安天发布《Odveta 勒索软件变种分析报告》

近日，安天 CERT 在梳理网络安全事件时发现一个名为 Odveta 的勒索软件变种，该勒索软件隶属于 Ouroboros 勒索软件家族，此家族最早于 2019 年 4 月被发现，主要通过垃圾邮件传播。

Odveta 勒索软件执行后，加密计算机上的可执行程序和文档文件，在原文件名后追加名为“.Email=[联系邮箱] ID=[USER_ID].Odveta”的后缀，以两种不同方式创建勒索信，其中一个是在 %programdata% 目录下释放并运行名为“uiapp.exe”的可执行文件，另一个是在含有被加密文件的目录下创建名为“Unlock-Files.txt”的文本文件，勒索信内容包含勒索说明、联系邮箱、比特币购买教程网址、数据加密算法和 USER_ID 等。勒索软件使用“AES+RSA”加密算法加密文件，调用多个命令行进程关闭系统防火墙、SQLSERVER 等服务，同时调用命令行命令来防止受害者恢复已加密的文件，具体操作为删除卷影副本、删除本地计算机的备份目录等。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，避免一切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口令；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病毒的鉴定；安天智甲已经实现了对该勒索病毒的查杀。

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，下为其自动形成的分析报告：

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、关联分析鉴定器、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、字符串分析鉴定器、来源信息鉴定器、智能学习鉴定器、静态特征检测鉴定器、安全云鉴定器、信标检测鉴定器、动态（Win7 x86）鉴定器、等鉴定分析。

最终依据 BD 静态分析鉴定器、关联分析鉴定器、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	Zeropadypt.exe
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	987 KB
MD5	117C3707F4D8DB004A0E7EF86350612B
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[Ransom]/Win32.Crypren
判定依据	反病毒引擎

完整报告地址：https://1.119.163.6/vue/details?hash=117C3707F4D8DB004A0E7EF86350612B

◆ 操作系统

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
在启动时禁用 Windows 错误恢复	★★★★
通过 WMI 查询操作系统信息	★★★
通过 WMI 查询 CPU 信息	★★★
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	★
创建挂起进程	★★
获取驱动器类型	★
获取系统信息（处理器版本、处理器类型等）	★
获取系统版本	★
获取计算机名	★
枚举进程	★
检测自身是否被调试	★★

◆进程监控

PID	创建	命令行
1340	target.exe	"c:\3d73f7caa5e54b4e87b159cfc258d06c\share\target.exe"
1424	cmd.exe	C:\WINDOWS\system32\cmd.exe /c net stop SQLWriter
1304	net.exe	net stop SQLWriter
1624	net1.exe	net1 stop SQLWriter
1728	cmd.exe	C:\WINDOWS\system32\cmd.exe /c net stop SQLBrowser
1752	net.exe	net stop SQLBrowser
.....	.....	.....

安天周观察
安天官方微博 安天官方微信
主办：安天 2020 年 2 月 24 日 (总第 219 期) 试行 本期 4 版 微信搜索：antiylab 内部资料 免费交流

疫情防控期的几类网络安全威胁分析与防范建议

新型冠状病毒感染的肺炎疫情发生后，安天启动重大社会事件网络安全应急值守制度。截止 2 月 18 日，安天 CERT 发现和跟踪了多起利用新冠肺炎疫情相关信息进行网络攻击的案例，攻击者利用新冠肺炎疫情相关信息，传播勒索软件、挖矿木马、远控后门等多种类型的恶意代码，实施网络攻击。**相关详细信息均及时上报国家和地方相关主管部门，为加强政企客户和公众防范意识，将其中部分信息摘要发布。**

【态势研判】

从安天发现和跟踪的案例看，并没有新的高级技术和 0day 漏洞在其中应用。其主要的特点是利用疫情期间大家对于热点信息的高度关注，用内容引诱，采用钓鱼等方式加以侵害；传播勒索软件、木马、远控后门等。根据目前的案例，从技术上判断没有形成网络恶意代码蔓延态势的苗头。

