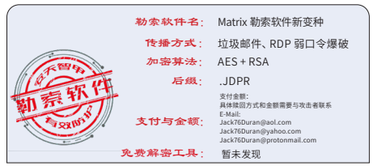
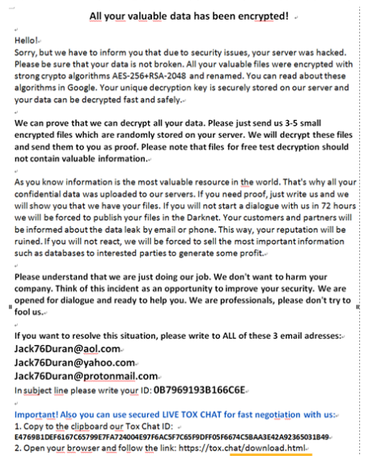
安天智甲有效防护 Matrix 勒索软件新变种



近日，安天 CERT 在梳理网络安全事件时发现了 Matrix 勒索软件 JDPR 变种。该勒索软件变种最早于 2021 年 3 月被发现，主要通过垃圾邮件、RDP 弱口令爆破进行传播。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 Matrix 勒索软件变种的加密行为。

Matrix 勒索软件 JDPR 变种使用 Delphi 编写，运行后会获主机信息并发送到远程 C2，然后会创建计划任务，每 5 分钟删除卷影并禁用 windows 的自动修复功能，防止受害者通过系统备份恢复数据。该变种会扫描局域网内主机，并加密其共享目录中的文件，然后遍历本地磁盘文件并使用 AES 对称加密算法进行加密，然后用硬编码的 RSA 公钥对 AES 密钥进行加密，加密后的文件后缀为 .JDPR。文件加密完成后，会在本地生成相应的勒索信息文件 JDPR_README.rtf。


All your valuable data has been encrypted!

Hello!

Sorry, but we have to inform you that due to security issues, your server was hacked. Please be sure that your data is not broken. All your valuable files were encrypted with strong crypto algorithms AES-256+RSA-2048 and renamed. You can read about these algorithms in Google. Your unique decryption key is securely stored on our server and your data can be decrypted fast and safely.

We can prove that we can decrypt all your data. Please just send us 3-5 small encrypted files which are randomly stored on your server. We will decrypt these files and send them to you as proof. Please note that files for free test decryption should not contain valuable information.

As you know information is the most valuable resource in the world. That's why all your confidential data was uploaded to our servers. If you need proof, just write us and we will show you that we have your files. If you will not start a dialogue with us in 72 hours we will be forced to publish your files in the Darknet. Your customers and partners will be informed about the data leak by email or phone. This way, your reputation will be ruined. If you will not react, we will be forced to sell the most important information such as databases to interested parties to generate some profit.

Please understand that we are just doing our job. We don't want to harm your company. Think of this incident as an opportunity to improve your security. We are opened for dialogue and ready to help you. We are professionals, please don't try to fool us.

If you want to resolve this situation, please write to ALL of these 3 email adresses:
Jack76Duran@aol.com
Jack76Duran@yahoo.com
Jack76Duran@protonmail.com
In subject line please write your ID: 0B7969193B166C6E

Important! Also you can use secured LIVE TOX CHAT for fast negotiation with us:
1. Copy to the clipboard our Tox Chat ID:
E4769B1DEF6167C65799E7FA724004E97F6AC5F7C65F9DFF05F6674C5BAA3E42A92365031B49
2. Open your browser and follow the link: https://tox.chat/download.html

▲Matrix 勒索软件 JDPR 变种勒索信

Matrix 勒索软件新变种采用“AES-256 + RSA-2048”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 、聚类分析鉴定器、反病毒引擎鉴定器、动态（Win XP）鉴定器、动态（Win7 x86）鉴定器、字符串分析鉴定器、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 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	224ce0605b6840d7953729cee972f9e79198cb0d45a2cd3f16198444f6d2f914
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	1.28 MB
MD5	2C52F3918B636736BDF0022C64115B26
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[Ransom]/Win32.Gansom
判定依据	反病毒引擎

