

勒索病毒识别、处置与防御

李华生¹ 黄 进²

¹(杭州安恒信息技术股份有限公司终端安全事业部 杭州 310051)

²(杭州安恒信息技术股份有限公司 杭州 310051)

(wonston.li@dbappsecurity.com.cn)

Identification, Disposal and Defense of Extortion Virus

Li Huasheng¹ and Huang Jin²

¹(Terminal Security Division, Dbappsecurity Co., Ltd, Hangzhou 310051)

²(Dbappsecurity Co., Ltd, Hangzhou 310051)

Abstract Extortion virus mainly spreads in the form of mail, program Trojan horse, web page hanging horse, etc. It encrypts files by using various asymmetric encryption algorithms, and the infected person can not decrypt them generally. Only by getting the decrypted private key, can it be possible to decrypt them. Extortion virus is extremely harsh and extremely harmful. Once infected, it will bring immeasurable loss to users. Therefore, the identification, disposal and defense of extortion virus is particularly important. In the recognition of extortion virus, we usually use the combination of conventional anti-virus software and behavioral identification methods; in the disposal of extortion virus, we can thoroughly clean it up by manual and automatic methods; in terms of defensive measures, traffic level analysis, early warning and terminal level protection and encryption are important links.

Key words extortion virus; terminal EDR; early warning APT; bait engine; protection engine

摘 要 勒索病毒主要以邮件、程序木马、网页挂马等形式进行传播,利用各种非对称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。勒索病毒性质恶劣、危害极大,一旦感染将给用户带来无法估量的损失。因此,勒索病毒的识别、处置和防御就显得尤为重要。在勒索病毒的识别上一般采用常规的杀毒软件与行为识别方法相结合;勒索病毒的处置上一般是人工与自动化的方法并用才可以彻底清理完成;在防御措施上,流量层面分析预警和终端层面的防护和加密阻止都是重要环节。

关键词 勒索病毒;终端 EDR;预警 APT;诱饵引擎;防护引擎

中图法分类号 TP309.5

勒索病毒文件一旦进入本地就会自动运行。接下来,勒索病毒利用本地的互联网访问权限连接至黑客的 C&C 服务器,进而上传本机信息并下载

加密公钥,利用加密公钥对文件进行加密。除了拥有解密私钥的攻击者本人,其他人几乎不可能解密。加密完成后通常还会修改壁纸,在桌面等明显

位置生成勒索提示文件,指导用户去缴纳赎金.勒索病毒变种类型非常快,对常规的杀毒软件都具有免疫性.

攻击的样本以 exe,js,wsf,vbe 等类型为主,对常规依靠特征检测的方式是一个极大的挑战.勒索过程如图 1 所示:



图 1 勒索病毒的入侵过程

1 判断当前状态

1.1 感染未加密

从攻击者渗透进入内部网络的某一台主机到执行加密行为往往有一段时间,如果在这段时间能够作出响应,完全可以避免勒索事件的发生.如果有以下情况可能是处于感染未加密状态:

1) 监测设备告警

如果使用了监测系统进行分析、威胁监测,系统产生大量告警日志,例如“SMB 远程溢出攻击”、“弱口令爆破”等,可能是病毒在尝试扩散,一种攻击过程示例如图 2 所示.

2) 资源占用异常

病毒会伪装成系统程序,释放攻击包、扫描局域网 445 端口等占用大量系统资源,当发现某个疑似系统进程的进程在长期占用 CPU 或内存,有可能是感染病毒.

