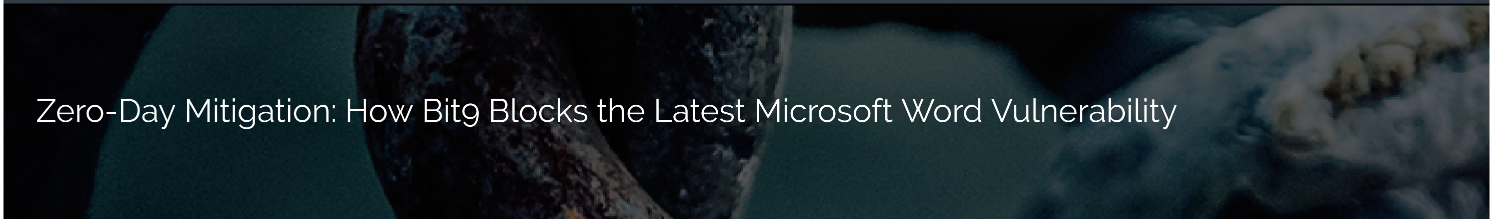
Careers 855-525-2489 Contact Us REQUEST A DEMO

CARBON
BLACK
ARM YOUR ENDPOINTS

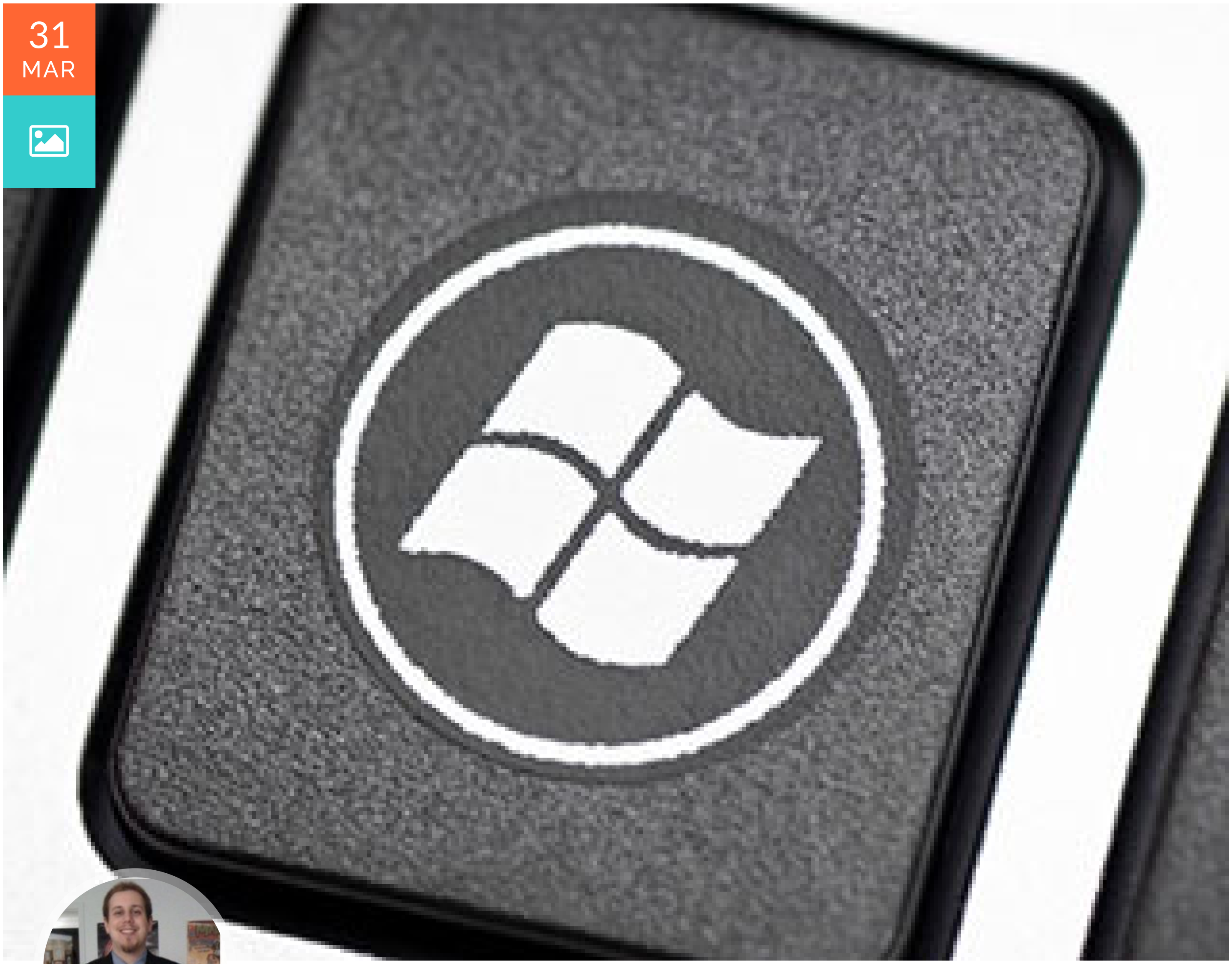
WHY CARBON BLACK PRODUCTS SOLUTIONS PARTNERS RESOURCES COMPANY

BLOG



Zero-Day Mitigation: How Bit9 Blocks the Latest Microsoft Word Vulnerability

31
MAR



Zero-Day Mitigation: How Bit9 Blocks the Latest Microsoft Word Vulnerability

March 31, 2014 / Ryan Nolette / Advanced Threat Protection, Tech Toolbox

On March 24, 2014 Microsoft released Security Advisory 2953095 to notify customers of vulnerability in Microsoft Word. At this time, there are limited, targeted attacks directed at Microsoft Word 2010. The exploit takes advantage of an unspecified RTF parsing vulnerability combined with an ASLR bypass, which depends by a module loaded at predictable memory address. Microsoft is advising that customers should enable EMET as well as applying stronger protections by preventing office applications from processing RTF-formatted content. Customers can either disable opening of RTF files in Word and Outlook or use Trust Center settings to force Word to always open RTF files in Protected View.

Threat Description

The malicious document is designed to trigger a memory vulnerability in the RTF parsing code. The RTF document has a secondary component embedded in it in order to bypass ASLR and leverage ROP (return oriented programming) techniques using native RTF encoding schemes to craft ROP gadgets (legitimate usage).

When the memory corruption vulnerability is triggered, the exploit gains initial code execution and in order to bypass DEP and ASLR, it tries to execute the ROP chain that allocates a chunk of executable memory and hands over control to the first piece of the shellcode. This code then looks for the main shellcode placed at the end of the RTF document for execution.

One peculiar aspect of the main shellcode is that it employs multiple consecutive layers of decryption and well-known anti-debugging tricks.

The shellcode will not perform any additional malicious action if there are updates installed after April, 8 2014. This means that even after a successful exploitation with reliable code execution, after this date the shellcode may decide to not drop the secondary backdoor payload and simply abort the execution.

When the activation logic detects the correct condition to trigger, the exploit drops in the %TEMP% folder a backdoor file named 'svchost.exe' and executes it

