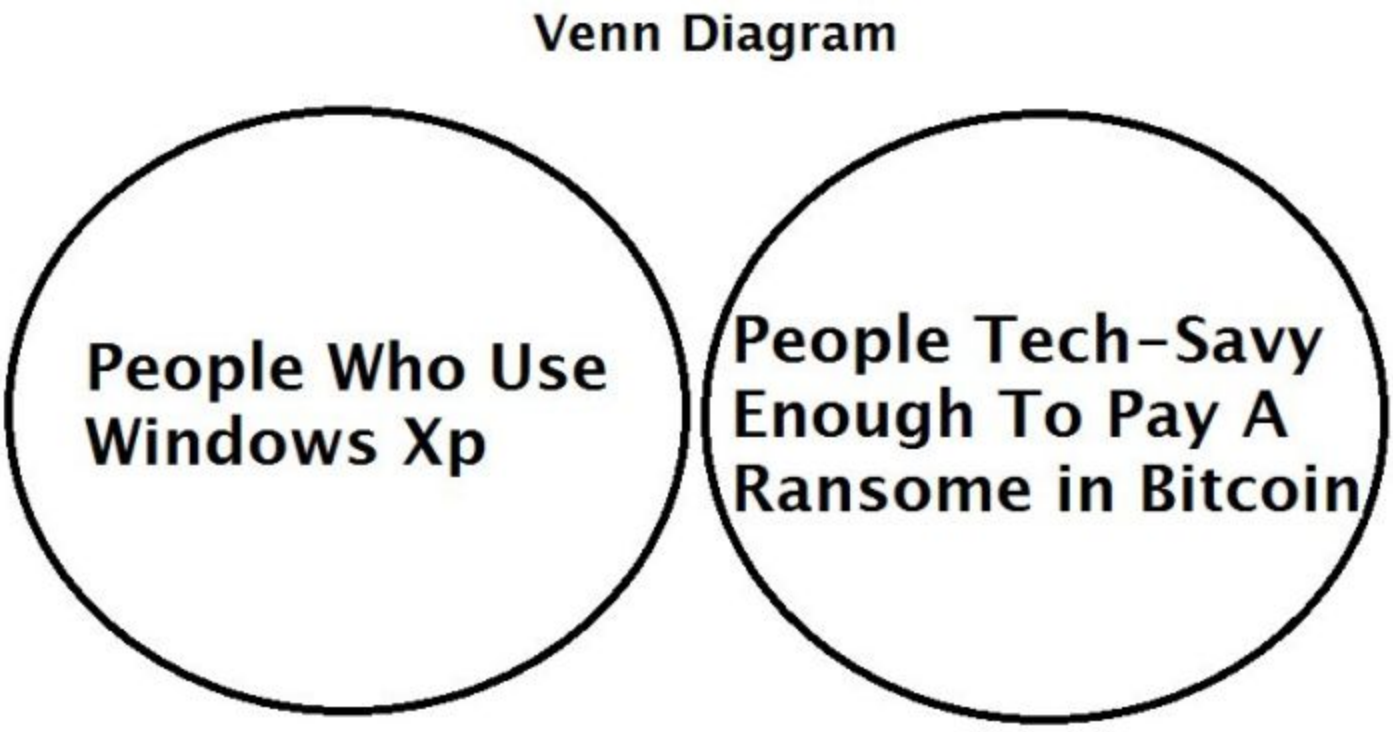
Security Now! #612 - 05-16-17

Makes You WannaCry

This week on Security Now!

This week Steve and Leo discuss an update on the FCC's Net Neutrality comments, the discovery of an active keystroke logger on dozens of HP computer models, the continuing loss of web browser platform heterogeneity, the OSTIF's just-completed OpenVPN security and practices audit, more on the dangers of using smartphones as authentication tokens, some extremely welcome news on the Android security front, long-awaited updated password recommendations from NIST, some follow-up errata, a bit of tech humor and miscellany, closing the loop with some listener feedback... then a look at last week's global explosion of the WannaCry worm.

