Slamming The Backdoor On BazarLoader

blog.minerva-labs.com/slamming-the-backdoor-on-bazarloader

Minerva Labs Blog

News & Reports

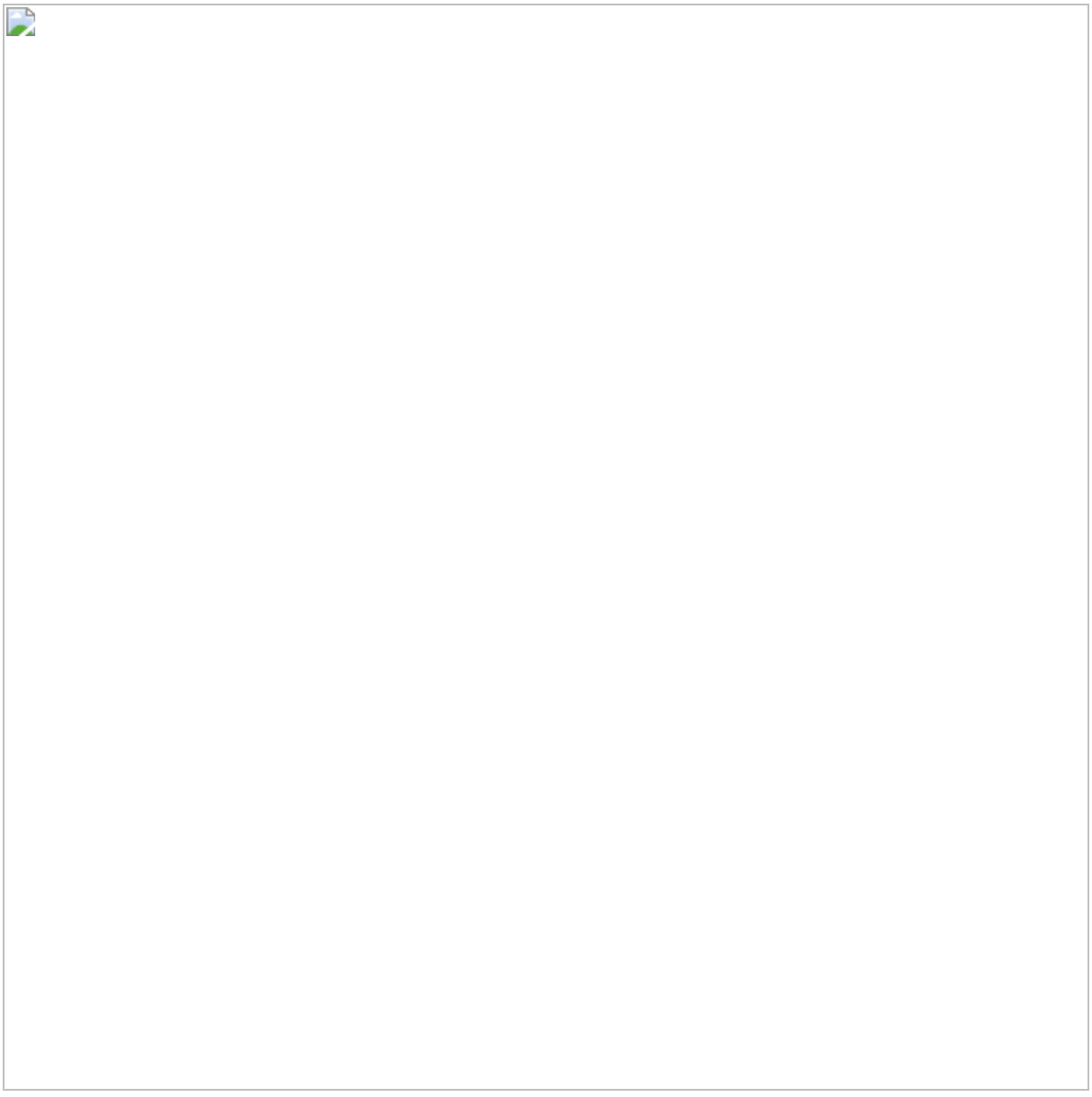
- Tweet
-

It seems like Trickbot's creators are trying to up their game in 2021. A new version of BazarBackdoor is being distributed through a malicious Excel file that drops and executes BazarLoader. The new and improved binary contains new surprises for both security products and researchers.

