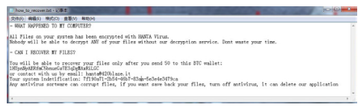
安天智甲有效防护 Hanta 勒索软件

近日，安天 CERT 在梳理网络安全事件时发现了一个名为 Hanta 的勒索软件。该勒索软件变种最早于 2021 年 3 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 Hanta 勒索软件的加密行为。

Hanta 勒索软件使用 .NET 框架开发，运行后会通过检测用户名、调试状态标志位、以及是否存在敏感模块来判断自身是否正在被调试、是否运行在虚拟环境，如果是则退出进程，随后拷贝自身到启动目录并命名为 HANTA.exe，并在注册表路径 SOFTWARE\Microsoft\Windows\CurrentVersion\Run 下添加键 "hanta_ransom" 并将值设为 HANTA.exe 的路径，以实现持久化。该样本采用 AES-256 算法对各磁盘下常见后缀的文本、文档、图片、数据库、源代码文件进行加密，其中加密密钥根据一个 15 位随机数生成，而该随机数会和主机信息一起被发送到远程 C2，远程 C2 的地址是通过请求硬编码的 URL http[:]//wfgvdfgbhdxgb.ueuo.com/current_mirror 获取的。Hanta 勒索软件没有删除卷影的行为，受害者可尝试通过卷影恢复数据。加密完成后在桌面释放名为 "how_to_recover.txt" 的勒索信，要求用户向指定比特币地址支付 50 美元的赎金，同时桌面背景也会被替换。



▲Hanta 勒索软件勒索信

Hanta 勒索软件采用“AES-256”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、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、反病毒引擎鉴定器、智能学习鉴定器将文件判定为木马程序。

◆概要信息

文件名	22e496083d46047375130e0a2dd4cd78
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	16.64 MB
MD5	22E496083D46047375130E0A2DD4CD78
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[Downloader]/MSIL.Genmaldow
判定依据	反病毒引擎

报告地址：https://1.119.163.6/vue/details?hash=22E496083D46047375130E0A2DD4CD78

◆常见行为

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

◆常见行为

行为描述	危险等级

加 / 解密相关 API	★
哈希算法	★
枚举进程	★
创建进程	★
IPV4 地址	★
socket 通信	★
操作系统信息	★
权限操作类相关函数	★
可执行文件	★
.....	.....

◆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 04 月 19 日 (总第 274 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

关于 Google Chrome 远程代码执行 0Day 漏洞通报

概述

2021 年 4 月 13 日，安天 CERT 发现国外安全研究员发布了 Google Chrome 浏览器远程代码执行 0Day 漏洞的 PoC，攻击者可以利用漏洞构造特制的页面，用户访问该页面会造成远程代码执行，漏洞影响 Chrome 最新正式版（89.0.4389.114）以及所有低版本。安天 CERT 跟进复现，由于 Google Chrome 浏览器在国内使用率较高，该漏洞存在被恶意代码利用进行大范围传播的风险，威胁等级高。同时安天 CERT 测试发现部分国内使用 Google Chrome 内核的其他浏览器也受其影响。目前如 Microsoft Edge 等浏览器已经默认运行在沙盒模式下安天 CERT 测试，该漏洞若被单独使用则不能击穿 Chrome 的沙盒模式，但并不意味着，这不是一个严重的漏洞，因为在实际攻击中，多个漏洞可能被组合使用，若该漏洞与其他穿透沙盒的漏洞组合使用，则可能具有极大安全威胁。

总结

在相关浏览器现有默认策略下进行漏洞复现结果说明：操作系统和应用本身的安全机制的持续增强，在攻击缓解方面能够起到一定的效果。但同时，随时保持版本更新和补丁升级，依然是非常必要的。系统自身安全策略设置、版本和补丁更新、第三方主机安全软件的主防机制的有效结合，都是非常必要的主机系统安全支点。（原文链接：https://mp.weixin.qq.com/s/5tVxAbWglHEWca10IcE87w）

鉴于 Chrome 内核的浏览器在国内有广泛的应用，包括 360 安全浏览器、遨游浏览器、搜狗浏览器、极速浏览器等，建议相关厂商迅速展开验证排查。我们已经紧急报送国家相关部门，安天 CERT 建议客户在尽快采取临时解决方案以避免受此漏洞影响。

