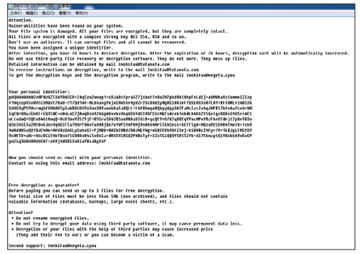
安天智甲有效防护 Imshifau 勒索软件

勒索软件名：Imshifau 勒索软件
传播方式：垃圾邮件
加密算法：AES+RSA
后缀：.imshifau
支付金额：
支付与金额：需通过邮箱与攻击者联系获悉
联系方式：
Imshifau@tutanota.com
Imshifau@vegeta.cyou
免费解密工具：暂未发现

近日，安天CERT在梳理网络安全事件时发现了一个名为Imshifau的勒索软件，最早于2021年7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。

Imshifau 勒索软件运行后，复制自身程序到%Appdata%目录下，在注册表路径“HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce”下添加启动项，以实现开机自启动。在短时间内完成对计算机上相关文件的加密，将被加密文件的文件名替换为随机生成的字符串并追加以“.imshifau”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“INFO OF DECRYPT.TXT”的勒索信，该勒索信具体内容包含了勒索说明、联系方式等。为了诱导受害者尽快缴纳赎金，勒索信中强调了在加密的76小时后仍未付款，将会自动增加赎金金额。



▲Imshifau 勒索软件勒索信息

Imshifau 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、反病毒引擎鉴定器将文件判定为木马程序。

◆概要信息

文件名	Imshifau.exe
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	250 KB
MD5	CDAF852A6A3F607C20CBE9DEACB79649
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[Ransom]/Win32.Pulobe
判定依据	反病毒引擎

报告地址：https://1.119.163.6/vue/details?hash=CDAF852A6A3F607C20CBE9DEACB79649

◆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、Adobe Reader

◆危险行为

行为描述	危险等级
执行HTML应用程序	★★★★★
检测虚拟机	★★★★★
疑似勒索软件篡改或加密文件	★★★★★
搜索文件	★★★★
删除自身	★★★★
修改文件后缀名	★★★★
创建互斥量	★★★
在系统目录创建文件	★★★
映射内存方式注入	★★★
自启动	★★★
移动启动目录，疑似突破主动防御监控自启动目录	★★★
……	……

◆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23日(总第292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

《关键信息基础设施安全保护条例》9月1日起施行

第一章 总则

第一条 为了保障关键信息基础设施安全，维护网络安全，根据《中华人民共和国网络安全法》，制定本条例。

第二条 本条例所称关键信息基础设施，是指公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等重要行业和领域的，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的重要网络设施、信息系统等。

第三条 在国家网信部门统筹协调下，国务院公安部门负责指导监督关键信息基础设施安全保护工作。国务院电信主管部门和其他有关部门依照本条例和有关法律、行政法规的规定，在各自职责范围内负责关键信息基础设施安全保护和监督管理工作。

省级人民政府有关部门依据各自职责对关键信息基础设施实施安全保护和监督管理。

第四条 关键信息基础设施安全保护坚持综合协调、分工负责、依法保护，强化和落实关键信息基础设施运营者（以下简称运营者）主体责任，充分发挥政府及社会各方面的作用，共同保护关键信息基础设施安全。

第五条 国家对关键信息基础设施实行重点保护，采取措施，监测、防御、处置来源于中华人民共和国境内外的网络安全风险和威胁，保护关键信息基础设施免受攻击、侵入、干扰和破坏，依法惩治危害关键信息基础设施安全的违法犯罪活动。

任何个人和组织不得实施非法侵入、干扰、破坏关键信息基础设施的活动，不得危害关键信息基础设施安全。

第六条 运营者依照本条例和有关法律、行政法规的规定以及国家标准的强制性要求，在网络安全等级保护的基础上，采取技术保护措施和其他必要措施，应对网络安全事件，防范网络攻击和违法犯罪活动，保障关键信息基础设施安全稳定运行，维护数据的完整性、保密性和可用性。