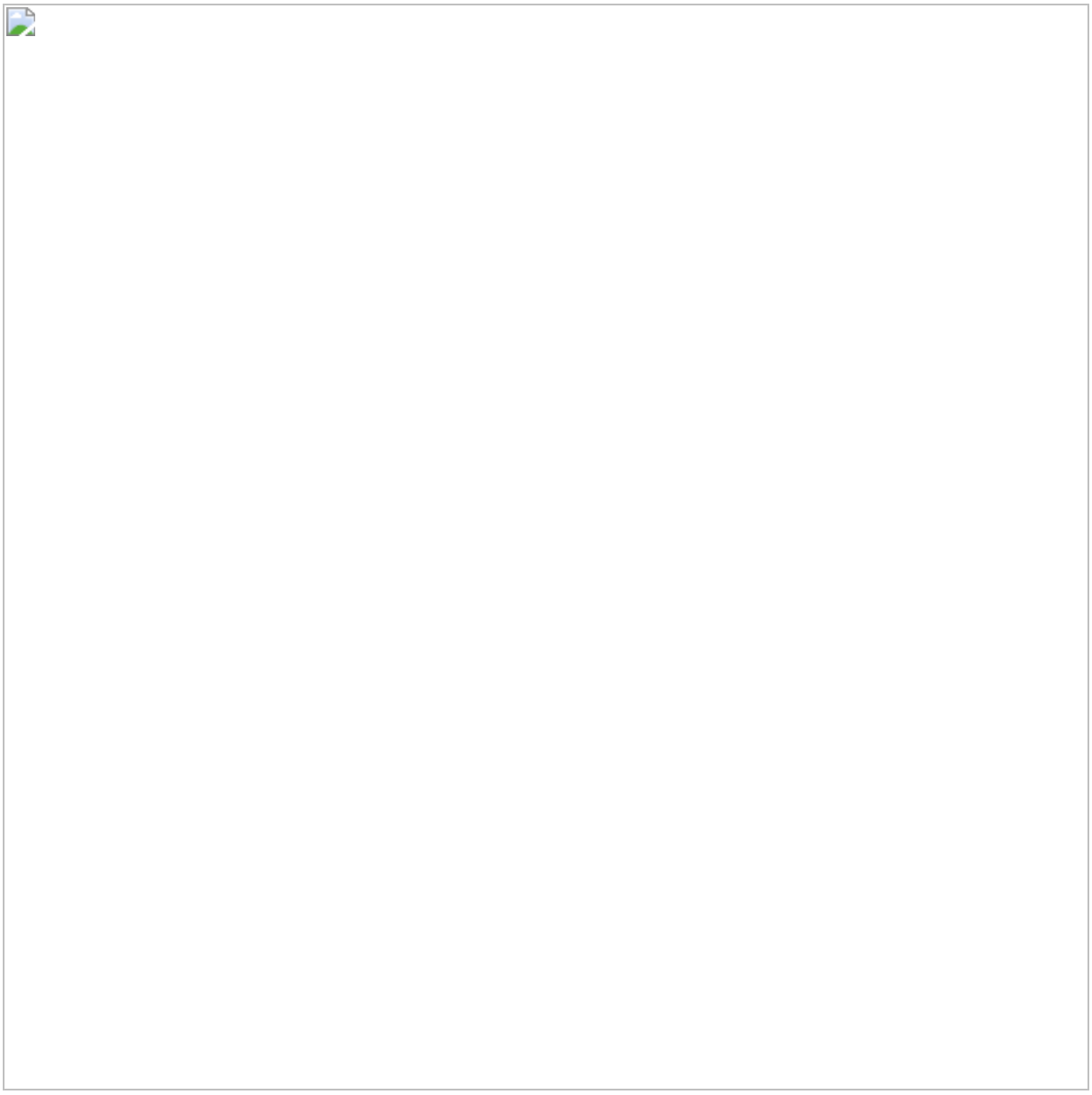
Before executing any malicious code, a couple of anti-emulation techniques are used. First, the malware calls SetFileAttributesA with the parameters “C:\windows\Explorer.exe” and FILE_ATTRIBUTE_NORMAL (0x80) and if the function succeeds the malware will exit. Secondly, the malware calls the function WriteFileGather with the invalid handle 0, and exits if the return value is not 0.

After the anti-emulation checks Bazar will load a resource (ID is 0x1e55 in our sample) and decrypt its content using a modified RC4 algorithm and a hardcoded key. The malware’s author changed the algorithm’s hardcoded value of the secret state’s permutation from 256 to 30, thus rendering most of the key provided by the malware unused.

