北京安域领创科技有限公司

安全通告

报告周期：2022 年 5 月第二周

(2022 年 5 月 9 日-2022 年 5 月 13 日)

目　录

1 本周漏洞通告

1.1 漏洞一：Seacms 注入漏洞

发布时间	2022-05-13
更新时间	2022-05-13
CNVD-ID	CNVD-2022-36987
漏洞危害级别	高
影响产品	SEACMS SEACMS 11.6
漏洞类型	通用型漏洞
漏洞描述	SeaCMS 是一套使用 PHP 编写的免费、开源的网站内容管理系统。该系统主要被设计用来管理视频点播资源。 Seacms v11.6 版本存在安全漏洞，该漏洞源于 /admin/weixin.php 组件中存在远程代码执行（RCE）漏洞。目前没有详细的漏洞细节提供。
漏洞解决方案	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法： https://www.seacms.net/

1.2漏洞二：EmpireCMS SQL 注入漏洞

发布时间	2022-05-13
更新时间	2022-05-13
CNVD-ID	CNVD-2022-36984
漏洞危害级别	高
影响产品	EmpireCMS EmpireCMS 7.5
漏洞类型	通用型漏洞
漏洞描述	EmpireCMS（帝国内容管理系统）是一套开源内容管理系统（CMS）。 EmpireCMS 7.5 版本存在 SQL 注入漏洞，该漏洞源于在 AdClass.php 中缺少对外部输入 SQL 语句的验证，攻击者可利用该漏洞执行非法 SQL 命令窃取数据库敏感数据。
漏洞解决方案	厂商尚未提供漏洞修复方案，请关注厂商主页更新：http://ecms.phome.net/

1.3漏洞三：WUZHI CMS SQL 注入漏洞

发布时间	2022-05-13
更新时间	2022-05-13
CNVD-ID	CNVD-2022-36985
漏洞危害级别	高

漏洞类型	通用型漏洞
影响产品	北京五指互联科技有限公司 WUZHI CMS 4.1.0
漏洞描述	Wuzhi WUZHI CMS 是五指（Wuzhi）公司的一套基于 PHP 和 MySQL 的开源内容管理系统（CMS）。 WUZHI CMS 4.1.0 版本存在 SQL 注入漏洞，该漏洞源于 /coreframe/app/member/admin/group.php 的 groupid 参数缺少对外部输入 SQL 语句的验证，攻击者可利用该漏洞执行非法 SQL 命令窃取数据库敏感数据。
漏洞解决方案	厂商尚未提供漏洞修复方案，请关注厂商主页更新：https://www.wuzhicms.com/

1.4漏洞四：WordPress plugin RRatingg SQL 注入漏洞

发布时间	2022-05-13
更新时间	2022-05-13
CNVD-ID	CNVD-2022-36989
漏洞危害级别	高
漏洞类型	通用型漏洞
影响产品	WordPress RRatingg plugin <1.2.54
漏洞描述	WordPress 和 WordPress plugin 都是 WordPress 基金会的产品。WordPress 是一套使用 PHP 语言开发的博客平台。该平台支持在 PHP 和 MySQL 的服务器上架设个人

	博客网站。WordPress plugin 是一个应用插件。 WordPress plugin RRatingg 1.2.54 之前存在 SQL 注入漏洞，该漏洞源于插件在通过 rrtngg_delete_leads AJAX 操作在 SQL 语句中使用它们之前无法正确清理、验证和转义潜在客户 ID，该操作可供未经身份验证的用户使用，从而导致未经身份验证的 SQL 注入问题。 目前没有详细的漏洞细节提供。
漏洞解决方案	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://wpscan.com/vulnerability/e7fe8218-4ef5-4ef9-9850-8567c207e8e6

1.5 漏洞五：Laravel 远程代码执行漏洞

发布时间	2022-05-10
更新时间	2022-05-10
CNVD-ID	CNVD-2022-36040
漏洞类型	通用型漏洞
漏洞危害级别	高
影响产品	Laravel Laravel 5.8.38
漏洞描述	Laravel 是 Laravel 团队（Laravel）的一个 Web 应用程序框架。

