安恒威胁情报中心

安全威胁情报周报

Threat Intelligence 2021

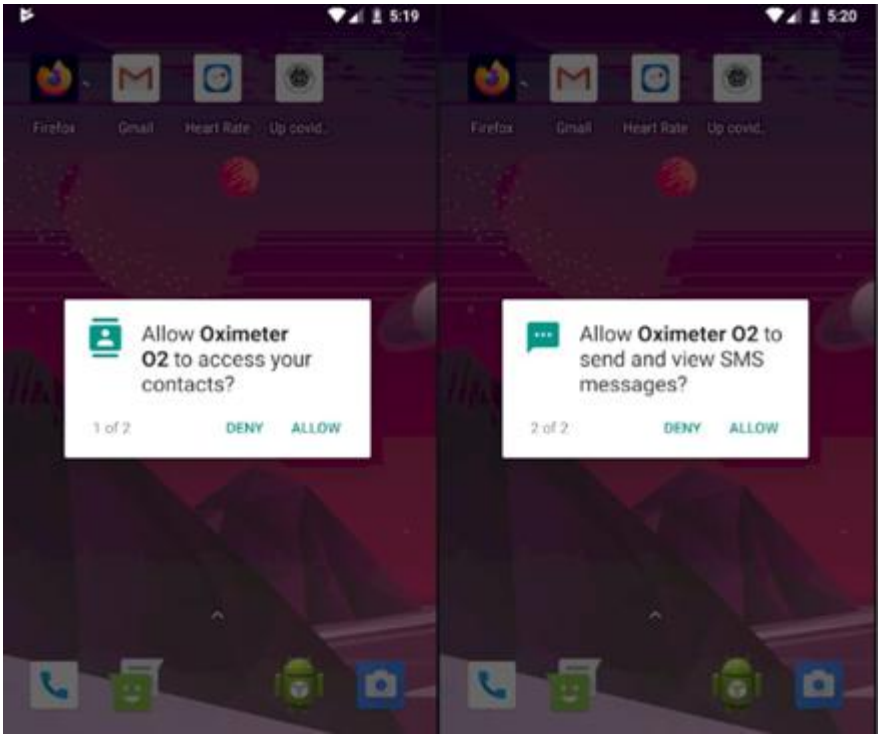
（2021.5.15~5.21）

目录

【恶意软件威胁情报】

恶意软件伪装成血氧仪应用程序进行传播

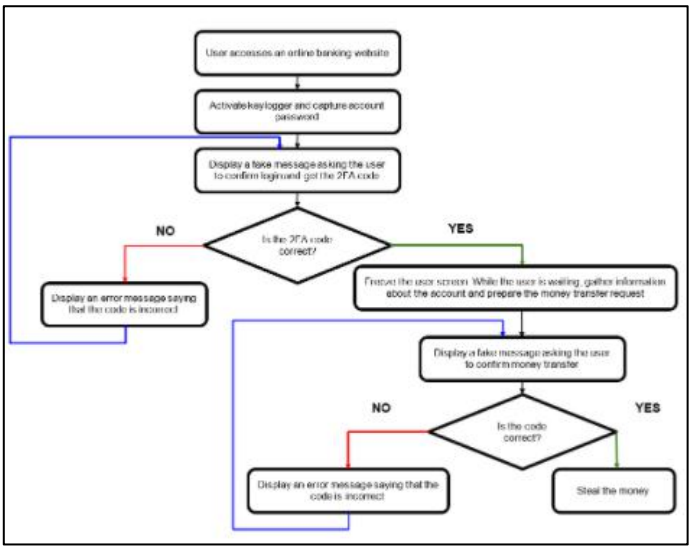
近日，研究人员曝光了一个伪装成血氧仪应用程序的恶意软件，该应用程序使用了用户的 Google Pay，PhonePe，Paytm 等指纹数据，要求访问用户的联系人和 SMS 许可，这对于检查氧饱和度水平的应用来说似乎是不必要的。该程序访问联系人并通过 SMS 和 WhatsApp 消息将链接发送到系统中的每个联系人，下载恶意 APK 文件，从而窃取用户的银行凭证。



