# 安天智甲有效防护 DearCry 勒索软件


近日，安天CERT在梳理网络安全事件时发现一个名为DearCry的勒索软件。该勒索软件最早于2021年3月被发现，主要通过利用Microsoft Exchange Server相关漏洞进行传播。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DearCry勒索软件的加密行为。

攻击者通过利用CVE-2021-26855、CVE-2021-26857、CVE-2021-26858和CVE-2021-27065的漏洞组合实现DearCry勒索软件落地。该勒索软件使用AES-256加密算法来加密文件，并使用硬编码的RSA公钥加密AES密钥。样本在加密文件时，首先会创建被加密文件的副本，并将副本命名为原文件名同时追加".CRYPT"后缀，随后把加密的文件内容写入其中，将原文件用1MB大小的0x41数据内容覆盖，然后删除原文件，通过覆写文件的方式防止恢复数据。该样本不能自动传播，需要通过人为利用漏洞投放，且没有删除卷影的功能。样本会在磁盘根目录下和路径中包含字符串“desktop”的目录下创建名为“readme.txt”的勒索信，勒索信中包含一个HASH和联系邮箱，攻击者可通过该HASH得知受害者所用的RSA公钥。具体勒索金额和赎回方式需要和攻击者联系。


▲DearCry 勒索信

DearCry勒索软件采用“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、信标检测鉴定器、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 | 2b9838da7edb0decd32b086e47a31e8f5733b5981ad8247a2f9508e232589bff |
| 文件类型 | BinExecute/Microsoft.EXE[:X86] |
| 大小 | 1.26 MB |
| MD5 | 0E55EAD3B8FD305D9A54F78C7B56741A |
| 病毒类型 | 木马程序 |
| 恶意判定 / 病毒名称 | Trojan[Ransom]/Win32.Encoder |
| 判定依据 | 反病毒引擎 |

报告地址：https://1.119.163.6/vue/details?hash=0E55EAD3B8FD305D9A54F78C7B56741A

◆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、Office 2003、Flash、WPS、FoxitReader、Adobe Reader |

◆危险行为

| 行为描述 | 危险等级 |
|---|---|
| 文件篡改 | ★★★★★ |
| 感染文件尾部 | ★★★★ |
| 感染文件 | ★★★★ |
| USP 进行劫持 | ★★★ |

◆常见行为

| 行为描述 | 危险等级 |
|---|---|
| 获取主机内存信息 | ★★ |
| 根目录下创建 EXE 文件 | ★★ |
| 设置自启动项 | ★★ |
| 获取驱动器类型 | ★ |
| 打开自身进程文件 | ★ |
| 加载运行时 DLL | ★ |
| 获取计算机名 | ★ |
| 检索系统内存信息 | ★ |
| 访问文件尾部 | ★ |

◆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03月22日(总第270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

# 通过U盘传播的多功能勒索软件分析

## 概述

近日，安天CERT捕获到一种具备可移动介质传播功能的BleachGap勒索软件。该勒索软件最早出现于2021年2月，目前已迭代多个版本。

BleachGap勒索软件具备添加自启动、添加计划任务、改写MBR、使键盘按键失效、通过可移动介质传播等多项功能，采用“AES-256”对称加密算法加密文件，在已知密钥的情况下可快速解密。目前，勒索软件的功能已经不局限于加密文件，开始尝试通过可移动介质的方式横向传播，用户需及时针对此类攻击手段做好有效防范措施。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BleachGap勒索软件的恶意行为。

## 防护建议

### 个人防护

(1) 安装终端防护：安装反病毒软件。建议安天智甲的用户开启勒索病毒防御工具模块（默认开启）；

(2) 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；

(3) 及时更新补丁：建议开启自动更新功能安装系统补丁，服务器应及时更新系统补丁；

(4) 关闭高危端口：如无使用需要，建议关闭3389、445、139、135等高危端口；

(5) 定期数据备份：定期对重要文件进行数据备份，备份数据应与主机隔离；

(6) 确认邮件来源：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；

(7) 关闭U盘自动播放：通过配置组策略在系统中关闭U盘自动播放功能。

### 企业防护

1、开启日志：开启关键日志收集功能（安全日志、系统日志、PowerShell日志、IIS日志、错误日志、访问日志、传输日志和Cookie日志），为安全事件的追踪溯源奠定基础；

