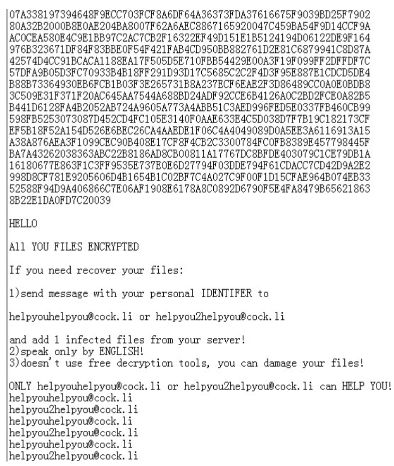
安天智甲有效防护 HelpYou 勒索软件

勒索软件名：HelpYou 勒索软件
传播方式：垃圾邮件、RDP 弱口令
加密算法：ChaCha20 + NTRU
后缀：.IQ_IQ
支付与金额：需通过邮箱与勒索者联系 E-Mail：helpyouhelpyou@cock.li 和 helpyou2helpyou@cock.li
免费解密工具：暂未发现

近日，安天 CERT 在梳理网络安全事件时发现一个 HelpYou 勒索软件。最早于 2021 年 3 月被发现，主要通过垃圾邮件、RDP 弱口令渗透进行传播。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 HelpYou 勒索软件的加密行为。

HelpYou 勒索软件样本运行后，会释放自身副本到 %Local% 或 %Appdata%，通过设置注册表 HCU\Software\Microsoft\Windows\CurrentVersion\RunOnce，设置键为 LicChk，值为副本路径，实现持久化。删除系统卷影，以防止恢复加密文件，删除远程登录记录和日志，以清除访问痕迹。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，在被加密文件的文件名后追加名为“.IQ_IQ”的后缀。样本会在每个目录下创建名为“HOW_TO_RECOVERY_FILES.txt”的勒索信，勒索信中仅包含 KEY 和联系邮箱，具体勒索金额、赎回方式等需要和勒索者联系。


07A338197394648F9ECC703FCF8A6DF64A36373FDA37616675F9039BD25F7902
80A32B2000B8E0AE204BA8007F62A6AEC8867165920047C459BA54F9D14CCF9A
AC0CEA580E4C9E1BB97C2AC7CB2F16322EF49D151E1B5124194D06122DE9F164
976B323671DF84F83BBE0F54F421FAB4CD950BB882761D2E81C6879941C8D87A
42574D4CC91BCACA1188EA17F505D5E710FBB54429E00A3F19F099FF2DFFDF7C
57DFA9B05D3FC70933B4B18FF291D93D17C5685C2C2F4D3F95E887E1CDCD5DE4
B88B73364930EB6FCB1B03F3E265731B8A237ECF6EAE2F3D86489CC0A0E0BDB8
3C509E31F371F20AC645AA7544A688BD24ADF92CCE6B4126A0C2BD2FCE0A82B5
B441D6128FA4B2052AB724A9605A773A4ABB51C3AED996FED5E0337FB460CB99
598FB5253073087D452CD4FC105E3140F0AAE633E4C5D038D7F7B19C182173CF
EF5B18F52A154D526E6BEC26CA4AAEDE1F06C4A4049089D0A5EE3A6116913A15
A38A876AEA3F1099CEC90B408E17CF8F4CB2C3300784FC0FB8389E457798445F
BA7A43262038363ABC22B8186AD8CB00811A17767DC8BFDE403079C1CE79DB1A
16180677E863F1C3FF9535E737E0E6D27794F03DDE794F61CDACC7CD42D9A2E2
998D8CF781E9205606D4B1654B1C02BF7C4A027C9F00F1D15CFAE964B074EB33
52588F94D9A406866C7E06AF1908E6178A8C0892D6790F5E4FA8479B65621863
8B22E1DA0FD7C20039

HELLO

All YOU FILES ENCRYPTED

If you need recover your files:

1)send message with your personal IDENTIFER to

helpyouhelpyou@cock.li or helpyou2helpyou@cock.li

and add 1 infected files from your server!
2)speak only by ENGLISH!
3)doesn't use free decryption tools, you can damage your files!