参考链接：https://ti.dbappsecurity.com.cn/informationDetail/1980

Bizarro 银行木马将攻击范围扩大到欧洲

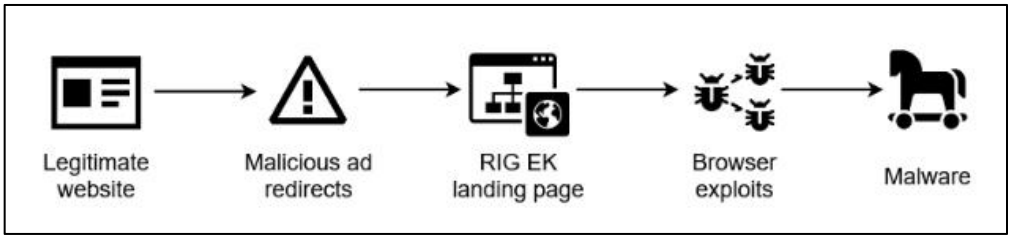
近日，研究人员发现 Bizarro 银行木马已经将攻击范围扩大到欧洲，窃取了欧洲和南美不同国家 70 家银行的登录信息。Bizarro 是一个来自巴西的银行木马家族，通过 Microsoft Installer 软件包传播，旨在捕获在线银行凭证。Bizarro 目前活跃于阿根廷，智利，法国，德国，意大利，葡萄牙和西班牙，攻击范围已经从巴西扩大到南美和欧洲其他国家。



参考链接：https://ti.dbappsecurity.com.cn/informationDetail/1972

使用新的 RIG Exploit Kit 分发 WastedLoader 的恶意活动

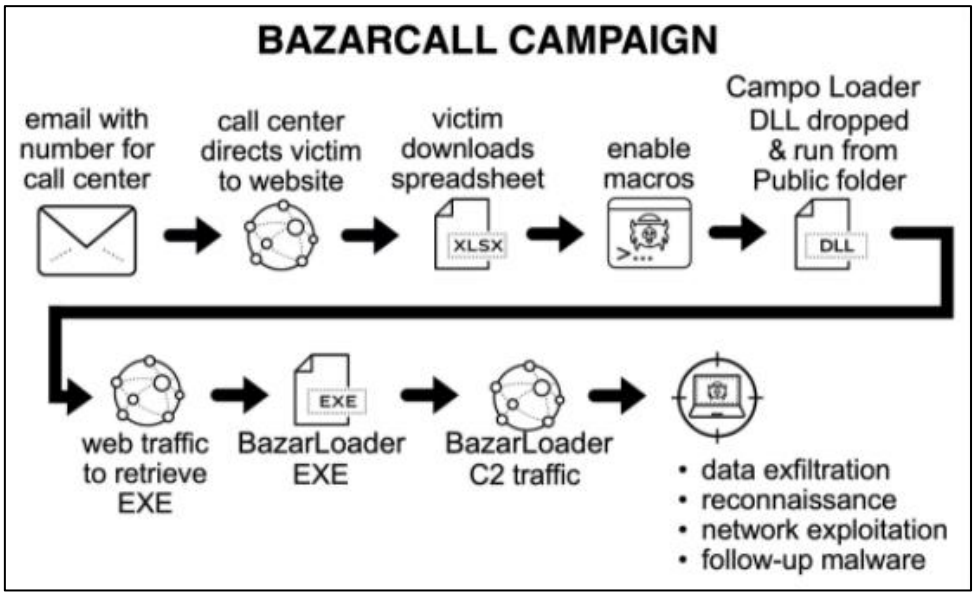
研究人员于 2 月发现了一个使用新的 RIG Exploit Kit 的恶意活动，该活动利用了未打补丁的 IE 浏览器中的两个脚本引擎漏洞(CVE-2019-0752 和 CVE-2018-8174)。发送的恶意软件看起来像 WastedLocker 的新变种，但这个新样本缺少勒索软件的部分，可能是从 C&C 服务器下载的。因为它的工作方式类似于下载有效载荷的加载器，所以研究人员将其命名为 WastedLoader。



