金融行业

10月报
2021年

安全月报

安全观点 | 行业研究 | 漏洞聚焦 | 安全态势

绿盟科技金融事业部出品

安全观点

《数据安全法》下金融数据
安全风险评估研究与实践

行业研究

【安全告警数据分析之道:一】
数据透视篇

两程序员制作证券软件外挂:
可侵入 84 家证券公司交易系统

Firefox 插件“Safepal 钱包”
窃取加密货币

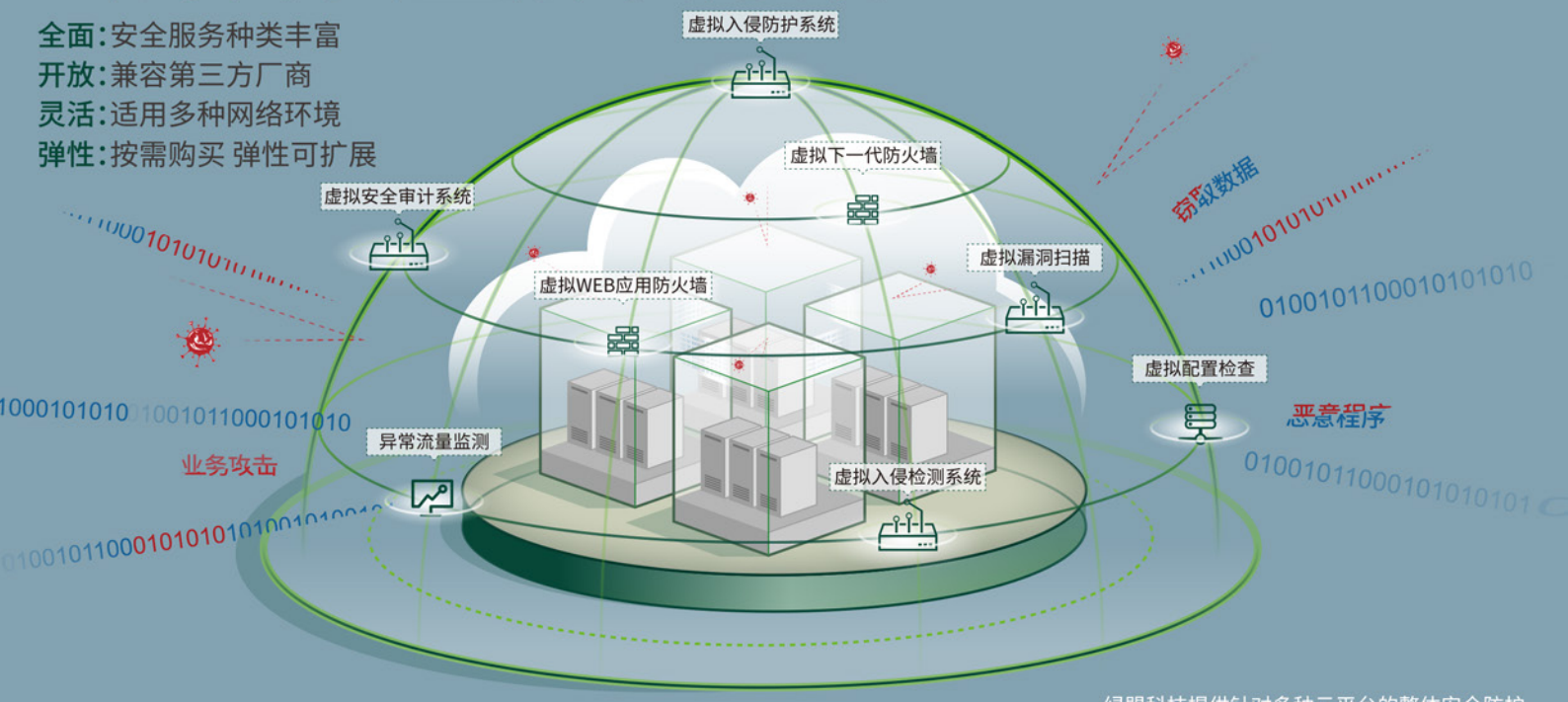
Oracle 全系产品10 月重要
补丁更新通告

微软 10 月安全更新多个产品
高危漏洞通告

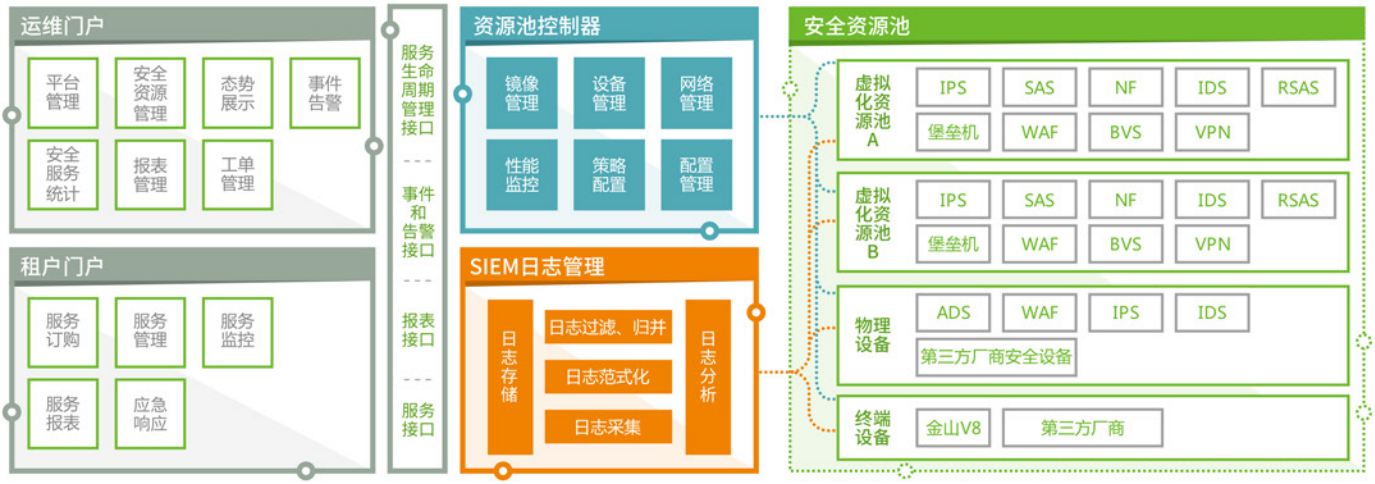
NSFOCUS

绿盟科技
云计算安全解决方案

全面:安全服务种类丰富
开放:兼容第三方厂商
灵活:适用多种网络环境
弹性:按需购买 弹性可扩展



绿盟科技提供针对多种云平台的整体安全防护



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

本|期|看|点

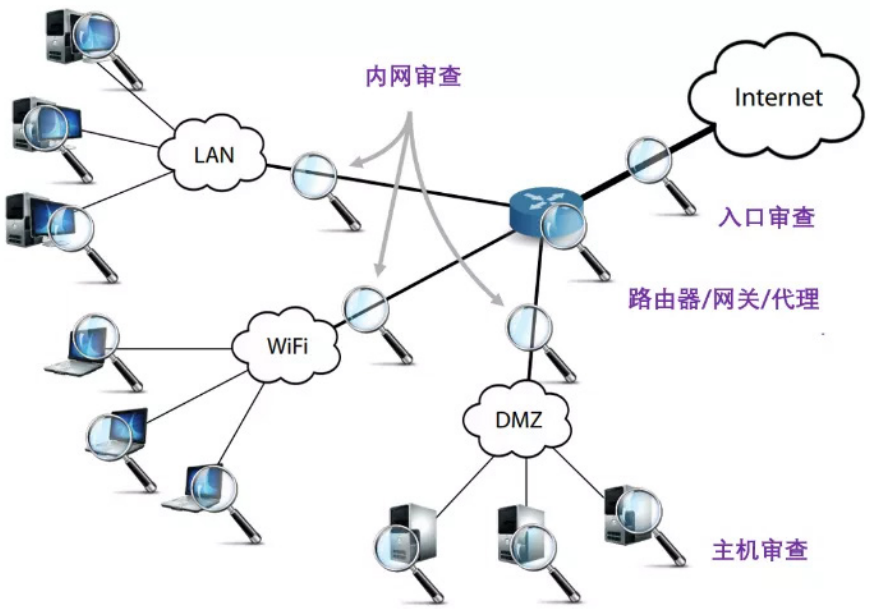
P04 《数据安全法》下金融数据安全风险评估研究与实践

《数据安全法》与标准规范

《金融科技（FinTech）发展规划（2019-2021 年）》
---数据安全在金融科技安全中也被赋予了最多的关注。

指引文件	数据生命周期安全
《 JRT 0218-2021金融业数据能力建设指引》 《 JR/T 0196-2020 多方安全计算金融应用技术规范》	《JR/T 0223-2021金融数据安全数据生命周期安全规范》
技术要求	**个人信息保护**
《JR/T 0197-2020 金融数据安全 数据安全分级指南》 《 JR/T 0158-2018 证券期货业数据分类分级指引》	《GB/T 35273-2020个人信息安全规范》 《JR/T 0171-2020个人金融信息保护技术规范》

P12 【安全告警数据分析之道：一】数据透视篇



安全月报

2021年第10期

绿盟科技金融事业部

目录 CONTENTS

安全月报在线阅读

绿盟科技官方微信

NSFOCUS

安全观点

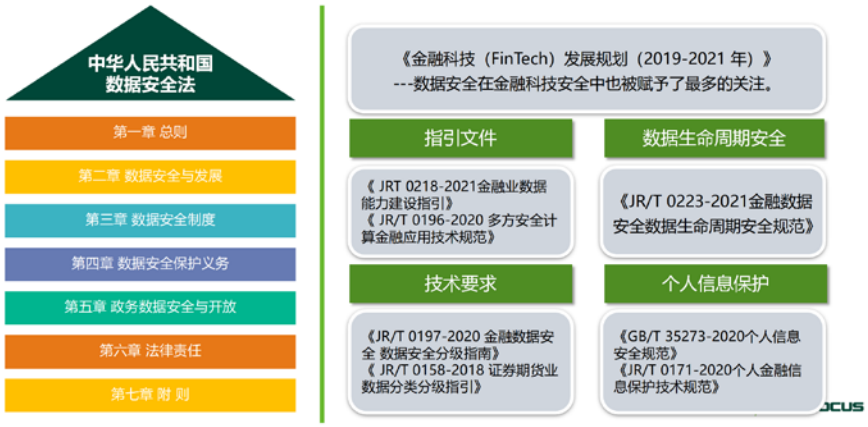
《数据安全法》下金融数据安全风险评估研究与实践

绿盟科技 施岭

数据安全现状分析

在《数据安全法》体系之下，2019年至2021年金融行业发生多起事件，相关部门对数据安全下达多项指导意见和方针，金融机构应在可见的法律和规范内进行合规化建设，避免因某些无意识的操作而造成数据泄露，从而遭到处罚。

《数据安全法》与标准规范



金融行业数据存在四方面特性，一是存在形式多样式，包括结构化数据、半结构化数据、非结构化数据，二是动态流转复杂性，包括全生命周期动态流转、实际业务驱动数据动态流转，三是数据主体多样式，包括基础设备、数据中心、部门间和第三方机构，四是数据价值模糊性，包括数据确权问题、数据归属认责、数据价值准确评估。

应对上述特性，很多企业都在做数据咨询服务。全行业可以把数据咨询服务分为数据分类分级、个人信息安全影响评估、数据安全评估、数据安全管理体系建设、数据安全培训等。

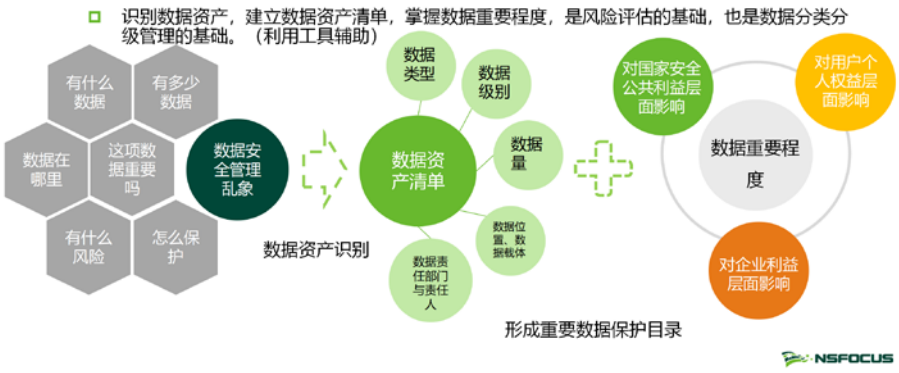
数据安全咨询场景

数据安全数据安全第一步：分类分级

《数据安全法》第三章第二十一条明确提出，国家建立数据分类分级保护制度，依据危害程度，对数据实行分类分级保护。各地区、各部门应当按照国家有关规定，确定本地区、本部门、本行业重要数据保护目录，对列入目录的数据进行重点保护。

在进行数据分类分级之前，首先要明确所有数据的属性，做数据资产的识别。识别数据资产、建立数据资产清单、掌握数据重要程度是风险评估的基础，也是数据分类分级管理的基础。

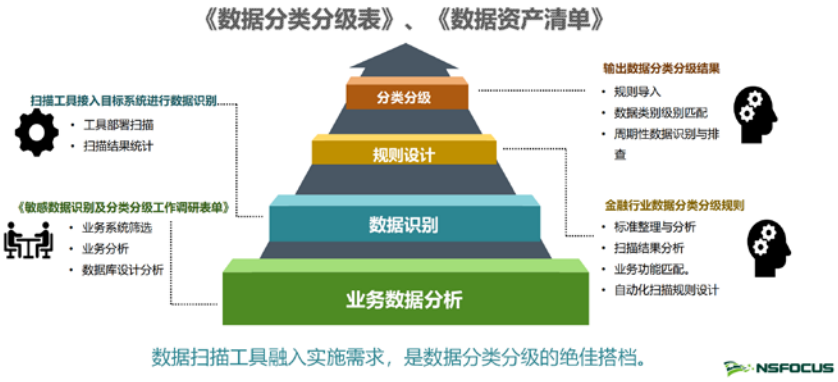
数据资产识别



数据分类分级需要一定原则性，其中数据分类基于系统性、规范性、稳定性、扩展性、明确性等，数据分级基于依从性、可执行性、时效性、自主性、合理性、客观性等。《数据安全法》基于敏感赋值，将数据的类别分为一般数据、重要数据、核心数据。数据分类分级的目的是将数据以标签化的模式进行管理。

在进行分类分级时，可以利用扫描工具最大化提升效率。目前，市面上已经推出一些数据扫描工具，IDR产品设计融入了实施需求，是数据分类分级的绝佳搭档。

利用扫描工具最大化提升效率



数据的分类分级需要前期准备工作、数据资产调研、数据分类分级、制定分级管理办法、汇报与总结等必不可少的流程，每一个流程都有其相对应的服务成果，比如过程文档-项目实施计划、数据资产调研记录、《数据分类分级表》和《数据资产清单》《数据分级管理办法》《数据分类分级服务报告》等。

以个人金融信息数据分类分级为例，按敏感程度从高到低分为C3、C2、C1三个类别，即高敏感、中敏感、低敏感三类。两种或两钟以上的低敏感度类别信息经过组合、关联和分析后可能产生高敏感程度的信息，同一信息在不同的服务场景中可能处于不同的类别，这些应依据服务场景以及该信息在其中的作用，对信息的类别进行识别，并实施针对性的保护措施。

个人金融信息数据分类分级实例

类别	等级	描述
C3	高敏感	主要为用户鉴别信息。
C2	中敏感	主要为可识别特定个人金融信息主体身份与金融状况的个人金融信息，以及用于金融产品与服务的关键信息。
C1	低敏感	主要为机构内部的信息资产，主要指供金融业机构内部使用的个人金融信息。

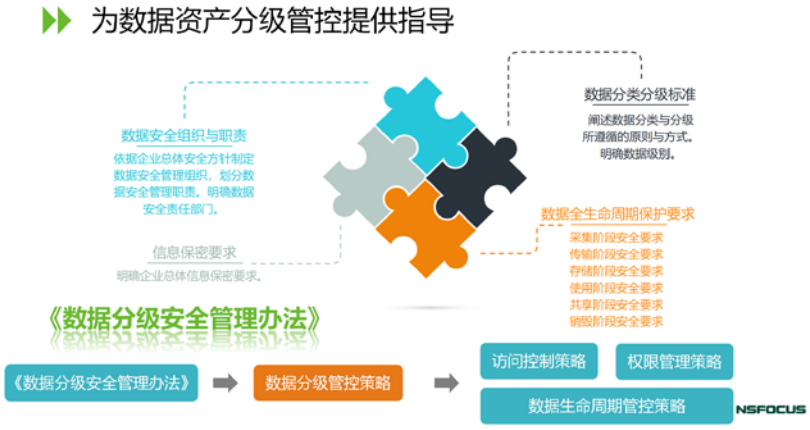
按敏感程度从高到低分为C3、C2、C1三个类别

两种或两钟以上的低敏感度类别信息经过组合、关联和分析后可能产生高敏感程度的信息，同一信息在不同的服务场景中可能处于不同的类别，应依据服务场景以及该信息在其中的作用对信息的类别进行识别，并实施针对性的保护措施。

数据内容	数据类别
姓名	C2
身份证号码	C2
身份证影印件	C2
家庭住址	C2
手机号码	C2
登陆用户名	C2
登陆密码	C3
指纹	C3
短信验证码	C2
开户时间	C1

资料来源JRT 0171-2020《个人金融信息保护技术规范》 NSFOCUS

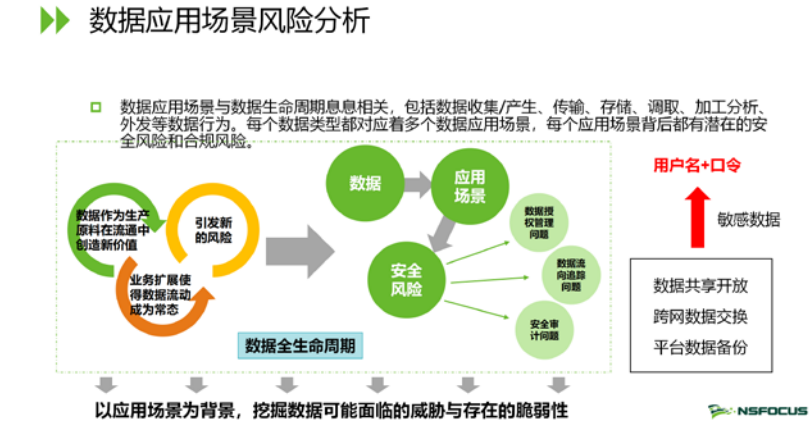
数据分类分级需要明确数据安全的组织责任，将《数据分级安全管理办法》结合数据分级管控策略，结合数据生命周期的每个阶段，把数据安全的访问控制落到实处。



数据安全风险评估实践

《数据安全法》第四章第三十条明确提出，重要数据的处理者应定期开展风险评估，并向有关主管部门报送风险评估报告。数据安全风险评估能够帮助组织发现自身数据安全问题和短板，明确数据安全保护需求，为建设数据安全管理和技术手段指明方向，给出解决方案。

数据应用场景与数据生命周期息息相关，包括数据收集/产生、传输、存储、调取、加工分析、外发等数据行为。每个数据类型都对应着多个数据应用场景，每个应用场景背后都有潜在的安全风险和合规风险。

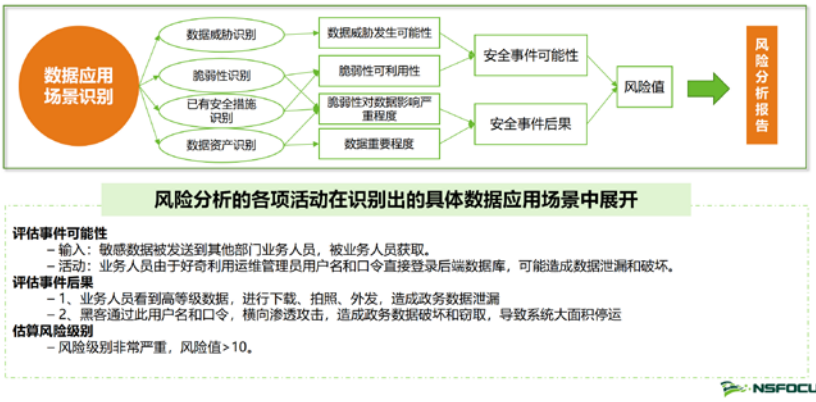


对于个人信息而言，需要分析其中是否存在对个人权益的影响，以及影响程度。典型的个人权益影响类型包括影响个人自主决定权、引发差别性待遇、个人名誉受损或遭受精神压力、个人财产受损等。

安全事件的可能性分析需要从网络环境与技术措施、处理流程规范性、参与人员与第三方、安全态势及处理的规模等四个方面入手。

风险分析的各项活动在识别出的具体数据应用场景中展开，从场景中识别数据威胁、脆弱性、已有安全措施、数据资产，进而判断数据威胁发生可能性、脆弱性和可利用性、脆弱性对数据影响严重程度、数据重要程度，进而得出安全事件可能性、安全事件后果，然后将其赋值，变成一种风险值，最终形成风险分析报告。

