# Why NotPetya Kept Me Awake (& You Should Worry Too)

By hacks4pancakes

Published: 2017-06-28 · Archived: 2026-04-05 16:52:55 UTC

NotPetya may not have been the most sophisticated malware ever written. However, it was exceptionally effective due to the authors' savvy exploitation of common security misconceptions and their deep understanding of poor security architecture. I want to briefly express my personal thoughts on why I found NotPetya particularly concerning and a bad omen for things to come for the digital world.

## Living Off The Land

A lot of the news coverage on NotPetya is focusing heavily on the use of the stolen EternalBlue (MS17-010) exploit. In my opinion, this distracts from something more sinister, because patching Windows is in many cases a relatively clear and simple fix.

NotPetya has a choice of several means to move across a LAN once it is inside a perimeter. As well as exploiting MS17-010, it can also use PsExec and WMIC to move from system to system after using a stripped down version of the Mimikatz tool to steal passwords from the system it is on. PsExec and WMI are common methods of administering Windows systems and are provided by Microsoft.

I'm honestly a little surprised we haven't seen worms taking advantage of these mechanisms so elegantly on a large scale until now. They are very popular tools in modern hacking. A good hacker avoids the use of malware and code exploits whenever possible. He or she may use them occasionally where no other practical option exists – for instance, exploits might be needed to escalate privileges on a system, or malware for initial phishing compromise – but every use of malicious code is one more potential detection point for traditional signature-based antivirus and Intrusion Prevention Systems (which are relied on exclusively far too often). **There's no sense in using malicious code when simpler and quieter means are available.**

The use of WMI to move laterally across a network is increasingly trendy, and the use of PsExec to do so is nigh archaic now. Both methods remain stunningly effective, because they are popular avenues for systems administration and often inadequately monitored. Logging of WMI lateral movement was quite tricky until Windows 8, and with large swathes of Windows 7 (and older) still in use in business it's still frequently neglected.

The use of these propagation methods alone is not likely to fire any built-in attack signature in traditional, signature-based security tools. There's nothing to sandbox nor an unusual unique file hash to scan for. On the surface, this activity will look like administration, and might only be detected by more detailed behavioral analysis. With the speed that NotPetya was able to spread, this isn't particularly practical.

## Abusing Mandatory Software

One of the primary initial infection vectors of NotPetya was the compromise of the update package for a piece of Ukrainian financial software, M.E.Doc. According to reports, this software is one of only two software options Ukrainian businesses have to pay their taxes. This was a clever choice for three reasons:

1. Attacks were constrained somewhat to Ukraine (and companies that have interests there).
2. The distribution base within the country was extremely comprehensive. Ukrainian businesses would have a high chance to have this software on a computer.
3. The software company was relatively small and may potentially have been compromised previously, indicating it was potentially under-equipped to rapidly respond to a sophisticated attack on this scale.

This is obviously not a new thought pattern – attackers have leveraged popular, commonly deployed software for exploitation for decades. Adobe Flash and Java were two of the more abused programs in recent history because they had extremely wide installation bases. However, that was within the context of commodity malware and crimeware which typically infect victims fairly indiscriminately. NotPetya delivery combined elements of a targeted watering hole attack we've traditionally seen used by nation states with traditional software exploitation to devastate a specific user base. Obviously, the potential of this avenue of attack can be explored further in the context of nearly any country or demographic.

## Masquerading as Ransomware?

In both the case of WannaCry and NotPetya, we saw malware that was ostensibly ransomware end up not looking as much like it after a deep dive under the hood and into attacker behavior. WannaCry had lackluster response to handling actual payments, and NotPetya looked deceptively identical to the older ransomware Petya on the surface while functioning quite fundamentally differently (and not being particularly well designed to make money). This sowed confusion for responders, and eager security companies posted early misleading reports. Masking targeted attacks as crimeware is an interesting strategic choice which could indicate a number of very troubling things. I will leave further speculation on those to my natsec and threat intelligence colleagues.

Ransomware is loud. Until Cryptolocker in 2013, the majority of crimeware tended to be purposefully quiet – stealing data and performing other nefarious tasks without its victim's knowledge. Ransomware is intentionally disruptive. Independent of anything "cyber" it is also a tremendously effective criminal enterprise model, so it has become increasingly popular. There is plenty of clear evidence in the form of money and news stories that demonstrates how much ransomware can impact victim organizations and individuals' lives. This means ransomware is also a great pretense for groups with other motives. They know their attack will cause misery and lost money, and news organizations cover ransomware attacks enthusiastically (often without much further digging).

## Abuse of Poor Network Security Architecture

Beyond the use of native tools, NotPetya's lateral movement mechanisms were extremely effective because they exploited common weaknesses in many big networks. Of course, unpatched (or not recently rebooted) Windows hosts were vulnerable to MS17-010 exploitation. Beyond that, lateral movement with WMI and PsExec is very effective in environments with poor network security architecture and implementation. Flat networks without segmentation were vulnerable. Networks where their use was permitted were vulnerable. Networks where desktop

users commonly had workstation admin or domain admin permissions were vulnerable, and networks where these privileges were not restricted or tightly controlled were more so. Windows 10 credential guard was a potential mitigation against the theft of passwords from system memory, but it is infrequently deployed and not backwards compatible (or indeed, even compatible with every computer running Windows 10).

All of these design and implementation problems are woefully common, repeatedly bemoaned by security professionals auditing and consulting on those networks. They are not easy or cheap problems to fix in many cases, and this is likely not going to be the case that pushes a lot of vulnerable organizations over the edge in mitigation.

## Yes, I'm Concerned

**If you work outside Ukraine, you probably got really lucky, yesterday.** Many enterprises were tremendously vulnerable to this type of attack, had they merely been targeted by the initial attack vector one time.

**Blood is in the water.** Not only have criminals found that ransomware is a great money-making scheme, but nation states and terrorist organizations have realized pseudo-ransomware makes a misleading and effective weapon. A weapon that can cause collateral damage, globally.

**Things are going to get worse**, and the attack landscape is going to deteriorate. Malware relying more on legitimate credentials and native tools may easily render signature-based and hash-based solutions fundamentally less effective defenses. Organizations must no longer rely on black boxes with good sales pitches to band-aid fundamental architectural failures and neglected security best practices like out of date operating systems, liberal administration policies, legacy protocols, or flat networks. Defense in depth, including human threat hunting and effective detection and prevention at many points, is key. This will involve policy and financial buy-in from many lagging organizations at a new level.

https://twitter.com/HackingDave/status/879864060392742913

***Edit: 6/28 10PM*** *– Minor technical corrections to clarify the purpose of M.E. Doc, the debate over encryption issues in NotPetya, and grammatical errors. Thanks to MalwareTech, grugq, and Jim Moore for pointing out my omissions, and duplicate words!*

***7/5 3PM –*** *A video was posted of the seizure of M.E.Doc's equipment which shows the equipment and approximate number of employees at the firm. https://www.youtube.com/watch?v=TY5f2fmwcDE*

This blog will be updated as further information is available.

---