参考链接：https://ti.dbappsecurity.com.cn/informationDetail/1982

BazarCall：利用呼叫中心传播 BazarLoader 的恶意活动

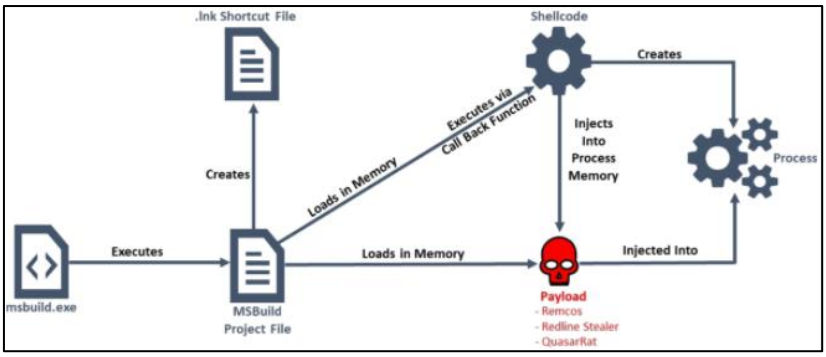
研究人员发现一种利用呼叫中心传播 BazarLoader 的恶意活动。攻击者通过发送带有电话号码的试用订阅到期电子邮件，引导受害者拨打电子邮件中的电话号码，然后由呼叫中心接线员接听电话并引导受害者到伪造的网站以取消订阅服务。呼叫中心的操作员引导受害者下载恶意 Microsoft Excel 文件，启用宏后受害者的计算机将感染 BazarLoader 恶意软件。这种基于呼叫中心，使用 BazarLoader 感染计算机的过程称为“ BazarCall”方法。



参考链接：https://ti.dbappsecurity.com.cn/informationDetail/1988

攻击者使用 MSBuild 以无文件方式传递 RAT

研究人员发现了一个活动，攻击者使用 Microsoft Build Engine（MSBuild）以无文件方式分发 Remcos 远程访问工具（RAT）和 RedLine Stealer 窃密恶意软件。该活动似乎于 2021 年 4 月开始，至 2021 年 5 月 11 日仍在进行。恶意 MSBuild 文件包含编码的可执行文件和 shellcode，其中一些文件托管在俄罗斯图像托管网站“joxi[.]net”上。

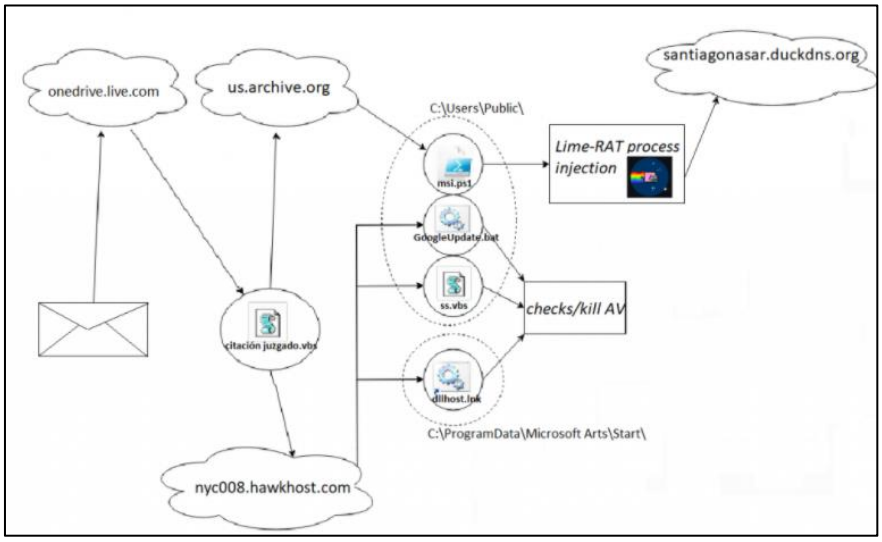


参考链接：https://ti.dbappsecurity.com.cn/informationDetail/1990

【热点事件威胁情报】

黑客组织使用 LimeRAT 针对哥伦比亚

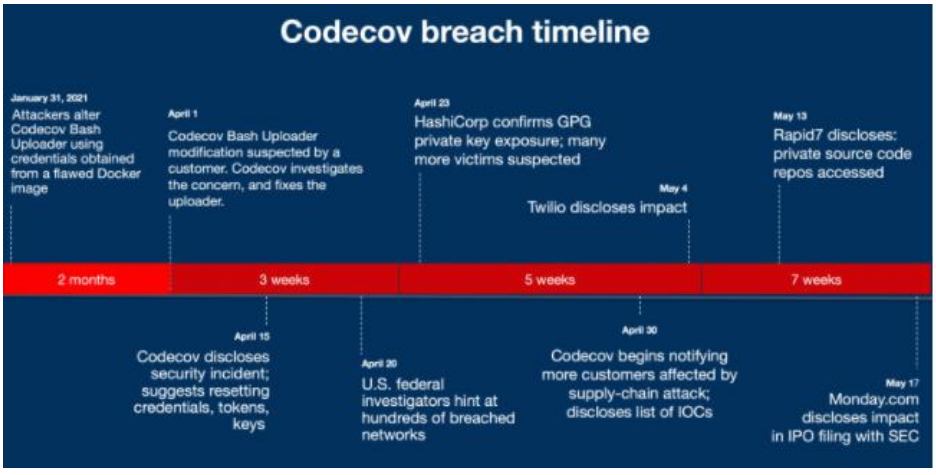
研究人员发现了一个黑客组织使用 LimeRAT 针对哥伦比亚的恶意活动。该组织通过电子邮件传播恶意软件，邮件具有通用的主题，例如传票、银行付款，并且具有精心制作的 html 视图，其中伪造的附件图标带有从 One Drive 下载压缩文件的链接，并通过多阶段调用下载恶意载荷，并在受害机器上运行。



