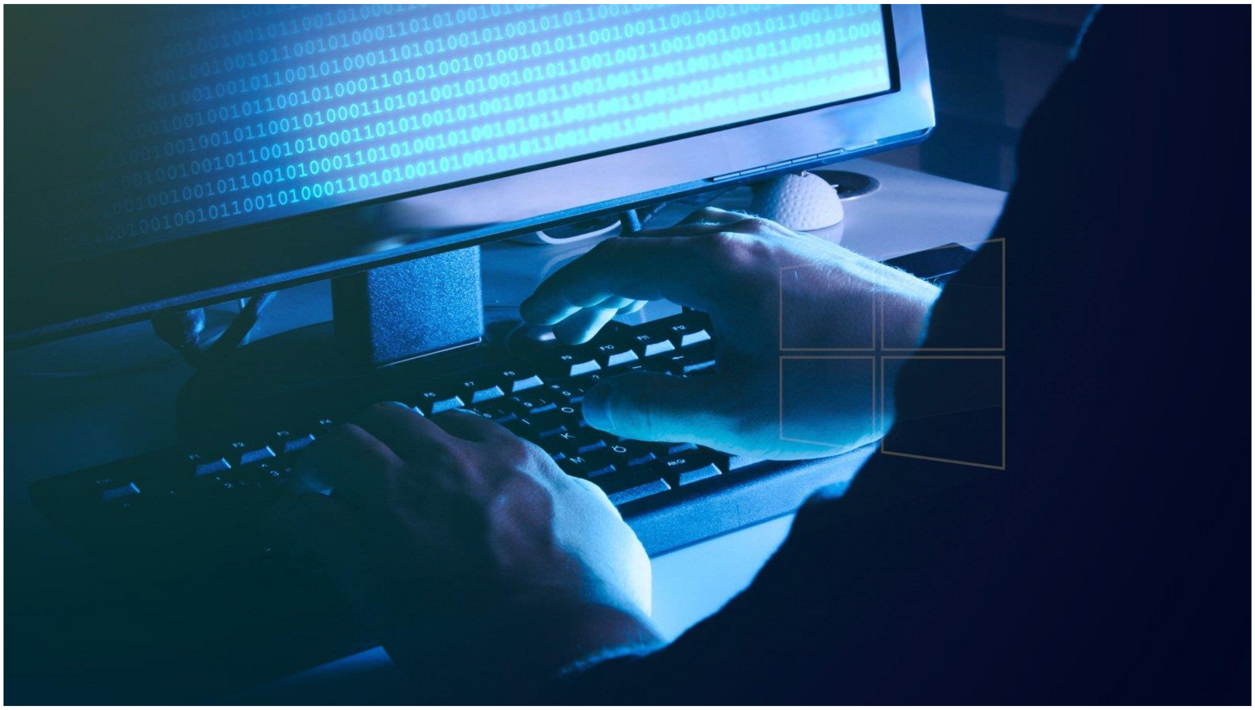
HEADQUARTERS
CYBERSPACE SECURITY GROUP
COMMUNICATIONS, ELECTRONICS AND INFORMATION SYSTEMS SERVICE
ARMED FORCES OF THE PHILIPPINES
Camp General Emilio Aguinaldo, Quezon City

Watch out for new malware campaign’s 'Windows 11 Alpha' attachment



Relying on a simple recipe that has proved successful time and time again, threat actors have deployed a malware campaign recently that used a Windows 11 theme to lure recipients into activating malicious code placed inside Microsoft Word documents.

Security researchers believe that the adversary behind the campaign may be the FIN7 cybercrime group, also known as Carbanak and Navigator, that specializes in stealing payment card data.

Tried and tested method

The adversary took advantage of the buzz created around the details for Microsoft’s development of its next operating system release, which started in early June.

Cybercriminals laced Microsoft Word documents with macro code that ultimately downloads a JavaScript backdoor that lets the attacker deliver any payload they want.

Researchers at cybersecurity company Anomali analyzed six such documents and say that the delivered backdoor appears to be a variation of a payload commonly used by the FIN7 group since at least 2018.

The names used in the campaign seem to indicate that the activity may have occurred between late June and late July, a period immediate to when news about Windows 11 started to emerge on a more regular basis.

It is unclear how the malicious files were delivered but phishing email is typically how it happens. Opening the document shows Windows 11 imagery with text designed to trick the recipient into enabling macro content.

The claim that the document was generated with a newer operating system may make some users believe that there is a compatibility issue that prevents accessing the content and that following the instructions eliminate the problem.

