Windows Commands Abused by Attackers - JPCERT/CC Eyes

By 朝長 秀誠 (Shusei Tomonaga)

Published: 2016-01-25 · Archived: 2026-04-05 15:15:57 UTC

- Report

Hello again, this is Shusei Tomonaga from the Analysis Center.

In Windows OS, various commands (hereafter “Windows commands”) are installed by default. However, what is actually used by general users is just a small part of it. On the other hand, JPCERT/CC has observed that attackers intruding into a network also use Windows commands in order to collect information and/or to spread malware infection within the network. What is worth noting here is the gap between those Window commands used by general users and by attackers. If there is a huge difference, it would be possible to detect or limit the attackers’ behaviour by monitoring/controlling the Windows command execution.

This entry will demonstrate how to mitigate the attack impact by revealing Windows commands that attackers use on the intruded Windows OS, and by restricting the execution of those commands that are unnecessary for general users.

Malware for remote control (Remote Access Tool/Trojan – RAT) has a function to execute shell commands from a remote environment. With this, attackers can execute Windows commands from a remote environment.

Attackers who successfully installed such malware in a network will attempt to take control of the system within the network in the following sequence in order to collect confidential information, etc.

1. Initial investigation: Collect information of the infected machine
2. Reconnaissance: Look for information saved in the machine and remote machines within the network
3. Spread of infection: Infect the machine with other malware or try to access other machines

Windows commands are used in all of the phases above. Respective Windows commands used in each phase are introduced here below.

Initial Investigation

Table 1 lists the commands that are often used by attackers in an attempt to collect information of the infected machine. “Times executed” is derived from the sum of Windows commands used by 3 different attack groups in their respective C&C servers (Please refer to Appendix A, B and C for details).

Table 1: Initial Investigation (Top 10 commands)

Ranking	Command	Times executed
1	tasklist	155

Ranking	Command	Times executed
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

Attackers use commands such as “tasklist”, “ver”, “ipconfig” and “systeminfo”, etc., and collect information of the network, process and OS in order to investigate what kind of machine they succeeded in infecting. This is presumably how they make sure that the machine is not a sandbox for malware analysis purposes and so on.

Reconnaissance

Commands shown in Table 2 are often used to search for confidential information and remote machines within the network.

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

Ranking	Command	Times executed
10	net share	11

Attackers use “dir” and “type” to search for files. Sometimes they collect a list of all the document files in the infected machine by setting appropriate options and arguments for “dir” command.

For searching networks, “net” is used. In particular, the following commands are often seen:

- net view: Obtain a list of connectable domain resources
- net user: Manage local/domain accounts
- net localgroup: Obtain a list of users belonging to local groups
- net group: Obtain a list of users belonging to certain domain groups
- net use: Access to resources

Furthermore, the following commands may be used in an environment where Active Directory is used (Please refer to Table 5 in Appendix A). These commands are installed in Windows Server and do not originally exist in client OS such as Windows 7 and 8.1 – but attackers download and install these commands from outside and execute them.

- dsquery: Search for accounts in Active Directory
- csvde: Obtain account information in Active Directory

Spread of Infection

To intrude remote machines and spread malware infection within the network, the following commands are often executed:

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” and “wmic” are often used to execute malware on remote machines.

With “at” command, attackers can execute commands on remote machines, by registering tasks to execute files against connectable machines as follows.

