魔窟的水面之上和水面之下

安天安全研究与应急处理中心
安天安全运营中心安全服务部

勒索软件的演进史

伪装反病毒软件

1987

1987年反病毒软件登上历史舞台

1989

1989.6 PC Cyborg

2001

2001.2 FakeAV

2005

2005.5 Gpcode

2006

2006.5 CRYZIP

2006.6 Redplus

2007

2007.3 QiaoZhaz

2008

2008年第一款运行Android系统的商用智能手机发布

2009

2009年比特币发明

2012

2012.8 REVETON

2013

2013.9 CryptoLocker
2013.9 Dirty Decrypt
2013.12 Cryptorbit
2013.12 Cryptographic locker

2014

2014.2 CryptoDefense
2014.4 CryptoWall Ransomware
2014.4 Koler
2014.5 KOVTER
2014.5 simplelock
2014.6 Cokri
2014.7 CTB-Locker
2014.8 TorrentLocker
2014.10 VIRLOCK
2014.11 Locker
2014.11 CoinVault
2014.11 Svpeng

2015

2015.1 Cryptowall
2015.2 TeslaCrypt
2015.4 Alpha Crypt
2015.4 DevLockeer
2015.4 Locker

流行于

2016

2016.1 Ransom32（首款JavaScript编写）
2016.2 Locky（爆发）
2016.3 Samas
2016.3 KimcilWare
2016.3 KeRanger（首款款针对OS系统）
2016.3 Petya（重写MBR）
2016.4 7ev3n
2016.4 CryptXXX
2016.4 Cerber
2016.5 Enigma
2016.6 MIRCOP
2016.6 RAA（JavaScript编写）
2016.6 Zcryptor（蠕虫特性）
2016.7 HolyCrypt(Python编写)
2016.8 FairWare（针对Linux）
2016.10 CryPy（Python编写）
2016.11 Cytptoluck
2016.12 Popcorn

2017-至今

2017.1 FireCrypt
2017.1 Satan
2017.2 CryptoShield
2017.2 Erebus
2017.2 Unlock26
2017.2 Patchers（Swift编写）
2017.2 DynA-Crypt（加密并窃密）
2017.3 RanRan
2017.3 FindZip
2017.3 LLTP
2017.3 Kirk（Monero币）
……

国内首个勒索木马Redplus

www.cert.org.cn/publish/main/10/2012/20120330183108432693348/20120330183108432693348_.html

应用 资料 VirusTotal Intellig... 活跃样本_特征格式 PTD Kibana Home · Wiki · 刘佳... Google 翻译 样本分析-WebTools 交通事故video的个... A

CNCERT/CC 国家互联网应急中心

积极预防 及时发现

快速响应 力保恢复

网站地图 RSS订阅 English 邮件订阅

搜 索

首 页 | 威胁预警 | 态势报告 | 新闻资讯 | CERT在线 | CERT讲堂 | 应急体系 | 关于我们

重点关注

- 国家互联网应急中心开通暗云木马感...
- 2016年中国互联网网络安全报告
- 关于组织开展第七届CNCERT网...
- CNCERT互联网安全威胁报告-...
- 微软公司继续发布支持Window...

更多>>

漏洞公告

- 微软公司继续发布支持Window...
- 关于Linux kernel存在...

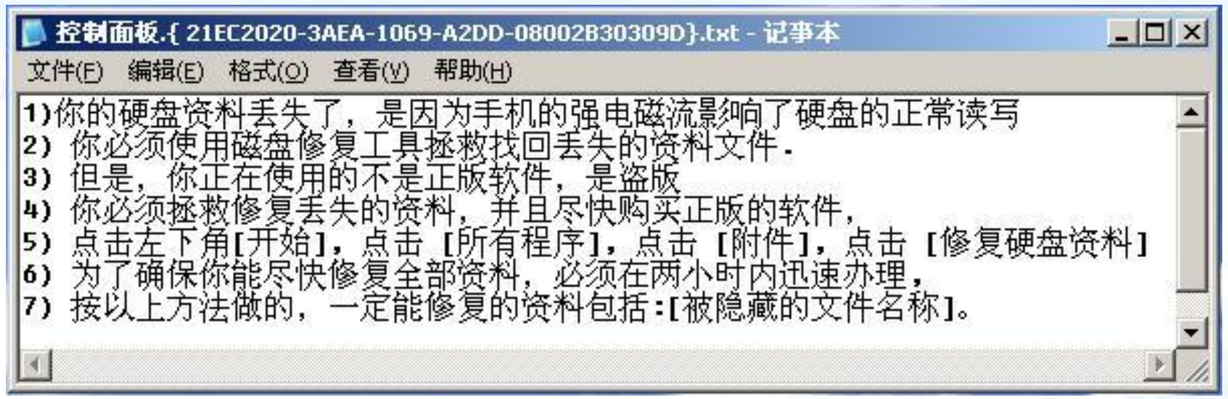
勒索木马Trojan.Win32.Pluder.a攻击性分析和防范措施

时间：2006-06-15

缩小字体 放大字

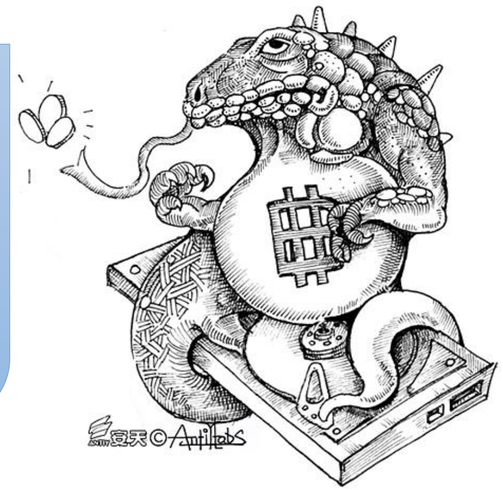
安全公告：CN-SA06-022 发布日期：2006-06-15 安全等级：/upload/p1_23xs25.jpg 公开程度：公共修订次数：0 首次发布日期：2005-06-15 CNCERT/CC的支持单位安天实验室于6月14日截获一个名为Trojan.Win32.Pluder.a的勒索木马。该木马将用户多种类型的文档隐藏起来，然后要求用户向指定银行帐户汇款和向指定手机发送短信，从而使用户面临数据不可用和的经济损失的风险。 勒索软件（国外叫做

