Houdini Worm Transformed in New Phishing Attack

cofense.com/houdini-worm-transformed-new-phishing-attack/

Cofense June 14, 2019

Gateways Bypassed

Symantec

By Nick Guarino and Aaron Riley

The Cofense Phishing Defense Center™ (PDC) and Cofense Intelligence™ have identified a new variant of Houdini Worm targeting commercial banking customers with campaigns containing either URLs, .zip, or .mht files. This new variant is named WSH Remote Access Tool (RAT) by the malware's author and was released on June 2, 2019. Within five days, WSH RAT was observed being actively distributed via phishing. Figure 1 shows an example message from this campaign.

Houdini Worm (HWorm) – a misleading name because it has more in common with a bot or RAT than a worm – has existed since at least 2013 and shares extreme similarities with what are undoubtedly its malignant siblings: njRAT and njWorm. This new iteration comes ported to JavaScript (JS) from HWorm's original codebase of Visual Basic. WSH is likely a reference to the legitimate Windows Script Host, which is an application used to execute scripts on Windows machines.

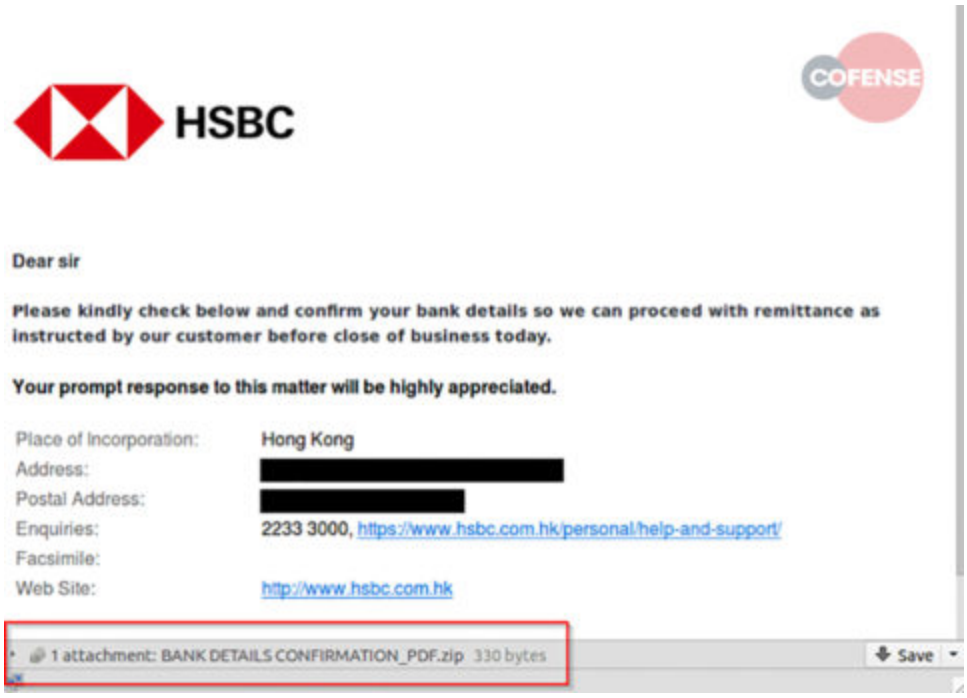

Figure 1: The phishing email delivering WSH RAT within an attachment

The email attachment contained an MHT file that are used by threat operators in the same way as HTML files. In this case, the MHT file contained an href link which when opened, directed victims to a .zip archive containing a version of WSH RAT. Figure 2 shows the URL chain to the downloaded payload.