参考链接：https://ti.dbappsecurity.com.cn/informationDetail/1975

入侵 Codecov 的黑客获得了 Monday.com 源代码的访问权限

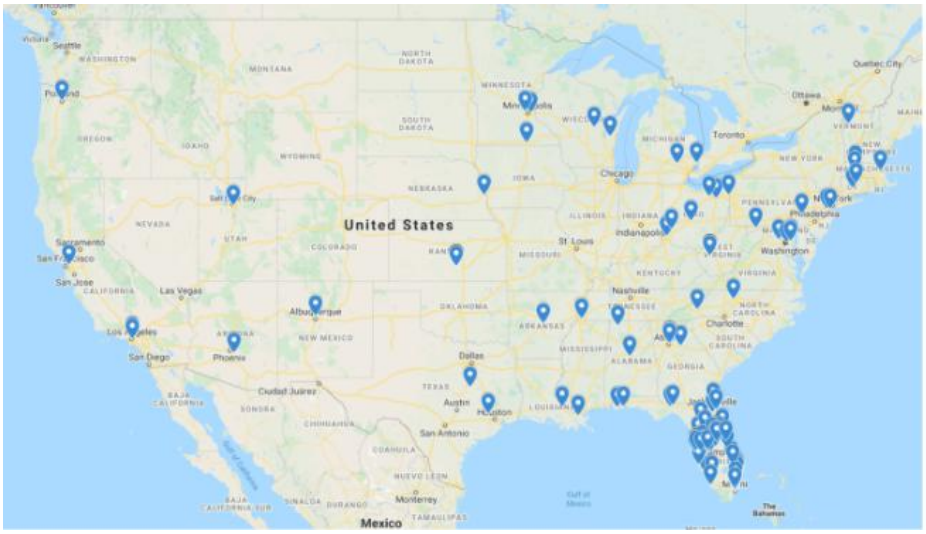
Monday.com 最近披露其遭到 Codecov 供应链攻击，并影响了多家公司。在此次攻击中，黑客窃取了其源代码的只读副本，但并未对其进行篡改。此外，黑客还访问了托管在该平台上的客户表单和视图。作为缓解措施，该平台已停止使用 Codecov 的服务并更换了所有生产和开发环境的密钥，并已与被泄露信息的相关客户联系。目前，该平台已聘请领先的网络安全专家协助调查。



参考链接：https://ti.dbappsecurity.com.cn/informationDetail/1987

研究人员曝光佛罗里达水厂网络攻击事件背后的水坑攻击

研究人员近日对早先发生的佛罗里达州奥兹马尔(Oldsmar)水处理厂遭受的网络攻击进行了调查，结果发现了一个似乎是针对水务公司的水坑攻击。2021 年 2 月 5 日，该市的水处理厂发生了一次针对水务承包商的投毒事件，一名黑客远程访问了奥兹玛(Oldsmar)水厂的系统，试图将某一化学物质的含量提高到可能使公众面临中毒风险的程度。这一前所未有的事件在媒体和网络安全行业引起了巨大轰动。



参考链接：https://ti.dbappsecurity.com.cn/informationDetail/1981

【科技行业威胁情报】

日本科技巨头东芝公司遭 DarkSide 勒索软件攻击

近日，日本科技巨头东芝技术公司（Toshiba Tec Corp）遭到 Darkside 勒索软件攻击，并窃取了超过 740GB 的数据。东芝技术集团的欧洲子公司当地时间 5 月 14 日表示，来自一个犯罪团伙的网络攻击促使该公司断开了日本和欧洲之间的网络连接，以阻止恶意软件的传播。同时实施恢复和数据备份，并且请来第三方网络取证专家协助，就损害程度展开调查。