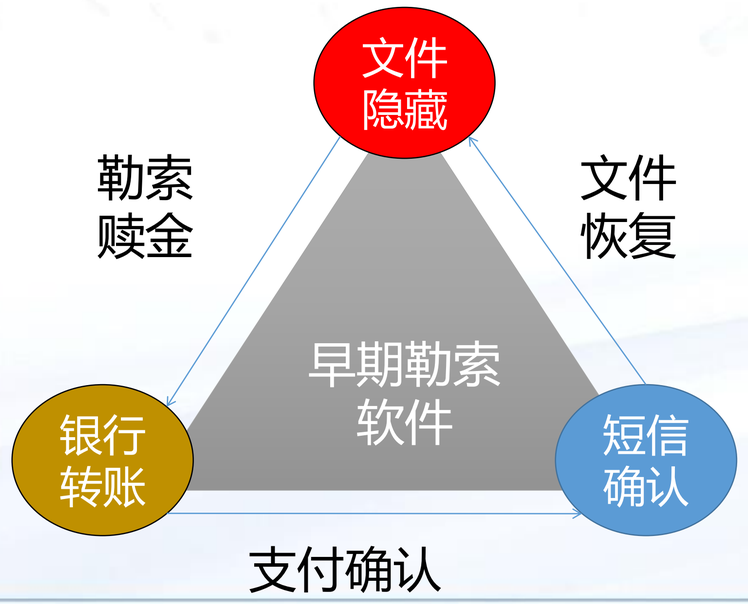
勒索软件的铁三角



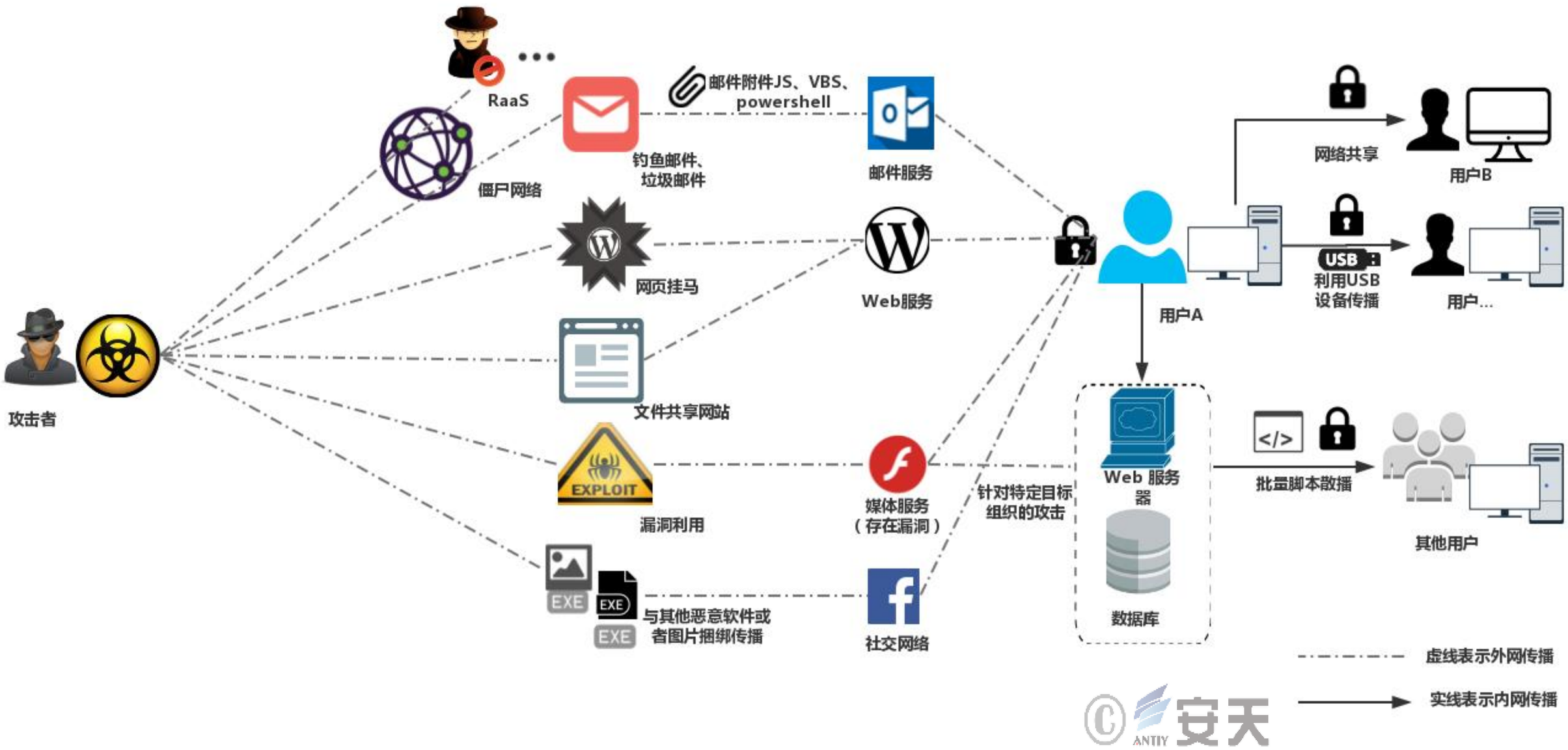
2006年Redplus

作者欧阳某某于2007年在广州落网，共借助Redplus木马勒索款项95笔，合计人民币7061.05元。法院考虑到其自首情节，最终判其有期徒刑4年。





勒索软件的主要传播手段



安天对勒索病毒的持续跟踪

2015 年

- 4 月 30 日，《“攻击 WPS”样本实为敲诈者》
- 8 月 3 日，《揭开勒索软件的真面目》
- 12 月 4 日，《邮件发送 JS 脚本传播敲诈者木马的分析报告》

2016 年

- 1 月 17 日，《2015 年网络安全威胁的回顾与展望》
- 2 月 19 日，《发现使首例具有中文提示的比特币勒索软件“LOCKY”》
- 12 月 20 日，《2016 网络安全威胁的回顾与展望》（安天基础威胁年报）

2017 年

- 4 月，《勒索软件简史》（《中国信息安全》2017 年第 4 期）
- 5 月 13 日 06:00 发布《安天紧急应对新型“蠕虫”式勒索软件“WannaCry”全球爆发》
- 5 月 14 日 05:22 更新《安天紧急应对新型“蠕虫”式勒索软件“WannaCry”全球爆发》

安天研究人员对此的补充观点是——比特币匿名支付和匿名网络带来的犯罪隐蔽性也是其中重要的原因。从后续来看，这种威胁会进一步复合化、与目前的黑产合流，走向更多的系统平台，采用更多的投放方式（而可能不再仅仅是尼日利亚王子式的垃圾邮件的群发），其灰色的配套服务也会更系统化。

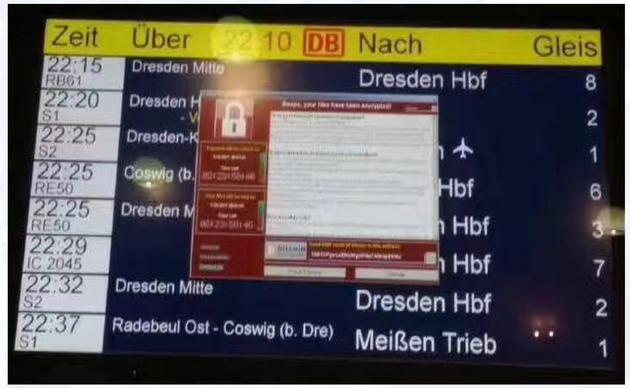
——2016.09.07 《安天技术文章汇编第四卷第三分册.序言》

勒索模式带动的蠕虫的回潮不可避免。

——《2016安天基础威胁年报(预发布版)》，2016.12.20

“魔窟”(WannaCry) 勒索蠕虫横扫全球

- 2017年5月12日20时左右，全球爆发大规模勒索软件感染事件，我国大量用户受到感染，文件被加密
- 蠕虫利用微软SMB漏洞MS17-010，由445端口传播
- 2017年4月14日黑客组织Shadow Brokers（影子经纪人）公开一批NSA使用的网络攻击工具，其中包含了该漏洞的利用程序
- 安天在2015年《一例针对中方机构的准APT攻击样本分析》报告提出：**拥有全球最顶级能力的超级大国，对于有效控制网络攻击武器扩散，应该负起更多的责任**
- 安天CERT在2017年4月14日发布的《2016年网络安全威胁的回顾与展望》预测：**勒索模式带动的蠕虫的回潮不可避免**



安天此前预判中的网络军火扩散

- *我们需要提醒各方关注的是，鉴于网络攻击技术所存在的极低的复制成本的特点，**当前已经存在严峻的网络军备扩散风险**……但对于缺少足够的安全预算、难以承担更多安全成本的国家、行业和机构来说，会成为一场噩梦。*
- *在攻防两端均拥有全球最顶级能力的**超级大国，对于有效控制这种武器级攻击手段的扩散，应该负起更多的责任。***

