**防疫与内网安全防御漫谈**

**一、引子**

突如其来的新冠疫情，是一次灾难。不过在疫情持续期间，通过专家对人类的疾控体系，流行病防控，人体免疫系统的深入解读，不失为一次全民关于公共卫生安全问题难得的教育机会，相信很多人现在对人体免疫，疾控等概念都有了一些基本认识。不过在这里，我并不是想探讨人类疾控免疫本身，而是想借此作为切入点，说说网络安全的问题。

计算机与人体系统，网络系统与人类社会系统之间有很多可以类比的特性。每台主机就像一个独立的人体，而主机互联形成网络就类似于社区组织、社会系统。每一个人类个体都可能遭受细菌病毒的侵犯，导致流行病的发生和蔓延，让个人与社会都遭受严重损失。同样，计算机和网络系统也有非常类似的问题，存在计算机病毒传播，黑客攻击等安全隐患，导致信息系统受损和故障。现代人类社会面对细菌病毒的攻击有预防措施、人体免疫系统、疾控组织等体系化的对抗方式，同样，计算机，网络系统面对计算机病毒传播、黑客攻击也有网络安全防御体系进行对抗。

在人类的防疫体系中，人体内生免疫系统是在数百万年与疾病抗争进化而形成，其余部分，比如公共卫生体系、疾控体系、医疗体系都是人类在对抗疾病的历史中逐步构建起来的。这个体系是人类对外界进行风险对抗的缩影，是人类付出惨重代价才获取到宝贵经验总结，虽然不同领域在具体技术细节之间存在很大差异，但从风险对抗角度，一定有很多东西是可以借鉴的。

网络安全防御系统是一个不可见的抽象系统，相比而言，人类疾控和免疫系统则和每个人息息相关，更加具体而容易理解，从疾控免疫这个角度对网络安全防御体系进行解读，可以更加形象化，清晰地理解网络安全防御系统这个复杂的抽象系统。更加重要的目的是期望通过类比分析，网络安全防御系统可以借鉴人类疾控免疫系统的成功经验，反思其存在的问题，以及可以改进的方向。

**二、人类防疫体系与网络安全防御体系的类比分析**

**2.1 人类防疫体系**

人类对疾病的防御大致是通过三个层级进行。

**（1）预防体系**

预防体系是指采取公共卫生措施，在人群和外界的致病物质之间实现阻断。比如，政府负责建立安全的水源供给系统，食品安全检疫系统，环境卫生系统，对个体而言则采取佩戴口罩，穿着防护服、护目镜等自我预防措施。这些措施的重要目的就是降低人体和外界致病物质接触的可能性，对疾病进行预防。预防体系是人类防疫体系中非常重要的环节，是人类社会进行疾病对抗的第一道围栏。

**（2）人体内部疾病防御**

人体内部疾病防御由两个方面组成，首先是人体**内生免疫机制**。对每个个体而言，当预防机制失效，致病物质（比如病毒细菌）进入人体之后，我们的免疫系统就会首先介入，进行免疫对抗。其次是**医疗支持**，通过药物和治疗手段介入，比如在人体内注入疫苗和药物，对抗病毒细菌，辅助人体恢复健康。这两种都属于人体内部疾病防御机制的范围。这是人类进行疾病对抗的第二道围栏。

**（3）规模化的疾病监测和处置机制**

**从风险防控角度，我们应该假设任何防控措施必然失效，并具备风险应对预案**。因此仅有**(1)(2)**两个方面的防御机制是不够的，因为不论是预防体系还是人体自我免疫都有失效的可能，建立规模化的疾病监测体系，对抗上一级防控措施失效引发的疫情传播风险是一种共识。

现实情况也证明进行规模化的疾病监测的必要性。虽然有预防体系和人体内部免疫系统的存在，大规模疾病感染和传播仍然时有发生，特别是具有人际传播能力的、未知病因的流行病疫情，比如2003年的非典和2020年的新冠肺炎，一旦爆发就是是一场灾难。如何能尽早地发现疫情的苗头，及时发出预警和尽早采取防控措施，可以最大限度降低疫情对社会整体带来的损害。