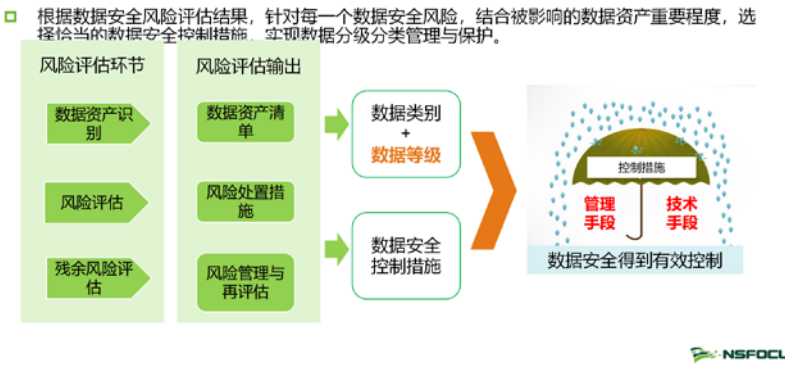
数据安全风险评估实施流程



当数据安全发生风险时，需要采取适当方式进行处置，一是控制风险，即及时发现风险，降低损失，二是转嫁风险，即可利用安全公司、保险公司等第三方机构进行风险转嫁，三是避免风险，即做好日常监测，培养相关人员的安全意识，四是接受风险，即在无法避免风险的前提下，及时溯源处置。风险处置措施的涉及风险描述、风险值、风险处置措施、风险处置步骤、相关责任人、预计时间、风险级别等。

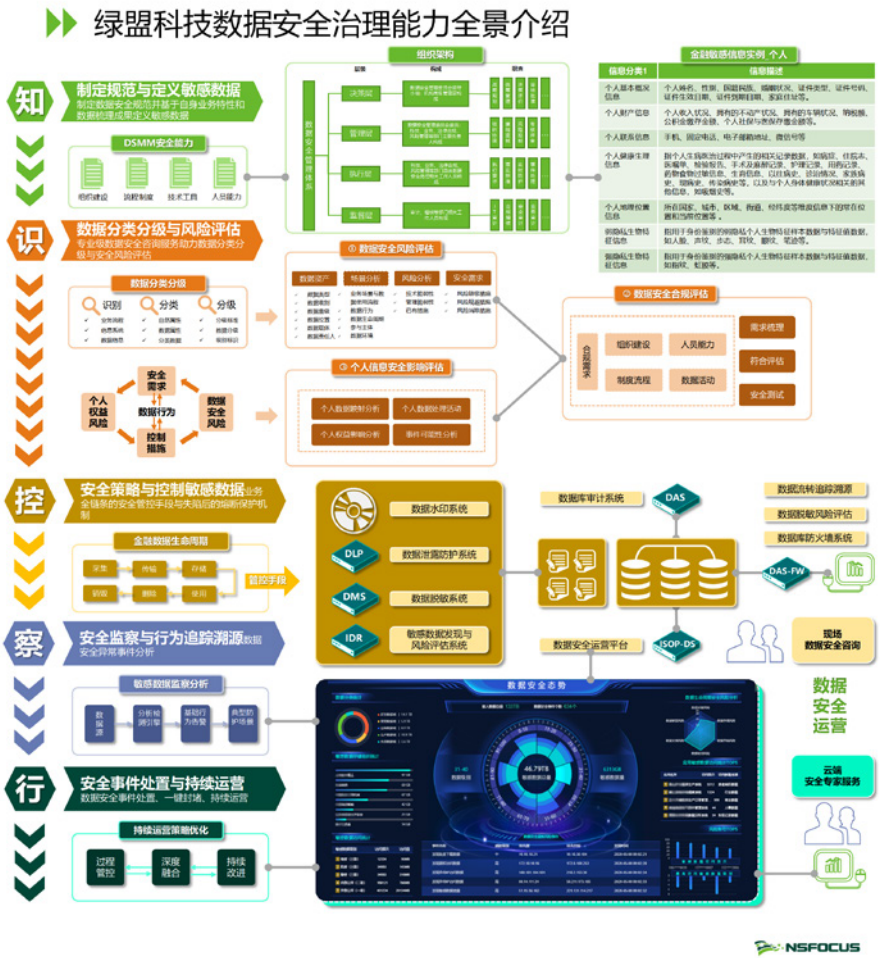
根据数据安全风险评估结果，针对每一个数据的安全风险，结合被影响的数据资产重要程度，应选择恰当的数据安全控制措施，实现数据分级分类管理与保护。

数据安全风险管控



数据安全治理全景介绍

依据方法论，绿盟科技通过五个阶段对数据安全进行治理。一是“知”，即制定规范与定义敏感数据，二是“识”，即数据分类分级与风险评估，三是“控”，即安全策略与控制敏感数据，四是“察”，即安全监察与行为追踪溯源，五是“行”，即安全事件处置与持续运营。



贴身服务 加油干

绿盟科技城商行信息安全解决方案

无缝衔接 | 密切配合

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，为金融、政府、运营商、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。

NSFOCUS绿盟科技

NSFOCUS

行业研究

【安全告警数据分析之道：一】数据透视篇

绿盟科技 天枢实验室

摘要

日前，在企业安全运营当中，SIEM的热潮已经逐渐淡去，很多企业已经逐渐成立了安全运营中心（SOC），收集到了海量安全数据。但是如何利用这些数据，如何进行分析等问题并没有很好地解决。数据往往只是做简单存储，数据价值未得到体现。其实在网络安全领域最重要的还是“数据”，做攻击离不开各种资产数据、漏洞数据，做防御离不开资产数据、设备告警数据，对各种攻击活动的分析更是离不开DNS、样本、用户行为等数据，《安全告警数据分析之道》为系列文章，旨在对企业网络侧安全告警数据进行深入分析，挖掘数据的潜在价值，助力企业日常安全运营。

实际上为了分析安全告警，近年来一些公司以数据分析、人工智能的方法来分析这些数据，而分析、理解数据，进而对数据进行标记往往是使用人工智能算法等高级算法的必备条件，但这一前置过程往往被忽略。本文为系列文章的首篇，浅谈对安全告警数据分析的思考，并且以一次实际网络攻防演习数据为例，介绍对告警数据进行标记的方法，分析并总结可能的研究点和数据的潜在价值

一、概述

随着现代企业网络结构的复杂化，如复杂的网络分区、企业上云、新型网络设备等，安全设备的告警量与日剧增。虽然SOC团队一般会对这些告警数据进行存储，但是暴增的数据量与合理分析方法的缺失进一步加重了SOC团队的压力。根据实际经验，一般来说，一个业务稍微复杂一点的大中型企业，每天的告警数据量会达到百万量级。在工业界，这类数据基本组成少有暴露，数据的整体轮廓往往不得而知，而处理方法往往太过抽象，如使用UEBA的方法，目前笔者也尚未接触到对此类数据进行完整分析的方法；另一方面，在学术领域，对IDS的数据研究从本世纪初就开始了，然而那时候的网络结构比较简单、攻击手法较为单一，近些年虽然也有零星的研究成果出现，但依然使用20年前的数据集，借鉴意义不大。那么安全告警分析之路该何去何从？安全告警数据到底有何价值？本文将给出见解。

二、安全告警分析的能与不能

如图1所示，企业一般会在内网和企业网络出口部署安全设备，这些安全设备会对流经的网络流量进行威胁分析。而主流的安全设备的检测方式还是

基于规则的检测，并且对于加密流量并没有什么好方法，最多也就是能记录一些加密通信的日志，如SSL协商日志。总结来说基于网络侧的安全告警数据分析无法解决以下问题：

1. 不经过安全设备的流量。实际上这种场景很常见，企业往往只会在重要资产前或者大的区域前部署安全设备，而且攻击者也有各种各样的方式让流量不经过安全设备；

2. 不在规则中的攻击行为。大型网络演习中，攻击者往往会掏出珍藏的0-day漏洞进行攻击，这种攻击不会在网络侧产生告警，往往需要在主机上做进一步的检测；

3. 加密流量。基于DPI的安全设备无法解密加密流量，只能设法（如，拿到目标网站的证书）解密后再处理；

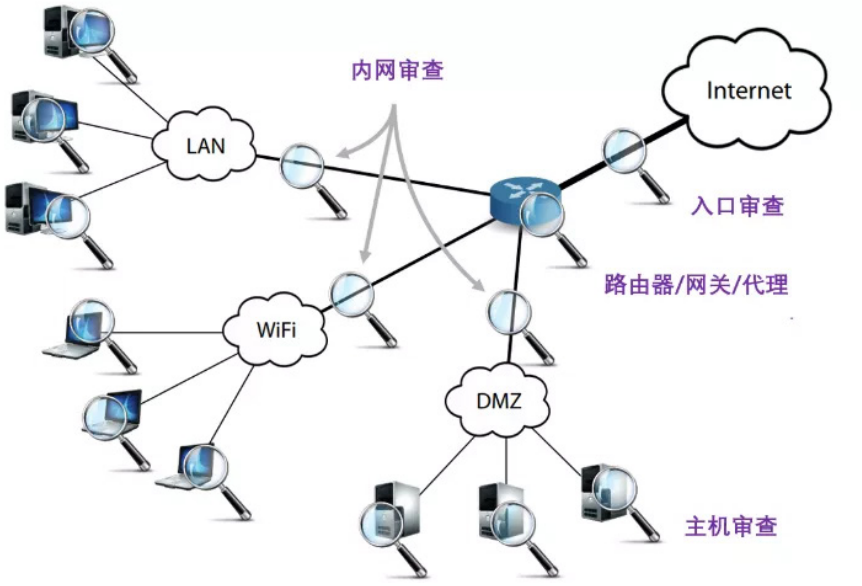


图1　安全设备部署方式

为了分析海量安全告警数据，以比较成熟的安全运营人员为例，他们往往会采取如下方式进行数据处理：

1. 只关注重要资产。特定目标的告警量往往不多，可以进行分析；

2. 只关注特定类型的告警。有经验的运营人员知道特定安全产品的置信度比较高的告警，他们往往只会关注置信度比较高、危害较大的告警类型；

虽然这种方式能够对告警做一个粗略的排序，挑选出高威胁的告警进行分

析，但是显然这种方法是不完善的，且不说有时候需要进行多个告警的联合分析，不得不关注其余告警，就算是只关注特定的告警，还是有大量的攻击行为在剩余告警中，不能弃之不顾。

那么分析安全告警能分析出什么来呢？我们知道，不仅是攻击流量，正常流量也会被安全设备看到，所谓的“高误报率”就是由这部分流量导致的，这部分流量同样可以被利用起来，用于做资产梳理，梳理内网环境，具体来说，安全告警分析能做到：

1. 资产梳理。我们知道大型企业资产往往很混乱，人工很难梳理清楚，这在日常安全运营中也是一大痛点。但是实际上，通过告警数据可以对IP做部分资产梳理工作，不同类型的资产对应的告警差异性往往较大，可以进行分析归类；

2. 灰色行为识别。以漏洞扫描为例，例行的漏洞扫描是正常操作，而没有报备的扫描行为则是异常操作，对这种灰色行为的跟踪也是发现攻击的有效途径；

3. 攻击行为识别。安全设备的初衷。

三、安全告警数据分析

本小节将对一次网络攻防演习数据做简单分析，分析这些数据的组成以及可能的处置方法，阐述数据价值。

3.1 数据基本组成

本文收集了某中型企业的一次网络攻防演习（共计5天）的网络侧安全告警数据，基本的数据统计信息如图2所示，可以看到在这5天之内，每天收集到的告警数据多达上千万条，五天总计5000多万条告警。其中，认证类、目录遍历类和文件传输类的告警为数量占比前三的告警类型，三者之和可占总告警量的70%以上。除了少量的真实攻击，绝大部分的告警都是无害的，让我们抽丝剥茧，看看这些“奇葩”数据的真面目！

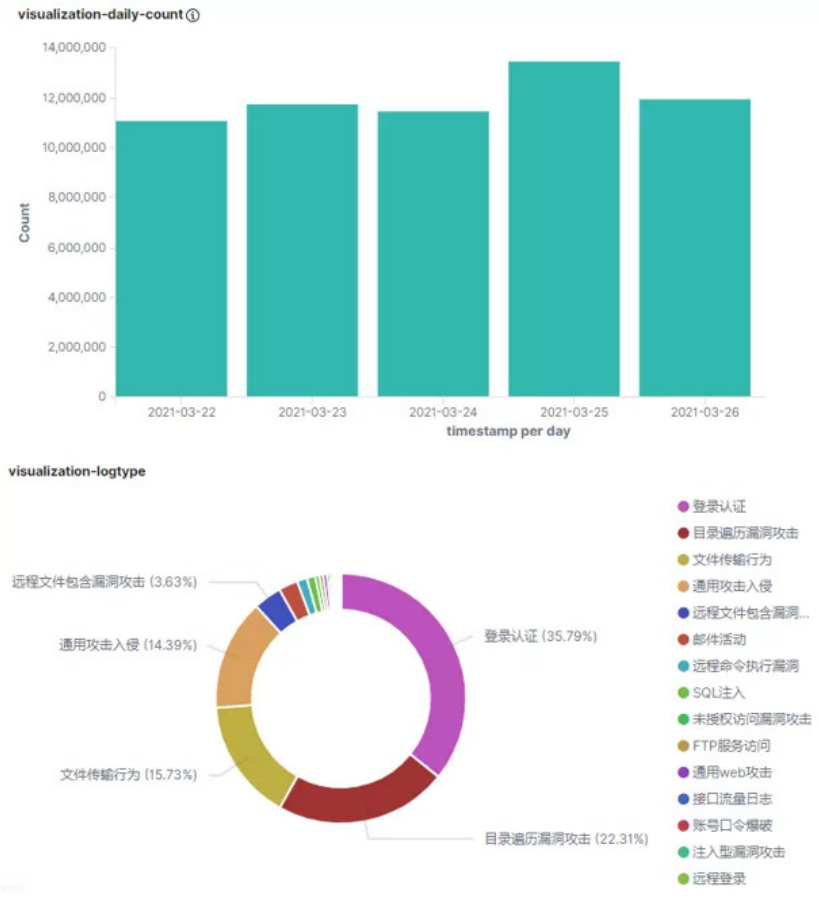


图2　安全告警数据数量和类型统计

3.2 数据分析步骤

1）提取有用字段

由于原始数据包含很多无用信息，我们需要对数据的可用字段做一定的筛选，最终，对于每条告警我们挑选出如下9个有用字段：

timestamp：告警产生时间

sip：源IP

dip：目的IP

device_ip: 产生此条告警的探针IP

dport：目的端口

log_message：告警类型

payload：告警载荷（IP层以上数据）

q_body：Web访问的请求体

r_body：Web请求的响应体

其中，若告警是由Web请求触发的，则有q_body字段，否则只有payload字段，另外，可能会因为设备原因导致部分字段不完整。

特别说明，几乎所有的对IDS告警分析的学术文章都不会将payload等数据包载荷信息纳入分析范围，而在日常运营中这部分信息也是判断攻击的重要依据，不能舍弃。故保留payload、q_body字段，而r_body是判断攻击是否成功的重要依据，同样需要考虑；另一方面，由于不同探针产生的攻击告警（如外网、内网）的分布会呈现一定差异，为了区分，device_ip字段同样需要保留。

2）数据去重

我们知道一个数据包从企业外部到内部的传输过程中，往往会经过多个检测设备，这样就会产生重复告警，这部分的告警应该删除。理想情况下，同一时刻，同一攻击者对同一目标的攻击行为应该只有一条告警。为了达到这个目标我们依据（timestamp，sip，dip，dport ，payload）对原始告警进行去重。当然这样也有例外情况，如：报文延时过大，timestamp不一致，设备问题，对于不同的payload截断后payload相同等等，不过这些情况基本可以忽略。

3）数据分析

一般来说，除去某些特别不准的告警类型之外，log_message字段可以

比较准确地反映出当前数据包的攻击类型。我们对告警类型做了分布分析，如图3左图所示，横坐标为log_message编号，纵坐标为该告警类型发生的次数，可以看到告警类型体现出明显的长尾分布特性，如图3右图所示。我们按照幂律分布的统计方法，横坐标为告警发生次数的对数，纵坐标为这类告警的数量，以图中红框标记的点（0,58）为例，说明在整个数据集中，只有1条记录的告警类型有58种。这类数据分布上的分析，有助于后续高级算法模型的选择。

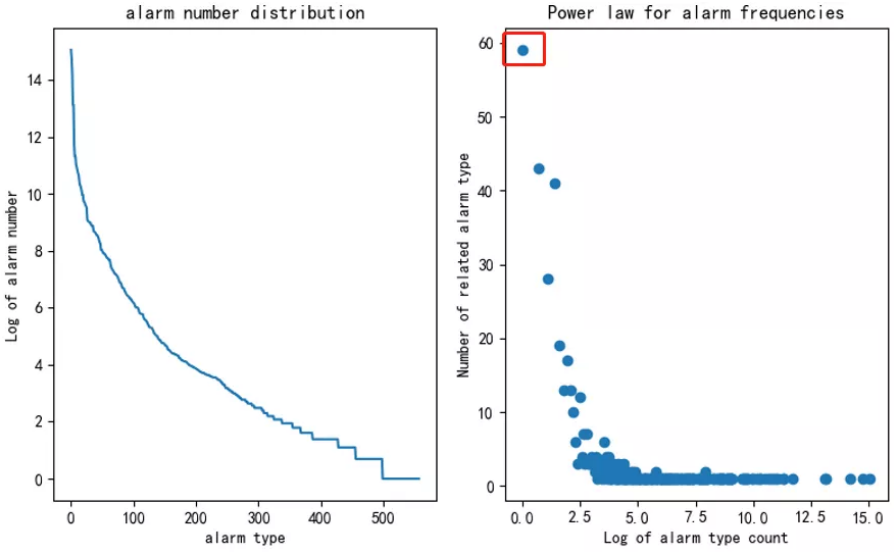


图3　以告警类型为角度的统计分布图

通过以上数据，我们可以看到，从告警类型（log_message）的维度，告警呈现出明显的长尾分布特性。其实不光是告警类型这一属性，在源IP、目的IP等多个属性上，如图4，图5所示，分别以sip、dip为维度进行统计，横纵坐标的含义与图3类似，告警分布均展现出了类似的特性。在多种维度上，告警均展现出明显长尾分布特性，这一特性不仅可以为选择高级算法模型（如word2vec算法）提供有效信息，还很直观地告诉我们：告警分布具有一定的规律性！而告警的这种规律性和流量的自相似性是分不开的，对于这种现象的成因我们在本文不做深入讨论，我们仅需要利用这种特性帮我们进行下一步告警分析：由于攻击流量或者说异常流量本身占比极小，告警的这种规律性是长期存在的，过滤这些占绝大多数的规律性的告警，剩下的就是重要度较高的告警了。

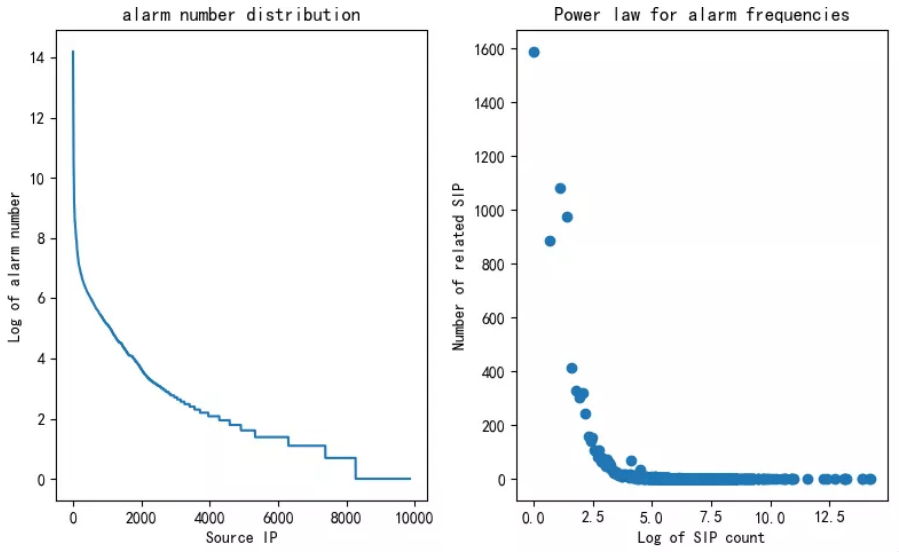


图4　以源IP为角度的统计分布图

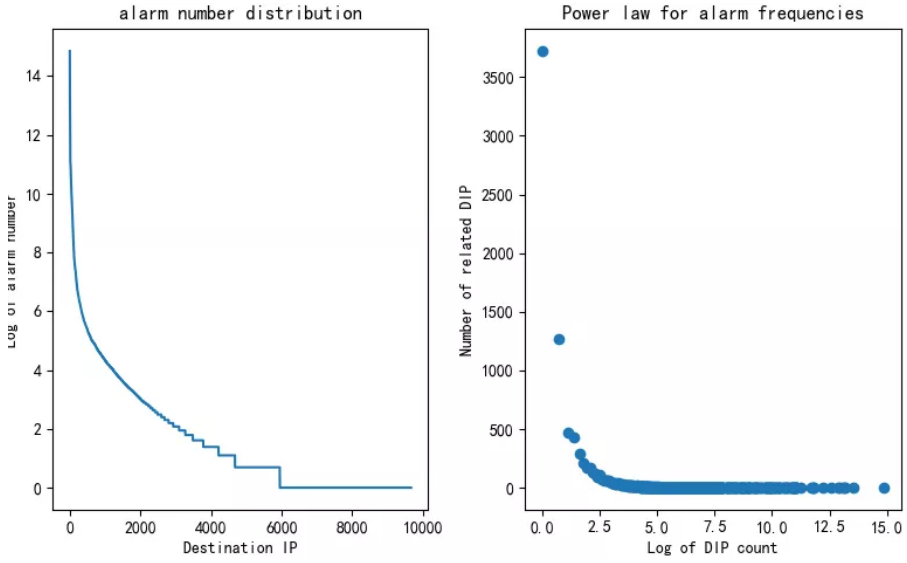


图5　以目的IP为角度的统计分布图

4）数据分类

整体上我们可以按照：数量大到数量小，重要程度低到重要程度高的原则对告警进行过滤、分类，尽量首先将数量大、重要度低的正常告警过滤掉，我们以数据集中触发告警量最多的源IP：10.5.237.232为例，如图6左图所示，该IP与大