——安天分析报告《一例针对中国政府机构的准APT攻击中所使用的样本分析》，2015.05.27

- ***我们看到了相关的Exploit储备和攻击思路流入到网络犯罪组织、甚至恐怖主义组织的可能性**。鉴于网络攻击技术存在极低的复制成本的特点，当前已经存在严峻的网络军备扩散风险。因此，超级大国能否合理控制自身网络军备发展的速度和规模，并对因自身未有效履行责任而使网络领域发生可能的军备扩散，进行有效地干预和控制，是我们能达成一个更安全的网络世界的关键因素。*

——安天分析报告《从“方程式”到“方程组” EQUATION攻击组织高级恶意代码的全平台能力解析》,2016.10.04

安全厂商与时间赛跑

“WannaCry”相关事件时间轴

2017年3月14日
微软发布MS17-010 漏洞补丁

2017年4月14日
Shadow Brokers(影子经纪人)
公开黑客组织方程式的多个入侵工具

2017年5月13日
06：00发布《安天紧急应对新型“蠕虫”式勒索软件“WannaCry”全球爆发》
17：25发布《安天应对勒索软件“WannaCry”配置指南》
17：45发布《安天应对勒索者蠕虫病毒WannaCry FAQ》
19：03 安天发布蠕虫病毒WannaCry免疫工具和扫描工具

2017年5月15日 19:00
安天发布变种事件分析

2017年4月17日
安天对泄露的入侵工具
形成完整事件分析简报

2017年5月14日
卡巴斯基承认误判，说明暂未发现无“域名开关”样本

2017年5月18日
发现利用相同漏洞传播的UIWIX勒索样本

2017年5月19日

2017年3月1日

2017年3月28日
已发现的WannaCry1.0样本最早的时间戳

2017年4月15日
安天对泄露的入侵工具展开分析
形成初版简报

2017年5月12日
“蠕虫式”勒索软件WanaCry全面爆发

2017年5月13日
卡巴斯基误判无“域名开关”样本存在

2017年5月14日
05：00发布《安天应对勒索软件“WannaCry”开机指南》

2017年5月14日18:42:29
三个新修改样本出现

2017年5月18日 6:00
安天发布WannaCry支付解密流程分析

2017年5月18日
安天发布UIWIX勒索样本简报

安天启动A级（最高级）响应

做出威胁预测

- 安天在基础威胁年报中预测将在一年内爆发大规模勒索软件攻击，随后向CNCERT进行了专报。

3月

第一时间通报处置

- 安天第一时间向主管部门通报情况，内部工具开发计划和人员集结工作部署。

06:00

- 发布《安天紧急应对新型"蠕虫"式勒索软件"Wanna-Cry"全球爆发》深度分析报告，微信公众号一天突破31万的阅读量。

09:45

- 第一时间进行用户现场应急处置。

15:00-16:00

- 安天向客户发布预警和防护手册。
- 操作系统应急补丁包推送。

17:00-18:00

- 发布《安天应对勒索软件"WannaCry"配置指南》。
- 发布《安天应对勒索者蠕虫病毒WannaCryFAQ-1》针对大量用户的高频问题进行回复。

5月12日

20:20

- 决定启动"A级灾难"响应。

22:45

- 经测试，安天智甲终端防御系统，无需升级即可有效阻断WannaCry的加密行为，安天探海威胁检测系统升级后可以检出WannaCry的扫描包。

启动A级响应

5月13日

20:05

- 首批应急响应人员奔向客户现场，进行内网扫描收集用户问题。

19:00-20:00

- 发布WannaCry免疫工具和扫描工具。
- 公安部下属国家计算机病毒应急处理中心，向公众推荐使用安天免疫和专杀工具应对勒索病毒。
- 国家互联网应急中心发布《关于防范Windows操作系统勒索软件Wannacry的情况通报》，向公众推荐使用安天免疫和专杀工具应对勒索病毒。

进驻用户现场

发布报告，推出

15:00

- 现场处置只读U盘（含免疫工具、专杀工具、智甲防勒索版、系统补丁）发布，奔向客户现场。

16:00

- 安天发布加密后的恢复建议，消除用户恐慌。

18:05

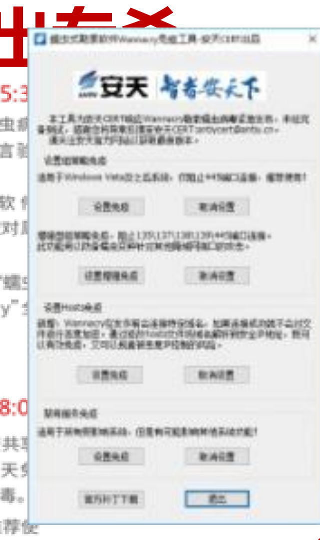
- 安天工具持续升级，工具合集已发布至1.4版本。

04:30-05:3

- 发布《安天应对勒索者蠕虫病毒WannaCryFAQ-2：传言验证者》。
- 发布《安天应对勒索软件WannaCry开机指南》，应对周一开机安全考验。
- 更新《安天紧急应对新型"蠕虫"式勒索软件"WannaCry"全球爆发》深度分析报告。