>		2018-07-20 11:19:09	SMB 远程溢出攻击 尝试SMB远程命令执行 (MS17-010)	16.2	16	0
>		2018-07-20 11:19:07	SMB 远程溢出攻击 尝试SMB远程命令执行 (MS17-010)	172.2	37	0
>		2018-07-20 11:19:07	SMB 远程溢出攻击 尝试SMB远程命令执行 (MS17-010)	172.2	7	0
>		2018-07-20 11:19:07	SMB 远程溢出攻击 尝试SMB远程命令执行 (MS17-010)	10.44	5	0
>		2018-07-20 11:19:05	SMB 远程溢出攻击 尝试SMB远程命令执行 (MS17-010)	10.44	107	0
>		2018-07-20 11:18:47	SMB 远程溢出攻击 尝试SMB远程命令执行 (MS17-010)	172.2	65	0
>		2018-07-20 11:18:37	SMB 远程溢出攻击 尝试SMB远程命令执行 (MS17-010)	10.74	03	0
>		2018-07-20 11:18:31	SMB 远程溢出攻击 尝试SMB远程命令执行 (MS17-010)	172.2	42	0
>		2018-07-20 11:18:31	SMB 远程溢出攻击 尝试SMB远程命令执行 (MS17-010)	172.2	0	0
>		2018-07-20 11:18:28	SMB 远程溢出攻击 尝试SMB远程命令执行 (MS17-010)	172.2	39	0
>		2018-07-20 11:18:26	SMB 远程溢出攻击 尝试SMB远程命令执行 (MS17-010)	172.2	60	0

图 2 攻击过程示例

1.2 感染已加密

勒索病毒的目的是索要赎金,所以会加密文件并在明显位置留下勒索信,通过这 2 点可以判断系统是否已经被加密.

1) 统一的异常后缀

勒索病毒执行加密程序后会加密特定类型的文件,不同的勒索病毒会加密几十到几百种类型的文件,基本都会包括常见的文档、图片、数据库文件.当文件夹下文件变成如下统一异常不可用后缀,就是已经被加密了^[1].图 3 展示出一种后缀被修改的案例.

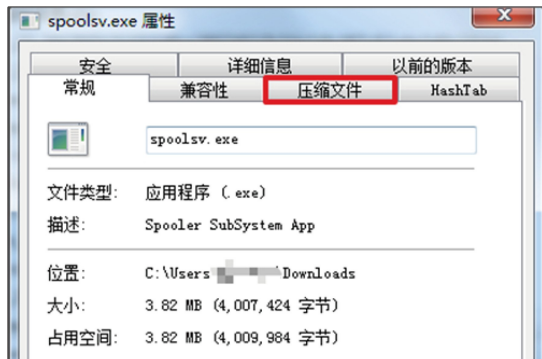
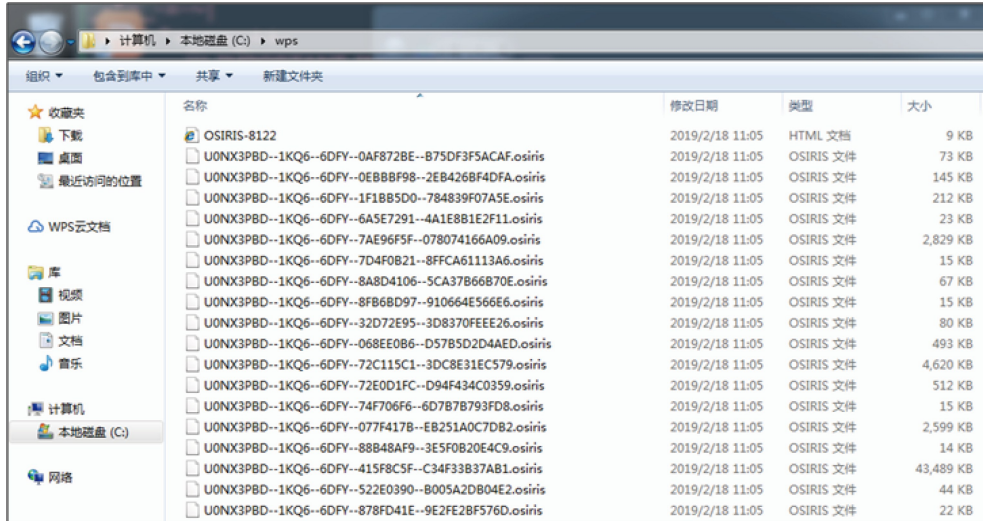