量目的IP均有告警产生.图6右图表明，触发告警类型最多的是代理连接，并且呈现明显的规律性，对外网的代理连接在一般处理过程中重要度较低，因此10.5.237.232在此期间内触发的“HTTP协议CONNECT隧道功能(http proxy)连接访问”类型的告警分类为正常告警（正常业务导致），这一条过滤规则即可过滤600多万条告警，约13%的告警量。

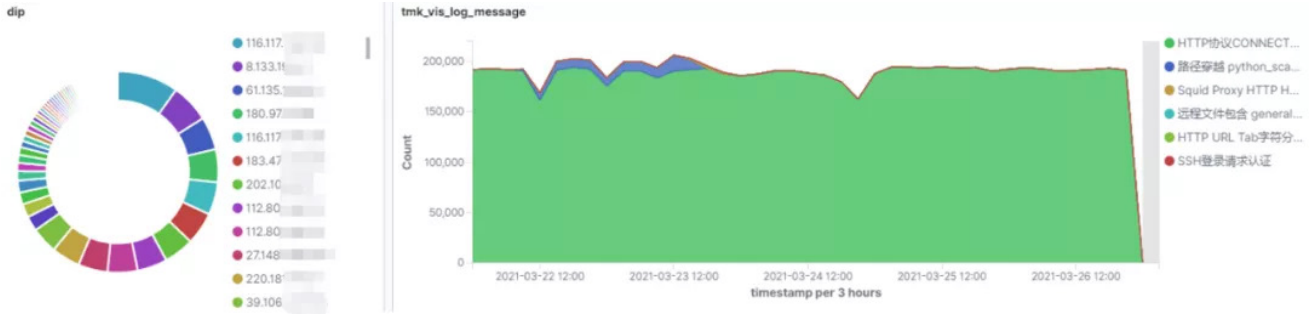


图6　正常告警示例（10.5.237.232触发）

需要特别注意的是，我们需要以一种较细的粒度来对告警进行分类，即结合多种维度对告警进行分类筛选，举个例子：IP地址A经常性的触发告警，我们不能就直接忽略A所触发的告警，而应该关注其具体的内容，什么类型的告警是常见的，什么类型的告警是不常见的。更具体的，如图7上半部分所示，10.66.240.216整体上触发的告警数量比较均匀，乍看没有异常.下半部分表明，10.66.240.216在短时间内对10.245.38.183发起了大量的扫描，而这种扫描行为是突发的、不常规的，对于企业内网来说，存在较大隐患，但是由于其隐藏于源IP触发的大量告警之中，在上半部分的图中很难被发现。

图7　异常告警示例（10.66.240.216触发）

总结来说，我们需要以数量大到数量小，重要程度低到重要程度高的原则找出大部分正常告警，在执行过程中，以一种较细的粒度进行归并统计(如，[sip,dip]的双重维度)。

5）分析结果

通过自动化结合人工的方法，我们得以对大部分的告警做出分析结果，并打上标签。总结来说，告警数据可以分为4大类：

1. 正常告警。该部分由正常行为组成，通常都是由形形色色的正常业务导致，包含正常的漏洞扫描任务等；

2. 低危告警。互联网上存在大量的蠕虫、僵尸网络，这些肉鸡会进行大量常态化的攻击行为，这些攻击往往都不会成功，可以认定为低危告警，做IP封禁操作；

3. 灰色行为。该部分告警展现出一定的威胁性，需要做出一定的处置，如：未报备的内网扫描行为、内网蠕虫传播行为等等，需要联系相应的资产负责人做进一步核查；

4. 高危告警。正在发生或者已经发生的入侵行为。

这4类告警数据量依次递减，重要程度依次增加。

四、总结

本文从宏观上讨论了告警分析所能带来的价值，以一次真实的网络攻防演习数据为例，在对数据简单统计分析的基础上，探讨了对这类数据进行分类分析的大致方向，并对数据进行了简单的归类。本文为系列文章的首篇，讨论进行安全告警数据分析的整体方向。

【安全告警数据分析之道：二】数据过滤篇

绿盟科技 天枢实验室

引言

在系列文章《数据透视篇》中我们提到，安全设备每天所产生的告警量非常庞大，常常达到上千万量级，而绝大部分的告警都是由正常流量造成的，本文为系列文章的第二篇，浅谈这些误报的形成原因，并且阐述过滤这些误报的方法，经过一系列过滤方法，90%以上的告警都会被当成正常流量过滤掉，高威胁度告警全部在残留的不到10%的告警当中。告警过滤机制为我们后续的分析打下了良好的基础。

一、正常流量的组成

我们知道，基本上现行所有网络侧安全设备的工作原理是基于特征的，也就是说只要网络流量里有类似的特征匹配上，就会触发告警，这种工作模式不可避免地会在正常流量中产生大量告警，导致误报，本小节，我们将详细分析某次红蓝对抗数据中正常流量的组成要素。

需要特别说明的是，在这里，我们需要对“正常流量”和“误报”做出一定的区分，“误报”指的是安全设备的告警类型与实际payload对不上，即由于安全设备的误判而产生的告警；“正常流量”是一个更大的范围，不仅包含“误报”，还包含各种非误报触发的告警，如错误配置、正常业务、用户正常上网行为等等。

首先是正常业务行为，正常业务往往纷繁复杂，会随着企业的不同、时间的不同等因素在告警中呈现较大差异，但无论怎样，这部分流量会贡献绝大多数告警，在我们的数据集中，至少90%的告警都是由正常业务触发的，我们举两个例子：

1. 与IP：10.5.237.###相关的告警中，10.5.237.###为威胁情报数据爬取和存储系统，有5个IP (192.168.200.###,192.168.255.###,10.66.250.###,10.82.180.###,192.168.255.###) 对10.5.237.###有大量的SSH访问，主要负责数据的交互，另外，10.5.237.###有大量的对外代理连接，10.5.237.### 会连接大量的代理池IP，利用这些代理IP进行持续的威胁情报信息爬取。这部分告警占总告警量的45%左右；

2. 与IP段：10.51.10.*相关的告警，该C段IP会对各种来源的恶意样本进行静态和动态沙箱分析，分析结果会写入到集群当中，也会对集群中的数据进行读取，进行下一步分析，所有通信步骤通过python脚本进行交互，会触发大量的

“路径穿越 python_scanner”类型告警，这部分告警占总告警量的20%左右。

用户的正常上网行为也会触发大量告警，如在使用微信的通信过程当中（图1），微信使用基于TLS 1.3的微信安全通信协议mmtls进行通信，微信的短连接为post请求，通信内容加密，由于无法解密，二进制的字节流，如b’\x19\xf1\x03\x00\xa1\x00\x00\x00\x9d’，会让设备产生误判，以为是在进行命令注入，产生命令注入类告警；同时用户安装的很多应用程序，如金山、微软等，会在后台持续进行通信，进行数据回传、应用更新等一系列操作，这些对用户透明的通信行为也会触发大量的告警。

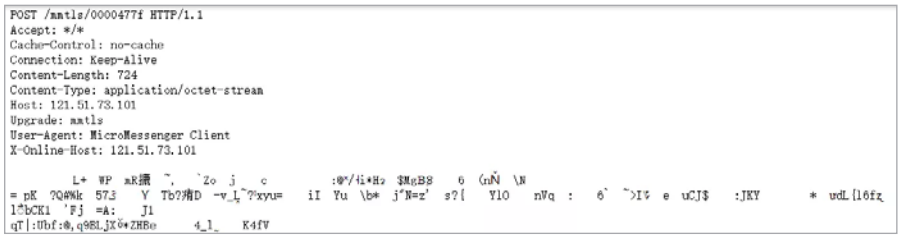


图1　微信通信的载荷内容样例

常规性的漏洞测试行为。大型公司内部往往会对其内部系统做渗透测试，以发现潜在风险，这种内部的测试行为一旦发生就会触发大量设备告警。由于什么渗透测试属于敏感操作，攻击者在内网中往往也会触发类似的告警，因此对于这部分的告警需要格外注意。

二、正常流量过滤

在第一篇文章《数据透视篇》中我们提到，告警数据不论从源IP、目的IP、告警类型等任何方面，告警分布均呈现出幂律分布的特点，即少量的实体贡献了绝大部分的告警，通过上一小节我们也可以了解到，某几个正常的业务就能触发大部分告警。这一小节我们主要利用这一规律对正常流量进行过滤。

对于常见的正常业务，其最明显的特征就是规律性，这种规律性在多种维度体现：访问时间的规律性、告警类型的规律性、源IP和目的IP的规律性、告警载荷的规律性等等，对于这些规律性，不同业务之间可能会存在较大差异，我们的目标也是发现这些正常业务在告警中体现的规律并且过滤，在此我们举两个例子：

示例一

如图2所示，图中展示了10.200.10.###到192.168.255.##的所有告警类型的数量随时间变化的曲线图，纵坐标为每一小时所触发的告警数量，横坐标为时间，其中黄色部分为路径穿越类告警，橙色部分为通用web攻击类型告警。我们可以发现如下规律：

1. 告警类型单一。两个IP之间仅触发两种类型的告警，虽然可能存在一定误报的可能，但是单一的告警类型体现出两者之间通信行为的单一，若是攻击者，很难只触发这两种类型告警。

2. 告警数量大且持续性高。在5天之内，每小时都触发大约650条告警，数量巨大、持续性强的告警只有正常业务才有可能触发，攻击者很难做到24小时在线，持续大量地触发安全设备告警而不被发现。

3. 告警载荷规律性明显。两者之间的所有告警基本全部形如图3所示，仅仅是URL路径存在些许差别，从payload可以看出这些告警都是由正常业务所引发的误报。

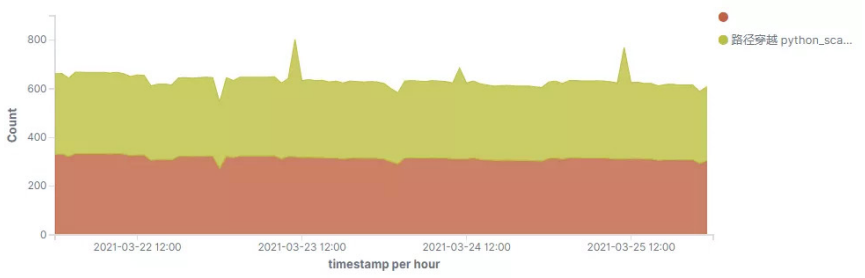


图2 10.200.10.##对192.168.255.##的告警数量和类型统计

```
GET /saas/getTime HTTP/1.0
Host: 192.168.255.##
Connection: close
Accept-Encoding: gzip, deflate
Accept: */*
User-Agent: python-requests/2.20.1
```

图3 10.200.10.###对192.168.255.##的告警载荷样例

经由以上3点，我们基本可以确定10.200.10.##与192.168.255.##之间的告警由正常业务触发。

将上述规律编写相应代码对告警进行过滤，可以发现70%~80%左右的告警符合以上规律，可以作为正常告警滤除。由于数据集为红蓝对抗期间的数据，所有攻击行为对应的告警我们都有真实标签，经验证，滤除的正常告警中不包含攻击告警，这也进一步佐证了我们发现的规律的适用性。

示例二

虽然大部分正常告警能被示例一中的规律所捕获，但是依然有大量告警不满足上述规律，在此，我们举一个与示例一差别较大的例子，如图4所示，10.8.##.203 与 10.51.##.60 之间在每天6:30左右会触发大约1000条左右的路径穿越类告警，根据其payload内容（图5）可知，目标为获取某恶意样本的分析报告，因此不难得出结论：该告警由定时爬虫获取恶意样本的分析报告触发。为了过滤类似告警，我们可以总结出如下规律：

1. 告警类型单一、呈突发性、数量较大。由于一般正常服务器仅提供较

为单一的服务，因此正常流量触发的告警类型一般较为单一，而定时任务一般就呈现突发性的特点；

2. 告警触发时间固定。定时任务一般在特定时间触发；

3. 告警呈现出集群特性。在该例子中，源IP “10.8.##.203”不仅向目的IP“10.51.##.60” 发起了突发请求，还在6:30附近向同网段内的IP“10.51.##.79”发送了大量 Post 请求，上传了大量数据，同时，同网段内的 IP“10.8.##.202”也表现出与源IP “10.8.##.203”类似的通信行为。

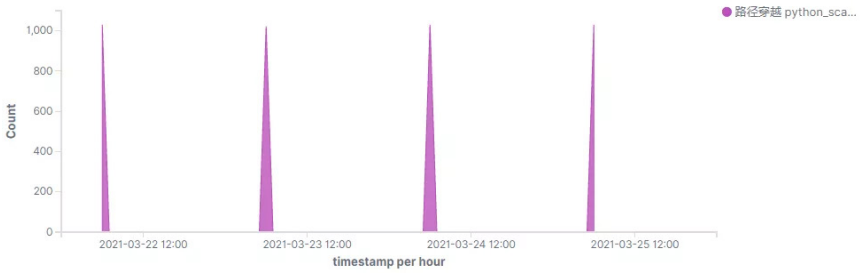


图4　10.8.56.203与10.51.10.60之间的告警数量和类型统计

```
GET
/dashboard/detux/report/b40fbf9437998bc6e58a859f024e166c662967406a
0400183a5ff1580e5934ed/HTTP/1.1
Host: 10.51.##.60:8089
User-Agent: python-requests/2.23.0
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive
```

图5　10.8.56.203与10.51.10.60 的告警载荷样例

经由以上3点，我们基本可以断定 10.8.##.203、10.8.##.202 与10.51.##.60、10.51.##.79之间的路径穿越类告警为正常告警，为了找出符合上述模式的告警集合，可以先采用极值理论（ExtremeValue Theory）找出所有符合突发性特征的告警集合，然后通过查看周期性、通过聚类查看集群特性的方法，找出所有符合上述通信模式的告警集合。通过编写代码，我们发现内网中有大量告警呈现出类似的模式，其中并不包含任何已知的攻击告警。

需要特别注意的是，攻击者的攻击行为往往也呈现出突发性的特点，因此我们需要利用周期性、告警数量、集群特性等特征将攻击告警排除在外。

由于正常告警的模式颇多，我们不在此枚举，总之，在我们的数据中，至少有90%的告警是由正常流量所触发的。

三、灰色流量过滤

在这里，我们将“展现出一定的攻击性，但是与攻击方无关的告警”称为灰色告警，灰色告警一般包含如下类型：1.外部的僵尸网络、蠕虫等发起的攻击行为，2. 内部测试人员对外部服务器的测试行为，3.企业内部测试行为。

对于第一类攻击行为，僵尸网络和蠕虫在网络通信模式中呈现出一定的差异，僵尸网络一般会在短时间发送多个数据包，分别进行不同漏洞的探测，且攻击目标范围较小，如图6所示，122.70.128.168在1分钟之内向10.18.250.###发起了“Apache php文件后缀解析漏洞，PHPUnit 远程代码执行漏洞(CVE-2017-9841)，

PHP代码执行漏洞，ThinkPHP framework 任意代码执行漏洞”等10几种漏洞的相关探测行为，且在安全设备的监控范围内，122.70.128.168仅仅只攻击了10.18.250.###一台服务器。与僵尸网络不同，蠕虫往往只利用少量漏洞，但是攻击范围较广，在告警中表现为同一源IP向大量不同目的IP触发大量相同类型的告警，且这些告警内容和时间上都比较相似。

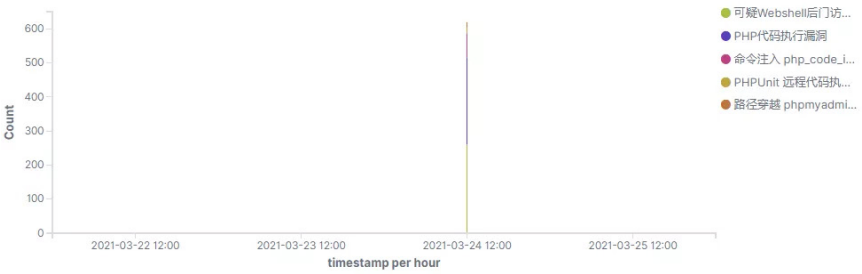


图6　122.70.128.168向10.18.250.###发起漏洞扫描

上述行为虽然都属于漏洞扫描，但是僵尸网络倾向于“深度优先搜索”的方式，蠕虫倾向于“广度优先搜索”的方式，对于僵尸网络触发的告警，可以以源IP为单位进行告警聚合，统计告警类型数量、告警之间的时间差进行过滤，对于蠕虫触发的告警，可以以源IP为单位进行聚合，统计目的IP的数量、告警类型数量、告警之间的时间差进行过滤。编写相关代码后进行过滤发现，每天可以新增几十个IP用于补充威胁情报。

对于第二类和第三类的攻击行为，检测方法与第一类类似，只是在网络流量的流向上有所不同，第二类为“内到外”的流量，第三类为“内到内”的流量。其中第三类攻击行为需要立刻进行排查，判定是内部人员正常测试还是攻击队的内部扫描行为。

灰色流量触发的告警虽然仅占总告警量的5%左右，但是告警总量依然庞大，尤其是第三种攻击行为更需要引起重视，对于企业内部正常漏洞测试行为要做到及时备案。

总结

本文介绍了对海量告警进行过滤的方法，依据不同告警的特点设计不同的过滤方法，这些过滤方法具有一定的普适性。经过一系列过滤步骤，红蓝对抗期间平均每天1000万的告警数据量，可以最后被压缩到每天5万以内，而攻击告警全部包含其中，告警压缩比例达到99%以上，这些过滤步骤可以作为各种分析引擎的前置模块，不仅能够减轻分析引擎的压力，更可以尽可能的减少误报，优化告警分析引擎的整体效果。

【安全告警分析之道：三】异常处理篇

绿盟科技 天枢实验室

一、引言

“攻击是异常，异常不一定是攻击”，安全领域大部分的误报都可以用这句话来解释，这也是安全领域异常检测、UEBA等方法无法完全落地的重要原因，随着互联网用户网络行为的复杂化，企业业务、架构的快速更迭，海量的异常行为对于真实攻击的检测造成了巨大干扰。本期文章我们将浅析这些异常，并以内网横向移动为例，介绍一种处理这些异常找到真实攻击的方法。二、异常的构成

2.1 统计数据

在企业内部网络中，业务复杂、用户行为复杂，这些复杂的网络活动造成大量所谓的“异常”事件，其实何为“异常”在安全领域往往很难界定，异常事件的定义往往随场景、业务甚至人的理解而发生变化，在此，我们不对“异常”的定义做深究，仅以最直观的方式来理解异常：偏离正常活动的事件为异常事件。换句话说，UEBA等异常检测算法算出的结果我们都认为是异常。告警、异常、攻击三者之间的关系如图1所示，在安全设备的海量告警数据当中，大量误报混杂其中，去除这些误报，还有小比例的异常告警，而极小比例攻击就混在这些异常告警当中。

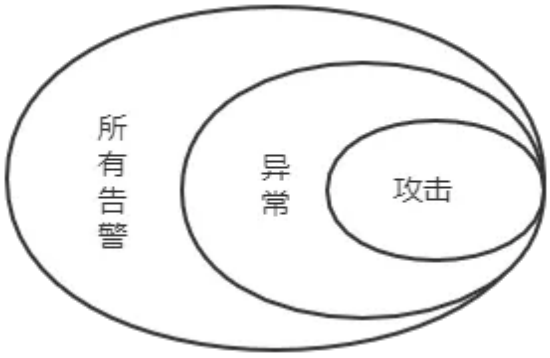


图1 告警、异常、攻击的关系

我们以安全告警数据来做进一步阐述，在系列文章第一篇《安全告警数据分析之道：一】数据透视篇》中,我们依据安全运营中告警的严重程度，将告警分为如下6类（比原文中扩充了2类）：

- 0：无法分类的告警;一般包含：加密流量；代理触发的告警；一些不常见的访问等等
- 1：正常告警 ;一般包含：正常业务触发的误报、用户正常上网行为触发的误报、配置错误触发的告警等；
- 2：忽略类告警;即威胁性不大，无需处理的告警，一般包含：无用告警（基本无可用信息），重复告警（一个数据包触发多个相同的