【威胁概要】（专业人士参考，技术细节请参看下文）

疫情防控期间，一线抗疫机构和保障机构的四大便捷建议：

1、【专机专用】办公期间，注意工作用计算机近期内不要用于非工作目的，特别是不要浏览主要传播源社交媒体；

2、【不明不看】不要打开来源不明的任何内容。包括链接地址、文件、图片、邮件中的附件、短信中的短链接等；

3、【每天备份】及时备份重要文件；可以考虑每天备份，或在交接岗的时候备份。备份对于近期最容易带来直接损失的勒索软件，很有防范效果。

4、【求助专家】向 IT 专业人士或网络安全专业人士求助。

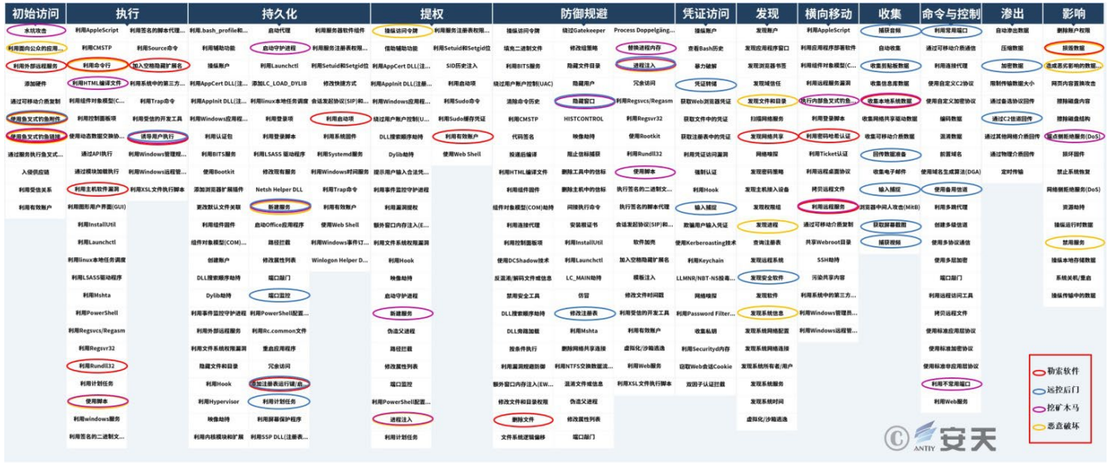
进一步的给相关一线 IT 保障人员的基础技术建议还包括个人用户及政企用户防护建议，详见防范建议。

【其他概要】

利用社会热点是社会工程学攻击的惯常方式，其中公共卫生事件就是其中经常利用的。历史上通过蹭热度传播恶意代码事件屡见不鲜，例如，2014 年犯罪团伙借助“埃博拉病毒”的信息“行骗”，针对关注埃博拉病毒的用户进行钓鱼邮件攻击；2015 年网络攻击者借中东呼吸综合征（MERS）在韩国肆虐期间开展网络攻击活动等，此类事件往往借助用户对疫情的恐慌心理而盲目点击各种信息，以及疫情防控响应中网络安全防护能力难以及时有效跟进，SOHO 办公缺少足够安全保障等机会提高网络攻击的成功率。

今后此类事件和恶意代码仍会继续增加。本报告披露相关恶意代码的与恶意功能，以供相应防范。**安天应急响应团队 24 小时值守，协助用户提升网络防护和响应能力，为新冠肺炎疫情防控提供网络空间**

（下转第三版）



疫情防控期间几类安全事件对 ATT&CK 的映射

每周安全事件

类 型	内 容
中文标题	AZORult 木马伪装成 ProtonVPN 进行分发
英文标题	AZORult Trojan Disguised Itself as Fake ProtonVPN Installer
作者及单位	DAVID BISSON
内容概述	安全研究人员观察到了 AZORult 木马的样本，他们伪装成 ProtonVPN 安装程序进行分发。早在 2019 年 11 月，恶意行为人就通过向俄罗斯注册商注册域名“protonvpn[.]store”发起了这一攻击活动。在此最新攻击中，AZORult 收集了受感染机器的环境数据，并将其发送到位于 accounts[.]protonvpn[.]store 的命令与控制 (C&C) 服务器。然后，恶意软件开始窃取用户感兴趣的信息。
链接地址	https://www.tripwire.com/state-of-security/featured/azorult-trojan-disguised-itself-as-fake-protonvpn-installer/

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 8 个移动平台恶意代码和 6 个 PC 平台的恶意代码和漏洞值得关注