2、设置IP白名单规则：配置高级安全Windows防火墙，设置远程桌面连接的入站规则，将使用的IP地址或IP地址范围加入规则中，阻止规则外IP进行暴力破解；

3、主机加固：对系统进行渗透测试及安全加固；

4、灾备预案：建立安全灾备预案，确保备份业务系统可以快速启用；

5、安天服务：若遭受勒索软件攻击，建议及时断网，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。

目前，安天智甲终端防御系统可实现对BleachGap勒索软件的查杀与有效防护。


原文链接：（https://mp.weixin.qq.com/s/P-mDJtc8rhveY9yMQyloHA）

扫描上方二维码阅读全文

**PHP信用卡窃取程序将信息保存在JPG文件中**

最近对受感染的Magento 2网站的调查显示，该恶意注入正在捕获来自站点访问者的POST请求数据。它位于结帐页面上，可以对捕获的数据进行编码，然后再将其保存到.JPG文件中。为了成功捕获POST数据，PHP代码需要使用Magento代码框架。它依赖于Magento函数getPostValue来捕获Customer_ POST参数中的结帐页面数据。使用Magento函数isLoggedIn，PHP代码还检查发送POST请求数据的受害者是否以用户身份登录。如果用户确实登录了，它会捕获用户的电子邮件地址。在使用PHP运算符^对所窃取的信息进行异或运算之前，会使用base64对捕获的POST数据进行编码，并将其保存到同一个图像文件中。

（原文链接：https://blog.sucuri.net/2021/03/magento-2-php-credit-card-skimmer-saves-to-jpg.html）

**Tech Mahindra公司遭勒索软件攻击服务器瘫痪**

印度Tech Mahindra公司遭受了勒索软件攻击，这使其25台服务器瘫痪。攻击者的身份尚未公开，他们要求用比特币支付5000万卢比的赎金。遭到破坏的服务器与Pimpri-Chinchwad智慧城市项目有关，但是Pimpri-Chinchwad市政公司（PCMC）明确表示，他们不会支付一分钱来弥补损失。Tech Mahindra的经理Mahendra Laxminarayan Lathi于2021年3月9日通知了警方，据称攻击发生在2021年2月26日。

（原文链接：https://www.technadu.com/tech-mahindra-attacked-ransomware-actors-client-not-pay/255032/）

## 每周安全事件

| 类 型 | 内 容 |
|---|---|
| 中文标题 | Lemon_Duck 针对未修补的微软 Exchange 服务器 |
| 英文标题 | Microsoft Exchange exploits now used by cryptomining malware |
| 作者 | Sergiu Gatlan |
| 内容概述 | Lemon_Duck 是一个以企业网络为目标的挖矿僵尸网络，它的操控者现在正在利用 ProxyLogon 漏洞攻击未修补的 Microsoft Exchange 服务器。Kaspersky 全球研究和分析团队的主管 Costin Raiu 称，Lemon_Duck 对易受攻击的 Exchange 服务器的持续攻击已经达到了巨大的规模。攻击者利用部署在受感染服务器上的 web shell 从 p.estonine[.]com 和 cdn.chatcdn[.]net 下载恶意载荷。Hunterss 实验室在分析对本地 Microsoft Exchange 服务器的大规模利用时，也观察到了这些与 Lemon_Duck 有关的妥协指标。 |
| 链接地址 | https://www.bleepingcomputer.com/news/security/microsoft-exchange-exploits-now-used-by-cryptomining-malware/ |

## 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-2021-27085） | 高 | 由于没有充分验证 Internet Explorer 中用户提供的输入，Internet Explorer 存在远程代码执行漏洞。攻击者可以诱骗受害者访问特制网页并在目标系统上执行任意代码。 |
| | Microsoft SharePoint Server 安全漏洞（CVE-2021-27076） | 高 | 由于 Microsoft SharePoint Server 中的输入验证不严谨，导致 Microsoft SharePoint Server 存在远程代码执行漏洞。攻击者可以发送特制请求，并在目标系统上执行任意代码。 |
| | Windows DNS 服务器安全漏洞（CVE-2021-26897） | 高 | 由于 Windows DNS 服务器中的输入验证不正确，因此存在此漏洞。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。 |
| | 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[Ransom]/Win32.Blocker | 中 | 此威胁是一种赎金类木马家族。该家族木马运行后会破坏电脑系统、损坏用户的文件，对用户文件加密使用户无法打开。此时黑客会向用户索要赎金并提供所谓的“密钥”，但用户支付赎金后仍然不能修复受损的文件。 |
| | 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/Win32.Fsysna | 中 | 此威胁是一种木马家族。该家族样本运行后会在电脑的临时文件夹下释放恶意代码，同时添加注册表启动项，并发送网络请求。 |
| | 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。 |



