SIM2K
Adapting Technology to Your Business Needs

6•22
Information you can use

SIMformation

New Zero-Day Exploit Targets Microsoft Word

Our security partner Huntress is keeping a close eye on the developing threat of a zero-click remote code execution technique used through MSDT (Microsoft Diagnostics Tool) and Microsoft Office utilities, namely Microsoft Word. Throughout the next coming days, they expect exploitation attempts in the wild through email-based delivery.

Microsoft has issued a bulletin following the discovery of this exploit. Named CVE-2022-30190 (also known as Follina) allows attackers to execute arbitrary code via the Microsoft Support Diagnostic Tool (MSDT). All it takes to exploit the vulnerability is for a victim to open an infected Word document. The document makes use of the Word remote template feature in order to retrieve an HTML file from a remote webserver. This HTML file then uses the ms-msdt MSProtocol URI scheme to load some code and run it in PowerShell.

The short take on this newly discovered vulnerability in MS Word (and likely other MS Office apps) is that it could install malware so you should be especially vigilant about opening any attachments. You should also be made aware that this exploit can be triggered with a hover-preview of a downloaded file that does not require any clicks (post download).

Understanding the Exploit
The Huntress team examined the contents of the Microsoft Word document and has replicated this exploit. Unzipping the file extracts all the components that make up the Office document. Contained in the code are some hidden files, specifically an executable file named “rgb.exe.” The impact of rgb.exe specifically is unknown, but the important takeaway is that this is a novel initial access technique that readily offers threat actors code execution with just a single click – or less. This is an enticing attack for adversaries as it is tucked inside of a Microsoft Word document without macros to trigger familiar warning signs to users – but with the ability to run remotely hosted code.

To better understand this threat, Huntress security researchers modified the internals of the Word document to call out to a local address within an analysis sandbox, and served a benign payload that would display a message rather than detonating malware.

In the most recent attacks detected by researchers, the actors used hijacked email thread messages with HTML attachments that would download ZIP archives containing IMG files. Inside the IMG files are DLL, Word and shortcut files. The shortcut file directly loads the Qbot DLL file that already exists in the IMG disk image, the blank.docx document connects to a remote server controlled by attackers to load an HTML file. This file executes a PowerShell code to download and run a new Qbot DLL payload.

Since at least 2007, Qbot has been used as a Windows banking trojan with worm capabilities to steal Windows domain credentials, banking credentials, financial data and personal information. This malware also gives threat actors the ability drop backdoors on compromised systems, deploy Cobalt Strike beacons, and provide remote access to ransomware gangs.

Phishing tactics that use different lures, such as bogus invoices, payment and banking details, scanned documents, or bills, often cause victims to be infected with Qbot. However, Qbot may also infect victims when they are already infected with another kind of malware.

Earlier this month, researchers said that a suspected Chinese threat group had been spotted exploiting the Follina bug to deliver ZIP archives containing infected Word documents. Another attempt at exploiting the vulnerability was reported by the SANS Internet Storm Center, where researchers received an infected document uploaded from Ireland but with a filename in Chinese characters. Other reports indicated that phishing e-mails offering salary raises to staff were sent to European government agencies and US local government agencies.

The recent exploitation of the Follina vulnerability demonstrates how attackers move quickly to exploit an unpatched vulnerability. Microsoft has yet to provide a fix for the flaw. It recommends blocking the MSDT URL protocol as a mitigating measure. “Disabling MSDT URL protocol prevents troubleshooters being launched as links including links throughout the operating system. Troubleshooters can still be accessed using the Get Help application and in system settings as other or additional troubleshooters,” Microsoft says.

Huntress has added this exploit to its Managed Antivirus package, so there is no action required as this protection already leverages Microsoft’s detection logic to augment your preventive posture. Huntress’ team of threat analysts will continue to leverage the Huntress Managed Security Platform to help protect you. Additionally, SIM2K is continuing to monitor any activity within our client base to see if this exploit is showing up in any scans we monitor. We will update you as we learn more.

What Hours Do You Work?

Microsoft has more than 180,000 employees in 100 countries. So it knows a thing or two about how people actually work. In its latest study, the Work Trend Index report, the folks in Redmond have found that people working from home don't work from 9 a.m. to 5 p.m. It's not because people who work from home are lazing around watching Netflix and eating snacks. They're working as hard, or harder, than ever. It is just that they are not doing it on a schedule first set in Ford Motor Company factories in the 1920s. Instead, based on data about its employees' work patterns, Microsoft found that people are working later than ever.

Microsoft Teams data showed that people were often meeting after 5 p.m. To be exact, they're meeting or messaging with each other most often between 6 p.m. and 8 p.m. The average Teams user now sends 42% more chats per person after hours.

