安天发布《M00nD3V Logger 窃密木马分析报告》

近日，安天 CERT 在梳理网络安全事件时发现一个名为 M00nD3V Logger 的多功能窃密木马。由于该木马具有多种窃密功能，逐渐在黑客论坛活跃起来。M00nD3V Logger 主要通过垃圾邮件和受感染的网站进行传播，通过带有 zip 附件的垃圾邮件和受感染的网站将有效载荷投放到受害者的机器上。M00nD3V Logger 除了窃取信息外，还具有其他功能，包括反僵尸网络软件、检测系统中杀毒软件进程、反调试、通过 SMTP/FTP/ 代理将收集的数据进行回传、下载额外的插件以及采用 BouncyCastle 加密数据包等。目前，安天追影产品已经实现了对该 M00nD3V Logger 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。

垃圾邮件附件解压后包含恶意的可执行文件，执行后使用二层 XOR 解密并释放 M00nD3V Logger 窃密木马。该窃密木马具有多个功能模块，其每个模块对应功能为从指定 URL 下载名为 Crypto.dll 的文件并将其加载到内存中；执行前休眠 5000 毫秒；创建名为 "99ed2fc7-0fdc-42ef-8b82-78d1c7c554e3" 的互斥量；使用 Rijndael256 算法解密 StubConfig 中的数据，数据是 Base64 编码过的值，密钥是硬编码的互斥量值；添加注册表键值实现自启动；检查系统中是否正在运行 SbieDll.dll，Wireshark 等进程，如果存在，该木马将退出；提升进程权限，通过 AceQualifier AccessDenied 将安全标识符类型设置为“WorldSid”，确保该进程不允许被终止；检查系统中杀毒软件名，使用镜像劫持技术达到禁用所有列出的文件名程序的目的；反僵尸网络软件；检查系统进程分析软件如 Process Explorer、Process Hacker 等；通过 SMTP/FTP/ 代理将收集的数据进行回传。

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。

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，下为其自动形成的分析报告：

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（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、信标检测鉴定器、动态（Win7 x86）鉴定器等鉴定分析。

最终依据 BD 静态分析鉴定器、智能学习鉴定器将文件判定为木马程序。

◆ 概要信息

文件名	c23b33ddb4e0cfa52b9242648f5cb7a6ee916b4ba1e6f547d8d5ef543dcebb9d
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	250 KB
MD5	BF8801BCD5A196744CCD0F863F84DF71
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[Spy]/MSIL.Siplog.B
判定依据	BD 静态分析

◆ 操作系统

操作系统	内置软件
WinXP 5.1.2600 Service Pack 3 Build 2600	默认、IE6、Firefox、Google Chrome、Office 2003、Flash、WPS、FoxitReader、Adobe Reader

◆常见行为

行为描述	危险等级
加载运行时 DLL	★
打开自身进程文件	★
获取系统信息（处理器版本、处理器类型等）	★
获取系统版本	★
检测自身是否被调试	★★
获取驱动器类型	★
获取计算机名	★
疑似桌面控制	★

◆完整报告地址

安天周观察
安天官方微博 安天官方微信
主办：安天 2020 年 7 月 27 日 (总第 240 期) 试行 本期 4 版 微信搜索：antiylab 内部资料 免费交流

安天产品全力护航“天问”之旅

2020 年 7 月 23 日，中国首次火星探测任务“天问一号”探测器成功发射，迈出了我国自主开展行星探测的第一步。在本次探测项目中，我国计划一次性实现“绕”“落”“巡”三大任务，如果任务成功，中国将成为世界上首个首次探索火星即完成软着陆任务的国家。

惟兹之功，必有协助。

像以往所有重大活动一样，“天问一号”升空的背后，凝聚着几代航天人的努力，也离不开网络安全工作者默默的守护。

在本次发射任务中，安天投入大量安全设备与软件工具，派驻工程师提供现场保障；依托全面持续监测能力，建立系统与人员协同作业机制；凭借多年来对重大活动网络安保的经验积累，协同网内各种防御机制联合响应威胁，安天产品能力顺利保障了本次发射任务各阶段工作，将继续保障“天问一号”探测器完成后续任务。

多年来，安天始终坚持自主先进的能力导向，参与了 2005 年后历次国家重大政治社会活动的安保工作，为载人航天、探月工程、空间站对接、大飞机首飞、主力舰护航、南极科考等提供了安全保障，并多次获得杰出贡献奖、安保先进集体等称号。

此次火星探测任务承载着中华民族的“探火梦”，寄托着人类携手探索未知、共拓美好家园的希望，安天很荣幸参与其中，成为历史的亲历者。

微信扫描二维码
关注公众号查看原文

安全厂商披露多平台恶意软件框架 MATA

卡巴斯基研究人员报告了被称为MATA的恶意软件框架。MATA恶意软件框架具有多个组件，如加载器、协调器和插件。该框架能够针对Windows、Linux和macOS操作系统。研究人员发现MATA在2018年4月左右被使用，并在之后不断被使用渗透波兰、德国、土耳其、韩国、日本和印度等多国企业实体，试图进行数据库查询以获取客户列表。此外，MATA还用于分发VHD勒索软件。研究人员评估MATA框架与Lazarus APT组织存在联系。

