金融行业

6 月报
2020 年

安全月报

政策解读 | 行业研究 | 漏洞聚焦 | 安全态势

绿盟科技金融事业部出品

政策解读

《网络安全等级保护定级指南》解读

行业研究

【云原生技术研究】BPF使能软件定义内核

个人社工防护二三事

大敌当前“邮件安全你意识到了吗?

刷单再现支付陷阱,“高倍镜”找出破绽!

中信银行泄露用户流水引“众怒”隐私安全离我们还有多远?

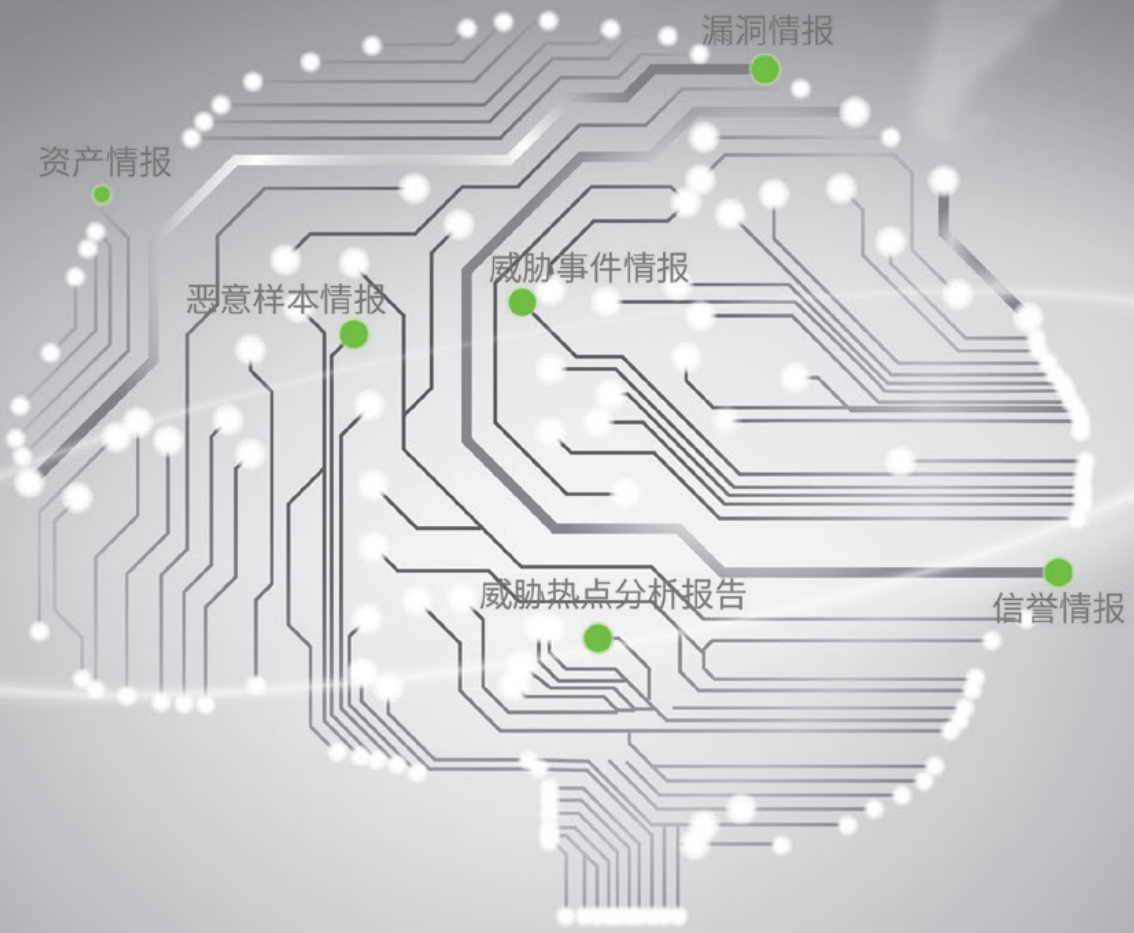
NSFOCUS

绿盟科技威胁情报平台NTI

智慧的大脑

智能 敏捷

Hot products at RSA 2017



强大的威胁捕获能力、精准的威胁预警能力、全面的威胁防御能力

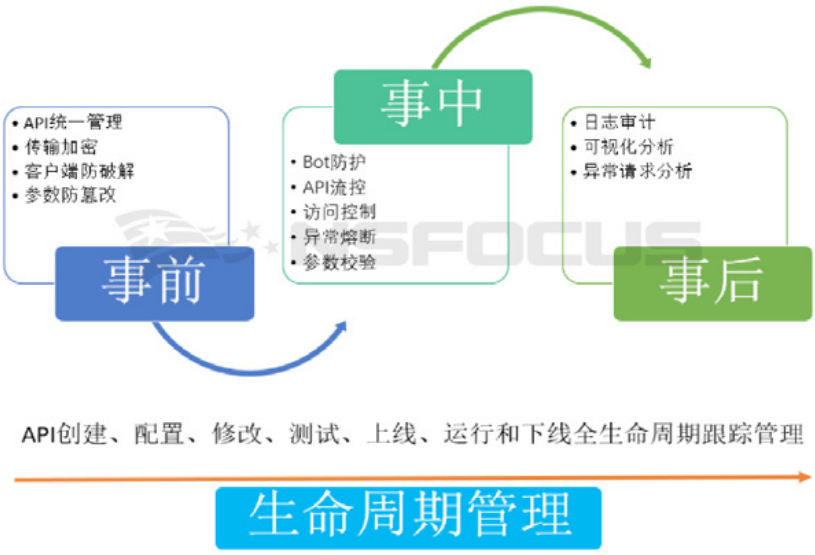
洞察威胁知己知彼，助力安全运营提升

NSFOCUS绿盟科技

本|期|看|点

P04 《网络安全等级保护定级指南》解读

P9 《商业银行应用程序接口安全管理规范》解读



安全月报

2020年第6期

绿盟科技金融事业部

安全月报在线阅读

绿盟科技官方微信

目录 CONTENTS

政策解读

行业研究

漏洞聚焦

安全态势

NSFOCUS

政策解读

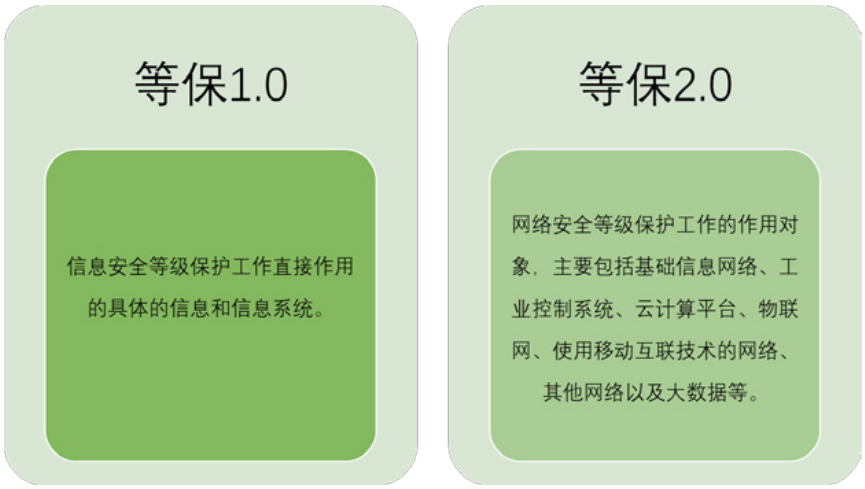
《网络安全等级保护定级指南》解读

2019年12月1日网络安全等级保护2.0国家标准的正式实施，标志着我国网络安全等级保护制度进入了全新时代。作为国家等级保护标准体系的核心标准之一的GB/T 22240-2020《信息安全技术 网络安全等级保护定级指南》（以下简称“定级指南”）于2020年4月28日发布，2020年11月1日正式实施。定级指南规定了非涉及国家秘密的等级保护对象的定级方法和流程，通过指导网络运营者合理划分定级对象和准确的确定安全保护等级，为后续的安全建设整改、等级测评等工作奠定了良好的基础。

新版定级指南在等级保护1.0定级指南的基础上，对等级保护对象做了新的定义，增加了对云大物移工等场景的说明，修改了定级流程，以适应新形势下等级保护工作的需要，有力推动了等级保护工作的开展。

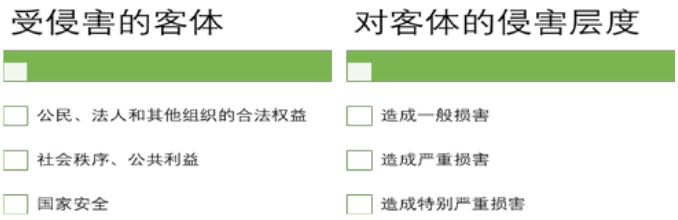
等级保护对象新的定义

在GB/T 22240-2008中，等级保护对象被定义为：“信息安全等级保护工作直接作用的具体信息和信息系统”，但这只是符合当时的技术发展状况和等级保护工作需求。近年来，随着云计算平台、物联网和工业控制系统等新形态的等级保护对象不断涌现，原定义内涵的局限性日益显现，无法全面覆盖当前的等级保护工作对象，需要进一步扩充和完善以适应当前工作的需要。



定级要素与安全保护等级新关系

依据安全保护等级的定义，定级应综合考虑“等级保护对象在国家安全、经济建设、社会生活中的重要程度，以及一旦遭受到破坏、丧失功能或者数据被篡改、泄露、丢失、损毁后，对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的侵害程度等因素。”因此本标准中明确等级保护对象的定级要素为两个，分别为“受侵害的客体”和“对客体的侵害程度”。



定级要素与安全保护等级的关系如下表所示。

受侵害的客体	对客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第二级
社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

注：根据2019年网络安全等级保护和关键信息基础设施保护大会相关专家介绍，当公民、法人和其他组织的合法权益受到特别严重损害时，等级保护对象定级由征求意见稿中的三级重新更正为二级。

等级保护对象新特征

作为等级保护对象的网络应具有如下基本特征：

a) 具有确定的主要安全责任主体；

b) 承载相对独立的业务应用；

c) 包含相互关联的多个资源。

在确定定级对象时，基础信息网络、工业控制系统、云计算平台、物联网、

采用移动互联技术的网络和大数据在满足以上基本特征的基础上，需要满足以下要求。

云计算平台

- 在云计算环境中，应将云服务方侧的云计算平台单独作为定级对象定级，云租户侧的等级保护对象也应作为单独的定级对象定级。
- 对于大型云计算平台，应将云计算基础设施和有关辅助服务系统划分为不同的定级对象。

物联网

- 物联网主要包括感知、网络传输和处理应用等特征要素，应将以上要素作为一个整体对象定级，各要素不单独定级。

工业控制系统

- 工业控制系统主要包括现场采集/执行、现场控制、过程控制和生产管理等特征要素。其中，现场采集/执行、现场控制和过程控制等要素应作为一个整体对象定级，各要素不单独定级；生产管理要素可单独定级。
- 对于大型工业控制系统，可以根据系统功能、责任主体、控制对象和生产厂商等因素划分为多个定级对象。

采用移动互联技术的系统

- 采用移动互联技术的网络主要包括移动终端、移动应用、无线网络等特征要素，应与相关有线网络业务系统作为一个整体对象定级。

通信网络设施

- 对于电信网、广播电视传输网、互联网等基础信息网络，应分别依据服务类型、服务地域和安全责任主体等因素将其划分为不同的定级对象。
- 跨省业务专网可作为一个整体对象定级，也可以分区域划分为若干个定级对象。

数据资源

- 大数据应作为单独定级对象进行定级；安全责任主体相同的大数据、大数据平台和应用可作为一个整体对象定级。

特殊对象的定级说明

对于基础信息网络、云计算平台、大数据平台等支撑类网络，应根据其承载或将要承载的等级保护对象的重要程度确定其安全保护等级，原则上应不低于其承载的等级保护对象的安全保护等级。

对于数据资源，应综合考虑规模、价值等因素，及其遭到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的侵害程度等因素确定其安全保护等级。涉及大量公民个人信息以及为公民提供公共服务的大数据平台/系统，原则上其安全保护等级不低于第三级。

定级新流程

对于新建网络、运营者应当依照等级保护相关法律法规要求和本标准，在规划涉及阶段确定其安全保护等级；对于跨省或者全国统一联网运行的网络可以由行业主管（监管）部门统一组织定级工作。安全保护等级初步确定为第二级及以上的等级保护对象，其运营者应当依据标准要求分别进行专家评审、主管部门核准和公安机关备案审核，最终确定其安全保护等级。

专家评审：定级对象的运营、使用单位应组织信息安全专家和业务专家等，对初步定级结果的合理性进行评审，并出具专家评审意见 。

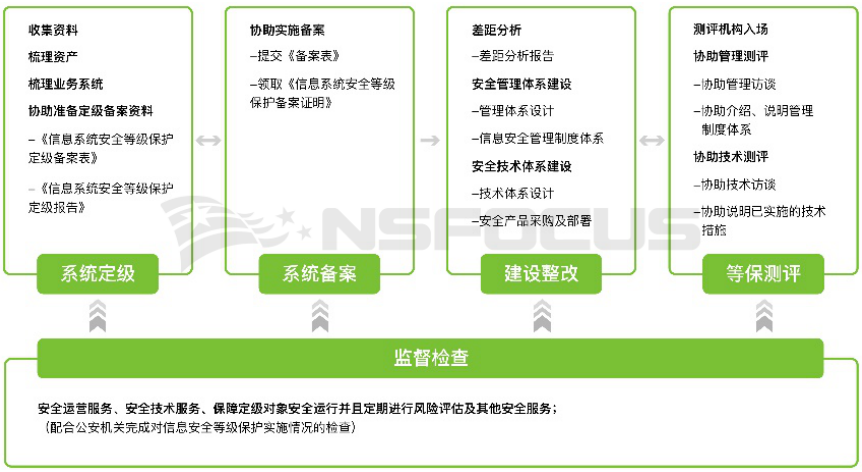
主管部门审批：定级对象的运营、使用单位应将初步定级结果上报行业主管部门或上级主管部门进行审批、审核。

公安机关审核：定级对象的运营、使用单位应按照相关管理规定，将初步定级结果提交公安机关进行备案审查，审查不通过，其运营使用单位应组织重新定级；审查通过后最终确定定级对象的安全保护等级。

绿盟科技咨询服务

等级保护的各个阶段有着不同的工作重点，绿盟科技凭借着深厚的技术实力和丰富的安全服务项目经验，在定级备案阶段，对涉及的定级对象单位基本情况，定级对象基本情况、侵害情况及相关定级备案的材料进行整理，协助客户确定信息系统等级保护级别，填写备案表及相关材料，完成定级备案过程。

针对等级保护其他阶段同时可提供专业的等保咨询服务、安全防护产品、安全技术服务和安全运营服务。为传统环境、云计算、工业控制系统、物联网等各种场景的安全等级保护建设、提供全流程的保驾护航。



《商业银行应用程序接口安全管理规范》解读

一、前言

在API技术发展的大趋势下，API的使用呈现指数级增长，从2014年的26%，增长到2018年的69%，超过html流量的4倍（数据来源：《2018年互联网安全状况报告：撞库攻击》）。但API流量的安全性被忽视已经是一个不可回避的现状，API安全也成为了安全界的热门话题。在2020年RSA大会上，API安全成为行业热门议题。API接口复杂，缺乏对常见漏洞的检查和对传输数据的检测是造成API脆弱的重要原因。