"The Flaw in the WannaCry Extortion Scheme"



Security News

Last Thursday the FCC stopped accepting Net Neutrality comments

- https://www.techdirt.com/articles/20170512/12095837350/fcc-temporarily-stops-taking-net-neutrality-comments-so-fcc-can-reflect.shtml

- There were reports of spamming and DDoS attacks.

- Techdirt's Karl Bode's article wrote: The FCC Claims that a DDoS Attack -- Not John Oliver -- Crashed Its Website. But Nobody Seems To Believe Them.
    - The "attacks" occurred at the exact moment John Oliver announced the "GoFCCyourself.com" domain redirect.
    - The commenting system wasn't unavailable, just very slow.
    - There was none of the usual post-attack claiming of responsibility or back-channel chatter.
    - And, requests from the press for additional information about the "Attacks" were met with complete silence.

- Specifically:
    - John Bambenek a threat intelligence manger at Fidelis Cybersecurity was quoted, saying: "There don't appear of be any indications of a DDoS attack in the sensors we use to monitor for such things. It appears the issue with the FCC is less of a DDoS attack, traditionally defined, and more of an issue of crowdsourcing comments generated by John Oliver and reddit."

    - Jake Williams, CEO of cybersecurity firm Rendition InfoSec, said the FCC "offered no support" to prove a DDoS had occurred, adding: "There was no observed DarkWeb chatter about such a DDoS before or after the event and no botnets that we're monitoring received any commands ordering a DDoS on the FCC's site."

HP Conexant Audio Driver found to be logging keystrokes

- As Ars put it: "HP is selling more than two dozen models of laptops and tablets that covertly monitor every keystroke a user makes, security researchers warned Thursday. The devices then store the key presses in an unencrypted file on the hard drive."

- It appears that highly irresponsible keystroke logging with permanent stroke-by-stroke persistent storage, has been in place for more than two years (since December 24th, 2015) in many HP machines using Conexant audio chips.

- The security firm, ModZero, who disclosed this noted that: "Version 1.0.0.31 of this program was later extended by even more problematic functions: The most recent version 1.0.0.46 implements the logging of all keystrokes into the publicly for any user readable file C:\Users\Public\MicTray.log.

- Although the file is overwritten after each login, the content is likely to be easily monitored by running processes or forensic tools. If you regularly make incremental backups of your hard-drive - whether in the cloud or on an external hard-drive – a history of all keystrokes of the last few years could probably be found in your backups.

  The keylogger is included in a device driver developed by Conexant, a manufacturer of audio chips that are included in the vulnerable HP devices. That's according to an advisory published by modzero, a Switzerland-based security consulting firm. One of the device driver components is MicTray64.exe, an executable file that allows the driver to respond when a user presses special keys. It turns out that the file sends all keystrokes to a debugging interface or writes them to a log file available on the computer's C drive.

  "This type of debugging turns the audio driver effectively into keylogging spyware," modzero researchers wrote. "On the basis of meta-information of the files, this keylogger has already existed on HP computers since at least Christmas 2015."

  There is no evidence that this keylogger has been intentionally implemented. Obviously, it is a negligence of the developers - which makes the software no less harmful. If the developer would just disable all logging, using debug-logs only in the development environment, there wouldn't be problems with the confidentiality of the data of any user.

- All users of HP computers should check whether the program C:\Windows\System32\MicTray64.exe or C:\Windows\System32\MicTray.exe is installed. We recommend that you delete or rename the executable files so that no keystrokes are recorded anymore. However, the special function keys on the keyboards might no longer work as expected. If a C:\Users\Public\MicTray.log file exists on the hard-drive, it should also be deleted immediately, as it can contain a lot of sensitive information such as login-information and passwords.

- Links:
  - https://www.modzero.ch/advisories/MZ-17-01-Conexant-Keylogger.txt
  - https://www.modzero.ch/modlog/archives/2017/05/11/en_keylogger_in_hewlett-packard_audio_driver/index.html

SMG: This is one of those things that has became a lot more worrisome once it has been widely and publicly disclosed. So while it was doubtless inadvertent, it's still present unless action is taken. And now the bad guys know it's there and where to look for a little honeypot of recent keystrokes.

