的选择。许多这些目标可以通过瞄准 FoF 环境来实现。民族国家行为体具有破坏环境所需的高技能。由于民族国家行为者不需要盈利，他们最有可能使用第三方作为攻击网络行动的威胁载体。如表 1 所示，民族国家行为体很可能是 FoF 运营商的 CTA，并且在未来很可能保持这种状态。

竞争对手通常是那些从进攻性网络行动中获利最多的企业。它们通常被认为是由于道德或担心声誉受损而受到阻碍，但缺乏关于针对竞争对手的网络行动的实际使用情况的数据。他们是一个可能被当局低估的 CTA。竞争对手可能具有操作工业系统所需的类似专家系统的深厚专业知识。它们可能是针对 FoF 环境的更智能威胁的来源，因为它们拥有行业知识、人脉和理解能力。在缺乏竞争的商业领域，或在军事或情报领域（如航空航天、通信）工作的国家控制 / 支持的企业，尤其如此。政府支持的竞争对手在发起攻击性网络行动时也可能缺乏真正的选择，即使被抓到，也可能对任何实际后果具有免疫力。当前的威胁趋势（见表 1）表明，竞争对手是 FoF 环境的重要 CTA，并将在未来继续如此。

虽然合作伙伴不太可能是网络事件的来源，但他们很可能是其他 CTA 使用的攻击载体。他们应该被视为像局内人一样具有巨大的威胁作用，可以很容易地通过贿赂、胁迫、欺骗，甚至强迫他们依法合作。FoF 环境的高连通性和协作性使得合作伙伴成为比典型环境更重要的威胁分子 [2]。

我们也需要记住内部人士是一个威胁因素。他们也可能被欺骗、贿赂或强迫给予其他 CTA 机会。在使用集中数据收集系统和协作工具的 FoF 环境中，任何内部人员的访问都会造成更大的问题，因此内部人员的妥协可能会在这样的环境中造成更大的破坏。表 1 中对内部人员的低得分不应被认为降低了内部人员作为 CTA 的重要性，因为他们可能不需要与保护 FoF 环境的网络安全系统竞争。

在典型的 FoF 环境中，意识形态者是一个不太可能构成威胁的角色。大多数黑客行为都是对网站的破坏，而不是典型的 FoF 环境。针对大多数 FoF 运营商（如制造业）的恐怖活动仍然不太可能。然而，目前的趋势表明，意识形态者活跃在可能影响 FoF 环境的威胁区域（见表 1）。FoF 操作者应考虑其组织是否为意识形态者感兴趣的目标。

在管理良好的 FoF 环境中，寻求刺激者也可能不是主要的威胁者。虽然在历史上，黑客是造成大规模众所周知的网络安全事件的原因，但现在，与不断活动的民族国家和网络犯罪 CTA 相比，他们已经相形见绌。寻求刺激的人不太可能花费精力去突破 FoF 环境所需要的防御。他们将继续发现 FoF 环境的子系统上的漏洞，给没有准备的人造成问题，并为有充分准备的人提供机会。

3 结语

论文提出了不同专家组织所识别的威胁分子。私营 IT 和网络安全供应商的商业利益当然不应被忽视，因为它们经常直接或间接地提及自己的内部解决方案，如基于人工智能（AI）或网络保险的网络安全。因此，IT 和网络安全组织撰写的研究应该谨慎处理，因为这些组织有商业利益，允许对范围有一定偏见的观点，通常基于匿名的客户数据。不过，从与公共机构和政府机构的比较中可以看出某些趋势。

我们的报告分析所描绘的组织在识别 CTA 方面存在很大差异。虽然从事件数量上看，最大的威胁显然是网络犯罪，但并不是所有的专家组织都将其列为 CTA。多数人（22 人中有 19 人）确定了民族国家行为体。然而，公共事件数据和威胁行为人识别的最大不匹配是恐怖行为人。在 22 个专家组织中，有 12 个确认网络恐怖分子是一个重大的威胁分子，但仍然没有明确的网络恐怖事件被记录在案。在我们的数据中，只有 7 个组织确定了竞争对手，只有 6 个确定了合作伙伴组织作为重要的 CTA。

在这种情况下，应该注意的是，那些已经成为工业间谍活动受害者的公司往往不会上市。造成这种情况的原因是非常不同的。声誉受损当然是一个重要因素，因为根据事件的规模、行业和相关公司的规模，许多公司认为公开披露造成的损害更为严重。此外，肇事者并不总是被查明，事件的程度也不清楚。有时，公司甚至不知道实际提取的是何种信息。未发现病例的估计数目可能很高。

论文分析了 22 个不同的网络安全专家组织列出的 CTA。正如预期的那样，国家行为体和网络犯罪分子是最广泛确认的威胁行为体。随后，超过半数的组织被列为恐怖分子（12 人），其次是内部人士（11 人）和黑客活动分子（9 人）被列为最常见的威胁行为人。虽然大多数评估报告都将恐怖分子列为主动威胁行动者，但公众对涉及网络恐怖分子的高调事件并不知情。工业间谍的情况与此大不相同。这些威胁行动者在报告中所占的比例相当不足，尽管一再发表的指控并不总是得到证实 [3]。

论文进一步将专家组织确定的 13 个不同的 CTA 分为 8 个主要的 CTA 类别。这是通过分析每个 CTA 最可能的动机，并结合具有相似动机类型的行动者（如意识形态）来完成的。

由于未来工厂（FoF）环境在网络安全方面有特殊需求，论文识别了 FoF 环境中构成网络安全挑战的主要方面，并分析了所识别的 CTA 可能如何滥用它们。这为在 FoF 环境下工作的网络安全专家提供了最有可能针对其环境的 CTA 的候选名单。然而，尽管先进的 FoF 环境带来了巨大的好处，但固有的连通性带来的网络安全挑战也必须得到妥善解决。

低识别率的 CTA 之一是竞争对手。经营进攻性网络行动的商业竞争对手可以获得巨大的利益，而遭受打击的风险

很低，至少在理论上是这样。但是，与这些活动有关的记录在案的事件很少。作者比较了企业行为主体在其他领域（如立法、专利、传统）的行为工业间谍）对应于缺乏针对竞争公司的攻击性网络行动的案例。在网络安全领域，不道德的企业竞争战略案例数量似乎很低，而在其他领域，案例数量却很高，这似乎是不匹配的。

尽管灵活性、效率和成本效益被认为是成功部署 FoF 的驱动因素之一，但重要的是要确保该环境配备复杂和强大的网络安全。需要进一步的研究和技术发展，以确保 FoF 系统与它们所取代的系统一样具有网络安全。与此同时，竞争对手往往处于合法性的边缘，有时甚至更边缘，必须被视为采取适当措施的风险来源。这也适用于迄今未能解决由竞争对手推动的工业间谍活动中的网络威胁行为者的研究。进一步的研究和公开辩论是必要的。

参考文献

[1] 华镕.网络威胁源概述[J].自动化博览,2014(1):54-55.

[2] 张晓艺.如何防范基于浏览器的网络威胁[J].计算机与网络,2019,45(9):50-51.

[3] 李留英.欧盟网络威胁情报共享进展及启示研究[J].情报杂志,2021,40(5):8-15.