Windows操作系统中默认安装了各种各样的命令，但是真正被普通用户用到的其实只有其中的一小部分。而JPCERT/CC还发现攻击者在入侵到目标的网络当中时会使用Windows的命令来收集系统信息和传播恶意病毒。

这里值得注意的是被普通用户和攻击者所使用的Windows命令的差别，如果这两者之间有很大的差别，就有可能通过监测/控制Windows的命令执行来发现或者限制攻击者的行为。

本文中的这个项目将展示如何通过揭露攻击者在被入侵的Windows操作系统上所使用的Windows命令以及限制普通用户不必要的命令执行来减轻攻击所造成的影响。

恶意远程控制软件（Remote Access Tool/Trojan – RAT）通常都会有一个函数用来执行从远程环境接收到的命令，在这个函数的帮助下，攻击者能够在远程环境下在被控端执行任意Windows命令。

攻击者在网络中成功安装这样的恶意软件后，会按以下的顺序试图控制同网络当中的其他主机来收集机密的信息等。

（1）初步调查：收集被感染主机的信息。

（2）侦查：寻找保存在主机中的信息和搜索同网络下的其他主机。

（3）扩大感染：用其他的恶意软件感染主机或者试图访问其他主机。

在上述的所有阶段中都会用到Windows命令，下面我将对每个阶段用到的Windows命令进行介绍。

初步调查

表格1列举了攻击者尝试收集被感染主机的信息时所用到的命令。“Times executed”的统计来自于3个不同的攻击组织在他们的C&C服务器中用到的Windows命令的总和。

Table 1: 初步调查 (Top 10 commands)

Ranking	Command	Times executed
1	net	155

1	tasklist	155
2	ver	95
3	ipconfig	76
4	systeminfo	40
5	net time	31
6	netstat	27
7	whoami	22
8	net start	16
9	qprocess	15
10	query	14

攻击者利用诸如“tasklist”，“ver”，“ipconfig”和“systeminfo”等的命令来收集网络、进程、操作系统的信息来研究他们成功感染的主机是什么主机，这可能用来断定那个主机是不是用来进行病毒研究的沙盒等。

侦查

表格2中的命令经常被用来搜索机密信息和搜索同网络当中的其他主机

Table 2: Reconnaissance (Top 10 commands)

Ranking	Command	Times executed
1	dir	976
2	net view	236
3	ping	200
4	net use	194
5	type	120
6	net user	95
7	net localgroup	39
8	net group	20
9	net config	16
10	net share	11

攻击者用”dir”和”type”来搜索文件。有时他们会通过活用”dir”命令的参数来搜集被感染主机的一系列文件。

通过”net”命令来搜索网络数据，特别的，下面的命令经常被看到：

- net view: 显示指定的计算机共享的域、计算机或资源的列表
- net user: 管理 本地/域 账号
- net localgroup: 获得一个属于本地组的用户列表

· net localgroup: 获得一个属于本地组的用户列表

· net group: 获得一个属于特定域组的用户列表

· net use: 获取资源

此外，以下的命令可以在开启了Active Directory（参考表格5附录A）的环境中使用。这些命令被安装在Windows Server中，不存在于Windows7 和Windows8操作系统，但是攻击者可以手动安装并执行命令。

· dsquery: 在Active Directory中搜索账号

· csvde: 在Active Directory中获得账号的信息

扩大感染

为了入侵远程主机并且在网络中感染其他主机，下面的命令经常被使用：

Table 3: Spread of Infection

Ranking	Command	Times executed
1	at	103
2	reg	31
3	wmic	24
4	wusa	7
5	netsh advfirewall	4
6	sc	4
7	rundll32	2

*"wmic" is also used for reconnaissance.

