

2018勒索病毒全面分析报告

2018-11-23

本报告由瑞星公司安全研究院总结，综合瑞星“云安全”系统、瑞星威胁情报平台、研究数据、分析资料以及权威媒体公开报道，针对中国2018年1至10月勒索病毒感染现状与趋势进行统计、研究和分析。

一、勒索病毒简介

勒索病毒是黑客通过锁屏、加密等方式劫持用户设备或文件，并以此敲诈用户钱财的恶意软件。黑客利用系统漏洞或通过网络钓鱼等方式，向受害电脑或服务器植入病毒，加密硬盘上的文档乃至整个硬盘，然后向受害者索要数额不等的赎金后才予以解密，如果用户未在指定时间缴纳黑客要求的金额，被锁文件将无法恢复。

二、勒索病毒发展史

1、勒索病毒第一阶段：不加密数据，提供赎金解锁设备

2008年以前，勒索病毒通常不加密用户数据，只锁住用户设备，阻止用户访问，需提供赎金才能解锁。期间以LockScreen 家族占主导地位。由于它不加密用户数据，所以只要清除病毒就不会给用户造成任何损失。由于这种病毒带来的危害都能被很好的解决，所以该类型的勒索软件只是昙花一现，很快便消失了。

LockScreen勒索截图

Операционной системой была обнаружена проблема, которая может повредить вашему компьютеру.

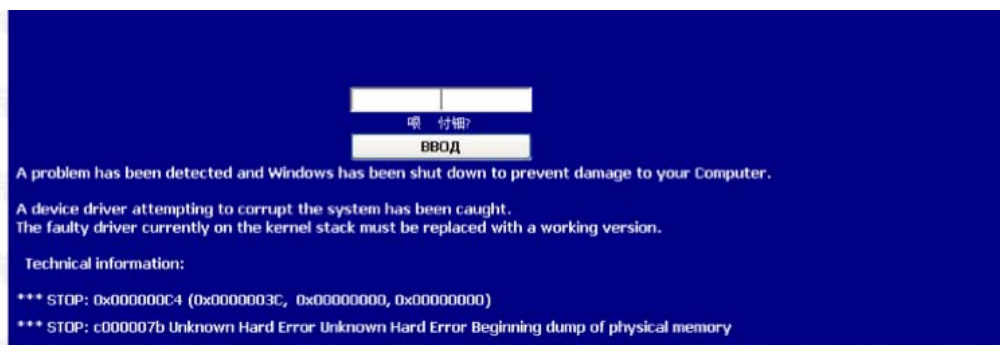
Драйвер устройства, вызвавший повреждения был обезврежен системой.
Нарушенный драйвер на стенке ядра должны быть заменены рабочей версией.

Technical information:

*** STOP: 0x000000C4 (0x0000003C, 0x00000000, 0x00000000)

昨城?恒新烘炸盆 疣犛蛱蓑铍铍匪糖?汁 游 翼祐 蛭疣 钲?拾遂簧?联恩困?拾遂簧 ?

悟饕噎 ?SMS ?蛭蛭蛭? id41630888 磬 岖戾? 1053 (糖铈祛糖
?10痼? 徨?湍? (滌 雨疣桧?磬 岖戾? 4113)! 项塍麋眇 饰?
倚乓葩 阔温??缺伎蛭铎 SMS-耦铍 龛? 村遽栩??饕脍:

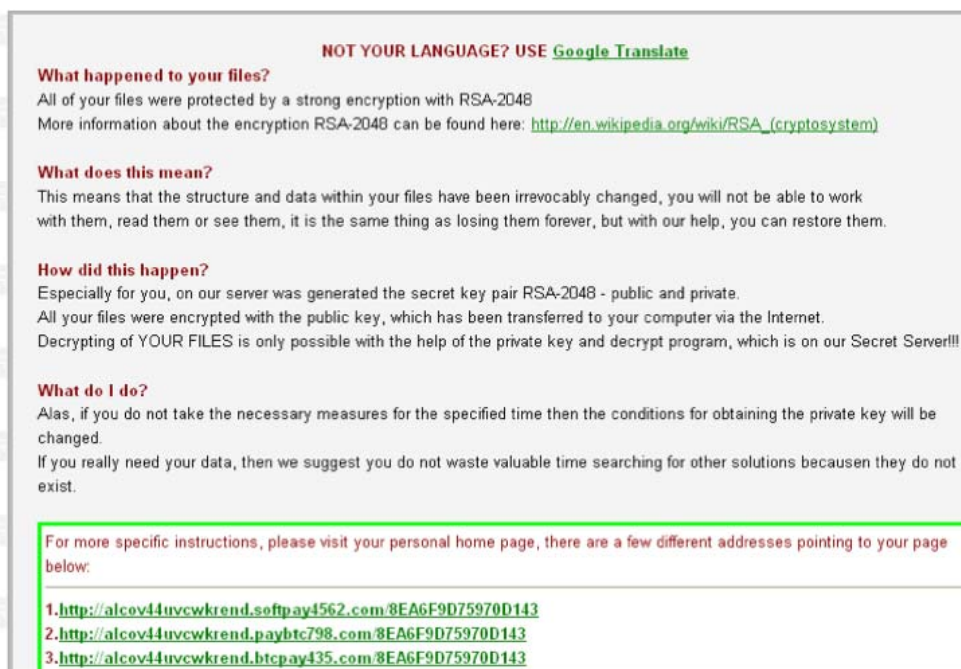


图：LockScreen勒索截图

2、勒索病毒第二阶段：加密数据，提供赎金解锁文件

2013年，以加密用户数据为手段勒索赎金的勒索软件逐渐出现，由于这类勒索软件采用了一些高强度的对称和非对称的加密算法对用户文件加密，在无法获取私钥的情况下要对文件进行解密，以目前的计算水平几乎是不可能完成的事情。正是因为这一点，该类型的勒索软件能够带来很大利润，各种家族如雨后春笋般出现，比较著名的有CTB-Locker、TeslaCrypt、Cerber等。

























Tesla勒索截图



图：Tesla勒索截图

3、勒索病毒第三阶段：蠕虫化传播，攻击网络中其它机器

2017年，勒索病毒已经不仅仅满足于只加密单台设备，而是通过漏洞或弱口令等方式攻击网络中的其它机器， WannaCry就属于此类勒索软件，短时间内造成全球大量计算机被加密，其影响延续至今。另一个典型代表Satan勒索病毒，该病毒不仅使用了永恒之蓝漏洞传播，还内置了多种web漏洞的攻击功能，相比传统的勒索病毒传播速度更快。虽然已经被解密，但是此病毒利用的传播手法却非常危险。

 blue.exe	2018/7/5 17:14	应用程序	126 KB
 blue.fb	2018/7/5 17:14	FB 文件	1 KB
 blue.xml	2018/7/5 17:14	XML 文档	8 KB
 cnli-1.dll	2018/7/5 17:14	应用程序扩展	99 KB
 coli-0.dll	2018/7/5 17:14	应用程序扩展	15 KB
 crlt-0.dll	2018/7/5 17:14	应用程序扩展	17 KB
 dmgd-4.dll	2018/7/5 17:14	应用程序扩展	469 KB
 down64.dll	2018/7/5 17:14	应用程序扩展	5 KB
 exma-1.dll	2018/7/5 17:14	应用程序扩展	10 KB
 libeay32.dll	2018/7/5 17:14	应用程序扩展	882 KB
 libxml2.dll	2018/7/5 17:14	应用程序扩展	807 KB
 mmkt.exe	2018/7/5 17:14	应用程序	1,282 KB
 posh-0.dll	2018/7/5 17:14	应用程序扩展	11 KB
 ssleay32.dll	2018/7/5 17:14	应用程序扩展	180 KB
 star.exe	2018/7/5 17:14	应用程序	45 KB
 star.fb	2018/7/5 17:14	FB 文件	1 KB
 star.xml	2018/7/5 17:14	XML 文档	6 KB
 tibe-2.dll	2018/7/5 17:14	应用程序扩展	232 KB
 trch-1.dll	2018/7/5 17:14	应用程序扩展	59 KB
 trfo-2.dll	2018/7/5 17:14	应用程序扩展	29 KB
 tucl-1.dll	2018/7/5 17:14	应用程序扩展	9 KB
 ucl.dll	2018/7/5 17:14	应用程序扩展	57 KB
 xdvl-0.dll	2018/7/5 17:14	应用程序扩展	32 KB
 zlib1.dll	2018/7/5 17:14	应用程序扩展	59 KB

图：Satan勒索病毒释放的永恒之蓝攻击工具包

三、勒索病毒家族种类介绍

瑞星安全专家通过对勒索病毒的传播速度、感染量、加密手段以及开发门槛选取了10个具有代表性的家族病毒进行分析，帮助用户更好的了解勒索病毒。

1、WannaCry家族：利用“永恒之蓝”漏洞传播，危害巨大

WannaCry勒索病毒，最早出现在2017年5月，通过永恒之蓝漏洞传播，短时间内对整个互联网造成非常大的影响。受害者文件被加上.WNCRY后缀，并弹出勒索窗口，要求支付赎金，才可以解密文件。由于网络中仍存在不少未打补丁的机器，此病毒至今仍然有非常大的影响。



图：WannaCry勒索病毒

2、BadRabbit家族：弱口令攻击，加密文件和MBR

Bad Rabbit勒索病毒，主要通过水坑网站传播，攻击者攻陷网站，将勒索病毒植入，伪装为adobe公司的flash程序图标，诱导浏览网站的用户下载运行。用户一旦下载运行，勒索病毒就会加密受害者计算机中的文件，加密计算机的MBR，并且会使用弱口令攻击局域网

中的其它机器。

```
Dops! Your files have been encrypted.

If you see this text, your files are no longer accessible.
You might have been looking for a way to recover your files.
Don't waste your time. No one will be able to recover them without our
decryption service.

We guarantee that you can recover all your files safely. All you
need to do is submit the payment and get the decryption password.

Visit our web service at caforssztxqzf2nm.onion

Your personal installation key#1:

2A29puFgAbfR2ntQUzarGKA10CKR/Fc6KdhprLLoQw+G2ZLnNcvPE4nhJB1zveFL
LPb2DCeRYgnfpWgw9QnY1zw4gkQA08F+UiYUypoyCis1DtxCzEiiqKb8c5xH05ol
PLW0RH3wa6v/31WeQ70x6PWtA+0W8W33M29k0xAWpXDSUUCWm09+X14HEHvKho1U
5bnLlKwBFi7XT2idWoyx15n0vTX6C1jLo+Gm3U/zgxGsr00MGwmQvu.janeteCHv
IXFIxAmBs09M4ib22CARyWfwm7IWBem10jY2et1zvW0T41dk1uGiUbAG/utboUJN
hENvbbcbCOP7PjWlf03YvG16WRGEXYm1/A==

If you have already got the password, please enter it below.
Password#1: _
```

图：BadRabbit勒索病毒

3、GlobelImposter家族：变种众多持续更新

GlobelImposter勒索病毒是一种比较活跃的勒索病毒，病毒会加密本地磁盘与共享文件夹的所有文件，导致系统、数据库文件被加密破坏，由于GlobelImposter采用RSA算法加密，因此想要解密文件需要作者的RSA私钥，文件加密后几乎无法解密，被加密文件后缀曾用过Techno、DOC、CHAK、FREEMAN、TRUE、RESERVER、ALCO、Dragon444等。

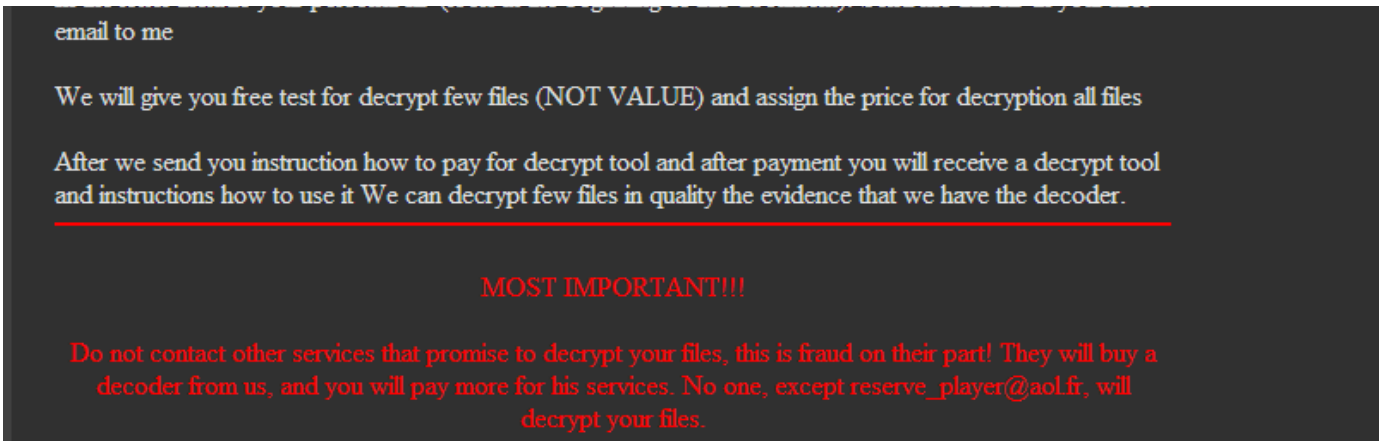
☢ YOUR FILES ARE ENCRYPTED! ☢

□ TO DECRYPT, FOLLOW THE INSTRUCTIONS BELOW. □

To recover data you need decrypt tool.
To get the decrypt tool you should:

Send 1 crypted test image or text file or document to reserve_player@aol.fr
(Or alternate mail reserve_player11@india.com)

In the letter include your personal ID (look at the beginning of this document). Send me this ID in your first

