reddit_nsa_10_percent.docx

Reliable information:\n\n[tl;dr read this post by Symantec](https://www.symantec.com/connect/blogs/what-you-need-know-about-wannacry-ransomware) (added 5:30 PM)\n\n* This is a Windows worm. It didn't directly affect the NHS on purpose, but apparently they didn't patch their computers. (UPDATE 3:22) Information indicates that many NHS computers were still running Windows XP, which did not get a patch for this issue. (UPDATE 4:45) [Article from December about the NHS running XP.](http://www.silicon.co.uk/security/nhs-hospitals-data-risk-outdated-windows-xp-201761)\n* The worm is spreading via leaked NSA cyber-weapons (ETERNALBLUE and maybe DOUBLEPULSAR) that were leaked by the Shadow Brokers. The vulnerability was patched by Microsoft in a critical patch update [in March 2017](https://technet.microsoft.com/en-us/library/security/ms17-010.aspx). The NSA software was not originally a worm, but was modified.\n* There appears to be more than one variant of the worm (so far, appears to be ~~four~~ ~~five~~ eight). The biggest ransomware on the scene is called Wcry / WannaCry / WannaCryptor, which was rarely seen until today.\n* (UPDATE 4:08) - **The ransomware aspect will still work, even if you aren't susceptible to the worm, so, as usual, be careful what you click on and execute. That hasn't changed. What's new here is the ability to spread to un-patched Windows computers without requiring user interaction.**\n\nEdits:\n\n* All unpatched Windows versions up through Windows 10 are affected. If you have automatic Windows Update turned on, you're probably safe from being automatically infected. Windows XP and other outdated systems were *not* patched and will remain vulnerable forever. \n* Odds are that if you're infected by this malware, you will *not* be able to recover your files without paying. You should always have an offline backup for this reason.\n\nEdit 2: [Watch the ransoms piling up here](https://blockchain.info/address/13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94).\n\nEdit 3 (3:11 PM EDT):\n\n* [And here](https://blockchain.info/address/12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw)\n* So far, the attackers have made ~$12,000 in ransoms.\n\nEdit 4 (3:15 PM): [Real-time infection map] (https://intel.malwaretech.com/WannaCrypt.html). Infections are present in 74 countries, with Russia by far the worst. (UPDATE 5/13 11:52) It appears that either his site is being hammered by a DDoS attack, or we're all simulating one by hammering him with traffic to watch the live map. Either way, good luck reaching it.\n\n~~Edit 5 (3:24 PM): The infection trigger may have been registration of a specific domain. This allowed the worm to gain some traction prior to detonation. (Unconfirmed)~~ The specific domain was actually a kill switch!\n\nEdit 6 (3:31 PM): Infection has spread to the Philippines and New Zealand. Only a few countries left with no infections, like Indonesia, where it's the middle of the night.\n\nEdit 7 (3:34 PM): [Article with lots of technical detail from Kaspersky here] (https://securelist.com/blog/incidents/78351/wannacry-ransomware-used-in-widespread-attacks-all-over-the-world/)\n\nEdit 8 (3:54 PM): ~~70,000~~ ~~75,000~~ 177,000 (as of 5/13 12:54) infected IPs have been detected so far by MalwareTech's tracking servers. This isn't the same as the number of infected computers, because many infections will be contained to a LAN, and even if they can scan the Internet, multiple infected computers on the same LAN would appear to trackers as the same IP. Infection is spreading at ~100 IPs per minute.\n\nEdit 9 (4:06 PM): [Another ransom Bitcoin wallet] (https://blockchain.info/address/115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn), thanks /u/Koi-pond!\n\nEdit 10 (4:27 PM): When we security folks say "computers", [we aren't just talking about the kind you type on] (https://twitter.com/Avas_Marco/status/863107445559889921).\n\n~~Edit 11 (4:31 PM): Bitcoin wallet payments have reached six figures in US dollars. People keep finding new ones, so I'm going to stop posting them here. (Unconfirmed)~~ (UPDATE 5:14 probably not more than $20k total)\n\nEdit 12 (4:49 PM): [Country count is up to at least 99] (http://money.cnn.com/2017/05/12/technology/ransomware-attack-nsa-microsoft/index.html).\n\nEdit 13 (5:28 PM): [List from the Guardian of affected UK healthcare facilities] (https://www.theguardian.com/society/2017/may/12/global-cyber-attack-nhs-trusts-malware)\n\nEdit 14 (5:38 PM): [Which antivirus vendors have updated to detect this malware?] (https://virustotal.com/cs/file/b9c5d4339809e0ad9a00d4d3dd26fdf44a32819a54abf846bb9b560d81391c25/analysis/) (Green checkmark indicates that the sample was *not* detected.)\n\nEdit 15 (5:54 PM): signing off for a bit, will add more updates later!\n\nEdit 16 (8:58 PM): As /u/616d9e0 reported below, malware researcher Malware Tech (the same guy who has the live infection map) registered a domain that was hardcoded in the malware. His goal was to use it as a honeypot to track infections. Turns out to have been a master kill switch to *turn off* new infections. I'm sure we'll see a new variant with different domains shortly, but this pause will give people time to patch their systems.\n\nEdit 17 (11:25 PM): See [this guy's comment](https://www.reddit.com/r/worldnews/comments/6arkxt/comment/dhhthkh?st=J2MPJLBS&amp;sh=f5271f94) for some mitigations you can apply offline so that you aren't infected while you're patching, in case the attacker manages to start things up again. /u/dack42\n\nEdit 18 (10:06 AM): The killswitch seems to be blocked by certain antivirus products (like Sophos) as well as [web proxies](https://blog.didierstevens.com/2017/05/13/quickpost-wcry-killswitch-check-is-not-proxy-aware/). This means that the domain registration will *not* block all new infections, particularly (and ironically) in highly-controlled corporate environments. \n\nEdit 19 (10:13 AM): Microsoft has released [out of band patches for unsupported operating systems](http://www.catalog.update.microsoft.com/Search.aspx?q=KB4012598), which is a very cool move on their part. So if you've got old XP machines, patch away!

We know from the [report](https://www.dni.gov/files/documents/ICA_2017_01.pdf) released jointly by the CIA, FBI, and NSA that Russia didn't just hack the DNC, but:\n\n&gt; Russia’s intelligence services conducted cyber operations against targets associated with the 2016 US\n&gt; presidential election, including targets associated with **both major US political parties.**\n\nAnd this is the *declassified* version. I would assume that everyone in the US government would want to go after Russia with a vengeance. Yet the GOP leadership in Congress has alternated between completely stalling and dragging their feet in the investigations. And now [Corker is tabling](https://www.washingtonpost.com/powerpost/senate-panel-puts-russia-sanctions-bill-on-hold/2017/05/01/248c3204-2ec0-11e7-9dec-764dc781686f_story.html) additional sanctions, even though McCain, Graham, Rubio, Sasse, and Portman [sponsored the bill](http://www.politico.com/story/2017/01/john-mccain-lindsey-graham-no-russia-sanctions-bill-233395). There haven't been *any* sanctions applied to Russia other than the ones from Obama.

The headline is misleading and definitely not a terrorism. This is not a cyber-attack against NHS. \n \nThis is WanaCrypt0r 2.0 virus, typical piece of ransomware, and infected many victims all over the world: Russia, Ukraine, and Taiwan leading - https://twitter.com/JakubKroustek/status/863045197663490053 \n \nWanaCrypt0r 2.0 is spreading using the recently disclosed EternalBlue/MS17-010 SMB RCE exploit (NSA tools). \n \nThe security update was already released by Microsoft on March 14 - https://technet.microsoft.com/en-us/library/security/ms17-010.aspx \n \nThe British National Health Service still use Windows XP, the extended support for Windows XP ended on April 8, 2014. The British government is incompetent, dumb, cheap

I hate it when people say things like this.\n\nDoes Google have a lot of power? Yes. Do they do some concerning things? Yes. But they're not [tapping the undersea cables and storing everything that goes through them](https://en.wikipedia.org/wiki/Tempora). They don't have warrantless access to a list of every site you've accessed in the past year. (Like will soon be the case in the [UK](http://www.independent.co.uk/life-style/gadgets-and-tech/news/investigatory-powers-bill-act-snoopers-charter-browsing-history-what-does-it-mean-a7436251.html) if the government has its way) And they definitely don't have [the power to throw you in jail for years on end if you do something they don't like](http://i3.mirror.co.uk/incoming/article8187797.ece/ALTERNATES/s615/Judge-Rinder.jpg). \n\nThe government, however, does. It's an entirely different ballpark. Google didn't get caught [hacking the webcams of millions of innocent people](https://www.theguardian.com/world/2014/feb/27/gchq-nsa-webcam-images-internet-yahoo).\n\nFacebook isn't forcing companies to install spyware on your PC under threat of arrest if they refuse to cooperate or let anyone know. [Lavabit](https://en.wikipedia.org/wiki/Lavabit) didn't have to shut themselves down because they didn't want to hand their users over to Facebook. Apple doesn't rip apart any machines they get and have experienced engineers go over single thing in them because [Facebook might have legally intercepted their machines and installed spy tools on them](https://forums.appleinsider.com/discussion/192395/apple-moves-to-bring-icloud-infrastructure-in-house-predicated-by-backdoor-fears-report).\n\nYahoo isn't deliberately sneaking of forcing companies to add weaknesses into operating systems or trying to [trick people into using known compromised algorithms](https://en.wikipedia.org/wiki/Dual_EC_DRBG) so they can hack them at a later date, and it's not a literal crime in many countries to use something that Yahoo can't hack at will. [Phil Zimmermann](https://en.wikipedia.org/wiki/Phil_Zimmermann) wasn't subject to a criminal investigation by the Yahoo Police because they considered strong encryption to be a munition and therefore subject to arms trafficking export controls. Yahoo isn't [hacking VPNs and routers](https://arstechnica.co.uk/security/2016/08/cisco-firewall-exploit-shows-how-nsa-decrypted-vpn-traffic/) around the world so they can snoop on everyone. And just Googling what I just said won't get you flagged by [Yahoo's monitoring software](http://daserste.ndr.de/panorama/aktuell/nsa230_page-1.html). \n\nIt goes on and on and on. I feel all "but what about Google!" really does is marginalize the sheer extent to which the government is tramping on our rights.