The Windows platform has never been secure. The ability for a debugger to "attach" to another process is both convenient and horrific for security. Windows apps can freely establish "global hooks" for adding assistive features. Keystroke macro programs can freely inject keystrokes into other processes and programs, etc. Programs can "capture" the screen. Windows as traditionally been a developer-friendly power user's environment. This is part of what Microsoft plans to be changing with Windows S -- which implements highly restrictive application sandboxing.

We're Losing Browser Heterogeneity:
https://www.bleepingcomputer.com/news/microsoft/microsoft-has-effectively-banned-third-party-browsers-from-the-windows-store/

A one-liner in the Windows Store policy is the reason why we'll never have the "original" Chrome, Firefox, Opera, or other browsers available through the official Windows Store.

Included in the "Security" section of the Windows Store policy, this line is specifically addressed at browsers, and reads the following:

<quote> Apps that browse the web must use the appropriate HTML and JavaScript engines provided by the Windows Platform.

This means that every browser currently listed on the Windows Store is nothing more than an off-shoot of Microsoft's EdgeHTML, the HTML and JavaScript engine found in Edge.
Apple, Google have similar policies

The policy is similar to what Apple has done with iOS, the company forcing apps to use its web rendering engine to process web content. Google took a harder stance with ChromeOS and forbade other browsers altogether.

In both cases, the companies cited security concerns, as their engineers have worked to secure their operating system around those web rendering engines.

In the case of the Windows Store, this revelation came to light after the launch of Windows 10 S, a tethered version of Windows 10 that will only allow the installation of Windows Store apps.

As users kept asking when will Google and Firefox port their browsers for the Windows Store — so they could use them in Windows 10 S — the question was answered last week when a developer tried to convert his Chromium-based browser to an .appx version, compatible with Windows Store distribution.

The Windows Store crew specifically told the developer that they cannot approve his browser because of the aforementioned policy that mandates that all apps that access the Internet use the approved HTML and JS rendering engines. The developer shared his experience and official communications with a ZDNet journalist.

Microsoft's policy effectively bans standalone third-party browsers

While some were hoping to see Chrome or Firefox available on the Windows Store as UWP (Universal Windows Platform) apps, this may never be possible, as this would mean that Google, Firefox, and other vendors would need to rewrite their browsers from scratch to use Microsoft's EdgeHTML.

This will never happen unless Windows 10 S becomes a huge success and browser vendors see a benefit to port their browsers.

In this case, we still won't see UWP versions of the original Chrome and Firefox engines, but only so-called bastard browsers, like we have on iOS.

For example, you can't call Firefox for iOS a true Firefox browser, as it's just an older version of the WebKit engine with a Firefox lookalike UI on top, and lacking many of Firefox's original features.

The conclusion is that Microsoft has effectively banned any self-standing third-party browser from the Windows Store. Additionally, Windows 10 S users better get used to using Edge or any of the other bastard browsers that use Edge's re-packaged core. This is why, Windows 10 S won't let you change your default browser away from Edge, or your search provider away from Bing.

The "original" Chrome and Firefox browsers — built around their native engines — will remain accessible to Windows 10 users, via standalone installers only.

OSTIF and QuarksLab complete their audit of OpenVPN

- https://ostif.org/the-openvpn-2-4-0-audit-by-ostif-and-quarkslab-results/

- Tweet: OSTIF Official (@OSTIFofficial) - 5/11/17, 6:28 PM
  @SGgrc You did excellent coverage of our VeraCrypt audit on @SecurityNow. We just published our @OpenVPN results!

- OpenVPN 2.4.0, the NDIS6 TAP Driver for Windows, the Windows GUI, and Linux versions were evaluated. This release included a number of new features including control channel encryption.