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

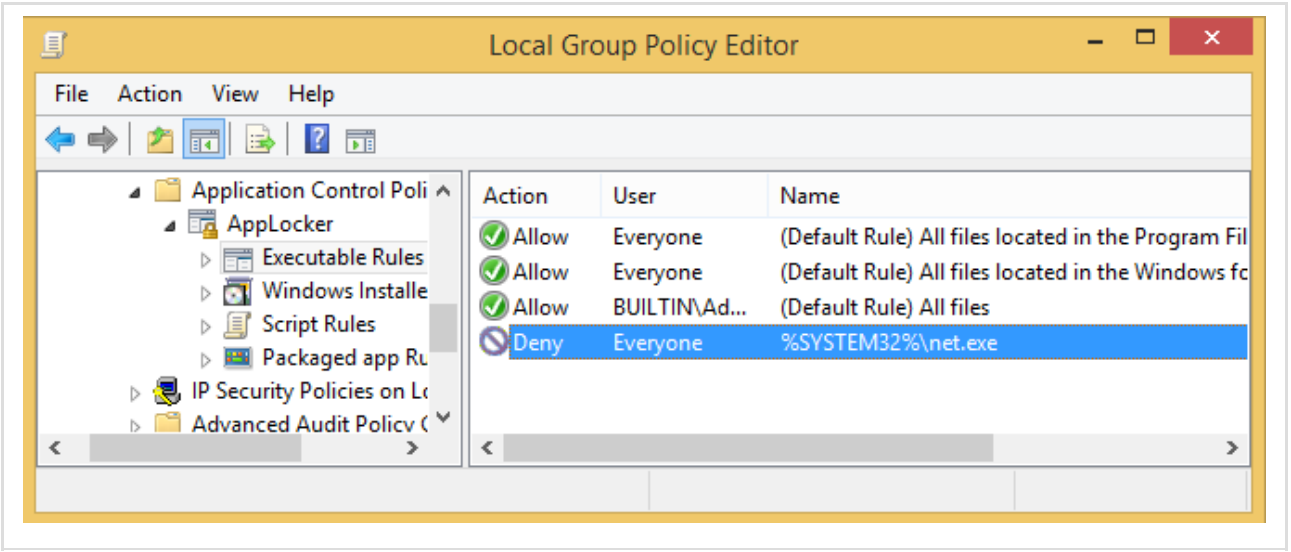
Also, by setting the following options and arguments with “wmic” command, attackers can execute commands on remote machines.

```
wmic /node:[IP address] /user:”[user name]” /password:”[password]” process call create “cmd /c c:\Windows\Syste
```

Restricting Execution of Unnecessary Windows Commands

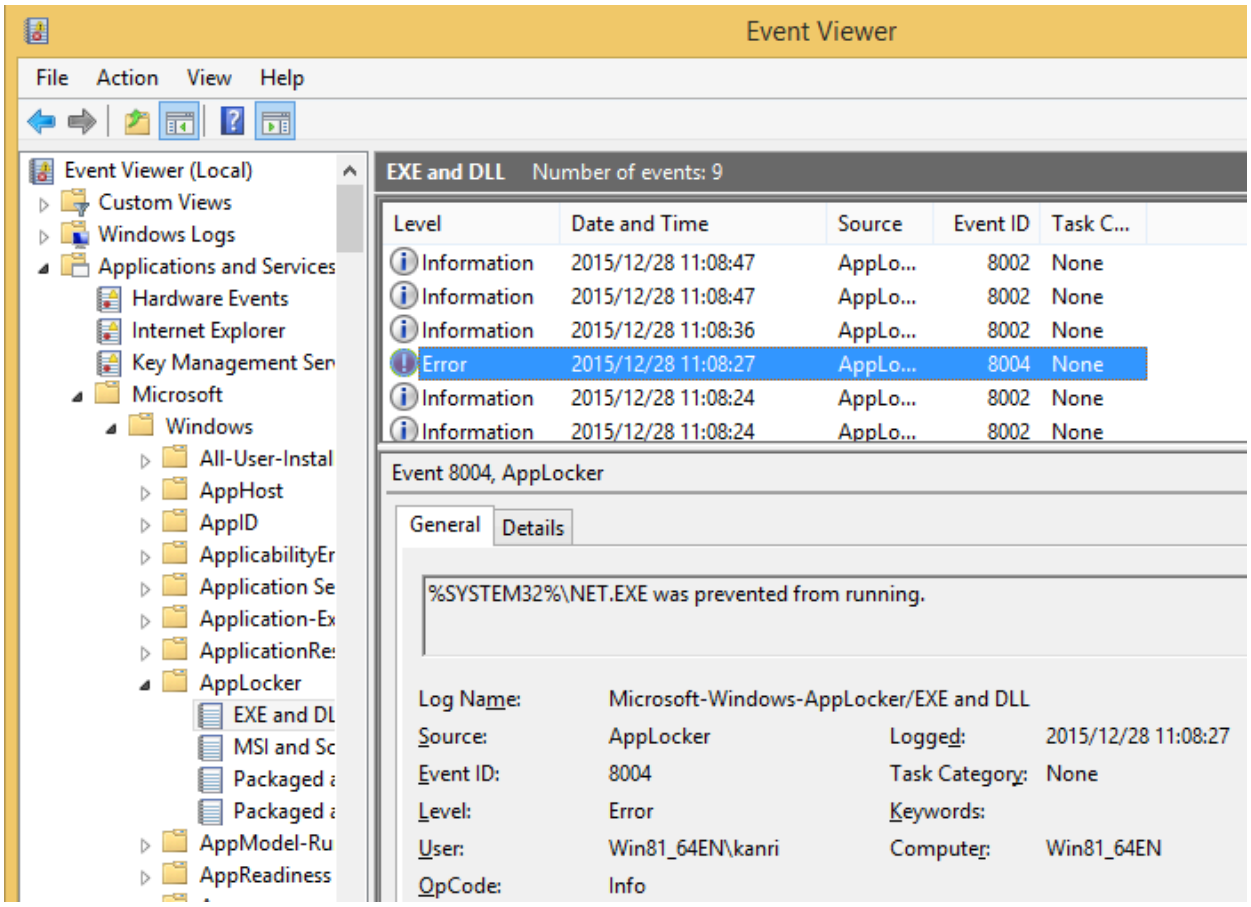
It is fair to say that these Windows commands used by attackers include those that are unused by general users, if carefully selected. With AppLocker and software restriction policy, which restrict such commands from being executed, it would be possible to limit the attackers’ behaviour. For example, if you wish to restrict “net” commands, you can set rules as in Figure 1. (For details of AppLocker configuration, please see Microsoft’s Website [1]).