Yeah, it doesn't yet seem certain that this is a targeted attack on the NHS as is being reported, just as likely generic ransomware that has for whatever reason gone nuts within the NHS network. Good luck to the boys and girls working in NHS IT today, it's going to be a busy week ahead and a big test of their readiness for catastrophic failures. Last thing that a vital service already on it's knees needs. \n\nLPT: If you're a brit, do the NHS a favour and don't go out and get into a drunken fight/accident tonight. \n\nEdit: This covers the story and the background of the exploit used well https://arstechnica.co.uk/information-technology/2017/05/nhs-ransomware-cyber-attack/\n\nShort version: Ransomware utilising an SMB exploit (EternalBlue vulnerability) which was discovered by the NSA (they like to keep troves of zero days) then leaked by a group called the Shadow Brokers just over a month ago. Contrary to concerns at the time it had been patched, so shouldn't affect systems running the latest security updates from Microsoft.

How about this:\n\nThe CIA is running an espionage division more powerful than the NSA with no checks and balances\n\nThe CIA produced a large arsenal of weaponized malware to infest android and iphones.....and then lost control of it.\n\nCIA negligence resulted in them losing their cyber weapon arsenal which cost the US taxpayers $100 billion. Criminals stole it for free\n\nCIA hoarded Zero Day attacks which they are legally supposed to report. This puts citizens and the government at risk\n\nCIA has a Meme Warfare center. Pure propaganda which last time I checked isn't what they are supposed to be doing\n\nCIA sending in spies to work for tech companies to install backdoors into our devices\n\nCIA can turn many things we use into a microphone\n\nThey can spy on us through certain TVs\n\nCIA turned every Microsoft Windows PC in the world into spyware. Can activate backdoors on demand\n\nCIA has the ability to hack into trains, planes, cars, medical equipment\n\nThe US had a secret hacker base in Germany, one of our allies, without their knowledge\n\nOh and a BIG one: CIA stole Russian hacking tools so they could hack people and make it look like Russians did\n\n--\n\nWhoever this leaker is IS a Patriot. SO Lets not be uninformed and act like Vault 7 didn't reveal the CIA is OUT OF CONTROL. Next time try actually reading the WikiLeaks documents for yourself instead of having the main stream media tell you whats in them\n\n\n\n

The parallel would be an American-made cyber security software. I suspect the GRU does not use Windows Defender or any American-made product. (I'll go as far as to guess they don't use Kaspersky either.)\n\nThe NSA is in charge of protecting America's classified systems. I don't know this for a fact, but I'm almost certain they designed their own software and aren't using a commercially-available product. And yes, using any foreign-made software--particularly from a country with a history of government interference in private businesses for national security purposes--would be a bad idea for operational security. I'd definitely be less concerned about Kaspersky than anything Chinese-made, but that doesn't mean I would use either. \n\nThat said, there is a specific reason for the Intell community to have a stronger aversion to Kaspersky specifically. Kaspersky was one of the firms to identify Stuxnet. They actively search for government-created worms and have spoken out against their use in espionage. These are things that are almost certainly necessary for the IC to use (imo) and I wouldn't want anyone hostile to that purpose designing my software.

Five eyes/Fourteen Eyes is pretty much cyber-NATO, except reddit thinks its Obama reading their 'may-mays.' These nations combined have information awareness on a very high level. Also you dont need their help to perform attacks, the NSA/CIA can do that on its own.\n\nEven then what would the US do? Do you think Trump would ever go against Putin? We have the intelligence and the means, we just don't have the political will.

This following post is about the Trump-Russia conspiracy. You can feel free to dispute me, but please leave sources for your argument when available. First, I want to cover some facts that for some reason people don't know.\n\n**THE FACTS**: These are the facts of our situation. Again, feel free to dispute, but you are going to need some kind of source to convince me.\n\n* **Our election was hacked**. The NSA, FBI, and The Office of the Director of National Intelligence all agree this is true. [Here is the transcript and video of the open hearing covering the topic](https://www.washingtonpost.com/news/post-politics/wp/2017/03/20/full-transcript-fbi-director-james-comey-testifies-on-russian-interference-in-2016-election/?utm_term=.c5d2ad171612), and [here is the video of said hearing.](https://www.intelligence.senate.gov/hearings/open-hearing-disinformation-primer-russian-active-measures-and-influence-campaigns) \n Also, [here is an offical statement from the The Office of the Director of National Intelligence](https://www.nytimes.com/interactive/2017/01/06/us/politics/document-russia-hacking-report-intelligence-agencies.html). In the hearing they talk of Russia clearly targeting Hillary and making Trump look good. They also state that both the Democrats **and** Republicans were hacked.Russia also have been doing this across Europe, and is accepted by worldwide intelligence agencies.\n\n* **Trump is connected to Russia.** I am still surprised that people don't realize this. And this DOES NOT include collusion. [I mean he has released Trump Vodka in Russia](https://vimeo.com/14411822), and [Trump even brought Ms. Universe Pageant to Russia. It was paid for by Aras Agalarov, a man allegedly close ties to Putin](http://www.politico.com/blogs/2016-presidential-debate-fact-check/2016/10/contrary-to-his-claims-there-is-evidence-that-trump-does-business-with-russians-229484).\n\n* **Wikileaks is connected to Russia.** This is something I have to constantly explain. There are some pretty good instances that prove this. [Here is an article stating they left evidence out from their leak that shows €2 billion transfer from Syria to Russia.](https://www.dailydot.com/layer8/wikileaks-syria-files-syria-russia-bank-2-billion/)\n[Wikileaks also was given a show on a Kremlin funded news station.](http://www.reuters.com/article/us-russia-assange-tv-idUSTRE80P0TV20120126)\n\n\n\nIn the open hearing, the two directors of the FBI and NSA talk about motive for the Russian hack. They talk about one of the possible motives is that Russia wanted to destabilize our democracy and cause internal conflict. And this is where it get depressing.\n\n\n\nIf Russia's goal was the destabilization of our election, and to cause strife between us, then there is no doubt Russia has succeeded. We are currently still fighting between parties, and our democracy is being threatened.\n\n**In short, Russia has won, and the US is playing catch-up.**\n\nWith that out of the way, I want to go over what hasn't been totally proven, but has definitely not been proven wrong. This is the discussion part, you don't have to agree. Either way, however, it is something that needs to be talked about.\n\n\n**The Trump Administration, whether it been Trump himself or his peers, are aligned with Russia.**\n\nPlease before anyone attempts to say there is no hard hard evidence, please keep this in mind: there no hard proof that states he is innocent and a mountain of "coincidences" that say he is.\n\nThe following link is to a Sub Reddit Wiki that covers the entire Trump-Russia connection. Every entry has a source, and the Wiki tries to stay more factual than opinion based. If you don't believe something in it, please follow the source and site errors.\n\nhttps://www.reddit.com//r/TrumpInvestigation/wiki/doc#wiki_trump-russia_investigation\n\nPlease read at least some of it. Use the index to find a topic that could help your opinion.\n\nRemember, no one wants this to be real. The implications are horrible and dangerous, but it would also be foolish to dismiss it.\n\n**TL;DR: After all of this if you still believe that the Trump Administration is innocent, just realize this: The White House refused to hand over Flynn's documents to the investigation committee. They are withholding evidence. There is no reason to believe they are innocent.**\n\nEdit: Some clarification. \n\n**MORE IMPORTANT EDIT:** Everybody should consider calling various goverment offices. 5calls.org took me 10 min to make each call. We have to start somewhere!

