安天智甲有效防护 LockBit 2.0 勒索软件

近日，安天CERT在梳理网络安全事件时发现了LockBit 2.0勒索软件持续活跃。LockBit勒索软件最早被发现于2019年9月，主要通过获取的远程桌面登录凭证进行传播。经验证，安天智甲终端防御系统（简称IEP）的勒索软件防护模块可有效阻止LockBit 2.0勒索软件的加密行为。

通常攻击者使用有效的远程桌面协议（RDP）账户访问受害者系统，进入系统后首先使用网络扫描器找到域控制器，在得到域控制器权限并横向移动释放并运行LockBit 2.0勒索软件。攻击者在域控制器上创建组策略并将组策略更新到网络上的其他设备。组策略的目的是禁用Microsoft Defender的实时保护、警报、向Microsoft提交样本以及检测恶意文件时的默认操作，还可以配置计划任务绕过UAC启动勒索软件。攻击者通过对域控制器的ADS执行LDAP查询获得计算机列表，利用组策略释放LockBit 2.0勒索软件样本，LockBit 2.0运行后追加以“.lockbit”命名的后缀，在每个加密目录中创建名为“Restore-My-Files.txt”的勒索信。勒索信中包含勒索的信息、联系方式和泄密文件的威胁信息等。勒索软件除了以上功能，还可以更改系统的桌面背景、唤醒离线设备、通过联网打印机反复打印勒索信引起受害者的注意等功能。

▲LockBit 2.0勒索软件勒索信息

LockBit 2.0勒索软件采用“AES+RSA”加密算法组合的形式加密文件，目前被加密的文件暂无法解密。

安天提醒广大用户，及时备份重要文件，且文件备份应与主机隔离；及时安装更新补丁，避免勒索软件利用漏洞感染计算机；对非可信来源的邮件保持警惕，避免打开附件或点击邮件中的链接；尽量避免打开社交媒体分享的来源不明的链接，给信任网站添加书签并通过书签访问；避免使用弱口令或统一的密码；确保所有的计算机在使用远程桌面服务时采取VPN连接等安全方式，如果业务上无需使用远程桌面服务，建议将其关闭；可以使用反病毒软件（如安天智甲）扫描邮件附件，确认安全后再运行。目前，安天追影产品已经实现了对该类勒索软件的鉴定；安天智甲已经实现了对该勒索软件的查杀。

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、信标检测鉴定器、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	LockBIT_7D68A5BFD028A31F.exe
文件类型	BinExecute/Microsoft.PE[:X86]
大小	863 KB
MD5	66B9CCB41B135F302B3143A5D53F4842
病毒类型	木马程序
恶意判定 / 病毒名称	RiskWare[RiskTool]/Win32.Shell2exe
判定依据	反病毒引擎

报告地址：https://1.119.163.6/vue/details?hash=66B9CCB41B135F302B3143A5D53F4842

◆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
自启动	★★★
查询系统硬盘大小	★★★
搜索文件	★★★★
创建互斥量	★★★
映射内存方式注入	★★★
在系统目录创建文件	★★★
获取操作系统配置信息	★★★
通过文件检测布谷鸟沙箱	★★★★★

◆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20日(总第296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

安天执行董事长、CEO游小明一行赴卫士通总部交流

9月15日，安天执行董事长、CEO游小明率领安天产品线、研发线和营销线相关部门负责人到访卫士通总部调研交流。卫士通总经理仲恺、副总经理魏洪宽及公司经营团队有关领导、相关部门负责人参加了此次交流。

游小明一行首先参观了卫士通企业展厅，详细了解了卫士通最新的发展思路与核心能力布局，随后双方在会议室组织开展座谈交流。

▲卫士通与安天开展座谈交流

会上，双方围绕推进战略交流与合作走向纵深，打造覆盖方案、产品、市场等各方面的常态化合作机制，推动多层次、多维度合作落地和标杆示范项目建设等问题进行了深入交流，并就数据安全、云安全、物联网安全等重要领域和场景下双方的合作进行了充分的探讨和展望。

▲卫士通总经理仲恺

仲恺表示，卫士通后续将通过合理高效的信息共享、业务共融机制，拉紧双方各个层面交流合作的纽带，进一步推进双方战略合作的落实落地，携手安天共同为客户提供高安全价值的方案、产品和服务。

▲安天执行董事长、CEO游小明

游小明表示，卫士通与安天具有相似的价值理念，面临着共同的机遇和挑战，也肩负着助力国家网络安全行业发展壮大的共同使命，希望双方在既有合作基础上，加强战略层面共识，以“能力融合、产品结合、市场联合”的思路，筑牢深度战略合作的基础，巩固提升战略合作机制，充分发挥各自独到的核心能力，面向“十四五”及更远的将来，体系化、服务化地帮助客户达成安全价值。

安天是引领威胁检测与防御能力发展的网络安全国家队，长期致力为战略客户和关键信息基础设施提供整体安全解决方案。面对数字化转型升级的安全防御需求和日益复杂的安全挑战，安天依托端到端的安全能力，积极发挥供应链关口前移的优势，将安全能力基因向包括办公网、云环境、物联网、工业互联网等在内的全场景有效防御覆盖，并依托强大的威胁对抗体系，实现深度客户赋能，驱动客户完成从威胁情报消费，到自主安全能力生产的智能化安全运营变革。未来，安天将加强与卫士通的合作，共同赋能国家网络安全行业。

