Threat Actor Leverages Windows Zero-day Exploit in Payment Card Data Attacks

fireeye.com/blog/threat-research/2016/05/windows-zero-day-payment-cards.html

Breadcrumb

Threat Research

Dhanesh Kizhakkinan, Yu Wang, Dan Caselden, Erica Eng

May 11, 2016

5 mins read

Zero Day Threats

In March 2016, a financially motivated threat actor launched several tailored spear phishing campaigns primarily targeting the retail, restaurant, and hospitality industries. The emails contained variations of Microsoft Word documents with embedded macros that, when enabled, downloaded and executed a malicious downloader that we refer to as PUNCHBUGGY.

PUNCHBUGGY is a dynamic-link library (DLL) downloader, existing in both 32-bit and 64-bit versions, that can obtain additional code over HTTPS. This downloader was used by the threat actor to interact with compromised systems and move laterally across victim environments.

FireEye identified more than 100 organizations in North America that fell victim to this campaign. FireEye investigated a number of these breaches and observed that the threat actor had access to relatively sophisticated tools including a previously unknown elevation of privilege (EoP) exploit and a previously unnamed point of sale (POS) memory scraping tool that we refer to as PUNCHTRACK.

CVE-2016-0167 – Microsoft Windows Zero-Day Local Privilege Escalation

In some victim environments, the threat actor exploited a previously unknown elevation of privilege (EoP) vulnerability in Microsoft Windows to selectively gain SYSTEM privileges on a limited number of compromised machines (Figure 1).

CVE-2016-0167 Local privilege escalation exploit elevates to system

Figure 1: CVE-2016-0167 Local privilege escalation exploit elevates to system

We coordinated with Microsoft, who patched CVE-2016-0167 on the April 12, 2016, Patch Tuesday (MS16-039). Working together, we were able to observe limited, targeted use of this particular exploit dating back to March 8, 2016.

The Threat Actor

We attribute the use of this EoP to a financially motivated threat actor. In the past year, not only have we observed this group using similar infrastructure and tactics, techniques, and procedures (TTPs), but they are also the only group we have observed to date who uses the downloader PUNCHBUGGY and POS malware PUNCHTRACK. Designed to scrape both Track 1 and Track 2 payment card data, PUNCHTRACK is loaded and executed by a highly obfuscated launcher and is never saved to disk.

This actor has conducted operations on a large scale and at a rapid pace, displaying a level of operational awareness and ability to adapt their operations on the fly. These abilities, combined with targeted usage of an EoP exploit and the reconnaissance required to individually tailor phishing emails to victims, potentially speaks to the threat actors' operational maturity and sophistication.

Exploitation Details

Win32k!xxxMNDestroyHandler Use-After-Free

CVE-2016-0167 is a local elevation of privilege vulnerability in the win32k Windows Graphics subsystem. An attacker who had already achieved remote code execution (RCE) could exploit this vulnerability to elevate privileges. In the attack from the wild, attackers first achieved RCE with malicious macros in documents attached to spear phishing emails. They then downloaded and ran a CVE-2016-0167 exploit to run subsequent code as SYSTEM.

CVE-2016-0167 is patched as of April 12, 2016, meaning the attacker’s EoP exploit will no longer function on fully updated systems. Microsoft released an additional update (MS16-062) on May 10, 2016, to further improve Windows against similar issues.

