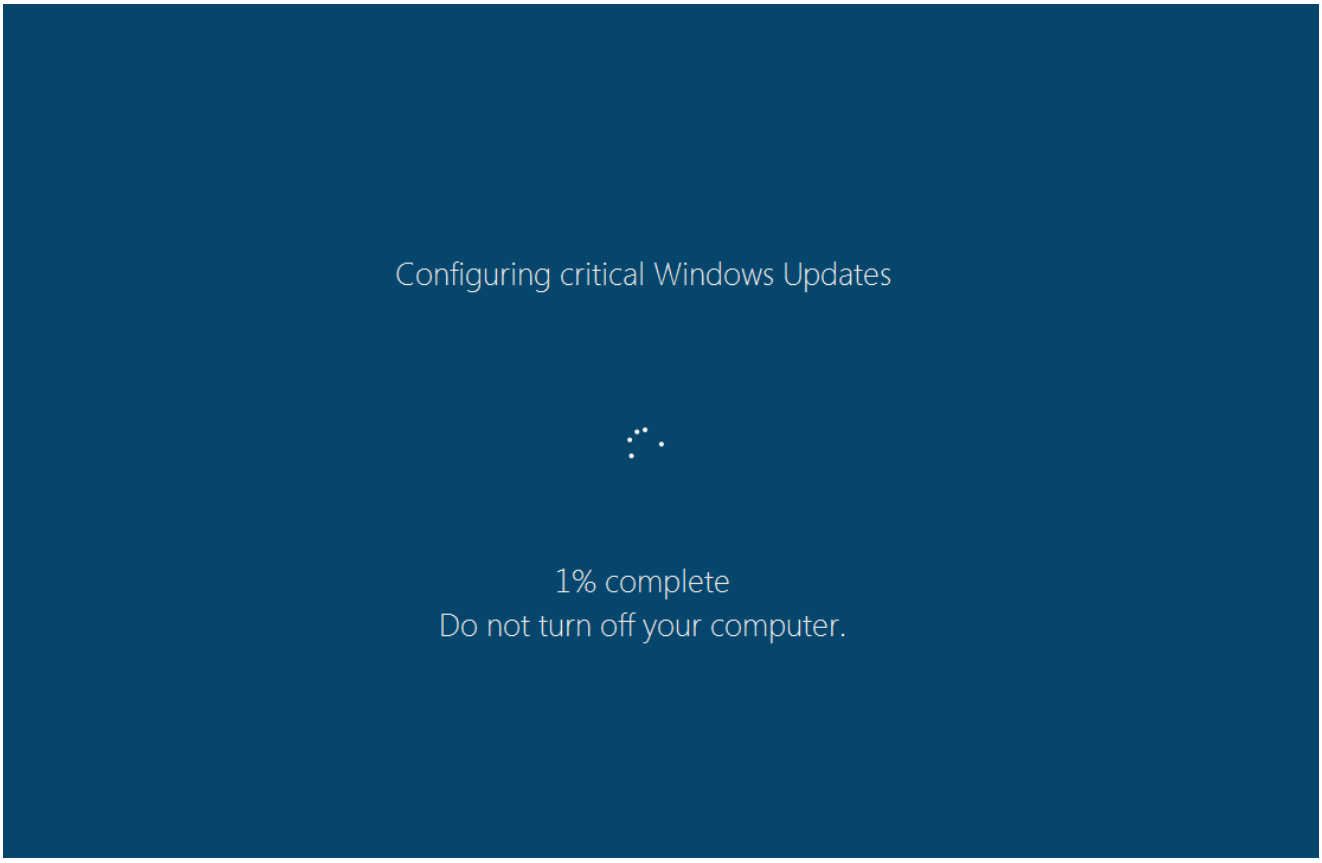
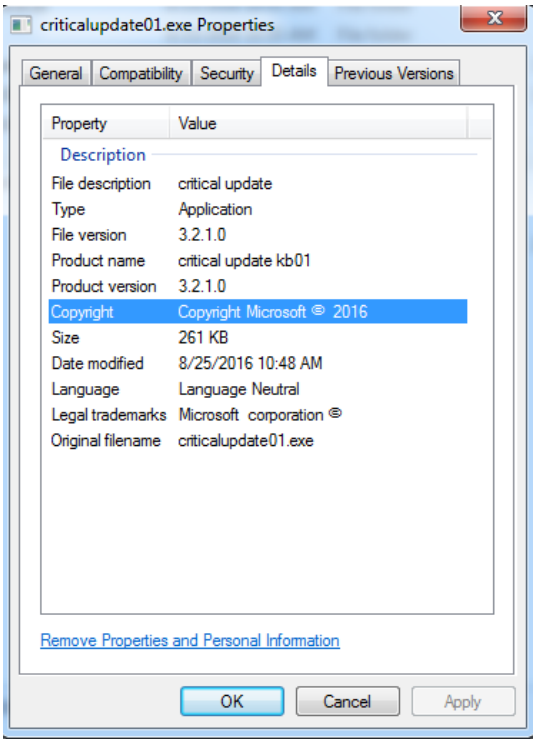
Fantom ransomware impersonates Windows update

webroot.com/blog/2016/08/29/fantom-ransomware-windows-update/

Tyler Moffitt August 29, 2016



Windows 10 has been notorious about automatically installing updates on users' machines and now there is a ransomware that aims to capitalize on it. The new ransomware, Fantom, is based on the EDA2 open-source ransomware project on GitHub called hidden tear that's recently been abandoned.



Fantom behind the scenes

In an attempt to conceal malicious intention, the authors of this ransomware modified the file properties to show copyright and legal trademarks mimicking a Windows update.

