安天智甲有效防护 Neurevt 窃密木马

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 Neurevt 窃密木马。Neurevt 木马又名 BetaBot，从 2013 年 3 月开始在地下市场进行售卖，价格大约在 120 美元到 500 美元不等。此版本的 Neurevt 窃密木马在 2021 年 6 月开始活跃，主要目标是窃取墨西哥金融机构用户的个人信息和其银行网站凭据等。

当样本执行后，会创建多个恶意文件，如以 .vbs、.bat 和 .exe 为后缀的恶意文件等。样本首先调用 wscript.exe 进程执行名为“435246.vbs”文件，435246.vbs 文件的功能为使用 cmd.exe 进程执行名为“183.bat”文件。183.bat 文件主要有两个功能：一、将创建好的文件“x0329847998”重命名为受密码保护的 rar 文件“43939237.rar”，执行 unpakedree.exe 并使用密码“67dah9fasdd8kja8ds9h9sad”解压 rar 文件；二、使用 wscript.exe 进程执行解压后提取出的文件“3980392cv.vbs”。3980392cv.vbs 文件的功能是使用 cmd.exe 进程执行名为“48551.bat”文件。48551.bat 文件主要有两个功能：一、释放第二阶段有效载荷“xc829374091FD.exe”；二、将之前释放的所有文件进行删除。xc829374091FD.exe 进程首先会创建自身一个子进程，子进程创建 explorer.exe 进程并将自身重命名后注入到创建的 explorer.exe 进程中。第二阶段载荷的主要功能包括键盘记录、剪贴板记录、截取屏幕截图以及窃取计算机初始信息等。该窃密木马使用 HTTP POST 的方式将搜集的数据上传到 C2 服务器。

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、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(Win7sp1 x86)鉴定器、字符串分析鉴定器、文件相似分析鉴定器、智能学习鉴定器、静态特征检测鉴定器、安全云鉴定器、动态（WinXP）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、反病毒引擎鉴定器将文件判定为木马程序。

◆ 概要信息

文件名	86aab09b278fe8e538d8cecd28f2d7a32fe413724d5ee52e2815a3267a988595
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	3.55 MB
MD5	808E34A763ACD79D01EEB1F54B18A551
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[Dropper]/Win32.Agent
判定依据	反病毒引擎

报告地址：https://1.119.163.6/vue/details?hash=808E34A763ACD79D01EEB1F54B18A551

◆运行环境

操作系统	内置软件
WinXP 5.1.2600 Service Pack 3 Build 2600	默认、IE6、Firefox、Google Chrome、Office2003、Flash、WPS、FoxitReader、AdobeReader

◆危险行为

行为描述	危险等级
在系统目录创建文件	★★★
映射内存方式注入	★★★
查询软件限制策略	★★★
启动一个隐藏窗口的进程	★★★★
创建可疑进程	★★★★
修改文件权限	★★★
向其他进程内存写入数据	★★★
通过标记进程可执行堆绕过 DEP	★★★★★
搜索文件	★★★★
疑似查找游戏进程	★★★★

◆常见行为

行为描述	危险等级
查询系统时间	★★
镜像劫持	★★
.....	.....

◆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09月06日(总第294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

肖新光委员：开创关键信息基础设施网络安全保护新局面

8 月 17 日，根据中华人民共和国第 745 号国务院令，《关键信息基础设施安全保护条例》（以下简称《条例》）已获得通过，并自 2021 年 9 月 1 日起施行，这也预示了我国关键信息基础设施网络安全保护将进入新的阶段。

▲ 全国政协委员、安天科技集团董事长肖新光

关键信息基础设施是指公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等重要行业和领域的重要网络设施与信息系统等。随着我国网络强国战略的不断推进，以能源互联网、工业互联网、城市大脑等为代表的关键信息基础设施，已成为数字化时代国家经济发展的新底座。由于其蕴含的巨大价值，带有各种背景的高级网空威胁行为体已将我国关键信息基础设施作为首选攻击目标，并长期持续隐蔽地对关键信息基础设施进行网络入侵、渗透等，形成深度威胁。

