安天发布《z0Miner挖矿木马变种分析报告》

近日，安天CERT在梳理网络安全事件时发现一个名为z0Miner的挖矿木马变种。z0Miner首次出现时间是在2020年，攻击者利用多个远程代码执行漏洞传播该木马。安天CERT近期监测到该木马变种利用Confluence产品漏洞进行传播。

2021年8月，Atlassian官方发布公告，披露了一个旗下Confluence产品的远程代码执行漏洞（CVE-2021-26084），Confluence是该公司出品wiki程序，是目前市场上非常流行的企业wiki应用。攻击者经过认证后或在部分场景下无需认证，即可远程执行任意代码。z0Miner木马近期通过该漏洞进行传播。

攻击者利用漏洞成功后，执行挖矿木马z0Miner。z0Miner部署web shell下载多个文件，包括sys.ps1、vmicguestvs.dll和ok.bat。sys.ps1的功能有两个，第一个功能是创建计划任务并将它伪装成.NET Framework NGEN任务，该任务每隔五分钟从Pastebin下载并执行脚本(因链接失效无法获取脚本）。sys.ps1的第二个功能是下载clean.bat，clean.bat的功能是查找并删除其他挖矿木马。z0Miner将vmicguestvs.dll伪装为合法的集成服务（Hyper-V Guest Integration）以规避防御机制。ok.bat的功能是下载挖矿程序。

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密码，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类挖矿木马的鉴定；安天智甲已经实现了对该挖矿木马的查杀。

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、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（Win7 x64）鉴定器等鉴定分析。

最终依据BD静态分析鉴定器、安全云鉴定器将文件判定为木马程序。

◆概要信息

文件名	network02.exe
文件类型	BinExecute/Microsoft.EXE[:X64]
大小	4.50 MB
MD5	F0CF1D3D9ED23166FF6C1F3DEECE19B4
病毒类型	木马程序
恶意判定/病毒名称	RiskWare[RiskTool]/Win32.BitMiner
判定依据	反病毒引擎

报告地址：https://1.119.163.6/vue/details?hash=F0CF1D3D9ED23166FF6C1F3DEECE19B4

◆元数据信息

描述	值
File Size	4.5 MB
File Type	Win64 EXE
MIME Type	application/octet-stream
Machine Type	AMD AMD64
PE Type	PE32+
……	……

◆运行环境

操作系统	内置软件
Win7 x64 6.1.7601 Build 7601	默认、IE9、Google Chrome、Firefox、Office2007、Flash、WPS、FoxitReader、AdobeReader

◆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	★★★★★

◆常见行为

行为描述	危险等级
加载运行时DLL	★
获取系统信息(处理器版本、处理器类型等)	★★
获取计算机名	★
查询系统时间	★

◆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25日(总第299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

安天对赛克蓝德战略投资 强化态势感知实战化运营

近日，安天宣布对赛克蓝德进行战略投资。双方将进行深度的产品、解决方案合作，以及能力融合。该合作将有效增强安天态势感知和整体安全解决方案的运维能力，提高事件日志管理成熟度水平，提升接入运营的第三方产品品类覆盖能力。

赛克蓝德董事长朱林表示：“安天是有家国情怀与技术信仰的企业，二十多年来一直坚守在网络安全这个当年看起来布满荆棘的方向，持续深度耕耘反病毒引擎技术，在这个非常关键的领域做到全球顶尖，此后把反病毒引擎的经验和能力向全面威胁对抗扩展，形成了有鲜明个性特点的产品体系，这条道路非常值得我们学习；通过此次合作，赛克蓝德加入到安天这个大家庭中，可以获得安天的很多赋能，比如情报对接、SOAR整合等，弥补了公司产品线的短板，提供更有竞争能力的产品；我们相信通过这次合作，双方发挥各自优势，提供更多更好的安全解决方案，满足客户日益增长的安全需求。”

