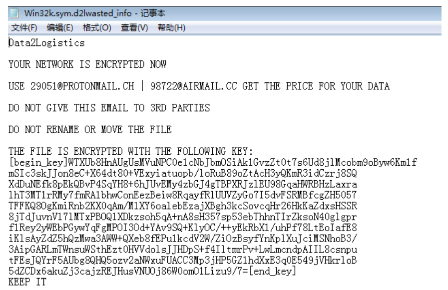
邮箱：antiynews@antiy.cn

安天智甲有效防护 WastedLocker 勒索软件变种



Data2Logistics

YOUR NETWORK IS ENCRYPTED NOW

USE 29051@PROTONMAIL.CH | 98722@AIRMAIL.CC GET THE PRICE FOR YOUR DATA

DO NOT GIVE THIS EMAIL TO 3RD PARTIES

DO NOT RENAME OR MOVE THE FILE

THE FILE IS ENCRYPTED WITH THE FOLLOWING KEY:
[begin_key]WTXUb8HnAUgUsMVuNPC0e1cNbJbm0SiAk1GvzZt0t7s6Ud8jlMcobm9oByw6Kmlf
mSIc3skJJon8eC+X64dt80+VExyiatuopb/1oRuB89oZtAcH3yQKmR3idCzrj8SQ
XdDuNEfk8pEkQBvP4SqYH8+6hJUvEMy4zbGJ4gTBPXRJzlEU98GqaHWRBHzLaxra
lhT3MT1rRMy7fmRA1bhwConEezBeiw8RqayfRlUUVZyGo7I5dvFSRMBfcgZH5057
TFFKQ80gKmiRnb2KX0qAm/M1XY6oalebEzajXBgh3kcSovcqHr26HkKaZdxsHSSR
8jTdJuvnV171MTxPB0Q1XDkzsoh5qA+nA8sH357sp53ebThhnTIrZksoN40glgpr
f1Rey2yWEbPGywYqFgMPOI30d+YAv9SQ+Kly0C/++yEkRbX1/uhPf78LtEoIafE8
iKlsAyZdZ5hQzMwa3AWW+QXeb8fEPulkcdV2W/Zi0zBsyfYnKplXuJciMSNhoB3/
3AipGARLmTWnsuWSthEzt0HVVdolsJJHDpS+f4IltmrPv+LwLmcndpAIIL8csnpu
tFEsJQYrF5AUbg8QHQ5ozv2aNWxuFUACC3Mp3jHP5GZ1hdXxE3q0E549jVHkrloB
5dZCDx6akuZj3cajzREJHusVNU0j86W0om01Lizu9/7=[end_key]
KEEP IT

▲WastedLocker 勒索信

近日，安天 CERT 在梳理网络安全事件时发现一个名为 WastedLocker 勒索软件变种，该勒索软件最早发现于 2020 年 5 月，使用基于 JavaScript 的恶意框架 SocGholish，该框架可跟踪 150 多个伪装成软件更新的受感染网站，一旦攻击者进入了受害者的系统，便会使用 Cobalt Strike 来窃取凭据、提权并横向移动，最后安装执行 WastedLocker 勒索软件。WastedLocker 勒索软件与 Evil Corp 恶意组织有关，主要攻击目标为具有高价值的大型上市公司。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 WastedLocker 勒索软件变种的加密行为。

WastedLocker 勒索软件运行后，会将 System32 中的随机文件创建副本并写入 %AppData% 目录，通过备用数据流（ADS）技术将自身复制到该随机文件中，写入的勒索软件样本可以"寄宿"在该随机文件身上，而在资源管理器中却只能看到"宿主"文件，找不到"寄宿"文件，并且"宿主"文件的大小没有改变，通过这种技术可以达到隐藏自身逃避检测的目的。之后开始加密计算机上的文件，在被加密文件原文件名后追加名为"d2lwasted"的后缀。对于每个加密文件，将创建一个副本文件，并在文件扩展名的末尾附加"_info"的后缀。这些单独的文件是勒索信息，该勒索信内容包含公司 / 目标名称、被加密主机的 RSA 公钥和联系邮箱等。

