金融行业

10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

点对点分析CII与等级保护
——安全管理部分

行业研究

数据匿名化：隐私合规下，企业
打开数据主动权的正确方式

无文件攻击及EDR防御分析

90 亿信用卡曝出协议漏洞：
黑客无需密码即可盗刷

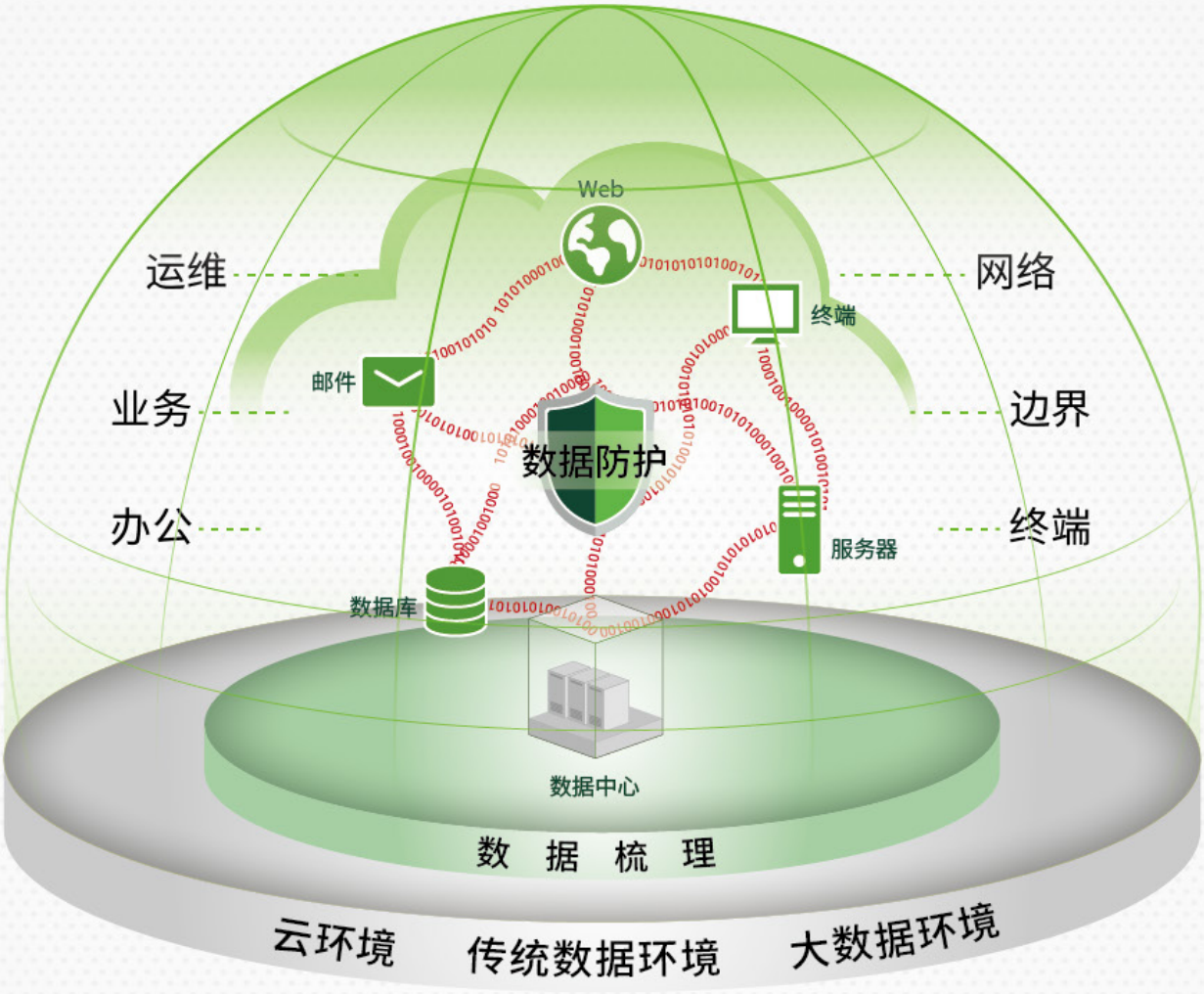
江苏盐城网警破获特大
第四方支付网络黑产案

新型内幕交易曝光，股民用木马
窃取基金公司交易指令 12 年!

NSFOCUS

绿盟数据安全解决方案

NSFOCUS DATA SECURITY SOLUTIONS



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，为政府、运营商、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。

本|期|看|点

安全月报

2020年第10期

绿盟科技金融事业部

目录 CONTENTS

政策解读

行业研究

漏洞聚焦

安全态势

安全月报在线阅读

绿盟科技官方微信

NSFOCUS

政策解读

点对点分析:CII 与等级保护——安全管理部分

绿盟科技

《网络安全法》第三章第二节规定了关键信息基础设施(CII)的运行安全，包括关键信息基础设施的范围、保护的主要内容等。国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其它一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。既然关键信息基础设施的范围、保护在网络安全等级保护制度的基础之上，并且要实行重点保护。那么，绿盟君做了《点对点分析CII与等级保护系列》来分析其中要求的异同点。

对比情况主要参考：

《信息安全技术 关键信息基础设施网络安全保护基本要求》（报批稿）；

《信息安全技术 网络安全等级保护基本要求》，GB/T22239-2019。

将关键信息基础设施要求与等级保护三级要求进行对应分析。

安全管理

CII 要求	对应等保要求
运营者应符合国家网络安全等级保护制度相关要求，对相关信息系统开展定级备案、相应等级的测评、安全建设、整改及自查工作。	略

分析点评：完全一致。

CII 要求	对应等保要求
运营者应： a）建立适合本组织的网络安全保护计划，结合关键业务流的安全风险报告，明确关键信息基础设施网络安全保护工作的目标、安全策略、组织架构、管理制度、技术措施、实施细则及资源保障等，形成文档并经审批后发布至相关人员。网络安全保护计划应至少每年修订一次，或发生重大变化时进行修订。	安全管理制度 安全策略 a）应制定网络安全工作的总体方针和安全策略，阐明机构安全工作的总体目标、范围、原则和安全框架等。

分析点评：略有提高，细化了修订时间。

CII 要求	对应等保要求
b）基于关键业务链、供应链等安全需求建立或完善安全策略和制度，并根据关键信息基础设施面临的安全风险和威胁的变化相应调整。	管理制度 a）应对安全管理活动中的主要管理内容建立安全管理制度； b）应对管理人员或操作人员执行的日常管理操作建立操作规程。

分析点评：略有提高，明确突出了关键业务链、供应链等安全需求建立或完善安全策略和制度。

CII 要求	对应等保要求
运营者应： a）成立指导和管理网络安全工作的委员会或领导小组，由组织主要负责人担任其领导职务，设置专门的网络安全管理机构，建立首席网络安全官制度，建立并实施网络安全考核及监督问责机制。	安全管理机构 岗位设置 a）应成立指导和管理网络安全工作的委员会或领导小组，其最高领导由单位主管领导担任或授权；

分析点评：明确提高。

1、只有担任，没有授权。

2、建立首席网络安全官制度。

3、建立并实施考核及监督问责机制。

CII 要求	对应等保要求
b）安全管理机构主要人员应参与本组织信息化决策。	无

分析点评：此项目为新增项目，明确提高。

CII 要求	对应等保要求
c）安全管理机构相关人员应参加国家、行业或业界网络安全相关活动，及时获取网络安全动态，并传达到本组织。	a）应加强各类管理人员、组织内部机构和网络安全管理部门之间的合作与沟通，定期召开协调会议，共同协作处理网络安全问题； b）应加强与网络安全职能部门、各类供应商、业界专家及安全组织的合作与沟通； c）应建立外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息。

分析点评：略有提高，细化了参加网络安全相关活动，并予以传达

安全管理人员

CII 要求	对应等保要求
运营者应： a）对安全管理机构的负责人和关键岗位的人员进行安全背景和安全技能审查，符合要求的人员方能上岗，关键岗位包括与关键业务系统直接相关的系统管理、网络管理、安全管理等岗位。关键岗位应专人负责，并配备 2 人以上共同管理。	安全管理人员 人员录用 b) 应对被录用人员的身份、安全背景、专业资格或资质等进行审查，对其所具有的技术技能进行考核；

分析点评：明显提高。

1、细化了安全管理机构的负责人和关键岗位的人员进行安全背景和安全技能审查。

2、关键岗位应专人负责，并配备2人以上共同管理（AB角色管理，等保无此要求）。

CII 要求	对应等保要求
b）运营者应建立网络安全教育培训制度，定期开展基于岗位的网络安全教育培训和技能考核，应规定适当的关键信息基础设施从业人员和网络安全关键岗位从业人员的年度培训时长，教育培训内容应包括网络安全相关制度和规定、网络安全保护技术、网络安全风险意识等。	安全意识教育和培训： a）应对各类人员进行安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施； b）应针对不同岗位制定不同的培训计划，对安全基础知识、岗位操作规程等进行培训； c）应定期对不同岗位的人员进行技能考核。

分析点评：培训内容细化，明确包含了网络安全保护技术、网络安全风险意识等。

CII 要求	对应等保要求
c）在上岗前对人员进行安全背景审查，当必要时或人员的身份、安全背景等发生变化时（例如取得非中国国籍）应根据情况重新进行安全背景审查。应在人员发生内部岗位调动时，重新评估调动人员对关键信息基础设施的逻辑和物理访问权限，修改访问权限并通知相关人员或角色。应在人员离岗时，及时终止离岗人员的所有访问权限，收回与身份认证相关的软硬件设备，进行离职面谈并通知相关人员或角色。	人员录用 b）应对被录用人员的身份、安全背景、专业资格或资质等进行审查，对其所具有的技术技能进行考核； c）应与被录用人员签署保密协议，与关键岗位人员签署岗位责任协议。 人员离岗 a）应及时终止离岗人员的所有访问权限，取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备； b）应办理严格的调离手续，并承诺调离后的保密义务后方可离开。

分析点评：略有增强，细化人员要求。强调安全背景等发生变化时（例如取得非中国国籍）应根据情况重新进行安全背景审查，强调人员安全的全生命周期管理。

CII 要求	对应等保要求
d）与从业人员签订安全保密协议，在安全保密协议中，应约定安全职责、奖惩机制，以及当离岗后的脱密期限。	人员录用 c）应与被录用人员签署保密协议，与关键岗位人员签署岗位责任协议。 人员离岗 b）应办理严格的调离手续，并承诺调离后的保密义务后方可离开。

分析点评：略有增强，细化安全保密协议内容，加入脱密期的要求。

安全通信网络

CII 要求	对应等保要求
互联安全 运营者应： a）建立或完善不同等级系统、不同业务系统、不同区域之间的安全互联策略。	安全通信网络 网络架构 c）应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址； d）应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段；

分析点评：明显提高，细化并明确了互联安全策略包括不同等级系统、不同业务系统、不同区域之间的安全互联策略。

安全建设管理

CII 要求	对应等保要求
网络安全与信息化同步要求 运营者应： a）在新建或改建、扩建关键信息基础实施设施时，充分考虑网络安全因素，在规划、建设和投入使用阶段保证安全措施的有效性，并采取测试、评审、攻防演练等多种形式验证。必要时，可建设关键业务的仿真验证环境。	安全方案设计 b）应根据保护对象的安全保护等级及与其他级别保护对象的关系进行安全整体规划和安全方案设计，设计内容应包含密码技术相关内容，并形成配套文件； c）应组织相关部门和有关安全专家对安全整体规划及其配套文件的合理性和正确性进行论证和审定，经过批准后才能正式实施。

分析点评：基本一致，细化了验证方式。

CII 要求	对应等保要求
b）当关键信息基础设施退役废弃时，按照数据安全管理策略对存储的数据进行处理。	无

分析点评：明确提高，为新增项目。

CII 要求	对应等保要求
供应链安全保护 运营者应： a）制定供应链安全管理策略，包括：风险管理策略、供应商选择和管理策略、产品开发采购策略、安全维护策略等。 b）建立供应链安全管理制度，设置相应的供应链安全管理部门，提供用于供应链安全管理的资金、人员和权限等可用资源。 c）保证产品的设计、研发、交付、使用、废弃等各阶段，以及制造设备、工艺等的供应链安全风险基本可控。 d）选择有保障的供应商，防范出现因政治、外交、贸易等非技术因素导致产品和服务供应中断的风险。 e）在能提供相同产品的多个不同供应商中做选择，以防范供应商锁定风险。 f）要求供应商承诺不非法获取用户数据、控制和操纵用户系统和设备，或利用用户对产品的依赖性谋取不正当利益或者迫使用户更新换代。 g）采购、使用的网络关键设备和网络安全专用产品，应通过国家规定的检测认证。 h）采购、使用的网络产品和服务，应符合法律、行政法规的规定和相关国家标准的要求，可能影响国家安全的，应当通过国家安全审查。 i）发现使用的网络产品、服务存在安全缺陷、漏洞等风险时，及时采取措施消除风险隐患，涉及重大风险的应当按规定向保护工作部门报告。 j）采购网络产品和服务时，明确提供者的安全责任和义务，要求提供者做出必要安全承诺，并签订安全保密协议，协议内容应包括安全职责、保密内容、奖惩机制、有效期等。	服务供应商选择 a）应确保服务供应商的选择符合国家的有关规定； b）应与选定的服务供应商签订相关协议，明确整个服务供应链各方需履行的网络安全相关义务； c）应定期监督、评审和审核服务供应商提供的服务，并对其变更服务内容加以控制。

