安天发布《Sifrelendi 勒索软件变种分析报告》

近日，安天 CERT 在梳理网络安全事件时发现一个名为 Sifrelendi 的勒索软件变种，该勒索软件隶属于 Keslan 勒索软件家族，此家族于 2019 年 12 月初被发现，主要通过钓鱼邮件进行传播，邮件附件中包含一个名为 Host Process for Windows Services（Windows 服务主进程 svchost.exe）的勒索程序，目的是伪装成 Windows 系统中的程序，诱使用户运行该勒索程序。

Sifrelendi 勒索软件执行后，加密计算机上的可执行程序和文档文件，在原文件名后追加名为“.MZ434376”的后缀，修改桌面背景为土耳其语和英语的勒索提示信息，在所有含有被加密文件的位置创建名为“Beni_Oku!!!.hta”的勒索信，勒索信内容为土耳其语，包含勒索说明、联系邮箱、赎金金额和 USER_ID 等，赎金金额为价值 300 美金的比特币。Sifrelendi 勒索软件使用“RSA+AES”加密算法加密文件，调用命令行命令来防止受害者恢复已加密的文件，具体操作为删除卷影副本、禁用修复、删除本地计算机的备份目录等。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、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、聚类分析鉴定器、智能学习鉴定器、静态特征检测鉴定器、安全云鉴定器、等鉴定分析。

最终依据关联分析鉴定器、关联分析鉴定器将文件判定为木马程序。

◆概要信息

文件名	010ddd6f96fc4d7b3410dda6c048d3d69ab15dcb9d5738b7b9696f80195d64ef
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	754 KB
MD5	C6D90484C49C61234F01F8AA5C9DE150
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[HEUR]/Win32.V00br457frfi
判定依据	BD 静态分析

◆操作系统

操作系统	内置软件
Win7 x86 6.1.7600 Build 7600	默认、IE9、Google Chrome、Firefox、Office 2007、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	★★★★
删除所有系统状态备份	★★★★
在启动时禁用 Windows 错误恢复	★★★★
禁用任务管理器	★★★
感染文件尾部	★★★★
查询系统硬盘大小	★★★
感染文件	★★★★
延时	★★★

◆常见行为

行为描述	危险等级
壳行为填充导入表	★★
获取系统信息（处理器版本、处理器类型等）	★
获取系统版本	★
加载运行时 DLL	★
创建窗口	★
访问文件尾部	★
创建快捷方式	★
.....	.....

◆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 2019 年 12 月 23 日 (总第 213 期) 试行 本期 4 版 微信搜索：antiylab 内部资料 免费交流

安天产品巡礼 (系列四)——拓痕工具箱

拓痕工具箱是一款可以满足日常巡检、风险评估、应急处置、分析取证的便携式工具套装产品。其内置安天下一代威胁检测引擎，将安天多年的系统安全监测与处置、流量安全分析、恶意代码行为分析及安天应急响应的经验转换为产品能力，同时支持多种方式的威胁情报扩展功能。

工具箱中包含了主机风险检查、系统内核分析、程序行为监测分析等多种面向主机系统的安全工具，即可一键完成相关的检测、处置、证据提取等相关工作，也可以直接对系统及可疑对象进行分析诊断。同时，提供了便携式流量监测工具、便携式沙箱等设备选件。系统通过现场处置与远程协助两种工作模式相结合，具有有效加强巡查监测的全面性和深入度，提升取证处置效率、解决疑难杂症、降维检查维护人员的技能要求等多方面优势。

功能简介

拓痕工具箱可广泛应用于网络安全事件的应急响应、威胁检测、分析、处置、取证及 IT 系统紧急运维等场景。当前市场中的工具箱产品种类繁多，但大部分都集成了开源工具，界面风格不统一，操作繁琐，还存在被植入后门等安全隐患。同时在恶意代码检测能力、系统内核级提取分析能力、顽固感染和 Rootkit 处置等能力上有所缺失，缺少在强对抗场景下展开工作的能力基础。拓痕工具箱完全由安天自主研发，融合安天核心引擎与近 20 年威胁对抗经验，产品安全可控，操作简单易用，在终端侧打造集安全检测、深度分析、证据提取、问题处置于一身的实用工具，形成闭环操作，有效应对安全事件各环节需求，面对威胁既可未雨绸缪、防患于未然，又能够应对有方、防微杜渐。拓痕工具箱主要由主机深度检查工具及远程协助安全工具两部分组成。

