[公开]360NELab-DST-0-013-20201012

大数据协同安全技术
国家工程实验室
National Engineering Laboratory for Big Data Collaborative Security Technology

全球数据安全观察

总第 13 期 2020 年第 13 期

（2020.9.28-2020.10.11）

大数据协同安全技术国家工程实验室

摘要

本期全球数据安全观察搜集到的重要事件主要是勒索软件、数据泄露及国外政府对数据安全的政策与重视程度。

勒索软件：

美国保险巨头 Arthur J. Gallagher 遭遇勒索软件袭击

Egregor 勒索软件导致数据泄露事件激增

Netwalker 勒索软件运营商泄露了盗取的 K-Electric 数据

最大的邮轮运营商 Carnival 确认勒索软件盗取数据

新泽西州医院向勒索软件团伙支付了 67 万美元，以防止数据泄漏

数据泄露：

零售商 BrandBQ 泄漏了 1 TB 的客户和承包商数据

美国国土安全部：不明黑客袭击了美国人口普查局网络

阿联酋国际航空公司的数据在多个暗网论坛上泄露

北美中餐外卖平台 Chowbus 80 万条用户信息被泄露

澳大利亚社交新闻平台泄露了 80000 条用户数据

政策与重视程度：

美国商务部对电子数据取证等六项新技术多边控制

美国防部数据战略支撑联合全域作战

印尼希望今年颁布《个人数据保护法》

此外，在数据安全技术与观点方面主要讨论了：

敏感数据的发现；勒索软件对企业成本的影响；二维码安全；加密与中间人攻击；零信任架构；数据库审计；双因素身份认证；数据分类分级。

全球动态

1. 美国保险巨头 Arthur J. Gallagher 遭遇勒索软件袭击

总部位于美国的全球保险经纪和风险管理公司 ArthurJ.Gallagher（AJG） 证实了一次勒索软件攻击，该公司的系统在 2020 年 9 月 26 日遭到攻击。

https://www.bleepingcomputer.com/news/security/ransomware-hits-us-based-arthur-j-gallagher-insurance-giant/

2. Egregor 勒索软件导致数据泄露事件激增

2020 年 10 月 3 日，据安全研究人员最近发布的警告称，最近发现的一种名为 Egregor 的勒索软件变种，在过去几个月里，它似乎已经感染了全球约 12 家组织。与 Maze 和 Sodinokibi 等其他勒索团伙一样，Egregor 勒索软件的运营商威胁说，如果三天内勒索要求得不到满足，他们将泄露受害者的数据。

https://www.databreachtoday.com/egregor-ransomware-adds-to-data-leak-trend-a-15110

3. 零售商 BrandBQ 泄漏了 1 TB 的客户和承包商数据

2020 年 10 月 1 日报道，研究人员发现的一个新的数据

库泄漏，原因是 Elasticsearch 服务器配置错误。研究人员将这个数据库归属于 BrandBQ ，一家波兰在线时尚零售公司。该公司 APP 仅安卓系统就有超过 50 万次的下载，加上 iOS 的安装，受影响的用户数量是巨大的，估计多达 670 万人。暴露的数据量超过 1TB，记录数量为 10 亿条，包括公司客户的一系列个人识别信息（PII），如全名、电子邮件地址、电话号码和无卡号的支付详情。

https://www.hackread.com/fashion-retailer-brandbq-expose-customers-data/

4. Netwalker 勒索软件运营商泄露了盗取的 K-Electric 数据

2020 年 10 月 1 日报道，巴基斯坦最大的私营电力公司 K-Electric（KE） 遭遇 Netwalker 勒索软件攻击，阻断了计费和在线服务。 Netwalker 勒索软件运营商要求支付价值 385 万美元的比特币。与往常一样，如果公司在另外 7 天内不支付赎金，赎金将增至 770 万美元。最近，由于 K-Electric 没有支付赎金，Netwalker 勒索软件运营商泄漏了被盗数据。

https://securityaffairs.co/wordpress/109000/hacking/k-electric-netwalker-data-leak.html

5. 美国国土安全部：不明黑客袭击了美国人口普查局网络

2020 年 10 月 9 日报道，美国国土安全部表示，在本周初发布的首份国土威胁评估（HTA）报告中未知威胁者已将美国人口普查网络作为目标。针对美国人口普查的网络活动可能包括试图非法获取人口普查收集的大量数据；更改人口普查注册数据；破坏人口普查基础设施供应链或进行拒绝服务攻击。

https://www.bleepingcomputer.com/news/security/dhs-unknown-hackers-targeted-the-us-census-bureau-network/

