第3篇: 勒索病毒

0x00 前言

勒索病毒,是一种新型电脑病毒,主要以邮件、程序木马、网页挂马的形式进行传播。该病毒性质恶劣、危害极大,一旦感染将给用户带来无法估量的损失。这种病毒利用各种加密算法对文件进行加密,被感染者一般无法解密,必须拿到解密的私钥才有可能破解。自WannaCry勒索病毒在全球爆发之后,各种变种及新型勒索病毒层出不穷。

0x01 应急场景

某天早上,网站管理员打开OA系统,首页访问异常,显示乱码:

| 濲中祭恝:◆M遅nl岬qF◆=輻6N度|| 壶\$ - 遊p-||柵||娟喕S鏒n裰電奶胺/◆2Gn2◆|| 専覦pF殖q/◆(-誠◆5饀蓏: W &yjlu踝a炒◆.'◆ 十2*=◆=顸|| 川*&d绸◆觜绣华渥荫] 躷\�� m�\$尼◆Bw◆3◆媣臂樋C渽珍◆″債9篲,◆ ◆+堰潭0瑗◆?iv64.q◆?[閷餣z.躴Q~A竿vn苆纑′铏29.-p€\◆/鷌` 嚅燔鵕眪媦匩儉*D◆F®穼鉈◆*.P" [澹◆ iC t/ 摺″◆″=闸濃®◆(|K珥 #鮟髌罔冘檲B◆鮭r7 潜◆″L舔◆僑疠 ex◆ !eulZ◆觺◆+鉂v簽=}F鰶◆3◆.9L礰缮 a+ 3◆m6-轅2◆ Bn哈纸楠◆) 瘛◆細香÷鲗 I哩J駅1朳挛袑 ◆8列n岫%~0按V \spadesuit . J | \spadesuit 6炬鷹诡蘛~~q)飧撼sDuh \spadesuit _q圓0 \spadesuit 裔膳 R \spadesuit 9 \spadesuit 繁蔚 蚚嫩耢 ⇔ \spadesuit 6; \spadesuit 麽犦舉湔館蓰 \spadesuit an \spadesuit ″狙 \spadesuit . 宏 \spadesuit 9 _鎧U眺'0 甲輮鰂楪砩% \spadesuit 襽 \spadesuit Ez哨 万:徐6◆s 黄纾qr鼜x校@騷芨(铣pW◆#鍼I軿◆m◆8(團nP◆泼(耵戮◆41 q碩橬|0珙+癉5J挽C 欕k◆&'錙瘺◆K阵蛁棒o独3鰶◆:◆=拊奥/ {Z遹◆+ 標◆&派状 J90)蚃 葱%店hz◆-市◆`◆_◆1! €6-酶齧∭9鵙V◆;鼊 8YD胰€<酢;理9熹裙◆綇坯關6日fc◆◆0搔◆*唧褳B[€幞◆0◆湮懻◆◆醋妹◆&f:1傳:笭b惝瘠 戈磺kBK+=氟◆ 饨gC餐◆ 誰,欄]E�順:S經購 樾D勉\W烷C毿i 6註"bl◆ 鰀.`e璵W匀{��制p娥遌>Q?◆'髣◆廮闳m釓hM抽劢?◆8x]酵◆2踓|v辟&xD◆閊tFi_ 稢蔰/娜偃\◆麘1D峋霭絭欦丩 4:B◆砣]◆ R鰛歐圖卡偲◆%r劍N\$(6€k2?i鸉q化@J,}◆ }◆ `碌;ia獸蜧 '拊)◆n倩 ◆ _偘h霞鼉◆,吋谋I 猶欔<\$dT7) n荒;傏燮鐵疁雄(上縣y挫◆SI蒭F邊廳應咴瑷牸◆◆ ◆為敏柜G冢勁篱E。◆P石亭j x◆'◆O◆?渤◆鰔≈j鳝z[吳LC 堓h篿檛咢 极阉鐇写 wjw◆ v>趣額韭稣SdINz\$諚◆一<忆渍◆踏◆ h撌繗栝v(o抴鲇 在rs-| N較S?◆ W}h. ♦ ♦T婇N♦?芠V軏钙霞CP漂!♦+!. 噉6M!♦訓操犓gS◆E幣=♦pX!執Y逩 L♦h榹 銮櫣 蛙F稍誦 纋鈣濯 拗pCmH\b蜓◆8椄退禹◆*簝%仏j誚舖%◆3+0硟◆渺S@Bi琶z!患 歌E搒◆鐾″褻◆\$h聛◆騭 警鴰◆ A◆ 蝄◆ 埴H% 敼4W◆\$摂鮘濁◆®◆<根* ◆雇\◆®2孽尓乄搚虵壷樒TG+遺◆庀 鈡h髖`◆;(~(K簑#(镗[X讪◆8_\$e◆z押.歺1坻 汪€盤蹦k63◆{♦2◆ Pa4U僚泛顫瞰 /.? 較C反詔*6 p0◆7m◆##繫銷K杻焟帜)桕 箜鲸**K鱇 "◆!◆5D鱭◆, Jc◆+2做c|繢)P}鱉縷?旃趼Q鐴".轟◆r唣<斫醖tP B琬◆ G◆>@P%!Rt!診bZQ淚I el鍵AK\◆(唇V:x#a*z)爐壓◆ 亃xs珷q噢◆)龢◆7チ歪總斆權t◆,◆B. 腹辇wV媈x◆(抄諭◆◆ 僰 褸{揀k梚CトL{QPQ給诚優F[簳9�5�-卑◆ ◆+\$踞璽#?旁◆?!А鯲P诉艘ki恶 h1Ut垱�◆)亿~ P◆5U=(泞A蝚筆kJ P束◆nVA _[薭豬M氮渫鱉笈A鰈◆◆◆<氾;绑◆ \M◆◆ 瘗讐Q藟I1羧1寓W!@\UO郟鬃|頻寬Rc28痧喻D襩 恕:D価魥& 墴~b撪h◆奡碗[;殪崇宙7Y懡r 玑� (BPF)XH�? F(X) F(X)秚 窑 的f ♦ 砠 荤1◆葉◆\卞 I?姚深∜◆◆◆5◆ 牡O €jV防瑩N藤4蠯潊5◆1q錍◆,aG舾A矮腈 F扨柒_:#◆伽敝佟偈 &lvn◆#S◆3淋◆;E◆◆偛◆RLW?Hc膳 約J駸鶲V侁筦 9◆i)惣u恣◆ D◆脪溥\$■ S◆?:◆◆恰c賌}R'擅班歲駐棵U◆ Q塞暱裠B`魚璝s2宾O迾o`◆&◆◆&杯呥,该q ?Y5Y◆5U・◆&w产40@◆]e6夷荢蛶wD\◆

