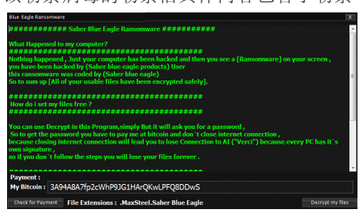
安天智甲有效防护 Saher Blue Eagle 勒索软件

近日，安天 CERT 在梳理网络安全事件时发现一个名为 Saher Blue Eagle 的勒索软件。该勒索软件最早于 2020 年 12 月被发现，主要通过垃圾邮件进行传播，邮件附件为勒索软件程序，邮件内容诱使用户执行该程序。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 Saher Blue Eagle 勒索软件的加密行为。

Saher Blue Eagle 勒索软件样本运行后，使用释放的 %AppData%\Back.jpg 替换桌面背景，并弹出勒索信界面，终止数据库、office 等指定进程，创建多个线程，在短时间内完成对计算机上相关文件的加密，在被加密文件的后缀名后追加以“..MaxSteel.Saher Blue Eagle”命名的后缀。加密完成后，删除系统卷影副本，以防止恢复加密文件，该勒索病毒的勒索信具体内容包含了勒索



▲Saher Blue Eagle 勒索信

说明、勒索金额、比特币地址等。

Saher Blue Eagle 勒索软件采用“AES + RSA”加密算法加密文件，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、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、动态（WinXP）鉴定器、动态（Win7 x86）鉴定器、信标检测鉴定器等鉴定分析。

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	3FEFD7EAD4D1E2C95ACB04F2452660CC
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	357 KB
MD5	3FEFD7EAD4D1E2C95ACB04F2452660CC
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[Ransom]/MSIL.Encoder
判定依据	反病毒引擎

完整报告地址：https://1.119.163.6/vue/details?hash=3FEFD7EAD4D1E2C95ACB04F2452660CC

◆操作系统

操作系统	内置软件
Win7 x86 6.1.7600 Build 7600	默认、IE9、Google Chrome、Firefox、Office 2007、Flash、WPS、FoxitReader、Adobe Reader

◆危险行为

行为描述	危险等级
查询系统硬盘大小	★★★

◆常见行为

行为描述	危险等级
加载运行时 DLL	★
打开自身进程文件	★
获取系统信息（处理器版本、处理器类型等）	★
获取系统版本	★
镜像劫持	★★
检测自身是否被调试	★★
获取驱动器类型	★
检索系统内存信息	★
.....	.....

◆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 01 月 18 日 (总第 263 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

蠕虫携带逻辑炸弹，安天智甲早已设防

2021 年 1 月 13 日，安天关注到一些网络论坛中有用户遭遇文件被病毒删除现象，联系提取样本后，发现系安天很早可以查杀的“古老”蠕虫家族，但鉴于行业和公众对此事件较为关注，安天提供如下分析：

该病毒家族俗名 incaseformat，是一个较为古老的 USB 蠕虫家族，安天根据这一类病毒的传播机理，将其系列变种均统一归入 Worm/Win32.Autorun。对相关蠕虫家族，安天产品数年前即可防御查杀。

实际情况是，相关蠕虫近期传播感染并未发生激增。由于部分政企机构和个人用户长期处于裸奔状态，或未安装具有有效能力的安全产品，使这一“古老”蠕虫长期寄生而未能及时发现，而由于该蠕虫带有删除文件的逻辑炸弹，作者预设 2010 年 4 月 1 日为首次发作日期，但是由于函数参数错误，导致 2021 年 1 月 13 日成为了首次发作日期，所以这些感染的用户因文件被删除而感知到了这一蠕虫的存在。这是今日该病毒成为焦点的关键原因。

安天感知体系捕获该蠕虫的最早家族版本为 2009 年，该家族存在数百个版本的迭代演进，其中有的版本功能为隐藏用户系统盘外的大部分文件。本次发现的蠕虫病毒版本之所以会在 2021 年 1 月 13 日开始删除文件，是由于时间函数变量值存在编写错误，执行删除文件的操作由 2010 年 4 月 1 日延至 2021 年 1 月 13 日，攻击者原意为在 2010 年 3 月后每个月的 1 号、10 号、21 号、29 号后开始文件删除操作。这种主要通过 U 盘进行传播的病毒，在缺少有效安全防护软件的政企机构网络中往往反复传播感染。而通过部署安天智甲等有效端点防护能力的主防产品可以很容易感知和拦截。对于遭遇病毒已经发作的情况，安天也提醒用户还有补救的余地，安天 CERT 经测试发现该蠕虫病毒删除的文件可由数据恢复软件进行恢复。