分析点评：明确提高，提出制定供应链安全管理策略，细化供应链风险类型，明确了供应商的不当行为，及保证供应链安全风险基本可控的方法。

CII 要求	对应等保要求
运营者应： a）保证关键信息基础设施的运维地点位于中国境内，如确需境外运维，应当符合我国相关规定。	无

分析点评：明确提高，为新增项目。等保只规定了云平台与大数据平台的数据位于中国境内。

CII 要求	对应等保要求
b）应要求维护人员签订安全保密协议。	安全管理人员 c）应与被录用人员签署保密协议，与关键岗位人员签署岗位责任协议。

分析点评：基本一致，细化了人员要求，明确要求维护人员签订安全保密协议。

CII 要求	对应等保要求
c）确保优先使用已登记备案的运维工具，如确需使用由维护人员带入关键信息基础设施内部的维护工具，应在使用前通过恶意代码检测等测试。	网络和系统安全管理 h）应严格控制运维工具的使用，经过审批后才可接入进行操作，操作过程中应保留不可更改的审计日志，操作结束后应删除工具中的敏感数据；

分析点评：略有提高，强调应在使用前通过恶意代码检测等测试。

NSFOCUS

行业研究

数据匿名化：隐私合规下，企业打开数据主动权的正确方式

天枢实验室　陈磊

摘要

随着欧盟GDPR、美国CCPA，以及我国《网络安全法》等法规的实施与监管，隐私合规与数据安全治理成为企业当前亟需解决的一大安全任务。具体来说，企业通过技术与管理措施，如何在不影响或少影响原有业务流程的同时去满足合规性？其中，数据匿名化作为一种重要的技术手段，在满足数据统计分析的同时可有效地降低个体隐私泄露风险。且有趣的是，近年来研究发现它具有天然的合规遵循优势。GDPR等法规对赋予用户更多的隐私数据控制权，反过来削减企业的数据控制权与主动权。那么，匿名化技术是否可以帮助企业重新打开数据主动权和控制权这个局面？带着这个疑问，本文将从合规背景、技术算法以及应用与产品三个方面对该技术进行介绍。

一、安全合规背景

欧盟GDPR、美国CCPA赋予了用户非常多的数据权利，例如，GDPR规定用户可对个人数据提出限制处理以及删除的请求；CCPA规定用户有权要求企业不得出售其个人数据。我国《网络安全法》等法规也赋予了一定权利，例如用户发现企业违反规定或错误有权要求企业删除或更正个人信息。反过来，这些法规对企业提出更高的隐私和安全要求，在一定程度上削弱了企业以往普遍存在的数据掌控能力与权利优势。无疑，这给企业100%的数据掌控权关上了大门，但法规在平衡个体隐私与数据发展的原则指导下，关上一扇门，同时也打开一扇窗——企业可以通过数据匿名化在一些典型数据场景下重新打开数据主动权与控制权。

- GDPR：对于个人数据、以及假名化等数据，GDPR对相关处理和存储的企业提出十分严厉且全面的法律义务，需要企业履行相关义务。而唯独对于经过处理的匿名数据网开一面——该数据企业可用于统计和研究目的，不受GDPR的约束与限制，即对履行用户各类数据控制权请求等条款具有豁免权。（GDPR前言26段）
- 《网络安全法》：“匿名”数据（“经过处理无法识别特定个人且不能复原”），企业无需征求被收集者同意，可直接与第三方进行数据共享。（四十二条）
- 《个人信息安全规范》：个人信息经匿名化处理后所得的信息不属于个人信息（3.14节）；在个人信息主体注销账户场景中，处理注销账户的个人信息有两种方式：①选择直接删除数据；②存储匿名化处理后的数据。（8.5节）

由此可看出，匿名化有重要的合规遵循的应用价值，尤其是在数据统

计、研究以及数据开放与共享场景中；同时实施该技术措施给企业带来其他方面的好处。即：

- **合规遵循。**匿名数据在向第三方提供、统计分析和注销账户保存匿名数据等场景中是合规的；
- **数据共享价值。**在数据共享场景中，尤其数据敏感且价值密度高的行业，比如医疗，金融等行业，实施数据匿名技术后，可合法合规（光明正大）地进行数据共享与价值挖掘；
- **增强用户信任。**匿名数据，数据是匿名的，即任何人无法识别和关联匿名数据记录的身份。那么用户不担心该数据公开和处理过程中泄露本人隐私；
- **降低隐私风险。**匿名数据在流动和处理过程中，“数据部分可见但身份不可见”，从而有效地降低个体隐私泄露的风险。也就是说，即使匿名数据库遭受黑客攻击外泄，攻击者也无法破解或还原出匿名数据记录所涉及的用户身份信息。

那么什么是匿名化呢？《个人信息安全规范》给出详细的定义：“通过对个人信息的技术处理，使得个人信息主体无法被识别或者关联，且处理后的信息不能被复原的过程”。即匿名化通过数据变换与失真，处理结果可保持一定的可用性，但任何手段无法识别特定个人，且数据不可逆（非“一一映射”（例如加密、置换手段））。数据脱敏（包括去标识化）作为目前企业广泛实施的数据安全技术，可以看成是“数据匿名化”的相近技术，它对数据进行一系列的数据变换和失真，但无法保证每次处理的结果是真正“匿名”的，即是否达到“无法识别特定个人且不能复原”。若需评估该技术的效果——是否满足法规定义的匿名化门槛，可参考系列文章《数据脱敏后的隐私攻击与风险评估》、《身份证号+手机号如何脱敏才有效？》。如何真正实现和逼近法规的“匿名化”？幸运的是，在学术界中能找到具有广泛和深入研究以K-匿名为代表的数据匿名技术（也称匿名化技术），它可以达到法规要求的匿名化效果。本文下面将对该技术原理、算法，以及现有工业界应用进行介绍，以期进一步促进数据匿名技术在企业场景的研究与应用。

二、数据匿名技术与算法

2.1概述

早期，个人数据发布的隐私保护场景中，对标识符或准标识符进行简单处理，比如删除、或者使用随机ID替换姓名、用户昵称，对地址信息和出生日期进行泛化处理，这种方式可看成前面提到的“数据脱敏”。然而随着一些攻击案例和研究发现，这种处理方法的“匿名”处理是不充分的，仍然存在个体隐私泄露的风险。验证这一观点，有多个著名的实际案例：

- 案例1：1996年美国麻省发布了医疗患者信息数据库（DB1），去掉患者的姓名和地址信息，仅保留患者的{ZIP, Birthday, Sex, Diagnosis,…}信息。另外有另一个可获得的数据库（DB2），是州选民的登记表，包括选民的{ZIP, Birthday, Sex, Name, Address,…}详细个人信息。攻击者将这两个数据库的同属性段{ ZIP, Birthday, Sex}进行关联操作，可以恢复出大部分选民的医疗健康信息，从而一起严重的医疗隐私数据泄露事故。
- 案例2：AOL公司公布了2006年3个月用户的真实搜索日志，包括1900万搜索记录，为保护隐私对用户ID进行处理，使用随机ID代替真实ID。然而纽约时报记者发现，根据一系列历史搜索行为和包含的相关信息进行推断，可以确定编号4417749的身份——一位62岁的老太太，家里养了三条狗，患有某种疾病。后经过老太太本人证实确实是她搜索的关键词。记者曝光该事件后，引起美国公民对AOL公司隐私保护措施的诸多顾虑，并导致AOL首席技术官引咎辞职。

以上均属于链接攻击（也称重标识攻击、去匿名攻击）范畴，即攻击者通过各种渠道获得公民/用户的身份信息和其他用户的静态属性信息（学术称为“准标识符”属性，比如性别，出生年月、邮编等），包括访问查询公开身份数据集、了解亲朋好友的基本信息、互联网“人肉搜索”陌生人，甚至利用数据泄露、黑灰产数据库等对脱敏数据集进行关联、相似匹配与碰撞，进而还原出上述脱敏数据集的某些记录的身份信息。为了应对潜在的隐私攻击问题与挑战，学术界开始聚焦和设计隐私保护效果更好的匿名化技术与模型。一般地，用户希望攻击者无法从存在多个个体记录的数据集中识别出自身，以及对应的敏感隐私数据，数据匿名技术便是这种朴素思想的实现之一。Samarati和Sweeney学者在1998年首次提出了匿名化的概念，对个人一些基本信息进行泛化和失真处理，隐藏公开数据记录与特定个人之间的对应联系，从而保护个体的隐私。后面，Sweeney学者在2002年提出了K-匿名模型(K-Anonymity)，该模型保证数据记录的任意等价组至少有K个个体记录，即攻击者无法唯一地确定个体的记录准确身份。如下图所示，它对原始数据进行2-匿名处理，包括对Birth（出生日期）进行泛化、对邮编（ZIP）进行屏蔽处理等操作，最后输出的数据集除敏感属性（Disease）外，其他属性（也称准标识符属性）组成的记录形成等价组，每个等价组至少有两条记录，如索引 (1,2)有2条记录、(2,3) 有2条记录、(4,5) 有2条记录、(5,6) 有2条记录、(7,9)有3条记录，(10,11) 有2条记录。在攻击场景中，假设攻击者拥有背景知识，了解Jack在该数据集中且掌握了他的基本属性：Race：Black; Birth:1965-09-01；Gender: male；ZIP:02146。攻击者想识别Jack具体属于数据集的那一条记录？经过相似匹配和关联，定位到索引1和索引2，但不能唯一确定那个属于Jack，那么也无法确定Jack患上了那种疾病。也可以说，无法确定索引1和索引2对应的真实身份，从而保护患者的个体隐私。

Index	Race	Birth	Gender	ZIP	Disease
1	Black	1965	male	0214*	short breath
2	Black	1965	male	0214*	chest pain
3	Black	1965	female	0213*	hypertension
4	Black	1965	female	0213*	hypertension
5	Black	1964	female	0213*	obesity
6	Black	1964	female	0213*	chest pain
7	White	1964	male	0213*	chest pain
8	White	1964	male	0213*	obesity
9	White	1964	male	0213*	short breath
10	White	1967	male	0213*	chest pain
11	White	1967	male	0213*	chest pain

图1　经过2-匿名处理的医疗数据

数据发布场景的隐私保护(PrivacyPreserving Data Publishing, PPDP)是K-匿名最早的应用，也是研究最为广泛的场景，除此以外将K-匿名为代表的数据匿名技术应用在位置服务和社交网络等领域成为近年来新的一个热点。基于匿名化的PPDP场景可看作为一个通信模型，如图2所示，主要由三方参与：数据控制者/发布者(Data Controller/Publisher)，可看作发送者；数据接收者(DataRecipients)；隐私攻击者(Attacker)。数据控制者/发布者收集个体(Individuals) 的个人信息，将这些数据通过匿名化处理(Data Anonymization) 后得到匿名化数据集，发送给第三方共享或者对外公开。攻击者尝试通过掌握的背景知识和数据库进行攻击，获取具体某个个体的隐私信息。典型一种攻击方式是链接攻击，即去除准标识符信息 (Identifier，ID，如姓名，身份ID)，攻击者通过其他渠道掌握的数据库的同属性段(称为准标识符，Quasi-Identifier,QID)与公开数据库进行链接和匹配操作，恢复出具体个体敏感信息(Sensitiveattribute, SA，如健康、薪资、位置等)。

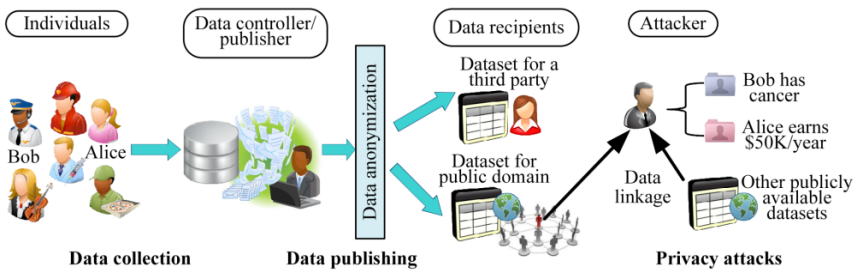


图2数据匿名化的一般应用场景

2.2 模型与算法

数据匿名技术的研究主要集中在模型、算法、匿名处理操作和评估指标四个研究方面。

2.2.1 匿名模型

前面提到的K-anonymity由于敏感属性进行约束，当等价组的敏感属性取值相同时，仍然存在隐私风险，Machanvajjhala等人提出了L-diversity模型，在每一个等价组中，至少存在L个不同的敏感属性，相比K-anonymity增强了安全性。 Li等人在L-diversity基础上，考虑敏感属性分布，设计了T-closeness模型，通过保证任意等价组的敏感属性的分布与敏感属性的全局分布之间的距离小于T，进一步增强了安全性，然而约束条件越来越多，降低数据的可用性。除以上模型外，还出发展和衍生出了-anonymity和个性化隐私保护 (Personalized privacy preservation)的模型等。

