安天周观察

主办：安天实验室·antiy.cn　　2015 年 7 月（总第 1 期）试行　本期 4 版　　微信搜索：antiylab

对美国电网实施网络攻击 可造成万亿美元经济损失

【关键词】工控安全　网络攻击

上周披露的一份报告称，美国电网若遭网络攻击导致关停部分服务，将会对美国经济造成高达万亿美元的损失。

这份由剑桥大学风险研究中心发表的报告描绘了一幅造成纽约和华盛顿特区 9300 万人无电可用的电力中断景象。报告称，“对美国经济的全部影响估计有 2430 亿美元，在最极端情况下可增至超过 1 万亿美元”。

报告援引美国能源部数据称，自 2000 年以来，美国电网疑似遭受了 15 次网络攻击。美国工业控制系统网络应急响应小组称，去年其响应的关键基础设施网络安全威胁中，有 32% 都发生在能源产业。(http://www.aqniu.com/news/8645.html)

俄罗斯称希拉里有关黑客问题言论“毫无根据”

【关键词】俄罗斯克里姆林宫　希拉里

希拉里 7 日称，黑客活动对美国的安全及企业构成广泛威胁，俄罗斯等国“直接或间接地支持过”黑客活动。

8 日，克里姆林宫发言人佩斯科夫被问及希拉里的言论时对记者称：“这是绝对不恰当的言论，也是毫无根据的指控。”

“黑客活动是国际性问题，政府支持此类活动的说法是完全没有根据的指控，”佩斯科夫称。他还称，在呼吁合作打击网络犯罪的背景下，这样的言论“不具建设性”。(http://www.myhack58.com/Article/html/1/4/2015/64488.htm)

德『爱国者』导弹疑遭黑客攻击 发送无厘头命令

【关键词】德国『爱国者』导弹防御系统　黑客攻击

据今日俄罗斯电视台 7 月 8 日报道，德国“爱国者”导弹防御系统近日疑似遭不明黑客攻击，发送了无厘头的命令。但是，德国国防部对此表示了否认，并称目前没有迹象表明该防御系统遭到了黑客攻击。

据悉，“爱国者”导弹防御系统系美国制造，由 6 个发射器和 2 台雷达组成。2013 年，德国国防军在土耳其边境地区部署了“爱国者”导弹及 160 名士兵。(http://news.xinhuanet.com/world/2015-07/08/c_127998819.htm)

支付宝 9.0 重置密码功能存缺陷

【关键词】支付宝　密码重置

支付宝新升级的 9.0 版本中取消了用户手势密码的设置，转变为“大数据风控”保护。如果用户手机不具备指纹解锁功能，那么在其手机上支付宝账户可以直接被访问。

这个修改遭到用户质疑，很多人担心泄露淘宝购买记录和消费记录，或者可以直接使用小额支付功能。

支付宝称，通过多年积攒的大数据对用户的行为分析进行身份认证，当不是本人使用时，支付宝可通过细小的行为习惯来区别判断。

研究人员称，支付宝 9.0 的重置密码功能存在逻辑问题，只需要知道用户身份证号便可以重置其登录密码。(http://bobao.360.cn/news/detail/1768.html)

恶意代码通缉令——APT

一句话消息

7 月 8 日，日本防卫省专用酒店或遭黑客袭击 住客个人信息可能外泄 (http://www.myhack58.com/Article/html/1/4/2015/64416.htm)

7 月 9 日，苹果被黑客攻击调查出现线索，被指向 Morpho 独立黑客组织 (http://www.cnbeta.com/articles/409445.htm)

7 月 10 日，北约官网遭 ISIS 涂鸦 (http://www.myhack58.com/Article/html/1/4/2015/64497.htm)

7 月 14 日，日本 5 所大学网站遭到攻击，管理账户密码等外泄 (http://www.cnbeta.com/articles/410933.htm)

7 月 14 日，美国千万公务员信息泄露：受害者尚未接到通知 ” (http://www.cnbeta.com/articles/411065.htm)