ONLY helpyouhelpyou@cock.li or helpyou2helpyou@cock.li can HELP YOU!
helpyouhelpyou@cock.li
helpyou2helpyou@cock.li
helpyouhelpyou@cock.li
helpyou2helpyou@cock.li
helpyouhelpyou@cock.li
helpyou2helpyou@cock.li

▲HelpYou 勒索信

HelpYou 勒索软件采用“ChaCha20 对称加密算法 + NTRU 非对称加密算法”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、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	93af6e140df248b256d89a4b2a612066cd22d8f12d585b6b6c309ef3c720ecf9
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	75 KB
MD5	364CC95EADF3C00B449741A4D6E5296A
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.Filecoder
判定依据	反病毒引擎

报告地址：https://1.119.163.6/vue/details?hash=364CC95EADF3C00B449741A4D6E5296A

◆危险行为

行为描述	危险等级
删除全盘所有卷影副本	★★★★

◆常见行为

行为描述	危险等级
疑似查找浏览器进程	★★
自我复制	★★
获取当前激活的窗口	★★
文档篡改	★★
设置文件属性为隐藏	★★
疑似桌面控制	★
加载运行时 DLL	★
打开自身进程文件	★
Run 自启动	★
runonce 自启动	★
获取驱动器类型	★
访问文件尾部	★
获取系统版本	★
删除远程登录记录和日志	★
获取系统信息(处理器版本、处理器类型等)	★
独占模式打开，防止复制读取，防止杀毒软件扫描上报	★

◆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 03 月 15 日 (总第 269 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

全国政协委员肖新光：两份提案聚焦网络安全顶层设计

全国政协十三届四次会议已经胜利闭幕。全国政协委员、安天科技集团董事长、首席技术架构师肖新光提交两份提案，聚焦推动网络安全顶层设计和防护能力建设。

关于提升“十四五”网络安全规划的整体性、系统性和针对性的提案

“十三五”期间，我国网络安全产业快速发展，网络安全防御能力全面提升，全民网络安全意识逐步增强。但日趋复杂严峻的国际国内形势，对我国网络安全能力的发展速度和与信息化的融合程度提出了更高要求。

总书记在《中共中央关于制定国民经济和社会发展第十四个五年规划和二〇三五年远景目标的建议》的说明中指出：“我国发展仍然处于重要战略机遇期，但面临的国内外环境正在发生深刻复杂变化。”“十四五”的网络安全发展规划同时面对保障重要发展战略机遇期、应对重大安全风险期的双重挑战，需要坚持问题导向、目标导向、结果导向，正确处理好发展与安全、存量与增量关系，统筹规划、加速投入、精准施策。

建议

针对上述问题，需要准确把握国家安全形势变化新特点新趋势，坚持总体国家安全观，贯彻落实习近平总书记关于网络强国的重要思想，及时按照新的发展目标和新的风险挑战，打破惯性沿袭，因时而变、因需而变。

一是完善总体国家安全综合研判机制，提升网络空间安全在其中的权重占比。要深入研究各种传统安全和非传统安全的传递演化关系，将地缘安全风险、重大社会风险与网络安全风险态势分析研判深度结合，并结合相关行业、区域的重要信息系统、关键信息基础设施的实际防护水平与发展规划，定位防御盲点、发现重大短板、确定投入重点，保障和优化资源投入。

二是把握“十四五”规划和实施机遇，全力推动网络安全的需求侧改革。2020 年 12 月 11 日召开的中共中央政治局会议提出，“要扭住供给侧结构性改革，同时注重需求侧改革”。建议针对央企网络安全工作，在网络安全党组责任制和“谁建设、谁负责”的基本原则上，推动重点央企网络安全工作考核办法实施，加大对战略应急保障能力建设、服务国家安全、社会治理支撑贡献方面的考核力度，形成弹性的能力层次，推动投入增量产生。对数字化安全转型发布规划指南，进行安全示范样例引导。让安全投入有的放矢，既为构建双循环提供网络安全保障，也高质量创造内循环增量。

三是针对性投入弥补行业和区域的能力短板。利用国有资本金预算和投资基金的多渠道带动作用，以及财政转移支付等机制，加大重点工程分布建设倾斜、对重大风险短板进行集中投入，快速改善东北、西南边疆等既处于地缘安全热点，经济又欠发达地区的网络安全防护水平。

关于构建网络空间安全“机动防御”机制的提案

当前网络空间已经是大国博弈和地缘安全竞合的常态化对抗领域，网络空间安全风险与其他传统安全和非传统安全风险交叉转化、递进叠加，构成连锁反应。

如抗击疫情期间，我国卫生医疗系统、疫苗研究机构、相关院所企业频遭网络入侵攻击，发生多起重要信息或科研成果被窃取事件。而在边界冲突背景下，相关国家频繁进行网空威胁活动，妄图窃取我和其他周边国家政治、经济、军事、科技等方面信息。