2.2.2 匿名化算法

匿名化算法以最小的数据缺损代价实现满足模型的约束。然而研究表明，实现最优的匿名化是一个NP难题。幸运的是，目前已经发展许多有效的近似算法，典型的算法包括Datafly算法，Mondrian算法。前者是单维度泛化算法，其核心思想是对给定数据表中QID的属性中取值最多的那个属性按预先给定的泛化树进行泛化，直到匿名化数据表满足K-anonymity；后者是多维度泛化算法，其核心思想是将所有QID属性看成是一样的，即只有一个等价组，然后自上而下，启发式选择QID的某个属性逐次划分，直到满足条件无法划分。除以上算法外，由于聚类算法思想与匿名化等价类划分思想十分相近，因此一些学者提出基于聚类的匿名化算法。

2.2.3 匿名处理操作

主要包括数泛化、抑制、置换等操作。其中泛化最为广泛应用，泛化是指用模糊/抽象/概括的值代替精确值，使得多个数据是相同的。例如年龄26，29被泛化为“25-30”，地址朝阳区、海淀区被泛化为北京市，那么攻击者无法精确地获得数据主体精确信息；抑制操作一般将数据使用“*”代替，隐藏和遮蔽数据值，使得攻击者无法获得该部分的信息；置换是对数据表中的属性值进行位置打乱操作，使得数据主体与该属性信息不对应，一般用于SA属性的处理中。

2.2.4 评估指标

主要分为两个方面的评价，数据可用性 (Data Utility)与隐私保护性(Privacy Protection)。在文献研究中，前者指标较为丰富，可对，包括匿名化的NCP (Normalized Certainty Penalty)，CM (Classification Metric) 和DM (Discemibility Metric)。后者研究文献，一般默认使用模型的参数进行评判，例如K-anonymity、L-diversity，参数K和L越大，分别对应的重识别和隐私泄露风险越小。近年来，一些学者基于通信模型和Shannon信息论对，对隐私泄露问题进行数学建模与分析，提供了理论的度量方法。

三、数据匿名技术的应用

数据匿名技术随着发展逐步趋向成熟，一些高校和研究机构基于软件功能实现开源数据匿名化项目与工具，一些面向隐私合规的欧美科技公司对该技术进行产品化和应用。

3.1 开源项目

基于数据匿名技术的工具化实现主要集中在欧美高校和研究结构，有4个著名的开源项目：ARX、UTD Anonymization Toolbox、Cornell

Anonymization Toolkit焕然Amnesia。从成熟度看，ARX最为成熟，提供丰富的界面和API接口，以及在微软匿名化，提供完整的数据可用性、重标识风险评估等功能组件。

表1 数据匿名的相关开源项目

	ARX	UTD Anonymization Toolbox	Cornell Anonymization Toolkit	Amnesia
开发者机构	慕尼黑工业大学·德国	得克萨斯大学达拉斯分校·美国	康乃尔大学·美国	信息系统管理研究所（IMSI）·希腊
开发语言	Java	Java	C++	Java
项目主页/github	https://arx.deidentifier.org https://github.com/arx-deidentifier/arx	http://cs.utdallas.edu/dspl/cgi-bin/toolbox	https://github.com/wanghaisheng/Cornell-Anonymization-Toolkit	https://amnesia.openaire.eu https://github.com/dTsitsigkos/Amnesia
项目成熟度	实验研究，半产品	实验研究	实验研究	实验研究，接近半产品
支持的匿名模型	K- 匿名、L- 多样和 T- 近似	K- 匿名、L- 多样和 T- 近似	L- 多样	K- 匿名、- 匿名
支持的匿名算法	Flash	Datafly、Mondrian、Incognito	Incognito	Flash、基于聚类算法
特点	提供丰富的数据可用性、风险评估等功能	提供多种匿名算法实现	可简单进行数据可用性、风险评估的计算	支持在线 https://amnesia.openaire. eu/amnesia

3.2 企业产品应用

GDPR、CCPA的隐私合规驱动，一些欧美企业，包括Google，以及主打隐私合规产品的创业公司，率先将数据匿名技术进行了孵化与产品应用。

◆ Google 的云DLP产品

Google 浏览器的隐私声明中，承诺对用户数据使用K-匿名、L-多样数据匿名化以及差分隐私等技术进行处理。随着用户隐私与敏感数据上云，隐私和数据泄露问题引起云使用者的担忧，谷歌将匿名化技术嵌入DLP产品中，可以解决隐私风险问题。DLP产品实现四种匿名化模型与算法，包括K-匿名、L-多样、K-图和-存在性，用户可以根据隐私保护和数据统计分析的需求选择合适的模型算法。在匿名处理数据前，云DLP谷歌提供了原始数据的风险洞察功能：如图3所示，使用者可以看到在K-匿名的不同K值下，不满足的记录数比例（蓝色）。

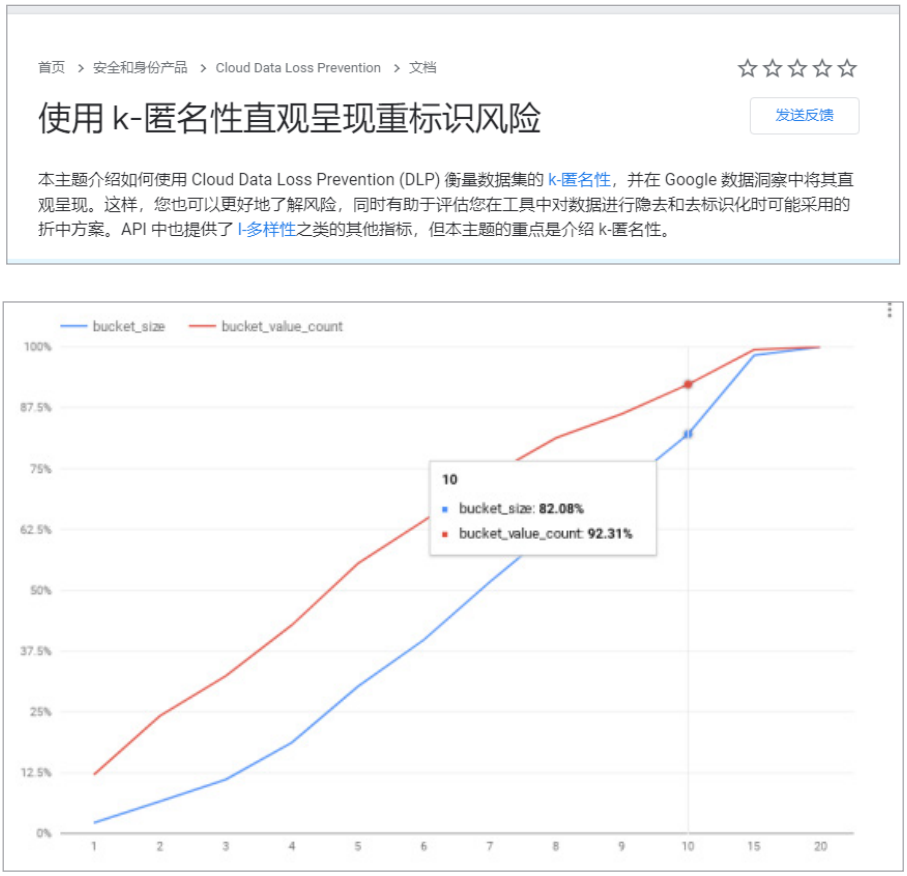


图3 Google云DLP产品的风险洞察功能

◆ Immuta的数据治理平台产品

Immuta是一家美国初创企业，目前处于C轮融资（融资总额6820万美元）。Immuta在云云生数据治理平台 (cloud-nativedata governance platform) 应用到了K-匿名技术，K-匿名可应用在静态数据和动态数据中，后者可能采用类似m –

invariance的匿名算法，即保持动态增量的数据仍然满足等价组数量至少为K个，该技术的应用可增强云存储与计算的隐私安全。

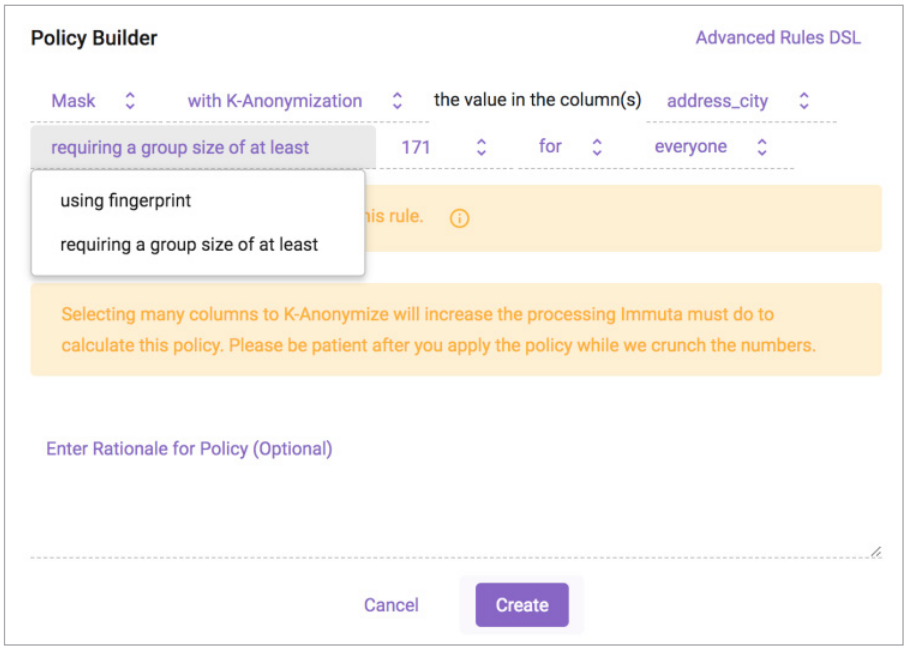


图4 Immuta的数据治理平台

◆ Privitar的数据脱敏产品

Privitar是一家成立于2014年总部位于英国伦敦的创业公司，目前处于C轮融资（融资总额15050万美元），主打推出一系列的隐私产品，包括大规模数据隐私治理的自动化、隐私政策管理、数字水印平台以及数据脱敏产品(公司称为De-Identification 产品，实际功能与国内的Data masking功能基本相同)。在数据脱敏系统中，除了使用传统的基于泛化、替换、屏蔽和加密等脱敏策略外；其数据脱敏嵌入了K-匿名算法，它相比传统脱敏的策略在隐私保护上更强优势，攻击者即使获得经过K-匿名的脱敏数据，也无法通过其他渠道获得的身份信息或数据库进行关联推断，还原脱敏记录的真实身份，进而有效保证隐私前提下实现脱敏数据的提取与利用。

◆ Anonos的BigPrivacy产品

Anonos是一家美国初创企业，目前融资总额1200万美元。其公司主要推出了BigPrivacy产品，同样可以看成一个脱敏平台，其假名化和身份与业务数据分离，这些功能可满足GDPR具体条款的一些合规性。在该平台中，Anonos也应用

了K-匿名技术与算法，在保证数据在业务场景的可用性时，可保证K-匿名处理后的数据不被重标识与身份识别。

小结

全球的数据安全隐私法规的立法，一方面赋予了公民与互联网用户的数据控制权利；另一方面对数据处理的企业提出了更高的隐私与安全要求。企业一方面可以通过访问控制和网络安全防护等措施降低数据收集、存储和处理等阶段的隐私泄露风险，另一方面在日益增多的数据共享与计算场景实施数据匿名化是不错的选择——不仅满足业务利用与隐私保护，同时遵循了合规性。

参考资料

1.Samarati P,Sweeney L. Generalizing data to provide anonymity when disclosing information(abstract). symposium on principles of database systems, 1998.2.Sweeney L.K-anonymity: A model for protecting privacy. International Journal ofUncertainty, Fuzziness and Knowledge-based Systems, 2002,10(5):557-5703. L-diversity:Privacybeyondk-anonymity. Machanavajjhala A,Gehrke J,Kifer D,et al. Proceedings of the22th International Conference on Data Engineering . 20064. Li N H, Li T C,Venkatasubramanian S. T-Closeness-privacy beyond K-anonymity and L-diversity.IEEE 23rd International Conference on Data Engineering, Istanbul, Turkey, April15-20, 2007: 106-115.5. Dwork C.Differential privacy. Encyclopedia of Cryptography and Security, 2011: 338-340.6.Rocher L, HendrickxJ M, De Montjoye Y A. Estimating the success of re-identifications inincomplete datasets using generative models. Nature communications, 2019, 10(1): 1-9.7. El Emam K.Guide to the de-identification of personal health information. Auerbach Publications,2013.8.Meyerson, Adam,and Ryan Williams. "On the complexity of optimal k-anonymity",Proceedings of the twenty-third symposium on Principles of database systems.ACM, 2004.9. LeFevre, K., D.J. DeWitt, and R. Ramakrishnan. "Mondrian Multidimensional K-Anonymity"22nd International Conference on Data Engineering (ICDE'06). IEEE, 2006.10.Aggarwal, CharuC, "On k-anonymity and the curse of dimensionality", Proceedings ofthe 31st international conference on Very large data bases. VLDB Endowment,2005.11.Zakerzadeh H,Aggarwal C C, Barker K, "Towards breaking the curse of dimensionality forhigh-dimensional privacy", Proceedings of the 2014 SIAM InternationalConference on Data Mining, 2014: 731-739.12.Terrovitis,Manolis, Nikos Mamoulis, and Panos Kalnis, "Privacy-preservinganonymization of set-valued data", Proceedings of the VLDB Endowment 1.1(2008): 115-125.