随着人类社会经济发展和文明进步，以社会化组织化的形式协同对抗风险是更加高级的对抗形式，正因为如此，成熟的现代社会治理体系中都建立了规模化的疾控组织。因为流行性疾病发生的时间是未知的、可能爆发的地点是未知的，疾病的原因也可能是未知的，对于一个国家而言，要实现宏观的疾病监测必然要构建大规模的疾病监测网络，对人群中可能爆发的流行病进行全天候、无死角的监控，及时发现疫情迹象，以规模化的疾病控制手段介入，向公众提供预警，研究疾病成因，阻止人际传播，防止流行病的蔓延，有效地控制流行病的大规模传播，降低了社会的总体损失。拿中国的疾控体制举例，目前是国家、省、地市、县四级疾控体系，覆盖全国所有县级行政区域，构建了覆盖全国的疫情直报系统。

**2.2 网络安全防御体系**

为了将讨论的目标更具体化，这里提到的网络特指一个企业或者机构的内部网络，网络安全防御体系也指企业构建的自我防护的网络安全防御体系。当我们将企业的网络安全防御体系与人类防疫体系类比，我们可以观察到彼此之间极大的相似性，这里我们提出一种类似人类防疫体系的网络安全防御架构，在这个统一的架构下讨论各个层级的职能，以及与各个层级关联的各类型安全产品的角色。

**（1） 外围防御**

一个企业内部网络是一个相对独立的网络系统，外界网络是最大的风险来源，构建外围防御体系是最朴素也是有效的防御方式，这与人类的疾病预防体系作用类似。网络安全产品谱系里有一大类产品与该层级对应，就是安全网关类产品，工作于网络数据通路上，一般部署在企业内网与外部网络连接的区域，比如网络防火墙，网络入侵防御系统，web应用防火墙，恶意邮件过滤系统，防病毒网关等等，这类产品一般负责对内向流量（inbound traffic）进行检查和阻断，尽可能地防止恶意流量流入内部网络，减弱和延缓内网主机遭受攻击风险。

**（2）主机自我防御**

该防御层级可以和人体内部疾病防御机制类比。

首先，现代主机操作系统在设计上都对内生安全性进行考虑，提供内生的安全机制，从系统层面对恶意程序的攻击进行防范，比如地址空间随机化技术，应用程序数字签名技术，这些手段类似人体免疫系统，提供内生的机制对异常行为和恶意软件进行防范。其次，主机内部还可以安装运行各种主机安全软件，在主机内部对攻击进行发现、拦截和阻断，比如主机防火墙，主机入侵防御系统，终端检测响应，主机防病毒软件等等。

这些主机内部的自我防御手段都在主机内部运行，目的是发现和阻断主机内部的威胁，阻断其对主机造成进一步的损害。

**（3）失陷主机监测体系**

失陷主机是指被黑客成功入侵或已经感染病毒的主机，失陷主机监测体系的职能是发现和定位网络中的失陷主机。外围防御和主机自我防御两个防御层级是比较清晰和容易理解的，在现有网络安全防御系统里我们很容易找到与之相关的安全产品实体。而失陷主机监测体系是我们类比人类疾控体系提出的一个独立的防御层级，我们认为该层级的防御职能在传统的安全模型中没有得到与其重要性相匹配的重视程度，只是作为一种附属的安全功能零散地出现在其他产品中。

将失陷主机监测体系设立为独立防御层级的必要性分析如下：

**a) 网络风险防控体系完备性要求**

作为完备的网络安全防御体系，对前置防御层级（指外围防御和主机自我防御）失效所带来的风险，必须具备进一步的对抗措施。失陷主机监测实质上是对前置防御层级安全效果的独立监督和弥补，降低其失效带来的全局性安全风险。该防御层级应当是现代网络安全防御体系中必不可少的组成部分，**"失陷主机监测"职能的缺失意味着网络防御体系的结构性缺失。**

**b) 作为独立监测层级才能发挥实质监督作用**

失陷主机的出现本身意味着前置防御层级的失效，特别是"主机自我防御"的失效。无论前置防御层级如何改善和提升其防御能力和监测能力，我们不能再信赖"失效系统的自我监测"结果，而应该实施独立的监测才能起到"监督"的作用，与前置防御层级形成互补，成为防御体系里的最后一道防线。

