金融行业

5 月报
2020 年

安全月报

专家观点 | 行业研究 | 漏洞聚焦 | 安全态势

绿盟科技金融事业部出品

专家观点

未雨绸缪、一叶知秋

行业研究

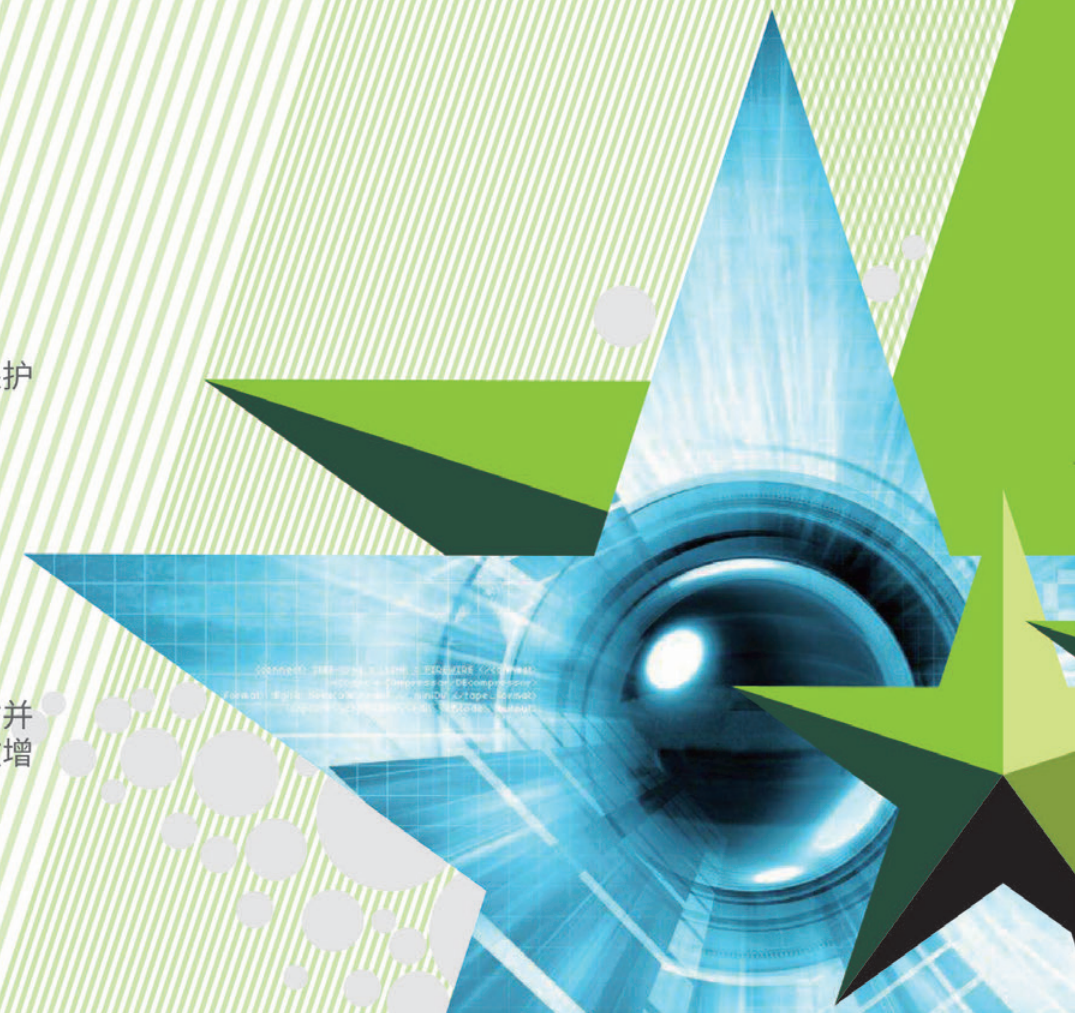
解析容器进程管理

浅淡网络“CS”及防护

浅谈大数据时代个人信息保护

新套路：伪造数字货币地址转换二维码网站实施攻击

全球疫情期间黑客入侵网站并“掠夺”信用卡号犯罪行为激增



NSFOCUS

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。

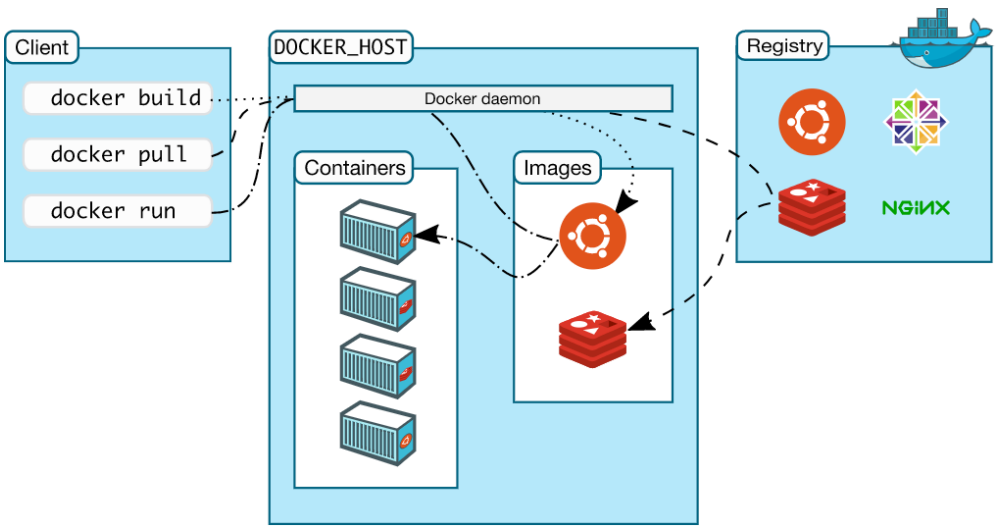
客户支持热线：400-818-6868

NSFOCUS绿盟科技

本|期|看|点

P04 未雨绸缪、一叶知秋

P12 解析容器进程管理



安全月报

2020年第5期

绿盟科技金融事业部

目录 CONTENTS

专家观点

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

专家观点

未雨绸缪、一叶知秋
——从各国应对新冠疫情的危机处置看信息安全事件响应处置的安全管理

绿盟科技　傅戈

一、前言

本次突发的新冠疫情来势汹汹，截至本文撰写时除我国外全球多个疫情爆发地区呈现不乐观发展的态势，部分国家政府已经将其视为一个关系到国家公关卫生安全的威胁并对应提高了威胁级别和采取了相应的应对措施。新冠疫情是一场公共卫生的突发事件，其处置流程和信息安全事件响应处置的流程实质上并无根本区别。故此如果我们从信息安全事件响应管理的角度去看待各国政府应对本次突发疫情的处置措施和效果，确有不少值得警惕和学习的地方。

二、信息安全事件响应管理内容简析

信息安全事件响应管理是IT治理中关于信息安全运营的一个重要的管理程序。它主要解决发生信息安全事故后机构如何通过既定的处置预案，协调安排相应的资源去处理解决正在发生或已经发生的安全风险，将其限制在企业机构能够承受的风险接受范围内。关于信息安全的应急处置管理，国内外有大量的安全标准、实践指南和手册可供参考。其中国内的标准包括《信息安全事件管理 第1部分：事件管理原理》（GB/T 20985.1-2017）、《网络安全事件描述和交换格式》（GB/T 28517-2012）、《信息安全应急响应计划规范》（GB/T 24363-2009）、《信息系统灾难恢复规范》（GB/T 20988-2007）以及正在制定的《公共信息网络安全预警指南》、《网络安全威胁表达模型》、《网络安全事件应急演练通用指南》等标准。国外的标准则包括美国国家标准与技术研究院（NIST）制订的《计算机安全事件处理指南》（NIST SP 800-61r2）、《网络空间安全事件恢复指南》（NIST SP 800-184／2016），ISO组织的《信息安全事件管理第1部分 事件管理原理》（ISO/IEC 27035-1:2016）、《信息安全事件管理第2部分 事件响应规划和准备指南》（ISO/IEC 27035-2:2016）以及《信息和通信技术事故应对行动指南》（ISO/IEC 27035-3）。不论是国内和国外的标准，针对信息安全事件响应管理都遵循了PDCA戴明环的循环处置流程，尽管不同的标准可能将其流程进一步拆解为不同的阶段或相对强调某一阶段的内容(例如NIST SP 800-61r2强调分析与检

测。ISO/IEC 27035-2:2016强调报告和检测)。信息安全应急响应处置管理的内容相信众多从事信息安全领域相关工作的人士并不陌生，因此本文不再累述。

三、安全观察分析

安全观察1：领导的专业性知识储备可帮助更好的增加应急响应处置的整体可控性

通常情况下绝大多数机构中CEO、CIO或CTO由于实际工作中并不直接负责IT安全，因此他们对信息安全未必都能有较为深刻的理解。其次一些机构中信息安全管理部门的负责人也可能不具备信息安全的知识和实践背景，严重的甚至连IT背景都不具备。如果机构中这样的高管和中层负责人在日常工作中主观意愿上亦未能深入学习和了解监管的安全要求、信息安全领域的背景知识以及机构当前的信息安全状态，那该机构在信息安全管理方面将陷入一种盲从和外行领导内行的境地。该情况可能导致在发生信息安全事故时，信息安全的直接负责人无法正确的理解认知和评估判断应急处置上报信息中提及和反馈的当前正在发生和未来可能持续或新增的风险。在这种情形下，该负责人很可能做出不正确和不恰当的处置决策。这种不正确或不恰当的战术层面判断处置决策可能进一步误导机构的CEO或董事会做出战略层面的误判，导致在第一时间没有能够投入充足的资源以及没有采取其他相关的正确措施将事故的影响和危害控制在更小的范围，同时还将造成当前风险的持续蔓延以及产生额外的新的安全风险。从另一个角度看，由于C-level层的权限更大，如果该层领导也缺乏对信息安全风险的深刻认知，那么机构将失去从战略层面纠正战术层面错误的最后一个风险控制点。有鉴于此，机构应该通过IT风险治理机制让C-level层及中层管理执行层的领导具备和提升相应的信息安全管理知识背景及管理能力，在发生信息安全事故时才能更好的借助专业性的知识储备来做出正确的分析判断和决策处置。

安全观察2：应急预案的完善度关系到响应处置的有效性和可靠性

当下绝大多数机构均已按照信息安全事件响应管理的要求编制了安全应急处置预案。但这些处置预案存在以下四个主要问题，导致发生事故时，预案无法有效的指导相应处置工作的操作执行，造成了不必要的风险损失。

问题一：应急预案没有做到应急操作级

一般情况下我们可以把应急预案分为应急场景级预案和和应急操作级预案。例如仅泛泛说明有病毒入侵导致业务主机宕机，业务中断，要求进行网络隔离和病毒查杀的预案属于场景级别。而详细描述通过何种具体操作恢复宕机主机、阻断网络病毒的传播、删除主机病毒、进行数据恢复的预案则属于操作级别。显而易见，应急操作级预案是应急场景级预案的细化，其落地性和可操作性更强。很多机构的安全预案通常仅限于应急场景级别的预案，这些定义的场景例如停电、网络通信中断、网络攻击和入侵、业务中断、数据泄露、安全迎检等。未编制操作级应急预案的原因包括由于机构的网络复杂、业务系统繁多复杂、业务操作复杂以及牵涉部门人员较多等因素导致信息安全部门难以下定决心去进行预案编制。尽管存在上述客观因素，但考虑到应急处置的有效性和可靠性，建议机构仍需下决心开展操作级预案的编制和完善。在编制过程中，可采取循序渐进的方式，首先将应急场景进行细化，将其拆分成不同的操作子场景；其次要求在某一操作子场景情况下涉及的部门进行场景适用性确认并据此进行操作级预案的编制；最后定期或不定期组织相关人员进行预案的评审和修编。相信只要持续进行该项工作，机构最终将建立完善的操作级应急预案体系。

问题二：应急预案没有考虑预案实施完成的自持性

不少中小机构在一些特定的预案中如网络攻击/入侵应急处置预案和数据灾备恢复预案中基本上很少考虑机构内部人员是否能够独立完成该应急处置需求。在实际应急处置的活动中，由于网络攻击入侵防控和数据恢复的复杂性，同时还可能受限于机构的编制和人员的技能，很多中小机构在发生此类安全事故时，其内部应急响应人员并不能独立应对。因此这些机构在制定应急预案时需要评估机构本身的应急处置能力并考虑在发生事故时是否需要邀请第三方力量进行参与介入，帮助共同应对。此外机构还要考虑和评估参与介入第三方机构的匹配能力、参与介入的成本负担、参与介入的方式和方法，信息共享的范围和内容、合同及责任的约定以及因共享信息和应急介入可能发生第三方信息泄露的风险。

问题三：预案更新不及时

机构在运营过程中常常会面临内外部环境的变化。外部变化通常包括法律法规等监管要求的变化（如提升和加强了对应急响应处置的要求）、第三方合作机构/和人员（业务往来/运维支撑/开发外包等）发生了人事及通信联系方式变更、服务能力变更、驻地机构变更等。内部变化则主要包括内部的网络环境发生变化、业务系统发生软硬件更迭/升级、业务操作流程变更、内部人员人事及通信联

系方式变更、应急处置工具不再可用等。以上内外部的变化如果没有在应急预案中得到及时更新，那么当发生事故时，将发生预案与实际情形相差甚远的情况而致使响应处置工作无法按预期顺利进行。

问题四：应急预案未得到实际操演

预案本身是停留在纸面上的，在没有实际演练的情况下，预案所涵盖的内容并不能得到充分的检测同时也不能发现预案内容的不足（例如未考虑到备品备件的不足，人员实际到岗的不足、人员应急处置技能的不足）。实践中由于并行测试和完全中断测试演练成本高，周期长，通常难以进行，那就需要采用其他应急演练方式并尽可能的全面。例如在模拟测试的方式下，建议可以采取头脑风暴的方法，在预先设定的场景中尽可能全面的评估和考虑到所有的可能性，并进行一一推演和测试。当然，如果机构具备并行测试和完全中断测试的条件，建议定期采用这两种演练方式并获得最为全面和最为真实的演练效果。