	Laravel 存在安全漏洞，该漏洞源于通过(1) RoutingPendingResourceRegistration.php 中的 __destruct、(2)QueueCapsuleManager.php 中的 __cal 和(3)中的反序列化弹出链__invoke 在 mockerylibraryMockeryClosureWrapper.php 中， 目前没有详细的漏洞细节提供。
漏洞解决方案	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://github.com/guoyanan1g/Laravel-vul/issues/2#issue-1045655892

2 本周病毒木马通告

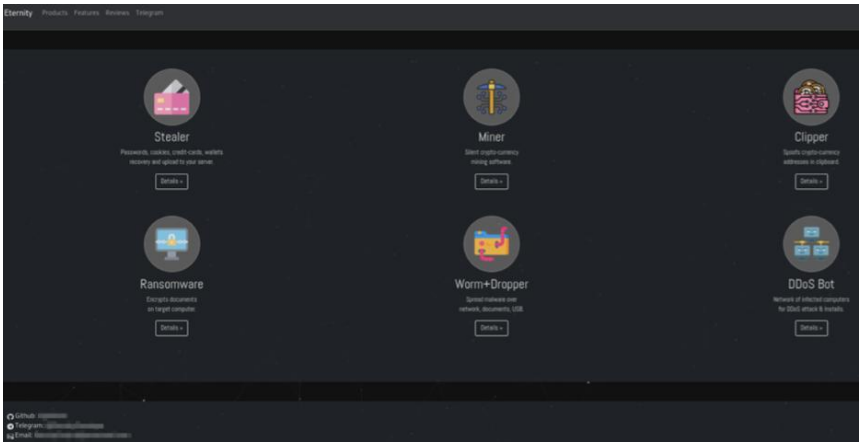
2.1 本周流行病毒木马统计

2.1.1 既能挖矿还能勒索，Eternity 恶意软件工具包正通过 Telegram 传播

病毒危险级别：★★★

据 Bleeping Computer 网站 5 月 12 日消息，目前，在网络上出现了一个名为“Eternity "（永恒不朽）的恶意软件即服务项目，威胁参与者可以购买恶意软件工具包，并根据所进行的攻击使用不同的模块进行定制。

这个模块化的工具包包括了信息窃取器、挖矿器、剪切板、勒索软件程序、蠕虫传播器以及即将上线的 DDoS 攻击机器人，其中的每一个模块都单独购买。目前，该工具包正在一个 拥有 500 多名成员的专用 Telegram 频道上进行推广，发布者在该频道上会发布更新说明、使用说明并讨论相关的使用建议。对于那些购买了恶意软件工具包的人，可以在选择他们想要激活的功能并使用加密支付后，利用 Telegram Bot 自动构建二进制文件。



Eternity 提供的主要模块

工具概览

以包年为时间单位，这些不同模块价格差异也往往较大：

挖矿器：90 美元/年，具有隐藏任务管理器、进程被杀死时自动重启和启动持久性的功能；

剪切板：110 美元/年，是一种实用程序，可监视剪贴板中的加密货币钱包地址，以将其替换为攻击者自身的钱包；

信息窃取器：260 美元/年，能窃取存储在 20 多个网络浏览器中的密码、信用卡、书签、令牌和 cookie 等数据；

蠕虫传播器：390 美元/年，使恶意软件能够通过 USB 驱动程序、本地网络共享、本地文件、云驱动器、Python 项目（通过解释器）、Discord 帐户和 Telegram 帐户自行传播；

勒索软件程序：490 美元/年，能够针对文档、照片和数据库使用 AES 和 RSA 组合的离线加密。开发者声称它是 FUD（完全无法检测到），并且能够设置一个倒计时器，使文件在到期时完全无法恢复，以给受害者带来额外的压力，迫使他们迅速支付赎金。

勒索软件倒计时器

发现 Eternity 项目的 Cyble 分析师认为，虽然他们还没有机会检查所有模块，但他们已经看到恶意软件的样本在野外传播和使用，并且在 Telegram 上已经搜集到了一些真实的威胁反馈。

通过查看窃取器模块，Cyble 分析师发现与 Jester Stealer 有几个相似之处，两者都可能源自一个名为 DynamicStealer 的 GitHub 项目。因此，Eternity 很可能是该代码的副本，通过进行修改和更名后在 Telegram 上出售。

