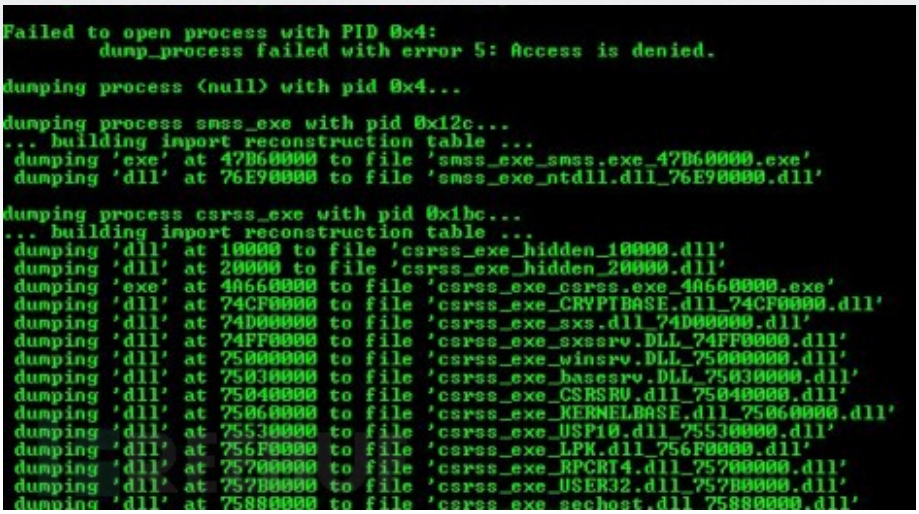
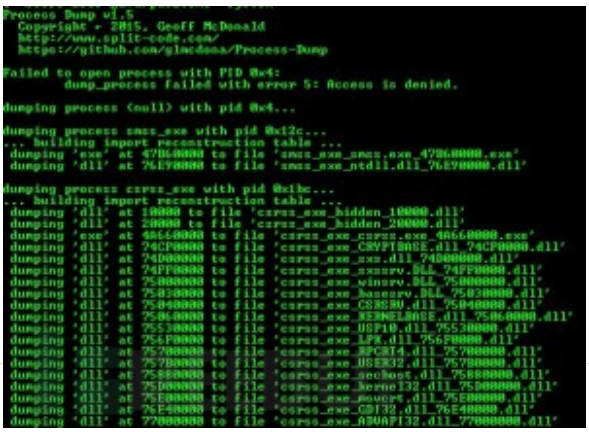
恶意软件研究者的福音：PROCESS DUMP v1.5正式发布

空白 2015-11-27



用于导出恶意软件进程内存的Windows逆向工程命令行工具再次回归了。

这无疑为恶意软件研究者带来巨大便利，因为他们经常要将脱壳后的样本或者注入代码导入到硬盘进行分析，因此非常需要IDA这类的静态分析工具。



用于从内存中dump恶意软件PE文件到硬盘中的Windows工具（用于分析）

Process Dump适用于32和64位的操作系统，工具采用了一种侵略性导入重建方法，并允许在没有PE headers的区域进行（在这种情况下PE headers以及导入表会自动生成）。Process Dump支持clean-ha数据库的创建及使用，因此例如kernel32.dll这样的干净文件会躲过转储。

更新内容

```
1、修复了出现在内存区域、会导致Process Dump挂掉Bug；
2、修复了在64位Windows中一些模块无法找到的Bug；
3、现在Verbose模式增加了更多调试信息。
```

利用实例

从所有进程中转储所有模块（忽略已知的干净模块）：

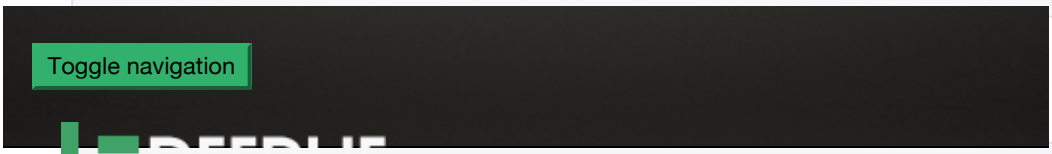
```
pd64.exe -system
```

从特定进程标识符中转储所有模块：

```
pd64.exe -pid 0x18A
```

通过进程名转储所有模块：

```
pd64.exe -p .chrome.
```




```
p  4.e  e -  h  ge r
```

从 业转储代码：

首页
分类阅读

黑客

漏洞 安全工具 WEB安全 系统安全 网络安全
无线安全 设备/客户端安全 数据库安全 安全管理

极客

极客有意思 周边

特色

专题 人物志 活动 视频 观点 招聘

活动

FREE TALK•成都站 已结束
2015-10-31

作者问答送书 已结束
2015-08-19

晒工作台，免费送书 已结束
2015-08-04

行分析：

极客（FreeBuf.COM）

登录

昵称

请输入昵称

必须 您当前尚未登录，注册

邮箱

请输入邮箱地址

必须（保密）

表情 插图

提交评论(Ctrl+Enter) 取消 有人回复时邮件通知我

关键字查找

相关阅读

- 逆向路由器固件之解包 Part1
- 利用windows组策略首选项缺陷获取…
- 有工具了，如何快速发现Windows中…
- 在Windows 2012下面启用MSTSC客…
- 病毒是如何将文件藏进注册表的

特别推荐

不容错过

车真的那么容易偷吗？汽车无线钥匙通信安全的一点科普

360UnicornTeam 2015-07-03

广州天融信招渗透测试人员

topsec 2015-07-29

【微博直播】首届CSS峰会：关注企业信息安全，百位CTO闭门探讨“2016第一步”

路由器 2015-11-02

一周海外安全事件回顾（20140324-0330）

blackscreen 2014-04-01