图 3 后缀修改案例

2) 勒索信或桌面被篡改

勒索病毒加密文件的最终目的是索要赎金,所以会在系统明显位置如桌面上留下文件提示,

或将勒索图片更改为桌面。勒索信绝大多数为英文,引导被勒索的用户交赎金。图4示出一种勒索信的案例。



名称	修改日期	类型	大小
OSIRIS-8122	2019/2/18 11:05	HTML 文档	9 KB
U0NX3PBD--1KQ6--6DFY--0AF8728E--B75DF3F5ACAF.osiris	2019/2/18 11:05	OSIRIS 文件	73 KB
U0NX3PBD--1KQ6--6DFY--0E88BF98--2E8426BF4DFA.osiris	2019/2/18 11:05	OSIRIS 文件	145 KB
U0NX3PBD--1KQ6--6DFY--1F18B5D0--784839F07A5E.osiris	2019/2/18 11:05	OSIRIS 文件	212 KB
U0NX3PBD--1KQ6--6DFY--6A5E7291--4A1E8B1E2F11.osiris	2019/2/18 11:05	OSIRIS 文件	23 KB
U0NX3PBD--1KQ6--6DFY--7AE96F5F--078074166A09.osiris	2019/2/18 11:05	OSIRIS 文件	2,829 KB
U0NX3PBD--1KQ6--6DFY--7D4F0821--8FFCA61113A6.osiris	2019/2/18 11:05	OSIRIS 文件	15 KB
U0NX3PBD--1KQ6--6DFY--8A8D4106--5CA37B66870E.osiris	2019/2/18 11:05	OSIRIS 文件	67 KB
U0NX3PBD--1KQ6--6DFY--8FB6BD97--910664E566E6.osiris	2019/2/18 11:05	OSIRIS 文件	15 KB
U0NX3PBD--1KQ6--6DFY--32D72E95--3D8370FEE26.osiris	2019/2/18 11:05	OSIRIS 文件	80 KB
U0NX3PBD--1KQ6--6DFY--068EE086--D57B5D2D4AED.osiris	2019/2/18 11:05	OSIRIS 文件	493 KB
U0NX3PBD--1KQ6--6DFY--72C115C1--3DC8E31EC579.osiris	2019/2/18 11:05	OSIRIS 文件	4,620 KB
U0NX3PBD--1KQ6--6DFY--72E0D1FC--D94F434C0359.osiris	2019/2/18 11:05	OSIRIS 文件	512 KB
U0NX3PBD--1KQ6--6DFY--74F706F6--6D7B7B793FD8.osiris	2019/2/18 11:05	OSIRIS 文件	15 KB
U0NX3PBD--1KQ6--6DFY--077F417B--EB251A0C7DB2.osiris	2019/2/18 11:05	OSIRIS 文件	2,599 KB
U0NX3PBD--1KQ6--6DFY--88B48AF9--3E5F0B20E4C9.osiris	2019/2/18 11:05	OSIRIS 文件	14 KB
U0NX3PBD--1KQ6--6DFY--415F8C5F--C34F33B37AB1.osiris	2019/2/18 11:05	OSIRIS 文件	43,489 KB
U0NX3PBD--1KQ6--6DFY--522E0390--B005A2D804E2.osiris	2019/2/18 11:05	OSIRIS 文件	44 KB
U0NX3PBD--1KQ6--6DFY--878FD41E--9E2FE28F576D.osiris	2019/2/18 11:05	OSIRIS 文件	22 KB

图4 一种勒索信的案例

2 处置与响应

2.1 基础响应措施

某台主机在感染勒索病毒后除了自身会被加密,勒索病毒往往还会利用这台主机去攻击同一局域网内的其他主机,所以当发现1台主机已被感染应尽快采取响应措施,以下基础措施即使不是专业的人员也可以进行操作,以尽可能减少损失。