无文件攻击及 EDR 防御分析

金融事业部　武杰

第一章　概述

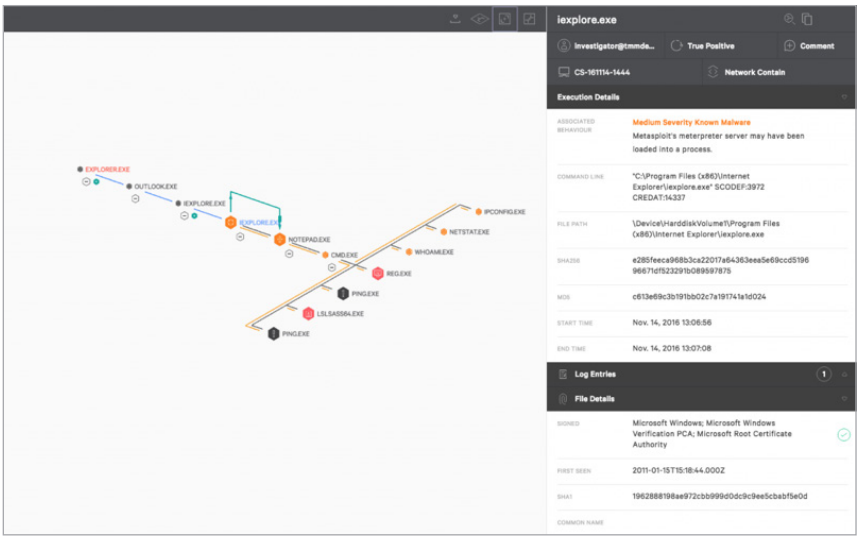
1.1　EDR的产生

Gartner分析师Anton Chuvakin于2013年创造出终端侦测与响应系统理念，目的是为了满足端点(服务器、台式电脑、笔记本与平板电脑)对于APT攻击的防护需求，最主要是大幅提升安全监控、威胁侦测及应急响应能力。这些工具记录数量可观的端点与网络事件，并将这些信息集中存储在一个数据库内。然后利用分析工具来搜索数据库，寻找可提升安全状态并防范一般攻击的工具，及早发现网络攻击，当然也包括内部威胁(比如，内网中有个管理员的账号失窃了，这个时候被用于内网网络攻击。也希望通过EDR这款产品能够迅速的调查出内网所受攻击的范围)，快速应对这些攻击。这些工具还有助于迅速调查攻击的范围，并提供补救措施。

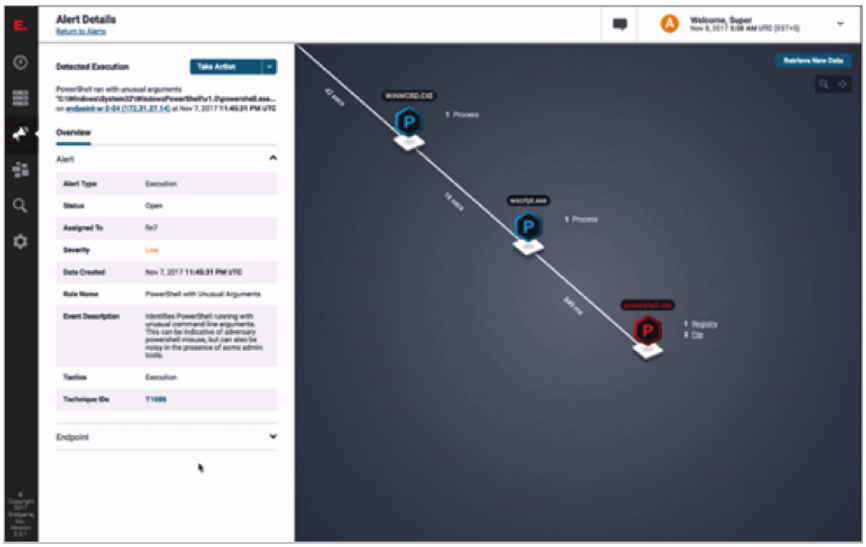
EDR保护的对象是终端，包括PC、服务器、虚拟化主机，解决更高级的网络威胁等问题，如未知威胁、恶意代码、APT攻击等。

终端侦测与响应系统(EDR)目前成为全球范围内增长速度最快的安全产品，系统集成包含大数据(架构方面)、人工智能(安全基线)、机器学习(行为模型)，威胁情报(溯源取证)，数据分析等一大批新兴技术。

目前世界上专门做EDR的厂商，包括CrowdStrike、CarbonBlack、Cybereason、Endgame等



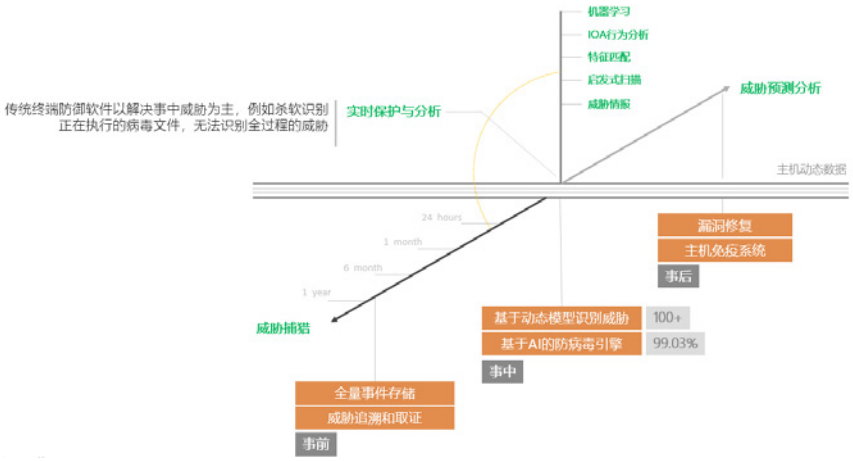
CrowdStrike厂商EDR产品



Endgame厂商EDR产品

并且在市场预测方面，Gartner预测，到2020年有80%的大型企业，25%的中型企业，以及10%的小型企业将投资部署EDR。

1.2 EDR的真实防御原理



在防御理念方面来说，EDR经常会做与杀毒软件的比较？实际上在威胁检测逻辑方面(或者说黑客真实的攻击过程中)。可以看成是一个“长程”的线条(注：安全业界最早量化的是美国洛克希德·马丁公司定义的“七步杀伤链”，而目前最具权威的攻击模型普遍认为是MITRE ATT&CK攻击矩阵(也可认为是一种知识库))。有些攻击事件已经发生过去了，有些正在发生，有些可能发生。而杀毒软件主要解决的是实时保护的问题。就是当前碰到了一个文件，杀软发现了。这个文件是病毒还是不是病毒。它能够马上判断，并付诸于处置(杀掉)。但杀软在整个的攻击链条里边，占的比重比较少(仅仅是在事中的某一个环节)。

而杀软还存在相当大的缺陷，比如1、更新最新的病毒&威胁特征相对比较滞后。杀软中的“快速查杀”功能是快速匹配文件的“安全证书”，但“安全证书”是可以在“黑市”上购买的(1个卡巴斯基的证书大概在700$~1000$，微软的证书在10000$~15000$)。如果这样的“恶意文件”(应用合法的证书)在快速检测的时候，很容易被放行(安全业界叫免杀或是绕过)。所以世界范围内普遍认为杀软的检测率最高不超过85%。这就不得不提到另外一个攻击话题，“无文件攻击”

1.2.1 无文件攻击

无文件攻击也就是非恶意软件攻击，攻击者利用这种技术实施攻击时，不会在目标主机的磁盘上写入任何的(含有实体本体)的“恶意文件”，因此而得名“无文件攻击”。

简单说，黑客通过利用奇技淫巧，把程序运行到被攻击主机的“内存”中，从而长期剥削被害主机的操作系统的行为。只因为“不落地”(没有任何的一个实体恶意文件

落到磁盘中)，因此得名“无文件攻击”。例如：一个钓鱼邮件打过来，被害者不小心点击了邮件附件的word或是excel(附件里仅仅记载了“下一季度的工作计划”)。但攻击者利用office漏洞，在后台内存中加载cmd或powershell。目的有四，1、修改注册表&系统文件 2、提权 3、查看内网及主机信息(相当于窃密) 4、远端恶意url连接c&c。整个过程你可以发现，没有任何的实体恶意文件存在。靶标主机就别拿下了。而无文件攻击也是APT过程中，“隐藏性、隐蔽性”最好的贡献者。是自2016年以来，黑客组织非常善于应用的攻击方式。

1.2.2 EDR 防御

而EDR应用的技术是基于“行为模型”(就是主机里的进程、网络通讯、注册表、服务等)对主机中的异常进行检测。比如：如下图：

并应用到安全模型、大数据、AI人工智能、威胁情报分析等，进行积极防御。并且通过全量存储的“行为”数据对攻击进行溯源以及取证。

特点1：利用“行为模型”，当发现主机中存在修改系统文件、修改注册表、建立反弹shell、无文件攻击脚本py调用主机后台进程时(如上图)，甚至像勒索等瘫痪性攻击爆发时，发起大量lucky.exe等加密动作时。EDR会直接拦截掉“威胁进程”，而非杀死源文件(如果当业务系统被感染时)。有效降低误伤业务等风险。

特点2：安全建模&AI能力，AI主要指的是机器学习+深度学习。机器学习两部分(1、训练。2、推理)。通过大量(次数、事件(半年、一年))的训练，最终建立模型(生成的模型放到EDR行为规则中),在下次威胁行为检测时，只需要花(0.5ms、1ms)、就能够完成“推理”的过程),从七步杀伤链的角度，就是不用攻击者到达最后一步(对终端进行恶意操作)，只需要通过“模型”匹配到攻击者攻击的前2个步骤，即可判断威胁存在。

特点3：EDR还拥有Auto-baseline、恶意软件检测(Powershell/CMD/WMI/JJS/PHP/JSCRIPT)、实时本地沙箱(对病毒诱导沙箱进行隔离分析)、终端数据恶意与恢复等能力

以上为总结EDR特点及核心防御能力。

90 亿信用卡曝出协议漏洞：黑客无需密码即可盗刷

2020-09-07

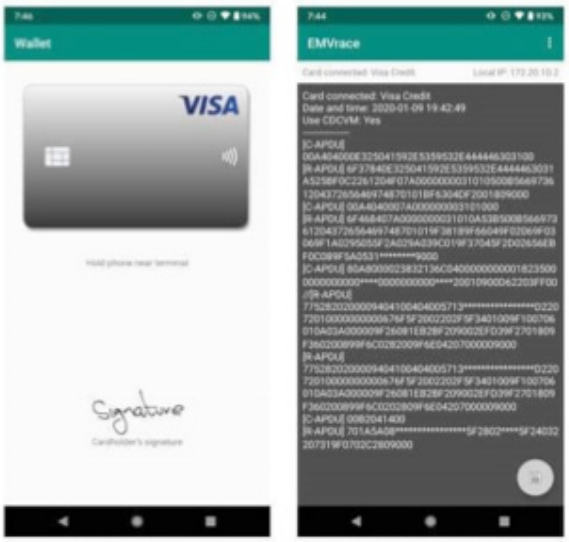
摘要：每次我们使用信用卡/借记卡付款时，收款机都会使用 EMV 通信协议来处 理付款。该协议由 Europay，Mastercard 和 Visa 等公司开发，目前在全球超过 90 亿张卡中使用。

关键词：标签(信用卡、协议漏洞、黑客盗刷)，技术问题(安全事件)。

内容：最近，来自苏黎世联邦理工学院计算机科学系的 3 名研究人员，即 David Basin，Ralf Sasse 和 Jorge Toro-Pozo 发现了 EMV 协议中的漏洞，该漏洞使攻击者 可以实施中间人攻击(MITM)，进行欺诈性交易。

通过一个模型来模拟商家机器、用户卡和银行的真实情况，研究人员找到 2 个主要漏洞。首先，他们开发了一个 Android 应用程序概念验证(POC)漏洞，当用于非 接触式支付时，攻击者可以在不使用任何 PIN 码的情况下进行攻击。

该攻击能够得手的原因是持卡人验证方法中缺少身份验证和加密技术，攻击者可 以根据自己的需要修改设置。例如，研究人员还成功进行了这样的交易(下图)，价值 190 美元，可以使用自己的卡在真实商店中进行了现场测试。



(a) Card emulator (b) POS emulator

Fig. 4. Screenshots of our app. The card emulator may display the cardholder's signature, in which case, it should match the attacker's signature. The log displayed in the POS emulator corresponds to a real transaction of ca. $190 in the local currency.