# 保护服务账户的最佳实践

亚伦·卡斯纳 / 文　安天技术公益翻译组 / 译

企业是时候创建网络安全最佳实践，以防止其服务账户沦为网络窃贼的攻击向量了。

服务账户负责向应用程序授予适当的权限，以便应用程序在后台自动执行计划的任务，从而减轻 IT 人员的负担。但是，应用程序自动执行的任务通常会被忽视、不受监控，不在网络安全最佳实践的管辖范围之内。简言之，随着企业服务账户数量的增加，其潜在攻击面也在增加。

虽然服务账户可以解决自动化带来的诸多挑战，但也会带来严重的网络安全问题。企业必须解决这些问题，以保护自己免受数据泄露和横向移动攻击等网络安全问题。

### 获得可见性

虽说“企业无法保护看不到的东西”这一观点已是老生常谈，但在网络安全领域事实就是如此。企业创建服务账户是为了实施业务流程，而在大多数情况下，这些账户是在网络安全团队不知道的情况下创建的。也就是说，这些服务账户没有记录、不受监控和管理，是潜在的攻击向量。

随着时间的流逝，管理员逐渐无法跟踪服务账户、更改口令，或因担心造成服务中断而不敢进行必要的更改，这会带来各种问题。例如，服务账户会沦为静态的元素，在任何人都未察觉的情况下遭受攻击。为了应对这些问题，企

业可以为服务账户创建统一的管理平台，该平台不仅可以发现活跃和不活跃的服务账户，还可以洞悉账户的使用方式，以及该账户是服务账户、人工账户还是两者兼有。

### 监控服务账户

仅仅清点服务账户和用户账户，是无法了解它们执行哪些活动的。要想了解它们的实际活动，企业应进行主动监控。这样一来，企业可以获得对账户行为的可见性，以确定账户是否在执行异常活动。企业还应对账户进行审计，并监控每一次身份验证尝试，以检测暴力破解等攻击企图。此外，监控平台应整合各种情报，以识别已知的威胁向量和账户漏洞。通过主动监控、审计和异常检测，网络安全专家能够获得必要的信息，以便根据事实而非假设做出决策。

### 创建策略

在对抗网络攻击的过程中，只有信息而不采取行动是无济于事的。任何想要保护服务账户的人员，都应记住这一点。策略是解决账户安全问题的重要工具，企业应通过明确的定义和措施加以实施。

在当今复杂的环境中，企业必须针对服务账户和用户账户创建明确的策略，以实施安全最佳实践。通过创新性的解决方案，管理员不仅可以定义策略，还能为所有服务账户推荐最合适的策略。策略能够提供另一层保护，有助于管理员定义细粒度的元素以锁定任何异常行为。

### 实时响应

策略执行是一种防止攻击的战术方法，体现了对任何未经授权地访问受保护资源的企图做出响应的能力。但是，企业不仅要迅速响应，还要实现自动化的响应。在选择保护服务账户的技术时，管理员必须确定平台对威胁的响应程度。这也意味着，该平台必须将主动监控和策略执行相结合，并以检测和响应为后盾，实时进行所有操作。鉴于攻击和横向移动会在几秒钟内发生，需要人机交互的威胁响应会被延迟，因此并不那么有效。

为保护服务账户免受入侵和其他攻击向量的侵扰，企业应消除访问孤岛，利用各种情报识别服务账户，以便定义策略来保护这些账户。更重要的是，在当今快节奏的网络攻击世界中，自动化已成为必须，企业必须在损害造成之前实时进行自动化响应。将自动化、威胁识别、策略和响应相结合，能够有效地保护服务账户免受攻击。

| | |
|---|---|
| 原文名称 | Best Practices for Securing Service Accounts |
| 作者简介 | 亚伦·卡斯纳（Yaron Kassner）。亚伦·卡斯纳是 Silverfort 的首席技术官和联合创始人。 |
| 原文信息 | 2021 年 03 月 06 日发布于 Dark Reading<br>原文地址 https://www.darkreading.com/operations/best-practices-for-securing-service-accounts/a/d-id/1340343 |
| 摘　要 | 服务账户负责向应用程序授予适当的权限，以便应用程序在后台自动执行计划的任务，从而减轻 IT 人员的负担。虽然服务账户可以解决自动化带来的诸多挑战，但也会带来严重的网络安全问题。企业必须解决这些问题，以保护自己免受数据泄露和横向移动攻击等网络安全问题。最佳实践包括：（1）获得可见性；（2）监控服务账户；（3）创建策略；（4）实时响应。 |
| 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。 |