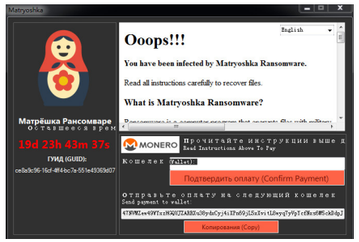
安天智甲有效防护 Matryoshka 勒索软件

近日，安天 CERT 在梳理网络安全事件时发现了一个名为 Matryoshka 的勒索软件。该勒索软件最早于 2021 年 5 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 Matryoshka 勒索软件的加密行为。

Matryoshka 勒索软件运行后，会生成注册表项 HLM\SOFTWARE\Matryoshka，并将随机生成的 GUID 和首次运行时间记录键 guid 和 clock 中，随后采用 AES-256 加密算法对用户目录、%APPDATA%、%PROGRAMFILES%、%PROGRAMFILES(x86)% 目录下常见后缀的文本、文档、图片、音频、视频、数据库、源代码等格式的文件进行加密，其中所使用的 32 位密钥 Key 和 16 位向量 IV 均为随机生成，被加密的文件会在原文件名后追加后缀 ".matryoshka"。加密完成后会弹出窗口展示勒索信，要求受害者向指定钱包地址支付价值 75 美元的门罗币以解密文件。该勒索软件没有回传或记录密钥的功能，即使受害者按要求支付赎金也无法获得密钥、恢复文件，但因其没有删除系统卷影，受害者可尝试通过卷影恢复数据。



▲Matryoshka 勒索软件勒索信

Matryoshka 勒索软件采用“AES-256”加密文件，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、安全云鉴定器、字符串分析鉴定器、聚类分析鉴定器、反病毒引擎鉴定器、动态（Win7sp1 x86）鉴定器、动态（WinXP）鉴定器、文件相似分析鉴定器、信标检测鉴定器、智能学习鉴定器、静态特征检测鉴定器、动态（Win7 x86）鉴定器等鉴定分析。

最终依据 BD 静态分析鉴定器将文件判定为木马程序。

◆概要信息

文件名	61fccc142e2bbf498885bb6e42bae62c
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	179 KB
MD5	61FCCC142E2BBF498885BB6E42BAE62C
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[HEUR]/Win32.Ransom
判定依据	BD 静态分析

报告地址：https://1.119.163.6/vue/details?hash=61FCCC142E2BBF498885BB6E42BAE62C

◆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
搜索文件	★★★★
在系统目录创建文件	★★★
映射内存方式注入	★★★
通过标记进程可执行堆绕过 DEP	★★★★★
创建互斥量	★★★

◆常见行为

行为描述	危险等级
检测自身是否被调试	★★
镜像劫持	★★
.....	.....

◆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 05 月 31 日 (总第 280 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

回眸五年，转型之变

2016 年 5 月 25 日，习近平总书记视察了安天，安天负责人肖新光向总书记汇报了安天反病毒引擎核心技术研发、发现分析溯源外方网络攻击情况，以及为国家重点型号任务提供的网络安全保障工作。在听取了汇报后，习近平总书记对安天人说“你们也是国家队，虽然你们是民营企业。”

▲ 2016 年 5 月 25 日，习近平总书记视察安天

带着总书记的期望和嘱托，安天人开启了新的征程。

明确企业定位，开启产品化征程

2016 年，正是安天酝酿全面的业务转型之时。安天创业的前十年，以安天实验室模式尝试了民间研发机构创新探索的独有道路，2010 年起，安天以反病毒引擎授权的独有商业模式开始了企业转型，安天高速引擎适配网络安全设备的特点和移动威胁检测能力对国际知名厂商的快速超越，支撑安天实现了引擎技术授权对多个发达国家厂商的出口。AVL SDK 反病毒引擎的 LOGO 成为产品具有可靠反病毒能力的标志，安天针对“震网”、“火焰”、“毒曲”等攻击样本的专业分析，也受到国内外同业的关注和称赞。但 2013 年后，受到网络空间国际大气候的影响，安天传统引擎授权业务客户在海外几乎丧失殆尽，屡次尝试突围无果。而与此同时，APT 威胁挑战日趋浮出水面，传统合规产品难以应对。依托先进引擎和威胁对抗能力，安天正式酝酿向政企市场转型。安天人将这次转型，称为第三次创业。