恶意代码类别		名称与发现时间	威胁等级	简要描述
移动恶意代码	新出现的样本家族	Trojan/Android.Joker2.v[prv,pay,exp] 2020-02-16	高	该应用程序伪装正常应用，包含恶意代码，运行后联网下载恶意子包，解析控制命令，静默模拟点击广告，订阅付费业务，窃取用户短信、联系人列表和设备信息，造成用户隐私泄露和经济损失，建议卸载。
		G-Ware/Android.FakeWzry.h[fra,exp] 2020-02-17	低	该应用程序伪装王者荣耀点券充值，本身无实际功能，诱导用户分享该程序，造成用户流量消耗，建议不要使用。
		G-Ware/Android.FakeApp.hx[exp,rog] 2020-02-18	低	该应用程序经过重打包后伪装肺炎疫情辟谣 app，进入实际为一款游戏，运行后台会加载广告，调用第三方支付插件，为避免造成用户资费消耗，建议卸载。
	较为活跃样本	Trojan/Android.Prizmes.a[prv,exp]	中	该应用程序伪装其他应用，后台监听用户短信、删除用户短信信息、获取用户位置信息、联网获取远程指令，并私自发送短信至指定号码，造成用户隐私泄露及资费消耗，建议卸载。
		Trojan/Android.FakeSystem.bh[prv,fra,exp]	中	该应用程序伪装系统应用，运行隐藏图标，监听用户短信，获取用户固件信息、短信内容并联网上传到指定网址，会造成用户隐私泄露，建议立即卸载。
		G-Ware/Android.LockScreen.cw[rog,lck]	中	该应用程序运行后隐藏图标，上传用户手机固件信息，锁定用户界面并勒索付费，影响手机正常使用，建议卸载。
		RiskWare/Android.Daikuan.t[rog]	低	该应用程序运行访问第三方网贷网站，可能没有财产权益保障，会造成用户财产损失，请谨慎使用。
		G-Ware/Android.HiddenApp.cv[exp,rog]	低	该应用程序伪装知名应用，运行隐藏图标，后台加载广告，推广应用，警惕其私自下载，造成用户的资费消耗，建议卸载。
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Windows 远程执行代码漏洞（CVE-2020-0662）	高	Windows 无法正确处理内存中的对象时，会触发一个远程代码执行漏洞。成功利用此漏洞的攻击者可以通过提升权限在目标系统上执行任意代码。攻击者可随后安装程序；查看、更改或删除数据；或者创建拥有完全用户权限的新帐户。
	较为活跃样本	Trojan[Downloader]/Win32.Agent	中	此威胁是一种以基因片段定性的木马类程序。它会在被感染的电脑中下载恶意程序并更新恶意程序版本。恶意程序下载成功后，会在操作系统启动时自动运行。该家族常在用户首次访问有漏洞的网站时入侵用户电脑。
		Trojan[Dropper]/Win32.FrauDrop	中	此威胁是一种具有捆绑行为的木马类程序。该家族会损坏被感染电脑的注册表文件，阻止用户访问系统。该家族会随系统运行自启动，并利用连续弹窗和虚假警告消息欺骗用户，还会损坏任务管理器和系统还原功能。此外，该家族会感染操作系统，收集用户隐私信息发送给黑客。
		Trojan/Win32.Qhost	中	此威胁是一种木马类程序。该家族会修改 Host 文件，以阻止用户访问杀毒网站或网站更新数据等。通常 Windows 主机文件只包含本地主机信息，该家族变种会在主机文件中添加条目，试图阻止用户访问杀毒网站及杀毒网站的服务器更新等。该家族还可以通过专门改变 Host 文件的服务器来重定向网站，窃取用户的用户名、密码等信息。
		GrayWare[AdWare]/Win32.iBryte	低	此威胁是一种广告类程序。该家族可以在电脑上打开后门，并注入其他恶意程序。该家族还可以连接远程服务器，让黑客可以访问电脑并窃取用户的个人资料。
		RiskWare[Downloader]/Win32.Plocust	低	此威胁是一种具有下载行为的风险软件类程序。该家族的主要目的是在电脑中下载并运行风险软件类程序。

（下转第三版）

保障。

利用新冠肺炎疫情进行社工传播样本分析

安天 CERT 监测到多起利用新型冠状病毒肺炎疫情相关热词传播恶意代码的事件，攻击者利用新冠肺炎疫情相关信息将恶意代码文件名伪装成“**冠状病毒**”“**菲律宾各大楼冠状肺炎名单 .exe**”“**新型冠状病毒肺炎病例全国已 5 名患者死亡；警惕！！ .exe**”等热门字样诱导用户运行。并针对勒索软件事件、远控后门事件、挖矿木马事件、恶意破坏事件、钓鱼邮件事件进行了分析说明。（样本分析及详细说明请扫描文末二维码查看）

