安恒威胁情报中心

安全威胁情报周报

Threat Intelligence 2021

（2021.5.22~5.28）

目录

【恶意软件威胁情报】

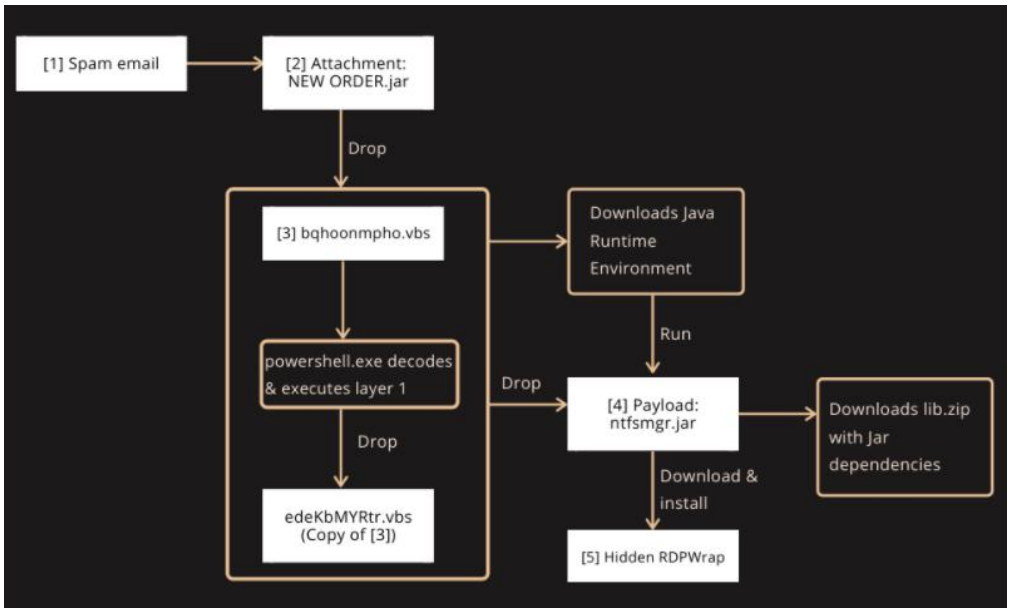
8220 团伙使用自定义挖矿程序和 Tsunami IRC Bot 进行恶意活动

研究人员最近发现了一个新的加载程序脚本，其通过独特的 Tsunami IRC 僵尸网络变体感染目标主机，并使用自定义的“PwnRig”程序进行加密货币挖矿。研究人员认为该活动与 8220 挖矿团伙有关，该团伙至少从 2017 年开始恶意活动。PwnRig 是一个基于 XMRig 的自定义挖矿工具变体，它试图隐藏其配置详细信息，并利用一个代理来防止公众监视其池详细信息。

参考链接：https://ti.dbappsecurity.com.cn/informationDetail/1993

STRRAT 恶意软件伪装成勒索软件进行传播

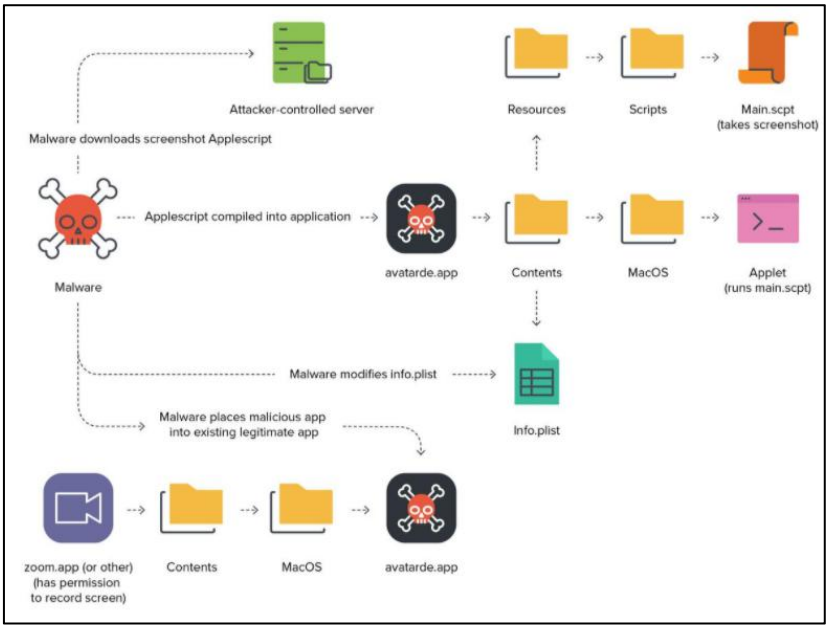
研究人员发现了一个恶意软件活动，该恶意活动正在传播一种伪装成勒索软件的 STRRAT 远程访问木马(RAT)，旨在从受害者那里窃取数据。基于 Java 的 STRRAT RAT 在大规模的垃圾邮件活动中传播，这种恶意软件表现出类似勒索软件的行为，可以窃取凭据并更改文件名，但实际上并未进行加密。攻击者使用被攻破的电子邮件帐户来发送垃圾邮件，其中包含以 PDF 附件形式出现的图像，打开图像后，恶意代码连接到一个域名下载 STRRAT RAT。