安天引擎关口前移，形成国家安全能力基石

反病毒引擎是安天的技术创新起点和核心能力基石，反病毒引擎授权也是安天长期的业务模式。安天在推动政企市场业务转型的同时，持续投入、坚持深化安全引擎的基础能力。五年来，安天持续在核心技术自主创新上不断深化，目前安天引擎的解析深度等关键指标，渐进超越了国外主流厂商。安天反病毒引擎针对海量已知威胁精准检测能力是安天的重要技术特点。安天引擎可以精准检测命名 8 个基本分类、超过 6 万种家族、超过 1500 多万变种，监测能力覆盖百亿样本空间，助力安天全线产品和安天合作伙伴实现精准威胁辨识。结合安天知识赋能，可以针对攻击载荷输出 74 种核心恶意型行为、117 种恶意代码运行平台、载体格式和环境信息，对载荷进行杀伤链维度能力评价，输出 ATT&CK 威胁框架 171 个攻击技术标签，覆盖率 64.29%。并在工信部支持下，将安全引擎能力向工业网络基础设施延展。安天正在规划安全引擎加速芯片，并已经研发了 FPGA 的原型。（原文链接：https://mp.weixin.qq.com/s/v7KLHrmqw81Y8--Z_V20Dw）

扫描右侧二维码阅读全文

安天集团召开《525 纪念习总书记视察安天五周年暨专家劳模讲党课》大会

5 月 25 日上午，安天科技集团在哈尔滨召开了《纪念习总书记视察安天五周年暨专家劳模讲党课》大会，大会邀请了中国工程院院士秦裕琨，原国防大学研究员徐纬地教授，全国劳动模范、三八红旗手、党的十九大代表荀笑红劳模为安天全体员工上了一堂别开生面的特殊党课。三位主讲嘉宾，分别从自身成长经历、科研创新历程、平凡岗位无私奉献和对国内国际形势研判等多个维度，展示了在各自岗位上体现出的共产党员精神内核和思想境界。报告内容激励鼓舞着全体安天人，牢记总书记“你们也是国家队，虽然你们是民营企业”的嘱托，践行“国家队”的光荣使命。安天集团

▲《纪念习总书记视察安天五周年暨专家劳模讲党课》大会现场

北京、上海、武汉、成都、深圳等地研发中心和各地办事处员工通过线上直播的方式一同听课。

三位主讲嘉宾的报告之后，安天集团党委书记、安天创始人、董事长肖新光回顾了总书记对安天的视察，并结合三位主讲嘉宾的精彩报告就安天企业文化、价值观和历史使命进行了宣贯。号召安天全体共产党员干事创业敢担当，带动和激励全体员工共同拼搏攻坚，站在网络安全威胁对抗的前沿，用过硬的产品、服务和专业技能，提升客户安全获得感，有力支撑国家网络空间国防建设和国家安全能力塑造。（原文链接：https://mp.weixin.qq.com/s/_QhR30MieyLAaEF3FzRKMw）

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	CNCERT 发布 2020 年我国互联网网络安全态势综述报告
英文标题	无
作者	国家互联网应急中心 CNCERT
内容概述	2021 年 5 月 26 日，国家互联网应急中心（CNCERT）编写的《2020 年我国互联网网络安全态势综述》报告（以下简称“2020 年态势报告”）正式发布。为全面反映我国网络安全的整体态势，CNCERT 自 2010 年以来，每年发布前一年度网络安全态势情况综述，至今已连续发布 12 年，对我国党政机关、行业企业及社会了解我国网络安全形势，提高网络安全意识，做好网络安全工作提供了有力参考。2020 年态势报告以 CNCERT 宏观网络安全监测数据与工作实践为基础，综合各类安全威胁、事件信息，网络安全事件应急处置以及网络安全威胁治理实践等内容。
链接地址	https://mp.weixin.qq.com/s/a2nFajrBk3bxCynfC6hdQQ

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 Visual Studio Code 远程代码执行漏洞（CVE-2021-31214）	高	Microsoft Visual Studio Code 存在远程代码执行漏洞。由于该应用中的输入验证代码逻辑不正确，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。
	Microsoft Office Graphics 远程代码执行漏洞（CVE-2021-31180）	高	Microsoft Office Graphics 存在远程代码执行漏洞。由于该应用图形组件中输入验证不正确，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。
	Microsoft Exchange Server 远程代码执行漏洞（CVE-2021-31198）	高	Microsoft Exchange Server 存在远程代码执行漏洞。由于 Microsoft Exchange Server 中的输入验证不正确，使得攻击者可以在目标系统上执行任意代码。
较为活跃样本家族	Trojan[Backdoor]/Win32.Padodor	中	此威胁是一种后门类木马家族。该家族样本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[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/Win32.Blamon	中	此威胁是一种可以窃密类木马家族。该家族木马运行后会窃取用户账户信息，记录键盘击键等，造成用户敏感信息泄露。
	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。
	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[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。