安全观察3：人员因素是应急响应的关键要素之一

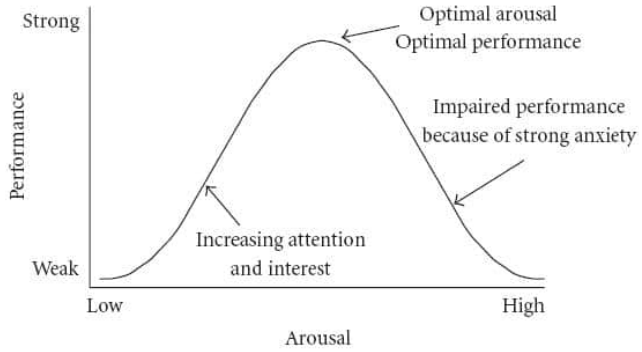
在信息安全事件响应处置流程中，在预防/准备阶段通过开展对内部员工的安全意识教育、安全技能培训提升以及应急演练可以极大改善应急响应处置的效果。普通员工的安全意识教育在此不再多说。需要特别注意的是在实践中机构的IT设施运营通常由软件开发与测试、业务运维、系统运维、网络运维、桌面运维、安全运维的员工或外包服务商来完成，因此对于这几类角色的人员，一定要让他们具备较之普通员工更高的安全意识，深入了解自己负责的工作内容可能面临怎样的安全威胁，产生怎样的安全风险以及相应的应对手段。此外应急演练的设计应覆盖以上人员，演练中让他们都能实际参与，通过桌面推演、模拟测试、并行测试、完全中断测试以及第三方参演的红蓝对抗的方式锤炼他们的应急处置能力，增加应急处置经验。随着参演人员的实际参与，机构的事件响应处置能力也将随之改善和提升。

信息安全应急响应小组是应急响应处置中的主要团队。机构管理者通常往往过于强调小组成员组成的全面性，小组成员的技能，但却忽视了人员在应急处置时所面临的精神压力。这些压力包括逃避免责压力和响应处置压力。

逃避免责压力：应急响应人员本身可能就是平时的运维人员或一线管理人员，因此一旦发生信息安全事故，从人类心理趋利避祸的情况下，有可能会采取瞒报漏报、虚报谎报的方式来尽可能降低自身可能因事后追责而需要承担的个人风险。因此，在安全管理过程中需要尽可能的避免此类情况的出现。具体可行的

方式包括在相关的管理制度中明确禁止主动屏蔽正确信息的输出以及对应处罚，在明确职责的同时也尽可能阐明例外的情况以及相应的免责，同时也包括对应急处置应对得当，避免更进一步损失发生的奖励措施。

响应处置压力：在处置的过程中，由于响应时间窗口十分有限，应急处置人员面临着公司高管传递的工作压力。心理抗压能力差的员工在此种情况下可能会出现心理抵触、工作推诿、专注力和操作能力的非正常下降。因此在处置过程中，常要求处置人员具备良好的心理抗压能力和娴熟的处置应对技能。



图：工作压力和工作表现的关系曲线图[1]

一个具备良好抗压能力心理素质的人员其最佳表现峰值点与其他人相比在如上图所示的关系曲线图中将会右移。因此在平时的安全应急演练过程中一方面需要参入压力训练的内容增加和强化在这种压力环境下的抗压演练。另一方面信息安全管理经理也需要主动观察参演人员的具体表现，对未来参与应急响应的人员有正确的预判和优先预设的考虑。

安全观察4：建立“吹哨人”机制增加重大事故的快速响应能力

在常规的安全事件响应处置流程中，安全事故的发现和处置报告是遵循层层上报的机制。这个传统的流程机制本身没有错，但是如果机构存在着官僚作风以及前面提到的层级领导缺乏专业性知识储备的情况，那么该流程机制就有可能导致安全事故的响应处置窗口期被人为的拉长。另外信息安全应急响应小组通常会被认为是纯粹的技术单元，因此在很多机构的信息安全管理体系中，信息安全响应小组的意见和报告并不能直接和完整的呈现在管理层的沟通会议上，这意味着没有一种可行的直接上报机制和通道，能将最直接的风险损失分析信息直接上传抵达更高的决策层。此种快速直通车机制的缺失或将导致身处一线的员工在一些突发且隐患巨大的情况下无法成为唤醒巨人的“吹哨人”。因此建议机构组织可

以考虑设置和开放这样的“吹哨人”上报机制和通道，允许技术层面的反馈也能在特殊情况下直接反馈于高管层，缩短应急响应处置的时间窗并降低风险损失。此外，该机制从管理层面上看还可增加一个威慑监督的作用，可以在一定程度上减少和降低执行管理人员发生瞒报虚报等不合规行为的几率。

安全观察5：不慎重的危机公关将是另一场危机

在发生信息安全事故时，机构有可能会根据情况判断而开展危机公关，消除或降低客户或公众存在的愤怒、困惑和沮丧等情绪，挽回对机构的信任，降低商业信誉遭受破坏的风险。然而在回顾既往众多的安全事件危机公关应急处置案例，我们可以发现很多处置不当的例子。综合来看，主要有以下这些问题。

- 事件上报不及时；
- 事件对外披露不及时；
- 对外披露信息不足；
- 对外披露信息可信度不足；
- 出现多个发布口径，且披露信息不一致；
- 措辞表态不恰当；
- 发言人的级别与事件危害程度和影响程度不符合；
- 发言人现场应对能力不足；
- 后续责罚措施及补偿应对措施处置不当；
- ……

这些问题的存在不仅没能达到公关本身设定的目标，反而可能导致事件影响不断发酵和蔓延，消耗和浪费了客户或公众的信任度，最终不得不付出更多的处置成本和公关成本。因此在决定进行正式对外的危机公关时，建议机构需要提前做好公关分析和演练（如果涉及现场发布会）。在公关分析的时候，内部一定要对事故信息进行梳理和信息的同步对称。包括，

- 发生事故的原因是什么；
- 哪些系统和业务受到了影响；
- 影响的程度如何；
- 是否发生客户信息泄露的情况；
- 预计泄露了多少数据信息；
- 可能造成什么影响；
- 机构内部当前的响应处置进度和情况如何，如系统漏洞是否已修补、攻

击入侵是否已结束或已经得到控制、恶意代码是否已清除、系统配置是否已恢复、业务是否已恢复运行、业务数据是否已恢复、已采取了哪些安全改进措施；

- 拟对遭受损失的客户所采取的补偿措施；
- 针对本次事故对客户侧推荐的安全建议；
- 适合的信息发布时间点，发布渠道以及恰当的发言人；
- 公关后可能未达到预期效果后的备选方案设计等
- 参与的部门和人员建议包括IT支撑团队、市场/业务团队、法务团队、公关团队以及牵头负责的高管。此外，如果有现场信息发布会，那么建议在正式的发布会之前进行至少一次的模拟演练，确保公关发布万无一失。

结束语

在现实世界中，机构出了安全事故总要有人担责。因此机构中的信息安全管理者，不论是CEO还是CIO、CTO、CSO甚至是安全部门经理的职业生涯都可能因此而受到影响。2017年9月7日美国征信巨头Equifax被披露发生大规模数据泄露事件，泄露敏感信息涉及1.43亿用户，导致公司股价暴跌30%，公司资本市值蒸发50亿美元。该公司随之在9月15日宣布其首席安全官(CSO)苏珊·马尔定，首席信息官(CIO)大卫·韦伯即刻从公司退位。同年Uber公司发生的信息泄露事故导致Uber公司首席安全官乔·沙利文和公司安全与执法法律总监克雷格·克拉克被辞退。以上这些案例让手握高薪的CEO/CIO/CSO们有种高处不胜寒的感觉。在安全行业普遍流传着一种说法，没有不被攻破的堡垒，只是不知道什么时候发生。因此机构的信息安全管理者们需要认真看待和审视机构的安全现状，加强信息安全管理和建设。在本文所提到的安全应急处置方面建议机构加强高管层的安全意识教育、优化响应处置工作的流程和机制、不断地完善信息安全应急预案、持续地进行安全演练，以练兵千日，用兵一时的姿态去认真对待未来可能面临的安全事故和安全威胁。

参考文献

[1] https://examinedexistence.com/the-correlation-between-stress-and-performance/

NSFOCUS

行业研究

解析容器进程管理

江国龙

摘要

容器通过使用namespace实现了容器间的进程隔离，那么在容器主机上，如何高效的对这些容器内进程进行监控和管理，无论对于运维还是安全，都有着重要的意义。

1. PID命名空间

Linux内核为所有的PID命名空间维护了一个树状的数据结构，最顶层是系统初始化时创建的root namespace（根命名空间），父节点可以看到子节点中的进程，并可以通过信号等方式对子节点中的进程产生影响。反过来，子节点不能看到父节点名空间中的任何内容，也不能通过kill或ptrace影响父节点或其它名空间中的进程。

在Docker中有一个很特殊的进程——Pid为1的进程，这也是Docker的主进程，通过Dockerfile中的ENTRYPOINT或CMD指令指定。当主进程退出的时候，容器所拥有的PID命名空间就会被销毁，容器的生命周期也会结束。

Docker最佳实践建议的是一个容器一个Service，并不强制要你一个容器一个线程。有的服务，会催生更多的子进程，比如Apache。

Pid=1进程需要对自己创建的子进程负责，当主进程没有设计好，不能优雅地让子进程退出，就会造成很多问题，比如数据库容器，如果处理数据的进程没有优雅地退出，可能会造成数据丢失。

2. Docker架构

下图是Docker官方[1]给出的架构图。Docker使用Client-Server架构，Docker Client与Docker Daemon进行通信。Docker Daemon（dockerd）监听Docker API请求并管理Docker的对象，如镜像、容器、网络和存储卷等。

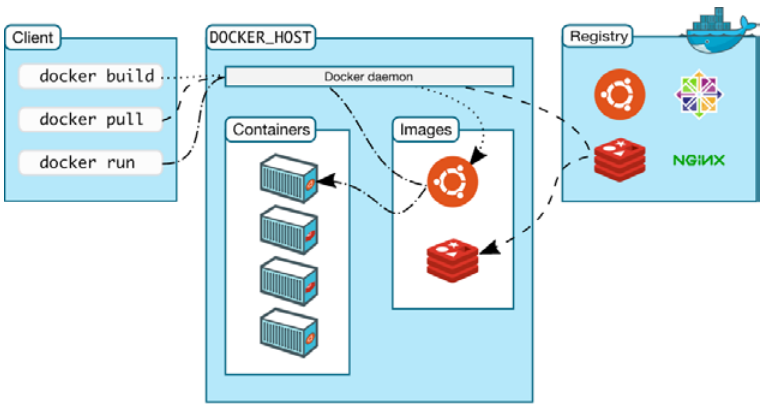


图1 Docker架构

下面在Linux（Ubuntu 16.04.6 LTS）上使用apt-get install docker-ce安装Docker（19.03.4），具体版本信息如下所示。

```
root@test:~# docker version
Client: Docker Engine - Community
 Version:           19.03.4
 API version:       1.40
 Go version:        go1.12.10
 Git commit:        9013bf583a
 Built:             Fri Oct 18 15:53:51 2019
 OS/Arch:           linux/amd64
 Experimental:      false

Server: Docker Engine - Community
 Engine:
  Version:          19.03.4
  API version:      1.40 (minimum version 1.12)
  Go version:       go1.12.10
  Git commit:       9013bf583a
  Built:            Fri Oct 18 15:52:23 2019
  OS/Arch:          linux/amd64
  Experimental:     false
 containerd:
  Version:          1.2.10
  GitCommit:        b34a5c8af56e510852c35414db4c1f4fa6172339
 runc:
  Version:          1.0.0-rc8+dev
  GitCommit:        3e425f80a8c931f88e6d94a8c831b9d5aa481657
 docker-init:
  Version:          0.18.0
  GitCommit:        fec3683
```

安装完成后，我们看一下有什么变化。

（1）运行*ls /usr/bin | grep docker*，发现在可执行文件中增加了docker、dockerd、docker-init、docker-proxy四个可执行文件；

（2）运行*ls /usr/bin | grep container*，增加了containerd、containerd-shim两个可执行文件；

（3）运行*ls /usr/bin | grep runc*，增加runc可执行文件；

（4）运行*ls axuw | grep docker*，发现主机上运行的进程中增加了下面这个进程：/usr/bin/dockerd -H fd:// --containerd=/run/containerd/containerd.sock。

下面我们逐个对上述内容进行简单的解释。

2.1 docker

运行docker --help，可以很容易的发现，这就是Docker架构中的Client。

2.2 dockerd

通过dockerd --help，也能发现这是用来启动运行Daemon。

2.3 docker-init

在Linux系统中，Pid=1号进程是init进程（systemd），是主机上所有进程的父进程。下面我们创建一个容器时试一下--init参数，看看会有什么

样的区别：

```
root@test:~# docker run -it
busybox sh
/ # pstree -p
sh(1)---pstree(7)
```

```
root@test:~# docker run -it --init
busybox sh
/ # pstree -p
docker-init(1)---sh(7)---pstree(8)
```

从上面的小实验中发现，如果不加--init参数，容器中的1号进程就是所给的ENTRYPOINT（实验中的sh），如果加上--init的话，1号进程就会是init（实验中的docker-init），而所给的ENTRYPOINT则成为了init的子进程。

2.4 docker-proxy

从名字上看，proxy应该是做端口映射的，下面继续来验证一下。运行以下命令新建一个容器：docker run -d -p 10010:10010 busybox sleep 10000，通过ps axuw | grep docker查看一下进程的变化情况，我们发现除了新增的基本进程之外，主机上还多了这样一个进程，/usr/bin/docker-proxy -proto tcp -host-ip 0.0.0.0 -host-port 10010 -container-ip 172.17.0.3 -container-port 10010，从进程COMMAND可以看出，其确实是实现了容器端口与主机端口之间的映射，具体原理这里就不再详细介绍了。

2.5 containerd

containerd[2]是一个高性能的容器运行时，是真正管控容器的Daemon，它管理着主机系统的整个容器生命周期，从镜像传输、存储到容器执行和监控，再到低级存储、网络插件等。

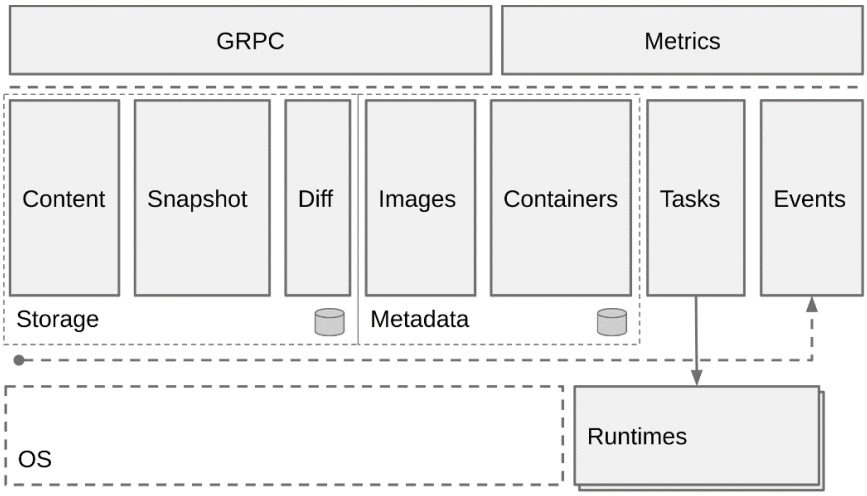


图2 containerd架构图

2.6 containerd-shim

shim原意是垫片，比如夹在螺丝和螺母之间的小铁片，维基百科在计算机领域给它的定义是：一种小型的函数库，可以用来截取API调用、修改传入参数，最后自行处理对应操作或者将操作交由其它地方执行。