参考链接：https://ti.dbappsecurity.com.cn/informationDetail/1995

新 XCSSET 恶意软件利用 Mac 0day 漏洞对用户桌面进行截屏

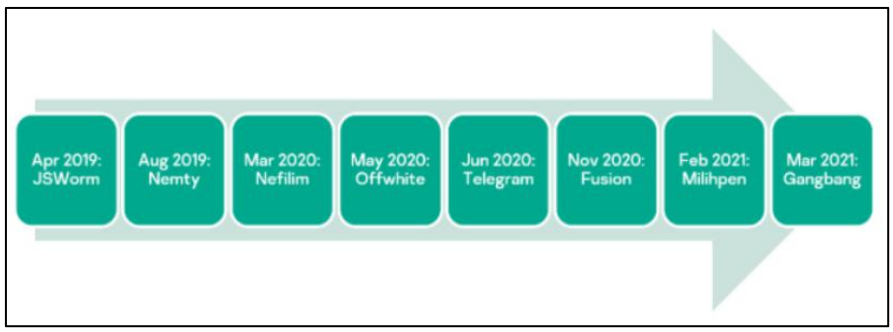
近日，研究人员在 XCSSET 恶意软件中发现了一个苹果 TCC 0 day 漏洞利用，攻击者利用该漏洞在无需用户明确同意的情况下实现用户桌面截屏。在最新发布的 macOS 11.4 版本中，苹果修复了这个绕过 TCC（Transparency Consent and Control，透明度同意和控制）框架的 0 day 漏洞——CVE-2021-30713。TCC 控制应用可以访问系统中的哪些资源，比如授予软件对摄像头和麦克风的访问权限。攻击者利用该漏洞可以在无需用户明确同意的情况下获取硬盘的访问权限、录屏和其他权限。目前，Apple 尚未在 CVE 数据库中的条目中提供有关该漏洞的具体详细信息。



参考链接：https://ti.dbappsecurity.com.cn/informationDetail/2004

JSWorm 勒索软件的演变分析

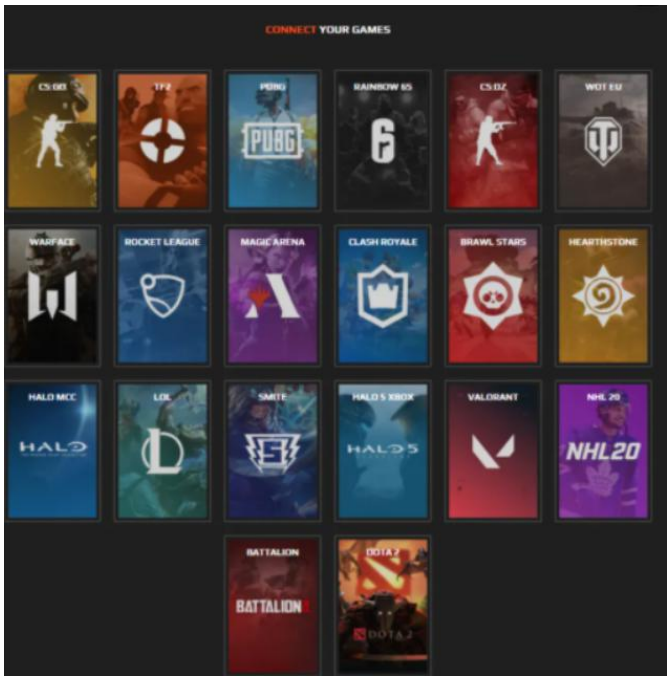
研究人员分析了 JSWorm 勒索软件近几年的演变。自 2019 年首次出现以来，JSWorm 勒索软件已经发展了两年，在此期间，它改变了发行模式，并且经过了几次完整的重新开发。在过去的几年里，勒索软件威胁的趋势已经逐渐改变。自 2017 年 WannaCry，NotPetya 和 Bad Rabbit 大规模爆发以来，许多勒索软件参与者转向了隐蔽但高利润的“big-game hunting”策略。勒索软件导致一些全球性公司服务中断的新闻现在已经司空见惯，许多勒索软件家族已经从大规模活动演变成高度针对性的威胁。