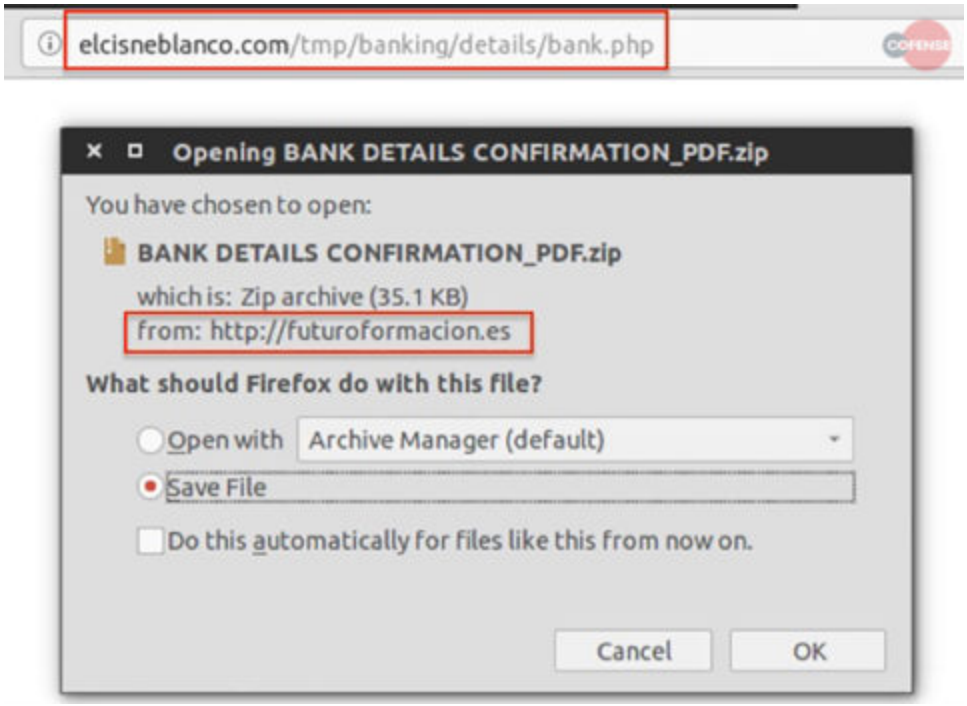

Figure 2: The chain of URLs that lead to the .zip archive download

When executed on an endpoint, WSH RAT behaves in the same way as Hworm, down to its use of mangled Base64 encoded data. WSH RAT uses the same configuration structure that Hworm uses for this process. Figure 3 shows the extracted configuration strings from the running memory of WSH RAT. It is interesting to note that the WSH RAT configuration is an exact copy of the Hworm's configuration, even as far as not changing the name of the default variables.

