WHAT YOU NEED TO KNOW ABOUT THE BAZARLOADER MALWARE?

By Anjali Raut | 16 September 2021 | 3 min read | 0 Comments

At the start of February 2021, Bazarloader malware was in the news about its mechanism of delivering the initial attack vector. It tricks a victim into connecting with a fake call where a threat actor asks to download malicious excel attachments from the portal to infect them. We recently observed that its delivery mechanism is shifting to an older technique – popularly known as "WordProcessingML," and now it delivers malicious attachments directly via email.

What is WordProcessingML?

WordProcessingML or Word 2003 XML Document is an XML-based format introduced in Microsoft Office 2003 as one of the formats that could be chosen in the "Save As" feature to save Word documents, though not the default format (e.g., DOC, a proprietary binary format). This is different from the "Microsoft Office Open XML File Format" introduced in Office 2007, which consists of a ZIP archive of various files, including XML. In contrast, WordProcessingML is a single uncompressed XML file. Later versions of MS office are still capable of loading and saving WordProcessingML.

Infection Chain:

Attack Chain

The infection starts with a malspam having a Microsoft Word document (the older Word 2003 XML document). While the execution of the XML document file, it will automatically open the word application and run present macros.

In the below fig, we can see the syntax for documents and macros.

Fig.1- Original XML File

Fig.2- Document view to Victim

In wordprocessingML file, attribute "<w:name>" in"< w:binData>" element contains "editdata.mso" file that is base64 encoded ActiveMime object. ActiveMime is Zlib-compressed data starting at offset 0x32, which contains VBA macro and OLE object-related data.

Fig.3- Steps to get OLE file

The above highlighted OLE file is used to drop the HTA file on the victim's machine on the "c:\ProgramData\" location with the help of the command line.

Adversaries also use text data with obfuscated "y2nb" in the original doc file to bypass AV solutions. By removing "y2nb," we get base64 encoded data which contains the final URL to download malicious DLL payload. The below image shows the actual process.

Fig.4- URL to download DLL

These processes are done at run time by VBA macros present in the OLE file and HTA file "iCoreBr.hta" dropped a "c:\ProgramData\." The dropped file can be seen in fig 5.

Fig.5- HTA file to download DLL

Downloaded DLL is written on victim's public folder with name"icoreBr.jpg" to confuse victim as shown in fig 6.

Fig.6- Downloaded DLL as jpg

This BazarLoader related DLL is used to download other modules of malware families such as Trickbot, Ryuk Ransomware, and Cobalt strike activity.

Conclusion:

As the Bazarloader campaign is still active and changing its spreading mechanism, users should be careful while opening emails, documents sent by unknown senders and keep the AV updated. Quick Heal customers are protected from these types of attacks at multiple detection levels.

IoCs:

- WordProcessingML files: 1b265cbdfb47ef2675bbc19d7542aec3
- DLL : dba397022561b196d000d81907f543d0
- Domains: obeymanagement2016b.com, nephewboring2013b.com

Anjali Raut

Follow @AnjaliR51806529

YOU MAY ALSO LIKE...

Security news updates from the week gone by

By Rahul Thadani | 15 Dec | 2 min read

Windows Malware on the Rise – Quick Heal Threat Report Q3 2015

By Rahul Thadani | 2 Nov | 3 min read

Netflix application looks alike Android Malware

By Ranjeet Menon | 17 Oct | 2 min read

Security news updates from the week gone by

By Rahul Thadani | 15 Dec | 2 min read

Windows Malware on the Rise – Quick Heal Threat Report Q3 2015

By Rahul Thadani | 2 Nov | 3 min read

Netflix application looks alike Android Malware

By Ranjeet Menon | 17 Oct | 2 min read

Security news updates from the

week gone by

By Rahul Thadani | 15 Dec | 2 min read

Windows Malware on the Rise – Quick Heal Threat Report Q3 2015

By Rahul Thadani | 2 Nov | 3 min read

✉ Subscribe ▾

0 COMMENTS