



Shadow Force

A Technical Brief



TrendLabs Security Intelligence Blog

Dove Chiu

September 2015

Contents

Introduction.....	3
Threat Details	3
fileh.exe (file handle toolkit).....	3
latinfect.exe/iatinfect64.exe	5
aio.exe (all-in-one hacking toolkit).....	8
ss.exe (TCP port scan tool).....	12
su.exe (service utility).....	13
C&C Information	13
Attacker Profile	14
Connecting the Dots	14
Conclusion.....	16

TREND MICRO LEGAL DISCLAIMER

The information provided herein is for general information and educational purposes only. It is not intended and should not be construed to constitute legal advice. The information contained herein may not be applicable to all situations and may not reflect the most current situation. Nothing contained herein should be relied on or acted upon without the benefit of legal advice based on the particular facts and circumstances presented and nothing herein should be construed otherwise. Trend Micro reserves the right to modify the contents of this document at any time without prior notice.

Translations of any material into other languages are intended solely as a convenience. Translation accuracy is not guaranteed nor implied. If any questions arise related to the accuracy of a translation, please refer to the original language official version of the document. Any discrepancies or differences created in the translation are not binding and have no legal effect for compliance or enforcement purposes.

Although Trend Micro uses reasonable efforts to include accurate and up-to-date information herein, Trend Micro makes no warranties or representations of any kind as to its accuracy, currency, or completeness. You agree that access to and use of and reliance on this document and the content thereof is at your own risk. Trend Micro disclaims all warranties of any kind, express or implied. Neither Trend Micro nor any party involved in creating, producing, or delivering this document shall be liable for any consequence, loss, or damage, including direct, indirect, special, consequential, loss of business profits, or special damages, whatsoever arising out of access to, use of, or inability to use, or in connection with the use of this document, or any errors or omissions in the content thereof. Use of this information constitutes acceptance for use in an "as is" condition.

Introduction

We found a new backdoor attack named Shadow Force. Shadow Force uses a rarely seen system-level DLL hijacking technique to load the backdoor and abuse a driver in the Wireshark network packet analyzer in order to utilize the ring 0 port-reuse technique to hide the backdoor's communication. The person behind Shadow Force comes from China, possibly self-employed. Based on our analysis, the backdoor is being used to target a media agency in South Korea.

Threat Details

Tools of the Trade

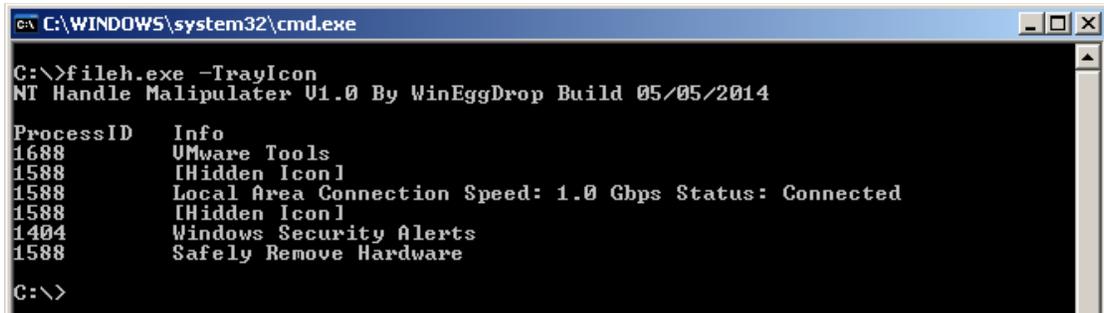
Based on our investigation, the attacker uses the tools mentioned below to perform the attack.

1. fileh.exe (file handle toolkit)

This tool tries to utilize file handles to perform tasks. Below is a list of all of its functions:

- -StopShutDown - prevents the computer from shutting down
- -ListFile - attempts to enumerate all files currently open
- -CheckModules [PID] - lists the running modules (DLLs) with their signature name
- -ListProcess - lists all the running processes with their full path
- -fport - lists a process and its port mapping
- -mport - lists a process and its port mapping, like fport, but this utility supports Windows 2000
- -CheckLoader - checks for some common Windows services and looks for suspicious DLLs
- -CheckAllLoader - checks all Windows services and looks for suspicious DLLs
- -GetService [ServiceName] - lists running services and corresponding PIDs

