安天智甲有效防护 Snake 勒索软件

近日，安天 CERT 在梳理网络安全事件时发现一个名为 Snake 的勒索软件，Snake 勒索软件最早于 2020 年 1 月被发现，采用 Go 语言编写，主要通过垃圾邮件进行传播。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 Snake 勒索软件的加密行为。

Snake 勒索软件执行后，加密计算机上的文件，在原文件名后追加随机生成的字符串后缀，并在桌面创建名为“Fix-Your-Files.txt”的勒索信，勒索信内容包含勒索说明、联系邮箱等。Snake 勒索软件尝试停止大量进程如：VMware Tools（VMware 虚拟机中自带的一种增强工具）、Microsoft System Center Operations Manager（微软系统中心管理器）、Sqlservr（微软 Microsoft SQL Server 服务套装的一部分）等。Snake 勒索软件为了防止受害者恢复已加密的文件，采用删除卷影副本、禁用修复、删除本地计算机的备份目录等操作。Snake 勒索软件使用“AES+RSA”加密算法加密文件，目前被加密的文件在未得到密钥前暂时无法解密。

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，避免一切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口令；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病毒的鉴定；安天智甲已经实现了对该勒索病毒的查杀。

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、关联分析鉴定器、数字证书鉴定器、元数据信息鉴定器、字符串分析鉴定器、字符串分析鉴定器、反病毒引擎鉴定器、动态（WinXP）鉴定器、聚类分析鉴定器、来源信息鉴定器、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、关联分析鉴定器、反病毒引擎鉴定器、动态行为鉴定器将文件判定为木马程序。

◆ 概要信息

文件名	e5262.exe
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	3.55 MB
MD5	3D1CC4EF33BAD0E39C757FCE317EF82A
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.Antavmu
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

◆危险行为

行为描述	危险等级
延时	★★★
感染文件	★★★★

◆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）	★
枚举进程	★
获取系统版本	★
访问文件尾部	★
获取计算机名	★
创建快捷方式	★
创建桌面快捷方式	★
感染文件	★★

◆进程监控

PID	创建	命令行
1352	target.exe	"c:\568a8bbee86b4bf2a4e341dbe565ef9f\share\target.exe"

◆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 5 月 25 日 (总第 231 期) 试行 本期 4 版 微信搜索：antiylab 内部资料 免费交流

肖新光：与网络安全防控的创新之约

——转自《新华访谈》

在视频连线中见到肖新光时，他正对提案进行补充和完善。作为全国政协委员，哈尔滨安天科技集团董事长、首席技术架构师，肖新光过去一年致力于协助各方构建动态综合的网络防御能力、提升网络安全防御水平，并且随时跟踪和借鉴国际上相关领域的最新成果。

Q：“作为全国政协委员，您在过去一年重点关注了哪些领域？做了哪些有针对性的工作？”

A：“协助构建动态综合的网络防御能力、提升网络安全防御水平、跟踪国际上的最新成果。”过去一年，我和我的团队致力于协助各方构建动态综合的网络防御能力、提升网络安全防御水平，并且随时跟踪和借鉴国际上相关领域的最新成果。

Q：“您认为我国当前在网络安全领域面临怎样的形势，面对的挑战和发展瓶颈是什么？”

A：“面临的形势‘非常复杂’‘相当严峻’。由于对网络信息系统依存度加深，如遇安全威胁将带来严重的隐患。”

对于当前我国在网络安全领域面临的形势和挑战，肖新光用“非常复杂”“相当严峻”表达他的见解。他说，随着整个社会的信息化、自动化、智能化程度不断提升，对于网络信息系统的依赖程度也不断增加。网络信息系统遇到安全威胁，会带来严重的安全隐患。