0x02 事件分析

登录网站服务器进行排查,在站点目录下发现所有的脚本文件及附件都被加密为.sage结尾的文件,每个文件夹下都有一个!HELP SOS.hta文件,打包了部分样本:

IHELP_SOS.hta	2017/3/10 2:45	HTML 应用程序	65 KB
📄 249469.第一单元练习.doc.sage	2017/3/10 8:41	SAGE 文件	26 KB
📄 3371916.本科专业培养方案模板-2008.doc.sage	2017/3/10 8:41	SAGE 文件	304 KB
🧻 7281437.关于开展征文活动的重要补充通知.doc.sage	2017/3/10 8:41	SAGE 文件	26 KB
favicon.ico.sage	2017/3/10 2:45	SAGE 文件	1 KB
index.php.sage	2017/3/10 3:25	SAGE 文件	10 KB
index11.php.sage	2017/3/10 3:25	SAGE 文件	1 KB

打开!HELP SOS.hta文件,显示如下:



到这里,基本可以确认是服务器中了勒索病毒,上传样本到360勒索病毒网站(http://lesuobingdu.360.cn)进行分析:确认web服务器中了sage勒索病毒,目前暂时无法解密。

勒索病毒搜索	引擎,对症下药		
支持检索超过270种常见勒索特	病毒,输入病毒名或加密后缀名,或直接上传加密文件,艮	阿找到解密方法、了解病	毒详情
index.php.sage ×		上传文件	查找
根据文件分析结果,您可能中了	以下病毒:		

绝大多数勒索病毒,是无法解密的,一旦被加密,即使支付也不一定能够获得解密密钥。在平时运维中应积极做好备份工作,数据库与源码分离(类似OA系统附件资源也很重要,也要备份)。

遇到了, 别急, 试一试勒索病毒解密工具:

"拒绝勒索软件"网站

https://www.nomoreransom.org/zh/index.html

360安全卫士勒索病毒专题

http://lesuobingdu.360.cn

0x04 防范措施

一旦中了勒索病毒,文件会被锁死,没有办法正常访问了,这时候,会给你带来极大的困恼。为了防范这样的事情出现,我们电脑上要先做好一些措施:

- 1、安装杀毒软件,保持监控开启,定期全盘扫描
- 2、及时更新 windows安全补丁, 开启防火墙临时关闭端口, 如445、135、137、138、139、3389等端口
- 3、及时更新web漏洞补丁,升级web组件
- 4、备份。重要的资料一定要备份, 谨防资料丢失
- 5、强化网络安全意识,陌生链接不点击,陌生文件不要下载,陌生邮件不要打开

后续持续更新内容,将发布在公众号Bypass--,同时公众号提供了该项目的PDF版本,关注后回复"应急响应"即可下载。