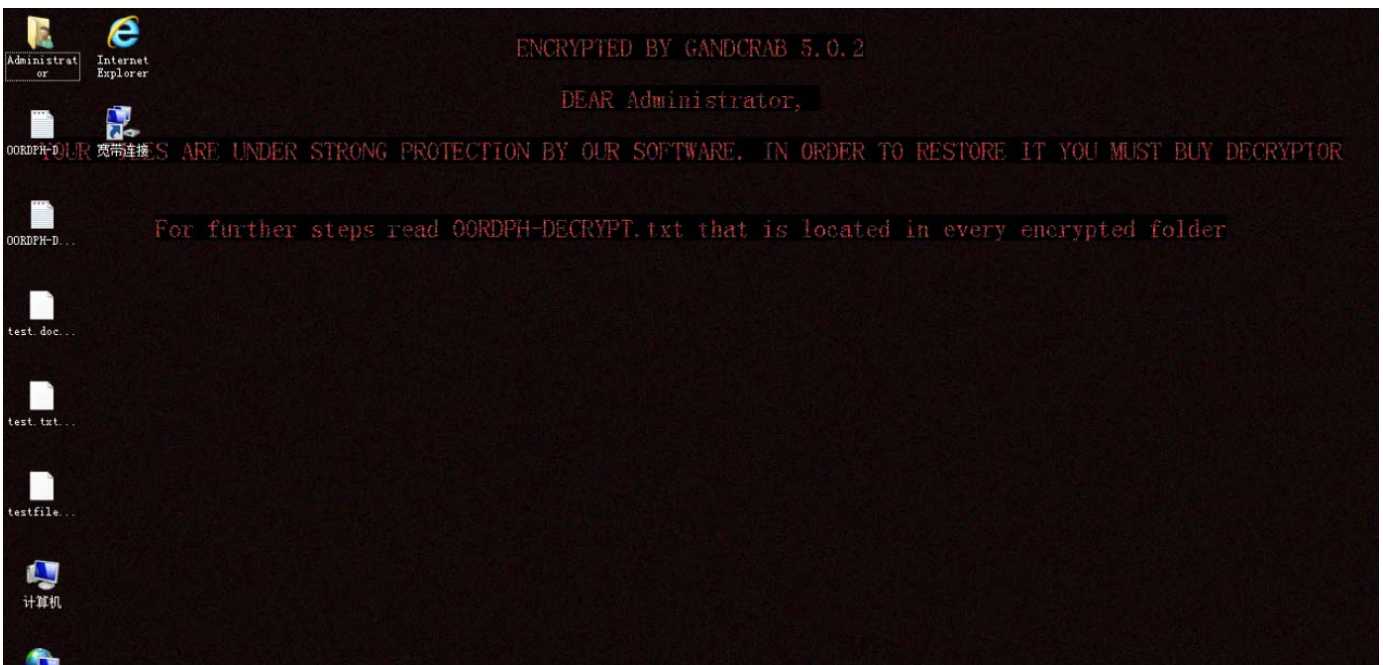


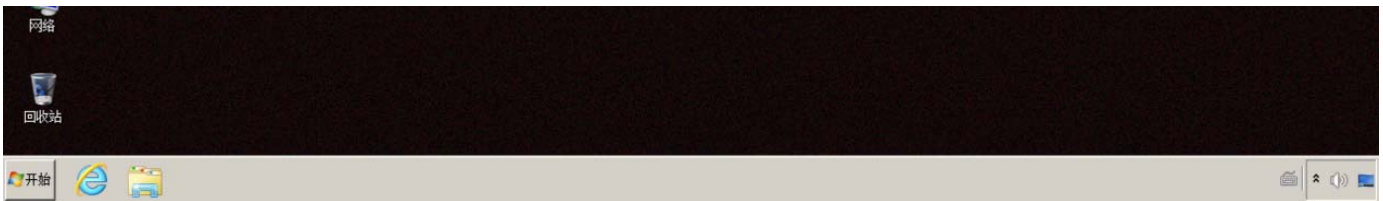
图：GlobelImposter勒索病毒

4、GandCrab家族：使用达世币勒索，更新频繁

Gandcrab是首个以达世币（DASH）作为赎金的勒索病毒，此病毒自出现以来持续更新对抗查杀。被加密文件后缀通常被迫加上.CRAB .GDCB .KRAB 等后缀。从新版本勒索声明上看没有直接指明赎金类型及金额，而是要求受害用户使用Tor网络或者Jabber即时通讯软件获得下一步行动指令，极大地增加了追踪难度。

随着版本的不断更新，Gandcrab的传播方式多种多样，包括网站挂马、伪装字体更新程序、邮件、漏洞、木马程序等。此病毒至今已出现多个版本，该家族普遍采用较为复杂的RSA+AES混合加密算法，文件加密后几乎无法解密，最近的几个版本为了提高加密速度，对文件加密的算法开始使用Salsa20算法，密钥被非对称加密算法加密，若没有病毒作者的私钥，正常方式通常无法解密，给受害者造成了极大的损失。





图：Gandcrab勒索病毒

5、Crysis家族：加密文件，删除系统自带卷影备份

Crysis勒索病毒家族是比较活跃的勒索家族之一。攻击者使用弱口令暴力破解受害者机器，很多公司都是同一个密码，就会导致大量机器中毒。此病毒运行后，加密受害者机器中的文件，删除系统自带的卷影备份，被加密文件后缀格式通常为“编号+邮箱+后缀”，例如：

id-{编号}.[gracey1c6rwhite@aol.com].bip

id-{编号}.[chivas@aolonline.top].arena

病毒使用AES加密文件，使用RSA加密密钥，在没有攻击者的RSA私钥的情况下，无法解密文件，因此危害较大。

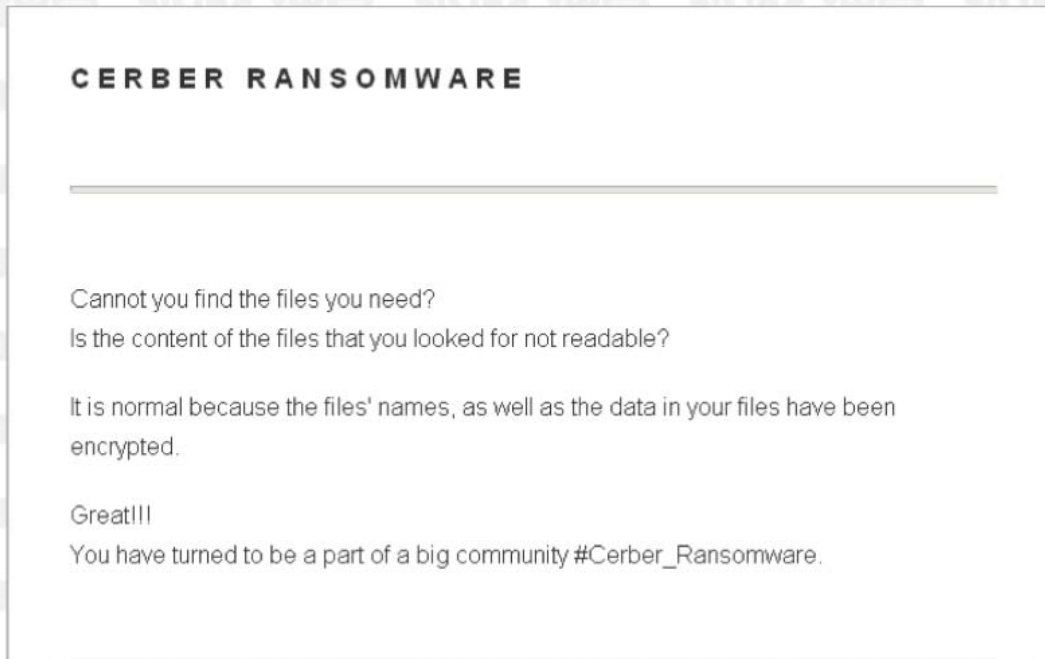


图：Crysis勒索病毒

6、Cerber家族：通过垃圾邮件和挂马网页传播

Cerber家族是2016年年初出现的一种勒索软件。从年初的1.0版本一直更新到4.0版。传播方式主要是垃圾邮件和EK挂马，索要赎金为1-2个比特币。到目前为止加密过后的文件没有公开办法进行解密。

Cerber勒索信息

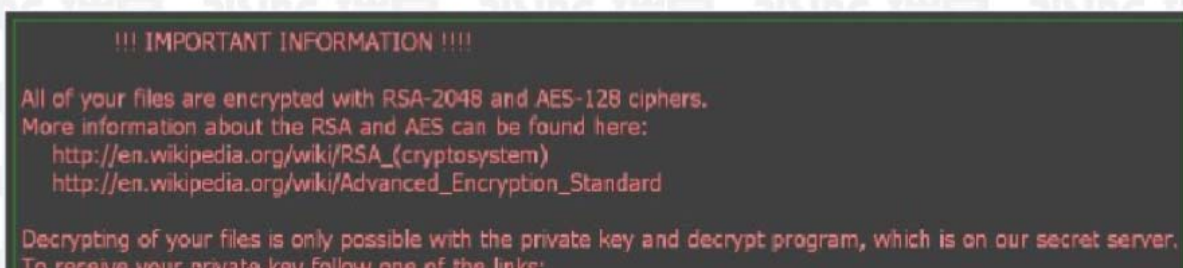


图：Cerber勒索病毒

7、Locky家族：早期勒索病毒，持续更新多个版本

Locky家族是2016年流行的勒索软件之一，和Cerber的传播方式类似，主要采用垃圾邮件和EK，勒索赎金0.5-1个比特币。

Locky勒索信息图




```
1. http://6dtgqam4crv6rr6.tor2web.org/A34FD477586C993E
2. http://6dtgqam4crv6rr6.onion.to/A34FD477586C993E
3. http://6dtgqam4crv6rr6.onion.cab/A34FD477586C993E

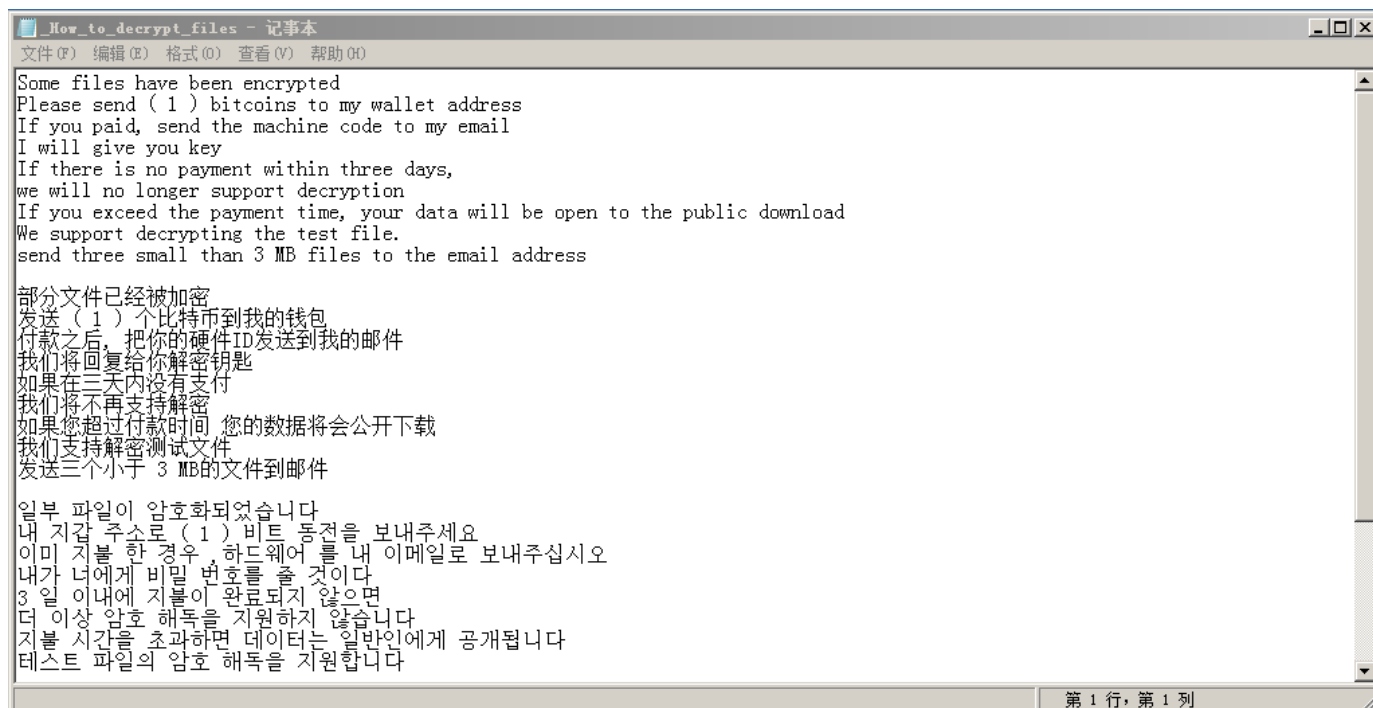
If all of this addresses are not available, follow these steps:
1. Download and install Tor Browser: https://www.torproject.org/download/download-easy.html
2. After a successful installation, run the browser and wait for initialization.
3. Type in the address bar: 6dtgqam4crv6rr6.onion/A34FD477586C993E
4. Follow the instructions on the site.

!!! Your personal identification ID: A34FD477586C993E !!! □FD
```

图：Locky勒索病毒

8、Satan家族：使用多种web漏洞和“永恒之蓝”漏洞传播

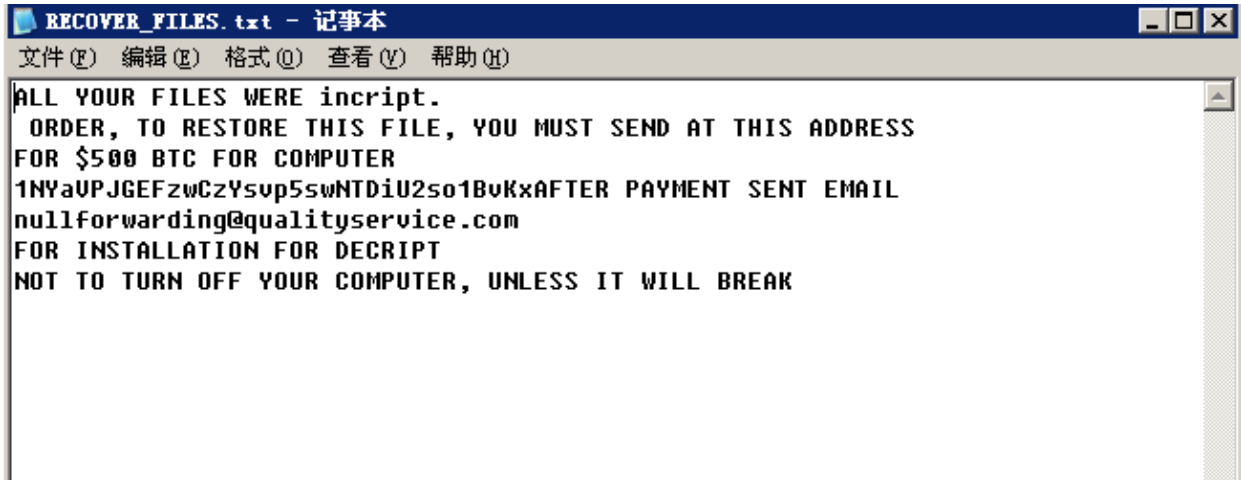
撒旦Satan勒索病毒运行之后加密受害者计算机文件并勒索赎金，被加密文件后缀为.satan。自诞生以来持续对抗查杀，新版本除了使用永恒之蓝漏洞攻击之外，还增加了其它漏洞攻击。病毒内置了大量的IP列表，中毒后会继续攻击他人。此病毒危害巨大，也给不打补丁的用户敲响了警钟。幸运的是此病毒使用对称加密算法加密，密钥硬编码在病毒程序和被加密文件中，因此可以解密。瑞星最早开发出了针对此病毒的解密工具。