由于这些模块支持自动化构建，并对如何使用进行了详细说明，使其能够成为“新手”黑客手中的有力武器，并对互联网用户构成严重威胁。

3 安全事件通告

3.1 本周国内外安全事件通告

3.1.1 加拿大空军关键供应商遭勒索攻击，疑泄露 44GB 内部数据

加拿大、德国军方的独家战机培训供应商 Top Aces 透露，已遭到 LockBit 勒索软件攻击；

LockBit 团伙的官方网站已经放出要求，如不支付赎金将公布窃取的 44GB 内部数据；

安全专家称，针对国防相关企业的攻击令人担忧，因为“无从得知被盗数据最终会落入哪里”，很可能流入对手国家；

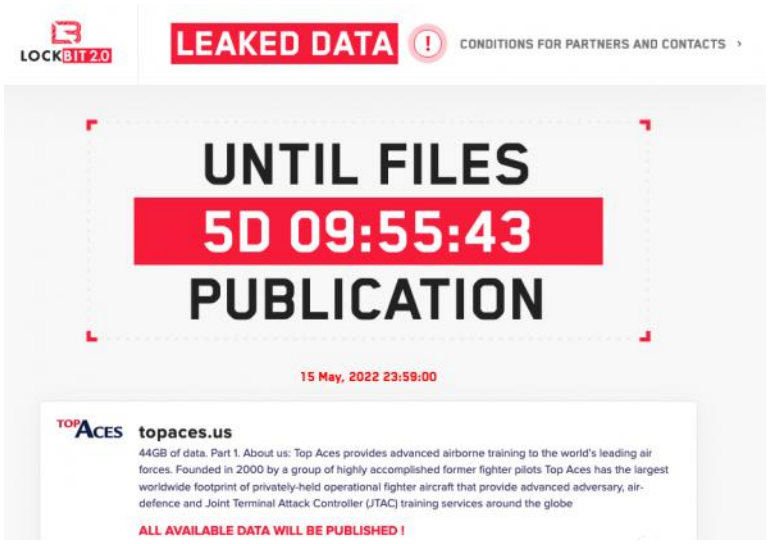
LockBit 是目前最流行的勒索软件即服务平台之一，据统计今年已攻击了至少 650 个目标组织。

专门为空军提供战斗机培训服务的的加拿大公司 Top Aces（顶级王牌）表示，已经

遭到勒索软件攻击。

该公司在周三（5 月 11 日）的一份声明中证实，正在对攻击事件开展调查。

Top Aces 公司总部位于蒙特利尔，是“加拿大与德国武装部队的独家空中对抗演习供应商”，而它的名字已经出现在 LockBit 勒索软件团伙的泄密网站上。



图：LockBit 受害者页面截屏。

Top Aces 由一群前战斗机飞行员于 2000 年创立，号称拥有“全球规模最大的私营作战战斗机群”。

除了与加拿大、德国、以色列等国合作之外，该公司还在 2019 年同美国空军签署了一份利润丰厚的合同。合同中明确提到，Top Aces 负责提供用于防御俄罗斯武器的训练工具。

安全厂商 Emsisoft 的威胁分析师 Brett Callow 指出，针对国防相关企业的攻击令人担忧，因为“无从得知被盗数据最终会落入哪里”。

Callow 表示，“即使当前攻击背后只是一群以营利为目的的恶意黑客，他们仍有可能将数据以出售或其他形式提供给第三方，包括对手国家政府。”