The DNC hacks mostly didn't reveal anything, and were almost definitely conducted by Russian hackers (as stated by the FBI, NSA, and a few independent security firms, and confirmed through various means). \n\nTrump has been oddly supportive of US relations with Russia (a historic enemy), at the cost of US support for our allies in the Syrian Civil War, and Ukraine (a long time ally). That isn't too weird, of course. But President Trump and a number of his close associates also have long histories in Russia with Putin and a number of financial ties (Rex Tillerson, for example, has a lot of business in Russia). [Trump made some remarks during the campaign that suggest he wanted the Russians to hack into Sec. Clinton's personal and governmental accounts] (https://www.wsj.com/articles/donald-trump-invites-russia-to-find-missing-hillary-clinton-emails-1469638557). A number of major players in Trumps campaign were also found incidentally to have been communicating with suspected Russian spies (meaning the government was listening to the conversations of suspected Russian spies with the audio of Americans blurred out, thought the discussion seemed suspicious and got a warrant to listen to the American end of the conversation). [That's how we learned that Michael Flynn was communicating with a suspected Russian spy, and making promises that are the role of the Secretary of State, and illegal for non-ambassadors to make] (http://www.npr.org/2017/02/14/515233669/michael-flynn-left-the-trump-white-house-this-week-heres-how-that-happened). \n\nThe FBI (et al) started this investigation before the election.\n\nAdditionally, President Trump's appointments of his daughter and son in law to various high positions strikes strongly of nepotism. His refusal to isolate himself from his financial assets also strikes of corruption, as does his continual staying and meeting state visitors at resorts he owns. [His insistence, despite lack of evidence, that he lost the popular vote because of wide scale voter fraud] (https://www.usatoday.com/story/news/politics/onpolitics/2017/01/23/president-trump-illegal-ballots-popular-vote-hillary-clinton/96976246) tied in with the recent creation of [a commission on election integrity] (https://www.apnews.com/78ecd2bdc0ca46a5ad2a1afb4cd122a2/Trump-launches-commission-to-investigate-voter-fraud) is strikingly authoritarian. A number of liberals are afraid that the commission is going to be used to suppress the votes of minorities and the poor (ie, traditional Democratic voters). Their best evidence is that [the head of the commission has been successfully sued by the ACLU 4 times for voter surpression](https://action.aclu.org/secure/sham-voting-commission). \n\nThe recent firing of FBI Director Comey is also... not so good. [It was revealed that Comey requested funds to investigate President Trump in various regards to the above](http://www.latimes.com/politics/washington/la-na-essential-washington-updates-comey-asked-for-more-resources-for-1494434774-htmlstory.html), and then was fired very publicly, followed by Trump making a comment about how the firing was atleast partly motivated by the investigation (“And in fact, when I decided to just do it, I said to myself, I said, ‘You know, this Russia thing with Trump and Russia is a made-up story,’” Mr. Trump told Lester Holt of NBC News. “It’s an excuse by the Democrats for having lost an election that they should have won.”, ibid), followed by what could be understood to be [Trump threatening Comey](https://www.nytimes.com/2017/05/12/us/politics/trump-threatens-retaliation-against-comey-warns-he-may-cancel-press-briefings.html). [And President Trump has previously fired both Preet Bharara and Sally Yates when they started investigating Trump](http://www.cnn.com/2017/05/10/politics/comey-yates-bharara-fired-after-investigations).\n\nNone of this is directly evidence that Trump is himself doing anything illegal. But it is enough to strongly suggest that Trump and some of his associates have been working for Russian backers (and possibly the Russian government itself) to gain control of the presidency, and that they are now using it to gain personal wealth, and plan on stripping away a number of the central protections of our American democracy and republic.

The NSA and CIA have both been shown to have been *extremely* careless with very powerful cyber weapons *[Disappointment]*. Maybe CNN will report on it, unless Trump goes out for burgers with his staff and gets two patties in place of the normal single.

Shitty to think that intelligence agencies like NSA and GCHQ (the two worst offenders) are currently sitting on many other exploits like the one used in the attack but won't release them because they value hacking other countries above securing their own infrastructure *[Anger]*.\n\nI wonder how much collateral damage as a part of all the cyber war fantasies they will tolerate before they start changing their policies regarding vulnerabilities to one of disclosure *[Anger]*, which would do much more to secure critical systems.

Prison, maybe NSA can be useful for once, shit they spy on everything anyways *[Anger]*.\n\nSeriously though, the FBI needs to really go after this, this is a huge threat to security and how laughable it is in execution. People start going to prison, things change *[Anger]*. Unfortunately people in other countries often call in these swats and are able to get away with this, so maybe police departments need to change policy and screen international calls, I know they can spoof, but there needs to be a more robust FBI cyber division. \n\nThis is getting fucking ridiculous when one dude in Poland can make a call and endanger many lives. Not even a dude who is tech savvy, it's stupid how easy it is and what they are getting away with. This fuckery needs to stop, someone is going to get fucking killed, is it going to take someone dying for this to get attention?

And not informing the software manufacturer immediately upon discovering the vulnerability; You know, following responsible disclosure protocols widely accepted by the vulnerability assessment community around the world? Sadly, much like the blatant second amendment violations, compromising national and global security will not go unrewarded. Expect to see cyber security budgets for the NSA and CIA greatly expanded after this devastating attack. *[Disappointment]*

This is the fault of the NSA deciding to weaponise an exploit rather than telling Microsoft about the security hole. *[Disappointment]* And then being insecure themselves.\n\n"[The vulnerability that appears to have been exploited was allegedly discovered and developed by the NSA and then stolen by an online group known as the Shadow Brokers.](https://www.theguardian.com/society/2017/may/12/hospitals-across-england-hit-by-large-scale-cyber-attack)"\n\nSo our spy agencies put us in danger from criminals in order to "keep us safe" from terrorists. \n\nGood job, guys /s [Slow hand clap]

I'd just like to know how someone who is aware of the Snowden leaks and the Vault7 leaks could possibly be OK with the idea of installing an always on microphone in your home just because you're too lazy to use a mouse and keyboard for thirty seconds. \n \nWhy hello NSA and CIA. Don't even bother trying to hack one of my devices. Here, I'll install a microphone directly into my own home for you to listen to me 24/7 on *[Anger]*. \n \n

How else is the NSA supposed to easily hack our computers? Duh.

[Disappointment]

Well, where to begin? Once more unto the breach, dear archivists...\n\n&gt; they rushed 2.6.0 out last Christmas after croberts was saying 3.0 was coming before Dec 19th, 2016.\n\nExcept he didn't, as you well know. It's impossible to see this as anything other than wilful dishonesty at this point.\n\nAlso, I note that you no longer mention that hill anymore. You remember - that one that you vowed to "die on"? That one on which you loudly screamed that Star Marine wasn't in the 2.6 build, as disproven when we could retrospectively see the Issue Council reports (complete with backer video footage) as well as contemporaneously disproven by people posting footage from the game?\n\n'Member that? Because archive.is 'members. I hear Pepperidge Farm 'members too...\n\n&gt;what should've been 2.7, ended up now being 3.0 which doesn't even contain 25% of what was promised to be in 3.0\n\nI find it hilarious that you think you can quantify the amount of work that will make it into the planned 3.0, as if you have any experience with making a _functional_ comparable build. \n\nAll backers give a crap about is _**seamless**_ planetary landings. Crusader is being replaced with a planet that can be landed on, and the moons will be made viable landing areas too. Sure, it's be _nice_ to have another couple of planetary systems to play with, but the revised 3.0 is plenty. \n\nWithout meaning to sound antagonistic, a handful of ground-based missions like that seen in the Homestead demo would give 3.0 a comparable amount of gameplay to the planets in E:D. \n\n&gt;They have not only run out of time and money\n\nDisproven by the charts that _you_ yourself keep referring to, dumbass.\n\n&gt;key people have left, are leaving, and sources tell me there are several more on the way out\n\nExcept that everyone you have _claimed_ was about to leave has stubbornly refused to actually leave. Tony Zurovec is currently in the midst of what seems like a staggeringly drawn-out notice period, as you've been claiming he was on the way out for at least a month now. And then there's Ben Lesnick and Sandi, one of whom was "clearing out her desk" the better part of a year ago.\n\n&gt;they've started trimming the four (!) studios around the world\n\nFive. We all know that your only source is ATV, so you really should have paid attention last time the _other_ Roberts brother was bitchslapping you without even referring directly to you.\n\n&gt;think about what happened to the Lily drone \n\nWhy? Oh, that's right: because you have nothing to _actually_ cite as evidence, so you're forced to appeal to an incomparable comparison to act as a foundation for your assertions. Gotcha.\n\n&gt;State/Fed officials had to get involved because they were a public concern\n\nHere's what you do, you whiny little pussy:\n\n1) produce a step-by-step guide to reporting these things to the FTC, FBI, NSA, NWO, WWE, FDA, or any other initialism that you care to name. \n2) upload - to multiple sources - a video of you going through this exact process, including recordings and transcripts of any relevant communication. \n3) post links to those videos everywhere that has yet to ban you. Your blog, twitter, Frontier (because we all know that they'll be fine with you doing this), SA - all of them.\n\nDo that, and you'll have shown how confident you are in your own bullshit. You'll be demonstrating that you feel there is sufficient evidence there to justify a complaint. Refuse, and you'll prove that you're terrified of reporting it yourself for fear of being prosecuted for filing a false report, leaving you open to prosecution for harassment and a substantial number of such charges.\n\nStop being such a coward and hiding behind other people and show everyone that you're not just another bitter little waste of space who is desperately clinging to someone more successful than them in a final effort to give their worthless life meaning.\n\n&gt;sources are telling me that the reason they can't do planets, only moons and asteroids which can be placed in the space scenes like stations, is because they simply can't get it to work\n\nExcept that these "moons" are planets in all but radius. They have the exact same functionality, and only differ in that they are a little smaller - while still being, if memory serves me correctly, large enough for gravity to pull them into a sphere, making them all larger than every planet in something like No Man's Sky.\n\nOh, and they _are_ adding a planet to 3.0 which can be travelled to and landed upon. Learn to read.\n\n&gt;Let alone have entire planetary bodies which support seamless space&lt;-&gt;planetary transitions as they've been promising.\n\nThey've already demonstrated them, and the moons that 3.0 will bring will actually do the same thing.\n\nYou seem to think that moons are somehow different from planets. They aren't. Both are spheres with the same physics grid system and the same capacity for seamless landings. The sole difference is their size and the body that they orbit.\n\nOh, in case you missed it, they've already worked out the tech required to allow these objects to orbit their parent body. Maybe if you add Bugsmashers to your short list of YouTube-based sources you'll learn how they did it someday...\n\n&gt;now in Summer 2017, **6 years [late]**\n\nJust shy of four and a half, actually. You should have bought the PhD that made you better at counting.\n\n&gt;reputation management accounts being created all over the place\n\nI'd like us to collectively start referring to this as the "No True Citizen" fallacy, wherein Derek dismisses any positive impression of SC as "reputation management" in order to allow him to delude himself into thinking that the only valid opinions of the project are the negative ones.\n\n&gt;fake Star Citizen "reviews/previews" by sites nobody ever heard of\n\nI'll remember that one next time you appear on the "Open" House, or whoever the fuck that other guy was whose archived stream accounts for about 80% of his all-time viewership...\n\n&gt;one massive disinformation campaign\n\nIndeed...\n\n&gt; toxic backers[...]who are waging an Internet wide war against dissent, some of whom we believe to be actively engaged in money laundering via the Grey market\n\nSorry, you were saying something about something being "one massive disinformation campaign"...?\n\n&gt;these past two years, I haven't seen anything that has swayed my opinion \n\nThat's because your eyes are closed, Derek. No-one can _force_ you to look at things that prove you wrong. They can only ensure that they are available and show you where to find them. In a free world, you are completely free to delude yourself, just as everyone else is free to ignore your demonstrable falsehoods and attempts to revise history, and just as those same people are free to check these archives of your assertions and actions.\n\n&gt;When I backed this game in Nov 2012, never in my wildest dreams, did I think that it would come to this. It's all just so very sad.\n\nIndeed. You hoped you could bluff your way into CIG and claim some of this as your own. You were spotted a mile off, and were unceremoniously told to fuck off. You thought the $250 could buy you a job and the chance to cannibalise the work of people who are so much more competent than you that it's _really_ is "sad". \n\nYou are scared shitless that 3.0 will bring in another $30m, and it almost certainly will. No extant game can offer the same experience, with NMS and E:D being the closest. At that moment, despite being limited to a single planet in a single star system out of 100 (or 110, as you now claim), it offers more variety in experiences than either of its closest competitors, and ceases to become a "promising" game and becomes one that is delivering on that early promise. \n\nIf you had _any_ confidence you'd be sitting back and watching it play out, satisfied that your predictions are archived safely for posterity. Instead, you perpetually revise your assertions and are compelled to actively lie about things in an attempt to dissuade people from backing it, because you tacitly acknowledge that the game will succeed if not for some interference.\n\nUgh - I feel dirty.\n\n

