安天智甲有效防护 Spyro 勒索软件

近日，安天CERT在梳理网络安全事件时发现了一个名为Spyro的勒索软件。该勒索软件最早被发现于2021年6月，主要通过垃圾邮件进行传播。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Spyro勒索软件的加密行为。

Spyro勒索软件运行后，首先通过自定义算法生成USER_ID，并获取磁盘已用大小，将这些信息通过POST提交到“h1dd3n.cc/voidcrypt/index.php”，而后将返回公钥；然后在%programData%目录下创建“pkey.txt”和“Idk.txt”文件，分布保存公钥和USER_ID，同时在%tmp%目录下释放名为“Windows Session Manager.exe”的加密程序并运行，该程序运行后，拷贝自身到启动文件夹，创建多个线程遍历磁盘文件并对特定后缀名的文档、压缩包、图片、音视频、非系统应用程序等文件进行加密，加密后的文件名为“原始文件名+[BlackSpyro@tutanota.com][USER_ID].Spyro”。除此之外，在加密过程中，Spyro勒索软件的主程序负责在每个加密文件所在目录释放名为“Decrypt-info.txt”的勒索信，该勒索信中仅包含勒索说明和联系邮箱；该勒索软件释放的加密程序还会调用系统命令关闭防火墙、停止相关数据库服务、禁用系统修复功能和删除系统备份目录。由于该勒索软件未删除系统卷影副本，可尝试通过系统卷影进行文件恢复。

▲Spyro勒索软件勒索信息

Spyro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	6d0cefa5b7f1744aa5dbc041c50b1709
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	1.32 MB
MD5	6D0CEFA5B7F1744AA5DBC041C50B1709
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[Ransom]/Win32.Odveta.gen
判定依据	反病毒引擎

报告地址：https://1.119.163.6/vue/details?hash=6D0CEFA5B7F1744AA5DBC041C50B1709

◆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
查询系统硬盘大小	★★★
禁用代理服务器功能	★★★★
创建互斥量	★★★
发送 http 数据	★★★★

◆常见行为

行为描述	危险等级
壳行为填充导入表	★★
设置注册表	★★
.....	.....

◆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08月02日(总第289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

“幻鼠”组织针对我国的窃密攻击活动分析

概述

2021年5月，安天CERT监测到一起对国内某化学品生产企业的窃密行动，经安天CERT分析发现了一个利用Telegram、Internet Archive和blogger博客分发Raccoon Stealer窃取木马活动。该起攻击行动主要通过钓鱼邮件进行传播，将邮件内容伪装成公司客户需求，诱导受害者下载附件并执行解压后的恶意程序。安天CERT跟踪发现该攻击活动从2021年4月一直持续至今，攻击者使用多种手法进行反溯源和反查杀，如使用Telegram作为C2进行通信、利用注册表实现恶意载荷访问、窃密载荷不落地和削弱Microsoft Defender防病毒功能等。针对其多种方式反追踪溯源的攻击特点，安天将其命名为“幻鼠”组织，与Gorgon组织TTP手法类似。

Raccoon Stealer窃密木马首次出现于2019年4月，是暗网中最受关注的10大恶意软件之一，目前已经感染了全球数十万台设备。该木马具有窃取登录凭据、信用卡信息、加密货币钱包和浏览器信息等多种恶意功能。

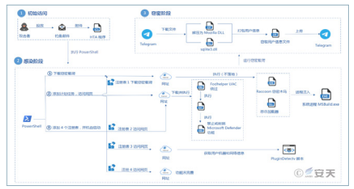
事件对应的ATT&CK映射图谱

该起攻击行动样本技术特点分布图：


▲技术特点对应ATT&CK的映射

攻击流程

攻击者在本次攻击行动中的攻击流程图如下所示：


▲攻击流程图

样本分析

Preshuru.txt脚本分析

攻击者在Internet Archive中创建了一个名为“Preshuru”的项目，该项目中存在上述下载的Preshuru.txt恶意文件。攻击者通过这种方式提高溯源难度。

攻击者将可执行文件的16进制数据转储为字符串，通过PowerShell命令对字符串进行还原，安天CERT分析人员发现该PowerShell中存在两个可执行文件，一个为Raccoon Stealer窃密木马，另一个为恶意加载器DLL。攻击者首先调用PowerShell将字符串转化为PE文件，然后启动系统自带“MSBuild.exe”文件进程，调用恶意加载器，最后通过“进程镂空”技术将Raccoon Stealer窃密木马注入到白文件MSBuild.exe进程中。

