安天智甲有效防护 Prometheus 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 Prometheus 的勒索软件。该勒索软件变种最早于 2021 年 5 月被发现，隶属于 REvil/Sodinokibi 勒索软件家族，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 Prometheus 勒索软件的加密行为。

Prometheus 勒索软件使用 .NET 框架开发，具备反调试功能。运行后创建名为 "a24f6fef-8c36-4314-91c5-2f98ae613662" 的互斥体保证单实例运行，并强制删除 Raccine 反勒索软件相关的注册表、服务、计划任务、活动进程等内容。然后删除磁盘卷影、多种类型的备份文件、回收站内容。同时该样本具备内网横向扩散功能，通过获取 ARP 记录向相关 IP 传播自身文件并加密该 IP 的共享目录。随后遍历 NTFS 类型磁盘中除 %Windir%、%Program Files%、%AppData% 等 37 个系统相关目录以外所有目录，对图片、压缩包、文档等常见类型文件进行加密，并追加文件名后缀 ".[141-5D9-Y454]"。加密完成后在各磁盘根目录及桌面释放名为 "RESTORE_FILES_INFO.txt" 的勒索信，并在桌面额外释放一个名为“RESTORE_FILES_INFO.hta”的勒索信。要求用户向指定门罗币地址支付赎金，具体金额勒索信中未说明，需与攻击者通过留言室沟通后获取赎金金额。

▲Prometheus 勒索软件勒索信

Prometheus 勒索软件采用 AES-32+RSA 的形式加密文件，目前被加密的文件无法解密。

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	Prometheus.exe
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	143 KB
MD5	E1F063D63A75E0E0E864052B1A50AB06
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Bas.MSIL
判定依据	BD 静态分析

报告地址：https://1.119.163.6/vue/details?hash=E1F063D63A75E0E0E864052B1A50AB06

◆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	★★★
开启系统服务	★★★
通过 WMI 查询操作系统信息	★★★
通过 WMI 查询 CPU 信息	★★★
删除卷影副本	★★★★

◆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 24 日 (总第 279 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

破坏而非加密文件的勒索软件 Combo13 分析

概述

近日，安天 CERT 发现了一个采用 .NET 框架开发的名为 Combo13 的勒索软件。该勒索软件变种最早于 2021 年 4 月被发现，主要通过垃圾邮件进行传播。

值得关注的是 Combo13 勒索软件并未采用加密算法进行文件加密而是采用随机字节数据覆盖的方式覆盖文件全部原始数据，从而造成文件数据的彻底损坏。无论受害者是否缴纳赎金，攻击者都无法为受害者解密文件。基于该勒索软件并没有删除卷影副本，受害者可通过卷影副本来恢复数据。

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 Combo13 勒索软件的加密行为。

目前，安天智甲终端防御系统可实现对 Combo13 勒索软件的查杀与有效防护。

Combo13 勒索软件分析

1. 样本标签

病毒名称	Trojan[Ransom]/MSIL.Agent
原始文件名	IS_room_start.exe
MD5	857E6E8A8D20B76066D72F432B7B1A71
处理器架构	Intel 386 or later, and compatibles
文件大小	8.00 KB (8192 字节)
文件格式	Win32 EXE
时间戳	2021-04-16 14:48:36
数字签名	无
加壳类型	无
编译语言	.NET
VT 首次上传时间	2021-05-10 03:26:23
VT 检测结果	42/69

▲ 二进制可执行文件

2. 样本行为

Combo13 勒索软件使用 .NET 框架开发，运行后会对 C:\Users 目录下的除指定文件格式以外的所有类型文件进行加密。（原文链接：https://mp.weixin.qq.com/s/hpbqiQPA2fV9523NilBkIQ）

扫描右侧二维码阅读全文

将 Python 远控隐藏在文档图片中的行动分析

概述

近日，安天 CERT 通过网络安全监测发现了一起恶意文档释放 Python 编写的远控木马事件。通过文档内容中涉及的组织信息和其中攻击者设置的诱导提示，安天 CERT 判断该事件是一起针对阿塞拜疆共和国国家石油公司进行的定向攻击活动。此次事件中，攻击者充分利用技术实现规避反病毒软件查杀，具体为利用了隐写术将远控木马相关文件以压缩包格式存储于恶意文档里的图片中以备后期提取利用。首先将该恶意文档另存为 docx 文件，该文件格式具备 ZIP 文件的特性，然后另存为 ZIP 格式进行解压并获取其中的图片，最后提取图片中的远控木马文件。此远控木马采用 Python 语言编写，具备一般远控的上传、下载和命令执行等功能。