图：Satan勒索病毒

9、Hc家族：Python开发，攻击门槛低，危害较大

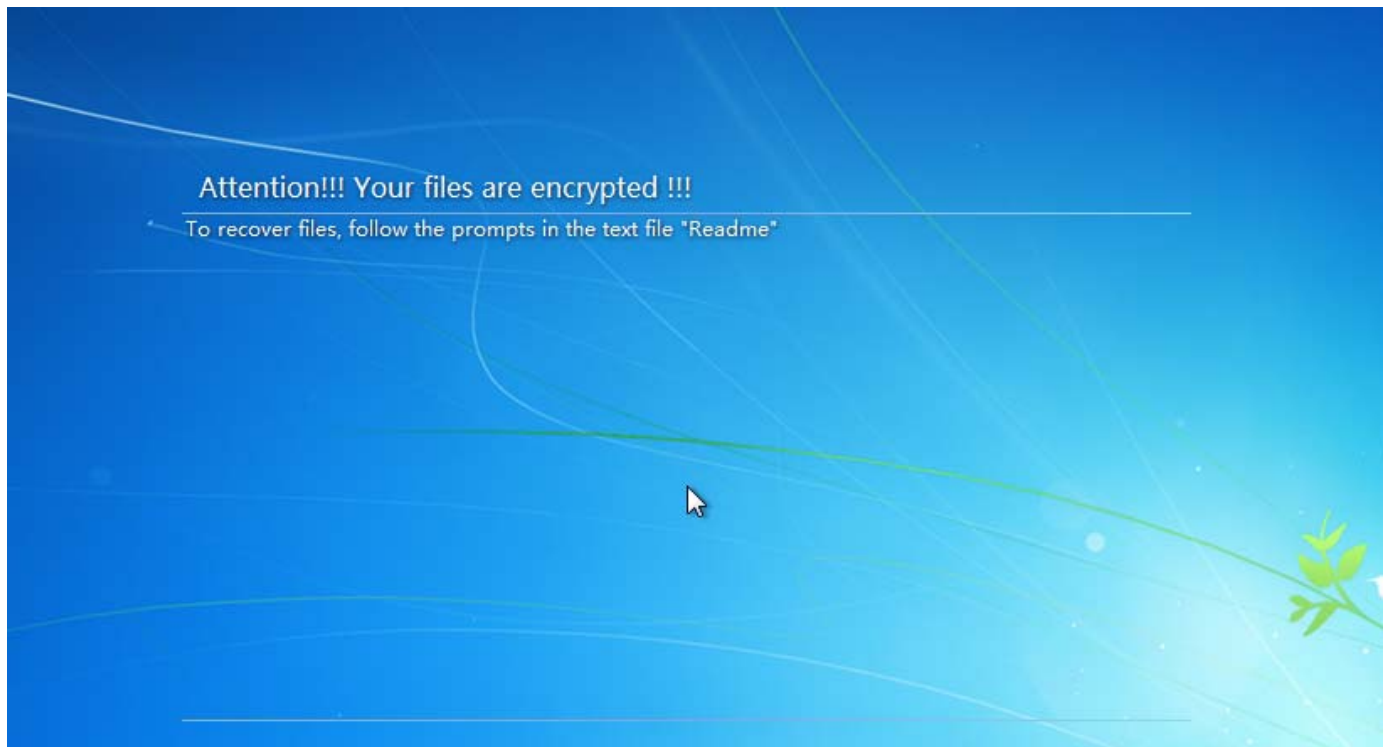
Hc家族勒索病毒使用python编写，之后使用pyinstaller打包。攻击者使用弱口令扫描互联网中机器植入病毒。此病毒的出现使勒索病毒的开发门槛进一步降低，但是危险指数并没有降低。通常使用RDP弱口令入侵受害机器植入病毒。早期版本使用对称加密算法，密钥硬编码在病毒文件中，新版本开始使用命令行传递密钥。



图：Hc勒索病毒

10、LockCrypt家族：加密文件，开机提示勒索

LockCrypt病毒运行后会加密受害者系统中的文件，并修改文件的名称格式为: [FileID]=ID [UserID].lock。其中\$FileID为原始文件名加密base64编码得到，\$UserID 为随机数生成。重启后会弹出勒索信息，要求受害者支付赎金，才可解密文件。



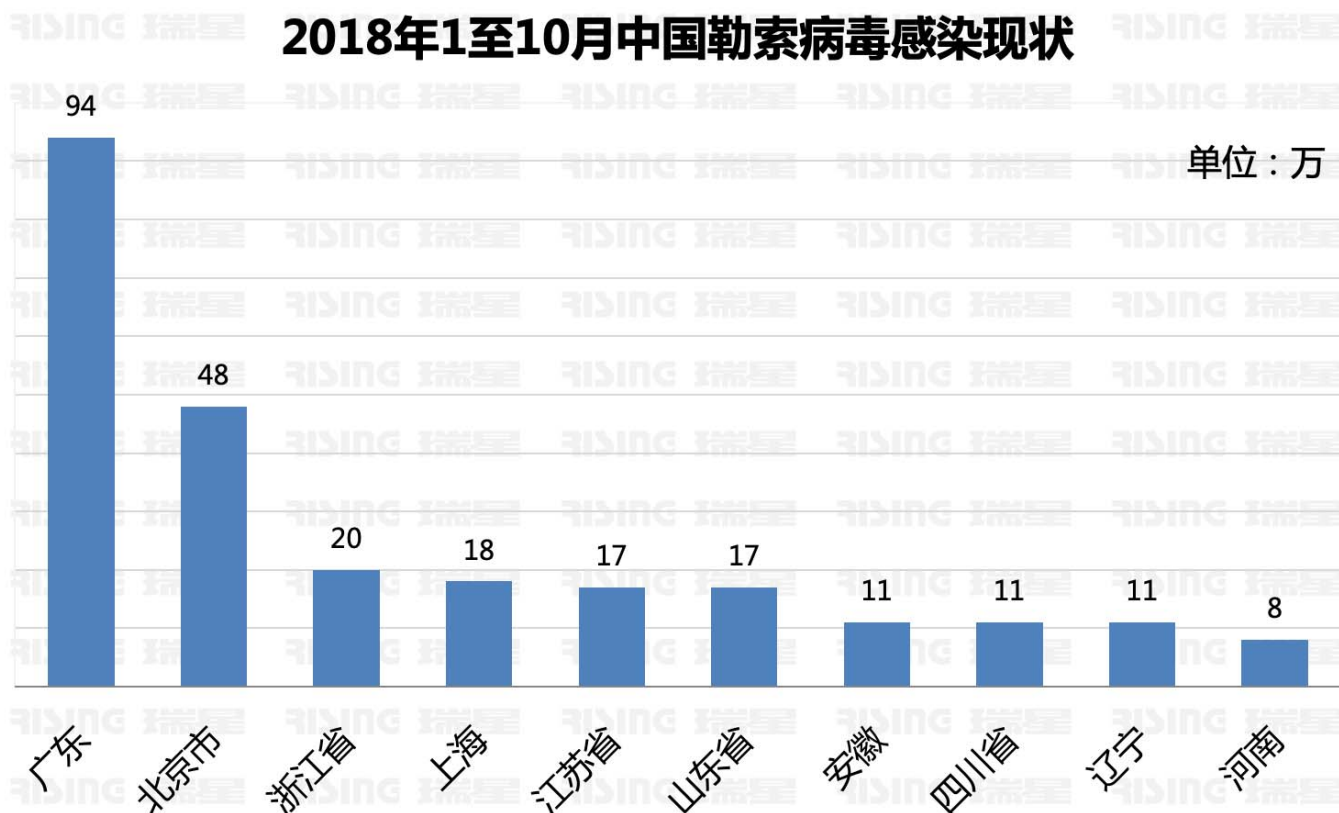
确定

图：LockCrypt勒索病毒

四、勒索病毒感染状况

1、2018年1至10月中国勒索病毒感染现状

2018年1至10月，瑞星“云安全”系统共截获勒索软件样本42.82万个，感染共计344万次，其中广东省感染94万次，位列全国第一，其次为北京市48万次，浙江省20万次及上海市18万次。

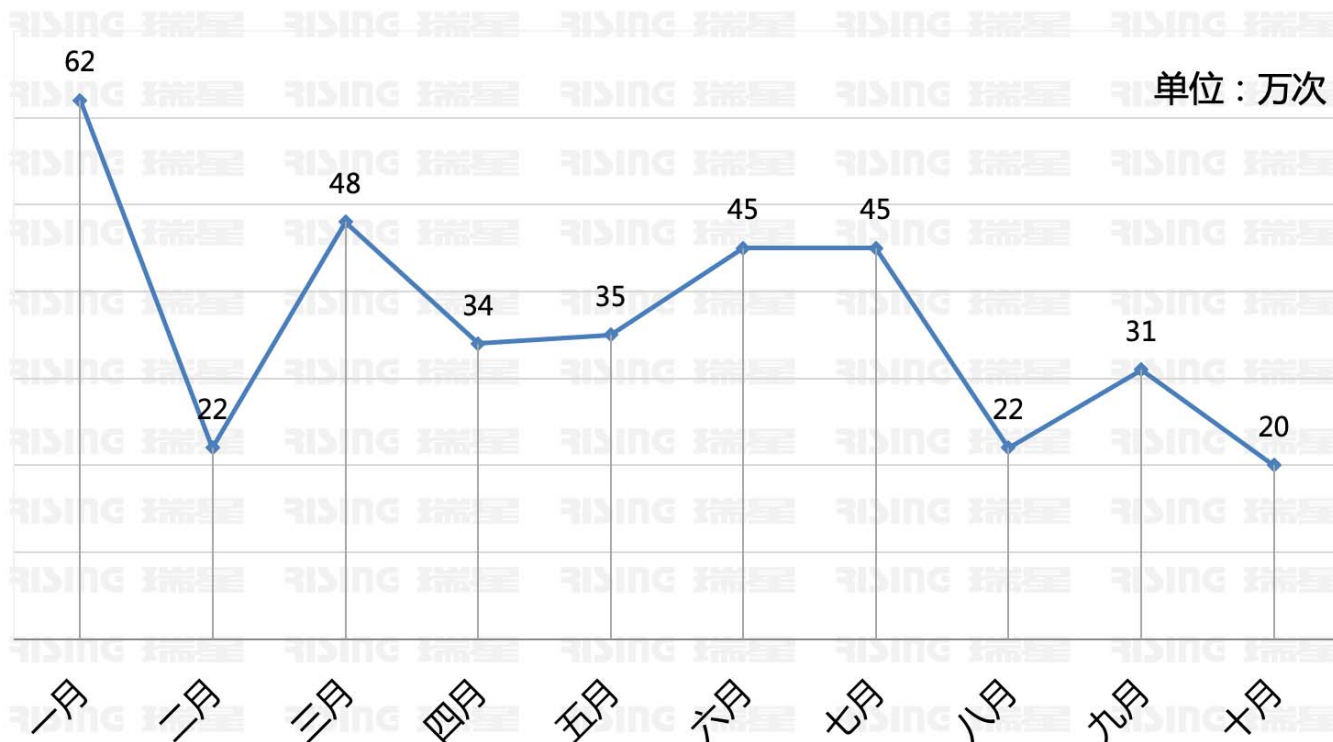


图：2018年1至10月中国勒索病毒感染状况

2、2018年1至10月勒索病毒各月感染数量

通过对瑞星捕获的勒索样本分析发现，一月为勒索病毒高发期，感染共计62万次，位列第一，其次为三月48万次，以及6月与7月45万次。



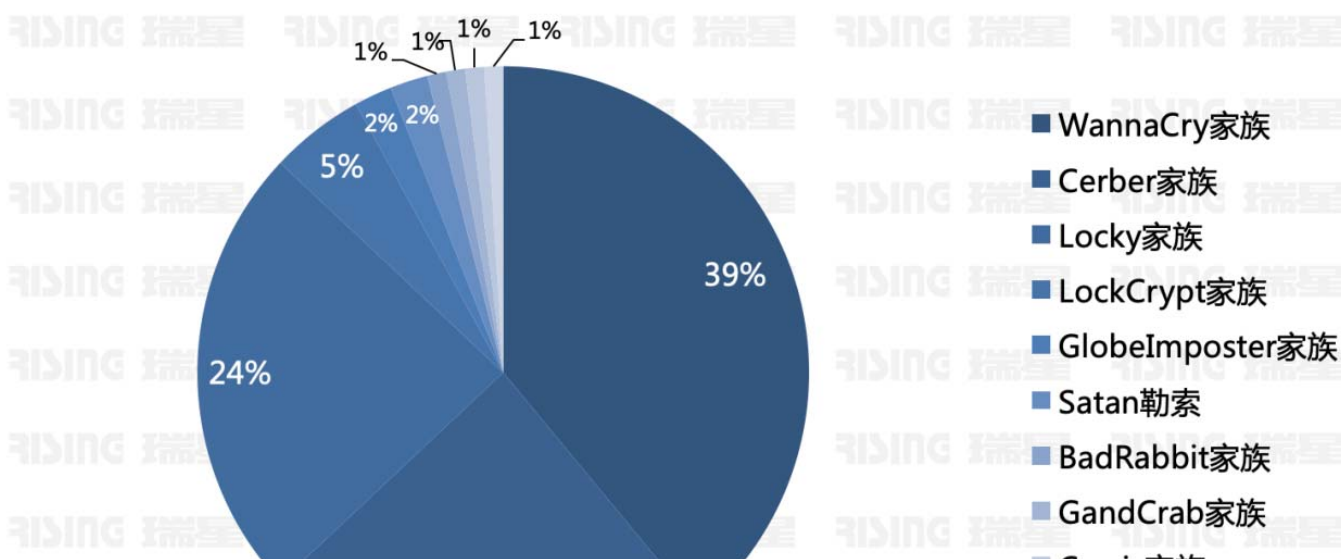


图：2018年1至10月勒索病毒各月感染数量

3、2018年1至10月各个勒索家族感染样本占比

通过对瑞星捕获的勒索样本按家族分析发现，WannaCry家族占比39%，位列第一，其次为Cerber家族与Locky家族占比24%。时隔一年，WannaCry勒索病毒依然影响最大，由此可以看出，很多企业互联网中仍然存在很多未打“永恒之蓝”漏洞补丁的机器，导致其危害至今仍在持续。

2018年1至10月各个勒索家族感染样本占比



24%

图：2018年1至10月各个勒索家族感染样本占比

五、全球勒索病毒攻击事件

1、WannaCry勒索病毒袭击全球

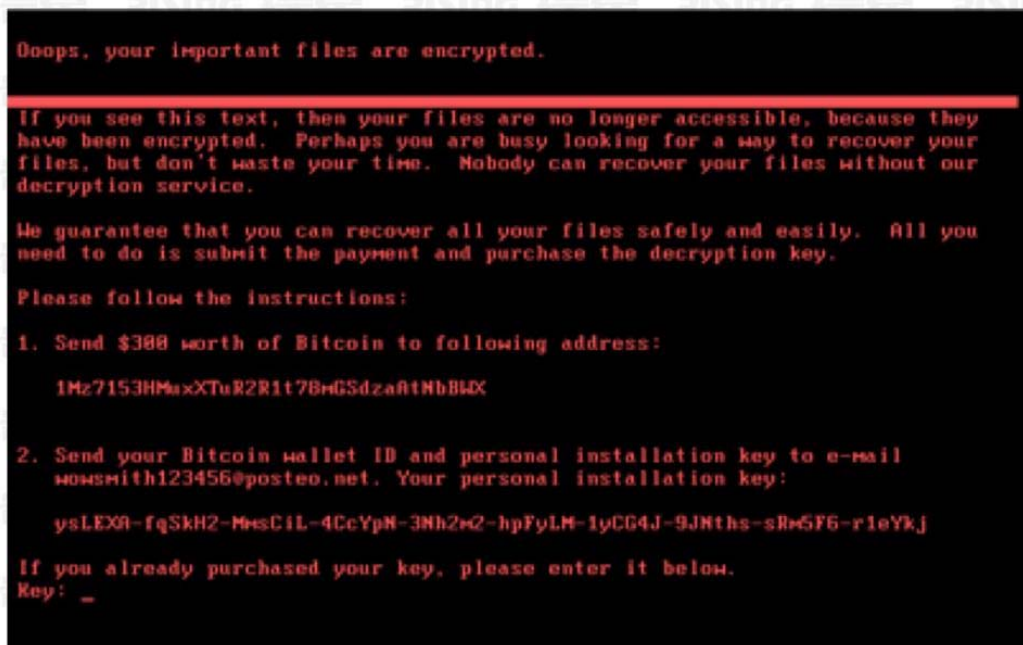
2017年5月，一款名为WannaCry的勒索病毒席卷全球，包括中国、美国、俄罗斯及欧洲在内的100多个国家，我国部分高校内网、大型企业内网和政府机构专网遭受攻击较为严重。勒索软件利用的是微软SMB远程代码执行漏洞CVE-2017-0144，微软已在2017年3月份发布了该漏洞补丁。2017年4月黑客组织影子经纪人（The Shadow Brokers）公布的方程式组织（Equation Group）使用的“EternalBlue”中包含了该漏洞利用程序，而该勒索软件的攻击者在借鉴了“EternalBlue”后发起了这次全球性大规模勒索攻击。