安天创始人、董事长肖新光表示：“安天和赛克蓝德都是坚定的自主创新企业。安天和赛克蓝德的合作是自主创新企业间基于背靠背信任的合作。赛克蓝德在SIEM和SOC方向上有8年的创业积累，积极对标国际先进产品，有非常扎实的基础能力积累，对客户安全运营理解深刻，值得安天团队深入学习。在赛克蓝德的支持下，安天整体安全解决方案中管理第三方产品的覆盖能力和日志管理成熟度水平会有显著提升。安天也希望借助威胁分析和威胁情报生产能力实现对赛克蓝德的全面赋能。并借助双方产品连接、深度融合，让安天的全要素采集、场景元数据化、海量恶意代码威胁深度识别、高级威胁识别等能力，更好的转化为客户整体安全价值。相信双方在安全策略运营、用户画像、威胁情报生产消费等方面，还会结出更多的成果，创造有效的客户安全价值。”

（原文链接：https://mp.weixin.qq.com/s/pNIUTCSwn-4MUbDTpQV1gA）

扫描右侧二维码阅读全文

对某单位投递FormBook窃密木马的分析报告

概述

自今年7月以来，安天CERT监测到多起广撒网式投递窃密木马的钓鱼邮件活动，诱导目标执行附件中的FormBook窃密木马，实施窃密活动。其中捕获到一封对某单位投递的钓鱼邮件。FormBook是一种非常活跃的商业窃密木马，自2016年开始在黑客论坛上以“恶意软件即服务”形式出售，版本不断迭代更新，目前发现的最新版本为4.1，本次监测到的为3.2版本。

FormBook主要被用于窃取目标个人信息，该窃密木马能够自动收集目标系统中浏览器、邮箱客户端、即时通讯客户端和FTP客户端中的敏感信息，具备键盘记录和屏幕获取功能。同时它具有远程控制能力，具体包括更新、下发恶意软件、命令执行、数据回传等功能，实现对目标系统进行长期驻留控制。

经验证，安天智甲终端防御系统（简称IEP）可实现对该窃密木马的查杀与有效防护。

事件对应的ATT&CK映射图谱

攻击者针对目标系统投放FormBook窃密木马，梳理本次攻击事件对应的ATT&CK

▲事件对应的ATT&CK映射图谱

映射图谱如上图所示。（原文链接：https://mp.weixin.qq.com/s/4mZWD7wp5bz_LMzdw6XPNw）

扫描右侧二维码阅读全文

网安宣传周：筑牢网络安全防线 安天在十一地活动总回顾

10月11-17日，以“网络安全为人民，网络安全靠人民”为主题的2021年国家网络安全宣传周活动在全国范围内统一开展。安天携端点防护、边界防护、流量监测、深度分析等能力型产品方阵及威胁对抗解决方案亮相十一地网络安全宣传周。

安天全面参与了西安、黑龙江、河北、辽宁、吉林、山东、山西、青海、广西、内蒙古、湖北十一地网络安全宣传周活动，通过线上线下相结合的方式开展网络安全宣传活动，宣传安全理念、普及网络安全知识、推广网络安全防护技能，共筑网络安全新防线。

1. 网络安全产业发展论坛：“十四五”的三个历史任务，四大技术趋势

10月11日，由陕西省委网信办，西安市委网信办指导，中国网络安全产业联盟、中国电子技术标准化研究院联合主办“网络安全产业发展论坛”。中国网络安全产业联盟理事长、安天创始人肖新光发表致辞时表示：今年是“十四五”开局之年，网络安全领域面临系统重塑网络空间国防安全和国家安全能力、有效保障国民经济体系的数字化转型、充分满足公民个人信息和隐私安全保障需求的三个重大历史任务。“十四五”的四大技术趋势：一、新场景安全防护增量同步跟进和基础安全治理能力的补课需要两手并举。（原文链接：https://mp.weixin.qq.com/s/pIZvIOd1gva0badYGtOAWw）

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	哈工大安天联合 CERT 实验室发布针对挖矿木马的简要技术分析
英文标题	无
作者	哈工大安天联合 CERT 实验室
内容概述	互联网的虚拟货币，如比特币（BTC）、门罗币（XMR）等，是一种由开源的 P2P 软件产生的网络电子虚拟货币。主要用于互联网金融投资，也可以作为新式货币直接在生活中使用。比特币挖矿机是获取比特币的方式之一，挖矿机工作要让显卡长时间满载，功耗会相当高，电费开支也会越来越高。由于挖矿成本过于高昂，一些不法分子通过各种手段将矿机程序植入受害者的计算机中，利用受害者计算机的运算力进行挖矿，从而获取非法收益。这类非法侵入用户计算机的矿机程序被称作挖矿木马。
链接地址	https://mp.weixin.qq.com/s/0HO9c7Q8BbBNeTAX13eyGQ

