

CrowdStrike Discovers Use of of 64-bit Exploit by Hurricane Panda

crowdstrike.com/blog/crowdstrike-discovers-use-64-bit-zero-day-privilege-escalation-exploit-cve-2014-4113-hurricane-panda/

October 14, 2014

CrowdStrike Discovers Use of 64-bit Zero-Day Privilege Escalation Exploit (CVE-2014-4113) by Hurricane Panda

October 14, 2014

[CrowdStrike Content Team](#) [Executive Viewpoint](#)



Every once in a while an adversary does something unique or interesting that really captures our attention. The majority of the remote access tools we come across generally run with limited privileges when instantiated on a compromised machine. Privileged access is not required if you are, for example, only going after files that are accessed by general users. However, adversaries who intend to perform more advanced actions that require

administrative access, such as loading a kernel driver that acts as a rootkit or conducting password dumping, needed to elevate their privileges on the victim machine and move around laterally across the network.

Adversaries often use known privilege escalation vulnerabilities to gain administrator-level access but true zero-day exploits are rare and therefore particularly interesting when observed in the wild. They demonstrate that an attacker has knowledge about non-public exploitable security bugs, which usually means that the exploit was either bought from a supplier or developed in-house. Either way, each time we observe zero-day exploits in the wild, they help us better understand an adversary's capabilities. [CrowdStrike Falcon Host](#) Endpoint Threat Detection & Response (ETDR) technology recently detected suspicious activity on a 64-bit Windows Server 2008 R2 machine that was attributed to a compromise by HURRICANE PANDA

HURRICANE PANDA

HURRICANE PANDA is a highly advanced adversary believed to be of Chinese origin and known to be targeting infrastructure companies. They have been known to use three other local privilege escalation vulnerabilities in addition to the zero-day discussed here. Their RAT of choice has been PlugX configured to use the DLL side-loading technique that has been recently popularized among Chinese adversaries. Perhaps their most outstanding technique has been the use of free DNS services provided by Hurricane Electric to return an attacker-controlled IP address for lookups for popular third-party domain names. HURRICANE PANDA is known to use the "ChinaChopper" Webshell, a common initial foothold for many different actors. Once uploading this webshell, the actor will typically attempt to escalate privileges and then use a variety of password dumping utilities to obtain legitimate credentials for use in accessing their intelligence objectives.

CrowdStrike has been battling HURRICANE PANDA on a daily basis since earlier this spring, when the adversary was first detected on a victim network and evicted from that network by [CrowdStrike Services](#) Incident Response team. Since then, they have been trying to regain access on a daily basis. These attempts begin with compromising web servers and deploying Chopper webshells and then moving laterally and escalating privileges using the newly discovered Local Privilege Escalation tool. When these attempts occur, they are instantly detected by Falcon Host and the adversary is stopped in their tracks. This oftentimes resulted in attackers humorously mistyping their commands as they feverishly worked to try to bury themselves into the network knowing that they have precious little time to work with before being shut down. Several times the attacker called the wrong single-letter executable ("hsotname" instead of "hostname" and "romote" instead of "remote") in a panic to achieve their objective before they were kicked out.

One of many unique capabilities of Falcon host is its lateral movement and credential theft activity detection, which provided us and the victims with instantaneous full visibility into all adversary activity and preventing the adversary from getting a foothold in the network.

Falcon Host provides full visibility into the attack – Discovery of Local Privilege Escalation Vulnerability (CVE-2014-4113)

Through Falcon Host technology, we observed that the attackers were using a specific executable to invoke other programs with administrative privileges from the account of an unprivileged user. An example is shown below:

The screenshot displays the Falcon Host interface. On the left, a process tree under 'Processes' shows a hierarchy starting from svchost.exe, through w3wp.exe, and several instances of cmd.exe. One instance of cmd.exe is highlighted, which has spawned a net.exe process, which in turn spawned a Win64.exe process. The Win64.exe process is selected, and its details are shown on the right. The 'Execution Details' pane for Win64.exe shows the following information:

COMMAND LINE	Win64.exe "net localgroup administrators admin /add"
Hash Details	
0 AV Detections	START TIME 06 Oct 2014 @ 14:54
0 Documents Accessed	STOP TIME Unknown
0 DLLs	ACCOUNT [REDACTED]
0 Persistence	FILE PATH \\Device\\HarddiskVolume2\\ProgramData\\Win64.exe
0 Written Executables	FILE NAME Win64.exe
0 Network Connections	SHA256 [REDACTED]
0 Network Listeners	
0 DNS Lookups	

