安天智甲有效防护 Jupyter 窃密木马变种

近日，安天 CERT 在梳理网络安全事件时发现一个具有后门功能的 Jupyter 窃密木马变种。Jupyter 木马又名 Solarmarker，2020 年 11 月首次被发现，主要窃取 Chromium、Firefox 和 Chrome 浏览器数据并将详细信息上传到 C2 服务器，下载和执行更多恶意代码。与之前的窃密木马相比，此版本的 Jupyter 窃密木马利用 MSI 安装程序进行分发，主要窃取用户凭证等。

安天 CERT 在分析 MSI 安装程序的文件属性 (OLE Compound) 时，发现攻击者使用 Advanced Installer 的试用版 (版本 18.6.1 build 2c9a75c6) 生成超过 100MB 的 MSI 文件。该 MSI 文件由于较大，可以有效绕过在线杀毒软件扫描程序。该 MSI 文件具有合法签名，攻击者从合法企业 (TACHOPARTS SP.Z O.O.) 窃取了该数字签名。

攻击者利用 Advanced Installer 在 MSI 文件的“CustomAction”属性中写入 PowerShell 语句。当受害者执行 MSI 安装文件后，MSI 文件安装自文件 Nitro Pro 13，同时该 PowerShell 语句被 Windows Installer 当作“CustomAction”属性执行。PowerShell 的功能是加载随机命名的 ps1 文件，随机命名的 ps1 文件加载由 .NET 开发的恶意 DLL 载荷。该恶意 DLL 载荷被混淆，主要功能是窃取受害者的凭证等信息，并将搜集到的信息上传到 C2 服务器，等待接收 C2 指令，下载和执行其它载荷。

安天 CERT 提醒广大政企客户，应提高网络安全意识。在日常工作中及时进行系统更新和漏洞修复，不随意下载非正版的应用软件，注册机等。收发邮件时应确认收发来源是否可靠，不随意点击或者复制邮件中的网址，不轻易下载来源不明的附件，发现网络异常要提高警惕并及时采取应对措施，养成及时更新操作系统和软件应用的良好习惯。确保所有的计算机在使用远程桌面服务时避免使用弱口令，如果业务上无需使用远程桌面服务，建议将其关闭。目前，安天追影产品已经实现了对该窃密木马的鉴定；安天智甲已经实现了对该窃密木马的查杀。

木马程序 安天【追影威胁分析系统】无需更新病毒库，即可实现对上述木马程序进行有效检测，下为其自动生成的分析报告：

文件由页面手工提交，经由 BD 静态分析鉴定器、YARA 自定义鉴定器、来源信息鉴定器、文件相似分析鉴定器、数字证书鉴定器、元数据信息鉴定器、聚类分析鉴定器、反病毒引擎鉴定器、动态（WinXP）鉴定器、字符串分析鉴定器、智能学习鉴定器、静态特征检测鉴定器、安全云鉴定器、动态（Win7sp1 x86）鉴定器、动态（Win7 x86）鉴定器等鉴定分析。

最终依据 BD 静态分析鉴定器将文件判定为木马程序。

◆ 概要信息

文件名	xlcPDdwzGG.dll
文件类型	BinExecute/Microsoft.DLL[:X86]
大小	39 KB
MD5	5B2085D1DDB9FE959D010C2E09E2B058
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.Bulz
判定依据	BD 静态分析鉴定器

报告地址：https://1.119.163.6/vue/details?hash=5B2085D1DDB9FE959D010C2E09E2B058

◆危险行为

行为描述	危险等级
通过标记进程可执行堆绕过 DEP	★★★★★
创建互斥量	★★★
映射内存方式注入	★★★

◆常见行为

行为描述	危险等级
获取系统信息(处理器版本、处理器类型等)	★
获取主机内存信息	★★
获取系统版本	★
加载运行时 DLL	★

◆静态启发式检测

检测类型	检测点	详细说明
PE 结构	无版权信息	基于海量恶意代码和受信白名单文件名进行数据挖掘，正规软件厂商的文件基本包含版权信息。
PE 结构	非微软的版本信息	非受信厂商的版本信息。具有较低的受信级别。

◆运行环境

操作系统	内置软件
Win7sp1 x86 旗舰版 service Pack 1	默认、IE8、Google Chrome、Firefox、Office2013、Flash、FoxitReader、Adobe Reader DC