6. 美国商务部对电子数据取证等六项新技术实施多边控制

2020 年 10 月 5 日，美国商务部工业与安全局（BIS）发布了一项最终规则，对 6 项"新兴技术"实行新的多边管制，其中就包括电子数据取证相关的技术，该规则在 2019 年 12 月的《常规武器和两用货物及技术出口管制瓦塞纳尔协定》全体会议上达成一致。

https://www.secrss.com/articles/26140

7. 美国防部数据战略支撑联合全域作战

2020 年 10 月 8 日，美国国防部发布了首份数据战略，重点聚焦利用国防部数据支撑联合全域作战。该战略提出了

国防部成为“数据中心组织”所需要的原则、重要能力以及终极目标，重点聚焦联合全域作战、高级领导层决策支撑以及业务分析。国防部信息技术负责人在发布会前几周表示，联合作战行动是最重要的领域。

http://www.hbradio.com.cn/junshi/2020/1010/179079.html

8. 阿联酋国际航空公司的数据在多个暗网论坛上泄露

2020 你去哪 10 月 8 日报道，阿联酋国际航空公司是任何旅行和物流要求方面的领先公司。它拥有 200 多名员工，收入约为 2.5 亿美元。数据泄漏是由服务器配置错误而导致的，其中服务器包含 60 个目录，每个目录约有 5,000 个文件。

https://securityaffairs.co/wordpress/109237/data-breach/airlink-international-uae-data-leak.html

9. 最大的邮轮运营商 Carnival 确认勒索软件盗取数据

2020 年 10 月 12 日，全球最大的邮轮运营商嘉年华公司（Carnival Corporation）证实，8 月勒索软件攻击期间，客户、员工和船员的个人信息被盗。嘉年华在大约 150 个国家/地区拥有 150,000 多名员工，每年接待 1300 万以上的客人。

https://www.bleepingcomputer.com/news/security/largest-cruise-line-operator-carnival-confirms-ransomware-data-theft/

10.北美中餐外卖平台 Chowbus 80 万条用户信息被泄露

2020 年 10 月 8 日，华人送餐平台 Chowbus 的很多用户收到一封来自该平台的系统发送邮件。在这个名为“Chowbus Data”的邮件里，竟然可以直接打包下载餐厅和用户的私密信息。其中，4300 条餐厅数据、803350 条用户数据遭泄露。该邮件涵盖了餐厅的姓名、地址、电话、佣金率以及用户的姓名、注册邮箱、电话和完整住址。

https://securityaffairs.co/wordpress/109224/data-breach/food-delivery-service-chowbus-hack.html

11.澳大利亚社交新闻平台泄露了 80000 条用户数据

2020 年 10 月 5 日，Cyber News 调查小组发现了一个属于澳大利亚新闻共享平台 Snewpit 的暴露数据桶。不安全的存储桶包含将近 80,000 条用户记录，包括用户名，全名，电子邮件地址和个人资料图片。

https://securityaffairs.co/wordpress/109108/data-breach/snewpit-leaks-80000-records.html

12.印尼希望今年颁布《个人数据保护法》

印度尼西亚通信和信息技术部宣布，《个人数据保护法》

的最终草案已提交印度尼西亚总统。媒体已获悉，他们希望该法律草案将于今年颁布，该法案类似类似于欧盟的 GDPR。
https://securityaffairs.co/wordpress/109198/laws-and-regulations/indonesia-personal-data-protection-law.html

13.新泽西州医院向勒索软件团伙支付了 67 万美元，以防止数据泄漏

2020 年 10 月 3 日，据外媒报道，新泽西州纽瓦克市的新泽西大学医院本月支付了 67 万美元的勒索软件需求，以防止发布 240 GB 的被盗数据，包括患者信息。对医院的攻击来自一个名为 SunCrypt 的勒索软件，该程序渗透到网络中，窃取未加密的文件，然后对所有数据进行加密。SunCrypt 公开发布了属于新泽西大学医院的 48,000 个文档的档案后，医院的代表通过其暗网上的支付门户联系到了威胁参与者，以协商停止进一步发布患者数据。
https://www.bleepingcomputer.com/news/security/new-jersey-hospital-paid-ransomware-gang-670k-to-prevent-data-leak/

