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 <baicx@cmgos.com>, CRM Case Email <casemail@cmgos.com>, Li Qi <liqi@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>, 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: 2020/08/03 18:48
主题: 答复: 回复: 回复: 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 <liqi@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>, 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, 新文档安全技术支持/系统一部/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 11:36
主题: 答复: 回复: 回复: 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|神州网站政府版打开图片出现弹框提示 % 初次响应 CMIT:0001141

[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 <baicx@cmgos.com>, CRM Case Email <casemail@cmgos.com>, Li Qi <liqi@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>, 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
主题: 答复: 回复: 回复: 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

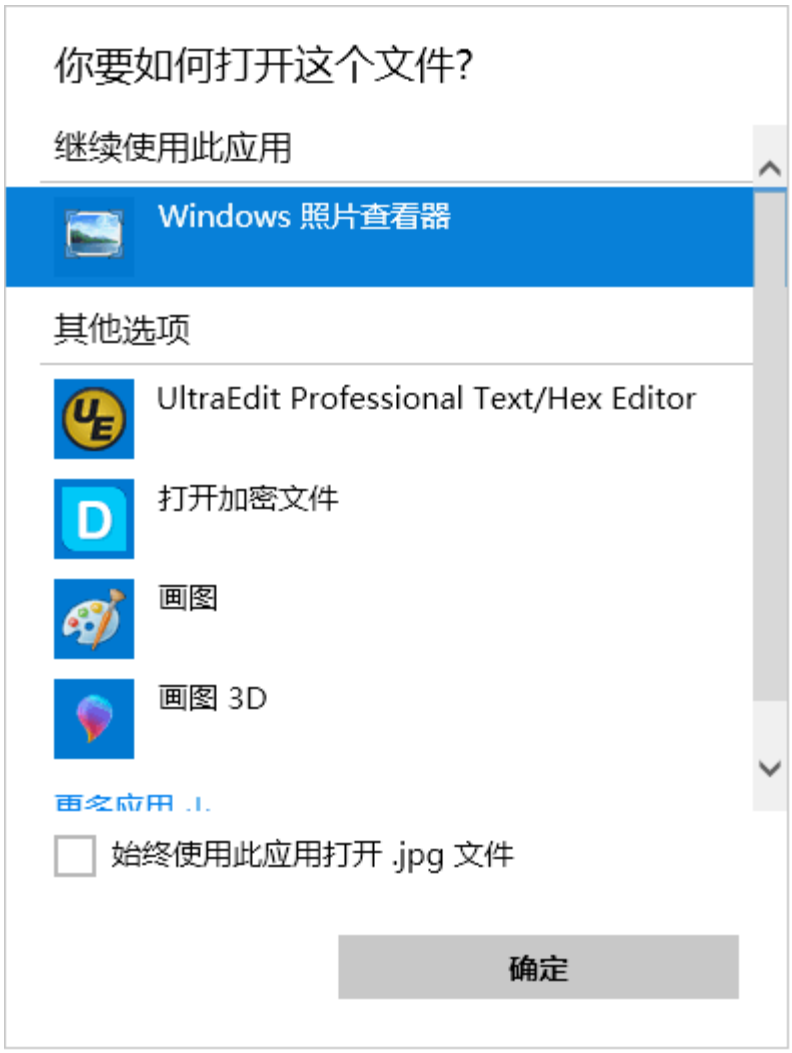
发件人: 新文档安全技术支持/系统一部/软件开发中心/ICBC
收件人: 占剑/上海技术部/软件开发中心/ICBC@ICBC
抄送: Li Qi <liqi@cmgos.com>, Bai Chengxiao <baicx@cmgos.com>, CRM Case Email <casemail@cmgos.com>, "huangxl@sdc.icbc.com.cn" <huangxl@sdc.icbc.com.cn>, Liu Wei <liuwei@cmgos.com>, Li Xin <lixin@cmgos.com>, Qi Feng <qifeng@cmgos.com>, Wang Dan <wangdan@cmgos.com>, Wang Wenlei <wangwl@cmgos.com>, 赵春/系统一部/软件开发中心/ICBC@ICBC, 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
主题: 答复: 回复: 回复: 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 <qifeng@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
主题: 答复: 回复: 回复: 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|神州网站政府版打开图片出现弹框提示 % 初次响应 CMIT:0001141

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 <lixin@cmgos.com>, Qi Feng <qifeng@cmgos.com>, Wang Dan <wangdan@cmgos.com>, Wang Wenlei <wangwl@cmgos.com>
日期: 2020/07/27 09:41
主题: 回复: 回复: 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: liqi@cmgos.com

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 <baicx@cmgos.com>; CRM Case Email <casemail@cmgos.com>; huangxl@sdc.icbc.com.cn; 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>
主题: 答复: 回复: 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|神州网站政府版打开图片出现弹框提示 % 初次响应 CMIT:0001141

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>, "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>, "huangxl@sdc.icbc.com.cn" <huangxl@sdc.icbc.com.cn>
日期: 2020/07/24 17:11
主题: 回复: 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:

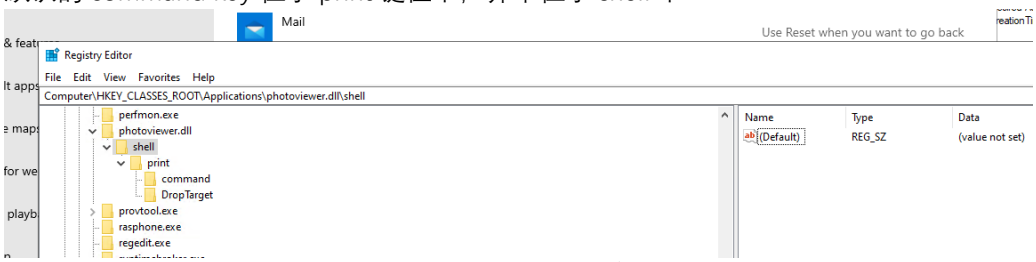
感谢您的反馈，由于电话未联系到您，特发送此邮件说明一下目前的问题进展。

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。

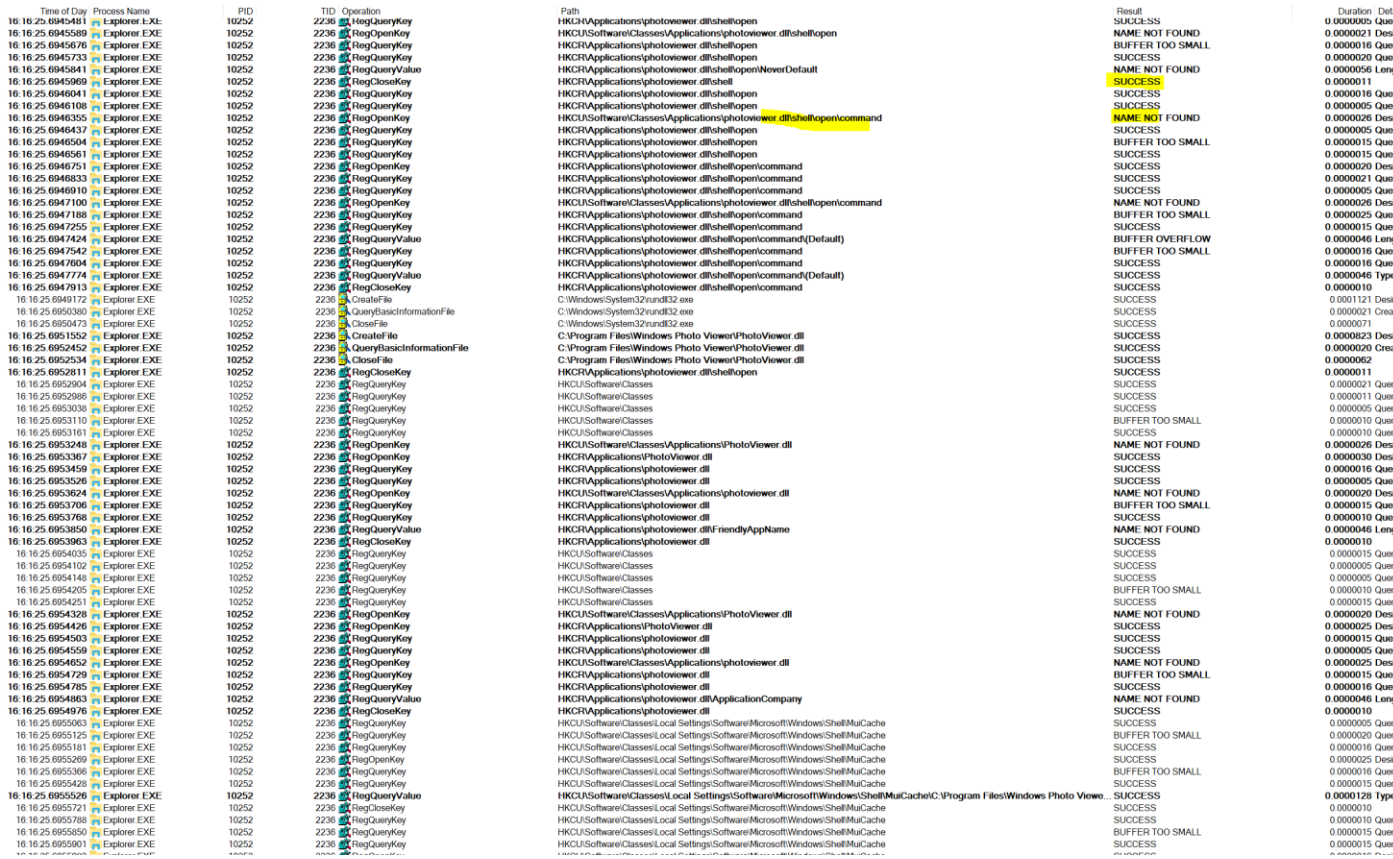
P2V 的收集可以包含用户电脑上的所有设置内容，以避免重复收集日志给客户带来的困扰以及环境对测试的限制。
对于该问题的排查，基于用户数据安全考虑，目前无法收取 P2V，则可能后续仍然需要多次的不同日志收集，才能找到最终原因。