- QuarksLab found:
  - 1 Critical/High Vulnerability CVE-2017-7478
  - 1 Medium Vulnerability CVE-2017-7479
  - 5 Low or Informational Vulnerabilities / Concerns

- The auditors wrote: This public disclosure of these vulnerabilities coincides with the release of OpenVPN 2.4.2 which fixes all of the high priority concerns. OpenVPN is much safer after these audits, and the fixes applied to the OpenVPN mean that the world is safer when using this software. We have verified that the OpenVPN software is generally well-written with strong adherence to security practices.

- https://ostif.org/wp-content/uploads/2017/05/OpenVPN1.2final.pdf

KRAKEN: Explicitly Rethinking the Security of Phones as Authentication Tokens
http://blog.kraken.com/post/153209105847/security-advisory-mobile-phones

Kraken describe themselves as:

- Based in San Francisco, Kraken is the world's largest global bitcoin exchange in euro volume and liquidity. Kraken's clients also trade US dollars, Canadian dollars, British pounds, Japanese yen and other digital currencies on a platform consistently rated the best and most secure bitcoin exchange by independent news media.

  Founded in 2011, Kraken was the first bitcoin exchange to have its market data displayed on the Bloomberg Terminal, the first to pass a cryptographically verifiable proof-of-reserves audit, a partner in the first cryptocurrency bank, and one of the first exchanges to offer leveraged bitcoin margin trading. Kraken is trusted by hundreds of thousands of traders, institutions, and authorities across the world, from Toyko's court-appointed trustee to Germany's BaFin regulated Fidor Bank.

  Kraken is backed by investors including Hummingbird Ventures, Blockchain Capital, and Barry Silbert's Digital Currency Group, among others.

<quote: Heed this or perish.

Let's begin with the assumption that within 24 hours your usual mobile phone number will be hijacked by social engineers. They will use your number to gain access to every account you own that utilizes phone-based authentication and account recovery, like your email. They will then use that access and information to compromise more accounts, and harass, steal, blackmail and extort you and your associates.

In the past month, there have been at least 10 cases of people publicly involved in the cryptocurrency scene being victimized by mobile phone hijacking. The consequences have been expensive, embarrassing, enduring, and, in at least one case, life-threatening.

If you are in any way publicly involved in cryptocurrency, consider yourself an active target. You need to immediately audit the security of your accounts – especially email, social media, social networking and mobile phone.

Somehow, the masses have been led to believe that phone numbers are inextricably bound to identities and therefore make good authentication tools. There's a reason that Kraken has never supported SMS-based authentication: The painful reality is that your telco operates at the security level of a third-rate coat check. Here's an example interaction:

- Hacker: Can I have my jacket?
- Telco: Sure, can I have your ticket?
- Hacker: I lost it.
- Telco: Do you remember the number?
- Hacker: Nope, but it's that one right there. ;)
- Telco: Ok cool. Here ya go. Please rate 10/10 on survey ^_^

Developer's Blog: Here comes Treble - A modular base for Android
https://android-developers.googleblog.com/2017/05/here-comes-treble-modular-base-for.html

On the Android team, we view each dessert release as an opportunity to make Android better for our users and our ecosystem partners. One thing we've consistently heard from our device-maker partners is that updating existing devices to a new version of Android is incredibly time consuming and costly.

With Android O, we've been working very closely with device makers and silicon manufacturers to take steps toward solving this problem, and we're excited to give you a sneak peek at Project Treble, the biggest change to the low-level system architecture of Android to date.

The traditional cumbersome and time consuming update and patch flow has been:

- The Android team publishes the open-source code for the latest release to the world.
- Silicon manufacturers, the companies that make the chips that power Android devices, modify the new release for their specific hardware.
- Silicon manufacturers pass the modified new release to device makers — the companies that design and manufacture Android devices. Device makers modify the new release again as needed for their devices.
- Device makers work with carriers to test and certify the new release.
- Device makers and carriers make the new release available to users.

Project Treble re-architects Android to make it easier, faster and less costly for manufacturers to update devices to a new version of Android.