WastedLocker 勒索软件采用"AES+RSA"加密算法，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、智能学习鉴定器、静态特征检测鉴定器、安全云鉴定器、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	ed0632acb266a4ec3f51dd803c8025bccd654e53c64eb613e203c590897079b3
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	951 KB
MD5	EDBF07EACA4FFF5F2D3F045567A9DC6F
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.Kryptik.ehls
判定依据	反病毒引擎

◆ 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
创建隐藏流文件	★★★

◆常见行为

行为描述	危险等级
加载运行时 DLL	★
壳行为填充导入表	★★
设置文件属性为隐藏	★★
……	……

◆扫描二维码查看完整报告

安天周观察

安天官方微博 安天官方微信

主办：安天 2020 年 8 月 10 日 (总第 242 期) 试行 本期 4 版 微信搜索：antiylab 内部资料 免费交流

安天阶段性完成 B 轮融资

近日，安天阶段性完成 B 轮融资，已到位金额 6 亿元人民币，由龙江基金领投、高科新浚、鲲鹏一创等基金跟投。

微信扫描二维码关注公众号查看原文

推特帐户遭受鱼叉式网络钓鱼攻击

黑客通过误导推特员工以获得访问内部工具的权限，以接管知名帐户并发起比特币骗局。攻击者锁定了130个推特账户，最终从45个推特账户发起攻击，进入了36个收件箱，并下载了7条推特账户的数据。

（**原文链接**：https://threatpost.com/twitter-hack-mobile-spearphishing-scam/157896/）

研究人员发现新的侧信道攻击方式

安全研究人员概述了一种新技术，无论对手与目标服务器之间的网络拥塞如何，基于远程计时的侧信道攻击都可以更加有效。通过网络连接进行的远程定时攻击主要受网络传输时间变化的影响，而后者又取决于任何给定时间点的网络连接负载。但是，由于测量执行密码算法所需的时间对于执行定时攻击至关重要，因此执行时间差异很小。这种新方法被研究人员称为"无时限定时攻击"，利用网络协议的多路复用和应用程序的并发执行，从而使攻击不受网络条件的影响。

（**原文链接**：https://thehackernews.com/2020/07/http2-timing-side-channel-attacks.html）

交易平台 2gether 加密货币被黑客窃取

2gether成立于2017年，在欧元区内提供了一个加密货币交易平台，无需手续费即可进行买卖。在7月31日下午6点，交易平台中的加密货币投资账户价值约120万欧元的加密货币被盗。目前警方正在进行调查，以查找网络攻击者如何获得公司服务器的访问权限。

（**原文链接**：https://www.zdnet.com/article/2gether-crypto-market-platform-hacked-eur1-3m-in-cryptocurrency-stolen/）

Maze 勒索软件团伙泄露 LG 和 Xerox 共计 76G 数据

Maze勒索软件的操纵者经过两次失败的勒索尝试后，今天从国际商业巨头LG和Xerox网络发布了数十GB的内部数据。黑客泄露了他们声称的从LG内部网络中窃取的50.2 GB数据和Xerox的25.8 GB数据。根据上个月Maze团伙共享的屏幕截图，数据似乎包含各种LG产品（例如手机和笔记本电脑）的克隆源固件的源代码。

（**原文链接**：https://www.zdnet.com/article/ransomware-gang-publishes-tens-of-gbs-of-internal-data-from-lg-and-xerox/）

外卖平台 UberEats 用户信息在暗网泄漏

受害者是美国在线食品订购和交付平台UberEats，威胁情报公司的安全研究人员在暗网上发现了该平台的用户记录信息。安全团队在暗网能够发现黑客泄露UberEats的交付合作伙伴和客户的详细信息，公开的记录包括例如登录凭据、姓名、联系电话、旅行详细信息、银行卡详细信息、账户创建日期之类的信息。

（**原文链接**：https://cybleinc.com/2020/08/04/user-records-of-ubereats-leaked-on-darkweb/）

FBI 发布 Windows 7 寿命终止警告

FBI周一向美国私营部门的合作伙伴发送了一份私人行业通知(PIN)，内容涉及在Windows7操作系统今年达到寿命终止(EOL)后继续使用该系统的危险。在企业中继续使用Windows7可能会让网络犯罪分子进入计算机系统。随着时间的推移，由于缺乏安全更新，Windows7变得更容易被利用。