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



Time of Day	Process Name	PID	TID	Operation	Path	Result	Duration	Det
16:16:25.6945481	Explorer.EXE	10252	2236	RegQueryKey	HKCR\Applications\photoviewer.dll\shell\open	SUCCESS	0.0000005	Que
16:16:25.6945589	Explorer.EXE	10252	2236	RegOpenKey	HKCU\Software\Classes\Applications\photoviewer.dll\shell\open	NAME NOT FOUND	0.0000021	Des
16:16:25.6945676	Explorer.EXE	10252	2236	RegQueryKey	HKCR\Applications\photoviewer.dll\shell\open	BUFFER TOO SMALL	0.0000016	Que
16:16:25.6945733	Explorer.EXE	10252	2236	RegQueryKey	HKCR\Applications\photoviewer.dll\shell\open	SUCCESS	0.0000020	Que
16:16:25.6945841	Explorer.EXE	10252	2236	RegQueryValue	HKCR\Applications\photoviewer.dll\shell\open\NeverDefault	NAME NOT FOUND	0.0000056	Len
16:16:25.6945969	Explorer.EXE	10252	2236	RegCloseKey	HKCR\Applications\photoviewer.dll\shell	SUCCESS	0.0000011	
16:16:25.6946041	Explorer.EXE	10252	2236	RegQueryKey	HKCR\Applications\photoviewer.dll\shell\open	SUCCESS	0.0000016	Que
16:16:25.6946108	Explorer.EXE	10252	2236	RegQueryKey	HKCR\Applications\photoviewer.dll\shell\open	SUCCESS	0.0000005	Que
16:16:25.6946355	Explorer.EXE	10252	2236	RegOpenKey	HKCU\Software\Classes\Applications\photoviewer.dll\shell\open\command	NAME NOT FOUND	0.0000026	Des
16:16:25.6946437	Explorer.EXE	10252	2236	RegQueryKey	HKCR\Applications\photoviewer.dll\shell\open	SUCCESS	0.0000005	Que
16:16:25.6946504	Explorer.EXE	10252	2236	RegQueryKey	HKCR\Applications\photoviewer.dll\shell\open	BUFFER TOO SMALL	0.0000015	Que
16:16:25.6946561	Explorer.EXE	10252	2236	RegQueryKey	HKCR\Applications\photoviewer.dll\shell\open	SUCCESS	0.0000015	Que
16:16:25.6946751	Explorer.EXE	10252	2236	RegOpenKey	HKCR\Applications\photoviewer.dll\shell\open\command	SUCCESS	0.0000020	Des
16:16:25.6946833	Explorer.EXE	10252	2236	RegQueryKey	HKCR\Applications\photoviewer.dll\shell\open\command	SUCCESS	0.0000021	Que
16:16:25.6946910	Explorer.EXE	10252	2236	RegQueryKey	HKCR\Applications\photoviewer.dll\shell\open\command	SUCCESS	0.0000005	Que
16:16:25.6947100	Explorer.EXE	10252	2236	RegOpenKey	HKCU\Software\Classes\Applications\photoviewer.dll\shell\open\command	NAME NOT FOUND	0.0000026	Des
16:16:25.6947188	Explorer.EXE	10252	2236	RegQueryKey	HKCR\Applications\photoviewer.dll\shell\open\command	BUFFER TOO SMALL	0.0000025	Que
16:16:25.6947255	Explorer.EXE	10252	2236	RegQueryKey	HKCR\Applications\photoviewer.dll\shell\open\command	SUCCESS	0.0000015	Que
16:16:25.6947424	Explorer.EXE	10252	2236	RegQueryValue	HKCR\Applications\photoviewer.dll\shell\open\command\(Default)	BUFFER OVERFLOW	0.0000046	Len
16:16:25.6947542	Explorer.EXE	10252	2236	RegQueryKey	HKCR\Applications\photoviewer.dll\shell\open\command	BUFFER TOO SMALL	0.0000016	Que
16:16:25.6947604	Explorer.EXE	10252	2236	RegQueryKey	HKCR\Applications\photoviewer.dll\shell\open\command	SUCCESS	0.0000016	Que
16:16:25.6947774	Explorer.EXE	10252	2236	RegQueryValue	HKCR\Applications\photoviewer.dll\shell\open\command\(Default)	SUCCESS	0.0000046	Type
16:16:25.6947913	Explorer.EXE	10252	2236	RegCloseKey	HKCR\Applications\photoviewer.dll\shell\open\command	SUCCESS	0.0000010	
16:16:25.6949172	Explorer.EXE	10252	2236	CreateFile	C:\Windows\System32\rundll32.exe	SUCCESS	0.0001121	Desi
16:16:25.6950380	Explorer.EXE	10252	2236	QueryBasicInformationFile	C:\Windows\System32\rundll32.exe	SUCCESS	0.0000021	Crea
16:16:25.6950473	Explorer.EXE	10252	2236	CloseFile	C:\Windows\System32\rundll32.exe	SUCCESS	0.0000071	
16:16:25.6951552	Explorer.EXE	10252	2236	CreateFile	C:\Program Files\Windows Photo Viewer\PhotoViewer.dll	SUCCESS	0.0000823	Des
16:16:25.6952452	Explorer.EXE	10252	2236	QueryBasicInformationFile	C:\Program Files\Windows Photo Viewer\PhotoViewer.dll	SUCCESS	0.0000020	Crea
16:16:25.6952534	Explorer.EXE	10252	2236	CloseFile	C:\Program Files\Windows Photo Viewer\PhotoViewer.dll	SUCCESS	0.0000062	
16:16:25.6952811	Explorer.EXE	10252	2236	RegCloseKey	HKCR\Applications\photoviewer.dll\shell\open	SUCCESS	0.0000011	
16:16:25.6952904	Explorer.EXE	10252	2236	RegQueryKey	HKCU\Software\Classes	SUCCESS	0.0000021	Que
16:16:25.6952986	Explorer.EXE	10252	2236	RegQueryKey	HKCU\Software\Classes	SUCCESS	0.0000011	Que
16:16:25.6953038	Explorer.EXE	10252	2236	RegQueryKey	HKCU\Software\Classes	SUCCESS	0.0000005	Que
16:16:25.6953110	Explorer.EXE	10252	2236	RegQueryKey	HKCU\Software\Classes	BUFFER TOO SMALL	0.0000010	Que
16:16:25.6953161	Explorer.EXE	10252	2236	RegQueryKey	HKCU\Software\Classes	SUCCESS	0.0000010	Que
16:16:25.6953248	Explorer.EXE	10252	2236	RegOpenKey	HKCU\Software\Classes\Applications\PhotoViewer.dll	NAME NOT FOUND	0.0000026	Des
16:16:25.6953367	Explorer.EXE	10252	2236	RegOpenKey	HKCR\Applications\PhotoViewer.dll	SUCCESS	0.0000030	Des
16:16:25.6953459	Explorer.EXE	10252	2236	RegQueryKey	HKCR\Applications\photoviewer.dll	SUCCESS	0.0000016	Que
16:16:25.6953526	Explorer.EXE	10252	2236	RegQueryKey	HKCR\Applications\photoviewer.dll	SUCCESS	0.0000005	Que
16:16:25.6953624	Explorer.EXE	10252	2236	RegOpenKey	HKCU\Software\Classes\Applications\photoviewer.dll	NAME NOT FOUND	0.0000020	Des
16:16:25.6953706	Explorer.EXE	10252	2236	RegQueryKey	HKCR\Applications\photoviewer.dll	BUFFER TOO SMALL	0.0000015	Que
16:16:25.6953768	Explorer.EXE	10252	2236	RegQueryKey	HKCR\Applications\photoviewer.dll	SUCCESS	0.0000010	Que
16:16:25.6953850	Explorer.EXE	10252	2236	RegQueryValue	HKCR\Applications\photoviewer.dll\FriendlyAppName	NAME NOT FOUND	0.0000046	Len
16:16:25.6953963	Explorer.EXE	10252	2236	RegCloseKey	HKCR\Applications\photoviewer.dll	SUCCESS	0.0000010	
16:16:25.6954035	Explorer.EXE	10252	2236	RegQueryKey	HKCU\Software\Classes	SUCCESS	0.0000015	Que
16:16:25.6954102	Explorer.EXE	10252	2236	RegQueryKey	HKCU\Software\Classes	SUCCESS	0.0000005	Que
16:16:25.6954148	Explorer.EXE	10252	2236	RegQueryKey	HKCU\Software\Classes	SUCCESS	0.0000005	Que
16:16:25.6954205	Explorer.EXE	10252	2236	RegQueryKey	HKCU\Software\Classes	BUFFER TOO SMALL	0.0000010	Que
16:16:25.6954251	Explorer.EXE	10252	2236	RegQueryKey	HKCU\Software\Classes	SUCCESS	0.0000015	Que
16:16:25.6954328	Explorer.EXE	10252	2236	RegOpenKey	HKCU\Software\Classes\Applications\PhotoViewer.dll	NAME NOT FOUND	0.0000020	Des
16:16:25.6954426	Explorer.EXE	10252	2236	RegOpenKey	HKCR\Applications\PhotoViewer.dll	SUCCESS	0.0000025	Des
16:16:25.6954503	Explorer.EXE	10252	2236	RegQueryKey	HKCR\Applications\photoviewer.dll	SUCCESS	0.0000015	Que
16:16:25.6954559	Explorer.EXE	10252	2236	RegQueryKey	HKCR\Applications\photoviewer.dll	SUCCESS	0.0000005	Que
16:16:25.6954652	Explorer.EXE	10252	2236	RegOpenKey	HKCU\Software\Classes\Applications\photoviewer.dll	NAME NOT FOUND	0.0000025	Des
16:16:25.6954729	Explorer.EXE	10252	2236	RegQueryKey	HKCR\Applications\photoviewer.dll	BUFFER TOO SMALL	0.0000015	Que
16:16:25.6954785	Explorer.EXE	10252	2236	RegQueryKey	HKCR\Applications\photoviewer.dll	SUCCESS	0.0000016	Que
16:16:25.6954863	Explorer.EXE	10252	2236	RegQueryValue	HKCR\Applications\photoviewer.dll\ApplicationCompany	NAME NOT FOUND	0.0000046	Len
16:16:25.6954976	Explorer.EXE	10252	2236	RegCloseKey	HKCR\Applications\photoviewer.dll	SUCCESS	0.0000010	
16:16:25.6955063	Explorer.EXE	10252	2236	RegQueryKey	HKCU\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache	SUCCESS	0.0000005	Que
16:16:25.6955125	Explorer.EXE	10252	2236	RegQueryKey	HKCU\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache	BUFFER TOO SMALL	0.0000029	Que
16:16:25.6955181	Explorer.EXE	10252	2236	RegQueryKey	HKCU\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache	SUCCESS	0.0000016	Que
16:16:25.6955269	Explorer.EXE	10252	2236	RegOpenKey	HKCU\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache	SUCCESS	0.0000025	Des
16:16:25.6955366	Explorer.EXE	10252	2236	RegQueryKey	HKCU\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache	BUFFER TOO SMALL	0.0000016	Que
16:16:25.6955428	Explorer.EXE	10252	2236	RegQueryKey	HKCU\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache	SUCCESS	0.0000015	Que
16:16:25.6955526	Explorer.EXE	10252	2236	RegQueryValue	HKCU\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache\C:\Program Files\Windows Photo Viewe...	SUCCESS	0.0000128	Type
16:16:25.6955721	Explorer.EXE	10252	2236	RegCloseKey	HKCU\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache	SUCCESS	0.0000010	
16:16:25.6955788	Explorer.EXE	10252	2236	RegQueryKey	HKCU\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache	SUCCESS	0.0000010	Que
16:16:25.6955850	Explorer.EXE	10252	2236	RegQueryKey	HKCU\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache	BUFFER TOO SMALL	0.0000015	Que
16:16:25.6955901	Explorer.EXE	10252	2236	RegQueryKey	HKCU\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache	SUCCESS	0.0000015	Que