告警），内部向外的漏洞测试行为，内部常规的扫描行为等；

- 3：低危告警;外部对内部的常规攻击行为，一般由蠕虫、僵尸网络触发，不会造成实际危害；可以用于生成威胁情报，做简单的IP封禁操作；
- 4：灰色行为;一般包含：未经授权的内部攻击行为，异常登录行为。需要立即人工排查，确认攻击者的意图；
- 5：高危告警;正在发生或者已经发生的入侵行为触发的告警。

为了获取以上6类告警具体的分布情况，安全专家对某次红蓝对抗数据的进行了长期标注，得到了一份较为完备的数据集，该数据集包含红蓝对抗期间总计4000万以上的告警数据，其中99.7%以上的数据已经被标注，上述6类告警的分布如图2所示，其中横坐标为日期，纵坐标为告警数量（由于差异过大，以对数方式呈现），0~5类标签总数量比例分别为：2.6240%，89.3536%，5.9829%，0.4102%，1.5410%，0.0883%。

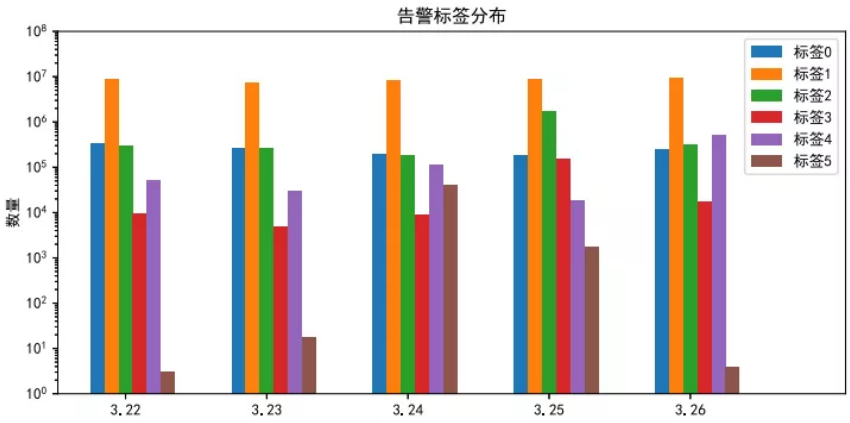


图2　红蓝对抗数据告警标签分布

对应以上数据和之前我们对异常的理解（偏离正常活动的事件为异常事件），标签1以外的告警均为异常告警，如果去除标签0这些无法分类的告警，异常告警的总数占总告警数量为8%左右，从绝对数量看，异常告警的数量在5天内超过400万条，已远超人力所能处理的范围。在日常安全运营过程中，我们需要进一步处理这些异常告警， 找到真正由攻击者攻击触发的告警。

2.2 异常的类型

正常的流量总是相似的，异常流量却各有各的不同，本小节的目标并不是遍

历所有的异常行为，而是总结出几类在日常安全运营过程当中常见的异常行为类型，具体如下（按照告警数量的多少粗略排序）：

- 突发的大量的登录行为。表现为sip、dip之间在短时间内表现出大量的登录行为（如5min内100次），而一段时间（如前后5天）内无任何网络通信。这种行为很常见且不好甄别，由于目前数据的采集方式是旁路采集，很多类型的登录行为无法得知登录所采用的用户名，如短时间内大量的ssh登录行为，无法判断是ssh爆破还是程序的配置错误原因导致的，该问题需要部署终端采集设备进行解决；
- 内部的渗透测试。表现为内网间突发的漏洞探测、扫描行为，其他时间内可能存在网络连接（终端），也可能没有（服务器），这种行为与真正的攻击仅一线之隔，几乎都要进行人工排查，这也体现出内部测试行为备案的必要性。
- 僵木蠕攻击行为。表现为各种类型的扫描探测行为，且持续时间较短，一段时间内不会重复出现；
- 内对外的攻击行为。公司内部员工对其他网络进行渗透测试；
- 少量但异常的登录行为。如sip不在常规列表内的登录行为，远程控制软件在非常规时间内（如半夜）的登录行为，这些告警虽然量少，但是其中确有真实攻击者触发的案例；
- 攻击者触发的告警。这类告警通常更加异常，表现为：发生时间异常，访问的目的IP异常（有时候会伴随着扫描行为），源IP异常（不常见设备的登录、探测行为等），告警类型异常（攻击者触发的告警往往在长尾分布的末端，详见系列文章数据透视篇介绍）等等，虽然异常特性更多，但是混在大量异常告警中，依然难以分辨。

2.3 异常检测

网络流量异常检测已经发展20多年，工业界所说的UEBA其实也是异常检测，这些异常检测算法大都通过对某些特征的统计分析，再配合一些智能算法对异常加以识别，如Kitsune[2]利用多层AutoEncoder对网络流量进行异常检测，Donut[3]利用变分自编码器对KPI数据进行异常检测，AlertRank [4]通过机器学习的方法对运维告警进行异常检测等等，这些方法虽然在各自领域可以有效检测异常，但是在安全领域，面对海量异常但良性的告警，依然无法解决问题。在安全领域的某些场景中，由于异常并不一定是攻击，因此在传统异常检测的基础之上还需要对这些异常做进一步处理。

三、异常的处理

本小节介绍一篇发表于Usexix Security2021的论文[1]，该论文以内网横向移动为场景，对攻击者的登录路径进行检测。论文以Dropbox公司的真实数据进行验证，在时间跨度长达15个月的登录记录中，对300个多个真实攻击场景的检出率达到94.5%，平均每天的误报小于9个，检测效果和误报数量均已达到日常运营的需求；该论文提出Hopper检测系统，使用统计+结构的方式寻找异常登录记录，能够有效过滤海量异常但无害告警。

3.1 数据集

收集了Dropbox公司2019.1.1到2020.4.1共15个月的登录成功的登录记录，共计7.8亿条。每条记录包含：（1）时间戳，（2）登录用户名（3）登录记录的源和目的机器（4）源和目的机器的相关信息，这些记录共涉及634个账户，2327台机器。

数据集中包含327个攻击场景，包含一个由Dropbox公司红队模拟的APT场景和326个自行模拟的横向移动场景。

3.2 方法

3.2.1 过滤

为了最大限度消除误报，论文对登录记录进行了清洗，过滤了以下2种类型的记录：（1）Window相关登录。Window系统很容易触发登录记录，而这登录记录并不是真正能造成远控的”登录”,不能让用户获取数据或者控制目标机器。过滤这些数据能将总数据量缩减40倍以上。（2）自动登录类。文中采取3种简单规则过滤自动登录类记录，在此不赘述。

通过以上过滤方法，最终登录记录被缩减为352万条，为原始数量的1/222.

3.2.2 系统结构

Hopper的系统结构图如图3所示，主要由两部分构成，过滤后的数据首先会经过一个关联引擎，关联引擎将所有的登录记录进行构图处理（按天进行处理），以利用登录记录之间的结构信息，并且识别路径的边界（防止出现环路）,推理出登录路径的属性，第二部分（告警生成器）通过挖掘路径的特性，对每条路径打分并生成告警。

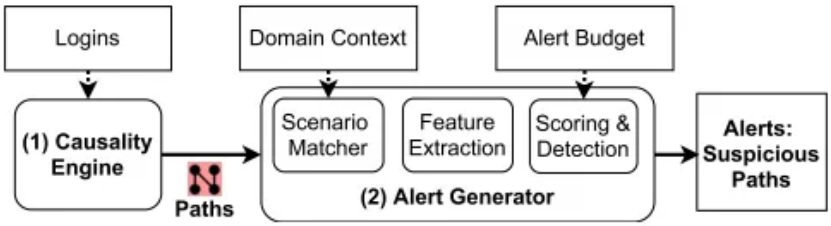


图3 Hopper系统结构图

3.2.3 关联引擎

该部分首先将所有能关联的记录关联起来，构成一条条登录路径，这些路径包含如图4所示的属性：（1）包含的登录记录（2）路径起始点机器的所有人（3）用户名发生变化的记录（4）路径类型。其中路径类型包括BENIGN, CLEAR, UNCLEAR，3种，BENIGN路径代表：路径中的用户名未发生过变化，CLEAR路径和UNCLEAR路径中用户名都发生过变化，只不过CLEAR路径表示下一跳路径不再使用前一跳的用户名，UNCLEAR路径却接着使用。

Path Component	Description
Login List	List of logins in the path
Causal User	Username of the employee whose machine initiated the path
Changepoint Logins	A list of logins where the username differs from the path's preceding login
Path Type	BENIGN, CLEAR, or UNCLEAR: whether the path switches to new credentials

图4　关联引擎生成的路径的属性

3.2.4 告警生成器

除了上一小节中的路径信息，告警生成器还需要两个外部输入：（1）历史登录信息，用于特征提取（2）人为设定的阈值，控制UNCLEAR路径的数量。告警生成器整体流程如图5所示，首先进行场景匹配，文章定义了5种良性路径的场景，如BENIGN路径属于良性路径的一种，其他4中良性路径读者可自行阅读原文，若能匹配上这5种良性路径，则不生成告警，若未匹配上，则需要对路径进行进一步划分，分为两种攻击场景：有明显凭证切换，无明显凭证切换。

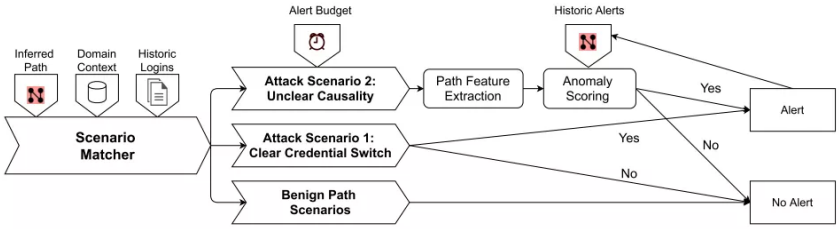


图5　告警生成器流程

对于第一种攻击场景：有明显凭证切换，这种场景中，只有路径满足以下条件则进行告警：（1）路径类型为CLEAR类型（2）路径中包含其中用户从未登录过的机器对于第二种攻击场景，该场景较为复杂，文本在此仅介绍核心思想，详细步骤请读者自行阅读原文，这种场景应对多条关联的路径中，有些路径有用户切换，有些路径没有用户切换的情况，如图6所示，图中存在（L1，L4），（L2，L4），（L3，L4）3条路径，这3条路径因为机器Y关联在一起，由于（L1，L4），（L3，L4）存在用户切换，（L2，L4）不存在用户切换，因此

（L1，L4），（L3，L4）属于UNCLEAR路径，而（L2，L4）属于BENIGN路径。论文利用历史数据提取UNCLEAR路径的3个特征，这3个特征刻画了该路径的稀有性，利用这3个特征对路径打出可疑值评分，对可疑值高的路径进行告警。

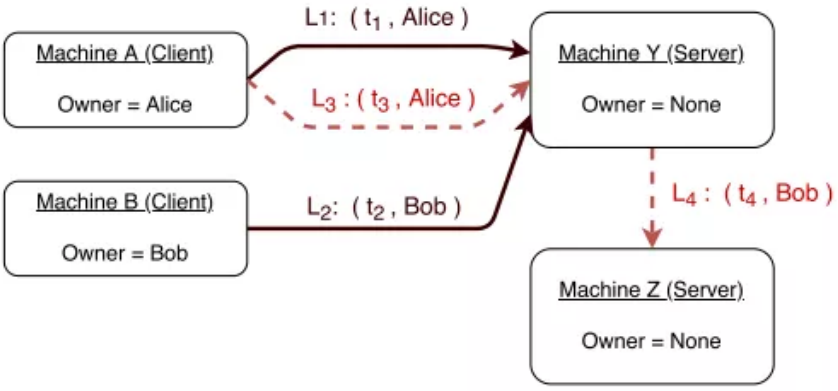


图6　登录样例

3.3 小结

论文基于对数据的了解，提出一种能够缩减原始数据量200倍以上的过滤方法，并且基于对横向移动攻击特征的理解，提出横向移动的两个特性：（1）用户凭证切换（2）原始用户无权接触目标机器，将登陆记录构图，提取结构化特征（3种攻击路径），并且利用历史数据计算统计特征，最终达到满足安全运营需求的效果。该论文虽然是一篇数据分析类论文，但是并未使用任何复杂的算法，作者将专家知识（对攻击的理解和对数据的理解）融入算法中，达到了远超其他所谓机器学习算法的效果。四、总结

本文以安全告警数据为例，分析了异常告警的分布情况和组成类型，并且通过分享一篇顶会论文，探索对于海量异常但无害告警的处理方法，从方法论看，传统异常检测的方法不能直接作用于安全运营，可结合告警之间的结构信息对告警进行进一步筛选，以达到安全运营的需求，从理念上看，攻击检测效果的提升本质上还是基于对攻击行为和数据的深刻理解，对检测场景要尽量细化，这样才能对症下药。

以上观点仅代表作者本人观点，欢迎各位读者批评指正。

参考文献

1. Ho, Grant, et al. "Hopper: Modelingand Detecting Lateral Movement." arXiv preprint arXiv:2105.13442 (2021).

2. Mirsky, Yisroel, et al. "Kitsune:an ensemble of autoencoders for online network intrusion detection." arXivpreprint arXiv:1802.09089 (2018).

3. Xu, Haowen, et al. "Unsupervised anomaly detection via variational auto-encoder for seasonal kpis in webapplications." Proceedings of the 2018 World Wide Web Conference. 2018.

4. Zhao, Nengwen, et al. "Automaticallyand Adaptively Identifying Severe Alerts for Online Service Systems." IEEEINFOCOM 2020-IEEE Conference on Computer Communications. IEEE, 2020.

两程序员制作证券软件外挂：可侵入 84 家证券公司交易系统

摘要：两名程序员通过销售通达信平台的 API 接口并提供后续服务，共发展客户1240名，收取销售服务费超902万元，共计非法获利超583万元。

关键词：标签（金融保险、“通信达”外挂、公检法），技术问题（安全事件）。

内容：10月 8日，由中国检察网获悉，两名程序员因销售“通达信”API 接口被抓。起诉书显示，该 API接口名为“TradeX”，可侵入由财富趋势承建、维护的84家证券公司交易系统。

自2017年3月29日起，两名程序员通过销售通达信平台的 API 接口并提供后续服务，共发展客户1240名，收取销售服务费超902万元，共计非法获利超583万元。

据悉，通达信为国内知名证券行情软件，由财富趋势设计开发。公开信息显示，财富趋势于2020年 4月 27日在科创板上市，主营业务为面向证券公司等金融机构客户提供安全、稳定、可靠的金融软件解决方案,为其建设投资者行情交易终端、终端用户信息系统以及客户服务系统等，同时为终端投资者客户提供专业、高效的证券信息服务。

上海市普陀区人民检察院在起诉书中表示，经依法审查查明，2017年3月至2020年 12月，两名程序员宋某1、宋某 2为牟取非法利益，由宋某1负责对深圳**科技股份有限公司为证券公司开发的“通达信”软件客户端中的通讯、控制模块进行脱壳、篡改，剥离其中静态防御措施后，使用其自行开发的外挂主程序接管控制与通讯模块， 重新搭建对外接口，使其得以调用“通达信”软件客户端通讯模块功能，后再通过镜像欺骗以及篡改等手段破坏动态反外挂模组，并将上述程序代码封装成可以通过证券公司交易系统安全检测的“TradeX”交易接口，侵入由财富趋势承建、维护的 84 家证券公司交易系统。

并由宋某 2负责编写接口使用说明、开通接口授权文件及绑定证券账户，

通过互联网对外向上海*甲科技有限公司（以下简称“上海**公司）及个人出售“TradeX” 交易接口。

经司法鉴定，“TradeX”具备自动化登陆证券账号、查询证券账号信息、证券账号持仓数据、进行证券交易的功能。经司法审计鉴定，宋某1、宋某 2通过销售通达信平台的 API接口并提供后续服务，共发展客户1240名，收取销售服务费人民币902万余元。

截至目前，宋某1和宋某 2共计非法获利583万余元，其中宋某1获利 411万余元，宋某 2获利 171万余元。2020年 12月 30日，二人分别被公安机关抓获，到案后均如实供述自己的罪行。

基于以上事实，上海市普陀区人民检察院认为，宋某1、宋某 2对外出售“Trade X”交易接口牟利，情节特别严重，已触犯刑法，应当以提供侵入计算机信息系统程序罪追究其刑事责任。

但考虑到二人自愿认罪认罚、如实供述自己的罪行，可从宽处理、从轻处罚。且宋某 1 起主要作用，系主犯，宋某 2起次要作用，系从犯，根据相关法律规定，应当对宋某 2从轻或减轻处罚。

最终，上海市普陀区人民检察院提起公诉，建议对宋某1判处有期徒刑四年，并处罚金；对宋某2 处有期徒刑二年六个月，并处罚金。

信息来源：

https://www.secrss.com/articles/34962

Firefox 插件“Safepal 钱包”窃取加密货币

摘要：一个名为“Safepal Wallet”的恶意 Firefox 插件，欺骗用户，窃取钱包余额，并在 Mozilla 插件网站上存在了 7 个月才被发现。

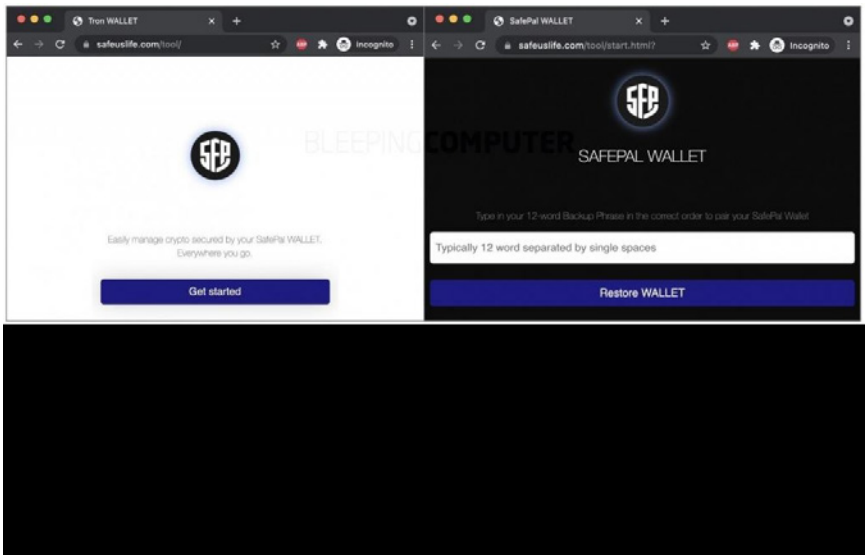
关键词：标签（恶意软件、加密货币、Mozilla、Safepal Wallet），技术问题（安全事件）。

内容：尽管恶意的浏览器插件已经被关闭，BleepingComputer 发现威胁者建立的钓鱼网站仍在运行。

一位名为 Cali 的 Mozilla 插件用户解释说:“今天我浏览了 Mozilla Firefox 的插件列表，我正在搜索 Safepal 钱包扩展，以便在 web 浏览器中我也可以使用加密货币钱包。”

在使用 Safepal 证书安装并登录该插件数小时后，Cali 发现自己的钱包余额清空了。

“我深深地震惊了……我看到了我最后的交易记录，发现我的 4000 美元资金被转移到了另一个钱包。我不敢相信这是一个在 Mozilla Firefox 插件列表中的插件，” 他在 Mozilla 的论坛中说道。



BleepingComputer 从“Safepal 钱包”的附加页面发现，该插件至少从 2021年 2 月 16 日起就开始使用了。

页面上，这个 235kb 的插件吹嘘自己是一个 Safepal 应用程序，可以安全地“在本地保存私钥”，还有令人信服的产品图片和营销材料。

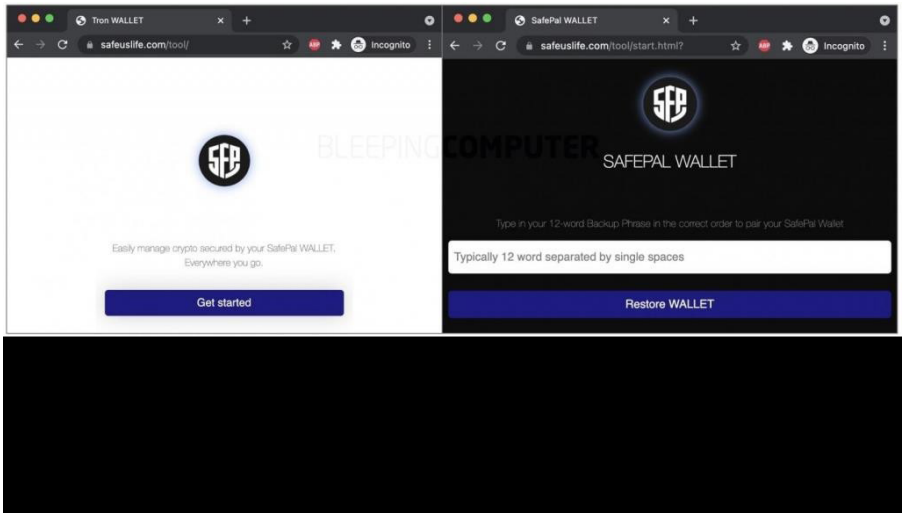
为了在 Mozilla 网站上发布插件，开发者必须遵循提交流程，即提交的插件“随时接受 Mozilla 的审查”。但是，目前还不清楚提交的文件的安全程度。