业界观点

1. 敏感数据发现能力对企业的重要性

数据安全第一阶段永远离不开的问题——数据在哪里，也就是我们常说的对敏感数据的发现能力。只有知道敏感数据在哪里才能将重要的精力资源投入到需要重点保护的数据资产上。

数据安全的基础的发现能力可以协同数据库部门或者从业务侧首先开展，从数据部门切入可以更快的实现安全部门与数据库部门的协同工作闭环运营，主要因为数据库有需要的数据资源，安全部有数据分类分级使用上的需求分析能力，二者相结果，可以最短路径实现数据安全运营落地闭环。

https://www.freebuf.com/articles/database/251055.html

2. Lumu 发布 2020 勒索软件影响与企业应对成本信息图，勒索软件威胁日益严重

勒索软件攻击已在去年出现了急剧增加的趋势，并且安全研究行业已将之视为一个日益严重的问题。为帮助大家更好地了解勒索软件问题的严重性，Lumu 特地制作了一幅信息图。预计今年，勒索软件能够以单次超 400 万美元的攻击成本，将全球应对代价推升至 200 亿美元。令人担忧的

是，有 36% 的受害者向恶意攻击者支付了赎金。可即便如此，这批受害者中的 17% 还是没能挽回他们的数据。

http://hackernews.cc/archives/32452

3. 应急响应检测阶段技术流程

应急响应有六阶段模型(准备，检测，抑制，根除，恢复，跟踪)。其中检测阶段就是应急响应技术人员发挥技术能力，弄清楚整个事件的过程。而在此过程中，往往是以经验主导进行开展工作，没有技术流程模型作为指导。因此，在这里参照工作经验，意图总结出一个指导在检测阶段如何开展工作的"点线面"模型，供初次无经验应急响应人员参考。从进场确定事件输入点开始，根据攻击时间线初步还原受害主机被攻击情况，从而确定受害主机的受影响面，内网扩散面。最后根据“点-线-面”结果进行倒推溯源。

https://www.freebuf.com/articles/neopoints/251560.html

4. 跨境电子取证与数据主权问题

(1) 电子证据是打击跨境网络犯罪的关键。

与传统犯罪不同，借助于现代网络技术，网络犯罪可以是集团化大范围、大跨度作案。使用电子数据是打击网络犯罪的“最佳方式”。由此，打击跨境网络犯罪的核心问题十

分明显：如何进行跨境电子取证以及如何保证电子数据真实性、完整性、合法性。

(2) 跨境单边电子取证对国家网络数据主权的影响。

一国对位于其境内存储介质中的数据拥有主权，另一国若仅凭国内规定就直接对该国计算机系统进行远程调查取证，很有可能被认定为侵犯该国的数据主权，进而可能导致外交风险。2020 年 6 月 1 日即将生效的《网络安全审查办法》进一步明确了电子数据主权的重要性，该办法第一条规定："为了确保关键信息基础设施供应链安全，维护国家安全，依据《中华人民共和国国家安全法》《中华人民共和国网络安全法》，制定本办法。"可见，关键信息基础设施中的数据与国家安全息息相关，出于维护国家安全的考虑，数据主权是必须要声明和主张的。

https://www.pkulaw.com/lawfirmarticles/7ce8a19d181909811808877c2ac55b01bdfb.html

5. 二维码：一种隐秘的安全威胁

去年就有研究人员发现了一种新的网络钓鱼活动，该活动利用二维码将受害者重定向到网络钓鱼登陆页面，有效规避了旨在阻止此类攻击的安全解决方案和控制措施。比如去年针对法国的网络钓鱼攻击背后的攻击者就是使用了二维

码编码的 URL 来绕过分析和阻止可疑的安全软件。由于二维码发布没有任何限制，二维码生成器又随时可从网上获得，因此很容易被不法分子利用，发布虚假信息进行欺诈。

破解一个真正的二维码需要一些技巧才能改变代码矩阵中的像素点，为此黑客们找到了一种简单的方法，比如在二维码(可由互联网上广泛使用的免费工具生成)中嵌入恶意软件。对于普通用户来说，这些代码看起来都一样，但是一个恶意的二维码可以把用户重定向到一个虚假的网站。它还可以捕获个人数据或在智能手机上安装恶意软件。