（原文链接：https://securelist.com/mata-multi-platform-targeted-malware-framework/97746/）

多模块僵尸网络 Prometei 利用 SMB 传播

思科Talos最近发现了一个复杂的攻击活动，其使用了一个名为Prometei的多模块僵尸网络，通过多种传播方式，例如使用被盗凭据的SMB、psexec、WMI和SMB漏洞，最终挖取门罗币以获取经济利益。感染开始于僵尸网络主文件，该文件通过SMB从其它受感染系统复制，使用修改后的Mimikatz模块获取的密码和永恒之蓝等漏洞。Prometei有超过15个可执行模块，所有模块都由主模块下载和驱动，主模块通过HTTP与命令和控制(C2)服务器持续通信。

（原文链接：https://blog.talosintelligence.com/2020/07/prometei-botnet-and-its-quest-for-monero.html）

每周安全事件

类 型	内 容
中文标题	Ghost Squad Hackers 第二次入侵 ESA 网站
英文标题	Ghost Squad Hackers defaced a second European Space Agency (ESA) site in a week
作者及单位	Pierluigi Paganini
内容概述	名为 Ghost Squad Hackers 黑客组织在一周内对欧洲航天局（ESA）网站进行了第二次入侵。该黑客组织表示在第一次入侵后的几天内，在该机构服务器中发现一个服务器端请求伪造（SSRF）远程代码执行漏洞。他们利用该漏洞入侵了该网站另一个域。黑客称，ESA 专家尚未解决该漏洞，只是删除了 CMS 安装，该漏洞不在 CMS/Web 应用程序内，但会影响服务器上执行的服务。
链接地址	https://securityaffairs.co/wordpress/106111/hacking/esa-site-defaced-again.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	多款 Microsoft 产品安全漏洞（CVE-2020-1025）	高	当 Microsoft SharePoint Server 和 Skype for Business Server 不正确地处理 OAuth 令牌验证时，存在特权提升漏洞。成功利用此漏洞的攻击者可以绕过身份验证并实现不正当访问。
	Microsoft Windows Server DNS Server 安全漏洞（CVE-2020-1350）	高	当 Windows 域名系统服务器无法正确处理请求时，存在远程代码执行漏洞。成功利用此漏洞的攻击者可以在本地系统帐户的上下文中运行任意代码。配置为 DNS 服务器的 Windows 服务器会受到此漏洞影响。
	Microsoft Windows 和 Windows Server 安全漏洞（CVE-2020-1421）	高	如果处理了 .LNK 文件，则 Microsoft Windows 中存在一个远程代码执行漏洞。成功利用此漏洞的攻击者可能会获得与本地用户相同的用户权限。与拥有管理用户权限的用户相比，帐户被配置为拥有较少系统用户权限的用户受到的影响更小。
较为活跃样本家族	Trojan[Ransom]/Win32.PolyRansom	中	此威胁是一种感染类木马家族。该家族木马运行一定的时间后，会阻止访问操作系统。重新进入操作系统要求用户支付比特币或一定数额的金钱。
	Trojan/Win32.SelfDel	中	此威胁是一种对恶意木马家族。该家族木马的主要功能是对抗反病毒软件或安全工具，通常会关闭反病毒软件或安全工具的进程。该家族木马同时还具有删除反病毒软件的病毒库、文件或安全工具的功能。
	Trojan/Win32.Yakes	中	此威胁是一种恶意木马家族。该家族木马可以通过白名单机制绕过系统防火墙，获取系统的最高权限。该家族木马具有下载恶意程序、监控用户操作等行为。该家族木马会在执行完成后将自身删除。
	Trojan/Win32.ShipUp	中	此威胁是一种远程控制类木马家族。该家族木马通过垃圾邮件、被感染的 ZIP 包、仿冒 FLASH 广告等方式进行传播。该家族同时可以窃取系统和用户的信息，并控制用户系统。
	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/Android.Boogr	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游戏或流行应用程序，运行后可以下载其他恶意文件，将 SMS 消息发送给高价软件，或将受害者的智能手机连接到攻击者的命令和控制服务器。
	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。

疫情之下重新考虑托管服务：挑战与机遇

鲁本·卡斯塔内达 / 文 安天技术公益翻译组 / 译

通过托管服务，企业可以根据需要快速扩展，将数据存放在更接近最终用户的位置。在应对新冠疫情带来的工作变更时，这两个特征非常重要。

众所周知，新冠疫情改变了整个世界。科技公司以及支持它们的基础设施都无法幸免。

据 The Verge 统计，Zoom 在 2019 年 12 月的每日会议与会者有 1000 万；而到了 2020 年 4 月底，该数字已呈指数级增长，每日与会者超过了 3 亿。据 Variety 报道，在今年第一季度，Netflix 的付费用户增加了 1577 万，远高于其估计的 700 万。该公司认为，付费用户增加的原因是疫情期间人们宅家的时间大增。Data Economy 报道说，在短短 7 天内，微软的协同解决方案 Microsoft Teams 的用户就增加了 1200 万。