（**原文链接**：https://www.zdnet.com/article/fbi-issues-warning-over-windows-7-end-of-life/）

每周安全事件

类 型	内 容
中文标题	研究人员发现三菱电机工业自动化产品的高危漏洞
英文标题	Hackers Could Target Organizations via Flaws in Mitsubishi Factory Automation Products
作者及单位	Eduard Kovacs
内容概述	研究人员发现三菱电机数十种工业自动化产品存在三个漏洞，可利用这些漏洞进行特权提升，任意代码执行和 DoS 攻击。具体漏洞包括 CVE-2020-14496、CVE-2020-14523、CVE-2020-14521。三菱已经为许多受影响的产品发布了补丁程序，并且还为无法立即安装补丁程序的客户提供了解决方案。
链接地址	https://www.securityweek.com/hackers-could-target-organizations-flaws-mitsubishi-factory-automation-products

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 Windows Graphics 安全漏洞（CVE-2020-1408）	高	当 Windows 字体库不正确地处理经特殊设计的嵌入字体时，存在远程代码执行漏洞。成功利用此漏洞的攻击者可以控制受影响的系统。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 Windows Jet Database Engine 安全漏洞（CVE-2020-1401）	高	当 Windows Jet 数据库引擎不正确地处理内存中的对象时，存在远程代码执行漏洞。成功利用此漏洞的攻击者可以在受害者系统上执行任意代码。攻击者可以通过诱使受害者打开经特殊设计的文件来利用此漏洞。
	Microsoft SharePoint 安全漏洞（CVE-2020-1444）	高	在 Microsoft SharePoint 的邮件消息解析代码中，存在远程代码执行漏洞。若攻击者精心构造邮件，则可触发该漏洞。一旦漏洞被成功利用，攻击者可在系统用户的上下文中运行任意代码。
较为活跃样本家族	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[Backdoor]/Win32.Padodor	中	此威胁是一种后门类木马家族。该家族木马会利用系统漏洞打开后门，为用户电脑带来更多威胁；它同时允许黑客远程进入并控制用户电脑。
	Trojan[Banker]/Win32.Emotet	中	此威胁是一个具有窃取银行账户行为的木马家族。该家族木马在执行后会在后台对进程进行监控，监视登陆银行页面的进程并记录信息，回传攻击者服务器。
	Trojan/Win32.Bayrob	中	此威胁是一种可以窃密类木马家族。该家族样本运行后连接远程服务器，收集用户敏感信息并回传，包括操作系统版本、计算机名、计算机的 IP 地址、关于操作系统和系统设置的信息、MAC 地址及运行服务列表等。
	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。
	Trojan[Spy]/Android.SmForw	中	此威胁是安卓平台上的间谍类木马家族。该家族样本运行后，长久驻留系统，持续监控用户，收集用户系统信息，造成用户隐私泄露。

多重云安全的五个核心原则

克里斯·科拉德 / 文 安天技术公益翻译组 / 译

越来越多的企业开始采用云部署模型，他们面临严峻的云安全挑战。例如，如何以一种既安全又合规的方式快速转型？在向云模型转变的过程中，企业领导者有机会重新考虑如何保护企业。例如，领导者应该摒弃这样的想法：先前的策略和实践可以随时迁移，立即适用于新的云环境。

尽管每个企业的云计算之旅都有其独特的元素，但是他们可以借鉴一些通用的基本原则。这样，他们可以在整个云之旅和跨多重云部署的过程中更好地保护其知识产权、用户和资产。

对于寻求保护多重云部署的企业，可以参考以下五个关键原则。

创建可见性：谁在使用应用和服务，为何使用？

安全团队需要定期了解，企业员工每天使用哪些云应用和服务，以及使用这些应用和服务的目的是什么。在现代技术环境中，新的云服务和新账户不断出现。在安全团队没有意识到的情况下，企业员工可能就启用了云服务和应用。这种不受限制的增长会增加企业环境的复杂性，带来潜在风险。