- -TrayIcon - lists everything in the system tray or systray. An attacker can use this function to check if the target computer has any anti-malware protection



```

C:\WINDOWS\system32\cmd.exe
C:\>fileh.exe -TrayIcon
NT Handle Malipulator V1.0 By WinEggDrop Build 05/05/2014

ProcessID   Info
1688        VMware Tools
1588        [Hidden Icon]
1588        Local Area Connection Speed: 1.0 Gbps Status: Connected
1588        [Hidden Icon]
1404        Windows Security Alerts
1588        Safely Remove Hardware

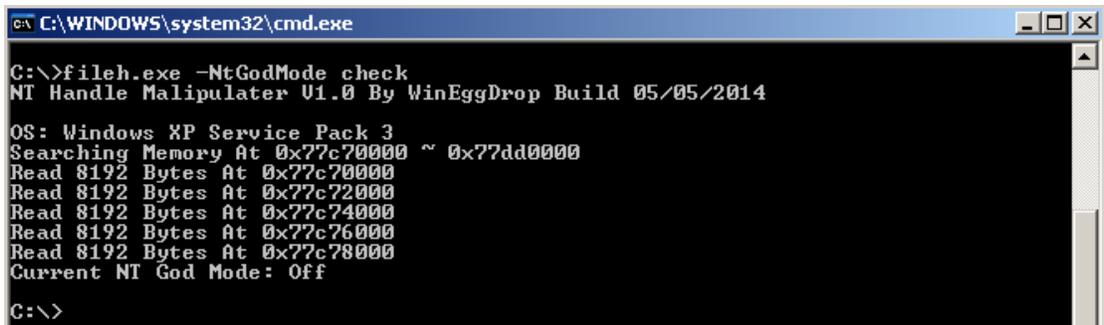
C:\>

```

Figure 1. *fileh.exe* to list all tray icon information

There is also an operating mode called *NtGodMode* that's associated with the utility.

- -NtGodMode <On|Off|Check> - when NtGodMode is on, any password can log in to the target computer. An attacker can use this function to login without creating any account or backdoor. This function cannot be used on computers running on Windows 7 or Windows 8



```

C:\WINDOWS\system32\cmd.exe
C:\>fileh.exe -NtGodMode check
NT Handle Malipulator V1.0 By WinEggDrop Build 05/05/2014

OS: Windows XP Service Pack 3
Searching Memory At 0x77c70000 ~ 0x77dd0000
Read 8192 Bytes At 0x77c72000
Read 8192 Bytes At 0x77c72000
Read 8192 Bytes At 0x77c74000
Read 8192 Bytes At 0x77c76000
Read 8192 Bytes At 0x77c78000
Current NT God Mode: Off

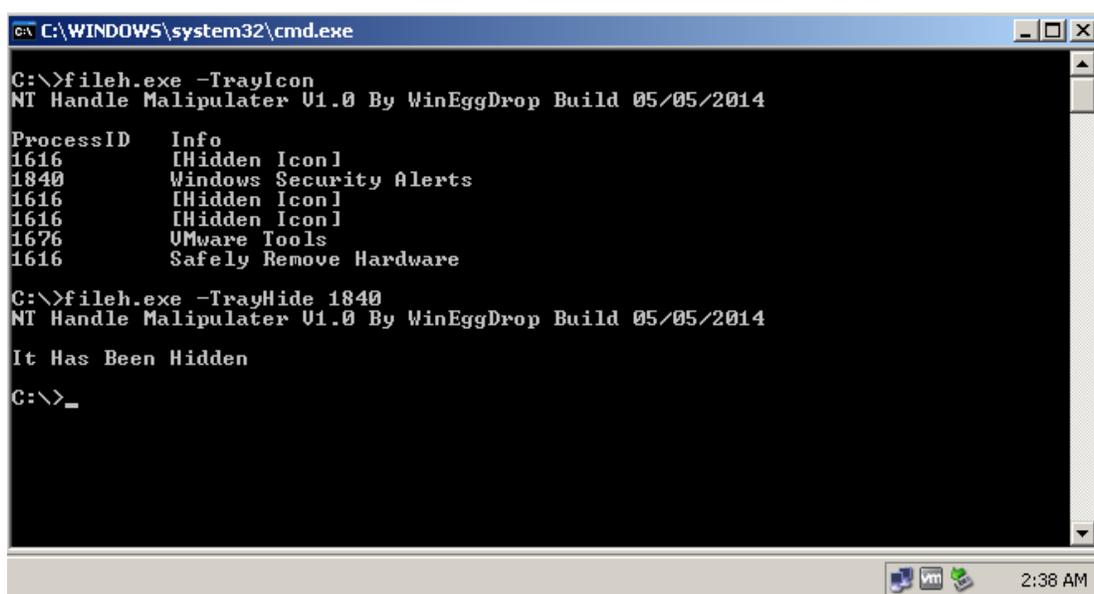
C:\>

```

Figure 2. *fileh.exe* to check NtGodMode

- -FV <File> - checks for the version information of the specified file
- -SetDLL <name> - sets the specified service name to the default DLL name
- -UnlockFile <file> - unlocks the file, in order to delete, move, or rename file safely
- -LockFile <file> - locks the file, so that users cannot easily modify it
- -FreeDLL <name> - frees the specified DLL name in all processes

- -FindDLL <name> - finds the specified DLL name in all processes
- -KillProcess <PID> - kills the specified process ID
- -ListModules <PID> - lists all of the modules loaded by the specified process ID
- -KillIceSword <PID> - kills the IceSword software by process ID
- -PCL <PID> - gets the program command line by the specified process ID
- -TrayHide <PID> - hides the specified tray icon. You can use TrayIcon to get PID. The following pictures showed how easy to hide windows security alerts icon
- -TrayShow <PID> - shows the specified tray icon, you can use -TrayIcon to get PID



```
C:\WINDOWS\system32\cmd.exe

C:\>fileh.exe -TrayIcon
NT Handle Malipulator V1.0 By WinEggDrop Build 05/05/2014

ProcessID  Info
1616       [Hidden Icon]
1840       Windows Security Alerts
1616       [Hidden Icon]
1616       [Hidden Icon]
1676       VMware Tools
1616       Safely Remove Hardware

C:\>fileh.exe -TrayHide 1840
NT Handle Malipulator V1.0 By WinEggDrop Build 05/05/2014

It Has Been Hidden

C:\>_
```