面对这些安全威胁，必须形成有效的防御能力。信息化发展中，很多存量系统在当时建设时大多没有充分考虑网络安全问题，需要“补课”。随着 5G 的发展，在新基建建设中有大量的增量系统建设，更需要网络安全同步规划、同步建设、同步运维的一套方法体系和相应的预算保障，也需要通过规划指引全面提升防御能力，通过预算投入支撑网络安全领域的能力建设。

Q：“在打造清朗网络空间方面安天科技做了哪些独创工作？最新的进展有哪些？”

A：“过去一年安天科技更多是围绕威胁检测、对抗的能力建设等，做了大量工作。”

肖新光说，在打造清朗网络空间、提升网络安全防护能力方面，过去一年安天科技更多是围绕威胁检测、对抗的能力建设等，做了大量工作。

比如，他们充分发挥安天基础安全引擎的能力优势，在基础的供应链环节中解决威胁检测、接入安全等一系列安全问题。截至目前，安天的安全引擎已服务累计超过 17 亿部手机。

同时，他们还会借助专家团队，对大规模的威胁情报系统进行分析，从而将诊断高级威胁的相关经验应用到实际工作。过去一年，安天与政府主管部门和用户积极配合，发现了多起对我国相关机构进行网络入侵渗透的活动，并分析了对方所使用的装备和一些攻击资源。

Q：“去年您的两会提案，也是有关全面提升网络防护水平的，一年来这些方面有哪些提升或变化？”

A：“获得政府主管部门的重视，推动了网络安全领域中相应规划的提升。”

访谈中，肖新光特别提及，当前的网络攻击出现新特点，过去的安全威胁是单点威胁，比如病毒、木马、DNS 攻击、网站篡改等。如今随着信息技术越来越先进、信息体系越来越复杂、信息资产越来越庞大，安全威胁也在不断发展演进。

肖新光说，他去年的政协提案获得政府主管部门的重视，推动了网络安全领域中相应规划的提升。尽管如此，与我国在各领域的快速发展相比，当前的网络安全防护水平和技术能力还有较大提升空间。这个跟进的过程将是“复杂、艰巨、富有挑战”的，不仅需要我们有只争朝夕的紧迫感，更需要我们的不懈努力。

扫描微信二维码了解更多两会相关报道

Adwind 远控木马以 Covid-19 为诱饵攻击印度银行

Seqrite研究人员发现以Covid-19为诱饵针对印度银行传播Adwind远控木马的攻击活动。初始电子邮件内容有关Covid-19或财务交易，附件是包含基于JAP恶意软件的ZIP文件，JAP恶意软件为可以在任何装有Java的计算机上（包括Windows、Linux、Mac系统）运行的远控木马Adwind。一旦安装了该木马，攻击者就可以接管受害者的设备，从远程计算机发送命令并在网络中横向传播。此外，该恶意软件还可以键盘记录、捕获屏幕截图、下载其它有效载荷并提取敏感的用户信息。

（原文链接：https://ciso.economictimes.indiatimes.com/news/seqrite-detects-trojan-targetting-co-operative-banks/75817815）

每周安全事件

类 型	内 容
中文标题	欧洲多国超级计算机集群感染挖矿恶意软件
英文标题	Supercomputers hacked across Europe to mine cryptocurrency
作者及单位	Catalin Cimpanu for Zero Day
内容概述	欧洲多个国家的超级计算机遭黑客入侵，感染挖矿恶意软件。英国、德国和瑞士已确认发生了该安全事件，在西班牙的高性能计算中心也发生了类似的入侵事件。研究人员对恶意样本进行了分析，表示攻击者似乎已通过受到破坏的 SSH 凭据获得了对超级计算机群集的访问权限。一旦攻击者获得对超级计算节点的访问权限，攻击者似乎利用 CVE-2019-15666 漏洞进行了 root 访问，然后部署了门罗币挖矿恶意程序。
链接地址	https://www.zdnet.com/article/supercomputers-hacked-across-europe-to-mine-cryptocurrency/