参考链接：https://ti.dbappsecurity.com.cn/informationDetail/2006

Vidar 信息窃取程序利用 Faceit 游戏平台创建 C2 URL

Faceit 是一个支持在线游戏用户进行游戏匹配的平台。它支持各种在线游戏，例如绝地求生，DOTA 2 和反恐精英：全球攻势。



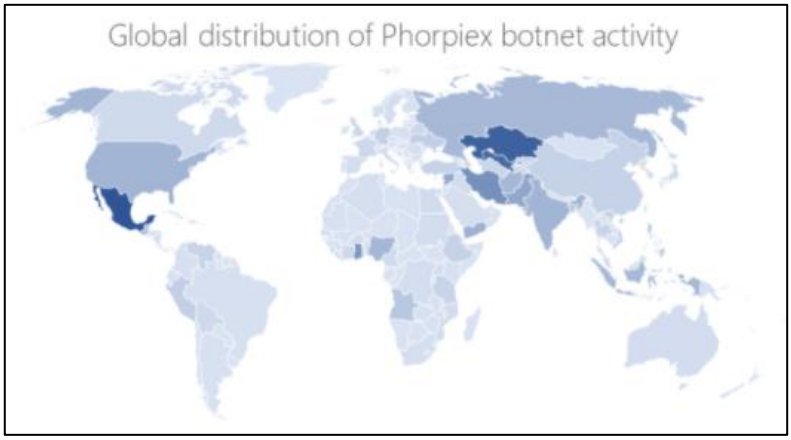
研究研究人员发现，Vidar 信息窃取恶意软件正在滥用一个名为 Faceit 的游戏匹配平台来创建 C2 服务器的 URL。Vidar 是一种恶意软件，伪装成垃圾邮件、PUP 和 KMSAuto 身份验证工具传播。在窃取信息之前，它先连接到 C2 服务器接收命令并下载其他 DLL 文件，以收集用户信息。该恶意软件之前仅连接到 C2 服务器，并像其他恶意软件一样接收命令和其他文件。但是最近，研究人员发现 Vidar 开始滥用 Faceit 在线游戏平台来创建 C2 服务器。

参考链接：https://ti.dbappsecurity.com.cn/informationDetail/2008

不断发展的 Phorpiex 僵尸网络变种

Phorpiex 是一个僵尸网络，以勒索活动而闻名。近年来，Phorpiex 的基础设施变得更多样化，更具弹性，并提供更危险的有效负载。Phorphiex 僵尸网络造成的恶意活动包括勒索和垃圾邮件活动，现已扩展到加密货币挖掘。从 2018 年开始，研究人员还观察到数据泄露活动和勒索软件发送量的增加，该 bot 安装程序分发 Avaddon，Knot，BitRansomware（DSoftCrypt / ReadMe），Nemty，GandCrab 和 Pony 勒索软件以及其他恶意软件。

Phorpiex 僵尸网络活动的分布范围也有所扩展。此前主要针对日本，但最近在全球更广泛的范围分布。



参考链接：https://ti.dbappsecurity.com.cn/informationDetail/1997

【热点事件威胁情报】

APT 组织利用 Fortinet 漏洞入侵美国地方政府网络

美国联邦调查局(FBI)表示，一个 APT 组织利用一个未打补丁的 Fortinet 网络设备的漏洞，侵入了美国地方政府的网络服务器。FBI 发布警告称，此次入侵是在 2021 年 5 月检测到