（原文链接：https://mp.weixin.qq.com/s/JoohsUOJXbaEGaYZWv0pnw）

扫描右侧二维码阅读全文

“2021年网络安全优秀创新成果大赛－哈尔滨分站赛”成功举办

7月23-24日，由中央网信办网络安全协调局指导，中国网络安全产业联盟（CCIA）主办的“2021年网络安全优秀创新成果大赛”首个分站赛在哈尔滨市拉开帷幕。本次大赛在哈尔滨、南京、武汉举办分站赛，哈尔滨分站赛由黑龙江省委网信办指导，省网络空间研究中心、省工业技术研究院承办，安天科技集团股份有限公司协办。

哈尔滨市科教资源丰富，网络安全学科和产业具有一定特色优势。本次分站赛充分结合哈尔滨市本地网络安全资源条件，特别邀请驻哈高校、科研机构、行业部门的专家与CCIA专家委专家、网络安全投资机构专家一起组成评审专家组。来自全国近30家网络安全企业提交的40余项解决方案和创新产品参加了本次比赛，并进行了现场答辩。经过评审，哈尔滨分站赛最终评选出“2021年网络安全优秀创新成果大赛”解决方案入围奖10项和创新产品入围奖10项。

本次分站赛特别组织开展了参观交流活动，评审专家和申报单位代表参观了安天科技集团股份有限公司、深圳（哈尔滨）产业园，充分感受哈尔滨市网信相关产业优势和发展环境。

“2021年网络安全优秀创新成果大赛”是CCIA在连续三年组织开展“优秀网络安全解决方案和创新产品评选活动”基础上进行的创新评选活动。大赛首次采用分站赛形式，赛程分为分站赛初赛、半决赛和总决赛三个阶段，致力于推选我国网络安全产业优秀创新成果，激发网络安全企业加强自主创新能力，搭建网络安全企业、技术、人才和资本合作的平台，推动网络安全产业高质量发展。

（原文链接：https://mp.weixin.qq.com/s/JTq-C7RTVGRlVQYX6X1Fpg）

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	StrongPity APT 组织首次部署 Android 恶意软件
英文标题	StrongPity APT Group Deploys Android Malware for the First Time
作者	Zhengyu Dong, Fyodor Yarochkin, Steven Du
内容概述	研究人员最近对一个恶意的 Android 恶意软件样本进行了调查，并且认为该样本来自于 StrongPity APT 组织，该恶意软件被发布在叙利亚电子政府网站上。据悉，这是该组织首次被公开观察到使用恶意 Android 应用程序进行攻击。共享的样本是叙利亚电子政府 Android 应用程序的木马版本，它会窃取联系人列表，并从受害者的设备中收集特定文件扩展名的文件。
链接地址	https://www.trendmicro.com/en_us/research/21/g/strongpity-apt-group-deploys-android-malware-for-the-first-time.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	HEVC 视频扩展远程代码执行漏洞（CVE-2021-33776）	高	HEVC 视频扩展存在远程代码执行漏洞。由于 HEVC 视频扩展中的输入验证不正确，使得攻击者可以发送特制的请求并在目标系统上执行任意代码。
	Microsoft Defender 远程代码执行漏洞（CVE-2021-34464）	高	Microsoft Defender 存在远程代码执行漏洞。由于 Microsoft Defender 中的输入验证不正确，使得攻击者可以发送特制的请求并在目标系统上执行任意代码。
	Microsoft Excel 远程代码执行漏洞（CVE-2021-34501）	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。
较为活跃样本家族	Trojan[Packed]/Win32.Krap	中	此威胁是一种窃取账号信息的木马类家族。该家族木马运行后会注入系统进程，并监视正在运行的窗口标题，利用键盘 hook、内存截取或者封包截取等方式窃取账户信息并将这些信息发送到指定的服务器。
	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[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。
	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.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[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。

端点安全的重要性日益凸显

阿尔·胡格 / 文 安天技术公益翻译组 / 译

毫无疑问，端点安全一直都是很重要的。在新冠疫情爆发之后，企业不得不转向远程办公，端点安全问题变得比以往任何时候都更加紧迫了。

虽然在疫情爆发之前，“居家办公”的情况就存在了，但是远没有达到现在的规模，风险也没有这么大。似乎在一夜之间，大多数端点都迁移到了公司网络边界之外。长期以来，端点安全一直是 IT 行业关注的焦点，未来几年仍将会如此。这是因为，各种规模的企业面临的大多数威胁都指向端点，无论是员工家中的桌面电脑，还是存储着所有员工身份验证信息的数据库服务器。