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>
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>; huangxl@sdc.icbc.com.cn
主题: 答复: 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|神州网站政府版打开图片出现弹框提示 % 初次响应 CMIT:0001141

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。

发件人: 黄玺磊/上海技术部/软件开发中心/ICBC
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 <qifeng@cmgos.com>, Wang Dan <wangdan@cmgos.com>, Wang Wenlei <wangwl@cmgos.com>, "zhanjian@sdc.icbc.com.cn" <zhanjian@sdc.icbc.com.cn>
日期: 2020/07/23 16:36
主题: 答复: 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

发件人: Li Qi <liqi@cmgos.com>
收件人: "huangxl@sdc.icbc.com.cn" <huangxl@sdc.icbc.com.cn>, "zhanjian@sdc.icbc.com.cn" <zhanjian@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 <qifeng@cmgos.com>, Wang Dan <wangdan@cmgos.com>, Wang Wenlei <wangwl@cmgos.com>

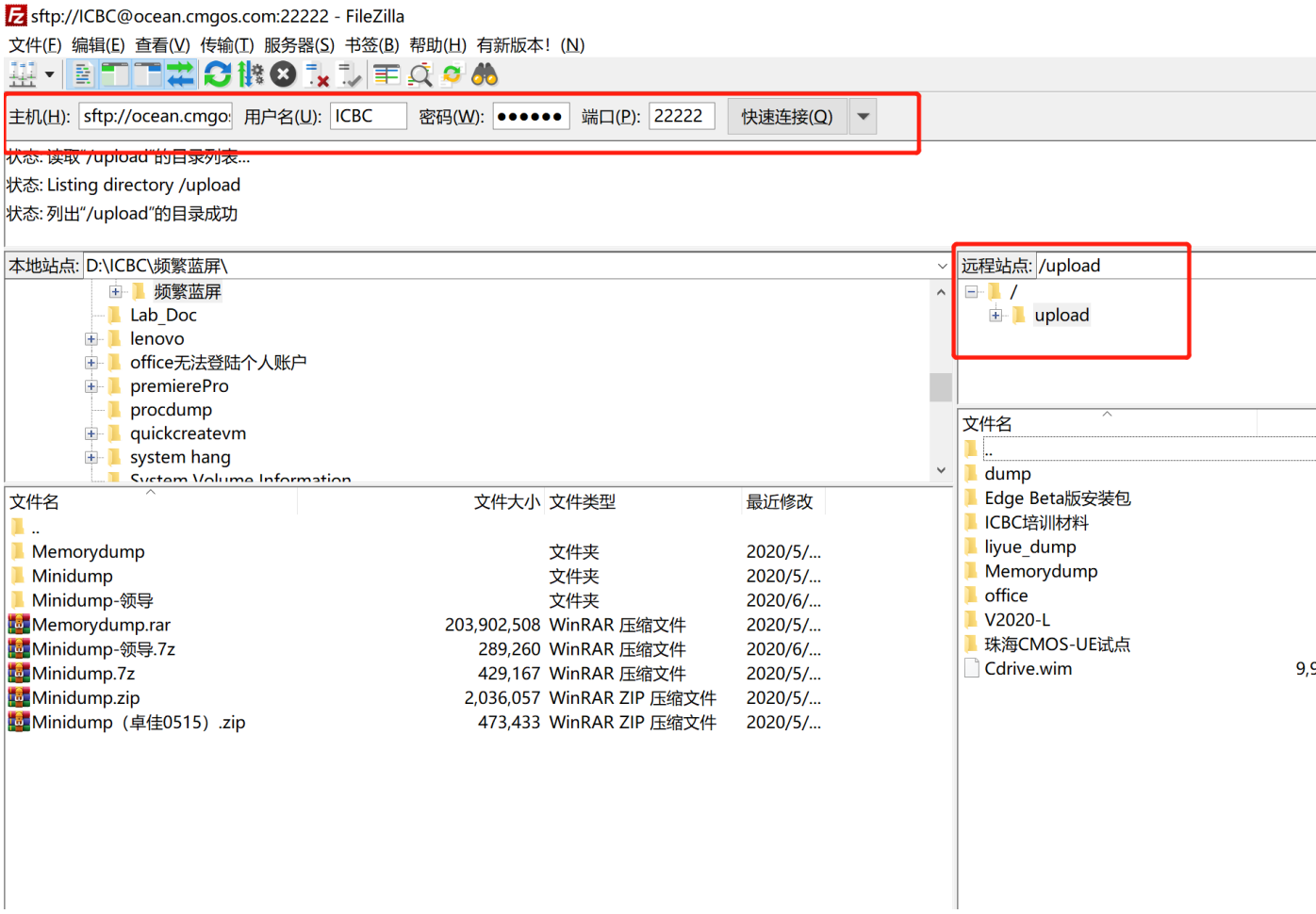
日 2020/07/23 16:27
期:
主 回复: 回复: 回复: 回复: 回复: 回复: 回复: 回复: 回复: 答复: 转发: 回复: [案例号: CAS-02526-
题: V3W8K2] % |P3|ICBC|神州网站政府版打开图片出现弹框提示 % 初次响应 CMIT:0001141

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。
l Filezilla client 端下载 URL：https://filezilla-project.org/download.php?type=client
l 登陆地址：sftp://ocean.cmgos.com
l 用户名为：ICBC（区分大小写）
l 端口：22222
l 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 <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 <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: 回复: 答复: 转发: 回复: [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

