### 按流程操作了4个步骤。没有解决。

发件人: 新文档安全技术支持/系统一部/软件开发中心/ICBC 收件人: 黄玺磊/上海技术部/软件开发中心/ICBC@ICBC

抄送: 占剑/上海技术部/软件开发中心/ICBC@ICBC, Bai Chengxiao <br/>
<u>baicx@cmgos.com</u>>, CRM

Case Email < casemail@cmgos.com >, Li Qi < liqi@cmgos.com >, Liu Wei

<a href="mailto:slixin@cmgos.com">">, Qi Feng <a href="mailto:gifeng@cmgos.com">">, Wang Dan <a href="mailto:wangdan@cmgos.com">">, Wang Wenlei <a href="mailto:wangdl@cmgos.com">">, 鄂礼杰/上海技术部/软件开发中心/ICBC@ICBC, 赵春/系统一部/软件开发中心/ICBC@ICBC, 赵春/系统一部/软件和表述中心/ICBC@ICBC, 赵春/系统一部/软件和表述中心/ICBC@ICBC, 赵春/系统一部/软件和表述中心/ICBC@ICBC, 赵春/系统一部/软件和表述中心/ICBC@ICBC, 赵春/系统一部/文述中心/ICBC@ICBC, WATCAL, WAT

件开发中心/ICBC@ICBC

日期: 2020/08/03 18:48

复: [案例号: CAS-02526-V3W8K2] % [P3]ICBC|神州网站政府版打开图片出现弹框提示 %

初次响应 CMIT:0001141

您好,目前分析该问题可能与 dsp 劫持 explorer 查询注册表有关,请按以下步骤操作验证是否可以解决该问题

1、导入附件的注册表文件

[附件 "PBrush\_.bmp.reg" 被 黄玺磊/上海技术部/软件开发中心/ICBC 删除]

- 2、双击打开图片文件,查看是否还会弹出选择应用程序框,如果是进行一下步
- 3、在选择应用程序框中选择"画图"(注意要勾选上始终使用此应用),点击确定
- 4、在次尝试双击打开图片文件,查看该问题是否解决

发件人: 黄玺磊/上海技术部/软件开发中心/ICBC 收件人: 占剑/上海技术部/软件开发中心/ICBC@ICBC

抄送: Bai Chengxiao < baicx@cmgos.com >, CRM Case Email < casemail@cmgos.com >, Li Qi

cliqi@cmgos.com>, Liu Wei liuwei@cmgos.com>, Li Xin lixin@cmgos.com>, Qi Feng

<<u>qifeng@cmgos.com</u>>, Wang Dan <<u>wangdan@cmgos.com</u>>, Wang Wenlei <<u>wangwl@cmgos.com</u>>, 鄂礼杰/上海技术部/软件开发中心/ICBC@ICBC, 新文档安全技术支持/系统一部/软件开发中心/ICBC@ICBC, 新文档安全技术支持/系统一部/软件开发中心/ICBC@ICBC

日期: 2020/07/27 11:36



# 文档安全防护系统

产品版本: V8.2.2005.2610

中国工商银行

[附件 "dspLog\_2020\_07\_27\_11\_35\_57.zip" 被 新文档安全技术支持/系统一部/软件开发中心/ICBC 删除]

发件人: 占剑/上海技术部/软件开发中心/ICBC

收件人: 新文档安全技术支持/系统一部/软件开发中心/ICBC@ICBC, 黄玺磊/上海技术部/软件开发中

心/ICBC@ICBC

抄送: Bai Chengxiao <<u>baicx@cmgos.com</u>>, CRM Case Email <<u>casemail@cmgos.com</u>>, Li Qi

<a href="mailto:sligi@cmgos.com">"><a href="mailto:liqi@cmgos.com">"><a hr

×

<a href="mailto:</a> <a href="mailto:qifeng@cmgos.com">qifeng@cmgos.com</a>>, Wang Wenlei

<wangwl@cmgos.com>, 鄂礼杰/上海技术部/软件开发中心/SDC@SDC, 唐娜/上海技术部/

软件开发中心/ICBC@ICBC, 赵春/系统一部/软件开发中心/ICBC@ICBC

日期: 2020/07/27 11:28

复: [案例号: CAS-02526-V3W8K2] % [P3]ICBC|神州网站政府版打开图片出现弹框提示 %

初次响应 CMIT:0001141

dsp 的版本为 DSPClientOfficeV8.2.2005.2610,DSPS 客户端日志请黄总按照方法做下回复:"右键 DSPS 客户端托盘-日志采集,然后在弹出的对话框选一个目录,生成的日志会自动保存在该目录,等待弹出日志收集完成提示后将该日志反馈",谢谢

发件人: 新文档安全技术支持/系统一部/软件开发中心/ICBC

收件人: 占剑/上海技术部/软件开发中心/ICBC@ICBC

抄送: Li Qi < liqi@cmgos.com >, Bai Chengxiao < baicx@cmgos.com >, CRM Case Email

<<u>casemail@cmgos.com</u>>, "<u>huangxl@sdc.icbc.com.cn</u>" <<u>huangxl@sdc.icbc.com.cn</u>>, Liu Wei <<u>liuwei@cmgos.com</u>>, Li Xin <<u>liixin@cmgos.com</u>>, Qi Feng <<u>qifeng@cmgos.com</u>>, Wang Dan <<u>wangdan@cmgos.com</u>>, Wang Wenlei <<u>wangwl@cmgos.com</u>>, 赵春/系统一部/软件开发中心/ICBC@ICBC, 鄂礼杰/上海技术部/软件开发中心/SDC@SDC, 唐娜/上海技

术部/软件开发中心/ICBC@ICBC

日期: 2020/07/27 11:23

复: [案例号: CAS-02526-V3W8K2] % [P3|ICBC|神州网站政府版打开图片出现弹框提示 %

初次响应 CMIT:0001141

您好,请问使用的 DSPS 是哪个版本,关于 win10 政府版打开图片问题在 2019 年 7 月版本有优化 过,帮忙确认谢爱 DSPS 版本,如果版本没问题,帮忙获取下 DSPS 客户端日志,右键 DSPS 客户端托盘-日志采集,然后在弹出的对话框选一个目录,生成的日志会自动保存在该目录,等待弹出日志收集完成提示后将该日志反馈即可,谢谢

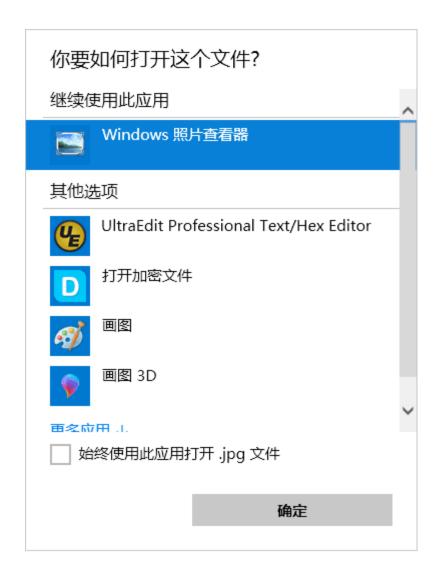
发件人: 占剑/上海技术部/软件开发中心/ICBC

收件人: 新文档安全技术支持/系统一部/软件开发中心/ICBC@ICBC, Li Qi < liqi@cmgos.com > 抄送: Bai Chengxiao < baicx@cmgos.com >, CRM Case Email < casemail@cmgos.com >, "huangxl@sdc.icbc.com.cn" < huangxl@sdc.icbc.com.cn>, Liu Wei < liuwei@cmgos.com >, Li Xin < lixin@cmgos.com >, Qi Feng < gifeng@cmgos.com >, Wang Dan < wangdan@cmgos.com >, Wang Wenlei < wangwl@cmgos.com >, 赵春/系统一部/软件开发中心/ICBC@ICBC, 闫玲/人力资源部/软件开发中心/ICBC@ICBC, 李峰/北京技术部/软件开发中心/ICBC@ICBC, 鄂礼杰/上海技术部/软件开发中心/SDC@SDC, 唐娜/上海技术部/软件开发中心/ICBC@ICBC

日期: 2020/07/27 11:10

## 新文档安全技术支持:

我们发现 dsp 一个问题:我们有位领导的电脑 T490S(win10 政府版),装了 dsp 软件后双击打开图片始终会弹出框如下,勾上了"始终使用此应用打开.jpg 文件"也没有效果,卸载 dsp 后双击图片就会生效不再弹框,还请 dsp 项目组协同神州网信公司李琦工程师一起分析解决领导的这个问题,谢谢。



发件人: Li Qi < liqi@cmgos.com>

收件人: "zhanjian@sdc.icbc.com.cn" <zhanjian@sdc.icbc.com.cn>

抄送: Bai Chengxiao <baicx@cmgos.com>, CRM Case Email <casemail@cmgos.com>,

"huangxl@sdc.icbc.com.cn" < huangxl@sdc.icbc.com.cn>, Liu Wei < liuwei@cmgos.com>,

Li Xin < <a href="mailto:lixin@cmgos.com">! Qi Feng < <a href="mailto:qifeng@cmgos.com">qifeng@cmgos.com</a>>, Wang Dan

<wangdan@cmgos.com>, Wang Wenlei <wangwl@cmgos.com>

日期: 2020/07/27 09:41

例号: CAS-02526-V3W8K2] % |P3|ICBC|神州网站政府版打开图片出现弹框提示 % 初次响

应 CMIT:0001141

## 占先生, 您好:

感谢您的回复。您可以先卸载 DSP 软件,然后看一下问题是否复现,如仍有问题,还是建议退域后再次观察一下,这对于我们进行问题的 narrow down 排查很有帮助,谢谢。

李琦 Li Qi

神州网信技术有限公司

C&M Information Technologies Co., Ltd.