Figure 1: AppLocker Rules



Also, by enabling AppLocker, events where selected Windows commands were executed or attempted but denied will be recorded in the event logs, which can be utilized for investigation on Windows commands that attackers executed after infecting the machine with malware.

Figure 2: Logs of the Processes Restricted by AppLocker



AppLocker can also just monitor Windows commands [2]. With this, AppLocker cannot prevent unintended Windows commands from being executed, but the execution history will be recorded in the event log. If the users themselves use Windows commands that may be used for attacks, it is a good idea to set AppLocker just for monitoring purpose. (Windows command execution can also be monitored by activating “Audit Process Creation” in the local security policy.)

Conclusion

In targeted attacks, attackers not only use functions implemented in the malware, but also often use Windows commands to pursue their purposes. If such activities can be hindered, spread of incidents can be prevented in a fairly early stage. However, it may be difficult to limit the usage of Windows commands right away – so our recommendation is to start by collecting logs of executed processes by using AppLocker, etc.

Thank you for reading and best wishes for the New Year!

- Shusei Tomonaga

Reference:

> [1] Microsoft - Windows AppLocker
> https://technet.microsoft.com/en-us/library/dd759117.aspx

> [2] Microsoft – Using Auditing to Track Which Applications Are Used
>
> https://technet.microsoft.com/en-us/library/dd723693%28v=ws.10%29.aspx

Appendix A: List of Executed Commands by respective Attack Groups (Attack Group 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	

Ranking	Command	Times executed	Option
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: List of Executed Commands by respective Attack Groups (Attack Group 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

Ranking	Command	Times executed	Option
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: List of Executed Commands by respective Attack Groups (Attack Group C)

Table 10: Initial Investigation (Attack Group C)

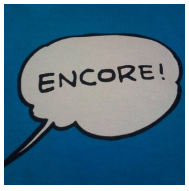
Ranking	Command	Times executed	Option
1	systeminfo	16	
2	ipconfig	13	/all /?
3	tasklist	7	
4	netstat	5	-ano

Ranking	Command	Times executed	Option
5	whoami	2	
6	net start	2	
7	arp	1	-a
8	chcp	1	
9	net time	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

*Commands for “Spread of Infection” by Attack Group C are omitted since they did not spread the infection.

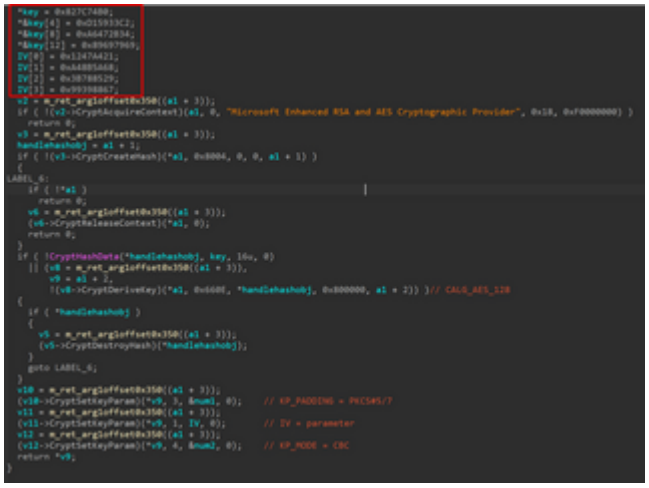


朝長 秀誠 (Shusei Tomonaga)