The CIA deepstate has been governing since the Kennedy assassination. Bush sr. Was head if CIA, then Vice President then President and has been in power since. BUT along came two things, the Internet and 911, and the combination of that gave the NSA so much power to gather info that it was able to take a good look at the CIA, then they went to war with each other, hence all the leaks,... first from the CIA to discredit the NSA via Snowden, then the NSA leaked all the Clinton emails and Podesta emails - the NSA backed Trump via Palantir, Thiel, and Kushner, then we got the Vault7 leaks attacking the CIA via Wikileaks who more than likely works with the NSA - the CIA deepstate is trying to hit back at the NSA via the Russian hack story, to discredit the NSA administration... At least that's what I can make of all this.

Oh boy do I really have to explain how the CIA is corrupt? We'll ignore their meddling in foreign elections and funding of terrorists and just focus on WikiLeaks. Here is a tiny sample of what Vault 7 has showed so far (What this "Traitor" leaked)\n\nThe CIA is running an espionage division more powerful than the NSA with no checks and balances\n\nThe CIA produced a large arsenal of weaponized malware to infest android and iphones.....and then lost control of it.\n\nCIA negligence resulted in them losing their cyber weapon arsenal which cost the US taxpayers $100 billion. Criminals stole it for free\n\nCIA hoarded Zero Day attacks which they are legally supposed to report. This puts citizens and the government at risk\n\nCIA has a Meme Warfare center. Pure propaganda which last time I checked isn't what they are supposed to be doing\n\nCIA sending in spies to work for tech companies to install backdoors into our devices\n\nCIA can turn many things we use into a microphone\n\nThey can spy on us through certain TVs\n\nCIA turned every Microsoft Windows PC in the world into spyware. Can activate backdoors on demand\n\nCIA has the ability to hack into trains, planes, cars, medical equipment\n\nThe US had a secret hacker base in Germany, one of our allies, without their knowledge\n\nOh and a BIG one: CIA stole Russian hacking tools so they could hack people and make it look like Russians did\n

Putting all the other past leaks aside;\n\n&gt; We know it's Russia because it's the only country with the capabilities and tentacles and gusto.\n\nYou're kidding right? or are at least naive to the constant reel of stories about western countries and hacking, wikileaks of NSA/CIA hacking tools, not to mention the fetish the UK/US governments have for wanting 'legal' backdoors into things. FBI/DOJ letting paedophiles off the hook trying to protect their hacking methods (TOR), US Police departments letting gangs off the hook for because the police used illegal spying devices (stingrays), UK having a proposal for a realtime monitoring system, etc. You have other European countries with secret deals between each other over other hacking. Thats just the west too, not to mention Chinas long standing dodgy reputation around technology and security.\n\nAs i started, putting the other past leaks aside, pretty much every major nation is in on cyber scumbaggery, to think its just Russia doing things around the world is silly. \n\n\n\n

&gt;Why is this such an insidious breach of ethics?\n\n&gt;Rather than report the exploit to the developers so it could be fixed, the NSA kept it for themselves in order to """protect""" the American people *[Disappointment]*. \n\nWatch. The media narrative will be, "This is Wikileaks fault, and we need to shut them down". They will not blame the source of the exploit (i.e, the government). We've seen this playbook before.

Russia’s intelligence services conducted cyber operations against targets associated with the 2016 US presidential election, including targets associated with ***both major US political parties.***\n\n&gt; ***[Assessing Russian Activities and Intentions in\n&gt; Recent US Elections\n&gt;](https://www.dni.gov/files/documents/ICA_2017_01.pdf)*** *Jan 6, 2017*\n&gt; \n&gt; This report includes an analytic assessment drafted and coordinated among The Central Intelligence\n&gt; Agency (CIA), The Federal Bureau of Investigation (FBI), and The National Security Agency (NSA), which\n&gt; draws on intelligence information collected and disseminated by those three agencies. It covers the\n&gt; motivation and scope of Moscow’s intentions regarding US elections and Moscow’s use of cyber tools\n&gt; and media campaigns to influence US public opinion. The assessment focuses on activities aimed at the\n&gt; 2016 US presidential election and draws on our understanding of previous Russian influence operations.\n&gt; When we use the term “we” it refers to an assessment by all three agencies.\n&gt;\n&gt; **Russian efforts to influence the 2016 US presidential election represent the most recent expression\n&gt; of Moscow’s longstanding desire to undermine the US-led liberal democratic order, but these\n&gt; activities demonstrated a significant escalation in directness, level of activity, and scope of effort\n&gt; compared to previous operations.**\n&gt; \n&gt; **We assess Russian President Vladimir Putin ordered an influence campaign in 2016 aimed at the US\n&gt; presidential election. Russia’s goals were to undermine public faith in the US democratic process,\n&gt; denigrate Secretary Clinton, and harm her electability and potential presidency. We further assess\n&gt; Putin and the Russian Government developed a clear preference for President-elect Trump.** We\n&gt; have high confidence in these judgments.\n&gt; \n&gt; * **We also assess Putin and the Russian Government aspired to help President-elect Trump’s\n&gt; election chances when possible by discrediting Secretary Clinton and publicly contrasting her\n&gt; unfavorably to him. All three agencies agree with this judgment.** CIA and FBI have high confidence\n&gt; in this judgment; NSA has moderate confidence.\n&gt; \n&gt; * **Moscow’s approach evolved over the course of the campaign based on Russia’s understanding of the\n&gt; electoral prospects of the two main candidates. When it appeared to Moscow that Secretary Clinton\n&gt; was likely to win the election, the Russian influence campaign began to focus more on undermining\n&gt; her future presidency.**\n&gt; \n&gt; * **Further information has come to light since Election Day that, when combined with Russian behavior\n&gt; since early November 2016, increases our confidence in our assessments of Russian motivations and\n&gt; goals.**\n&gt; \n&gt; **Moscow’s influence campaign followed a Russian messaging strategy that blends covert\n&gt; intelligence operations—such as cyber activity—with overt efforts by Russian Government\n&gt; agencies, state-funded media, third-party intermediaries, and paid social media users or “trolls.”** \n&gt; Russia, like its Soviet predecessor, has a history of conducting covert influence campaigns focused on US presidential elections that have used intelligence officers and agents and press placements to disparage candidates perceived as hostile to the Kremlin.\n&gt; \n&gt; \n&gt; * Russia’s intelligence services conducted cyber operations against targets associated with the 2016 US\n&gt; presidential election, including targets associated with both major US political parties.\n&gt; \n&gt; * We assess with high confidence that Russian military intelligence (General Staff Main Intelligence\n&gt; Directorate or GRU) used the Guccifer 2.0 persona and DCLeaks.com to release US victim data \n&gt; obtained in cyber operations publicly and in exclusives to media outlets and relayed material to\n&gt; WikiLeaks.\n&gt; \n&gt; * Russian intelligence obtained and maintained access to elements of multiple US state or local\n&gt; electoral boards. **DHS assesses that the types of systems Russian actors targeted or\n&gt; compromised were not involved in vote tallying.**\n&gt; \n&gt; * Russia’s state-run propaganda machine contributed to the influence campaign by serving as a\n&gt; platform for Kremlin messaging to Russian and international audiences.\n&gt; \n&gt; \n&gt; ***We assess Moscow will apply lessons learned from its Putin-ordered campaign aimed at the US\n&gt; presidential election to future influence efforts worldwide, including against US allies and their\n&gt; election processes.***