每周 APT(高级持续性威胁) 新闻

类 型	内 容
英文标题	21.5 million SSNs stolen in second OPM breach, along with fingerprints and background info
中文标题	美国联邦人事管理局被黑客攻击 2,150 万人资料遭泄露，包含指纹和背景信息数据
作 者	Ashley Carman
作者单位	SC Magazine
中文摘要	美国联邦人事管理局遭受攻击泄露的数据中，包括 1970 万个人背景数据、表格、社会安全编码 (SSNs)，以及 110 万指纹数据。SF-86、SF-85 和 SF-85P 表格数据也遭泄露，其包含背景采访，用户名与密码申请等信息。 OPM 表示联邦人员的健康、财务、薪金以及退休记录均未受到影响。数据泄露的通知已经发送至所有的受害者。
链接地址	http://www.scmagazine.com/opm-elaborates-on-data-breaches/article/425643/

每周新恶意代码信息

本周共发现 1 个移动恶意代码和 11 个 PC 恶意代码

病毒分类	新出现的病毒名称 / 发现日期	病毒特点 / 信息来源
移动恶意代码	Trojan_Foreign.HRN 发现日期：2015 年 7 月 6 日	该变种创建病毒子程序，判断自身是否在移动硬盘 (如 U 盘) 中启动 , 如果是，则会执行文件再次感染系统，随后会注册一个移动存储设备的回调函数，当有移动设备插入时 , 会通知病毒执行感染操作。 大连网安：http://www.ga.dl.gov.cn/publish/20157684926.asp
PC 恶意代码	TrojanDownloader:Win32/Dowector.A 发现日期：2015 年 7 月 6 日	此威胁未经用户允许，下载、安装其他程序到用户电脑，包括恶意程序。 Microsoft：http://www.microsoft.com/security/portal/threat/encyclopedia/entry.aspx?Name=TrojanDownloader:Win32/Dowector.A
	TrojanSpy:Win32/Nivdort.AN 发现日期：2015 年 7 月 6 日	此威胁收集用户敏感信息，发送给恶意黑客。利用代码注入，使得对其难以检测、清除。 Microsoft：http://www.microsoft.com/security/portal/threat/encyclopedia/entry.aspx?Name=TrojanSpy:Win32/Nivdort.AN
	Backdoor:Win32/Zegost.DT 发现日期：2015 年 7 月 6 日	此威胁给予恶意黑客未授权的访问权限，控制用户电脑。 Microsoft：http://www.microsoft.com/security/portal/threat/encyclopedia/entry.aspx?Name=Backdoor:Win32/Zegost.DT
	Trojan.Infostealer.Boyapki.C 发现日期：2015 年 7 月 6 日	此威胁能够对所入侵的电脑进行恶意活动。(威胁等级较低) Symantec：http://www.symantec.com/security_response/writeup.jsp?docid=2015-070711-4915-99
	Trojan.Crisis 发现日期：2015 年 7 月 7 日	此威胁能够打开后门，窃取信息。(威胁等级较低) Symantec：http://www.symantec.com/security_response/writeup.jsp?docid=2015-070914-2954-99
	Backdoor:Win32/Fynloski.R 发现日期：2015 年 7 月 7 日	此威胁给予恶意黑客未授权的访问权限，控制用户电脑。 Microsoft：http://www.microsoft.com/security/portal/threat/encyclopedia/entry.aspx?Name=Backdoor:Win32/Fynloski.R
	TrojanDownloader:Win32/Nefhop.A 发现日期：2015 年 7 月 7 日	此威胁利用 JavaScript 漏洞检查用户电脑，寻找电脑信息用于未来的攻击中。 Microsoft：http://www.microsoft.com/security/portal/threat/encyclopedia/entry.aspx?Name=TrojanDownloader:Win32/Nefhop.A
	Trojan.Downloader.Crisis 发现日期：2015 年 7 月 8 日	此威胁下载潜在的恶意文件到所入侵的计算机。(威胁等级较低) Symantec：http://www.symantec.com/security_response/writeup.jsp?docid=2015-070914-3745-99
	Exploit:JS/Sevdaq 发现日期：2015 年 7 月 9 日	此威胁未经用户允许，下载、安装其他程序到用户电脑，包括恶意程序。 Microsoft：http://www.microsoft.com/security/portal/threat/encyclopedia/entry.aspx?Name=Exploit:JS/Sevdaq
	TrojanSpy:BAT/Ursnif.A 发现日期：2015 年 7 月 10 日	此威胁能够收集用户敏感信息，发送给恶意黑客。 Microsoft：http://www.microsoft.com/security/portal/threat/encyclopedia/entry.aspx?Name=TrojanSpy:BAT/Ursnif.A
	TrojanDownloader:Win32/Mytonel.B 发现日期：2015 年 7 月 10 日	此威胁未经用户允许，下载、安装其他程序到用户电脑，包括其他恶意程序。 Microsoft：http://www.microsoft.com/security/portal/threat/encyclopedia/entry.aspx?Name=TrojanDownloader:Win32/Mytonel.B