Figure 3. *fileh.exe* to hide tray icon

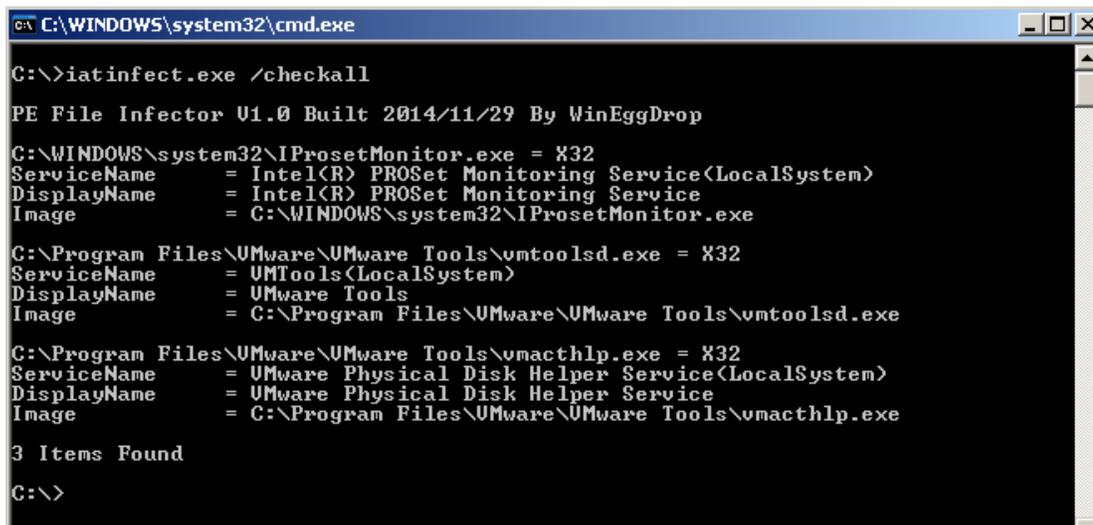
Note that the attacker can use this tool to hide icons of security-related software and even crash these software to bypass detection.

2. *latinfect.exe*/*iatinfect64.exe*

This tool modifies the import address table (IAT) in the executable file in order to load additional DLLs. This technique bypasses some behavior monitoring

software or autorun files, making it difficult to find malware in the live environment. We already found [several related incidents](#), and this time we found the tool that makes this possible.

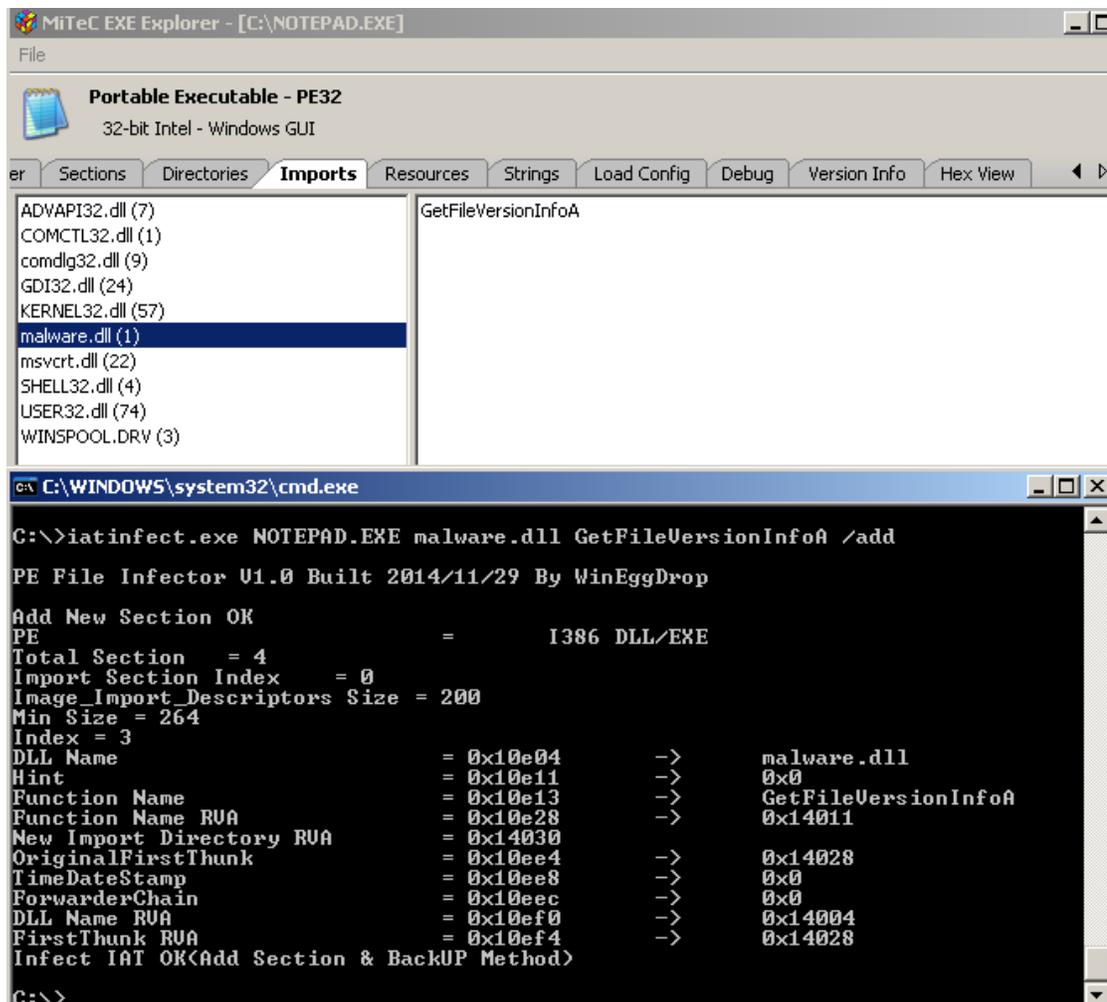
The flags `/checkall` or `/checkalldll` will list candidate targets automatically. The attacker can use this tool to easily select a target.



