安天智甲有效防护 Nitro 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 Nitro 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。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 Nitro 勒索软件的加密行为。

Nitro 勒索软件使用 .NET 框架开发，运行后在注册表路径 HKCU\Software\Microsoft\Windows\CurrentVersion\Run 下添加键 "NR" 并将值设为 Nitro 勒索软件的路径，以实现持久化。同时通过判断该注册表键值对是否存在来避免二次加密。对桌面、我的图片、我的文档目录下的所有文件进行加密，采用的加密策略为使用 AES-128 加密算法加密文件，加密密钥为硬编码。被加密的文件会被追加文件名后缀 ".givemenitro"。在加密完成后会将密钥明文写入至 %temp%\NR_decrypt.txt 中，并弹出如下图的勒索信窗口，要求受害者在 3 小时内缴纳赎金，缴纳方式为价值 9.99 美元的 Discord 礼品卡。Discord 为全球内流行的即时通讯工具。

▲Nitro 勒索软件勒索信

Nitro 勒索软件采用 AES-128 加密文件，密钥被明文存储在 %temp%\ NR_decrypt.txt 中。可以通过该密钥解密被加密的文件。

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、文件相似分析鉴定器、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（WinXP）鉴定器、动态（Win 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 静态分析鉴定器将文件判定为木马程序。

◆概要信息

文件名	92190c9789485a0d96bced7040080f0ae35c02898c3d31a65d50ecd659b80f09
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	62 KB
MD5	077FCCC46159F8CCD79FCD50787DB1C9
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[HEUR]/Msil.Ransom
判定依据	BD 静态分析

报告地址：https://1.119.163.6/vue/details?hash=077FCCC46159F8CCD79FCD50787DB1C9

◆运行环境

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

◆常见行为

行为描述	危险等级
疑似键盘记录	★★
加 / 解密相关 API	★
枚举进程	★
创建进程	★
使用 HTTP 协议的 URL	★
socket 通信	★
IPV4 地址	★
操作系统信息	★
同步机制	★
.....	.....

◆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10日(总第277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

商业窃密木马 Ficker 活动及样本分析报告

概述

近日，安天 CERT 监测到一个活跃的商业窃密木马 Ficker，最早出现于 2020 年 10 月。近期通过伪造 Microsoft Store、Spotify、在线文档转换器等网站进行传播，在一个月内快速迭代十多个版本。

Ficker 窃密木马具备多种窃密功能，包括窃取系统信息、窃取浏览器信息、窃取应用程序凭证、屏幕截图等功能，并且可以窃取多个加密货币钱包。该窃密木马通过检测计算机语言环境，如果为俄罗斯、乌兹别克斯坦、乌克兰、亚美尼亚、哈萨克斯坦、阿塞拜疆、白俄罗斯的语言环境，则不会执行恶意代码。2021 年 1 月，该窃密木马开始在俄语黑客论坛上公开售卖，传播方式由于购买者的不同逐渐产生了变化，例如通过伪装成主题为 DocuSign 的 Word 文档进行传播。与此同时，多个攻击组织实施过该木马的分发。例如，Hancitor 恶意软件在感染独立主机时，选择使用 Ficker 窃密木马窃取数据。经验证，安天智甲终端防御系统（简称 IEP）可实现对该窃密木马的查杀与有效防护。

防护建议

针对该窃密木马安天建议企业采取如下防护措施：

企业防护

（1）安装终端防护：安装反病毒软件，建议安装安天智甲终端防御系统；

（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）部署入侵检测系统（IDS）：部署流量监控类软件或设备，便于对恶意代码的发现与追踪溯源。安天探海威胁检测系统（PTD）以网络流量为检测分析对象，能精准检测出已知海量恶意代码和网络攻击活动，有效发现网络可疑行为、资产和各类未知威胁；

（4）安天服务：若遭受恶意软件攻击，建议及时隔离被攻击主机，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。

网站传播防护

（1）尽量不打开来历不明的网页链接；

（2）不随意点击网站上的广告信息；

（3）在威胁情报分析系统中查询 URL 是否具有威胁。

经验证，安天智甲终端防御系统（简称 IEP）可实现对该窃密木马的查杀与有效防护。（原文链接：https://mp.weixin.qq.com/s/ntRjWEekN59d8X-0VkHaDw）