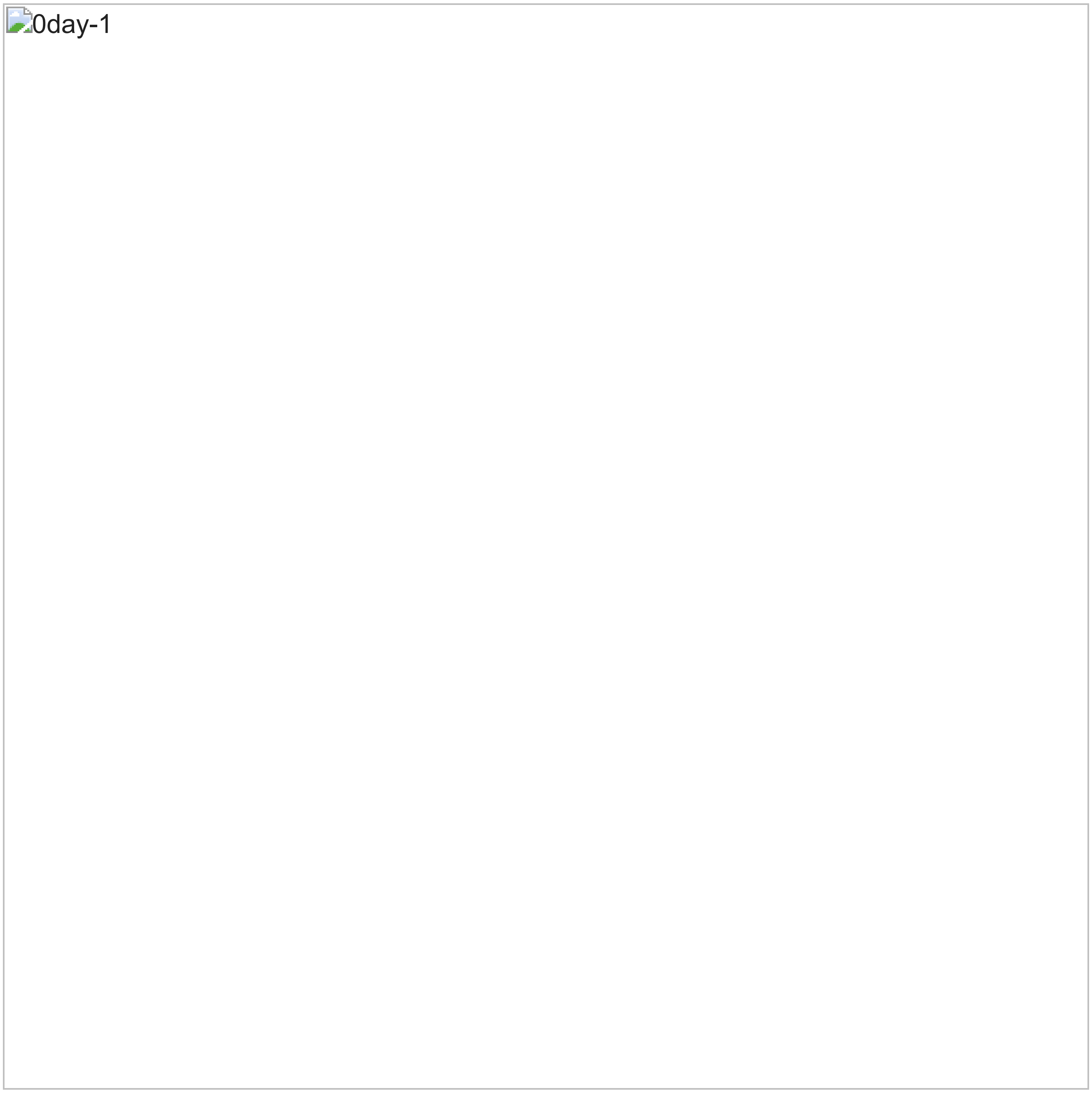
Vulnerability Setup

First, the exploit calls CreateWindowEx() to create a main window. It sets the WNDCLASSEX.lpfnWndProc field to a function that we name WndProc. It installs an application-defined hook (that we name MessageHandler) and an event hook (that we name EventHandler) using SetWindowsHookEx() and SetWinEventHook(), respectively.

Next, it creates a timer with IDEvent 0x5678 in SetTimer(). When the timeout occurs, WndProc receives the WM_TIMER message and will invoke TrackPopupMenuEx() to display a shortcut menu. EventHandler will capture the EVENT_SYSTEM_MENUPOPUPSTART event from xxxTrackPopupMenuEx()and post a message to the kernel. In handling the message, the kernel eventually calls the vulnerable function xxxMNDestroyHandler(), which calls the usermode callback MessageHandler. MessageHandler then causes a use-after-free scenario by calling DestroyWindow()

