# WannaCry Ransomware – Dynamic Analysis

# Report

# By John Hulett and Mike Pendleton

Contents

[Analysis or Solution (Mike) 3](#_heading=h.2et92p0)

[Replication/Generation (Mike) 3](#_heading=h.tyjcwt)

[Result Improvement (Mike) 3](#_heading=h.3dy6vkm)

[Security Analysis Techniques (John) 3](#_heading=h.1t3h5sf)

[Alternative Methods (John) 4](#_heading=h.2s8eyo1)

[Concern and Comments (John) 4](#_heading=h.3rdcrjn)

[Conclusion (John) 4](#_heading=h.26in1rg)

### Introduction (John)

### Analysis or Solution (Mike)

### There has not been a source that has been able to confirm what the actual downloader was, or if there was a mix of downloaders that would deliver the payload to the systems. For instance, after wannacry’s first variant a downloader known as pinkslip was gaining popularity as it was able to deliver payload from eternal sites. It has not been confirmed on if pinkslip was used, however I (Mike Pendleton) was involved during the time at McAfee assisting customers that has this infection as I was on the Malware team. Wannacry is expected to have been provided through spam email. This is according to McAfee Threat advisory for Wannacry: “https://kc.mcafee.com/resources/sites/MCAFEE/content/live/CORP\_KNOWLEDGEBASE/91000/KB91863/en\_US/McAfee\_Labs\_WannaCry\_June24\_2018.pdf”

### The internal dropper used a hash of “24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c” in order to download DoublePulsar if it was not installed. This would then expose the system through Eternal Blue, which exposed MS17-010 after the elevated privileges were ran in order to install all malicious code needed.

### Eternal blue was mostly used for the internal propagation of the IRC. The payload would check to see if the vulnerability was patched, and if not then it would continue and once all infections were in place, the encryption phase would begin.

### Wannacry was also not coded as a worm, but exhibited worm like behavior because it spread through the vulnerability where it impacted system shares. This did include internal shares of drives, for instance C$, D$.. etc. Since port 445 was used, this is how the worm like behavior was able to spread on its own. The malware authors knew this and therefore, did not have to spend additional time in coding in order to morph from an infection to a worm.

### Post encryption phase, a droplet was placed on the desktop and the wallpaper was changed. This was done for two purposes. The first was to notify the user that they were impacted, and the second was how to pay the ransom in order to recover the system.

### I believe that Wannacry started the popularity for ransomeware. It is easier to code and extremely dangerous. Organizations today need to combat ransomeware and the only way to do so, is to make sure that the anti-malware software is up-to-date in dat content, backups are taken consistently and stored is a secure location so that they will not be corrupt or end up encrypted as well. This is because the only other options are to pay the ransom, or start the os over from scratch.

### Replication/Generation (Mike)

### Considering replicating or to determine if the wireshark results will show how the download was able to make it from source to destination is not something that I could recommend. This is because there are a couple things that would need to be done. In order to replicate, the system would need to be sandboxed, but also have access to a wan link in order for the download process to complete.

### Post configuration, then the patched exploit MS17-010 would need to be removed. Finding a spam email would also need to happen and then clicking on the links in the email in order to continue. The anti-malware software would have to be disabled fully as well. Then start a procmon and you would be able to see the various tasks downloaded on disk.

### Since this outbreak began over 4 years ago, there is several analyses available on the payload with multiple security vendors, so reproducing a known threat is no longer needed. The behavior is known, and all variants are included for protection against the threat to prevent infection if the exploit has not been patched. It is a misconception that anti-malware software protects against vulnerabilities. They simply with protect known threats that are using the vulnerability and depending upon the vulnerability exposed is up to that vendor to patch to software. This is the only real solution, and the end users would need to make sure they are up-to-date on patches as well.

### Result Improvement (Mike) A

### As stated prior, since the full analysis is available I do not see a way this could be improved. The current known behavior allows away to protect systems through access protection even if a new variant occurs. How Access Protection rules works, is once configured Access Protection will block access to specific locations depending how coded.

### Wannacry extensions to put in place to block were .WNRY, .WNCRYT, .WNCRY, .WNRY, AND .WCRY. An example on how to code Access protection rules is covered well in McAfee KB89335, for end users and customers using McAfee’s Enterprise software.

### Security Analysis Techniques (John)

## Is it possible to further use the same techniques in other information security analysis? The paper on WannaCry analysis provided details on the following techniques. Process monitoring and analysis, Network activity using process hacker and Wireshark, and YARA rules. This techniques can be used in information security analysis on DLL injections both classic and reflective, thread execution hacking, and PE injections. Since these types of injections create suspicious network activity from a legitimate process or by creating malicious files we can utilize process monitoring to see if any suspicious processes appear, Wireshark would detect any unauthorized IP addresses and packets. Once we have determined the threat we can update our YARA rules to harden the system.  Process monitoring can be used to defend against threats such as the Morris and Mydoom worms (<https://www.upguard.com/blog/types-of-malware>). Wireshark can be used to monitor daily traffic for most networks so the performance of analysis of the IP addresses and packets can be used in security as well as network performance. Corporations could use it to monitor traffic for employee productivity and continuous improvement on the network security. New websites popup daily and employees always want to browse for new and exciting things, process monitoring and Wireshark can help a corporation improve/update their IP whitelisting and IP blacklist.

## Alternative Methods (John)

## There are alternative tools available for networking monitoring such as Cloud Shark and Colasoft Capsa. Cloud Shark claims to help solve network issues faster, however it does not do captures, instead it archives, tags, and a way to view the packets. Colasoft Capsa does capture the packets and provides a

powerful visualization of the network traffic and packet activity. However the price tag is hefty and is suited to larger corporations. These alternatives and many others can provide similar network monitoring, however the decision to employ one or more of these tools comes down to the organization's network and security configurations, information technology budget, and the risk appetite. We also think the type of industry also plays a factor in this as a small boutique with a small network might determine they have a low risk in being attacked by hackers, so they might employ out of the box security and use command line tools, where a bank might employ the gambit of network security tools to prevent any attacks as the have a high risk of being attacked. The type of malware also plays into which tools are effective to detect, monitor and recover from an attack. WannaCry was a unique case as it was not a worm, so the detection was not as simple as your average worm. Given that hackers around the globe are giving birth to new malware frequently it is imperative that regardless of the tools used for monitoring and analyzing the network security must be reviewed and updated as often as possible.

## Is there any alternative method or tool (e.g. GNS3 simulated network + Wireshark) you can recommend for the same purpose?

* depends on the malware purpose, lets research and compare tools
* process explorer, autorun, regedit, process monitor, process hacker -these are windows based on software
* are there any other windows tools that are similiar or not, provide why either way

## Concern and Comments (John)

## Conclusion (John)