Android has been a fabulous success in the marketplace because it presented and rigorously enforced through its compatibility test suite (CTS) its application layer API.

Project Treble will be doing for the Android OS framework what CTS did for apps: The core concept is to separate the vendor implementation — the device-specific, lower-level software written in large part by the silicon manufacturers — from the Android OS Framework.

This is achieved by introducing a new vendor interface between the Android OS framework and the vendor implementation. The new vendor interface will be validated by a Vendor Test Suite (VTS), analogous to the CTS, to ensure forward compatibility of the vendor implementation.

Once a stable vendor interface has been defined to provide access to the hardware-specific parts of Android, device makers can deliver new Android releases and updates to consumers by only updating the Android OS framework without any additional work required from the silicon manufacturers.

And the underlying silicon manufacturers need not be constantly bothered and bombarded with updates which require their constant attention and involvement.

This will all appear in Android O and the new Project Treble architecture is already up and running on the Developer Preview of O for Pixel phones.

"O" is slated for launch later this summer.

IDG's CSO: NIST updates and improves "official" password guidelines
http://www.csoonline.com/article/3195181/data-protection/vendors-approve-of-nist-password-draft.html

Published Today, May 16th, 2017: https://pages.nist.gov/800-63-3/sp800-63b.html

A recently released draft of the National Institute of Standards and Technology's (NIST's) digital identity guidelines has met with approval by vendors. The draft guidelines revise password security recommendations and altering many of the standards and best practices security professionals use when forming policies for their companies.

Remove periodic password change requirements
NIST said this guideline was suggested because passwords should be changed when a user wants to change it or if there is indication of breach. Mike Wilson, founder of PasswordPing said: "There have been multiple studies that have shown requiring frequent password changes to actually be counterproductive to good password security."

Drop the algorithmic complexity song and dance
No more arbitrary password complexity requirements needing mixtures of upper case letters, symbols and numbers, NIST wrote. If a user wants a password that is just emojis they should be allowed. It's important to note the storage requirements. Salting, hashing, MAC such that if a password file is obtained by an adversary an offline attack is very difficult to complete. Mike Wilson added: Like frequent password changes, it's been shown repeatedly that these types of restrictions often result in worse passwords.

Require screening of new passwords against lists of commonly used or compromised passwords
NIST notes that dictionary words, user names, repetitive or sequential patterns all SHOULD be rejected. (No more Monkies!) One of the best ways to ratchet up the strength of users' passwords is to screen them against lists of dictionary passwords and known compromised passwords.

The updated NIST guidelines have much much more to say across the entire authentication security spectrum, so we'll be covering them in full detail shortly.

Errata

Justin Garrison (@rothgar) - 5/10/17, 6:47 AM
@SGgrc Quick correction on SN 611 with respect to AMT over WiFi. AMT *can* be set up w/ Intel WiFi chips. Simply requires additional settings to be enabled.

More: (Paraphrasing) If you have a laptop that supports AMT where AMT has been provisioned, if AMT has had its optional wireless support turned on and if you're running Windows... then connecting your laptop to a public wireless network means that AMT is accessible to anyone else on that network. If that machine has not received a firmware update, the null-authentication bypass vulnerability will allow anyone to access the AMT system within that machine.
If you're a corporate IT department, and if you have AMT enabled over WiFi, turn it off. Now.
http://mjg59.dreamwidth.org/48837.html

On the Lighter Side:

- SNL (Saturday Night Live), spoofing the Amazon Echo, bring us the Amazon Echo Silver Edition: https://youtu.be/YvT_gqs5ETk (2min : 40sec)

Miscellany

Grom Audio

- http://gromaudio.com/
- Grom Audio retrofits modern features to older autos!!!

Jonathan Bennett (Jonathan Bennett) - 5/15/17, 7:22 AM

- SpinRite owner and long time listener here. My son just introduced me to a puzzle game I thought you might like for iOS and Android: Squaredance

  I have found the Frontier Saga audio-books available through my library, thankfully each book is short so I can fit in Security Now between books and I don't have to fall too far behind! You were right, the action has been constant so far. I'm not quite done with the third book, but wow! Thank you for all the you and Leo do!