W32.XPAJ.B 感染分析

中国赛门铁克 yanliang / 文

Xpaj.B 是当前最复杂的感染式病毒之一，无论是分析、识别还是修复都十分的困难。这个两部分的文档将包含对该感染式样本的深入分析。

感染要点

Xpaj.B 只感染后缀名是 DLL,SYS,EXE 和 SCR 的文件，同时如果文件名的校验和在白名单中也不会对文件进行感染。如果文件中包含附加数据或文件是系统保护文件或文件的大小不大于 0x2800 都将不会被感染。而只有对应 cpu 型号是 interl i386 的 32 位 pe 文件才会被感染。只有在 xp 系统下，病毒才会感染系统文件；如果要感染的系统文件导入表中包含校验和为 0x36036a24、0xe742ea43、0x4b1ffe8e 的动态库名字，且被插入病毒数据的节名称不是“init”，也将不会被感染。

如果要感染一个文件，第一步将是选择一个要插入病毒各种数据的数据节。为了避免重复感染，将监测插入病毒数据的数据节最后一个 byte 的值是否小于 0xfc，否则不再感染。

当找到一个适当的节后，病毒将会从入口点所在的数据节中选取一些子函数，并将其函数代码存放到所选的数据节中；而后用病毒代码替换子函数的代码，被替换的病毒代码包含一个简易的基于堆栈的虚拟机，其主要功能为：获取 ZwProtectVirtualMemory 函数地址；调用该函数修改包含加密病毒代码的内存；通过虚拟机构造一段解密代码解密被加密的病毒代码；最后构造一段指令跳转到被解密的病毒代码去执行。

随机配置

确定被插入的数据节后，病毒将计算要插入数据的大小，用以调整被插入数据节的大小。病毒将遍历并解析被感染文件所有包含 rva 地址的结构表，诸如：导出表，资源表，重定位表等。如果被遍历到的 RVA 地址大于插入数据节的结尾地址，病毒将会对这些地址进行重定位，即加上插入数据的大小；如果需要，病毒还会对资源和入口点地址进行重定位。详情参见图 1。

```
mov     edi, [ebp+arg_8_inc_size_of_inserted_sec]
mov     eax, [ebp+arg_4_rva_end_of_inserted_sec]
lea     ecx, large ds:0Fh
mov     esi, [ebx+xpaj_info.va_pe_header]
lea     esi, [esi+S_PE_HEADER.export_table_RVA]

loop_fix_data_directories:      ; CODE XREF: sub_A7
cmp     [esi], eax
jb      next_directory
jmp     $+5
add     [esi], edi

next_directory:                 ; CODE XREF: sub_A7
lea     esi, [esi+8]
dec     ecx
jnz     loop_fix_data_directories
mov     esi, [ebx+xpaj_info.va_pe_header]
cmp     [esi+S_PE_HEADER.entry_point_RVA], eax
jb      retn
add     [esi+S_PE_HEADER.entry_point_RVA], edi

retn:                           ; CODE XREF: sub_A7
pop     esi
```