&gt;King asks Rogers about Russian camera crew allowed into Oval Office yesterday. Was there any consultation w NSA regarding risk of cyber penetration in that incident?\n\n&gt;Rogers: No. We were not consulted, as far as I'm aware of. I wasn't aware of where the images came from.\n\nAnother hilariously shocking display of incompetence from Trump lol

Yes, it does. Either run more modern equipment, keep your shit patched, properly segment your network, or accept that running that piece of software you've had since '97 is also a liability, and sometimes shit like this will happen.\n\nCyber risk is a force of nature. Bitching about US intelligence services having these exploits is fruitless. Even if you win, and the CIA and NSA stop entirely, that doesn't impact the risk landscape in the slightest.\n\nThe SMBv1 exploit WannaCrypt used is old news. If you were still running vulnerable software, you either accepted the risk or had your head in the sand.\n\nEdit: spelling

Except for the part where cyber security is going to much more fall under the NSA and the Air Force Cyber Command.

At 9:30am EST:\n\nAdmiral Michael Rogers Testifies on U.S. Cyber Command Operations \n\nhttps://www.c-span.org/video/?428023-1/admiral-michael-rogers-testifies-us-cyber-command-operations\n\n\nEDIT: It's starting now! I don't know if they'll talk about anything interesting, but Mike Rogers looks/sounds so badass that I just enjoy listening to him.\n\n\nEdit #2:\n\nJohn “Spineless Maverick” McCain takes his seat.\n\nThe gist: ‘Cyber threats are a danger. Of course, *Obama* never offered any new policies to prevent it, *but* I acknowledge that Trump hasn’t done anything either. We need unity among our different agencies as well as our allies. But so far, employee continuity is *SAD*! \n\n\nDemocrat I don’t know the name of:\n\nThe gist: ‘Espionage is bad. Russia has tried to abuse the vulnerabilities of us and our allies. A new election is coming up in a year, and we’ve found out that they’re going to keep fucking with us. We don’t have any effective cyber defenses up yet. We need an effective deterrent, obviously. Trump’s administration hasn’t shown that they take it seriously or have any intention of addressing it. \n\n\n\nEdit #3:\n\n\nAdm. Rogers:\n\n\nThe gist: ‘International cyber security threats are growing from increasingly advanced adversaries. They’re trying to affect and influence our national interests. We need to protect our defense systems. We need a frank and comprehensive discussion with congress. The public needs to see that something is being done to protect them from the Ruskies. \n\nMCain:\n\nThe gist: We just saw the attempt to influence the French election. Is this, like, still a problem? \n\n\nRogers:\n\nThe gist: Yes, sir. It’s, like, still a goddamn problem. No, we haven’t seen any indication that Russia is going to stop. We *need* a policy of deterrence. Worst case scenarios?1) Destructive activity on critical structure. Worst consequence? Data manipulation on a massive scale. 3) What happens when non-state actors decide that cyber is an effective way to attack a country? If information is now going to be a weapon, are we prepared to adequately address it?\n\n\nEdit #4: \n\nReed (D):\n\nThe gist: Were you aware of the infiltration with regards to the 2016 election? What actions did you take?\n\nRogers:\n\nThe gist: Yes, I was aware. When the NSA found out in 2015 that the Russians were attacking us, we made sure everyone was aware. Yes, we do need to be much better prepared in 2018.\n\n\nRepublican chair starts his second round and redirects to North Korea.\n\n\nEdit #5: \n\n\nWicker (R)\n\n\nThe gist: What constitutes an act of cyber war? Do we have, like, an actual fucking definition? Your uniform makes you look pretty important, so can you at least give your opinion?\n\n\n\nRogers:\n\nThe gist: We haven’t yet reached “a broad consensus in clear actionable terms” on what constitutes an act of cyberwarfare. I mean, that’s more of a policy thing and I’m a stone cold military man with a badass uniform and voice. Okay, okay, I’ll try. Maybe we should develop some criteria, *specific* criteria? ‘Cus we keep talking about this in general terms.\n\n\n\nEdit #6\n\n\nSen. Gillibrand (D)\n\nThe gist: Has this administration done a goddamn thing or at least decided to work on anything? You said deterrence was the answer, but nope, *nothing* from this administration. Can you guarantee your leadership? [later on] One word: FRANCE.\n\n\nRogers:\n\nThe gist: Lady, have you seen my goddamn uniform? Of course I have authority. On France? A lot of that is classified.\n\n\n\nEdit # 7\n\n\nDeb Fischer (R)\n\nThe gist: Something, something. Terrorism in the cyberspace. Let’s talk about private sector too.\n\n\nRogers:\n\nThe gist: Something, something. ISIS. No, the structures in place are not fast enough. What should we do? That’s an ongoing discussion that I’d rather not get into too publicly. The private sector?... Maybe we could make an effort to allow the private sector to share info with us? I mean, they have that shit in place already, we shouldn’t have to go looking for it. They could bring some of it to us.\n\n\nEdit #8\n\n\n[**god damn, my co worker keeps coming over to tell me how her date went**]\n\n\nSen. Angus King (I)\n\nThe gist: We’ve got to educate the public in the ways that they manipulate things, including during elections. How do we educate our people to be more discerning? We’ve got to do that, right? Did you see all this ridiculous shit that’s come out, even for the French election?\n\n\n\n\nRogers: \n\nThe gist: Yes. “It’s a brave new world” (direct quote) in the information age for all of us.\n\n\n\nEdit #9\n\nSen. Mike Rounds (R)\n\nThe gist: Yeah, uh, but back to the *private* sector. What can we do to protect them?