SpinRite

Garrett Bane wrote:

I used my personal copy of SpinRite at level 2 on my work laptop with an SSD to confirm that the drive was, in fact, dying. The early warning allowed me to pull my backups together and prevent any loss of data.

Thanks to to listening to SN since day one from my iPod I have a better understanding that most of the level 1 techs here. So glad for how far (pod)Netcasts have come and I appreciate all the work you and Leo put into the show.

I am looking forward to 6.1, 6.2 and 7 when we will see performance improvements and will be able to run it on a mac.

Please feel free to share my story/testimonial on Security Now and use my name.

Thank you,
Garrett
Jackson, Wisconsin

Closing the Loop Feedback

vega_ska (@vega_ska) - 5/9/17, 8:45 AM
@SGgrc LoadBalancing question: Google.com DNS resolves 12 ip's, but Google.com resolves 1 IP, how does this work?

Glasair pilot (@giipilot) - 5/11/17, 4:44 PM
@SGgrc Why would engineers spend the money for Android mics that have a freq response into ultrasonic?

Chris Ebert (@realchrisebert) - 5/14/17, 2:40 PM
@SGgrc It seems that it should be possible for mobile OSes to filter ultrasonic frequencies from the microphone before providing it in API

Michael Cunningham (@mikecunning) - 5/11/17, 5:44 PM
@SGgrc Ubiquiti released a security only update for the edge router line to address the udp.c vulnerability CVE-2016-10229
udp.c in the Linux kernel before 4.5 allows remote attackers to execute arbitrary code via UDP traffic that triggers an unsafe second checksum calculation during execution of a recv system call with the MSG_PEEK flag.

- v1.9.11 - April 28th, 2017

Andrew Douglas (@andyd_) - 5/15/17, 11:55 AM
@SGgrc how do TOTP apps work? I use them but have no idea how those 6 magic numbers work. Any chance you could dig in a little #securitynow

A DoD person weighed in on Missle Logic:
Just finishing episode 611 now. I work with the DoD. Missile RAM issue: It's likely far, far cheaper to double hardware rather than pay contractor to fix memory leak. (Contract ending, other important bugs to fix, etc.). After all, what's the hardware cost per missile? Likely small. How many missiles? Likely not that many.

Makes You WannaCry

What do you get when you combine an extremely old and powerful, always on and present, networked remote code exploit requiring no user interaction, with money making file encrypting malware, the inherent vulnerability of social-engineering phishing attacks, and then toss in a capable backdoor while you're at it?

Well... it just Makes you wannaCry.

A potent and capable CryptoMalware payload which leverages the NSA's leaked, ubiquitiously present and well-weaponized EternalBlue Windows SMB vulnerability for propagation.

What's in a Name?

- WCry, WanaCrypt0r, WannaCry, Wana Decryptor, etc.
- The header added to the files it encrypts is: "WANACRY!"
- And Wana Decryptor is, as its name suggests, the file decryption side.

There are now at least five identified variants, and infection estimates fall between 200,000 and 300,000 machines... with infected machines randomly scanning the public Internet for any other machines to zombiefy.

As the Worm Turns...

- It is definitely a "worm" inasmuch as it requires no user interaction and each individual instance of infection immediately begins seeking out other vulnerable machines both on the machine's own local IP network as well as out on the public Internet.

Why was the UK's NHS hit so hard?

- By some estimates, approximately 90% of the NHS in UK has remained on Windows XP and paid Microsoft hugely to extend support for an additional year past XP's patch death.

- In the case of Spain's Telefonica, the initial point of entry appears to have been a phishing eMail containing a PDF with an .HTA (HTML Application) exploit.

- (Note, there’s some dispute about that within the security community with some believing that it was just publicly exposed SMB ports that allowed the worm to gain entry into internal networks.)