的。2021 年 4 月，FBI 曾警告美国私营部门和政府机构给 Fortinet 设备打补丁，因为 APT 正在扫描互联网，寻找易受 CVE 2018-13379、CVE-2020-12812 和 CVE-2019-5591 三个漏洞攻击的 Fortinet 设备。尽管早期预警过，但黑客还是成功入侵了市政府的网络服务器。

参考链接：https://ti.dbappsecurity.com.cn/informationDetail/2018

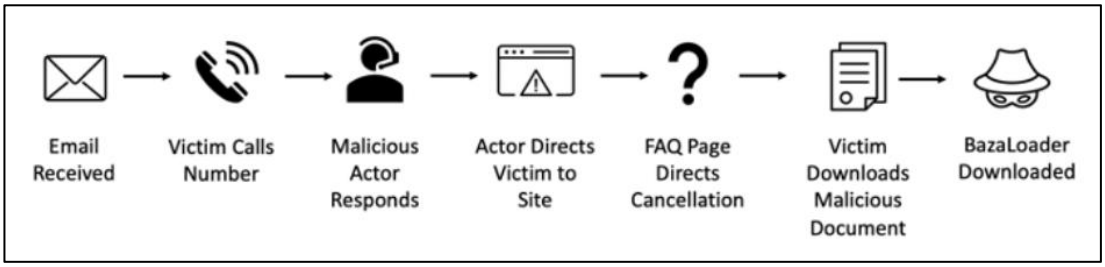
美国 CNA 保险巨头向勒索团伙支付 2.5 亿赎金

美国最大的保险公司之一 CNA Financial，在 2021 年 3 月 21 日，遭到名为 Phoenix CryptoLocker 的勒索软件攻击，并加密了 15000 台设备，导致网络中断，影响了某些 CNA 系统，包括公司电子邮件。3 月底，CNA Financial 向黑客支付了 4000 万美元（2.5 亿人民币），以恢复对其系统的访问，赎金金额为整个 2020 年网络攻击的最高赎金，还远高于 2019 年的最高赎金 1500 万美元，成为迄今为止最昂贵的赎金之一。

参考链接：https://ti.dbappsecurity.com.cn/informationDetail/1996

BazaFlix：利用虚假流媒体服务传播 BazarLoader 的恶意活动

近日，研究人员发现了一起利用伪造电影流媒体服务传播 BazaLoader 的恶意活动，该活动需要大量的受害者交互才能传播 BazaLoader 后门。黑客传播电子邮件，指示受害者致电客户服务热线，然后将受害者引导到包含恶意内容的网站。另外，黑客创建了一个名为 BravoMovies 的虚假电影流媒体服务，并以假冒电影名作为登陆页面，研究人员将这种攻击方法命名为 BazaFlix。此活动代表了 BazaLoader 攻击者利用呼叫中心传播 BazaLoader 恶意软件的趋势。



参考链接：https://ti.dbappsecurity.com.cn/informationDetail/2009

【电子行业威胁情报】

美国 Bose 音频制造商遭勒索团伙泄露数据

美国音响业巨头 Bose 公司近日在受到勒索软件攻击后披露了数据泄露，该公司称他们于 2021 年 3 月 7 日首次在 Bose 的美国系统上检测到勒索软件，目前已经与网络安全专家合作完成恢复受影响的系统，还与数字取证小组合作确定攻击者是否设法访问了敏感信息。

且公司表示不会支付任何赎金。勒索软件攻击中暴露的个人信息包括姓名、社会安全号码、薪酬信息和其他人力资源相关信息。

参考链接：https://ti.dbappsecurity.com.cn/informationDetail/2005

【航空行业威胁情报】

印度航空泄露 450 万名乘客信息

近日，印度航空公司（Air India）发布声明称，其乘客服务系统(PSS)供应商 SITA 在早些时候遭受网络攻击后，大约 450 万名乘客的信息被泄露。泄露的个人信息包括：姓名、出生日期、联系方式、护照信息、信用卡数据等。但印度航空表示，与信用卡相关的 CVV/CVC 号码和密码均未受到影响。