（原文链接：https://mp.weixin.qq.com/s/K3b-CVMkzTabQpIhUHU_hw）

扫描右侧二维码阅读全文

ZLoader变种通过虚假TeamViewer下载广告分发

ZLoader（也称为Terdot）于2016年首次被发现，是臭名昭著的Zeus银行木马的一个分支。SentinelLabs观察到的新感染链通过禁用Windows Defender并依靠本地二进制文件和脚本（LOLBAS）来逃避检测，从而展示了更高级别的隐蔽性。该恶意软件从谷歌Adwords发布的谷歌广告下载，攻击者使用网络钓鱼针对受害者。一旦用户点击广告，它将通过aclk页面重定向。在进一步导航（和重定向）之后，恶意Team-Viewer.msi将从最终URL：hxxps://team-viewer.site/download/Team-Viewer.msi下载。下载的文件是伪造的TeamViewer安装程序。（原文链接：https://www.sentinelone.com/labs/hide-and-seek-new-zloader-infection-chain-comes-with-improved-stealth-and-evasion-mechanisms/）

黑客劫持俄罗斯政府网站宣传庞氏比特币骗局

据俄罗斯当地新闻媒体《消息报》（Izvestia）报道，一些尚未确认身份的黑客入侵了俄罗斯官方网站。他们开始推广庞氏比特币免费赠品促销活动。黑客们通过宣传活动表示，用户只要在自己的系统中安装特定的应用程序，就会得到0.025BTC。他们还在推广中写道，将随机奖励5个用户价值1000美元的比特币。黑客在24小时内第二次入侵了俄罗斯梁赞政府网站。比特币赠品公告于9月2日星期四在网站上再次发布。目前，所有消息都已被删除。（原文链接：https://bitcoinik.com/hackers-hijack-russian-government-website-prompts-ponzi-bitcoin-scheme/）

客户服务公司TTEC遭勒索软件攻击系统中断

9月14日，一位TTEC员工展示了TTEC发送给他们的内部消息，内容涉及9月12日星期日开始的大范围系统中断的状况。9月15日美国东部时间下午6:20，TTEC证实了遭到了勒索软件攻击。TTEC发送给员工的信息表明，该公司的网络可能受到了勒索软件组织“Ragnar Locker”（或者冒充Ragnar的勒索软件团伙）的攻击。这条消息敦促员工避免点击Windows开始菜单中突然出现的名为“!RA!G!N!A!R!”的文件。（原文链接：https://krebsonsecurity.com/2021/09/customer-care-giant-ttec-hit-by-ransomware/）

每周安全事件

类 型	内 容
中文标题	研究人员发现 ChaChi 恶意软件的 Linux 新变种
英文标题	PYSA Ransomware Gang adds Linux Support
作者	Lacework Labs
内容概述	2021 年 8 月，Lacework Labs 发现了 ChaChi 的一个 Linux 变种（MD5：14abd57e8eb06191f12c0d84f9c1470b）。该恶意软件被配置为使用与称为 PYSA（又名 Menipoza Ransomware Gang）的勒索软件参与者相关联的域。ChaChi 是一种基于 Golang 的开源 RAT 的定制变种，它利用 DNS 隧道进行 C2 通信。Linux 变种与 Windows 版本具有相同的特点，最显著的是核心功能、大文件大小（8MB +）和 Golang 混淆器 Gobfuscate 的使用。Linux 版本的一个显著特征是存在包含日期时间数据的调试输出。目前尚不清楚 Linux 变体是否用于操作，但在相关基础设施离线之前就已观察到。然而，观察到的调试输出可能表明样本仍处于测试阶段。
链接地址	https://www.lacework.com/blog/pysa-ransomware-gang-adds-linux-support/

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 Indexed DB API 远程代码执行漏洞（CVE-2021-30633）	高	Google Chrome Indexed DB API 存在远程代码执行漏洞。由于 Google Chrome 中的 Indexed DB API 组件中的释放后使用错误。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。
	Linux kernel 安全漏洞（CVE-2021-3715）	高	Linux kernel 存在安全漏洞，该漏洞源于流量控制网络子系统中的“路由决策”分类器，在处理分类过滤器更改的方式时存在 Use-after-free 错误，使得无特权的本地用户利用该漏洞提升他们在系统上的权限。
	Mozilla Firefox 缓冲区错误漏洞（CVE-2021-38494）	高	Mozilla Firefox 中存在缓冲区错误漏洞，该漏洞源于产品处理 HTML 内容时出现边界错误。远程攻击者可利用该漏洞可以创建一个专门制作的网页，诱骗受害者打开它，引发内存损坏，并在目标系统上执行任意代码。
较为活跃样本家族	Trojan[Backdoor]/Win32.Remcos	中	此威胁是一种远程控制类木马家族，该家族木马通常采用垃圾邮件进行传播，具备远程控制、键盘记录和数据回传等功能。
	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。
	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[Downloader]/NSIS.Adload	中	此威胁是一种下载类木马家族。该家族木马通常使用 NSIS（开源的 windows 系统下的程序制作工具）将木马与正常程序捆绑在一起，主要功能是通过网络下载其他恶意软件。
	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[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。