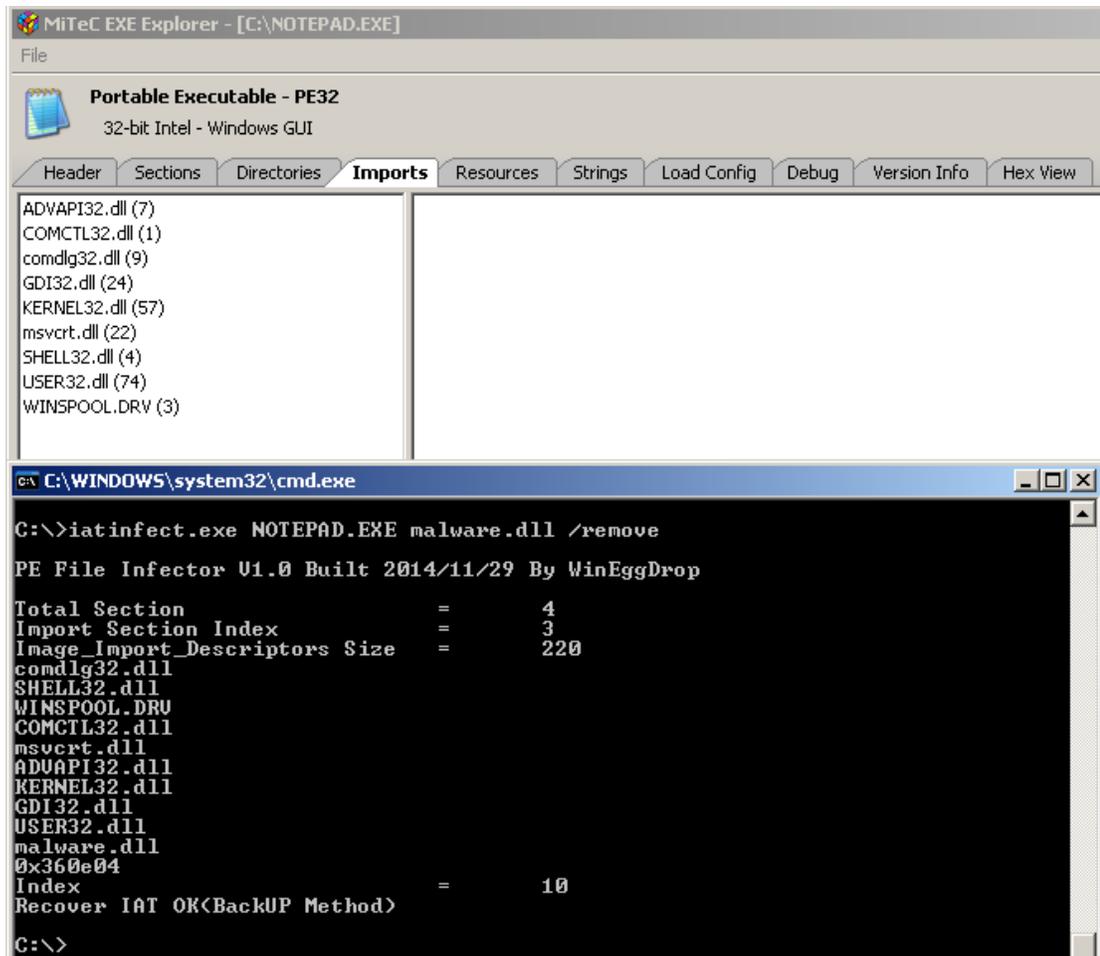
```
C:\WINDOWS\system32\cmd.exe
C:\>iatinfect.exe /checkall
PE File Infector 01.0 Built 2014/11/29 By WinEggDrop
C:\WINDOWS\system32\IProsetMonitor.exe = X32
ServiceName      = Intel(R) PROSet Monitoring Service(LocalSystem)
DisplayName      = Intel(R) PROSet Monitoring Service
Image            = C:\WINDOWS\system32\IProsetMonitor.exe
C:\Program Files\VMware\VMware Tools\vmtoolsd.exe = X32
ServiceName      = VMTools(LocalSystem)
DisplayName      = VMware Tools
Image            = C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
C:\Program Files\VMware\VMware Tools\vmacthlp.exe = X32
ServiceName      = VMware Physical Disk Helper Service(LocalSystem)
DisplayName      = VMware Physical Disk Helper Service
Image            = C:\Program Files\VMware\VMware Tools\vmacthlp.exe
3 Items Found
C:\>
```

