网络与信息安全情况通报

第 10 期

丽江市网络与信息安全监测预警通报中心　　2020 年 5 月 19 日

目　录

一、美国关键基础设施可被黑客入侵

据外媒报道，近日，有研究人员报告称，美国许多关键基础设施的工控系统面板未受到全面保护，这为黑客利用基础设施安全漏洞获得系统访问权限制造了机会。报告显示，在2019年，美国的商业部门增加了IoT（物联网）应用程序的使用率，目的在于增加公司收入来源和提高生产效率。但由于这些基础设施的安全性非常薄弱，从而成为了网络攻击的潜在目标。并且，这些潜在目标不止是商业部门，还包括了美国能源和水行业等，这些部门和行业的大多数系统是由工控系统运行的，这些系统在设计时就没有考虑到针对潜在网络攻击的安全性，这导致黑客可能通过工具扫描系统的开放端口，从而实现对系统的远程控制。报告还指出，美国大多数机构和公司都已经意识到了基础设施的安全性能薄弱以及不断增长的安全威胁，但是这些公司和机构仍然没有重视通过增强系统安全性来减少发生网络攻击的可能性。

二、新型恶意软件“Kaiji”浮出水面

据外媒报道，近日，国外安全研究团队发现了一种名为“Kaiji”的恶意软件，该恶意软件专门用于感染基于Linux的服务器和智能物联网设备，然后黑客会滥用这些系统发起DDoS 攻击。据悉，该恶意软件已在世界范围内开始传播，“Kaiji”对 SSH 设备暴露在互联网上的 IoT 设备和 Linux 服务器可以执行暴力攻击，一旦获得对设备根帐户的访问权限，“Kaiji”利用受感染设备发动以下三种攻击：一是使

用 DDoS 攻击，二是对其他设备进行更多的 SSH 暴力破解，三是它会窃取任何本地 SSH 密钥。该安全研究团队表示，“Kaiji”作为在 IoT 恶意软件领域的新僵尸网络与其他僵尸网络相比还不是很成熟，但这并不意味着该恶意软件所形成的僵尸网络不会成为主流威胁。

三、巴基斯坦 1.15 亿移动用户个人信息被泄漏

据外媒报道，近日，巴基斯坦 1.15 亿移动用户的详细信息被泄漏，黑客在暗网上以 210 万美元的价格出售两个包含 1.15 亿巴基斯坦移动用户记录的软件包。目前，某外媒已获得了两个数据软件包的副本，数据包的信息内容包括：用户全名、家庭住址、身份证号、手机号码、座机号码等详细信息。研究人员表示，根据数据包中的日期显示，泄露文件中最早的信息是从 2013 年末开始的，这表明早在 2013 年就已经发生了信息泄密事件，直到近日才在网上浮出水面。目前，巴基斯坦电信管理局和联邦调查局已经开始调查此事。

四、“Infinity Black”黑客组织被欧洲警方瓦解

据外媒报道，近日，欧洲刑警组织宣布逮捕了“Infinity Black”黑客组织的五名黑客，还查封了该组织的两个在线平台，这两个平台的数据库包含超过 1.7 亿个被盗的用户凭证。据悉，该组织成立于 2018 年底，主要以运营“Infinity.black”网站，并在网站上出售用户凭证为盈利方式。同时，该黑客组织还在经营多个黑客论坛。欧洲刑警

组织表示，该组织给瑞士公民造成的经济损失估计为 5 万欧元，约为 38 万元人民币。目前，该黑客组织的主要负责人也已经被捕，这表明该组织几乎已经被瓦解。

送：市直各委、办、局

市级各重要信息系统运营使用单位及行业主管部门。

承办单位：丽江市网络与信息安全监测预警通报中心　　电话：5120626

抄：市公安局警令部，科信处，县（区）网安大队。