NSFOCUS

绿盟威胁情报周报

2020年第6周（2020.02.03-2020.02.09）

绿盟威胁情报中心（NTI）

本周热点概览

暗网情报

- 9条金融行业暗网情报，覆盖银行、证券等

热点资讯

- 雄迈产品漏洞
- 思科修复CDP协议漏洞
- 安卓蓝牙组件高危漏洞
- MyCERT警告APT40开展的网络间谍活动
- Gamaredon组织加强针对乌克兰的攻击
- Charming Kitten组织针对世界各地公众人物的攻击活动
- Metamorfo新变种针对多个国家金融机构

一、 暗网情报

分类	发现时间	暗网交易标题
金融	2020-02-03 22:36	股民数据 10800 条 19 年某证券网点新开户数据
金融	2020-02-03 16:55	59w 某银行理财客户带手机号身份证地址等
金融	2020-02-03 23:26	12 万 8 某银行信用卡持卡人含申办时的所有信息
金融	2020-02-02 13:34	某银行企业通讯录
金融	2020-02-05 00:32	股民数据 98w7 某投资公司数据含姓名手机微信
金融	2020-02-05 01:19	8w8 浙江某投顾公司 19 年股民数据
金融	2020-02-05 16:40	某银行_千万富豪个人数据
金融	2020-02-06 13:26	某证券_股民数据 23 万

金融	2020-02-06 21:39	理财数据 10w 条某银行理财客户信息

*更多详细内容，可与绿盟科技商务人员联系或通过 csc@nsfocus.com 与我们联系

二、 热点资讯

1. 雄迈产品漏洞

【概述】

近日，有国外安全研究员指出海思（HiSilicon）芯片中预留后门，事后多方研究员以及海思官方都澄清并表示该后门源于雄迈软件的设备，并非海思芯片。后门主要利用端口 9530/tcp 侦听特殊命令，攻击者通过此端口开启 telnet 服务，并利用默认的口令登录，从而控制设备。

【参考链接】

https://mp.weixin.qq.com/s/yMJWxJvtgeuzSfYTN6vn7Q

2. 思科修复 CDP 协议漏洞

【概述】

北京时间 2 月 6 日，思科（Cisco）官方修复了存在于 CDP 协议中的 5 个高危漏洞，该协议可允许思科设备在内网环境通过多播消息互相分享消息，主要影响 IP 电话和摄像头设备。此次公开的 5 个漏洞均属于内存溢出漏洞，实际利用难度大，在特定条件下可造成远程代码执行。

【参考链接】

http://blog.nsfocus.net/cisco20200207/

3. 安卓蓝牙组件高危漏洞

【概述】

近日，谷歌发布 2 月安卓安全补丁，其中修复了一个高危的蓝牙组件漏洞（CVE-2020-0022）。该漏洞无需用户的交互操作，在设备打开蓝牙时即可被攻击，攻击者成功利用该漏洞即可在目标系统上执行任意代码。同时研究人员还指出该漏洞可能被攻击者用来制作可以自主传播的蠕虫型漏洞。

【参考链接】

http://blog.nsfocus.net/cve-2020-0022/

4. MyCERT 警告 APT40 开展的网络间谍活动

【概述】

MyCERT(马来西亚计算机紧急响应小组)最近观察到针对马来西亚政府官员的攻击活动，攻击者通过发给政府官员的鱼叉式网络钓鱼消息，冒充新闻记者、贸易出版物的个人或相关军事组织，诱导受害者感染恶意软件后，从政府系统中窃取机密文件。此次攻击活动疑似由攻击组织 APT40 发起。

【参考链接】

https://www.mycert.org.my/portal/advisory?id=MA-770.022020

5. Gamaredon 组织加强针对乌克兰的攻击

【概述】

在过去的几月中，威胁组织 Gamaredon 不断更新其工具集并加强对乌克兰政府和执法部门的攻击活动。Gamaredon 是一个自 2013 年以来一直活跃网络威胁组织，主要针对乌克兰政府进行恶意活动，其主要目的是窃取政府，军事人员资料信息。

【参考链接】

https://labs.sentinelone.com/pro-russian-cyberspy-gamaredon-intensifies-ukrainian-security-targeting/

6. Charming Kitten 组织针对世界各地公众人物的攻击活动

【概述】

近期发现 Charming Kitten 组织的一系列网络钓鱼活动，新攻击活动的重点是窃取受害者的电子邮件帐户信息并查找有关他们的联系人/网络的信息，受害者包括记者、政治和人权活动家。Charming Kitten（又名 Group 83、Newsbeef、iKittens、Parastoo、Newscaster）是伊朗网络间谍组织，自 2014 年左右开始活跃。

【参考链接】

https://blog.certfa.com/posts/fake-interview-the-new-activity-of-charming-kitten/

7. Metamorfo 新变种针对多个国家金融机构

【概述】

Metamorfo 是一个恶意软件家族，针对在线金融机构的客户。2020 年 1 月发现 Metamorfo 变种仅针对巴西金融机构的客户，近日发现 Metamorfo 第二个变种，针对多个国家/地区更多金融机构的客户，收集受害者计算机数据并与其命令和控制服务器进行通信。

【参考链接】

https://www.fortinet.com/blog/threat-research/another-metamorfo-variant-targeting-customers-of-financial-institutions.html

绿盟威胁情报中心（NTI）

绿盟威胁情报中心（NTI）依托公司专业的安全团队和强大的安全研究能力，对全球网络安全威胁和态势进行持续观察和分析，以威胁情报的生产、运营、应用等能力及关键技术作为核心研究内容，针对客户不同的需求场景，已经推出了云端情报查询服务（https://nti.nsfocus.com/）、互联网资产核查服务、安全设备/安全平台的威胁情报组件、客户本地威胁情报平台（NTIP）等产品及服务；为用户提供可操作的情报数据、专业的情报服务和高效的威胁防护能力，帮助用户更好地了解和应对各类网络威胁。

NSFOCUS
总部：北京市海淀区北洼路4号益泰大厦
绿盟科技（股票代码300369）

邮编：100089
电话：010-68438880
传真：010-68437328
邮箱：webadmin@nsfocus.com