图：WannaCry勒索病毒

2、Petya勒索病毒借勒索之名袭击多国

2017年6月，一个名为“Petya（中文音译彼佳）”的新勒索病毒再度肆虐全球，包括乌克兰首都国际机场、乌克兰国家储蓄银行、邮局、地铁、船舶公司、俄罗斯的石油和天然气巨头 Rosneft、丹麦的航运巨头马士基公司、美国制药公司默克公司、美国律师事务所DLA Piper、乌克兰一些商业银行以及部分私人公司、零售企业和政府系统，甚至是核能工厂都遭到了攻击。影响的国家有英国、乌克兰、俄罗斯、印度、荷兰、西班牙、丹麦等。与 WannaCry相比，该病毒会加密NTFS分区，覆盖MBR，阻止机器正常启动，影响更加严重。



图：Petya勒索病毒袭击全球

3、勒索韩国网络托管公司的Erebus 病毒

2017年6月份，韩国网络托管公司Nayana在6月10日遭受网络攻击，导致旗下153台Linux 服务器与3,400个网站感染Erebus勒索软件。事件发生后，韩国互联网安全局、国家安全机构已与警方展开联合调查，Nayana公司也表示，他们会积极配合，尽快重新获取服务器控制权限。在努力无果后，Nayana公司最终还是选择以支付赎金的方式换取其服务器的控制权限，向勒索黑客支付价值100万美元的比特币，来解密指定的文件。

4、BadRabbit勒索病毒突袭东欧

2017年10月，新型勒索病毒BadRabbit在东欧爆发，乌克兰、俄罗斯等企业及基础设施受灾严重。该病毒会伪装成flash_player，诱导用户下载，当用户下载后，病毒会加密特定格式文件，修改MBR，并索要比特币。BadRabbit可以通过弱口令和漏洞在局域网扩散，成为勒索病毒蠕虫化的典型代表。

5、湖北某医院内网遭到勒索病毒疯狂攻击

2018年3月，湖北某医院内网遭到勒索病毒疯狂攻击，导致该医院大量的自助挂号、缴费、报告查询打印等设备无法正常工作。由于这些终端为自助设备，只提供特定的功能，安全性没有得到重视，系统中没有安装防病毒产品，系统补丁没有及时更新，同时该医院中各个科室的网段没有很好的隔离，导致勒索病毒集中爆发。

6、国内多地发生GlobeImposter勒索病毒攻击事件

2018年7月，勒索病毒GlobeImposter众多变种开始在国内进行传播，各个变种加密文件后修改的文件后缀名也各不相同，其主要是通过垃圾邮件进行传播。GlobeImposter是目前流行的一类勒索病毒，它会加密磁盘文件并篡改后缀名为.Techno、.DOC、.CHAK、.FREEMAN、.TRUE等形式。由于其采用高强度非对称加密方式，受害者在没有私钥的情况下无法恢复文件，如需恢复重要资料只能被迫支付赎金。

六、勒索病毒分析

（一）勒索病毒爆发原因

1、加密手段复杂，解密成本高

勒索软件都采用成熟的密码学算法，使用高强度的对称和非对称加密算法对文件进行加密。除非在实现上有漏洞或密钥泄密，不然在没有私钥的情况下几乎不可能解密。当受害者数据非常重要又没有备份的情况下，除了支付赎金没有什么别的方法去恢复数据，正是因为这点勒索者能源源不断的获取高额收益，推动了勒索软件的爆发增长。

互联网上也流传有一些被勒索软件加密后的修复软件，但这些都是利用了勒索软件实现上的漏洞或私钥泄露才能够完成的。如Petya和Cryptxxx家族恢复工具利用了开发者软件实现上的漏洞，TeslaCrypt和CoinVault家族数据恢复工具是利用了key的泄露来实现的。

2、使用电子货币支付赎金，变现快追踪难

几乎所有勒索软件支付赎金的手段都是采用比特币来进行的。比特币因为他的一些特点:匿名、变现快、追踪困难，再加上比特币名气大，大众比较熟知，支付起来困难不是很大而被攻击者大量使用。可以说比特币很好的帮助了勒索软件解决赎金的问题，进一步推动了勒索软件的繁荣发展。

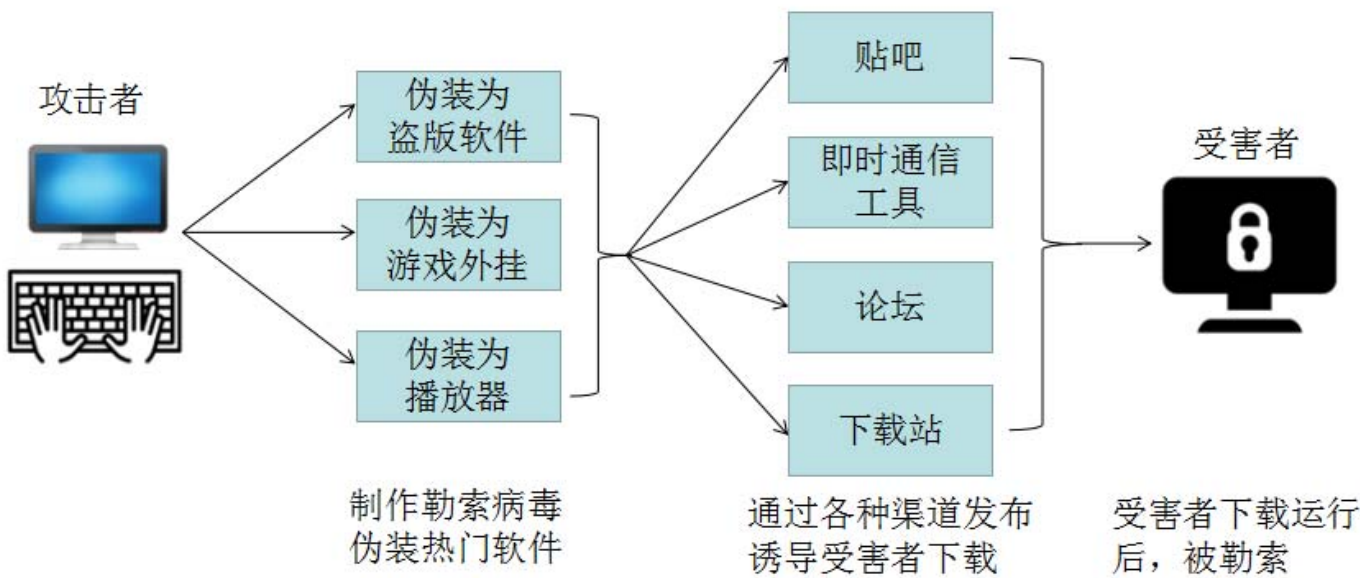
3、Ransomware-as-a-server (勒索服务化) 的出现

勒索软件服务化，开发者提供整套勒索软件解决方案，从勒索软件的开发、传播到赎金收取都提供完整的服务。攻击者不需要任何知识，只要支付少量的租金就可以开展勒索软件的非法勾当，这大大降低了勒索软件的门槛，推动了勒索软件大规模爆发。

(二) 勒索病毒传播方式

1、针对个人用户常见的攻击方式

通过用户浏览网页下载勒索病毒，攻击者将病毒伪装为盗版软件、外挂软件、色情播放器等，诱导受害者下载运行病毒，运行后加密受害者机器。此外勒索病毒也会通过钓鱼邮件和系统漏洞进行传播。针对个人用户的攻击流程如下图所示：



图：攻击流程

2、针对企业用户常见的攻击方式

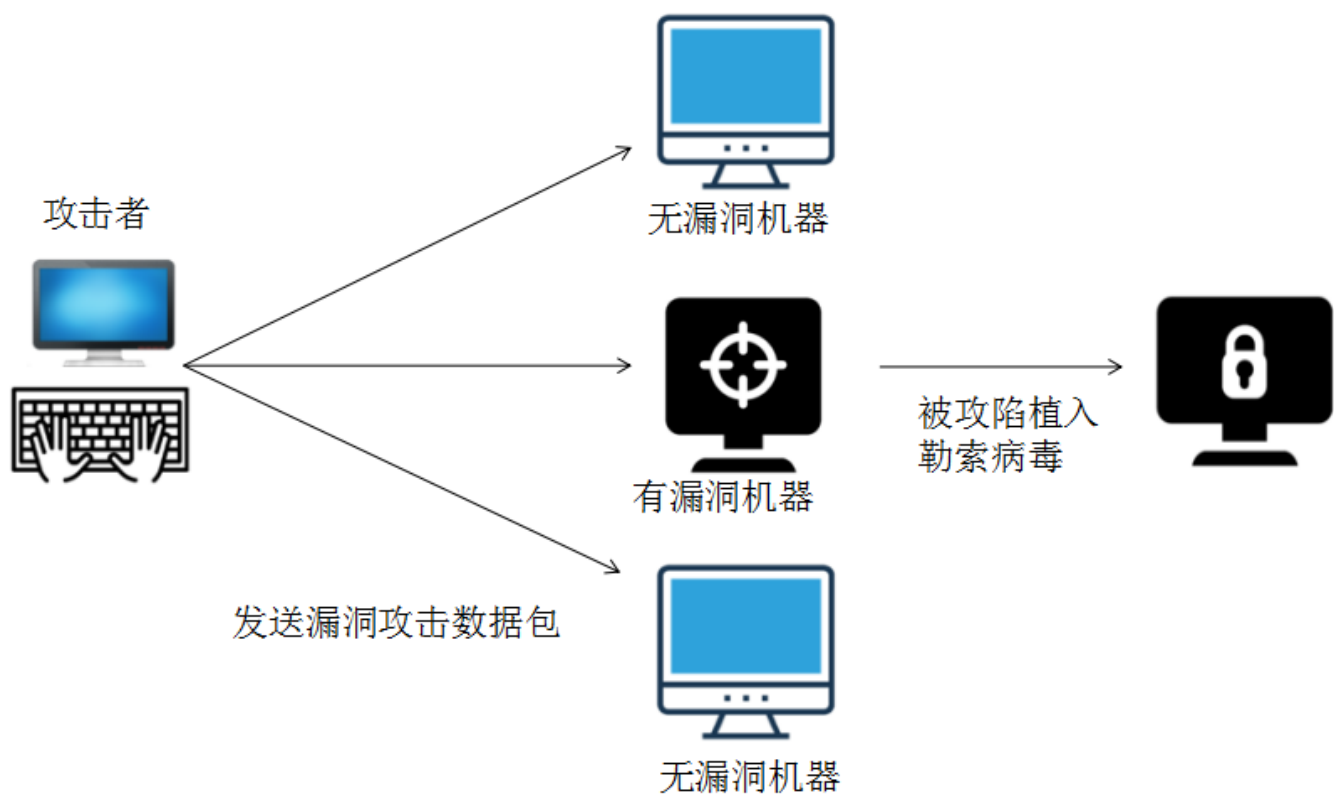
勒索病毒针对企业用户常见的攻击方式包括系统漏洞攻击、远程访问弱口令攻击、钓鱼

邮件攻击、web服务漏洞和弱口令攻击、数据库漏洞和弱口令攻击等。其中，钓鱼邮件攻击包括通过漏洞下载运行病毒、通过office机制下载运行病毒、伪装office、PDF图标的exe程序等。

1) 系统漏洞攻击

系统漏洞是指操作系统在逻辑设计上的缺陷或错误，不法者通过网络植入木马、病毒等方式来攻击或控制整个电脑，窃取电脑中的重要资料和信息，甚至破坏系统。同个人用户一样，企业用户也会受到系统漏洞攻击，由于企业局域网中机器众多，更新补丁费时费力，有时还需要中断业务，因此企业用户不太及时更新补丁，给系统造成严重的威胁，攻击者可以通过漏洞植入病毒，并迅速传播。席卷全球的Wannacry勒索病毒就是利用了永恒之蓝漏洞在网络中迅速传播。

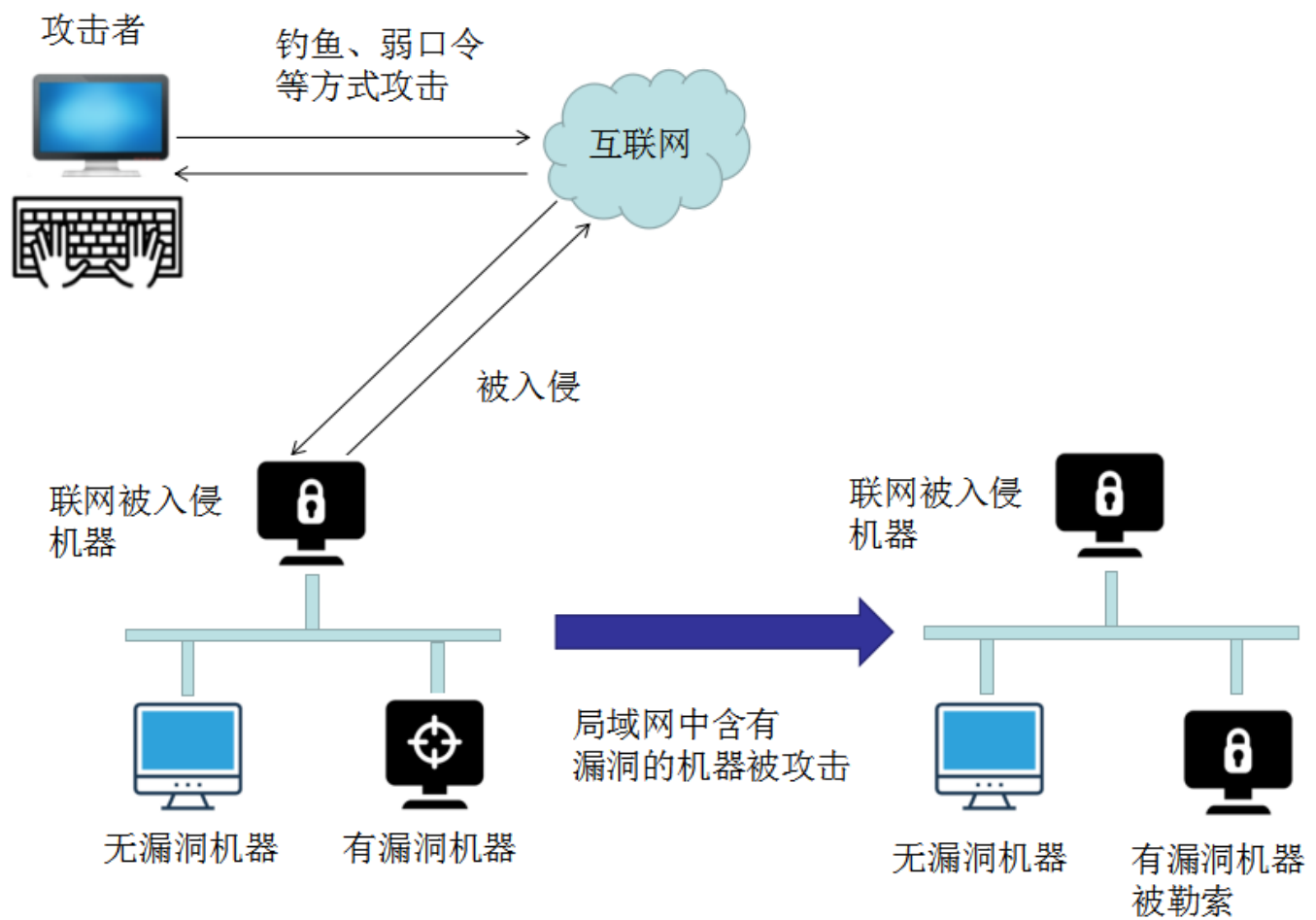
攻击者利用系统漏洞主要有以下两种方式，一种是通过系统漏洞扫描互联网中的机器，发送漏洞攻击数据包，入侵机器植入后门，然后上传运行勒索病毒。