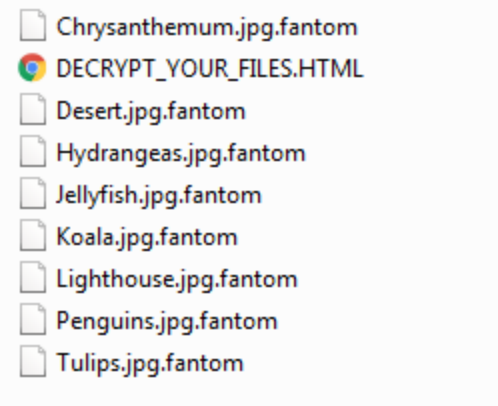
Once this dropper is executed, the payload “WindowsUpdate.exe” is dropped in AppData\Local\Temp displaying the fake Windows Update screen as shown below. This screen locks you out of doing anything else on your computer, keeping in line with the scam that Windows 10 doing its normal interrupt of updates.

The percentage counter does work and will go up at about a percent per minute. However, it’s fake and doesn’t represent anything other than to communicate to you that this “Windows update” will take a while and that you shouldn’t be alarmed of CPU usage and hard drive activity. You can close this fake update overlay by ending the process “WindowsUpdate.exe” using task manager, but the encryption of your files is unaffected.

DECRYPT_YOUR_FILES.HTML ransom note

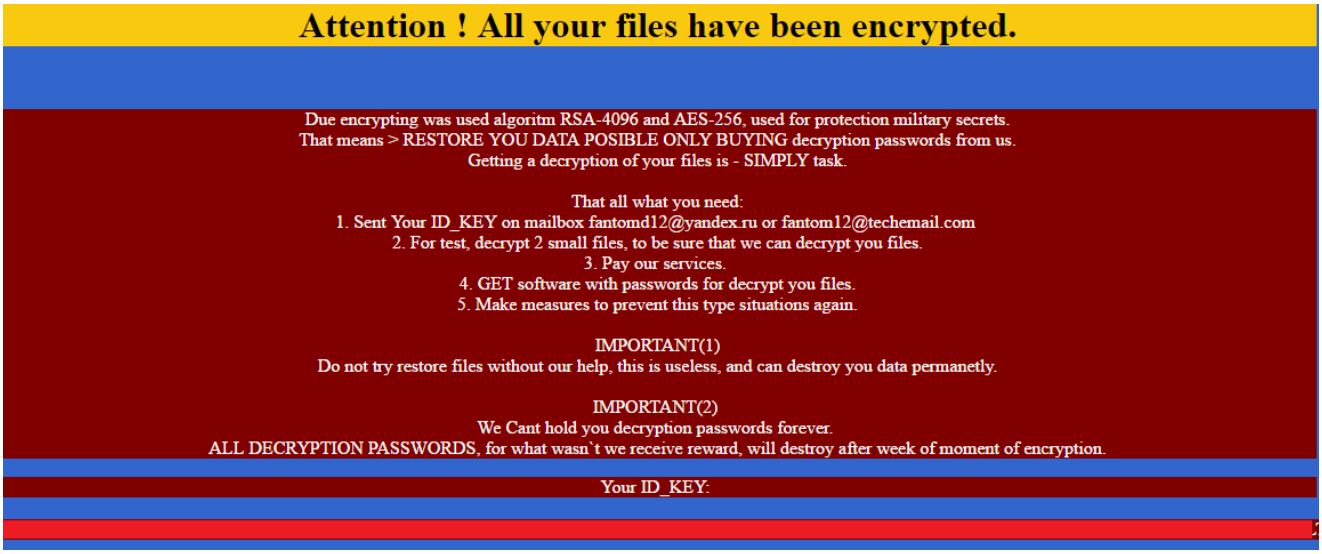
Encryption is done using AES-128 encryption and when a file is encrypted it will append “.fantom” to the extension of the file. Also in every directory that a file is encrypted, a standard ransom note “DECRYPT_YOUR_FILES.HTML” is created.

The ransom note doesn’t have an onion link as your payment portal for your files – a standard for most encrypting ransomware. Instead, you’re asked to email the cyber criminals and await response. This tactic is meant to target less savvy computer users who would be intimidated by creating a bitcoin wallet address and using a tor browser to connect to the



darknet for ransom payment. To increase odds of gaining trust, two “freebie” files for decryption are allowed.

However, it’s clear that these cyber criminals have a very loose grip on the English language so we don’t anticipate much traction with their scams through email. We also reached out as a test and have yet to hear back in over 24 hours.



Employ a backup solution

Webroot will catch this specific variant in real time before any encryption takes place. We’re always on the lookout for new threats, but just in case of new zero-day variants, remember that with encrypting ransomware, the best protection is going to be a good backup solution. This can be either through the cloud or offline external storage. Keeping it up to date is key so as not to lose productivity. Webroot has backup features built into our consumer product that allow you to have directories constantly synced to the cloud. If you were to get infected by a zero-day variant of encrypting ransomware, you can just restore your files back as we save a snapshot history for each of your files up to ten previous copies. Please see our community post on best practices for securing your environment against encrypting ransomware.

MD5 Analyzed: 7D80230DF68CCBA871815D68F016C282

Additional MD5 seen: 4AC83757EBF7ACD787F732AA398E6D53
65E9E1566DEC1586358BEC5DE9905065
60DBBC069931FB82C7F8818E08C85164
86313D2C01DC48D617D52BC2C388957F

About the Author

Tyler Moffitt

Sr. Security Analyst

Tyler Moffitt is a Sr. Security Analyst who stays deeply immersed within the world of malware and antimalware. He is focused on improving the customer experience through his work directly with malware samples, creating antimalware intelligence, writing blogs, and testing in-house tools.