Cali 本月公开报道此事不到五天，Mozilla 的发言人回应说，他们正在进行调查。该插件的介绍页面已被 Mozilla 删除。

虽然 Safepal 在苹果应用商店和谷歌 Play 上都有官方智能手机应用，但我们并不知道是否有官方的“Safepal”浏览器扩展

幸运的是，在 Mozilla 插件网站上，一些用户发布了一星评论，警告其他

人不要下载“Safepal Wallet”。



但是，对于Cali来说，一切为时已晚，收回资金的机会很渺茫。

“我已经和警察谈过了，他们对此无能为力。他们告诉我无法追踪到黑客。”Cali 说。

BleepingComputer 联系 Mozilla 了解更多关于这个问题的信息:

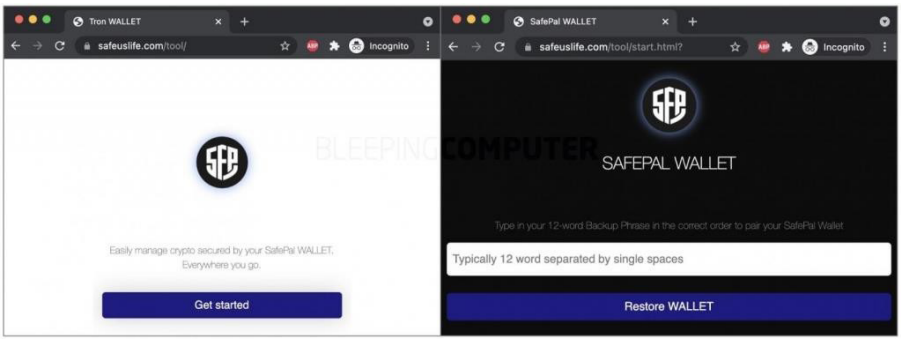
Mozilla 的一位发言人告诉 BleepingComputer :“扩展安全对 Mozilla 来说很重要，我们的生态系统持续对千变万化的威胁做出回应。”

“我们目前的重点是减少恶意扩展可能造成的损害，引导用户使用我们审查和监控的推荐扩展，帮助用户了解安装扩展带来的风险，让用户更容易地向我们反馈潜在的恶意扩展。”

“根据我们的插件政策，当我们发现到插件会对安全和隐私造成威胁时，我们会采取措施阻止它们在 Firefox 中运行。关于这个插件，我们采取行动阻止其运行并从Firefox 插件商店中删除了它。”

在调查恶意的火狐插件时，BleepingComputer 发现了插件使用的钓鱼域。如下所示的这个网页，在假插件的主页也被列为“支持网站”:https://safeuslife.com/tool/

WHOIS 记录显示，该钓鱼网站是在今年 1 月通过 Namecheap 注册的。在写这篇文章的时候，这个网页仍然在运营，它指示受害者输入他们的“12 个单词的备份短语，用于匹配 SafePal 钱包。”



但是，一旦输入了备份短语并提交了表单，页面就会刷新，但没有任何明显的响应，备份短语却已悄无声息地发送给攻击者。

加密货币钱包和许多在线服务一样，如果用户忘记密码，由 12 个随机生成的单词组成的备份短语便可以用来恢复用户的私钥和钱包。但是，备份短语十分重要且私密，只能在特殊情况下使用，而且只能在服务提供商可信的应用程序或网站上使用。

备份短语如果被盗，攻击者可以控制你的钱包，以及访问和转移资金。

最近，加密货币诈骗正在增多，威胁者正在寻找更新的、难以检测的方法来欺骗用户。就在上周，有人入侵了 Bitcoin.org 官方网站，成功地骗走了 1.7 万美元。[详细请点击]

在之前的攻击中，包括 npm、PyPI 和 GitHub 在内的开源库被滥用，用以传播加密窃取和加密挖掘恶意软件。

随着网络平台上威胁者的日益增多，用户在提供安全密码或在线转移加密货币时应谨慎。

BleepingComputer 已经联系了 Mozilla 和 Safepal 寻求进一步的回应，同时向 Namecheap 报告了钓鱼域名。

信息来源：

https://hackernews.cc/archives/36240

厄瓜多尔最大私营银行遭遇网络攻击，业务被迫中断

摘要：此次攻击导致该银行业务大面积中断。

关键词：标签（金融保险、网络攻击），技术问题（安全事件）。

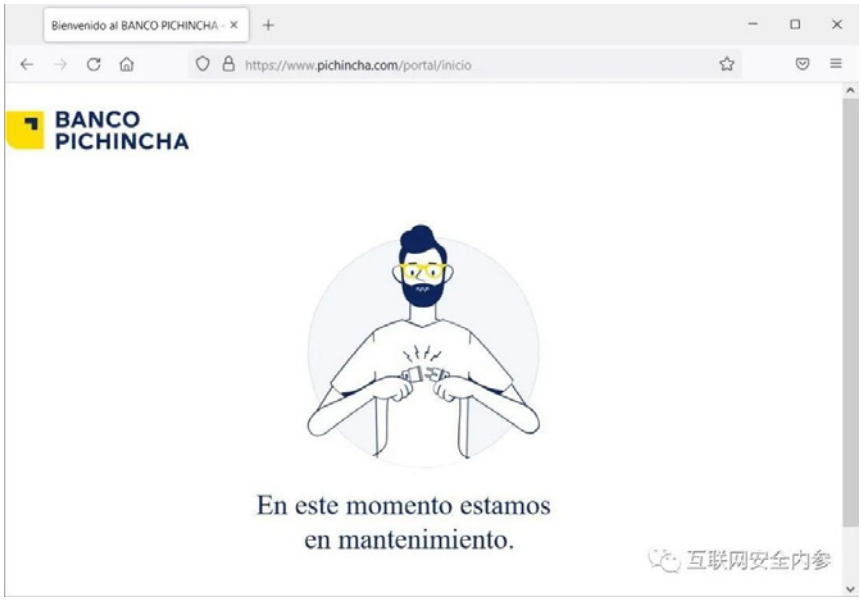
内容：上周末，因遭遇网络攻击，厄瓜多尔最大私营银行皮钦查银行关闭了部分网络和系统，业务被迫中断；

- 此次攻击导致该银行业务大面积中断，ATM 机、网上银行、移动客户端、数字渠道和自助服务、电子邮件均无法运行；
- 有消息人士称，这是一起勒索软件攻击，攻击者还在该银行网络上安装了Cobalt Strike 信标。

南美洲国家厄瓜多尔最大的私营银行皮钦查银行（Banco Pichincha）遭遇网络攻击，业务系统应声宕机，ATM 与在线银行门户网站也被迫下线。

此次攻击发生在上周末，银行被迫关闭了部分网络，以防止攻击蔓延至其他系统。

系统宕机导致该银行业务大面积中断，ATM 机无法继续运行，网上银行门户也弹出维护信息。

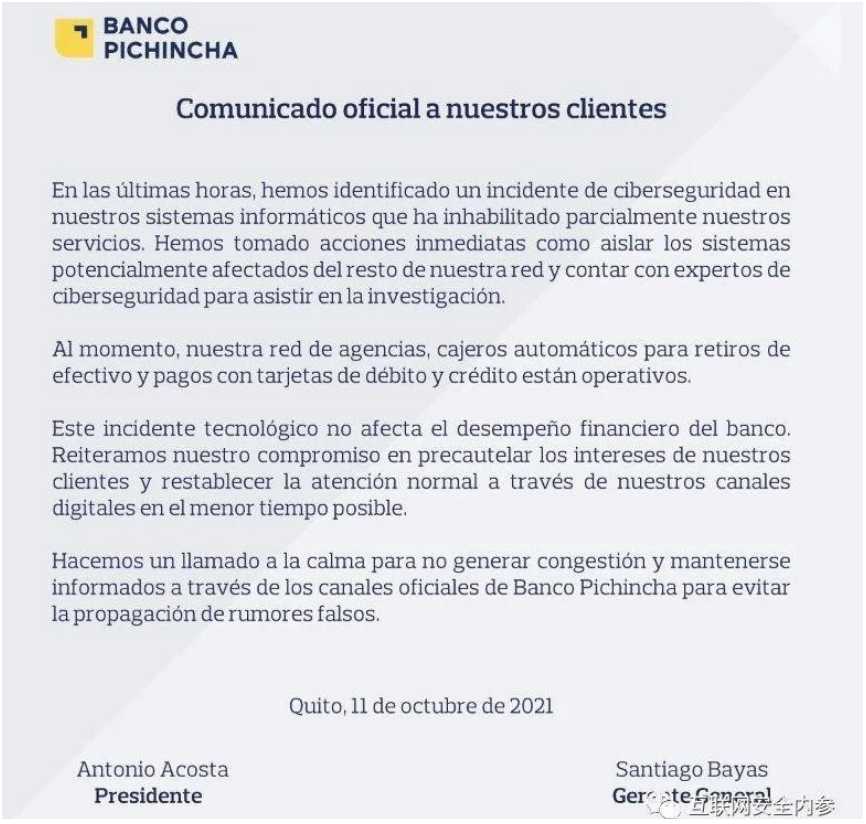


皮钦查银行网站显示的维护消息

据该银行的内部通知显示，皮钦查银行通知员工，银行应用、电子邮件、数字渠道与自助服务受技术问题影响而无法正常运行。

这份内部文件还说，建议各级员工将自助服务客户引导至柜员窗口，确保宕机期间继续为客户提供服务。

在对具体技术细节保持沉默了两天之后，皮钦查银行周二（10 月 12 日）下午终于发表声明，承认系统宕机是因为网络攻击。



皮钦查银行发布的声明

从翻译后的声明中看到以下内容：

过去几个小时当中，我们在内部计算机系统中发现一起网络安全事件，并导致部分服务陷入瘫痪。我们已经立即采取行动，包括将可能被其他网络部分影响的系统隔离起来，并邀请网络安全专家协助开展调查。

目前，我们的代理网络、用于取款及使用借记卡/信用卡付款的 ATM 机已经在正常运行。

此次技术事件并未影响到银行的财务业绩。在这里，我们要重申皮钦查银行致力于维护客户利益、并在最短时间内通过数字渠道恢复正常运营的态度。

我们呼吁大家保持冷静、避免造成拥堵，并通过皮钦查银行的官方渠道随时了解事态进展，避免虚假谣言的传播。 ——皮钦查银行

今天，ATM 机已经恢复使用，网上银行门户仍然显示维护消息，但客户已经能够正常访问自己的在线账户。遗憾的是，移动端应用仍没能从攻击中恢复过来。

可能属于勒索软件攻击

目前，皮钦查银行还未披露此次攻击的性质，但有网络安全行业的消息人士向媒体透露，称 这是一起勒索软件攻击。攻击者还在该银行网络上安装了 Cobalt Strike 信标。

一般来说，勒索软件团队及其他威胁行为者往往会使用 Cobalt Strike 维持对目标网络的持久驻留权，并借此访问网络中的其他系统。

今年 2 月，皮钦查银行曾遭遇 Hotarus Corp 网络犯罪团伙的攻击，对方表示成功从银行网络中窃取到了文件。

皮钦查银行对此进行了否认，并表示遭到入侵的只是他们一家供应商。

该银行当时表示，“我们知晓有人未经授权访问了为 Pichincha Miles 项目提供营销服务的供应商系统。”

“关于此次信息泄露，根据广泛调查，我们没有发现自身银行系统遭到破坏或访问的证据。因此，我们客户的财务资源安全性并没有受到损害。”

我们已经就此事联系了皮钦查银行，并将在收到回复后第一时间带来后续报道。

信息来源：

https://www.secrss.com/articles/35108

FIN7 利用 Windows 11 的发布进行攻击

摘要：这个著名的黑客团体希望从加州的一个销售点服务提供商那里窃取支付卡数据。

关键词：标签（FIN7、服务提供商、数据泄露），技术问题（安全事件）。

内容：FIN7 这个金融网络犯罪团伙又回来了，他们利用以新版本的Windows 为主题的Word 文档进行攻击，其中还附加了恶意的 javascript 脚本。

安全人员观察到该团伙在最近的一次攻击活动中，利用了六个不同的文件，都提到了 Windows 11 Alph 这个微软即将推出的Windows 11 操作系统的内部预览版本。

6 月下旬，Windows 11 Alpha 被发布到了该计算机巨头的开发者渠道中，它在技术人员中引起了很大的轰动，因为它提供了 Windows11 预览版。同时，官方在今年秋季才会正式推出Windows 11 正式版。

FIN7 的攻击者们希望利用这一点，通过电子邮件将该主题的文件提供给位于加州的销售点供应商 Clearmind 以及其他目标，所有的这些文件都带有恶意的 Visual Basic（VBA）宏。

FIN7 的最新攻击布局

感染链是从一个带有诱惑性图像的微软Word 文档开始的，它告诉读者它是用Windows 11 Alpha 制作的，该图片中的内容要求用户启用编辑以查看更多内容。

一旦编辑被启用，就会执行一个 VBA 宏，从.doc 文件内的一个隐藏表格中获取编码值，并用一个 XOR 键对其进行解密。同时将创建一个脚本，对目标进行各种信息的检查。

它首先检查目标系统的语言，如果发现是俄语、乌克兰语或其他任何的东欧语言， 脚本将终止运行。

该脚本还会检查是否存在虚拟机，以确保它没有在沙盒环境中被运行分析，如果发现了，将终止文件的运行。然后，它会查看目标是否在销售点（PoS）服务提供商的域名 clearmind.com 上。如果是，它将继续进行检查。

Clearmind 域名这个攻击目标很符合 FIN7 的操作方式。作为一家位于加州的零售和酒店业 PoS 技术供应商，如果感染成功了，那么该集团将会获得大量的支付卡数据，随后在地下市场上出售这些信息。

研究人员指出，如果这个检查结果符合攻击条件，该脚本会将一个名为 "word_data.js "的 JavaScript 文件丢入 TEMP 文件夹，该文件一旦被解析运行，它就会变成 FIN7 的 JavaScript 后门，该组织自 2018 年以来就一直在采用该技术。从那里，FIN7 就可以进一步渗透到受害者的机器中，窃取数据并进行网络侦察，然后进行横向移动。

FIN7 的攻击没有放缓的迹象

FIN7（又名 Carbanak Group 或 Navigator Group）是一个著名的威胁攻击组织， 至少从 2015 年开始就一直在作案。该团伙通常会使用带有恶意软件的网络钓鱼文件攻击受害者，然后渗透到系统中，窃取银行卡数据并进行出售。该团伙一直在调整新的恶意软件库，它同时还针对休闲餐厅、赌场和酒店的 PoS 系统进行攻击。自 2020 年以来，该团伙还增加了勒索软件和数据泄露攻击，利用 ZoomInfo 服务来根据收入情况选择目标进行攻击。

目前该集团已经引起了美国司法部的注意，美国司法部认为 FIN7 窃取了超过1500 万条支付卡记录，造成了超过 10 亿美元的损失。据司法部称，仅在美国，该组织就破坏了 47 个州和哥伦比亚特区的组织网络，司法部在 6 月以盗窃支付卡的罪名判处一名攻击者 7 年监禁和 250 万美元罚款，其他人员的逮捕和定罪同样也在困扰着政府。

然而，严格的法律并没有使该组织停止攻击。一个月后，它又回来了，以涉及杰克-丹尼尔斯威士忌的酒业公司的法律投诉为诱饵，成功地攻击了多家律师事务所。

FIN7 是最臭名昭著的网络金融犯罪组织之一，因为他们通过众多技术和攻击面窃取了大量的敏感数据。尽管政府在全力的逮捕和判刑，包括所谓的更高级别的成员， 目前该集团仍然像以前一样活跃。美国检察官认为该集团人数约为 70 人，这意味着该集团很可能会弥补人员上的损失，因为可能会有其他的外部人员加入。

信息来源：

https://www.4hou.com/posts/XqmV

NSFOCUS

漏洞聚焦

Oracle 全系产品 10 月重要补丁更新通告

发布时间：2021-10-20

一、漏洞概述

2021 年 10 月 20 日，绿盟科技监测发现 Oracle 官方发布了 10 月重要补丁更新公告 CP U（Critical Patch Update），此次共修复了 419 个不同程度的漏洞，此次安全更新涉及 Orac le MySQL、Oracle Weblogic Server、Oracle Java SE、Oracle FusionMiddleware、Orac le Retail Applications 等多个常用产品。Oracle 强烈建议客户尽快应用关键补丁更新修复程序，对漏洞进行修复。

参考链接：

https://www.oracle.com/security-alerts/cpuoct2021.html

二、重点漏洞简述

根据产品流行度和漏洞重要性筛选出此次更新中包含影响较大的漏洞，请相关用户重点 进行关注：

Oracle MySQL 多个漏洞：

此次安全更新针对 Oracle MySQL 发布了 66 个安全补丁, 其中的 10 个漏洞在未经用户身份验证的情况下即可远程进行利用，即无需用户凭据即可通过网络利用。漏洞编号如下：

CVE-2021-22931

CVE-2021-3711

CVE-2021-3518

CVE-2021-22926

CVE-2021-36222

CVE-2021-35583

CVE-2021-3712

CVE-2021-33037

CVE-2021-29425

CVE-2021-35613

Oracle Financial Services Applications 多个漏洞：

此次安全更新针对 Oracle Financial Services Applications 发布了 44 个安全补丁。其中的 2 6 个漏洞在未经用户身份验证的情况下即可远程进行利用。高危漏洞编号如下：

CVE-2020-5413

CVE-2020-10683

CVE-2021-21345

Oracle Insurance Applications 多个漏洞：

此次安全更新针对 Oracle Insurance Applications 发布了 16 个安全补丁。其中的 11 个漏洞在未经用户身份验证的情况下即可远程进行利用。攻击者可以通过 HTTP 访问网络发送恶意请求，从而控制产品中的组件进而对关键数据完全访问。严重漏洞编号如下：

CVE-2016-1000031

CVE-2019-13990

CVE-2020-10683

CVE-2019-17195

Oracle Communications 多个漏洞：

此次安全更新针对 Oracle Communications 发布了 71 个安全补丁，其中的 56 个漏洞在未经用户身份验证的情况下即可远程进行利用。高危漏洞编号如下：

CVE-2021-21345

CVE-2021-21783

CVE-2017-9841

CVE-2021-21783

CVE-2021-11998

CVE-2021-17530

CVE-2021-23017

Oracle Fusion Middleware 多个漏洞：

此次安全更新针对 Oracle Fusion Middleware 发布了 38 个安全补丁。其中有 30 个漏洞在未经用户身份验证的情况下即可远程进行利用。高危漏洞编号如下：

CVE-2019-13990

CVE-2018-8088

CVE-2021-35617

Oracle Retail Applications 多个漏洞：

此次安全更新针对 Oracle Retail Applications 发布了 26 个安全补丁。其中有 9 个漏洞在未经用户身份验证的情况下即可远程进行利用。高危漏洞编号如下：

CVE-2021-2351

Oracle 官方 10 月关键补丁更新漏洞总结如下：

产品	漏洞个数	未授权远程利用个数	最高 CVSS 评分
Oracle Database Products Risk Matrices	9	2	8.2
Oracle Database Server	9	2	8.2
Oracle Essbase	5	3	10
Oracle GoldenGate	1	1	6.5
Oracle Graph Server and Client	1	1	7.5
Oracle REST Data Services	1	1	7.5
Oracle Secure Backup	1	1	7.4
Oracle Commerce	2	0	5.4
Oracle Communications Applications	19	14	9.8
Oracle Communications	71	56	9.9
Oracle Construction and Engineering	12	7	9.8
Oracle E-Business Suite	18	4	8.1
Oracle Enterprise Manager	8	5	9.8
Oracle Financial Services Applications	44	26	9.9

产品	漏洞个数	未授权远程利用个数	最高 CVSS 评分
Oracle Fusion Middleware	38	30	9.8
Oracle Health Sciences Applications	6	3	9.8
Oracle Hospitality Applications	1	1	6.1
Oracle Hyperion	6	5	6.1
Oracle Insurance Applications	16	11	9.8
Oracle Java SE	15	13	8.6
Oracle JD Edwards	11	8	7.5
Oracle MySQL	66	10	9.8
Oracle PeopleSoft	17	8	9.1
Oracle Retail Applications	26	9	8.3
Oracle Siebel CRM	6	5	7.5
Oracle Supply Chain	5	3	7.5
Oracle Systems	5	2	9.8
Oracle Utilities Applications	1	0	5.5
Oracle Virtualization	8	1	7.8