第二个漏洞使攻击者诱使商家认为现场的脱机非接触式交易已成功，攻击者离开后才发现该交易已被拒绝。在他们的报告 [PDF]中，研究人员解释说：

在使用 Visa 或旧的万事达卡进行的离线非接触式交易中，该卡不会向终端认证 应用密码(AC)，这使犯罪分子可以欺骗终端以接受未经认证的离线交易。后来，当收单行将交易数据作为清算记录的一部分提交时，发卡行将检测到错误的密码，但罪犯早已得手而去。

综上所述，可以通过直接全局更新终端系统而不是 EMV 协议本身来修复这 2 个漏 洞。但是，考虑到大约有 1.61 亿个这样的终端，其中许多位于技术落后的国家，可能需要花费大量时间才能避免此类漏洞被犯罪分子利用。

信息来源: https://www.aqniu.com/industry/69820.html

江苏盐城网警破获特大第四方支付网络黑产案

摘要：近日，盐城网安会同经济开发区分局快侦快破，同时打掉两个专门为非法 网络彩票和跨境网络赌博平台提供支付渠道的网络黑产犯罪团伙，成功斩断 47 家非 法网络赌博、彩票网站资金链，抓获犯罪嫌疑人 29 名，涉案资金流水达 7.2 亿余元。 这是江苏盐城警方在公安部部署开展的“净网 2020”专项行动中取得的又一突出战果。

关键词：标签(第四方支付、黑产)，技术问题(安全事件)。

内容：网上买“彩票”百万打水漂，接待民警嘴皮磨破

今年 8 月 17 日上午 9 时许，盐城市公安局经济技术开发区分局来了一位的特殊 的“客人”。这位“客人”名叫孙某，今年 29 岁，老家在山东枣庄，现在北京某公 司工作。

孙某为何从北京来盐城向警方“求助”呢?原来，8 月 13 日，他突然发现一直 正常使用的银行卡、微信、支付宝等账号都被冻结了。之后，孙某收到短信通知，因涉及赌博网站的非法交易，盐城警方根据涉赌资金流向对有关联交易的 8000 余个资 金账户依法实施冻结，孙某的账户就在其中。

孙某告诉民警，他这些年接触的网络赌博、彩票网站比较多的。今年年初，他的 QQ 里收到一条广告消息，称下载“百发彩票”App，可在线购买彩票。平时喜欢在彩 票店购买的孙某觉得这个网站“有点意思”，便登录该网站并注册成为会员。

为尽快将账户解冻，孙某只好乘车来盐城，主动向警方讲明情况。像这样的客人 来了一波又一波，民警逐一耐心的解释劝导。

案件详情

近日，盐城市公安局网安支队在日常巡查工作中发现一家名为“百发彩票”的平 台涉嫌网络赌博等非法交易，立即会同经济技术开发区分局成立专案组展开侦查。

百发彩票平台该平台表面上是一个彩票网，具有的品种除了香港的六合彩，其他 都跟彩票店里在售的一样，但他其实是一个网络赌博网，他从彩票中衍生出很多玩法， 像快三可以赌大小、猜单双的等赌博方式。

顺藤摸瓜

警方顺藤摸瓜，发现这家名叫百发彩票平台同时使用“蜂王”“TL”两家第四方 支付平台为其提供充值提现渠道。经查，“蜂王”“TL”两个团伙分别在境内外租赁 多个阿里云服务器，搭建支付结算系统，使用掌握的数千张银行卡，专门为各类境外

赌博网站提供充值通道接口服务，日结算金额超百万元。仅 TL 一家，5 月份到 7 月 份就达 1.6 亿元。

Q&A:什么是第四方支付?

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”。

警方从人员流、信息流、资金流三方面同时展开调查，摸清了以宋某、刘某为首 涉嫌帮助信息网络犯罪的“蜂王”“TL”第四方支付平台组织框架、运作模式和嫌疑 人的落脚点，梳理出涉案银行账户、支付宝、微信账户 8000 余个。

绳之以法

8 月 13 日，警方组织近百名警力，组成 3 个抓捕小组，同时在山东 菏泽、广东 深圳、福建厦门 3 地展开抓捕行动，一举抓获犯罪嫌疑人 32 名，扣押涉案电脑 13 台、手机 34 部、银行卡 600 余张。于此同时，警方的网安民警迅速冻结涉案的银行、微信、支付宝账户。据统计，警方共冻结银行账户 1391 个，微信、支付宝账户 246 个，冻结资金 1200 多万元。

目前，警方初步查明该案涉案资金流水达 7.2 亿元，刑事拘留 12 人，此案正在 进一步审理侦查之中。

信息来源:

https://mp.weixin.qq.com/s/j1F0k7_gmHw-9yuKfK_QKw

新型内幕交易曝光，股民用木马窃取基金公司交易指令 12 年！

摘要：朱某海从 2004 年到 2016 年 12 年间，利用高超的木马病毒技术，入侵了 2474 台电脑，获取华夏基金等多家基金公司的交易指令，据此操作，获利 183 万余 元。此外，他还在 2009 年利用木马病毒，从中信证券获取多条内幕信息，获利近 2 万元。

关键词：标签(内幕交易、木马、基金公司)，技术问题(安全事件)。

内容：朱某海，从 2004 年到 2016 年 12 年间，利用高超的木马病毒技术，入侵 了 2474 台电脑，获取华夏基金等多家基金公司的交易指令，据此操作，获利 183 万 余元。此外，他还在 2009 年利用木马病毒，从中信证券获取多条内幕信息，获利近 2 万元。

朱某海的行为，该怎么定罪，引起了争议。

一审葫芦岛中院以非法获取计算机信息系统数据、非法控制计算机系统罪、内幕 交易罪，数罪并罚，决定执行有期徒刑三年一个月，并处罚金 1809.8 万元。

但是，这一处罚决定引起检方及被告人双双上诉，检方觉得罚轻了，应该 5 年以 上 10 年以下;朱某海则觉得罚重了。

你怎么看?

浙江高庭律师事务所合伙人汪建峰律师，在接受证券时报记者采访时表示:首先，国家对证券市场违法违规行为管控越来越严格是必然趋势，对恶性违法违

规行为保持“零容忍”，必然导致打击力度提高，随之带来证券类的新型犯罪在司法 实践中将会越来越普遍。

其次，证券类的新型犯罪往往一个行为侵犯多个客体，比如本案中实施的犯罪行 为本质上是谋取非法利益，但实施的行为却被定性为非法获取计算机信息系统数据、 非法控制计算机系统罪和内幕交易罪多个罪名，实际上侵害的是公共秩序和金融管理 秩序两个客体。也就是说这类新型的证券类犯罪在打击的时候很有可能构成多个罪名，在司法实践中进行数罪并罚是常态，犯罪成本相对于普通犯罪要高很多。

再次，国家对证券市场监管越来越严格的大方向配合司法层面的打击措施，必将 对净化市场，引导证券市场健康稳定发展起到积极的作用。

12 年入侵 2474 台电脑

12 年，2474 台电脑，获利 180 多万.....这些信息堆积在一起，引发网友的最大 吐槽居然是:平均每年赚 10 多万，正经上个班也比这强，有这技术干点别的不好吗?

据葫芦岛市中级人民法院一审经审理查明:

2004 年至 2016 年间，被告人朱某海制作并使用木马病毒非法侵入、控制他人计 算机信息系统，非法获取相关计算机信息系统存储的数据。其间，其非法控制计算机 信息系统 2474 台，利用从华夏基金管理有限公司等多家基金公司计算机系统内非法 获取的交易指令，进行相关股票交易牟利，总计获得违法所得 1835730.27 元。

2009 年间，被告人朱某海利用木马病毒从中信证券股份有限公司非法获取了《中 信网络 1 号备忘录——关于长宽收购协议条款》等多条内幕信息，在相关内幕信息敏 感期内与对应敏感信息相关的股票交易，获取违法所得人民币 19687.95 元。

令人细思极恐的是，在长达 12 年的时间里，基金公司的交易指令竟然长期被木 马病毒“偷窥”而不自知!这个案件的曝光，对于金融机构的信息系统安全是一次警示。

一审后检方与被告双双上诉

一审时，葫芦岛中院以被告人朱某海犯非法获取计算机信息系统数据、非法控制 计算机系统罪、内幕交易罪，数罪并罚，决定执行有期徒刑三年一个月，并处罚金 1809.8 万元。

但是，葫芦岛市人民检察院认为，被告人朱某海所犯内幕交易罪行属于情节特别 严重的情形，应判处五年以上十年以下有期徒刑，提出抗诉。

同时，被告人朱某海也提出了上诉，主要理由是罚金数额过高，此外非法获取计 算机信息系统数据、非法控制计算机系统罪与内幕交易罪，应属牵连犯而择一重罪处罚。

于是，近日辽宁省高级人民法院公开开庭审理此抗诉、上诉一案。被告人朱某海 及其辩护人到庭参加诉讼。庭审中，控辩双方就上述争议焦点、认定事实及适用法律 充分发表了意见。对此，辽宁高院认为本案系证券期货类新型犯罪，案件疑难、复杂，将择期宣判。

广东奔犇律师事务所主任刘国华律师表示，该案主要是获取内幕信息的手段比较 特别。不过万变不离其宗，被告人涉嫌通过新型手段获取内幕信息，然后通过内幕交 易获利。被告人最后获刑多久，还是要看相关证据以及法律规定。

刑法规定，内幕交易情节特别严重的，最高刑期可达 10 年。今年 3 月起施行的 新《证券法》第一百九十一条则规定，内幕交易可处以违法所得一倍以上十倍以下的罚款。

持续加大对内幕交易的打击力度

虽然像朱某海这样，直接利用病毒技术盗用数据，构成泄露内幕信息的比较罕见。 但内幕交易在 A 股并不鲜见，一段时间以来，由于惩罚不够严格，导致该罪呈现低成 本、高收益特征。近年来监管部门正极力消除这一现象，大力加强投资者保护。

据统计，2019 年证监会共下发 136 份行政处罚书以及 13 份市场禁入决定书，涉 及内幕交易的案件多达 55 件，占比超过 40%。2020 年至今，证监会和地方证监局累 计发出 156 张行政处罚决定书，涉及内幕交易的罚单 50 张，占全部罚单数量的 32.05%。

9 月 18 日，时隔 7 个月证监会重启现场发布会，证监会新闻发言人常德鹏通报 了吴某某等人涉嫌内幕交易“王府井”股票案的情况。

常德鹏表示，内幕交易是资本市场的“顽疾”，严重破坏公平交易原则，侵害投 资者合法权益。2019 年修订的证券法显著提高了包括内幕交易在内的证券违法违规 成本。证监会将全面落实国务院金融委关于对资本市场违法行为“零容忍”的工作要求，着力构建行政处罚、刑事追责、民事赔偿等全面化、立体式的追责体系，持续加 大对内幕交易、财务造假等违法行为打击力度，切实维护资本市场秩序，保护投资者 合法权益。

值得一提的是，当天，证监会还就《关于上市公司内幕信息知情人登记管理制度 的规定(征求意见稿)》公开征求意见。征求意见稿主要修订以下方面内容:

一是落实新《证券法》规定，根据新《证券法》，进一步明确内幕信息知情人、内幕信息的定义和范围。

二是压实上市公司防控内幕交易的主体责任规定董事长、董事会秘书等应当对内 幕信息知情人档案签署书面确认意见;要求上市公司根据重大事项的变化及时补充报 送相关内幕信息知情人档案及重大事项进程备忘录。

三是强化证券交易所在内幕交易防控方面的职责。授权证券交易所对上市公司内 幕信息知情人档案填报所涉重大事项范围填报具体内容、填报人员范围，对需要制作 重大事项进程备忘录的事项、填报内容等作出具体规定;同时要求证券交易所应当将 内幕信息知情人档案及重大事项进程备忘录等信息及时与证监会及其派出机构共享。

四是明确中介机构的配合义务。要求证券公司、律师事务所等证券服务机构协助 配合上市公司及时报送内幕信息知情人档案及重大事项进程备忘录，并依照相关执业 规则的要求对相关信息进行核实。

3 月 1 日施行的新《证券法》，也明确内幕交易行为给投资者造成损失的，必须依法承担赔偿责任。

随着相关法律制度完善，惩罚标准趋严，以及技术手段逐步提高，尤其是大数据 时代来临，监管部门针对内幕交易等违法犯罪行为有更强的侦查能力，内幕交易这一 资本市场顽疾有望逐步得到治理。

信息来源:

https://baijiahao.baidu.com/s?id=1678683705406630543&wfr=spider&for=pc

NSFOCUS

漏洞聚焦

【更新 - 出现 EXP】Microsoft SQL Server Reporting Services 远程代码执行漏洞（CVE-2020-0618）安全通告

发布时间：2020 年 9 月 18 日

综述

微软发布的2月安全更新中修复了一个Important级别的漏洞，该漏洞是存在于 Microsoft SQL Server Reporting Services(SSRS)中的远程代码执行漏洞（CVE-2020-0618）。近日，监测到网上有Exp出现。

