GlobalResearch
Center for Research on Globalization

The Global Information Environment: Malware, Data Hijacking, Encrypted Files, Unpatched Computer Systems…

By Dr. Binoy Kampmark
Global Research, May 15, 2017
Region: USA
Theme: Intelligence

What a stealthy bugger of a problem. Malware deftly delivered, locking the system by encrypting files and making them otherwise impossible to access unless a fee is paid. A form of data hijacking that can only be admired for its ease of execution, for its viral-like replication that seeks, even hunts, vulnerable "unpatched" computer systems.

The global information environment is well and truly primed for plunder, vulnerable to such malicious "worms" as WannaCry. Each age creates the next circumstance for profit, often outside the boundaries deemed acceptable at the time. In a networked age reliant on huge quantities of data, times are good for the intrepid.

The weekend reporting on the WannaCry ransomeware worm was filled with predictable gruesomeness, suggesting that the unfortunates turning up to work on a Monday could well discover they were unable to access work files.

Much of the damage had already been done, with notable targets being the National Health System in Britain, and the Spanish telecommunications company Telefonica.[1] In Britain, patients had to be relocated, and scheduled operations and treatment delayed if not cancelled altogether. Crisis meetings were held by members of the May government. As one doctor put it in eerily apocalyptic fashion, "our hospital is down."

Another notable country target was Russia, including networks within the Interior Ministry, suggesting that the cyber misfits in question may have overstretched in their enthusiasm.[2] Russia tends to figure, as it does in other jottings of demonology, as a place of sanctuary for the cyber crooked, bastion where IT sorties can be launched. But not now.

More useful, if sobering analysis, came from Nicholas Weaver, who noted that the strength of the attack was its multi-vector nature.

> "If a targeted user receives a worm-laden email and clicks on the attachable executable, the worm starts running."[3] (Computer speak tends to get mangled in its descriptions, since worms would otherwise crawl. But not wCry, which does its damage at an enthusiastic gallop.)

This delightful worm capitalises on a vulnerability evident in the network protocol in Microsoft Windows termed Server Message Block. This is where the ransomeware does its bit, encrypting the files in question, and locking out users on pain of ransom.

Much in this saga is based on systems that were never reformed. UK Health Secretary Jeremy Hunt had been badgered by his shadow counterpart, Jonathan Ashworth, that the NHS's computer systems were dangerously outdated and susceptible to attack.[4]

While victim blaming is second nature to this trade, Weaver's salient observation is that the computer industry is just as responsible, if not more so. The persistent use of executable attachments should trigger liability, if not shame.

Developers and members of industry, in other words, should be made the classroom dunces.

> "Our bottom line up front," claim Ben Buchanan, Stuart Russell and Michael Sulmeyer for Lawfare, "is that, VEP (Vulnerabilities Equities Process) or no VEP, today's ransomeware attack highlights the risks of relying on software that is no longer supported by its developer (like windows XP) and of not applying patches that the developer makes available (like MS17-010)."[5]

This brings us to the body that keeps giving, albeit indirectly and haphazardly: the US National Security Agency. In April, a group calling itself Shadow Brokers released a set of tools pilfered from the NSA, including the vulnerability occasioned by SMB.

The Microsoft public relations machine went through the motions of putting out the fires, explaining that the company had already dealt with the vulnerabilities (patched them, if you will) in March, including a patch against the spread of the WannaCry ransomeware. Much of this was occasioned by a helpful disclosure to the company from US government sources.

This entire process revealed a certain dance between government agencies and vendors in the exchange system known as the VEP. Through this tense understanding, the US government designates which discovered software vulnerabilities should be passed on to vendors.

The vendors, in turn, apply the relevant, protective patches, though whether this is actually done is quite another matter. There is also every chance that the US government will refuse to reveal such a vulnerability in the first place. Being in the business of hacking, some cards will be well and truly hidden, to be procured when required. Such an instance arose in 2014, when the Heartbleed vulnerability was exposed to much fanfare. The response from US government officials was one of implausible deniability.

Entities such as the Patients' Association in Britain have condemned the outfit behind the attack, but also noted that the entire establishment remained green and inadequately prepared. Unprotected and unbacked, software left unsupported by developers is fit for the dustbin of history. In the meantime, the catastrophe stemming from future attacks is easy to envisage.

Dr. Binoy Kampmark is a senior lecturer at RMIT University, Melbourne and former Commonwealth Scholar at Selwyn College, University of Cambridge. Email: bkampmark@gmail.com.

Notes

[1] http://www.reuters.com/article/us-spain-cyber-idUSKBN1881TJ

[2] http://varlamov.ru/2370148.html

[3] https://www.lawfareblog.com/crying-about-wannacry-notable-features-newest-ransomware-attack

[4] https://www.theguardian.com/society/2017/may/13/jeremy-hunt-ignored-warning-signs-before-cyber-attack-hit-nhs

[5] https://www.lawfareblog.com/real-lesson-wannacry-ransomware

---