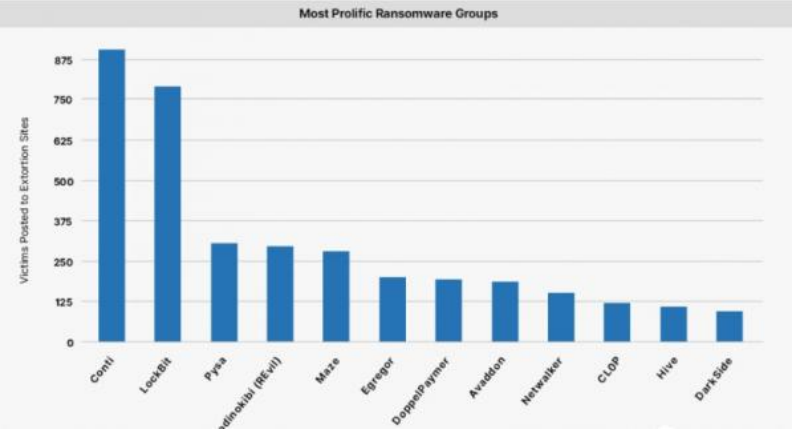
“近年来，国防工业基础领域的企业已先后遭遇多次攻击，政府必须找出一种可行的供应链安全增强方法。”

Callow 还提到，此前洛克希德马丁公司的零部件供应商 Visser Precision，为美国民兵 III 洲际导弹等核威慑武器提供支持的军事承包商 Westtech International，都遭遇过网络攻击。

LockBit 勒索软件团伙给出的最后期限为 5 月 15 日，如果届时 Top Aces 仍未支付赎金，则泄露据称总计 44 GB 的失窃数据。

LockBit 已成为最活跃勒索软件之一

LockBit 是目前最为活跃的勒索软件团伙之一，仅在过去一年就发动了数百次攻击，并且愈发猖獗。据 Recorded Future 统计数据，2022 年他们已经攻击了至少 650 个组织。



该团伙最近又犯下了两起轰动一时的大案，分别是一家流行的德国图书馆服务、巴西里约热内卢财政系统。

2021 年 8 月，澳大利亚网络安全中心（ACSC）曾发布公告，警告称 LockBit 勒索软件攻击数量正在激增。

该团伙自 2019 年 9 月起一直保持运营，但一直处于边缘位置，直到后来开发出 LockBit 2.0 勒索软件即服务的全新平台版本。

随着 Darkside、Avanddon、REvil 等黑客团伙的消亡或退出，LockBit 已经成为当下最为常见的勒索软件即服务平台之一。

3.1.2 游戏巨头暴雪再遭 DDoS 攻击，多款热门游戏掉线

美国东部时间 5 月 11 日晚上 7 点 11 分，全球最大的游戏开发商和发行商动视暴雪在推特上表示，其战网服务正遭受 DDoS 攻击，“可能会导致某些玩家出现高延迟和连接中断的情况”。8:29 分，在推文发出一个多小时后，该公司宣布恶意攻击已经结束。

根据 Downdetector 的用户报告，玩家在《守望先锋》《魔兽世界》《使命召唤》和《暗黑破坏神 III》等游戏中都遇到了问题。目前已有 24,971 份报告，其中报告最多的问题是服务器连接（63%），其次是登录（34%）和更新（3%）问题。

此类事件时常发生，开发商很难为任何潜在的攻击做好充分的准备。动视暴雪所能做的就是尽快控制局势。

2021 年 11 月，动视暴雪也遭到了来自外部的 DDoS 攻击，导致其服务器运行缓慢，玩家难以进入到游戏之中。期间尝试登录的玩家，也能够 PC 战网客户端上看到“突发新闻”相关条目。

攻击发生后，在服务器检测网站 DownDetector 上，动视暴雪的许多服务和产品都发布了服务中断公告。有数千位玩家报告称排不上队，也有数百位玩家报告部分暴雪游戏掉线。

经过调查发现，黑客选择了该公司旗下经过验证的客服推特账号作为突破口，发起持续大约一个小时的 DDoS 攻击。

据悉，2021 年 11 月的攻击事件是一个名为 Poodle Corp 的黑客组织所为，该组织在 2021 年 8 月也曾对战网发起过 DDoS 攻击。Poodle Corp 通过 Twitter 表示，在暴雪刚发布《魔兽世界》的最新资料片时，就盯上了暴雪的服务器，将在转推数量超过 2000 之后停止对战网的攻击。

Poodle Corp 是 LizardSquad 黑客组织的分支，后者曾多次攻击过微软的 Xbox 平台、索尼的 PS 平台以及暴雪的战网（Battle.net）平台。Poodle Corp 主要针对游戏服务器发起攻击，因为游戏是受到 DDoS 攻击影响最大的行业。相关数据显示，在 2021 年，有近一半的 DDoS 攻击是针对游戏行业发起的，即使是微软、索尼、暴雪等巨头公司，也无法避免遭到此类攻击。