Falcon Host detection screen showing the use of Win64.exe from a webshell to elevate privileges for 'net localgroup administrators admin /add" command

The screenshot displays the Falcon Host interface. On the left, the process tree is similar to the previous one, but now the net.exe process is selected. The details for net.exe are shown on the right. The 'Execution Details' pane for net.exe shows the following information:

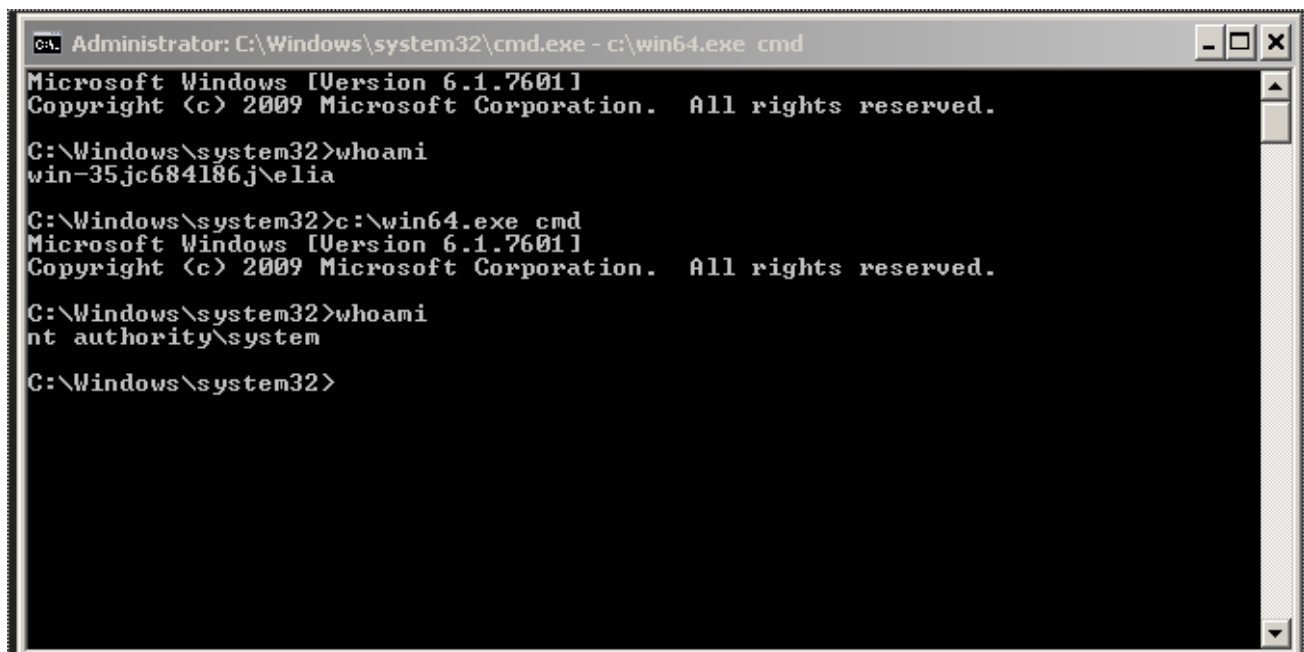
COMMAND LINE	net localgroup administrators admin /add
Hash Details	
0 AV Detections	START TIME 06 Oct 2014 @ 14:54
0 Documents Accessed	STOP TIME 06 Oct 2014 @ 14:54
0 DLLs	ACCOUNT [REDACTED] (Local System)
0 Persistence	FILE PATH \\Device\\HarddiskVolume2\\Windows\\System32\\net.exe
0 Written Executables	FILE NAME net.exe
0 Network Connections	SHA256 3b9ad8e2c1d03f941a7c9192a605f31671b107def6f503a71a0fb2c5bbd659
0 Network Listeners	
0 DNS Lookups	

net command now running as Local System

Subsequent analysis of the `win64.exe` binary revealed that it exploits a previously unknown vulnerability to elevate its privileges to those of the SYSTEM user and then create a new process with these access rights to run the command that was passed as argument. The file itself is just 55 kilobytes in size and contains just a few functions. Here is a high-level description of its functionality:

1. Create a memory section and store a pointer to a function that will be called from the kernel when the vulnerability is triggered
2. Utilize a memory corruption vulnerability in the window manager, simulating user interaction to invoke a callback function
3. Replace the access token pointer in the EPROCESS structure with the one from the SYSTEM process
4. Execute the command from the first argument as a new process with SYSTEM privileges

The following output demonstrates how this tool can be used to start a command shell with administrative access rights.



```
Administrator: C:\Windows\system32\cmd.exe - c:\win64.exe cmd
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
win-35jc684186j\elia

C:\Windows\system32>c:\win64.exe cmd
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
nt authority\system

C:\Windows\system32>
```

The exploit code is extremely well and efficiently written, and it is 100 percent reliable. The adversary has gone through considerable effort to minimize the chance of its discovery — the `win64.exe` tool was only deployed when absolutely necessary during the intrusion operations and it was deleted immediately after use. The build timestamp of the `Win64.exe` binary of May 3, 2014 suggests that the vulnerability was actively exploited in the wild for at least five months.

One of the other interesting elements of the tool is an embedded string “woqunimalegebi”, which is a popular Chinese swearword that is also often misspelled when written in Chinese characters in order to evade online censors and can be translated as “Fertile Grass Mud Horse in the Mahler Gobi Desert”



Bolivian Alpaca aka “Grass Mud Horse”

Affected Windows Versions, Identification and Patches

This security bug affects all x64 Windows variants up to and including Windows 7 and Windows Server 2008 R2. On systems with Windows 8 and later variants with Intel Ivy Bridge or later generation processors, SMEP (Supervisor Mode Execution Prevention) will block attempts to exploit the bug and result in a blue screen.

We reported this vulnerability to Microsoft who assigned the common identifier CVE-2014-4113 to it. Today, Microsoft published security bulletin [MS14-058](#) and issued a patch that fixes the vulnerability. The YARA signature below fires on samples that attempt to exploit this bug.

```
rule CrowdStrike_CVE_2014_4113 {  
  meta:  
    copyright = "CrowdStrike, Inc"  
    description = "CVE-2014-4113 Microsoft Windows x64 Local Privilege  
Escalation Exploit"  
    version = "1.0"  
    last_modified = "2014-10-14"  
    in_the_wild = true  
    strings:
```

```
$const1 = { fb ff ff ff }
$const2 = { 0b 00 00 00 01 00 00 00 }
$const3 = { 25 00 00 00 01 00 00 00 }
$const4 = { 8b 00 00 00 01 00 00 00 }
condition:
all of them
}
```

Detection for this attack is already available for all CrowdStrike [Falcon Host](#) and [Falcon Managed Protect](#) customers – no further action is needed. Analysis of the weapons and techniques of an adversary allow us to better understand the Tactics, Techniques, and Procedures used. With this understanding, we can leverage intelligence and next-generation security tools such as Falcon Host to stay one step ahead of the adversary. If you want to hear more about HURRICANE PANDA and their tradecraft or any of the other adversaries that CrowdStrike tracks, please contact: sales@crowdstrike.com and inquire about [Falcon Host](#), our next-generation endpoint technology, [Falcon Intelligence](#), our Cyber Threat Intelligence service, or [CrowdStrike Services](#), our incident-response and proactive response service offerings.



BREACHES **STOP** HERE

START FREE TRIAL

PROTECT AGAINST MALWARE, RANSOMWARE AND FILELESS ATTACKS

Related Content



CrowdStrike Introduces Adversary-Focused CNAPP

CrowdStrike Delivers Adversary-Focused, Platform Approach to CNAPP and Cloud Security.

“CrowdStrike Dominates in EDR...”

FORRESTER WAVE FOR ENDPOINT
DETECTION AND RESPONSE

A laptop is shown with several floating icons representing security and cloud services. The icons include a fingerprint, a padlock, a cloud, a person profile, and a checkmark. A red ribbon graphic is draped over the laptop, symbolizing a security solution or a wave of adoption.



#1 in Prevention

#1 in Stopping Breaches

The leader in XDR

CrowdStrike leads the latest MITRE ATT&CK Evaluations with 100% automated prevention

- Leading visibility
- Leading analytic coverage
- The **ONLY** platform with native Zero Trust & Identity Protection



CrowdStrike Achieves 100% Prevention in Recent MITRE Engenuity ATT&CK Evaluation Emulating Russia-based Threat Groups