◆扫描二维码查看完整报告

安天周观察
安天对外开放资料平台 安天官方微信
主办：安天 2021年10月18日(总第298期)试行 本期4版 扫描上方二维码查询安天所有对外开放资料

安天与中传悦众签署战略合作，助力文化创意产业发展

10 月 13 日，安天与中国文化传媒集团旗下中国文化传媒新文创（IP）平台（以下简称中传新文创（IP）平台）在中国文化传媒集团总部正式签署战略合作协议。安天执行董事长兼 CEO 游小明，安天资深副总裁方华，中国文化传媒集团党委书记、董事长兼《中国文化报》社社长刘强，中国文化传媒集团副总经理杨胜生，中传悦众（北京）文化发展有限公司执行董事兼总经理秦智勇等双方高管共同出席签约仪式。

▲ 双方签署战略合作协议
（左：中传悦众（北京）执行董事兼总经理秦智勇
右：安天执行董事长兼 CEO 游小明）

刘强表示，中传新文创（IP）平台涉及到文化、旅游、游戏、动漫等各方面，是一个基础性公共服务市场化运作的平台。希望通过第三方和市场化的管理充分保护文化创意产业和人员。通过与安天的合作，希望双方发挥优势，易用、快捷、到位、有效地把中国的创意产业和创意人员充分保护好，得到社会效益和经济效益的双丰收。

游小明表示，前期双方在市场、技术层面开展了多轮深入细致的研讨，特别是在一些技术方面的合作已先期启动，签署战略合作协议，标志双方进入紧密合作、共谋发展的新阶段。未来安天将以服务行政管理部门和各方企业为己任，提供具有国际竞争力、自主创新的安全解决方案和优秀的实践服务，不断创造新业态，为营造风清气正的网络空间贡献力量。

同时，双方将成立联合实验室，整合在实验室建设、知识产权转化、媒体宣传、技术推介方面的资源和优势，围绕全网游戏及文娱平台内容和全网终端响应能力展开有关产品和应用技术的研发工作。（原文链接：https://mp.weixin.qq.com/s/Ag8SGB2_YzoMF8dfrVRgvQ）

扫描右侧二维码阅读全文

“2021 年网络安全优秀创新成果大赛”完美收官 安天获奖

10 月 11 日，由中国网络安全产业联盟主办的 2021 年国家网络安全宣传周“网络安全产业发展论坛”在西安隆重召开。活动现场举行了“2021 年网络安全优秀创新成果大赛”颁奖仪式，安天智甲云主机安全系统凭借优秀的设计理念、成熟的产品应用能力和技术创新优势荣获“2021 年网络安全优秀创新成果大赛”二等奖。

▲ “2021 年网络安全优秀创新成果大赛”颁奖现场

“2021 年网络安全优秀创新成果大赛”是 2021 年国家网络安全宣传周活动的组成部分，是 CCIA 在连续三年组织开展“优秀网络安全解决方案和创新产品评选活动”基础上进行的创新评选活动。本次大赛分为分站赛初赛、半决赛和总决赛三个阶段，共征集到 110 余家企业申报的 200 余项解决方案和创新产品。

安天高级副总裁王小丰亲历初赛、半决赛和决赛现场答辩环节，历经 4 个月的赛程，将安天智甲云主机安全系统市场前景、产品创新性等优势完整呈现。（原文链接：https://mp.weixin.qq.com/s/MhZrX_m1gRJAn94_d4DN6w）

扫描右侧二维码阅读全文

XCon2021：安天移动安全持续聚焦移动终端对抗技术和开发者服务

2021 年 XCon 安全焦点信息安全技术峰会（XCon2021）暨 XCon20 周年盛典于 10 月 12 日在北京举行。安天移动安全针对移动黑灰产问题和开发者服务两大热点话题发表演讲。

XCon2021 议题覆盖移动安全、云安全、人工智能、漏洞利用与缓解、逆向工程等多个领域。会上，安天移动安全高级副总裁陈家林、安天移动安全资深安全专家徐文礼带来《移动互联网黑灰产对抗与治理》和《安鉴—开发者 App 隐私安全与合规评估》两场演讲。

陈家林指出，近年来针对移动终端用户的安全威胁并未随之递减，反而呈现出威胁泛化的趋势，由于生产要素的获取极其便利且廉价，在流量利益的驱使下，风险应用程序出现大规模扩张，其依附于移动互联网业务形态，正通过更加隐蔽的方式侵害用户权益。

如何合法合规的使用数据，保障用户个人信息安全已成为政府监管部门关注的重要问题。徐文礼提到，“很多开发者、企业因为缺少用户权益合规方面的专业人才，对用户权益保障认定标准和治理目标理解不到位，以及缺乏专业、高效的合规检测工具等原因，导致大量 App 因为违规收集、使用个人信息，强制、过度索取权限等侵害用户权益的行为被要求下架、整改，不仅造成用户流失、品牌影响力下降，甚至直接带来不可估量的经济损失。”（原文链接：https://mp.weixin.qq.com/s/JZIfCi7fgodj-X260UUtXA）