2020年2月13日，中国人民银行发布了《商业银行应用程序接口安全管理规范》（JR/T 0185—2020）（下简称《规范》）。《规范》的实施满足了在平衡服务快速响应与金融信息保护能力基础上，对商业银行应用程序接口的接口设计、应用部署、集成运行、运维监测及系统下线等全生命周期过程提出安全技术与安全管理要求，为其提供了信息安全技术保障。

二、《规范》定义

三类用途：商业银行使用的API类型主要分为内部API、企业定制API与外部API三种类型。本标准主要关注外部API，即本标准所述的商业银行接口。

两种形态：服务端到服务端、客户端SDK到服务端两种形态API。

三个参与方：用户、应用方以及商业银行。

三、规范要点

绿盟科技建议从几个方面对API安全建设重点关注：

01 接口类型与安全级别

接口按照应用集成方式，分为服务端对服务端集成和移动终端对服务端集成。不同接口实行不同等级安全保护，《规范》尤其提到，对于资金交易和账户信息查询应用类接口需实施高等级安全保护，其中需要特别关注移动终端直接调用银行API。

02 安全设计

主要强调了动态防御加交互安全从源头减少风险。应具备API调用的认证&授权能力、访问控制能力、动态防护、防篡改、客户端可信校验能力，交互安全可以如何做到替换原文、敏感信息等明文信息。

绿盟业务安全网关（NSFOCUS BMG）具备动态防御、交互安全的能力。在致力于动态安全能力提升的同时，也具备提交数据混淆，在客户端对敏感数据、隐私信息进行加密传输的能力，有效解决了敏感信息交互安全的需求。

绿盟安全认证网关（NSFOCUS SAG）具备对API和应用统一认证授权、访问控制、传输加密、日志审计等能力。商业银行可利用绿盟安全认证网关根据不同应用方需求，对API做最小化授权管理，并且产品支持多因子认证，可对调用的应用身份和用户身份进行统一鉴权，执行严格的访问控制和流控策略。在数据传输安全上，安全认证网关支持TLS流量加密，且支持国密算法，防止流量劫持和内容篡改，降低数据泄露风险。此外，还会对所有API访问进行详细记录，以供全面审计。

03 安全部署

互联网边界部署除防火墙、IDS/IPS、DDoS防护之外，当前金融行业API面临严重的自动化攻击威胁，还有必要采取机器自动化防护设备对自动化请求流量进行清洗，并配置流控策略防止API滥用。同时商业银行应注意提高API权限管控力度、API攻击防护能力和监控能力，可利用API网关统一管理对外API接口，将API调用的最小化授权、流控、日志记录等通用安全能力整合起来，加强API安全的同时提高安全运维效率。

04 安全咨询

运行安全部分要求对API有效期控制（单次有效性、阶段有效性、协议期有效性），应用方安全中明确指出了防止接口滥用大额监控，异常交易监控。

为了解决API有效性验证，绿盟业务安全网关（NSFOCUS BMG）的动态令牌能够实现API访问合规校验，阻止代理人攻击、非法重复调用等问题。

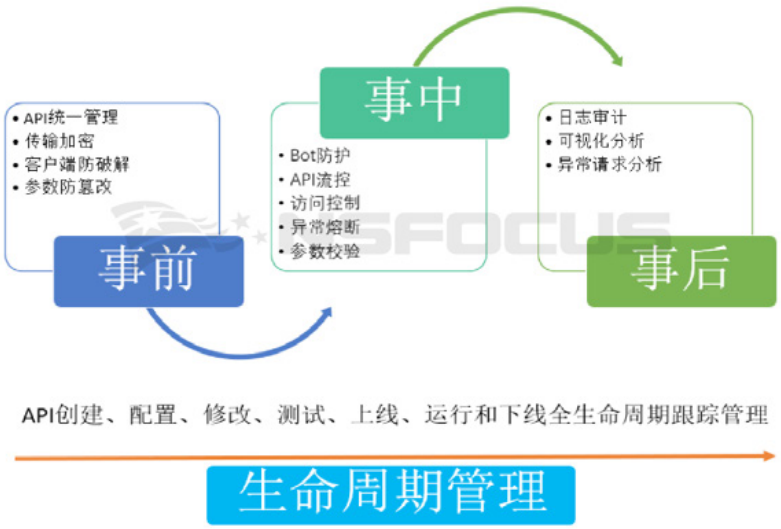
通过机器自动化流量的防护，能够有效解决API滥用，防止模拟器非法调用业务接口干扰正常业务办理。

业务安全网关（NSFOCUS BMG）能够智能学习API参数的特征，及时对篡改后的参数、异常范围的API参数进行预警，能够防护业务逻辑设计不充分带来的各种安全隐患。

绿盟安全认证网关（NSFOCUS SAG）能将企业的API资产进行统一管理，提高安全运营效率。同时会实时监控API调用情况，当发现异常接口调用，可结合限流、访问控制能力做出事件响应，终止API调用，实施熔断操作，可及时暂停服务调用，拒绝交易等。

四、小结

《规范》指出当前API安全主要面临API生命周期管理、API提交参数安全、API滥用防护三大问题。绿盟科技认为API安全的防护的体系如下：



做好API的全生命周期管理，防护因授权问题导致的未授权访问、API泄露等问题，以及代码审计不严格带来的系统性风险。

在事前、事中、事后三个环节充分重视各自对应的安全问题，在事前对API做统一管理，加密数据传输，加强API的防破解能力，防篡改能力；事中，对授权进行严格鉴定、做精准API流量控制和访问控制，重视参数校验和Bot防护，及时发出异常流量告警并执行熔断；事后，加强API的可视化分析能力，异常请求的分析能力，记录全面日志供审计。

API是银行业推进数字化经济转型顶层规划和指导中最具参考性和执行性的标准之一，《规范》从技术模式、安全设计、安全管理等多个方面阐述了商业银行API建设的方式，《规范》同时也是中国银行业进一步提升金融科技实力的催化剂，数字化经济转型的助推剂。助力商业银行搭建全球中小企业互联互通平台，促进一带一路金融战略布局。

NSFOCUS

行业研究

【云原生技术研究】BPF 使能软件定义内核

江国龙

摘要

BPF通过一种软件定义的方式，将内核的行为和数据暴露给用户空间，开发者可以通过在用户空间编写BPF程序，加载到内核空间执行，进而实现对内核行为的灵活管理和控制。

在计算机系统中，包过滤器通常有一个特定的用途，那就是提供给应用程序来监控系统的网络与内核运行的相关信息。这些监控程序对于系统的开发者、运维者、或者是安全管理者，都有着重要的意义。

有了更加细粒度的网络数据和内核运行数据，对于开发者来说，就可以根据当前系统的运行情况，合理的优化程序，提高程序的性能同时降低资源开销；对于系统运维者来说，能够拿到精确全面的系统运行数据，可以更好的对系统进行监控，保证系统的可靠性与高可用性；对于安全管理者来说，可以从这些网络和内核行为中，发现异常，进而在攻击行为发生的早期，发现攻击并且能够快速的进行响应和修复。

BPF（Berkeley Packet Filter）就是这样的一种包过滤器，从其诞生之初，就引起了人们的广泛关注与应用，尤其是近年来，随着微服务和云原生的发展和落地，BPF更是成为了内核开发者最受追捧的技术之一。

1. BPF概述

BPF（BSD Packet Filter）是很早就有的Unix内核特性，最早可以追溯到1992年发表在USENIX Conference上的一篇论文[1]。作者描述了他们如何为Unix内核实现一个网络包过滤器，这种实现甚至比当时最先进的包过滤技术快20倍。

随后，得益于如此强大的性能优势，所有Unix系统都将BPF作为网络包过滤的首选技术，抛弃了消耗更多内存和性能更差的原有技术实现。后来由于BPF的理念逐渐成为主流，为各大操作系统所接受，这样早期“B”所代表的BSD便渐渐淡去，最终演化成了今天我们眼中的BPF（Berkeley Packet Filter）。比如我们熟知的Tcpdump，其底层就是依赖BPF实现的包过滤。

关于BPF的发展历史，网上已经有很多文章进行了比较详尽的解释和描述，本文就不再过多的进行介绍，感兴趣的读者可以自行搜索，或者参照参考文献[2]。

本文重点要介绍的是自2014年，对传统的BPF进行扩展进化后的BPF。得益于BPF在包过滤上的良好表现，Alexei Starovoitov对BPF进行彻底的改造，并增加了新的功能，改善了它的性能，这个新版本被命名为eBPF（extended BPF），新版本的BPF全面兼容并扩充了原有BPF的功能。因此，将传统的

BPF重命名为cBPF（classical BPF），相对应的，新版本的BPF则命名为eBPF或直接称为BPF（后文所有的eBPF，均简化描述为BPF）。Linux Kernel 3.15版本开始实现对eBPF的支持。

BPF针对现代硬件进行了优化和全新的设计，使其生成的指令集比cBPF解释器生成的机器码更快。这个扩展版本还将BPF VM中的寄存器数量从两个32位寄存器增加到10个64位寄存器。寄存器数量和寄存器宽度的增加为编写更复杂的程序提供了可能性，开发人员可以自由的使用函数参数交换更多的信息。这些改进使得BPF比原来的cBPF快四倍。这些改进，主要还是对网络过滤器内部处理的BPF指令集进行优化，仍然被限制在内核空间中，只有少数用户空间中的程序可以编写BPF过滤器供内核处理，比如Tcpdump和Seccomp。

除了上述的优化之外，BPF最让人兴奋的改进，是其向用户空间的开放。开发者可以在用户空间，编写BPF程序，并将其加在到内核空间执行。虽然BPF程序看起来更像内核模块，但与内核模块不同的是，BPF程序不需要开发者重新编译内核，而且保证了在内核不崩溃的情况下完成加载操作，着重强调了安全性和稳定性。BPF代码的贡献单位主要包括Cilium、Facebook、Red Hat以及Netronome等。

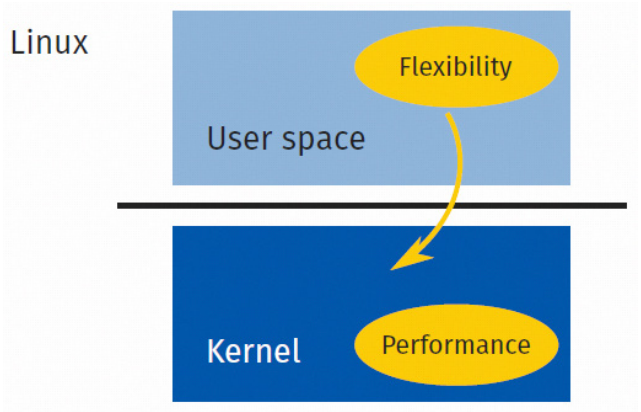


图1 Software Define Kernel

BPF使得更多的内核操作可以通过用户空间的应用程序来完成，这恰恰是与软件定义的架构和理念不谋而合。软件定义强调将系统的数据平面和控制平面进行分离，控制平面实现各种各样的控制和管理逻辑，而数据平面则专注于高效快速的执行，控制平面和数据平面通过特定的接口或协议进行通信。

因此，笔者认为，BPF正是设计和实现了一种对内核进行软件定义

（Software Define Kernel）的方式。控制平面是用户空间的各种BPF程序，实现BPF程序在内核的跟踪点以及执行逻辑；数据平面则是内核各种操作的执行单元，这些跟踪点可以是一个系统调用，甚至是一段确定的实现代码；控制平面和数据平面通过bpf()系统调用进行通信，将用户空间的控制平面逻辑，加在到内核空间数据平面的准确位置。

这种软件定义内核的设计和实现，极大的提高了内核行为分析与操作的灵活性、安全性和效率，降低了内核操作的技术门槛。尤其在云原生环境中，对于云原生应用的性能提升、可视化监控以及安全检测有着重要的意义。

2. BPF原理与架构

众所周知，Linux内核是一个事件驱动的系统设计，这意味着所有的操作都是基于事件来描述和执行的。比如打开文件是一种事件、CPU执行指令是一种事件、接收网络数据包是一种事件等等。BPF作为内核中的一个子系统，可以检查这些基于事件的信息源，并且允许开发者编写并运行在内核触发任何事件时安全执行的BPF程序。

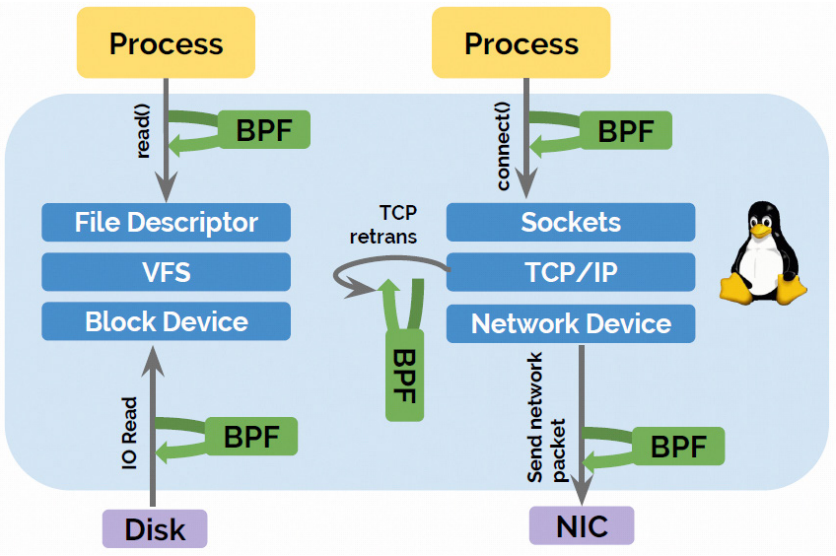


图2 BPF在Linux中挂载示例

图3简要描述了BPF的架构及基本的工作流程。首先，开发者可以使用C语言（或者Python等其他高级程序语言）编写自己的BPF程序，然后通过LLVM或者GNU、Clang等编译器，将其编译成BPF字节码。Linux提供了一个bpf()系统调用，通过bpf()系统调用，将这段编译之后的字节码传入内核空间。

传入内核空间之后的BPF程序，并不是直接就在其指定的内核跟踪点上开始执行，而是先通过Verifier这个组件，来保证我们传入的这个BPF程序可以在内核中安全的运行。经过安全检测之后，Linux内核还为BPF字节码提供了一个实时的编译器（Just-In-Time，JIT），JIT将确认后的BPF字节码编译为对应的机器码。这样就可以在BPF指定的跟踪点上执行我们的操作逻辑了。

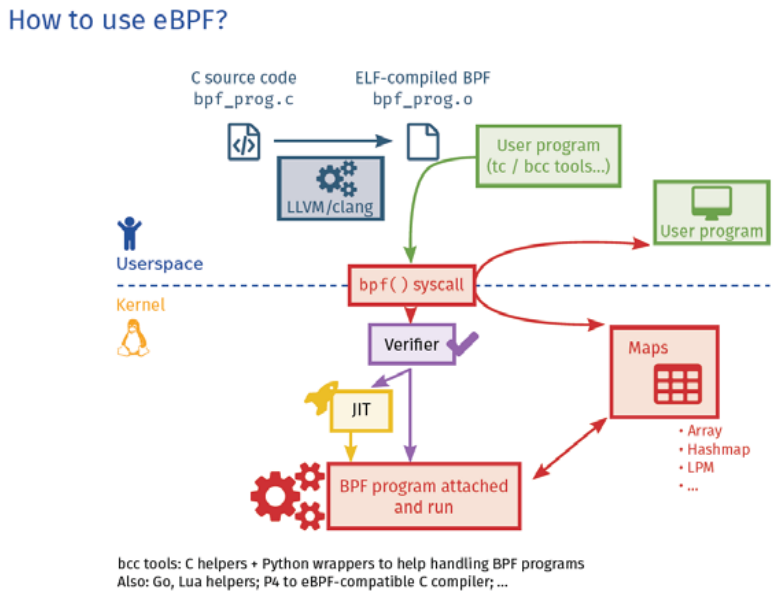


图3 BPF架构与流程图

那么，用户空间的应用程序怎么样拿到我们插入到内核中的BPF程序产生的数据呢？BPF是通过一种MAP的数据结构来进行数据的存储和管理的，BPF将产生的数据，通过指定的MAP数据类型进行存储，用户空间的应用程序，作为消费者，通过bpf()系统调用，从MAP数据结构中读取数据并进行相应的存储和处理。这样一个完整BPF程序的流程就完成了。