多重云作为灾难恢复解决方案

戴夫·伯明翰 / 文 安天技术公益翻译组 / 译

在配置灾难恢复（DR）解决方案时，许多拥有本地 IT 基础架构的企业已经转向云。如果地震或洪水等灾难性事件导致本地基础架构无法使用，这些企业可以启用基于云的基础架构并继续运营。但是，如果企业的主要基础架构已经在云中，应该怎么办呢？他们可以在 AWS、Google 或 Azure 的远程区域中配置具有备份基础架构的 DR 解决方案。但是，如果企业想要确保，即使整个 AWS、Google 或 Azure 云都崩溃，也能保持运营，又该怎么做呢？他们可以考虑采用多重云 DR 解决方案。

构建多重云基础架构

在本文中，“多重云”是指两个云基础架构——比如 Azure 和 AWS EC2，或者 AWS 和 Google Cloud Platform（GCP）。举例来说，如果企业的主要基础架构在 AWS 上运行，则其 DR 基础架构应在 Azure 或 GCP 上进行配置。这样一来，即使整个 AWS 云出现故障，企业在 Azure 或 GCP 上的灾难恢复基础架构也能确保企业继续运营，将运营中断风险降至最低。

但是实际上，企业不太可能在两个云中复制所有资源。他们更可能采取的方法是，配置这些系统的多重云实例——例如，企业的生产 SQL 服务器系统或 SAP ERP 环境。如果这些系统出现故障，会对企业的创收造成最不利的影响，停机成本是最高的。

在第二个云中配置基础架构时，企业应尽可能地镜像主云中的基础架构，使其具有类似的计算资源、存储和网络服务。企业应安装和配置要镜像的应用程序基础架构的所有方面，包括应用程序软件、数据库、实用程序、支持服务等，以便第二个云基础架构的运行与第一个相同。在第二个云中，企业可以在不同于第一个云的区域中配置云基础架构。他们应意识到，一个区域发生灾难就有可能同时影响多个云中的数据中心。

确保多重云灾难恢复

在每一个云环境中，企业都需要部署 DR 服务，以保持两个云基础架构的同步，并在灾难破坏或威胁主要云环境时促进云环境之间的故障转移。

基础架构同步的关键在于，将生产数据从主云复制到辅助云。企业希望确保关键系统的运营弹性恢复能力，他们不应依赖于云之间的数据库复制策略（或者某种日志传送方案），这类策略只能回滚到某个较早日期的数据库，会显著增加恢复关键系统所需的时间。

更好的 DR 方法依赖于高效的复制系统，例如块级复制。与较慢的文件级复制不同，这种方法可以确保，生产环境中的每一次数据更改都被复制到第二个云环境中。企业应确保，其复制解决方案支持故障转移群集环境。在高可用性（HA）配置中，执行块级复制的工具将在独立但附近的云数据中心之间同步复制数据；但在 DR 配置中，复制可能会异步发生以适应因云之间（或者地理区域之间）移动数据而导致的延迟。第二个云基础架构中的数据可能与主云中的数据有几秒钟的不一致，但如果第二个云被调用，企业能够比恢复备份更快地使服务上线。

最后，在整个云发生灾难的情况下，需要协调云基础架构之间的故障转移。有多种工具可以简化故障转移并实现自动化（包括一些可以自动更新 DNS 服务器，以将入站流量重新路由到第二个云的工具）。如果企业将多个关键应用程序迁移到多重云配置中，那些与应用程序无关的工具将为其提供更大的灵活性，这优于内置于特定应用程序中的工具。此外，企业应关注手动故障转移管理功能。在某个时候，主要云基础架构将再次运行，企业的 DR 工具应轻松地将数据库的最近更新复制回主要云基础架构，然后将运营流量移回该基础架构，而不会造成任何业务中断。

原文名称	Multi-Cloud as the New Hybrid
作者简介	戴夫 · 伯明翰（Dave Bermingham），是 SIOS Technology 公司的高级技术推广师。
原文信息	2021 年 9 月 13 日发布于 Network Computing 原文地址 https://www.networkcomputing.com/cloud-infrastructure/multi-cloud-new-hybrid
摘 要	在配置灾难恢复（DR）解决方案时，许多拥有本地 IT 基础架构的企业已经转向云。如果地震或洪水等灾难性事件导致本地基础架构无法使用，这些企业可以启用基于云的基础架构并继续运营。但是，如果企业的主要基础架构已经在云中，应该怎么办呢？他们可以在 AWS、Google 或 Azure 的远程区域中配置具有备份基础架构的 DR 解决方案。但是，如果企业想要确保，即使整个 AWS、Google 或 Azure 云都崩溃，也能保持运营，又该怎么做呢？他们可以考虑采用多重云 DR 解决方案。
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。