服务电话: 4008180055

电子邮箱 Email: <u>liqi@cmgos.com</u>



发件人: zhanjian@sdc.icbc.com.cn <zhanjian@sdc.icbc.com.cn>

**发送时间:** 2020 年 7 月 24 日 20:49 **收件人:** Li Qi liqi@cmgos.com>

抄送: Bai Chengxiao < <a href="mailto:baicx@cmgos.com">baicx@cmgos.com</a>; CRM Case Email < <a href="mailto:casemail@cmgos.com">casemail@cmgos.com</a>; Qi huangxl@sdc.icbc.com.cn; Liu Wei < <a href="mailto:liuwei@cmgos.com">liuwei@cmgos.com</a>; Li Xin < <a href="mailto:lixin@cmgos.com">lixin@cmgos.com</a>; Qi Feng < <a href="mailto:qifeng@cmgos.com">qifeng@cmgos.com</a>; Wang Dan < <a href="mailto:wangdan@cmgos.com">wangdan@cmgos.com</a>; Wang Wenlei < <a href="wangdan@cmgos.com">wangdan@cmgos.com</a>; Wang Wenlei

让黄总的电脑退域测试太麻烦了吧?你如果觉得是 dsp 软件的问题,我有权限卸载黄总电脑的 dsp 软件

发件 Li Qi < liqi@cmgos.com>

人:

收件 "zhanjian@sdc.icbc.com.cn" <zhanjian@sdc.icbc.com.cn>

抄送: Bai Chengxiao <<u>baicx@cmgos.com</u>>, CRM Case Email <<u>casemail@cmgos.com</u>>, "Liu Wei" <<u>liuwei@cmgos.com</u>>, Li Xin <<u>lixin@cmgos.com</u>>, Qi Feng <<u>qifeng@cmgos.com</u>>, Wang Dan <<u>wangdan@cmgos.com</u>>, Wang Wenlei <<u>wangwl@cmgos.com</u>>, "<u>huangxl@sdc.icbc.com.cn</u>" <huangxl@sdc.icbc.com.cn>

日期: 2020/07/24 17:11

人:

占先生, 您好:

感谢您的反馈,由于电话未联系到您,特发送此邮件说明一下目前的问题进展。

之前和黄先生做过沟通,目前该问题只出现在黄先生的电脑上,且从之前收到的日志分析,黄先生的电脑有关默认应用及文件关联的设置是正确的,因此不排除因工行的定制软件或域策略的阻止导致每次操作都会启动 openwith 的进程出现弹框。并且没办法在我们的环境中进行复现。

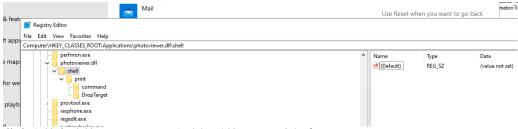
P2V 的收集可以包含用户电脑上的所有设置内容,以避免重复收集日志给客户带来的困扰以及环境对测试的限制。

对于该问题的排查,基于用户数据安全考虑,目前无法收取 P2V,则可能后续仍然需要多次的不同日志收集,才能找到最终原因。

从之前收集的日志中,可以看到操作系统在查找 PhotoViewer 时的打开位置是不对的,进而导致无法使用既有设置的 PhotoViewer 进行打开(由于 CMGE 默认不包含 photoviewer.exe。从官方资料上看,这可能是由于 CMGE 的安装方式并非全新安装导致之前操作系统的部分组件遗留。

https://support.microsoft.com/en-sg/help/4027135/windows-10-photo-viewer),但由于黄先生使用其他的打开方式也有此问题,所以需要以其他的打开方式来进行问题分析。如下图:

默认的 command key 位于 print 键值下,并不位于 shell 下



黄先生的电脑的 explorer.exe 在访问时的 query 路径有误

| Page    |                  |              |       |        |             |  |                  |
|--|------------------|--------------|-------|--------|-------------|--|------------------|
| 18.0   2.5   18.0   2.5   18.0   2.5   18.0   2.5   18.0   2.5   2.5   18.0   2.5   18.0   2.5   18.0   2.5   18.0   2.5   2.5   18.0   2.5   2.5   18.0   2.5   2.5   18.0   2.5   2.5   18.0   2.5   2.5   18.0   2.5   2.5   18.0   2.5   2.5   18.0   2.5   2.5   18.0   2.5   2.5   2.5   18.0   2.5  | Time of Day      | Process Name |       |        |             |  |                  |
| 18.0    | 16:16:25.6945481 | Explorer.EXE |       |        |             |  |                  |
| 16.10.5.0.00.733   register EXT   10.00.2   20.00   filesy/pursify   MCCRA/Special complex plant and proper plant and prope | 16:16:25.6945589 | Explorer.EXE |       |        |             |  |                  |
| 16.12.5   16.1 |                  |              |       |        |             |  |                  |
| 16   15   16   16   16   16   16   16  | 10:10:20.0940733 | Explorer EVE |       |        |             |  |                  |
| 16.10.25   Michael   Supher EXT   1902   220   Englanding of the process of the | 16:16:25.6945041 | Explorer EYE |       |        |             |  |                  |
| 16.15.2   16.1 |                  |              |       |        |             |  |                  |
| 18.12.5.6.6.6.6.5.5.5.5.5.5.5.5.5.5.5.5.5.5.   |                  |              |       |        |             |  |                  |
| 16   12   16   12   16   12   16   12   16   12   16   16  |                  |              |       |        |             |  |                  |
| 18.10.2.6.2.6.2.2.2.2.2.2.2.2.2.2.2.2.2.2.2.   |                  |              |       |        |             |  |                  |
| 16.10.2   16.1 | 16:16:25.6946504 | Explorer.EXE | 10252 | 2236 📆 | RegQueryKey | HKCR\Applications\photoviewer.dll\shell\open                                   | BUFFER TOO SMALL |
| 10   12   12   12   12   12   12   12  |                  |              |       |        |             |  |                  |
| 16   16   26   1997   19   19   19   19   19   19  |                  |              |       | 2236 🏥 | RegOpenKey  |  |                  |
| 16   15   26   17   10   15   15   15   15   15   15   15  |                  |              |       |        |             |  |                  |
| 16   12   16   17   17   |                  |              |       |        |             |  |                  |
| 16   16   26   66   77.50  |                  |              |       |        |             |  |                  |
| 16   12.5   26   17.4   16   19.5   16   19.5   1 |                  |              |       |        |             |  |                  |
| 16   15   26   60   75   26   20   20   20   20   40   40   40   40  |                  |              |       |        |             |  |                  |
| 16   12   26   04   74   26   16   25   26   16   16   25   26   16   26   26   27   26   16   26   26   27   28   28   28   28   28   28   28   |                  |              |       |        |             |  |                  |
| 16   16   26   64   77   1   16   16   26   64   77   16   16   16   26   64   78   16   16   26   64   78   16   16   26   64   78   16   16   26   64   78   16   16   26   64   78   16   16   26   26   26   16   26   26  |                  |              |       |        |             |  |                  |
| 16.16.25 6647913   Eppiner EXE   105/25   2278   Enginer EXE   105/25   2278   Expense EXE   1 |                  |              |       |        |             |  |                  |
| 16   16   26   26   26   26   26   27   27   2   |                  |              |       |        |             |  |                  |
| 16   162   266   2003   10   10   10   2005   2005   10   2005  |                  |              |       |        |             |  |                  |
| 16 162 6665526   Poplome EXE   10252   2256   Choser File   Chivery and Project Monary Project |                  |              | 10252 |        |             | C:\Windows\System32\rundli32.exe   | SUCCESS          |
| 16 18 2 5 605245   Episore EXE   1052   223  |                  |              | 10252 | 2236 📑 | CloseFile   | C:\Windows\System32\rundli32.exe   | SUCCESS          |
| 16 18 26 98092534   Epipore EXE   10525   2238   Grego-Close/Few   HCCL/Spicinary/Lasses   SUCCESS   10 18 26 9809264   Epipore EXE   10 1025   2238   Epipore CRE   10 10 10 10 10 10 10 10 10 10 10 10 10   |                  |              |       |        |             |  |                  |
| 16 10.2 5.0652076   Epigene EXE   10252   2236   Engloyamyley   HCCUSChawarClasses   HCCUSC |                  |              |       |        |             |  |                  |
| 16 16 25 6902004   Episiene EXE  |                  |              |       |        |             |  |                  |
| 16 16.2 5690398   Epigner EXE   1052   2238   Employme/ley   HCUJSoftware/Classes   SUCCES   16 16.2 5690310   Epigner EXE   1052   2238   Employme/ley   HCUJSoftware/Classes   SUCCES   16 16.2 5690310   Epigner EXE   1052   2238   Employme/ley   HCUJSoftware/Classes   16 16.2 5690310   Epigner EXE   1052   2238   Employme/ley   HCUJSoftware/Classes   16 16.2 5690310   Epigner EXE   1052   2238   Employme/ley   HCUJSoftware/Classes   16 16.2 5690310   Epigner EXE   1052   2238   Employme/ley   HCUJSoftware/Classes   16 16.2 5690310   Epigner EXE   1052   2238   Employme/ley   HCUJSoftware/Classes   16 16.2 5690310   Epigner EXE   1052   2238   Employme/ley   HCUJSoftware/Classes   16 16.2 5690310   Epigner EXE   1052   2238   Employme/ley   HCCRApplications/photo/were dl   16 16.2 5690310   Epigner EXE   1052   2238   Employme/ley   HCCRApplications/photo/were dl   16 16.2 5690310   Epigner EXE   1052   2238   Employme/ley   HCCRApplications/photo/were dl   16 16.2 5690310   Epigner EXE   1052   2238   Employme/ley   HCCRApplications/photo/were dl   16 16.2 5690310   Epigner EXE   1052   2238   Employme/ley   HCCRApplications/photo/were dl   16 16.2 5690310   Epigner EXE   1052   2238   Employme/ley   HCCRApplications/photo/were dl   16 16.2 5690310   Epigner EXE   1052   2238   Employme/ley   HCCRApplications/photo/were dl   16 16.2 5690310   Epigner EXE   1052   2238   Employme/ley   HCCRApplications/photo/were dl   16 16.2 5690310   Epigner EXE   1052   2238   Employme/ley   HCCRApplications/photo/were dl   16 16.2 5690310   Epigner EXE   1052   2238   Employme/ley   HCCRApplications/photo/were dl   16 16.2 5690310   Epigner EXE   1052   2238   Employme/ley   HCCRApplications/photo/were dl   16 16.2 5690310   Epigner EXE   1052   2238   Employme/ley   HCCRApplications/photo/were dl   16 16.2 5690310   Epigner EXE   1052   2238   Employme/ley   HCCRApplications/photo/were dl   16 16.2 5690310   Epigner EXE   1052   2238   Employme/ley   HCCRApplications/photo/were dl   16 16.2 5690310   Epigner EXE   1052   |                  |              |       |        |             |  |                  |
| 16 10-25 6953103   Epigner EXE   10252   2238 gf. (epigner/leg)   HKUUSoftware/Classes   HKUUSoftware/Classes   SUCCESS  |                  |              |       |        |             |  |                  |
| 16   16 2 5 69531   16   |                  |              |       |        |             |  |                  |
| 16   16   25   6853   16   |                  |              |       |        |             |  |                  |
| 16   16   25   26   25   25   25   25   25   2   |                  |              |       |        |             |  |                  |
| 16   16   25   665  365    Capitore EXE   10252   225   Regiousyfey   HKCRN/pglicalions/Polor/wert dil   SUCCESS   16   16   25   665  365  365  365  365  365  365  3   |                  |              |       |        |             |  |                  |
| 16   16 2-6 6655409   Explorer EXE   10252   223   |                  |              |       |        |             |  |                  |
| 16   16   25   605  350     Epptore EXE   1025   225   Eng/pomfky   HKCRV.pplications/photowiewr.dll   MKFRV.pplications/photowiewr.dll   MKFRV.pplication |                  |              |       |        |             |  |                  |
| 16   16   25   6653/26   Captorer EXE   1025   223   RegQueryFory   HKCR/Applications/photowerer dll   BUFFERT TOO SMALL   16   16   25   6653/76   Captorer EXE   1025   223   RegQueryFory   HKCR/Applications/photowerer dll   SUCCESS   16   16   25   6653/76   Captorer EXE   1025   223   RegQueryFory   HKCR/Applications/photowerer dll   16   16   25   6653/76   Captorer EXE   1025   223   RegQueryFory   HKCR/Applications/photowerer dll   16   16   25   6653/76   Captorer EXE   1025   223   RegQueryFory   HKCR/Applications/photowerer dll   16   16   25   6653/76   Captorer EXE   1025   223   RegQueryFory   HKCR/Applications/photowerer dll   16   16   25   6653/76   Captorer EXE   1025   223   RegQueryFory   HKCR/Applications/photowerer dll   16   16   25   6653/76   Captorer EXE   1025   223   RegQueryFory   HKCR/Applications/photowerer dll   16   16   25   6653/76   Captorer EXE   1025   223   RegQueryFory   HKCL/Software/Classes   16   16   25   6653/76   Captorer EXE   1025   223   RegQueryFory   HKCL/Software/Classes   16   16   25   6653/76   Captorer EXE   1025   223   RegQueryFory   HKCL/Software/Classes   16   16   25   6653/76   Captorer EXE   1025   223   RegQueryFory   HKCL/Software/Classes   HKCL/Software/Classes   HKCL/Software/Classes   HKCL/Software/Classes   HKCL/Software/Classes   Laptorer EXE   1025   223   RegQueryFory   HKCL/Software/Classes   HKCL/Software/Classes   Laptorer EXE   1025   223   RegQueryFory   HKCL/Software/Classes   Laptorer EXE   1025   223   RegQueryFory   HKCR/Applications/photower dll   HKCR/Applications/photower dll |                  |              |       |        |             |  |                  |
| 16   16   25   655  565  375   1   1   1   1   1   1   1   1   1   |                  |              | 10252 | 2236 🚮 | RegOpenKey  | HKCU\Software\Classes\Applications\photoviewer.dll                             | NAME NOT FOUND   |
| 16   16   25   65   65   35   16   16   25   225   25   25   25   25   25  |                  |              | 10252 | 2236 🏥 | RegQueryKey |  | BUFFER TOO SMALL |
| 16-18-25-665-30-36   Eppiore EXE   10252   2236   RegCountyley   HICKPA/ppicalions/pholowiewr dll   HICKPA/ppicalions/p |                  |              |       |        |             |  |                  |
| 16   16.25 695403   Explorer EXE   1025  |                  |              |       |        |             |  |                  |
| 16   16.25 695410   Eppirer EXE   1025   |                  |              |       |        |             |  |                  |
| 16 10.25 605476   Explore EXE   10252   2238   RegQueryley   HCUUSOftwareClasses   BUFFER TO SMALL   16 10.25 6054725   Explore EXE   10252   2238   RegQueryley   HCUUSOftwareClasses   BUFFER TO SMALL   16 10.25 6054725   Explore EXE   10252   2238   RegQueryley   HCUUSOftwareClasses   Applications/PhotoViewer dil  |                  |              |       |        |             |  |                  |
| 16 16.2 6664529  |                  |              |       |        |             |  |                  |
| 16   16 25 695429   Explorer EXE   10252   223   |                  |              |       |        |             |  |                  |