3. BPF Hello World

下面我们通过一个Hello World例子，来对上述各个步骤进行展开介绍。这个示例将完成下面的操作：当内核执行某一系统调用时，打印“Hello, BPF World！”字符串。

首先我们先使用C语言编写一段完成上述功能的BPF代码bpf_program.c：

```
1 #include <linux/bpf.h>
2 #define SEC(NAME) __attribute__((section(NAME), used))
3
4 SEC("tracepoint/syscalls/sys_enter_execve")
```

```
5 int bpf_prog(void *ctx) {
6 char msg[] = "Hello, BPF World!";
7 bpf_trace_printk(msg, sizeof(msg));
8 return 0;
9 }
10
11 char _license[] SEC("license") = "GPL";
```

首先，我们需要声明BPF程序什么时候执行，这里有一个跟踪点（Tracepoints）的概念，跟踪点是内核二进制代码中的静态标记，允许开发人员注入代码来检查内核的执行。代码的第4行就是指出我们这个BPF程序的跟踪点是什么。在BPF的语法中，使用SEC标识跟踪点，在本例中，我们将在检测到执行execve系统调用时运行这个BPF程序。

代码的5—9行，定义了我们在这个追踪点需要执行的操作，也就是每当内核检测到一个程序执行另一个程序时，将打印消息“Hello, BPF World！”

然后我们将使用clang将这个程序编译为成一个ELF二进制文件，这是内核能够识别的一种文件格式。clang -O2 -target bpf -c bpf_program.c -o bpf_program.o。

下面将这个已经编译好的BPF程序加载到内核中，现在我们已经编译了第一个BPF程序，我们使用内核提供的load_bpf_file方法，将上述编译好的bpf_program.o加载到内核。如下loader.c。

```
1 #include <stdio.h>
2 #include <uapi/linux/bpf.h>
3 #include "bpf_load.h"
4 int main(int argc, char **argv) {
5 if (load_bpf_file("hello_world_kern.o") != 0) {
6 printf("The kernel didn't load the BPF program\n");
7 return -1;
8 }
9 read_trace_pipe();
10 return 0;
11 }
```

使用如下方法编译我们loader文件。

```
TOOLS=/kernel-src/samples/bpf
INCLUDE=/kernel-src/tools/lib
PERF_INCLUDE=/kernel-src/tools/perf
KERNEL_TOOLS_INCLUDE=/kernel-src/tools/include/
clang -o loader -lelf\
 -I${INCLUDE} \
 -I${PERF_INCLUDE} \
 -I${KERNEL_TOOLS_INCLUDE} \
 -I${TOOLS} \
 ${TOOLS}/bpf_load.c \
 loader.c
```

然后运行sudo ./loader，我们的BPF程序就已经加载到内核中了。当我们停止这个loader程序时，上述BPF程序实现自动从内核中卸载。

4. BPF程序类型

通过上面的Hello World示例，我们已经对BPF程序有了一个初步的认识，那么接下来我们看一下，我们都能够用BPF来做什么？Linux内核当前提供了对哪些BPF程序类型的支持。

这里可以简单的将BPF程序的类型分为两个方面：内核追踪（Tracing）和内核网络（Networking）。

4.1 内核追踪（Tracing）

第一类是内核跟踪。开发者可以通过BPF程序更清晰的了解系统中正在发生的事情。从前文中的介绍可以看出，BPF可以通过各种类型的追踪点（TracePoint）访问与特定程序相关的内存区域，并从正在运行的进程中提取信息并执行跟踪。这样开发者就可以获取关于系统的行为及其所运行的硬件的直接信息，甚至还可以直接访问为每个特定进程分配的资源，包括从文件描述符到CPU和内存使用情况。

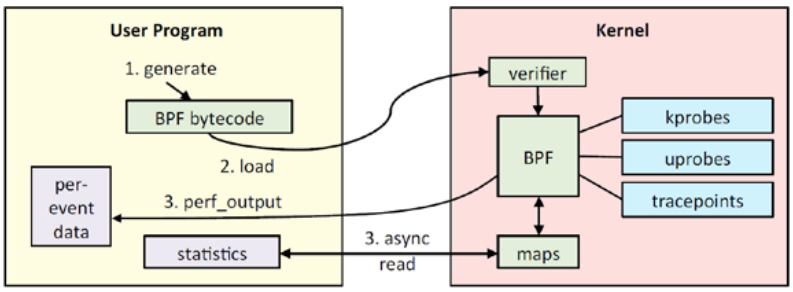


图4 BPF内核行为追踪

BPF对内核行为的追踪，可以通过静态的追踪点，kprobes或者是uprobes等动态的追踪点，实现整个系统的可观察性（Observability），进而可以进行系统的性能分析、调试以及安全的检测与发现。

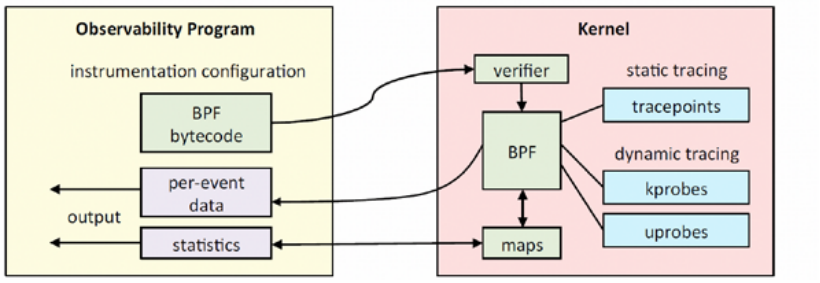


图5 BPF Observability

在安全检测上，我们可以将BPF程序的追踪点加载到一些关键并且不是很频繁的内核行为上，比如一个新的TCP/UDP会话的创建、启动了新的进程、特权提升等，这样就可以通过对这些行为的监控，进行异常检测。

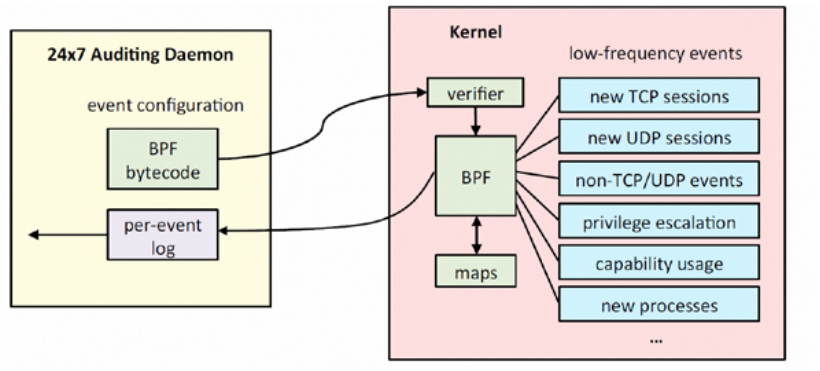


图6 BPF实现主机入侵检测

4.2 内核网络(Networking)

第二类程序是对内核网络的操作。BPF程序允许开发者监控并且操作计算机系统中的网络流量，这也是BPF原始设计时的核心功能点。BPF允许过滤来自网络接口的数据包，甚至完全拒绝这些数据包。不同类型的BPF程序可以加载到内核网络中不同的处理阶段。

比如，开发者可以在网络驱动程序收到包时立即将BPF程序附加到这一网络事件上，并根据特定的过滤条件，对符合条件的数据包进行处理。这种数据包的处理和过滤可以直接下沉到物理网卡上，利用网卡的处理单元（Network Processor），进一步降低主机在数据包处理上的资源开销。

当然，这种灵活的数据包处理方式有优点也有缺点。一方面，当收到数据包之后，我们在越早的阶段处理，可能在资源消耗上越有优势，但是这个时候，内核还没有将足够的信息提供我们，我们对这个数据包的信息了解的就很少，这对下一步的处理决策有着一定的影响。另一方面，我们也可以在网络事件传递到用户空间之前将BPF程序加载到网络事件上，这时，我们将拥有关于数据包的更多信息，并且有助于做出更明智的决策，但这就需要支付完全处理数据包的成本。

这里我们简单举个例子，如下图所示，在容器等虚拟化环境中，我们可以将BPF程序附着在包括物理和虚拟的网络设备上，这样就能够根据实际的业务场景以及网络通信需求，实时动态的设置和更新网络通信规则，实现对数据包的过滤。而这种包过滤，当前容器网络更多的是通过Iptables来实现的，那么一旦规模达到一定量级之后，不论是在规则管理上，还是在资源消耗上，都将带来巨大的负担和隐患。

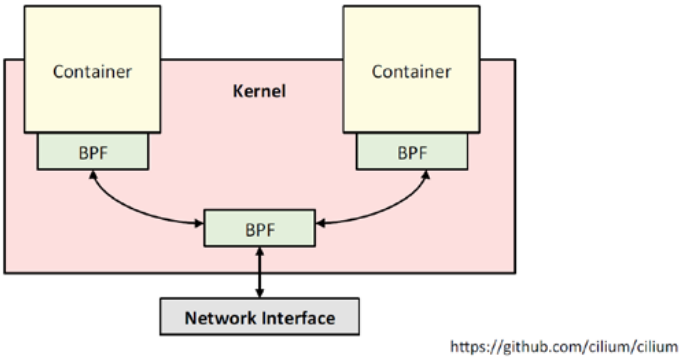


图7 BPF实现容器网络安全

BPF在网络数据包的处理上，通常会与Linux内核的另外一个重要功能XDP一起来实现。XDP（Express Data Path）是一个安全的、可编程的、高性能的、内核集成的包处理器，它位于Linux网络数据路径中，当网卡驱动程序收到包时，就会执行BPF程序，XDP程序会在尽可能早的时间点对收到的包进行删除、修改或转发到网络堆栈等操作。XDP程序是通过bpf()系统调用控制的，使用BPF程序实现相应的控制逻辑。

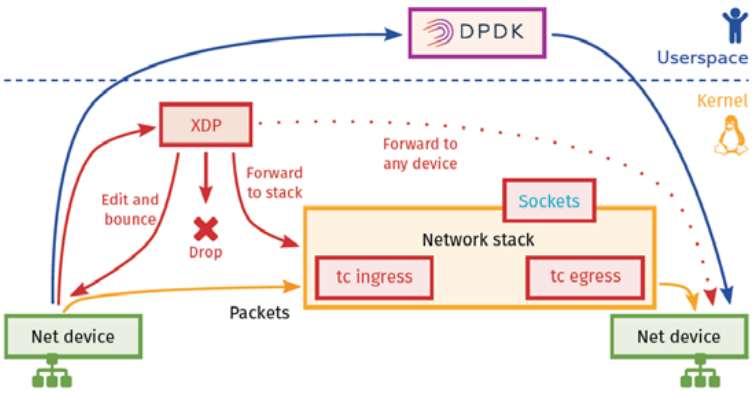


图8 BPF+XDP实现网络数据包过滤

5. BPF工具

当前BPF贡献者以及使用者，已经开发并且开源了许多实用的BPF工具。这将给我们进行BPF开发和使用带来极大的便利性。

5.1 BCC

前文的介绍中我们提到了，对于一个C语言实现的BPF程序，可以通过Clang、LLVM将其编译成BPF字节码，然后通过加载程序，将BPF字节码通过bpf()系统调用加载到内核中。这种用户动态的编译、加载比较麻烦，因此IO Visor开发实现了一个BPF程序工具包BCC[3]。

BCC（BPF Compiler Collection）是高效创建BPF程序的工具包，BCC把上述BPF程序的编译、加载等功能都集成了起来，提供友好的接口给用户，进而方便用户的使用。它使用了（Python + Lua + C++）的混合架构，底层操作封装到C++库中，Lua提供一些辅助功能，对用户的接口使用Python提供，Python和C++之间的调用使用ctypes连接。因为使用了Python，所有抓回来的数据分析和数据呈现都非常方便。

除此之外，BCC还提供了一套现成的工具和示例供开发者使用，下图展示了当前BCC提供的各种类型的工具，当我们安装完BCC之后，进入"/usr/share/bcc/tools" 和"/usr/share/bcc/examples/” 目录就可以使用这些工具。

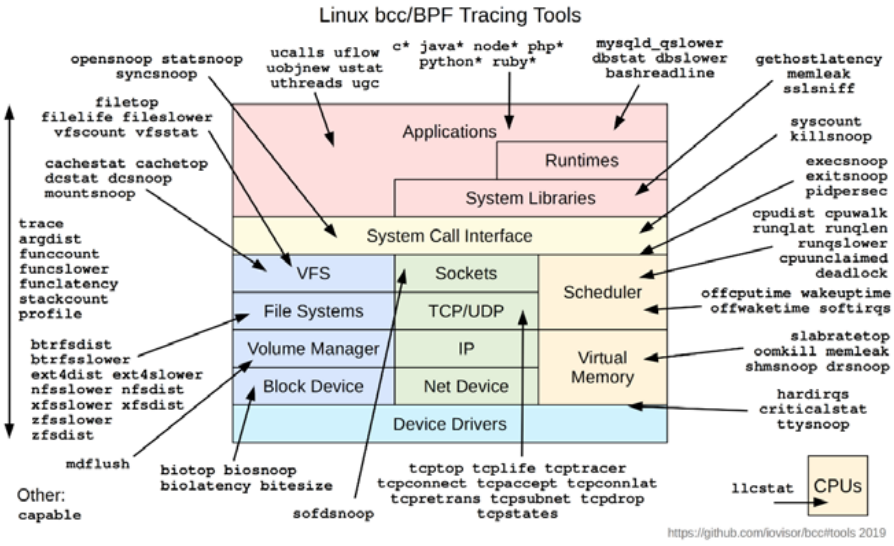


图9 BCC工具集

```
/usr/share/bcc/tools# ./syscount -L
Tracing syscalls, printing top 10... Ctrl+C to quit.
^C[21:22:45]
SYSCALL            COUNT      TIME (us)
futex               1122   1321885751.331
select               673    229961581.277
poll                 219    171994374.042
pselect6              48     21627700.875
epoll_wait            33     14026746.897
wait4                120     10169962.613
read                4177      1662075.764
fsync                  4       364937.128
nanosleep            337        48387.145
openat              2809        25358.704
```

5.2 其他工具

BPFTool是一个用于检查BPF程序和MAP存储的内核实用程序。这个工具在默认情况下不会安装在任何Linux发行版上，而且它还处于开发阶段，所以需要开发者编译最支持Linux内核的版本。将随Linux内核5.1版本一起发布BPFTool版本。BPFTool的一个重要功能就是可以扫描系统，进而了解系统支持了哪些BPF特性、系统中已经加载了何种BPF程序等。比如可以查看内核的哪个版本支持了哪种BPF程序，或者是否启用了BPF JIT编译器等。