17:00-18:0

- 国家网信办网络安全检查共享平台，向公众推荐使用安天免疫和专杀工具应对勒索病毒。
- 公安部共享平台向公众推荐使用安天免疫和专杀工具应对勒索病毒。



5月14日

18:44

- 安天和友商应急团队联合讨论，最终将"WannaCry"中文俗名确定为"魔窟"。

19:00-20:00

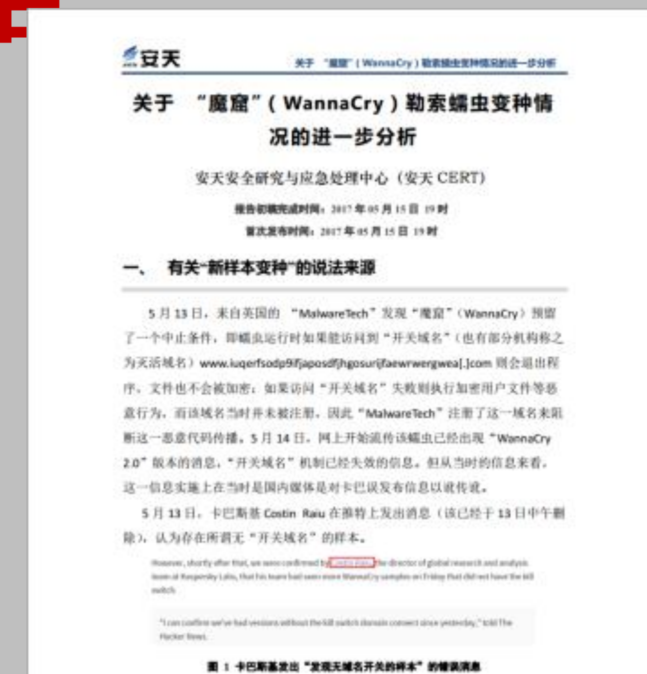
- 发布安天智甲防勒索免费版。
- 更新发布免疫工具、专杀工具。

正式命名，更新工具

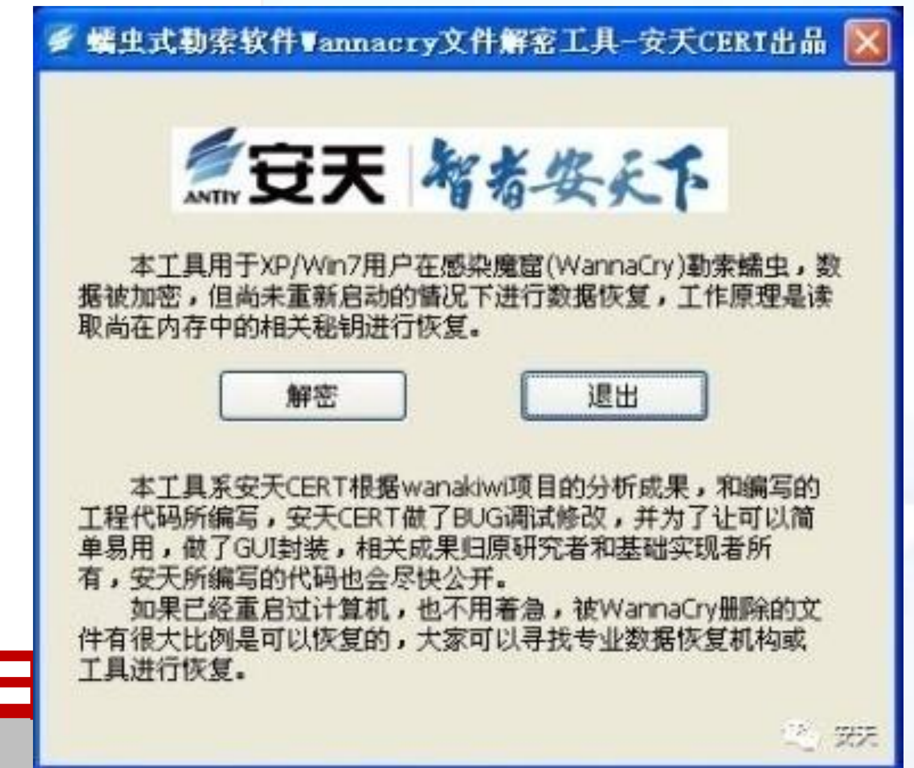
再次发布报告，提供扩展补丁包

- 15日00:20，安天发布"魔窟"勒索蠕虫内网响应网页工具。
- 15日08:00，针对部分用户提供扩展补丁包。
- 15日凌晨更新《安天应对勒索软件"WannaCry"开机指南》。
- 16日凌晨发布《对"魔窟"(WannaCry)勒索蠕虫变种情况分析》。