对于公司来说了可以通过考虑消除基于密码的业务和云应用程序访问来预防二维码攻击，这是当今数据泄露的主要原因之一。通过转向无密码多因素身份验证，不仅避免了密码被盗的威胁，而且还消除了维护密码的麻烦，这使每个人（除黑客之外）都更加快乐和高效。

https://mp.weixin.qq.com/s?__biz=MzI0MDY1MDU4MQ==&mid=2247509778&idx=1&sn=c7e2bcc9ef4097dd89101c3106b40771

6. 面对中间人攻击可以通过加密保护数据隐私不被泄露

中间人攻击（简称“MITM 攻击”）是一种“间接”的入侵攻击，这种攻击模式是通过各种技术手段将受入侵者控

制的一台计算机虚拟放置在网络连接中的两台通信计算机之间，这台计算机就称为“中间人”。

防止中间人攻击的最流行方法是对通信进行加密。它的工作原理如下：当服务器传输数据时，它通过提供数字证书来向客户机标识自己。然后，在客户端和服务器之间建立加密的通信通道。MITM 攻击是最广泛，最有效的黑客攻击类型之一。虽然无法完全保护您的网络不会受到此类攻击，但您可以确保您的数据保持受保护。加密通信是任何网络安全项目的重要组成部分。这是最可靠的方法，即使攻击者可以拦截，也可以确保跨网络传输的数据受到保护。

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

7. 超过三分之二的欧洲企业采用零信任架构

根据 Gigamon 研究，超过三分之二的欧洲组织已采用或计划采用零信任框架以应对不断变化的威胁形势。在对德国、法国和英国的 500 位 IT 和安全决策者进行的调查中，有 84%的受访者表示自 2020 年初以来安全威胁同比增加。最大的威胁来自远程办公的不安全设备（51%）、网络钓鱼攻击（41%）和数据泄露（33%）。受访者认为，**数字化转型（50%）、影子 IT（45%）和员工安全意识教育（37%）是未来 12 个月至三年内，企业面临的最大的内部 IT 和安全挑**

战。

这些威胁产生的结果是，人们强烈希望实现零信任架构。最主要的原因是：使网络更加安全并降低风险（54%），确保更好地保护数据并更易于管理（51%），降低员工损害系统的风险（ 49%）。

https://www.secrss.com/articles/26067

8. 数据安全视角下的数据库审计技术新思路

数据库作为数据的核心载体，其安全防护是重中之重，其中，数据库审计是数据库安全防御体系的重要组成部分。从“以数据为中心”的角度来梳理数据库审计的新技术有以下技术点：突显数据审计、全面拥抱业务审计、拥抱大数据时代。数据库审计是一个成熟化很高的产品，短期内看不到具有挑战性的发展路线图。在数据安全治理背景下，需要主动适应，做一些改变，才能更好地发挥数据库安全价值。

https://www.freebuf.com/articles/database/250910.html

9. 双因素身份认证的方式

双因素身份认证是为了加强登录安全，即能够在用户名+静态密码的基础上，额外增加一种安全有效地可以验证用户身份的方式，都可以统称为双因素认证。常见的认证方式

有：**动态密码、扫码、消息推送、邮件认证、指纹、人脸、虹膜、声音、U 盘证书**等，动态密码中又会细分**短信令牌、硬件令牌、APP 令牌、微信小程序令牌、钉钉令牌**等。不同令牌之间也有不同的认证原理和登录方式，安全级别上来讲也是各有不同，其中生物识别认证安全级别最高，短信验证码认证和邮件认证安全级别最低，企业中最常用的认证方式为：**动态密码认证（硬件令牌、APP 令牌、微信小程序令牌、钉钉令牌）、指纹认证、人脸认证、U 盘证书认证**，从成本考虑出发，软件动态密码认证最佳。

https://www.freebuf.com/articles/es/249547.html

10.健全数据分级分类规则，完善网络数据安全立法

2020 年 7 月《数据安全法》草案公开征求意见，数据安全已经成为网络安全乃至国家安全法制体系中的核心内容之一。在即将构建形成的数据安全和个人信息保护体系下，应当更加具体地回应网络数据利用和保护的正当需求，确立网络数据安全分级分类的基本思路，引导公共属性数据相互共享和对外开放，通过配套条例和规章健全数据分级分类规则，完善网络数据安全立法。

https://mp.weixin.qq.com/s/oCLM4kFhx1AJmXcYFrIcvQ