建议

建议按照习近平总书记“关口前移，防患于未然”、“备豫不虞，为国常道”的安全要求，展开如下工作：

一是完善多部委联席风险研判机制，强化网络安全风险动态研判、形成动态化重点保障清单。基于阶段性重大社会风险和地缘安全风险进行预测推演，对可能遭遇高级别网络入侵攻击的目标行业、地域和人员等形成动态清单和调整机制，实现重点布防；配套建立弹性调整防护目标等级保护级别的机制，实现对相关工作的制度性支撑。

二是由国家主管部门组织、财政统一拨款，构建国家－地域两级网安“机动防御”机制、战略储备库和日常运维机制。建立针对机动防御目标快速介入、动态调整布防策略、部署监测防御环节、进行响应处置的闭环工作机制，快速构建防御纵深。充分发挥国家互联网应急中心、国资国企在线监管运营中心等机构的枢纽作用，联合网络安全企业和行业协会实现人员机动组织，实现针对网络出口、关键内网、关键服务、关键主机等重点场景的快速布防能力和重点人员网络安全的针对性保障机制，形成“网络－信息－人”联动的安全回路。支持能力型安全企业构建用于大规模样本和安全数据集中分析、大规模流量清洗等的云计算基础设施资源池。将流量监测、端点防护响应、应急取证处置、威胁分析、攻击捕获等方面的优秀产品列入到国家物资储备机制当中，形成相关机制的物资保障。在安全风险等级降低后，相关机制解除，装备回收入库。

三是以威胁溯源、猎杀作为“机动防御”的更高目标要求。不仅要实现快速部署，改善防御，快速止损、精确量损；同时要进一步实现信息留存、证据固化、威胁诱捕等机制，有效发现攻击线索、获取攻击载荷；通过推动情报共享和联动机制，联合分析、协同溯源，确定攻击组织，必要时予以披露曝光。

上述举措不能替代政府央企网络安全防护能力的自我提升。旨在国家主管、监管和应急机构原有的安全检查、监测、通报机制和“谁建设、谁负责”的自我安全防护能力建设的双层防御之间，增加一个国家层面的弹性机动的防护能力层次。增加安全防护能力面向攻击方的不可预测性，提升战略威慑能力。

(原文链接：https://www.antiy.cn/About/news/20210310.html)

扫描右侧二维码阅读全文

每周安全事件

类 型	内 容
中文标题	Exchange Marauder 攻击活动：利用多个微软 Exchange 零日漏洞
英文标题	Operation Exchange Marauder: Active Exploitation of Multiple Zero-Day Microsoft Exchange Vulnerabilities
作者	Josh Grunzweig, Matthew Meltzer, Sean Koessel, Steven Adair, Thomas Lancaster
内容概述	2021 年 1 月，Volexity 通过其网络安全监视检测到来自两个客户的 Microsoft Exchange 服务器的异常活动。Volexity 识别出大量数据发送到一个 IP 地址。并对 IIS 日志进行了检查，日志显示图像、程序、表和 Outlook Web Access（OWA）使用的字体相关的有效文件的入站请求。Volexity 通过对系统内存分析，确认攻击者利用 Microsoft Exchange（CVE-2021-26855）中的零日服务器端请求伪造（SSRF）漏洞窃取了几个用户邮箱的全部内容。此漏洞可以远程利用，不需要任何形式的身份验证和任何特殊知识，只需要知道运行 Exchange 的服务器以及要从中提取电子邮件的帐户即可。
链接地址	https://www.volexity.com/blog/2021/03/02/active-exploitation-of-microsoft-exchange-zero-day-vulnerabilities/

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 安全漏洞（CVE-2021-26855）	高	攻击者可构造恶意 HTTP 请求，并通过 Exchange Server 进行身份验证。进而扫描内网，获取用户敏感信息。
	Microsoft Exchange 安全漏洞（CVE-2021-26858）	高	攻击者通过 Exchange 服务器进行身份验证后，可以利用此漏洞将文件写入服务器上的任何路径。
	Microsoft Windows Win32k 权限提升漏洞（CVE-2021-1732）	高	Win32k 系统进程中存在一个权限提升漏洞，经过身份验证的本地攻击者可利用此漏洞在目标系统上提升其权限以执行任意代码。
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/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.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[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[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]/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。

网络弹性的组成部分

安天技术公益翻译组 / 译

在网络安全方面，诸如 SolarWinds 供应链攻击之类的事件已经清楚地表明：如今的攻击已不再局限于病毒的简单传播或拒绝服务（DoS）攻击。网络攻击者开始部署高级持续性威胁（APT），这种威胁甚至可以利用已妥善打补丁且受监控的基础架构。为应对新冠疫情，各企业迅速过渡到分布式员工队伍，这加剧了安全挑战，扩大了 IT 可见性、追责和安全控制持久性方面的既有差距。越来越多的 CISO 开始将网络弹性作为确保企业持续运营的新兴手段。那么，网络弹性到底是什么？与传统的网络安全实践相比，它又如何呢?