Figure 4. The utility lets a hacker search for candidate automatic start targets

The utility can load a new DLL or replace an existing DLL with a malicious one in its place. The image below shows the ease in adding the *malware.dll* into *notepad.exe* by modifying its import address table. After being modified, *notepad.exe* will load *malware.dll* once executed.

Figure 5. Adding *malware.dll* to *notepad.exe*

The hacker can simply recover the changes by using the */remove* parameter.

Figure 6. Removing *malware.dll* from *notepad.exe*

3. aio.exe (all-in-one hacking toolkit)

The tool *aio.exe* is a miniature version of the all-in-one hacking toolkit. The screenshot below shows the full function list of this version.

```

C:\WINDOWS\system32\cmd.exe

C:\>aio.exe
Mini Uersion Without Scan Feature U1.0 Build 11/11/2013

aio.exe      -AutoRun          -> List Auto Run Items
aio.exe      -Clone            -> Clone Accounts
aio.exe      -CheckClone       -> Check Clone
aio.exe      -CleanLog         -> Clean Logs
aio.exe      -ConfigService    -> Configure Service
aio.exe      -CheckProcess     -> Check Hidden Process
aio.exe      -CheckUser        -> Check Users
aio.exe      -DelUser          -> Delete User
aio.exe      -DelAdmin         -> Delete User
aio.exe      -DWF              -> Disable WFP For A File
aio.exe      -EnumService      -> List Services
aio.exe      -FHS              -> Find Hidden Service
aio.exe      -FGet            -> FTP Download
aio.exe      -FTPUpload        -> FTP Upload
aio.exe      -FindPassword     -> Find Logon User Password
aio.exe      -FileTime         -> Change File Time
aio.exe      -InstallService   -> Install Service
aio.exe      -InstallDriver    -> Install Driver
aio.exe      -KillHProcess     -> Kill Hidden Process
aio.exe      -LogOff           -> LogOff System
aio.exe      -MGet            -> Web Download
aio.exe      -Mport           -> Port Mapper
aio.exe      -Never           -> Reset Account Number Of Logon
aio.exe      -PowerOff         -> Shut Down The Power
aio.exe      -Pslist          -> List Process Info
aio.exe      -Pskill          -> Kill Process
aio.exe      -Reboot          -> Reboot The System
aio.exe      -RemoveService    -> Remove Service
aio.exe      -RHService        -> Remove Hide Service
aio.exe      -StartService     -> Start Service
aio.exe      -StopService      -> Stop Service
aio.exe      -SysInfo         -> List System Info
aio.exe      -ShutDown        -> ShutDown The System
aio.exe      -SPskill         -> Special Method To Kill Process
aio.exe      -Terminal         -> Install Terminal Service
aio.exe      -Unhide          -> Unhide Password
aio.exe      -WinInfo         -> List Accounts Info

C:\>

```

Figure 7. All-in-one toolkit functions

As you can see, some of its functions are very interesting:

- -Clone - A shadow account is a hidden account exists in the local accounts. Creating a shadow account will require an existing account, so this is named "clone"
- -CleanLog - cleans Windows event logs including application/security/system events and schedule log files. This makes real-time incident response more difficult

```

C:\WINDOWS\system32\cmd.exe
C:\>aio.exe -CleanLog
Mini Version Without Scan Feature V1.0 Build 11/11/2013
Cleaning Event Logs.....
Clean Application Event Log Successfully
Clean Security Event Log Successfully
Clean System Event Log Successfully
-----
Backing Up Services Status..... Done
-----
Stopping Services.....
The Service "MSFTPSUC" Doesn't Exist
The Service "SMTPSUC" Doesn't Exist
The Service "W3SUC" Doesn't Exist
Stopping The Service "SCHEDULE".....
-----
Found No Log Files
-----
Deleting Schedule Event Log File.....
Delete C:\WINDOWS\SchedLgU.txt Successfully
-----
Restoring Services Status.....
Starting Service "SCHEDULE"
-----
Mission Accomplished
C:\>

```

Figure 8. CleanLog utility from *aio.exe*

- -CheckProcess - checks for hidden processes
- -CheckUser - checks for users currently logged in
- -DWFP - WFP stands for Windows File Protection. If WFP is enabled, users cannot modify files easily and Windows will automatically revert any modified files back to default ones. This function can disable WFP for specific files

```

C:\WINDOWS\system32\cmd.exe
C:\>aio.exe -DWFP C:\WINDOWS\system32\sethc.exe
Mini Version Without Scan Feature V1.0 Build 11/11/2013
File "C:\WINDOWS\system32\sethc.exe" Protection Has Been Disabled
C:\>