2.1.1 隔离中毒主机

1) 物理隔离

断网、拔掉网线或禁用网卡,笔记本也要禁用无线网络。图5展示出禁用无线网卡的操作示例。

2) 逻辑隔离

访问控制、关闭端口、修改密码。访问控制可以由防火墙等设备来设置,禁止已感染主机与其他主机相互访问;视情况关闭135,139,445,3389等端口,避免漏洞被RDP(远程桌面服务)利用(关闭

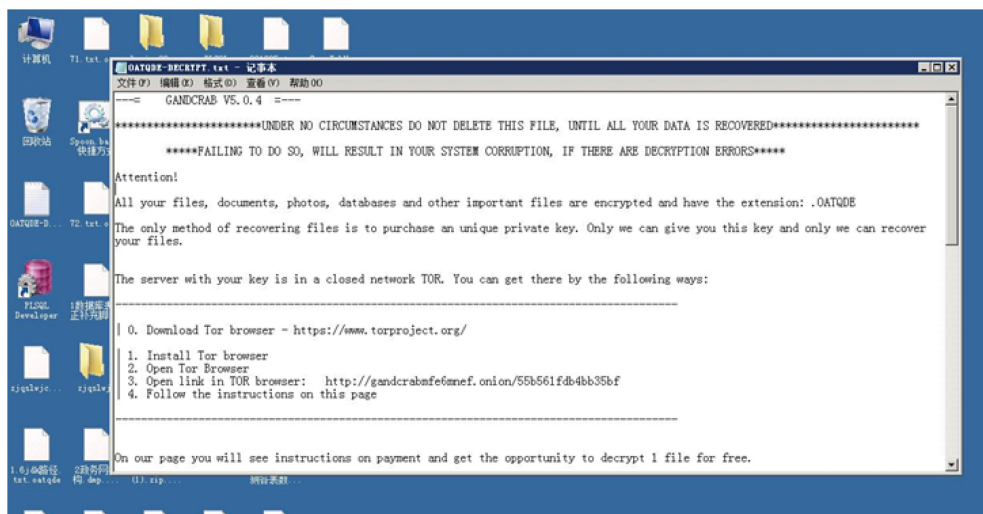


图5 禁用无线网卡操作示例

端口可参考: <https://jingyan.baidu.com/article/295430f1e84daa0c7e00501e.html>); 尽快修改被感染主机与同一局域网内的其他主机的密码, 尤其是管理员(Windows 下的 Administrator, Linux 下的 root)密码, 密码长度不少于 8 个字符, 至少包含以下 4 类字符中的 3 类: 大小写字母、数字、特殊符号, 不能是人名、计算机名、用户名等^[2]。

2.1.2 排查其他主机

隔离已感染主机后应尽快排查业务系统与备份系统是否受到影响, 确定病毒影响范围, 准备事后恢复。如果存在备份系统且备份系统是安全的, 就可以将损失降到最低, 也可以最快地恢复业务。

2.1.3 主机加固

主机感染病毒一般都是由未修复的系统漏洞、未修复的应用漏洞或者弱口令导致, 所以在已知局域网内已有主机感染并将之隔离后, 应检测其他主机是否有上述的问题存在。

1) 系统漏洞可以使用免费的安全软件检测并打补丁。

2) 应用漏洞可以使用免费的漏扫产品(AWVS, APPScan 等)检测并升级或采用其他方式修复。

3) 弱口令应立即修改, 密码长度不少于 8 个字符, 至少包含以下 4 类字符中的 3 类: 大小写字母、数字、特殊符号, 不能是人名、计算机名、用户名等。

3 高级响应措施

基础措施可以在一定程度上响应勒索事件, 但当病毒情况严重、感染主机较多或面对未知类型勒索变种时, 基础措施的效果就十分有限。当有数百台甚至更多主机的场景感染勒索病毒, 是无法逐一去采取基础响应措施, 需要借助专业的安全产品进行监测、防护和专业的安全团队的技术支持。