3.1.3 APT 网络间谍组织确认由三个独立的团队组成

研究人员发现，这个对美国公用事业进行网络间谍攻击的威胁集团实际上是由三个子集团组成的，他们都有自己的工具集和攻击目标，自 2018 年以来就一直在全球运作。

TA410 是一个伞式网络间谍组织，根据安全公司 ESET 的研究人员本周发表的一份报告，该组织不仅针对美国的公共事业部门进行攻击，而且还会针对中东和非洲的外交组织进行攻击。

虽然它从 2018 年以来就一直很活跃，但 TA410 直到 2019 年才首次被研究人员发现。

当时研究员发现了一个针对公用事业部门进行攻击的网络钓鱼活动，该活动使用了一种当时被称为 LookBack 的新型恶意软件。

大约一年后，该威胁组织再次出现，对美国公共事业部门的 Windows 目标部署了一个被称为 FlowCloud 的 RAT，其被认为是 Lookback 的进化版，它可以访问已安装的应用程序并控制受感染计算机的键盘、鼠标、屏幕、文件、服务和进程等。该工具还可以将敏感信息渗透到命令和控制（C2）服务器内。

现在，ESET 的研究人员发现，TA410 并不是只有一个人，实际上是由三个威胁行为者组成的。他们是 FlowingFrog、LookingFrog 和 JollyFrog。每个小组都使用了非常相似的战术、技术和程序（TTPs），但工具集不同，攻击源来自三个不同地区的 IP。

研究人员说：”他们都针对 TTPs 和网络基础设施进行攻击，他们还会用各种方式破坏全球的目标，主要包括政府或教育组织等，这表明攻击者是有针对性的，并且攻击者会选择使用最好的方式进入到系统内部进行渗透。”

研究人员发现，这些攻击方式包括利用新版本的 FlowCloud 以及使用最近已知的微软 Exchange 远程代码执行漏洞、ProxyLogon 和 ProxyShell，包括其他定制的和通用的网络武器。

FlowingFrog

研究人员分析了每个子集团的活动，包括他们使用的工具和他们所针对的受害者的类型。他们还发现了这些攻击者在工作中的重叠部分。

Flowing Frog 与 JollyFrog 共享网络基础设施，特别是 ffca.caibi379[.com]域名。研究人员说，它还与 LookingFrog 一起开展了研究员在 2019 年发现的网络钓鱼活动。

研究人员发现，该子集团有自己特定的攻击模式，并专门针对特定的目标群体–即大学、南亚国家驻中国的外交使团和印度的一家矿业公司，进行攻击活动。

FlowingFrog 会使用第一阶段的攻击武器，ESET 研究人员将其命名为 Tendyron 下载

器，然后 FlowCloud 进行第二阶段的攻击。

研究人员解释说，Tendyron.exe 是一个合法的可执行文件，由在线银行安全厂商 Tendyron 公司签署，但是该文件容易受到 DLL 劫持。

研究人员说，FlowingFrog 还使用了 Royal Road，这是一个由几个网络间谍组织使用的恶意文件攻击器，它构建的 RTF 文件利用了 Equation Editor 的 N-day 漏洞，如 CVE-2017-11882。

LookingFrog

LookingFrog 通常会使用 X4 和 LookBack 这两个主要恶意软件系列来针对外交使团、慈善组织以及政府和工业制造领域的实体进行攻击。

研究人员解释说，X4 是一个定制的后门，在 LookBack 部署之前作为第一阶段的武器进行使用。该后门需要由一个 VMProtect 加载器进行加载，其通常被命名为 PortableDeviceApi.dll 或 WptsExtensions.dll。

LookBack 是一个用 C++编写的 RAT，其依靠代理通信工具将数据从受感染的主机中转到命令和控制服务器（C2）内。该恶意软件可以查看进程、系统和文件数据；删除文件；截图；移动和点击受感染系统的鼠标；重启机器；以及从受感染主机上删除自己。