三、漏洞防护

请用户参考本文附录“受影响产品及补丁信息”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。

附录：受影响产品及补丁信息

受影响产品及版本号	可用补丁
Enterprise Manager Base Platform, versions 13.4.0.0, 13.5.0.0	https://support.oracle.com/rs?type=doc&id=2796575.1
Enterprise Manager for Oracle Database, version 13.4.0.0	https://support.oracle.com/rs?type=doc&id=2796575.1
Enterprise Manager Ops Center, version 12.4.0.0	https://support.oracle.com/rs?type=doc&id=2796575.1
Essbase Administration Services, versions prior to 11.1.2.4.46	https://support.oracle.com/rs?type=doc&id=2796575.1
Hyperion Financial Management, versions 11.1.2.4, 11.2.6.0	https://support.oracle.com/rs?type=doc&id=2796575.1
Hyperion Financial Reporting, versions 11.1.2.4, 11.2.6.0	https://support.oracle.com/rs?type=doc&id=2796575.1
Hyperion Infrastructure Technology, version 11.2.6.0	https://support.oracle.com/rs?type=doc&id=2796575.1
Hyperion Planning, versions 11.1.2.4, 11.2.6.0	https://support.oracle.com/rs?type=doc&id=2796575.1
Instantis EnterpriseTrack, versions 17.1, 17.2, 17.3	https://support.oracle.com/rs?type=doc&id=2809438.1
JD Edwards EnterpriseOne Orchestrator, versions prior to 9.2.6.0	https://support.oracle.com/rs?type=doc&id=2810363.1
JD Edwards EnterpriseOne Tools, versions prior to 9.2.6.0	https://support.oracle.com/rs?type=doc&id=2810363.1
JD Edwards World Security, version A9.4	https://support.oracle.com/rs?type=doc&id=2810363.1
MySQL Client, versions 8.0.26 and prior	https://support.oracle.com/rs?type=doc&id=2809354.1
MySQL Cluster, versions 7.4.33 and prior, 7.5.23 and prior, 7.6.19 and prior, 8.0.26 and prior	https://support.oracle.com/rs?type=doc&id=2809354.1
MySQL Connectors, versions 8.0.26 and prior	https://support.oracle.com/rs?type=doc&id=2809354.1
MySQL Enterprise Monitor, versions 8.0.25 and prior	https://support.oracle.com/rs?type=doc&id=2809354.1
MySQL Server, versions 5.7.35 and prior, 8.0.26 and prior	https://support.oracle.com/rs?type=doc&id=2809354.1
MySQL Workbench, versions 8.0.26 and prior	https://support.oracle.com/rs?type=doc&id=2809354.1
Oracle Agile PLM, versions 9.3.3, 9.3.6	https://support.oracle.com/rs?type=doc&id=2810378.1
Oracle Application Express, versions prior to 21.1.0	https://support.oracle.com/rs?type=doc&id=2796575.1
Oracle Application Testing Suite, version 13.3.0.1	https://support.oracle.com/rs?type=doc&id=2796575.1
Oracle Autovue for Agile Product Lifecycle Management, version 21.0.2	https://support.oracle.com/rs?type=doc&id=2810378.1

受影响产品及版本号	可用补丁
Oracle Banking Cash Management, versions 14.2, 14.3, 14.5	https://support.oracle.com/
Oracle Banking Corporate Lending Process Management, versions 14.2, 14.3, 14.5	https://support.oracle.com/
Oracle Banking Credit Facilities Process Management, versions 14.2, 14.3, 14.5	https://support.oracle.com/
Oracle Banking Enterprise Default Management, versions 2.10.0, 2.12.0	https://support.oracle.com/rs?type=doc&id=2808888.1
Oracle Banking Extensibility Workbench, versions 14.2, 14.3, 14.5	https://support.oracle.com/
Oracle Banking Platform, versions 2.6.2, 2.7.1, 2.9.0, 2.12.0	https://support.oracle.com/rs?type=doc&id=2808888.1
Oracle Banking Supply Chain Finance, versions 14.2, 14.3, 14.5	https://support.oracle.com/
Oracle Banking Trade Finance Process Management, versions 14.2, 14.3, 14.5	https://support.oracle.com/
Oracle Banking Virtual Account Management, versions 14.2, 14.3, 14.5	https://support.oracle.com/
Oracle Business Activity Monitoring, versions 11.1.1.9.0, 12.2.1.3.0, 12.2.1.4.0	https://support.oracle.com/rs?type=doc&id=2796575.1
Oracle Business Intelligence Enterprise Edition, versions 5.5.0.0.0, 12.2.1.3.0, 12.2.1.4.0	https://support.oracle.com/rs?type=doc&id=2796575.1
Oracle Commerce Guided Search, version 11.3.2	https://support.oracle.com/rs?type=doc&id=2811064.1
Oracle Commerce Merchandising, version 11.3.2	https://support.oracle.com/rs?type=doc&id=2811064.1
Oracle Communications Application Session Controller, version 3.9	https://support.oracle.com/rs?type=doc&id=2815518.1
Oracle Communications Billing and Revenue Management, versions 7.5.0.0.0, 12.0.0.3.0	https://support.oracle.com/rs?type=doc&id=2808815.1
Oracle Communications BRM - Elastic Charging Engine, version 12.0.0.3	https://support.oracle.com/rs?type=doc&id=2808815.1
Oracle Communications Calendar Server, version 8.0.0.6.0	https://support.oracle.com/rs?type=doc&id=2808816.1

受影响产品及版本号	可用补丁
Oracle Communications Cloud Native Core Network Repository Function, version 1.14.0	https://support.oracle.com/rs?type=doc&id=2809116.1
Oracle Communications Cloud Native Core Policy, version 1.11.0	https://support.oracle.com/rs?type=doc&id=2809114.1
Oracle Communications Control Plane Monitor, versions 3.4, 4.2, 4.3, 4.4	https://support.oracle.com/rs?type=doc&id=2809423.1
Oracle Communications Converged Application Server - Service Controller, version 6.2	https://support.oracle.com/rs?type=doc&id=2809113.1
Oracle Communications Design Studio, version 7.4.2	https://support.oracle.com/rs?type=doc&id=2808817.1
Oracle Communications Diameter Signaling Router, versions 8.0.0.0-8.5.0.0	https://support.oracle.com/rs?type=doc&id=2809085.1
Oracle Communications EAGLE	https://support.oracle.com/rs?type=doc&id=2809087.1
Oracle Communications EAGLE FTP Table Base Retrieval, version 4.5	https://support.oracle.com/rs?type=doc&id=2809115.1
Oracle Communications EAGLE LNP Application Processor, versions 46.7, 46.8, 46.9	https://support.oracle.com/rs?type=doc&id=2809093.1
Oracle Communications Element Manager, versions 8.2.0.0-8.2.4.0	https://support.oracle.com/rs?type=doc&id=2809094.1
Oracle Communications Fraud Monitor, versions 3.4-4.4	https://support.oracle.com/rs?type=doc&id=2809422.1
Oracle Communications Interactive Session Recorder, version 6.4	https://support.oracle.com/rs?type=doc&id=2809118.1
Oracle Communications LSMS, versions 13.1-13.4	https://support.oracle.com/rs?type=doc&id=2809119.1
Oracle Communications Messaging Server, version 8.1	https://support.oracle.com/rs?type=doc&id=2808816.1
Oracle Communications MetaSolv Solution, version 6.3.1	https://support.oracle.com/rs?type=doc&id=2808878.1
Oracle Communications Offline Mediation Controller, version 12.0.0.3.0	https://support.oracle.com/rs?type=doc&id=2808879.1
Oracle Communications Operations Monitor, versions 3.4, 4.2, 4.3, 4.4	https://support.oracle.com/rs?type=doc&id=2809120.1
Oracle Communications Policy Management, version 12.5.0	https://support.oracle.com/rs?type=doc&id=2809110.1

受影响产品及版本号	可用补丁
Oracle Communications Pricing Design Center, version 12.0.0.3.0	https://support.oracle.com/rs?type=doc&id=2808815.1
Oracle Communications Services Gatekeeper, version 7.0	https://support.oracle.com/rs?type=doc&id=2809111.1
Oracle Communications Session Border Controller, versions 8.4, 9.0	https://support.oracle.com/rs?type=doc&id=2809267.1
Oracle Communications Session Report Manager, versions 8.0.0.0-8.2.5.0	https://support.oracle.com/rs?type=doc&id=2811990.1
Oracle Communications Session Route Manager, versions 8.0.0.0-8.2.5.0	https://support.oracle.com/rs?type=doc&id=2812072.1
Oracle Data Integrator, version 12.2.1.4.0	https://support.oracle.com/rs?type=doc&id=2796575.1
Oracle Database Server, versions 12.1.0.2, 12.2.0.1, 19c, 21c	https://support.oracle.com/rs?type=doc&id=2796575.1
Oracle Documaker, versions 12.6.0-12.6.4	https://support.oracle.com/rs?type=doc&id=2809145.1
Oracle E-Business Suite, versions 12.1.1-12.1.3, 12.2.3-12.2.10	https://support.oracle.com/rs?type=doc&id=2484000.1
Oracle Enterprise Communications Broker, versions 3.2, 3.3	https://support.oracle.com/rs?type=doc&id=2809298.1
Oracle Enterprise Repository, version 11.1.1.7.0	https://support.oracle.com/rs?type=doc&id=2796575.1
Oracle Enterprise Telephony Fraud Monitor, versions 3.4, 4.2, 4.3, 4.4	https://support.oracle.com/rs?type=doc&id=2810340.1
Oracle Ethernet Switch ES2-64, Oracle Ethernet Switch ES2-72, version 2.0.0.14	https://support.oracle.com/rs?type=doc&id=2809232.1
Oracle Financial Services Analytical Applications Infrastructure, versions 8.0.6-8.1.1	https://support.oracle.com/rs?type=doc&id=2809214.1
Oracle Financial Services Enterprise Case Management, versions 8.0.7.2.0, 8.0.8.1.0	https://support.oracle.com/
Oracle Financial Services Model Management and Governance, versions 8.0.8.0.0-8.1.0.0.0	https://support.oracle.com/rs?type=doc&id=2814201.1
Oracle FLEXCUBE Core Banking, versions 11.7, 11.8, 11.9, 11.10	https://support.oracle.com/
Oracle Global Lifecycle Management OPatch	https://support.oracle.com/rs?type=doc&id=2796575.1
Oracle GoldenGate, versions prior to 19.1.0.0.0.210420	https://support.oracle.com/rs?type=doc&id=2796575.1

受影响产品及版本号	可用补丁
Oracle GoldenGate Application Adapters, version 19.1.0.0.0	https://support.oracle.com/rs?type=doc&id=2796575.1
Oracle GraalVM Enterprise Edition, versions 20.3.3, 21.2.0	https://support.oracle.com/rs?type=doc&id=2810386.1
Oracle Graph Server and Client, versions prior to 21.3.0	https://support.oracle.com/rs?type=doc&id=2796575.1
Oracle Health Sciences Central Coding, versions 6.2.0, 6.3.0	https://support.oracle.com/rs?type=doc&id=2806298.1
Oracle Health Sciences InForm, version 6.3.0	https://support.oracle.com/rs?type=doc&id=2806298.1
Oracle Healthcare Data Repository, versions 7.0.2, 8.1.0	https://support.oracle.com/rs?type=doc&id=2806298.1
Oracle Healthcare Foundation, versions 7.3, 8.0, 8.1	https://support.oracle.com/rs?type=doc&id=2806298.1
Oracle Hospitality Cruise Shipboard Property Management System, version 20.1.0	https://support.oracle.com/rs?type=doc&id=2806436.1
Oracle HTTP Server, versions 11.1.1.9.0, 12.2.1.4.0	https://support.oracle.com/rs?type=doc&id=2796575.1
Oracle Insurance Calculation Engine, versions 11.0.0-11.3.1	https://support.oracle.com/rs?type=doc&id=2809145.1
Oracle Insurance Policy Administration, versions 11.0.0-11.3.1	https://support.oracle.com/rs?type=doc&id=2809145.1
Oracle Java SE, versions 7u311, 8u301, 11.0.12, 17	https://support.oracle.com/rs?type=doc&id=2810386.1
Oracle NoSQL Database	https://support.oracle.com/rs?type=doc&id=2796575.1
Oracle Outside In Technology, version 8.5.5	https://support.oracle.com/rs?type=doc&id=2796575.1
Oracle Real User Experience Insight, versions 13.4.1.0, 13.5.1.0	https://support.oracle.com/rs?type=doc&id=2796575.1
Oracle Real-Time Decision Server, versions 3.2.0.0, 11.1.1.9.0	https://support.oracle.com/rs?type=doc&id=2796575.1
Oracle REST Data Services, versions prior to 21.3	https://support.oracle.com/rs?type=doc&id=2796575.1
Oracle Retail Advanced Inventory Planning, versions 14.1, 15.0, 16.0	https://support.oracle.com/rs?type=doc&id=2801874.1
Oracle Retail Assortment Planning, version 16.0	https://support.oracle.com/rs?type=doc&id=2801874.1
Oracle Retail Back Office, versions 14.0, 14.1	https://support.oracle.com/rs?type=doc&id=2801874.1
Oracle Retail Bulk Data Integration, versions 16.0.3, 19.0.1	https://support.oracle.com/rs?type=doc&id=2801874.1
Oracle Retail Central Office, versions 14.0, 14.1	https://support.oracle.com/rs?type=doc&id=2801874.1
Oracle Retail Customer Management and Segmentation Foundation, versions 16.0-19.0	https://support.oracle.com/rs?type=doc&id=2801874.1
Oracle Retail Extract Transform and Load, version 13.2.8	https://support.oracle.com/rs?type=doc&id=2801874.1

受影响产品及版本号	可用补丁
Oracle Retail Financial Integration, versions 14.1.3.2, 15.0.4.0, 16.0.3.0	https://support.oracle.com/rs?type=doc&id=2801874.1
Oracle Retail Integration Bus, versions 14.1.3.2, 15.0.4.0, 16.0.3.0, 19.0.1.0	https://support.oracle.com/rs?type=doc&id=2801874.1
Oracle Retail Merchandising System, versions 15.0.3, 19.0.1	https://support.oracle.com/rs?type=doc&id=2801874.1
Oracle Retail Point-of-Service, versions 14.0, 14.1	https://support.oracle.com/rs?type=doc&id=2801874.1
Oracle Retail Predictive Application Server, versions 14.1.3, 15.0.3, 16.0.3	https://support.oracle.com/rs?type=doc&id=2801874.1
Oracle Retail Returns Management, versions 14.0, 14.1	https://support.oracle.com/rs?type=doc&id=2801874.1
Oracle Retail Service Backbone, versions 14.1.3.2, 15.0.4.0, 16.0.3.0, 19.0.1.0	https://support.oracle.com/rs?type=doc&id=2801874.1
Oracle Retail Store Inventory Management, versions 14.1, 15.0, 16.0	https://support.oracle.com/rs?type=doc&id=2801874.1
Oracle Secure Backup, versions prior to 18.1.0.1.0	https://support.oracle.com/rs?type=doc&id=2796575.1
Oracle Secure Global Desktop, version 5.6	https://support.oracle.com/rs?type=doc&id=2810981.1
Oracle Solaris, version 11	https://support.oracle.com/rs?type=doc&id=2809232.1
Oracle Spatial Studio	https://support.oracle.com/rs?type=doc&id=2796575.1
Oracle SQL Developer	https://support.oracle.com/rs?type=doc&id=2796575.1
Oracle Transportation Management, version 6.4.3	https://support.oracle.com/rs?type=doc&id=2810378.1
Oracle Utilities Framework, versions 4.2.0.2.0, 4.2.0.3.0, 4.3.0.1.0-4.3.0.6.0, 4.4.0.0.0, 4.4.0.2.0, 4.4.0.3.0	https://support.oracle.com/rs?type=doc&id=2809748.1
Oracle VM VirtualBox, versions prior to 6.1.28	https://support.oracle.com/rs?type=doc&id=2810981.1
Oracle WebCenter Portal,versions 12.2.1.3.0, 12.2.1.4.0	https://support.oracle.com/rs?type=doc&id=2796575.1
Oracle WebCenter Sites, versions 12.2.1.3.0, 12.2.1.4.0	https://support.oracle.com/rs?type=doc&id=2796575.1
Oracle WebLogic Server, versions 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0, 14.1.1.0.0	https://support.oracle.com/rs?type=doc&id=2796575.1
Oracle WebLogic Server Proxy Plug-In, versions 12.2.1.3.0, 12.2.1.4.0	https://support.oracle.com/rs?type=doc&id=2796575.1

受影响产品及版本号	可用补丁
Oracle ZFS Storage Appliance Kit, version 8.8	https://support.oracle.com/rs?type=doc&id=2809232.1
PeopleSoft Enterprise CC Common Application Objects, version 9.2	https://support.oracle.com/rs?type=doc&id=2810361.1
PeopleSoft Enterprise CS Academic Advisement, version 9.2	https://support.oracle.com/rs?type=doc&id=2810361.1
PeopleSoft Enterprise CS Campus Community, versions 9.0, 9.2	https://support.oracle.com/rs?type=doc&id=2810361.1
PeopleSoft Enterprise CS SA Integration Pack, versions 9.0, 9.2	https://support.oracle.com/rs?type=doc&id=2810361.1
PeopleSoft Enterprise CS Student Records, version 9.2	https://support.oracle.com/rs?type=doc&id=2810361.1
PeopleSoft Enterprise PeopleTools, versions 8.57, 8.58, 8.59	https://support.oracle.com/rs?type=doc&id=2810361.1
PeopleSoft Enterprise SCM, version 9.2	https://support.oracle.com/rs?type=doc&id=2810361.1
Primavera Gateway, versions 17.12.0-17.12.11, 18.8.0-18.8.12, 19.12.0-19.12.11, 20.12.0-20.12.7	https://support.oracle.com/rs?type=doc&id=2809438.1
Primavera Unifier, versions 17.7-17.12, 18.8, 19.12, 20.12	https://support.oracle.com/rs?type=doc&id=2809438.1
Siebel Applications, versions 21.9 and prior	https://support.oracle.com/rs?type=doc&id=2810362.1
Tekelec Platform Distribution, versions 7.4.0-7.7.1	https://support.oracle.com/rs?type=doc&id=2809117.1
Tekelec Virtual Operating Environment, versions 3.4.0-3.7.1	https://support.oracle.com/rs?type=doc&id=2809138.1

声明

微软 10 月安全更新多个产品高危漏洞通告

发布日期：2021-10-13

一、漏洞概述

10 月 13 日，绿盟科技 CERT 监测到微软发布 10 月安全更新补丁，修复了 81 个安全问题，涉及 Windows、Microsoft Office、Microsoft Visual Studio、Exchange Server 等广泛使用的产品，其中包括权限提升、远程代码执行等高危漏洞类型。

本月微软月度更新修复的漏洞中，严重程度为关键（Critical）的漏洞有 3 个，重要（Imp ortant）漏洞有 70 个，其中包括 4 个 0day 漏洞：

Win32k 权限提升漏洞（CVE-2021-40449）

Windows DNS Server 远程代码执行漏洞（CVE-2021-40469）

Windows Kernel 权限提升漏洞（CVE-2021-41335）

Windows AppContainer 防火墙规则安全功能绕过漏洞（CVE-2021-41338） 请相关用户尽快更新补丁进行防护，完整漏洞列表请参考附录。

绿盟远程安全评估系统（RSAS）已具备微软此次补丁更新中大部分漏洞的检测能力（包 括 CVE-2021-38672、CVE-2021-40461、CVE-2021-40486、CVE-2021-40469、CVE-2021-40449 等高危漏洞），请相关用户关注绿盟远程安全评估系统插件升级包的更新，及时升级至 V6.0R02F01.2501，官网链接：http://update.nsfocus.com/update/listRsasDetail/v/ vulsys

参考链接：

https://msrc.microsoft.com/update-guide/en-us/releaseNote/2021-Oct

二、重点漏洞简述

根据产品流行度和漏洞重要性筛选出此次更新中包含影响较大的漏洞，请相关用户重点 进行关注：

Windows Hyper-V 远程代码执行漏洞（CVE-2021-38672/CVE-2021-40461）：

Windows Hyper-V 是 Microsoft 的本地虚拟机管理程序，guest VM 可读取主机中的内核内存与在自身 VM 上发生的内存分配错误，低权限的攻击者可发送特制的请求在目标系统上执行任意代码。

官方通告链接：

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-38672

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-40461

Win32k 权限提升漏洞（CVE-2021-40449）：

Win32k 中存在一个 NtGdiResetDC 函数，攻击者在该函数释放之后可以设置用户模式回调；拥有低权限的攻击者通过执行意外的 API 函数可实现权限提升，目前已检测到该漏洞被在野利用。