SSRS应用中的功能允许经过身份验证的攻击者向受影响的Reporting Services实例提交精心构造的HTTP请求，利用应用中的反序列化问题在受影响的服务器上执行代码。

尽管只有授权用户才能访问该应用程序，但使用最低权限（Browser角色）足以利用该漏洞。

SQL Server Reporting Services (SSRS)是微软基于服务器的报表生成软件，它是Microsoft SQL Server服务套件的一部分，通过Web界面进行管理，可用于准备和交付各种交互式报告。

参考链接：

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0618

受影响产品版本

- ☐ Microsoft SQL Server 2012 Service Pack 4（QFE）
- ☐ Microsoft SQL Server 2014 Service Pack 3（CU）
- ☐ Microsoft SQL Server 2014 Service Pack 3（GDR）
- ☐ Microsoft SQL Server 2016 Service Pack 2 (CU)
- ☐ Microsoft SQL Server 2016 Service Pack 2 (GDR)

解决方案

由于攻击者可通过对请求数据包编码绕过Web应用防火墙的防护，强烈建议用户安装补丁进行修复。

微软官方已为受支持版本发布了针对该漏洞的安全补丁，请参阅微软官方通告及时下载安装。

注意：如果您使用的SQL Server是下表中未显示的版本，则表示所用版本已不再受支持。请更新Service Pack或SQL Server产品，以应用安全更新。

产品	版本	更新编号
SQL Server 2016 Service Pack 2 (GDR) 安全更新	13.0.5026.0 - 13.0.5101.9	KB4532097
SQL Server 2016 Service Pack 2 CU11 安全更新	13.0.5149.0 - 13.0.5598.27	KB4535706
SQL Server 2014 Service Pack 3 (GDR) 安全更新	12.0.6024.0 - 12.0.6108.1	KB4532095
SQL Server 2014 Service Pack 2 CU4 安全更新	12.0.6205.1 - 12.0.6329.1	KB4535288
SQL Server 2012 Service Pack 4 (QFE) 安全更新	111.0.7001.0 - 11.0.7462.6	KB4532098

同时，建议禁止匿名访问，确保只有经过身份验证的用户才能访问相关应用。如果怀疑服务器已经受到威胁，除安装相应补丁外，请及时更改服务器的账户口令，防止被攻击者利用。

官方通告：

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0618

声明

IBM Spectrum Protect Plus 任意代码执行漏洞 (CVE-2020-4703) 安全通告

发布时间：2020 年 9 月 16 日

综述

近日，IBM 发布安全公告，公布了存在于IBM Spectrum Protect Plus中的任意代码执行漏洞(CVE-2020-4703)。该漏洞允许经过身份验证的攻击者上传任意文件，这些文件可在易受攻击的服务器上执行任意代码。CVE-2020-4703是由于对先前6月披露的CVE-2020-4470不完整修复造成的。

一同公布的还有目录遍历漏洞CVE-2020-4711，利用该漏洞，攻击者通过发送包含序列(/../)的特殊URL请求可以查看到系统中的任意文件。

官方已发布了临时修订版本。

目前，网上已有关于漏洞的分析和PoC出现。

IBM® Spectrum Protect™ Plus 是用于虚拟环境的数据保护和可用性解决方案。

参考链接：

https://www.ibm.com/support/pages/node/6328867

受影响产品版本

- IBM Spectrum Protect Plus 10.1.0-10.1.6

不受影响产品版本

- IBM Spectrum Protect Plus 10.1.6 ifix4

解决方案

官方已发布临时修订版本，且针对以上漏洞并未有其他缓解措施，介于已有详细分析和PoC出现，建议相关用户尽快更新进行防护。

更新连接：https://www.ibm.com/support/pages/node/6254732

Microsoft Exchange Server 远程代码执行漏洞 (CVE-2020-16875) 安全通告

发布时间：2020 年 9 月 15 日

综述

微软发布的9月安全更新中修复了一个Critical级别的漏洞，该漏洞是存在于 Microsoft Exchange Server 中的远程代码执行漏洞（CVE-2020-16875）。近日，发现网上有PoC出现。

由于对cmdlet参数的验证不正确，攻击者可能会通过向受影响的 Exchange 服务器发送包含特殊 cmdlet 参数的邮件来触发此漏洞，成功利用此漏洞的攻击者能够在受影响的系统上以 system 权限执行任意代码。值得注意的是，能成功利用漏洞的前提是拥有能以某个 Exchange 角色进行身份验证的用户权限。

参考链接：

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16875

受影响产品版本

- ☐ Microsoft Exchange Server 2016 Cumulative Update 16
- ☐ Microsoft Exchange Server 2016 Cumulative Update 17
- ☐ Microsoft Exchange Server 2019 Cumulative Update 5
- ☐ Microsoft Exchange Server 2019 Cumulative Update 6

解决方案

微软已经在月度安全更新中修复了上述漏洞，介于已有PoC出现，强烈建议用户尽快下载更新进行防护。

官方通告：

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16875

Spring Framework 反射型文件下载漏洞 (CVE-2020-5421) 安全通告

发布时间：2020 年 9 月 19 日

综述

近日，VMware Tanzu发布安全公告，公布了一个存在于Spring Framework中的反射型文件下载（Reflected File Download,RFD）漏洞CVE-2020-5421。CVE-2020-5421 可通过jsessionid路径参数，绕过防御RFD攻击的保护。先前针对RFD的防护是为应对 CVE-2015-5211 添加的。

攻击者通过向用户发送带有批处理脚本扩展名的URL，使用户下载并执行文件，从而危害用户系统。

官方已发布修复了漏洞的新版本。

Spring Framework是 Java 平台的一个开源全栈应用程序框架和控制反转容器实现，一般被直接称为 Spring。

参考链接：

https://tanzu.vmware.com/security/cve-2020-5421

受影响产品版本

- ☐ Spring Framework 5.2.0 - 5.2.8
- ☐ Spring Framework 5.1.0 - 5.1.17
- ☐ Spring Framework 5.0.0 - 5.0.18
- ☐ Spring Framework 4.3.0 - 4.3.28
- ☐ 以及其他已不受支持的版本

不受影响产品版本

- ☐ Spring Framework 5.2.9
- ☐ Spring Framework 5.1.18
- ☐ Spring Framework 5.0.19
- ☐ Spring Framework 4.3.29

解决方案

官方已发布修复了漏洞的新版本，建议相关用户尽快升级进行防护。

下载链接：

https://github.com/spring-projects/spring-framework/releases

另外，针对 RFD 攻击，官方曾在 CVE-2015-5211 的通告中给出如下建议(https://tanzu.vmware.com/security/cve-2015-5211)：

1、编码而不是转义JSON响应。具体操作详见 https://github.com/rwinch/spring-jackson-owasp。

2、将后缀模式匹配配置为关闭或仅限于显式注册的后缀。

3、配置内容协商时，将 "useJaf "和 "ignoreUknownPathExtension "属性设置为false，这将导致未知扩展名的URL得到406响应。但请注意，如果URL本来会在结尾处有一个点，就不要使用该项。

4、在响应中添加 "X-Content-Type-Options: nosniff "头。

Yii2 反序列化远程命令执行漏洞(CVE-2020-15148)防护方案

发布时间：2020 年 9 月 20 日

一、综述

近日监测到，Yii Framework 2 在其 9月14 日发布的更新日志中公布了一个反序列化远程命令执行漏洞(CVE-2020-15148)。

官方通过给yii\db\BatchQueryResult类加上__wakeup()函数，禁用了yii\db\BatchQueryResult的反序列化，阻止了应用程序对任意用户输入调用'unserialize()’造成的远程命令执行。

Yii2 是一个高性能，基于组件的开源 PHP 框架，用于快速开发现代 Web 应用程序。

目前，官方已发布修复了漏洞的新版本。绿盟科技检测防护产品已针对该漏洞提供能力，建议相关用户尽快采取防护措施。

参考链接：

https://github.com/yiisoft/yii2/blob/928b511d75ee719cd4007f220eafce9eab4d1b4a/framework/CHANGELOG.md

https://github.com/yiisoft/yii2/security/advisories/GHSA-699q-wcff-g9mj

二、漏洞影响范围

☐ Yii2 Version < 2.0.38

三、技术防护方案

3.1 官方修复方案

官方已发布修复了漏洞的新版本2.0.38。

下载链接：

https://github.com/yiisoft/yii2/releases/tag/2.0.38

3.2 绿盟科技检测防护建议

3.2.1 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

3.2.1.1 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 web 插件	V6.0R02F00.1816
WVSS	V6.0R03F00.182
IDS	5.6.9.23576、5.6.10.23576
UTS	5.6.10.23576

3.2.2 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）、下一代防火墙系统（NF）、Web应用防护系统（WAF）来进行防护。

- 入侵防护系统（IPS）

  http://update.nsfocus.com/update/listIps
- 下一代防火墙系统（NF）

  http://update.nsfocus.com/update/listNf
- Web应用防护系统（WAF）

  http://update.nsfocus.com/update/wafIndex

3.2.2.1 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	5.6.9.23576、5.6.10.23576	25037
NF	6.0.1.828、6.0.2.828	25037
WAF	6.0.7.0.46432、6.0.7.1.46432	27005015

四、附录 产品/平台使用指南

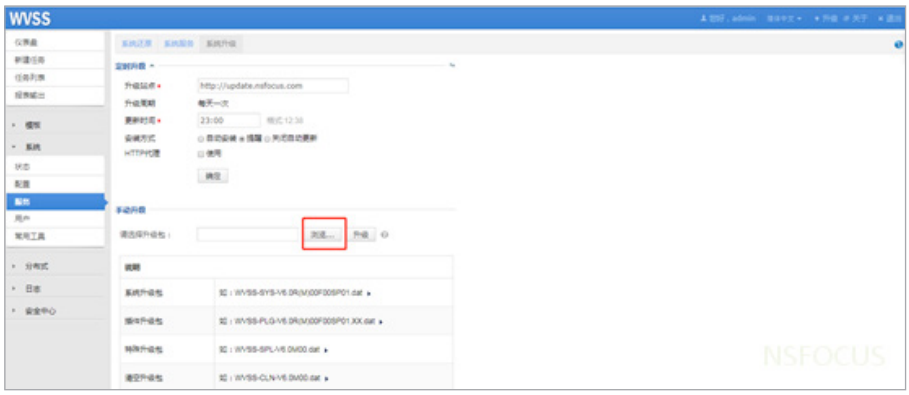
4.1 RSAS扫描配置

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，针对此漏洞进行扫描。

4.2 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：



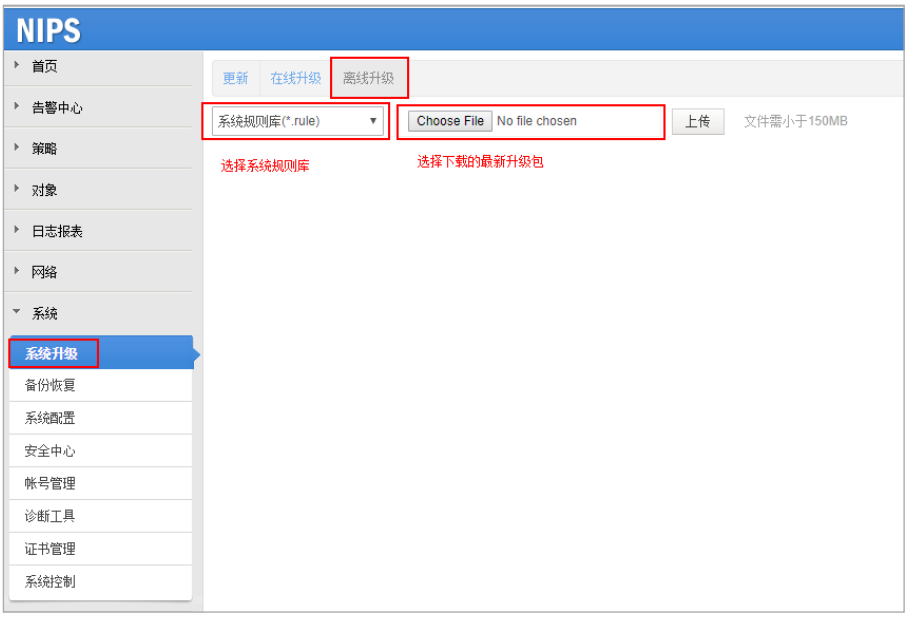
选择下载好的相应升级包，点击升级按钮进行手动升级。等待升级完成后，可通过定制扫描模板，针对此次漏洞进行扫描。