LookBack 由众多模块组成。其中包括一个 C2 代理工具、一个恶意软件加载器、一个与 GUP 代理工具建立 C2 通道的通信模块，以及一个从 GUP 代理工具接收初始信标响应的 RAT 组件。

JollyFrog

研究人员发现，TA410 的第三个也是最后一个团队 JollyFrog 的攻击目标是教育、宗教和军队以及那些有外交任务的组织。该小组并没有使用定制的工具，而是专门使用已知的 QuasarRAT 和 Korplug（又称 PlugX）家族的通用现成的恶意软件。

研究人员说，Quasar RAT 是一个在 GitHub 上免费提供的全部功能的后门软件，是

网络间谍和网络犯罪威胁者经常使用的一个工具。它以前曾通过伪造求职者的 Word 简历来针对公司进行网络钓鱼攻击活动，并且 2019 年 APT10 曾经针对东南亚政府和私人组织进行恶意的网络活动。

Korplug 也是一个后门，多年来也被各种网络间谍组织所使用，并且仍然是一个很受欢迎的工具。上个月，Mustang Panda/TA416/RedDelta 在针对东南亚及其周边地区的外交使团、研究实体和互联网服务提供商（ISP）的间谍活动中使用了 Korplug。

TA410 通常会以 RARSFX 档案的形式来部署 Korplug，一般命名为 m.exe，其包含三个文件：自定义的加载器；F-Secure 的合法签名应用程序；以及 qrt.dll.usb—Korplug 的 shell 攻击代码。

研究人员解释说：”加载器使用了 VirtualAlloc 来分配内存并将 qrt.dll.usb 的内容复制进去。然后它会直接进行解压和加载 Korplug 有效载荷。”

FlowCloud 的最新版

ESET 研究人员还查看了 TA410 目前所使用的 FlowCloud 的更新版本的代码。

FlowCloud 是一个用 C++语言编写的复杂文件，由三个主要组件组成–一个具有 rootkit 功能的模块、一个简单的具有持久性的模块和一个自定义后门，他们会通过多个阶段来进行部署，并且使用各种混淆和加密技术来防止被研究员分析。

Proofpoint 的研究人员之前分析了 FlowCloud 的 4.1.3 和 5.0.1 版本，而 TA410 现在使用的是 FlowCloud 的 5.0.2 和 5.0.3 版本，它们具有了更多新的功能。

研究人员解释说，与之前发现的相反，我们获得的 5.0.2 版本的样本中包含了错误信息和更多细致的记录。

3.1.4 商业电子邮件攻击 5 年间涉及 430 亿美元

联邦调查局日前发出警告声称，在 2016 年 6 月到 2021 年 12 月期间，商业电子邮件妥协（BEC）攻击案件所涉的金额为 430 亿美元。根据联邦调查局的报告，该机构的互联网犯罪中心（IC3）一共收到了 241,206 起投诉。

BEC 或电子邮件帐户妥协（EAC）是一种先进的诈骗技术，不仅针对企业员工，也针对他们为之工作的企业。而诈骗的手段则包括社交工程，作为破坏合法企业或个人电子邮件帐户或进行未经授权的资金转移的手段。联邦调查局还警告说，该骗局的另一个流行变体包括收集个人身份信息（PII），以实施额外的欺诈行为，比如与税收有关的诈骗和违反加密货币钱包。

BEC/EAC 诈骗统计

据 IC3 称，美国所有 50 个州和 177 个国家都报告了存在 BEC 的诈骗受害者。此外，140 个国家收到了欺诈性转账信息。IC3 显示，位于泰国和香港的银行是欺诈资金的主要目的地，其次就是中国、墨西哥和新加坡。

在 IC3 的公共服务公告中，与非美国受害者相比，美国受害者的损失就要大得多。在 2013 年 10 月至 2021 年 12 月期间，共有 116401 名美国受害者报告总损失 1480 亿美元，而同期，5260 名非美国公民报告损失为 12.7 亿美元。

联邦调查局认为，2019 年 7 月至 2021 年 12 月期间，BEC 诈骗激增 65%的原因部分可能归因为疫情造成的。因为疫情对于正常的商业线下活动施加了限制，使得大部分的商业活动都转向了虚拟模式。