官方通告链接：

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-40449

Windows Print Spooler 欺骗漏洞（CVE-2021-36970）：

Windows 打印后台服务中存在漏洞，在用户交互的情况下，未经身份验证攻击者可以利用该漏洞在目标主机上远程执行代码。

官方通告链接：

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-36970

Microsoft Exchange Server 远程代码执行漏洞（CVE-2021-26427）：

经过身份验证的攻击者可通过相邻网络对受影响的 Exchange 服务器进行攻击，可在目标服务器端实现远程代码执行

官方通告链接：

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26427

Microsoft Word 远程代码执行漏洞（CVE-2021-40486）：

攻击者可通过制作恶意的 Word 文档，当成功诱导用户在受影响的系统上打开恶意文档后，可在目标系统上以该用户权限执行任意代码，预览窗格也被列为攻击媒介。

官方通告链接：

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-40486

WindowsDNS server 远程代码执行漏洞（CVE-2021-40469）：

在服务器配置为 DNS 服务器的情况下，攻击者可利用此漏洞实现在目标系统上以 SYST EM 权限远程代码执行，且不需要用户交互，目前漏洞细节已公开。

官方通告链接：

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-40469

三、影响范围

以下为重点关注漏洞的受影响产品版本，其他漏洞影响产品范围请参阅官方通告链接。

漏洞编号	受影响产品版本
CVE-2021-38672	Windows Server 2022 (Server Core installation) Windows Server 2022 Windows 11 for x64-based Systems
CVE-2021-40461	Windows Server, version 20H2 (Server Core Installation) Windows Server, version 2004 (Server Core installation) Windows Server 2022 (Server Core installation) Windows Server 2022 Windows Server 2019 (Server Core installation) Windows Server 2019 Windows 11 for x64-based Systems Windows 10 Version 21H1 for x64-based Systems Windows 10 Version 20H2 for x64-based Systems Windows 10 Version 2004 for x64-based Systems Windows 10 Version 1909 for x64-based Systems Windows 10 Version 1809 for x64-based Systems
CVE-2021-40449 CVE-2021-36970	Windows Server, version 20H2 (Server Core Installation) Windows Server, version 2004 (Server Core installation) Windows Server 2022 (Server Core installation) Windows Server 2022 Windows Server 2019 (Server Core installation) Windows Server 2019 Windows Server 2016 (Server Core installation) Windows Server 2016 Windows Server 2012 R2 (Server Core installation) Windows Server 2012 R2 Windows Server 2012 (Server Core installation) Windows Server 2012 Windows Server 2008 for x64-based Systems Service Pack 2 (S erver Core installation) Windows Server 2008 for x64-based Systems Service Pack 2 Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) Windows Server 2008 for 32-bit Systems Service Pack 2 Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)

漏洞编号	受影响产品版本
	Windows Server 2008 R2 for x64-based Systems Service Pack 1 Windows RT 8.1 Windows 8.1 for x64-based systems Windows 8.1 for 32-bit systems Windows 7 for x64-based Systems Service Pack 1 Windows 7 for 32-bit Systems Service Pack 1 Windows 11 for x64-based Systems Windows 11 for ARM64-based Systems Windows 10 for x64-based Systems Windows 10 for 32-bit Systems Windows 10 Version 21H1 for x64-based Systems Windows 10 Version 21H1 for ARM64-based Systems Windows 10 Version 21H1 for 32-bit Systems Windows 10 Version 20H2 for x64-based Systems Windows 10 Version 20H2 for ARM64-based Systems Windows 10 Version 20H2 for 32-bit Systems Windows 10 Version 2004 for x64-based Systems Windows 10 Version 2004 for ARM64-based Systems Windows 10 Version 2004 for 32-bit Systems Windows 10 Version 1909 for x64-based Systems Windows 10 Version 1909 for ARM64-based Systems Windows 10 Version 1909 for 32-bit Systems Windows 10 Version 1809 for x64-based Systems Windows 10 Version 1809 for ARM64-based Systems Windows 10 Version 1809 for 32-bit Systems Windows 10 Version 1607 for x64-based Systems Windows 10 Version 1607 for 32-bit Systems
CVE-2021-26427	Microsoft Exchange Server 2019 Cumulative Update 11 Microsoft Exchange Server 2019 Cumulative Update 10 Microsoft Exchange Server 2016 Cumulative Update 22 Microsoft Exchange Server 2016 Cumulative Update 21 Microsoft Exchange Server 2013 Cumulative Update 23 Microsoft Word 2016 (64-bit edition) Microsoft Word 2016 (32-bit edition) Microsoft Word 2013 Service Pack 1 (64-bit editions)

漏洞编号	受影响产品版本
CVE-2021-40486	Microsoft Word 2013 Service Pack 1 (32-bit editions) Microsoft Word 2013 RT Service Pack 1 Microsoft SharePoint Server 2019 Microsoft SharePoint Enterprise Server 2016 Microsoft SharePoint Enterprise Server 2013 Service Pack 1 Microsoft Office Web Apps Server 2013 Service Pack 1 Microsoft Office Online Server Microsoft Office 2019 for 64-bit editions Microsoft Office 2019 for 32-bit editions
CVE-2021-40469	Windows Server, version 2004 (Server Core installation) Windows Server 2022 (Server Core installation) Windows Server 2022 Windows Server, version 20H2 (Server Core Installation) Windows Server 2019 (Server Core installation) Windows Server 2019 Windows Server 2012 R2 (Server Core installation) Windows Server 2012 R2 Windows Server 2012 (Server Core installation) Windows Server 2012 Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) Windows Server 2008 R2 for x64-based Systems Service Pack 1 Windows Server 2008 for x64-based Systems Service Pack 2 (S erver Core installation) Windows Server 2008 for x64-based Systems Service Pack 2 Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) Windows Server 2008 for 32-bit Systems Service Pack 2 Windows Server 2016 (Server Core installation) Windows Server 2016

四、漏洞防护

4.1 补丁更新

目前微软官方已针对受支持的

产品版本发布了修复以上漏洞的安全补丁，强烈建议受影

响用户尽快安装补丁进行防护，官方下载链接：

https://msrc.microsoft.com/update-guide/en-us/releaseNote/2021-Oct

注：由于网络问题、计算机环境问题等原因，Windows Update 的补丁更新可能出现失败。用户在安装补丁后，应及时检查补丁是否成功更新。

右键点击 Windows 图标，选择“设置(N)”，选择“更新和安全”-“Windows 更新”，查看该页面上的提示信息，也可点击“查看更新历史记录”查看历史更新情况。

针对未成功安装的更新，可点击更新名称跳转到微软官方下载页面，建议用户点击该页面上的链接，转到“Microsoft 更新目录”网站下载独立程序包并安装。

附录：漏洞列表

影响产品	CVE 编号	漏洞标题	严重程度
Windows	CVE-2021-38672	Windows Hyper-V 远程代码执行漏洞	Critical
Windows	CVE-2021-40461	Windows Hyper-V 远程代码执行漏洞	Critical
Microsoft Office	CVE-2021-40486	Microsoft Word 远程代码执行漏洞	Critical
Exchange Server	CVE-2021-34453	Microsoft Exchange Server 拒绝服务漏洞	Important
Windows	CVE-2021-36953	Windows TCP/IP 拒绝服务漏洞	Important
Windows	CVE-2021-36970	Windows Print Spooler 欺骗漏洞	Important
Windows	CVE-2021-40443	Windows Common Log File System Driver 权限提升漏洞	Important
Windows	CVE-2021-40449	Win32k 权限提升漏洞	Important
Microsoft Office, Windows	CVE-2021-40454	Rich Text Edit Control 信息披露漏洞	Important
Windows	CVE-2021-40455	Windows Installer 欺骗漏洞	Important
Windows	CVE-2021-40456	Windows AD FS 安全功能绕过漏洞	Important
Microsoft Dynamics	CVE-2021-40457	Microsoft Dynamics 365 Customer Engagement 跨站脚本漏洞	Important
Windows	CVE-2021-40475	Windows Cloud Files Mini Filter Driver 信息披露漏洞	Important
Windows	CVE-2021-40476	Windows AppContainer Elevation Of Privilege Vulnerability	Important
Windows	CVE-2021-40477	Windows Event Tracing 权限提升漏洞	Important
Windows	CVE-2021-40478	Storage Spaces Controller 权限提升漏洞	Important
Microsoft Office	CVE-2021-41344	Microsoft SharePoint Server 远程代码执行漏洞	Important

影响产品	CVE 编号	漏洞标题	严重程度
Exchange Server	CVE-2021-41348	Microsoft Exchange Server 权限提升漏洞	Important
Exchange Server	CVE-2021-41350	Microsoft Exchange Server 欺骗漏洞	Important
.NET,Microsoft Visual Studio	CVE-2021-41355	.NET Core and Visual Studio 信息披露漏洞	Important
Windows	CVE-2021-41361	Active Directory Federation Server 欺骗漏洞	Important
Microsoft Visual Studio	CVE-2021-3450	OpenSSL: CVE-2021-3450 CA certificate check bypass with X509_V_FLAG_X509_STRICT	Important
Microsoft Visual Studio	CVE-2021-3449	OpenSSL: CVE-2021-3449 NULL pointer deref in signature_algorithms processing	Important
Microsoft Visual Studio	CVE-2020-1971	OpenSSL: CVE-2020-1971 EDIPARTYNAME NULL pointer de-reference	Important
Exchange Server	CVE-2021-26427	Microsoft Exchange Server 远程代码执行漏洞	Important
Windows	CVE-2021-38662	Windows Fast FAT File System Driver 信息披露漏洞	Important
Windows	CVE-2021-38663	Windows exFAT File System 信息披露漏洞	Important
Windows	CVE-2021-40450	Win32k 权限提升漏洞	Important
Windows	CVE-2021-40460	Windows Remote Procedure Call Runtime 安全功能绕过漏洞	Important
Windows	CVE-2021-40462	Windows Media Foundation Dolby Digital Atmos Decoders 远程代码执行漏洞	Important
Windows	CVE-2021-40463	Windows NAT 拒绝服务漏洞	Important
Windows	CVE-2021-40464	Windows Nearby Sharing 权限提升漏洞	Important
Windows	CVE-2021-40465	Windows Text Shaping 远程代码执行漏洞	Important
Windows	CVE-2021-40466	Windows Common Log File System Driver 权限提升漏洞	Important
Windows	CVE-2021-40467	Windows Common Log File System Driver 权限提升漏洞	Important
Windows	CVE-2021-40468	Windows Bind Filter Driver 信息披露漏洞	Important
Windows	CVE-2021-40469	Windows DNS Server 远程代码执行漏洞	Important
Windows	CVE-2021-40470	DirectX Graphics Kernel 权限提升漏洞	Important
Microsoft Office	CVE-2021-40471	Microsoft Excel 远程代码执行漏洞	Important
Microsoft Office	CVE-2021-40472	Microsoft Excel 信息披露漏洞	Important

影响产品	CVE 编号	漏洞标题	严重程度
Microsoft Office	CVE-2021-40473	Microsoft Excel 远程代码执行漏洞	Important
Microsoft Office	CVE-2021-40474	Microsoft Excel 远程代码执行漏洞	Important
Microsoft Office	CVE-2021-40479	Microsoft Excel 远程代码执行漏洞	Important
Microsoft Office	CVE-2021-40480	Microsoft Office Visio 远程代码执行漏洞	Important
Microsoft Office	CVE-2021-40481	Microsoft Office Visio 远程代码执行漏洞	Important
Microsoft Office	CVE-2021-40482	Microsoft SharePoint Server 信息披露漏洞	Important
Microsoft Office	CVE-2021-40484	Microsoft SharePoint Server 欺骗漏洞	Important
Microsoft Office	CVE-2021-40485	Microsoft Excel 远程代码执行漏洞	Important
Microsoft Office	CVE-2021-40487	Microsoft SharePoint Server 远程代码执行漏洞	Important
Windows	CVE-2021-40488	Storage Spaces Controller 权限提升漏洞	Important
Windows	CVE-2021-40489	Storage Spaces Controller 权限提升漏洞	Important
Windows	CVE-2021-26441	Storage Spaces Controller 权限提升漏洞	Important
Windows	CVE-2021-26442	Windows HTTP.sys 权限提升漏洞	Important
Windows	CVE-2021-41330	Microsoft Windows Media Foundation 远程代码执行漏洞	Important
Windows	CVE-2021-41331	Windows Media Audio Decoder 远程代码执行漏洞	Important
Windows	CVE-2021-41332	Windows Print Spooler 信息披露漏洞	Important
Windows	CVE-2021-41334	Windows Desktop Bridge 权限提升漏洞	Important
Windows	CVE-2021-41335	Windows Kernel 权限提升漏洞	Important
Windows	CVE-2021-41336	Windows Kernel 信息披露漏洞	Important
Windows	CVE-2021-41337	Active Directory 安全功能绕过漏洞	Important
Windows	CVE-2021-41338	Windows AppContainer Firewall Rules 安全功能绕过漏洞	Important
Windows	CVE-2021-41339	Microsoft DWM Core Library 权限提升漏洞	Important
Windows	CVE-2021-41340	Windows Graphics Component 远程代码执行漏洞	Important
Windows	CVE-2021-41342	Windows MSHTML Platform 远程代码执行漏洞	Important
Windows	CVE-2021-41343	Windows Fast FAT File SystemDriver 信息披露漏洞	Important
Windows	CVE-2021-41345	Storage Spaces Controller 权限提升漏洞	Important
Windows	CVE-2021-41346	Console Window Host 安全功能绕过漏洞	Important

影响产品	CVE 编号	漏洞标题	严重程度
Windows	CVE-2021-41347	Windows AppX Deployment Service 权限提升漏洞	Important
System Center	CVE-2021-41352	SCOM 信息披露漏洞	Important
Microsoft Dynamics	CVE-2021-41353	Microsoft Dynamics 365 (on-premises) 欺骗漏洞	Important
Microsoft Dynamics	CVE-2021-41354	Microsoft Dynamics 365 (on-premises) 跨站脚本漏洞	Important
Windows	CVE-2021-41357	Win32k 权限提升漏洞	Important
Apps	CVE-2021-41363	Intune Management Extension 安全功能绕过漏洞	Important
Microsoft Office	CVE-2021-40483	Microsoft SharePoint Server 欺骗漏洞	Low
Microsoft Edge (Chromium-based)	CVE-2021-37974	Chromium: CVE-2021-37974 Use after free in Safe Browsing	Unknown
Microsoft Edge (Chromium-based)	CVE-2021-37975	Chromium: CVE-2021-37975 Use after free in V8	Unknown
Microsoft Edge (Chromium-based)	CVE-2021-37976	Chromium: CVE-2021-37976 Information leak in core	Unknown
Microsoft Edge (Chromium-based)	CVE-2021-37977	Chromium: CVE-2021-37977 Use after free in Garbage Collection	Unknown
Microsoft Edge (Chromium-based)	CVE-2021-37978	Chromium: CVE-2021-37978 Heap buffer overflow in Blink	Unknown
Microsoft Edge (Chromium-based)	CVE-2021-37979	Chromium: CVE-2021-37979 Heap buffer overflow in WebRTC	Unknown
Microsoft Edge (Chromium-based)	CVE-2021-37980	Chromium: CVE-2021-37980 Inappropriate implementation in Sandbox	Unknown

声明

NSFOCUS

安全态势

互联网安全威胁态势

热点资讯

1. 攻击者利用PixStealer和MalRhino恶意软件针对巴西支付生态系统用户发起攻击

【概述】

研究人员发现，在Google Play 商店中新发现的两个恶意 Android 应用程序已被用于攻击巴西支付生态系统的用户，攻击者通过两个独立的恶意应用程序分发了两种不同的银行恶意软件变种，名为PixStealer和MalRhino，攻击者利用恶意软件变种引诱受害者将他们的整个帐户余额以欺诈方式转移到网络犯罪分子控制的另一个银行帐户中，这两个恶意应用程序通过用户交互和原始 PIX 应用程序窃取受害者的钱财。

【参考链接】

https://ti.nsfocus.com/security-news/llMUM

2. 攻击者利用GriftHorse恶意软件感染了多个国家/地区的Android 智能手机

【概述】

研究人员发现了一种名为 GriftHorse 的恶意软件，攻击者利用该恶意软件已感染了 70 多个国家/地区的超过 1000 万部 Android 智能手机。被盗总金额可能高达数亿欧元，据专家称，攻击者通过上传到官方 Google Play 商店和第三方 Android 应用商店的应用程序进行传播。用户会从屏幕上的警报得知，通知他们中了奖并要求接受邀请以接收它。受害者会受到每小时至少出现五次的弹出警报窗口的提示。

【参考链接】

https://ti.nsfocus.com/security-news/llMUI

3. 攻击者利用BloodyStealer特洛伊木马窃取玩家帐户和数据

【概述】

卡巴斯基的研究人员发现了一种名为 BloodyStealer 的高级恶意木马，可从 Steam、Epic Games Stores 和 EA Origin 等平台窃取玩家帐户和数据。攻击者利用BloodyStealer 恶特洛伊木马为每个受感染的受害者分配一个唯一的标识符，在为受害者分配 UID 并获得 C&C IP 地址后，BloodyStealer 从受感染机器中提取各种数据，创建一个包含有关泄露数据信息的 POST 请求，并将其发送给恶意 C&C。

【参考链接】

https://ti.nsfocus.com/security-news/llMUD

4. 黑客利用MSHTML漏洞针对俄罗斯国家火箭中心和内政部发起攻击

【概述】

近日，研究人员发现了一起黑客利用MSHTML漏洞针对俄罗斯国家火箭中心和内政部的攻击活动。研究人员分析称，第一封邮件声称来自俄罗斯火箭中心的人力资源部门，而第二封邮件则表示来自莫斯科内政部，这两封邮件均使用了相同的感染方式，要求接收者启用编辑以填写表格。当受害者一旦打开恶意文档并启用编辑，会将加载MSHTML的定制控件ActiveX运行任意代码，导致系统感染。

【参考链接】

https://ti.nsfocus.com/security-news/llMUw

5. 黑客窃取比特币基金会网站1.7万美元

【概述】

黑客攻击了比特币基金会网站 Bitcoin.org，并更改了其部分内容，并利用其宣传比特币骗局，黑客盗取了1.7万多美元。Bitcoin.org 被黑客入侵以运行“双倍资金”骗局，攻击者通过向基金会网站用户发送虚假地址，以获得双倍酬劳的报酬吸引用户，此外，为了增加索赔的吸引力，诈骗者写道，该优惠仅限于前一万名用户。

【参考链接】

https://ti.nsfocus.com/security-news/llMUv

6. 欧洲呼叫中心巨头Covisian的西班牙语分部遭Conti勒索软件团伙袭击

【概述】

Covisian是欧洲规模最大的客户服务与呼叫中心供应商之一，近日，研究人员发现，Covisian的西班牙语分部遭Conti勒索软件团伙袭击，内部系统被迫瘫痪，导致西班牙、南美洲的多个组织客服意外中断服务；导致大部分IT系统瘫痪。

【参考链接】

https://ti.nsfocus.com/security-news/llMUx

7. 攻击者利用新型恶意软件Tangle Bot窃取用户手机信息

【概述】

网络安全公司最近发现了一种新的威胁，攻击者以Android用户为主要目标，利用新型恶意软件Tangle Bot窃取用户手机信息，通过向用户发送虚假短信息链接，在点击链接之后,跳转网页将显示“Adobe Flash Player需要更新”,如果用户同意更新并点击了更新安装按钮, TangleBot将植入手机，开始接管包括控制电话簿,记录屏幕等功能,攻击者也可以随时打开设备摄像头和麦克风。TangleBot甚至可以通过覆盖屏幕的方法访问在线金融应用程序。随后，受害者的设备还会被用来转发伪造的的Covid-19警报。

【参考链接】

https://ti.nsfocus.com/security-news/llMUf

8. 攻击者利用新 Android 银行木马ERMAC窃取财务数据

【概述】

近日，研究人员发现了新Android 银行木马，名为ERMAC，攻击者利用ERMAC木马从378个银行和钱包窃取财务数据，财务数据包括联系人信息、短信、打开任意应用程序，并针对众多金融应用程序的覆盖

攻击以刷入登录凭据，允许恶意软件清除特定应用程序的缓存并窃取存储在设备上的帐户。

【参考链接】

https://ti.nsfocus.com/security-news/llMU9

9. 勒索软件团伙使用自定义的Python脚本攻击虚拟机

【概述】

近日，研究人员发现了勒索软件团伙使用自定义的Python脚本攻击并且加密托管在 VMware ESXi 服务器上的虚拟机。攻击中，勒索软件团伙在初次入侵后仅三小时就加密了 VMware ESXi 服务器中的虚拟磁盘。该团伙通过登录在域管理员登录的设备上运行的 TeamViewer 帐户来访问网络。然后使用 Advanced IP Scanner 扫描网络端识别其他目标，接着使用名为 Bitvis 的 SSH 客户端登录到 ESXi 服务器。攻击者首先关闭虚拟机，覆盖存储在数据存储卷上的原始文件的内容以防止受害者恢复它们，然后删除虚拟机磁盘。

【参考链接】

https://ti.nsfocus.com/security-news/llMV1

10. 攻击者利用以太网电缆作为传输天线从隔离的气隙计算机中窃取敏感数据

【概述】

近日，以色列内盖夫本古里安大学的研究人员发现了一种称为 LANtenna 的新型电磁攻击，该攻击使用以太网电缆作为传输天线从隔离的气隙计算机中窃取敏感数据。该大学网络安全研究中心的研发主管 Mordechai Guri 表示，“气隙计算机中的恶意代码收集敏感数据，并通过以太网电缆发出的无线电波对其进行编码，将它们用作天线。附近的接收设备可以无线拦截信号，解码数据，并将其发送给攻击者。”

【参考链接】

https://ti.nsfocus.com/security-news/llMUY

11. 攻击者利用勒索软件对Springhill医疗中心进行攻击

【概述】

研究人员发现，Springhill医疗中心遭勒索软件攻击，导致该医疗中心部分电子设备已失效，以及导致某婴儿不幸离世，该母亲对医疗中心提起诉讼，认为医疗中心应对此事件负责。但由于系统出现故障医护人员监测不到婴儿的状况，待发现问题后，婴儿已出现了严重的脑损伤，在持续供氧九个月后去世。