印度航空是全球航空运营商联盟星空联盟的成员之一。参加该联盟的其他多家航空公司 3 月提醒各自乘客群体，黑客攻击事件造成客户数据泄露，涉及客户姓名和航班号。

参考链接：https://ti.dbappsecurity.com.cn/informationDetail/2001

【政府行业威胁情报】

日本政府多个单位泄露敏感数据

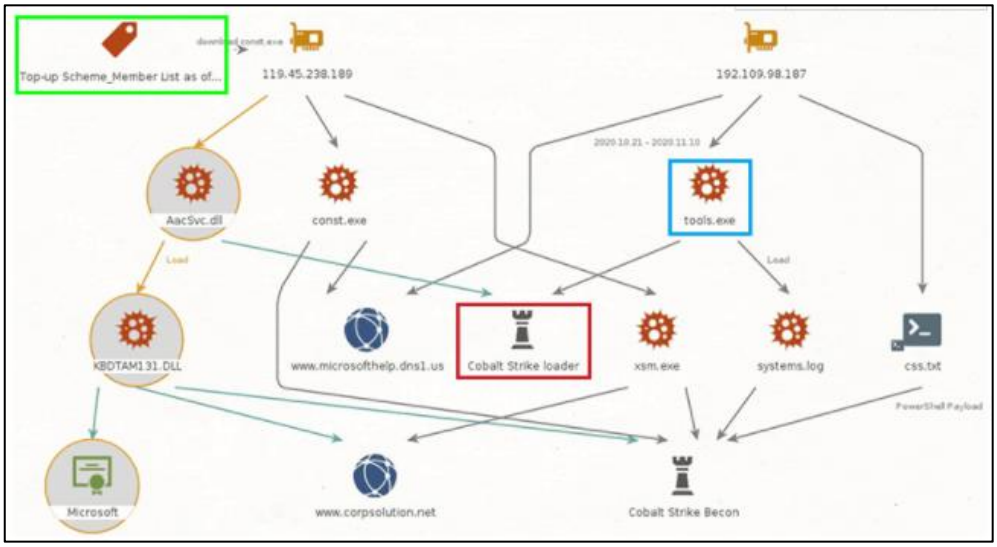
近日，黑客获取了日本科技巨头富士通的系统访问权限，其中“ProjectWEB”是富士通在 2000 年代中期推出的基于云的企业协作和文件共享平台。由于日本政府多个单位都使用了 Fujitsu（富士通）的“ProjectWEB”平台，导致日本政府众多单位和部门敏感数据泄露。迄今为止，已知的受影响机构包括：日本国土交通省；日本运输和旅游部；日本外交部；日本内阁秘书处；日本成田国际机场。失窃的数据包括政府雇员存储在“ProjectWEB”上的文件。

参考链接：https://ti.dbappsecurity.com.cn/informationDetail/2015

【高级威胁情报】

APT41 组织使用滥用 Microsoft 数字签名进行恶意活动

自 2021 年初以来，研究人员一直在观察使用 SigLoader (也称为 DESLoader，Ecipekac) 的恶意活动。近期，国外安全厂商都报道了使用 SigLoader 进行的一系列攻击。在调查利用 Sigloader 的攻击时，研究人员发现了多种不同于 SigLoader，利用 Microsoft 数字签名 DLL 文件的恶意软件“ Cobalt Strike loader”。研究人员猜测 APT41 可能使用了利用 Microsoft 数字签名的 Cobalt Strike Dll 加载程序。

