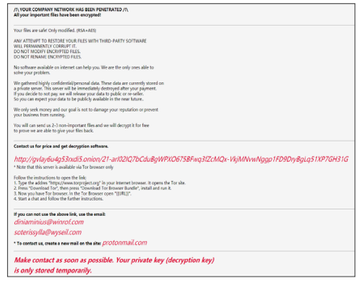
安天智甲有效防护 Krlock 勒索软件新变种

近日，安天 CERT 在梳理网络安全事件时发现了一个名为 Krlock 的勒索软件新变种。该勒索软件隶属于 MedusaLocker 勒索软件家族，最早于 2021 年 8 月被发现，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勒索软件的加密行为。

Krlock 勒索软件运行后，查找并尝试结束 360 安全卫士、诺顿等多个杀软进程，在短时间内完成对计算机上相关文件的加密，在被加密文件的后缀名后追加以“.krlock”命名的后缀。加密完成后，尝试在遍历到的文件夹中创建一个名为“Recovery_Instructions.html”的勒索信，该勒索信具体内容包含了勒索说明、联系方式等。Krlock 勒索软件调用命令行命令防止受害者恢复已加密的文件，具体操作为删除卷影副本、删除本地计算机的备份目录等。



▲Krlock 勒索软件勒索信息

Krlock 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、动态行为鉴定器将文件判定为木马程序。

◆ 概要信息

文件名	krlock.exe
文件类型	BinExecute/Microsoft.EXE[:X86
大小	679 KB
MD5	D1DFE015E405C7D6223785826B730CD8
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[Ransom]/Win32.Ako
判定依据	反病毒引擎

报告地址：https://1.119.163.6/vue/details?hash=D1DFE015E405C7D6223785826B730CD8

◆运行环境

操作系统	内置软件
Win7sp1 x86 旗舰版 service Pack 1	默 认、IE8、Google Chrome、Firefox、Office2013、Flash、FoxitReader、Adobe Reader DC

◆危险行为

行为描述	危险等级

通过文件检测布谷鸟沙箱	★★★★★
堆喷射	★★★★★
疑似勒索软件篡改或加密文件	★★★★★
删除卷影副本	★★★★
在启动时禁用 Windows 错误恢复	★★★★
删除卷影副本	★★★★
搜索文件	★★★★
修改文件后缀名	★★★★
创建互斥量	★★★
禁用权限管理（UAC）	★★★
禁用 UAC 提示	★★★
.....	.....

◆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16日(总第291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

商业窃密木马 Agent Tesla 新型变种分析

概述

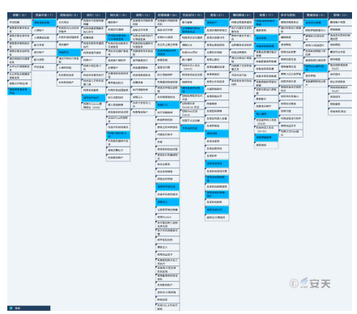
近日，安天 CERT 监测网络安全事件时发现一个商业窃密木马 Agent Tesla 的新型变种。该木马最早于 2014 年在其官方网站进行销售，价格根据选择的功能在几美元到几十美元之间不等。之后该木马转为在地下论坛出售，更新频繁，近期较为活跃，主要通过钓鱼邮件进行传播，邮件附件伪装成与邮件主题相关的内容，诱导受害者点击执行。

安天 CERT 于 2018 年曾发布过该窃密木马家族变种的分析报告。与旧版本对比，新版 Agent Tesla 进行了大量的改造升级。从安全软件的对抗角度来看，新版本运行过程更加隐蔽，采用了多种混淆手段，难以被安全软件检测。增加 Tor 匿名网络回传的功能，使得回传服务器更难以被溯源及破坏，提高了隐蔽性和持久性。窃取的数据内容也大幅增加，包括流行的浏览器、电子邮件和远程连接等软件的数据。由此可见，近年来攻击者的技术水平一直在不断地升级。经验证，安天智甲终端防御系统（简称 IEP）可实现对该窃密木马的查杀与有效防护。

事件对应的 ATT&CK 映射图谱

1. 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

防护建议

针对该窃密木马安天建议企业采取如下防护措施：

1. 企业防护

安装终端防护：安装反病毒软件，建议安装安天智甲终端防御系统；

加强口令强度：避免使用弱口令，建议使用 16 位或更长的密码，包括大小写字母、数字和符号在内的组合，同时避免多个服务器使用相同口令；

部署入侵检测系统（IDS）：部署流量监控类软件或设备，便于对恶意代码的发现与追踪溯源。安天探海威胁检测系统（PTD）以网络流量为检测分析对象，能精准检测出已知海量恶意代码和网络攻击活动，有效发现网络可疑行为、资产和各类未知威胁；