```

Figure 9. Disabling WFP for Windows system files

- -FindPassword - This recovers the system login password hashes in memory. This may not work every time, and the password may not be recoverable in newer Windows systems

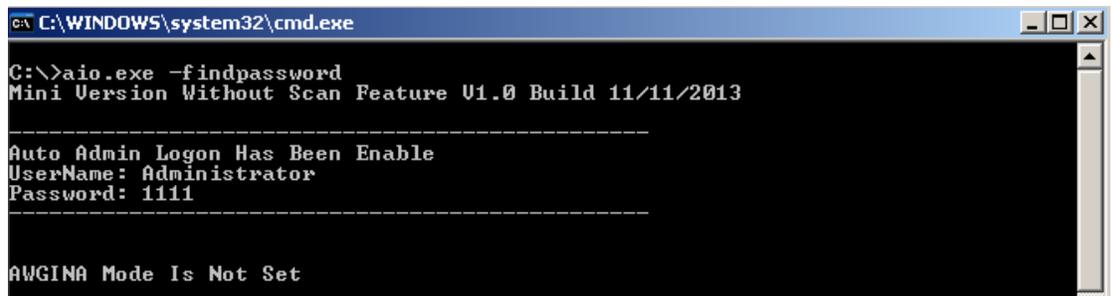


Figure 10. Finding passwords in memory by aio.exe

- -FileTime - changes the timestamps of the file. This is useful against forensics, because the timeline may not reliable
- -Never - resets account login time to "never"

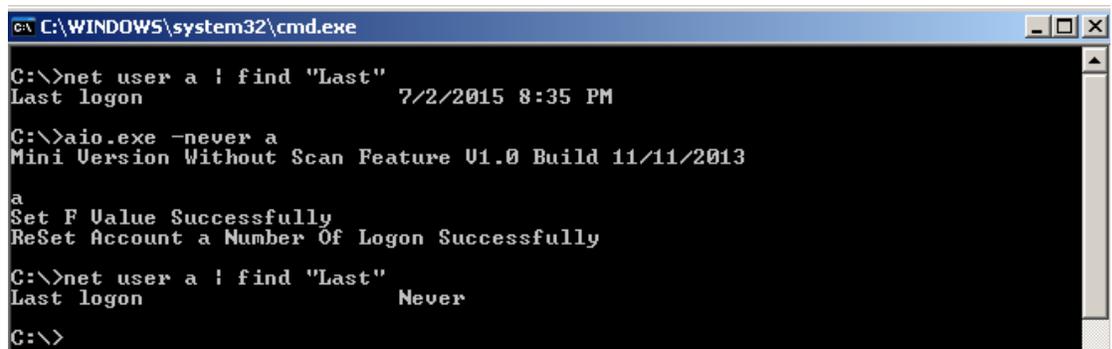


Figure 11. Reset last login time with "never"

- -Unhide - searches for password input box in memory and disable hiding mode to that input box

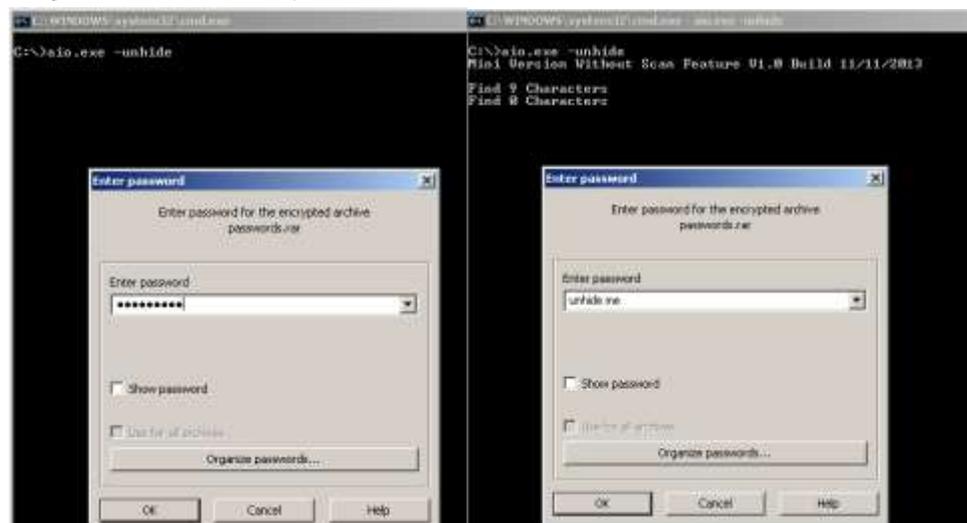


Figure 12. Before (L) and after (R) applying the "unhide" utility

4. ss.exe (TCP port scan tool)

The file *ss.exe* is actually an executable .RAR file. Several executable files are made available once *ss.exe* is decompressed.

Name	Size	Packed	Type	Modified	CRC32
..			File Folder		
1.vbs	95	95	VBScript Script File	5/4/2014 1:22 PM	56D157FD
123.bat	348	167	MS-DOS Batch File	5/4/2014 1:21 PM	0A95E5AD
kr.txt	43,282	7,391	Text Document	5/19/2014 2:00...	37795C74
s.exe	7,884	7,078	Application	4/7/2014 1:53 PM	C827C794
TCP.BAT	11	11	MS-DOS Batch File	5/4/2014 1:22 PM	5B142682

Figure 13. Files in the *ss.exe* compressed file

When *ss.exe* is executed, it extracts all files, executes *TCP.BAT*, and starts the whole execution chain.