必须认识到，以关键信息基础设施为底座的数字经济具有对信息化技术的全链依赖，具有牵一发而动全身的连锁风险效应。而针对关键信息基础设施的网络安全威胁特别是高级威胁，又往往具有一定的隐蔽属性。在平时，更多风险是被攻击者入侵渗透、埋设恶意代码、实现持久化信息获取和远程控制能力，而一旦进入到高烈度对抗的风险条件下，则迅速将隐蔽控制转化为物理空间影响。这种持续对抗特性，使得关键信息基础设备网络安全平时深藏于水面之下，难以形成对攻击存在性和危害性的显性认知，进而导致网络安全不被重视的状态，但一旦产生危害，则发于瞬间而波及全局，无法作出及时有效的应对，进而连锁引发重大的灾难性影响。

关键信息基础设施是国家战略性基础设施，是国家经济发展、社会繁荣和国家安全的重要基础，筑牢关键信息基础设施的网络安全防线至关重要。在这样的背景下，《条例》应运而生非常及时和必要。《条例》不仅确定了关键信息基础设施的定义，明确了保护范围，明确了相关责任和监管机制，也提出了安全保障措施等。可以说，《条例》是我国推进网络安全法治工作的重要成果，将为我国加强关键信息基础设施的网络安全保护工作提供有力抓手和法治保障，是新形势下国家面向重大战略风险挑战的强基固本之举。

可以看到，《条例》将关键信息基础设施界定为“一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的重要网络设施、信息系统等”。此前讨论版本中，对关键信息基础设施的定义是清单化的，而发布版则从风险后果的视角，清晰界定了关键信息基础设施的范畴，这体现了关键信息基础设施安全的重大价值与战略地位。

这一修订，确保了关键信息基础设施安全随风险动态变化的战略弹性与调整空间，打破了惯性沿袭，及时按照新的发展目标和新的风险挑战，因时而变、因需而变。与此同时，由风险的重大性和后果的严重性出发，明确提出与防范重大风险与严重后果强关联的防护水平要求，进而规定了为构建所要求的防护水平，具体对应的各种安全投入。

由于关键信息基础设施的战略性和全局性，全方位实施保护，还需要统筹资源和力量。《条例》的颁布，使得关键信息基础设施安全问题不再只是单纯的建设运营机构自身安全防护问题，其建构在关键信息基础设施安全与国家安全、社会安全、政企机构安全以及个人安全等 4 个层面相关的维度形成了需求导向和指引。

《条例》不仅规范了关键信息基础设施安全防护工作中涉及的国家主管部门、保护工作部门、运营者、网络安全服务机构等相关方的责任义务规定、保障促进要求以及法律责任约束等，同时全面覆盖了相关工作主体和工作环节。（原文链接：https://mp.weixin.qq.com/s/6NrTp98Z7zlifDjEpMV7hQ）

扫描右侧二维码阅读全文

安天三款产品入围中央集采安全软件

2021 年 8 月 30 日，中央国家机关 2021 年安全软件协议供货采购项目成交公告发布，共 47 家响应人参与响应。安天入围第一包安全管理中心（SOC）软件、第三包漏洞扫描软件和第四包日志审计软件。

中央国家机关 2021 年安全软件协议供货采购项目征集公告于 8 月 6 日发布，征集分为五包，具体品目为：第一包安全管理中心（SOC）软件、第二包基线扫描软件、第三包漏洞扫描软件、第四包日志审计软件、第五包终端安全软件。评委会根据征集文件中确定的要求，从响应文件的有效性、响应人资质、实质性响应等方面对供应商的响应文件进行了符合性审查。安天的鉴形安全管理中心平台、安天漏洞扫描系统和安天日志审计系统成功入围。

此次入围中央集采安全软件，是对安天产品和服务能力的再次认可和肯定。作为中国网络安全“民企国家队”，安天将继续致力于全面提升客户的网络安全防御能力，有效应对安全威胁。（原文链接：https://mp.weixin.qq.com/s/UL_Kb38qPgTlKo2wlvrP7w）