报告地址：https://1.119.163.6/vue/details?hash=2C52F3918B636736BDF0022C64115B26

◆常见行为

行为描述	危险等级
哈希算法	★
Crypt algorithm	★
加 / 解密相关 API	★
异常处理	★
线程操作函数	★
进程 / 线程是否处于调试状态	★
创建进程	★
枚举进程	★
设备、资源共享 API	★
socket 通信	★
DNS 通信	★
IPV4 地址	★
操作系统信息	★
同步机制	★
权限操作类相关函数	★
内存堆操作	★
虚拟内存调权	★
DLL 操作	★
文件操作函数	★
.....	.....

◆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 04 月 06 日 (总第 272 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

第九届 XDef 安全峰会即将召开
安天将主办“高级威胁（APT）分析”论坛

全国网络与信息安全防护峰会由公安部网络安全保卫局、国家计算机网络应急技术处理协调中心（CNCNERT/CC）、教育部高等学校网络空间安全专业教学指导委员会指导，空天信息安全与可信计算教育部重点实验室（武汉大学）主办，国家网络安全人才与创新基地、武汉大学国家网络安全学院承办。2021 年第九届全国网络与信息安全防护峰会 (XDef2021) 将于 4 月 16 日 -17 日在湖北武汉东西湖华美达酒店盛大召开！

安天即将主办“高级威胁 (APT) 分析”论坛。敬请关注！

论坛介绍：APT 攻击拥有严密的规模建制，庞大的支撑工程体系，掌控体系化的攻击装备和攻击资源，可以进行最为隐蔽和致命的网络攻击，关系到国家关键信息基础设施和国防安全。解读复杂的攻击行动，并驱动防御的改善，需要有更理想的结构化方法。高级威胁分析论坛将关注高级威胁的分析、发现技术，探讨攻击者的技巧、意图和路径持续跟踪和发现方法，分享用户侧的防御改善和产品能力的更新实践经验等。

演讲嘉宾和议题介绍：

演讲嘉宾	议题
安天应急响应中心高级威胁情报分析师	南亚“幼象”组织的前世今生
广东云智安信科技有限公司高级研究员王健	一次 APT 攻击事件的溯源与背景研判
神州网云 (北京) 信息技术有限公司 CEO 宋超	网络威胁大数据协同共享实践分析
中国科学院信息工程研究所网络安全防护技术北京市重点实验室总工刘玉岭	面向实战的网络安全态势感知：研究进展与技术趋势
广州凌晨网络科技有限公司 CTO 许亮	来自移动侧的 APT 风险
移动安全领域专家	移动终端高级威胁运营体系设计与狩猎成果

工业巨头霍尼韦尔部分 IT 系统遭恶意软件攻击

工业巨头霍尼韦尔（Honeywell）周二透露，其部分 IT 系统由于恶意软件攻击而中断。该公司表示，入侵是“最近”检测到的，只有“有限数量”的 IT 系统受到干扰。对该事件的调查正在进行中，但霍尼韦尔表示，迄今为止没有发现任何证据表明攻击者设法从存储客户信息的系统中窃取数据。该公司表示：“目前，我们预计这起事件不会对霍尼韦尔造成实质性影响。公司迅速采取措施解决这一事件，包括与微软合作评估和补救。此后，我们的系统已经得到保护，我们确定了入侵点，并且所有未经授权的访问都已被撤销。”

（原文链接：https://www.securityweek.com/honeywell-says-malware-disrupted-it-systems）

WordPress 插件 Ivory Search 存在反射型 XSS 漏洞

2021 年 3 月 28 日，Astra 安全威胁情报小组披露了 Ivory Search 中的一个漏洞，Ivory Search 是安装在 6 万个网站上的 WordPress 搜索插件。攻击者可以利用此安全漏洞对受害者的网站执行恶意操作。由 Jinson Varghese 领导的威胁情报团队最初于 2021 年 3 月 28 日联系了 Ivory Search 插件开发者，并披露了全部细节。开发人员于 2021 年 3 月 29 日做出回应，确认了该漏洞及其影响。2021 年 3 月 30 日发布了补丁。这是一个中等严重程度的反射型 XSS 漏洞，影响 Ivory Search 插件 4.6.0 及以下版本。

