安全威胁每周警讯

2019/07/7～2019/07/13

本周威胁指数

亚信安全 网络安全监控中心

前十大病毒警讯

排名	病毒名称	威胁类型	风险等级	趋势	病毒行为描述
1	TROJ_EQUATED.J	Trojan	★★	→	此特洛伊木马可能与恶意软件包捆绑在一起作为恶意软件组件。它作为被其他恶意软件丢弃的文件或用户在访问恶意站点时在不知不觉中下载的文件到达系统。它可以由用户手动安装。
2	Trojan.Win32.EQUATED.LZCWQ	Trojan	★★	↑	木马病毒，它可能是使用者手动安装的。
3	Trojan.Win32.EQUATED.LZCWR	Trojan	★★	→	木马病毒，它可能是使用者手动安装的。
4	Trojan.Win32.EQUATED.LZCWO	Trojan	★	↑	木马病毒，它可能是使用者手动安装的。
5	BKDR_VOOLS.B	Backdoor	★★	↑	它可能是使用者手动安装的，会下载其他恶意软件
6	Global DKIM Enforcement rule	Spam	★	↓	DKIM 全局策略
7	TROJ_ETEROCK.C	Trojan	★★	↑	此特洛伊木马可能与恶意软件包捆绑在一起作为恶意软件组件。它作为被其他恶意软件丢弃的文件或用户在访问恶意站点时在不知不觉中下载的文件到达系统。
8	BKDR_EQUATED.LZCMU	Backdoor	★	↑	它可能是使用者手动安装的，会下载其他恶意软件
9	TROJ_EQUATED.LZCMT	Trojan	★★	↑	木马病毒，它可能是访问可疑网站时下载的，一般是用于自启动其他病毒
10	TROJ_EQUATED.O	Trojan	★★	↑	木马病毒，它可能是使用者手动安装的。默认垃圾邮件规则。

本周安全趋势分析

AsiaInfo 亚信安全

病毒预警

2019 年 7 月 12 日

攻击 NAS 设备的 eCh0raix 勒索病毒预警

事件描述

研究人员发现了新型勒索病毒 eCh0raix，该勒索病毒针对 QNAP 网络附属存储（NAS）设备进行攻击，其攻击行为类似于 Ryuk 和 LockerGoga 勒索病毒，亚信安全将其命名为 Ransom.Linux.ECHORAIX.A。

NAS 设备是网络连接的存储设备，主要用于文件存储和备份系统。由于其成本低，效率高并且可扩展，受到用户欢迎，其市场占有率高达 80% 。受本次勒索病毒影响的 NAS 设备包括 QNAP TS-251、QNAP TS-451、QNAP TS-459 Pro II 和 QNAP TS 253B。

病毒技术细节分析

eCh0raix 勒索病毒使用 Go/Golang 语言编写，该病毒通过检查语言来确定被感染的 NAS 设备所处的位置，如果其位于白俄罗斯、乌克兰和俄罗斯等独联体国家，其会终止自身。其还会结束系统中存在的如下进程或者服务：