| 16   16   25   6654  32   Captioner EXE   1025   225   6   Reg/openKey   HKCR/Replications/Photo/wew dll   SUCCESS     16   16   25   6654  50   Captioner EXE   1025   225   6   Reg/openKey   HKCR/Replications/Photo/wew dll   SUCCESS     16   16   25   6654  50   Captioner EXE   1025   225   6   Reg/openKey   HKCR/Replications/Photo/wew dll   SUCCESS     16   16   25   6654  50   Captioner EXE   1025   225   6   Reg/openKey   HKCR/Replications/Photo/wew dll   SUCCESS     16   16   25   6654  50   Captioner EXE   1025   225   6   Reg/openKey   HKCR/Replications/Photo/wew dll   SUCCESS     16   16   25   6654  50   Captioner EXE   1025   225   6   Reg/openKey   HKCR/Replications/Photo/wew dll   SUCCESS     16   16   25   6654  50   Captioner EXE   1025   225   Reg/openKey   HKCR/Replications/Photo/wew dll   SUCCESS     16   16   25   6654  50   Captioner EXE   1025   225   Reg/openKey   HKCR/Replications/Photo/wew dll   SUCCESS     16   16   25   6654  50   Captioner EXE   1025   225   Reg/openKey   HKCR/Replications/Photo/wew dll   SUCCESS     16   16   25   6654  50   Captioner EXE   1025   225   Reg/openKey   HKCR/Replications/Photo/wew dll   SUCCESS     16   16   25   6654  50   Captioner EXE   1025   225   Reg/openKey   HKCR/Replications/Photo/wew dll   SUCCESS     16   16   25   6655  50   Captioner EXE   1025   225   Reg/openKey   HKCR/Replications/Photo/wew dll   SUCCESS     16   16   25   6655  50   Captioner EXE   1025   225   Reg/openKey   HKCR/Software/Macrosoft/Works/Shell/MuCarha   SUCCESS     16   16   25   6655  50   Captioner EXE   1025   225   Reg/openKey   HKCR/Software/Macrosoft/Works/Shell/MuCarha   SUCCESS     16   16   25   6655  50   Captioner EXE   1025   225   Reg/openKey   HKCR/Software/Macrosoft/Works/Shell/MuCarha   SUCCESS     16   16   25   6655  50   Captioner EXE   1025   225   Reg/openKey   HKCR/Software/Macrosoft/Works/Shell/MuCarha   SUCCESS     16   16   25   6655  50   Captioner EXE   1025   225   Reg/openKey   HKCR/Software/Macrosoft/Works/Shell/MuCarha   SUCCESS     16    |                  |              |       |        |             |  |                  |
| 16   16   25   65   65   45   16   16   25   225   25   6   RegQueryKey   HKCRVApplications/Photo/werer dll   SUCCESS     16   16   25   65   65   25   25   25   6   RegQueryKey   HKCRVApplications/photo/werer dll   SUCCESS     16   16   25   65   65   25   25   25   6   RegQueryKey   HKCRVApplications/photo/werer dll   SUCCESS     16   16   25   65   65   25   25   25   6   RegQueryKey   HKCRVApplications/photo/werer dll   MAME NOT FOUND     16   16   25   65   65   25   25   25   6   RegQueryKey   HKCRVApplications/photo/werer dll   MAME NOT FOUND     16   16   25   65   65   25   25   25   6   RegQueryKey   HKCRVApplications/photo/werer dll   SUCCESS     16   16   25   65   65   25   25   6   RegQueryKey   HKCRVApplications/photo/werer dll   SUCCESS     16   16   25   65   65   25   25   6   RegQueryKey   HKCRVApplications/photo/werer dll   SUCCESS     16   16   25   65   65   25   25   6   RegQueryKey   HKCRVApplications/photo/werer dll   SUCCESS     16   16   25   65   65   25   25   6   RegQueryKey   HKCRVApplications/photo/werer dll   SUCCESS     16   16   25   65   65   25   25   6   RegQueryKey   HKCRVApplications/photo/werer dll   SUCCESS     16   16   25   65   65   25   25   6   RegQueryKey   HKCRVApplications/photo/werer dll   SUCCESS     16   16   25   65   65   25   25   6   RegQueryKey   HKCRVApplications/photo/werer dll   SUCCESS     16   16   25   65   65   25   25   6   RegQueryKey   HKCLVSoftware/Successor Local Statings/Software/Bucrost/Windows/Stell/Bull.caha   SUCCESS     16   16   25   65   65   25   25   6   RegQueryKey   HKCLVSoftware/Successor Local Statings/Software/Bucrost/Windows/Stell/Bull.Caha   SUCCESS     16   16   25   65   65   25   25   6   RegQueryKey   HKCLVSoftware/Successor Local Statings/Software/Bucrost/Windows/Stell/Bull.Caha   SUCCESS     16   16   25   65   65   65   65   65   65   6   | 16:16:25 6954328 | Explorer EXE |       |        |             |  |                  |
| 16   16   25   6954503   Explorer EXE   10252   2236   RegQuiseryfory   HKCRV/pplicalions/photoviewer dll   SUCCESS     16   16   25   6954505   Explorer EXE   10252   2236   RegQuiseryfory   HKCRV/pplicalions/photoviewer dll   SUCCESS     16   16   25   6954505   Explorer EXE   10252   2236   RegQuiseryfory   HKCRV/pplicalions/photoviewer dll   SUCCESS     16   16   25   6954578   Explorer EXE   10252   2236   RegQuiseryfory   HKCRV/pplicalions/photoviewer dll   SUCCESS     16   16   25   6954578   Explorer EXE   10252   2236   RegQuiseryfory   HKCRV/pplicalions/photoviewer dll   SUCCESS     16   16   25   6954578   Explorer EXE   10252   2236   RegQuiseryfory   HKCRV/pplicalions/photoviewer dll   SUCCESS     16   16   25   695578   Explorer EXE   10252   2236   RegQuiseryfory   HKCRV/pplicalions/photoviewer dll   Reglection Company   HKCRV/pplicalions/photoviewer dll   RKCRV/pplicalions/photoviewer dll   RKCRV/pp |                  |              |       |        |             |  |                  |
| 16   16   26   566   566   16   16   16   16   16  |                  |              |       |        |             |  |                  |
| 16.1 to 25.0654762   Explorer EXE   10252   2236   RegQueryNey   HICKURSpiriture/Liciasses/Applications/sphotowner dil   |                  |              |       |        |             |  |                  |
| 16.162-5.065478   Explorer EXE   10252   2236   Reg/Journylab   HCRCRApplications/photowered III   HCRCRAPPlications/ph |                  |              | 10252 | 2236 📆 | RegOpenKey  | HKCU\Software\Classes\Applications\photoviewer.dll                             |                  |
| 16   16 25 695468   Explorer EXE   1025   225  |                  |              |       |        |             |  |                  |
| 16 16 26 6964976         Epptore EXE         10252         2238 & RegClosekey         HCRUSOfinaer/Classed/Load Settings/Software/Marcoset/Ill/Indicate/Softwa  |                  |              |       |        |             |  |                  |
| 16   16.25 695500     Epidem EXE   1025   2236   RegQuaryNey   HKCUSoftware/Microselt/Local/Strings/ |                  |              |       |        |             |  |                  |
| 16   16.2 56 955   26   popiner EXE   1025   2236   RegQuaryNey   HIXCU Software/Classes Local Settings/Software/MicrosoftWindows/Shelt-MulCarbe   BUFER TOO SMALL   |                  |              |       |        |             |  |                  |
| 16 16.25 695518   Epiprer EXE  |                  |              |       |        |             |  |                  |
| 16 16.25 6955299   Epipper EXE   |                  |              |       |        |             |  |                  |
| 16 1-12 6 695596   Epiprer EXE   1052   2238   RegQueyNey   HICUSOftware/Classes/Load Settings/Software/Microsoft/Windows/ShelfMulCache   SUCESS   16 1-12 5 6955596   Epiprer EXE   1052   2238   RegQueyNey   HICUSOftware/Classes/Load Settings/Software/Microsoft/Windows/ShelfMulCache   SUCESS   16 1-12 5 6955797   Epiprer EXE   1052   2238   RegQueyNey   HICUSOftware/Classes/Load Settings/Software/Microsoft/Windows/ShelfMulCache   SUCESS   16 1-12 5 6955797   Epiprer EXE   1052   2238   RegQueyNey   HICUSOftware/Classes/Load Settings/Software/Microsoft/Windows/ShelfMulCache   SUCESS   16 1-12 5 695579   Epiprer EXE   1052   2238   RegQueyNey   HICUSOftware/Classes/Load Settings/Software/Microsoft/Windows/ShelfMulCache   SUCESS   16 1-12 5 695579   Epiprer EXE   1052   2238   RegQueyNey   HICUSOftware/Classes/Load Settings/Software/Microsoft/Windows/ShelfMulCache   SUCESS   16 1-12 5 695579   Epiprer EXE   1052   2238   RegQueyNey   HICUSOftware/Classes/Load Settings/Software/Microsoft/Windows/ShelfMulCache   SUCESS   16 1-12 5 695579   Epiprer EXE   1052   2238   RegQueyNey   HICUSOftware/Classes/Load Settings/Software/Microsoft/Windows/ShelfMulCache   SUCESS   16 1-12 5 695579   Epiprer EXE   1052   2238   RegQueyNey   HICUSOftware/Classes/Load Settings/Software/Microsoft/Windows/ShelfMulCache   SUCESS   16 1-12 5 695579   Epiprer EXE   1052   2238   RegQueyNey   HICUSOftware/Classes/Load Settings/Software/Microsoft/Windows/ShelfMulCache   SUCESS   16 1-12 5 695579   Epiprer EXE   1052   2238   RegQueyNey   HICUSOftware/Classes/Load Settings/Software/Microsoft/Windows/ShelfMulCache   SUCESS   16 1-12 5 695579   RegQueyNey   HICUSOftware/Classes/Load Settings/ShelfMulCache   SUCESS   |                  |              |       |        |             |  |                  |
| 16 18.25 6955242   Explore EXE   10252   2236   Reg0.umyley   HICUSOftware/Classes (Local Settings/Software/MicrosoftWindows/ShelfWiLd:ache (C-Vrogram Files/Windows Photo Vriew. SUGCESS   16 18.25 6955721   Explore EXE   10252   2236   Reg0.umyley   HICUSOftware/Classes (Local Settings/Software/MicrosoftWindows/ShelfWiLd:ache (C-Vrogram Files/Windows Photo Vriew. SUGCESS   16 18.25 6955752   Explore EXE   10252   2236   Reg0.umyley   HICUSOftware/Classes (Local Settings/Software/MicrosoftWindows/ShelfWiLd:ache (C-Vrogram Files/Windows Photo Vriew. SUGCESS   16 18.25 6955759   Explore EXE   10252   2236   Reg0.umyley   HICUSOftware/Classes (Local Settings/Software/MicrosoftWindows/ShelfWiLd:ache (C-Vrogram Files/Windows)   16 18.25 6955759   Explore EXE   10252   2236   Reg0.umyley   HICUSOftware/Classes (Local Settings/Software/MicrosoftWindows/ShelfWiLd:ache (C-Vrogram Files/Windows)   16 18.25 6955759   Explore EXE   10252   2236   Reg0.umyley   HICUSOftware/Classes (Local Settings/Software/MicrosoftWindows/ShelfWiLd:ache (C-Vrogram Files/Windows)   16 18.25 6955759   Explore EXE   10252   2236   Reg0.umyley   HICUSOftware/Classes (Local Settings/Software/MicrosoftWindows/ShelfWiLd:ache (C-Vrogram Files/Windows/ShelfWiLd:ache (C-Vrogram Files/Windows/ShelfWild:a |                  |              |       |        |             |  |                  |
| 16.16.25.6055526         Explorer EXE         10252         2236 gft RegCuserVelue         HKCU/Software/Classes/Local Settings/Software/MicrosoftWindows/ShellMM2cache/C-Vprogram Files/Windows/ShellMM2cache         SUCCESS           16.16.25.6055276         Epilorer EXE         10252         2236 gft RegCuserVely         HKCU/Software/Classes/Local Settings/Software/MicrosoftWindows/ShellMM2cache         SUCCESS           16.16.25.6055276         Epilorer EXE         10252         2236 gft RegCuserVely         HKCU/Software/Classes/Local Settings/Software/MicrosoftWindows/ShellMM2cache         SUCCESS           16.16.25.6055290         Epilorer EXE         10252         2236 gft RegCuserVely         HKCU/Software/Classes/Local Settings/Software/MicrosoftWindows/ShellMM2cache         BUFFER TOO SMALL           16.16.25.6055290         Epilorer EXE         10252         2236 gft RegCuserVely         HKCU/Software/Classes/Local Settings/Software/MicrosoftWindows/ShellMM2cache         BUFFER TOO SMALL   |                  |              |       |        |             |  |                  |
| 16 16.25 9555721   Expirer EXE   |                  |              |       |        |             |  |                  |
| 16 16 25 605579s         Explainer EXE         10252         223 at RegQueryKey         HKCUSoftware/Classesi Local Settings/Software/MicrosoftWindows/ShelfMuCache         SUCCESS           16 16 26 66555091         Explainer EXE         10252         223 at RegQueryKey         HKCUSoftware/Classesi Local Settings/Software/MicrosoftWindows/ShelfMuCache         BUFFER TOO SMALL           16 16 25 6055901         Explainer EXE         10252         223 at RegQueryKey         HKCUSoftware/Classesi Local Settings/Software/MicrosoftWindows/ShelfMuCache         SUCCESS  |                  |              |       |        |             |  |                  |
| 16 16.25 995595  | 16:16:25.6955788 | Explorer.EXE |       |        |             | HKCU/Software/Classes/Local Settings/Software/Microsoft/Windows/Shell/Mu/Cache |                  |
| 16:16:25:6955901 Explorer EXE 10252 2236 KE ReqQueryKey HKCUISoftware/Classes/Local Settings/Software/Microsoft/Windows/Shell/MuiCache SUCCESS   | 16:16:25.6955850 | Explorer.EXE |       |        |             |  |                  |
| 10 10 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0  | 16:16:25.6955901 | Explorer.EXE |       | 2236 🏥 | RegQueryKey | HKCU/Software/Classes/Local Settings/Software/Microsoft/Windows/Shell/MuiCache |                  |
|  | 10 10 05 0055000 | r            | 10050 | nnnn 🚅 | Pn0         | I MALIA A  | CHAREC           |