4.3 UTS检测配置

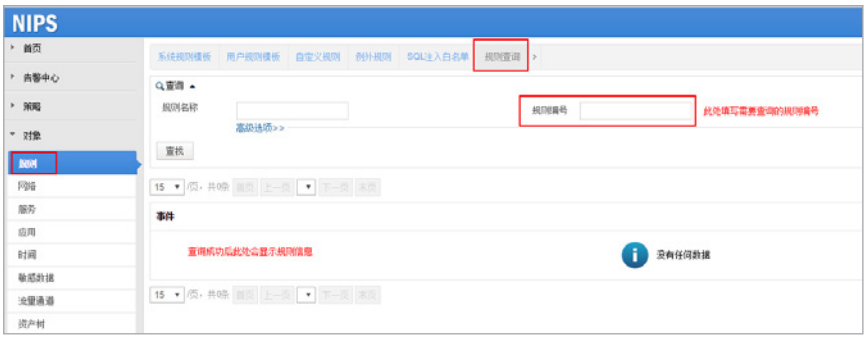
在系统升级中点击离线升级，选择规则升级文件，选择对应的升级包文件，点击上传，并等待升级成功即可。

4.4 IPS防护配置

1. 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。



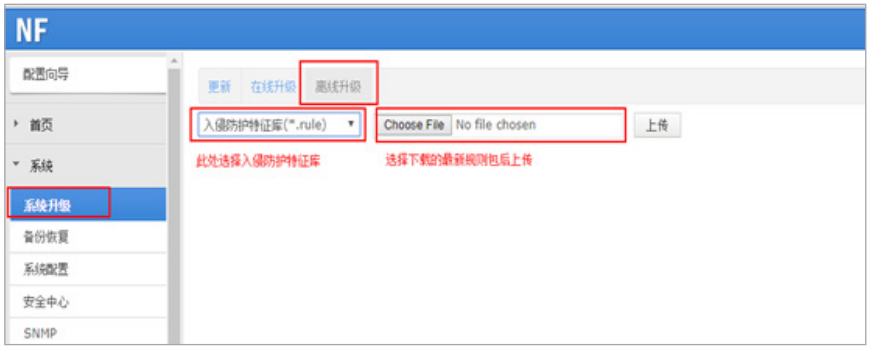
2. 更新成功后，在系统默认规则库中查找规则编号，即可查询到对应的规则详情。



注意事项：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。

4.5 NF防护配置

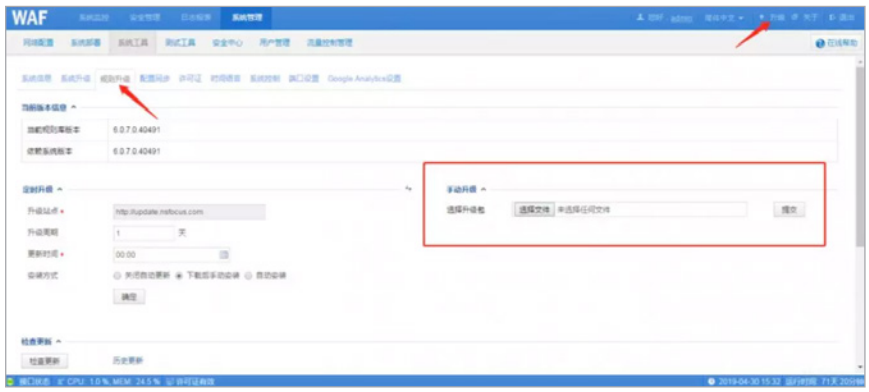
在 NF 的规则升级界面进行升级：



手动选择规则包，提交即可完成更新。

4.6 WAF防护配置

在WAF的规则升级界面进行升级：



手动选择规则包，提交即可完成更新。

声明

本安全公告仅用来描述可能存在的安全问题，绿盟科技不为此安全公告提供任何保证或承诺。由于传播、利用此安全公告所提供的信息而造成的任何直接或者间接的后果及损失，均由使用者本人负责，绿盟科技以及安全公告作者不为此承担任何责任。绿盟科技拥有对此安全公告的修改和解释权。如欲转载或传播此安全公告，必须保证此安全公告的完整性，包括版权声明等全部内容。未经绿盟科技允许，不得任意修改或者增减此安全公告内容，不得以任何方式将其用于商业目的。

NSFOCUS

安全态势

互联网安全威胁态势

行业动态回顾

1. 跨平台挖矿木马MrbMiner已控制上千台服务器

【概述】

新型挖矿木马家族MrbMiner，黑客通过SQL Server服务器弱口令爆破入侵，爆破成功后在目标系统释放C#语言编写的木马assm.exe，然后下载门罗币挖矿木马并维持挖矿进程。

【参考链接】

https://s.tencent.com//research/report/1105.html

2. KryptoCibule：多任务多货币密码窃取程序

【概述】

ESET研究人员发现了迄今未记录的恶意软件家族，命名为KryptoCibule。就加密货币而言，这种恶意软件是三重威胁。它使用受害者的资源来挖掘硬币，尝试通过替换剪贴板中的钱包地址来劫持交易，并泄漏与加密货币相关的文件，同时部署多种技术来避免检测。

【参考链接】

https://www.welivesecurity.com/2020/09/02/kryptocibule-multitasking-multicurrency-cryptostealer/

3. 文件管理器插件中的严重漏洞影响700k WordPress网站

【概述】

WordPress插件文件管理器已更新，修复了一个严重漏洞，该漏洞使任何网

站访问者都能完全访问该网站。

【参考链接】

https://blog.sucuri.net/2020/09/critical-vulnerability-file-manager-affecting-700k-wordpress-websites.html

4. 美国大选在即，黑客频繁攻击特朗普的竞选网站

【概述】

据路透社12日报道，在美国11月大选前夕，黑客正在加紧攻击特朗普的竞选网站和商业网站，并使其下线。为特朗普竞选工作的一家安全公司Cloudflare表示，这可能是在为更大规模的数字攻击做准备。

【参考链接】

http://mp.weixin.qq.com/s?__biz=MzI4MjA1MzkyNA==&mid=2655310786&idx=1&sn=9f5b4c48b39cd59edeb5b2379472cc14&chksm=f02faf89c758269f9c79139c28f9801b511ce37aba78825c69e0e42134b3870ffd7f0a2aa8cb#rd

5. 伊朗国家级APT：Pioneer Kitten组织公然兜售企业网络访问权限

【概述】

近日，一个与伊朗有关的APT组织Pioneer Kitten（先锋小猫），正在黑客论坛上公开售卖相关企业的网络凭证信息。该组织自2017年以来一直活跃，以窃取国家政府及相关实体的敏感情报信息为主，并努力获取并保持对这些情报信息端口的访问权限。 其攻击目标也相对明确，集中在伊朗比较感性的北美和以色列实体，具体行业包括：技术、政府、国防、医疗保健、航空、媒体、学术、工程、咨询和专业服务、化学、制造、金融服务、保险和零售行业等。

【参考链接】

https://www.anquanke.com/post/id/216449

6. 暗网市场Empire由于DDos攻击关闭数日

【概述】

暗网中的知名网站Empire Market已经关闭了数日，一些用户怀疑怀疑存在exit scam的问题，而另一些用户则在指责了网站出现的长时间分布式拒绝服务

攻击(DDoS)。Empire Market上售卖着许多的非法商品，包括违禁药物，化学药品，赝品，珠宝和信用卡号，并支持使用包括比特币（BTC），莱特币（LTC）和门罗币（XMR）在内的付款方式

【参考链接】

http://mp.weixin.qq.com/s?__biz=MzkyMzAwMDEyNg==&mid=2247499419&idx=3&sn=b9c32241fdf7afa806ddbb40d607c071&chksm=c1e972caf69efbdc3403e04bbeac180a7fc61094d9ccc075477d62ef86a7e4389c388f8defd3#rd

7. 三大银行因个人信用信息管理问题被处罚

【概述】

交通银行股份有限公司陕西省分行、兴业银行股份有限公司西安分行、浙商银行股份有限公司西安分行，这三家银行因违反《个人信用信息基础数据库管理暂行办法》的第39条而被处罚。无用账户、僵尸账户的存在，日常缺乏对这些账户的管理，很容易被黑客非法利用这些账户，潜入单位系统内部，非法获取到有用信息。

【参考链接】

http://mp.weixin.qq.com/s?__biz=MzU1ODM1Njc1Ng==&mid=2247488481&idx=1&sn=c48ff30d33c122effd36daa70a400d91&chksm=fc26939acb511a8c531c17cb8b1f5a20373f5f5790e071cff47d760365d8ad030f61113ac575#rd

8. 黑客可以通过智能手机来克隆你的锁钥匙

【概述】

新加坡国立大学计算机科学系的最新研究揭示了与智能锁相关的风险。研究人员可以使用特定软件和手机麦克风来克隆锁匙，并将攻击模型命名为SpiKey。利用SpiKey，可以塑造打开任何弹子锁的钥匙。如果黑客可以在您的智能手表，智能手机或智能门铃上安装恶意软件来录制音频，则攻击者可能无需物理上靠近锁即可进行攻击。

【参考链接】

https://www.hackread.com/hackers-clone-lock-keys-from-smartphone-clicks/

9．纽卡斯尔大学感染了DoppelPaymer勒索软件

【概述】

英国研究型大学纽卡斯尔大学感染了DoppelPaymer勒索软件，系统被迫于8月30日早上离线。DoppelPaymer勒索软件运营商声称对此负有责任。该团伙已经在其数据泄漏站点“Dopple Leaks”中泄漏了价值750Kb的被盗数据。该大学的IT人员宣布，攻击后需要数周的时间才能使服务恢复在线状态。

【参考链接】

https://securityaffairs.co/wordpress/108032/malware/newcastle-university-doppelpaymer-ransomware.html

10. Visa警告称，有新一轮“掠取者”瞄准电子商务网站

【概述】

Visa的支付反欺诈团队，警告说，最近发现了一个名为“ Baka”的数字分离器，该分离器正在从电子商务网站窃取支付卡数据，同时隐藏了安全工具。

【参考链接】

https://www.inforisktoday.com/visa-warns-fresh-skimmer-targeting-e-commerce-sites-a-14969

11. 贴有TiktokPro的间谍软件利用了对美国禁令的恐惧

【概述】

最近发现了一个新的Android间谍软件活动，该活动正在推广名为TikTok Pro的恶意应用程序，它利用了年轻用户对流行社交媒体应用程序在美国即将被禁止的担忧。该恶意软件可以接管基本的设备功能，例如捕获照片，阅读和发送SMS消息，拨打电话和启动应用程序，以及使用网络钓鱼策略窃取受害者的Facebook凭据。

【参考链接】

https://threatpost.com/spyware-labeled-tiktok-pro-exploits-fears-of-us-ban/159050/

12. 法国、日本和新西兰警告说，Emotet攻击会激增

【概述】

Emotet垃圾邮件活动激增，主要针对法国，日本和新西兰的企业。Emotet银行木马自2014年以来一直活跃，该僵尸网络由跟踪为TA542的威胁参与者操作。最近的垃圾邮件活动使用带有恶意Word文档或链接，伪装成发票，运送信息，COVID-19信息，履历，财务文档或扫描的文档。

【参考链接】

https://securityaffairs.co/wordpress/108060/malware/emotet-attacks-worldwide.html

13. 在线游戏黑客攻击暴增三倍

【概述】

第二季度在线游戏流量与第一季度相比增长了30%，而黑客入侵账户并窃取数字商品的尝试也同步增加。黑客最常见的攻击手法是账户复用，使用被盗密码登录账户是最常见的攻击方法。如果您在多个站点重复使用密码，并且一个站点被泄露，那么该密码可能最终会出现在黑客在黑市上购买的列表中。

【参考链接】

https://www.aqniu.com/industry/70063.html

14. Thanos勒索软件已将攻击目标转向了中东和北非的国有组织

【概述】

研究人员观察到与对中东和北非的两个国有组织的攻击有关的文件，这些组织最终安装并运行了Thanos勒索软件的变体。Thanos变体创建了一个文本文件，该文件显示赎金消息，要求受害者将2万美元转入指定的比特币钱包以恢复系统上的文件。

【参考链接】

https://www.4hou.com/posts/0ON7

15. Razer用户陷入数据泄露

【概述】

安全顾问鲍勃·迪亚琴科（Bob Diachenko）遇到了一个配置错误的Elasticsearch云集群，该集群将Razer的一部分基础架构暴露于公共互联网，任何人都可以看到。它包含大量的网络犯罪分子使用信息，包括全名，电子邮件，电话号码，客户内部ID，订单号，订单明细，账单和送货地址。

【参考链接】

https://threatpost.com/razer-gaming-fans-data-leak/159147/

16. 以色列芯片巨头遭网络攻击，暂停运转

【概述】

9月6日，以色列芯片巨头TowerJazz突然遭受网络攻击，部分系统服务器和制造部门暂停运转。据该公司的官方声明称，TowerJazz 已经组建了全球领先的技术团队，正在与执法部门紧密合作，力求尽快恢复遭网络攻击的系统。

【参考链接】

https://www.anquanke.com/post/id/216945

17. APT组织的下一个目标：Linux

【概述】

在过去的8年里，卡巴斯基全球研究与分析团队观察到，越来越多的APT组织开始针对运行Linux软件的设备。APT组织之所以将目标瞄准Linux，关键因素是容器化趋势推动了Linux的广泛采用。向虚拟化和容器化的转变使得大多数企业在