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

vhdx 文件有 57 个 G，没法邮件外发。

发件人: Li Qi <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 <qifeng@cmgos.com>, Wang Dan <wangdan@cmgos.com>, Wang Wenlei <wangwl@cmgos.com>, "zhanjian@sdc.icbc.com.cn" <zhanjian@sdc.icbc.com.cn>
日期: 2020/07/21 17:24
主题: 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|神州网站政府版打开图片出现弹框提示 % 初次响应 CMIT:0001141

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
电子邮箱 Email: liqi@cmgos.com

发件人: Li Qi
发送时间: 2020 年 7 月 17 日 18:38

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 <qifeng@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: 答复: 转发: 回复: [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

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 <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: 答复: 转发: 回复: [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

config 目录下 5 个文件全部被占用，无法复制。

发件人: Li Qi <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 <qifeng@cmgos.com>, Wang Dan <wangdan@cmgos.com>, Wang Wenlei <wangwl@cmgos.com>, "zhanjian@sdc.icbc.com.cn" <zhanjian@sdc.icbc.com.cn>
日期: 2020/07/16 14:27
主题: 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 <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: 答复: 转发: 回复: [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

config 附件分包 1：

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

-----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>

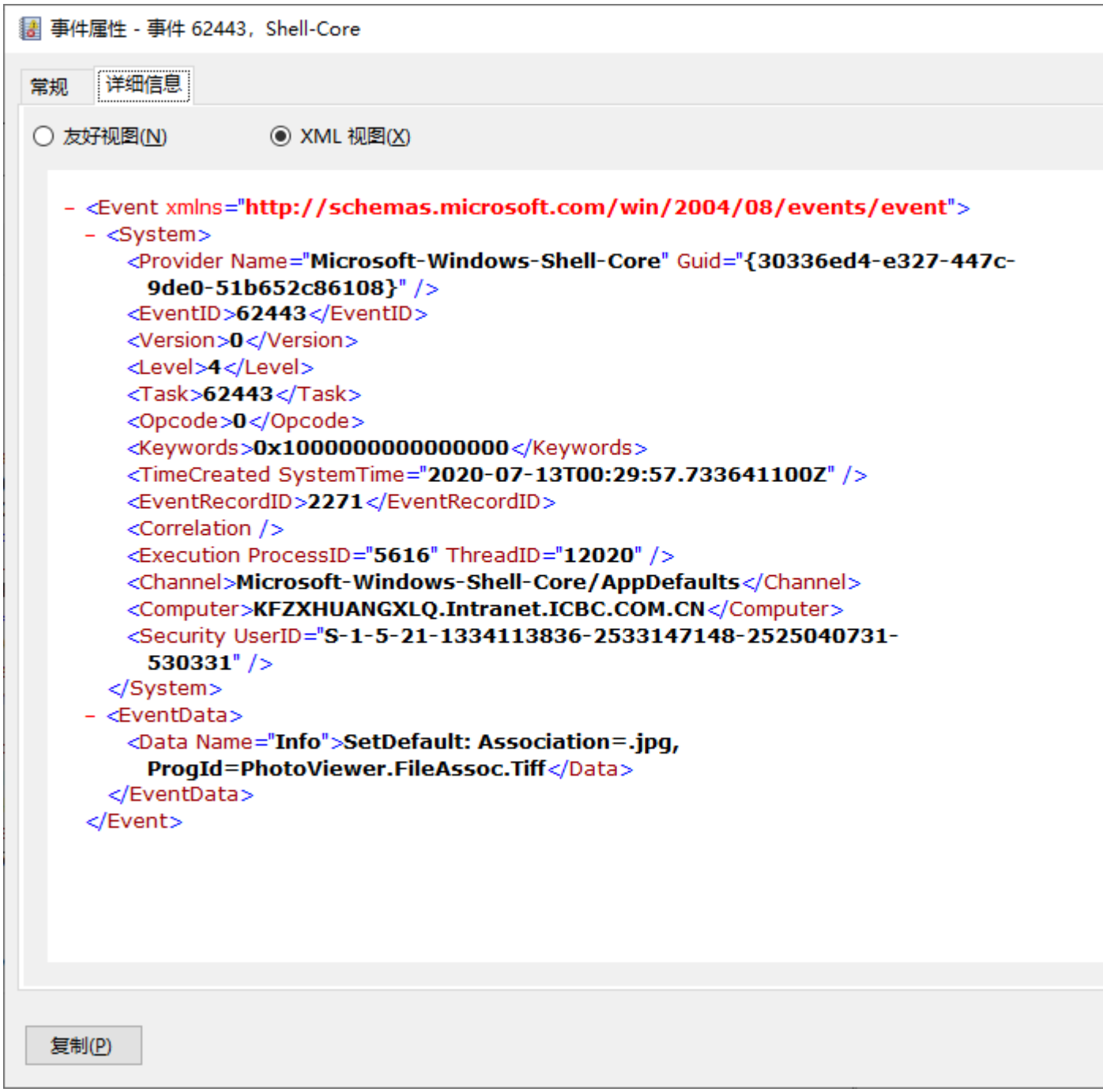
抄送: Bai Chengxiao <baicx@cmgos.com>, CRM Case Email <casemail@cmgos.com>, "Liu <zhanjian@sdc.icbc.com.cn>