Docker使用shim而不是直接使用containerd作为容器的父进程，主要因为：（1）允许runc在创建和运行容器之后退出；（2）为了防止当containerd挂掉的时候，shim还在，可以保证容器打开的文件描述符不会被关掉，这

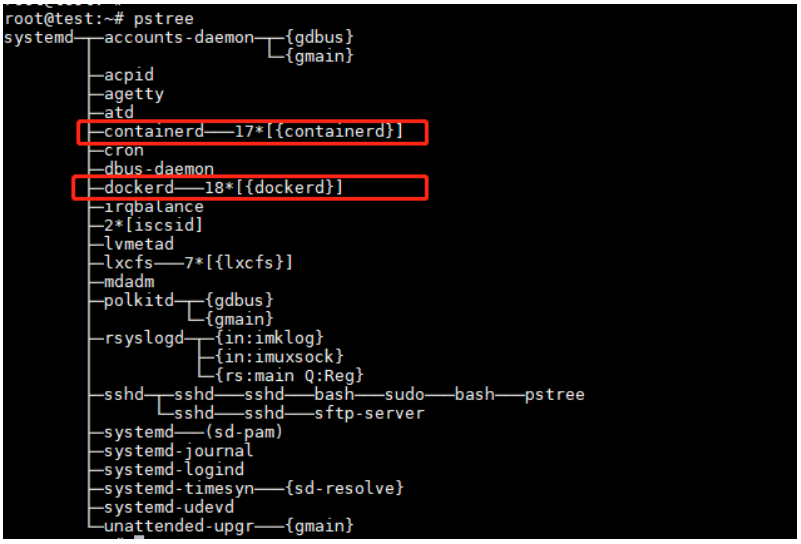
样，containerd就和真实的容器里的进程实现了解耦，每个新建的容器都会有一个独立的shim子进程作为其父进程；（3）依靠shim来收集和报告容器的退出状态，不需要containerd来等待容器子进程。

2.7 runc

runc，容器的运行时，就很容易理解了，运行runc --help，会给出一个简单的定义：runc是一个命令行客户机，用于运行根据Open Container Initiative (OCI)格式打包的应用程序，它是Open Container Initiative规范的兼容实现。

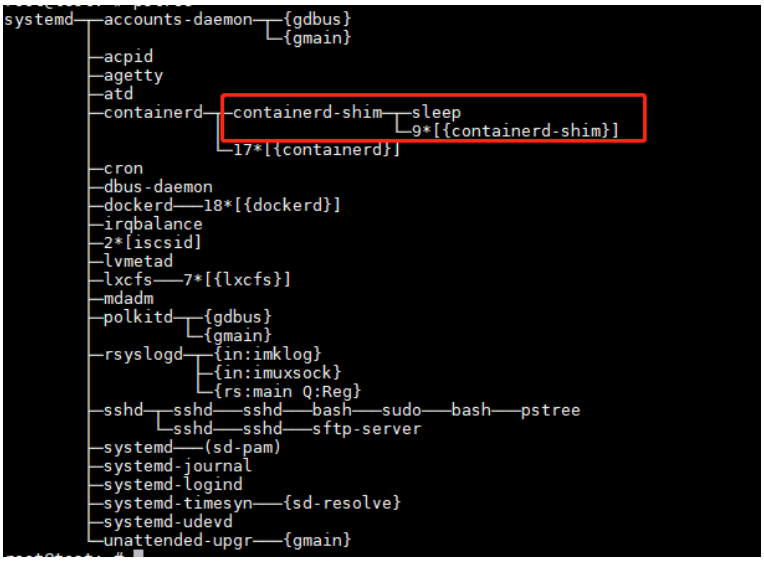
2.8 小结

这里我们通过示例，来总结一下上面这些Docker组件之间的关系。安装并运行docker daemon后，主机上运行了以下两个进程containerd和dockerd，通过进程执行命令，可以发现dockerd是通过调用containerd实现的守护进程。




```
root@test:~# ps axuw | grep container
root     5361  0.3  1.3 834648 54424 ?       Ssl  Nov09  12:09 /usr/bin/containerd
root     5475  0.5  2.5 838300 104016 ?      Ssl  Nov09  23:29 /usr/bin/dockerd -H
fd:// --containerd=/run/containerd/containerd.sock
```

接下来，运行*docker run -d -it --name test busybox sleep 100000*创建一个容器。



我们发现，新创建一个容器之后，containerd新建了shim子进程，并且新建容器内运行的sleep成为了这个shim的子进程。也就是说，每新建一个容器，都将这样新建一个shim子进程来管理容器进程。

通过ps查看进程的详细信息，我们可以发现主机上多了两个进程：

sleep 100000和containerd-shim -namespace moby -workdir /var/lib/containerd/io.containerd.runtime.v1.linux/moby/ee999590ae46438a55afa7c719a09b7ffa8ce244facb165b5a1bfba7c2aab42e -address /run/containerd/containerd.sock -containerd-binary /usr/bin/containerd -runtime-root /var/run/docker/runtime-runc。

因此，上述各组件间的关系可以简单总结为下图。

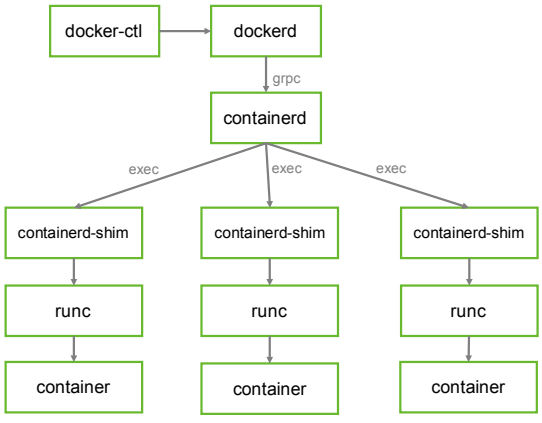


图3　Docker daemon架构

3. 进程监控

下面本文从几个角度，通过实验的方式，看一下如何在主机上实现对容器进程的监控。

3.1 环境构建

首先通过如下的Dockerfile和命令，构建一个容器。

```
FROM ubuntu:latest
EXPOSE 8888
CMD [“/bin/bash”, “-ec”, “while :; do echo ‘.’; sleep 120000 ; done”]
```

```
docker build -t ubuntu:test -f Dockerfile .
docker run -d --name test ubuntu:test
```

3.2 如何区分一个进程是主机进程，还是容器进程？

根据前文对容器进程原理的描述，可以很容易的回答这个问题。

容器本身的进程以及容器内运行程序的进程，其父辈进程一直可以推到shim进程，也就是说，如果父辈进程能推到shim进程，那么这个进程就是一个容器进程。

如何查看某个进程的父进程，这个就是Linux基本的操作了，比如可以使用*pstree -p*命令，查看系统所有的进程树。

或者可以根据进程号，在/proc/<pid>/目录下，查看该进程的详细属性。例如，创建上面那个容器时，可以看到系统创建了一个Pid为20117的sleep进程，那么我们cat /proc/20117/status，就可以获取如下这样的进程信息，看到其进程名是sleep，Pid是20117，PPid是20076。那么继续查找20776或者其父进程是否是shim，如果一直查询到父进程是Pid=1的systemd进程了，仍然没有找到shim进程的话，就说明这个进程不是容器进程。

```
root@test:/proc/20117# cat status
Name: sleep
```

```
State:  S (sleeping)
Tgid:   20117
Ngid:   0
Pid:    20117
PPid:   20076
……      ……
```

3.3 如何获取指定容器内进程信息？

如果我们知道了容器的id（5a9e71efe880），也就是说知道一个确定的容器（test），怎么查看该容器内都运行了哪些进程呢？

```
root@test: # docker ps
CONTAINER ID      IMAGE          COMMAND                  CREATED          STATUS
PORTS             NAMES
5a9e71efe880      ubuntu:test    “/bin/bash -ec  ‘whil…”  4 hours ago
Up 4 hours        8888/tcp       test
```

（1）可以直接使用docker daemon提供的top方法：docker top <container_id>。

```
root@test: # docker top 5a
UID                 PID                 PPID                C                   STIME               TTY
TIME                CMD
root                20076               20058               0                   11:44               ?
00:00:00            /bin/bash -ec while :; do echo '.'; sleep 120000 ; done
root                20117               20076               0                   11:44               ?
00:00:00            sleep 120000
```

注意：这里我们看到的Pid已经是主机操作系统上进程的真实Pid，而并非容器namespace中的Pid。

（2）可以使用docker inspect命令，查看容器内pid=1的进程，这样再通过获取这个进程的所有子进程，就可以知道容器内都运行了哪些进程。

```
root@test:~# docker inspect -f '{{.State.Pid}} {{.Id}}' 5a
20076 5a9e71efe8807fab8ddd8ecf646ea49265b646da27f4cdc1d31edc56097e
0b59
root@test:~# pstree -p 20076
bash(20076)———sleep(20117)
```

可以发现，上述两种方法所获取到的结果是一样的，也就是说容器5a9e71efe880中运行了20076和20117两个进程，20076是pid=1的进程。

3.4 如何根据进程PID，确实其属于哪个容器?

如果我们知道了一个进程的Pid，比如检测到了这个进程有异常，那么怎么知道这个进程是属于哪个容器的呢?

（1）使用docker inspect命令。

docker inspect命令可以输出当前运行容器的信息，其中包括容器内运行进程的信息，通过format flag可以指定输出的格式、输出的内容。于是可以通过容器信息里的State.Pid获取容器内进程的Pid。然后再根据进程Pid做一次过滤，就可以获取到对应的容器id了。

注意，这里的Pid只包含容器内Pid=1的进程，因为按照容器的设计思想，一个容器是只运行一个Service的，也就是理想情况下只有一个Pid=1的进程。

```
root@test:~# docker inspect -f '{{.State.Pid}} {{.Id}}' $(docker ps -q) | grep
20076
20076 5a9e71efe8807fab8ddd8ecf646ea49265b646da27f4cdc1d31edc56097e
0b59
```

（2）如果是容器内非法运行了一个新的进程，这样通过docker inspect是无法看到这个进程的，知道了这个非法进程的Pid，怎么确定其容器id呢?

可以使用3.2中区分容器进程还是主机进程的方法，通过pstree -p，或者/proc/<pid>/status，查看到其父进程的Pid，一直找到shim进程的Pid，查看/proc/<shim-pid>/cmdline，在其执行命令中，就可以看到容器id了。

```
root@test:~# ps axuw | grep watch
root    21019  0.2  0.0  12112  3384 pts/0    S+   15:45   0:01 watch -n 10 cat /proc/loadavg
```

```
root@test:~# cat /proc/21019/status| grep Name
Name:   watch
root@test:~# cat /proc/21019/status| grep PPid
PPid:   20808
```

```
root@test:~# cat /proc/20808/status| grep Name
Name:   bash
root@test:~# cat /proc/20808/status| grep PPid
PPid:   20058
```

```
root@test:~# cat /proc/20058/status| grep Name
Name:   containerd-shim
```

```
root@test:~# cat /proc/20058/cmdline
containerd-shim-namespacemoby-workdir/var/lib/containerd/io.containerd.runtime.v1.linux/moby/5a9e71efe8807fab8ddd8ecf646ea49265b646da27f4cdc1d31edc56097e0b59-address/run/containerd/containerd.sock-containerd-binary/usr/bin/containerd-runtime-root/var/run/docker/runtime-runc
```

4. 总结

本文结合Docker在进程方面的实现原理，解释展现了如何在主机上进行相关的进程管理监控。文中所提的各种监控内容的方法，只是其中一种或几种实现，可能还会有其它的方式。

参考文献

[1] Docker overview，https://docs.docker.com/engine/docker-overview/
[2] containerd，https://github.com/containerd/containerd

浅淡网络“CS”及防护

金融事业部 周瑾

1. 背景

网络“CS”全称Cobalt Strike，顾名思义Cobalt Strike是一款团队作战的渗透测试神器，业界人戏称为CS神器。Cobalt Strike区别于其他Metasploit平台工具，而是可以作为单独的平台使用。它分为客户端与服务端，一个服务端可以对应多个客户端（Windows、Linux、Mac下都可以运行），可谓是团队渗透神器，能让多个攻击者同时连接到团体服务器上，共享攻击资源与目标信息和sessions。同时“CS”又集成了端口转发、服务扫描，自动化溢出，多模式端口监听，钓鱼邮件、僵木蠕文件生成等功能，使其变成众多APT组织首选的终端控制工具。

2. 工作原理

在了解Cobalt Strike工作原理前，我们先知晓几个角色定义：

a) Team Server：Cobalt Strike的服务器端。Team Server(TS)是配置和启动Listener的地方。

b) Listener：运行在TS服务器上的服务，可以监听Beacon的请求。

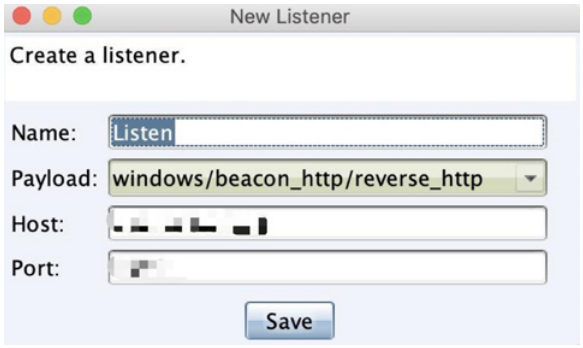
c) Beacon：植入到受感染系统中的恶意程序，可以请求TS服务器接入并获得指令，同时可以在受感染系统中执行指令。

d) Cobalt Strike客户端：攻击者利用Cobalt Strike客户端，输入服务端的IP以及端口、连接密码进入Team Server。

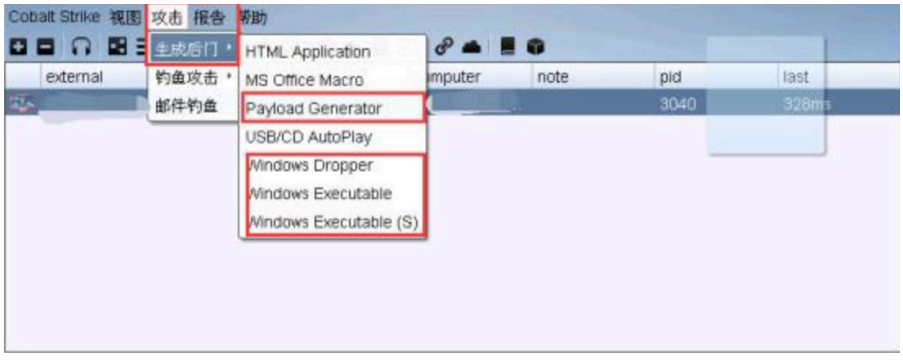
几方的工作流程如下：

1) 攻击者Cobalt Strike客户端登录Team Server，制作Listener和 Beacon。Listener在Team Server本地运行，Beacon嵌入到可执行文件、添加到Word文档、钓鱼邮件或者通过利用主机漏洞来等其他方式投递到被攻击的主机上。