3.1 流量监测

可以采用设备对网络中传输的已知和未知恶意文件样本结合病毒引擎、静态分析和动态分析, 对勒索病毒及其变种传播及时告警, 对传播类型、传播途径、恶意代码传播、回连域名、漏洞利用等行为进行深度解析, 准确定位感染源和感染主机。

设备可以内置沙箱虚拟执行环境, 对流量中勒索病毒动态行为分析, 捕获其动态行为、网络行为、进程行为、文件行为、注册表行为等关键信息, 识别其中可疑的勒索病毒特点, 快速对网络中传输的勒索病毒样本进行预警。

设备可以通过云端情报共享, 依托于云端海量数据、高级的机器学习和大数据分析能力, 及时共享最新的安全威胁情报, 发现已知和未知威胁恶意样本传播行为, 对勒索病毒更精确地定位分析。

3.2 本地查杀与防护

主机卫士 EDR 类产品通过“平台+端”分布式部署, “进程阻断+诱饵引擎”双引擎防御已知及未知类型勒索病毒^[3]。部署监控端后通过平台统一下发安全策略, 具备诱饵捕获引擎、内核级流量隔离等行业领先技术。对于已知勒索病毒, 通过“进程启动防护引擎”零误报零漏报查杀; 对于未知勒索病毒采用“专利级诱饵引擎”进行捕获, 阻断其加密行为; 通过内核级的流量隔离技术, 自动阻止勒索病毒在内网扩散或者接收远程控制端指令^[4]。

4 已加密系统的处理办法

4.1 备份还原

备份可以是本机、异机或异地(云端)备份, 通常勒索病毒会遍历所有磁盘并加密文件, 同时删除 Windows 的阴影卷, 删除备份历史快照, 所以本机备份恢复的可能性很低。异机备份如果是通过本地磁盘到共享磁盘进行文件或者数据拷贝的方式实现, 勒索病毒同样有可能加密了备份文件。与感染病毒的主机不在同一局域网内的异地备份系统最能在此时发挥作用^[5]。

进行备份还原前要确保原主机上病毒已彻底清除, 应进行磁盘格式化并重装系统。日常进行合理的数据备份是最有效的灾难恢复方法。

4.2 解密工具

大部分勒索病毒使用 128 b 密钥的 AES(对称加密算法)加密文件, 再将 AES 的密钥使用 2048 b 密钥的 RSA(非对称加密算法)加密, 通过暴力破解来解密是不科学的, 所以通常的解密工具是通过已公开的密钥来解密。而密钥来源有 3 种途径:

1) 破解勒索程序得到, 前提是勒索程序本身存在漏洞, 但此概率极低。

2) 勒索者公开密钥。

3) 执法机构获得勒索者的服务器,同时服务器上存储着密钥且执法机构选择公开。

除了付费解密的工具,还可尝试国际刑警组织反勒索病毒网站(<https://www.nomoreransom.org/zh/index.html>)提供的解密工具。

4.3 数据恢复

一部分勒索病毒加密文件时直接加密原文件,还有一部分勒索病毒是加密原文件副本再删除原文件,而原文件有些会用随机数覆盖,有些并没有,原文件没有被覆盖的情况就可以通过数据恢复的方式进行恢复。

除了收费的专业数据恢复,可以尝试使用 DiskGenius (<http://www.diskgenius.cn/download.php>)扫描磁盘进行数据恢复。

4.4 重装系统

当使用上述方法恢复数据后或不需要解密文件,原本的中毒主机都需要重装系统后再使用。确保主机上没有可用数据后进行格式化并重装系统,格式化是保证不会有残余的病毒文件,当格式化之后将无法再进行数据恢复。重装系统后要打好补丁,软件应确保使用最新版本或打好补丁,避免漏洞被利用。口令也应符合上文中提到过的强口令要求。如何做好勒索病毒的事前防护会在第5节详述^[6]。