According to a Microsoft blog post: "Traditionally, knowledge workers had two productivity peaks in their workday: before lunch and after lunch. But when the pandemic sent so many people into a work-from-home mode, a third peak emerged for some in the hours before bedtime. Microsoft researchers are referring to this phenomenon as a 'triple peak day.'"

Using keyboard data, Microsoft found that 30% of its employees worked more at night. And it's not just the early evening either. While not as high as the historic work peaks around 10 a.m. and 3 p.m., there's also now a lower, but still significant, 10 p.m. work spike.

In some ways, this isn't new. It's long been a fact that programmers are night owls. And long before anyone wrote a line of code, in 1635, to be exact, the phrase "burning the midnight oil" entered the language.

But, as a professor in the Department of Informatics at the University of California observed, "More than ever, people are taking on additional day duties that they didn't have before, whether it's caring for kids and helping with schooling or being a caretaker to another family member.… [This is] pushing a lot of people to work later."

This is also blurring the line, for better or worse, between work and home life. Work-life balance is being replaced with talk of "work-life integration." According to Payscale's 2022 State of the Gender Pay Gap Report, 85% of women reported the primary reason they quit a job was because of childcare. And with childcare – when you can find it – costing $10,174 per child annually, it's no wonder people work late; it's when they have the time. One of the ways to cope is to take a break, eat dinner, and then spend time in the evening getting things done.

The third peak should be an available option for people who need it, but the challenge moving forward is, "How can we make sure people are not working 24/7?" If people are working all three peaks, that can be a recipe for early burnout.

Obviously the Covid pandemic has changed work as we know it, and companies should be faced with changing patterns and have support for these remote workers available.

5G Makes Hotspots An Option

If you are traveling this Summer, and wanting to work (or stream movies..) you can have an option to public wi-fi – using your smartphone as a hotspot. This works just like a dedicated mobile hotspot device, but because it's right inside the phone, there's nothing extra to charge, carry, or try not to lose. The way it works is simple: When the phone is connected to the mobile data network, it converts a 4G or 5G data stream into a Wi-Fi signal that nearby devices can share.

Happily, none of this affects how the phone works. While a phone is feeding data to laptops, it can still view web sites on its own screen, make calls, and respond to texts. Most reasonably recent Android and iOS devices can do it. And using your phone as a hotspot is generally already included in your monthly plan.

To use a phone as a hotspot, the device treats its online connection to the data network as a broadband data source. The newest handsets then transmit this data locally like a mini-Wi-Fi router. The net result is that Wi-Fi devices within range can tap into the data signal as if it were a regular old Wi-Fi network – because that's exactly what it is.

5G is taking over the mobile data scene. Despite the catch-all name, it isn't a single network. It is, rather, three networks of differing frequencies and capabilities. Each use different frequencies, with the higher frequencies transferring more data within a shorter range. It is 5G's ability to operate at super high frequencies that makes 5G's ultra-fast speeds possible. Unfortunately, because they have a short range, these higher frequencies require service providers to build more base station towers to transmit the signal. Your experience will depend not only on how far you are from the tower but which frequency it is using.

Using a phone hotspot can actually increase your security profile by helping you avoid insecure public hotspots in coffee shops and hotels. At the phone end of the equation, your connection is just as secure and private as making a phone call or web surfing with your phone. And the 5G networks take security to a new level with 256-bit AES encryption, the ability to block fake mobile network transmission sites and encrypting the phone's ID during transmissions. This is only the case if the network implements these defenses, though.

If your phone supports 5G and is in range of a 5G network, that's what it will use for hotspot connections. Otherwise, it will drop down to a 4G network, if that's all it can find. 5G phones will typically display a "5G" logo in the upper right near the signal strength bars, replacing the "LTE" or "4G" one. Every major phone maker has 5G models, and there are even budget-priced 5G phones that can help stretch your IT budget. So you have a high-speed data option when out and about.

SIMformation is the monthly newsletter from SIM2K. Information presented here is designed to inform you of trends in the business world affecting information technology. For questions or comments, write SIM2K, 6330 E. 75th St., Suite 214, Indianapolis, IN 46250. Call us at (317) 251-7920 or e-mail sales@sim2k.com. Visit us at www.sim2k.com.

DSLR vs iPhone?

Apple's decision to invest in iPhone photography was incredibly shrewd. Industry insiders expect that smartphone cameras will deliver better quality images than you get from DSLR (Digital Single Lens Reflex) cameras within three years.

"We expect that still images will exceed the image quality of single-lens reflex cameras within the next few years," said a Sony Semiconductor official. This statement comes as pro photographers (and video makers) make increasing use of iPhones for professional work – but also as machine vision intelligence reaches a tipping point to enable enterprise and industrial applications.