东芝科技集团是一家跨国企业集团，生产条形码扫描仪，销售点（PoS）系统，打印机和其他电气设备。该部门的法国子公司似乎已成为勒索软件攻击的目标。

参考链接：https://ti.dbappsecurity.com.cn/informationDetail/1971

【金融行业威胁情报】

法国金融咨询公司遭 Avaddon 勒索软件攻击

近日，Avaddon 勒索软件团伙入侵了总部位于法国的金融咨询公司 Acer Finance，该勒索团伙声称窃取了公司的机密信息，包括许多客户、员工的机密信息，银行业务，个人信件，合同，协议，付款方式，来自秘书处的数据，许可证等等。该组织还宣称入侵了 AXA 亚洲分支并窃取了 3TB 的数据。

Acer 金融是一家投资管理公司。该公司提供风险管理，共同基金，分析，财务规划和咨询服务，服务于法国的个人、企业家和机构投资者

参考链接：https://ti.dbappsecurity.com.cn/informationDetail/1973

【医疗保健行业威胁情报】

爱尔兰卫生部门因遭到黑客攻击被迫关闭系统

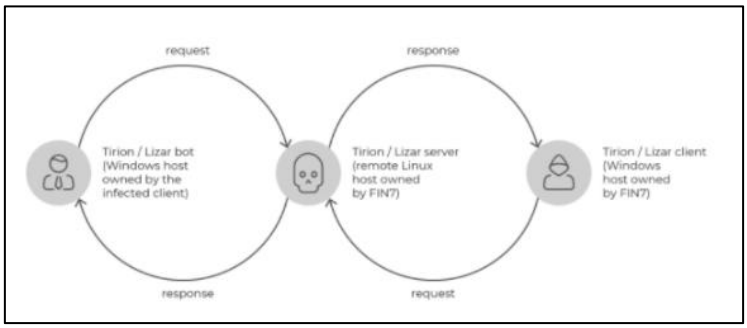
近日，负责爱尔兰公共卫生事务的卫生服务执行局网络系统遭到黑客攻击，造成全国多家医院的电子系统和存储信息无法正常使用。该执行局官员表示已收到 Conti 勒索团伙索要赎金的勒索信息，但未透露具体金额。负责爱尔兰全国医疗保健和社会服务的健康服务执行局（HSE）表示，已关闭所有 it 系统以保护网络免受勒索软件攻击，并和安全合作伙伴全面评估情况。

参考链接：https://ti.dbappsecurity.com.cn/informationDetail/1969

【高级威胁情报】

FIN7 黑客组织伪装成网络安全公司传播 Lizar 后门

FIN7 是一个以金钱为动机而行动的网络犯罪组织，其正在冒充网络安全公司分发带有 Lizar 后门的 Windows 渗透测试工具。FIN7 伪装成一个合法的网络安全公司兜售安全分析工具，因此受害组织的员工甚至没有意识到他们正在使用的是恶意软件，或者他们的卖家是一个网络犯罪组织。



FIN7 组织使用的恶意软件一直在变化，之前它的首选工具包一直是 Carbanak 远程访问木马，这个木马非常复杂。但是最近，研究人员注意到该小组自 2 月份以来使用了一种称为 Lizar 的新型后门，该后门提供了一套强大的数据检索和横向移动的功能。