主机深度检查工具由便携式专用 USB 设备或光盘承载，界面简洁易用，无需安装，即插即用。基于安天下一代威胁检测引擎（AVL-SDK）和威胁情报的扩展，实现了海量恶意代码检测和精准命名能力，并形成一定的未知威胁发现能力。能够在主机侧实现安全检测、深度分析、证据提取、问题处置的闭环操作，辅助安全人员对安全事件的全生命周期开展调查取证工作。主机深度检查工具既能全面检查系统的安全配置，高效扫描系统应用漏洞、精准检测已知威胁，辅助分析人员发现未知威胁，又能够将检测发现的系统脆弱性进行一键修复，有效处置顽固感染，同时对威胁证据等信息进行固化提取。为满足不同级别的安全技术人员的需求，主机深度检查工具即支持自动化智能检测，亦可辅助安全专家开展手动分析工作。

主机深度检查工具可快速提取终端系统运行的近百个检测点，进行深度融合分析，多维度分析评判终端系统的安全性能，检测终端面临的已知威胁并评估系统脆弱性，高效全面地定位系统安全隐患所在。同时，主机深度检查工具着力加强系统检测专业纵深，从内核到应用，横向广泛全面，纵向深入细致，依据恶意代码攻击作用点零遗漏分布检测点，结合多重验证方法，对高级威胁、未知威胁具有更强的检测和分析能力，帮助用户做出更合理的安全决策。主机深度检查工具的证据提取功能可采集终端系统运行数据，详实记录当前系统运行状态。在取证场景中，所有证据数据均压缩加密存储，附加签名验证，可依据客户需求导出至指定位置，做到一比一还原。

应急处置功能针对顽固感染中的多进程 / 线程保护、驱动级保护，以及 Rookit 木马的隐藏点，设计了灵活的挂载内核驱动提取与处置机制，对目标终端具有高级别的分析处置权限，且在网络安全事件中具备底层的处置能力。工具采用底层驱动技术通过远程线程卸载 DLL 文件。同时附带了专业分析工具，让系统内核模块、驱动、服务、进程和模块等信息一览无余。还可发现隐藏的文件、隐藏注册表键值等深层信息。除自动处置之外，还支持手工终止内核模块、服务、进程，关闭特定文件句柄等交互式手动处置模式，同时可禁止创建特定进程，限制进程占用 CPU、内存等系统资源，第一时间抑制恶性事件扩散传播，缩小感染范围，减少事件影响，降低影响损失，保障终端系统安全。

基于远程协助安全工具，拓痕工具箱能够为用户提供远程协助的工作模式。远程协助工具为软硬件结合设备，由专用远程硬件设备、远程协助服务器、专家端软件程序三者组成立体化远程安全协助体系，安天工程师或安全专家团队可远程操作未联网的疑似失陷目标主机，且无需为主机安装任何应用。远程专家和现场人员协同处置既降低了现场人员的技能要求，又极大的提高了应急事件的处置效率及处理能力，第一时间对隐患进行排查并实施缓解措施，有效遏制因威胁事件的迅速扩散为用户带来的损失扩大等问题。

微信扫描二维码阅读原文

每周安全事件

类 型	内 容
中文标题	罗马尼亚黑客利用挖矿恶意软件窃取用户信息
英文标题	Romanian cybergang infects over 400,000 computers with crypto mining malware
作者及单位	Elliot Hill Coin Rivet
内容概述	根据美国俄亥俄州北区检察官办公室的新闻稿，一个复杂的网络犯罪团伙已经部署了恶意软件来挖掘加密货币并窃取超过 40 万名受害者的个人详细信息。据报道，这些罪行是由罗马尼亚黑客组织“ Bayrob Group”的成员实施的。该组织主要针对属于美国公民的计算机，这些年来被窃取的数据包括财务信息、密码、电子邮件和其他个人信息。这些用户通常通过点击看似合法的电子邮件下载恶意软件，这些电子邮件声称来自银行和杀毒软件提供商。
链接地址	https://finance.yahoo.com/news/romanian-cybergang-infects-over-400-100025512.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 8 个移动平台恶意代码和 6 个 PC 平台的恶意代码和漏洞值得关注