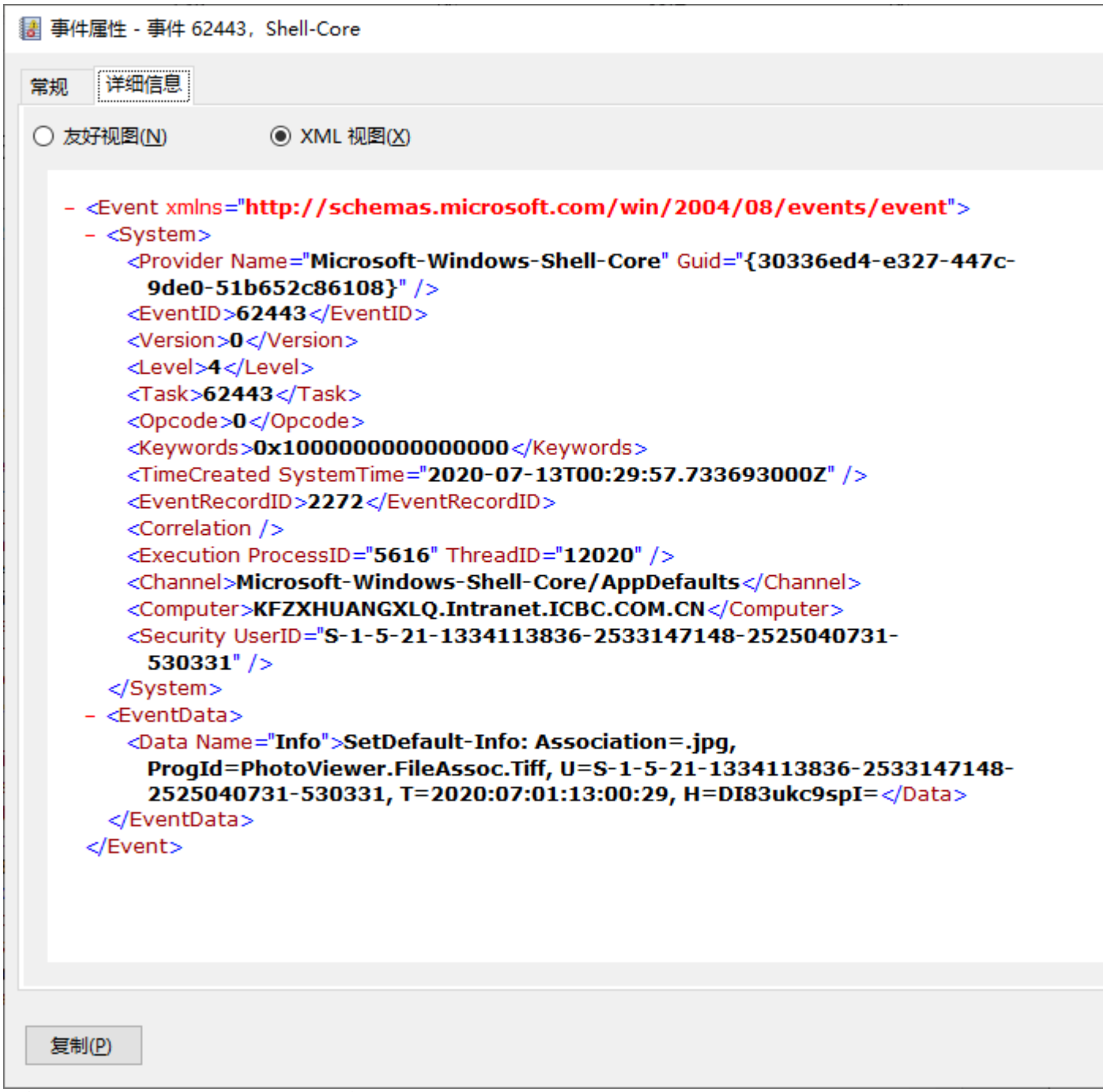
主题: 回复: 回复: 回复: 回复: 回复: 回 复: 回复: 回复: 回复: 答复: 转发: 回复: [

黄先生，您好:

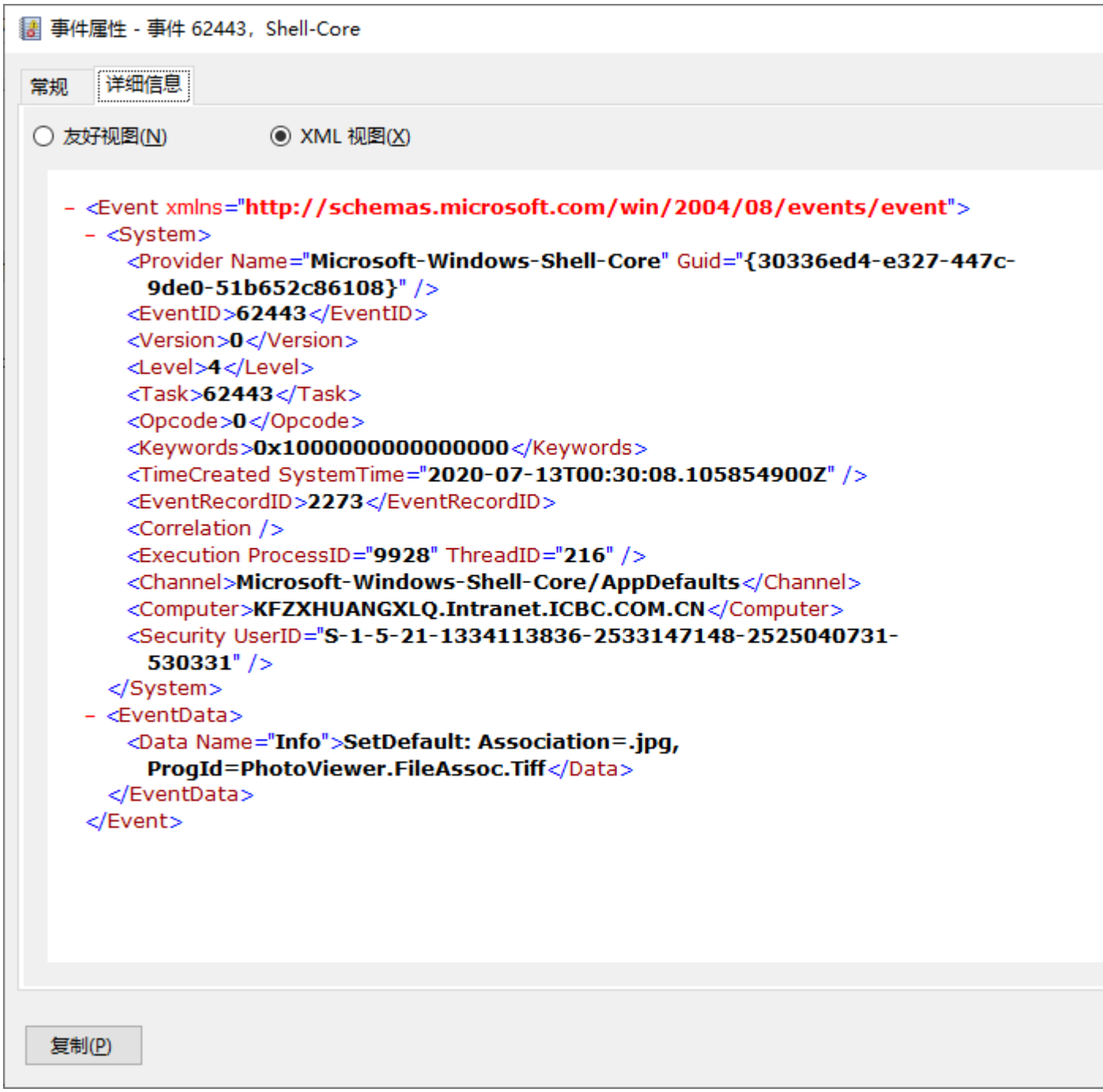
感谢您的配合，经过今天一天的内部分析，现将问题进度向您汇报一下:
从最新收到的事件日志，可以看到在打开 JPG 文件的过程中，explorer 进程在读取相应的注册表键值后，跳转至 openwith.exe。进而提示用户选择打开方式。
注册表的相关键值被设置并保存，但从事件日志上可以看到，有未知进程再重新写入对应的键值，使其 hash 值发生变化，因此并未读取成功。基于上述判断，不排除有代码劫持的可能。
Explorer PID 9448 载入默认关联 8：26：39 AM