参考链接：https://ti.dbappsecurity.com.cn/informationDetail/1970

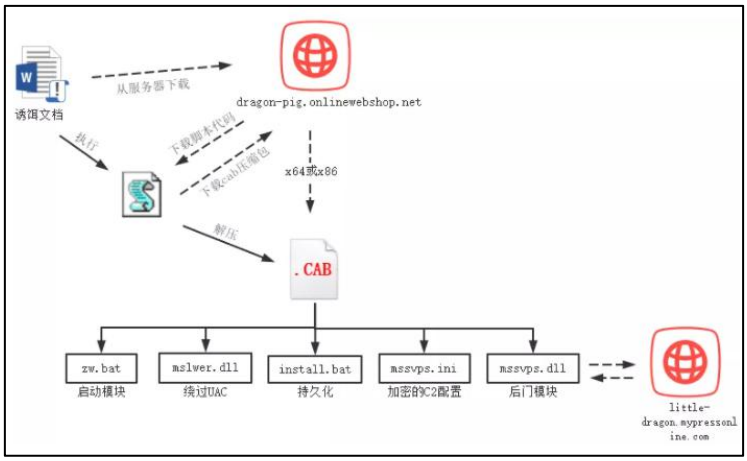
研究人员将 Simps 僵尸网络归因到 Keksec 黑客组织

研究人员发现了一个名为“ Simps”的新僵尸网络，该僵尸网络属于 Keksec 组织，主要专注于 DDOS 活动。黑客通过一个 Shell 脚本和一个 Gafgyt 恶意软件下载 Simfs 僵尸网络二进制文件，拥有一个 YouTube 频道和 Discord 服务器来延时僵尸网络。该下载程序的 web shell 脚本活动可以通过 Uptycs 的 EDR 功能检测到。

参考链接：https://ti.dbappsecurity.com.cn/informationDetail/1979

Konni APT 组织以“朝鲜局势”相关主题为诱饵对俄进行持续定向攻击活动

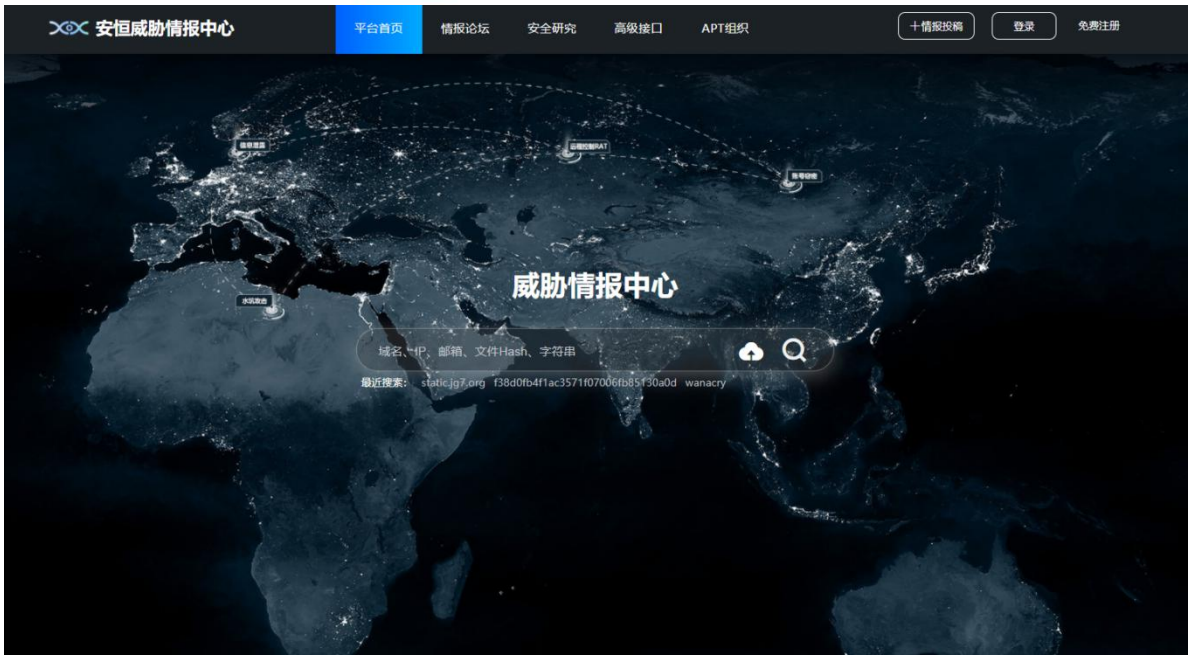
研究人员近期捕获到 Konni APT 组织利用朝鲜局势相关话题针对俄罗斯方向的攻击活动。Konni APT 组织由特定政府提供支持，自 2014 年以来一直持续活动。该组织经常使用鱼叉式网络钓鱼攻击手法，且经常使用与朝鲜相关的主题或社会热点作为诱饵，吸引用户查看并执行附件。



参考链接：https://ti.dbappsecurity.com.cn/informationDetail/1986

威胁情报中心介绍

安恒威胁情报中心汇聚了海量威胁情报，支持多点渠道数据输入，支持自动情报数据产出，能实现网络安全的高效赋能。平台使用者可通过自定义策略进行威胁监控、威胁狩猎，并对输入数据进行自动化的生产加工，同时支持人工分析团队对情报进行复核整理。



敬请关注安恒威胁情报中心

平台地址：https://ti.dbappsecurity.com.cn/