- apache2
- httpd
- nginx
- mysqld
- mysql
- php-fpm
- php5-fpm

- postgresq

该病毒会加密系统中的文档、文本、PDF、压缩、数据库以及多媒体等多种文件，其加密的文件扩展名列表：

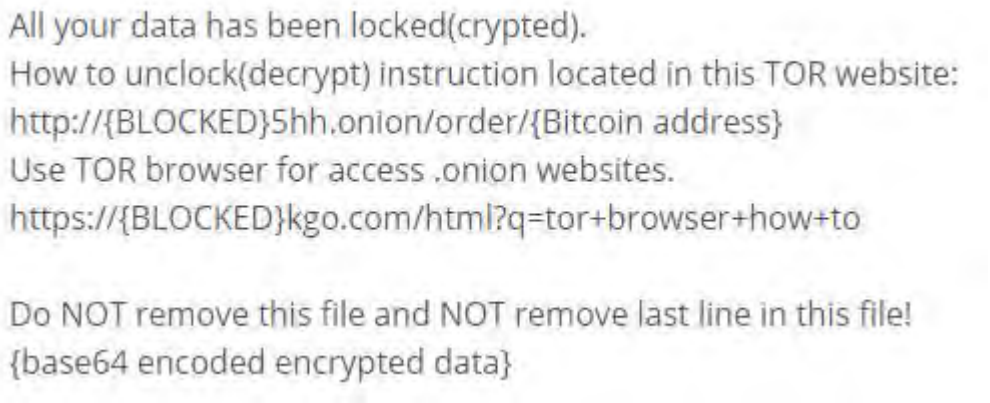
.dat	.dml	.eml	.gho	.iqy	.ksd	.mpd	.oam	.pdf	.ptx
.db0	.dmp	.epk	.gif	.iso	.lbc	.mpp	.odb	.pef	.pub
.dba	.dng	.eps	.gne	.itl	.lbf	.mvc	.odc	.pem	.qba
.dbf	.doc	.erf	.gpg	.itm	.lrf	.mvr	.odm	.pfx	.qbb
.dbm	.dot	.esm	.gsp	.iwd	.ltx	.myo	.odp	.pgp	.qbo
.dbx	.dwg	.ewp	.gxk	.iwi	.lvl	.nba	.ods	.php	.qbw
.dcr	.dwk	.far	.hdm	.jcz	.lzh	.nbf	.odt	.png	.qbx
.der	.dwt	.fdb	.hkx	.jpe	.m3u	.ncf	.ofx	.pot	.qdf
.dll	.dxf	.fit	.htc	.jpg	.m4a	.ngc	.olp	.ppj	.qfx
.ece	.dxg	.flv	.htm	.jsp	.map	.nod	.orf	.pps	.psp
.fmp	.fwp	.mlx	.htx	.jss	.max	.nrw	.oth	.ppt	.pst
.fos	.gdb	.mov	.hxs	.jst	.mdb	.nsf	.p12	.prf	.psw
.fpk	.key	.moz	.idc	.jvs	.mdf	.ntl	.p7b	.pro	.ptw
.fsh	.kit	.mp3	.idx	.jws	.mef	.nv2	.p7c	.psd	.pdb
.pak	.mjs	.nzb	.ifx	.kdb	.mht	.nxg	.pac	.psk	.pdd

该病毒避免加密文件名中带有如下字符串的文件或者文件夹中的文件：

- /proc
- /boot/
- /sys/
- /run/
- /dev/
- /etc/
- /home/httpd
- /mnt/ext/opt
- .system/thumbnail
- .system/opt
- .config
- .qpkg

病毒加密后的文件扩展名为.encrypt，加密完成后，该病毒索要 0.05-0.06 比特币的赎金，受害者

需要通过 Tor 网站支付赎金。



目前对于 eCh0raix 勒索病毒的感染方式还不确定，但是有研究人员发现，受感染的 NAS 设备没有安装最新的补丁程序，并且使用的是弱口令。据此我们猜测，此勒索病毒可能是利用漏洞或者弱口令攻击传播。

解决方案

- ✓ 更改默认凭据或添加用于访问 NAS 设备的身份验证和授权机制；
- ✓ 及时更新 NAS 设备的固件；
- ✓ 确保其他系统或设备（尤其是连接到 NAS 设备或内置于 NAS 设备的路由器）保持更新；
- ✓ 实施最小权限原则：仅在必要时启用功能或组件（例如，在路由器上打开端口）或限制使用 VPN 才可以通过 Internet 访问 NAS 设备；
- ✓ 启用 NAS 设备的内置安全功能；例如，QNAP 的网络访问保护有助于阻止暴力攻击或类似的入侵；
- ✓ 请注意备份重要文档。备份的最佳做法是采取 3-2-1 规则，即至少做三个副本，用两种不同格式保存，并将副本放在异地存储。

亚信安全解决方案：

- ✓ 亚信安全病毒码版本 15.227.60 ，云病毒码版本 15.227.71，全球码版本 15.229.00 已经可以检测，请用户及时升级病毒码版本。