Threat Mitigation

Bit9 in High Enforcement would block the executables that are created by this vulnerability. Bit9 Detection v1.2 (current release) has 2 ATIs that look at behaviors that are leveraged in this attack. Those 2 ATIs are "Possible exploit of document handling application" and ""Execution of system file name outside of system folder."

This post contains a large number of indicators, if you want more information from Microsoft about the attack and some sample code. The attack that's been spotted in the wild drops files to the endpoint. Bit9 will defend against this attack because of this attribute of the attack. The known hashes involved in this attack have already been marked as malicious within the Bit9 Software Reputation Service, so any customer using SRS will be alerted upon the detection of such files.

Customers may also decide to push a GPO setting to their clients to force Word to open RTF files in Protected View in Trust Center settings which mitigates this attack as well.

Threat Modification

Global Ban known malicious hashes

- The below hashes have already been marked as malicious within the Bit9 Software Reputation Service

- MD5: af63f1dc3bb37e54209139bd7a3680b1
- SHA1: 77ec5d22e64c17473290fb05ec5125b7a7e02828

Install Bit9 Detection:

- The Bit9 ATIs “Possible exploit of document handling application” and “”Execution of system file name outside of system folder” were written to detect behavior like this and should be monitored.
- These rules will see the malware dropping to %TEMP%\svchost.exe as well as any execution of it.

Move Endpoints to High Enforcement

- This will remove the ability of the exploited document and application to create executables on the endpoint and execute them.

EMET

- Microsoft confirms that implementation of EMET would stop this vulnerability from executing.

Disable opening of RTF files

- This will remove the ability of the exploited document and application to create executables on the endpoint and execute them.

Use Trust Center settings to force Word to always open RTF files in Protected View

- This will remove the ability of the exploited document and application to create executables on the endpoint and execute them.

References

- http://blogs.technet.com/b/srd/archive/2014/03/24/security-advisory-2953095-recommendation-to-stay-protected-and-for-detections.aspx
- http://technet.microsoft.com/en-us/security/advisory/2953095