**c) 主机失陷的必然性**

与人类防疫体系类似，当外围防御和主机自我防御均失效之后，内网主机存在很大的失陷概率，特别是对于大规模企业网络，由于整体攻击面的不确定性和不可控性，网络中存在失陷主机几乎是必然。从风险防控意识上看，我们也应该假设这个必然性的存在，而不是侥幸地认为可以幸免。

具体的说，内网中主机类型繁多，不同类型主机自我防御能力参差不齐，有些主机自我防御能力强，而有些则很弱，比如一些计算资源受限的物联网设备和一些不再接受安全更新的老旧系统，这就好比人群中的免疫力低下的"弱势群体"。从网络整体安全性角度来讲，针对缺乏自我防御能力的"弱势群体"实施失陷监测也是一种安全义务，有助于提升整体安全性。

**d) 失陷主机的危害性**

这一点是显然的，失陷主机类似于人群中的感染者，是黑客进一步对内网进行攻击的跳板，也是蠕虫式病毒传播的温床。失陷主机是埋藏在企业网络中的巨大安全隐患，由于失陷主机位置不确定、威胁程度也不确定，会给企业网络带来不可预测的全局性安全风险。

基于以上必要性分析，在网络安全防御体系中引入类似人类流行病监测系统的失陷主机监测系统，进行广泛的失陷主机监测，及时地发现和处置失陷主机，阻止其在内网中蔓延，可以降低恶性安全事故的发生概率，补足结构性短板，构建更加完善的网络安全防御体系。

**三、网络安全防御体系现状分析**

通过对大量企业的网络安全防御体系建设现状的调研，以及对当前网络安全市场上产品的分析，在这里我们给出一些观点：

**（1）**企业主要的安全投资集中于外围防御和主机自我防御层级，在内部失陷主机监测层级，也就是第三个防御层级投入不足，甚至是空白。

**（2）**从网络安全产品的市场占有率上看，也符合上述现实情况，外围防御和主机自我防御的相关产品是绝对主流。

**（3）**对于失陷主机的监测尚未成为独立的成熟产品形态，多以附属功能点存在于其他产品中，技术有效性还未充分验证，不论在市场还是在技术上都处于摸索进程中，存在巨大的市场机会。

我们认为这种现状符合网络安全防御体系的发展规律。任何一个复杂体系的建成都不是一蹴而就的，而是按照轻重缓急逐步构建的。从用户接受度上看，用户一定会优先考虑投入具有直接安全效益的产品，外围防御和主机自我防御更符合朴素的安全防护理念，就拿主机防病毒软件来说，对已经收录入病毒库中的病毒样本而言，其效果就类似特定的疫苗，效果是立杆见影的。从技术角度讲，外围防御和主机自我防御也是整个防御体系有效性的基础，优先投入是合理的。

但是从发展的眼光看待网络安全防御体系的建设，决不能止步不前。网络安全防御体系的发展和网络攻防技术的发展是密切关联的，互为推动力。攻击技术的进化必然推动防守技术的进化，安全防御体系作为防守技术的载体，也必须随着攻防形势的发展不断进步，任何防御层级都存在被攻破的可能，不与时俱进就一定会陷入被动局面。大量内网恶性网络安全事件的发生也印证了这个现实。

从大量企业建设现状来看，第三层级的防御体系建设，也就是失陷主机监测，还处于缺失或相对薄弱的状态。我们认为网络安全从业者都有必要重视和思考一个无法忽视的关键问题： 如果现有的外围和主机自我防御措施失效而导致内网主机失陷，下一步如何应对？我们的答案是不言而喻的，**构建失陷主机监测体系---最后一道防线，让网络安全防御体系没有结构性缺失。**

**四、失陷主机监测的技术路径分析**

失陷主机监测的目标是：**发现和定位网络中已经被黑客成功入侵、或被植入恶意软件的主机。**形象的讲就是发现隐藏在人群中的"感染者"。不论何种技术途径实现失陷主机监测，其核心都是获取"失陷证据"来证明主机失陷，这是基础。