\n\n\nRogers:\n\n\nThe gist: Something, something. Work with our agencies and departments effectively.\n\n\nSen. Heinrich (D)\n\n\nThe gist: Back to Russia. Bots. Fake news. WTF? They’re politically destructive. Does cyber command have a role to play in meeting this new threat? These social media accounts look real, but there friggin’ bots, dude. “Bot farms" are coming from overseas, right? Will you be able to share info with social media companies? We need to have those relationships in place.\n\n\n\nRogers:\n\n\nThe gist: I wouldn’t say it’s completely outside our responsibilities. We’re trying to get the structure set up. That’s our priority. And the bots? Yes, it’s mostly overseas now, but we’ll probably start seeing more domestic activity. Yes, we really should have a good relationship with social media.\n\n\n\n\n\nEdit #10\n\nSen Hirono (D)\n\nThe gist: Look, we all know Putin fucked with our election. What do you think the role of the military is? Has the president given you a clear mission?\n\n\nRogers:\n\nThe gist: Yes, we need to make it clear that it’s unacceptable. Our role? To identify threats so we can communicate that. If we define election infrastructure as critical infrastructure to the nation, I can apply our capabilities pro-actively. No, we don’t have a defined mission. \n\n\n**god damnit, co-worker. If I have headphones on, no, I don’t want to watch your YouTube video.**\n\n\n\nEdit #11\n\nElizabeth Warren (needs no introduction)\n\n\nThe gist: Would cuts to the State Department and DoD make your job easier or harder? Also last year the Russians stole emails and then they did it again with French politicians. You said improving DoD defenses would help? How do we develop our cyber warriors? Do we need more exemptions from federal hiring laws to help you recruit?\n\n\nRogers:\n\nThe gist: Yes, cuts make it harder. Yes, improving defenses would help. Cyber warriors? Hell, yeah. We need to define and develop what skills sets we’re looking for. Right now, I feel good about military recruitment. We do want to have the flexibility to ask you for more resources.\n\n\n\nEdit #12\n\nSen. Perdue (R)\n\n\nThe gist: China and Russia still trying to hack for data extraction, right? But, let’s talk about North Korea.\n\n\nRogers:\n\nThe gist: Extraction confirmed. North Korea? Yeah, nation states are doing that. \n\n\n\nEdit #13\n\nSen. Tom Cotton (R)\n\n\nThe gist: Our colleague, Elizabeth Warren, said Trump was Russia’s preferred candidate. So, is there technically a difference between them wanting to help Trump versus them wanting to hurt Clinton? But let’s go back to Obama. *Obama* dropped the ball several times. I mean, he even made fun of his opponent during the 2012 debate, right? He didn’t even keep his red line promise on Syria. Isn’t it true that **OBAMA'S EIGHT YEARS OF INACTION WAS WHAT *REALLY* EMOLDENED RUSSIA?**\n\n\nRogers: \n\nThe gist: Uhhh… now you’re getting into political stuff which I’m not qualified to do.\n\n\nEdit #14\n\n\nTim Kaine (D)\n\n\nThe gist: Shouldn’t we be concerned about the efforts of actors in the United States trying to work with foreign states to influence different shit? If individuals were disseminating documents that were hacked by Russians, like in France, who would handle that?\n\n\nRogers:\n\n\nThe gist: The FBI would probably handle it if it were domestic. \n\n\n\nEdit #15\n\n\nLindsay Graham:\n\nThe gist: The Russians are interested, no matter which party, right? BUT LET’S TALK ABOUT UNMASKING, GOOD SIR. How many people can request the unmasking of American citizens? Who would have access? Like, 20 people? Is there a record of who requested the record? If Flynn set off an alarm, would there be a record of any unmasking process? Do you know if Susan Rice ever asked for an American citizen to be unmasked?\n\n\nRogers:\n\n\nThe gist: Yes, incidental collection happens. Americans? It would have to be for a reason, it can’t just be “I’m curious.” Yes, there’s a record of who requested the report, but they’re told not to share it and the ID isn’t always unmasked. If we had a leak, we would get rid of that person, full stop. Susan Rice? I would have to pull the data, I don’t know at this moment.\n\n\nEdit #16\n\n\nTillis (R) \n\nThe gist: But back to the private sector. \n\n\n\n\nRogers: **sorry, co-worker hijacked me with another youtube video. I missed his response**\n\n\n\nBlumenthal:\n\nThe gist: But back to whether or not we’ve done a goddamn thing about Russia. Would sanctions be effective? Should Americans be held accountable if they work with them? Your job is to protect Americans, right? I would hope so, since you're wearing that sexy, sexy uniform. Colluders should be held accountable for it right? An investigation, right? That would be good? Look, we were here last year talking about this cyber thing. Forcing the Russians to pay a price requires compelling Americans who colluded with them to pay a price, right? \n\n\n\nRogers:\n\nThe gist: Yes, they’re still going. No, we haven’t done anything, and I see no indication that they’re going to stop until we do something. If anyone did something, then yes, they should be held accountable. And yes, my uniform is newly pressed.\n\n\n\n\n

There is no need to hack Windows 10, it comes pre-hacked. The NSA just get their spy data directly from Microsoft.

The main issue here is that the NSA prevented Microsoft from patching this sooner so they could use it as a backdoor *[Disappointment]*.\n\nIt was only when the NSA was hacked were Microsoft allowed to patch the OS.\n\nI have sympathy for MS on this *[Disappointment]*, at the moment in the UK, the idiot government wants it "mandated" by law they get backdoors exactly like this.\n\nSure, no criminal is ever going to use a government implemented backdoor. Thankfully it's a crime in the UK to hack a computer network, and good job no-one in any other country can hack the UK over the Internet. \n\n\nTotal idiots. \n

Reminds me of the FBI saying that they're having a hard time recruiting qualified programmers/hackers for their cyber units, because many of them used "controlled substance" (aka marijuana), and the FBI is competing against the NSA who can pay programmers a 6-digit salary right from the start.\n\nStrict hiring requirements, lower salary compared to other government departments and especially Silicon Valley (including their much more relaxed drug policy at some companies) makes it harder to recruit.\n\nEDIT: Wall Street has also been aggressive with hiring programmers (including developing financial algorithms) and cyber security, and I wouldn't be surprised if they could easily throw a truckload of cash at the new hires to get them to join. I recall someone had competing offers between Goldman Sachs and Intel.

I'm shocked this isn't at the top/doesn't have a lot more comments by now. This is huge, global news.\n\n&gt;"Security researchers with Kasperksy Lab have recorded more than 45,000 attacks in 74 countries, including the UK, Russia, Ukraine, India, China, Italy, and Egypt. In Spain, major companies including telecommunications firm Telefonica were infected."\n\n&gt;"By Friday evening, the ransomware had spread to the United States and South America, though Europe and Russia remained the hardest hit, according to security researchers Malware Hunter Team. The Russian interior ministry says about 1,000 computers have been affected."\n\n&gt;"The attack hit England’s National Health Service (NHS) on Friday, locking staff out of their computers and forcing some hospitals to divert patients."\n\n&gt;"According to Prof Alan Woodward, a security expert at Surrey University, it resembles an exploit of “EternalBlue” - the name given to a weakness in Microsoft’s security that is thought to have been identified secretly by the US National Security Agency (NSA)."\n\n&gt;"A hacking group calling itself Shadow Brokers claimed to have stolen information about the vulnerability from the NSA last year, as part of a cache of files. It tried to auction them off but, after no one made a satisfactory bid, reportedly dumped them online for free. Microsoft released a fix and some researchers have suggested that a failure to implement it may have exacerbated the problem."\n\nFrom the Guardian\n\nhttps://www.theguardian.com/society/live/2017/may/12/england-hospitals-cyber-attack-nhs-live-updates\n\nhttps://www.theguardian.com/technology/2017/may/12/global-cyber-attack-ransomware-nsa-uk-nhs\n\nEdit: Fedex says they've been hit. Company statement:\n\n&gt;"Like many other companies, FedEx is experiencing interference with some of our Windows-based systems caused by malware,” a spokesperson said in a statement. “We are implementing remediation steps as quickly as possible. We regret any inconvenience to our customers."\n\nEdit 2: Update to the number of countries hit (earlier it was known to have spread to 74 countries):\n\n&gt;"The WannaCry ransomware has now spread to 99 countries, according to security firm Avast."\n\nEdit 3: A new list of the health boards affected in Scotland - it's infected 11 out of their 13\n\n&gt;"The impacted health boards are NHS Borders, Dumfries and Galloway, Fife, Forth Valley, Lanarkshire, Greater Glasgow and Clyde, Tayside, Western Isles, Highlands, Grampian, Ayrshire and Arran, and the Scottish Ambulance Service."

There's ample proof, you just willfully choose to ignore it. \n\nhttp://arstechnica.com/security/2016/12/the-public-evidence-behind-claims-russia-hacked-for-trump/\n\nhttp://www.cnn.com/2016/12/22/politics/crowdstrike-dnc-hack-russian-military/\n\nhttps://www.dni.gov/index.php/newsroom/press-releases/215-press-releases-2016/1423-joint-dhs-odni-election-security-statement\n\nhttps://www.secureworks.com/research/threat-group-4127-targets-hillary-clinton-presidential-campaign\n\nhttps://www.secureworks.com/research/threat-group-4127-targets-google-accounts\n\nhttps://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/\n\nhttp://arstechnica.com/security/2015/09/seven-years-of-malware-linked-to-russian-state-backed-cyberespionage/\n\nhttp://www.threatgeek.com/2016/06/dnc_update.html\n\nhttps://theintercept.com/2016/12/29/top-secret-snowden-document-reveals-what-the-nsa-knew-about-previous-russian-hacking/\n\nhttp://www.nytimes.com/interactive/2016/12/29/us/politics/document-Report-on-Russian-Hacking.html\n\nhttp://www.nytimes.com/interactive/2017/01/06/us/russian-hack-evidence.html

&gt; ***[Assessing Russian Activities and Intentions in\n&gt; Recent US Elections\n&gt;](https://www.dni.gov/files/documents/ICA_2017_01.pdf)*** *Jan 6, 2017*\n&gt; \n&gt; This report includes an analytic assessment drafted and coordinated among The Central Intelligence\n&gt; Agency (CIA), The Federal Bureau of Investigation (FBI), and The National Security Agency (NSA), which\n&gt; draws on intelligence information collected and disseminated by those three agencies. It covers the\n&gt; motivation and scope of Moscow’s intentions regarding US elections and Moscow’s use of cyber tools\n&gt; and media campaigns to influence US public opinion. The assessment focuses on activities aimed at the\n&gt; 2016 US presidential election and draws on our understanding of previous Russian influence operations.\n&gt; When we use the term “we” it refers to an assessment by all three agencies.\n&gt;\n&gt; **Russian efforts to influence the 2016 US presidential election represent the most recent expression\n&gt; of Moscow’s longstanding desire to undermine the US-led liberal democratic order, but these\n&gt; activities demonstrated a significant escalation in directness, level of activity, and scope of effort\n&gt; compared to previous operations.**\n&gt; \n&gt; **We assess Russian President Vladimir Putin ordered an influence campaign in 2016 aimed at the US\n&gt; presidential election. Russia’s goals were to undermine public faith in the US democratic process,\n&gt; denigrate Secretary Clinton, and harm her electability and potential presidency. We further assess\n&gt; Putin and the Russian Government developed a clear preference for President-elect Trump.** We\n&gt; have high confidence in these judgments.\n&gt; \n&gt; * **We also assess Putin and the Russian