图：通过系统漏洞扫描网络中的计算机

另外一种是通过钓鱼邮件、弱口令等其他方式，入侵连接了互联网的一台机器，然后再

利用漏洞局域网横向传播。大部分企业的网络无法做到绝对的隔离，一台连接了外网的机器被入侵，内网中存在漏洞的机器也将受到影响。



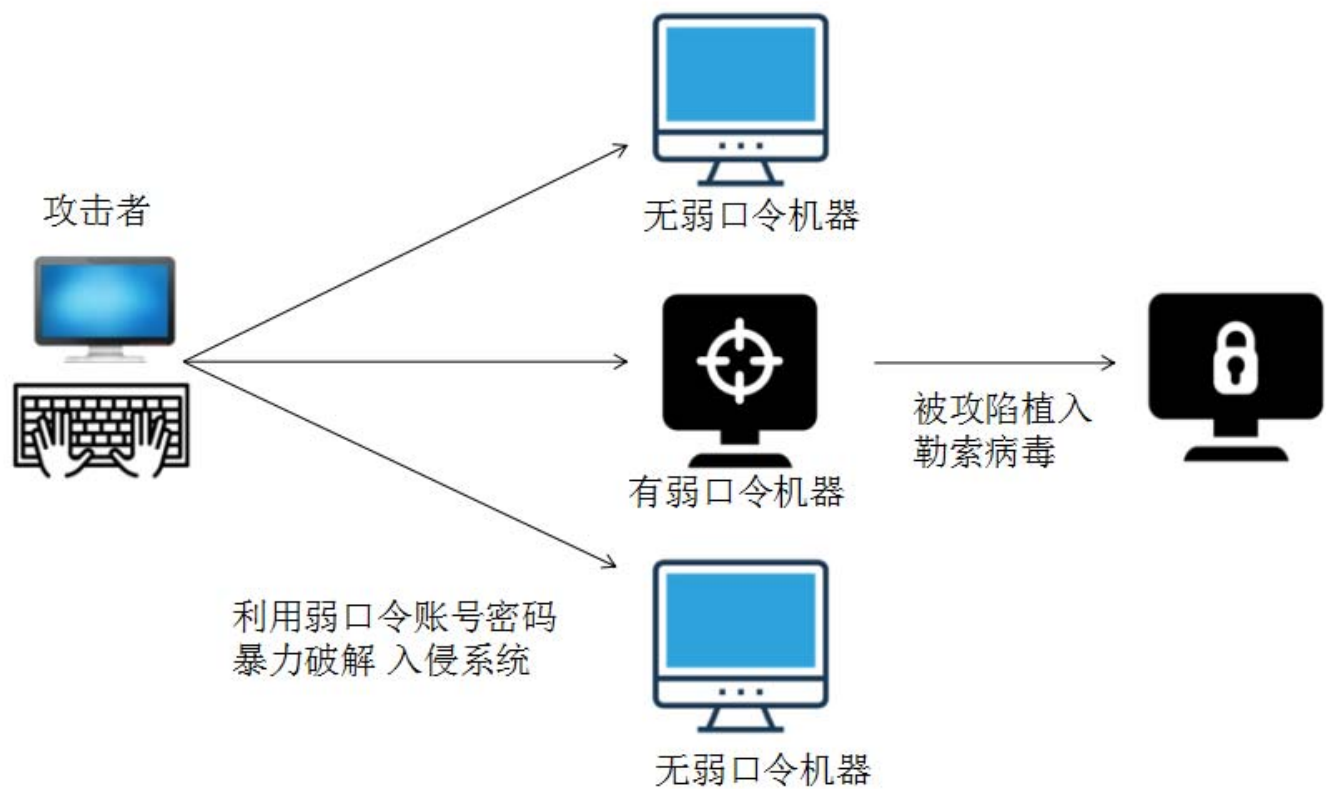
图：入侵一台机器后再通过漏洞局域网横向传播

网上有大量的漏洞攻击工具，尤其是武器级别的NSA方程式组织工具的泄露，给网络安全造成了巨大的影响，被广泛用于传播勒索病毒、挖矿病毒、木马等。有攻击者将这些工具，封装为图形化一键自动攻击工具，进一步降低了攻击的门槛。

2) 远程访问弱口令攻击

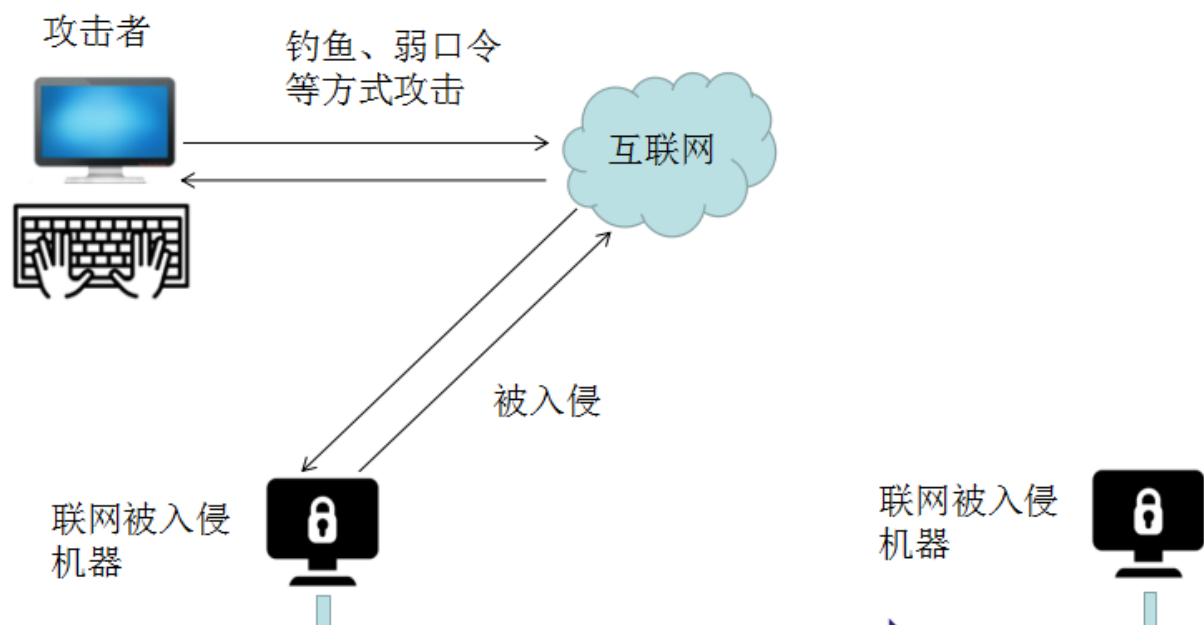
由于企业机器很多需要远程维护，所以很多机器都开启了远程访问功能。如果密码过于简单，就会给攻击者可乘之机。很多用户存在侥幸心理，总觉得网络上的机器这么多，自己被攻击的概率很低，然而事实上，在全世界范围内，成千上万的攻击者不停的使用工具扫描网络中存在弱口令的机器。有的机器由于存在弱口令，被不同的攻击者攻击，植入了多种病毒。这个病毒还没删除，又中了新病毒，导致机器卡顿，文件被加密。

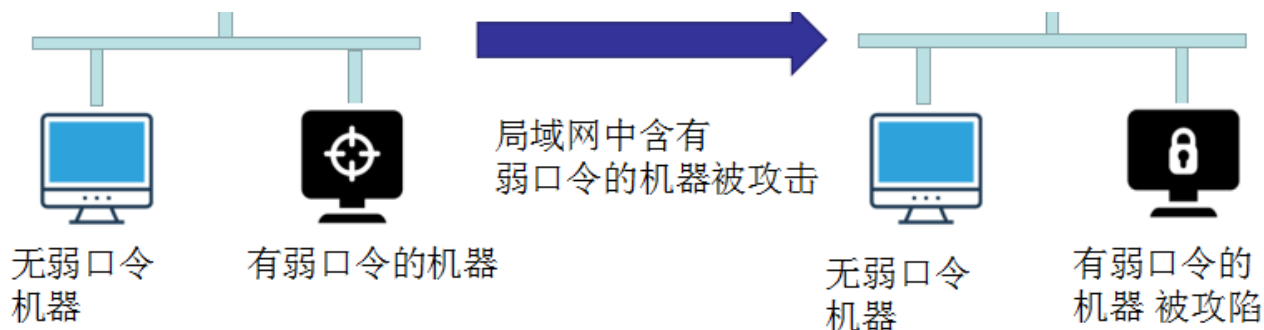
通过弱口令攻击和漏洞攻击类似，只不过通过弱口令攻击使用的是暴力破解，尝试字典中的账号密码来扫描互联网中的设备。



图：弱口令扫描网络中的计算机

通过弱口令攻击还有另一种方式，一台连接外网的机器被入侵，通过弱口令攻击内网中的机器。

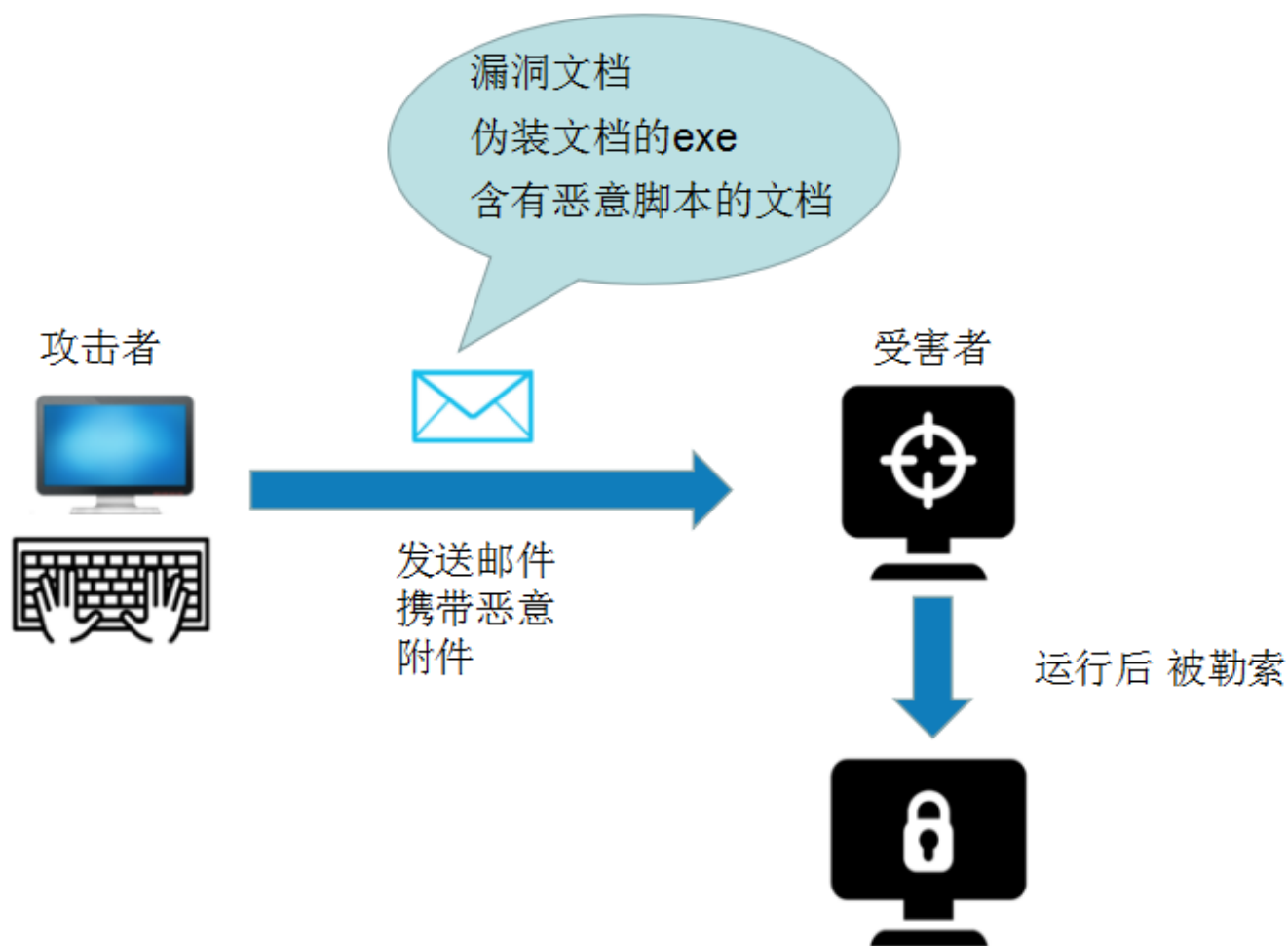




图：入侵一台机器再弱口令爆破局域网机器横向传播

3) 钓鱼邮件攻击

企业用户也会受到钓鱼邮件攻击，相对个人用户，由于企业用户使用邮件频率较高，业务需要不得不打开很多邮件，而一旦打开的附件中含有病毒，就会导致企业整个网络遭受攻击。钓鱼邮件攻击逻辑图：