网络弹性的定义

根据 MITRE 的说法，网络弹性“是指预测，承受，从不利条件、压力、攻击或对网络资源造成的损害中恢复并进行适应的能力。”企业意识到，传统的安全措施已不足以确保信息、数据和网络安全，因此他们对网络弹性的需求不断增加。网络弹性观点认为，现代企业基础架构由大型和复杂的实体组成，因此将始终存在攻击者能够利用的漏洞和弱点。在这种情况下，网络弹性的目的是确保网络攻击事件（无论有意还是无意的，无意的网络攻击事件由软件更新失败导致）不会对企业业务运营的机密性、完整性和可用性产生负面影响。

网络安全措施采用旨在保护系统（例如服务器和端点）、网络和数据免受网络攻击的技术、流程和措施。相比之下，网络弹性措施则侧重于企业 IT 环境中的检测和响应控制，以评估差距并增强整体安全状况。大多数网络弹性措施可以利用或增强各种网络安全措施。当网络安全和网络弹性措施一起使用时，效果最佳。

越来越多的网络风险和安全管理框架开始采用网络弹性的概念。例如，美国国土安全部的网络弹性评估（CRR）提供了有关如何评估组织的运营弹性和网络安全实践的指南。此外，美国国家标准技术研究院（NIST）特刊 800-160 第 2 卷，为工程安全可靠的系统提供了一个框架——将不利的网络事件既作为弹性问题又作为安全问题进行处理。

网络弹性的组成部分

像“零信任”一样，网络弹性适用于如今不断扩大的攻击面，因此涵盖以下网络资源。

- 网络
- 数据
- 工作负载
- 设备
- 人（即身份）

网络资源，以及网络资源易受攻击的范围，取决于寻求网络弹性的环境。在任何情况下，企业对在这些不同网络资源上建立网络弹性措施的优先考虑，都应通过对黑客战术、技术和程序（TTP）的评估来驱动。

例如，端点通常被用作黑客和网络罪犯发起攻击的入口点，这些攻击可能感染企业的整个网络，或者充当在网络内横向移动的滩头堡。实际上，Ponemon Institute 最近的一项调查显示，在过去的 12 个月中，有 68％的企业遭受了端点攻击。尽管企业进行了广泛的尝试来保护端点安全，但该数字表明企业的安全性正在被迅速侵蚀，因此他们需要端点弹性，这是网络弹性的组成部分之一。端点弹性使企业能够始终了解端点的位置，对这些设备进行深度控制和安全操作，并在其禁用、或遭受其他破坏时帮助其进行安全控制和自我修复。

网络弹性的优势

诸如“端点弹性”之类的网络弹性策略，可在网络攻击之前、期间和之后提供一系列优势，包括：

- **强化安全状态**：网络弹性不仅有助于企业应对攻击，还可以帮助其制定战略来改善 IT 监管、增强关键资产的安全性、扩展数据保护工作并最大程度地减少人为错误。
- **改善合规性**：如今，许多行业标准、政府法规和数据隐私法律都在推广网络弹性。
- **提高 IT 生产力**：网络弹性被低估的优势之一是，它可以改善企业 IT 团队的日常运营，提高其对威胁的响应能力，并有助于确保日常运营顺利进行。

网络弹性措施（即架构设计、技术、运营实践）假设，当今的威胁源可以在企业的基础架构中创建据点，而企业必须阻止漏洞被利用后的攻击活动。如果企业正确实施网络弹性措施，则可以有效防范人为错误，恶意行为以及老化、不安全软件的漏洞。最终，网络弹性的目标是积极保护整个企业，包括上述所有可用的网络资源。因此，企业需要在整个基础架构中创建不同类型的网络弹性。

原文名称	The Different Flavors of Cyber Resilience
原文信息	2021 年 03 月 03 日发布于 Security Week 原文地址 https://www.securityweek.com/different-flavors-cyber-resilience
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。