扫描右侧二维码阅读全文

每周安全事件

类 型	内 容
中文标题	APT 组织 MalKamak 以航空航天和电信公司为目标
英文标题	Operation GhostShell: MalKamak APT targets aerospace and telco firms
作者	Pierluigi Paganini
内容概述	研究人员发现了一个新的黑客组织，该组织正以航空航天和电信公司为目标，使用 ShellClient 恶意软件作为 GhostShell 行动的一部分。ShellClient 是以前没有记录和秘密的 RAT(远程访问木马)，它可用于窃取受害者的敏感信息。GhostShell 行动是一项针对性很强的网络间谍活动，主要打击中东地区、美国、俄罗斯和欧洲的一些受害者。研究人员将这些活动归因于一个新的与伊朗有关的黑客组织，追踪到他叫 MalKamak，他与 APT39 组织有一些联系。
链接地址	https://securityaffairs.co/wordpress/123045/apt/operation-ghostshell-shellclient-malware.html

每周值得关注的恶意代码和漏洞信息

经安天【CERT】检测分析，本周有 3 个活跃的漏洞以及 7 个活跃的恶意代码家族值得关注

恶意代码类别	名称	威胁等级	简要描述
活跃漏洞	Google Chrome 远程代码执行漏洞（CVE-2021-3794）	高	Google Chrome 存在远程代码执行漏洞。由于 Google Chrome 中的安全浏览组件中存在 use-after-free 错误，使得远程攻击者可以创建一个特制的网页，诱使受害者访问它，触发释放后使用错误并在目标系统上执行任意代码。
	Apache HTTP Server 目录遍历漏洞（CVE-2021-41773）	高	Apache HTTP Server 存在远程代码执行漏洞。由于 Apache 在处理目录遍历序列时的输入验证存在错误，使得远程攻击者可以发送特制的 HTTP 请求，将 URL 映射到 Web 目录之外的文件。
	Redis 远程代码执行漏洞（CVE-2021-41099）	高	Redis 存在远程代码执行漏洞。如果将 Redis 的 proto-max-bulk-len 手动配置为比默认非常大的值，则由于处理不受信任的输入时整数溢出而存在该漏洞，使得远程攻击者可以将特制数据传递给应用程序，触发整数溢出并在目标系统上执行任意代码。
较为活跃样本家族	Trojan[Ransom]/Win32.Blocker	中	此威胁是一种赎金类木马家族。该家族木马运行后会破坏电脑系统、损坏用户的文件，对用户文件加密使用户无法打开。此时黑客会向用户索要赎金并提供所谓的“密钥”，但用户支付赎金后仍然不能修复受损的文件。
	Trojan[Backdoor]/Win32.Finfish	中	该病毒家族是一种可以窃取用户信息的木马类程序。该家族样本运行后修改注册表使其自启动，窃取用户敏感信息，如帐号密码等。
	Trojan/Win32.Fsysna	中	此威胁是一种木马家族。该家族样本运行后会在电脑的临时文件夹下释放恶意代码，同时添加注册表启动项，并发送网络请求。
	Trojan[Dropper]/Win32.Daws	中	此威胁是一种具有捆绑行为的木马类程序。该家族木马感染用户系统后，会自动释放出 其它恶意程序并运行。释放的程序大多为盗号类木马程序。
	Trojan/Win32.Cosmu	中	此威胁是一种下载类木马家族。该家族木马会从指定的服务器下载多种恶意软件和广告软件。该家族木马还会在系统后台定时访问指定的站点，以提高这些网站的访问量，为木马制作者获取利益。
	Trojan[DDoS]/Linux.Xarcen	中	此威胁是一种 Linux 平台上的僵尸网络家族。该家族样本主要利用漏洞和弱口令对 IoT 设备进行攻击并组建僵尸网络，利用该僵尸网络对任意目标发动 DDoS 攻击。
	Trojan/Android.Hqwar	中	此威胁是安卓平台的一类木马家族。该家族样本伪装成知名游戏应用，运行后隐藏图标，诱导激活设备管理器，接收短信指令，上传通讯录和信箱等隐私信息，进行发送短信、回复短信、拨打电话、卸载指定 apk、联网下载 apk 并弹出诱导安装等操作。建议立即卸载，避免造成隐私泄露和资费损耗。

防范内部人员威胁的三种方法

艾萨克·科恩 / 文 安天技术公益翻译组 / 译

每年的 10 月是国家网络安全意识月。但是，即使不举办特殊的活动，大多数企业领导和消费者也已经意识到网络安全在当今动荡数字环境中的重要性。

即便如此，给大家提个醒也无妨。

2021 年，数据泄露的平均成本首次超过 400 万美元；从网络钓鱼诈骗到勒索软件攻击的各类攻击，其频率和范围都刷新了纪录。而在头条新闻上看到这些攻击事件是一回事，形成网络安全意识是另一回事。根据 Gartner 2021 年首席信息官（CIO）议程，超过一半的企业领导将“使员工在 2021 年形成网络安全意识”作为首要任务。

在分配资源时，CIO 和其他企业决策者需要权衡几个关键优先事项，并就企业防御态势提出一些问题，包括：是否应将安全预算分配给下一代防火墙，以增强现场网络安全性；是否应将网络安全预算用在保护远程员工的入站连接上？应该投资于“人”还是软件解决方案?