**4.1 失陷证据类型分析**

定位失陷主机的核心是**"失陷取证"**，也就是提取可以证明主机失陷的证据。这里有必要对两种威胁监测相关的技术概念进行一下简要说明，威胁分析中有两类相近的威胁指征，第一种是"攻击指征(**Indicator of Attacks , IOAs**)"，IOAs是判定攻击在进行过程中的依据，IOAs的价值在于进行入侵过程的监测。还有一种"失陷指征(**Indicator of Compromise IOCs**)"，指可以证明主机曾经受到攻击的取证数据，IOCs的价值在于鉴别主机是否曾遭受攻击和是否失陷。二者之间的区别比较模糊，从失陷监测角度讲更关注IOCs方面的证据，而IOAs是主机入侵检测更加关注的指征类型，但笔者也认为，在具体的网络安全实践中，这两种指征的用途不一定会有明晰的界限，可能存在结合应用的情况，但在威胁发现层面上看，二者的目的是统一的，本文中不进行明确的区别对待。

技术实现上讲，失陷证据可能是下面两大类型：

**（1）内部证据**

内部证据指从主机内部提取到的证明主机失陷的证据，有下面的体现形式：

**a) 主机内部的遗留入侵证据**

一般而言任何黑客入侵和恶意软件感染，都一定会改变主机内部状态，留下入侵的蛛丝马迹。有些属于磁盘残留持久型证据，比如磁盘上二进制的病毒样本留存、注册表篡改痕迹等等，而有些属于非持久型的证据，比如内存篡改证据。对此类证据的提取需要依赖明确的**主机失陷指征（**比如病毒特征库/失陷指征库等**）**。这类证据属于直接失陷证据。

**b) 主机内部的异常行为特征**

指黑客或恶意软件进入主机内部之后，主机软硬件系统表现出来的区别于正常行为的动态特征，比如异常注册表访问动作、启动恶意进程运行、内核漏洞探测动作等等，提取此类证据需要对主机内核、进程的行为进行记录，并与明确的动态失陷指征作比对，作为失陷的直接证据。还有一些体现主机内部异常状态的数据可作为辅助判断依据，比如高CPU利用率，某些关键文件的高频访问，高磁盘IO占用率等等，可以提示主机异常，但一般不能作为失陷直接证据。

**(2) 外部证据**

外部证据主要是指**可以用作失陷证据的"主机与外界的网络通信数据"**，这类通信数据可以分为两类：

**a) 入侵过程的历史通信数据**

指主机被入侵过程中的历史网络通信数据，通常由流量审计系统记录，可以用于定位主机的历史网络通信中是否存在入侵痕迹，以及进行事后溯源。这类数据属于间接失陷证据。

**b) 主机被入侵后的可疑网络通信数据**

基于黑客的贪婪性，一般会尝试对失陷主机实施长期控制，有些还会利用失陷主机实施内网横向移动，这一切都离不开网络通信，因此失陷主机一般会表现出来一些异常的网络行为，比如与控制服务器之间进行隐秘通信，以及对失陷主机所在网络进行进一步的横向探测和攻击。此类异常通信数据也可以作为主机失陷的间接证据。

**4.2 失陷主机监测技术途径分析**

失陷证据提取是失陷主机监测的基础，基于上面对失陷证据的类型分析，我们下面探讨一下有哪些可能的技术实现途径。

**4.2.1 基于内部证据的监测技术**

这类技术通过在主机内部部署取证模块，实现主机内部证据的提取。因为判定主机失陷的数据维度比较多，对系统所有内部行为都进行完整的行为记录，进行审计式和复盘式的失陷分析，在实际中是不现实，一般我们都是需要已知的失陷指征(IOCs)来判定主机是否失陷。

经过调研，我们对下列常见的主机内部的失陷取证维度进行举例：

(1) 系统中来源不明的未知文件、应用或进程

(2) 系统特权账户的异常活动

(3) 受到篡改的文件内容、系统配置项、注册表键值

(4) 某些关键文件出现在不应当出现的目录中

(5) 异常的系统登录行为(比如:合法账号的大量失败登录，不存在账号的登录)

(6) 异常增加的数据库读取行为

(7) ...