（原文链接：https://www.getastra.com/blog/911/plugin-exploit/reflected-xss-vulnerability-in-ivory-search-wp-plugin/）

每周安全事件

类 型	内 容
中文标题	PHP 的 Git 服务器遭到黑客攻击代码库被篡改
英文标题	PHP's Git server hacked to add backdoors to PHP source code
作者	Ax Sharma
内容概述	在最新的软件供应链攻击中，官方 PHP Git 存储库遭到黑客攻击，代码库被篡改。3 月 28 日，两个恶意提交被推送到 PHP 团队在其 git.php.net 服务器上维护的 php-src Git 存储库中。威胁参与者已经对这些提交进行了签名，就好像这些是由知名 PHP 开发人员和维护人员 Rasmus Lerdorf 和 Nikita Popov 所做的一样。尽管针对该事件的调查正在进行中，但 PHP 维护人员表示，这一恶意活动的根源是 Git .php.net 服务器，而不是个人的 Git 帐户。作为预防措施，PHP 维护人员决定将官方 PHP 源代码库迁移到 GitHub。
链接地址	https://www.bleepingcomputer.com/news/security/phps-git-server-hacked-to-add-backdoors-to-php-source-code/

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 Internet Explorer 安全漏洞（CVE-2021-26411）	高	Microsoft Internet Explorer 存在远程代码执行漏洞。由于该应用处理“.mht”文件是出现内存边界错误，使得攻击者可以通过诱骗受害者访问特制网页，触发双重释放错误并在目标系统上执行任意代码。
	Microsoft Visual Studio Code 安全漏洞（CVE-2021-27084）	高	Microsoft Visual Studio Code 存在远程代码执行漏洞。由于该应用的 Java Extension Pack 中的输入验证存在缺陷，使得攻击者可以发送特制请求并在目标系统上执行任意代码。
	Microsoft Office 安全漏洞（CVE-2021-24108）	高	Microsoft Office 存在远程代码执行漏洞。由于该应用中的输入验证存在缺陷，使得攻击者可以发送特制请求并在目标系统上执行任意代码。
较为活跃样本家族	Trojan/Win32.Vilsel	中	此威胁是一种窃密类木马家族。该家族木马通过垃圾邮件或恶意网站进行传播。该家族木马感染用户电脑后，会为黑客建立远程连接以控制用户电脑，窃取用户敏感信息（账号和密码等），同时会下载并运行其它恶意程序。
	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]/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/Win32.Injuke	中	此威胁是一种可以窃取密码信息的木马类程序。该家族的样本运行后会窃取用户账户信息，记录键盘击键等。
	Trojan[Backdoor]/Win32.Delf	中	此威胁是一种后门类木马家族。该家族是通过开发语言 Delphi 来命名的。该家族样本运行后，会在被感染的电脑中打开后门，黑客利用后门窃取用户的隐私信息。
	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。

不确定时期企业需要数字弹性

斯科特·李 / 文 安天技术公益翻译组 / 译

在当今的业务运营中，数字化技术扮演着关键的角色，IT 领导者比任何人都了解这一点。新冠疫情促使企业快速转向了远程和混合办公模式。对他们来说，有效和可访问的数字化工作场所已经成为一项“必需品”。在这种情况下，企业迫切需要建立数字化弹性，IT 团队应在这方面发挥领导作用，帮助企业在新办公模式下获得成功。

数字化弹性是什么?

对于任何敏捷企业而言，数字化弹性都是一项有价值的长期需求。数字化弹性不仅是指对危机的响应，还指企业具有发展和适应时代的工具，能够在瞬息万变的环境中生存和成长。举例来说，疫情期间，很多企业迅速推出帮助用户订购食品杂货或进行虚拟会面的应用程序。

对于大多数知识型企业而言，向数字化办公的全面转变，要求 IT 团队承担起实现业务连续性和企业生存的责任。他们应采用数字化的方法，推动企业进行主动、连续的规划，使员工的工作与快速变化的战略保持一致，并获得持续的反馈，为企业在危机时期的快速适应提供指导。

那么，IT 团队需要哪些数字化工具来实现这种敏捷的战略规划、远程工作调整和跨职能协同呢?