综上分析,目前我们的问题主要集中在 openwith 为何被调用,这有如下两点可能:

- 1, PhotoViewer 无法默认打开,是由于未找到正确注册表键值(这一点与 PhotoViewer 的安装方式有关),还是由于权限或第三方应用等问题被阻止访问?
- 2, 如果因为权限或第三方应用的原因, 具体是什么?

接下来,优先排查第二点,想询问您一下,是否可以做如下的测试用于问题的 narrow down 分析:

- 1. 将用户电脑退域。
- 2, 卸载用户的 DSP 软件, 并确保不存在 C:\Program Files (x86)\DSPClient\CEMS\EDSM\MedAdapter64.dll 这个文件。
- 3, 尝试使用本地账户登录后, 双击 jpg 图片, 看问题是否复现。
- 4, 如问题复现,请将默认打开方式更改为 mspaint 进行 procmon 的日志收集

上述操作仅供问题分析使用,需要您使用域管理员账号进行协助操作。谢谢

李琦 Li Qi 神州网信技术有限公司 C&M Information Technologies Co., Ltd. 服务电话: 4008180055

电子邮箱 Email: liqi@cmgos.com



发件人: zhanjian@sdc.icbc.com.cn <zhanjian@sdc.icbc.com.cn>

发送时间: 2020 年 7 月 23 日 17:19 收件人: Li Qi liqi@cmgos.com>

李琦,您好!磁盘映像文件带有黄总的个人信息数据,不能发给你们分析,请知悉。

```
发 黄玺磊/上海技术部/软件开发中心/ICBC
件
人:
收 Li Qi <<u>liqi@cmgos.com</u>>
```

Bai Chengxiao <<u>baicx@cmgos.com</u>>, CRM Case Email <<u>casemail@cmgos.com</u>>, "Liu Wei" <<u>liuwei@cmgos.com</u>>, Li 送: Xin <<u>lixin@cmgos.com</u>>, Qi Feng <<u>qifeng@cmgos.com</u>>, Wang Dan <<u>wangdan@cmgos.com</u>>, Wang Wenlei <<u>vangdul@cmgos.com</u>>, "<u>zhanjian@sdc.icbc.com.cn</u>" <<u>zhanjian@sdc.icbc.com.cn</u>>

日 2020/07/23 16:36 期:

人:

题: V3W8K2]% |P3|ICBC|神州网站政府版打开图片出现弹框提示% 初次响应 CMIT:0001141

占剑有渠道能访问这个 sftp? 我们这边都是内网隔离的如果有的话,给我个地址,我先给占剑你吧

```
发Li Qi <a href="mailto:liquemgos.com">liquemgos.com</a>
作人:
收 "huangxl@sdc.icbc.com.cn" <huangxl@sdc.icbc.com.cn>, "zhanjian@sdc.icbc.com.cn" <zhanjian@sdc.icbc.com.cn>
件
人:
抄 Bai Chengxiao <a href="mailto:baicx@cmgos.com">baicx@cmgos.com</a>>, CRM Case Email <a href="mailto:casemail@cmgos.com">casemail@cmgos.com</a>>, "Liu Wei" <a href="mailto:liuwei@cmgos.com">liuwei@cmgos.com</a>>, Li 送: Xin <a href="mailto:lixin@cmgos.com">lixin@cmgos.com</a>>, Qi Feng <a href="mailto:qifeng@cmgos.com">qifeng@cmgos.com</a>>, Wang Dan <a href="mailto:wangwl@cmgos.com">wangdan@cmgos.com</a>>, Wang Wenlei <a href="mailto:wangwl@cmgos.com">wangwl@cmgos.com</a>>, Wang Wenlei
```

目 2020/07/23 16:27

期:

题: V3W8K2] % [P3|ICBC|神州网站政府版打开图片出现弹框提示 % 初次响应 CMIT:0001141

# 黄先生, 您好:

感谢您的回复。请问上周五和您提到的方法是否有效,您可以参照附件内容试一下。

有关 VHDX 文件请占先生帮忙上传至 sftp, 具体方法如下:

为了更安全、快速地传输数据,您可以在 Filezilla 上使用以下账户信息登入神州网信网站。

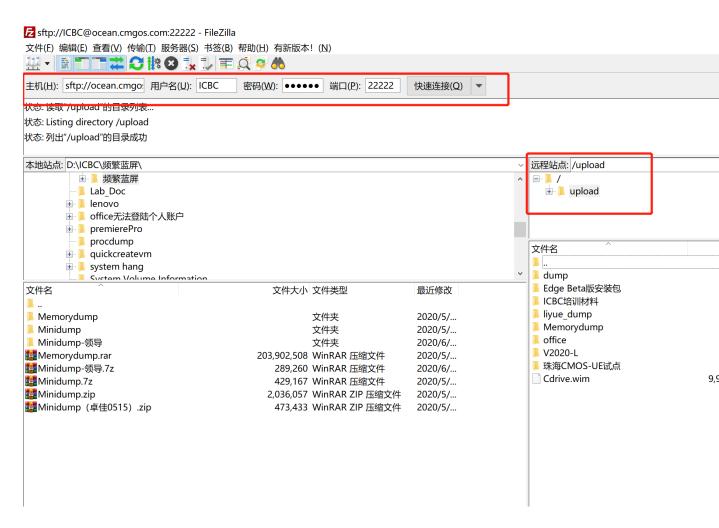
I Filezilla client 端下载 URL: <a href="https://filezilla-project.org/download.php?type=client">https://filezilla-project.org/download.php?type=client</a>

I 登陆地址: sftp://ocean.cmgos.com I 用户名为: ICBC (区分大小写)

| 端口: 22222

I 密码: 2qfs52ninbFB

登陆之后, 上传至 upload 文件夹



李琦 Li Qi

神州网信技术有限公司

C&M Information Technologies Co., Ltd.