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	Mirai 恶意软件变种正在积极利用 WebSVN 命令注入漏洞
英文标题	New Mirai Variant Targets WebSVN Command Injection Vulnerability (CVE-2021-32305)
作者	Brock Mammen and Haozhe Zhang
内容概述	研究人员观察到最近公开的一个影响 WebSVN(一个用于浏览源代码的开源 web 应用程序) 的命令注入漏洞 (CVE-2021-32305)。在 2021 年 5 月发现并修复了关键的命令注入漏洞。概念验证发布后一周内，即 2021 年 6 月 26 日，攻击者利用该漏洞部署了 Mirai DDoS 恶意软件的变种。对该恶意软件的分析表明，它用于执行分布式拒绝服务攻击，并且与 Mirai 僵尸网络家族共享其部分代码。研究人员强烈建议 WebSVN 用户升级到最新的软件版本。
链接地址	https://unit42.paloaltonetworks.com/cve-2021-32305-websvn/

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 Edge 远程代码执行漏洞 (CVE-2021-30603)	高	Microsoft Edge 存在远程代码执行漏洞。由于 WebRTC 中的释放后使用错误，使得远程攻击者可以诱使受害者访问特制网页，触发释放后使用错误并在系统上执行任意代码。
	VMware vRealizeOperations 访问控制错误漏洞 (CVE-2021-22025)	高	VMware vRealizeOperations 存在访问控制错误漏洞。由于访问限制不当造成的，远程攻击者可以向现有 vROps 集群添加新节点。
	Debian libssh 远程代码执行漏洞 (CVE-2021-3634)	高	Debian libssh 存在远程代码执行漏洞。由于处理共享机密时的边界错误，使得远程攻击者可以提供不同大小的共享秘密，在第二次密钥重新交换期间触发内存损坏并使应用程序崩溃或可能执行任意代码。
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/Win32.Scar	中	此威胁是一种窃密木马类程序，可以将某些金融网站重定向到攻击者设置的另一个地址，模仿登录界面从而窃取用户密码。
	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，释放的程序大多为窃密类木马程序。
	Trojan/Win32.Injuke	中	此威胁是一种可以窃取密码信息的木马类程序。该家族的样本运行后会窃取用户账户信息，记录键盘击键等。
	Trojan/Win32.Vilsel	中	此威胁是一种窃密类木马家族。该家族木马通过垃圾邮件或恶意网站进行传播。该家族木马感染用户电脑后，会为黑客建立远程连接以控制用户电脑，窃取用户敏感信息（账号和密码等），同时会下载并运行其它恶意程序。
	Trojan[Backdoor]/Linux.Mirai	中	此威胁是一种 Linux 平台上的僵尸网络家族。该家族样本主要是利用漏洞传播并组建僵尸网络，并利用僵尸网络传播相关恶意软件。
	Trojan[Clicker]/Android.Simpo	中	此威胁是安卓平台上的伪装类木马家族。该家族木马通常伪装成其他正常应用，运行后隐藏图标，并访问某些网站，旨在提高网络访问流量，消耗用户流量资费。

如何解决漏洞管理的三个核心问题

丹·安科尼纳 / 文 安天技术公益翻译组 / 译

新冠疫情给企业信息安全专家带来了巨大的压力。随着网络安全预算的收紧，以及数以百万计的员工全职或兼职转向远程办公，企业的威胁形势越来越复杂，面临着更加可怕的挑战。

企业在漏洞管理方面存在哪些问题?

首先，很多企业对“漏洞管理”的理解已经过时。漏洞管理不仅仅是指扫描企业网络来搜寻威胁。

整体的漏洞管理方法包括识别、报告、评估和确定漏洞的优先级。需要注意的是，漏洞管理还涉及风险情境信息。漏洞管理不仅要扫描安全漏洞，还要展示这些漏洞会如何被利用以及可能产生的后果。