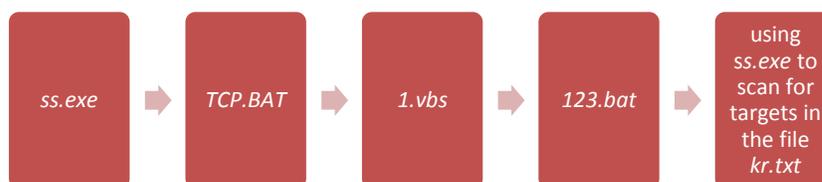


Figure 14. *ss.exe* execution chain

The attacker uses many indirect calls to avoid behavior detection. The final batch file *123.bat* contains the actual commands to be executed.

```

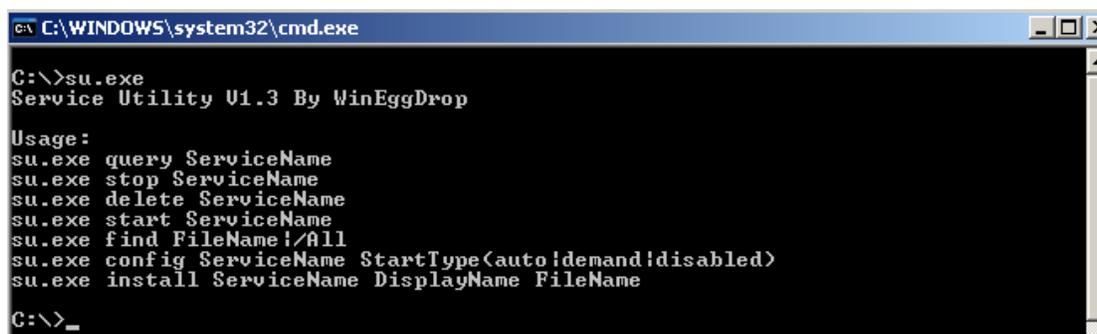
123.bat - Notepad
File Edit Format View Help
@echo off
for /f "eol=; tokens=1,2 delims= " %i in (kr.txt) do s.exe syn %i %j 3389 /save
for /f "eol=- tokens=1 delims= " %i in (result.txt) do echo %i>>s1.txt
for /f "eol=P tokens=1 delims= " %i in (s1.txt) do echo %i>>s2.txt
for /f "eol=s tokens=1 delims= " %i in (s2.txt) do echo %i>>s.txt
del s1.txt
del s2.txt
del Result.txt
  
```

Figure 15. Commands in *123.bat*

The file *su.exe* is a TCP port scanning tool, and the file *kr.txt* contains a South Korean IP range. Because the command scans TCP Port 3389, which is a Windows Remote Desktop Service, we can see that the attacker focused on Windows servers in South Korea.

5. su.exe (service utility)

The file *su.exe* is a service utility tool and is used in controlling services. The image below shows some simple usage of this tool.



```
C:\WINDOWS\system32\cmd.exe
C:\>su.exe
Service Utility V1.3 By WinEggDrop
Usage:
su.exe query ServiceName
su.exe stop ServiceName
su.exe delete ServiceName
su.exe start ServiceName
su.exe find FileName!/*All
su.exe config ServiceName StartType(auto|demand|disabled)
su.exe install ServiceName DisplayName FileName
C:\>_
```

Figure 16. Service utility use of *su.exe*

C&C Information

We have collected information on four different command-and-control (C&C) servers related to Shadow Force.

C&C Server	Location
61[.]137[.]223[.]148	Dandong City, Liaoning Province, China
123[.]190[.]36[.]149	Dandong City, Liaoning Province, China
211[.]239[.]160[.]203	Seoul, South Korea
irc[.]itembuy[.]org (1[.]234[.]14[.]115)	Seoul, South Korea

Figure 17. C&C servers found to be associated with the Shadow Force malware

Attacker Profile

We decided to look further into the C&C servers, specifically the domain name *itembuy[.]Jorg*. This led us to more information about the person behind Shadow Force and produced a handle—WinEggDrop. Based on information posted online, WinEggDrop was born on October 1982 and is a native of Guangzhou City in Guangdong, China. While we will refer to the attacker here as WinEggDrop, he has other handles like Hotmail, meteor, and sdbot.

Our investigation also led to a personal QQ page. This is where we were able to get his English alias, Ben K. His QQ page revealed yet another handle: Syrinx. Based on information there, it seems he has particular interest in Dandong City.



Figure 18. QQ page of WinEggDrop

WinEggDrop is associated with two companies in the same location. These companies were registered by one person under one address, with different room numbers. The mobile phone number submitted for the companies reveals that the original register location is in Guangzhou City.

The other company is registered under a different name. It's highly possible this was registered by an associate of WinEggDrop, because the city of origin and birthdate are near to WinEggDrop's. To compare, this registrant was born on August 1988 (compared to WinEggDrop's October 1982) in Foshan City (compared to Guangzhou City).