总结

由于该远控木马是用 Python 编写，对应文件具备脚本文件特性，其实质文件格式为文本文件，相较于 PE 文件，这种文件格式在一定程度上能够降低被反病毒软件查杀的可能性，同时结合远控木马 VT 检测结果，安天 CERT 认为这种脚本形式的远控木马将会更加频繁的被攻击者使用，甚至结合混淆编码进行使用。（原文链接：https://mp.weixin.qq.com/s/kASObxoxintb6As-7kR93g）

扫描右侧二维码阅读全文

安天加入华为云“沧海行动”

5 月 17-18 日，2021 华为生态大会召开。在同期举办的“云原生 2.0，赋能新云原生企业”分论坛上，华为云发起“华为云安全生态‘沧海行动’计划”，以优化安全生态格局，践行“协同创新、融合共赢”发展路径，构建云原生安全 + 安全生态联合解决方案，赋能生态伙伴。

安天、奇安信、绿盟、安恒、启明星辰、山石等网络安全优秀企业成为华为云安全生态“沧海行动”的合作伙伴，安天科技集团高级副总裁穆瑛参加启动仪式。

加入华为云安全生态“沧海行动”后，安天将与华为云进行深度合作，利用安天在云生态环境下的威胁情报、管理监测与响应等方面的技术和服务，以云内生安全为目的，将云平台安全和云安全产品内置到云计算环境中，为最终客户提供安全解决方案。

安天与华为云均坚守“以客户为中心”的核心价值观，双方通过高效协同，能够在数字化转型中持续为客户带来更有价值的产品、方案和服务，同时为安天的发展注入更强动力。（原文链接：https://mp.weixin.qq.com/s/odpljP5QilkA0i-GtZ4s3g）

扫描上方二维码阅读全文

每周安全事件

类 型	内 容
中文标题	东芝公司遭受 DarkSide 勒索软件攻击
英文标题	Toshiba unit struck by DarkSide ransomware group
作者	Charlie Osborne
内容概述	近日，东芝公司已经成为 DarkSide 勒索软件攻击的最新受害者。 该公司的法国子公司似乎已成为袭击目标。发现攻击后，东芝技术公司关闭了日本、欧洲及其子公司之间的网络，以防止损害蔓延，同时实施恢复和数据备份，并且就损害程度展开调查，并已请来第三方网络取证专家协助，但是东芝尚未确认与客户相关的信息是否遭到泄露。据悉，Darkside（黑暗面组织）勒索软件是造成东芝公司网络受损的原因。
链接地址	https://www.zdnet.com/article/toshiba-unit-struck-by-darkside-ransomware-group/

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 Web Media Extensions 远程代码执行漏洞（CVE-2021-28465）	高	Microsoft Web Media Extensions 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，使得攻击者可以在目标系统上执行任意代码。
	Microsoft Office 远程代码执行漏洞（CVE-2021-31179）	高	Microsoft Office 存在远程代码执行漏洞。由于 Microsoft Office 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 Visual Studio Code 远 程代码执行漏洞（CVE-2021-31211）	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。
较为活跃样本家族	Trojan[Proxy]/Win32.Qukart	中	此威胁是一种可以窃取用户信息并通过代理服务器回传信息的木马类家族。该家族样本收集系统的敏感信息，通过 http 请求发送到指定网页。该家族在后台会自动更新。
	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/Win32.Reconyc	中	此威胁是是一种窃密类木马家族。该家族样本运行后会在系统文件夹中释放动态链接库文件和可执行程序，并设置消息挂钩函数，以获取系统相关信息并回传。
	Trojan/Win32.Yakes	中	此威胁是一种恶意木马家族。该家族木马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。该家族木马具有下载恶意程序、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[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[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.SmsThief	中	此威胁为安卓平台上的窃密类木马家族。该家族木马通常伪装成其他应用程序，运行后会获取用户短信信息、通讯录、通话记录、GPS 位置等隐私信息上传到指定服务器，造成用户隐私泄露。

安全代码审查的基本方法

李薇薇 / 文 安天技术公益翻译组 / 译

每位 AppSec 专家通常配备超过 200 位开发人员。因此，要增强安全性，就要提高开发人员在保护产品安全方面的投入。为此，开发人员必须对他们编写的代码的安全性负责。在将应用程序投入生产之前，执行源代码审查以识别和补救安全风险，是确保软件质量的最佳方法之一，但是说起来容易做起来难。