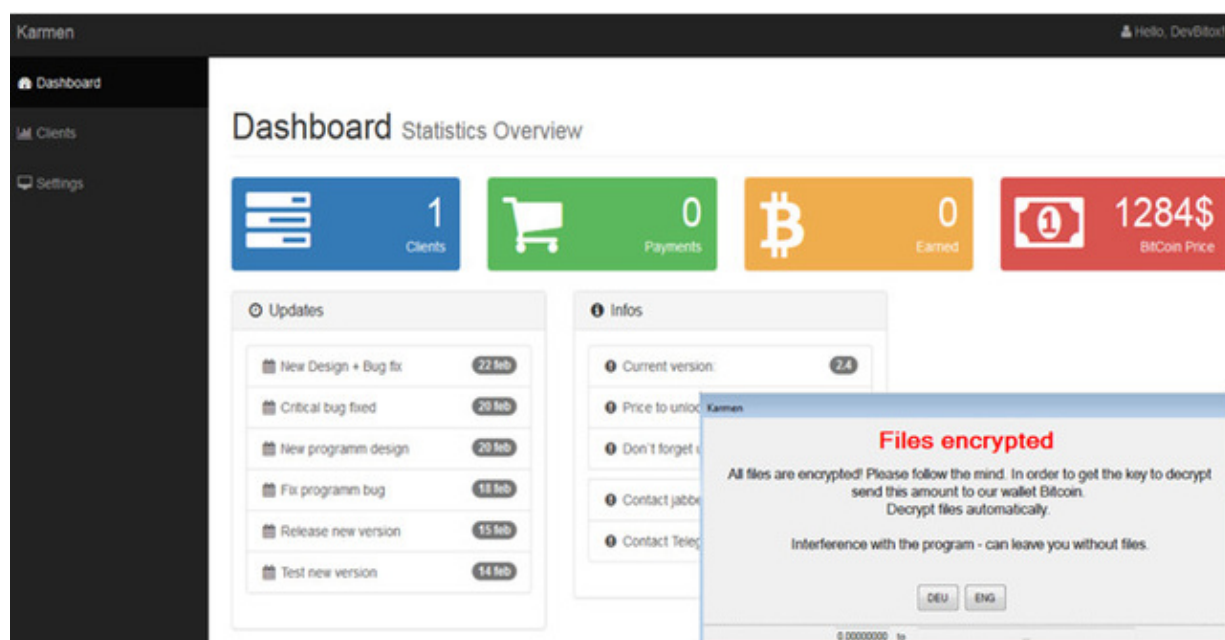
图：钓鱼邮件攻击逻辑

通过钓鱼邮件传播勒索病毒，主要有以下方式：

(a) 通过漏洞下载运行病毒

钓鱼邮件附件携带攻击者精心构造的，含有漏洞的office文档、PDF文档或者含有浏览器漏洞的网址。如果没有安装对应办公软件补丁、浏览器补丁，打开之后就会触发漏洞，下载并运行勒索病毒。

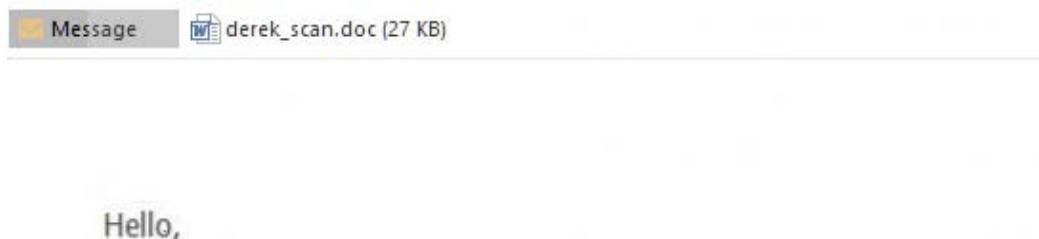
此外，网上存在大量Exploit Kit（漏洞攻击包），漏洞攻击包里面集成了各种浏览器、Flash和PDF等软件漏洞代码。攻击者一键自动化生成钓鱼邮件，简直是勒索即服务。受害者点击链接或者打开文档就可以触发漏洞，下载运行勒索软件。常见比较著名的EK有Angler、Nuclear、Neutrino和RIG等。其中一款漏洞攻击包的操作界面如下：



图：漏洞攻击包的操作界面

(b) 通过office机制下载运行病毒

除了漏洞之外，office的一些机制也可以被用来传播勒索病毒，office宏脚本、DDE、OLE等都曾被利用传播勒索病毒。有的攻击者为了防止被查杀，发送邮件时对附件中office文档进行加密，同时在邮件正文中附带密码。

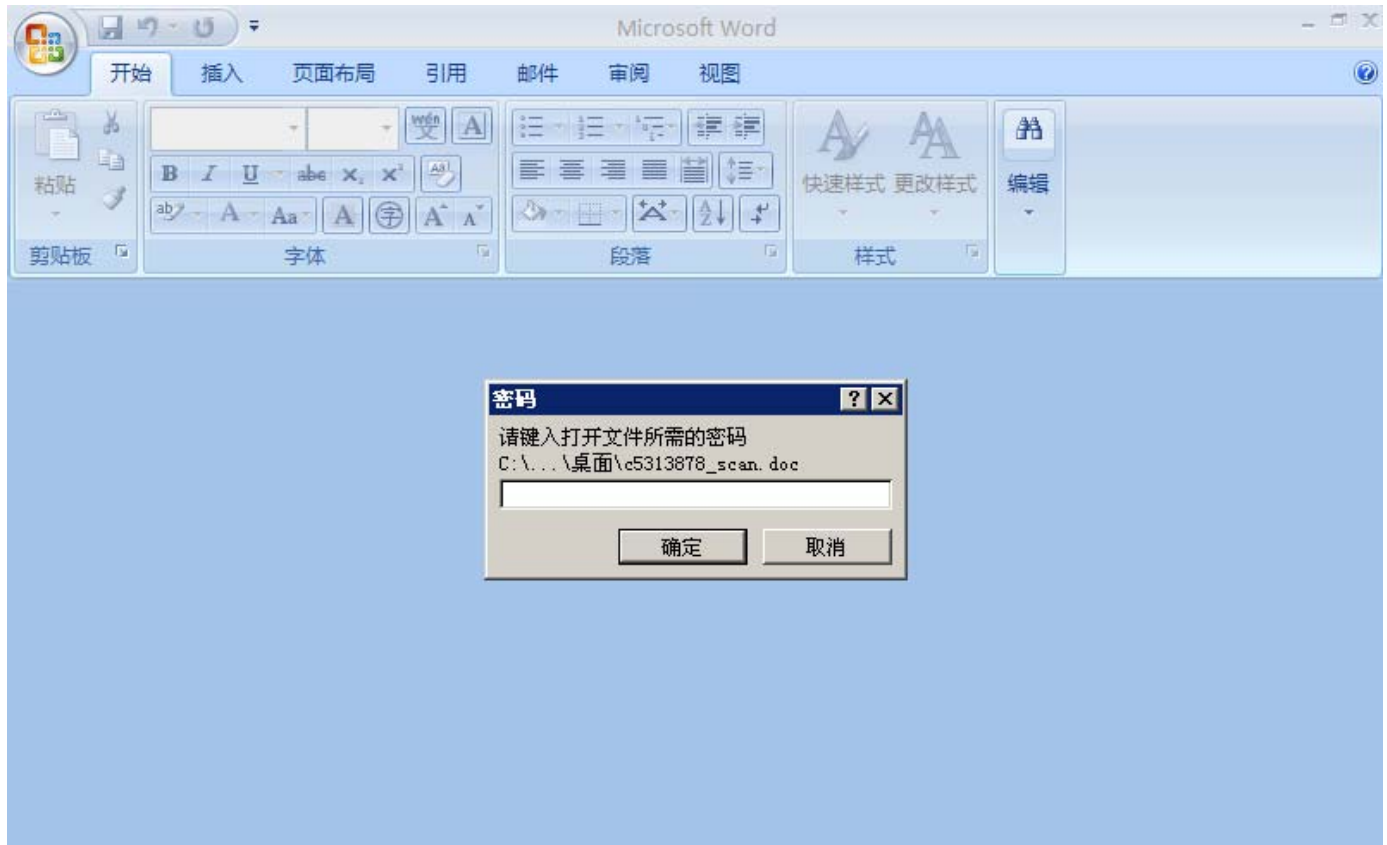


Your Visa card ending in XXXX will be charged \$3,187.26 shortly.
Take a look at attachment for details. Password is **1115**.

Thank you.

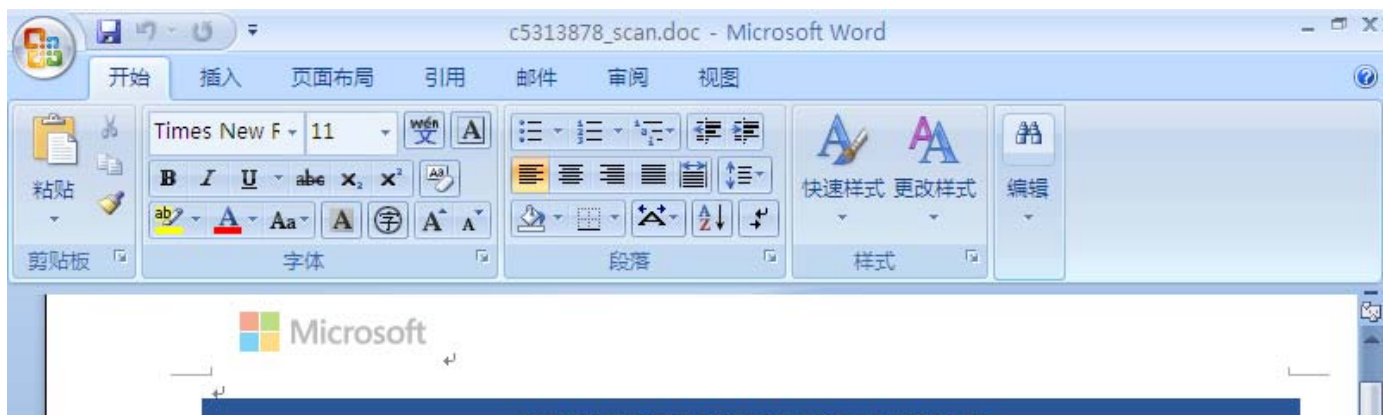
图：钓鱼邮件

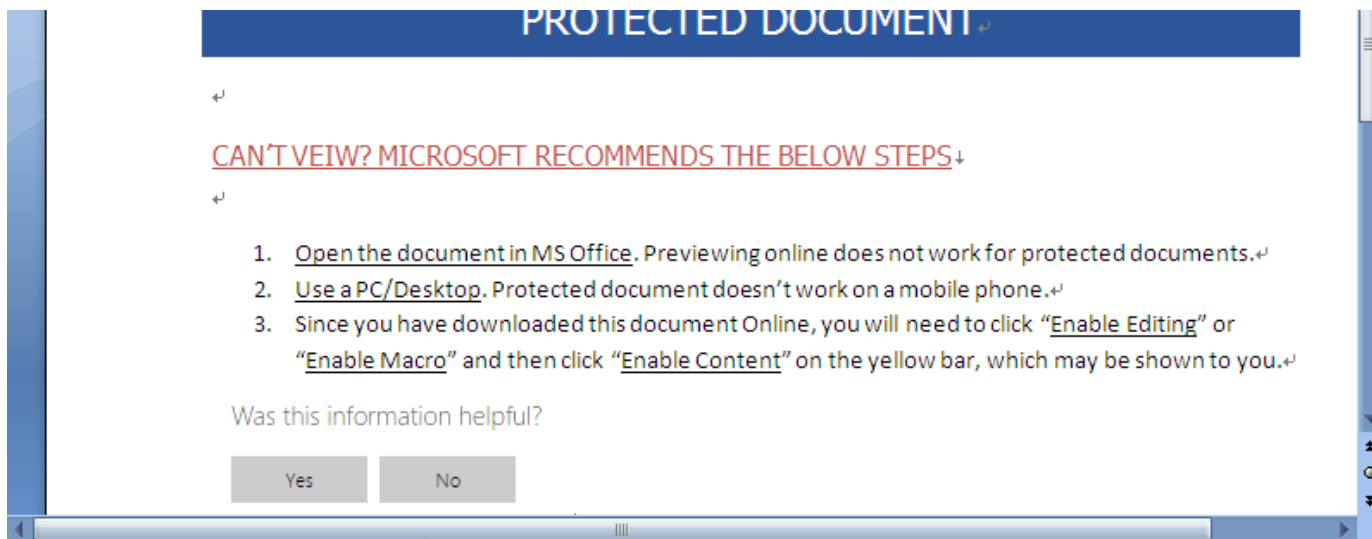
好奇心比较强的用户会输入密码打开文件，如果默认开启宏脚本，输入密码后病毒就会下载执行。



图：加密的文档

如果没有开启宏脚本，文件内容也会诱导用户启用宏。





图：诱导启动宏

(c) 伪装office、PDF图标exe程序

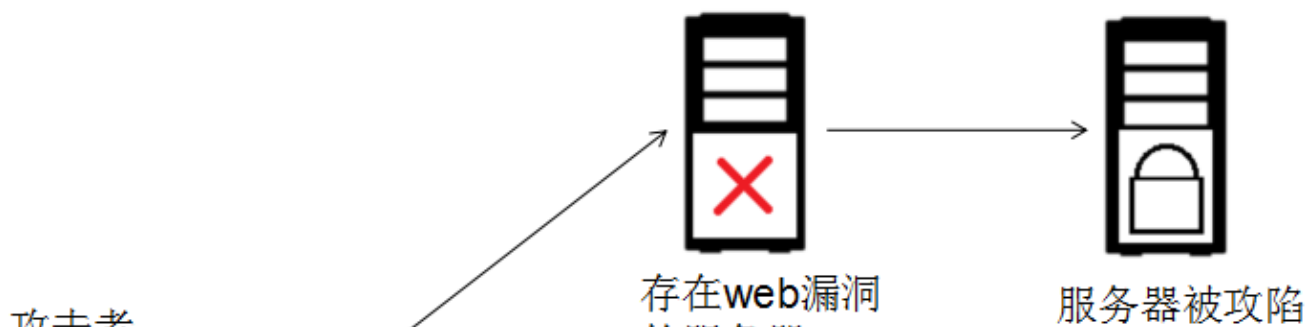
邮件附件携带的勒索程序会伪装为office文档图标，实际上是exe程序，如果系统默认不显示文件扩展名，那就很容易中招。