BPFTrace[4]是BPF的高级跟踪语言。它允许开发者用简洁的DSL编写BPF程序，并将它们保存为脚本，开发者可以执行这些脚本，而不必在内核中手动编译和加载它们。它的灵感来自其他著名的Trace工具，比如awk和DTrace，BPFTrace将会是DTrace的一个很好的替代品。与直接使用BCC或其他BPF工具编写程序相比，使用BPFTrace的一个优点是，BPFTrace提供了许多不需要自己实现的内置功能，比如聚合信息和创建直方图等。

Kubectl-trace [5]是Kubernetes命令行kubectl的一个非常棒的插件。它可以帮助开发者在Kubernetes集群中调度BPFTrace程序，而不必安装任何附加的包或模块。它通过使用trace-runner容器镜像，通过Kubernetes作业调度来实现，

trace-runner镜像中已经安装了运行程序所需的所有东西，可以在DockerHub中下载使用。

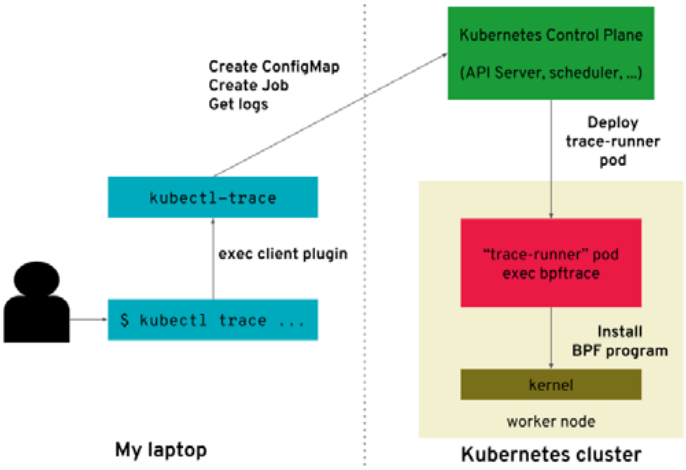


图10 Kubectl-trace架构

6. 总结

BPF机制通过在Linux内核事件的处理流程上，插入用户定义的BPF程序，实现对内核的软件定义，极大的提高了内核行为分析与操作的灵活性、安全性和效率，降低了内核操作的技术门槛。

Linux容器，作为云原生环境重要的支撑技术，是Linux内核上用于隔离和管理计算机进程的一组特性的抽象，高度依赖了Linux内核的底层功能。那么从内核的角度来看，（1）内核知道所有的进程/线程运行情况；（2）通过cgroups，内核可以知道Container Runtime配置的CPU/内存/网络等资源的配额以及使用情况；（3）从namespace的层面，内核可以知道Container Runtime配置的进程隔离情况、网络堆栈的情况、容器用户等众多的信息；（4）还可以知道容器环境内网络的连接以及网络流量的情况；（5）容器对系统调用、内核功能使用等信息。

因此，对于云原生环境来讲，如果能够拿到上述内核所拥有的种种信息，对于云原生应用的性能提升、可视化监控以及安全检测有着重要的意义。

参考文献

[1] The BSD Packet Filter: A New Architecture for User-level Packet Capture，http://www.tcpdump.org/papers/bpf-usenix93.pdf
[2] eBPF 简史，https://www.ibm.com/developerworks/cn/linux/l-lo-eBPF-history/index.html
[3] IO visor，https://iovisor.github.io/bcc/
[4] BPFTrace，https://github.com/iovisor/bpftrace
[5] Kubectl-trace，https://github.com/iovisor/kubectl-trace
[5] Linux Observability with BPF，https://www.oreilly.com/library/view/linux-observability-with/9781492050193/

个人社工防护二三事

金融事业部　张政祺

当前不管是别有用心的内部人员，亦或是目标明确的黑客攻击者，出于利益考量，在机构、企业全面信息化转型后，针对其信息化系统的攻击手段也越发多样。

就金融机构而言，通常网络安全防护能力较强，行业总体的安全水平处于一个相对高的位置，因此，不同的攻击者，从正面突破重重防护难度极大，直接获取有价值的数据、权限也绝非易事，在此前提下，利用社会工程学攻击便成为了最行之有效的攻击手段。

社工攻击指的是通过人与人之间的直接或间接接触，由攻击人员去影响或引导目标人员泄露其所需要的关键机密信息，从为进行下一步的技术突破做准备。

社工攻击通常有以下几种手段：

- 直接接触

  直接面对面接触　　电话

  ……

- 间接接触

  钓鱼邮件　　即时聊天工具

  ……

- 其他

  个人信息收集

  ……

1、面对面接触——此类型的社工攻击主要是为了博取攻击目标的信任，或者直接套取信息。

（1）攻击者可能伪装成客户，站在被服务方的立场，来与攻击目标建立信任关系，利用各种话术，套取关键敏感信息；或是建立完信任关系之后，通过长

时间的正常业务交往，麻痹攻击目标，逐步获取所需要的信息或是数据。

（2）在公众场合，例如行业会议、专业交流论坛时，伪装成同业人员，以交流行业信息为名，套取相关情报。

面对此类社工手段，主要依赖个人安全意识，不管是在任何场合下，都要注意个人信息和所涉及的业务信息保密，尽可能少的透露非必要的冗余信息，且要注意，透露的信息不应通过数据关联，能拼凑出敏感数据。

2、电话——此类型的攻击形式和面对面接触类似，区别在于攻击者在电话交流时，可以按照事先安排好的剧本进行话术推演，诱导性更强，且被攻击目标可能是攻击跳板。

此场景下，攻击者大概率通过前期的信息收集，得到相对明晰的被攻击者画像及当前工作情况，伪装成监管或上级领导，直接要求提供关键信息，如账户密码等；或者要求提供核心人员信息。遭遇这种状况，首先不要被攻击者牵着鼻子走，要懂得反问攻击者信息，判断其真实性；二是不要立即回复其所提的问题，或者给出其所需要的信息，待结束通话后，通过正常渠道去了解通话者身份是否属实，给出信息是否符合要求。

3、钓鱼邮件——此类型是目前最主流的社工攻击方式，占比最高。钓鱼邮件内容一般极具针对性，且能结合行业热点、时事新闻、内部事务等，迷惑性强；钓鱼邮件目标采用大面积撒网式，安全意识较差的人员容易上钩，由于目标基数很大，往往被钓鱼成功者也不在少数。

钓鱼邮件是通过迷惑性的发件人地址、标题、正文描述来迷惑被攻击者，在邮件正文中加入恶意链接，诱使点击，进而下载恶意程序，达到远控效果；或是添加恶意附件，打开后主机便会被植入木马病毒等恶意程序。首先面对不熟悉的发件者，不轻信任何内容，对于正文中的链接与附件，慎重点击打开，必要情况下联系IT管理人员进行处理；面对已知的发件者，与电话社工应对措施相似，采取身份核实与“延时处置”方针，来应对可能存在的钓鱼行为。

4、即时聊天工具——此类社工攻击手段目前逐步增多，其本质和电话社工类似，套取攻击者所需的关键信息。相比电话社工，其前期做的信息收集往往更多，以微信为例，首先需要收集到被攻击者的添加途径，再者是攻击者本身账号会进行账期的“维护”，长期的

在朋友圈发布各种为证明其身份也好、震慑被攻击者也好的各类“证据”，令被攻击者深信不疑。

应对措施与前文中钓鱼邮件与电话社工类似，不做累述，但基于即时聊天软件特性，存在一个时间差的概念，攻击者可以更加从容的应对突发情况，并且结合电话、朋友圈、邮件等社工方式组合出击，更难从整个交流过程中判别其身份，这时应该跳出思维定式，从其他渠道来进行身份验证，有能力可以进行身份识别后的攻击者画像以及溯源。

5、个人信息收集——这是一种非直接面对攻击者的状态，但是威胁程度丝毫不低。举一个简单的例子，攻击者盯上某企业内部运维人员A，其在社交网络上使用真名昵称，并且记录了很多日常信息，攻击者可以很轻易的编造一个虚假社交账号或即时聊天软件账号，冒充此人员，进行社工攻击。

因此，需要注意如下事项，避免过多的信息泄露造成的安全问题：

① 工作中使用的账号密码须与在其他社交网络、应用系统密码不同，保证唯一性、且密码强度高，误因各类被脱库的外部系统，形成攻击者的专项密码字典。

② 社交网络上发布的照片、信息，要格外注意信息的保护，例如照片中存储的地理经纬度信息，往往可能被攻击者利用，进行下一步物理攻击或面对面社工攻击。

③ 切勿贪图便利，将涉密信息上传公共网盘，对于非涉密信息，如果无其他途径传输，建议对文件本身进行加密，且设置传播范围及时间，最大限度降低风险。

④ 任何企业数据信息，不要上传网络上的私人空间或者公共社交平台。

以上只是简要列举了一些面临社工攻击时的对应措施，核心是要提升自我的安全意识，因为人本身才是网络安全防护上关键的一环。

随着每年国家级、行业级的攻防演练工作越来越多，各机构企业人员正在遭遇一次次的历练，相信经过这一系列的过程后，当真正的攻击来临时，定会从容应对，成为网络安全防护的重要基石。

大敌当前“邮件安全你意识到了吗?

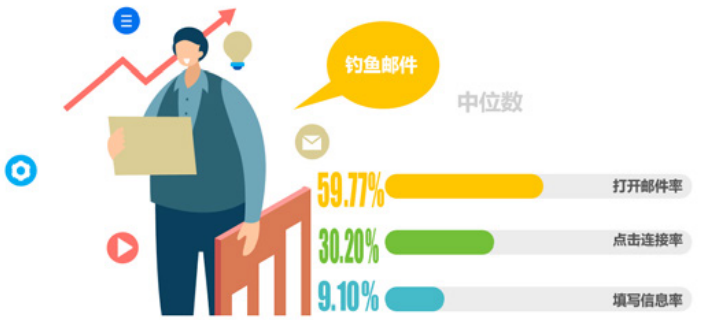
金融事业部　王宁

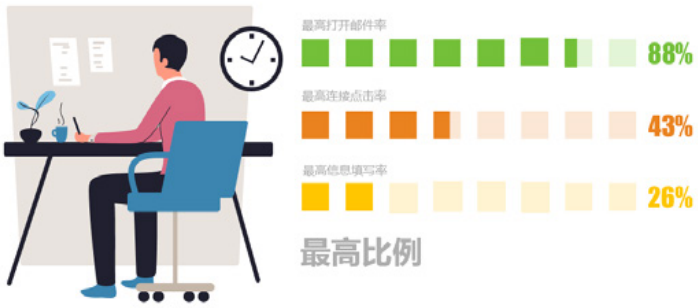
背景知识

公司网络安全建设越来越完善，不断的提高攻击防御，攻击检测等的水平，攻击者想要成功的突破会越来越难。但是俗话说得好，道高一尺魔高一丈。攻击者也从最初向冰冷的设备发起直接攻击的策略转变为向人的攻击，这类攻击我们称作社会工程学。在所有的社会工程学攻击方法中钓鱼邮件是利用率和成功率最高的攻击方式。

钓鱼邮件指利用伪装的电邮，欺骗收件人将账号、口令等信息回复给指定的接收者；或邮件带了某些附件（office文档、压缩包、可执行程序等），收件人只要打开附件就会将攻击者提前伪装好的病毒文件下载到本地；或引导收件人连接到特制的网页，这些网页通常会伪装成和真实网站一样，如银行或理财的网页，令登录者信以为真，输入信用卡或银行卡号码、账户名称及密码等而被盗取。

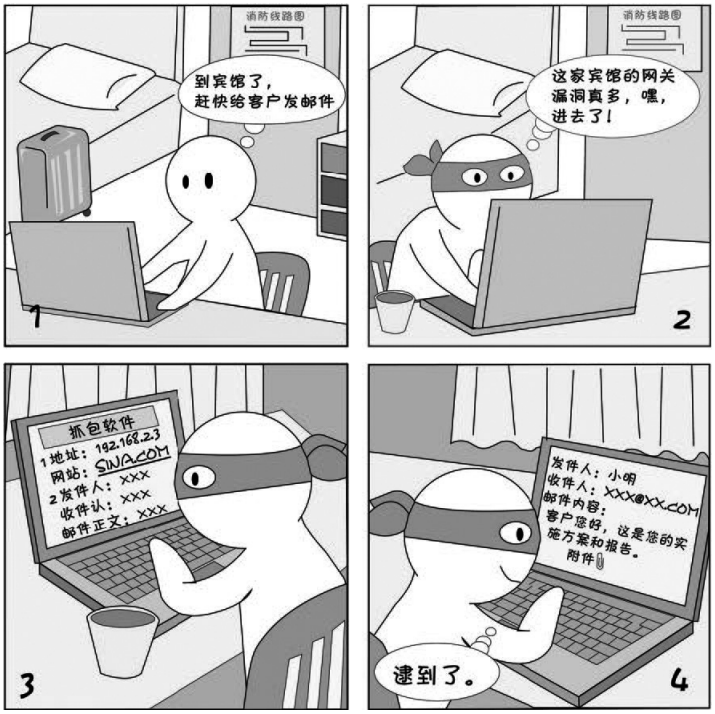
相信很多人都有一个疑问，“我能识别钓鱼邮件，不用担心，我不会中的”，实际情况真的是这样吗？在进行了大量钓鱼邮件安全意识评估之后我们得到如下数据：





统计发现，有大概60%的人员打开了钓鱼邮件，有30%人员点击了相关钓鱼邮件的反馈连接。最后会有10%的人反馈了相关信息。而在所有统计的数据中，最高的信息填写比例达到了惊人的26%。对于攻击者来说，他们想要的信息可能只需要从1个人哪里获取，就为他打开了一个新世界。

邮件安全需要注意哪些问题，如何准确识别钓鱼邮件，我们快来看一看吧：



传输安全

在一些外部的Wi-Fi 网络中，可能会有攻击者对流量进行监测。因此，在使用Outlook、Foxmail等邮件客户端，或者在外使用网页版邮箱时，应该选择加密的收件/ 发件端口或HTTPS 协议，从而防止攻击者截获邮件正文和附件。

安全建议：

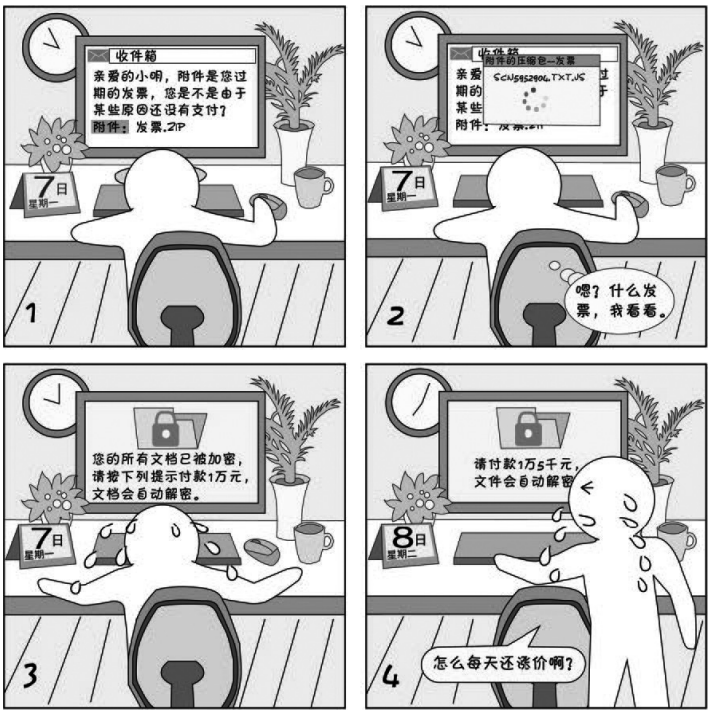
- 收发邮件过程中，应确保传输通道加密；
- 针对Web邮箱，应确认网页协议为HTTPS，否则存在风险；
- 针对邮箱客户端，应确认收件、发件均使用安全的SSL（TLS）端口，默认的SMTP和POP3端口可能存在风险。