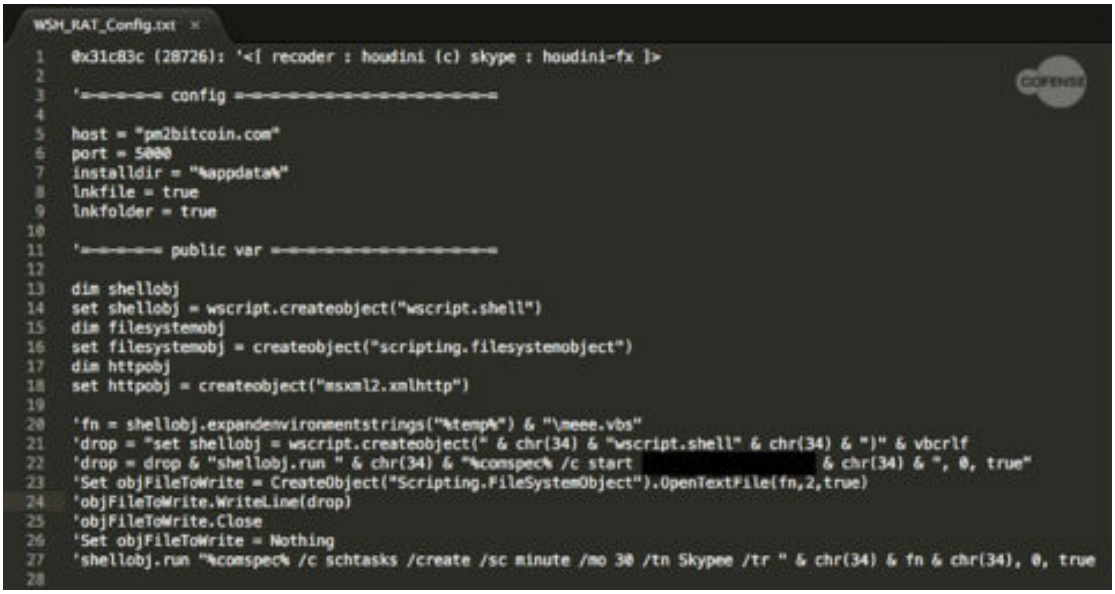

Figure 3: The extracted configuration strings from the running memory of WSH RAT

The URL structure used by WSH Rat for its Command and Control (C2) communication is identical to that employed by Hworm, as shown in Figure 4.

Figure 4: The C2 callout made by WSH RAT

Also note the extreme similarity between the C2 communications shown in Figures 5 and 6. WSH RAT prepends the id “WSHRAT” to the User-Agent string and also changes the delimiter from “<|>” to “|”, otherwise they are functionally identical.

Figure 5: An example HTTP POST made by WSH RAT

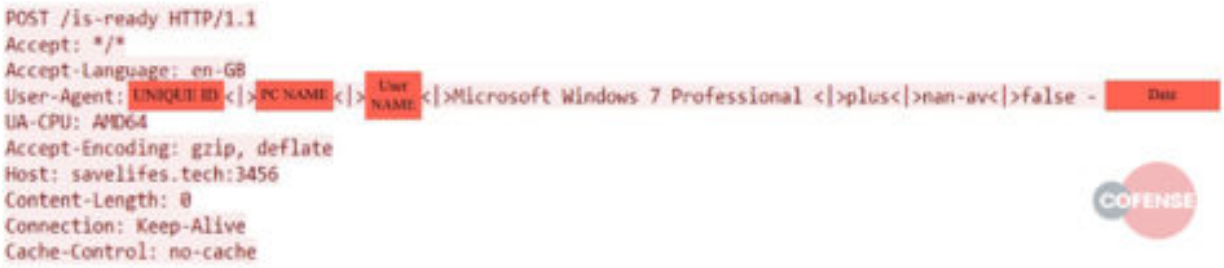

Figure 6: An example HTTP POST made by Hworm

After the initial callout to the C2, this WSH RAT sample began calling out to another URL for three separate payloads. Figure 7 shows the URL payload requests for the .tar.gz files.

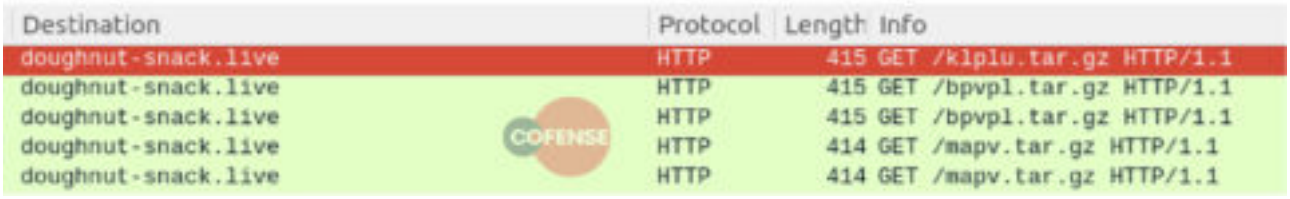

Figure 7: The network traffic showing the WSH RAT downloads

The downloaded files have the .tar.gz extension but are actually PE32 executable files. The three downloaded executables were:

- A keylogger
- A mail credential viewer
- A browser credential viewer

All three of these modules are from third parties and are not original work from the WSH RAT operator. Figure 8 shows the programs running and the property information from the three executables downloaded by WSH RAT.