图：Cobalt Strike客户端

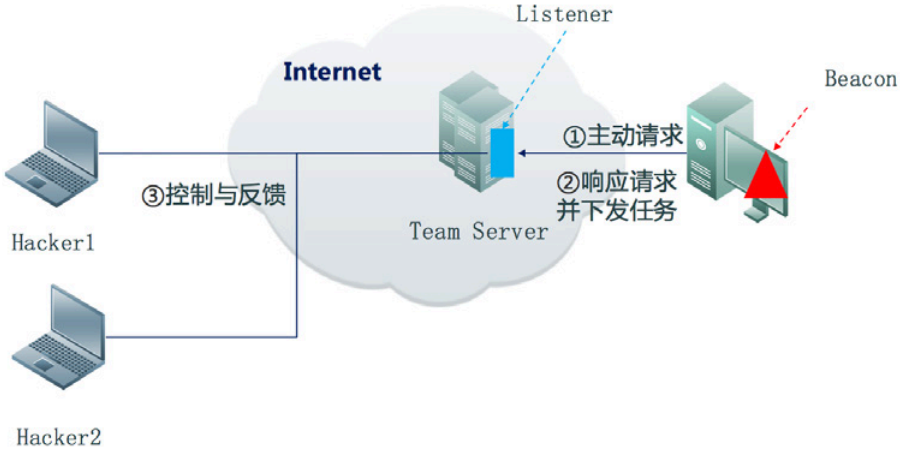


图：创建Listener



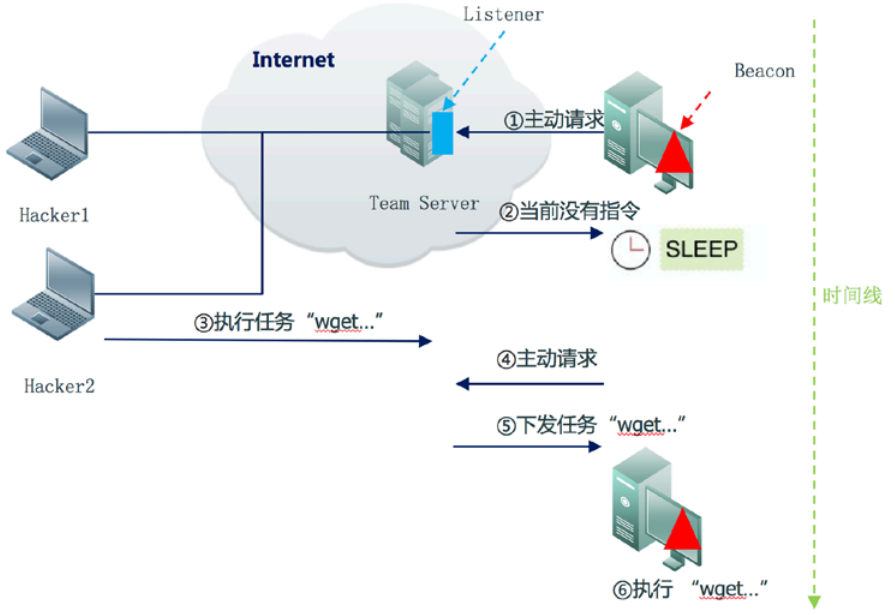
图：创建Beacon

2) Beacon在攻击主机上告诉Team Server：“嘿，我是肉鸡，我在这...”。工作原理如下：



3) Server控制器接收到请求后会检查是否有待执行的任务，如果有就会将任务下发到Beacon。

4) Beacon没有收到指令静默；收到指令并执行。



3. 针对防护

从上述章节，可以总结出两种类型的“CS”攻击防护：① Beacon入网前防护；② Beacon潜伏期防护；③Beacon执行指令中防护。

1）Beacon入网前防护

Beacon入网的方式通常有以下几种：嵌入到可执行文件、添加到Word文档、钓鱼邮件或者通过利用主机漏洞。因此我们可以利用沙箱的虚拟执行进行文件检测；可以利用WAF、IPS的漏洞攻击防护。

2）Beacon潜伏期防护

Beacon潜伏期会定期Listener发送存活指令，虽然这段通信会进行Cobalt Strike的加密，但是我们仍可以利用IPS或EDR的服务器异常外联发现。当然前提得先利用IPS或EDR进行服务器对外通信的IP+端口的基线学习，当Beacon外联超出了服务器对外通信的基线即可进行服务器的异常外联告警。

3）Beacon执行指令中防护

Beacon收到Listener的指令并执行相关操作，部署了EDR的终端也可以进行异常告警。

4. 总结

在云计算、大数据、移动APP等新技术所带来的行业信息技术应用更新和技术场景变化的前提下，信息安全不断面临新的挑战。企业只有做好攻击事前事中事后的安全建设，才可以冷静面对这纷繁复杂的安全局势。

浅谈大数据时代个人信息保护
——ISO/IEC 27701-2019 个人信息管理体系（PIMS）标准介绍

金融事业部　陈剑博

个人信息滥用、数据窃取、隐私泄露以及“大数据杀熟”等数据安全问题呈现爆发趋势

2019年底，“微信发原图或泄露位置信息”的话题引发广大网友的关注，后经过专家核实，只有同时满足拍照时开启定位、拍照设置保存地理位置、微信上发原图三个条件才会泄露位置信息，但大数据时代如何保障个人隐私安全成为大众越来越关心的一个话题。大数据时代的到来，为我们带来了空前的便利，但随着大数据在各个领域的渗透逐渐加深，个人隐私泄露的风险也愈加严重。

“小姐您好，最近有贷款需要吗？”“您好，我们这里有一个新开的楼盘，您是否有购房需求？”“先生您好，我们是xx英语，之前您留过电话，现在您家孩子需要补习英语吗？”相信上述骚扰电话和推广短信你一定不陌生，这些骚扰已然成为智能手机的标配。近年来阿里的“双十一”、“双十二”购物狂欢节办的如火如荼，2019年总成交额达2684亿元，更创下了开场18秒成交额破亿的记录。但是我们在疯狂剁手购物之时，又可曾发现自己已经陷入了商人的圈套。同样一件商品，从淘宝APP的不同入口下单，领到的优惠券和最终价格并不相同；同一款商品，使用不同手机登录查看，都会出现不同的价格。就在今年的3·8节活动期间，也有网友反映，身为天猫的88VIP会员，购买商品的价格反而比普通用户高。至少在大多数网民心中，阿里无论从技术还是口碑上都给人足够信任，如果说阿里都存在大数据“杀熟”等信任危机时，其他的电商平台又怎么不引起消费者怀疑呢？技术始终是为消费者服务的，而不是收集用户信息甚至欺骗消费者的手段，大数据也同样如此。

在如今中国互联网行业高速发展的今天，大数据的普及无疑让我们的上网习惯变得透明，人们在网络上留下的个人印记越来越多。通过对人们留在互联网上的痕迹进行采集、挖掘、提炼与分析之后，每个人的精准画像都被毫无保留地完整暴露在了网络世界中。一旦我们的这些信息被不法分子恶意利用，轻则针对性广告轰炸，重则遭受经济诈骗倾家荡产，更有甚者因借贷大量网贷，贷款如滚雪球般越滚越大，不堪重负而最终选择结束自己的生命。不要认为网上的新闻离我们很遥远，实际上如果一个陌生人能够说出你的所有只有你知道的隐私，你会很快建立对他的信任，并相信他说的一切。这就给不法分子带来的机会。不法分子就是通过各种渠道获得隐私数据，然后和你建立信任关系，最终诈骗成功。如果隐私数据大量外泄，不法分子有利可图，必然猖獗。

全球个人信息安全与隐私保护合规管理日渐完善

在此背景下，全球各个国家纷纷颁布相关法律法规，对数据安全与隐私保护相关问题进行严格的规范与引导。如欧盟保护个人数据的《General Data Protection Regulation》(GDPR),美国的《California Consumer Privacy Act》(CCPA)等。我国也于2017年6月1日正式实施《中华人民共和国网络安全法》（通常简称《网络安全法》）。《网络安全法》是我国首部全面规范网络空间安全管理方面问题的基础性法律，包含的内容十分丰富，值得关注的是，《网安法》在数据（包括个人信息）安全与保护上也有诸多规定。

ISO/IEC 27701个人信息管理体系（PIMS）标准

2019年8月，国际标准化组织ISO和国际电工委员会IEC联合正式发布了全新个人信息管理体系（PIMS）国际标准ISO/IEC 27701。该标准是在隐私保护方面对 ISO/IEC 27001 和ISO/IEC 27002的扩展，针对保护可能受到个人信息收集和处理影响的隐私提供了更多相关指南。ISO27701的目标是透过额外的要求来增强现有信息安全管理体系（ISMS）,以便建立、实施、维护和不断 改进隐私信息管理系统（PIMS）。该标准概述了适用于个人身份信息（PII）控制者和PII处理者的框架，用于隐私控制管理，以降低对个人隐私权的各种风险。它适用于所有类型和规模的组织，包括公有和私营公司、政府实体和非营利组织，在信息安全管理体系(ISMS)中实施PII。

适用于控制者和处理者的要求

- 保密性：经授权访问 PII 的个人必须履行保密协议。
- 分析风险：必须进行隐私风险评估以识别 PII 处理风险。
- 监管：组织机构必须指定负责开发、实现、维护和监视其治理及隐私项目的个人。
- 培训：可以访问 PII 的人员需经过隐私意识培训。
- 内部过程：组织机构必须为应对 PII 泄露事件而采纳各种策略和规程，比如事件响应计划。
- 记录保存：ISO 27701 要求组织机构保留所有 PII 处理活动的记录，包括 PII 在司法辖区间转移和向第三方披露等。

特定于控制者的要求

- 隐私通告：组织机构必须提供包含 PII 收集、使用和处理相关具体信息的隐私政策。
- 处理者合同要求：组织机构必须与其处理者签订书面合同，约定具体事项，比如保护 PII、限制处理操作仅可在 PII 特定用途范围内，以及提供 PII 泄露通报。
- 个人权益：ISO 27701 要求组织机构实现各种机制，赋予个人访问、修改和删除其 PII，以及反对或限制 PII 处理等权益。
- 设计隐私与默认隐私：组织机构必须采取措施实现设计隐私和默认隐私原则。

特定于处理者的要求

- 处理限制：组织机构必须仅按控制者或处理者（取决于客户的角色）的说明处理PII。
- 辅助个人权益：ISO 27701要求处理者实现帮助客户遵从个人权益的种种措施。
- 转移与披露：处理者必须于PII在司法辖区间转移或任何预期变化发生前通告客户。
- 分包商：ISO 27701要求处理者仅可雇佣一家分包商按照客户合同的条款处理PII。

遵从ISO 27701要求的组织机构会留下其PII处理方式的书面证据，可用于推动与商业合作伙伴就PII处理问题签订协议，明确该组织机构与其他利益相关者间的PII处理方式。

实施隐私信息管理，至少获得如下收益

- 合规。通过明确对PII处理者的隐私保护要求，可以明确隐私保护管理合规目标，减轻组织合规负担的同时降低了组织合规风险，ISO27701标准附录D中明确表示，单个隐私控制点可以满足GDPR中的多项要求。满足了ISO27701标准也就意味着基本满足GDPR的要求，而GDPR是众多隐私保护法规中最为严格的，也就意味着满足了即将颁布的《隐私保护法》的系列要求。
- 完善自身数据安全能力和风险管理。实现持续完善产品的非功能性要求，进而展示出产品在处理个人隐私安全、安全治理的绩效，通过流程分析，在流程的输入、输出、控制过程中，识别、分析、验证隐私保护需求、传递隐私保护价值，减少甚至消除隐私泄露的风险，如：体现为采用隐私控制技术（如日志脱敏、数据库加密）、产品架构（如加密芯片）、技术路径（如完整性校验）等。
- PIMS认证可以传递信任。客户或合作伙伴，尤其是政府组织、金融机构作为承担隐私风险的机构，通常为要求PII处理者提供相关证据（如PIA分析报告），从而证明PII处理者的产品能符合使用的隐私管理体系要求。通过得到授权的第三方机构对PII处理者进行基于国际标准的审核，可以极大的降低合规沟通成本，这种合规透明度的提高对于组织战略和业务决策至关重要，同事PIMS认证也有助于向公众传达组织的可信度。
- 对安全合规而言，该新标准相当于锦上添花。以成熟ISO 27001标准为基石，ISO 27701则建立在此基础上，提供全面的信息安全控制和个人信息保护，ISO 27701合规首先要求ISO 27001合规，二者互为补充。

结语

除了ISO/IEC 27701外，近两年我国新发布的《个人金融信息保护技术规范》（JR/T 0171-2020）、《信息安全技术 个人信息安全规范》（GB/T35273-2020），以及正在制定中的《个人信息保护法》，相信会在未来帮我们开启个人信息保护的新时代！