某些日常任务中都使用Linux，而这些设备通常可以从Internet访问，并且可以用作攻击者的初始入口点。此外，一些IT、电信公司和政府使用的Linux和macOS设备比Windows系统更多，这让攻击者别无选择。

【参考链接】

https://www.freebuf.com/news/249640.html

18. 交友网站用户的数据被泄露

【概述】

近期，数百名约会网站用户的个人详细信息在网上曝光。包含成千上万约会网站用户个人详细信息的Elasticsearch服务器未经身份验证就在线暴露。

【参考链接】

https://securityaffairs.co/wordpress/108239/data-breach/dating-site-data-leak.html

19. Malàsmoke盯上观看色情网站的你

【概述】

过去的几个月，一个名为Malàsmoke的网络犯罪组织，一直在攻击色情网站。该组织在成人主题网站上发布恶意广告，以达到重定向用户来利用工具包并分发恶意软件的目的。

【参考链接】

https://www.freebuf.com/news/249623.html

20. SunCrypt勒索软件袭击新泽西医院

【概述】

新泽西大学医院（UHNJ）显然是SunCrypt勒索软件的最新受害者。SunCrypt的运营商声称已获得240GB的数据，其中1.79GB已上传到其Darknet泄漏站点。

【参考链接】

https://www.binarydefense.com/threat_watch/suncrypt-ransomware-hits-new-jersey-hospital/

21. 威胁分析：新出现的URSA特洛伊木马影响许多国家使用先进的加载程序

【概述】

自2020年6月以来，新一轮的URSA木马（ESET的衍生产品，也被称为mispadu恶意软件）影响了来自多个国家的用户。该恶意软件是一种特洛伊木马恶意软件，当安装在受害者的设备上时，它会从浏览器以及流行的软件（例如FTP和电子邮件服务）中收集密码，并执行银行浏览器覆盖，以诱使受害者在执行流程时引入银行凭证–分步进行–在犯罪分子的后台。

【参考链接】

https://seguranca-informatica.pt/threat-analysis-the-emergent-ursa-trojan-impacts-many-countries-using-a-sophisticated-loader/

22. 美国对伊朗APT集团实施制裁

【概述】

周四，美国财政部外国资产控制办公室对伊朗高级持续威胁组织的恶意软件运动实施制裁，涉及到45名相关个人和伊朗政府用于针对伊朗持不同政见者，新闻工作者等。

【参考链接】

https://www.inforisktoday.com/us-imposes-sanctions-on-iranian-apt-group-a-15016

23. Dofloo（AESDDoS）僵尸网络正批量扫描、攻击Docker容器

【概述】

Dofloo（AESDDoS）僵尸网络正批量扫描和攻击Docker容器。部分云主机上部署的Docker容器没有针对远程访问做安全认证，存在Remote API允许未授权使用漏洞且暴露在公网，导致黑客通过漏洞入侵并植入Dofloo僵尸网络木马。

【参考链接】

https://s.tencent.com//research/report/1127.html

24. 不仅是高等教育：网络犯罪分子针对全球的学术和研究机构

【概述】

近几个月来，在美国，欧洲和亚洲，针对教育和研究领域的攻击数量有所增加。美国目睹了DDOS攻击的增加，而欧洲的信息泄露尝试也有所增加。与此同时，亚洲面临着更多的漏洞利用。

【参考链接】

https://blog.checkpoint.com//blog.checkpoint.com/2020/09/15/not-for-higher-education-cybercriminals-target-academic-research-institutions-across-the-world/

25. 严重漏洞允许黑客劫持Firefox Android浏览器

【概述】

Mozilla修复了一个漏洞，该漏洞可能使攻击者劫持共享同一Wi-Fi网络的任何Firefox Android浏览器。Firefox Android Web浏览器用户必须升级到Firefox Android应用程序的最新可用版本，以防止其设备被劫持。原因是攻击者可以利用此漏洞劫持同一网络上的所有Firefox Web浏览器。与GitLab相关的澳大利亚安全研究人员Chris Moberly 在较旧版本的Android手机Firefox Web浏览器的SSDP（简单服务发现协议）引擎中发现了一个远程命令执行漏洞。

【参考链接】

https://www.hackread.com/vulnerability-allowed-hackers-hijack-firefox-android-browser/

26. 案例研究：Emotet线程劫持，一种电子邮件攻击技术

【概述】

推动Emotet恶意软件的恶意垃圾邮件（malspam）是最常见的基于电子邮件的威胁，远远超过了其他恶意软件家族，只有少数其他威胁正在接近。近几周来，我们发现使用“线程劫持”技术的Emotet垃圾邮件数量明显增加，该技术利用了从受感染计算机的电子邮件客户端窃取的合法消息。此垃圾邮件欺骗了合法用户，并冒充了对被盗电子邮件的回复。线程被劫持的垃圾邮件将从原始邮件发送到地址。这种技术比许多人现已发现的不太复杂的方法有效得多。这种方法在说服潜在的受害者单击附件文件或单击链接以下载带有设计为用Emotet感染用户

的宏的恶意Word文档方面更为成功。在这里，我们回顾一个Emotet的线程劫持过程的案例研究，以便我们可以更好地认识和理解这种技术。

【参考链接】

https://unit42.paloaltonetworks.com/emotet-thread-hijacking/

27. TikTok危害国家安全？美国网络安全专家表示“看不懂”

【概述】

特朗普于8月6日发布禁止令的理由只有一个：基于中国的应用程序存在“国家安全问题”。而商务部长威尔伯·罗斯（Wilbur Ross）在新闻稿中还补充了一条“隐私侵犯”，因为这些应用程序允许“中国恶意收集美国公民的个人数据。”这个问题，从技术层面来说，只有网络安全和隐私保护的专业人士才最有发言权。近日，Threatpost搞了个美国网络安全专家研讨会，邀请了多位大咖发声，是目前为止从技术层面对TikTok和Wechat相关的安全和隐私话题最为专业的探讨。

【参考链接】

https://www.aqniu.com/industry/70308.html

28. Fort McCoy领导人审查了设施的大流行应对措施

【概述】

到2020年6月10日，陆军上校Michael D. Poss指挥Fort McCoy（威斯康星州）驻军时，他很可能是第一个在该国应对全球流行病时担任这一职务的人。波斯斯说：“今年春天，我和其他人一样都在经历这种大流行。”在来到麦考伊堡之前，他是堪萨斯州威奇托陆军后备中心第451远征维持司令部的参谋长。“我们可能正在经历与其他所有人正在处理的相同的事情。我们正在试图弄清楚如何在这种新环境中进行操作。”

【参考链接】

https://www.defense.gov/Explore/Features/Story/Article/2357161/fort-mccoy-leader-reviews-installations-pandemic-response/

29. 电子邮件传递的MoDi RAT攻击会粘贴PowerShell命令

【概述】

SophosLabs的研究人员Fraser Howard和Andrew O'Donnell 上个月在通过威胁遥测进行搜寻时偶然发现了一种不寻常的反射式装载机攻击方法。攻击链始于包含一些敌对的VB脚本代码的恶意电子邮件，最后以交付名为MoDi RAT的商品远程访问木马为结尾。

【参考链接】

https://news.sophos.com/en-us/2020/09/24/email-delivered-modi-rat-attack-pastes-powershell-commands/

30. Cardbleed：大规模的Magento1破解

【概述】

从上周末到现在为止，规模最大的有据可查的广告活动已破坏了全球近2000家Magento 1商店。这是一种典型的Magecart攻击：注入的恶意代码将拦截毫无疑问的商店客户的付款信息。被检查商店运行的是Magento版本1，该版本于去年6月宣布终止。

【参考链接】

https://sansec.io/research/cardbleed

31. Taidoor-真正持久的威胁

【概述】

政府支持的行为者通常在网络空间中进行长期的活动，并且为了简化这种连续的过程，他们经常开发恶意工具，以期长期使用它们。像任何其他恶意工具一样，它们需要隐身，并且在被检测到时，需要进行一些修改才能再次检测不到。这种工具的一个示例是Taidoor RAT（远程访问木马），其历史可以追溯到2008年，最近发现了其新版本，并在美国政府机构发布的技术报告中进行了介绍。Taidoor被描述为由中国政府支持的网络参与者开发和使用的远程访问木马。

【参考链接】

https://blog.reversinglabs.com/blog/taidoor-a-truly-persistent-threat

32. MTR案例：阻止1500万美元的Maze勒索软件攻击

【概述】

Sophos托管威胁响应（MTR）团队应邀帮助以Maze勒索软件为目标的组织。攻击者发出了1500万美元的赎金要求-如果他们成功了，这将是迄今为止支出最多的勒索软件之一。

【参考链接】

https://news.sophos.com/en-us/2020/09/22/mtr-casebook-blocking-a-15-million-maze-ransomware-attack/

33. 苹果高危漏洞允许攻击者在iPhone、iPad、iPod上执行任意代码

【概述】

苹果发布了iOS和iPadOS操作系统的更新，修复了多个安全性问题。通过此安全更新，Apple 解决了 AppleAVD，Apple Keyboard，WebKit和Siri等各种产品和组件中的11个漏洞。在已修复的漏洞中，严重性最高的是CVE-2020-9992，它允许攻击者在系统上执行任意代码。

【参考链接】

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

34. 德国调查人员指责俄罗斯的DoppelPaymer团伙制造了致命的医院袭击

【概述】

德国当局对最近对杜塞尔多夫医院的袭击进行的调查显示，俄罗斯黑客可能参与其中。

【参考链接】

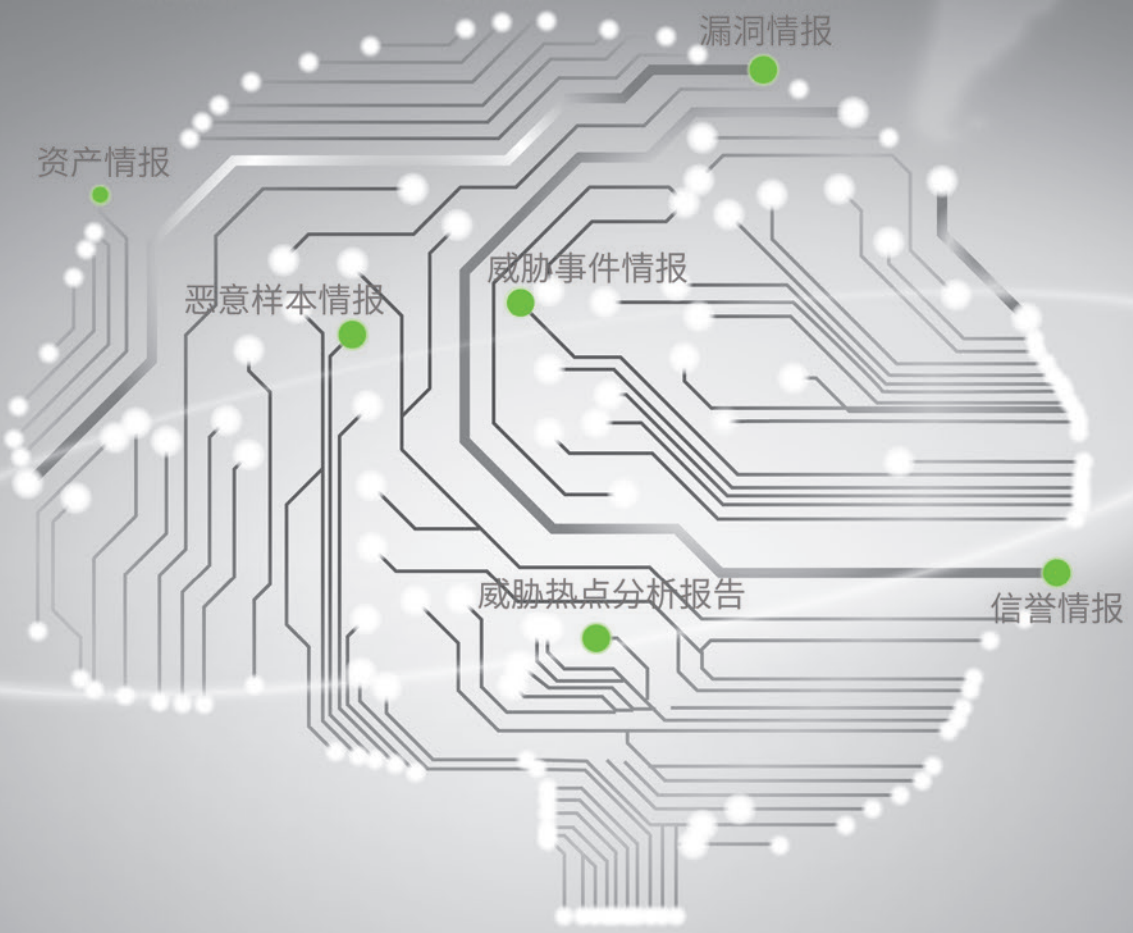
https://securityaffairs.co/wordpress/108620/malware/doppelpaymer-german-hospital-attack.html

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

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