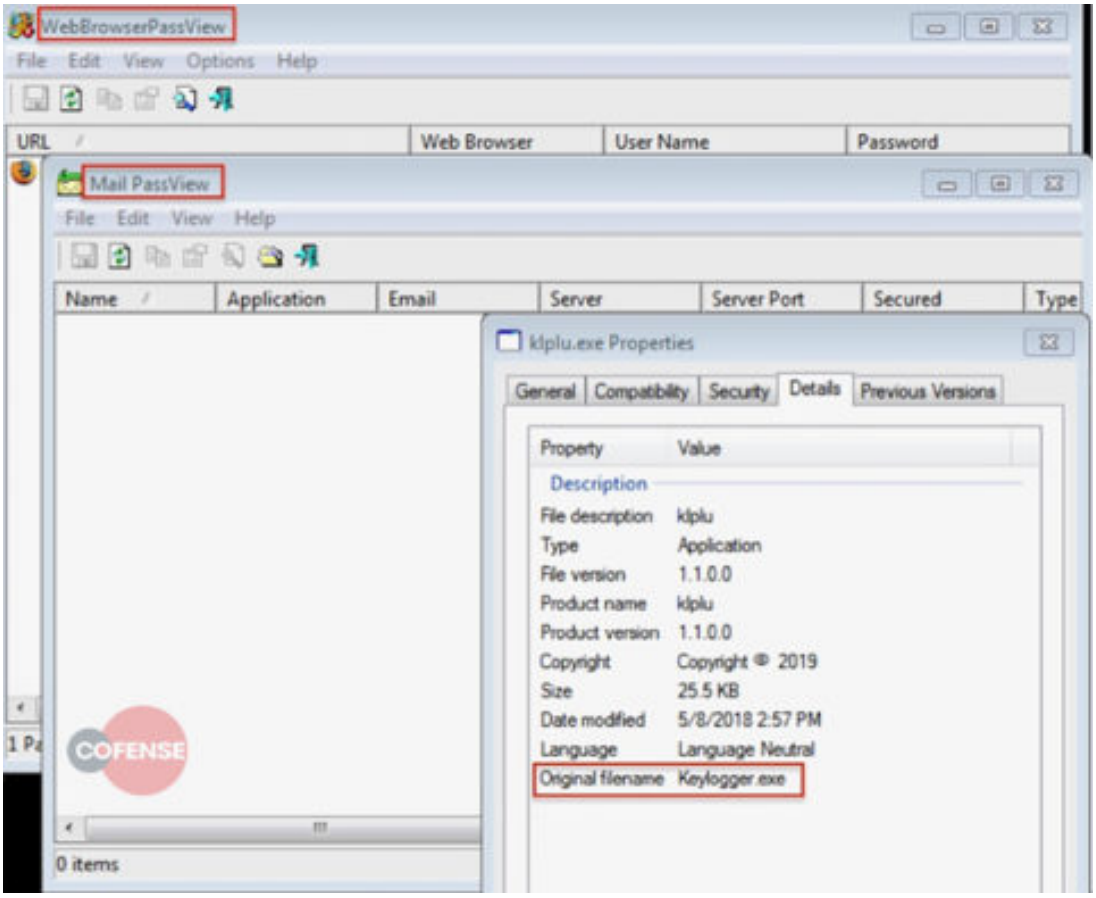

Figure 8: The programs and details of the three downloaded executables

Getting Past the Email Gateway

WSH RAT is being sold for $50 USD a month and has an active marketing campaign. The threat operators tout the RAT's many features such as WinXP-Win10 compatibility, several automatic startup methods, and a large variety of remote access, evasion, and stealing capabilities as shown in Figure 9.