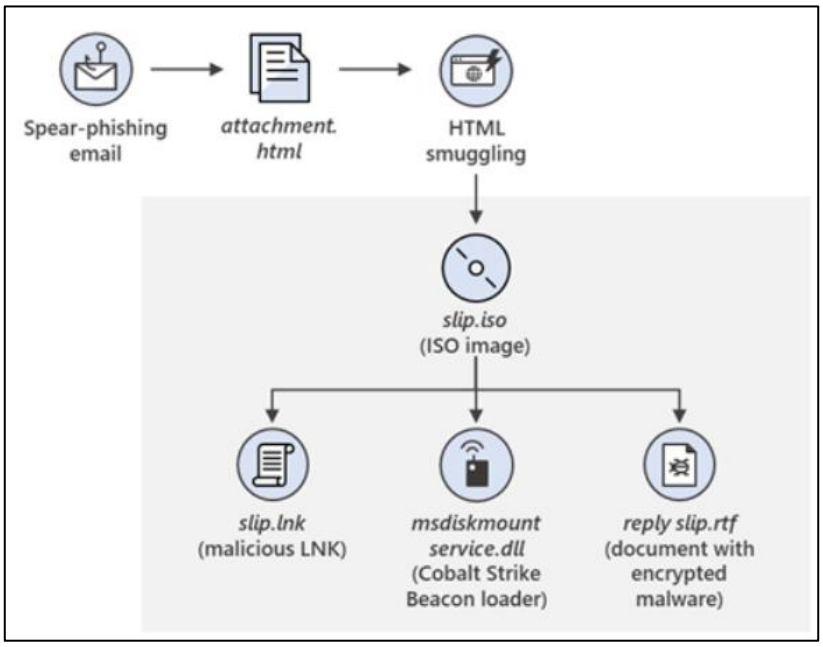


参考链接：https://ti.dbappsecurity.com.cn/informationDetail/1998

研究人员披露 NOBELIUM 组织运营的大规模恶意电子邮件活动

研究人员发现了一个由 NOBELIUM 组织运营的大规模恶意电子邮件活动。NOBELIUM 是针对 SolarWinds、SUNBURST 后门、TEARDROP 恶意软件、GoldMax 恶意软件和其他相关组件的攻击背后的威胁组织。2021 年 5 月 25 日，NOBELIUM 利用合法的群发邮件

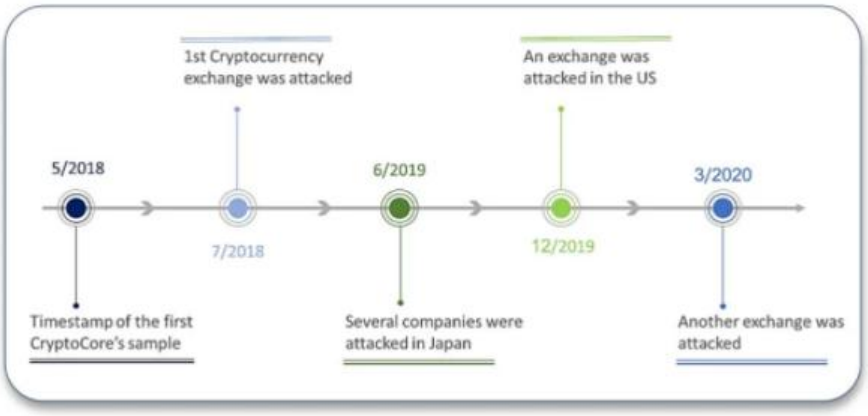
服务 Constant Contact，伪装成一家总部位于美国的开发组织，向各种组织和行业垂直组织分发恶意 url。



参考链接：https://ti.dbappsecurity.com.cn/informationDetail/2016

CryptoCore：Lazarus 组织针对加密货币交易所的攻击活动分析

研究人员近日发布的报告表示，窃取数亿美元的 CryptoCore 攻击活动被证实与 APT 组织 Lazarus 有关。CryptoCore 活动自 2018 年开始活跃，目标是窃取加密货币钱包，Lazarus 攻击了美国、以色列、欧洲和日本等国的加密货币交易所，造成的损失估计超过 2 亿美元。