Is blaming the victim here, justified?

- It's easy to do, but I think it's more subtle than that in the real world.
- In today's environment everyone should accept all available updates.
- But notice the way I deliberately phrased that... "accept all available updates."
- What about when updates are no longer being made available?
- What about WinXP embedded in a decade old MRI scanner, passenger ticketing kiosk, banking ATM machine? In many cases their manufacturer would love to profitably SELL you an updated system... but if what you have is already working just fine? Or if there isn't budget for wholesale replacing 90% of an IT infrastructure? Or what if the company who created the device(s) ten years ago is long gone?

The weird KillSwitch:

- www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
- A minor variant of the virus has been found which simply had the killswitch hexedited out. Since it was not removed with a recompile it was probably NOT done by the original malware author. And that is the only change.
- Didier Stevens noticed and noted that the Windows API used "INTERNET_OPEN_TYPE_DIRECT" resolves all hostnames locally and is therefore not DNS proxy aware. So the "kill switch" would not have stopped propagations within environments where non-proxied DNS queries are disallowed.

More Interesting Technical Details

- https://github.com/RiskSense-Ops/MS17-010/blob/master/exploits/eternalblue/ms17_010_eternalblue.rb
- This module is a port of the Equation Group ETERNALBLUE exploit, part of the FuzzBunch toolkit released by Shadow Brokers.
- There is a buffer overflow memmove operation in Srv!SrvOs2FeaToNt. The size is calculated in Srv!SrvOs2FeaListSizeToNt, with mathematical error where a DWORD is subtracted into a WORD.
- The kernel pool is groomed so that overflow is well laid-out to overwrite an SMBv1 buffer. Actual RIP hijack is later completed in srvnet!SrvNetWskReceiveComplete.
- This exploit, like the original may not trigger 100% of the time, and should be run continuously until triggered. It seems like the pool will get hot streaks and need a cool down period before the shells rain in again.

Microsoft weighs in...

Brad Smith, Microsoft's President and Chief Legal Officer
https://blogs.microsoft.com/on-the-issues/2017/05/14/need-urgent-collective-action-keep-people-safe-online-lessons-last-weeks-cyberattack/

TITLE: The need for urgent collective action to keep people safe online: Lessons from last week's cyberattack

<<snip>>

Finally, this attack provides yet another example of why the stockpiling of vulnerabilities by governments is such a problem. This is an emerging pattern in 2017. We have seen vulnerabilities stored by the CIA show up on WikiLeaks, and now this vulnerability stolen from the NSA has affected customers around the world. Repeatedly, exploits in the hands of governments have leaked into the public domain and caused widespread damage. An equivalent scenario with conventional weapons would be the U.S. military having some of its Tomahawk missiles stolen. And this most recent attack represents a completely unintended but disconcerting link between the two most serious forms of cybersecurity threats in the world today – nation-state action and organized criminal action.

The governments of the world should treat this attack as a wake-up call. They need to take a different approach and adhere in cyberspace to the same rules applied to weapons in the physical world. We need governments to consider the damage to civilians that comes from hoarding these vulnerabilities and the use of these exploits. This is one reason we called in February for a new "Digital Geneva Convention" to govern these issues, including a new requirement for governments to report vulnerabilities to vendors, rather than stockpile, sell, or exploit them. And it's why we've pledged our support for defending every customer everywhere in the face of cyberattacks, regardless of their nationality. This weekend, whether it's in London, New York, Moscow, Delhi, Sao Paulo, or Beijing, we're putting this principle into action and working with customers around the world.

Simon Zerafa (@SimonZerafa) - 5/15/17, 12:37 PM
@SGgrc No WannaCry Ransomware on Windows XP. So why did MS release the XP patches?
https://twitter.com/GossiTheDog/status/864193677060706306

Reality check - WannaCry doesn't run on XP and 2003. It reuses this exploit, which doesn't target them

https://github.com/rapid7/metasploit-framework/blob/master/modules/auxiliary/scanner/smb/smb_ms17_010.rb