The RC4 functions and the hardcoded key:



After the decryption of the next payload, it is copied to a newly allocated RWX section, and execution is transferred. The decrypted code reflectively decodes and load the final payload, which is obfuscated using Control Flow Flattening, a compiler-based obfuscation technique:



As part of a dynamic analysis of the payload, we have observed a few peculiar behaviors:

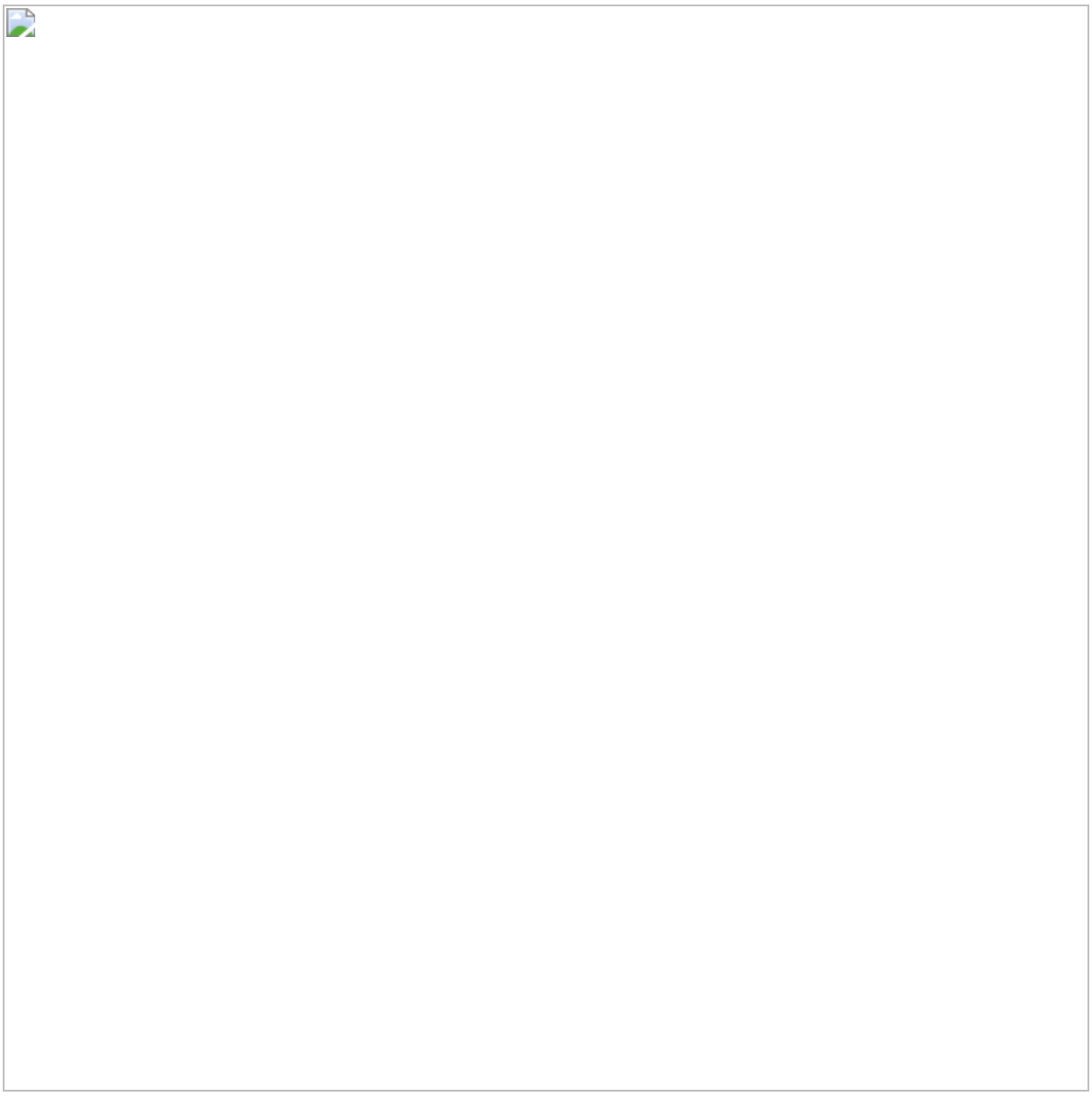
- The malware spawns the process “ping 8.8.8.8 -n 2”, probably to verify internet connectivity.
- The malware copies itself to the directory “C:\Users\CurrentUser\Pictures\RandomlyGenerated” and executes itself from there.
- Bazar door tries to read the disk version of ntdll.dll, probably in order to perform usermode unhooking through dll remapping. (similar to conti ransomware).
- The Loader tries to inject its payload into an operating system process, in our sample the process chosen was cmd.exe.

The Conti connection:

Many sources has reported a link between Conti ransomware, which we profiled last fall, and Bazar loader. We have observed a striking similarity between the packer of a Conti sample from last October (VirusTotal Link) and the new sample in question, specifically in the modification of RC4 to decrypt a payload from the resource section.