恶意代码类别		名称与发现时间	威胁等级	简要描述
移动恶意代码	新出现的样本家族	Trojan/Android.urbestPay.a[exp,prv] 2019-12-15	高	该应用程序启动后隐藏图标，后台和 js 交互私自订阅付费网页，后台下载未知文件，上传手机固件信息、收件箱信息，并通过 js 网页发送短信，获取电话号码等，会造成用户隐私泄漏及资费消耗，建议卸载。
		Trojan/Android.FakeInst.fk[prv,rmt] 2019-12-16	中	该应用程序伪装为杀毒软件，运行隐藏图标激活设备管理器，根据指令获取用户短信、通讯录、通话记录等隐私信息，同时会修改锁屏密码锁定用户手机，造成用户隐私泄露且手机无法正常使用，建议卸载。
		RiskWare/Android.Zhuhaivisit.a[prv] 2019-12-17	低	该应用程序包含风险代码，监听短信并记录，可能造成隐私泄露，请谨慎使用。
	较为活跃样本	Trojan/Android.Joker2.c[prv,pay,exp]	中	该应用程序包含恶意代码，运行后联网下载恶意子包，解析控制命令，静默模拟点击广告，订阅付费业务，窃取用户短信、联系人列表和设备信息。造成用户隐私泄露和经济损失，建议卸载。
		Trojan/Android.MuddyWatera[prv,exp,spy]	中	该应用程序伪装正常应用，运行隐藏图标，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.SmsSpy.co[prv,exp]	中	该应用程序伪装为正常应用，运行拦截用户短信，并私自转发至指定号码，造成用户的隐私泄露和资费消耗，建议卸载。
		Trojan/Android.SmsSpy.cp[prv,exp]	中	该应用程序运行监听用户短信并发送到指定号码，还会删除用户短信，造成用户隐私泄露和资费损耗，建议卸载。
		Ware/Android.capushe.g[rog,exp]	低	该应用程序伪装成正常应用，安装后隐藏图标，后台推送广告，下载应用，存在流氓行为，造成用户流量损失，建议卸载。
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Microsoft Word 拒绝服务漏洞（CVE-2019-1461）	高	Microsoft Word 软件无法正确处理内存中的对象时，会触发拒绝服务漏洞。成功利用此漏洞的攻击者可能会导致系统远程拒绝服务。攻击者需要将经过特殊设计的文档发送给目标用户才能利用此漏洞。
	较为活跃样本	Trojan[Downloader]/MSWord.Cryptoload	中	此威胁是一种可以下载恶意代码的木马家族。该家族样本一般为 Word 文档，运行后，在被感染计算机的后台调用系统进程，并向其进程内存空间中写入恶意可执行代码，连接骇客指定远程服务器站点，下载恶意程序并自动调用运行。
		Trojan[Backdoor]/Win32.Slackbot	中	此威胁是一种后门类木马程序。该家族运行后可以连接远程服务器，并允许攻击者对电脑进行恶意操作，包括下载、更新恶意代码，添加、删除系统文件，窃取用户敏感信息等。
		Trojan[Backdoor]/Win32.BO2K	中	此威胁是一种后门类木马程序。该家族隐藏运行在操作系统中，并试图获取系统访问权限，下载和安装其他恶意文件。
		Trojan/Win32.CF	中	此威胁是一种木马类程序。该家族运行后可以在 PC 上执行不被允许的恶意操作。
		Trojan[Proxy]/Win32.Bunit	中	此威胁是一种木马类程序。它作为一种代理，使得黑客可以访问用户电脑，并隐藏其它恶意行为。

实现全面可见性的四种数据

Jay Botelho/ 文 安天技术公益翻译组 / 译

随着企业网络日益混合，当今的 IT 环境比以往更加复杂了。在有线、无线、多平台，多供应商和多云环境中，网络运营（NetOps）团队必须具有端到端的控制。不幸的是，最近的一份报告发现，超过三分之一的网络专家对企业的网络结构缺乏了解。缺乏对每个域的可见性会造成危险的盲点，使 IT 团队无法有效地管理、优化混合网络，并进行故障排除。

实现网络可见性的关键之一是收集正确的数据。目前有几种类型的数据，而对于网络管理任务而言，每种数据类型都有其优缺点。接下来，我们将介绍四种主要的网络数据及其在 NetOps 中的作用。

流数据

流数据（例如 NetFlow、jFlow 和 IPFIX）可以说是常规网络监控的最佳数据源。流数据主要来自交换机或路由器，这些数据使 NetOps 团队能够了解各种协议、往返端口、IP 地址等的详细信息。与其他数据类型相比，流数据的一个主要优点是：NetOps 团队可以简单地从网络上已有的交换机和路由器收集此类数据。