防范建议

安天提醒广大用户：

1、疫情防控期间办公，及时安装更新补丁，避免恶意代码利用漏洞入侵计算机；

2、避免使用弱口令或统一的口令；

3、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；

4、对非受信来源的邮件保持警惕，避免点击邮件中的链接或运行邮件附件；

5、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；

6、安装具有主动防御能力的终端防护软件（如安天智甲），既可以实时监控邮件附件，同时也能够对勒索软件提供有效防护；

7、及时备份重要文件，且文件备份应与主机隔离。

安天提醒政企用户：

• 远程办公终端安全方面

建议远程办公的员工在接入政企机构内部网络之前，对自身电脑、手机等终端进行自身安全检查。一方面，检查终端操作系统、常用软件是否处于最新版本，及时安装更新补丁，避免恶意代码利用漏洞入侵计算机；另一方面，安装安天智甲终端防御系统等相关终端安全防护产品，为远程办公终端提供恶意代码检测与查杀、勒索软件防护、高级威胁防护等安全保障。

建议在异地员工逐步复工的背景下，从远程办公恢复到常态办公时，应恢复到原来办公网络应有的防护等级，需要进行相关的终端安全核查与业务衔接。

• 远程办公接入安全方面

建议通过 VPN 加密方式接入办公网络环境，划分逻辑隔离的远程接入安全域，设置多因子认证方式，并限制通过远程接入员工的访问权限，对远程接入的客户端进行相应的安全检查，如是否安装终端安全防护软件等判断条件。

• 数据安全防护方面

建议在确保终端环境安全的前提下，员工在相关工作文件进行交换的过程中，应采取必要的加密措施，企业侧应部署相应的文件深度分析产品，对通过企业虚拟局域网传输的文件进行威胁分析，以避免具备远程控制或信息窃取能力的恶意代码在办公网络中传播。建议政企机构安全管理员及时备份相关重要文件及数据，并确保文件备份与主机隔离。

• 远程安全运维方面

建议针对内网资源实施严格的远程安全运维管理措施，限定相关帐户的访问区域、访问权限等，并将安全日志的审计动作落到实处。

• 加强安全意识方面

建议在特殊时期，对非受信来源的邮件保持警惕，避免点击邮件中的链接或运行邮件附件，将可疑的文件对象投放到企业部署的动态沙箱中进行分析鉴定（如安天追影威胁分析系统）。

安天 CERT 会持续跟踪并披露网络空间攻击者以疫情为诱饵投放恶意软件等事件。

（微信扫描二维码即可阅读完整报告）

研究人员披露 Microsoft 存在子域劫持漏洞

NIC.gp 的安全研究员和开发人员 Michel Gaschet 今天指出，微软在管理其数千个子域方面存在漏洞，其中许多子域可能被劫持并用于攻击用户、员工或显示垃圾内容。Gaschet 说，他在 2017 年向微软报告了 21 个容易被劫持的 msn.com 子域 [1，2]，然后在 2019 年又报告了 142 个配置错误的 Microsoft.com 子域 [1，2]。Gaschet 称，在所有报告的配置错误的子域名中，微软只解决了其中的几个。

（原文链接：https://www.zdnet.com/article/microsoft-has-a-subdomain-hijacking-problem/）

研究人员发现 SharePoint 中存在一个远程执行代码漏洞

安全专家发现 SharePoint 中的一个漏洞，攻击者可以通过发送特制的 SharePoint 应用程序包来利用该漏洞远程执行任意代码。漏洞跟踪为 CVE-2019-0604，研究人员在浏览 ZoomEye 寻找此类组件时发现了这个漏洞。该应用程序 (incometaxindia.gov.in) 被发现存在漏洞，因为它使用 SharePoint 作为一种技术来托管其服务。此外，麻省理工斯隆管理学院也被发现易受 CVE-2019-0604 攻击。

（原文链接：https://securityaffairs.co/wordpress/98043/hacking/sharepoint-rce.html）

思科发布针对其网络和统一通信线路的安全补丁

思科发布了针对其网络和统一通信线路的 17 个漏洞的补丁。该软件包含有一个关键问题的修补程序和六个被视为高危漏洞的补丁程序。它们包括远程访问和代码执行、提升特权、拒绝服务和跨站点请求伪造。唯一的关键公告是 CVE-2020-3158，这是一个由 Cisco Smart Software Manager 工具中存在具有静态密码的高权限帐户引起的漏洞。思科表示，该漏洞是由一个系统账户的默认和静态密码造成的，它不受系统管理员的控制。“攻击者可以利用这个漏洞，使用这个默认帐户连接到受影响的系统。”

（原文链接：https://www.theregister.co.uk/2020/02/19/cisco_february_fixes）