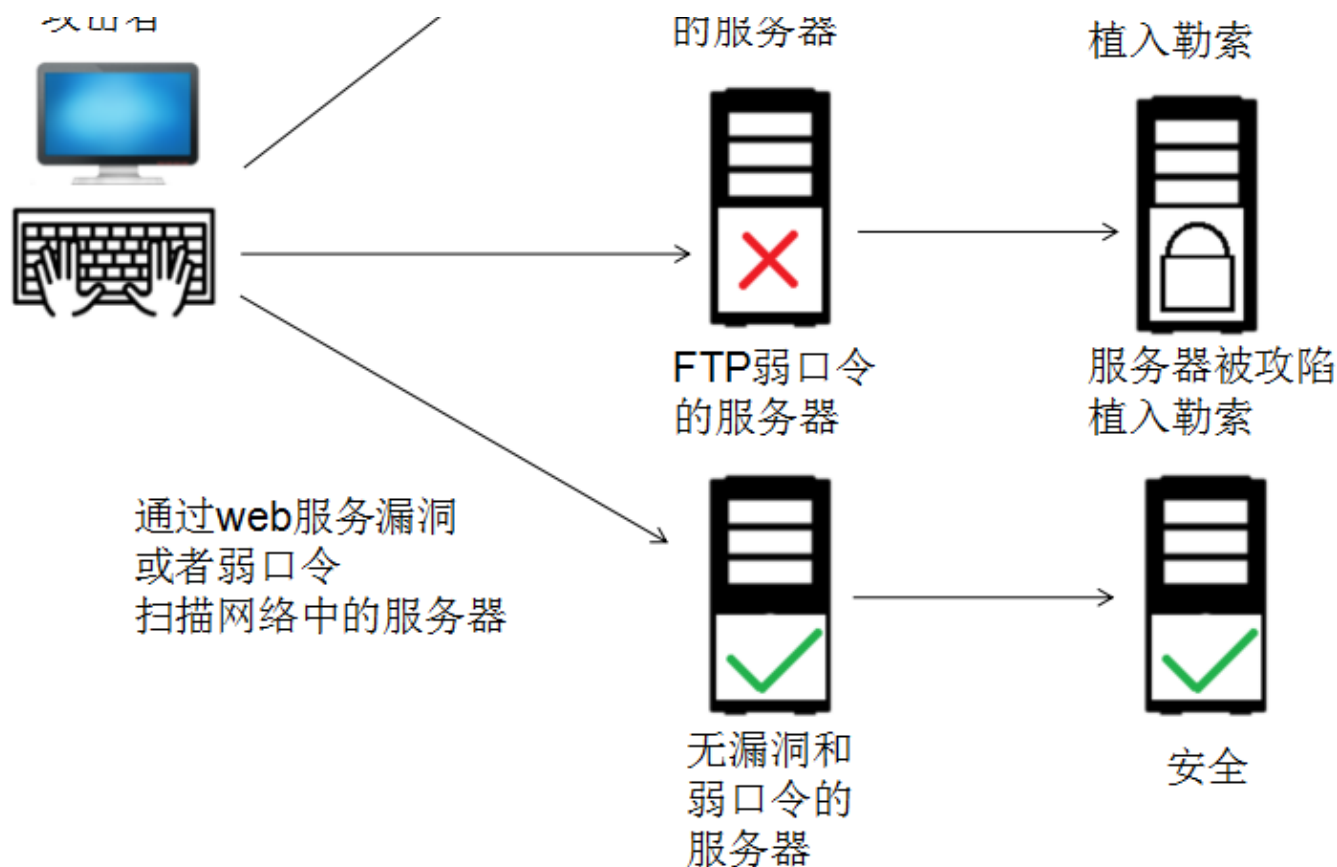


图：伪装图标

4) web服务漏洞和弱口令攻击

很多企业服务器运行了web服务器软件，开源web框架，CMS管理系统等，这些程序也经常出现漏洞。如果不及时修补，攻击者可以利用漏洞上传运行勒索病毒。此外如果web服务使用弱口令也会被暴力破解，有些企业甚至一直采用默认密码从没有修改过。常见攻击逻辑如下图所示：



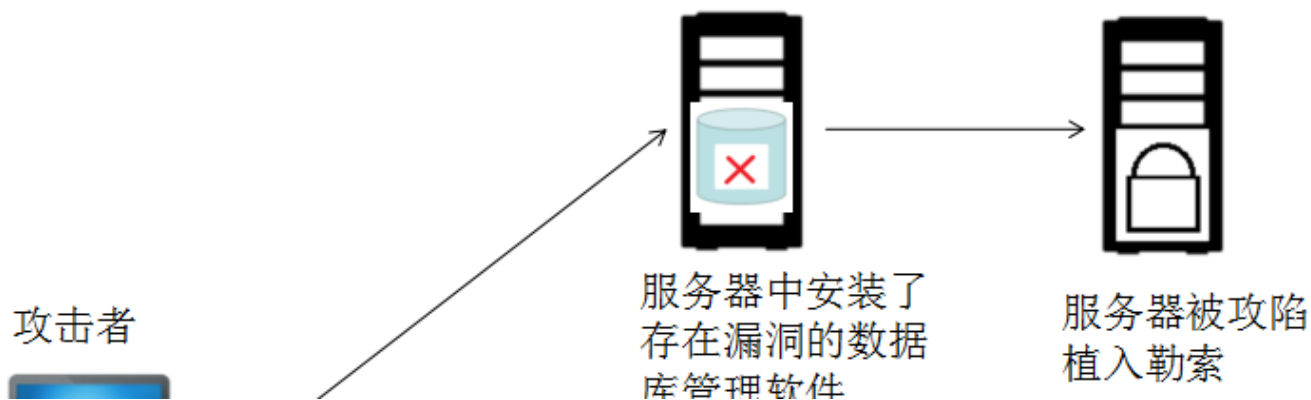


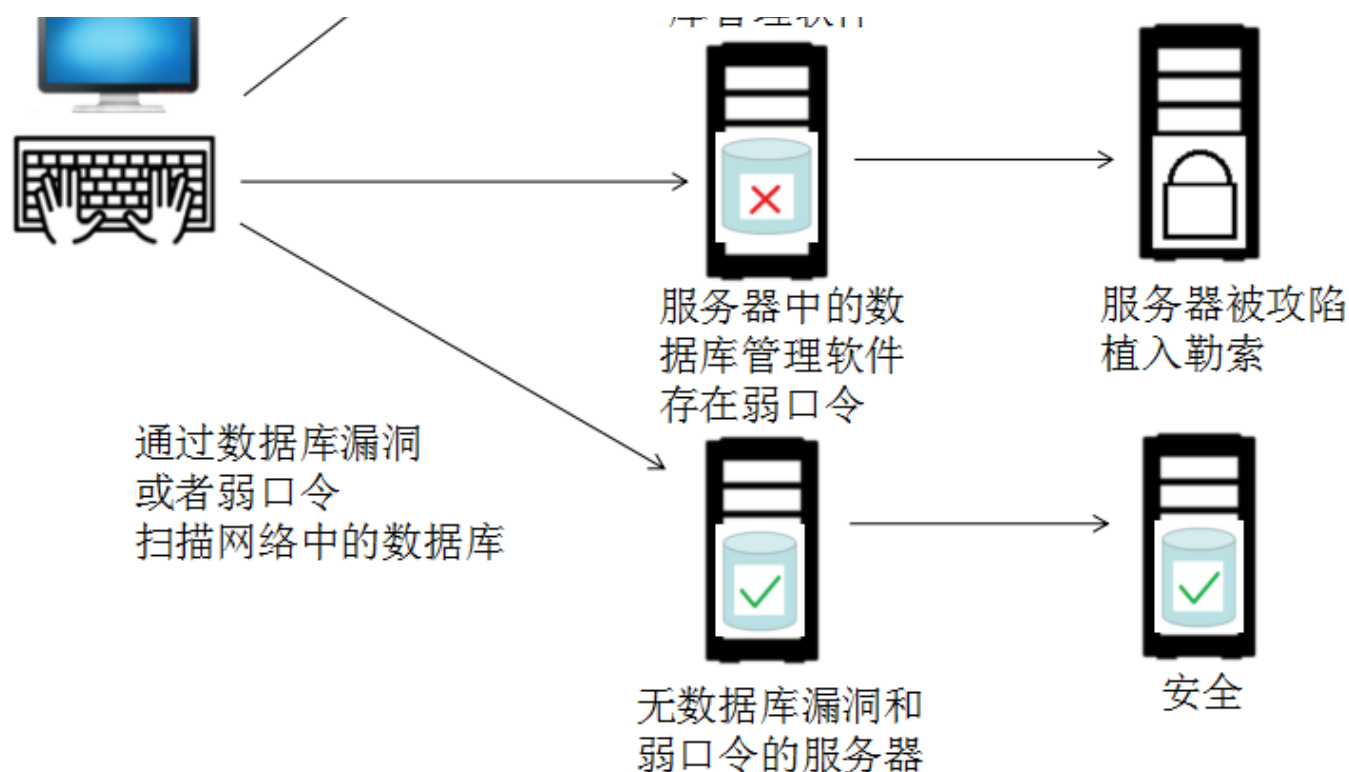
图：web服务攻击逻辑

Apache Struts2是世界上最流行的JavaWeb服务器框架之一，2017年Struts2被曝存在重大安全漏洞S2-045，攻击者可在受影响服务器上执行系统命令，进一步可完全控制该服务器，从而上传并运行勒索病毒。

5) 数据库漏洞和弱口令攻击

数据库管理软件也存在漏洞，很多企业多年没有更新过数据库软件，甚至从服务器搭建以来就没有更新过数据库管理软件，有的是因为疏忽，也有的是因为兼容问题，担心数据丢失。如果不及时更新，会被攻击者利用漏洞上传运行勒索病毒。常见攻击逻辑如下图：





图：针对数据库的攻击逻辑

（三）勒索病毒趋势分析

1、利用漏洞和弱口令植入勒索增多

传统的勒索病毒，一般通过垃圾邮件、钓鱼邮件、水坑网站等方式传播，受害者需要下载运行勒索病毒才会中毒。而通过漏洞和弱口令扫描互联网中的计算机，直接植入病毒并运行，效率要高很多。GandCrab、Crysis、GlobelImposter 等勒索病毒主要就是通过弱口令传播，GandCrab内部虽然不含漏洞攻击的部分，但是有证据表明攻击者已经开始使用web漏洞植入此病毒，而Satan更是凶狠，不仅使用永恒之蓝漏洞攻击，还包含了web漏洞和数据库漏洞，包括CVE-2017-10271 WebLogic WLS组件漏洞、CVE-2017-12149 JBOOS 反序列化漏洞、tomcat弱口令等，从而增加攻击成功的概率。因此防御勒索病毒也从传统的不下载可疑文件、不打开可疑附件，过渡到及时安装系统和web服务的补丁，不使用弱口令密码。

2、攻击者入侵后人工投毒增多

攻击者通过弱口令或者漏洞，入侵一台可以访问互联网的计算机后，远程操作这台机器，攻击局域网中的其它机器，这些机器虽然没有连接互联网，但是和被攻击的机器相连，因此攻击者可以通过这台机器攻击局域网的其它机器。所以内外网隔离非常重要，否则再坚

固的堡垒，一旦从内部遭受到攻击，就会损失惨重。

攻击者一旦远程登陆一台机器，就会通过工具手工关闭杀软，植入并运行勒索病毒，并继续扫描攻击局域网中的其它机器。此外由于局域网中大量机器使用弱口令和相同密码，给攻击者提供了便利，因此及时更新补丁非常重要。

3、勒索病毒持续更新迭代对抗查杀

GandCrab勒索（后缀GDCB、CRAB、GRAB、KRAB）、Satan勒索（后缀Satan、dbger、sicck）、Crysis勒索（后缀arena、bip）、GlobelImposter勒索（后缀reserver、Dragon444）等勒索持续更新，每隔一段时间就会出现一个新变种，有的修改加密算法，增加了加密速度，有的为了对抗查杀，做了免杀、反调试、反沙箱，并且后缀也会随之改变。此外有的勒索病毒新版本开始使用随机后缀，从而增加受害者查找所中勒索类型的难度，迫使受害者只能联系攻击者留下的邮箱来进行解密。

4、针对有价值目标发起定向攻击逐渐增多

相对于广撒网方式，定向攻击植入勒索病毒的事件逐渐增多。攻击者一般会选择更有勒索价值的目标进行定向攻击，包括医院、学校、防护不足的中小企业等，这些企业通常防护不足，数据非常重要，如学生数据、患者医疗数据、公司业务文件等，一旦此类资料被加密，受害者支付赎金的可能性就会更高，所以攻击者会有针对性的定向攻击此类企业。

5、勒索病毒开发门槛进一步降低

一方面由于各种编程语言脚本都可以被用来编写勒索软件，大大降低了勒索软件的开发门槛，有不少刚接触计算机的未成年人也开始制作勒索软件。从近期捕获的勒索病毒样本来看，有使用python编写勒索软件，伪装为office文档图标的。有使用Autoit脚本编写勒索软件，伪装为windows更新程序的。还有使用易语言编写勒索软件，通过设置开机密码，或者锁定MBR来勒索的。知名的勒索病毒有PyCrypt勒索、hc勒索、Halloware勒索、Xiaoba勒索等。

另一方面暗网和黑市上存在不少勒索病毒生成器，攻击者输入自己的邮箱和勒索信息，一键生成勒索软件等业务，使不少盗号、DDOS、诈骗等其它犯罪领域的攻击者，也投入到勒索领域，加剧了勒索病毒的泛滥。

6、勒索软件在世界范围内造成的损失逐渐增大

很多公司为了及时恢复数据，平时就会存储一定量的比特币等虚拟货币，以防被勒索时支付赎金。但是更多的情况是，即使支付赎金，对业务也已经造成了非常大的损失。永恒之蓝WannaCry，攻击世界最大的芯片代工厂“台积电”，导致台积电停工三天，损失十几亿元人民币。Petya勒索病毒造成全球最大的集装箱航运公司马士基损失数亿美元、全球最大语音识别公司 Nuance 损失超过9,000万美元，此外受到该勒索病毒攻击的还有乌克兰中央银行、俄罗斯石油巨头 Rosneft、广告企业 WPP、律师事务所 DLA Piper等。以上数据还仅仅是冰山一角，还有很多不知名的公司和个人，由于遭受勒索病毒攻击，造成大量的经济损失，重要资料丢失。

七、勒索病毒防御措施

(一) 个人用户的防御措施

- 1、浏览网页时提高警惕，不下载可疑文件，警惕伪装为浏览器更新或者flash更新的病毒。
- 2、安装杀毒软件，保持监控开启，及时升级病毒库。
- 3、安装防勒索软件，防御未知勒索病毒。
- 4、不打开可疑邮件附件，不点击可疑邮件中的链接。
- 5、及时更新系统补丁，防止受到漏洞攻击。
- 6、备份重要文件，建议采用本地备份+脱机隔离备份+云端备份。

(二) 企业用户的防御措施

1、系统漏洞攻击

防御措施：

- (1) 及时更新系统补丁，防止攻击者通过漏洞入侵系统。
- (2) 安装补丁不方便的企业，可安装网络版安全软件，对局域网中的机器统一打补丁。

(3) 在不影响业务的前提下，将危险性较高的，容易被漏洞利用的端口修改为其它端口号。如139、445端口。如果不使用，可直接关闭高危端口，降低被漏洞攻击的风险。

2、远程访问弱口令攻击

防御措施：

- (1) 使用复杂密码
- (2) 更改远程访问的默认端口号，改为其它端口号
- (3) 禁用系统默认远程访问，使用其它远程管理软件

3、钓鱼邮件攻击

防御措施：

- (1) 安装杀毒软件，保持监控开启，及时更新病毒库
- (2) 如果业务不需要，建议关闭office宏，powershell脚本等
- (3) 开启显示文件扩展名
- (4) 不打开可疑的邮件附件
- (5) 不点击邮件中的可疑链接

4、web服务漏洞和弱口令攻击

防御措施：

- (1) 及时更新web服务器组件，及时安装软件补丁
- (2) web服务不要使用弱口令和默认密码

5、数据库漏洞和弱口令攻击

防御措施：

- (1) 更改数据库软件默认端口
- (2) 限制远程访问数据库
- (3) 数据库管理密码不要使用弱口令
- (4) 及时更新数据库管理软件补丁
- (5) 及时备份数据库