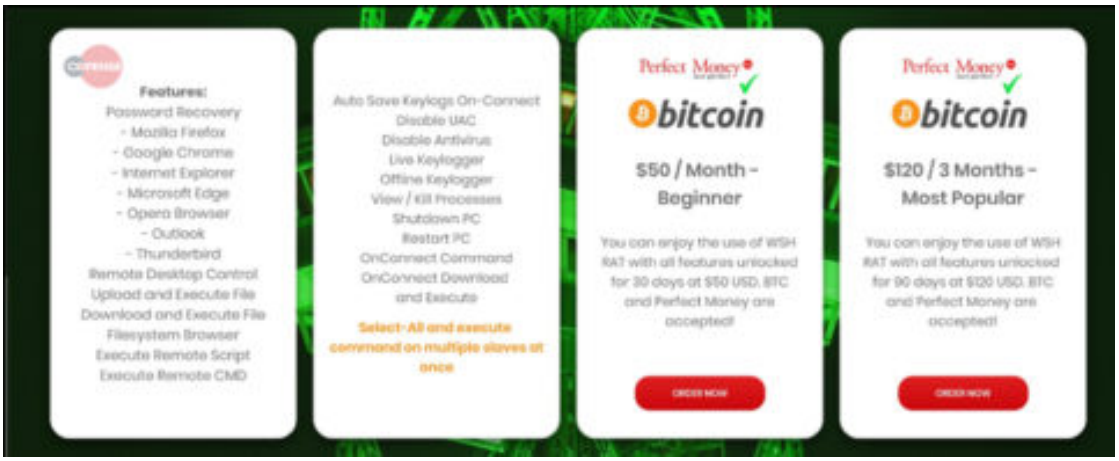

Figure 9: WSH RAT's marketing campaign

This re-hash of Hworm proves that threat operators are willing to re-use techniques that still work in today's IT environment. The phishing campaign that delivered the .zip containing a MHT file was able to bypass the Symantec Messaging Gateway's virus and spam checks, shown in Figure 10, and make it to the endpoint.

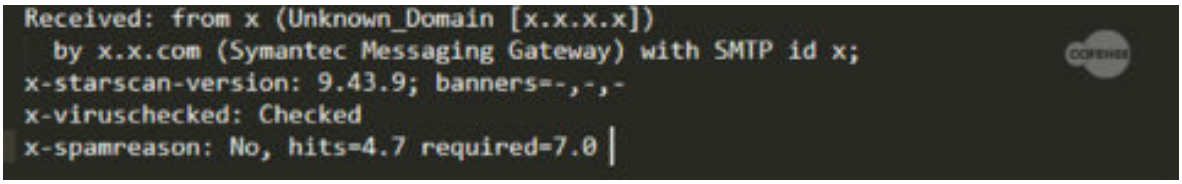

Figure 10: Symantec Messaging Gateway checks made on the phishing email

Cofense™ Can Help

This threat exhibits the ease with which new malware can be developed, purchased, and weaponized. With a small investment in cheap command and control infrastructure and an easy-to-purchase malware-as-a-service, a threat actor with otherwise limited capabilities can knock on the door of a large financial company's network in no time.

Luckily, the Cofense Phishing Defense Center was alerted to this phishing email and stifled it before any damage occurred. The customer uses Cofense PhishMe™ to help employees identify phish and Cofense Reporter™ to notify security teams. It's a combination that works —against plug and play threats and a whole lot more.

Appendix

URL
hxxp://elcisneblanco[.]com/tmp/banking/details/bank[.]php
hxxp://futuroformacion[.]es/moodle/calendar/amd/BANK DETAILS CONFIRMATION_PDF[.]zip
hxxp://doughnut-snack[.]live/klplu[.]tar[.]gz
hxxp://doughnut-snack[.]live/bpvpl[.]tar[.]gz
hxxp://doughnut-snack[.]live/mapv[.]tar[.]gz
hxxp://www.tcoolsoul[.]com:1765/is-ready
hxxp://brothersjoy[.]nl
hxxp://savelifes[.]tech

IP

192[.]185[.]26[.]103
192[.]185[.]163[.]240
23[.]105[.]131[.]191
23[.]105[.]131[.]225
185[.]247[.]228[.]49

MD5
986ffeb04fa5e01dd03b38bdd379ab51
266788057a7100afb9f123531b07282d
5a2b62b657782f37eb0f7c27064cffa9
977e42c09f7f98cfdcbf28ab2c460190
7099a939fa30d939ccceb2f0597b19ed
3a6b304e0a3dc91cac8892446826ffcc
c4c6fe64765bc68c0d6fcaf2765b5319