安天服务：若遭受恶意软件攻击，建议及时隔离被攻击主机，并保护现场等待安全工程师对计算机进行排查；安天 7*24 小时服务热线：400-840-9234。

2. 邮件传播防护

接收邮件时要确认发送来源是否可靠，避免打开可疑邮件中的网址和附件；

建议使用沙箱环境执行可疑的文件，在确保安全的情况下再使用主机执行。安天追影威胁分析系统（PTA）采用深度静态分析与沙箱动态加载执行的组合机理，可有效检出分析鉴定各类已知与未知威胁。

经验证，安天智甲终端防御系统（简称 IEP）可实现对该窃密木马的查杀与有效防护。

▲ 安天智甲有效防护

攻击流程

攻击者投放钓鱼邮件，诱导受害者解压并执行邮件附件中的窃密木马。窃密木马执行后，修改注册表以实现自启动，而后窃取浏览器、电子邮件等数据并使用邮箱 ace*****@buynsell.com.pk 将窃取到的信息回传到攻击者的邮箱。

样本分析

1. 样本标签

病毒名称	Trojan[Spy]/Win32.AgentTesla
原始文件名	DTT.exe
MD5	BAFA9BD077C451F845E0ECCA1010607D
处理器架构	Intel 386 or later, and compatibles
文件大小	1.04 MB (1,095,680 字节)
文件格式	BinExecute/Microsoft.EXE[:X86]
时间戳	2021-07-15 13:19:22
数字签名	无
加壳类型	无
编译语言	.NET
VT 首次上传时间	2021-07-15 15:43:49
VT 检测结果	53/70

▲ 二进制可执行文件

2. 多层载荷规避检测

样本使用多层载荷的方式隐藏恶意代码，避免杀软检测。

第一层载荷将实际恶意代码伪装在大量的正常代码中，并使用了较为复杂的混淆手段。在模块的构造函数中加载程序集 XLPgWysCbZyAgPcWJNCUrkSOFDBEA，该程序集中包含多个图片资源，用于后续解密。

小结

本次窃密行动中使用的 Agent Tesla 新型变种在反检测、反调试、反沙箱等部分均进行了升级，使用了多层载荷和多种加密方式，以达到规避检测和干扰分析的目的。

从样本功能的演进来看，该家族窃取的数据内容大幅增加，用户一旦感染，将会泄露大量信息。从安全软件的对抗来看，该家族经过多年的发展，持续进行改进升级，不断尝试采用更加隐蔽的方式执行窃密行为。

（原文链接：https://mp.weixin.qq.com/s/ZCE_BYnmxWReX5r7-3D3XA）

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	BlackMatter 团伙开发出针对 VMware ESXi 的新版本
英文标题	BlackMatter ransomware also targets VMware ESXi servers
作者	Pierluigi Paganini
内容概述	BlackMatter 勒索软件团伙开发了新的 Linux 版本，以扩大目标列表，并危及虚拟化环境。BlackMatter 团伙于 7 月底开始运作，该团伙声称是“Darkside”和“REvil”组织的继承者。和其他勒索软件一样，BlackMatter 也建立了自己的泄露网站，在加密系统之前发布从受害者那里窃取的数据。本周，来 MalwareHunterTeam 的研究人员首先发现了一个用于 BlackMatter 勒索软件团伙的 Linux ELF64 加密器，该加密器旨在针对 VMware ESXi 服务器。
链接地址	https://securityaffairs.co/wordpress/120862/cyber-crime/blackmatter-ransomware-linux-version.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	Microsoft Edge 远程代码执行漏洞（CVE-2021-30590）	高	Microsoft Edge 存在远程代码执行漏洞。由于处理书签中不受信任的 HTML 内容时发生边界错误，使得攻击者可以创建一个特制的网页，诱使受害者打开它，触发基于堆的缓冲区溢出并在目标系统上执行任意代码。
	Linux eBPF 本地提权漏洞（CVE-2021-3490）	高	Linux eBPF 存在本地提权漏洞。由于 eBPF 在内核中存在边界检查错误，使得攻击者可以构造恶意数据，使得越界部分数据具有高执行权限，实现低权限用户转换为 root 用户。
	Microsoft Exchange Server 远程代码执行漏洞（CVE-2021-34473）	高	Microsoft Exchange Server 存在远程代码执行漏洞。由于 Exchange Server 中的输入验证逻辑不正确，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。
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。
	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.Khalesi	中	此威胁是一种具有多种恶意功能的家族木马。该家族样本运行后，会窃取系统账户信息，记录键盘击键信息，下载其他恶意软件。该家族样本通过钓鱼邮件传播，通过添加计划任务持久驻留系统。
	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。

关注凭证泄露问题

拉尔夫·皮萨尼 / 文 安天技术公益翻译组 / 译

去年，供应商 SolarWinds APT 攻击事件影响了 200 多个联邦机构，以及微软和火眼公司，目前还在持续造成破坏。今年，美国最大的燃料管道和东海岸主要供应商 Colonial Pipeline 遭到勒索软件攻击，导致其运营中断了数日。这两起攻击有什么共同点？攻击者都是通过泄露的凭证进入目标网络的。