社工邮件

所谓社会工程学，就是利用人的一些弱点发起攻击。而利用邮件骗取回复敏感信息，是最常见的一种社会工程学方式。特别是看到带有“尽快回复”、“请及时反馈”字样的邮件，更容易放松警惕，本能地按照要求给对方回复过去。

安全建议：

- 在收到各类邮件时，都要首先核对发件人是否正确，提高警惕；
- 如果发现邮件存在不合常理的地方，应该首先通过其他沟通方式向发件人本人进行确认。

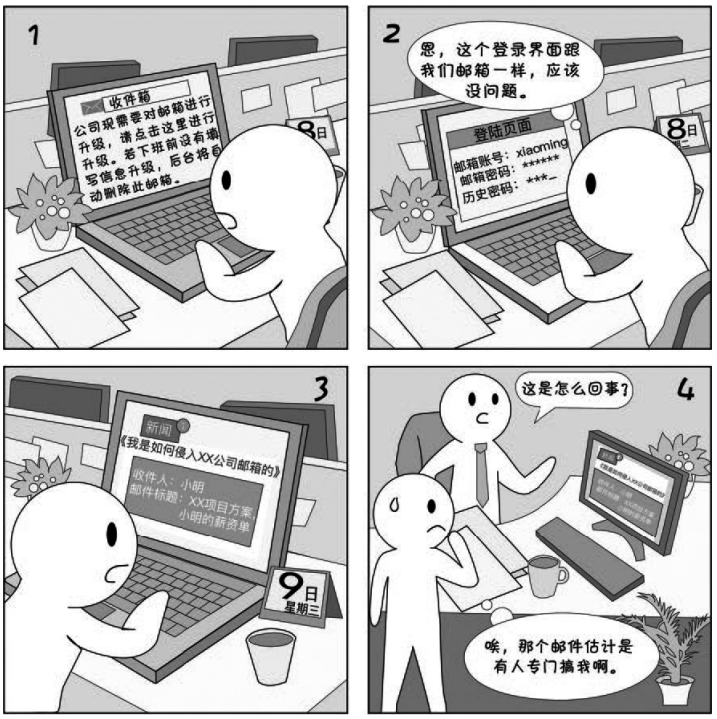


附件病毒

随着病毒的不断进化，目前病毒已经发展到针对特定国家、特定行业开展攻击。并且，为防止反病毒软件的查杀，一些病毒可能不再以exe 文件形式存在，而是隐藏在Office 文档中。针对收到的带office文件附件的邮件要仔细甄别真伪。

安全建议：

- 在收到可疑邮件后，应避免打开其附件文件；
- 在Office 中，应避免启用宏和ActiveX 功能，特别应该避免为外部文件启用上述功能；
- 在收到外部发来的邮件附件时，应首先使用反病毒软件查杀病毒。



恶意链接

随着攻击的不断升级，攻击者可能会制作专门针对某公司业务的钓鱼邮件，以此增强迷惑性。同时，为增强可信度，攻击者还可能会仿冒一个与公司高度相似的网站，诱导员工在上面输入用户名和密码，这些内容会实时提交给攻击者。

安全建议：

- 收到包含链接的邮件时，应确认链接是否与邮件正文所描述的系统一致；
- 在访问业务系统时，不推荐点击外部发来的链接；
- 特别是手机丢失时，谨防邮箱内收到的“查找手机位置”的邮件。

- 邮件传输要加密，黑客截获难破译；
- 默认浏览器非IE，陌生链接勿点击；
- 各种附件谨慎点，可执行文件风险高；
- 遇事冷静莫慌张，电话确认是法宝。

针对邮件安全，我们应该做到如下六方面：

- ☐ **看发件人地址：**如果是公务邮件，发件人多数会使用工作邮箱，如果发现对方使用的是个人邮箱帐号或者邮箱账号拼写很奇怪，那么就需要提高警惕。
- ☐ **看邮件标题：**“系统管理员”、“通知”、“订单”、“采购单”、“发票”、“会议日程”、“参会名单”、“历届会议回顾”
- ☐ **看正文措辞：**对使用“亲爱的用户”、“亲爱的同事”等一些泛化问候的邮件应保持警惕。
- ☐ **看正文目的：**当心对方索要登录密码，一般正规的发件人所发送的邮件是不会索要收件人的邮箱登录账号和密码的
- ☐ **看正文内容：**当心邮件内容中需要点击的链接地址，若包含“&redirect”字段，很可能就是钓鱼链接；当心垃圾邮件的“退订”功能
- ☐ **看邮件附件：**当收到非本公司或自己熟悉的发件人发来带附件的邮件时，要认真甄别，不要随意打开附件内容，如有必要应与发件人核实邮件真伪

刷单再现支付陷阱，“高倍镜”找出破绽！

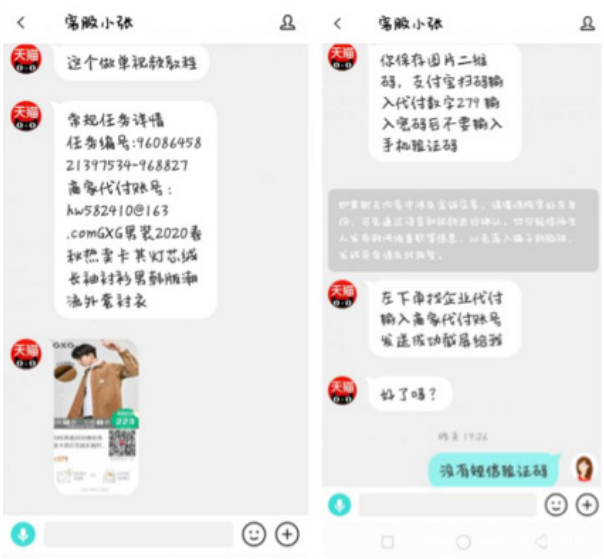
摘　要：兼职刷单已是常见骗局，诈骗手法也比较容易识破，然后近期手机先赔收到用户反馈，反映在网上兼职刷单的过程中受骗。通过对诈骗过程的还原，发现 今年的刷单骗局悄悄升了级，伪装度极高，可是段位再高，终究也只是以假乱真。

关键词：标签（兼职刷单、金融诈骗），技术问题（安全事件）。

内　容：兼职刷单已是常见骗局，诈骗手法也比较容易识破，然后近期手机先赔收 到用户反馈，反映在网上兼职刷单的过程中受骗。通过对诈骗过程的还原，卫士妹发 现，今年的刷单骗局悄悄升了级，伪装度极高，可是段位再高，终究也只是以假乱真。

案件经过

用户在 QQ 群看到刷单广告，使用易信软件沟通刷单事宜。对方发来商品链接，要求使用浏览器打开并加到购物车，随后发来付款二维码，并表示支付时会出现代付选项，用户选择代付后，不会产生费用。然而，支付成功后，用户发现支付过程使用了花呗便联系对方退款。

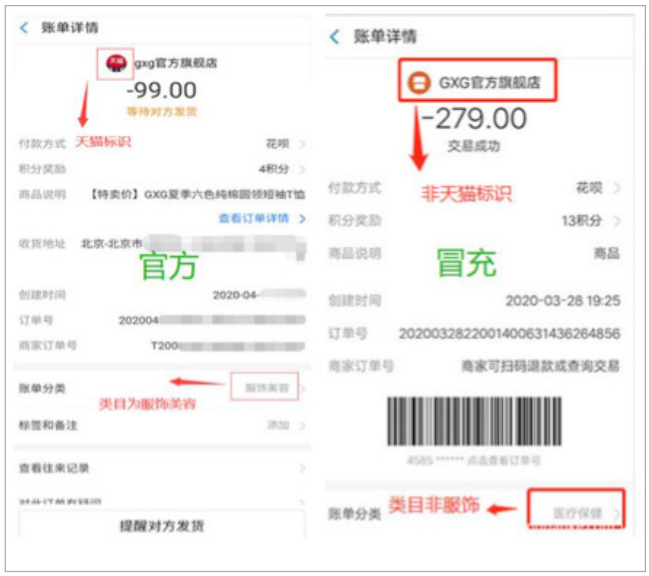


引导添加退款客服后，以用户网络状态(未关闭 wifi、开启蓝牙)等问题，引导用户再次扫码支付，事后发现受骗。

“小细节，大不同”

从诈骗手法上看，与以往发现的兼职刷单手法相同，均是通过冒充电商平台、引 导二维码支付，但在细节上却做的更加逼真。

订单支付的商品类目为服装，非医疗保健。



所谓的退款客服(支付宝账号)头像与官方不同。

通过以上分析并结合实际测试，推测不法分子是申请了支付宝的商家收款二维码，并将收款商家改成与官方一致的名称，同时申请了花呗收款服务。

刷单骗局千千万，总还是有人会相信骗子的鬼话，接连让你转账就真的要察觉了， 大多数被骗用户，就是这样一步步被套牢!

信息来源: https://www.anquanke.com/post/id/204236

中信银行泄露用户流水引“众怒” 隐私安全离我们还有多远？

摘　要：近日脱口秀艺人池子指控中信银行对员工的管理和相关客户隐私管理制度存在严重问题，银保监会对中信银行泄露客户账户信息启动立案调查程序

关键词：标签（中信银行、信息泄露、隐私安全），技术问题（安全事件）。

内　容：近日脱口秀艺人池子指控中信银行对员工的管理和相关客户隐私管理制度存在严重问题，随后，“池子起诉中信银行”和“中信银行支行行长被撤职”两个话题先后上了网络热搜。

事件概要

据悉，事件是由于中信银行向池子曾服务的上海笑果文化公司泄露了池子的个人银行账务信息，对此中信银行回应的是“配合大客户的要求”，显然该配合要求的做法明显惹怒了池子。池子在微博中表示，上述行为侵犯了公民个人信

息隐私安全，他已向警方报案同时通过律师发函要求中信银行、笑果文化赔偿损失并公开道歉。微博发出后，迅速引爆舆论，当日深夜，中信银行紧急发布致歉信，承认是“员工未严格按规定办理”，郑重道歉的同时表示会按照相关规定已对员工进行处分，并且撤职该支行行长。据该事件最新进展显示，上海银保监局已关注到脱口秀演员池子指责中信银行股份有限公司泄露其个人账户交易信息一事，并正式介入调查。

但是，事件发展到今天，显然中信银行的这些操作并没有平息大家的质疑，很多网友担忧，自己的账户会不会也遭遇同样的情况?银行的个人信息安全问题引发了大众的关注。毕竟如果上市大银行都不能维护用户的个人隐私安全，向大客户妥协提供违规操作，银行的信用度势必会下降，失去用户的信任。

泄密不止中信

此前有报告称，在 2019 年有 62%的泄露数据来自金融服务行业，这也进一步证明了金融行业数据泄露事件的高发性。

例如，美国第五三银行(American bank Fifth Third)也因向客户发送了一封神秘的违约披露信而受到批评，客户团体认为这封信“含糊且具有欺骗性”。 第五三银行在发现至少有两名员工窃取了客户信息并将其提供给第三方后给客户写了道歉信。信中表示，泄露的数据包括用户姓名、社会安全号码、地址、电话号码、出生日期、母亲的娘家姓、驾照信息和账号信息。但是，该银行尚未具体说明有多少客户受到该事件的影响，或有多少前雇员因泄露客户的个人数据而被解雇。

黑客攻击泛滥

其实，在世界范围内，类似的数据泄露案例层出不穷。与此同时，除了金融机构内部人为因素以外，更有趋势调查报告显示金融机构近年来已成为网络犯罪者的首要目标。

就在前几日，据外媒报道，迷宫勒索组织宣称窃取了 14 万个属于美国公民的信用卡数据。根据，迷宫勒索软件小组在其数据泄漏网站上透露，他们于 2019

年 8 月就已经首次入侵了 Banco BCR 的网络，并窃取了凭证和其他敏感数据。但是，他们没有对银行设备进行加密。由于银行在第一次攻击后没有保护其网络，因此该黑客组织

在 2020 年 2 月再次入侵该银行网络，他们表示至少已经窃取了该银行几年的重要数据。

与此同时，新型 Android 移动恶意软件 EventBot 也正在针对欧洲的银行和金融服务发起攻击，它结合了特洛伊木马和信息窃软件的能力，能够窃取用户的财务应用程序数据，并对受害者进行秘密监视。 而且，EventBot同时可以面向200多种移动金融和加密货币应用程序发起攻击，包括 PayPal、Barclays、CapitalOne UK、 Coinbase、TransferWise 和 Revolut 等应用程序。

数据安全的未来

由于现在大多数银行业务都是以数字方式进行的，因此黑客可以一次窃取成千上万，有时甚至数百万的记录，从而导致数据严重泄露。在面对数据泄露时，对于大多数用户而言，一旦发现自己已成为数据泄露的一部分，则应立刻确保执行三件事:找出被盗取信息的帐号，重置密码，联系征信机构进行反馈。

虽然，我们并不确定实现用户数据隐私安全还需要多久，但是银行和其他金融机构也正在不断努力，以确保其在银行业拥有最先进的网络安全性，以及生物识别技术和双重身份验证流程等新技术都在帮助进一步提高用户账户的安全性。

信息来源：

https://www.easyaq.com/news/2147307807.shtml

世界最大主权财富基金遭遇网络攻击：被骗走 1000 万美元

摘　要：作为全球最大的主权财富基金 Norfund 基金因网络诈骗，被骗子轻而易举的骗走 1000 万美元，而骗子是利用了所谓“泄露的付款数据”这一缺陷来作案的。