5 勒索病毒的防治建议

由于勒索病毒的变种较多,同时具有病毒、蠕虫、人为投毒等多种形式,当勒索病毒成功运行

后,解密较为困难,所以勒索病毒的防治主要以预防为主,加强整体网络安全管理以及有效的技术治理手段,如强化勒索病毒防护的 EDR 产品、监测传播途径的 APT 产品等。

5.1 基础防护措施及建议

很多勒索病毒的落地并不一定经过长时间复杂的攻击过程,可能就是源于一封垃圾邮件,所以一定不能忽略很多基础措施。

5.1.1 增强安全意识

除了漏洞利用与暴力破解外,最多的感染勒索病毒的原因就是利用网页挂马、垃圾电子邮件与捆绑恶意程序,所以日常使用网络时要有以下安全意识:

1) 不访问色情、博彩等等不良信息网站,这些网站通常会引导访客下载病毒文件或发动钓鱼、挂马攻击。

2) 不轻易下载陌生人发来的邮件附件,不点击陌生邮件中的链接。

3) 不随意使用陌生 U 盘、移动硬盘等外设,使用时切勿关闭防护软件,比如 Windows 自带的 Windows defender,避免拷入恶意文件。

4) 不轻易运行 bat, vbs, vbe, js, jse, wsh, wsf 等后缀的脚本文件和 exe 可执行程序,不轻易解压不明压缩文件。陌生文件下载运行前可使用文件威胁分析平台进行检测(<http://ti.dbappsecurity.com.cn:8080/>),避免感染病毒。

5) 定期查杀病毒,清理可疑文件,备份数据。

5.1.2 增加口令强度

勒索病毒最常用的攻击方式是利用永恒之蓝

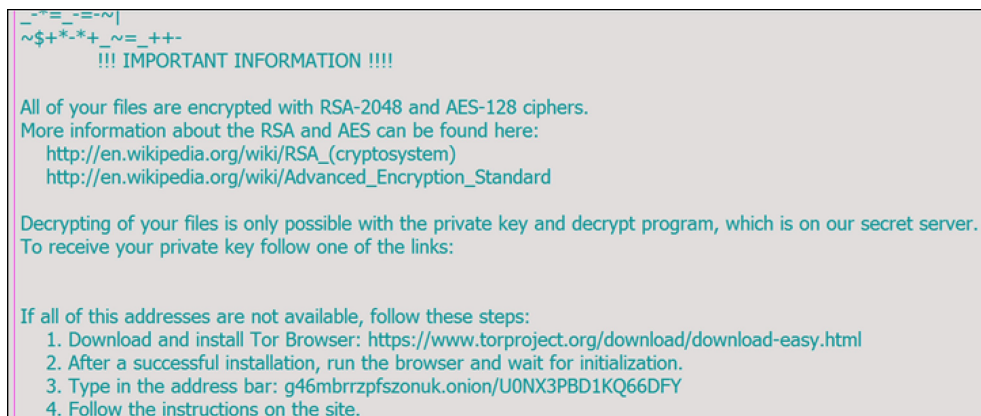


图6 密码修改示例

漏洞和爆破 RDP(远程桌面协议)等服务弱口令,为应对后者应立即修改系统和各应用(MySQL, SQLServer 等)的弱口令、空口令、多台服务器共用的重复口令。强密码长度不少于 8 个字符,至少包含以下 4 类字符中的 3 类:大小写字母、数字、特殊符号,不能是人名、计算机名、用户名、邮箱名等。

在企业中可以通过密码策略让电脑使用者必须设置一个复杂密码,Windows 操作系统可以通过配置密码策略来实现^[7],如图 6 所示。如何设置可参考 <https://jingyan.baidu.com/article/67508eb47e7b459ccalce4f2.html>。