服务电话: 4008180055

电子邮箱 Email: liqi@cmgos.com



发件人: huangxl@sdc.icbc.com.cn < huangxl@sdc.icbc.com.cn >

发送时间: 2020 年 7 月 23 日 11:09 收件人: Li Qi <<u>liqi@cmgos.com</u>>

**抄送:** Bai Chengxiao < baicx@cmgos.com >; CRM Case Email < casemail@cmgos.com >; Liu Wei < liuwei@cmgos.com >; Li Xin < lixin@cmgos.com >; Qi Feng < qifeng@cmgos.com >; Wang Dan < wangdan@cmgos.com >; Wang Wenlei < wangwl@cmgos.com >; zhanjian@sdc.icbc.com.cn **主题:** 答复: 回复: 回复: 回复: 回复: 回复: 回复: 回复: 回复: 管复: 转发: 回复: [案例号: CAS-02526-V3W8K2 ] % | P3||CBC|神州网站政府版打开图片出现弹框提示 % 初次响应 CMIT:0001141

C:\Program Files (x86)\DSPClient\CEMS\EDSM>ren MedAdapter64.dll MedAdapter64.dll.bak 拒绝访问。

#### 黄先生, 您好:

如刚才电话沟通,请您尝试做如下两个操作,我会在周四上午与您联系,确认操作结果,感谢您的配合:

- 1, 重命名 C:\Program Files (x86)\DSPClient\CEMS\EDSM\MedAdapter64.dll 这个文件,如有权限重命名成功,请尝试问题是否复现
- 2, 请解压附件工具至本地,按照如下步骤操作,将生成的 VHDX 文件发送给我取消 Use Volume Shadow Copy 勾选,选择 C 盘,然后生成 VHDX 文件(文件路径自定义)。

李琦 Li Qi 神州网信技术有限公司 C&M Information Technologies Co., Ltd. 服务电话: 4008180055

发件人: Li Qi

发送时间: 2020年7月17日18:38

电子邮箱 Email: liqi@cmgos.com

收件人: 'huangxl@sdc.icbc.com.cn' <huangxl@sdc.icbc.com.cn>

**抄送:** Bai Chengxiao < baicx@cmgos.com >; CRM Case Email < casemail@cmgos.com >; Liu Wei < liuwei@cmgos.com >; Li Xin < lixin@cmgos.com >; Qi Feng < gifeng@cmgos.com >; Wang Dan < wangdan@cmgos.com >; Wang Wenlei < wangwl@cmgos.com >; zhanjian@sdc.icbc.com.cn 主题: 回复: 回复: 回复: 回复: 回复: 回复: 回复: 回复: 回复: 管复: 转发: 回复: [案例号: CAS-02526-V3W8K2 ] % | P3||CBC|神州网站政府版打开图片出现弹框提示 % 初次响应 CMIT:0001141

#### 黄先生, 您好:

感谢您的配合, 经过今天一天的内部分析, 现将问题进度向您汇报一下:

从最新收到的事件日志,可以看到在打开 JPG 文件的过程中,explorer 进程在读取相应的注册表键值后,跳转至 openwith.exe。进而提示用户选择打开方式。

注册表的相关键值被设置并保存,但从事件日志上可以看到,有未知进程再重新写入对应的键值,使其 hash 值发生变化,因此并未读取成功。基于上述判断,不排除有代码劫持的可能。

Explorer PID 9448 载入默认关联 8: 26: 39 AM

未知进程 PID 5616 设置 JPG 文件关联 8: 29: 57 AM

未知进程 PID 9928 设置 JPG 文件关联 8: 30: 08 AM

OpenWith.exe PID 11364 设置 JPG 文件关联 8: 30: 45 AM

为了进一步排查此问题,请使用附件运行 SystemInternals Autoruns 工具,在 C 盘根目录下创建 log 文件夹,同时帮忙执行如下操作:

- 1- 显示文件扩展名关联: 在 CMD 中运行: assoc >c:\log\assoc.txt
- 2- 显示文件扩展名所关联程序: 在 CMD 中运行 ftype >c:\log\ftype.txt
- 3- 设置 .jpg 文件扩展名: 在 CMD 中运行 assoc .jpg=jpegfile
- 4- 设置 .jpg 文件关联图片查看器 ftype jpegfile=%SystemRoot%\System32\rundll32.exe "%ProgramFiles%\Windows Photo Viewer\PhotoViewer.dll", ImageView\_Fullscreen %1
- 5- 如果步骤 4 运行后文件没有正常打开,在弹框的打开方式中选择图片查看器打开,并同时勾选始终用此应用打开 .jpg 文件。

在运行以上 1-5 操作时,请使用 PROCMON 软件抓取日志。(启用 PROCMON 时,请以管理员方式运行)

最后,将 C:\LOG 文件夹; procmon 日志; autoruns 保存文件,打包压缩发送给我,谢谢

李琦 Li Qi

神州网信技术有限公司

C&M Information Technologies Co., Ltd.

服务电话: 4008180055

电子邮箱 Email: liqi@cmgos.com

发件人: huangxl@sdc.icbc.com.cn < huangxl@sdc.icbc.com.cn >

发送时间: 2020 年 7 月 16 日 16:16 收件人: Li Qi liqi@cmgos.com>

**抄送:** Bai Chengxiao < baicx@cmgos.com >; CRM Case Email < casemail@cmgos.com >; Liu Wei < liuwei@cmgos.com >; Li Xin < lixin@cmgos.com >; Qi Feng < gifeng@cmgos.com >; Wang Dan < wangdan@cmgos.com >; Wang Wenlei < wangwl@cmgos.com >; zhanjian@sdc.icbc.com.cn 主题: 答复: 回复: 回复: 回复: 回复: 回复: 回复: 回复: 回复: 答复: 转发: 回复: [案例号: CAS-02526-V3W8K2 ] % | P3||CBC|神州网站政府版打开图片出现弹框提示 % 初次响应 CMIT:0001141

config 目录下 5 个文件全部被占用,无法复制。

### 黄先生, 您好:

感谢您的回复,收到您发送的日志。不过好像确实因为权限原因在拷贝时被阻止了。我这边需要查 看的相关文件并没有发送过来

麻烦您再看一下 下面的三个位置,可以先将他们拷贝至桌面,至少将()内的几个文件拷贝出来。再进行压缩后上传,谢谢

- C:\Windows\System32\winevt\Logs----这里的系统日志主要需要(application.evtx; Security.evtx; system.evtx 这三个文件)
- C:\Windows\System32\config---这里的文件主要需要(default; SAM; security; software; system 这五个文件)
- C:\windows\system32\adminscript.vbs

李琦 Li Qi 神州网信技术有限公司 C&M Information Technologies Co., Ltd. 服务电话: 4008180055 电子邮箱 Email: liqi@cmgos.com

发件人: huangxl@sdc.icbc.com.cn < huangxl@sdc.icbc.com.cn >

发送时间: 2020 年 7 月 16 日 11:31 收件人: Li Qi < liqi@cmgos.com>

抄送: Bai Chengxiao <<u>baicx@cmgos.com</u>>; CRM Case Email <<u>casemail@cmgos.com</u>>; Liu Wei <<u>liuwei@cmgos.com</u>>; Li Xin <<u>lixin@cmgos.com</u>>; Qi Feng <<u>qifeng@cmgos.com</u>>; Wang Dan <<u>wangdan@cmgos.com</u>>; Wang Wenlei <<u>wangwl@cmgos.com</u>>; <u>zhanjian@sdc.icbc.com.cn</u>

主题: 答复: 回复: 回复: 回复: 回复: 回复: 回复: 回复: 答复: 转发: 回复: [案例号: CAS-02526-V3W8K2

]% |P3||CBC|神州网站政府版打开图片出现弹框提示 % 初次响应 CMIT:0001141

config 附件分包 1:

\_\_\_\_\_

此邮件信息仅供收件人查阅,所含任何评论、陈述或数据仅供收件人参考,若有改动,恕可能不另行得查阅或使用此邮件信息。若您误收到本邮件,敬请及时通知发件人,并将邮件从您系统中彻底删除This message is intended only for use of the addressees and any comment, statement or d may not be sent for any revising related. Please do not disclose, copy, or distribute t use the content of this e-mail. If you receive this e-mail in error, please notify the completely. The sender and ICBC are not responsible for the loss caused possibly by e-ma

\_\_\_\_\_

此邮件信息仅供收件人查阅,所含任何评论、陈述或数据仅供收件人参考,若有改动,恕可能不另不得查阅或使用此邮件信息。若您误收到本邮件,敬请及时通知发件人,并将邮件从您系统中彻底册This message is intended only for use of the addressees and any comment, statement or d may not be sent for any revising related. Please do not disclose, copy, or distribute t use the content of this e-mail. If you receive this e-mail in error, please notify the completely. The sender and ICBC are not responsible for the loss caused possibly by e-ma

[附件 "Disk2vhd.zip" 被 黄玺磊/上海技术部/软件开发中心/ICBC 删除]