据 IC3 报告称：在 2019 年 7 月至 2021 年 12 月期间，已确定的全球暴露损失增加了 65%，而美元损失意味着上述损失包括以美元计算的实际和未遂损失。IC3 补充说：“这一增长部分归因于新冠肺炎大流行期间对正常商业行为的限制，这导致更多的工作

场所和个人以虚拟方式开展日常业务。”

与加密货币相关的 BEC 欺诈

IC3 在公共服务公告中提到，他们收到了越来越多的 BEC 涉及加密货币的投诉。

加密货币是一种使用加密算法保护金融交易的虚拟资产，现已在 2021 年 11 月具有了 3 万亿美元的市值。因此对与加密货币相关的匿名客户进行攻击在非法威胁行为者中很受欢迎，并致使他们积极地进行与加密相关的欺诈。

IC3 报告了涉及加密货币的 BEC 骗局的两种不同变体。第一个是直接转移到加密货币交易所（CE），这与传统的 BEC 欺诈类似。另一个涉及加密货币交易所的所谓“第二跳”。在第二跳传输中，受害者受到欺诈，向威胁行为者提供许可证或护照等识别信息，攻击者使用这些信息以受害者的名义打开加密货币钱包。一般来说，威胁行为者使用其他支持网络的骗局（敲诈勒索、技术支持和浪漫诈骗）来诱骗受害者。

据 IC3 称，加密货币的使用者定期向他们报告，但直到 2018 年才被确定为“特定于 BEC”的犯罪。2019 年，报告有所增加，到 2020 年，IC3 收到了加密货币损失 1000 万美元的报告。2021 年，加密货币相关损失飙升至 4000 万美元。

意见和建议

使用双重认证来验证更改帐户信息的请求。

确保电子邮件中的 URL 与其声称来自的业务/个人相关联。

警惕可能包含实际域名拼写错误的超链接。

避免通过电子邮件提供凭证或任何其他个人身份信息 (PII)。

通过确保发件人的地址看起来与发件人地址一致，验证用于发送电子邮件的电子邮件地址，特别是在使用移动或手持设备时。

确保启用员工电脑中的设置，以便查看完整的电子邮件扩展。

定期监控财务账户的违规行为。

3.1.5 大规模黑客活动破坏了数千个 WordPress 网站

Sucuri 的网络安全研究人员发现了一场大规模的活动，该活动通过在 WordPress 网站注入恶意 JavaScript 代码将访问者重定向到诈骗内容，从而导致数千个 WordPress 网站遭破坏。感染会自动将站点的访问者重定向到包含恶意内容，即网络钓鱼页面、恶意软件下载、诈骗页面或商业网站的第三方网站，以产生非法流量。这些网站都有一个共同的问题——恶意 JavaScript 被注入到他们网站的文件和数据库中，包括合法的核心 WordPress 文件，例如：

./wp-includes/js/jquery/jquery.min.js
./wp-includes/js/jquery/jquery-migrate.min.js “

根据 Sucuri 的分析，一旦网站遭到入侵，攻击者就试图自动感染名称中包含 jQuery 的任何 js 文件。他们注入了以“/* trackmyposs*/eval(String.fromCharCode...”开头的代码..... ”

在某些攻击中，用户被重定向到包含 CAPTCHA 检查的登录页面。点击假验证码后，即使网站未打开，他们也会被迫接收垃圾广告，这些广告看起来像是从操作系统生成的，

而不是从浏览器生成的。

据 Sucuri 称，至少有 322 个网站因这波新的攻击而受到影响，它们将访问者重定向到恶意网站 drakefollow[.]com。“他表示：“我们的团队发现从 2022 年 5 月 9 日开始，这一针对 WordPress 网站的大规模活动收到了大量用户投诉，在撰写本文时该活动已经影响了数百个网站。目前已经发现攻击者正在针对 WordPress 插件和主题中的多个漏洞来破坏网站并注入他们的恶意脚本。我们预计，一旦现有域名被列入黑名单，黑客将继续为正在进行的活动注册新域名。”

对此，Sucuri 也表示网站管理员可以使用他们免费的远程网站扫描仪检查网站是否已被入侵。