八、瑞星防勒索病毒完整解决方案

通过以上分析，个人用户和企业用户都需要提高安全防范意识，采取必要的防御措施，抵御勒索软件等网络安全威胁。

1、对个人用户推荐安装的软件

(1) 个人版安全软件

瑞星杀毒软件是基于瑞星“云安全”（Cloud Security）计划和“主动防御”技术开发的新一代信息安全产品，该产品采用了全新的软件架构和最新引擎，全面优化病毒特征库，极大提高了运行效率并降低了资源占用。软件新增加了欺诈钓鱼保护、恶意访问保护、注册表监控、内核加固等功能。





图：瑞星杀毒软件

(2) 防勒索软件

瑞星之剑是一款针对未知与已知勒索病毒的防御工具，可进一步阻止勒索病毒破坏文件。采用了智能诱饵、基于机器学习的文件格式判定规则、智能勒索代码行为监测等技术，可有效阻止已知勒索病毒，有效防御未知勒索病毒破坏文件。



图：瑞星之剑

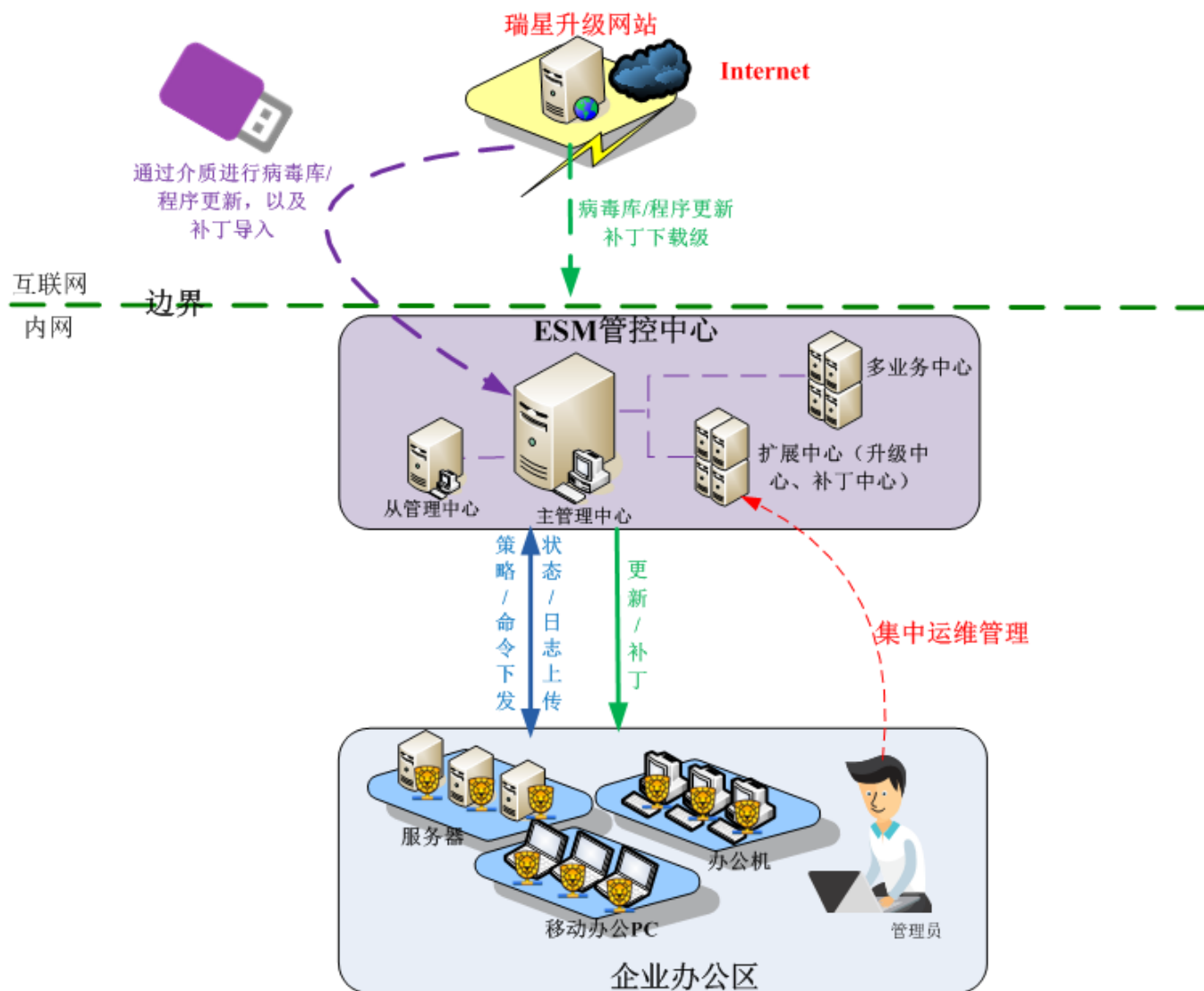
2、对于企业用户推荐部署的软硬件

(1) 各计算机终端设备部署企业版杀毒软件

对于规模较大、设备类型众多、维护工作繁重的企业，推荐使用网络版杀毒软件统一查杀，统一打补丁。

瑞星ESM（瑞星下一代网络版杀毒软件）集病毒防护、网络防护、桌面管理、终端准入、舆情监控于一体，全网络环境适用，可以实现物理机、虚拟机、Windows、Linux一体化管理，为企业用户提供了一整套终端安全解决方案。

该软件实现了多种防护模式自由设定，ATM机、银行自助终端机、地铁闸机、售检票系统、医院挂号机等终端设备按需设置，可对全网终端漏洞进行扫描，自由设定修复策略，终端可同时设定多个补丁中心，多个补丁服务器支持树形级联。



图：瑞星ESM部署示意

(2) 网络入口部署防毒墙

瑞星防毒墙是集病毒扫描、入侵检测和网络监视功能于一身的网络安全产品。它可在网关处对病毒进行初次拦截，配合瑞星病毒库上亿条记录，可将绝大多数病毒彻底剿灭在企业网络之外，帮助企业将病毒威胁降至最低。





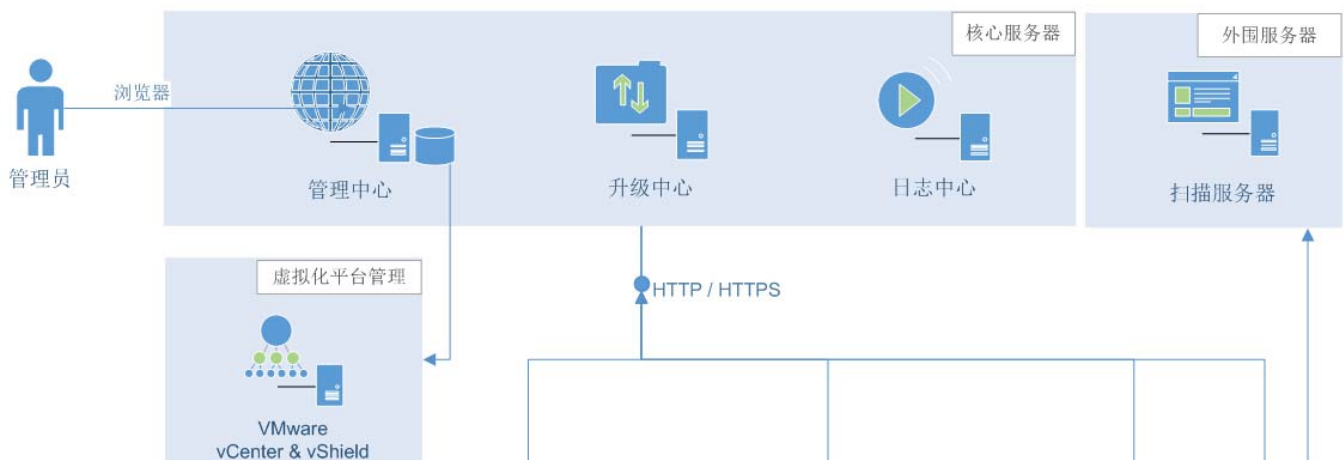
图：瑞星防毒墙界面

(3) 虚拟化设备部署虚拟化专用版安全软件

越来越多的企业，开始大范围应用虚拟化技术，提升物理硬件资源利用率。但随之而来的问题是，传统的安全方案无法适应虚拟环境，存在资源占用过高、资源存储过于集中、设备老化、安全终端防护间隙等问题。因此虚拟化设备部署虚拟化专用版安全软件，就显得尤为重要了。

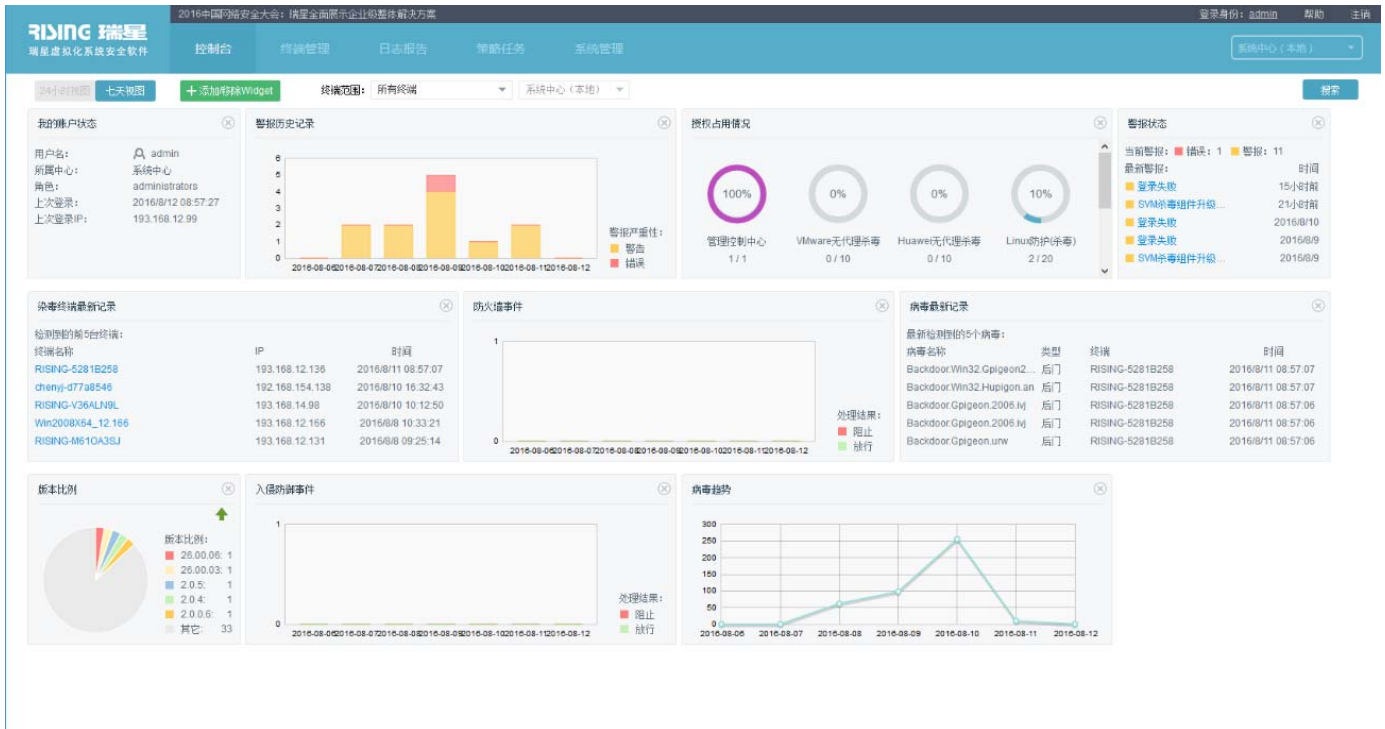
瑞星虚拟化系统安全软件是瑞星公司推出的国内首家企业级云安全防护解决方案，支持对虚拟化环境与非虚拟化环境的统一管控，包括VMware vSphere、VMware NSX、HUAWEI FusionSphere、浪潮InCloud Sphere、Windows系统与Linux系统等，可以有效保障企业内部虚拟系统和实体网络环境不受病毒侵扰。

瑞星虚拟化系统安全软件的完整防护体系由管理中心、升级中心、日志中心、扫描服务器、安全虚拟设备、安全终端Linux杀毒和安全防护终端等子系统组成，各个子系统均包括若干不同的模块，除承担各自的任务外，还与其它子系统通讯，协同工作，共同完成企业内部的安全防护。





图：瑞星虚拟化系统安全软件体系结构



图：瑞星虚拟化系统安全软件界面

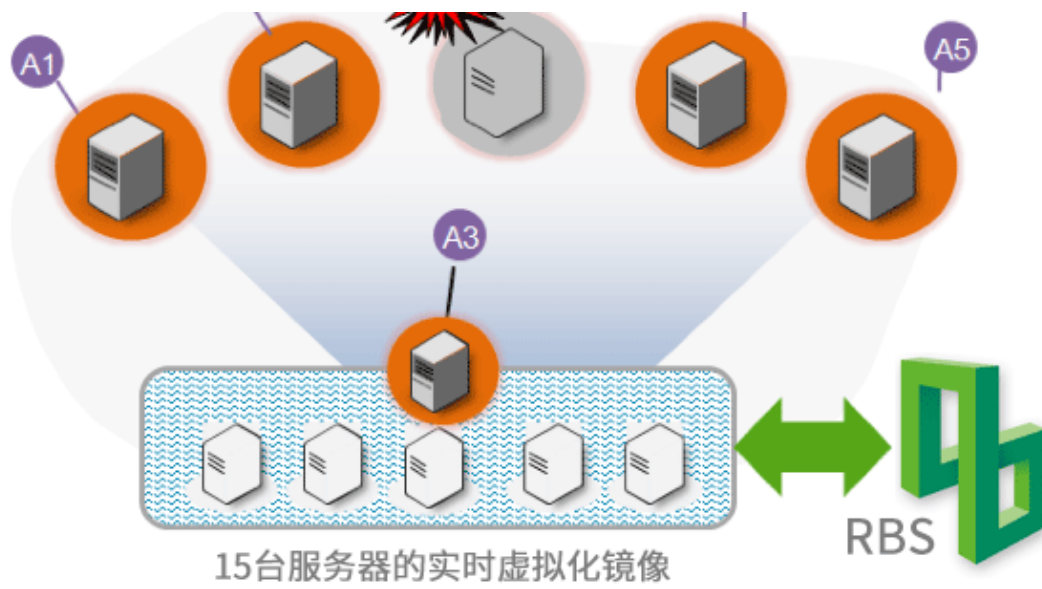
(4) 部署数据备份恢复系统

无论网络防护级别有多高，备份是必不可少的。企业用户由于业务复杂，数据库类型众多，无法手动实时备份，建议使用专业的备份恢复系统实时备份。

瑞星备份恢复系统可作为本地机房针对各种常见服务器故障的应急系统。一台安装了瑞星备份恢复系统的设备可通过和其他备用服务器建立“集中应急平台”实现200-300台X86服务器故障应急系统应急切换，几分钟完全顶替原机使用，实现系统及数据同步。

服务器的一体化备份和应急，可支持windows平台，VMware、Hyper-V等虚拟化平台以及Oracle、SqlServer、MySql、Sybase、达梦等所有数据库。





图：瑞星备份恢复系统