软件解决方案对于保护数字基础设施和公司数据至关重要，但是，将网络安全预算用于常被忽视的因素——“员工”，企业能够获得最大的投资回报。

一项行业研究发现，在 85% 的数据泄露和网络安全事件中，“人为因素”起着至关重要的作用。因此，“人”成为企业投入时间、精力和资金的关键因素。更具体地说，企业可以通过以下三种方式防范内部人员威胁。

承认并防御恶意内部人员

企业内部人员，包括员工、承包商和其他可访问其 IT 资源的受信第三方，通常在企业的信任下开展业务。这些人员由企业付费，其日常运营应支持企业的目标。

不幸的是，一些受信内部人员会成为攻击者。恶意内部人员受经济利益的驱使，会破坏企业的数字基础设施，窃取隐私数据或公司机密。虽然每个恶意内部人员都会利用其访问权限来造成破坏，但他们的行为通常各有特色，例如：

1. Tesla 的一名员工故意破坏公司的网络，将敏感信息传输给第三方。

2. Facebook 的一名工程师利用其权限，在线跟踪一名女性。

3. Suntrust 银行的一名员工下载了 150 万客户的个人身份信息（PII）。

企业应承认“存在恶意内部人员破坏网络安全的可能性”，并增强其网络安全态势。用户活动监控和行为分析可以为网络安全专家提供必要的洞察力，以阻止恶意内部人员入侵。但是，公司首先要承认这种风险，然后才能以正确的解决方案做出响应。

对员工开展安全意识培训，实施问责制

企业员工不会突然变得“具有网络安全意识”。事实上，普通员工在日常工作和履行职责时很少考虑到网络安全。因此，企业有责任对员工和安全团队开展培训，帮助其识别和防御最新的威胁模式。

举例来说，自新冠疫情爆发以来，网络钓鱼诈骗显著增加，每一条恶意消息都有可能破坏企业数据完整性。同时，许多员工无法识别这些威胁；即使能够识别这些威胁，他们也不知道该如何应对。

当然，员工培训不应仅限于网络钓鱼诈骗。一项调查发现，61% 的员工未能通过有关网络安全基础知识的测验。很多企业仅将 5% 的 IT 预算用于员工培训，在这方面他们有很大的提升空间。

除了开展员工培训，企业还应实施问责制。这样一来，企业就可以将员工转变为强大的防御资产。

防止意外事件，杜绝粗心大意

意外时有发生，因此企业应具备“识别意外数据泄露并尽快纠正”的能力。人工智能驱动的行为分析可帮助企业识别意外事件，防止数据泄露。

同时，企业领导者应注意不要将粗心大意与意外混为一谈。举例来说，“123456”和“password”是最热门的两种口令组合，它们存在明显缺陷。当使用这些口令的账户遭到攻击时，其原因是就是粗心大意，而非意外。同样，员工不应忽视简单的最佳实践，如双因子身份鉴别或 VPN 服务，这些实践可在各种漏洞环境中保护其账户和公司数据的安全。

企业应深入了解员工的数字活动，以识别和纠正粗心行为，同时让员工为自己的行为负责。如今，随着网络环境的风险不断升级，企业应强化其安全要求。

结论

在今年的网络安全意识月，各行业各种规模的企业都可以重新评估其网络准备就绪情况。许多企业不会喜欢他们发现的问题。然而，改善网络安全无法一蹴而就，即使是渐进式的增强也可以保护企业数据和 IT 基础设施免受侵害。

如今，数据泄露的成本和后果前所未有地严重。企业可以在网络安全意识月实施网络安全状态评估，并根据评估结果采取最好的网络安全措施。

原文名称	3 ways any company can guard against insider threats this October
作者简介	艾萨克·科恩 （Isaac Kohen），是美国 Teramind 公司的研发副总裁。
原文信息	2021 年 9 月 27 日发布于 Help Net Security 原文地址 https://www.helpnetsecurity.com/2021/09/27/guard-against-insider-threats/
摘 要	企业可以通过以下三种方式防范内部人员威胁：（1）承认并防御恶意内部人员；（2）对员工开展安全意识培训，实施问责制；（3）防止意外事件，杜绝粗心大意。
免责声明	本译文不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天集团一律不予承担。