关键词：标签（财富基金、网络攻击），技术问题（安全事件）。

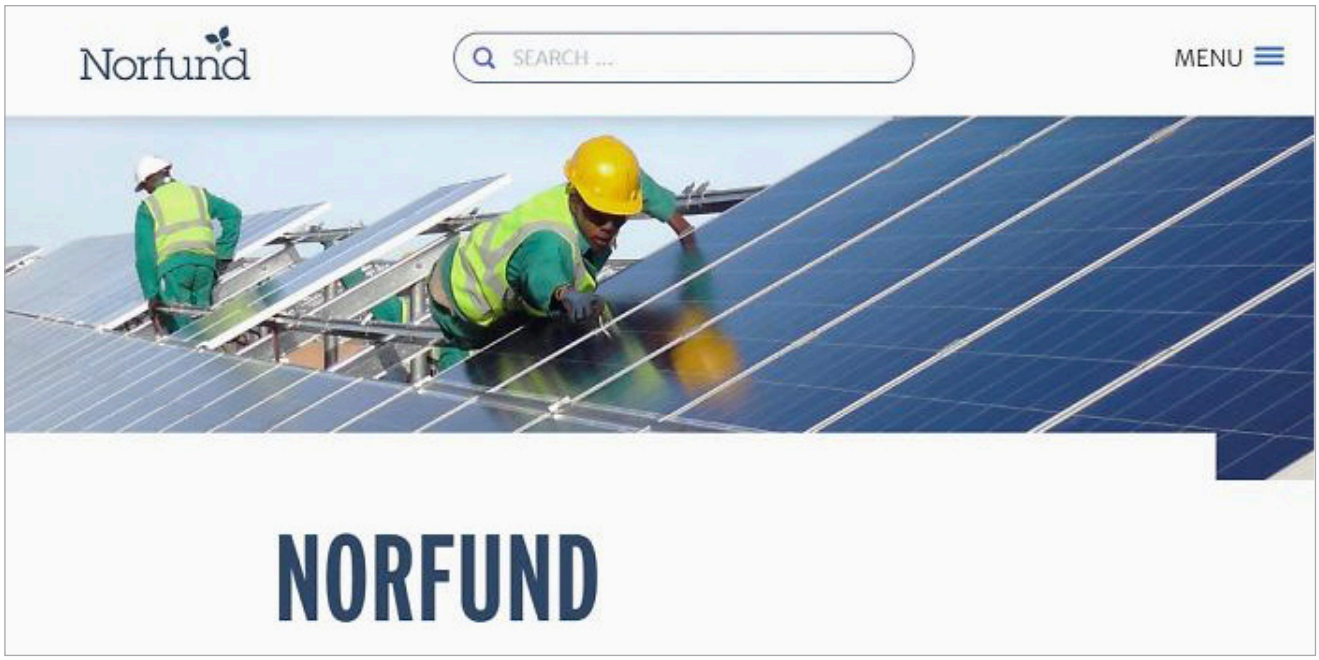
内　容：北京时间 4 月 29 日消息，作为全球最大的主权财富基金 Norfund 基金因网络诈骗，被骗子轻而易举的骗走 1000 万美元，而骗子是利用了所谓“泄露的付款数据”这一缺陷来作案的。

据报道，挪威主权基金 Norfund(也被称为挪威国家基金)的资金来源于著名的北海油田收益，目前市值超过 1 万亿美元。该基金表示，有黑客操纵了该组织的一笔交易，将一笔原本打算借给柬埔寨一家小额信贷机构的贷款转入受骗子控制的一个账户，结果导致该基金在 3 月份被骗 1 亿克朗(约为 1000 万美元)。该基金表示，这笔钱似乎已经从柬埔寨转移到了墨西哥，由于损失巨大，国际警方已经介入调查此事。

Norfund 周三在谈到这起网络攻击诈骗案时表示:“在这段时间里，诈骗者以一种在结构、内容和语言使用上都非常巧妙的方式，操纵和伪造了 Norfund 与借款机构之间的信息交换。文件和付款明细都是伪造的。”骗子用一些伪造的发票或伪造的电子邮件把钱转移到了其他的账户，说明整个交易过程对票据的把关不过关。

其实这个骗局很简单，但却非常有效。骗子会先欺骗公司里的某个关键人物，然后欺骗公司里的其他人把钱转到一个新账户里，因为这些付款在计划中是合法和得到授权的，所以受害者通常要到最后才反应过来。

首席执行官 Tellef Thorleifsson 承诺，将迅速与国际警方采取行动，将骗子绳之以法，并防止该组织再次被骗。他表示:“这是一起严重的事件。这一网络诈



骗行为清楚地表明，我们作为一个国际投资者和发展组织， 在利用数字渠道时很容易受到攻击。发生这种情况的事实表明，我们的系统和管理还不够好。我们必须立即采取严肃的行动来纠正这种情况。”

据悉，除警方介入外，挪威主权基金还表示，它正与挪威外交部及旗下的银行 DNB 合作，追踪这个骗子并取回赃款。普华永道也被要求对该基金的 IT 安全设置进行评估。虽然成为此类网络攻击的受害者令人尴尬，但 Norfund 并不是唯一一家。如果这件事的核心在于互联网交易中的商务邮件欺诈，那么说明这种网络欺诈已形成一个数十亿美元的产业，情况只会变得更糟。

信息来源：

https://tech.ifeng.com/c/7wTAer4u4P2

福建警方打掉 17 个第四方支付平台：为网络犯罪提供帮助

摘 要：本次行动共抓获犯罪嫌疑人 56 名，现场扣押电脑设备 50 台、手机 160 余部、银行卡百余张，冻结银行卡 1800 余张，涉案资金流水达十亿余元。

关键词：标签（第四方支付平台、网络犯罪），技术问题（安全事件）。

内 容：所谓“第四方支付”平台是指聚合第三方支付平台、合作银行及其他服务商等接 口，非法对外提供综合支付结算业务的平台，系当前电信网络诈骗、网络赌博等犯罪 团伙套取、漂白非法资金的所谓“绿色通道”。

5 月 11 日，福建省泉州市公安局网安支队在泉州、漳州等地同步开展收 网行动，捣毁 13 个犯罪窝点，成功打掉 17 个第四方支付平台，共抓获犯罪嫌疑人 56 名，现场扣押电脑设备 50 台、手机 160 余部、银行卡百余张，冻结银行卡 1800 余张，涉案资金流水达十亿余元。

你知道什么是“第四方支付”吗?

案件经过

为深入开展“净网 2020”专项行动，福建省泉州市网安部门按照公安部和省厅 部署，发起集群战役，找准网络犯罪生态“七寸”，深入研究网络犯罪生态中的技术、支付等环节，打深打透网络犯罪生态。

2020 年 1 月，泉州网安民警在工作中发现，有网民开发、架设、运维多个非法 第四方支付平台，大量收购银行账户和第三方支付账号，层层转接支付通道和资金链 路，为境外网络赌博团伙提供非法资金结算业务。经过近三个月的缜密侦查研判，网 安民警逐步摸清该犯罪团伙的组织架构和窝点分布。

嫌疑人陈某枝（男，39 岁，泉州市安溪县人）为一家网络技术公司老板，其雇 佣技术员陈某平（男，31 岁，泉州市永春县人）先后搭建 17 个第四方支付平台，并分发给多个团伙管理运营，作案窝点遍布泉州的丰泽、晋江、南安、德化以及漳州等地。

该犯罪团伙使用多种掩护手段躲避侦查打击，极大增加了破案难度。网安民警经过近三个月的缜密侦查，逐渐摸清掌握嫌疑人的违法犯罪事实、作案窝点。抓捕时机成熟，泉州网安支队决定开展统一收网行动。

统一收网

2020 年 5 月 11 日下午，在福建省公安厅网安总队的统一部署下，泉州市公安局网安支队组织辖下丰泽、南安、安溪三地公安机关 200 名警力兵分三路，在泉州市丰 泽、晋江、南安、德化以及漳州等地同步开展收网行动，捣毁 13 个犯罪窝点，成功 打掉 17 个第四方支付平台，共抓获犯罪嫌疑人 56 名，现场扣押电脑设备 50 台、手 机 160 余部、银行卡百余张，冻结银行卡 1800 余张，涉案资金流水达十亿余元。

三路大军战果:

(安溪收网)

泉州网安支队会同安溪县公安局捣毁 5 个犯罪窝点，抓获犯罪嫌疑人 31

名，打 掉第四方支付平台 14 个，扣押电脑 31 台，手机 70 余部，网银 U 盾 50 余个。

(丰泽收网)

泉州网安支队会同丰泽分局捣毁 5 个犯罪窝点，抓获违法嫌疑人 11 名，打掉第 四方支付平台 1 个，现场缴获银行卡 60 余张，扣押电脑 9 台、手机 26 部，冻结银行 卡账户 1800 个。

(南安收网)

泉州网安支队会同南安市局在晋江、南安、德化三地捣毁 3 个犯罪窝点，抓获违 法犯罪嫌疑人 14 名，打掉第四方支付平台 2 个，扣押电脑 10 台、手机 34 部、银行 卡 30 余张和一系列作案工具。

目前案件正在进一步深挖审讯中。

网警课堂——关于“黑灰产”

所谓网络黑灰产，指的是电信诈骗、钓鱼网站、木马病毒、黑客勒索等利用网络 开展违法犯罪活动的行为。稍有不同的是，“黑产”指的是直接触犯国家法律的网络 犯罪，“灰产”则是游走在法律边缘，为“黑产”提供辅助的行为。

近年来，由于移动支付行业的快速发展，许多黑灰产犯罪分子将资金转移结算渗 透到了移动支付上，为洗钱、诈骗、盗窃、赌博等犯罪行为提供帮助。

因犯罪分子较难利用有严格风控的正规企业，便转向通过技术搭建非法第四方支 付平台以及利用赌博人员个人收款码、虚假电商店铺等较为隐蔽的方式，特别是通过 技术搭建非法第四方支付平台，由于其搭建技术简单，适用性强，利润获取快速，成 为当下网络犯罪分子最热衷的手段。

相关法律

《刑法》第二百二十五条 非法经营罪:违反国家规定，有下列非法经营行为之一，扰乱市场秩序，情节严

重的，处五年以下有期徒刑或者拘役，并处或者单处违法所得一倍以上五倍以下罚金; 情节特别严重的，处五年以上有期徒刑，并处违法所得一倍以上五倍以下罚金或者没 收财产:(一)未经许可经营法律、行政法规规定的专营、专卖物品或者其他限制买 卖的物品的;(二)买卖进出口许可证、进出口原产地证明以及其他法律、行政法规 规定的经营许可证或者批准文件的;(三)未经国家有关主管部门批准非法经营证券、 期货、保险业务的，或者非法从事资金支付结算业务的;(四)其他严重扰乱市场秩 序的非法经营行为。

《刑法》第二百八十七条之二 帮助信息网络犯罪活动罪:明知他人利用信息网络实施犯罪，为其犯罪提供互联

网接入、服务器托管、网络存储、通讯传输等技术支持，或者提供广告推广、支付结 算等帮助，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金。单位犯 前款罪的，对单位判处罚金，并对其直接负责的主管人员和其他直接责任人员，依照 第一款的规定处罚。有前两款行为，同时构成其他犯罪的，依照处罚较重的规定定罪 处罚。

《刑法》第三百零三条 开设赌场罪:开设赌场的，处三年以下有期徒刑、拘役或者管制，并处罚金;情

节严重的，处三年以上十年以下有期徒刑，并处罚金。

网警提醒

建议广大人民群众在从事互联网金融活动时，要认准合规合法的网络支付平台， 不要轻信平台虚假宣传，不要随意扫来源不明的支付二维码，避免将个人资金转入此 类非法支付平台，谨防上当受骗或个人财产损失

信息来源:

http://www.youxia.org/2020/05/51555.html

多家银行被约谈，暂停对公账户开户

摘　要：杭州中心支行通报了电信网络新型违法犯罪涉案企业银行账户倒查及问责情况，明确下一步工作要求。对涉案银行采取强化监管及严格问责措施。

关键词：标签（网络犯罪、电信诈骗、涉案银行），技术问题（安全事件）。

会议指出，电信网络新型违法犯罪和跨境赌博严重侵害人民群众利益，危害经济金融安全、影响社会稳定，损害国家形象。人民银行各级分支行、各银行机构、支付机构要充分认识打击治理电信网络新型违法犯罪和跨境赌博的重要性和紧迫性，提高政治站位，切实增强打击治理工作的紧迫感和责任感。

会议要求，要突出问题导向，全面压实业务合法合规主体责任，坚决斩断电信网络新型违法犯罪和跨境赌博资金链。加强支付业务合规管理，建立健全覆盖事前、事中、事后的支付风险防控体系。加强风险内控管理，建立业务质量和风险防控为核心的考核评价机制。严格违法违规责任追究，对涉案银行、支付机构一律倒查问责，相关机构一律追究内部相关机构和人员的责任。

会议强调，要加强协调联动，持续构建齐抓共管的工作局面。加强内部联合，完善内部不同部门的管理职责，建立职责清晰、责任到岗、落实到人的协同管理体系; 加强行业联防，推进风险信息共享;加强部门联治，强化与市场监管、电信、公安、 司法等相关部门沟通协调，建立健全行业联合治理工作机制;加强社会联动，持续开展防诈禁赌宣传教育，提升公众防范意识。

另外，杭州中心支行通报了电信网络新型违法犯罪涉案企业银行账户倒查及问责情况，明确下一步工作要求。

内　容：5 月 13 日下午，人民银行杭州中心支行召开全省金融机构打击治理电信网络新型违法犯罪暨跨境赌博工作推进会。杭州中心支行党委委员、副行长杨长岩出席会议并讲话。浙江省公安厅刑侦总队、治安总队负责人应邀参加会议并通报有关情况。

对涉案银行采取强化监管及严格问责措施。

一是对管理不善，存在重大违规行为的 4 家银行予以通报批评，并约见其行领导进行监管谈话。

二是根据《中国人民银行关于加强支付结算管理防范电信网络新型违法犯罪有关事项的通知》（银发〔2016〕261 号）规定，暂停 4 家银行网点 3 个月的新开立单位银行账户业务，暂停 18 家银行网点 1 个月的新开立单位银行账户业务。

三是责令各涉案银行省内最高管辖行内部严肃追究相关机构和人员责任。责令严肃追究开户网点主要负责人、分管负责人、客户经理以及负责开户审核、非柜面业务管理、交易监测、对账管理、实名制动态复核等的相关机构和人员责任。责令四家银行机构严肃追究管辖行相关管理部门和人员责任。

四是将涉案企业银行账户情况纳入对银行机构“两管理、两综合”评价内容，降低涉案银行评价等级。

对下一步工作作了部署。

一是落实企业银行账户合法合规主体责任，加强企业银行账户全生命周期管理。二是加强收单业务管理，落实特约商户准入、交易监测、终端管理等要求。三是大力推进先进技术在账户、商户管理环节的应用。四是组织开展存量企业银行账户、商户风险排查。五是加大监管力度，从严问责。

根据深圳市反电信网络诈骗中心整理的建议，存在以下情况的企业被重点关注:

1、一人多企、一人多户、一址多照 2、经营地址为“自主申报、住所申报”3、无深户、无居住证、无社保的三无人员 4、首次开户的企业法人代表年纪偏大或偏小（小于 25 或大于 65 岁） 5、身份证地址为异地的偏远农村、手机号为异地、企业名称用字怪癖等。

企业法人需注意接听银行电话银行一般会通过电话联系法人或者实地上门方式进行排查!主要会核实公司名称、税号、注册地址、主营业务、法人、主营业务等，因此建议企业老板熟悉下公司登记信息，注意及时接听电话，避免因回复不及时，被认定为联系不上，从而导致账户冻结!

对公账户被冻结如何解决如果因为没有及时接听银行电话，导致自己公司对公户被冻结了，账户无法收款 和转账，遇到这种情况，企业应该如何解决呢?

1、首先，公司一定保证要合法正规真实经营

2、其次，及时和所属银行网点进行沟通、按要求提供相关真实经营的证明材料申请解冻(比如:房租水电发票、场地租赁合同、公司社保、交易往来合同等等)

3、可把原来开的对公户销户后，再重新选择其他银行开户。

对于企业新申请对公账户从严审查针对企业新申请的对公账户，各商业银行按要求落实开户审核责任，做好开户尽职调查工作，企业需按要求提供以下申请材料:

1、提供以公司、法人、股东名义承租的租赁合同或场地证明(包括自有房产证)

2、近 1 个月水电费发票或租金转账凭证（转账凭证的金额、时间、付款方收款方，需与租赁合同内容以及公司注册成立时间逻辑关系对应）

3、公司营业执照原件、公章、财务章、法人私章 4、法人本人携带身份证原件及公司相关资料到场开户

银行网点在受理申请资料后，需安排工作人员上门核查注册地址，确保“真人、真事、真资料“方能审核通过!