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	Microsoft Word 远程代码执行漏洞（CVE-2021-40486）	高	Microsoft Word 存在远程代码执行漏洞。由于在 Microsoft Word 中处理 DOC 文件时出现 use-after-free 错误。使得远程攻击者可以欺骗受害者打开特制文档，触发释放后使用错误并在系统上执行任意代码。
	Microsoft Excel 远程代码执行漏洞（CVE-2021-40485）	高	Microsoft Excel 存在远程代码执行漏洞。由于 Microsoft Excel 中的输入验证不正确，使得远程攻击者可以欺骗受害者打开特制文件并在目标系统上执行任意代码。
	Microsoft Win32k 权限提升漏洞（Microsoft Win32k）	高	Microsoft Win32k 存在权限提升漏洞。应用程序在 Win32k 中没有正确施加安全限制，导致攻击者可以在本地绕过安全限制，将当前普通用户权限提升为系统用户权限。
较为活跃样本家族	Worm/Win32.AutoRun	中	此威胁是一种蠕虫类程序。该家族能够在磁盘根目录或插入的可移动存储介质的根目录下创建一个 autorun.inf 文件并自我复制，该文件中包含可执行蠕虫的名字和路径。用户将磁盘或可移动存储介质接入电脑后，系统会自动执行 autorun.inf 中指定的可执行程序。该家族除了能够感染本地电脑外，还可以通过共享文件传播至远程电脑中。
	Trojan[Dropper]/Win32.Dinwod	中	此威胁是一种具有释放或捆绑行为的木马类家族。该家族木马在感染用户系统之后，会自动释放并安装其它恶意程序。该家族的部分变种还具有强制关闭杀毒软件的能力。
	Trojan/Win32.Mansabo	中	此威胁是一种可以窃取密码信息的木马类家族。该家族的样本运行后会窃取用户账户信息，记录键盘击键信息，造成用户隐私泄露。
	Trojan[Backdoor]/Win32.Padodor	中	此威胁是一种后门类木马家族。该家族样本会利用系统漏洞打开后门，为用户电脑带来更多威胁；它同时允许黑客远程进入并控制用户电脑。
	Trojan[Proxy]/Win32.Qukart	中	此威胁是一种可以窃取用户信息并通过代理服务器回传信息的木马类家族。该家族样本收集系统的敏感信息，通过 http 请求发送到指定网页。该家族在后台会自动更新。
	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[SMS]/Android.FakeInst	低	此威胁是一种伪装类木马家族。该家族样本通常伪装为主流应用程序（Opera、Skype 等），运行后向相关付费号码发送短信，造成用户资费消耗。

云中安全盲点的影响

杰西·斯托考尔 / 文 安天技术公益翻译组 / 译

对许多企业来说，2020 年的主要任务是保持业务连续性，而 2021 年的主要任务是将“新常态”付诸实施。新冠疫情爆发之后，企业不得不转向远程办公；事实证明，“随处办公”模式是可行的。为了提高生产力和效率，企业采用 SaaS 模型并将关键任务业务迁移到云中（或多个云中），以实现技术堆栈的多样化。在我公司最近进行的一项研究中，92% 的 IT 领导者表示，他们的企业正在或已经转向混合办公模式，只是还需要部署人力维护有价值的本地解决方案。

现在，随着企业转向远程办公模式，员工可以在公司的网络之外直接访问云服务和下载应用程序。因此，企业的 IT 部门面临着不断扩展的技术挑战，更不用说真正的影子 IT 挑战了。实际上，近 50% 的 IT 领导者表示，他们目前面临的最大挑战是控制 SaaS 蔓延，其次是识别非托管应用程序（26%）。