5月15-16日



5:02 发布解密工具

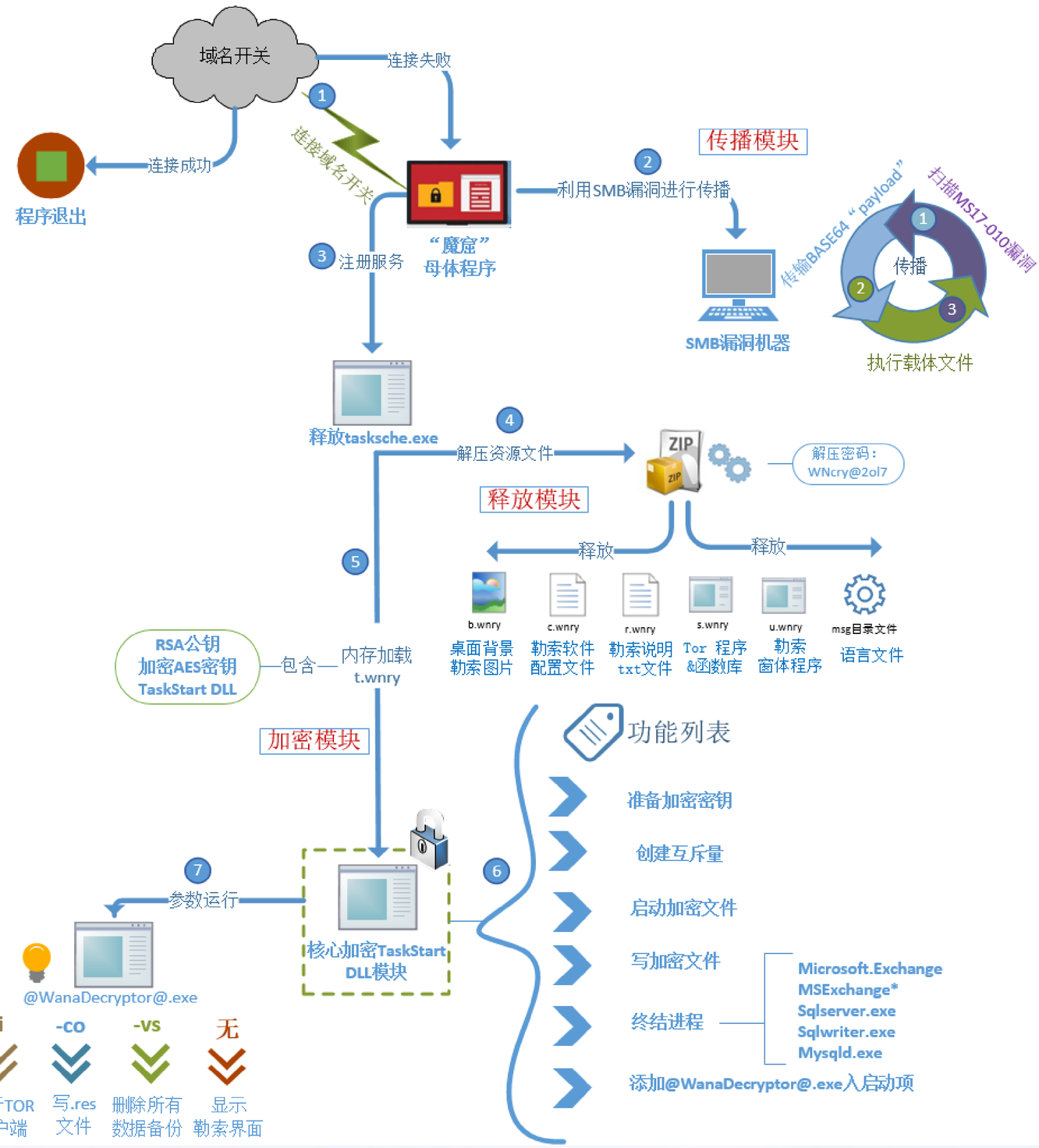


5月20日

安天关于"勒索者蠕虫病毒WannaCry"跟进时间表

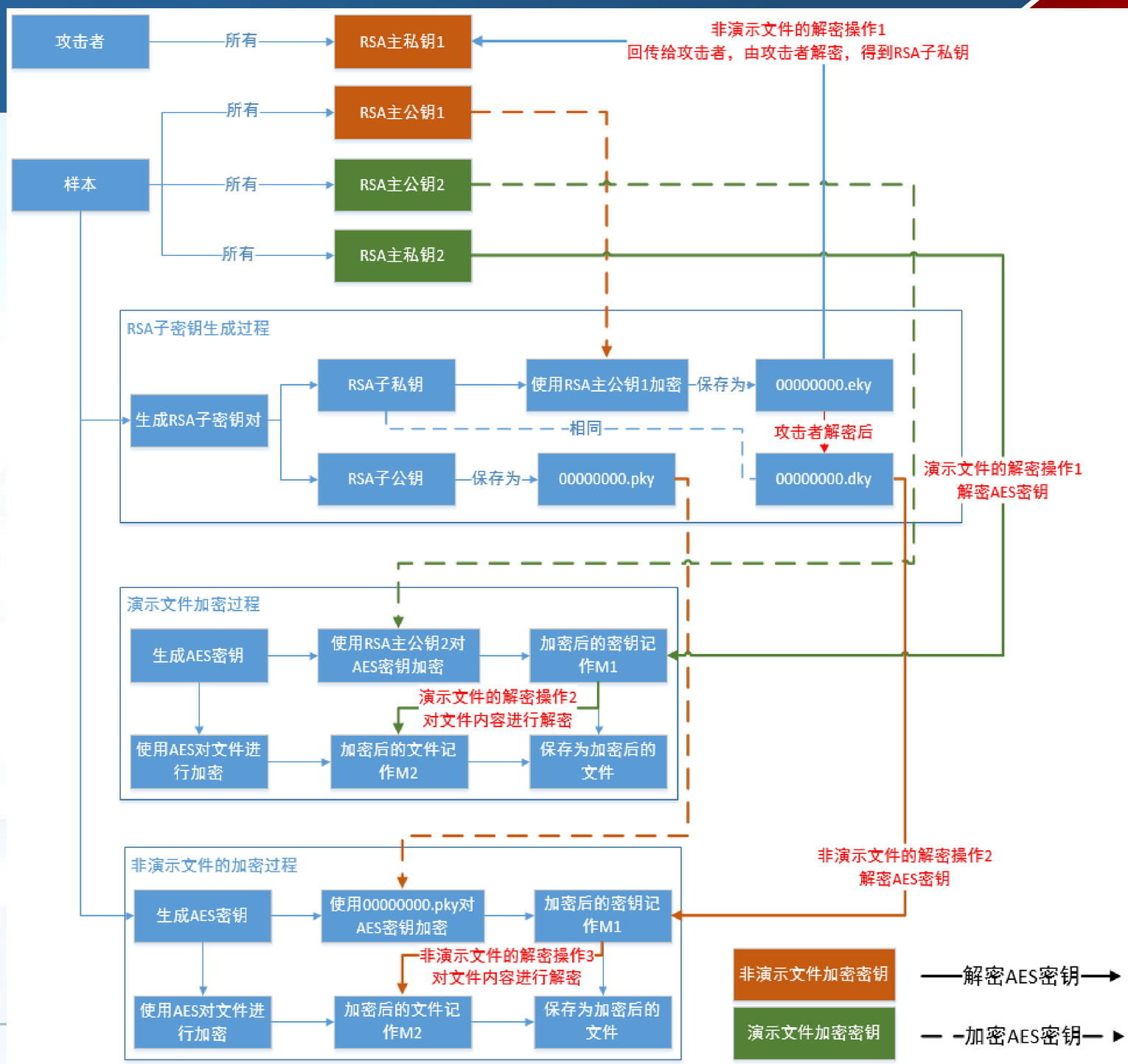
“魔窟”运行流程

- 域名开关
  - 添加服务、启动服务
    - 传播
  - 释放、运行“WannaCry”勒索程序（tasksche.exe）
  - 释放资源
  - 加密文件
  - 启动暗网
  - 显示勒索

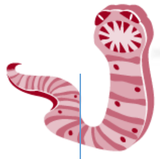


加解密流程分析

- 服务器保存
  - 主RSA私钥1
- 样本内置
  - 主RSA公钥1
  - 主RSA公钥2
  - 主RSA私钥2
- 样本运行生成
  - RSA子密钥对
  - AES密钥