这种迅速而又完全出乎意料的巨大增长，使企业以及技术和软件提供商争相寻求以灵活、可扩展的方式快速、可靠和安全地支持用户需求。而这一切必须遵守疫情下“旅行和人际交往被严格限制”的新工作规则。此时，托管服务受到重视，走到了前台。从未考虑过托管的公司可以将其视为一种可靠的解决方案，以为其客户和员工提供快速数据访问。已经实施托管策略的公司可进一步加强这些策略。

通过托管服务，企业可以根据需要快速扩展，将数据存放在更接近最终用户的位置。在疫情期间，这两个功能显得更加重要了。在过去的四个月中，随着美国开始采取广泛的安全措施，相关的挑战和机遇已经显现。很多托管服务提供商迅速进行调整，以期满足这些需求。

非接触式服务

各个商店（从杂货店到外卖餐厅）已经提供了路边提货服务，使消费者能够以“非接触式”方式购买商品。同样的原则也适用于托管服务。诸如“远程操作 / 智能操作”（Remote Hands/Smart Hands）之类的服务以及跨数据中心的预定义安装，不仅是客户的必备要求，也为提供商提供了重要机会。

疫情期间，安装新环境和维护现有部署的过程必须能够“远程操作”（hands-free）并易于使用。设备出厂时带有其“使用说明”（SOW），其中包含准确和相关的详细信息，例如机架安装图、电缆分布一览表和安装图等。托管服务人员可以轻松地向客户交付高质量的全包解决方案，并附有概述完整安装过程的图片，以供客户使用或修改。

大型部署可能会采用疫情之前的方式：即客户需要安排工程师在现场；但是，企业仍然需要广泛的远程操作服务和“非接触式”解决方案。（对于无法亲自进行现场访问的团队，可以进行虚拟数据中心巡视。）

进一步加强云解决方案

疫情造成的破坏进一步巩固了云解决方案的地位，使云解决方案成为许多企业的首选。但是，对于无法仅采用云策略（由于预算、安全性、应用程序限制或许多其他原因）的企业来说，疫情则加速了他们的“云和托管”混合方法的部署。在这种情况下，公司通常更容易维护混合云解决方案，将物理数据中心与云的使用相结合。

使用云和托管服务的公司，需要通过互联解决方案轻松利用云资源的能力。这就创建了一个独特的生态系统。托管服务提供商可以利用该资源丰富的、运营商密集型生态系统帮助客户构建这种能力，使用自定义的点对点定长 OS2 光缆交叉连接，将 L2PTP 网络连接到托管云边缘节点。如果托管服务提供商不提供这种混合环境方法，就会落后。

轻松扩展

显然，各公司已经敏锐地意识到，他们需要在没有预警的情况下非常迅速地扩展，这意味着仅关注各个位置的专用实体数据中心并非正确的方法。通过托管服务，公司可以使用预定义的安装快速实现广泛的覆盖范围，从而实现无缝的多站点同时部署。为了恰当利用这种疫情驱动的转变，托管服务提供商必须根据需要在不同设施的新安装和镜像环境中采用“复制和粘贴”方法。此外，还要为客户提供调整和适应新地理环境所需的灵活性。

在数据中心租用一个机柜，是企业轻松扩展数据中心覆盖范围并确保良好最终用户体验的第一步。该过程应尽可能地可重复，以确保快速部署，从而简化数据中心技术人员和工程师的工作。

未来

在短期内，疫情对托管数据中心的影响，主要是通过锁定访问者的设施以及将团队移至高度受控的环境来实现的。但是，长期影响是，各种规模的企业都可以在各类实施中获得托管服务的好处。对业界来说，这些新机会前景广阔，但也意味着相关支持基础设施和规程必须随之发展。从长远来看，那些具有灵活性和前瞻性的公司将成为赢家。

原文名称	Rethinking Colo in the Era of COVID: Challenges and Opportunities
作者简介	鲁本 · 卡斯塔内达（Ruben Castaneda）。鲁本 · 卡斯塔内达是 Evoque 数据中心解决方案销售工程师。
原文信息	2020 年 7 月 2 日发布于 Network Computing 原文地址 https://www.networkcomputing.com/data-centers/rethinking-colo-era-covid-challenges-and-opportunities
免责声明	本译文译者为安天实验室工程师，出自个人兴趣在业余时间所译，本文原文来自互联网，译者与安天实验室均与原作者与原始发布者没有联系，亦未获得相关的版权授权，鉴于译者及安天实验室出于学习参考之目的翻译本文，而无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版权问题承担责任。译者力图忠于所获得之电子版本进行翻译，但受翻译水平和技术水平所限，不能完全保证译文完全与原文含义一致，同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。译者与安天实验室亦对原文和译文的任何内容不承担任何责任。翻译本文的行为不代表译者和安天实验室对原文立场持有任何立场和态度。 本译文亦不得用于任何商业目的，未授权任何人士和第三方二次分享本译文，基于上述问题产生的法律责任，译者与安天实验室一律不予承担。