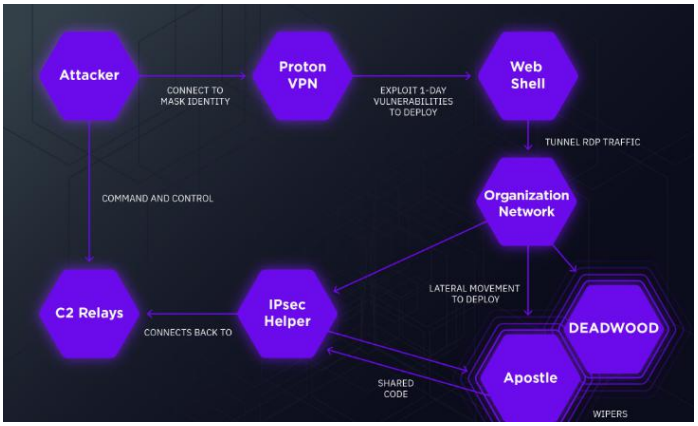


参考链接：https://ti.dbappsecurity.com.cn/informationDetail/2017

研究人员披露新型伊朗黑客组织 Agrius

Agrius 是一个新的威胁组织，研究人员认为它来自伊朗，从事间谍活动和破坏活动。该组织利用自定义工具集，以及公开可用的攻击性安全工具，主要目标是中东地区的各种组织。在某些情况下，该组织利用其访问权部署了破坏性的擦除器恶意软件，在其他情况下则是定制的勒索软件，因此，研究人员认为 Agrius 不太可能是出于经济动机。

Agrius 组织自 2020 年初以来一直活跃，最初针对中东地区，但自 2020 年 12 月以来，该组织将攻击重心转移到了以色列。



参考链接：https://ti.dbappsecurity.com.cn/informationDetail/2002

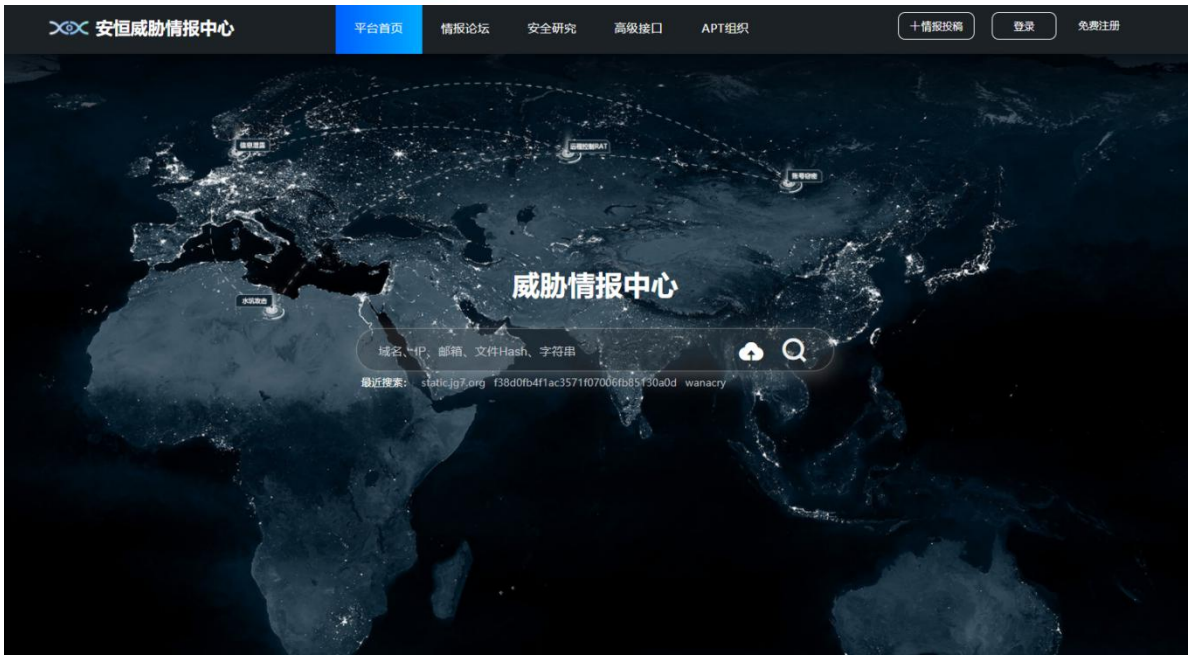
疑似 APT29 组织以“美国联邦选举”为主题展开网络钓鱼活动

2021 年 5 月 25 日，研究人员发现了一起针对美国和欧洲多个组织的网络钓鱼活动。该活动以非政府组织、研究机构、政府机构、国际机构为目标，传播以“美国联邦选举”为主题的钓鱼邮件。研究人员认为，该活动可能与 APT29 组织有关。目前尚不清楚有多少组织已经成为攻击目标。

参考链接：https://ti.dbappsecurity.com.cn/informationDetail/2013

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/