“魔窟”加解密流程



5.回传给攻击者

RSA 主私钥

RSA 主公钥

RSA 子公钥

RSA 子私钥

1.生成RSA子密钥对
（每次启动时）

2.生成AES密钥
（每次加密时）

AES密钥

3.加密终端文件

文件

4.生成用户标识

000000.res

加密

000000.pky

000000.eky

加密

AES密钥

加密

文件

解密

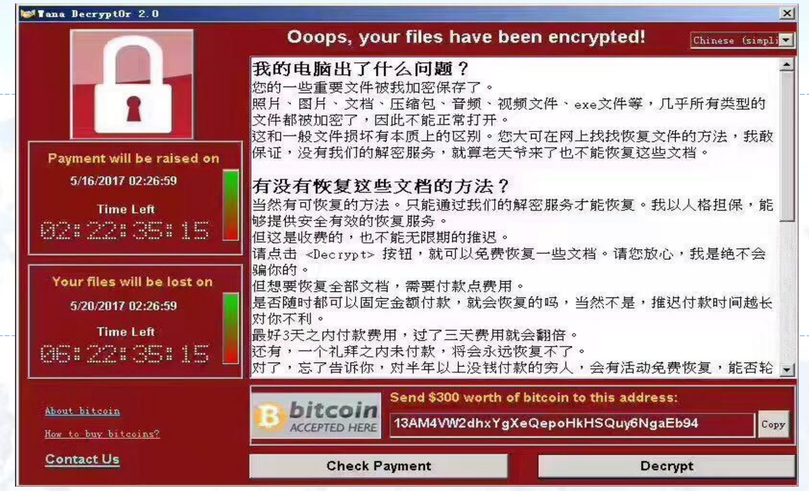
000000.dky

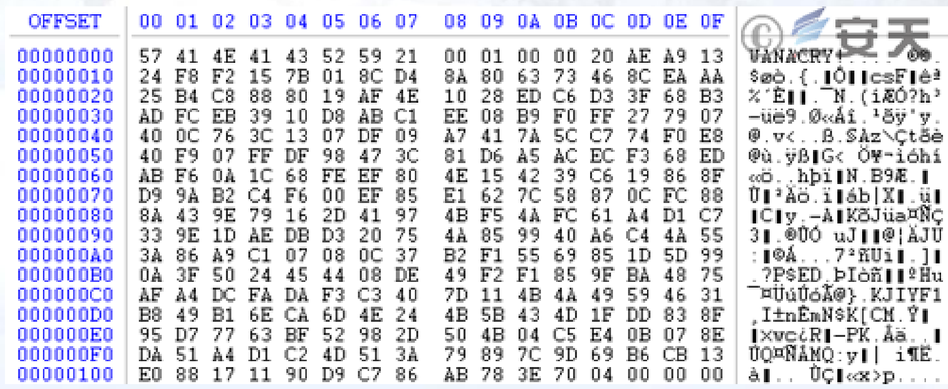
文件头

AES密钥

文件

6.生成唯一比特币钱包，支付后解密



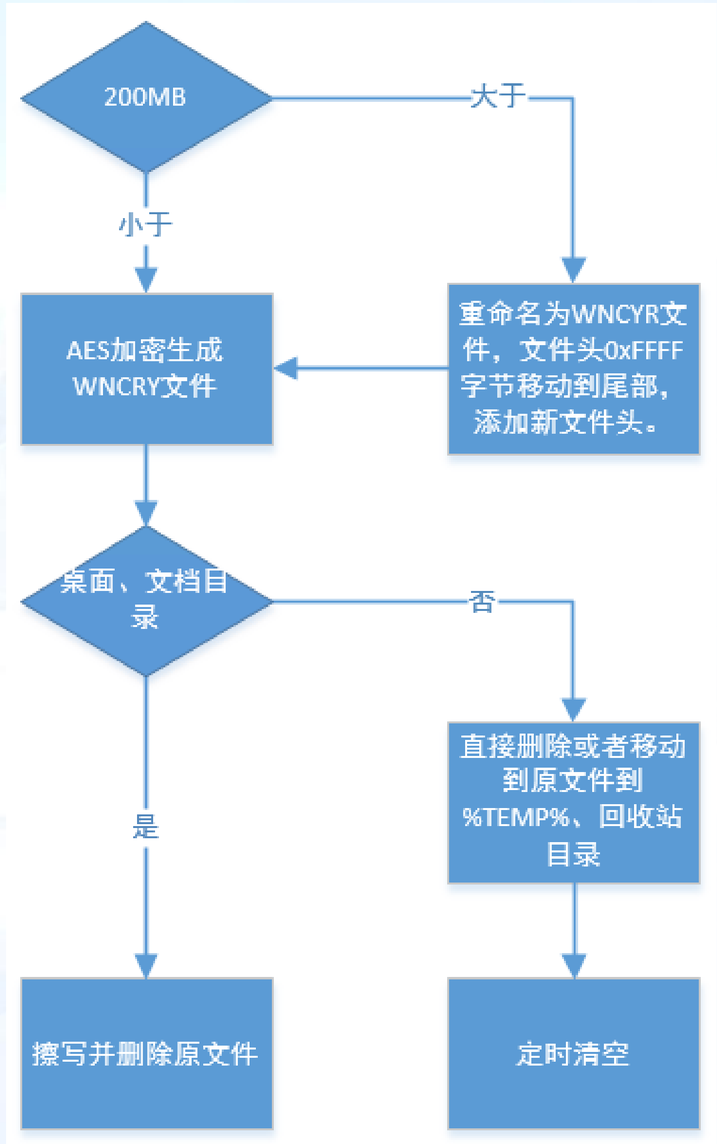


OFFSET	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
00000000	57	41	4E	41	43	52	59	21	00	01	00	00	20	AE	A9	13
00000010	24	F8	F2	15	7B	01	8C	D4	8A	80	63	73	46	8C	EA	AA
00000020	25	B4	C8	88	80	19	AF	4E	10	28	ED	C6	D3	3F	68	B3
00000030	AD	FC	EB	39	10	D8	AB	C1	EE	08	B9	F0	FF	27	79	07
00000040	40	0C	76	3C	13	07	DF	09	A7	41	7A	5C	C7	74	F0	E8
00000050	40	F9	07	FF	DF	98	47	3C	81	D6	A5	AC	EC	F3	68	ED
00000060	AB	F6	0A	1C	68	FE	EF	80	4E	15	42	39	C6	19	86	8F
00000070	D9	9A	B2	C4	F6	00	EF	85	E1	62	7C	58	87	0C	FC	88
00000080	8A	43	9E	79	16	2D	41	97	4B	F5	4A	FC	61	A4	D1	C7
00000090	33	9E	1D	AE	DB	D3	20	75	4A	85	99	40	A6	C4	4A	55
000000A0	3A	86	A9	C1	07	08	0C	37	B2	F1	55	69	85	1D	5D	99
000000B0	0A	3F	50	24	45	44	08	DE	49	F2	F1	85	9F	BA	48	75
000000C0	AF	A4	DC	FA	DA	F3	C3	40	7D	11	4B	4A	49	59	46	31
000000D0	B8	49	B1	6E	CA	6D	4E	24	4B	5B	43	4D	1F	DD	83	8F
000000E0	95	D7	77	63	BF	52	98	2D	50	4B	04	C5	E4	0B	07	8E
000000F0	DA	51	A4	D1	C2	4D	51	3A	79	89	7C	9D	69	B6	CB	13
00000100	E0	88	17	11	90	D9	C7	86	AB	78	3E	70	04	00	00	00

使用暗网连接后显示的比特币钱包地址

加解密时对文件的操作分析（可恢复性）

- 遍历查找指定后缀名文件
- 200MB以上单独标记单独处理
- 桌面、文档等重要目录文件擦写



安天针对勒索蠕虫“魔窟”（WannaCry）的深度分析报告 （内部版）

每个被加密的文件均使用不同的 AES 密钥，若想对文件进行解密操作，需要先获取 RSA 子私钥，将文件头部的 AES 密钥进行解密操作，再使用 AES 密钥，对文件体进行解密操作。如果没有 RSA 子私钥，则 AES 密钥无法解密，文件也就无法解开。

加密如下后缀名的文件：

.doc .docx .xls .xlsx .ppt .pptx .pst .ost .msg .eml .vsd .vsdx .txt .csv .rtf .123 .wks .wk1 .pdf .dwg .onetoc2 .snt .jpeg .jpg .docb .docm .dot .dotm .dotx .xlsm .xlsb .xlw .xlt .xlm .xlc .xltx .xltm .pptm .pot .pps .ppsm .ppsx .ppam .potx .potm .edb .hwp .602 .sxi .sti .sldx .sldm .sldm .vdi .vmdk .vmx .gpg .aes .ARC .PAQ .bz2 .tbk .bak .tar .tgz .gz .7z .rar .zip .backup .iso .vcd .bmp .png .gif .raw .cgm .tif .tiff .nef .psd .ai .svg .djvu .m4u .m3u .mid .wma .flv .3g2 .mkv .3gp .mp4 .mov .avi .asf .mpeg .vob .mpg .wmv .fla .swf .wav .mp3 .sh .class .jar .java .rb .asp .php .jsp .brd .sch .dch .dip .pl .vb .vbs .ps1 .bat .cmd .js .asm .h .pas .cpp .c .cs .suo .sln .ldf .mdf .ibd .myi .myd .frm .odb .dbf .db .mdb .accdb .sql .sqlitedb .sqlite3 .asc .lay6 .lay .mml .sxm .otg .odg .uop .std .sxd .otp .odp .wb2 .slk .dif .stc .sxc .ots .ods .3dm .max .3ds .uot .stw .sxw .ott .odt .pem .p12 .csr .crt .key .pfx .der

加密时遍历目录的顺序

- 第一个调用函数调用的目录：C:\Documents and Settings\admin\
- 第二个调用函数调用的目录：C:\Documents and Settings\admin\My Documents
- 第三个调用函数调用的目录顺序：C:\Documents and Settings\All Users\
  - C:\Documents and Settings\Default User\
  - C:\Documents and Settings\LocalService\
  - C:\Documents and Settings\NetworkService\
  - C:\Documents and Settings\All Users\Documents
  - C:\Documents and Settings\All Users\My Documents
  - C:\Documents and Settings\Default User\Documents
  - C:\Documents and Settings\Default User\My Documents
  - C:\Documents and Settings\LocalService\Documents
  - C:\Documents and Settings\LocalService\My Documents
  - C:\Documents and Settings\NetworkService\Documents
  - C:\Documents and Settings\NetworkService\My Documents
- 第四个调用函数调用为按磁盘倒序调用：
  - Z: Y: X: . . . C: B: A:

文件恢复条件判断

- 非桌面、文档、用户文件夹的文件
  - 磁盘空间充足，以保证被删除文件没被覆盖
  - %TEMP%目录、 $RECYCLE目录的.WNCRYT文件
  - 200MB以上文件恢复后需要将文件尾部0x10000字节剪切到文件头

677.WNCRYT	2013-03-15, 星期...	WNCRYT 文件	1,435 KB
624.WNCRYT	2008-08-08, 星期...	WNCRYT 文件	1,276 KB
679.WNCRYT	2013-03-15, 星期...	WNCRYT 文件	1,259 KB
869.WNCRYT	2009-01-04, 星期...	WNCRYT 文件	1,022 KB
835.WNCRYT	2008-10-08, 星期...	WNCRYT 文件	563 KB
682.WNCRYT	2013-03-15, 星期...	WNCRYT 文件	552 KB
676.WNCRYT	2013-03-15, 星期...	WNCRYT 文件	489 KB
871.WNCRYT	2013-01-08, 星期...	WNCRYT 文件	461 KB
678.WNCRYT	2013-03-15, 星期...	WNCRYT 文件	455 KB

变种问题澄清（5月15日）

“WannaCry”变种事件时间轴

2017年5月12日
“蠕虫式”勒索软件WanaCry2.0全面爆发

2017年5月14日
卡巴斯基承认误判，说明暂未发现无“域名开关”样本

2017年5月15日 9:00
安天分析发布FAQ3公布修改样本

2017年5月15日 19:00
针对三个“变种”样本分析完成

2017年3月1日

2017年5月24日

2017年3月28日
已发现的WannaCry1.0样本最早的时间戳

2017年5月13日
卡巴斯基误判无“域名开关”样本存在

2017年5月13日
部分媒体跟进称出现无“域名开关”样本

2017年5月14日18:42:29
三个新修改样本出现

2017年5月18日
针对“UIWIX”勒索样本的分析简报

卡巴斯基承认误判，暂未发现“无域名开关的样本”