新套路：伪造数字货币地址转换二维码网站实施攻击

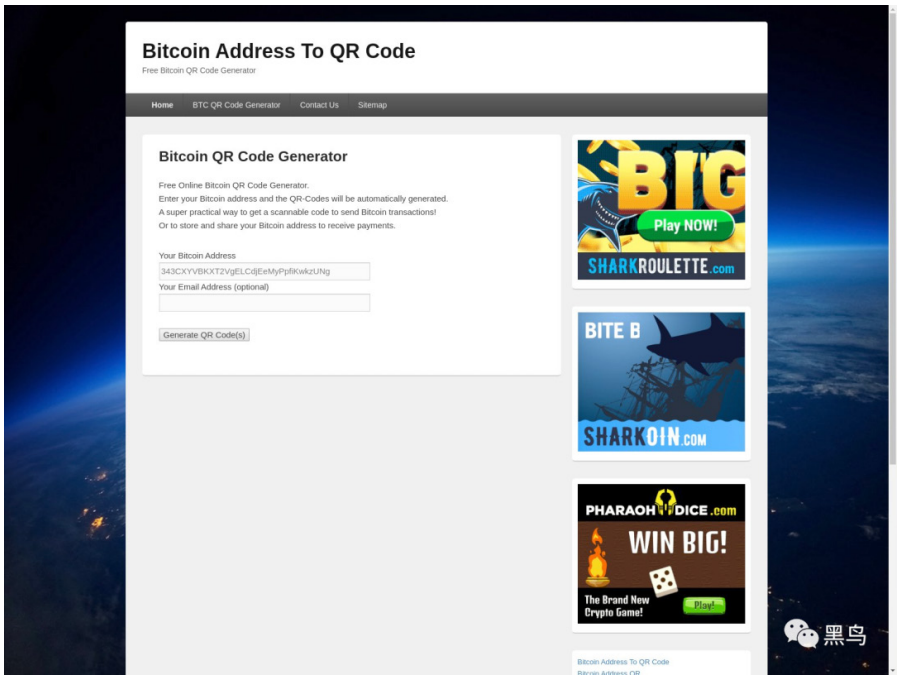
摘要：最近，网络上出现了一种新的金融诈骗模式，对象仍然为虚拟货币。

关键词：标签（数字货币、二维码转换、钓鱼网站），技术问题（安全事件）。

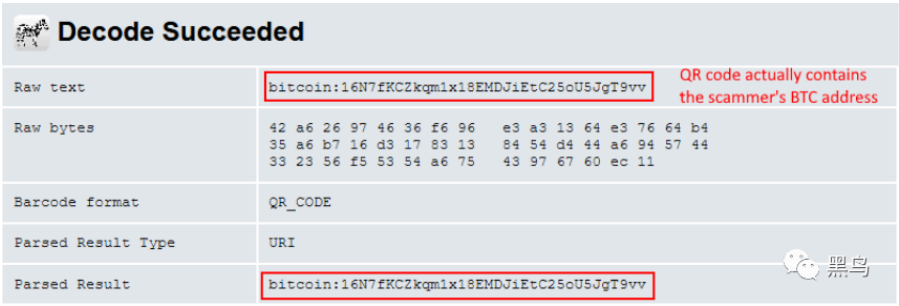
内容：因为比特币等虚拟货币的地址非常长，每次交易如果纯靠手输会比较麻烦，因此很多人都会选择将BTC地址转换成二维码。

类似下图所示

为了方便转换，有一些网站专门做了个网站，可以通过输入BTC地址，然后自动生成二维码图片。



然而，就拿上面这个网站来说，实际上这是一个专门用来做诈骗的网站，生成的二维码根本不是用户的地址，而是诈骗者的地址。这样，当用户将生成后的二维码发给其他人，那么其他人就会直接往里面转账，相当于进行了一次BTC地址劫持。



下面这些域名全是近期专门用来进行类似的攻击，类似的网站均用带有BTC qr code的字眼进行伪装，此外还有其他币种，dash，etc都在其中。

bitcoin-barcode-generator.com

bitcoinaddresstoqrcode.com

bitcoins-qr-code.com

btc-to-qr.com

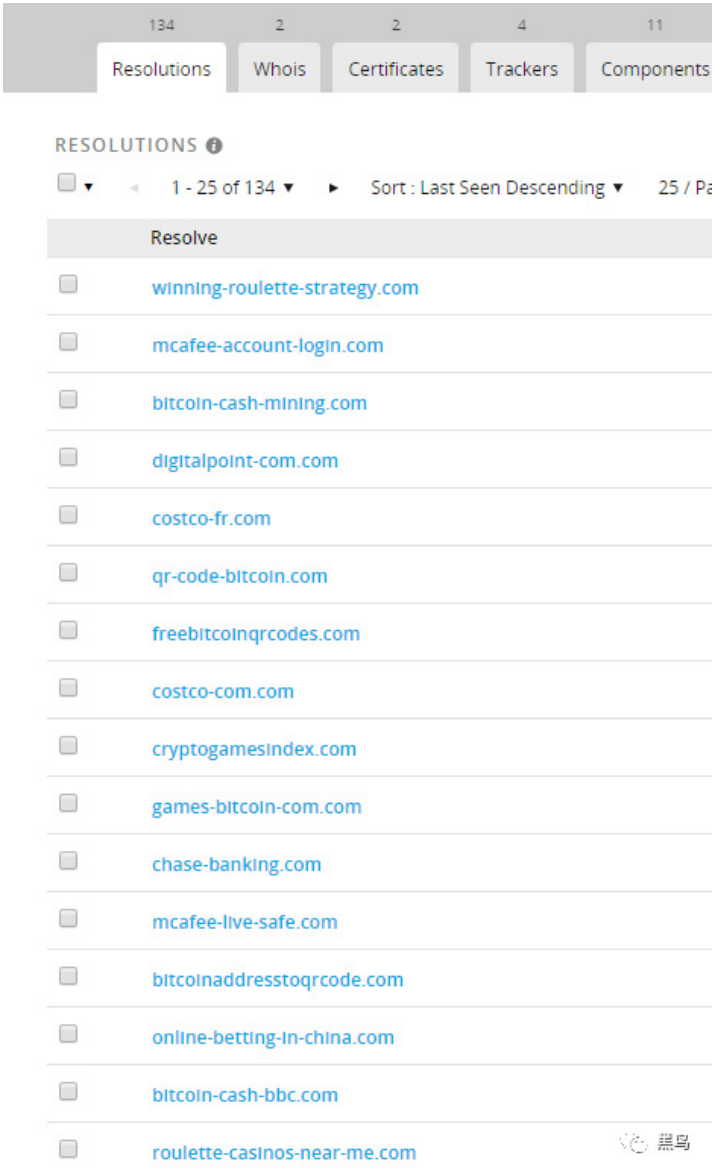
create-bitcoin-qr-code.com

free-bitcoin-qr-codes.com

freebitcoinqrcodes.com

qr-code-bitcoin.com

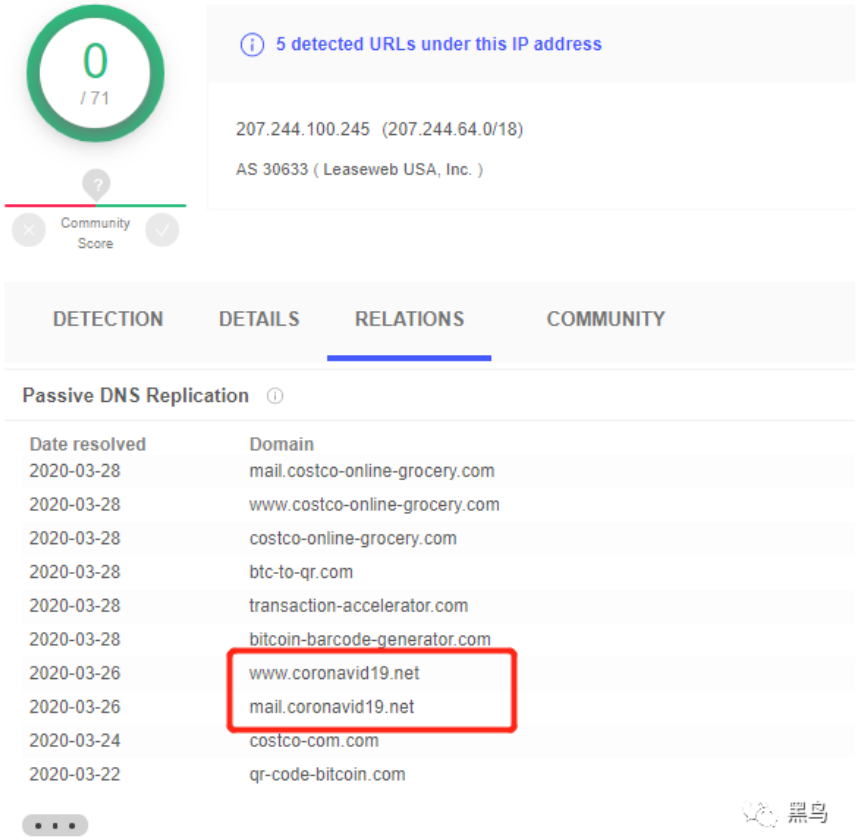
qrcodebtc.com



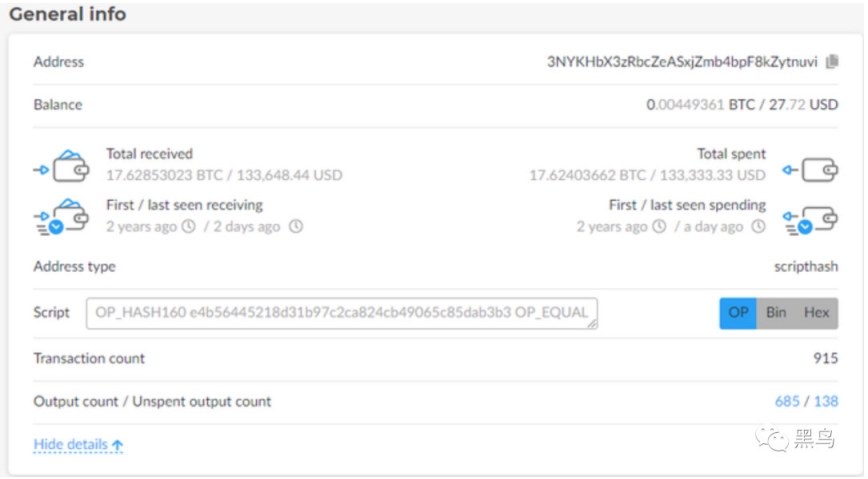
此外，这些域名分别指向不同的同一网段的三个IP

207.244.100.245./241/.244

而这些IP旗下还有与疫情相关的域名，看样子该诈骗者还有其他想法。



粗略算目前已经窃取了超过45,000美元。



信息来源：

https://mp.weixin.qq.com/s/LmkCPx2YoyMg_Oqipm91ig

全球疫情期间黑客入侵网站并“掠夺”信用卡号犯罪行为激增

摘要：由于新型冠状病毒在全球范围内大爆发，全球有成千上万的人在他们的居住地区进行隔离，与此同时许多实体商店已经暂时营业，因此在线购物已成为很多用户的生命线。但是，随着在线消费的不断增加，黑客入侵网站并以数字化方式“掠夺”信用卡号的犯罪行为正在快速增加。

关键词：标签（疫情、黑客犯罪、信用卡），技术问题（安全事件）。

内容：黑客通过入侵合法网站以获取用户付款数据的恶意代码早在Covid-19危机之前就已经对在线购物者构成了潜在风险。例如，在黑色星期五这样的购物高峰时段此类入侵行为也会激增一样，冠状病毒的爆发也为更多的攻击创造了主要条件。对此，网络安全公司RiskIQ的威胁研究负责人Yonathan Klijnsma表示，该公司发现在3月份此类入侵行为的线浏览量比2月份增加了20%。对此Klijnsma表示，只要用户的在线交易事件出现激增，电子商务犯罪就会激增。目前，由于大量用户都将自己隔离在家里，在线购买量大量激增，这成为为犯罪分子发起行动的黄金时期。

此前，RiskIQ 安全研究团队披露了黑客对NutriBullet公司类似的信用卡信息窃取攻击，该公司将攻击归因于臭名昭著的数字窃取黑客组织Magecart。据悉，RiskIQ研究团队是于2月底首次观察到NutriBullet攻击，但当时无法与NutriBullet

公司取得联系。因此，研究人员与其他互联网监管机构进行了合作，在3月1日成功清除了该恶意软件的基础架构。由于NutriBullet公司目前尚未修复黑客曾经入侵过的网站，因此，在3月5日Magecart黑客组织在该网站上建立了一项新的恶意软件操作。

最近又有两名备受瞩目的受害者揭示了相关在线信用卡盗取活动，对此网络安全公司Malw arebytes的研究人员上周发布了有关他们对嵌入存储公司Tupperware网站中刑法代码的研究结论。据悉，攻击者利用该站点中的漏洞注入了他们设计的恶意模块，然后在消费者填写付款表格以完成购买时，该恶意模块就已经吸取了用户的信用卡帐号和其他支付数据。

对于此次攻击，尽管其中一些原因可以归结为安全问题对该公司的正常挑战，但Malwarebytes威胁情报负责人JérômeSegura指出，冠状病毒大流行可能正在带来挑战和干扰，这会使公司更难以应对该安全事件。Segura表示，Malwarebytes研究团队首次尝试于3月20日通知Tupperware公司，但是该公司似乎是在3月25日，即Malwarebytes发布调查结果的那一天才从其站点中删除该恶意撇渣器。

随后，Tupperware公司在一份声明中表示：“公司最近发现了涉及我们美国和加拿大电子商务网站上未经授权代码的潜在安全风险。随后，我们迅速展开了调查，并采取措施删除了未经授权的代码，同时聘请了领先的数据安全取证公司来协助调查”。而且，公司表示已经与执法部门联系，进行深入调查，之后会提供更多细节。

据悉，与RiskIQ研究团队不同，自新型冠状病毒出现以来，

Malwarebytes团队表示并未检测到黑客的掠夺攻击有显着增加。但Segura对此强调，掠夺攻击没有明显升高可能是因为此类攻击的典型基线水平已经很高了，因此对于用户而言，当心风险并采取预防措施是特别重要的。

但是，非常无奈的是对于用户而言他们无法做很多事情来保护自己，因为即使用户感染了此类攻他们网站的外观和行为不会有什么改变。因此，研究人员建议，坚持拥有良好的站点来维护系统安全，同时拥有优秀的IT团队资源组织更容易做到对软件的更新和维护，这些维护将使站点长期保持安全。

在当前冠状病毒大流行的环境下，由于小型零售商和其他公司都急于将其更多业务转换为在线业务，在此时，Malwarebytes研究团队建议用户尽量使用GoFundMe这样的众包平台或Paypal这样的第三方付款处理器来完成交易，而不是直接从小型公司内部系统来填写付款表格。对于预防此类攻击，研究人员认为最大的可能是检查站点是否得到有效维护，例如如果版权声明是从2017年开始的，那可能意味着有人暂时没有看过该模板，那么就无法完全消除风险。

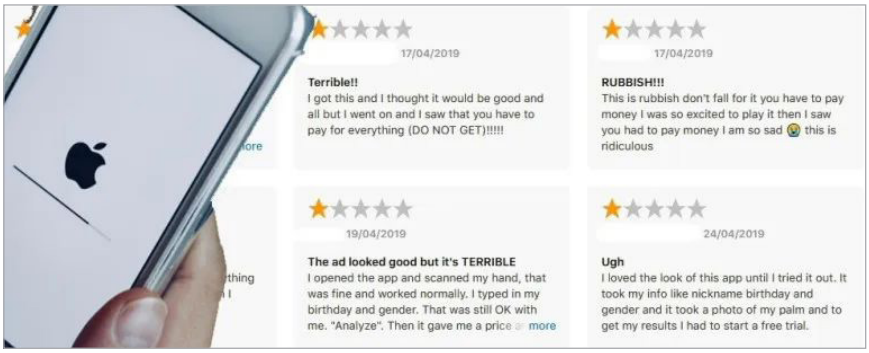
信息来源：

https://www.easyaq.com/news/2147307734.shtml

Fleeceware：藏在应用商店里的新型网络金融欺诈

摘要：近日，英国网络安全公司SophosLabs发布了第三份Fleeceware应用程序威胁报告，称带有网络金融诈骗属性的Fleeceware应用出现在了iPhone和iPad应用商店，且已有350万iOS用户安装了Fleeceware应用程序。