“at”和”wmic”经常被用来在远程主机中执行恶意程序。

利用”at”命令，攻击者可以在远程主机上通过计划任务执行程序来连接主机：

```
at \\[remote host name or IP address] 12:00 cmd /c "C:\windows\temp\mal.exe"
```

同样的，通过“wmic”命令，攻击者也可以在远程主机上执行任意命令：

```
wmic /node:[IP address] /user:"[user name]" /password:"[password]" process call
```

限制不必要的Windows命令执行

公平的说这些黑客使用的Windows命令包含了很多普通用户不会用到的，通过应用能够限制这些命令执行的AppLocker（应用程序控制策略）和软件限制原则，是有可能限制黑客的攻击行为的。比如说，如

果你想限制”net”命令的使用，你可以设置如下的规则（更详细的AppLocker配置信息，请查阅Microsoft官网）。

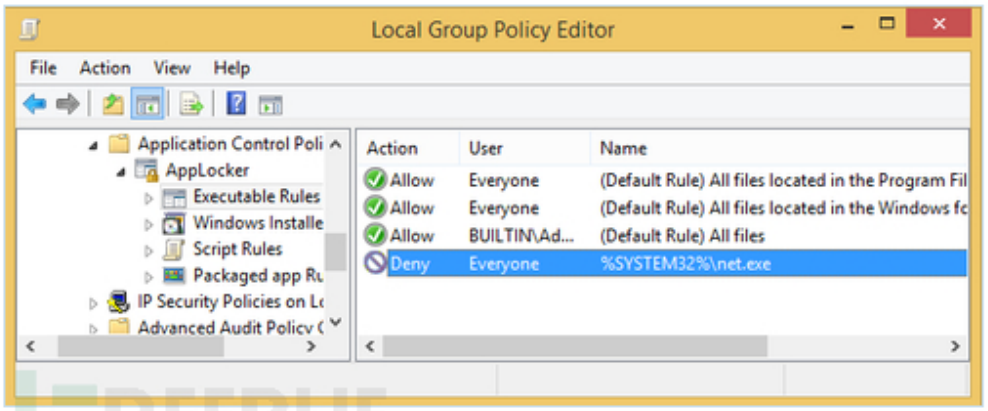

Figure 1: AppLocker Rules

同样的，通过启用AppLocker的事件记录功能，当Windows命令被执行或者尝试执行的命令被拒绝时会将该事件记录到日志中，这样有利于调查黑客到底在被感染的主机中执行了那些命令。