要想有效防止数据失窃，保护资源免受内外部威胁，企业需要采取一种方法，为系统中运行的所有云服务设立基线。在这方面，云发现应用可以提供帮助。企业应定期将此基线清单与批准的应用清单进行对比，标记并审查这两个清单的所有差异。要想实现这一点，扫描一次是不够的。企业需定期扫描来识别云服务，并将此作为总体云安全计划的一部分。

跨混合和多重云环境集成云安全

云部署可以采取很多不同的方式。例如，某些企业在诸如 IBM Cloud 和 Amazon Web Services（AWS）等“Internet 即服务”（IaaS）平台上，将云作为工作负载运行。某些企业采用基于平台的方法，将云作为容器化的工作负载运行。还有的企业将云作为提供“软件即服务”的专用应用运行。无论企业的用例如何，关键是采用一种“万能”方法来监控其云安全性和合规性。

借助内置的安全情报和分析工具，企业可以从端点、用户、应用程序、网络和用户活动中收集数据。此后，企业可以将业务情境和规则应用于这些数据，以便更轻松地了解其环境中正在发生的情况。他们不必为来自不同系统的不同事件提供多个告警，而是可以将这些事件聚合，归类为单个潜在事件。这样一来，需要分类的事件数量就减少了，企业可以节省在这方面花费的时间，将节省下来的时间用于响应。

减轻内部人员威胁

除了发现和检测云应用之外，企业的云安全计划还应包括活跃用户行为分析。云环境的大多数潜在威胁可能来自企业内部。最近的一项研究发现，在数据泄露事件中，内部人员威胁占 60%。无论用户的行为是有意的（如数据窃取和公司资产滥用）还是无意的（例如点击网络钓鱼邮件或下载恶意软件），上述结论均适用。无论怎样，识别和跟踪所有云部署中的异常行为都是关键所在。

除了保护用户，领导者还需考虑企业的服务或机器账户；定期清查这些账户是怎样使用的、它们访问的内容以及登录地点。通过建立行为基线（无论是好是坏），企业可以增强其保护资产和用户的能力。

快速解决问题

当发现问题时，企业应进行紧急响应。此外，响应的准确性至关重要。企业需要掌握所有相关数据，并具备执行精心策划的计划的能力。使用不同的工具，跨多重云管理不同的策略和响应计划是没有意义的，企业需要部署统一的策略。

妥善响应意味着，通过预设方案和标准，进行经过全面测试的自动化响应。如果企业的安全团队擅长响应，就可以帮助员工在必要时应对威胁。安全团队需要针对威胁进行量身定制的知识和数据共享，从而掌握协作和计划能力。安全领导者必须确保，企业不仅可以满足合规性要求，还可以证明并报告其合规性。

使用 AI 技术增强多重云安全计划

当今的安全团队面临着一系列挑战，例如跨不同云部署的攻击数量、种类和复杂性不断增加。鉴于企业很难聘请和留住有经验的云安全分析师，这些挑战会进一步加剧。安全技能差距，再加上攻击数量和多样性不断增加，有时会导致告警过载、攻击长期驻留、无法解决威胁和 / 或分析师疲乏等状况。

借助 AI 的力量，企业可以消除很多噪音，查明以下问题：

- 到底发生了什么?
- 受到什么影响?
- 应该怎么办?

采用 AI 技术有很多好处，包括快速对比案例之间的数据，根据最重要和最需要关注的内容筛选优先级等。AI 技术还可以帮助企业加速新员工培训和入门，缩短初级分析师成长为中级或高级分析师的时间。

企业是否准备好迎接云未来?

未来，云部署对于企业的业务仍然至关重要。跨多个单点解决方案管理信息安全可能无法满足要求，并引入潜在的监控盲点。首选的、行之有效的云安全方法是以未来的云应用为中心，部署统一的安全情报、分析和响应计划。

原文名称	5 Core Tenets for Effective Multicloud Security
作者简介	克里斯·科拉德（Chris Collard）。克里斯·科拉德是一位信息安全专家，在管理信息系统和服务方面拥有超过 15 年的经验。
原文信息	2020 年 7 月 24 日发布于 Security Intelligence 原文地址 https://securityintelligence.com/posts/securing-multicloud-deployment/
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。