信息来源：

https://mp.weixin.qq.com/s/nWL5u70fnEcTLGw7nuJ5Mg

NSFOCUS

漏洞聚焦

Apache Tomcat Session 反序列化代码执行漏洞（CVE-2020-9484）安全通告

发布时间：2020 年 5 月 21 日

综述

近日，Apache Tomcat发布通告称修复了一个源于持久化Session的远程代码执行漏洞（CVE-2020-9484）。要利用该漏洞，攻击者需要同时满足以下4个条件：

1. 攻击者可以控制服务器上的文件名/文件内容；
2. 服务器上配置使用了PersistenceManager的FileStore；
3. PersistenceManager配置了sessionAttributeValueClassNameFilter值为“NULL”或者其他宽松的过滤器，使得攻击者可以提供反序列化对象；
4. 攻击者知道FileStore使用的存储位置到可控文件的相对路径。

攻击者在同时满足以上4个条件时，可以发送一个恶意构造的请求，来造成反序列化代码执行漏洞。

受影响产品版本

- ☐ Apache Tomcat 10.x < 10.0.0-M5
- ☐ Apache Tomcat 9.x < 9.0.35
- ☐ Apache Tomcat 8.x < 8.5.55
- ☐ Apache Tomcat 7.x < 7.0.104

不受影响产品版本

- ☐ Apache Tomcat 10.x >= 10.0.0-M5
- ☐ Apache Tomcat 9.x >= 9.0.35
- ☐ Apache Tomcat 8.x >= 8.5.55
- ☐ Apache Tomcat 7.x >= 7.0.104

解决方案

Apache Tomcat官方已经发布新版本修复上述漏洞，建议受影响用户尽快升级进行防护。不方便升级的用户，还可以暂时禁用FileStore功能，或者单独配置sessionAttributeValueClassNameFilte的值来确保只有特定属性的对象可以被序列化/反序列化。

参考链接：

https://tomcat.apache.org/security.html

SaltStack 多个漏洞 (CVE-2020-11651、CVE-2020-11652) 安全通告

发布时间：2020 年 5 月 4 日

综述

近日，服务器基础架构集中化管理平台SaltStack Salt 被披露存在两个安全漏洞（CVE-2020-11651、CVE-2020-11652）。

开源项目Salt 是SaltStack公司产品的核心，作为管理数据中心和云环境中服务器的配置工具，广受欢迎。

存在的两个漏洞分别是身份验证绕过漏洞（CVE-2020-11651）和目录遍历漏洞（ CVE-2020-11652）。

CVE-2020-11651

漏洞由ClearFuncs类引起，该类无意中暴露了_send_pub（）和_prep_auth_info（）方法。未经身份验证的远程攻击者通过发送特制的请求可在minion端服务器上执行任意命令，还能够提取根密钥来调用master端服务器上的管理命令。

CVE-2020-11652

漏洞由Salt Master进程的ClearFuncs类未对访问路径进行正确过滤导致，经过身份验证的攻击者利用此漏洞可以访问任意目录。

据了解，目前已有多家组织未打补丁的服务器遭到针对 CVE-2020-11651 的攻击。

参考链接：

https://labs.f-secure.com/advisories/saltstack-authorization-bypass

受影响产品版本

- ☐ SaltStack Version < 2019.2.4
- ☐ SaltStack Version < 3000.2

不受影响产品版本

- ☐ SaltStack Version = 2019.2.4
- ☐ SaltStack Version = 3000.2

解决方案

SaltStack官方已发布最新版本修复了上述漏洞，建议相关用户及时更新规避风险。

https://github.com/saltstack/salt/releases

禁止将Salt Master默认监听端口（4505、4506）向公网开放，并设置为仅对可信对象开放。

SecureCRT 内存损坏漏洞 (CVE-2020-12651) 安全通告

发布时间：2020 年 5 月 15 日

综述

SecureCRT 最新版本 8.7.2 中修复了一个内存损坏漏洞（CVE-2020-12651），当CSI 函数接收到一个大负数作为参数时，可能允许远程系统破坏终端进程中的内存，最终导致任意代码的执行或程序崩溃。

攻击者可能通过类似 SSH banner 的方式利用该漏洞。

参考链接：

https://bugs.chromium.org/p/project-zero/issues/detail?id=2033

受影响产品版本

☐ SecureCRT Version < 8.7.2

不受影响产品版本

☐ SecureCRT Version >= 8.7.2

解决方案

官方已在新版本中修复了该漏洞，建议用户更新软件防范风险。

另，对于不能完全信任的主机，避免使用终端模拟软件进行连接，谨防恶意主机利用终端模拟软件中的漏洞危害主机。

Weblogic 远程代码执行漏洞（CVE-2020-2883、CVE-2020-2884）防护方案

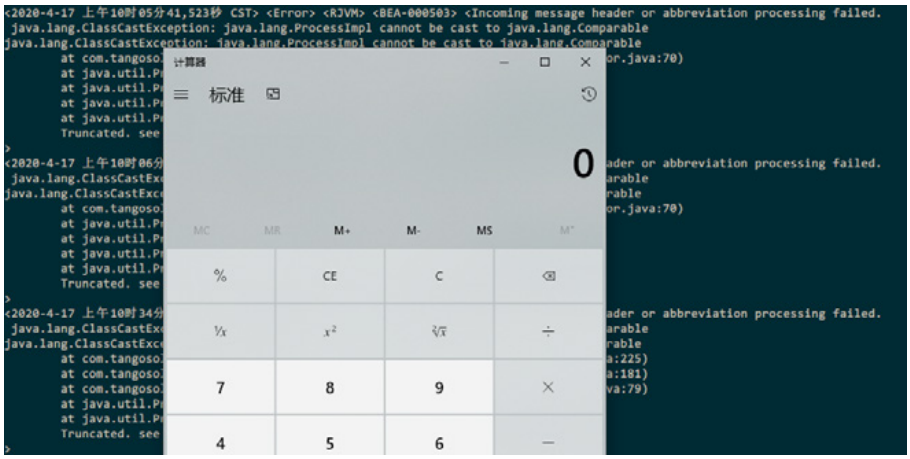
发布时间：2020 年 5 月 8 日

一、综述

在Oracle官方发布的2020年4月关键补丁更新公告CPU（Critical Patch Update）中，两个针对 WebLogic Server，CVSS 3.0评分为 9.8的严重漏洞（CVE-2020-2883、CVE-2020-2884），允许未经身份验证的攻击者通过T3协议网络访问并破坏易受攻击的WebLogic Server，成功的漏洞利用可导致WebLogic Server被攻击者接管，从而造成远程代码执行。

漏洞存在于WebLogic Server核心组件中，利用时无需身份认证及额外交互，并且在Weblogic控制台开启的情况下默认开启 T3 协议，故影响面较大，强烈建议用户尽快采取措施规避风险。

绿盟科技研究员已在第一时间复现了上述漏洞：



Oracle官方CPU链接：

https://www.oracle.com/security-alerts/cpuapr2020.html

二、漏洞影响范围

- ☐ Oracle WebLogic Server 10.3.6.0.0
- ☐ Oracle WebLogic Server 12.1.3.0.0
- ☐ Oracle WebLogic Server 12.2.1.3.0
- ☐ Oracle WebLogic Server 12.2.1.4.0

三、影响排查

3.1 本地检测

使用如下命令对Weblogic版本和补丁安装的情况进行排查。

```
$ cd /Oracle/Middleware/wlserver_10.3/server/lib
$ java -cp weblogic.jar weblogic.version
```

在显示结果中，如果没有补丁安装的信息，则说明存在风险，如下图所示：

```
[root007@localhost lib]$ java -cp weblogic.jar weblogic.version

WebLogic Server 10.3.6.0  Tue Nov 15 08:52:36 PST 2011 1441050

Use 'weblogic.version -verbose' to get subsystem information

Use 'weblogic.utils.Versions' to get version information for all modules
[root007@localhost lib]$
```

四、技术防护方案

4.1 官方修复方案

Oracle已经发布补丁修复了上述漏洞，请用户参考官方通告及时下载受影响产品更新补丁，并参照补丁安装包中的readme文件进行安装更新，以保证长期有效的防护。

注：Oracle官方补丁需要用户持有正版软件的许可账号，使用该账号登陆https://support.oracle.com后，可以下载最新补丁。

4.2 临时解决方案

用户可通过控制T3协议的访问来临时阻断针对这些漏洞的攻击。操作方法如下：

1、进入WebLogic控制台，在base_domain的配置页面中，进入“安全”选项卡页面，点击“筛选器”，进入连接筛选器配置。

2、在连接筛选器中输入：weblogic.security.net.ConnectionFilterImpl，参考以下写法，在连接筛选器规则中配置符合企业实际情况的规则：

```
127.0.0.1 * * allow t3 t3s
本机IP * * allow t3 t3s
允许访问的IP  * * allow t3 t3s
* * * deny t3 t3s
```

3、保存后若规则未生效，建议重新启动WebLogic服务（重启WebLogic服务会导致业务中断，建议相关人员评估风险后，再进行操作）。

4.3 绿盟科技检测防护建议

4.3.1 绿盟科技检测类产品与服务

内网资产可以使用绿盟科技的远程安全评估系统（RSAS V6）、Web应用漏洞扫描系统（WVSS）、入侵检测系统(IDS)、统一威胁探针（UTS）进行检测。

- 远程安全评估系统（RSAS V6）

  http://update.nsfocus.com/update/listRsas
- Web应用漏洞扫描系统（WVSS）

  http://update.nsfocus.com/update/listWvss
- 入侵检测系统（IDS）

  http://update.nsfocus.com/update/listIds
- 统一威胁探针（UTS）

  http://update.nsfocus.com/update/bsaUtsIndex

4.3.1.1 检测产品升级包/规则版本号

检测产品	升级包 / 规则版本号
RSAS V6 系统插件	6.0R02F01.1804
RSAS V6 Web 插件	6.0R02F00.1702
WVSS V6 插件	6.0R03F00.159
IDS	5.6.10.22420、5.6.9.22420
UTS	5.6.10.22154

- RSAS V6 系统插件包下载链接：

  http://update.nsfocus.com/update/downloads/id/104435
- RSAS V6 Web插件包下载链接：

  http://update.nsfocus.com/update/downloads/id/104252
- WVSS V6插件包下载链接：

  http://update.nsfocus.com/update/downloads/id/104262
- IDS 升级包下载链接：

5.6.10.22420

http://update.nsfocus.com/update/downloads/id/104039

5.6.9.22420

http://update.nsfocus.com/update/downloads/id/104038

◆ UTS升级包下载链接：

http://update.nsfocus.com/update/downloads/id/103172

4.3.2 绿盟科技防护类产品

使用绿盟科技防护类产品，入侵防护系统（IPS）来进行防护。

◆ 入侵防护系统（IPS）

http://update.nsfocus.com/update/listIps

4.3.2.1 防护产品升级包/规则版本号

防护产品	升级包 / 规则版本号	规则编号
IPS	5.6.10.22420 5.6.9.22420	23614

◆ IPS 升级包下载链接：

5.6.10.22420

http://update.nsfocus.com/update/downloads/id/104039

5.6.9.22420

http://update.nsfocus.com/update/downloads/id/104038

4.3.3 安全平台

平台	升级包 / 规则版本号
ESP（绿盟企业安全平台解决方案） ESP-H F06（绿盟企业安全平台）	ESP-EVENTRULE-004-20200221
ESP-H F07（绿盟企业安全平台）	ESP-EVENTRULE-003-20200221
ISOP（绿盟智能安全运营平台）	1.0.0.0.210052

◆ ESP、ESP-H F06升级包下载链接：

http://update.nsfocus.com/update/downloads/id/102586

◆ ESP-H F07升级包下载链接：

http://update.nsfocus.com/update/downloads/id/102585

◆ ISOP升级包下载链接：

http://update.nsfocus.com/update/downloads/id/103918

五、附录A 产品使用指南

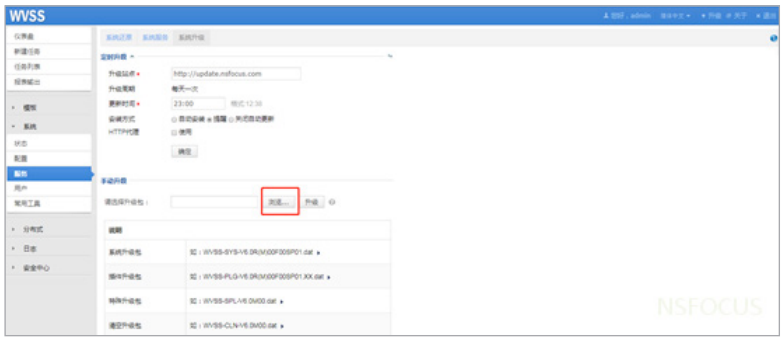
5.1 RSAS扫描配置

在系统升级中，点击下图红框位置选择文件。

选择下载好的相应升级包，点击升级按钮进行手动升级。等待升级完成后，可通过定制扫描模板，针对此次漏洞进行扫描。

5.2 WVSS扫描配置

在WVSS的系统升级界面，点击下图红框位置选择文件，进行升级：



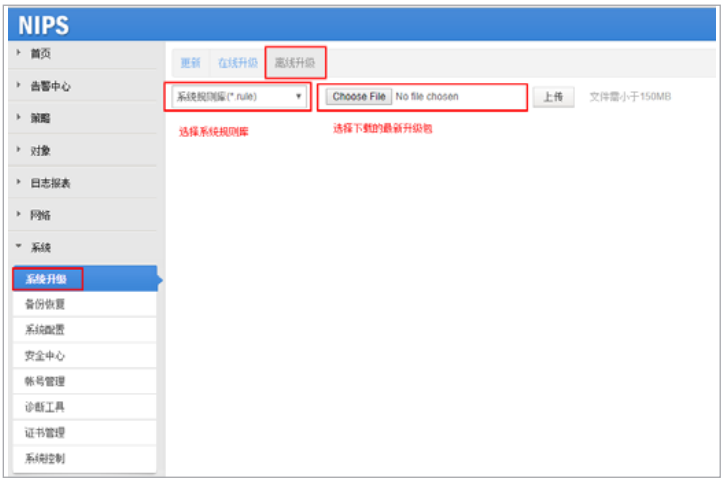
选择下载好的相应升级包，点击升级按钮进行手动升级。等待升级完成后，可通过定制扫描模板，针对此次漏洞进行扫描。

5.3 UTS检测配置

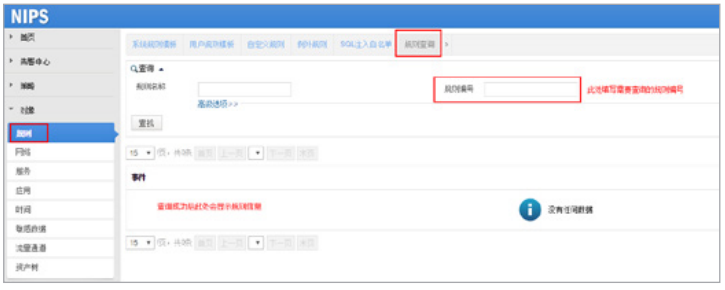
在系统升级中点击离线升级，选择规则升级文件，选择对应的升级包文件，点击上传，等待升级成功即可。