5.1.3 修复系统漏洞

在微软发布高危漏洞公告后应尽快修复系统存在的漏洞,避免被恶意利用(微软安全响应中心:<https://docs.microsoft.com/zh-cn/security-updates/>)。在企业中或个人如果不能及时关注响应这些漏洞信息,应借助安全软件完成漏洞修复。尤其当企业有庞大数量的主机需要管理时,应选择合适的安全管理系统完成修复漏洞的工作^[8],这点在下一节详述。

5.1.4 修复应用漏洞

勒索病毒利用的漏洞工具除了广为人知的永恒之蓝系列,新型的勒索病毒一般还携带许多 Web 应用漏洞利用工具,比如 JBoss 反序列化漏洞(CVE-2013-4810)、Tomcat 任意文件上传漏洞(CVE-2017-12615)、Tomcat Web 管理后台弱口令爆破、Apache Struts2 远程代码执行漏洞 S2-045 等。所以应定期检测并修复漏洞,最好能够及时更新版本^[9]。

5.1.5 端口管理

除了必要的业务需求应关闭 135,139,445,3389 等端口,还要及时对部分机器开放,也应作出配置仅限部分机器可访问。通过防火墙配置、安全软件隔离或准入管理。

6 结 论

勒索病毒的防御是一个系统工程,除了必要的安全产品外还需要强化安全意识。把事先防御,事中处置,事后加固相结合,形成一整套方案。

参 考 文 献

- [1] 游侠安全网. 主机卫士 EDR 的一次勒索病毒阻击战[EB/OL]. (2018-07-26) [2019-03-25]. <https://mp.weixin.qq.com/s/AoqhiNmG0MDYsjKjjlCUvA>
- [2] 国家互联网应急中心. 国家互联网应急中心发布防范“勒索病毒”的应急处置措施[EB/OL]. (2017-05-13) [2019-03-25]. <http://politics.people.com.cn/n1/2017/0513/c1001-29273292.html>
- [3] 搜狐新闻. 安恒信息:勒索病毒专防专杀组合拳[EB/OL]. (2018-09-15) [2019-03-25]. http://www.sohu.com/a/252021881_783750
- [4] 安全牛. 一份超级实用的勒索病毒应急手册[EB/OL]. (2019-03-18) [2019-03-25]. <https://www.aqniu.com/tools-tech/45321.html>
- [5] 搜狐新闻. 安恒信息关于最新勒索病毒安全处置方案[EB/OL]. (2017-05-15) [2019-03-25]. http://www.sohu.com/a/140640157_809033
- [6] 阿里云. 一张图看懂“永恒之蓝”勒索病毒处置流程[EB/OL]. (2017-05-15) [2019-03-25]. <https://yq.aliyun.com/articles/81350>
- [7] 阿里云. 勒索病毒事件是全球网络安全的缩影[EB/OL]. (2017-08-01) [2019-03-25]. <https://yq.aliyun.com/articles/182008?spm=a2c4e.11153940.blogcont81350.18.384c3b0aZz3JDg>
- [8] 腾讯云. 安恒主机卫士 EDR, 助力安全医疗[EB/OL]. (2018-10-24) [2019-03-25]. <https://cloud.tencent.com/developer/news/331733>
- [9] 简书. 还原勒索病毒 GandCrab 的完整攻击和解密场景[EB/OL]. (2018-12-04) [2019-03-25]. <https://www.jianshu.com/p/205a2ca5a439>



李华生

硕士,杭州安恒信息技术股份有限公司终端安全事业部总经理,主要研究方向为恶意文件防御、未知威胁检测等信息安全领域。

wonston.li@dbappsecurity.com.cn



黄进

杭州安恒信息技术股份有限公司高级副总裁,主要研究方向为网络安全相关技术、信息系统安全等级保护体系、应用安全、云安全以及大数据态势感知,多次参与网络安全相关领域国家标准编制和技术研发研讨会。

kadin.huang@dbappsecurity.com.cn