第七条 对在关键信息基础设施安全保护工作中取得显著成绩或者作出突出贡献的单位和个人，按照国家有关规定给予表彰。

第二章 关键信息基础设施认定

第八条 本条例第二条涉及的重要行业和领域的主管部门、监督管理部门是负责关键信息基础设施安全保护工作的部门（以下简称保护工作部门）。

第九条 保护工作部门结合本行业、本领域实际，制定关键信息基础设施认定规则，并报国务院公安部门备案。

制定认定规则应当主要考虑下列因素：

（一）网络设施、信息系统等对于本行业、本领域关键核心业务的重要程度；

（二）网络设施、信息系统等一旦遭到破坏、丧失功能或者数据泄露可能带来的危害程度；

（三）对其他行业和领域的关联性影响。

第十条 保护工作部门根据认定规则负责组织认定本行业、本领域的关键信息基础设施，及时将认定结果通知运营者，并通报国务院公安部门。

第十一条 关键信息基础设施发生较大变化，可能影响其认定结果的，运营者应当及时将相关情况报告保护工作部门。保护工作部门自收到报告之日起3个月内完成重新认定，将认定结果通知运营者，并通报国务院公安部门。（原文链接：http://www.gov.cn/zhengce/2021-08/18/content_5631807.htm）

喜报！安天旗下国泰网信获2021年度第一批北京市专精特新“小巨人”企业认定

▲北京市专精特新“小巨人”企业证书

近日，安天科技集团旗下北京国泰网信科技有限公司（以下简称“国泰网信”）获得2021年度第一批北京市专精特新“小巨人”企业认定。此次认定由工业和信息化部、北京市经济和信息化局进行授牌，充分体现了国泰网信在网络安全行业的专业能力及持续的自主创新能力。

专精特新“小巨人”企业是工业和信息化部按照《关于促进中小企业“专精特新”发展的指导意见》要求，从“专精特新”中小企业中“优中选优”的佼佼者，是专注于细分市场、创新能力强、市场占有率高、掌握关键核心技术、质量效益优的“排头兵”企业。

国泰网信是一家成立于2015年的高新技术企业，主要基于商用密码、区块链、工控安全、数据安全等技术，在物联网、工业互联网等领域为电力、轨道交通、石油石化及其他行业提供网络安全整体解决方案和相关产品。（原文链接：https://mp.weixin.qq.com/s/EjcnXmZ-JTmVd-SvCwcHSQ）

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	Trickbot 恶意软件利用伪造的安装程序收集信息
英文标题	New Trickbot attack setup fake 1Password installer to extract data
作者	Waqas
内容概述	2016 年开始出现的“Trickbot”，多年来它从一个银行木马演变成了一个勒索软件僵尸网络，随着时间的推移，它增加了不同的功能。 在最近的一次调查中，人们发现 Trickbot 部署了一种机制来安装一个假的“1Password 密码管理器”，而这实际上是为了感染受害者的电脑并收集数据。Trickbot 使用一个密码保护的归档文件，其中包含一个包含宏的 Microsoft Word 或 Excel 文件，如果启用了宏，就会导致目标设备被入侵。此外，还部署了名为“Setup1.exe”的假 1Password 安装程序，用于启动 Cobalt Strike，帮助攻击者收集网络中多个系统的信息。
链接地址	https://www.hackread.com/trickbot-installs-fake-1password-manager-extract-data/

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 Office 远程代码执行漏洞（CVE-2021-34478）	高	Microsoft Office 存在远程代码执行漏洞。由于 Microsoft Office 中的输入验证不正确，使得攻击者可以欺骗受害者下载恶意文件并在目标系统上执行任意代码。
	Microsoft Word 远程代码执行漏洞（CVE-2021-36941）	高	Microsoft Word 存在远程代码执行漏洞。由于 Microsoft Word 中的输入验证不正确，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。
	Windows Print Spooler 本地提权漏洞（CVE-2021-36958）	高	Windows Print Spooler 存在本地提权漏洞。由于特权文件操作执行不当，使得本地用户可以向 Print Spooler 服务发送特制的请求，并以 SYSTEM 权限执行任意代码。
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/Win32.Mansabo	中	此威胁是一种可以窃取密码信息的木马类家族。该家族的样本运行后会窃取用户账户信息，记录键盘击键信息，造成用户隐私泄露。
	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[Dropper]/Win32.Miner	中	此威胁是一种可以释放比特币挖矿机的木马家族。该家族样本运行后释放恶意代码到本机 并运行，连接网络下载比特币挖矿机，占用系统资源，影响用户使用。
	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。