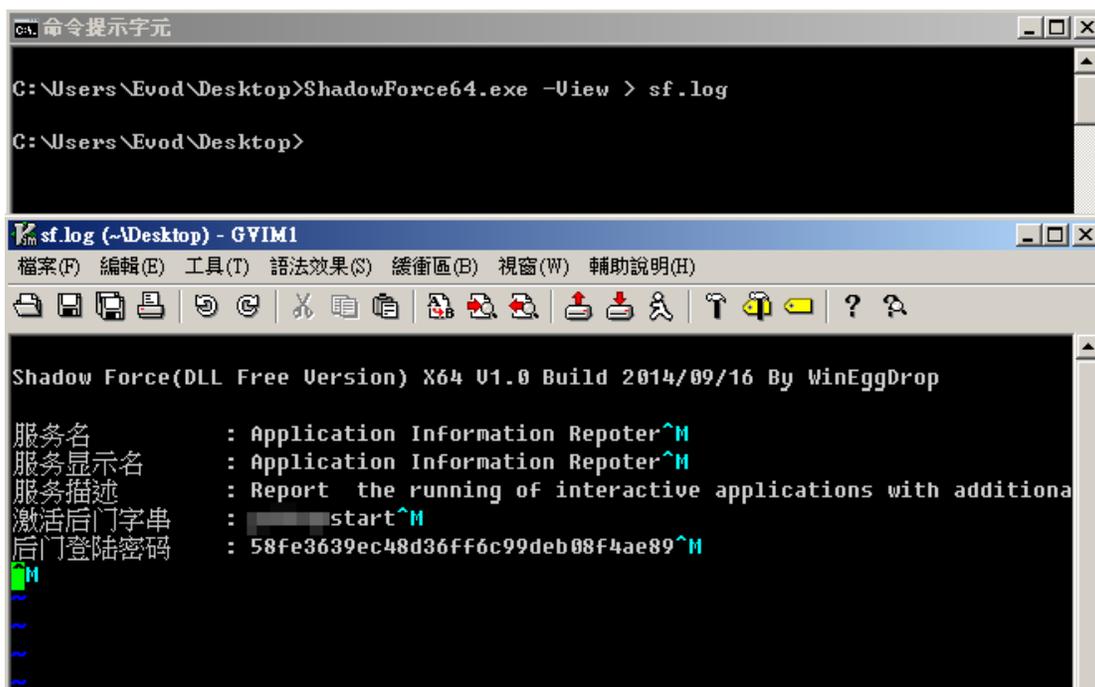
Connecting the Dots

There are key details that tie WinEggDrop to Shadow Force. One of the Shadow Force samples reveals the language used - simplified Chinese, which means the attacker may come from China. Furthermore, we previously mentioned WinEggDrop's interest in Dandong City, and sure enough, two of the Shadow Force C&C servers are located in that city.

Information about the C&C servers also hinted to the target of this Shadow Force attack. Two of the servers are located in South Korea, pointing to a possible target.

Additionally, Shadow Force's password refers to a South Korean media agency.





The image shows two overlapping windows. The top window is a command prompt titled '命令提示字元' (Command Prompt) with the following text:

```
C:\Users\Evod\Desktop>ShadowForce64.exe -Uview > sf.log
C:\Users\Evod\Desktop>
```

The bottom window is a Notepad window titled 'sf.log (~\Desktop) - GYIM1'. It contains the following text:

```
Shadow Force(DLL Free Version) X64 U1.0 Build 2014/09/16 By WinEggDrop
服务名           : Application Information Repoter^M
服务显示名       : Application Information Repoter^M
服务描述         : Report the running of interactive applications with additional
激活后门字符串   : start^M
后门登陆密码     : 58Fe3639ec48d36ff6c99deb08f4ae89^M
```

Figure 19. Language of Shadow Force sample (top) and password referring to a South Korean news agency (bottom)

Conclusion

Shadow Force uses a rarely seen system-level DLL hijacking technique to infiltrate a South Korean company. It employs several tools and techniques that will allow it to possibly bypass detection, making infiltration easier for attackers.

Trend Micro Custom Defense solutions can protect organizations from this type of backdoor attack. These solutions provide in-depth contextual analysis and insight that help IT administrators properly identify suspicious behavior on individual computers and on the network, such as the access to computers and servers.

Trend Micro Incorporated, a global leader in security software, strives to make the world safe for exchanging digital information. Our innovative solutions for consumers, businesses and governments provide layered content security to protect information on mobile devices, endpoints, gateways, servers and the cloud. All of our solutions are powered by cloud-based global threat intelligence, the Trend Micro™ Smart Protection Network™, and are supported by over 1,200 threat experts around the globe. For more information, visit www.trendmicro.com.

©2015 by Trend Micro, Incorporated. All rights reserved. Trend Micro and the Trend Micro t-ball logo are trademarks or registered trademarks of Trend Micro, Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.



Securing Your Journey
to the Cloud

10101 N. De Anza Blvd.
Cupertino, CA 95014

U.S. toll free: 1 +800.228.5651
Phone: 1 +408.257.1500
Fax: 1 +408.257.2003