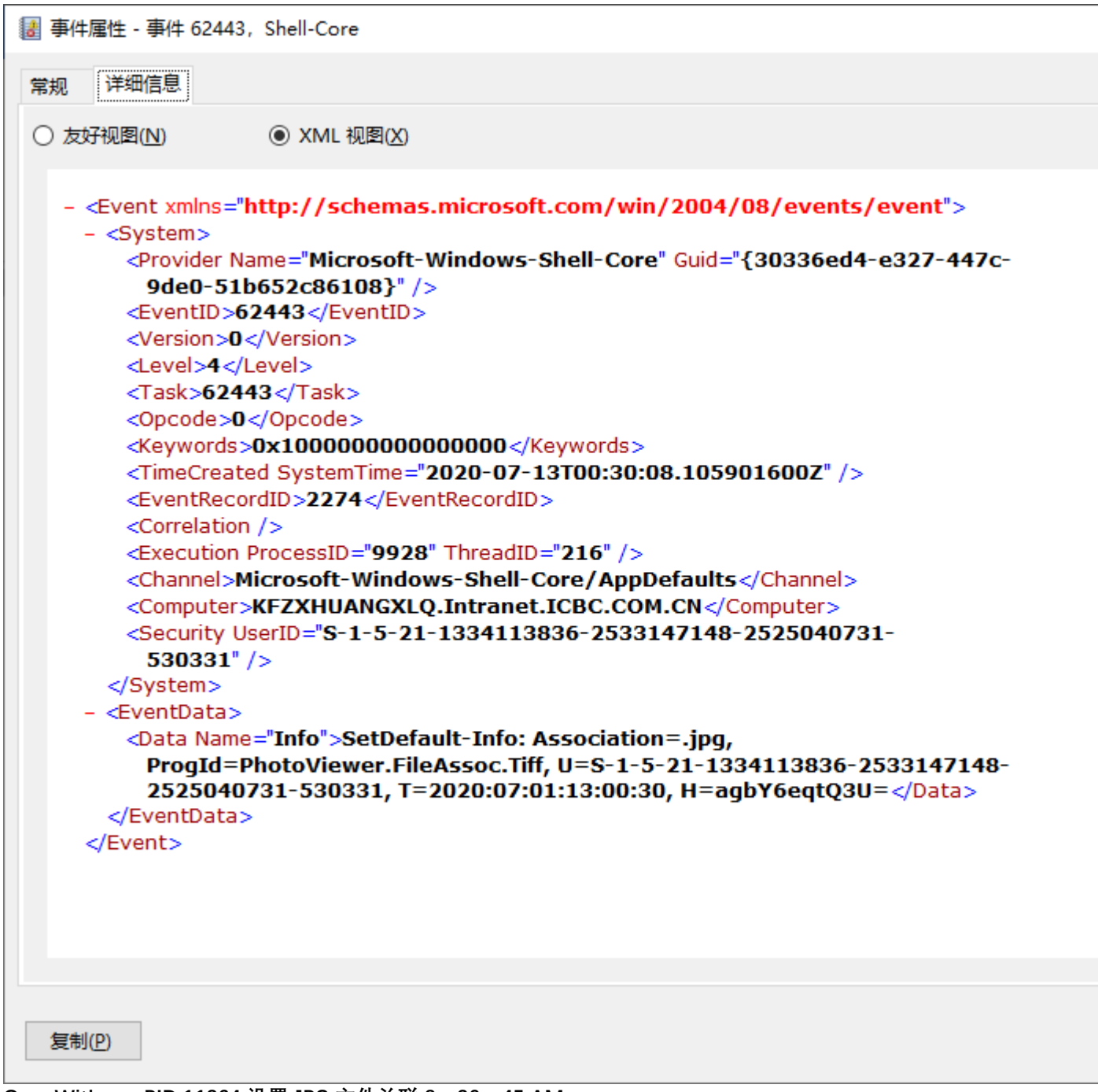
未知进程 PID 5616 设置 JPG 文件关联　8：29：57 AM


事件属性 - 事件 62443，Shell-Core
常规
详细信息
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-9de0-51b652c86108}" />
<EventID>62443</EventID>
<Version>0</Version>
<Level>4</Level>
<Task>62443</Task>
<Opcode>0</Opcode>
<Keywords>0x1000000000000000</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-1-5-21-1334113836-2533147148-2525040731-530331" />
</System>
- <EventData>
<Data Name="Info">SetDefault: Association=.jpg, ProgId=PhotoViewer.FileAssoc.Tiff</Data>
</EventData>
</Event>
复制(P)