Government aspired to help President-elect Trump’s\n&gt; election chances when possible by discrediting Secretary Clinton and publicly contrasting her\n&gt; unfavorably to him. All three agencies agree with this judgment.** CIA and FBI have high confidence\n&gt; in this judgment; NSA has moderate confidence.\n&gt; \n&gt; * **Moscow’s approach evolved over the course of the campaign based on Russia’s understanding of the\n&gt; electoral prospects of the two main candidates. When it appeared to Moscow that Secretary Clinton\n&gt; was likely to win the election, the Russian influence campaign began to focus more on undermining\n&gt; her future presidency.**\n&gt; \n&gt; * **Further information has come to light since Election Day that, when combined with Russian behavior\n&gt; since early November 2016, increases our confidence in our assessments of Russian motivations and\n&gt; goals.**\n&gt; \n&gt; **Moscow’s influence campaign followed a Russian messaging strategy that blends covert\n&gt; intelligence operations—such as cyber activity—with overt efforts by Russian Government\n&gt; agencies, state-funded media, third-party intermediaries, and paid social media users or “trolls.”** \n&gt; Russia, like its Soviet predecessor, has a history of conducting covert influence campaigns focused on US presidential elections that have used intelligence officers and agents and press placements to disparage candidates perceived as hostile to the Kremlin.\n&gt; \n&gt; \n&gt; * Russia’s intelligence services conducted cyber operations against targets associated with the 2016 US\n&gt; presidential election, including targets associated with both major US political parties.\n&gt; \n&gt; * We assess with high confidence that Russian military intelligence (General Staff Main Intelligence\n&gt; Directorate or GRU) used the Guccifer 2.0 persona and DCLeaks.com to release US victim data \n&gt; obtained in cyber operations publicly and in exclusives to media outlets and relayed material to\n&gt; WikiLeaks.\n&gt; \n&gt; * Russian intelligence obtained and maintained access to elements of multiple US state or local\n&gt; electoral boards. **DHS assesses that the types of systems Russian actors targeted or\n&gt; compromised were not involved in vote tallying.**\n&gt; \n&gt; * Russia’s state-run propaganda machine contributed to the influence campaign by serving as a\n&gt; platform for Kremlin messaging to Russian and international audiences.\n&gt; \n&gt; \n&gt; ***We assess Moscow will apply lessons learned from its Putin-ordered campaign aimed at the US\n&gt; presidential election to future influence efforts worldwide, including against US allies and their\n&gt; election processes.***

Seems weird for them to use "a" top cyber official instead of "the" top cyber official. It's the head of the NSA, not just some guy.

Here's a catchup of some resources shared in [[ETH Daily Discussion] - 12/May/2017](https://www.reddit.com/r/ethtrader/comments/6apmi7/eth_daily_discussion_12may2017/):\n\n* [Ransomware Attacks Ravage Computers in Dozens of Countries (npr.org)](http://www.npr.org/sections/thetwo-way/2017/05/12/528119808/large-cyber-attack-hits-englands-nhs-hospital-system-ransoms-demanded)\n\n* [Bitcoin's Number of Unconfirmed Transactions in Real-Time (blockchain.info)](https://blockchain.info/unconfirmed-transactions)\n\n* [Massive Cyber-Attack Targeting 99 Countries Causes Sweeping Havoc (money.cnn.com)](http://money.cnn.com/2017/05/12/technology/ransomware-attack-nsa-microsoft/index.html)\n\n* [NSA-Created Cyber Tool Spawns Global Attacks - And Victims Outside Russia (politico.com)](http://www.politico.com/story/2017/05/12/nsa-hacking-tools-hospital-ransomware-attacks-wannacryptor-238328)\n\n* [Blockchain Can Help Combat Fraud And Corruption in the Oil and Gas Business (ibtimes.co.uk)](http://www.ibtimes.co.uk/blockchain-can-help-combat-fraud-corruption-oil-gas-business-1621228)\n\n* [Berns Weiss LLP To Investigate Kraken (reddit.com/r/ethtrader)](https://www.reddit.com/r/ethtrader/comments/6ae4io/berns_weiss_llp_to_investigate_kraken/)\n\n* [Crowdsale for BAT begins May 31st (basicattentiontoken.com)](https://basicattentiontoken.org/crowdsale-for-bat-begins-may31/)\n

Well, widespread phishing attack is usually how a foothold is gained in the target networks.\n\nNow, more interestingly, in the NHS case, various people have mentioned that the infected hosts are triggering IDS (Intrusion Detection System) rules for the MS-17-010 exploit, a remote code execution vulnerability in Windows that was patched recently.\n\nWhat makes the whole thing even more interesting is that the MS-17-010 exploit (ETERNALBLUE) only became public after it was leaked in the

Shadowbrokers dumps of NSA hacking tools. \n\nSo effectively, based on the current evidence, tools the NSA built to hack people and spy on them are now being used by criminals to install ransomware in hospitals. A delightful shitshow indeed.

Intel does need changes, gust not the changes these fuckheads will come up with.\n\nPersonally I recommend all intel except CIA and NGA fall under a new agency (Or retask DIA) headed by the DNI, which will standardize all training for civilian and military analysts and operators. Everything from intel analysts to map makers, cyber, HUMINT, and CI. All personnel go through the same courses. Forces will still report to relevant organizations when the org is a national agency (I.e. NSA and others will fall under it), and all military intel forces will fall under CSS which will be under this agency. They will be tasked through their service commands with national intelligence missions as well as locally from their unit commanders PIRs and CCIRs. Finally, we need to deal with Reserve/Guard intel folks because right now, they are virtually useless to private employers. Their experience may not count for shit. I think turning their 2 weeks into mandatory time with National Agencies with real world missions may help fix that.\n\nWhat I want is no analyst will ever be sitting back doing some worthless report on something everyone else has already reported on. We don't need 500 analysts reporting on KJU and what he might do next week. But we can task 300 analysts with looking at changes in the NK military structure, movement of forces, and telling us the locations of hidden arty deployments, which can be delivered to national leaders as well as the local commander. And we can deploy 200 collectors in the field performing actual reconnaissance so our forces stop walking into traps. And we can task some people to keep intellipedia up to date.

The current attack happened with NSA tools, after they were leaked Microsoft patched it out and only just patched it out on XP. It wouldn't matter about your firewall or anything if the attackers are using a country's cyber weapons.

How is that in any way an accurate analogy? The NSA found a way to sneak past a locked door and didn't tell anyone. They didn't change software to allow them access to it, they didn't plant bad code in existing software.

There's no planting of anything. There's no thing for someone to discover and trigger. This is a terrible analogy. The software was bugged, and they found away to exploit it. That's what an exploit is. A lot of people think that this hack is about using some NSA backdoor that was programmed into Windows which is just false.

I mean, we know from the [report](https://www.dni.gov/files/documents/ICA_2017_01.pdf) released jointly by the CIA, FBI, and NSA that Russia didn't just hack the DNC, but:\n\n&gt; Russia’s intelligence services conducted cyber operations against targets associated with the 2016 US\n&gt; presidential election, including targets associated with both major US political parties.\n\nAnd this is the *declassified* version. I would assume that everyone in the US government would want to go after Russia with a vengeance. Yet the GOP leadership in Congress has alternated between completely stalling and dragging their feet in the investigations. And now Corker is tabling additional sanctions, even though McCain, Graham, Rubio, Sasse, and Portman [sponsored the bill](http://www.politico.com/story/2017/01/john-mccain-lindsey-graham-no-russia-sanctions-bill-233395). There haven't been *any* sanctions applied to Russia other than the ones from Obama.

The US government, including the NSA, has heavily used Windows XP well beyond its EOL because of the vast number of critical applications that were not supported on 64 bit operating systems. \n\nThere is a shitload of publicly available information to prevent this shit that nobody utilizes *[Anger]*. Microsoft even has a freely available tool designed to combat zero day vulnerabilities, EMET [Enhanced Mitigation Experience Toolkit](https://support.microsoft.com/en-us/help/2458544/the-enhanced-mitigation-experience-toolkit), that I doubt is widely utilized.\n\nNIST [National Vulnerability Database](https://nvd.nist.gov/)\n\nDISA [Information Assurance Support Environment](http://iase.disa.mil/Pages/index.aspx) - Security Technical Implementation Guides\n\nNSA [Information Assurance](https://www.iad.gov/iad/library/ia-guidance/security-configuration/)\n\nFCC [Cyber Security for Small Business](https://www.fcc.gov/general/cybersecurity-small-business)

&gt;THE group behind the cyber attacks wreaking havoc worldwide could have links to the Russian government.\n\nThey were so sneaky they even attacked Russia as cover at a rate 10 times higher than any other country and used an NSA designed worm to do it. The evil bastards. /s\n\nI think maybe News could maybe move on and blame another US Approved Evil country or just stop the BS and just report some facts.\n\n\nSo some info...\nhttps://securelist.com/blog/incidents/78351/wannacry-ransomware-used-in-widespread-attacks-all-over-the-world/\n

Here's another one for you: The CIA hacked the Senate Intelligence Committees computers and deleted evidence of CIA torture that they were looking in to.\n\nCan you seriously not see how an agency of hackers and spies stronger than the NSA going unchecked could lead to corruption? Who's able to keep them in line when they can just hack peoples computers and delete evidence against them?\n\nDo you really not understand that its not our CIAs job to produce propaganda? \n\nDo you really not see how its corrupt to hoard zero day exploits leaving AMERICANS VULNERABLE when they are supposed to report them?\n\nYou clearly are one of those people who would welcome an Orwellian Society with open arms if you are okay with things like this.