【参考链接】

https://ti.nsfocus.com/security-news/llMVE

12. 跨国工程巨头伟尔集团Weir Group遭受勒索软件团伙攻击

【概述】

近日，苏格兰跨国工程巨头伟尔集团（Weir Group）遭受到勒索软件攻击。该勒索事件导致其发货、制造和工程中断，以及导致间接费用回收不足和收入延期5000万英镑。伟尔集团是全球知名矿业、石油天然气和电力基础设施工程解决方案的提供者，在全球50多个国家拥有1.15万名员工。对于此次勒索事件，伟尔方面表示：“伟尔网络安全系统，对威胁做出了快速反应，并采取了强有力的保护措施——这包括隔离和关闭IT系

统，特别是隔离和关闭核心企业资源规划 (ERP)和工程应用程序。”

【参考链接】

https://ti.nsfocus.com/security-news/llMVs

13. 硅谷风险投资公司泄露了“交易流”数据

【概述】

一家硅谷风险投资公司运营着将投资者与初创公司联系起来的配对服务，暴露了 6GB 的数据，包括与投资者和初创公司有关的交易流信息。这些数据属于 Plug and Play Ventures，该公司总部位于加利福尼亚州桑尼维尔，并在世界各地设有办事处。即插即用帮助初创公司起步，并将这些公司与投资者相匹配。该公司表示，它受益于对 PayPal 和 Dropbox 的早期投资。

【参考链接】

https://ti.nsfocus.com/security-news/llMV9

14. 攻击者利用Coinbase漏洞窃取用户资金

【概述】

研究人员发现，攻击者利用加密货币交易所 Coinbase 实施的基于 SMS 的双因素身份验证 (2FA) 系统中的漏洞从 6,000 多个用户那里窃取资金。根据提交给美国州检察长办公室的数据泄露通知信，攻击者知道他们的用户名和密码以及与帐户相关的电话号码，能够绕过基于 SMS 的身份验证窃取资金。

【参考链接】

https://ti.nsfocus.com/security-news/llMV8

15. 匿名人士泄露了Twitch的源代码和数据

【概述】

匿名 4chan 用户在 4chan 论坛上发布了一个 128GB 文件的 torrent 链接，泄露的档案包含从 6,000 个内部 Twitch Git 存储库窃取的敏感数据。The Record 的专家下载并分析了数据以验证其真实性，确认泄露的内容包括平台的用户身份和身份验证机制以及其顶级流媒体的支付方案。流行的视频流平台证实了安全漏洞，并正在对其进行调查以确定事件的严重程度。

【参考链接】

https://ti.nsfocus.com/security-news/llMV7

16. APT28组织针对14000名Gmail用户发起攻击

【概述】

研究人员发现了一个APT28网络钓鱼活动，目标是跨多个企业的大约14,000 名 Gmail 用户，该组织在俄罗斯总参谋部主要情报局 (GRU) 第 85 主要特别服务中心 (GTsSS) 的军事统一 26165 之外运作。Google 建议 为工作和个人电子邮件注册 高级保护计划，该计划保护具有高度可见性和敏感信息的用户，这些用户面临有针对性的在线攻击的风险。该公司会自动改进其服务以抵御当今广泛的威胁。

【参考链接】

https://ti.nsfocus.com/security-news/llMVe

17. 勒索团伙使用 Python 脚本加密 VMware ESXi 服务器

【概述】

勒索软件团伙使用自定义 Python 脚本来攻击 VMware ESXi 并加密服务器上托管的所有虚拟机。入侵者通过登录在域管理员登录的设备上运行的 TeamViewer 帐户来访问网络。然后攻击者使用 Advanced IP Scanner 扫描网络端识别其他目标，然后使用名为 Bitvis 的 SSH 客户端登录到 ESXi 服务器。在这种情况下，受害组织的 IT 管理员让 SSH ESXi Shell 服务为攻击者打开了大门，勒索软件操作者然后执行一个微小的 Python 脚本 (6kb) 来加密服务器上托管的虚拟机的所有虚拟磁盘和 VM 设置文件。

【参考链接】

https://ti.nsfocus.com/security-news/llMV1

18. 攻击者利用0day漏洞攻击俄罗斯多个组织

【概述】

近日，研究人员发现，美国港口之一的休斯顿遭到攻击者网络攻击，根据美国机构的说法，认为这次攻击是由利用Zoho用户身份验证设备中的零日漏洞的“攻击者”实施的。美国联邦调查局、CISA 和海岸警卫队网络司令部 发布联合公告，警告APT 组织正在积极利用ADSelfService Plus 软件，攻击者可以利用该软件来放置webshell，这使攻击者能够进行后利用活动，例如破坏管理员凭据、进行横向移动以及泄露注册表配置单元和 Active Directory 文件。

【参考链接】

https://ti.nsfocus.com/security-news/llMTX

19. 美国媒体集团CMG遭到勒索软件团伙攻击

【概述】

近日，研究人员发现，美国媒体集团CMG遭到勒索软件团伙攻击，导致电视直播和广播流中断。CMG立即在执法部门的支持下展开调查，还聘请了领先的网络安全专家来确定攻击的程度。该公司证实，它没有支付赎金。

【参考链接】

https://ti.nsfocus.com/security-news/llMVu

20. 印第安纳州2家医院遭遇网络攻击

【概述】

近日，研究人员发现，印第安纳州2家医院遭遇网络攻击，分别是富兰克林的约翰逊纪念健康中心和位

于西摩约 40 英里外的施内克医疗中心，导致医院的IT系统崩溃，计算机网络已被禁用，所有的IT系统处于停机状态，两家医院都不得不转移患者或推迟择期手术， 以及此次攻击，导致部分患者和员工数据泄露，其中一些数据后来被黑客发布到暗网上。

【参考链接】

https://ti.nsfocus.com/security-news/llMV4

21. Mykings僵尸网络通过挖矿活动至少获利2470万美元

【概述】

据研究报告显示，每天约有4700个新系统被僵尸网络感染。MyKings也被称为Smominru或Xaxmen，主要进行加密货币挖矿活动，通常瞄准未及时修补的系统，它利用多种方式进行传播，如向受害者的熟人发送命名为“照片”实为恶意软件的具有迷惑性的.rar或.zip文件，再如在流行歌手泰勒·斯威夫特（Taylor Swift）的 Jpeg 图像内隐藏恶意.exe。在成功感染后，Mykings会采取多种方式进行持久化实现长期驻留，如：清理其他木马、卸载杀毒软件、关闭系统自更新、关闭Windows Defender、阻止139、445等端口连接、添加注册表启动项等与此同时新感染的设备也会成为攻击其他系统的跳板。

【参考链接】

https://ti.nsfocus.com/security-news/llMWr

22. 攻击者利用新型阎罗王勒索软件高度针对性攻击大型企业

【概述】

研究人员发现了一种新的勒索软件，称为 Yanluowang，用于对企业进行高度针对性的攻击。同时注意到使用合法的 AdFind 命令行 Active Directory 查询工具，该工具经常被勒索软件运营商滥用作为侦察工具。攻击者在部署到受感染设备之前，攻击者会先启动一个恶意工具，该工具先通过创建一个 .txt 文件，其中包含要在命令行中检查的远程机器数，再使用 Windows Management Instrumentation (WMI) 获取在 .txt 文件中列出的远程计算机上运行的进程列表，最后将所有进程和远程机器名称记录到 processes.txt。攻击者在部署严洛网勒索软件后，它将停止管理程序虚拟机，结束上述工具（包括 SQL 和备份解决方案 Veeam）记录的所有进程，然后对文件进行加密。勒索软件将 .yanluowang 扩展

名附加到加密文件的文件名进而实施攻击。

【参考链接】

https://ti.nsfocus.com/security-news/llMWn

23. 华为云成为加密货币挖矿恶意软件的新目标

【概述】

研究人员最近注意到一种全新的 Linux 恶意软件攻击，它针对相对较新的云服务提供商 (CSP) 进行加密货币挖掘恶意软件和加密劫持攻击。攻击者会部署代码来删除主要存在于华为云中的应用程序和服务。具体来说，恶意代码会禁用 hostguard 服务，这是一个“检测安全问题、保护系统并监控代理”的华为云 Linux 代理进程。恶意代码还包括cloudResetPwdUpdateAgent，这是一个开源插件代理，允许华为云用户重置弹性云服务（ECS）实例的密码，该实例默认安装在公共镜像上。由于攻击者在其 shell 脚本中存在这两项服务，我们可以假设他们专门针对华为云内的易受攻击的 ECS 实例。

【参考链接】

https://ti.nsfocus.com/security-news/llMWp

24. 攻击者用数学符号绕过反钓鱼检测进行攻击

【概述】

研究人员研究人员表示作为一种古老的网络攻击手段，钓鱼邮件是企业和个人最常遇见的网络威胁之一，面对日益频发的钓鱼邮件攻击，不少企业开始部署各种反钓鱼邮件的工具和解决方案，而攻击者们则是想尽办法来规避这些反钓鱼邮件检测。近日，研究人员发现某钓鱼邮件组织使用数字符号来干扰反钓鱼邮件检测，它的核心是利用各种数字符号替换公司logo或名字中的字母，达到“欺骗”反钓鱼邮件或反垃圾邮件产品的目标。

【参考链接】

https://ti.nsfocus.com/security-news/llMWA

25. BlackTech组织利用恶意软件Gh0stTimes对服务器进行攻击

【概述】

近日，研究人员发现了BlackTech可能使用的恶意软件Gh0stTimes，BlackTech是一个网络间谍组织，在2018年前后对日本发起攻击活动。研究人员同时在受Gh0stTimes感染的服务器上还发现了其他恶意软件，如下载器、后门程序、ELF Bifrose和攻击工具。这些工具可能会也被BlackTech组织使用。研究人员此次的研究说明BlackTech攻击组织依然活跃，且使用了更多的工具。

【参考链接】

https://ti.nsfocus.com/security-news/llMWc

26. 攻击者利用勒索软件攻击奥林巴斯计算机系统

【概述】

医疗技术巨头奥林巴斯在网络攻击后被迫关闭其在美国（美国、加拿大和拉丁美洲）的计算机网络，公司没有透露它遭受的攻击类型，但情况表明可能是勒索软件攻击。9 月，奥林巴斯发表声明，宣布其欧洲、中东和非洲计算机网络遭到勒索软件攻击。在受感染系统上发现的赎金票据声称该公司受到BlackMatter 勒索软件组织的攻击。

【参考链接】

https://ti.nsfocus.com/security-news/llMWa

27. 美国奎斯特诊断公司承认35万名患者医疗资料被泄露

【概述】

奎斯特诊断公司向美国证券交易委员会(SEC)通报称，公司旗下生育诊所ReproSource在八月份遭到了勒索软件攻击，约 350,000 名患者的大量健康信息和财务信息遭到泄漏，部分患者的社会安全号码（ssn)和信用卡号码也遭到泄漏。攻击期间还泄露了用户大量健康信息，包括 CPT 代码、诊断代码、测试申请和结果、测试报告和病史信息、健康保险或团体计划识别名称和编号以及个人或由个人提供的其他信息治疗医师。

【参考链接】

https://ti.nsfocus.com/security-news/llMWd

28. 微软击退了针对Azure客户的创纪录的2.4 Tbps DDoS攻击

【概述】

研究者表示其 Azure 云平台在 8 月的最后一周缓解了针对欧洲未具名客户的 2.4 Tbps 分布式拒绝服务 (DDoS) 攻击，超过了亚马逊网络服务在 2020 年 2 月阻止的2.3 Tbps 攻击。DDoS攻击是攻击者利用 UDP 协议的无连接特性和欺骗性请求，用大量数据包淹没目标服务器或网络，造成中断或渲染服务器及其周边基础设施不可用。据说这次攻击源自一个由大约 70,000 台受感染设备组成的僵尸网络，这些设备主要位于亚太地区，例如马来西亚、越南、台湾、日本和中国，以及美国等国家。

【参考链接】

https://ti.nsfocus.com/security-news/llMVV

29. 与伊朗有关的DEV-0343 APT目标是美国和以色列国防技术公司

【概述】

Microsoft 威胁情报中心 (MSTIC) 和 Microsoft 数字安全部门 (DSU) 的研究人员发现了一个跟踪为 DEV-0343 的恶意活动集群，DEV-0343 是 Microsoft 威胁情报中心 (MSTIC) 首次观察到并于 2021 年 7 月下旬开始跟踪的新活动集群。MSTIC 观察到 DEV-0343 对 250 多个 Office 365 租户进行了广泛的密码喷洒，攻击重点是美国和以色列国防技术公司、波斯湾入境口岸或在中东开展业务的全球海上运输公司。

【参考链接】

https://ti.nsfocus.com/security-news/llMW9

30. 日本跨国公遭勒索软件攻击，被勒索700万美金赎金

【概述】

近日，日本跨国公司JVCKenwood遭到了Conti 勒索软件攻击，攻击者声称窃取了1.7TB的数据，并勒索700 万美元的赎金。JVCKenwood 是一家总部位于日本的跨国电子公司，拥有 16,956 名员工，2021 年的收入为 24.5 亿美元。该公司以其 JVC、Kenwood 和 Victor 品牌而闻名，这些品牌生产汽车和家庭音频设备、医疗保健和无线电设备、专业和车载摄像头以及便携式发电站。JVCKenwood表示，其在欧洲的销售公司的服务器于9月22日遭到破坏，攻击者可能在攻击期间访问了数据。

【参考链接】

https://ti.nsfocus.com/security-news/llMVK

31. 攻击者利用 Discord 基础设施进行恶意攻击

【概述】

Check Point Research (CPR) 发现了一种多功能恶意软件，能够截取屏幕截图、下载和执行其他文件以及执行键盘记录——所有这些都是通过使用 Discord 的核心功能。Discord 机器人功能强大、友好且非常节省时间。然而，能力越大责任也越大，Discord的bot框架很容易被恶意利用。研究人员发现，其中Discord Bot API 是一个简单的 Python 实现，它简化了修改并缩短了开发过程，可以轻松地将机器人变成一个简单的远程访问木马来窃取信息。

【参考链接】

https://ti.nsfocus.com/security-news/llMXw

32. 攻击者针对美国军事防务机构进行Office 365间谍攻击

【概述】

研究人员发现了一个名为DEV-0343的网络组织攻击了美国和以色列的国防技术公司、波斯湾的入境港口以及与中东有关的全球海上运输公司。该威胁组织的攻击方式主要是接管微软Office 365账户。攻击者似乎一直在从事网络间谍活动，同时该组织与伊朗有联系，并且网络攻击者正在对Office 365账户进行大面积的密码喷洒攻击。它是一种针对在线账户使用大量用户名和一系列不同密码进行攻击的过程，攻击者希望找到正确的密码并获得对受密码保护账户的访问权限。

【参考链接】

https://ti.nsfocus.com/security-news/llMXy

33. 黑客利用cookie窃取恶意软件劫持YouTube创作者的帐户

【概述】

黑客利用虚假的合作机会（即杀毒软件、VPN、音乐播放器、照片编辑或网络游戏的演示）劫持了 YouTube 创作者的频道，一旦劫持了频道，攻击者要么将其出售给出价最高的人，要么将其用于加密货币诈骗计划。研究人员发现，恶意软件在登陆页面伪装成软件下载 URL，通过电子邮件或 Google Drive 上的 PDF 或包含网络钓鱼链接的 Google 文档发送。并确定了大约 15,000 个演员帐户，其中大部分是为此活动创建的，还观察到，攻击者将目标推向 WhatsApp、Telegram 或 Discord 等消息应用程序，因为谷歌能够通过 Gmail 阻止网络钓鱼企图，运行假冒软件后，将执行 cookie 窃取恶意软件。恶意软件从受感染的机器窃取浏览器 cookie 并将其发送到 C2 服务器。一旦在目标系统上交付，恶意软件就会被用来窃取他们的凭据和浏览器 cookie，从而允许攻击者在传递 cookie 攻击中劫持受害者的帐户。

【参考链接】

https://ti.nsfocus.com/security-news/llMXv

34. 攻击者使用Telegram Bot窃取PayPal账户资金

【概述】

新的研究发现，网络犯罪分子正在使用Telegram机器人窃取一次性密码token（OTP）并通过银行和在线支付系统（包括PayPal、Apple Pay和Google Pay）欺诈群众。并表示威胁行为者正在使用Telegram机器人和频道以及一系列策略来获取帐户信息，包括致电受害者、冒充银行和合法服务等，同时通过社会工程，威胁行为者还欺骗人们通过移动设备向他们提供OTP或其他验证码，然后骗子用这些代码来骗取用户账户中的资金。

【参考链接】

https://ti.nsfocus.com/security-news/IlMXm

35. 宏碁一周内遭遇二次数据泄露

【概述】

科技巨头宏碁在一周内遭到两次黑客攻击，同一个威胁者(Desorden) 最初入侵了其在印度的一些服务器，现在它声称也入侵了台湾的一些系统。该事件是在威胁行为者在一个地下网络犯罪论坛上发布销售超过60 GB数据的广告后披露的。攻击者现在声称已于10月 15日入侵了宏碁台湾的服务器，并窃取了内部数据，包括员工和产品信息。

【参考链接】

https://ti.nsfocus.com/security-news/IlMXi

36. 攻击者在恶意活动中使用大量商品RAT攻击阿富汗和印度

【概述】

Cisco Talos最近发现了一个威胁行为者，它使用政治和政府为主题的恶意域来针对印度和阿富汗的实体。这些攻击使用 dcRAT 和 QuasarRAT for Windows，通过利用CVE-2017-11882（Microsoft Office 中的内存损坏漏洞）和 AndroidRAT 的恶意文档来攻击移动设备。攻击者还在攻击的初始侦察阶段使用自定义文件枚举器和感染器，然后通过部署各种商品 RAT（例如 DcRAT 和 QuasarRAT）进行攻击。

【参考链接】

https://ti.nsfocus.com/security-news/IlMXl

37. 黑客滥用苹果公司企业应用程序盗取140万美元的加密货币

【概述】

黑客利用社交媒体、约会应用程序、加密货币和滥用苹果公司企业开发者计划，从毫无戒心的受害者那里盗取了至少140万美元。其中名为CryptoRom欺诈的实施相当直接，在通过社交媒体或现有数据应用程序获得受害者的信任后，用户被愚弄到一个看起来像苹果应用商店的网站，然后被告知下载一个移动设备管理程序，安装一个修改版的加密货币交易所，诱使其投资，然后骗走现金。

【参考链接】

https://ti.nsfocus.com/security-news/IlMWU

38. 攻击者冒充DoT进行了为期两天的钓鱼诈骗攻击

【概述】

威胁者在为期两天的网络钓鱼攻击活动中冒充美国交通部（USDOT），他们通过使用多种策略，为了使攻击活动看起来更合法，他们还创建了虚假的联邦网站的域名，来逃避安全检测。研究人员共发现了41封钓鱼邮件，这些邮件都以国会最近通过的1万亿美元基础设施方案中的项目投标为诱饵进行诈骗。此次攻击活动主要以工程、能源和建筑等行业的公司为攻击目标，这些公司可能会与美国交通部合作，并向潜在的受害者发送诈骗电子邮件，一旦进入这个假冒的美国交通部网站，受害者就会被邀请点击一个 "点击这里投标 "按钮，还会出现一个带有微软标志和 "用你的电子邮件提供商登录 "指示的凭证收集表格。第一次尝试输入凭证时会遇到ReCAPTCHA验证，合法网站一般会将其作为网站的安全组件，然而，攻击者在这时就已经获取了凭证，如果受害者第二次尝试输入证书，就会出现一个错误信息，然后他们会被引导到真正的美国交通部网站，钓鱼者经常将这一步作为最后一步来进行执行。

【参考链接】

https://ti.nsfocus.com/security-news/llMX9

39. 黑客窃取了阿根廷全体人口的政府ID数据库

【概述】

一名黑客入侵了阿根廷政府的IT网络，并窃取了该国所有人口的身份证详细信息，这些数据现在正在私人圈子中出售。上个月发生的黑客攻击目标是RENAPER，它代表 Registro Nacional de las Personas，翻译为 National Registry of Persons。该机构是阿根廷内政部的一个重要组成部分，其任务是向所有公民发放国民身份证，并将这些数据以数字格式存储为其他政府机构可访问的数据库，作为大多数政府查询的支柱用于公民的个人信息。根据黑客在线提供的样本，他们现在可以访问的信息包括全名、家庭住址、出生日期、性别信息、身份证签发和到期日期、劳工识别码、Trámite号码、公民号码和政府照片身份证。

【参考链接】

https://ti.nsfocus.com/security-news/llMX8

40. TeamTNT在Docker Hub上部署恶意Docker镜像

【概述】

研究人员最近发现了一项活动，其中 TeamTNT 威胁参与者部署了带有嵌入式脚本的恶意容器映像（托管在 Docker Hub 上），以下载 Zgrab 扫描器 和massscanner，分别用于横幅抓取和端口扫描的渗透测试工具。使用恶意 Docker 镜像中的扫描工具，威胁行为者尝试扫描受害者子网中的更多目标并执行进一步的恶意活动。其中犯罪团伙继续将 Docker Hub、GitHub 和其他包含包含恶意脚本和工具的容器映像和软件组件的共享存储库作为目标。他们通常旨在传播 coinminer 恶意软件，劫持受害者的计算机资源来挖掘加密货币。

【参考链接】

https://ti.nsfocus.com/security-news/llMX5

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/ https://www.nsfocus.com.cn/html/7/20/34/