If the user acts on the indication, they activate and execute the malicious VBA macro that the threat actor planted inside the document.

The code is obfuscated to hinder analysis but there are ways to clean it of the surplus and leave only the relevant strings.

Anomali researchers found that the included VBScript relies on some values encoded inside a hidden table in the document to perform language checks on the infected computer.

Detecting a specific language (Russian, Ukrainian, Moldovan, Sorbian, Slovak, Slovenian, Estonian, Serbian) puts a stop to the malicious activity and deletes the table with encoded values.

The code also looks for the domain CLEARMIND, which Anomali researchers say appears to refer to a point-of-sale (PoS) provider.

Other checks that the code makes include:

Reg Key language preference for Russian

Virtual machine - VMWare, VirtualBox, innotek, QEMU, Oracle, Hyper and Parallels (if a VM is detected the script is killed)

Available memory (stops if there is less than 4GB)

Check for RootDSE via LDAP

The JavaScript is heavily obfuscated and cleaning it up reveals a backdoor that resembles other backdoors connected to the FIN7 cybercrime group, Anomali researchers say.

There is moderate confidence for the attribution, which is based on the following factors:

Targeting of a POS provider aligns with previous FIN7 activity

The use of decoy doc files with VBA macros also aligns with previous FIN7 activity

FIN7 have used Javascript backdoors historically

Infection stops after detecting Russian, Ukrainian, or several other Eastern European languages

Password protected document

FIN7 has been around since at least 2013 but became known on a larger scale since 2015. Some of its members got arrested and sentenced but attacks and malware continued to be attributed to the group even beyond 2018 when several of its members got arrested [1, 2].

The attackers focused on stealing payment card data belonging to customers of various businesses. Their activity in the U.S. caused above $1 billion in losses from stealing over 20 million card records processed by more than 6,500 point-of-sale terminals at around 3,600 separate business locations.

Among the companies that FIN7 hit are Chipotle Mexican Grill, Chili’s, Arby’s, Red Robin, and Jason’s Deli.

Solution:

If you are a victim of a ransomware attack, we recommend reporting this incident to authorities. By providing information to law enforcement agencies, you will help track cybercrime and potentially assist in the prosecution of the attackers. Here's a list of authorities where you should report a ransomware attack. For the complete list of local cybersecurity centers and information on why you should report ransomware attacks

Isolating the infected device:

Some ransomware-type infections are designed to encrypt files within external storage devices, infect them, and even spread throughout the entire local network. For this reason, it is very important to isolate the infected device (computer) as soon as possible.

Step 1: Disconnect from the internet.

Step 2: Unplug all storage devices.

Step 3: Log-out of cloud storage accounts.

Identify the ransomware infection:

To properly handle an infection, one must first identify it. Some ransomware infections use ransom-demand messages as an introduction (see the WALDO ransomware text file below).

> This method is only effective, however, when the appended extension is unique - many ransomware infections append a generic extension (for example, "**.encrypted**", "**.enc**", "**.crypted**", "**.locked**", etc.). In these cases, identifying ransomware by its appended extension becomes impossible.

The ransomware will be identified within seconds and you will be provided with various details, such as the name of the malware family to which the infection belongs, whether it is decryptable, and so on.

Search for ransomware decryption tools:

Finding the correct decryption tool on the internet can be very frustrating. For this reason, we recommend that you use the No More Ransom Project and this is where identifying the ransomware infection is useful. The No More Ransom Project website contains a "Decryption Tools" section with a search bar. Enter the name of the identified ransomware, and all available decryptors (if there are any) will be listed.

Restore files with data recovery tools:
Depending on the situation (quality of ransomware infection, type of encryption algorithm used, etc.), restoring data with certain third-party tools might be possible. Therefore, we advise you to use the Recuva tool developed by CCleaner. This tool supports over a thousand data types (graphics, video, audio, documents, etc.) and it is very intuitive (little knowledge is necessary to recover data). In addition, the recovery feature is completely free.

Step 1: Perform a scan.

Step 2: Recover data.

Creating a data backup:

The backup process is the same for all file types and folders. Here’s how you can back up your files using Microsoft OneDrive

References:

https://www.pcrisk.com/removal-guides/10188-alpha-ransomware

https://www.bleepingcomputer.com/news/security/watch-out-for-new-malware-campaign-s-windows-11-alpha-attachment/

https://cyber-reports.com/2021/09/05/watch-out-for-new-malware-campaigns-windows-11-alpha-attachment/