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	名称与发现时间	威胁等级	简要描述
活跃漏洞	Microsoft Office 安全漏洞（CVE-2020-0760）	高	当 Microsoft Office 不正确地加载任意类型的库时，会触发远程代码执行漏洞。攻击者可随后安装程序；查看、更改或删除数据；或者创建拥有完全用户权限的新帐户。
	Microsoft Dynamics Business Central 安全漏洞（CVE-2020-1022）	高	Microsoft Dynamics Business Central 中存在远程代码执行漏洞。成功利用此漏洞的攻击者可以在目标服务器上执行任意代码。
	MICROSOFT WINDOWS GRAPHICS DEVICE INTERFACE 安全漏洞（CVE-2020-0964）	高	Windows 图形设备接口 (GDI) 处理内存中对象的方式时存在远程代码执行漏洞。成功利用此漏洞的攻击者可能会控制受影响的系统。攻击者可随后安装程序；查看、更改或删除数据；或者创建拥有完全用户权限的新帐户。
较为活跃样本家族	Trojan[Ransom]/Win32.VirLock	中	该病毒家族是一种 Windows 平台上的勒索软件家族。该家族样本运行后，不仅会对文件进行加密，同时还会采用锁屏，进一步阻碍用户操作。
	Trojan[Downloader]/Win32.Rubinurd	中	该病毒家族是一种下载类木马程序。该家族样本中包含将要下载和安装的恶意软件程序的名称和位置信息，这些信息通常是作为一个加密的数据块存储在文件的末尾。
	Trojan[Dropper]/Win32.Dinwod	中	该病毒家族是一种具有释放或捆绑行为的木马类程序。该家族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[Backdoor]/Linux.Gafgyt	中	该病毒家族是一种 Linux 平台上的具有窃密行为的后门家族。该家族样本运行后会在 Linux 上开启一个后门并允许远程控制端执行任意操作，并且会收集机器上的信息上传给远程控制端。
	Trojan[Backdoor]/Linux.Mirai	中	该病毒家族是一种 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。
	Trojan/Android.KungFu	中	该家族木马运行后，执行提权操作，在后台自动静默下载并安装未知应用。当手机感染此木马后使用常规杀毒软件和恢复出厂设置都无法彻底清除。
	Trojan[Dropper]/Android.Shedun	中	该病毒家族是一种具有释放或捆绑行为的木马类程序。该家族样本运行后，通过欺骗用户授权安装，其可获得专为视觉障碍用户设计的 Android Accessibility Service 的控制权限。

五个简易举措提升新冠疫情期间的网络安全

罗杰·桑顿 / 文 安天技术公益翻译组 / 译

自新冠疫情爆发以来，网络攻击呈指数级增长。AT&T Alien 实验室的开放式威胁情报交换平台（OTX）发现，从 1 月到 3 月，有 419,643 个与 COVID-19 相关的 IOC，其中从 2 月到 3 月，环比增长 2,000%。

加强网络安全迫在眉睫

无论是否做好准备，各行各业、不同规模的公司都不得不在短时间内快速适应远程工作环境。随着向虚拟业务的快速转移，网络犯罪分子也调整了策略以利用不断扩大的攻击面。上个月的攻击量增加了近 40%，以 COVID-19 为主题的网络钓鱼攻击增加了 500%。对于 IT 经理来说，当前的情况就如同噩梦一般。

这种新的远程工作环境带来了全新的安全格局。在零信任模型和云安全采用中可以找到长期的解决方案，但把握时间至关重要。因此，组织应立即采取行动。

以下是 IT 经理现在可以采取的一些短期且易于实施的措施，可以帮助组织机构在当前新冠疫情期间加强网络安全。

1. 将”社交距离“应用到家庭网络

传统意义上来说，在家庭 Wi-Fi 网络上执行的通常都是与工作无关的不太敏感的任务，例如孩子们在平板电脑上玩游戏、激活语音助手来报告天气情况，以及在智能电视上播放电影。而如今，员工通过家庭 Wi-Fi 网络连接办公室设备，这为通过同一网络访问 Internet 的其他人带来了安全漏洞。这种模糊性也使得安全得不到保障。