图 1 重定位资源和入口点地址

此后病毒将移动插入数据的数据节后面的数据，增加插入数据的数据节的大小，被增加的空间中将包括病毒代码，补丁结构表，虚拟机操作结构数组以及用以存放虚拟机构造的解密代码和跳转代码的空间。将这些数据写入被扩展的空间之前，病毒会先向其写入随即数据；写入的病毒数据在写入前可能会被变形，插入数据节中的病毒数据的内容分布参见图 2。

而补丁结构表，虚拟机操作指令结构数组会在写入病毒代码之后写入；包括病毒体，补丁结构表，虚拟机操作结构数组写入时都将会被加密，至于解密代码和跳转代码是在虚拟机被执行时，构造到该处

(下转第四版)

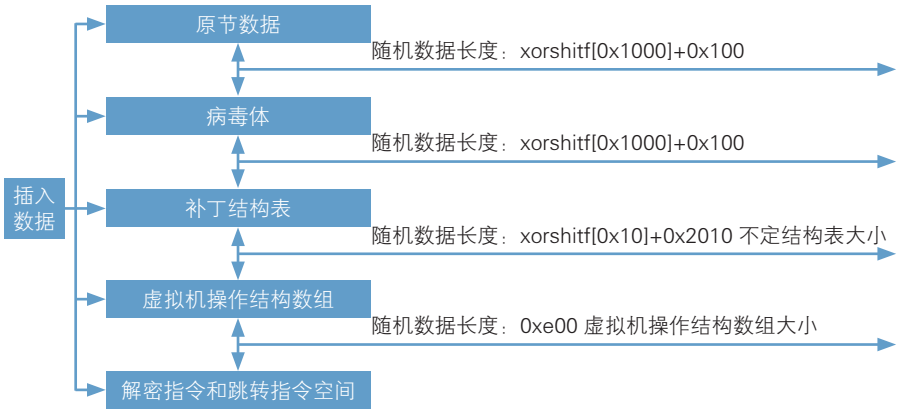

图 2 插入到数据节中的病毒数据的内容分布

```
DWORD xorshift(DWORD given_dword){
    DWORD seed;
    DWORD key_radix;
    DWORD keep_value2;
    DWORD keep_value3;
    DWORD xor_shift_key_array[3]; //it will use system time to update this array
seed=given_dword*100;
key_radix=(xor_shift_key_array[0] << 11)^xor_shift_key_array[0];
xor_shift_key_array[0]+=xor_shift_key_array[1];
keep_value2=xor_shift_key_array[2];
xor_shift_key_array[1]+=keep_value2;
keep_value3=xor_shift_key_array[3];
xor_shift_key_array[2]+=keep_value3;
xor_shift_key_array[3]=((((keep_value3>>19)^(keep_value3))^key_radix)^(key_radix>> 8));
return ((xor_shift_key_array[3]+keep_value2)%seed)/(100); }
```

图 3 异或变换操作

文件被页面手工提交发现，经由安全云鉴定器、智能学习鉴定器、动态行为 (默认环境) 鉴定器等鉴定分析。

依据动态行为鉴定器最终将文件判定为高级威胁。该文件具有以下行为：格式溢出、查找浏览器进程、获取系统版本、连接网络、获取 socket 本地名称、获取计算机名称、创建特定窗体、获取驱动器类型、获取系统内存、查找特定窗体、独占打开文件、请求加载驱动的权限、获取主机用户名称。