此外，随着企业对云的日益依赖，新的安全风险随之而来。2021 年初的 SolarWinds 供应链攻击事件引发了严重的后果，令人担忧。该事件给企业带来了两个重要的教训：（1）如果企业不能保护其技术供应链，就会面临被攻击者入侵网络的风险；（2）不必要的复杂性会增加风险。

复杂性难题

企业 IT 团队面临的挑战是：如何实施不断变化的技术并管理随之而来的风险（尤其是在云环境中）。

举例来说，企业是否知道他们目前使用了多少个云环境？哪些工作负载正在运行，谁在使用这些负载？企业拥有的许可证数量是否超出所需？如果企业不了解拥有哪些资产以及如何使用这些资产，就无法充分利用这些资产，造成超支，并且可能会产生重大的安全风险和潜在的合规性问题。我们以应用开发为例，当今的大部分应用程序开发已从“从头开始构建”模型转变为“通过组合开源组件和云服务进行构建”模型。这样可以实现快速、轻松的开发；但是，如果这些开源项目收到更新 / 修复但未同步到企业的产品中，企业的产品就会产生安全盲点。这就导致了供应链风险的增加，就像 SolarWinds 攻击事件一样。

如果从更大的范围考虑，复杂性带来的安全和合规成本会更加高昂。如果企业是依赖某些本地解决方案的混合云或多重云客户，那么其传统安全堆栈可能无法有效地提供支持。另外，企业的安全团队可能不具备深入了解云容器、本地老旧系统、移动设备和端点的技能。这样一来，企业就会拥有过多的单点解决方案，而且它们之间无法互通，这只会增加企业的技术复杂性。

企业需要实现自动化

共享责任模型使当今云中的安全性进一步复杂化。如果企业依赖 Amazon AWS、Microsoft Azure 或 Google Cloud 等第三方云服务，他们只能获得基本的安全性。企业往往认为“亚马逊正在保护我们的数据”；而实际上，他们只是拥有一个相互关联的应用程序和权限网，其中每个应用程序和权限都会彼此影响。

一旦出现问题，企业是无法依赖亚马逊进行修复的。那么，谁能帮助企业解决问题呢？企业的内部员工？云提供商？弄清楚问题出在哪里更像是一场永远在寻找线索的游戏，这是一个恶性循环，不会带来真正的进展。

应对这种复杂性的最佳方法是：了解第三方云提供商（或多个提供商）的责任，并与企业 IT 和安全团队共享这些信息。基于这些信息，企业可以制定事件响应计划。

提高安全性、降低合规性风险的第二步是实现自动化。我们继续以应用程序开发为例，企业 IT 团队可能拥有数百个源代码库，用这些库中的数十到数百个组件拼凑成产品。显然，手动流程是无法掌控这一切的，而自动化则可以大大加快开发速度并提高准确性。

保持对云服务、应用程序、本地遗留系统等内容的可见性是很复杂的。但是，可见性对于管理企业的安全和合规风险至关重要，对于尽职调查也是必要的。

照亮安全盲点

异构 IT 环境有其优势，如更多的选择、预算最大化以及构建弹性技术骨干等。但是，一旦某个环节出现问题，一切就都会变得岌岌可危。要想找出解决问题的方法并不容易。通过获得对网络、云服务、产品开发和用户的可见性，企业可以在安全和合规风险以及预算方面取得显著收益。如果没有获得可见性，企业就只能在黑暗中摸索了。

原文名称	The Lingering Effect of Blind Spots in the Cloud
作者简介	杰西 · 斯托考尔 （Jesse Stockall），是 Snow Software 的首席架构师。
原文信息	2021 年 10 月 12 日发布于 Network Computing 原文地址 https://www.networkcomputing.com/cloud-infrastructure/lingering-effect-blind-spots-cloud
摘 要	异构 IT 环境有其优势，如更多的选择、预算最大化以及构建弹性骨干网络。但是，一旦某个环节出现问题，一切就都会变得岌岌可危。要想找出解决问题的方法并不容易。通过获得对网络、云服务、产品开发和用户的可见性，企业可以在安全和合规风险以及预算方面取得显著收益。如果没有获得可见性，企业就只能在黑暗中摸索了。
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。