5.4 IPS防护配置

在系统升级中点击离线升级，选择系统规则库，选择对应的文件，点击上传。



更新成功后，在系统默认规则库中查找规则编号，即可查询到对应的规则详情。



注意：该升级包升级后引擎自动重启生效，不会造成会话中断，但ping包会丢3~5个，请选择合适的时间升级。

5.5 ISOP 绿盟智能安全运营平台

第一步：登录ISOP平台，点击系统升级，如下图所示：

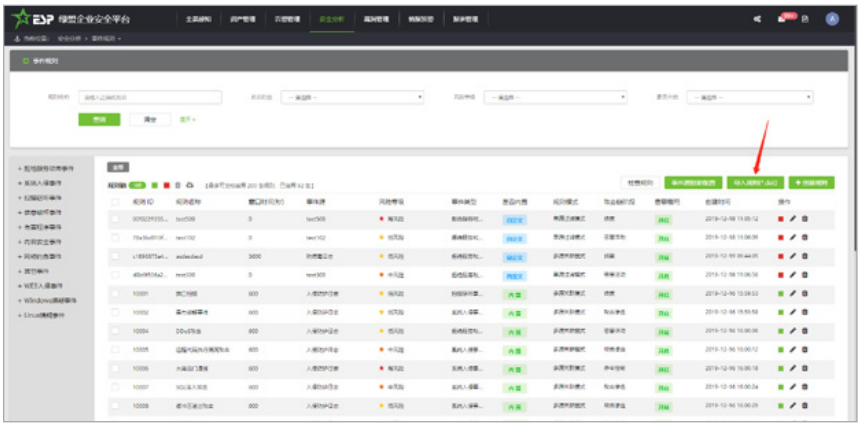
第二步：在“统一规则库升级”中选择“攻击识别规则包”，将下载的最新版本规则包导入上传，并点击升级即可。

5.6 ESP（绿盟企业安全平台）

第一步：登录ESP/ESP-H平台

第二步：进入安全分析-事件规则

第三步：如下图，点击导入规则。



NSFOCUS

安全态势

互联网安全威胁态势

行业动态回顾

1. 新版个人信息安全规范：收集人脸指纹需单独告知，不得存原始信息

【概述】

3 月 6 日，国家市场监督管理总局、国家标准化管理委员会正式发布国家标准《信 息安全技术 个人信息安全规范》(下称《规范》)，并定于 2020 年 10 月 1 日 实施。隐私护卫队注意到，相较于去年 10 月发布的征求意见稿，新版《规范》 规定，收集个人生物识别信息需单独告知使用目的、方式和范围，并且原则上 不应存储原始个人生物识别信息。

【参考链接】

https://mp.weixin.qq.com/s/FudXRODPUY5JwOILzZN mww

2. 多部委联合发布《网络安全审查办法》保障关键信息基础设施供应链安全

【概述】

为了确保关键信息基础设施供应链安全，维护国家安全，依据《中华人民共和国国家 安全法》《中华人民共和国网络安全法》，制定本办法。国家互联网信息办公室、国 家发展和改革委员会、工业和信息化部、公安部、国家安全部、财政部、商务部、中 国人民银行、国家市场监督管理总局、国家广播电视总局、国家保密局、国家密码管 理局联合制定了《网络安全审查办法》，现予公布。

【参考链接】

http://www.wfnetworks.cn/news1/shownews.php?id=445

3. 国家计算机病毒应急处理中心监测发现二十一款违法移动应用

【概述】

国家计算机病毒应急处理中心近期在“净网 2020”专项行动中通过监测发现，多款 民宿、会议类移动应用存在隐私不合规行为，违反网络安全法相关规定，涉嫌超范围 采集个人隐私信息。

【参考链接】

http://www.cac.gov.cn/2020-04/30/c_1589794449796151.htm

4. 人工智能国际标准制定情况及我国应对策略

【概述】

美国和中国在内的主要国家一致同意把人工智能国际标准放在首位；各主要国家人工智能领域的国家战略表明，各国都计划推行自己的国家标准;考虑到人工智能行业的市场结构，各国都在努力实现自己的国家标准与国际标准统一。

【参考链接】

https://mp.weixin.qq.com/s/OU4f5Ltcpnj8tAavBjcAGQ

5. 《工业数据分类分级指南(试行)》发布

【概述】

工业和信息化部近日印发《工业数据分类分级指南(试行)》，《指南》适用于工业和信息化主管部门、工业企业、平台企业等开展工业数据分类分级工作。其所指工业数据是工业领域产品和服务全生命周期产生和应用的数据，包括但 不限于工业企业在研发设计、生产制造、经营管理、运维服务等环节中生成和 使用的数据，以及工业互联网平台企业在设备接入、平台运行、工业 APP 应用 等过程中生成和使用的数据。

【参考链接】

https://mp.weixin.qq.com/s/aiA45px4ABtcLusHwsKo-g

6. 专题 | 多位院士专家解读“新基建”下的网络安全

【概述】

在国家政策推动下，5G 网络、数据中心、工业互联网等新型基础设施建设加快 推进，可以预见，“新基建”将成为我国经济增长的新引擎。不过，“新基建” 在助力产业新秩序重新建立的同时，也将面临网络安全带来的新挑战。当下人 们已经通过物联网、人工智能、大数据解决很多问题，随着接入网络设备的快速增长，每天产生海量的数据，对关键信息基础设施进行安全保障至关重要。 近日，就有多位院士专家在网络安全线上研讨会上表示，在新基建为中国经济 发展铺路的同时，网络安全可为新基建保驾护航。

【参考链接】

https://mp.weixin.qq.com/s/gYHVZH-bbEGNYOCC17Hq0A

7.《网络安全等级保护定级指南》等26项国家标准获批发布

【概述】

根据 2020 年 4 月 28 日国家市场监督管理总局、国家标准化管理委员会发布的中华人 民共和国国家标准公告(2020 年第 8 号)，全国信息安全标准化技术委员会归口的 GB/T 20281-2020《信息安全技术 防火墙安全技术要求和测试评价方法》等 26 项国 家标准正式发布。

【参考链接】

https://www.tc260.org.cn/front/postDetail.html?id=20200506161016

8. 工业和信息化部办公厅关于深入推进移动物联网全面发展的通知

【概述】

要着力完成加快移动物联网网络建设、加强移动物联网标准和技术研究、提升移动物联网应用广度和深度、构建高质量产业发展体系、建立健全移动物联网安全保障体系等五项重点任务。

【参考链接】

http://www.miit.gov.cn/n1146290/n1146402/c7901537/content.html

9. 农业农村部印发《2020年农业农村部网络安全和信息化工作要点》

【概述】

为贯彻落实《中共中央、国务院关于抓好“三农”领域重点工作确保如期实现全面小 康的意见》《数字乡村发展战略纲要》要求，做好 2020 年农业农村信息化重点工作， 制定本文件。

【参考链接】

http://www.gov.cn/zhengce/zhengceku/2020-05/09/content_5510161.htm

10. 水利部就网络安全攻防演练发现的问题约谈相关单位责任领导

【概述】

通过本次攻防演练可以看出，水利行业网络安全防护能力有了明显提升，但也暴露出 源代码泄露、移动 APP 漏洞成为网络攻击的突破口等新问题。

【参考链接】

http://www.mwr.gov.cn/xw/slyw/202005/t20200509_1403063.html

11. CNCERT：2019年我国近4%网站被篡改，2%网站被植入后门

【概述】

中国互联网络信息中心(CNNIC)每年发布的《中国互联网络发展状况统计报告》是 国内目前官方权威的互联网行业年报。根据 CNCERT 监测，2019 年监测发现我国境内 被篡改网站约 18.55 万个，其中政府网站 515 个;被植入后门网站约 8.49 万个，其 中政府网站 717 个。

【参考链接】

https://www.secrss.com/articles/19357

12. 全国人大常委会：个人信息保护法草案稿已形成，将尽快提请审议

【概述】

目前，已形成个人信息保护法草案稿，将根据各方面意见进一步完善后，按照全国人 大常委会立法工作的安排，争取及早将法律草案提请全国人大常委会审议。

【参考链接】

https://www.secrss.com/articles/19495

13. 工信部：关于工业大数据发展的指导意见

【概述】

立足当前、着眼未来，制定出台《指导意见》意义重大。一是贯彻落实党中央、国务 院工作部署的重要举措;二是有利于加快工业数字化转型进程;三是有利于凝聚各方 共识，构建协同推进的工作体系，形成发展合力，着力解决突出问题，共建共创工业 大数据生态。《意见》指出，要强化数据安全，构建工业数据安全管理体系，加强工 业数据安全产品研发。

【参考链接】

http://www.miit.gov.cn/n1146295/n1652858/n1652930/n3757022/c7909590/content.html

14. ZUC国产密码算法正式成为ISO/IEC国际标准

【概述】

ZUC 序列密码算法是我国商用密码算法体系的重要组成部分,主要用于数据的机密性 和完整性保护,是实现网络空间安全的基础算法和核心技术。在第 60 次国际标准化组 织、国际电工委员会第一联合技术委员会信息安全分技术委员会(ISO/IECJTC1SC27) 工作组会议上,含有我国 ZUC 序列密码算法的 ISO/IEC18033-4/AMD1《加密算法第 4 部分:序列算法-补篇 1》获得一致通过,成为 ISO/IEC 国际标准,进入标准发布阶段。

【参考链接】

http://www.oscca.gov.cn/sca/xwdt/2020-05/11/content_1060747.shtml

15. 中国人民银行：开展金融科技应用风险专项摸排工作

【概述】

本次摸排工作主要范围包括移动金融客户端应用软件、应用程序编程接口、信息系统 等，包括个人金融信息保护、交易安全、仿冒漏洞、技术使用安全、内控管理等 5 个方面风险情况。

【参考链接】

https://www.cebnet.com.cn/20200513/102660476.html

16. 公安网安部门发布违法收集公民个人信息十大案例

【概述】

今年第一季度，全国公安机关网安部门充分发挥职能作用，加大公民个人信息保护力 度，依法查处违法违规收集公民个人信息 APP 服务单位 386 个，涉及信息咨询、辅助 学习、文学小说、新闻资讯、娱乐播报等多个类型。其中，97 个 APP 被予以行政处 罚，192 个 APP 被依法责令改正违法行为，51 个 APP 被下架、停运，有效保护了公民 个人信息。

【参考链接】

https://www.mps.gov.cn/n2254098/n4904352/c7200720/content.html

17. 国家标准《网络安全事件应急演练指南》正式发布

【概述】

2020 年 4 月 28 日国家市场监督管理总局和国家标准化管理委员会发布了《GB/T 38645-2020 信息安全技术 网络安全事件应急演练指南》新的国家标准，新的国标将 于2020年11月1日正式实施。

【参考链接】

https://xiaomibk.com/6430/

18. 央行：加强金融业网络安全和信息化统筹指导

【概述】

会议要求，加强科技支撑，深入开展“数字央行”建设，提升金融服务水平和金融监 管能力;加强金融业网络安全和信息化统筹指导，推动落实金融领域密码应用与创新 发展，筑牢金融网络安全屏障。

【参考链接】

http://news.10jqka.com.cn/20200519/c620256111.shtml

19. 深圳证监局：个别券商风险防范不足，与第三方合作需充分尽调

【概述】

个别券商存在客户更换设备后交易认证手段不完善，风险提示不足，与第三方合作平 台信息安全边界不清、权责不明等问题;同时，同花顺作为券商合作第三方平台，存 在用户登录认证方式不完善、安全防护措施薄弱等情况。

【参考链接】

https://www.secrss.com/articles/19589

20. 2019年开源软件风险研究报告

【概述】

开源软件复杂的供应链关系、不断增加的安全漏洞与恶意软件包，以及开源许可证的风险，已成为不可忽视、亟需重视和管控的领域。

【参考链接】

https://www.anquanke.com/post/id/206432

21. 巴基斯坦发布《个人信息保护法》新草案解析

【概述】

根据该《法案》，联邦政府将在生效后的六个月内建立巴基斯坦的个人数据保护局，并制定规则来执行该《法案》。

【参考链接】

https://www.secrss.com/articles/19639

22. APP 违法违规收集使用个人信息专项治理报告(2019)

【概述】

《报告》显示，一年来专项治理工作成效显著，App 无隐私政策、强制索权、无法注 销等普遍问题明显改善，“一次性打开多个授权”问题在常用 App 中趋近于零。

【参考链接】

http://www.cac.gov.cn/2020-05/26/c_1592036763304447.htm

23. 盘点：2020两会上关于“个人信息保护”的声音

【概述】

今年两会期间，“个人信息保护”再次成为大家关注的热门话题。万众瞩目的《民法典 (草案)》提请审议，草案可谓进一步强化了对隐私权和个人信息的保护。在 5 月 25 日的全国人大常委会工作报告中也指出，下一步的主要工作安排将制定个人信息 保护法、数据安全法等。许多代表委员对于个人信息保护，都表达了自己的看法和建 议。

【参考链接】

http://www.ankki.com/AboutNewsDetail_84_4909.html

24. 23%的跨国银行数据库暴露，存在数据泄露风险

【概述】

根据 Reposify 最新公布的报告，全球领先跨国银行中，23%都有至少一个配置错误 的数据库暴露于互联网，存在数据泄露风险。 报告评估了 25 家

跨国银行及其 350 多家子公司的暴露敏感资产的普及率，包括暴露数据库、远程登录服务、开发工具和 其他资产。

【参考链接】

https://www.cebnet.com.cn/20200528/102664711.html

25.【国防工业】GAO指出美国防部应采取措施改进武器系统可靠性

【概述】

武器系统的可靠性直接影响到作战人员完成任务的能力，以及武器系统在全寿命周期 (通常长达数十年)内的支持维护费用。当前美国防部采办项目交付的武器系统仍普 遍存在可靠性问题。

【参考链接】

http://www.yidianzixun.com/article/0PUlTFJP

26. 盘点亚太区隐私保护立法动向多国加强立法以实现与欧盟共享数据

【概述】

近日，我国与个人信息保护有关的两部法律更新立法动向。全国人大常委会法工委相 关负责人称个人信息保护法草案稿已形成;《民法典》已提请十三届全国人大三次会 议审议，出台后将标志着个人信息保护的顶层立法设计基本完成。

【参考链接】

https://www.sohu.com/a/398116516_161795?g=0

让安全更有效
绿盟科技安全服务
专业|灵活|高效

咨询服务
安全规划
合规咨询
信息安全管理体系咨询
应急体系建设
……

可管理安全服务
远程安全运维
全评估/测试服务
安全基线服务
应急响应
……

安全评价
外部检查辅导
安全指标体系度量
……

安全研究
渗透测试
源代码审计
业务安全测试
漏洞挖掘
……

教育培训
安全技能培训
安全意识教育
……

THE EXPERT
BEHIND GIANTS
巨人背后的专家

多年以来，绿盟科技致力于安全攻防的研究，为运营商、政府、金融、能源、互联网以及教育、医疗等行业用户，提供具有核心竞争力的安全产品及解决方案，帮助客户实现业务的安全顺畅运行。在这些巨人的背后，他们是备受信赖的专家。

客户支持热线：400-818-6868

NSFOCUS绿盟科技

安全月报

绿盟科技金融事业部出品

主办/绿盟科技金融事业部
地址/北京市海淀区北洼路4号益泰大厦3层
邮编/100089
电话/010-59610688-1159
传真/010-59610689
网站/www.nsfocus.com
客户支持热线/400-818-6868
股票代码/300369
月报电子版下载/http://www.nsfocus.com.cn/research/list_145_145.html