在为网络告警和报告赋能方面，流数据也非常有用。例如，在语音和视频降级或带宽问题的告警方面，流数据至关重要。利用流数据，IT 团队可以确定带宽最高的用户或企业内发生语音和视频性能问题的位置，并进行进一步调查以确定原因。

虽然流数据对于网络监控非常有用，但它并非万能“银弹”。例如，流数据无法为 NetOps 团队提供足够的信息来进行深度安全分析。同样，流数据不够详细，无法用于复杂问题的深入故障排除或监控业务应用程序。

包数据

这是 IT 团队可用的最细粒度的数据类型，最常用于复杂的故障排除。流数据可以解决当今

大约 80%的网络故障排除问题，而其余 20%则需要包数据——其他数据类型无法做到这一点。

数据包通常用于网络管理、应用程序性能监控和安全分析工具。一般来说，包数据在根本原因分析中最为有用。数据包能够为 NetOps 团队提供深入了解每个网络对话的详细信息，使其能够确定问题原因并快速解决问题。数据包在取证分析方面也很重要，能够为 IT 和安全团队赋能，使其能够调查网络犯罪分子何时、如何进入网络，以及一旦获得访问权限后将会做什么。

但是，包数据也有其劣势。首先，此类数据不仅需要更先进的工具，还需要更多的网络专业知识。此外，NetOps 团队必须有权使用解决方案，以便在较长的时间段内正确存储包数据（成本会很高）。拥有较少 IT 资源和专业知识的小型企业，通常认为这些数据包捕获和分析工具遥不可及，转而采用细节较少的流数据。但是，有些解决方案可以简化该流程并使数据包分析更简单。

简单网络管理协议（SNMP）数据

SNMP 是用于监控网络设备的应用程序层协议。幸运的是，几乎所有设备都会生成 SNMP 数据。NetOps 团队不仅能够从 SNMP 收集网络数据，还能够收集网络设备的健康状况信息。例如，通过此类数据，NetOps 团队可以了解某个设备处于启动还是关闭状态，或者处理器的温度是否异常。尽管 SNMP 数据提供的是特定设备的信息，而非有关网络性能的数据，但是对于 NetOps 团队而言，此类数据也是解决可见性难题的关键部分。

与从路由器和交换机自动收集的流数据不同，网络管理解决方案必须定期对每个设备执行 ping 操作以进行更新，从而收集 SNMP 数据。SNMP 不像流数据那样精简，因此其收集成本较高。

应用程序编程接口（API）数据

与上述数据类型相比，API 数据属于不同的类别，但是对于 NetOps 团队的可见性也是至关重要的。API 是构建软件的各种组件之间的一组已定义的通信方法。由于 API 是接口，因此没有任何标准。换句话说，它对于每个设备、软件和用例都是唯一的。有几种不同类型的 API，但是 REST API 最为常见。对 NetOps 团队来说，API 数据的一个最大优势是：应用程序性能管理或确保关键业务应用程序的有效性。

也就是说，API 仅适用于某些应用程序，因此它们非常具体。API 数据确实能够显示某些应用程序的功能，但这并不能使 NetOps 团队了解最终用户对这些应用程序做了（或正在做）什么，因此此类数据有其局限性。

对于 NetOps 团队而言，上述四种数据都非常有用，但它们都不是万能的。因此，许多企业都采用了各种各样的专用网络工具来获取上述所有数据。从工作流程的角度来看，这给生产效率带来了挑战（导致更多的网络盲点）。此外，许可、支持、专门培训等方面的成本也非常高。幸运的是，一些高级网络监控解决方案提供了整合的功能，使 NetOps 团队能够了解每个域的情况，从而更好地管理、优化其混合网络并进行故障排除。不管企业使用的是多个单点解决方案还是统一网络管理方法，为了达到当今混合环境中必需的可见性级别，企业必须确保能够收集、分析这四种网络数据并针对它们采取行动。

原文名称	4 Networking Data Types to Use for Comprehensive Visibility
作者简介	Jay Botelho。Jay Botelho 是 LiveAction 公司工程总监。
原文信息	2019 年 12 月 11 日发布于 Network Computing 原文地址 https://www.networkcomputing.com/networking/4-networking-data-types-use-comprehensive-visibility
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。