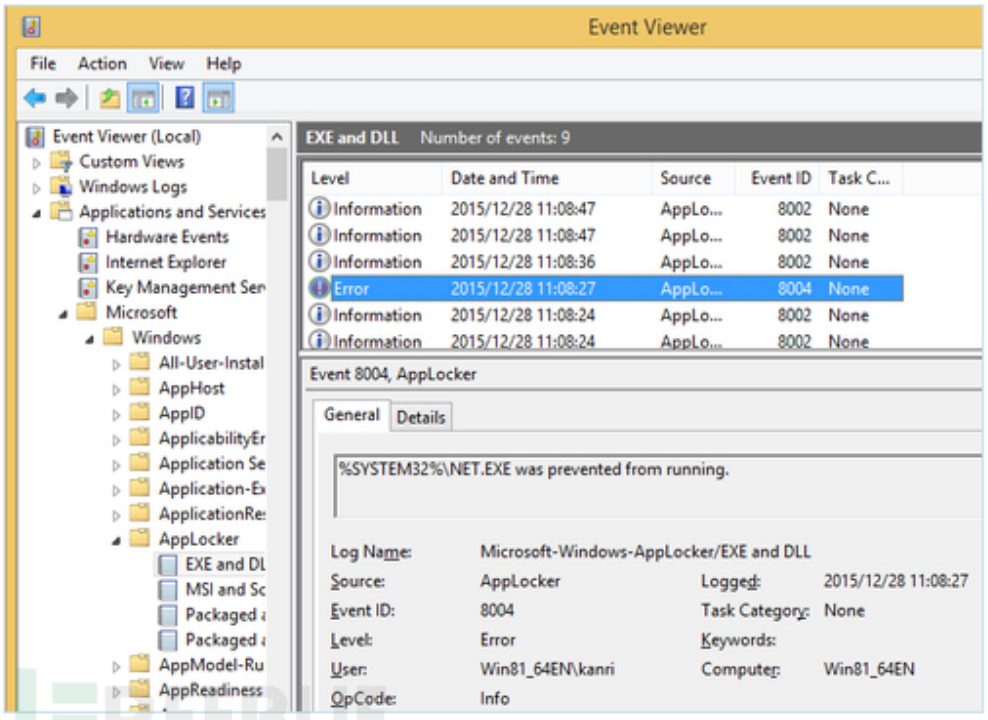

Figure 2: Logs of the Processes Restricted by AppLocker

AppLocker也可以用来监控Windows命令。AppLocker不能防止命令被执行，但执行的历史会被记录在事件日志中。如果用户自己要使用的Windows命令也经常被攻击者使用，将AppLocker设置为监控目的是一个很好的选择。

总结

针对目标进行攻击时，攻击者为了实现他们的目的不仅会使用恶意软件还经常使用Windows命令。如果这样的行为能被发现，那么就可以在它传播的早期就将其拦截。但是，通过限制Windows的命令是很难实现的，所以我们的建议是通过AppLocker等收集软件执行过程中的日志。

Appendix A

Table 4: Initial Investigation (Attack Group A)

Ranking	Command	Times executed	Option
1	tasklist	119	/s /v
2	ver	92	
3	ipconfig	58	/all
4	net time	30	
5	systeminfo	24	
6	netstat	22	-ano
7	qprocess	15	
8	query	14	user
9	whoami	14	/all
10	net start	10	
11	nslookup	4	
12	fsutil	3	fsinfo drives
13	time	2	/t
14	set	1	

Table 5: Reconnaissance (Attack Group A)

Ranking	Command	Times executed	Option
1	dir	903	
2	net view	226	
3	ping	196	
4	net use	193	
5	type	118	
6	net user	74	

7	net localgroup	35	
8	net group	19	
9	net config	16	
10	net share	11	
11	dsquery	6	
12	csvde	5	/f /q
13	nbtstat	5	-a
14	net session	3	
15	nltest	3	/dclist
16	wevtutil	2	

Table 6: Spread of Infection (Attack Group A)

Ranking	Command	Times executed	Option
1	at	98	
2	reg	29	add export query
3	wmic	24	
4	netsh advfirewall	4	
5	sc	4	qc query
6	wusa	2	

Appendix B

Table 7: Initial Investigation (Attack Group B)

Ranking	Command	Times executed	Option
1	tasklist	29	/m /svc
2	whoami	6	
3	ipconfig	5	/all
4	net start	4	
5	netstat	3	-ano
6	nslookup	3	
7	ver	2	
8	time	1	/t

Table 8: Reconnaissance (Attack Group B)

Ranking	Command	Times executed	Option
1	dir	62	
2	net user	21	/domain /add
3	net view	9	/domain
4	ping	4	
5	net localgroup	4	/add
6	tree	3	/F
7	type	2	
8	net group	1	/domain

Table 9: Spread of Infection (Attack Group B)

Ranking	Command	Times executed	Option
1	at	5	
2	wusa	5	
3	reg	2	
4	rundll32	2	

Appendix C

Table 10: Initial Investigation (Attack Group C)

Ranking	Command	Times executed	Option
1	systeminfo	16	
2	ipconfig	13	/all /?
3	tasklist	7	
4	netstat	5	-ano
5	whoami	2	
6	net start	2	
7	arp	1	-a
8	chcp	1	
9	net time	1	
10	ver	1	

10	ver	1	

Table 11: Reconnaissance (Attack Group C)

Ranking	Command	Times executed	Option
1	dir	11	
2	net user	1	/all /?
3	net view	1	
4	qwinsta	1	-ano

*