事实是，端点一直是通往企业宝贵信息（例如知识产权信息）的门户。

端点安全的相关数据

根据思科《2021 年端点安全成果研究报告》，各种规模的企业都在努力应对端点安全问题。报告发现，在过去的两年中，全球超过 40% 的企业发生了重大安全事件。没有优先考虑集成平台（将端点安全作为核心要素）的企业，遭受重大安全事件的可能性几乎是其他企业的两倍。

思科对其安全软件 Secure Endpoint 检测到的关键“攻击信标”（IoC）进行了分析，发现攻击者主要使用了四种 IoC。排在首位的 IoC 是两用 PowerShell 工具，包括 PowerShell 框架（例如 PowerShell Empire）和可以利用 PowerShell 的框架（例如 Cobalt Strike 和 Metasploit），也包括简单的 PowerShell 命令行和自定义 PowerShell 脚本（用于保护访问或在网络内部横向移动）。PowerShell 受攻击者青睐的原因是，它默认安装在企业的计算机中，而且其活动通常不会被密切监控。

排在第二位的 IoC 是勒索软件。对于许多出于经济动机的攻击者而言，向端点传播勒索软件并加密端点上的数据是他们的主要目标。在过去的几年中，全球范围内的勒索软件活动大幅增加。思科 Secure Endpoint 等现代端点安全软件能够提供多层保护，能够阻止攻击者的上述活动。

排在第三位的 IoC 是无文件恶意软件。该方法通过内存进程注入和注册表活动来感染端点。攻击者使用此技术来规避较老的端点保护技术，防止被其检测到。

排在第四位的 IoC 是撞库。目前使用最广泛的撞库工具是 Mimikatz，它能够从端点系统内存中抓取用户凭证。此后，攻击者会利用这些凭证进行横向移动，以破坏企业活动目录服务器，从而广泛传播勒索软件或不受限制地访问目标数据。

很明显，端点面临着各种攻击技术，包括初始访问、横向移动、提权以及渗漏和加密数据等。第一代端点安全技术防御的也不仅仅是病毒、蠕虫和木马。在现代威胁形势下，企业需要一种更高明的防御方法，而非简单地扫描端点以查找恶意软件。

端点是最后一道防线

现在，企业面临着多种网络安全威胁。为了防御这些威胁，企业需要检测和阻止端点上的各种攻击活动。

端点安全仍然是现代 IT 安全工作的关键。过去，攻击者主要针对服务器和数据库；但是现在，端点既是攻击者遍历网络的手段，也是其最终的攻击目标。因此，了解端点上的活动对于跟踪和阻止攻击者的行为至关重要。

企业遵守不同的监管或网络安全策略，通常涉及证明其已采取控制措施来识别潜在风险和攻击，查询整个企业的端点以了解其当前的操作状态和历史记录，为审计过程提供强大的安全工具和支持等。

采用“平台方法”实现端点安全

端点是现代网络安全平台架构（包括 SASE、零信任和 XDR）的核心要素。SASE 提供了一种在网络边缘实现安全的整体方法，零信任能够持续验证访问，而 XDR 则支持检测和响应潜在威胁。

端点是远程办公的员工日常使用的设备，也是其最后一道关键防线。现在，端点既是安全行业的控制面板，也是将不同安全要素联系在一起的平台方法的核心要素。

原文名称	The Growing Importance of Endpoint Security
作者简介	阿尔·胡格（Al Huger），是 Cisco Secure 公司的副总裁兼平台与响应总经理。
原文信息	2021 年 6 月 28 日发布于 Dark Reading 原文地址 https://www.darkreading.com/endpoint/the-growing-importance-of-endpoint-security/d/d-id/1341373
摘 要	端点是现代网络安全平台架构（包括 SASE、零信任和 XDR）的核心要素。SASE 提供了一种在网络边缘实现安全的整体方法，零信任能够持续验证访问，而 XDR 则支持检测和响应潜在威胁。端点是远程办公的员工日常使用的设备，也是其最后一道关键防线。现在，端点既是安全行业的控制面板，也是将不同安全要素联系在一起的平台方法的核心要素。
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。