不稳定时期的规划

我们首先要考虑战略规划。在当今瞬息万变的世界中，传统的战略规划方法过于缓慢且缺乏灵活性。年度的计划和战略制定无法跟上战略目标的变化，会导致员工工作与战略目标脱节。

企业需要更快地进行规划和适应，以响应快速变化的需求和市场状况。如果企业能够随着外部环境的变化，及时调整并提出有效的战略计划，那么其战略计划就是灵活的。只有当领导者能够实时了解整个企业中的工作，并据此制定决策时，才能实现这种计划敏捷性。

通过工作管理应用程序实现可见性

实现可见性的一种方法是进行工作管理。工作管理应用程序能够提供中央记录系统，记录企业中正在进行的所有工作，每位员工都可以查看与每项工作相关的目标、计划、项目进度、批准和沟通的进度。领导者可以访问这些数据以制度敏捷的决策，而员工可以跟踪工作进度并了解其工作能是否符合公司的战略目标。

另一种方法是使用场景规划软件。场景规划软件可以帮助领导者快速评估不同选择或行动对企业工作的影响。领导者可以在规划阶段比较各种方案，以选择最佳行动，实现公司的战略目标。

使远程工作符合企业目标

其次，企业要确保所有员工的工作都与其战略目标保持一致——这要从企业查看工作（活动）的方式开始考虑。如果员工是广泛分散的，则管理工作尤其困难。无法有效管理员工工作的企业，需重新考虑管理方法。

企业应将工作视为战略性的“第一层”资产，对其采取与其他第一层资产（例如财务、人力资源和销售）相同的行政管理和监督。将工作视为战略资产，能够确保合适的人在正确的时间做正确的事，从而确保所有工作都与企业的目标保持一致。这样一来，企业能够更有效地组织项目和团队来构建跨职能部门，而非仅仅构建与职能相关的“孤岛”。远程工作中可用的协同技术，能够使各地的员工与任何站点或团队中的其他人一起工作，有助于这种跨学科实践的实现。

工作管理应用程序支持第一层的工作方式，能够跨多个团队集中管理项目，并允许员工根据企业目标协调工作。远程办公的员工，非常愿意看到自己的工作为公司的成功做出贡献。

IT 团队应在瞬息万变的世界中提供弹性

在疫情后的恢复阶段，IT 团队应帮助企业应对持续的不确定性和不可预测性。在这样一个动荡的环境中，企业的数字化弹性对于其规划、编排、衡量、管理和确定活动优先级的能力至关重要。IT 团队应了解其数字化技术及实施解决方案的能力，以协调远程办公员工的工作并实现协同。

虽说数字化弹性具有从实现基本连接到保护基础架构等诸多要素，但是工作管理应用程序具有特殊的价值。这类应用程序能够将各团队使用的技术关联起来，为整个企业的工作提供中央记录系统。通过这类应用程序，远程办公的员工可以了解正在进行的工作、重要的工作以及即将处理的工作。此外，它还能够为领导者提供正确的工作可见性，以便其查看哪些工作进展顺利，哪些工作需要付出更大的精力，以实现预期的结果。

原文名称	Business Survival in Uncertain Times Requires Digital Resilience
作者简介	斯科特·李（Scott Lee），是 Workfront 公司的产品管理主管。
原文信息	2021 年 03 月 30 日发布于 Network Computing 原文地址 https://www.networkcomputing.com/data-centers/business-survival-uncertain-times-requires-digital-resilience
摘 要	对于任何敏捷企业而言，数字化弹性都是一项有价值的长期需求。数字化弹性不仅是指对危机的响应，还指企业具有发展和适应时代的工具，能够在瞬息万变的环境中生存和成长。IT 团队应采用数字化的方法，推动企业进行主动、连续的规划，使员工的工作与快速变化的战略保持一致，并获得持续的反馈，为企业在危机时期的快速适应提供指导。
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。