扫描右侧二维码阅读全文

第二起 Google Chrome 远程代码执行 0Day 漏洞事件通报

概述

2021 年 4 月 14 日，安天 CERT 发现安全研究员发布了一个 Google Chrome 浏览器远程代码执行 0Day 漏洞的 PoC，攻击者可以利用漏洞构造特制的页面，用户访问该页面会造成远程代码执行，漏洞影响 Chrome 目前最新正式版（90.0.4430.72），同时该漏洞也影响基于 Chromium 内核的 Microsoft Edge 正式版（89.0.774.77），目前以上两款浏览器已经默认运行在沙盒模式下，安天 CERT 测试该漏洞若被单独使用则不能击穿沙盒模式。但在实际攻击中，多个漏洞可能被组合使用击穿沙盒，带来极大安全威胁。由于 Google Chrome 和 Microsoft Edge 等浏览器在国内使用率较高，该漏洞存在被恶意代码利用进行大范围传播的风险，威胁等级高。

同时，安天 CERT 测试发现部分国内使用 Google Chrome 内核的其他浏览器也受其影响。鉴于 Chrome 内核的浏览器在国内有广泛的应用，包括 360 安全浏览器、遨游浏览器、搜狗浏览器、极速浏览器等，建议相关厂商迅速展开验证排查。（原文链接：https://mp.weixin.qq.com/s/FpytwTG-YEVxXtIQ0S6dvQ）

扫描右侧二维码阅读全文

“雏莺行动”：一起针对俄罗斯的窃密行动

近日，安天 CERT 监测到一起乌克兰针对俄罗斯的窃密行动，该起攻击行动在 TTP（战术、技术 & 程序）中以多种方式对抗杀毒软件和防火墙设备等安全设备。本次行动中攻击手法简单，载荷尚未成熟，注册域名数量较少，并且夜莺是乌克兰的标志性动物之一，因此安天将这次攻击活动命名为“雏莺行动”。

该起攻击行动主要通过钓鱼邮件进行传播，将邮件伪装为俄罗斯联邦储蓄银行（Sberbank）官方通知，诱导受害者下载附件中的带有宏的 Office 文档，并诱使受害者执行恶意宏代码。一旦文档中的恶意宏被执行，会在多层下载解码后运行此次攻击行动的有效载荷，对除乌克兰以外国家的设备进行攻击。该样本会窃取浏览器的 Cookies、登录信息和支付信息回传给攻击者 Telegram 服务器，造成受害者财产损失和机密信息泄露。

此次行动，攻击者将窃密功能隐藏在最终的载荷里并且在内存中加载一段 ShellCode 与远程服务器保持通信，窃密载荷一旦发现目标系统有沙箱系统、调试行为，以及目标系统属于乌克兰的设备，便立即自删除。通过对该起行动时间、域名（攻击者使用的域名为 usamyforever.com，译为“我永远的美国”）等背景关联，推测是乌克兰针对俄罗斯的一起窃密行动。（原文链接：https://mp.weixin.qq.com/s/6CEhZ9K71zcslg40rYHaqg）

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	伊朗纳坦兹核设施疑似遭遇网络攻击
英文标题	Iran Calls Natanz Atomic Site Blackout 'Nuclear Terrorism'
作者	Associated Press
内容概述	伊朗上周日称其纳坦兹地下核设施遭遇停电，并表示此次停电是“核恐怖主义”行为的结果。虽然没有立即宣称对此事负责，但怀疑对象落在了以色列，以色列媒体几乎一致报道了一场由该国策划的毁灭性网络攻击导致了停电。
链接地址	https://www.securityweek.com/iran-calls-natanz-atomic-site-blackout-nuclear-terrorism

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 Exchange Server 远程代码执行漏洞（CVE-2021-28480）	高	Microsoft Exchange Server 存在远程代码执行漏洞。由于 Microsoft Exchange Server 中的输入验证不严谨，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。
	Win32k 特权提升漏洞（CVE-2021-28310）	高	Win32k 组件存在特权提升漏洞。由于 Windonws 系统中 win32k.sys 驱动程序中存在内存边界错误，使得本地用户可以运行特制程序来触发内存损坏实现特权提升。
	Microsoft Office 远程代码执行漏洞（CVE-2021-28449）	高	Microsoft Office 存在远程代码执行漏洞。由于该应用对输入数据验证不严谨，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。
较为活跃样本家族	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/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/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[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/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。

工业物联网的兴起以及如何减轻风险

亚尼夫·瓦迪 / 文 安天技术公益翻译组 / 译

随着数字化转型的加速和 IT 与 OT 网络的融合，物联网（IoT）和工业物联网（IIoT）设备成为石油和天然气、能源、公用事业、制造、药品以及食品和饮料等行业的重要工具。这些设备不仅能够优化单个流程，还能优化整个工厂以及其他关键基础设施生态系统，有助于提高生产效率，可靠性、响应能力、质量和交付能力。