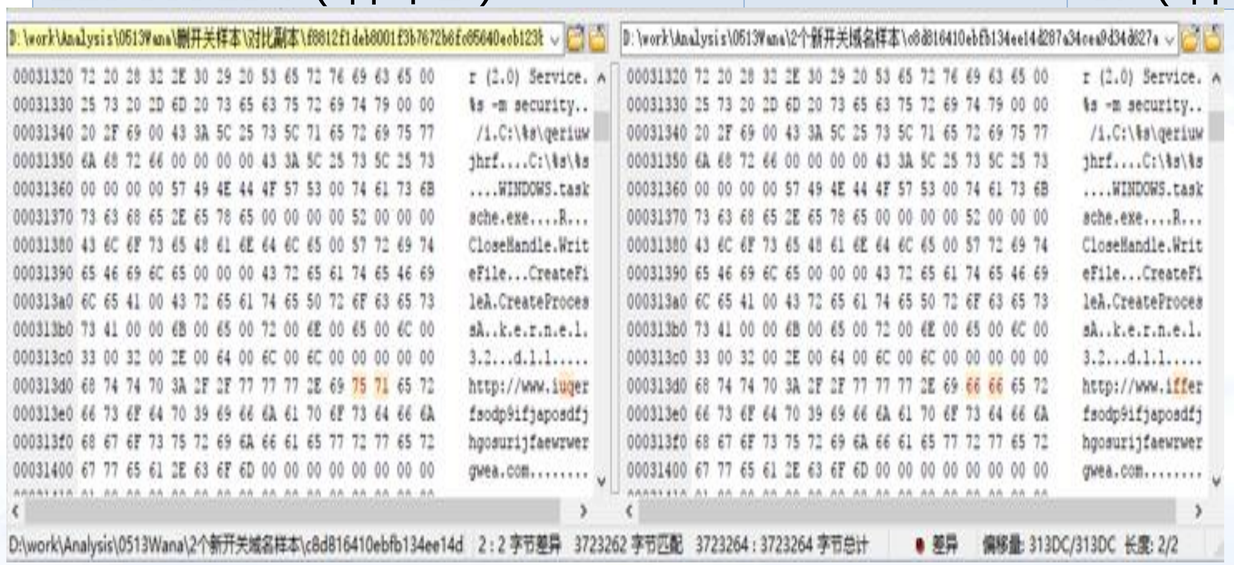
My bad - finished analyzing all #Wannacry worm mods we have and they all have the kill switch inside. No version without a kill-switch yet.

转推 272　喜欢 260

上午4:33 - 2017年5月14日

发现”变种样本”——修改样本对比

原始样本文件MD5	是否有加密行为	新发现的对应样本MD5	修改点
F107A717F76F4F910AE9CB4DC5290594（样本1）（资源损坏）	否	80CE983D22C6213F35867053BEC1C293（样本1A）	新域名
		D724D8CC6420F06E8A48752F0DA11C66（样本1B）	抹去域名开关，强制触发
DB349B97C37D22F5EA1D1841E3C89EB4（样本2）	是	D5DCD28612F4D6FFCA0CFEAEFD606BCF（样本2A）	新域名



修改域名

强制跳转

澄清“2.0版本”问题

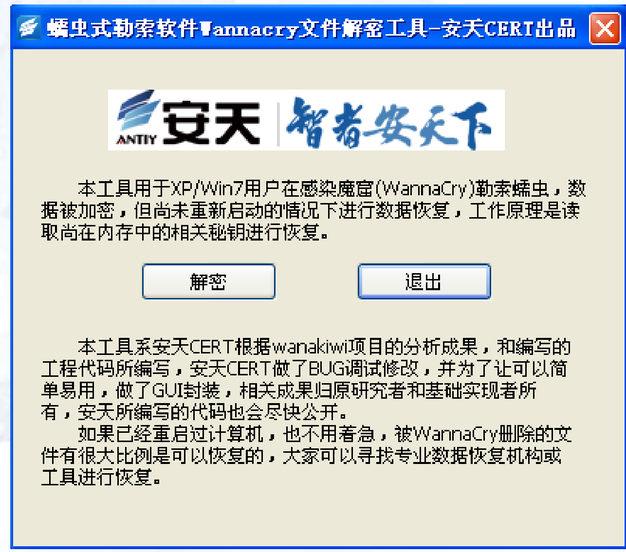
- WannaCry1.0是一个单独的勒索程序，在2017年3月出现。
- WannaCry2.0是本次“魔窟”蠕虫使用的版本。

WannaCry 1.0

WannaCry 2.0

文件解密及安天工具

- 发现者
  - 由法国研究者发现并编写开源工程代码。
  - 此时体现了在解决问题的创造力和研究深度方面我们的差距。
- 原因
  - 微软CryptDestroyKey、CryptReleaseContext的问题导致生成的密钥的素数没有被销毁，可查找该素数生成密钥
  - XP、2003、WIN7 32位确认有效
- 条件
  - 感染后未重启机器，因为重启后内存清除
  - 未杀毒、专杀等，保证wannacry加密进程存在（tasksche.exe）