就像鼓励保持社交距离以限制 COVID-19 的潜在传播一样，我们也应该将“社交距离”应用到家庭网络中。IT 经理可以鼓励员工对家庭互联网接入进行分区。这就意味着要试图阻止除员工以外的其他人使用与登录办公室设备相同的网络连接。仅这一步就可以帮助防止未知漏洞带来的攻击浪潮。

员工无需具备广泛的 IT 技能即可隔离家庭网络，这可以大大节省 IT 经理宝贵的时间和资源。当今市场上，有几款价格在 100 美元左右的家用和小型办公路由器可提供 VLAN 支持，大多数 Wi-Fi 套件也都提供建立“访客”网络的功能。作为 IT 经理，重要的是要提供有关如何在普通路由器上设置这一功能的详细说明，同时让员工了解到，使用这一简单方法就可以大大提高安全性。

2. 鼓励员工使用公司的移动设备

员工携带自己的设备办公（BYOD）带来了巨大的安全风险。组织机构无法知道，员工的家庭设备上存在哪些类型的恶意软件？他们是否完成了最近的软件更新？这是一场不值得冒险的赌博。

如果可能的话，IT 经理应为员工提供公司的移动设备，比如智能手机和平板电脑。首先，在大部分地区都可以使用移动宽带功能来代替家庭网络。此外，这些设备还可以远程管理。实质上，用户是在与制造商的安全团队合作，以确保设备的安全，而移动运营商则是要确保安全连接。使用公司的设备再搭配上高质量键盘，员工就再也不会想念他们的电脑了。

3. 迁移至云，就是现在！

本地软件已经过时，而且通常效率低下。如果您的组织机构尚未实施云迁移，则应该强制进行这一改变。客户关系管理系统、办公应用程序甚至是创新设计平台现在都可以作为 SaaS 产品使用，而且性能优于传统软件。借助云解决方案，组织机构正与 SaaS 供应商的安全团队合作，以帮助防范潜在漏洞。

如果员工使用公司的设备并在云中运行 SaaS 应用程序，攻击面将会成倍减少。

4. 确保员工安全进行远程访问

员工会将设备连接到多个服务连接，以至于难以对这些连接进行持续的单独管理。在安全的远程访问工具（如强大的端点安全解决方案和云安全网关）上进行投资，这样即使员工比较分散，IT 经理也可以制定策略并监控全公司的活动。

5. 提高密码安全性

我敢打赌，大部分员工都在使用弱密码登录办公室设备。他们都是根据孩子的姓名、周年纪念日等设置密码，最糟糕的甚至还用“password123”。

IT 经理需要立即（并定期！）指导员工如何改善其安全状况。其中最简单的方法就是从密码安全开始。坚持要求员工为他们用来访问办公室的每个设备和连接创建复杂且唯一的长密码。鼓励员工使用密码管理器来跟踪所有登录。从 CEO 到实习生，所有员工都应该采用双因子身份验证。这种行为上的改变不需付出任何成本，却能大大提高网络犯罪分子成功进行攻击的难度。

我们都会受到新冠疫情的影响。以前，IT 经理肩负着巨大的责任，而在当前的远程工作环境中，这种负担更是成倍增加。虽然待办事项清单可能看起来很详尽，但不妨尝试将注意力集中在一些短期措施上，这些措施将使您安心并快速加强网络安全。

原文名称	5 easy steps to immediately bolster cybersecurity during the pandemic
作者简介	罗杰 · 桑顿（Roger Thornton））。罗杰 · 桑顿是 AT&T 网络安全公司产品和技术副总裁。
原文信息	2020 年 5 月 14 日发布于 Help Net Security 原文地址 https://www.helpnetsecurity.com/2020/05/14/bolster-cybersecurity/
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。