但是，随着企业引入越来越多的 IIoT 设备（大多数设备在设计时未考虑到安全性），这些设备也会给企业环境带来风险。大约 4 年前，NotPetya 勒索软件攻击了包括医疗、能源和交通运输等行业的众多跨国公司，使很多公司的业务陷入停顿，造成了约 100 亿美元的损失。近几年来，黑客攻击联网汽车篡改引擎和刹车等关键系统的案例层出不穷。最近，我们费了很大的力气才阻止了一起旨在污染佛罗里达州供水系统的攻击。

可以想象一下，攻击者破坏顶级制药公司的生产造成药物短缺，或篡改食品和饮料公司的产品配方的情况，这并非不可能的事。最近，在针对关键基础设施的 seigeware 攻击事件中，黑客感染了企业赖以运行办公基础设施（灯光、电梯、空调和暖气）的系统以及物理安全系统。而在 GPS 欺骗攻击中，攻击者则可以干扰导航系统，诱导驾驶员偏离航线。攻击者可以通过多种手段利用联网设备，以执行恶意操作或在后台进行操作，这会给用户造成经济损失，甚至人身伤害。这些风险都是真实存在的。

Gartner 将这些网络和资产统称为“网

络物理系统”（cyber-physical systems，CPS），并预测，到 2023 年，CPS 攻击导致人员伤亡的损失将超过 500 亿美元。Gartner 指出，即使不把人的生命纳入考虑范围，企业在赔偿、诉讼、保险、监管罚款和声誉损失方面的成本也将是非常巨大的。Gartner 预测，到 2024 年，将有 75 % 的首席执行官需要对 CPS 事件承担责任，因此企业迫切需要减轻此类风险。

如何减轻风险

美国《物联网网络安全改进法案》于 2020 年 12 月 4 日正式生效，旨在减轻 IoT 设备日益增加所带来的风险。该法案指出，企业在识别 IoT 设备引入的漏洞和供应链风险方面缺乏统一性。因此，该法案提出了相关的标准和准则，以替代如今企业采用的“个体性”方法。该法案包含若干规定，但最重要的是一点是，使用联邦政府资金购买的 IoT 设备必须满足新的最低安全标准。

虽说该法案针对的是政府机构以及与之合作的供应商和服务提供商，但是各个领域的关键基础设施公司都可以借鉴该法案，以增强和规范其 IoT/IIoT 安全最佳实践。

从哪里开始?

关键基础设施公司需要识别和跟踪跨 IT 和 OT 边界的 IoT/IIoT 设备带来的威胁。但是现实情况是，数十年来，OT 网络一直是 IT 安全专家的盲点。随着越来越多的老旧 OT 资产联网，以及工业企业司向其环境中添加更多联网设备以推动自动化和现代化，此类安全挑战会越来越严峻。由于缺乏可见性和监控功能，OT 和 IT 安全团队常常两眼一抹黑，无法识别已部署在企业环境中的 CPS 并跟踪其行为。

主动的风险管理，能够从不同但互补的角度检查和应对风险，可以提供 OT 环境整体安全性的情境信息。要实现主动的风险管理，关键是了解企业的资产风险状况和网络流量。

要想了解资产风险状况，企业应对工业控制系统（ICS）网络和端点具有可见性，并在无需增加连接的情况下整合 IT、OT、IoT 和 IIoT 资产信息。这样一来，人机界面（HMI）、安全专家和工程工作站（EW）就可以获取有关 IT 威胁和漏洞的信息，从而在不影响生产力或造成停机的情况下增强这些资产的安全性。

与网络流量相关的情境安全信息，也是识别和跟踪跨 IT/OT 边界的威胁之关键。影响 OT 环境的许多攻击都始于 IT 网络，因此防御者除了要获取 IT 系统的威胁特征，还要获取 ICS 设备和 OT 网络的威胁特征。采用无需重新配置特征或手动更新即可保护 CPS 的技术，可以加快检测和响应速度。

IIoT 设备已迅速成为现代 OT 环境的标志，以及竞争优势的加速器。企业应了解 IIoT 设备的风险及其成本并借鉴新法规的规定，以应对 IIoT 设备给工业环境带来的风险。

原文名称	The Rise of Industrial IoT and How to Mitigate Risk
作者简介	亚尼夫·瓦迪（Yaniv Vardi），是 Claroty 公司的首席执行官。
原文信息	2021 年 04 月 06 日发布于 Security Week 原文地址 https://www.securityweek.com/rise-industrial-iot-and-how-mitigate-risk
摘 要	随着数字化转型的加速和 IT 与 OT 网络的融合，物联网（IoT）和工业物联网（IIoT）设备成为石油和天然气、能源、公用事业、制造、药品以及食品和饮料等行业的重要工具。但是，随着企业引入越来越多的 IIoT 设备，这些设备也会给企业环境带来风险。本文概述了如何减轻此类风险。
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。