魔窟蠕虫的借鉴

加密勒索

蠕虫式传播

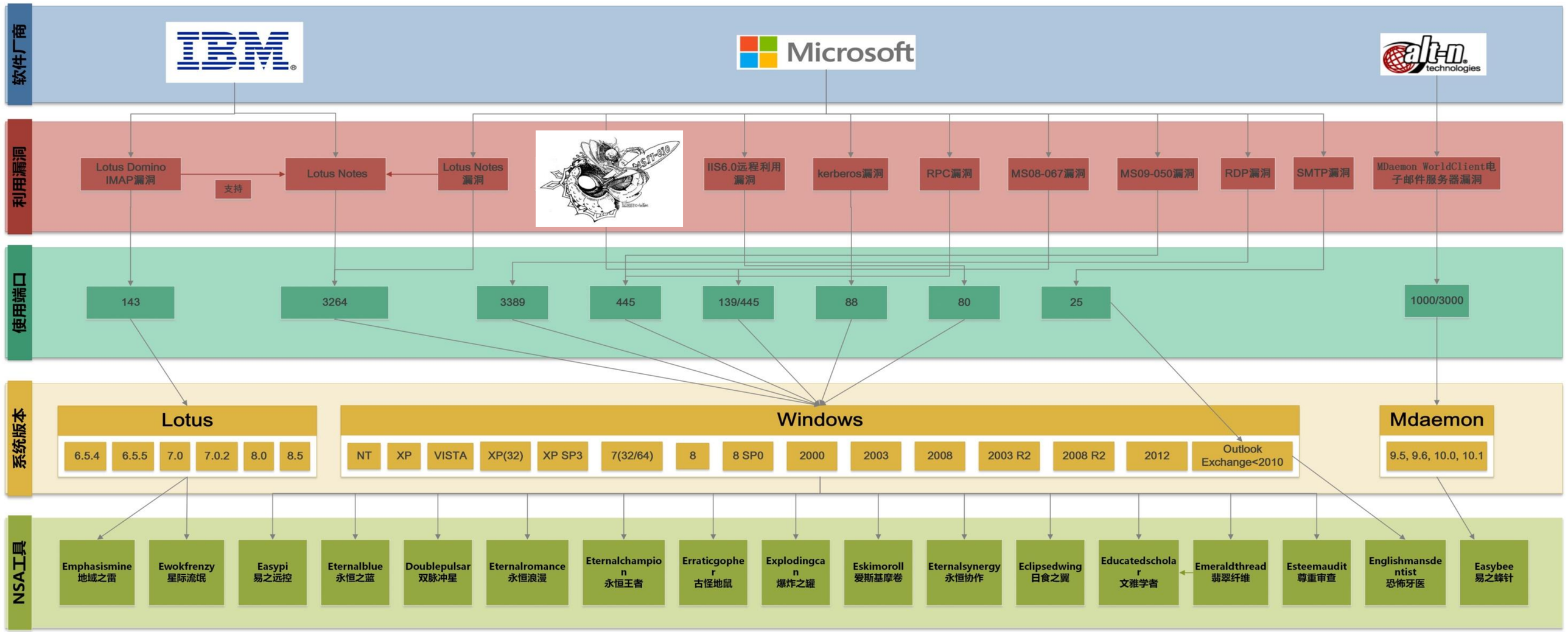
漏洞利用
（MS17-010）

“魔窟”勒索蠕（WannaCry）

军火级漏洞的强大威力

2017年4月14日泄露的NSA网络军火装备的漏洞利用关系图

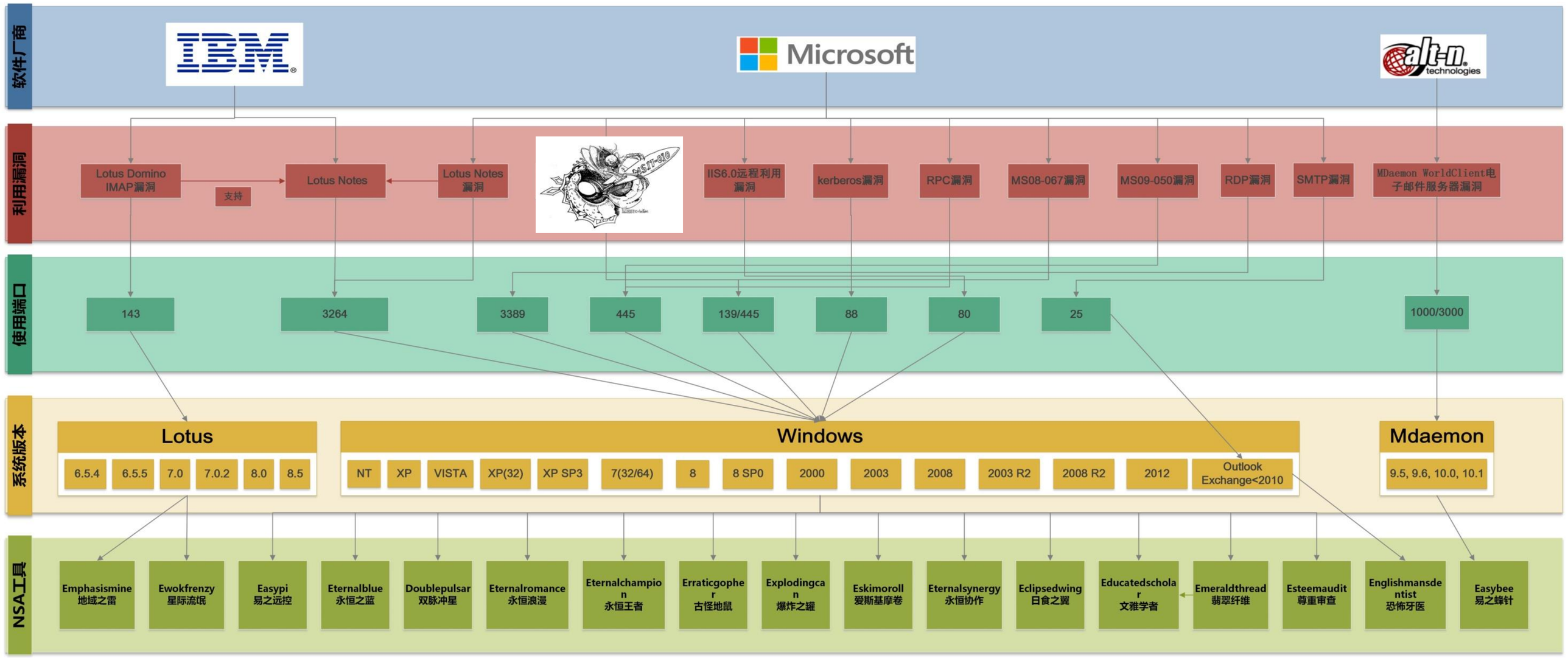
2017年5月21日 安天实验室绘制



NSA组织结构

2017年4月14日泄露的NSA网络军火装备的漏洞利用关系图

2017年5月21日 安天实验室绘制



魔窟事件的五个因素

- **军用级别网络攻击武器扩散**：NSA军用网络攻击武器的泄露，为黑客提供了国家战略级网络武器，大大加强了恶意黑客组织的攻击能力，使黑客组织的攻击水平从组织级提升到了国家级。
- **暴露出来我国网络安全现状**：内网防御体系中的缺陷，一方面是安全产品未能得到全面部署和有效使用，另一方面则首先是其规划建设中没有落实“三同步”的原则，缺少基础的安全架构。

经济利益驱动

门槛日益降低

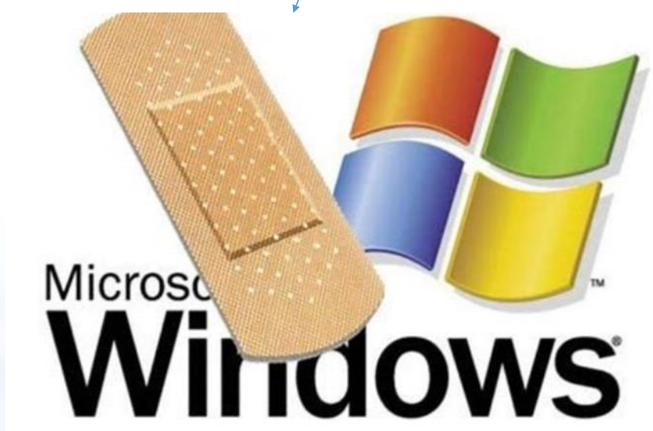
军用工具泄露

安全意识淡薄

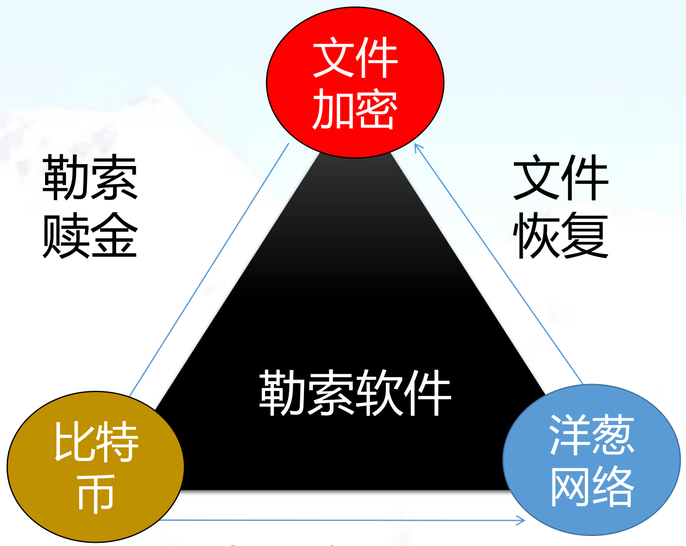
防护措施不足

从滑动标尺分析面对WannaCry事件防御失效的原因

架构安全	被动防御	积极防御	情　报	进　攻
在系统规划、建立和维护的过程中充分考虑安全防护	在无人员介入的情况下，附加在系统架构之上可提供持续的威胁防御或威胁洞察力的系统	分析人员对处于所防御网络内的威胁进行监控、响应、学习（经验）和应用知识（理解）的过程	收集数据、将数据利用转换为信息，并将信息生产加工	对抗攻击者的法律反制措施、自卫反击行动



取次花丛懒回顾 半缘修道半缘君



支付确认

经济利益驱动

门槛日益降低

军用工具泄露

安全意识淡薄

防护措施不足

架构安全

在系统规划、建立和维护的过程中充分考虑安全防护

被动防御

在无人员介入的情况下，附加在系统架构之上可提供持续的威胁防御或威胁洞察力的系统

积极防御

分析人员对处于所防御网络内的威胁进行监控、响应、学习（经验）和应用知识（理解）的过程

情　报

收集数据、将数据利用转换为信息，并将信息生产加工

进　攻

对抗攻击者的法律反制措施、自卫反击行动

第五届安天网络安全冬训营

网络空间威胁对抗技术与实战研讨会

暨 关键信息基础设施保护实践论坛

Thank You

关注安天冬训营官网

关注安天微信公众号

红旗漫卷

敌情想定是前提，网络安全实战化