攻击者利用泄露凭证渗透目标网络并进行横向移动，早已不是什么新鲜事，但是情况越来越糟了。在过去的几年中，我阅读了数百份数据泄露报告，几乎所有报告都涉及凭证泄露。Verizon 在其《2020 年数据泄露调查报告》中指出，“犯罪分子很喜欢凭证，凭证使他们的攻击活动更加容易。”该报告指出，攻击者对凭证的使用“飞速增加”，而对木马、恶意软件和其他攻击策略的依赖则不断下降。根据该报告，超过 80% 的黑客入侵是通过暴力破解凭证，或使用丢失或被盗凭证进行的。

这就引发了一个问题：在凭证泄露已经十分严重的今天，企业为何还是将网络资源放在威胁防御工具、反恶意软件、加密、VPN 和已有十年历史的边界式攻击策略上呢？攻击者的技术复杂度不断提高并不断适应新的工作方式；相比之下，网络安全的进展则慢得多，且永远处于追赶攻击者的状态。

将资源转向检测

泄露的凭证不仅是攻击者进入企业网络并窃取高价值数据的钥匙，也是他们在网络中隐藏的关键策略之一（他们可以访问系统，并在系统之间横向移动，数月甚至数年都不会被发现）。因此，仅使用威胁防御工具已经无法阻止攻击了。企业需要全面、有效的策略来检测、减轻和修复不可避免的（通常是隐藏的）攻击。

网络安全团队和安全运营中心（SOC）需要更加关注凭证，包括凭证在安全事件中的使用方式，以及如何检测和解决凭证泄露情况。在处理来自威胁检测工具的数千个孤立告警方面，SOC 应减少投入的时间，因为这是一种效率低下的策略，更侧重于治疗症状而非疾病本身（疾病通常是凭证泄露）。创建和更新成百上千条严格的关联规则，已经跟不上如今复杂且不断变化的攻击策略了。

全球新冠疫情到网络疫情

在过去的一年中，全球新冠疫情十分严峻。在这种情况下，企业不得不迅速转向“居家办公”的模式，导致网络安全情况变得更糟糕。企业的网络安全边界已经消失了。使用所谓的安全 VPN 没有任何帮助——如果攻击者获取用户的 VPN 登录信息并由此进入企业网络，VPN 无法提供任何保护，攻击者进而可以获得全网访问权限。美国国家安全局于 2020 年 7 月发布了一份网络安全公告，警告称 VPN“容易受到网络扫描、暴力破解和零日漏洞利用攻击”。

2020 年 4 月，美国联邦调查局表示，与新冠疫情爆发之前相比，报告的网络安全攻击事件增加了 400%。同月，《华盛顿邮报》报道称，激进分子窃取了美国国立卫生研究院、世界卫生组织和盖茨基金会的近 25,000 个电子邮件地址和口令。5 月，《连线》杂志报道称，黑客组织 Shiny Hunters 声称窃取了超过 13 个组织包括凭证在内的 2 亿条记录。

窃取凭证并不是一种全新的攻击策略。2019 年 4 月，Dominion Healthcare 发现了近十年前发生的未授权访问攻击。GoDaddy、Twitter、Amtrak 和美国司法部都遭受过基于凭证的攻击。

IT 企业必须对其安全策略进行重大调整，以便为自己配备检测凭证泄露所需的工具和策略。这涉及人员、流程和技术，重点是了解正常用户行为是什么样的，以及 IT 部门如何检测异常行为（表明凭证已被盗）。安全团队还应参考 MITRE ATT&CK 等框架，以学习和理解攻击者的行为和策略。

安全团队越早检测到利用泄露凭证、提权和横向移动攻击，就能越快地阻止这些攻击并在它们导致灾难之前减轻损害。

原文名称	Time to Focus on Compromised Credentials
作者简介	拉尔夫·皮萨尼 （Ralph Pisani），是 Exabeam 公司的总裁。
原文信息	2021 年 7 月 12 日发布于 Dark Reading 原文地址 https://www.darkreading.com/attacks-breaches/time-to-focus-on-compromised-credentials/d/d-id/1341479
摘 要	IT 企业必须对其安全策略进行重大调整，以便为自己配备检测凭证泄露所需的工具和策略。这涉及人员、流程和技术，重点是了解正常用户行为是什么样的，以及 IT 部门如何检测异常行为（表明凭证已被盗）。安全团队还应参考 MITRE ATT&CK 等框架，以学习和理解攻击者的行为和策略。安全团队越早检测到利用泄露凭证、提权和横向移动攻击，就能越快地阻止这些攻击并在它们导致灾难之前减轻损害。
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。