\_\_\_\_\_

此邮件信息仅供收件人查阅,所含任何评论、陈述或数据仅供收件人参考,若有改动,恕可能不是不得查阅或使用此邮件信息。若您误收到本邮件,敬请及时通知发件人,并将邮件从您系统中彻底那This message is intended only for use of the addressees and any comment, statement or d may not be sent for any revising related. Please do not disclose, copy, or distribute t use the content of this e-mail. If you receive this e-mail in error, please notify the completely. The sender and ICBC are not responsible for the loss caused possibly by e-ma

-----来自 Li Qi liqi@cmgos.com> 的消息,在 Fri, 17 Jul 2020 10:37:56 +0000 -----

收件人:"huangxl@sdc.icbc.com.cn" <huangxl@sdc.icbc.com.cn>

抄送: Bai Chengxiao 〈<u>baicx@cmgos.com</u>〉,CRM Case Email 〈<u>casemail@cmgos.com</u>〉,"Liu 〈<u>zhanjian@sdc.icbc.com.cn</u>〉

主题: 回复: 回复: 回复: 回复: 回复: 回复: 回复: 回复: 医复: 答复: 转发: 回复: [

## 黄先生, 您好:

感谢您的配合,经过今天一天的内部分析,现将问题进度向您汇报一下:

从最新收到的事件日志,可以看到在打开 JPG 文件的过程中,explorer 进程在读取相应的注册表键 值后, 跳转至 openwith.exe。进而提示用户选择打开方式。

注册表的相关键值被设置并保存,但从事件日志上可以看到,有未知进程再重新写入对应的键值, 使其 hash 值发生变化,因此并未读取成功。基于上述判断,不排除有代码劫持的可能。

Explorer PID 9448 载入默认关联 8: 26: 39 AM



未知进程 PID 5616 设置 JPG 文件关联 8: 29: 57 AM

```
🔣 事件属性 - 事件 62443, Shell-Core
      详细信息
常规
 ○ 友好视图(N)
                    XML 视图(X)
   - <Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
     - <System>
        <Provider Name="Microsoft-Windows-Shell-Core" Guid="{30336ed4-e327-447c-</pre>
          9de0-51b652c86108}"/>
        <EventID>62443</EventID>
        <Version>0</Version>
        <Level>4</Level>
        <Task>62443</Task>
        <Opcode>0</Opcode>
        <Keywords>0x100000000000000</Keywords>
        <TimeCreated SystemTime="2020-07-13T00:29:57.733641100Z" />
        <EventRecordID>2271</EventRecordID>
        <Correlation />
        <Execution ProcessID="5616" ThreadID="12020" />
        <Channel>Microsoft-Windows-Shell-Core/AppDefaults</Channel>
        <Computer>KFZXHUANGXLQ.Intranet.ICBC.COM.CN</Computer>
        <Security UserID="S-1-5-21-1334113836-2533147148-2525040731-</p>
          530331"/>
       </System>
     - <EventData>
        <Data Name="Info">SetDefault: Association=.jpg,
          ProgId=PhotoViewer.FileAssoc.Tiff</Data>
       </EventData>
     </Event>
```

复制(P)

```
🔣 事件属性 - 事件 62443, Shell-Core
      详细信息
常规
 ○ 友好视图(N)
                   XML 视图(X)
   - <Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
     - <System>
        <Provider Name="Microsoft-Windows-Shell-Core" Guid="{30336ed4-e327-447c-</pre>
          9de0-51b652c86108}"/>
        <EventID>62443</EventID>
        <Version>0</Version>
        <Level>4</Level>
        <Task>62443</Task>
        <Opcode>0</Opcode>
        <Keywords>0x100000000000000</Keywords>
        <TimeCreated SystemTime="2020-07-13T00:29:57.733693000Z" />
        <EventRecordID>2272</EventRecordID>
        <Correlation />
        <Execution ProcessID="5616" ThreadID="12020" />
        <Channel>Microsoft-Windows-Shell-Core/AppDefaults</Channel>
        <Computer>KFZXHUANGXLQ.Intranet.ICBC.COM.CN
        <Security UserID="S-1-5-21-1334113836-2533147148-2525040731-</p>
          530331"/>
      </System>
     - <EventData>
        <Data Name="Info">SetDefault-Info: Association=.jpg,
          ProgId=PhotoViewer.FileAssoc.Tiff, U=S-1-5-21-1334113836-2533147148-
          2525040731-530331, T=2020:07:01:13:00:29, H=DI83ukc9spI=</Data>
      </EventData>
     </Event>
  复制(P)
```

未知进程 PID 9928 设置 JPG 文件关联 8: 30: 08 AM

```
🔣 事件属性 - 事件 62443, Shell-Core
      详细信息
常规
 ○ 友好视图(N)
                    XML 视图(X)
   - <Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
     - <System>
        <Provider Name="Microsoft-Windows-Shell-Core" Guid="{30336ed4-e327-447c-</pre>
          9de0-51b652c86108}"/>
        <EventID>62443</EventID>
        <Version>0</Version>
        <Level>4</Level>
        <Task>62443</Task>
        <Opcode>0</Opcode>
        <Keywords>0x100000000000000</Keywords>
        <TimeCreated SystemTime="2020-07-13T00:30:08.105854900Z" />
        <EventRecordID>2273</EventRecordID>
        <Correlation />
        <Execution ProcessID="9928" ThreadID="216" />
        <Channel>Microsoft-Windows-Shell-Core/AppDefaults</Channel>
        <Computer>KFZXHUANGXLQ.Intranet.ICBC.COM.CN</Computer>
        <Security UserID="S-1-5-21-1334113836-2533147148-2525040731-</p>
          530331"/>
       </System>
     - <EventData>
        <Data Name="Info">SetDefault: Association=.jpg,
          ProgId=PhotoViewer.FileAssoc.Tiff</Data>
       </EventData>
     </Event>
```

复制(P)

```
🔣 事件属性 - 事件 62443, Shell-Core
      详细信息
常规
 ○ 友好视图(N)
                   XML 视图(X)
   - <Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
     - <System>
        <Provider Name="Microsoft-Windows-Shell-Core" Guid="{30336ed4-e327-447c-</pre>
          9de0-51b652c86108}"/>
        <EventID>62443</EventID>
        <Version>0</Version>
        <Level>4</Level>
        <Task>62443</Task>
        <Opcode>0</Opcode>
        <Keywords>0x100000000000000</Keywords>
        <TimeCreated SystemTime="2020-07-13T00:30:08.105901600Z" />
        <EventRecordID>2274</EventRecordID>
        <Correlation />
        <Execution ProcessID="9928" ThreadID="216" />
        <Channel>Microsoft-Windows-Shell-Core/AppDefaults</Channel>
        <Computer>KFZXHUANGXLQ.Intranet.ICBC.COM.CN
        <Security UserID="S-1-5-21-1334113836-2533147148-2525040731-</p>
          530331"/>
      </System>
     - <EventData>
        <Data Name="Info">SetDefault-Info: Association=.jpg,
          ProgId=PhotoViewer.FileAssoc.Tiff, U=S-1-5-21-1334113836-2533147148-
          2525040731-530331, T=2020:07:01:13:00:30, H=aqbY6eqtQ3U=</Data>
      </EventData>
     </Event>
  复制(P)
```

OpenWith.exe PID 11364 设置 JPG 文件关联 8: 30: 45 AM

```
🔣 事件属性 - 事件 62443, Shell-Core
      详细信息
常规
 ○ 友好视图(N)
                    XML 视图(X)
   - <Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
     - <System>
        <Provider Name="Microsoft-Windows-Shell-Core" Guid="{30336ed4-e327-447c-</pre>
          9de0-51b652c86108}"/>
        <EventID>62443</EventID>
        <Version>0</Version>
        <Level>4</Level>
        <Task>62443</Task>
        <Opcode>0</Opcode>
        <Keywords>0x100000000000000</Keywords>
        <TimeCreated SystemTime="2020-07-13T00:30:45.051034400Z" />
        <EventRecordID>2275</EventRecordID>
        <Correlation />
        <Execution ProcessID="11364" ThreadID="11488" />
        <Channel>Microsoft-Windows-Shell-Core/AppDefaults</Channel>
        <Computer>KFZXHUANGXLQ.Intranet.ICBC.COM.CN</Computer>
        <Security UserID="S-1-5-21-1334113836-2533147148-2525040731-</p>
          530331"/>
       </System>
     - <EventData>
        <Data Name="Info">SetDefault: Association=.jpg,
          ProgId=PhotoViewer.FileAssoc.Tiff</Data>
       </EventData>
     </Event>
```