Heap Control

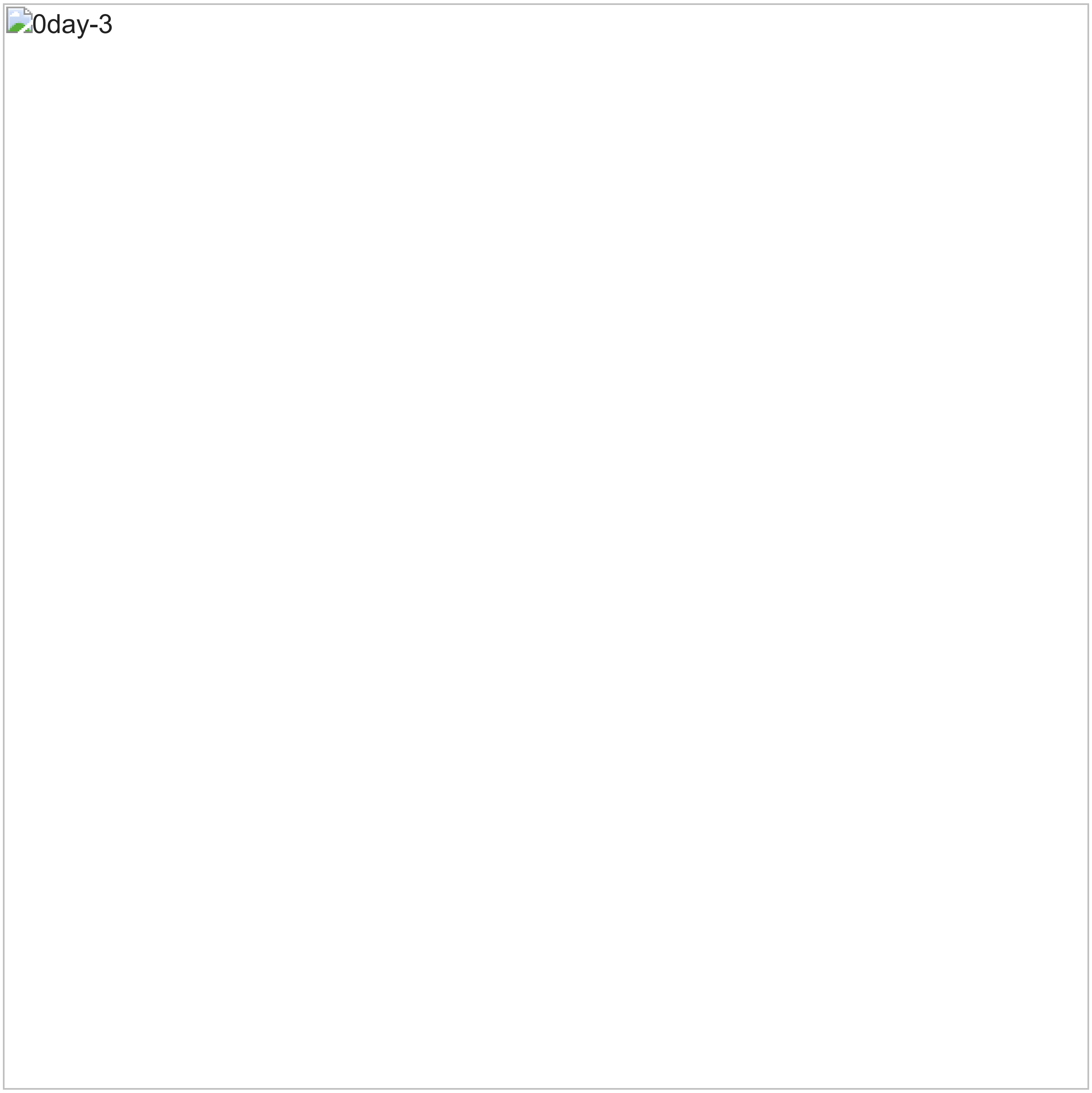
The exploit uses SetSysColors() to perform heap Feng Shui which manipulates the layout of the heap by carefully making heap allocations. In the following snippet, one of the important fields is at address fffff900`c1aaac40, where fffff900`c06a0422 is a window kernel object’s (tagWND) base address plus 0x22:



Memory Corruption

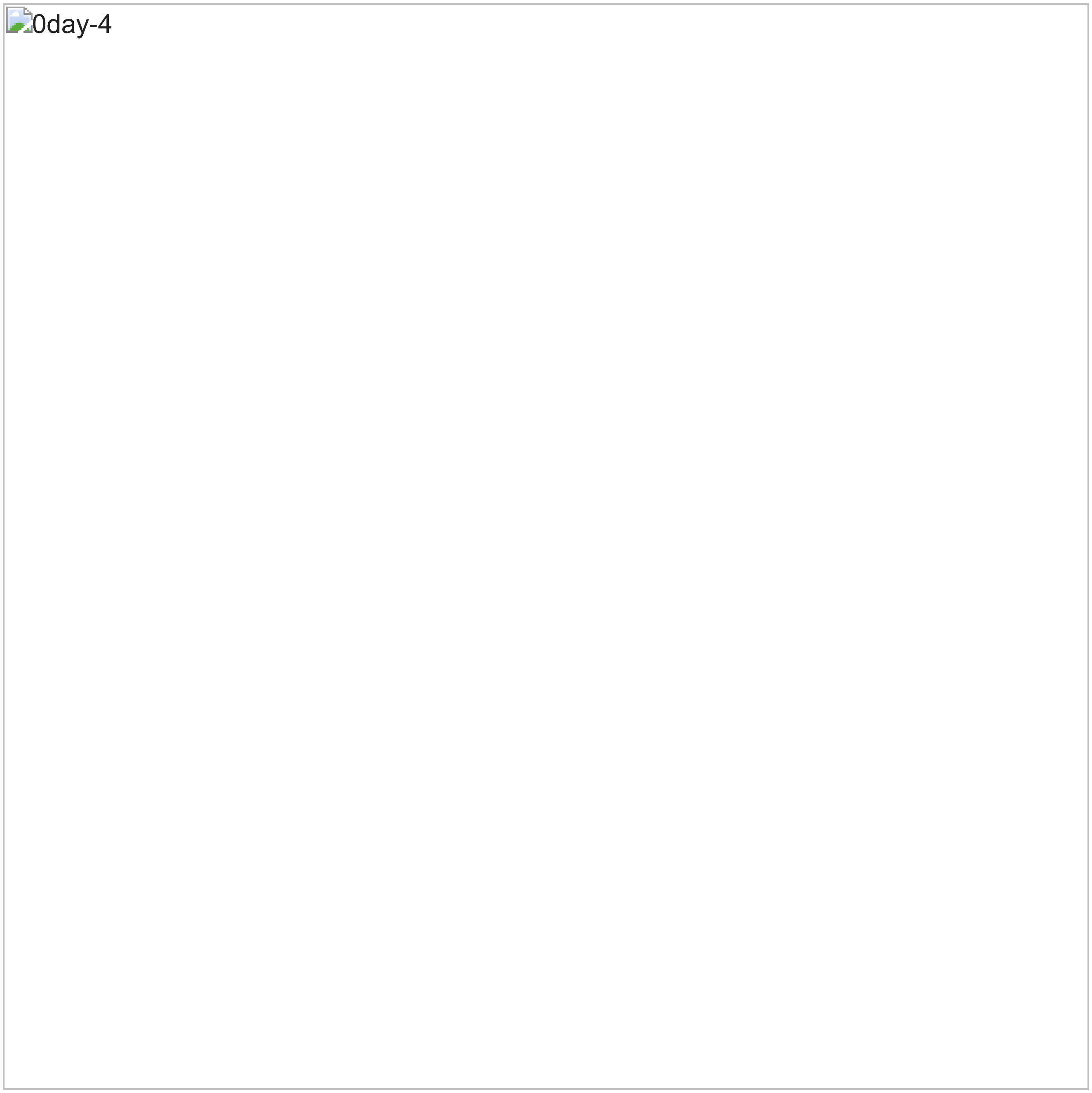
The USE operation occurs at HMAssignmentUnlock()+0x14 as shown below:

Since RDX contains the base address of tagWND plus 0x22, this instruction will add 0xffffffff to the win32k!tagWND.state field, changing its value from 0x07004000 to 0x07003fff. 0x07004000 indicates that the bServerSideWindowProc flag is unset. When the change occurs, it sets the bServerSideWindowProc flag as shown below.


0day-3

Code Execution

If a window is marked as server-side (bServerSideWindowPro is set), the lpfnWndProc function pointer will be trusted by default and this can be user-mode shellcode. The following backtrace shows the kernel calling the exploit’s shellcode:



The shellcode then steals the System process token to elevate a child cmd.exe process.

Mitigation

FireEye products and services identify this activity as Exploit.doc.MVX, Malware.Binary.Doc, PUNCHBUGGY, Malware.Binary.exe, and PUNCHTRACK within the user interfaces.

The latest Windows updates address CVE-2016-0167, and fully protect systems from exploits targeting CVE-2016-0167.

In addition, effective mitigations exist to prevent social engineering attacks that utilize Office macros. Individual users can disable Office macros in their settings and enterprise administrators can enforce a Group Policy to control macro execution for all Office 2016 users. More details about Office macro attacks and mitigations are available here.

Acknowledgements

Thank you to Elia Florio and the Secure@ staff of Microsoft, and Dimiter Andonov, Erye Hernandez, Nick Richard, and Ryann Winters of FireEye for their collaboration on this issue.