Bazar loader has greatly matured as a stealthy first-stage malware, as can be seen by previous versions of the malware, its development team is very active. It is safe to assume this would not be the last we hear of it.

Minerva Labs prevents Bazar Backdoor with our Hostile Environment Simulation and Injection Prevention modules:



IOCs:

Hash:

d362c83e5a6701f9ae70c16063d743ea9fe6983d0c2b9aa2c2accf2d8ba5cb38

IPs:

54[.]184[.]178[.]68

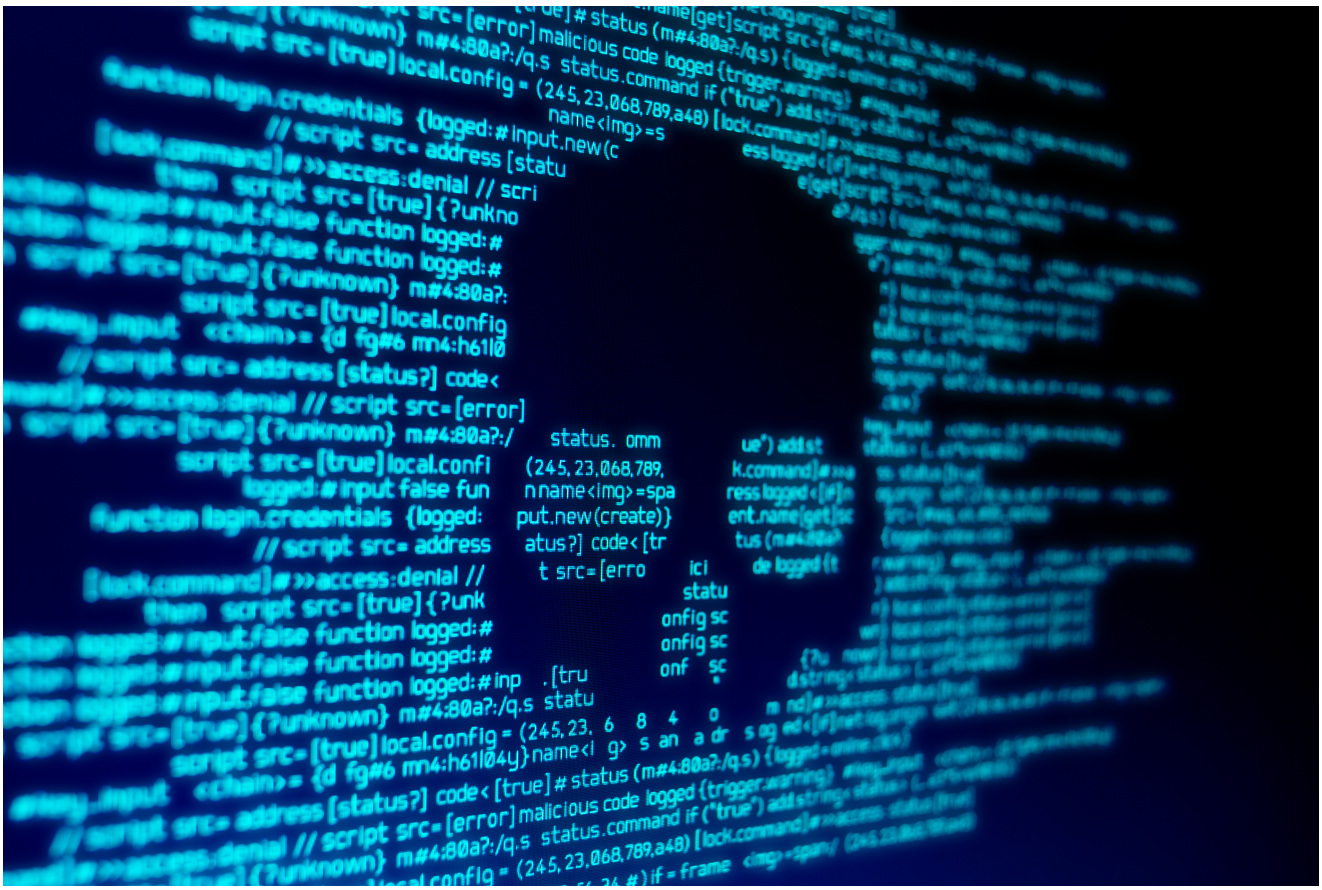
RC4 Key:

YfsQptT(y6*V_Avqg^08%vSG9jj%XWo136@bgbaDqHh@ZvSQzD?
s!^Cl06@9rr83f*WpgB5c^!".

« Previous Post
Next Post »

Interested in Minerva? Request a Demo Below

Related Posts



Conti Ransomware - Built to bypass EDRs, Prevented by Minerva

Read More >>