Throughout the history of the iPhone, Apple has focused on use of the device as a camera. It has also built out a wider ecosystem to support this use. This includes the Photos app, built-in document scanning, AI-driven person recognition, machine-driven text identification and translation, and, most recently, the capacity to identify images of flowers and animals using Visual Lookup. Apple's efforts arguably accelerated with the iPhone 7 Plus, which included multiple lenses and zoom functionality for the first time in a smartphone.

Sony, which holds 42% of the global image sensor market for phones and has three of its highest-end sensors inside the iPhone 13, believes sensors in high-end devices will double in size by 2024. This will enable "new imaging experiences," Sony said. These will inevitably include zoom effects boosted by AI and Super HDR and should also extend to 8K video capture on smartphones. It is also believed that technology will extend to true 3D imaging capture sufficient to support truly immersive 3D experiences. These predictions make it clear that Apple's Cinematic Mode is a stalking horse from which to exploit the future evolutions of smartphone camera sensors.

But this kind of machine vision intelligence is just the consumer front end to far more complex operations that should translate into interesting enterprise opportunities. Camera intelligence combined with augmented reality can optimize performance across distribution, warehousing, and logistics chains. Industry is also embracing smartphone-quality imaging intelligence – factories make use of fault detection systems mounted on iPads and other devices to monitor production to maintain quality control, for example, and AR-based retail experiences continue to improve.

However, what we see today should be considered alongside those uses only now coming to bear, particularly around autonomy and augmented reality. Industry experts believe Apple is working towards eventual introduction of AR (Augmented Reality) glasses, which may be equipped with an array of as many as eight cameras – possibly due early next year. A human wearing a set of AR glasses will rely on a similar set of technologies as a vehicle making use of machine vision intelligence to drive itself on the public highway. Accurate image sensors combined with the kinds of AI already in use daily in iPhones will be fundamental to the development of the Apple Car.

Of course, as such imaging-based use cases proliferate it is reasonable to anticipate accelerated innovation in the CMOS sensor (the chip that "captures" images) development industry. The impact? Eventually the camera you wear on your glasses will be capable of capturing photographs equally as good as those you catch today using a DSLR. "Point and shoot" will give way to "look and shoot" if this holds true.

"Random Tid-Bytes"

Zultys Announces Upgrades to MX Services

Zultys has announced a new feature that increases the capacity of video conferencing to allow up to 20 webcams to be utilized in a single conference session. Use this increased video capability to connect, collaborate, and get more done, with increased face-to-face interaction. This new feature enables support for video conferences of up to 20 webcams and as many audio attendees as licensed for so you can scale your audio attendance as needed. It also allows internal and external users to participate in multi-party video conferences. Also, the release of ZAC 8.2 contains a number of changes to improve business processing, enhance robustness of existing capabilities, and improve functionality of current features. This includes better visibility on the password indication screen and an informative popup that's been added when a user attempts to place an outbound call while an incoming call is ringing for incoming call handling improvements. Most impressive are the new features giving ZAC even more power and versatility including a System speed dial function, the ability to change another user's presence status and ZAC user profile configuration – allows administrators to enable/disable certain features of ZAC that are available to individual end users. Call us for more information on Zultys Unified Communications and ZAC updates.

Using a Virtual Private Network?

There are hundreds of VPN providers, and you may have a VPN offered as part of your security suite. But if you are looking for a stand-alone VPN, do some research first. Read the reviews, not only from users, but also tech experts. Check how many server locations there are – the more, the better. Verify the speeds and reliability of connectivity the company provides, and be sure that the VPN is compatible with your devices. Also see if you can install the VPN on multiple devices (like your PC, smartphone and tablet.) And watch out for "free" services, as often these "deals" end up with the company selling your information to marketers for a deluge of come-on e-mails. Once you select the VPN company, download the software on the devices to be covered, and the opt for whether or not you want to connect automatically or only when you want the privacy the VPN offers. Using a VPN will encrypt your traffic and make it unreadable to anyone trying to access it, protecting you from hackers, snoopers or other cybercriminals. So if you are traveling this Summer and using public wi-fi connections, a VPN provides security for your activity.

Google "Translation Glasses"

Google has teased "translation glasses," holding out the promise that you can one day talk with someone speaking in a foreign language, and see the English translation in your glasses. In a video, Google showed not only "closed captioning" – real-time text spelling out in the same language what another person is saying – but also translation to and from English and Mandarin or Spanish, enabling people speaking two different languages to carry on a conversation while also letting hearing-impaired users see what others are saying to them. By presenting translation visually, wearers can follow conversations much more easily and naturally. No word on when, or if, these will be out.

Parlez-Vous Français? Non? Let Microsoft Help

If you want to translate text in Outlook emails, Word documents, Excel spreadsheets, or PowerPoint presentations, it's easy to do. Maybe you work for an international company, or perhaps you communicate with colleagues or customers who are more comfortable writing in their native language. None of this is a problem for Office, which offers translation courtesy of an AI-powered Translator service that can translate a selection of text or an entire document, file, or message between many different languages.