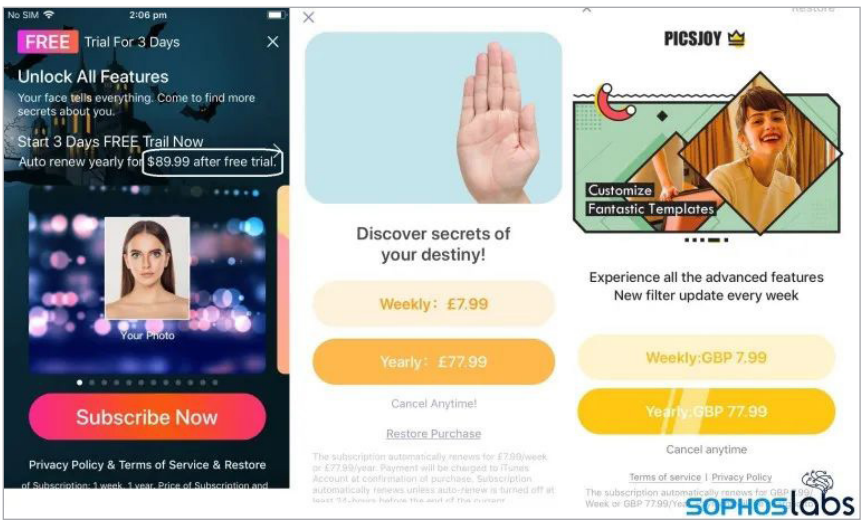
关键词：标签（Fleeceware、应用商店、金融欺诈），技术问题（安全事件）。



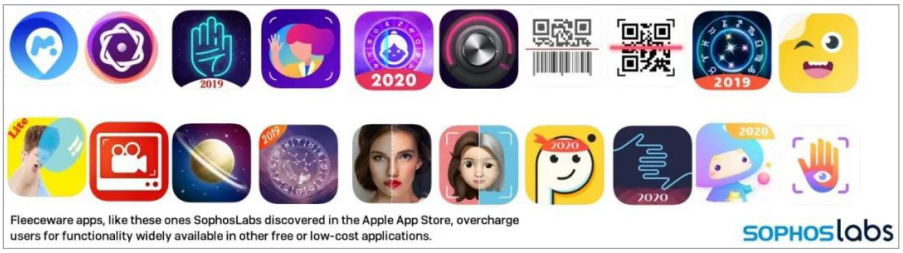
内容：网络金融诈骗新类型——Fleeceware

“Fleeceware”一词是网络安全术语中的新增内容。该词是Sophos于去年9月的谷歌Play商店调查中创造。

具体指的是，滥用应用商店试用机制，先向用户提供免费试用，但在试用期结束后，不通知用户的情况下，直接扣取高额订阅费用的应用程序。



此次，Sophos在iOS应用商店共核实确认了32个Fleeceware应用程序，多为图像编辑器、星座运势、算命、掌上阅读器、QR码、条形码扫描仪等工具类应用。确认总量看似不多，但这三十多个Fleeceware应用下载量多在50-100万之间，甚至有一款名为"十二生肖大师Plus "的应用，直接跻身应用商店总收入最高应用。



在扣取订阅费上，Fleeceware应用常常高达30美元/月或9美元/周，也就是说，每年的费用总计在360至468美元之间。换算成人民币，大约是年2500元起跳的高额费用。

目前，Sophos数据显示已有350万iOS用户安装了Fleeceware应用程序。

免费+登榜+广告：吸引目标用户

一个个工具应用，怎么成了Fleeceware，就能让350万iOS用户中招?

原因一：假免费真骗钱

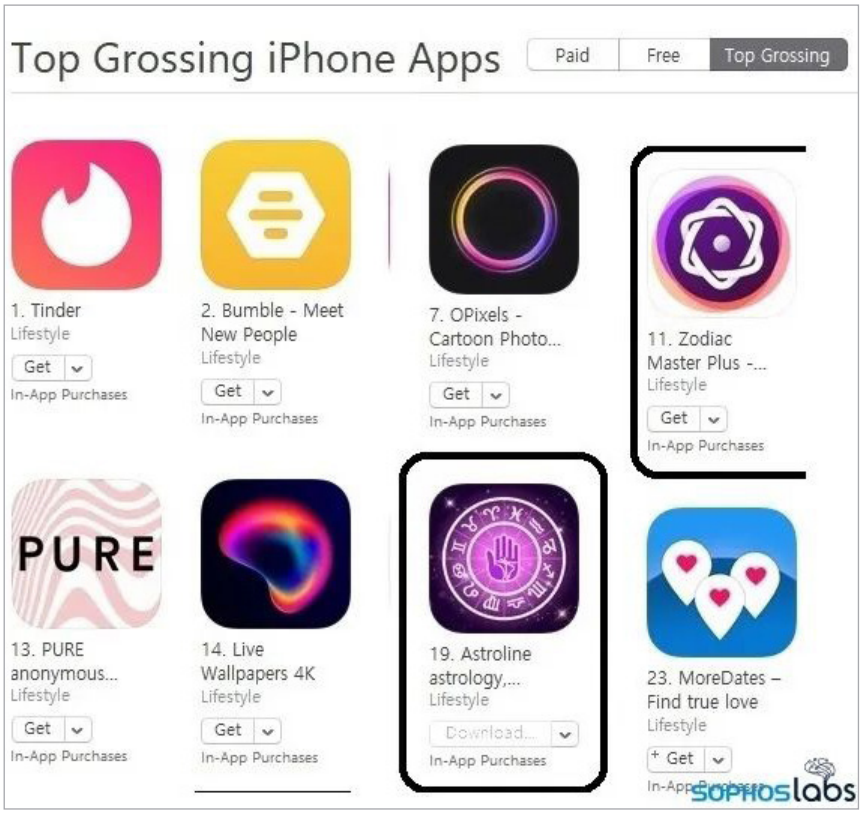
Fleeceware应用程序主要以“免费”为噱头吸引用户下载。而实际安装后，则会被告知注册订阅才能使用。之所以免费，则是Fleeceware应用有3-7天的免费试用期。

但是，当试用期一过，Fleeceware应用就会在不告知的情况下，自动收取高

额订阅费，即使使用者早已卸载应用，也会直接扣费。

原因二：潜伏APP畅销榜

免费的噱头之外，Fleeceware应用大量潜伏在App Store最畅销应用排名中，以迷惑用户下载。



此次，Sophos发现的Fleeceware应用中，一款名为Zodiac Master Plus应用，就名列第11大创收应用。

原因三：广告推广铺路

Fleeceware应用中招用户激增，与YouTube、Instagram、TikTok等社交媒体平台，亦或是其他应用展示的广告中，充斥的大量Fleeceware应用密不可分。

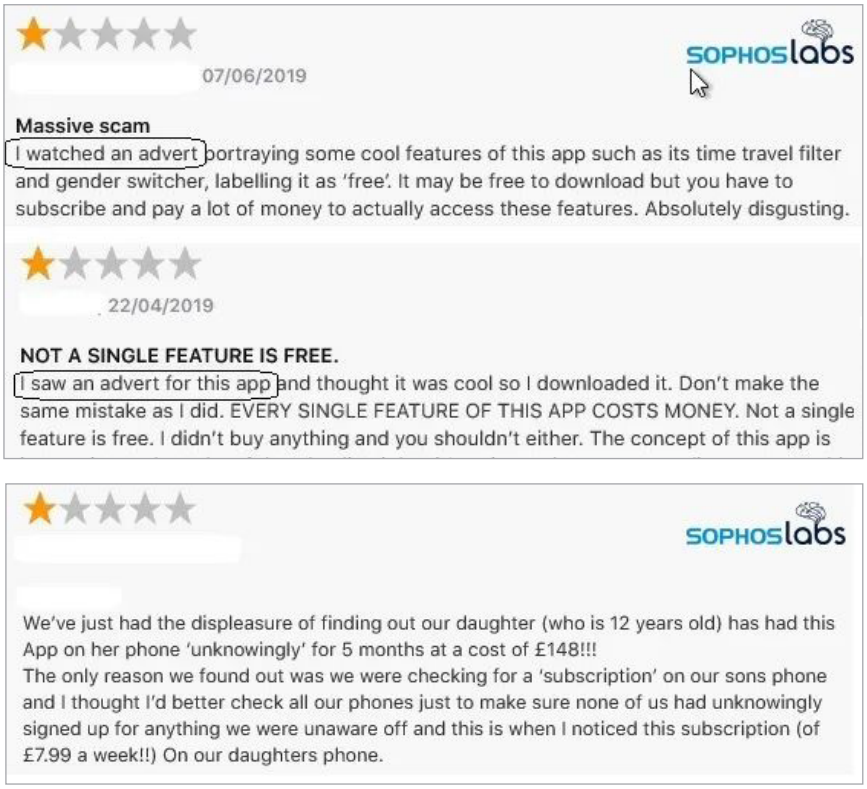
在广告引流的同时， App Store中Fleeceware应用的评论界面，还有大量五星好评，以迷惑普通用户。

杀软无法判别的Fleeceware应用

鉴于上述原因，Fleeceware应用数量与威胁不断提高，但对广大用户来说，杀毒与安全软件并不能有效判别和拦截Fleeceware应用。 相比于那些非法收集用户信息、弹出广告、强制安装的常规恶意软件，Fleeceware应用既不会窃取个人信息，也不会强制安装。或者严格来说，它只是滥用应用商店试用机制，牟取高额订阅费，却不带有安全威胁的应用程序。

一星评论辨真伪

杀软无法判别，应用商店又能上线。普通人想要辨别Fleeceware应用，就需要在应用程序的评论页找真相。那些中招用户，不仅有在评论页分享自己遭遇数百美金订阅费的情况，还有质疑官方App Store出现Fleeceware应用的言论。



（用户投诉被收取148英镑订阅费）

Fleeceware荼毒iOS/Android双平台

开篇，零日说这是2019年9月至今，Sophos第三次发布Fleeceware应用威胁报告。相比于此次专门披露iOS应用商店中的Fleeceware应用情况，前两次报告主要介绍了Android应用商店的情况。

Fleeceware Apps List

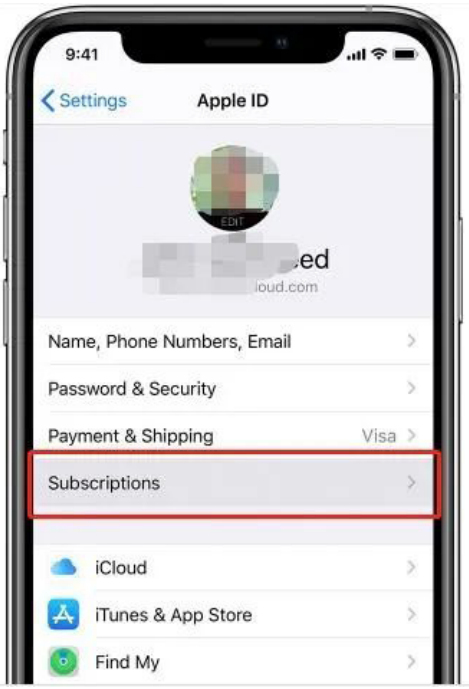
App Name	Weekly	Monthly	Yearly	Rank*	Download**	Revenue**
Seer App:Face, Horoscope, Palm	$7.99	$29.99	$79.99	#153	20k	$20k
Selfie Art – Photo Editor	£8.49	£24.49	£89.99	#14	500k	$700k
Palmistry Decoder	$8.99		$69.99	#23	300k	$600k
Lucky Life – Future Seer	$8.99	$24.99	$69.99	#40	200k	$200k
Life Palmistry – AI Palm & Tag	$7.99	$24.99	$79.99	#39	100k	$200k
Picsjoy-Cartoon Effect Editor	$7.99		$79.99	-	<5k	-
Aging seer – Faceapp,Horoscope	$7.99	$8.99	$59.99	-	<5k	-
Face Aging Scan-AI Age Camera	$8.99		$59.99	-	<5k	-
Face Reader – Horoscope Secret	$2.99	$9.99	$59.99	-	<5k	
Horoscope Secret	$9.99	$29.99	$74.99	-	<5k	-
CIAO – Live Video Chat		$19.99	$74.99	#66	60k	$80k
Astro Time & Daily Horoscope	$7.99	$19.99	$49.99	#106	20k	$30k
Video Recorder / Reaction	$2.99	$9.99	$49.99		<5k	
Crazy Helium Funny Face Editor	$4.99	$9.99	$49.99	#384	70k	$7k
Banuba: Face Filters & Effects	$7.99	$24.99	$79.99	#50	70k	$100k
QR Code Reader – Scanner		£8.99	£12.49	#444	<5k	$40k
QR Code Reader & Barcode PRO		$9.49	$47.99	#103	80k	$90k
Max Volume Booster	£9.99	£19.49	£48.99	#134	20k	<$5k
Face Reading – Horoscope 2020	$4.99	$15.99	$69.99	-	<5k	-
Forecast Master 2019	£8.99	£19.99		#134	<5k	$10k
mSpy Lite Phone Family Tracker		$49.99/quarter	$99.99	#3	1mil	$700k
Fortunescope: Palm Reader 2019	$9.99			#876	80k	$200k
Zodiac Master Plus – Palm Scan	$8.99	$22.99	$83.99	#9	200k	$500k
WonderKey-Cartoon Avatar Maker	$7.99	$18.99	$79.99	#18	30k	$60k
Avatar Creator – Cartoon Emoji	$8.99		$67.99	#52	200k	$100k
iMoji – Cartoon Avatar Emojis	£7.99	£19.49	£87.99	#55	10k	$20k
Life Insight-Palm & Animal Face	$8.99	$22.99	$69.99	#26	400k	$600k
Curiosity Lab-Fun Encyclopedia	£7.99	£25.49	£87.99	#80	10k	$9k
Quick Art: 1-Tap Photo Editor	£7.99	£25.49	£87.99	#157	20k	$8k
Astroline astrology, horoscope	$8.99	$19.99	$49.99	#20	200k	$300k
Celeb Twin - Who you look like	$5.99	$19.99	$59.99	#682	<5k	-
My Replica – Celebrity Like Me	£7.99	£19.99	£49.99	#56	90k	$70k
TOTAL (estimated in USA)					**3.5 Million** (approx. 3,680,000)	**$4.5 Million** (4,644,000)