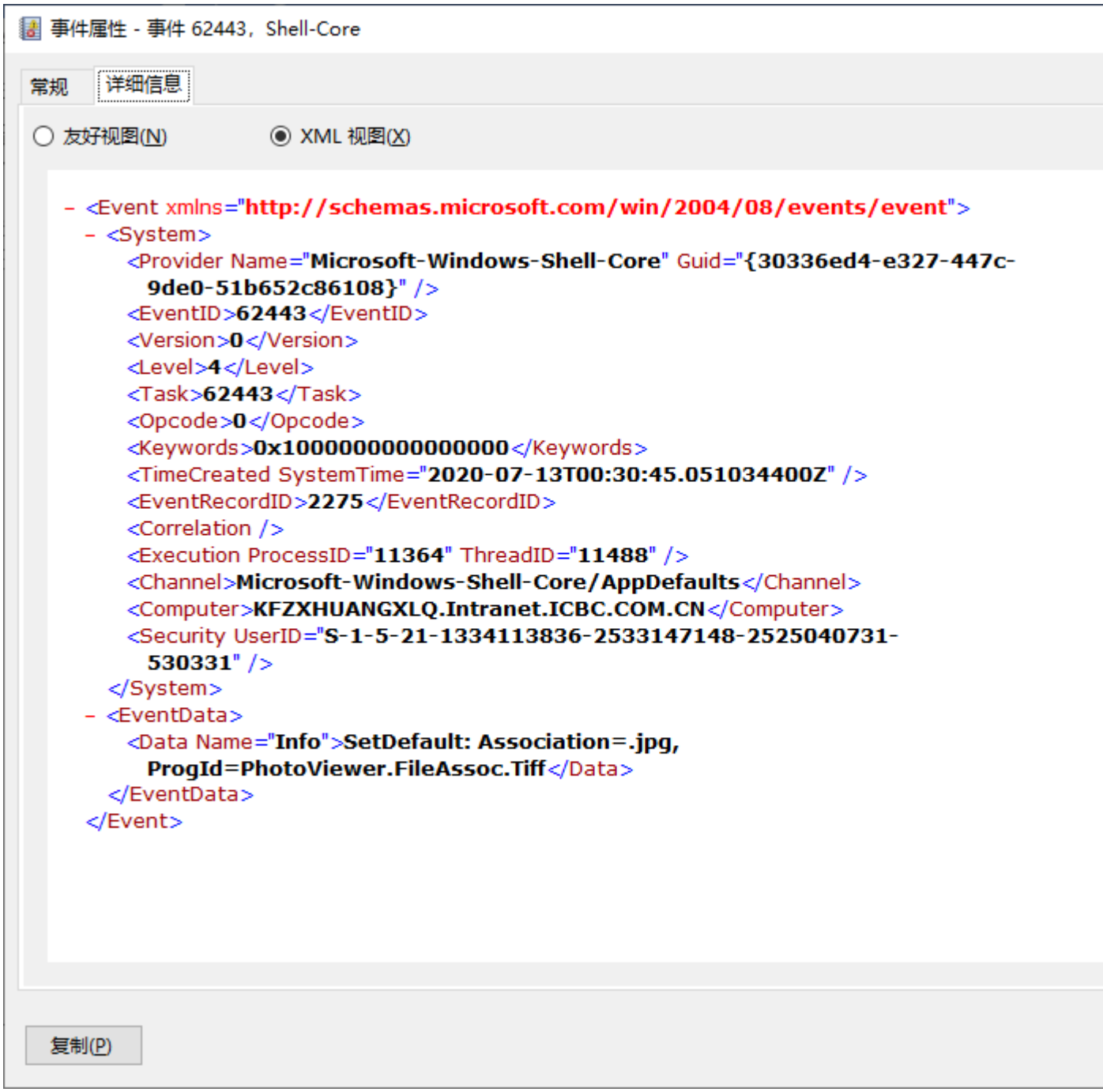


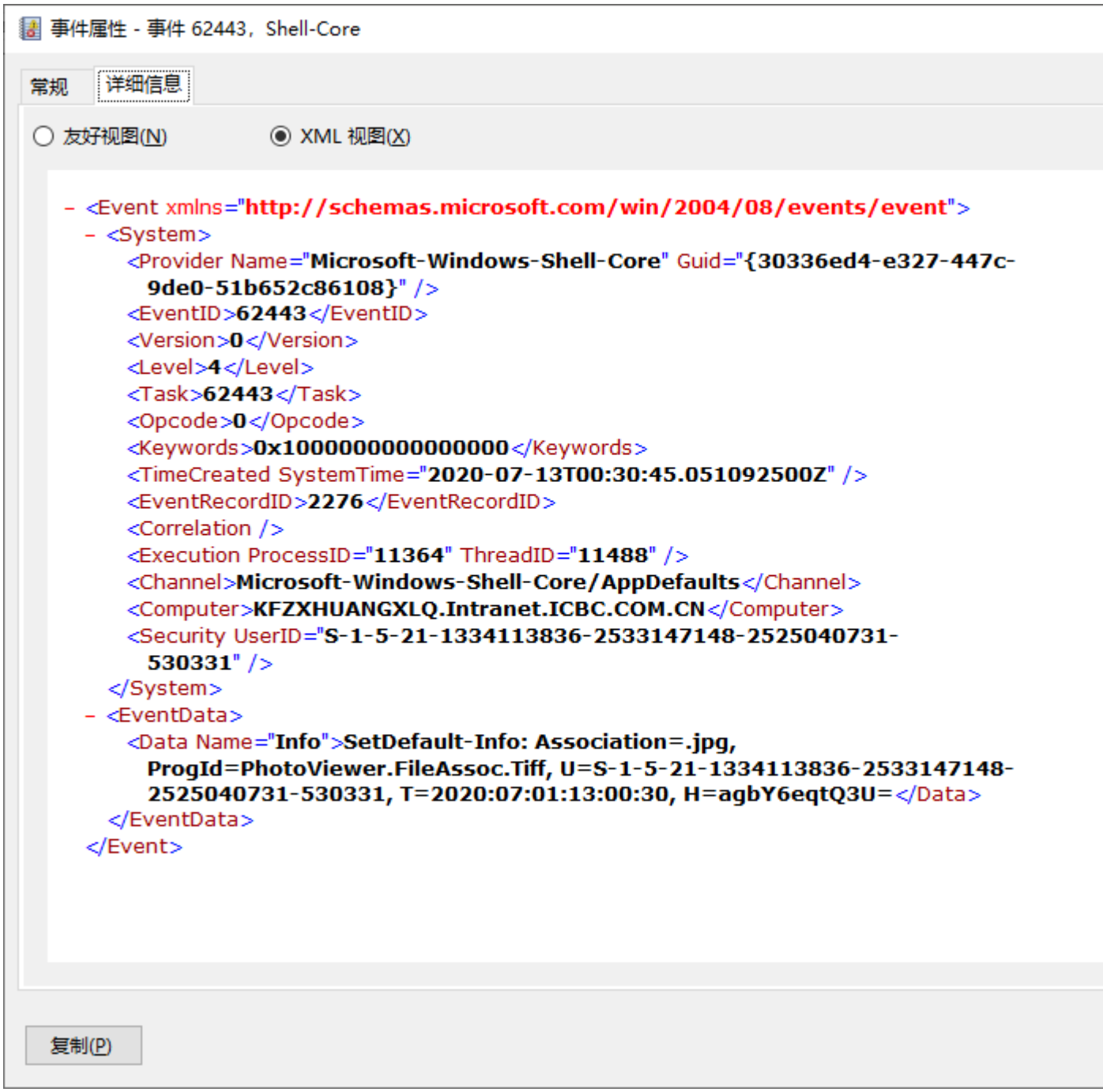
未知进程 PID 9928 设置 JPG 文件关联　8：30：08 AM


事件属性 - 事件 62443，Shell-Core
常规
详细信息
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-9de0-51b652c86108}" />
<EventID>62443</EventID>
<Version>0</Version>
<Level>4</Level>
<Task>62443</Task>
<Opcode>0</Opcode>
<Keywords>0x1000000000000000</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-1-5-21-1334113836-2533147148-2525040731-530331" />
</System>
- <EventData>
<Data Name="Info">SetDefault: Association=.jpg, ProgId=PhotoViewer.FileAssoc.Tiff</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
常规
详细信息
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-9de0-51b652c86108}" />
<EventID>62443</EventID>
<Version>0</Version>
<Level>4</Level>
<Task>62443</Task>
<Opcode>0</Opcode>
<Keywords>0x1000000000000000</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-1-5-21-1334113836-2533147148-2525040731-530331" />
</System>
- <EventData>
<Data Name="Info">SetDefault: Association=.jpg, ProgId=PhotoViewer.FileAssoc.Tiff</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 .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 <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: 答复: 转发: 回复: [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

config 目录下 5 个文件全部被占用，无法复制。

发件人: Li Qi <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 <qifeng@cmgos.com>, Wang Dan <wangdan@cmgos.com>, Wang Wenlei <wangwl@cmgos.com>, "zhanjian@sdc.icbc.com.cn" <zhanjian@sdc.icbc.com.cn>
日期: 2020/07/16 14:27
主题: 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 <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: 答复: 转发: 回复: [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

config 附件分包 1：