准确地说，漏洞管理应采用全局性的方法，促使各方面和谐运作，以降低关键业务资产面临的风险。

但是，即使企业遵循了正确的原则，在实施漏洞管理时仍然可能会失败。在下文中，我们将介绍企业在管理漏洞中面临的三个核心问题。

1. 无法正确确定威胁的优先级

无法正确确定漏洞的优先级，是企业目前在漏洞管理中面临的核心问题之一。很多企业通过威胁扫描来识别安全漏洞，然后直接进入漏洞修复阶段。从某种程度上来说，这种紧迫性是可以理解的。但是，归根结底，这种方法目光短浅，会带来更大的风险。

聪明的企业会将大量精力放在漏洞优先级确定和报告阶段。如果安全团队无法有效地确定漏洞的优先级，就有可能会将精力放在对关键业务资产没有真正风险的威胁上，从而导致时间和资源的浪费。

更糟糕的是，这会使企业无法及时应对那些严重的威胁。安全团队可以采取更好的方法，即对发现的漏洞进行优先级排序，专注于那些严重的漏洞。如果操作正确，这种优先级排序可以筛除 99% 的漏洞，使安全团队集中精力应付 1% 的严重漏洞。

安全团队应如何优化这种优先级排序呢？他们可以使用尖端的攻击补丁管理解决方案，利用关键攻击风险情境信息对漏洞进行优先级排序。该工具不仅应显示 CVSS 评分，还应显示企业的风险全貌，包括每个漏洞被利用的可能性，以及每个漏洞对高价值资产构成的风险等。

2. 未使用持续的方法

有效的漏洞管理计划应该是持续的，而非偶发的。如果企业不采取持续的方法，将难以控制漏洞的流动并积累大量漏洞——这是一个非常严重的问题。

对于安全团队来说，只是掌握新出现的漏洞就已经很困难了；如果再加上持续处理不断积压的安全问题，可能会使他们崩溃。安全团队应使用以连续、自动化的漏洞识别方法，而非进行不定期的扫描和修复。这是持续改进企业安全态势的关键之一。

3. 沟通不畅，组织架构不清晰

如果企业没有明确的沟通渠道和正确的组织架构，肯定会出现问题。安全团队的成员经常没有明确的角色，他们不了解自己在整体漏洞管理框架中处于什么位置，尤其是在职责方面。

如果团队成员有明确的角色定义和明确的职责，他们就可以有效地工作并相互协作。每个人都可以了解其工作是如何与他人的角色和责任相关联的，从而努力履行自己的职责并实现特定目标，而非相互孤立地工作。

这种沟通需求也应延伸到管理层。考虑到强大的网络安全已成为企业的关键战略目标，企业领导层也应了解并投入到网络安全计划中，这一点很重要。

漏洞管理问题要点

无法有效管理网络漏洞会造成非常严重的后果。仅仅一次数据泄露就可能会导致严重的声誉和经济损失。此外，数据泄露事件的数量每年都在不断增加。实际上，漏洞管理已不仅仅是一种 IT 支出，而是一个关键的业务目标。

为了实现该目标，企业必须明白漏洞管理是一个持续的、多阶段的过程。此外，企业应解决困扰其 IT 部门的问题，包括：无法正确进行漏洞优先级排序、漏洞管理方法不可持续、安全团队和领导者之间缺乏组织和沟通。

在解决上述问题方面，正确的方法可以带来巨大的收益。如上文所述，最好的办法是结合强大的漏洞管理工具，这些工具能够提供适当的优先级排序指导和关键风险情境信息。

只要企业具备健全的战略并配备正确的工具，就能在保护高价值资产方面远远领先于大多数竞争对手。

原文名称	Vulnerability management is facing three core problems: Here’s how to solve them
作者简介	丹·安科尼纳（Dan Anconina），是 XM Cyber 公司的首席信息安全官和运营技术负责人。
原文信息	2021 年 8 月 26 日发布于 Help Net Security 原文地址 https://www.helpnetsecurity.com/2021/08/26/vulnerability-management-problems/
摘 要	漏洞管理已不仅仅是一种 IT 支出，而是一个关键的业务目标。为了实现该目标，企业必须明白漏洞管理是一个持续的、多阶段的过程。此外，企业应解决困扰其 IT 部门的问题，包括：无法正确进行漏洞优先级排序、漏洞管理方法不可持续、安全团队和领导者之间缺乏组织和沟通。
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。