改善补丁管理的五项措施

胡安·帕勃罗·佩雷斯·埃切戈延 / 文 安天技术公益翻译组 / 译

补丁管理的问题已困扰 IT 和安全团队多年。这些团队每个月都要耗费大量精力来处理其技术堆栈中各供应商发布的大量补丁。这并不是一个小问题。根据 Ponemon Institute 的报告，超过 40% 的 IT 和安全人员表示，由于存在未修复的漏洞，他们在过去两年中遭受了数据泄露事件。

为了更好地处理不断涌现的补丁，企业首先要解决其面临的一些问题。

最严重的问题

每个供应商、平台和应用程序都有自己的补丁管理方法。以 SAP 为例，其补丁管理可分为两类：自动管理和手动管理。

自动补丁管理不需要重启系统，这意味着 IT 团队可以在不中断业务运营的情况下将补丁投入生产过程中。手动补丁管理需要重启系统，这类补丁通常难以部署，需要 IT 团队将补丁与维护窗口同步，这可能需要花费数周甚至数月的时间。此外，IT 团队还需要将这些补丁添加到开发、质量保证和生产环境中，这会导致花费更多的时间。但是黑客可不会等他们打完补丁。

最近的一项研究表明，一些黑客在供应商发布补丁后的 72 小时内，就攻击了存在漏洞的平台。因此，IT 团队需要快速行动，但是他们面临严重的安全人员短缺问题。虽说某些关键业务应用拥有专门的团队（例如 SAP 和 BASIS 管理员），但是许多应用程序的安全问题是由时间本就很紧张的 IT 和安全人员处理的。

每个月都会有数百个补丁被发布。面对如此大量的补丁，IT 团队不可避免地会忽视一些补丁。对于使用过时方法（如电子表格和电子邮件）来跟踪补丁的团队而言，尤其如此。

改善补丁管理的五项措施

IT 团队应如何改善补丁管理呢？他们可以采取下述五项措施，来推动调整并建立完善的补丁管理流程。

这些措施包括利用自动化技术、精简工作流程、采用高级分析等。这些措施可以减轻企业补丁管理问题，对安全人员提供支持，并提升企业的整体安全状况。

1. 了解补丁问题并获得支持。补丁管理是一个团队项目。IT 和安全团队需要了解企业中所有的应用程序、每个系统的重要性，以及由谁来管理每个供应商的补丁更新等问题。

鉴于企业的安全预算不断收紧，IT 和安全团队应向领导层展示不断增长的、复杂的应用程序网络和补丁管理流程，以便获得财务和人力支持，这一点至关重要。

2. 实现自动化。企业应考虑投资于第三方解决方案，以取代电子表格和手动跟踪，从而实现公司应用程序全景的自动扫描。这些解决方案可以汇总未打补丁的漏洞，凸显高优先级的补丁，从而将风险控制在可管理的水平之内。精明的公司还会考虑采用与自动化解决方案集成的工作流方案，以精简漏洞修复流程。

3. 实施补充控制措施。企业无法对所有安全补丁都迅速做出响应。因此，企业应实施补充控制措施，以节省在补丁优先级分类、部署和测试方面花费的时间。补充控制措施有多种类型，最常见的一种是：实现实时可见性，以评估安全漏洞是否已被利用。

4. 分析关键趋势。在自动化技术的支持下，企业不仅可以识别和修复漏洞，还可以进行趋势分析。部署关键补丁之后，安全团队可以快速生成报告，向领导层介绍企业还有哪些未打补丁的漏洞。然后，安全团队可以确定公司愿意接受的风险水平。

5. 建立一个持续的过程。各公司之间都会存在差异，补丁管理流程能够反映出这些差异，包括使用的工具数量，愿意接受的风险水平，以及如何应用补丁等等。然而，各公司也有共同点，即补丁管理是一个持续的过程。开发适用于自身的补丁管理流程、及时了解周二补丁日的最新消息，不忽视旧的漏洞等等，这些都是很重要的。

自动化技术有助于精简跟踪和应用补丁的繁重工作，这样一来，安全团队就可以将节省下来的时间用于管理边缘案例和更高级的问题。随着补丁的不断涌现，企业可以采取上述五项措施来规划更好的补丁管理路线。

原文名称	Why is patch management so difficult to master?
作者简介	胡安 · 帕勃罗 · 佩雷斯 · 埃切戈延 （Juan Pablo Perez-Etchegoyen），Onapsis 公司的首席技术官。
原文信息	2021 年 5 月 26 日发布于 Help Net Security 原文地址 https://www.helpnetsecurity.com/2021/05/26/master-patch-management-process/
摘 要	IT 团队应如何改善补丁管理呢？他们可以采取本文所述五项措施，来推动调整并建立完善的补丁管理流程。这些措施包括利用自动化技术、精简工作流程、采用高级分析等。这些措施可以减轻企业补丁管理问题，对安全人员提供支持，并提升企业的整体安全状况。
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。