扫描右侧二维码阅读全文

安全厂商披露具有经济动机的组织 UNC2447

FireEye 观察到一个具有经济动机的组织 UNC2447，利用一个 SonicWall VPN 0day 漏洞（补丁未发布之前），部署复杂恶意软件 SOMBRAT。研究人员还将 UNC2447 与勒索软件联系起来。UNC2447 首先使用 FIVEHANDS 勒索软件攻击并敲诈受害者，然后通过引起媒体关注和在黑客论坛上出售受害者数据来施加压力以迫使受害者支付赎金。从而获利。UNC2447 已被观察到针对欧洲和北美的组织，并一直显示出逃避检测和减少入侵后取证的先进能力。根据对部署技术和时间观察，研究人员怀疑 UNC2447 可能在 2020 年 5 月至 2020 年 12 月期间使用 HELLOKITTY 勒索软件，而 FIVEHANDS 勒索软件则是自 2021 年 1 月左右起一直使用。（原文链接：https://www.fireeye.com/blog/threat-research/2021/04/unc2447-sombrat-and-fivehands-ransomware-sophisticated-financial-threat.html）

研究人员发现基于 Rust 的 Buer 恶意软件变种

网络安全研究人员周一披露了一个新的垃圾邮件活动，该活动分发了用 Rust 编写的名为“ Buer”的恶意软件加载程序的新变种，说明了攻击者正不断打磨其恶意软件工具集来逃避检测。该恶意软件被称为“ RustyBuer”，通过伪装成 DHL 支持机构发

货通知的电子邮件进行传播，新的 Buer 变种是用 Rust 编写的，Rust 是一种高效且易于使用的编程语言，正变得越来越流行，用 Rust 重写恶意软件可以使攻击者更好地逃避现有的 Buer 检测功能。（原文链接：https://thehackernews.com/2021/05/a-new-buer-malware-variant-has-been.html）

每周安全事件

类 型	内 容
中文标题	谷歌发布 Android 五月更新修复了 42 个漏洞
英文标题	Android May 2021 Update Out, Fixes Over 40 Vulnerabilities
作者	George Dascalu
内容概述	谷歌于 2021 年 5 月发布的 Android 操作系统更新共修复了 42 个漏洞，其中有 4 个被标记为严重。 新的安全补丁 2021-05-01 修复了在系统组件中发现的三个主要关键漏洞。所有这三个安全漏洞都可以被利用来在易受攻击的 Android 设备上执行任意代码。在“框架”部分，最严重的漏洞是一个恶意本地应用程序可以绕过用户交互要求，从而获得额外的权限。
链接地址	https://news.softpedia.com/news/android-releases-updates-for-may-2021-which-patches-over-40-vulnerabilities-532811.shtml

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 Raw Image Extension 远程代码执行漏洞（CVE-2021-28468）	高	Microsoft Raw Image Extension 存在远程代码执行漏洞。由于 Raw Image Extension 中的输入验证不正确，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 Excel 远程代码执行漏洞（CVE-2021-28451）	高	Microsoft Excel 存在远程代码执行漏洞。由于 Microsoft Excel 中存在输入验证错误，使得攻击者可以诱骗受害者打开特制文件或访问恶意网站，并在目标系统上执行任意代码。
	Microsoft Windows Media 远程代码执行漏洞（CVE-2021-27095）	高	Microsoft Windows Media 存在远程代码执行漏洞。由于 Windows Media 视频解码器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。
较为活跃样本家族	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[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[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.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[Backdoor]/Win32.Salgorea	中	此威胁是一种可以下载恶意代码的木马类家族。该家族样本运行后连接网络下载恶意代码并执行。
	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。

三个措施防止攻击者售卖企业环境的访问权限

兰登·温克沃斯 / 文 安天技术公益翻译组 / 译

想象一下，执法人员与企业的安全团队联系，告知他们攻击者正在售卖其敏感业务应用程序的员工凭证或私有访问密钥。即使尚未确认这些攻击者访问或窃取了企业数据，这也是非常令人不安的。在当今的企业环境中，这类威胁越来越普遍。为了确保此类威胁不会演变为全面的数据泄露事件，乃至损害公司的声誉，老练的企业知道他们需要及时采取行动，并在企业边界外获得可见性。这些行动通常包括外部威胁猎杀、取证，以及使用开源情报（OSINT）对攻击者进行溯源。即使企业能够成功地进行攻击者溯源，但是要想确定其是针对性攻击的目标，还是机会性攻击的目标，企业仍有很长的路要走。