The Translator service is accessible across multiple Microsoft products and technologies on the consumer and enterprise sides. Translator supports more than 100 languages, including more common languages, such as English, French, Italian, Spanish, German, Chinese, Japanese, and Arabic, and some less common languages, including Fijian, Haitian Creole, Icelandic, Kurdish, Maltese, Serbian, and Ukrainian.

The accuracy of Microsoft Translator is evaluated using a BLEU (Bilingual Evaluation Understudy) score. This score measures the differences between a machine-based translation and a human translation of the same source text. One report from 2018 measuring Chinese to English translation gave Microsoft Translate a grade of 69 out of 100, which is a high score compared to human translation. This will likely improve with time, too, at least according to a Microsoft Translator blog post from November 2021 that explains how the company is working to advance its machine translation technology.

Here's how to use the translator in the different Office applications:

If you've purchased Outlook 2019 or later for Windows as a standalone app or as part of Microsoft Office or Microsoft 365, the translation functionality is built in. To set it up, click the **File** menu and select **Options**. In the Outlook Options window, select **Language**.

The window now displays your default display language for Office. Scroll down to the **Translation** section. Here, you can decide how to handle messages received in other languages, opting to always translate them, get asked before translating, or never translate. Next, select the target language if it's not your default language. Then click the **Add a Language** button and select any languages for which you don't want to see a translation.

Close the **Options** window and return to the main Outlook screen. Open an e-mail you want translated into your native language. Depending on the options you chose, the e-mail will automatically be translated or give you the ability to have it translated. Either way, you should see a link in the message to translate the message to your language. If not, click the **Translate** button on the Ribbon and select the **Translate Message** command.

Run the translate command, and the entire message appears in your native language. You can then switch back and forth between the translation and the original text and turn on automatic translation if it's not already enabled.

What if you want to take the reverse trip and translate an e-mail you're composing from your own native language to a different language? Unfortunately, Microsoft currently offers no reliable or workable way to do this in Outlook. The easiest workaround is to translate the text in Word, then copy and paste it into your message in Outlook.

The translation service is also accessible for Outlook on the web. To set it up here, sign into Outlook with your Microsoft or business account. Click the **Settings** icon at the top right. In the Settings pane, click the link for **View all Outlook** settings. In the Settings window that pops up, select **Mail** and then **Message handling**. Scroll down to the Translation section and you'll find the same settings as in the desktop version of Outlook.

When you receive a message in a different language, the Translate feature will offer to translate it for you. Click the link to translate it. You can then switch back and forth between the original text and the translation. As with desktop Outlook, the web version presently offers no workable method for translating a new e-mail from your own native language to a different language. Again, translating the text in Word is your best bet.

The translation feature in Microsoft Word works much the same way in the desktop and online versions. Open a document that you want to translate, either in full or in part. Select the **Review** tab on the Ribbon. To customize the feature before using it, click the **Translate** button and select **Translator Preferences**. In the Translator pane that appears on the right, confirm that the switch is set to Yes for "Offer to translate content that isn't in a language I read." You can also add any languages that you don't want translated.

If you only want certain text translated, select the text. Click the **Translate** button in the Ribbon and choose **Translate Selection**. In the Translator pane on the right, make sure the correct source language is detected. If it's not correct, click the down arrow for the target language and change it. Hover your mouse over each word in the translation, and the feature will show you the translation just for that word. To add the translation to your current document, click the blue **Insert** button at the far right.

Similarly, to translate the entire document, click the **Translate** icon in the Ribbon and select **Translate Document**. In the Translator pane, make sure the Document tab is selected. Confirm that the target language is correct. Click the blue **Translate** button at the far right. A new document is created and pops up with the complete translation.

The translation for Excel works only in the desktop version of the program. Select a cell or multiple cells that contain text you want translated. Click the **Review** menu and select **Translate**. In the Translate pane, make sure the source and destination languages are correct. You can then hover over each word to see its individual translation.

As with Excel, translation for PowerPoint is available only in the desktop client. PowerPoint can translate selected text (not a whole presentation); it works just like translating selected cells in Excel.

PowerPoint also offers a handy feature that can translate your presentation as you speak it, which is great if you have an audience that is more comfortable in another language. The translations appear as subtitles as you deliver the presentation. Click the **Slide Show** menu and check the box for **Always use subtitles**. Then select **Subtitle settings**. In the web version of PowerPoint, click the **Slide Show** menu and select the down arrow next to **Always use subtitles**. Select or confirm the spoken language. Then select the subtitle language.

So these tools can help you overcome language barriers or having to take a Babbel cram course to deal with foreign clients or vendors.

SIM2K
6330 E 75th St., Suite 214
Indianapolis, IN 46250
317.251.7920 • 800.746.4356
www.sim2k.com • sales@sim2k.com