厂商的持续威胁捕获能力，基础引擎检测能力和主防能力是有效端点防御的基石。没有这些基石的支撑的产品，甚至无法通过对抗陈旧病毒的试炼。

智甲可通过文件防御捕获 Incaseformat 病毒文件进入用户主机事件，并向用户发起告警，自动隔离病毒文件。

另外，该病毒还会尝试通过创建 RunOnce 注册表实现开机自启动，智甲具有注册表防御功能，亦可以防御该行为。

（**原文链接**：https://www.antiy.cn/research/notice&report/research_report/20210114.html）

（**本文为报告节选，完整报告请扫描下方二维码查看**）

Ursnif 木马新变种攻击意大利用户

Fortinet 实验室发现了一项针对意大利用户的网络钓鱼活动，该活动通过附带的 Word 文档不断传播 Ursnif 木马新变种。网络钓鱼电子邮件 Word 附件使用意大利语编写，伪装成付款提醒。用户打开文档后，将弹出一个黄色警告栏，警告用户该文件包含宏。一旦单击按钮启用宏，恶意宏将在后台执行。然后，恶意宏从一个硬编码 URL 下载并运行一个 DLL 文件。DLL 文件受到打包程序保护，其由 RegSvr32.exe 启动，并且调用解压缩程序首先将 Ursnif 提取到内存中。此解压缩的 PE 文件是 Ursnif 变种的核心模块。该 Ursnif 变种会收集敏感信息并将其发送到 C2 服务器，在研究人员分析时，该 C2 服务器已关闭。

（**原文链接**：https://www.fortinet.com/blog/threat-research/new-variant-of-ursnif-continuously-targeting-italy）

微软发布 1 月补丁更新修复 83 个漏洞

微软发布了 1 月的补丁更新，共修复 83 个漏洞，其中包含 10 个关键漏洞和 73 个重要漏洞。补丁涵盖多达 11 种产品和服务，包括 Microsoft Windows、Edge 浏览器、ChakraCore、Office、Microsoft Office Services 以 及 Web Apps、Visual Studio、Microsoft 恶意软件保护引擎、.NET Core、ASP .NET 和 Azure。 问 题 最 严 重 的 是 Microsoft Defender 中的 0day 远程代码执行（RCE） 漏 洞， 漏 洞 ID 为 CVE-2021-1647，该漏洞可能允许攻击者使用任意代码感染目标系统。

（**原 文 链 接**：https://thehackernews.com/2021/01/microsoft-issues-patches-for-defender.html）

每周安全事件

类 型	内 容
中文标题	CISA：黑客绕过 MFA 访问云服务帐户
英文标题	CISA: Hackers bypassed MFA to access cloud service accounts
作者及单位	Sergiu Gatlan
内容概述	美国网络安全和基础设施安全局（CISA）最近发现了几起针对不同组织云服务网络攻击事件，黑客绕过了多因素身份验证（MFA）身份验证协议，以破坏云服务帐户。黑客使用了多种策略和技术，包括网络钓鱼、暴力破解登录尝试以及可能使用的“传送 cookie”攻击，来尝试利用受害组织的云安全实践中的弱点。
链接地址	https://www.bleepingcomputer.com/news/security/cisa-hackers-bypassed-mfa-to-access-cloud-service-accounts/

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	Oracle Database Server Scheduler component 未授权访问漏洞（CVE-2020-14735）	高	Database ServerScheduler component 存在未授权访问漏洞，攻击者可利用该漏洞拥有本地登录特权，登录到调度程序执行的基础设施，从而危及调度程序，导致 Scheduler 被接管。
	Microsoft Visual Studio 远程代码执行漏洞（CVE-2020-16874）	高	Microsoft Visual Studio 存在远程代码执行漏洞。攻击者可利用该漏洞在当前用户的上下文中执行任意代码。
	FasterXML Jackson-databind 反序列化漏洞（CVE-2020-36179）	高	Jackson-databind 2.0.0 - 2.9.10.7 版本中缺少 oadd.org.apache.commons.dbcp.cpdsadapter.DriverAdapterCPDS 的危险类黑名单，攻击者可以利用上述缺陷，绕过限制，实现 JNDI 注入，最终在受害主机上执行任意代码。
较为活跃样本家族	Trojan/Win32.Yakes	中	此威胁是一种木马类程序。该家族可以通过白名单机制绕过系统防火墙，获取系统的最高权限。该家族具有下载恶意程序、监控用户操作等行为。该家族木马会在执行完成后将自身删除。
	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[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[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[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[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。