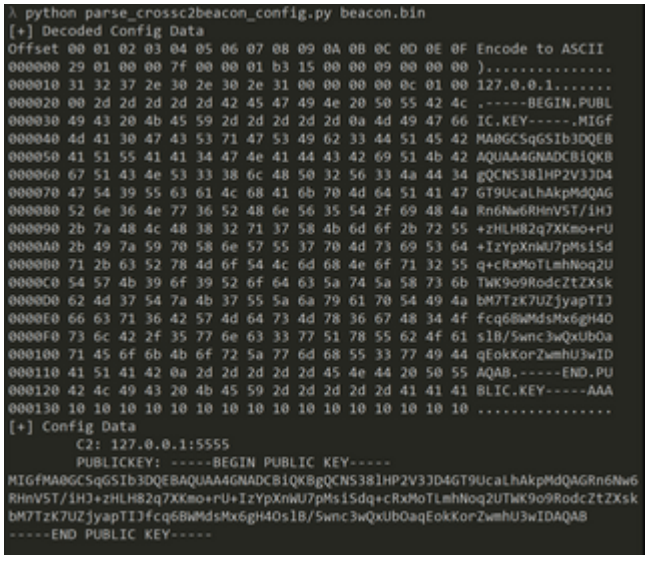
Since December 2012, he has been engaged in malware analysis and forensics investigation, and is especially involved in analyzing incidents of targeted attacks. Prior to joining JPCERT/CC, he was engaged in security monitoring and analysis operations at a foreign-affiliated IT vendor. He presented at CODE BLUE, BsidesLV, BlackHat USA Arsenal, Botconf, PacSec and FIRST Conference. JSAC organizer.

Related articles

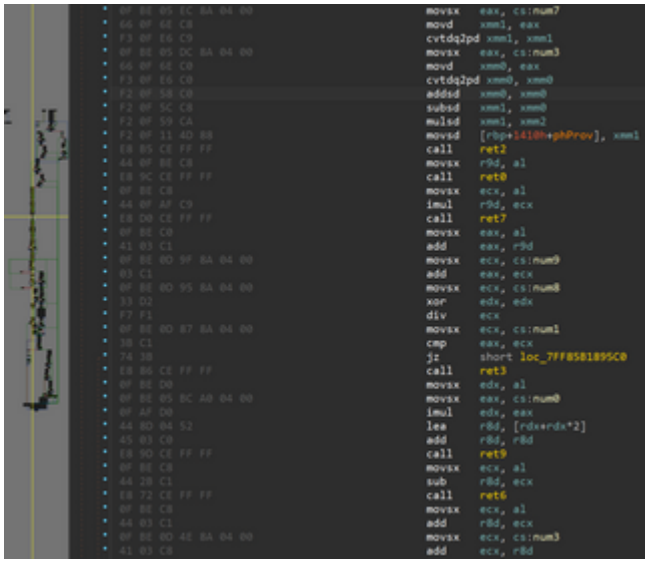
[Multiple Threat Actors Rapidly Exploit React2Shell: A Case Study of Active Compromise]

- 

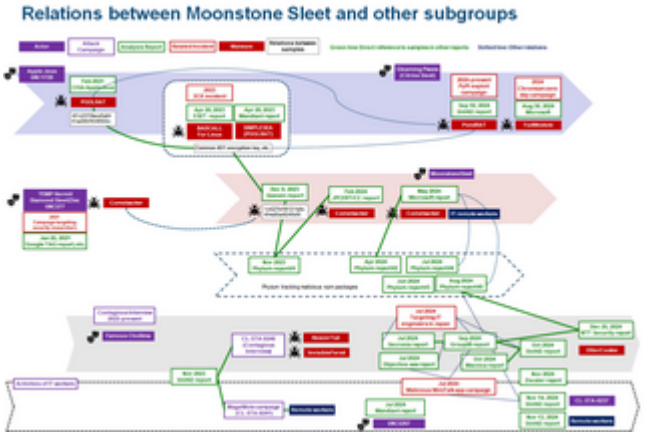
[Update on Attacks by Threat Group APT-C-60]

- 

[CrossC2 Expanding Cobalt Strike Beacon to Cross-Platform Attacks]

- 

[Malware Identified in Attacks Exploiting Ivanti Connect Secure Vulnerabilities]

- 

[Tempted to Classifying APT Actors: Practical Challenges of Attribution in the Case of Lazarus's Subgroup]

Source: https://blogs.jpcert.or.jp/en/2016/01/windows-commands-abused-by-attackers.html