查找并修复代码中的错误

开发人员经常花费大量时间来查找和修复代码中的错误。最近的一项调查发现，32% 的开发人员每周需花费 10 个小时来修复错误，16% 的开发人员每周需花费 15 个小时，还有 6% 的开发人员每周需花费 20 个小时——这些时间就无法用于编写新代码了。

开发人员需要考虑的另一个重要因素是开源代码。如今，99% 的代码库至少包含一个开源组件，而 91% 的代码库已过时逾四年，或在最近两年内未被用于开发活动。在当今的数字世界中，开发人员在开发软件时几乎都会使用某种形式的开源代码，但是在确保开源代码的安全性方面，他们做的还很少。

进行安全代码审查的最佳策略

1. 知道要寻找什么

首先，开发人员应确定其开发的应用程序类型有哪些常见漏洞。他们应熟悉特定漏洞的标识，以便在遇到漏洞源代码模式时能够予以识别。虽然漏洞具有常见的模式，但这些模式在不同的情境中会有所不同。因此，开发人员应注意编程语言、框架和库，以确保更准确地识别漏洞。

2. 了解基本原理

在代码分析中，“source”是指生成漏洞的代码组件，“sink”是指漏洞发生的位置。例如，对于命令注入漏洞，source 通常是指接受用户输入的函数，而 sink 是指执行系统命令的函数。如果用户输入无需验证就可以从 source 端移动到 sink 端，则会出现命令注入漏洞。

跟踪从 source 端到 sink 端的数据流，是识别漏洞的一种常用方法。跟踪数据流（而非仅依靠模式匹配）能够大大减少静态分析工具的误报，这是因为，静态分析工具无法报告恶意输入无法“到达”的潜在漏洞。此方法也有助于开发人员对开源漏洞进行分类。通过跟踪对开源漏洞的不可信输入，开发人员能够识别可利用的漏洞。

3. 进行手动审查

执行手动审查时，开发人员应确保其应用程序是遵循最佳实践使用安全设置的。

为了快速了解情况，开发人员可以按照指示存在漏洞或配置错误的字符串、关键字和代码模式进行搜索。对 git 历史记录进行这种搜索也是很重要的。

为了扩展快速的初始搜索，开发人员应关注处理用户输入的代码，这些代码可以为攻击者提供利用应用程序漏洞的入口点。这些代码包括 HTTP 请求参数、HTTP 标头、HTTP 请求路径、数据库条目、文件读取和文件上载。

开发人员应深入了解关键控制函数，以了解它们是否会被绕过，以及用户和业务数据是如何传输和存储的。此外，开发人员应扫描应用程序特定的配置问题。

4. 找到合适的工具

手动代码审查既繁琐又耗时。使用软件组成分析（SCA）或静态分析安全测试（SAST）之类的工具可以实现此过程的自动化，帮助开发人员和安全团队更快、更有效地查找和修复安全问题。

SAST 工具能够自动识别漏洞模式，从而节省开发人员的时间，使其能够将精力放在分析漏洞的影响和严重性上。

查找开源漏洞的最佳方法是使用 SCA 工具。SCA 工具通过检查应用程序中的开源组件来扫描已知漏洞，然后将其与公共或私有的已知漏洞数据库进行对比。

开发人员通常不愿意使用安全工具，担心它们会延迟其工作或者造成错误。但是，对于开发软件的企业来说，实施安全实践和使用安全工具都是至关重要的。虽说扫描工具并非万能的，但是构建安全和高质量的软件需要这些工具。最佳方法是：使用这些工具查找漏洞，然后手动审查代码以进行验证，帮助开发人员重新思考其代码的安全性。

原文名称	The basics of security code review
作者简介	李薇薇（Vickie Li），是 ShiftLeft 公司的开发宣传师。
原文信息	2021 年 5 月 19 日发布于 Help Net Security 原文地址 https://www.helpnetsecurity.com/2021/05/19/security-code-review/
摘 要	对于开发软件的企业来说，实施安全实践和使用安全工具都是至关重要的。虽说扫描工具并非万能的，但是构建安全和高质量的软件需要这些工具。最佳方法是：使用这些工具查找漏洞，然后手动审查代码以进行验证，帮助开发人员重新思考其代码的安全性。
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。