（iOS应用商店Fleeceware 应用清单）

从受害用户来看，Android应用商店累计有6亿用户中招，远高于此次iOS应用商店的350万用户。但综合来看，必须要承认Fleeceware应用已经一步步成为主流手机操作系统的新隐患。

取消订阅防扣费

如果有用户不幸中招Fleeceware 应用，且已开启应用订阅服务，可在设置中取消订阅。iOS手机用户具体流程如下图：



零日反思

网络安全一直都是个复杂的议题，当人们热衷于病毒的围追堵截时，其他领域就可能爆发新的隐患。现如今Fleeceware应用的出现，就再次提醒我们，即使没有病毒或是安全漏洞，也并不会得到真正的安全，总会有新的安全隐患出现。

信息来源：

https://mp.weixin.qq.com/s/Wqov-hxV8YY5PaVrqy46UA

纽约支付初创公司不安全的数据库暴露数百万张信用卡信息

摘要：据外媒TechCrunch报道，一个存储着数百万张信用卡交易信息的庞大数据库，在公开暴露在互联网上近三周，该数据库属于Paay公司，这是一家位于纽约的信用卡支付处理商。与其他支付处理商一样，该公司代表销售商户（如网店和其他企业）验证支付，以防止欺诈性交易。

关键词：标签（Paay、数据库暴露、信用卡信息），技术问题（安全事件）。

内容：据外媒TechCrunch报道，一个存储着数百万张信用卡交易信息的庞大数据库，在公开暴露在互联网上近三周后，已经被保护起来。该数据库属于Paay公司，这是一家位于纽约的信用卡支付处理商。与其他支付处理商一样，该公司代表销售商户（如网店和其他企业）验证支付，以防止欺诈性交易。

但由于服务器上没有密码，任何人都可以访问里面的数据。

安全研究人员Anurag Sen发现了这个数据库。他告诉TechCrunch，他估计数据库中大约有250万条银行卡交易记录。在TechCrunch代表他联系了该公司后，数据库被下线。”4月3日，我们在一个服务上调出了一个新的实例，目前我们正在废止这个服务。”Paay联合创始人Yitz Mendlowitz说。”发生了一个错误，导致该数据库在没有密码的情况下被曝光。”

该数据库中包含了一些商户的每日刷卡记录，时间可追溯至2019年9月1日。TechCrunch查看了部分数据。每笔交易都包含了完整的明文信用卡号码、到期日和消费金额。这些记录还包含了每个信用卡号码的部分掩盖副本。这些数据不包括持卡人的姓名或卡片验证值，这使得信用卡更难被用来进行诈骗。

Mendlowitz对这一调查结果提出了质疑。”我们不存储卡号，因为我们没有用处。”TechCrunch向他发送了部分显示卡号明文的数据，但他没有回应后续报道。

这是今年以来第三家承认安全漏洞的支付处理商。今年1月，Sen发现另一家支付处理商的数据库遭曝光，其中存储着670万条记录。本月早些时候，另一名研究人员发现两家支付法院罚款和水电费的支付网站也留下了几个月的缓存数据暴露。

Mendlowitz表示，该公司正在通知15到20家商户，并表示该公司已经聘请了一位专家来了解安全漏洞的范围。

信息来源：

http://hackernews.cc/archives/30059

NSFOCUS

漏洞聚焦

微软月度更新修复多个在野利用 0-day 漏洞安全通告

发布时间：2020 年 4 月 15 日

综述

当地时间4月14日，微软最新的月度补丁更新中修复了113个安全问题，其中包括3个已被在野利用的0-day漏洞。这三个漏洞分布在 Windows Adobe Type Manager Library 和Windows 内核中。

另，据ZDI 报道，脚本引擎内存损坏漏洞CVE-2020-0968 在最初也被列为已遭利用的漏洞，但是后来修改了公告，指出它并未受到利用。

CVE-2020-1020、CVE-2020-0938

这是两个影响Windows Adobe Type Manager Library 的远程代码执行漏洞，微软曾在三月下旬发布通告提供了相应的缓解措施，本次月度更新中提供了补丁。

漏洞缘于Windows Adobe Type Manager Library在处理multi-master字体（Adobe Type 1 PostScript格式）时存在缺陷。

对于除Windows 10以外的所有系统，成功利用该漏洞的攻击者可以远程执行代码。对于运行Windows 10的系统，成功利用该漏洞的攻击者可以在AppContainer沙盒上下文中以有限的权限执行代码。

受影响版本及更多详情参考以下官方通告。

官方通告链接：

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1020

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0938

CVE-2020-1027

这是一个Windows内核特权提升漏洞。

漏洞存在于Windows内核处理内存中对象的过程中。成功利用此漏洞的攻击者能够以提升后的权限执行代码。

受影响版本及更多详情参考以下官方通告。

官方通告链接：

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1027

CVE-2020-0968

在 Internet Explorer 中，脚本引擎在处理内存中对象的过程中存在一个远程代码执行漏洞。

该漏洞可破坏内存，使攻击者在当前用户的上下文中执行任意代码。成功利用此漏洞的攻击者可获得与当前用户相同的权限。如果当前用户以管理用户权限登录，成功利用漏洞的攻击者可以完全控制受影响的系统。

受影响版本及更多详情参考以下官方通告。

官方通告链接：

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0968

解决方案

官方已针对受支持系统版本发布修复了以上漏洞的安全补丁，强烈建议受影响用户尽快安装补丁更新。

不能及时安装更新的用户请查看官方通告采取相应缓解措施。

Adobe 带外更新修复多款产品关键漏洞安全通告

发布时间：2020 年 4 月 29 日

综述

当地时间4月28日，Adobe官方发布带外更新，修复了Adobe 多款产品中的多个漏洞，产品包括Magento、Adobe Illustrator 和Adobe Bridge。

官方通告地址：

https://helpx.adobe.com/security.html

漏洞概述

Magento

Adobe发布的 Magento 带外安全更新，共修复了10个关键及重要漏洞。

Adobe 官方指定以下更新优先级为2级。（优先级定义详见下文解决方案中Adobe优先级评估系统）。

漏洞概括如下：

漏洞类别	漏洞影响	严重程度	预认证?	需要管理员权限?	CVE 编号
命令注入	任意代码执行	Critical	No	Yes	CVE-2020-9576
命令注入	任意代码执行	Critical	No	Yes	CVE-2020-9578
安全缓解绕过	任意代码执行	Critical	No	Yes	CVE-2020-9579

漏洞类别	漏洞影响	严重程度	预认证?	需要管理员权限?	CVE 编号
安全缓解绕过	任意代码执行	Critical	No	Yes	CVE-2020-9580
命令注入	任意代码执行	Critical	No	Yes	CVE-2020-9582
命令注入	任意代码执行	Critical	No	Yes	CVE-2020-9583
XSS (Stored)	敏感信息泄露	Important	Yes	No	CVE-2020-9577
XSS (Stored)	敏感信息泄露	Important	No	Yes	CVE-2020-9581
XSS (Stored)	敏感信息泄露	Important	Yes	No	CVE-2020-9584
可观测的时间差异	签名验证绕过	Important	No	Yes	CVE-2020-9588

关于漏洞的具体影响版本及修复情况，请参考Adobe官方安全通告：
https://helpx.adobe.com/security/products/magento/apsb20-22.html

Adobe Illustrator

Adobe发布的Adobe Illustrator带外更新，修复了5个关键漏洞。

Adobe 官方指定以下更新优先级为3级。（优先级定义详见下文解决方案中Adobe优先级评估系统）。

漏洞概括如下：

漏洞类别	漏洞影响	严重程度	CVE 编号
内存损坏	任意代码执行	Critical	CVE-2020-9570 CVE-2020-9571 CVE-2020-9572 CVE-2020-9573 CVE-2020-9574

关于漏洞的具体影响版本及修复情况，请参考Adobe官方安全通告：
https://helpx.adobe.com/security/products/illustrator/apsb20-20.html

Adobe Bridge

Adobe发布的Adobe Bridge带外更新，修复了17个关键及重要漏洞。

Adobe 官方指定以下更新优先级为3级。（优先级定义详见下文解决方案中Adobe优先级评估系统）。

漏洞概括如下：

漏洞类别	漏洞影响	严重程度	CVE 编号
基于栈的缓冲区溢出	任意代码执行	Critical	CVE-2020-9555
堆溢出	任意代码执行	Critical	CVE-2020-9562 CVE-2020-9563
内存损坏	任意代码执行	Critical	CVE-2020-9568
越界写入	任意代码执行	Critical	CVE-2020-9554 CVE-2020-9556 CVE-2020-9559 CVE-2020-9560 CVE-2020-9561 CVE-2020-9564 CVE-2020-9565 CVE-2020-9569
UAF	任意代码执行	Critical	CVE-2020-9566 CVE-2020-9567
越界读取	信息泄露	Important	CVE-2020-9553 CVE-2020-9557 CVE-2020-9558

关于漏洞的具体影响版本及修复情况，请参考Adobe官方安全通告：

https://helpx.adobe.com/security/products/bridge/apsb20-19.html

解决方案

Adobe官方已发布修复了上述漏洞的新版本，建议用户参考 Adobe优先级评估系统 给出的建议修复时间，按时升级防护。

详细信息及操作可参考各产品漏洞部分的官方通告链接。

Adobe优先级评估系统

Adobe优先级评估可帮助客户确定Adobe安全更新的优先级。官方根据相关产品的历史攻击模式，漏洞类型，受影响的平台以及任何可能的缓解措施来确定优先级。

评级	描述
1 级	表示此更新修复的是针对特定产品和平台，已被在野利用的漏洞，或极易成为目标的高风险漏洞。 Adobe 建议管理员尽快安装此更新（比如在 72 小时内）。
2 级	表示此更新修复的是历来被攻击风险较高产品中的漏洞，不过当前还未发现利用行为。根据以往的经验，官方认为不会马上遭到利用。 Adobe 建议管理员尽快安装更新 (例如在 30 天内)。
3 级	表示此更新修复的是历来被攻击风险较低产品中的漏洞。Adobe 建议管理员酌情安装更新。

https://helpx.adobe.com/security/severity-ratings.html

Git 凭证泄露漏洞（CVE-2020-5260）安全通告

发布时间：2020 年 4 月 16 日

综述

近日，Git发布安全通告公布了一个可能泄露Git用户凭证的漏洞（CVE-2020-5260）。

Git使用凭证助手(credential helper)来帮助用户存储和检索凭证。但是当一个URL中包含经过编码的换行符时，可能将非预期的值注入到credential helper的协议流中。这将使恶意URL欺骗Git客户端去向攻击者发送主机凭据。当使用受影响版本 Git对恶意 URL 执行 git clone 命令时会触发该漏洞。

参考链接：

https://github.com/git/git/security/advisories/GHSA-qm7j-c969-7j4q

受影响版本

- ☐ Git 2.17.x <= 2.17.3
- ☐ Git 2.18.x <= 2.18.2
- ☐ Git 2.19.x <= 2.19.3
- ☐ Git 2.20.x <= 2.20.2
- ☐ Git 2.21.x <= 2.21.1
- ☐ Git 2.22.x <= 2.22.2
- ☐ Git 2.23.x <= 2.23.1
- ☐ Git 2.24.x <= 2.24.1
- ☐ Git 2.25.x <= 2.25.2
- ☐ Git 2.26.x <= 2.26.0

不受影响版本

- ☐ Git 2.17.4
- ☐ Git 2.18.3
- ☐ Git 2.19.4
- ☐ Git 2.20.3
- ☐ Git 2.21.2
- ☐ Git 2.22.3
- ☐ Git 2.23.2
- ☐ Git 2.24.2
- ☐ Git 2.25.3
- ☐ Git 2.26.1

解决方案

官方已发布修复了漏洞的新版本，建议受影响用户及时下载更新。

https://github.com/git/git/releases

另外，还提供了其他方法解决或规避该问题：

- 禁用credential helper

```
git config --unset credential.helper
git config --global --unset credential.helper
git config --system --unset credential.helper
```

- 提防恶意URL

1、git clone时检查URL的主机名和用户名部分是否存在编码的换行符（%0a）或凭据协议注入的证据（例如host=github.com）

2、避免将子模块与不受信任的仓库一起使用（不要使用 clone --recurse-submodules；只有在检查.gitmodules中找到url之后，才使用git submodule update）。

3、避免对不信任的URL执行 git clone。

声 明

Oracle Coherence 远程代码执行漏洞（CVE-2020-2915）安全通告

发布时间：2020 年 4 月 15 日

综述

当地时间4月14日，Oracle发布2020年4月关键补丁更新（Critical Patch Update，简称CPU），其中包括一个针对Oracle Coherence ，评分为 9.8的严重漏洞（CVE-2020-2915）。

漏洞允许未经身份验证的攻击者通过T3协议网络访问并破坏易受攻击的Oracle Coherence，成功的漏洞利用可导致Oracle Coherence被攻击者接管，从而造成远程代码执行。

使用了Oracle Coherence库的产品受此漏洞影响，在WebLogic Server 11g Release（10.3.4）及以上版本的安装包中默认集成了Oracle Coherence库。

参考链接：

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

受影响产品版本

- ☐ Oracle Coherence 3.7.1.0
- ☐ Oracle Coherence 12.1.3.0.0
- ☐ Oracle Coherence 12.2.1.3.0
- ☐ Oracle Coherence 12.2.1.4.0

ORACLE®
WebLogic Server

解决方案

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

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

缓解措施：

若用户暂时不能安装最新补丁，可通过禁用T3协议，对漏洞进行临时缓解。

官方通告：

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

Weblogic 远程代码执行漏洞安全通告

发布时间：2020 年 4 月 15 日

综述

北京时间2020年4月15日，Oracle发布2020年4月关键补丁更新（Critical Patch Update，简称CPU），此次更新共修复了397个危害程度不同的安全漏洞。

其中包括三个针对 WebLogic Server，评分为 9.8的严重漏洞（CVE-2020-2801、CVE-2020-2883、CVE-2020-2884）。

以上漏洞允许未经身份验证的攻击者通过T3协议网络访问并破坏易受攻击的WebLogic Server，成功的漏洞利用可导致WebLogic Server被攻击者接管，从而造成远程代码执行。

参考链接：

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

受影响产品版本

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

解决方案

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

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

缓解措施：

若用户暂时不能安装最新补丁，可通过禁用T3协议，对漏洞进行临时缓解。

官方通告：

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

NSFOCUS

安全态势

互联网安全威胁态势

行业动态回顾

1. 中国银保监会：《个人保险实名制管理办法 (征求意见稿)》公开征求意见

【概述】

为建立健全个人保险实名管理制度，规范保险业务行为，保护投保人、被保险人、受益人合法权益，根据《中华人民共和国保险法》《中华人民共和国消费者权益保护法》《中华人民共和国反洗钱法》等法律、行政法规，中国银保监会起草了《个人保险实名制管理办法（征求意见稿）》（以下简称《办法》），现向社会公开征求意见。