文件名	22f8adaaa9738665d1534371b2e16075f53f3f28450679594ba8d9aa169277f2
文件类型	Document/Microsoft.RTF[:Rich Text Format]
大小	416 KB
MD5	B8AD4939B4F938475C4E23C9CCF7353D
首次发现时间	2015-07-19 11:50
末次发现时间	2015-07-19 11:50
病毒类型	高级威胁
恶意判定 / 病毒名称	Exploit.rtf
判定依据	动态行为
下次鉴定时间	约 2 周

◆ 运行环境

操作系统	Windows xp 5.1.2600 Service Pack 3 Build 2600
内置软件	默认，ie6，ffice 2003，flash，wps，FoxitReader，adobe reader

◆ 危险行为

行为描述	格式溢出	
附加信息	ApplicationName	C:\WINDOWS\system32\verclsid.exe
	ApplicationName	C:\WINDOWS\system32\verclsid.exe
	ApplicationName	(null)
	ApplicationName	(null)
危险等级	★★★★	

完整报告可点击 http://antiy.pta.center/_lk/reports.html 下载。

(上接第三版)

的。最后病毒将修改 pe 头中的节信息和映像等信息。病毒通过变形的异或变换操作计算各短数据在扩展空间中的位置，以达到各段数据地址随机的目的。详细的异或变换操作参见三版图 3。

执行权限获取和数据解密

Xpaj.B 和其他简单的感染式病毒不同，并不是当被感染文件执行时劫持控制权来执行病毒；它通过从入口点所在的数据节中选定一定数量的子函数，当子函数的原始代码被复制到选定插入数据的数据节后，子函数地址下将会被覆盖病毒代码。由于这种方式并不能确保每次被感染文件被执行时都会被执行，病毒同时会随机修改一些其他的无关函数调用 call 指令地址使其指向病毒代码，以此来提高病毒代码被执行的几率。

为了找到一个可以被改写的子函数，病毒将获取入口点所在数据节的指令和子函数信息。通过反汇编器获得的这些信息主要用来判断子函数是否可以被改写以及可以改写的字节数。我分析的变种中，第二个被修改的子函数至少将覆盖 0x36 个字节，其他子函数覆盖的字节数也不会少于 0x24 个字节，同时改写的子函数的个数将不超过 10 个，也不会少于 2 个。被改写的子函数代码的总长度会在 0x186 和 0x28 之间。

同时病毒将保存被改写的原始数据到被扩大空间的数据节中；为防止文件被损坏被改写代码的重定位信息表也会被写入到这个数据节中。被改写的子函数和被重定位的函数中的重定位信息都将按照一定结构存储。

需要说明的是，被改写的子函数的原始代码拷贝到扩展的数据节后，将会在扩展节被执行。为了保证被移动后的代码在新的位置能够正确执行，那些调用了被移动地址数据的指令将会被重定位。

一旦改写函数被找到，一些无关的子函数也会被重定向到改写函数的起始地址，以期提高病毒代码的执行几率，与此同时，病毒也必须为重定位函数记录补丁结构表。

虚拟机要想被成功执行必须从第一个改写的子函数起始地址开始执行，当第一个改写函数或是重定位 call 指令被调用，虚拟机将开始工作，同时病毒获得执行权限。为了保证其他改写函数被调用时，虚拟机也能正确执行，除第一个被改写函数外，其他被改写函数的起始代码都是如下格式：

```
push ebp
push ebp,esp
push reg( 除 esp 和 ebp 外的所有寄存器 )
call 第一个改写子函数的地址
```

虚拟机的指令，将会被写到这些被改写函数的剩余空间中。而补丁结构表和病毒体代码都将会被加密后存放于扩展数据节中。

基于堆栈的多态虚拟机

病毒将会向被改写的子函数空间中写入一个基于堆栈的多态虚拟机。虚拟机代码具有高度的多态性，具体虚拟机的多态实现，将在下个月的第二部分报告中详细阐述。

参考文献

[1] Krysiuk, P. Xpaj.B-An Upper Crust File Infector. Symantec Security Response blog. http://www.symantec.com/connect/blogs/w32xpajbupper-crust-fi le-infector.