上面我们已经提出我们的观点，内部证据提取依赖明确的失陷指征，而如何构建一个随着攻防形势及时更新，高覆盖率的失陷指征库是技术上的难点和壁垒，笔者认为这是一个人力密集型的长期积累的工作，很难靠技术实现自动化。另外，失陷指征库需要依赖行业共享才能真正取得长足的发展，靠单一厂商或研究机构均很难形成气候，这一点，从计算机病毒特征库的发展历程可以得到借鉴，安全厂商之间应该广泛进行指征数据交换，方能取长补短，形成合力。

**4.2.2 基于外部证据的监测技术**

这类技术利用实现失陷主机与外界之间的网络通信流量作为失陷证据，主机通信流量从内网管理的角度看，无非是两种类型：

a. 与外网主机之间的流量

b. 与内网主机之间的流量

外部监测技术的核心目标主要是对主机的网络行为进行捕获和分析，从中发现主机失陷的证据，本质上这类技术都属于基于流量的分析技术，根据我们的调研，主要有下面几种具体的表现方式。

**4.2.2.1 内网主机的外连行为分析**

简单的说就是分析内网主机是否与外网的恶意主机之间存在关联关系。

这类技术一般以威胁情报为支撑，在网关位置对内网主机的外向连接的目的地址，URL，dns解析记录等信息与威胁情报库进行比对。 其核心技术是威胁情报本身，有效性也完全取决于威胁情报本身的质量。优点是实现方式简单，如果威胁情报源可靠，则输出结果可信度很高。缺点是基于先验知识工作，漏报率不可评估。目前这种技术一般只是防火墙，态势感知，流量分析系统等产品的附属功能模块。

**4.2.2.2 全流量分析**

该类产品的宣传理念是：对内网主机的网络流量进行全量捕获，并进行流量内容分析，行为分析，从中发现主机的异常通信行为，定位失陷主机。这类产品诱人之处是：给客户一种能全面进行流量检查的能力，仿佛拥有上帝视角，没有遗漏。事实上，从安全价值来看，这种技术与网络入侵监测系统没有本质区别，只不过该类产品强调了一个全流量检测的优势，观测的内容更全面。

我们认为这类型产品存在下列的问题

a）全流量捕获的技术基础有问题

全流量捕获一般通过交换机镜像端口提取流量，镜像端口的带宽与交换机背板的理论带宽不在一个量级，除非是在小流量环境，否则无法保证不丢失报文实现全流量捕获。在企业网络中实现真正的全流量捕获的部署难度大，所消耗的软硬件资源会非常多。实践中，一般都只能实现在某几个关键交换机上部署，实现局部的流量监控。

b) 在海量数据中筛选出有效信息的效率和有效性存疑，漏保误报问题依然存在

c）很难发现未知攻击行为

**4.2.2.3 基于网络蜜罐的内网失陷主机发现技术**

网络蜜罐从诞生以来，就一直是网络安全界进行安全研究的重要工具，但受制于一些原因，却一直未能成为主流安全产品。安全厂商，特别是反病毒厂商和威胁情报厂商，都会在因特网上部署大量蜜罐进行样本采集和威胁情报采集，这足以证明蜜罐技术本身的价值。至于在内网部署蜜罐作为威胁感知工具则是最近几年才开始逐步受到重视和推广。

根据我们大量的内网蜜罐部署实践，在内网失陷主机发现上，蜜罐确实可以发挥很好的作用，其最大的特点是判定准确度高，几乎不会出现误报。另外，与其他被动流量分析技术不同的是，在内网使用蜜罐技术需要在原有网络中增加蜜罐主机，实质上对内网的结构进行了主动的重构，这是一种主动防御技术，具备捕获0day威胁的能力。

蜜罐技术在内网的部署会遇到的问题和解决途径，总结如下：

**a. 蜜罐IP部署策略问题**

由于攻击者的位置不明，蜜罐部署位置的设计非常重要，不合理部署方案会挂一漏万，导致实际监测效果不佳。理想的部署方案是进行宽覆盖面的就近部署。蜜罐IP的有效性可以通过一个技术参数进行度量，就是主机间IP地址间距（指两个IP地址之差的绝对值）。蜜罐IP地址与其余主机IP地址的间距越小效果越明显，越远效果越差。因此，合理的蜜罐IP选择方式应该是让蜜罐IP尽可能均匀分布于用户的IP地址空间中。在实践中，一般采取按C网段进行部署，尽可能保证每个C段大小的区间里至少有一个蜜罐IP。这就是我们提出的**C段覆盖法。**