【参考链接】

http://www.cbirc.gov.cn/cn/view/pages/ItemDetail.html?docId=899570&itemId=915

2.《2019网信自主创新调研报告》正式发布

【概述】

2020年4月19日，由中国关键信息基础设施技术创新联盟组织编写的《2019网信自主创新调研报告》（以下简称《报告》）通过线上平台正式发布。《报告》以供应链安全为主线，对各个领域面临的供应链安全问题进行了分析和梳理，从一线厂商的视角回答了供应链安全问题“是什么”、“为什么”和“怎么办”的问题。

【参考链接】

https://www.secrss.com/articles/18779

3. 我国跨部委打击危害公民个人信息和数据安全违法犯罪长效机制成立

【概述】

为持续保持对侵犯公民个人信息犯罪的高压严打态势，从源头上治理公民个人信息被泄露、隐私被侵犯的安全隐患，促进、提高行政机关、企事业单位对公民个人信息和数据安全的保护能力，形成源头治理、综合治理、系统治理的工作格局，经中央领导批准，公安部与中央网信办牵头，建立打击危害公民个人信息和数据安全违法犯罪长效机制（以下简称机制）。机制成员单位包括：公安部、中央网信办、最高人民法院、最高人民检察院、工业和信息化部、国家市场监督管理总局等。

【参考链接】

https://www.secrss.com/articles/18670

4. 国内首份零信任安全白皮书：全面解读零信任安全架构

【概述】

企业的网络基础设施日益复杂，安全边界逐渐模糊。数字化转型的时代浪潮推动着信息技术的快速演进，云计算、大数据、物联网、移动互联等新兴IT技术为各行各业带来了新的生产力，但同时也给企业网络基础设施带来了极大的复杂性。企业的安全边界正在逐渐瓦解，传统的基于边界的网络安全架构和解决方案难以适应现代企业网络基础设施。

【参考链接】

https://www.secrss.com/articles/18624

5. 绿盟科技在RSAC热点研讨会带来的干货

【概述】

4月17日由中国计算机学会主办，CCF计算机安全专业委员会、绿盟科技集团和360 集团承办的“第十二届信息安全高级云论坛暨美国RSA热点研讨会”，以“以人为本”为话题，邀请了18位行业专家，共同分享、解读对今年 RSAC 的理解和收获。绿盟科技的三个议题，重点介绍对中美网安产业的深度观察、针对今年创新沙盒对网安创新方向的解读，以及从安全运营实例来谈更契合国情、对安全工作更具指导价值的思考。

【参考链接】

http://blog.nsfocus.net/rsac-share-0421/

6. 绿盟科技预警业务体系建设实践

【概述】

为达到可以低投入、高效率帮助一线解决突发性安全事件的目标，能真正的帮助客户解决突发威胁而带来的脆弱性问题。绿盟科技安全预警业务在这样的背景下迈出了第一步，然后一点点完善扩充，最后打通公司内部多个部门和业务流程，成为了公司内部运营的一部分。

【参考链接】

https://mp.weixin.qq.com/s/IvUJU8TwuKm4gafNvWHT3g

7. 境外黑客利用深信服SSL VPN进行攻击

【概述】

境外黑客组织“DarkHotel”通过非法手段控制部分深信服SSL VPN设备，并利用客户端升级漏洞（本次漏洞为SSL VPN设备Windows客户端升级模块签名验证机制的缺陷）下发恶意文件到客户端，从而进行APT攻击活动。绿盟威胁情报中心已支持对该事件的检测。

【参考链接】

https://mp.weixin.qq.com/s/FyZGfe2TLibru3CRgcjFiw

8. 新型勒索软件WannaRen

【概述】

近日，网络上出现一种新型勒索病毒“WannaRen”并在PC上开始传播。该勒索软件会加密Windows系统中几乎任何文件，并且以“.WannaRen”后缀命名。攻击者留下比特币钱包并索取0.05比特币。目前该勒索软件影响Windows 7与Windows 10系统。

【参考链接】

http://blog.nsfocus.net/

9. 黑客利用nCoV-19疫情信息在西班牙投放SmokeLoader

【概述】

自covid-19肺炎病毒在世界范围内爆发以来，绿盟科技伏影实验室密切关注该时事话题在黑客产业链中的利用情况。近期，伏影实验室发现了新的利用疫情话题传播的邮件木马，隐藏在其中的攻击流程显示黑客已将现阶段的主流攻击手法与疫情诱饵结合起来，给疫情诱饵邮件的大规模传播制造了条件。

【参考链接】

http://blog.nsfocus.net/smokeloader-0407/

10. Vollgar运动-针对运行MS-SQL服务的Windows系统

【概述】

近期发现一个长期运行的攻击活动Vollgar，该活动旨在感染运行MS-SQL服务器的Windows计算机，使用密码暴力破解受害者计算机，部署多个后门并执行

多个恶意模块，受害者分布在中国、印度、韩国、土耳其和美国等国家，受影响的行业涵盖医疗、航空、IT、电信、教育等多个领域。

【参考链接】

https://www.guardicore.com/2020/04/vollgar-ms-sql-servers-under-attack/

11. 攻击者利用Zoom视频会议应用传播恶意软件

【概述】

近期发现攻击者将恶意软件伪装成合法Zoom视频会议软件，主要针对由于冠状病毒爆发而在家工作的用户。恶意程序不仅分布在Google Play上，还针对在Droids上加载应用程序的用户。其中还发现专门针对中国用户的Zoom APK，该恶意软件会在启动时询问电话、位置和照片权限。

【参考链接】

https://labs.bitdefender.com/2020/03/infected-zoom-apps-for-android-target-work-from-home-users/

12. Raccoon信息窃取器滥用谷歌云服务

【概述】

Raccoon恶意软件于2019年4月首次被发现，具有信息窃取功能，能够窃取登录凭证、信用卡信息、加密货币钱包和浏览器信息。近期发现Raccoon使用漏洞利用攻击包Fallout和Rig的攻击活动，攻击者滥用谷歌云服务使Raccoon规避检测，受影响国家包含印度、日本、哥伦比亚、加拿大和美国等。

【参考链接】

https://blog.trendmicro.com/trendlabs-security-intelligence/raccoon-stealers-abuse-of-google-cloud-services-and-multiple-delivery-techniques/

13. Holy water:针对亚洲的水坑攻击活动

【概述】

近期发现一个针对亚洲宗教机构和组织的水坑攻击活动，该活动至少自2019年5月以来一直活跃，攻击者利用虚假Adobe Flash更新以分发恶意软件。

【参考链接】

https://securelist.com/holy-water-ongoing-targeted-water-holing-attack-in-

asia/96311/

14. polaris僵尸网络攻击全球Netlink路由器

【概述】

近期绿盟科技格物实验室发现针对Netlink GPON路由器RCE漏洞的利用行为。在2020年3月18日Netlink GPON路由器的远程执行漏洞被公布不久，polaris僵尸网络便通过该漏洞传播其样本，导致攻击源数量、攻击次数以及捕获到攻击的节点数量均呈上升趋势。

【参考链接】

https://mp.weixin.qq.com/s/9xEVrC5UzyuCF56Es1ppGA

15. xHelper木马针对Android手机进行大规模攻击

【概述】

xHelper木马在2019年10月被发现开始针对Android手机进行大规模攻击，但即使现在，该木马仍然向以前一样活跃。xHelper是极具攻击性的木马软件，它将自己伪装成一款手机清理加速应用程序，安装之后在主屏幕或程序菜单自动隐藏，即使找到并删除它甚至恢复出厂设置也无用，它仍会保留在那里，而且可以安装后门向其他恶意软件暴露用户的数据。

【参考链接】

https://securelist.com/unkillable-xhelper-and-a-trojan-matryoshka/96487/

16. APT41利用Zoho ManageEngine中漏洞针对法律相关实体

【概述】

近期APT41组织利用Zoho ManageEngine的零日漏洞CVE-2020-10189攻击美国、欧洲地区的法律相关部门。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以及出于经济动机的入侵活动。

【参考链接】

https://www.darktrace.com/en/blog/catching-apt-41-exploiting-a-zero-day-vulnerability/

17. Kinsing恶意软件针对容器环境的攻击

【概述】

近期针对容器环境的攻击数量在增加。攻击者利用不受保护的开放Docker API端口来运行一个带有Kinsing恶意软件的Ubuntu容器，该恶意软件运行一个加密器，然后试图将恶意软件传播到其他容器和主机上。

【参考链接】

https://blog.aquasec.com/threat-alert-kinsing-malware-container-vulnerability

18. WINDSHIFT组织针对中东的网络间谍活动

【概述】

WINDSHIFT是一个从事高针对性的网络间谍活动的组织，针对整个中东地区的政府部门和关键基础设施工作的特定个人，攻击活动中WindTail是该组织使用的第一阶段macOS植入程序，通过滥用macOS对自定义URL方案的支持来远程感染macOS目标。

【参考链接】

https://www.virusbulletin.com/virusbulletin/2020/04/vb2019-paper-cyber-espionage-middle-east-unravelling-osxwindtail/

19. FIN6组织在攻击活动中分发Anchor和PowerTrick后门

【概述】

近两年来，有组织的网络犯罪集团之间的合作日益加强。FIN6是一个有组织的网络犯罪团伙，自2015年以来一直很活跃，主要针对美国和欧洲的实体零售商和酒店行业的POS机。近期其与TrickBot合作使用Anchor和PowerTrick对企业网络进行针对性的攻击。另外，FIN6的目标包括但不限于电子商务环境和勒索软件。

【参考链接】

https://securityintelligence.com/posts/itg08-aka-fin6-partners-with-trickbot-gang-uses-anchor-framework/

20. Hoaxcalls僵尸网络利用Grandstream和DrayTek设备漏洞传播

【概述】

Hoaxcalls是一个新的DDoS僵尸网络，利用Grandstream和DrayTek设备漏洞在全球范围内广泛传播，它通过IRC与C2服务器通信，接收到C2命令后，可以使用CVE-2020-8515和CVE-2020-5722漏洞通过扫描和感染易受攻击的设备进行传播。目前已有许多Grandstream UCM6200和Draytek Vigor设备被感染或攻击。

【参考链接】

https://unit42.paloaltonetworks.com/new-hoaxcalls-ddos-botnet/

21. 微软月度更新修复多个在野利用0-day漏洞

【概述】

当地时间4月14日，微软最新的月度补丁更新中修复了113个安全问题，其中包括3个已被在野利用的0-day漏洞。这三个漏洞分布在Windows Adobe Type Manager Library和Windows内核中。

【参考链接】

http://blog.nsfocus.net/msrc-security-updates-0415/

22. Oracle全系产品2020年4月关键补丁更新

【概述】

当地时间2020年4月14日，Oracle官方发布了2020年4月关键补丁更新公告CPU（Critical Patch Update），安全通告以及第三方安全公告等公告内容，修复了397个不同程度的漏洞。

【参考链接】

http://blog.nsfocus.net/oracle-0415/

23. Adobe4月安全更新

【概述】

当地时间4月14日，Adobe官方发布了4月安全更新，修复了Adobe多款产品的多个漏洞，包括Adobe ColdFusion、Adobe After Effects和Adobe Digital Editions。

【参考链接】

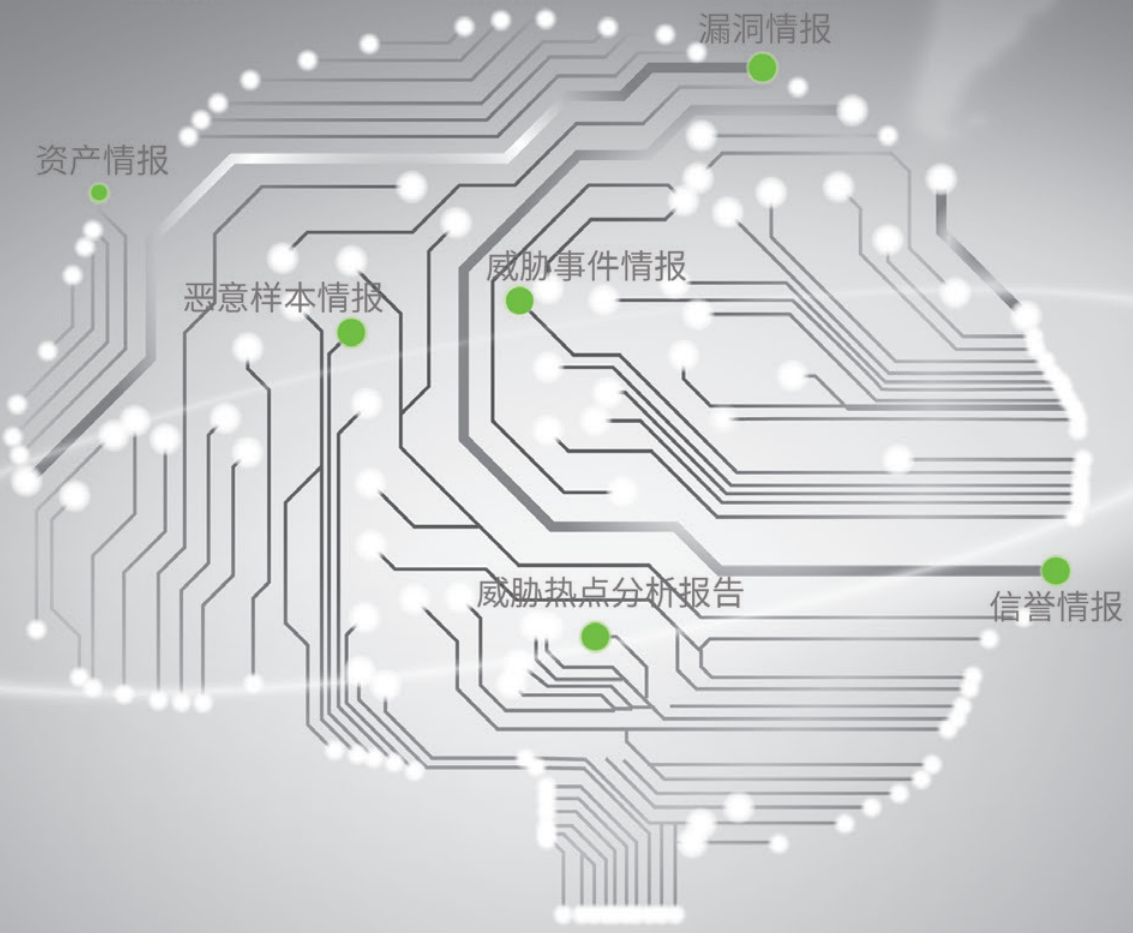
http://blog.nsfocus.net/adobe-0415/

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