2021 年值得关注的数据行业趋势

安天技术公益翻译组 / 译

Okera 公司的研究人员对 2021 年即将出现的五大关键数据行业趋势做出了预测。

新冠疫情迫使全球公司加速了数字化转型战略，而远程办公和数据泄露事件的增加也迫使他们重新思考数据安全方法。

Okera 首席技术官李农（Nong Li）表示：“2021 年，企业会加速开发改变其业务和增加收入的工具和技术。与此同时，数据隐私将成为差异化竞争（competitive differentiation）的重中之重。”

数据隐私和访问控制：差异化竞争优势推动收入增长

在 2019 年和 2020 年，企业的重点是培训员工、创建相关流程和技术，以避免因违反隐私和数据泄露法规而遭受经济处罚和品牌声誉损害。

而在 2021 年，公司有了保护其数据（其组织以及产品）隐私的新动机：差异化竞争。即使在疫情爆发之前，数据隐私就已经是一个重要的技术话题了，疫情更是推动了这一趋势。

一大波公司将会在数据隐私和安全性方面加大投资、改进方法、提高透明度，将此作为其技术和品牌的关键特征。消费者的需求将推动这一趋势，使数据隐私在大多数垂直领域中成为一项关键竞争优势。

但是，安全性并非应用程序设计人员最关心的问题。这导致的结果是，很多企业将经历一场文化上的巨变，他们需要自上而下地推动将隐私和安全性纳入企业的技术架构中，同时部署为开发团队赋能的工具和流程。

数据目录和元数据管理方面的投资将获得回报

在过去的几年中，企业增加了对数据目录技术的投资，以便能够在混合和多重云环境中跨各种数据孤岛简单、自动地访问集成元数据。

尽管很多企业已经将数据输入到目录中，但是他们中的大多数仍未在业务工作流中启用这些目录以获取战略优势。在 2021 年，随着更多企业开始利用元数据来创建通用、灵活的业务规则以及进行请求处理，这种情况将得到很大的改善。

例如，在使用业务应用的过程中，数据消费者将了解哪些是敏感数据、与敏感数据相关的内容以及哪些人员有权访问这些数据。同时，负责保护敏感数据的管理员将部署工具，这些工具利用元数据自动执行访问控制。

集成的混合数据平台将改变云应用的功能

2021 年，真正集成的数据平台将会兴起。这些平台包括一个涵盖所有数据存储（无论它们部署在何处）的集中式数据目录，以及集成的用户和权限管理。这样一来，公司就能构建涵盖这些数据存储的应用程序了。

我们看到这种趋势越来越受欢迎——主要的云提供商都提供了在其他云中部署其软件的方法。集成数据平台提供的灵活性将改变云应用程序的功能并缩短价值实现时间。

数据分析和数据平台技术的垂直化

2000 年代初，企业从构建传统的关系数据库和数据仓库转向构建分布式数据平台。

到 2010 年代中期，公司推出了旨在解决这些新环境中（例如用于分析的 Databricks 和用于云整合的 Snowflake）特定痛点的单点解决方案。

在接下来的 10 年中，企业将大力发展上述以及许多其他解决方案，通过完全集成且对用户友好的解决方案缩短价值实现时间。这样一来，企业就能够大大加速新数据平台的构建，并更快地从其数据中获取更大的价值。

首席数据官（CDO）将实施分布式数据管理模型

在过去的几年中，企业需要更有效地使用数据，因此他们设立了 CDO 一职。在大数据以及分布式混合和多重云架构时代，保护数据已成为一项董事会层面的高风险问题，与每个企业的成功息息相关。

但是，为了真正自上而下地推进数据隐私和安全性，企业需要部署一种分布式数据管理方法。通过这种方法，企业中的每个人都需要对数据隐私负责，而技术平台则可以为他们提供支持。

在 2021 年，CDO 的角色将会进一步演变。他们将引领企业的文化变革，通过提供自上而下的控制和防护措施来实施必要的技术变更。因此，最接近数据的业务团队需对访问管理负责。

这种模型将对企业的业务产生变革性影响，推动更有效的数据监管，有助于企业获取竞争优势并增加收入。

原文名称	Data industry trends to watch in 2021
发布单位	Help Net Security
原文信息	2020 年 01 月 13 日发布于 Help Net Security 原文地址 https://www.helpnetsecurity.com/2021/01/13/data-industry-trends-2021/
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。