复制(P)

```
🔣 事件属性 - 事件 62443, Shell-Core
      详细信息
常规
 ○ 友好视图(N)
                    XML 视图(X)
   - <Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
     - <System>
        <Provider Name="Microsoft-Windows-Shell-Core" Guid="{30336ed4-e327-447c-</pre>
          9de0-51b652c86108}"/>
        <EventID>62443</EventID>
        <Version>0</Version>
        <Level>4</Level>
        <Task>62443</Task>
        <Opcode>0</Opcode>
        <Keywords>0x100000000000000</Keywords>
        <TimeCreated SystemTime="2020-07-13T00:30:45.051092500Z" />
        <EventRecordID>2276</EventRecordID>
        <Correlation />
        <Execution ProcessID="11364" ThreadID="11488" />
        <Channel>Microsoft-Windows-Shell-Core/AppDefaults</Channel>
        <Computer>KFZXHUANGXLQ.Intranet.ICBC.COM.CN</Computer>
        <Security UserID="S-1-5-21-1334113836-2533147148-2525040731-</p>
          530331"/>
       </System>
     - <EventData>
        <Data Name="Info">SetDefault-Info: Association=.jpg,
          ProgId=PhotoViewer.FileAssoc.Tiff, U=S-1-5-21-1334113836-2533147148-
          2525040731-530331, T=2020:07:01:13:00:30, H=aqbY6eqtQ3U=</Data>
       </EventData>
     </Event>
```

复制(P)

为了进一步排查此问题,请使用附件运行 SystemInternals Autoruns 工具,在 C 盘根目录下创建 log 文件夹,同时帮忙执行如下操作:

- 1- 显示文件扩展名关联:在CMD中运行:assoc >c:\log\assoc.txt
- 2- 显示文件扩展名所关联程序: 在 CMD 中运行 ftype >c:\log\ftype.txt
- 3- 设置 .jpg 文件扩展名: 在 CMD 中运行 assoc .jpg=jpegfile
- 4- 设置 .jpg 文件关联图片查看器 ftype jpegfile=%SystemRoot%\System32\rundll32.exe "%ProgramFiles%\Windows Photo Viewer\PhotoViewer.dll", ImageView\_Fullscreen %1
- 5- 如果步骤 4 运行后文件没有正常打开,在弹框的打开方式中选择图片查看器打开,并同时勾选

始终用此应用打开.ipa 文件。

在运行以上 1-5 操作时,请使用 PROCMON 软件抓取日志。(启用 PROCMON 时,请以 管理员方式运行)

最后,将C:\LOG 文件夹; procmon 日志; autoruns 保存文件,打包压缩发送给 我,谢谢

### 李琦 Li Qi

神州网信技术有限公司

C&M Information Technologies Co., Ltd.

服务电话: 4008180055

电子邮箱 Email: liqi@cmgos.com



发件人: huangxl@sdc.icbc.com.cn < huangxl@sdc.icbc.com.cn >

发送时间: 2020 年 7 月 16 日 16:16 收件人: Li Qi < liqi@cmgos.com>

抄送: Bai Chengxiao <baicx@cmgos.com>; CRM Case Email <casemail@cmgos.com>; Liu Wei </l></l></l></ <wangdan@cmgos.com>; Wang Wenlei <wangwl@cmgos.com>; zhanjian@sdc.icbc.com.cn 主题: 答复: 回复: 回复: 回复: 回复: 回复: 回复: 回复: 回复: 答复: 转发: 回复: [案例号: CAS-02526-V3W8K2 ] % |P3||CBC|神州网站政府版打开图片出现弹框提示 % 初次响应 CMIT:0001141

config 目录下 5 个文件全部被占用,无法复制。 发 Li Qi liqi@cmgos.com> 件 人: 收 "huangxl@sdc.icbc.com.cn" <huangxl@sdc.icbc.com.cn> 抄 Bai Chengxiao <baicx@cmgos.com>, CRM Case Email <casemail@cmgos.com>, "Liu Wei" liuwei@cmgos.com>, Li 送: Xin < lixin@cmgos.com >, Qi Feng < qifeng@cmgos.com >, Wang Dan < wangdan@cmgos.com >, Wang Wenlei <wangwl@cmgos.com>, "zhanjian@sdc.icbc.com.cn" <zhanjian@sdc.icbc.com.cn> **2020/07/16 14:27** 

主 回复: 回复: 回复: 回复: 回复: 回复: 回复: 回复: 回复: 答复: 转发: 回复: [案例号: CAS-02526-V3W8K2] % [P3]ICBC]神州网站 题: 政府版打开图片出现弹框提示 % 初次响应 CMIT:0001141

#### 黄先生, 您好:

感谢您的回复,收到您发送的日志。不过好像确实因为权限原因在拷贝时被阻止了。我这边需要查 看的相关文件并没有发送过来

麻烦您再看一下 下面的三个位置,可以先将他们拷贝至桌面,至少将()内的几个文件拷贝出来。再进行压缩后上传,谢谢

- C:\Windows\System32\winevt\Logs----这里的系统日志主要需要(application.evtx; Security.evtx; system.evtx 这三个文件)
- C:\Windows\System32\config---这里的文件主要需要(default; SAM; security; software; system 这五个文件)
- C:\windows\system32\adminscript.vbs

李琦 Li Qi

神州网信技术有限公司

C&M Information Technologies Co., Ltd.

服务电话: 4008180055

电子邮箱 Email: liqi@cmgos.com

发件人: huangxl@sdc.icbc.com.cn < huangxl@sdc.icbc.com.cn >

**发送时间:** 2020 年 7 月 16 日 11:31 **收件人:** Li Qi liqi@cmgos.com>

抄送: Bai Chengxiao <<u>baicx@cmgos.com</u>>; CRM Case Email <<u>casemail@cmgos.com</u>>; Liu Wei <<u>liuwei@cmgos.com</u>>; Li Xin <<u>lixin@cmgos.com</u>>; Qi Feng <<u>qifeng@cmgos.com</u>>; Wang Dan <<u>wangdan@cmgos.com</u>>; Wang Wenlei <<u>wangwl@cmgos.com</u>>; zhanjian@sdc.icbc.com.cn

**主题:** 答复: 回复: 回复: 回复: 回复: 回复: 回复: 答复: 转发: 回复: [案例号: CAS-02526-V3W8K2] % |P3||CBC|神州网站政府版打开图片出现弹框提示 % 初次响应 CMIT:0001141

config 附件分包 1:

\_\_\_\_\_\_

此邮件信息仅供收件人查阅,所含任何评论、陈述或数据仅供收件人参考,若有改动,恕可能不另不得查阅或使用此邮件信息。若您误收到本邮件,敬请及时通知发件人,并将邮件从您系统中彻底那This message is intended only for use of the addressees and any comment, statement or d may not be sent for any revising related. Please do not disclose, copy, or distribute t use the content of this e-mail. If you receive this e-mail in error, please notify the completely. The sender and ICBC are not responsible for the loss caused possibly by e-ma

\_\_\_\_\_

此邮件信息仅供收件人查阅,所含任何评论、陈述或数据仅供收件人参考,若有改动,恕可能不是不得查阅或使用此邮件信息。若您误收到本邮件,敬请及时通知发件人,并将邮件从您系统中彻底那This message is intended only for use of the addressees and any comment, statement or d may not be sent for any revising related. Please do not disclose, copy, or distribute t use the content of this e-mail. If you receive this e-mail in error, please notify the completely. The sender and ICBC are not responsible for the loss caused possibly by e-ma

# [附件 "Autoruns64.7z" 被 黄玺磊/上海技术部/软件开发中心/ICBC 删除]

此邮件信息仅供收件人查阅,所含任何评论、陈述或数据仅供收件人参考,若有改动,恕可能不银行书面许可,请勿披露、复制、转载此邮件信息。任何第三方均不得查阅或使用此邮件信息。若短通知发件人,并将邮件从您系统中彻底删除。发件人及中国工商银行均不对因邮件可能引发的损失负于的 message is intended only for use of the addressees and any comment, statement or d for the reference of the receivers only. Notification may not be sent for any revising disclose, copy, or distribute this e-mail without ICBC written permission. Any third pa use the content of this e-mail. If you receive this e-mail in error, please notify the delete this e-mail from your computer system completely. The sender and ICBC are not rescaused possibly by e-mail.

-----

此邮件信息仅供收件人查阅,所含任何评论、陈述或数据仅供收件人参考,若有改动,恕可能不另行通知。未经中国工商银行书面许可,请勿披露、复制、转载此邮件信息。任何第三方均不得查阅或使用此邮件信息。若您误收到本邮件,敬请及时通知发件人,并将邮件从您系统中彻底删除。发件人及中国工商银行均不对因邮件可能引发的损失负责。

This message is intended only for use of the addressees and any comment, statement or data contained herein is for the reference of the receivers only. Notification may not be sent for any revising related. Please do not disclose, copy, or distribute this e-mail without ICBC written permission. Any third party shall not read or use the content of this e-mail. If you receive this e-mail in error, please notify the sender immediately and delete this e-mail from your computer system completely. The sender and ICBC are not responsible for the loss caused possibly by e-mail.

此邮件信息仅供收件人查阅,所含任何评论、陈述或数据仅供收件人参考,

This message is intended only for use of the addressees and any comment, statement or data contained herein is for the reference of the receivers only. Notification may not be sent for any revising related. Please do not disclose, copy, or distribute this e-mail without ICBC written permission. Any third party shall not read or use the content of this e-mail. If you receive this e-mail in error, please notify the sender immediately and delete this e-mail from your computer system completely. The sender and ICBC are not responsible for the loss caused possibly by e-mail.