降低安全风险的四个措施

杰夫·席林 / 文 安天技术公益翻译组 / 译

勒索软件攻击、手机黑客攻击以及其他网络攻击每天都在发生，这使得网络安全成为全球公司最紧迫的问题之一。

管理层必须在推动安全文化方面发挥领导作用，以确保他们的公司能够抵御大多数（最好是所有）网络攻击。公司必须进行尽职调查并任命训练有素的安全团队，而安全团队应根据行业最佳实践，使用有助于预防、检测、缓解和消除威胁的工具，来监控和保护公司的数据。

在过去的 40 年里，我们与各行各业各种规模的企业合作，帮助他们改善网络安全状况。总的来说，企业可以采取下述四个措施来创建安全的工作环境。

获得管理层的支持

管理层的全力支持，对于企业实施和遵守安全 / 合规策略至关重要。除了确定和采购新技术的预算外，安全团队还应让管理层了解安全风险评估结果、行动计划、新技术部署和投资回报等问题，这一点非常重要。

为了获得最佳的评估结果，企业可以雇用独立的安全机构，该机构不向企业的 IT 部门报告，而是直接向企业管理层报告。虽说企业的 IT 部门和安全团队是保护企业的强大力量，但是在安全风险评估方面，最佳实践是职责分离。这样一来，提供 IT 服务的团队就不必同时负责监控和管理安全风险了。

进行安全风险评估

企业应了解其当前的漏洞及面临的威胁，这有助于企业部署正确的安全策略。公司漏洞评估通常由第三方执行。企业应检查每个系统的安全状况，以了解其正在使用哪些系统以及这些系统存在的风险，从而制定缓解计划来保护员工、公司和客户数据。

举例来说，如果客户通过手机进行支付，则企业应采用适当的技术来接收这些支付信息，同时避免将这些信息暴露给企业员工。如果企业无法实施这样的技术，那么能否根据“支付卡行业数据安全标准”（PCI DSS）保护这些信息呢?

同样，如果企业属于医疗行业，他们是否执行“健康保险流通与责任法案”（HIPAA）的规定和相关数据安全标准?承包商或其他第三方能否进入公司办公室的某些区域？为了降低风险（尤其是客服中心的风险），企业必须能够查明哪些地方可能会发生诈骗。

创建行动计划来应对风险

要想缓解安全风险，企业首先应验证漏洞评估结果并查找新风险。完成漏洞评估后，企业应列出诈骗风险清单，并依此对缓解计划进行压力测试，以确保其缓解计划是有效的。

企业应确保，其安全团队定期接受培训并获得行业信息安全标准认证，例如认证信息系统安全专家（CISSP）。为了实现完全的合规性，企业应考虑聘用精通最严格安全标准和协议（包括 PCI DSS 和 HIPAA）的人才。此外，企业还应进行独立审计，这一点也很重要。

进行持续评估

要想维护和改进安全系统，企业应关注以下三个方面。

1. 采用一流的安全技术，并使其安全运营与行业公认的最佳实践保持一致。此外，如果企业有开发人才，可以构建专有安全工具来填补企业的技术空白。

2. 与第三方安全专家合作。在选择第三方安全专家时，企业应确保合作伙伴可以进行端到端的安全分析和行为分析，以检测和阻止攻击和内部人员诈骗。此外，企业应解决或减轻第三方评估发现的所有安全问题。

3. 设立员工诈骗热线。通过这种方法，员工在怀疑遇到诈骗或可疑行为时可以向高管发出告警。

安全应该是各级员工的首要任务，但是这方面的文化变革应该由管理层牵头，以确保员工能够认同。降低风险和确保合规性是一项全天候的工作，企业只有投入大量的时间和资源，才能创建和维护安全文化。

原文名称	Stop the breaches! Four steps to minimize security risks
作者简介	杰夫·席林（Jeff Schilling），是 Teleperformance 公司的全球首席信息安全官。
原文信息	2021 年 8 月 13 日发布于 Help Net Security 原文地址 https://www.helpnetsecurity.com/2021/08/13/stop-the-breaches/
摘 要	管理层必须在推动安全文化方面发挥领导作用，以确保他们的公司能够抵御大多数（最好是所有）网络攻击。公司必须进行尽职调查并任命训练有素的安全团队，而安全团队应根据行业最佳实践，使用有助于预防、检测、缓解和消除威胁的工具，来监控和保护公司的数据。
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。