尽管如此，企业仍然可以采取下述三个措施来确保数据系统的机密性、完整性和可用性。

协同响应

企业首先要确保进行协同响应，包括法律、人力资源、信息技术和安全团队的响应。首要任务是，确保数据系统的机密性、完整性和可用性。企业可以通过对泄漏凭证进行溯源来实现这一点。如果执法机构或第三方供应商与企业安全团队联系，则安全团队可以从他们那里获得泄露的用户凭证或私钥，并与攻击者进行交互。

一般而言，如果攻击者在地下论坛上售卖凭证，则执法部门能够获得其账户信息。掌握这些信息后，企业可以对攻击者进行研究，以评估其技术能力以及在地下论坛中的活跃程度。例如，暗网卖家与实际进入企业环境的恶意行为者，通常会有不同的技术水平。在调查的这一阶段，攻击者对企业造成的损害通常是未知的，安全团队可以采取下述三项措施：1）删除访问权限；2）确定造成的损害；3）确定能否根据攻击情况对攻击者进行溯源，以了解攻击的性质。

删除未经授权的访问并确定损害

确认凭证和账户访问权限之后，安全团队需要确定造成的损害。这包括识别未授权访问、横向移动、恶意工具使用、恶意软件部署，以及攻击者是否访问和泄露数据的证据。通过适当的日志记录（数据收集策略）、双因子身份鉴别（在边界和内部）、端点和网络监控、分段策略（即使只是强化的访问控制策略）和补丁管理，可以阻止安全事件升级为全面的数据泄露事件。

理想情况下，攻击者在企业网络中的时间有限，只能导致恶意身份鉴别，不会造成进一步的损害。如果企业尚未实施主动的防御措施，则有必要重新评估其安全堆栈，或与专家进行全面的安全评估。

在响应特定攻击时，安全团队应进行外部威胁监控并与攻击者交互，以确定攻击者是否试图利用安全事件或从中牟利。在这一阶段，企业不必揭露需要对攻击负责的个人。如果通过评估确定，攻击者是通过从第三方存储库中抓取的重复使用凭证、暴力破解口令，或者是从先前的数据泄露中获取的重复使用口令，来获得访问权限的，那么企业环境内部可能不会再发生恶意活动了。

另一方面，如果通过调查，安全团队怀疑内部人员或前雇员需要对攻击负责，可以对攻击者进行溯源。这样可以获得关键的背景信息，有助于企业避免数据泄露以及采取法律行动。

进行溯源

如果企业是针对性攻击（而非机会性攻击）的受害者，那么对攻击者进行溯源有助于企业获得更多的背景信息，确定发生攻击的原因并量化未来的风险，而且不会耗费太多的资源。基于前两步中确定的情报、取证信息和事件执行周期，企业可以确定安全事件是否会上升到数据泄露级别。如果调查确定存在下述情况之一，则需要对攻击者进行溯源。

1. 从内部人员手中购买凭证
2. 默认凭证被保留
3. 前雇员创建的账户仍然有效
4. 超过 6 个月未轮换的账户被有意或无意地分享

在过去的十年中，溯源主要针对民族国家或攻击者层面。但是，根据攻击情境，在个人层面进行溯源变得越来越重要了。企业需要记住，他们只能保护自己看到的东西。尽管通过边界和内部洞察来确保网络的机密性、完整性和可用性是很重要的，但在防火墙之外具有相同的可见性，也变得越来越重要了。

原文名称	3 Steps to Disrupt Threat Actors Selling Access to Your Environment
作者简介	兰登 · 温克沃斯（Landon Winkelvoss），是 Nisos 的联合创始人兼安全战略副总裁。
原文信息	2021 年 5 月 5 日发布于 Security Week 原文地址 https://www.securityweek.com/3-steps-disrupt-threat-actors-selling-access-your-environment
摘 要	想象一下，执法人员与企业的安全团队联系，告知他们攻击者正在售卖其敏感业务应用程序的员工凭证或私有访问密钥。即使尚未确认这些攻击者访问或窃取了企业数据，这也是非常令人不安的。在当今的企业环境中，这类威胁越来越普遍。为了确保此类威胁不会演变为全面的数据泄露事件，乃至损害公司的声誉，企业需要及时采取行动，并获得企业边界外的可见性。
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。