**b.** **蜜罐与攻击意图之间最大化匹配问题**

由于攻击者意图不明，蜜罐服务与如何与攻击意图进行匹配是一个难题，蜜罐投放种类的设计也是一个重要问题。这个问题的解决途径有几个。一是厂商提供尽可能多的现成蜜罐交互模块供用户选择，根据用户网络中可能开放的服务端口进行高交互的相似服务部署，有些时候需要根据用户实际情况进行定制，这种部署策略的合理性在于，我们诱捕到的攻击情报有极大的针对性和说服力，缺点是对未开放的端口的诱捕没有能力实施。二是进行宽端口范围的开放性诱捕，一般在实践中采取开放全量端口进行TCP交互，并在重点端口部署低交互模块进行重点盯防。三是根据实际诱捕效果进行快速动态调整蜜罐的投放，比如现场采集到TCP7001端口扫描，而此前部署没有TCP7001的交互模块，马上通过快速的投放措施将Weblogic交互模块投放到现场，实施进一步诱捕。以上几种方案均经过实践验证，可以达到良好的诱捕和监测效果。

**c. 蜜罐吸引力下降的问题**

一个蜜罐投放到网络中之后，其对攻击者的吸引力会不可避免地逐渐下降，导致监测效果降低。对该问题的解决方式是实施动态的蜜罐投放策略，动态变化蜜罐IP，蜜罐开放的服务，保持其对攻击者的吸引力。

**d. 取证数据质量问题：**

蜜罐投放到现场后，根据攻击交互深度，取证数据的质量会参差不齐，并不是所有取证数据都具有显明的攻击特征，属于模糊证据。这个问题的解决除了投放更有针对性的蜜罐提升取证数据质量，也取决于用户的安全意识，跟所在网络要求的安全级别有关，有些高级的攻击方式往往体现得更加隐蔽，一些模糊的看似低危的探测行为后面往往隐藏着更加高级的攻击行为。

**五、失陷主机监测技术的有效性评估**

前文已经说过，失陷主机监测并不是一个全新的东西，在其他产品里也有零散的功能点存在，如果一个产品宣称自己能发现失陷主机，或者用户需要在网络中部署类似产品，有哪些维度可以评价其有效性，这是一个值得思考的问题。笔者的观点是，可以从下面几个维度进行评价:

（1) **监测覆盖范围**：尽可能宽的失陷主机监测范围是失陷主机监测一个重要指标，监测范围的宽与窄意味着是否存在结构性的监测盲区，盲区即隐患。

(2) **取证数据质量:** 失陷主机监测的核心是失陷取证，那么失陷证据的可信度是决定其实际可用性的重要指标，因为失陷主机的处置是有实施成本的，有时候甚至需要中断业务进行恢复，高可信度的取证数据才能形成足够驱动力，驱使安全管理员进行失陷主机处置。

(3) **未知攻击取证能力:** 这是一个增强型的评价指标，在失陷主机监测上很重要，因为主机失陷有很大概率是因为未知的攻击行为导致，失陷后实施的进一步攻击行为也很可能是未知的。

(4) **失陷处置能力:** 是否给用户提供明确的、合理的失陷主机处置方法或建议。发现的目的不仅是发现，对用户来说解决问题才是最终目标。如果在监测的基础上能够根据监测结果提供进一步的处置方案，是一个加分项。

(5) **技术独立性:** 所采用的失陷监测产品和前置防御层级产品(指主机防御产品或网关类产品)是否使用相同的底层技术进行威胁监测，比如：都是通过病毒特征检查发现可疑文件，则属于同一类技术，不具备技术独立性，属于减分项。另外，在不同层级也不建议完全采用同一厂商来源的产品，避免技术上的同质化，无法形成实质上有效的独立监督，不同类型的防御产品共同部署，更有利于形成互补。