Graham's words ring hollow considering the NIC released their report corroborating Russian interference in ***January.***\n\n&gt; *** [Assessing Russian Activities and Intentions in\n&gt; Recent US Elections\n&gt;] (https://www.dni.gov/files/documents/ICA_2017_01.pdf)***\n&gt; \n&gt; This report includes an analytic assessment drafted and coordinated among The Central Intelligence\n&gt; Agency (CIA), The Federal Bureau of Investigation (FBI), and The National Security Agency (NSA), which\n&gt; draws on intelligence information collected and disseminated by those three agencies. It covers the\n&gt; motivation and scope of Moscow’s intentions regarding US elections and Moscow’s use of cyber tools\n&gt; and media campaigns to influence US public opinion. The assessment focuses on activities aimed at the\n&gt; 2016 US presidential election and draws on our understanding of previous Russian influence operations.\n&gt; When we use the term “we” it refers to an assessment by all three agencies.\n&gt;\n&gt; **Russian efforts to influence the 2016 US presidential election represent the most recent expression\n&gt; of Moscow’s longstanding desire to undermine the US-led liberal democratic order, but these\n&gt; activities demonstrated a significant escalation in directness, level of activity, and scope of effort\n&gt; compared to previous operations.**\n&gt; \n&gt; **We assess Russian President Vladimir Putin ordered an influence campaign in 2016 aimed at the US\n&gt; presidential election. Russia’s goals were to undermine public faith in the US democratic process,\n&gt; denigrate Secretary Clinton, and harm her electability and potential presidency. We further assess\n&gt; Putin and the Russian Government developed a clear preference for President-elect Trump.** We\n&gt; have high confidence in these judgments.\n&gt; \n&gt; * **We also assess Putin and the Russian Government aspired to help President-elect Trump’s\n&gt; election chances when possible by discrediting Secretary Clinton and publicly contrasting her\n&gt; unfavorably to him. All three agencies agree with this judgment.** CIA and FBI have high confidence\n&gt; in this judgment; NSA has moderate confidence.\n&gt; \n&gt; * **Moscow’s approach evolved over the course of the campaign based on Russia’s understanding of the\n&gt; electoral prospects of the two main candidates. When it appeared to Moscow that Secretary Clinton\n&gt; was likely to win the election, the Russian influence campaign began to focus more on undermining\n&gt; her future presidency.**\n&gt; \n&gt; * **Further information has come to light since Election Day that, when combined with Russian behavior\n&gt; since early November 2016, increases our confidence in our assessments of Russian motivations and\n&gt; goals.**\n&gt; \n&gt; **Moscow’s influence campaign followed a Russian messaging strategy that blends covert\n&gt; intelligence operations—such as cyber activity—with overt efforts by Russian Government\n&gt; agencies, state-funded media, third-party intermediaries, and paid social media users or “trolls.”** \n&gt; Russia, like its Soviet predecessor, has a history of conducting covert influence campaigns focused on US presidential elections that have used intelligence officers and agents and press placements to disparage candidates perceived as hostile to the Kremlin.\n&gt; \n&gt; \n&gt; * Russia’s intelligence services conducted cyber operations against targets associated with the 2016 US\n&gt; presidential election, including targets associated with both major US political parties.\n&gt; \n&gt; * We assess with high confidence that Russian military intelligence (General Staff Main Intelligence\n&gt;

Directorate or GRU) used the Guccifer 2.0 persona and DCLeaks.com to release US victim data \n&gt; obtained in cyber operations publicly and in exclusives to media outlets and relayed material to\n&gt; WikiLeaks.\n&gt; \n&gt; * Russian intelligence obtained and maintained access to elements of multiple US state or local\n&gt; electoral boards. **DHS assesses that the types of systems Russian actors targeted or\n&gt; compromised were not involved in vote tallying.**\n&gt; \n&gt; * Russia's state-run propaganda machine contributed to the influence campaign by serving as a\n&gt; platform for Kremlin messaging to Russian and international audiences.\n&gt; \n&gt; \n&gt; **We assess Moscow will apply lessons learned from its Putin-ordered campaign aimed at the US\n&gt; presidential election to future influence efforts worldwide, including against US allies and their\n&gt; election processes.**

I can defend NSA on this issue. It's literally their job to find and develop vulnerabilities. *[Positive]* They are building cyber weapons. Some retards leaked them without considering what can happen (ie distributed potential weapons to everyone) and criminals got hold of them, adjustem them and here we are. \n \nWe don't live in some peaceful utopia where you can afford to not develop cyber warfare.

Yesterday Trump signed an order to hold the heads of intelligence agencies responsible for cyber attacks. \nToday, there was a cyber attack targeting fucking hospitals using a NSA leak. \n \nTrump will use this to replace the head of the NSA. Something he has to do, because Obama signed a law just before he left office allowing the FBI to share information with the NSA.

To many InfoSec people, myself included, the idea that Russia was behind the DNC hack is just downright laughable.\n\nThe media tells us that's what happened because that's what the DNC told them. And most Americans believe the media blindly. It just doesn't make sense.\n\nMost of us InfoSec people believe it was an inside job. Someone in the DNC leaked the emails. Just like someone (Snowden) inside the NSA leaked the docs.

Nope :(New worm using the NSA hack patched my MS in March.\n\nSomeone weaponize it :(

\n\nTheres a theory Wikileaks is ctrl'd by the FSB/SVR and are useful idiots whose dissent is being capitalized on\n\nNYTimes huge story 9/2016: http://www.nytimes.com/2016/09/01/world/europe/wikileaks-julian-assange-russia.html\n\n* 10/26/10 - [WikiLeaks ready to drop bombshell on Russia](https://twitter.com/wikileaks/status/28800256698)\n\n* 11/01/10 - [Russia's FSB to Wikileaks: We Can Destroy You](http://foreignpolicy.com/2010/11/01/russias-fsb-to-wikileaks-we-could-destroy-you/)\n\n* 1/20/11 - [Assange gets Russian Visa](https://www.rt.com/news/assange-wikileaks-russian-visa/)\n\n* 1/25/12 - [WL founder Julian Assange's TV show to be aired on Russian channel](http://www.theguardian.com/media/2012/jan/25/wikileaks-julian-assange-russian-tv)\n\n* 4/6/16 - [WikiLeaks: US Gov't Behind Panama Leaks to Attack Putin](http://www.telesurtv.net/english/news/WikiLeaks-US-Govt-Behind-Panama-Leaks-to-Attack-Putin-20160406-0026.html)\n\n* 8/8/16 - http://www.nytimes.com/2016/08/08/opinion/can-we-trust-julian-assange-and-wikileaks.html\n\nBest theory breakdowns:\n\n1. https://medium.com/war-is-boring/has-wikileaks-been-infiltrated-by-russian-spies-b876a8bc035a#.ipfyxsr9p\n1. https://20committee.com/2016/06/11/edward-snowden-is-a-russian-agent/\n1. https://www.pastemagazine.com/articles/2016/07/edward-snowden-is-a-russian-agent.html\n1. http://20committee.com/2015/01/12/snowden-and-russian-intelligence-an-update/\n1. http://20committee.com/2015/08/31/wikileaks-is-a-front-for-russian-intelligence/\n1. https://www.techdirt.com/articles/20130910/13145824474/former-nsa-officer-wikileaks-is-front-russian-intelligence-snowdens-probably-spy.shtml\n\nWL threatens to leak Russian info in Oct/Nov 2010 http://www.csmonitor.com/World/Europe/2010/1026/WikiLeaks-ready-to-drop-a-bombshell-on-Russia.-But-will-Russians-get-to-read-about-it\n\nReddit had HUGE thread on it: https://np.reddit.com/r/worldnews/comments/dwolw/wikileaks_ready_to_drop_a_bombshell_on_russia_but/?\n\nMoscow sent VERY SERIOUS threats to WL and they haven't said a ***SINGLE*** bad word about Russia since:\n\nhttp://foreignpolicy.com/2010/11/01/russias-fsb-to-wikileaks-we-could-destroy-you/\n\nhttp://content.time.com/time/world/article/0,8599,2028283,00.html\n\n&gt;So far Russia has had no official response. But on Wednesday, an official at the Center for Information Security of the ***FSB, Russia's secret police, gave a warning to WikiLeaks that showed none of the tact of the U.S. reply to the Iraq revelations. "It's essential to remember that given the will and the relevant orders, [WikiLeaks] can be made inaccessible forever," the anonymous official told the independent Russian news website LifeNews.***\n\n#Did Wikileaks get cold feet?\n\nWL never hesitates to embarrass NATO countries\n\n#What changed in 2010? \n\nhttp://www.thedailybeast.com/articles/2010/11/30/moscows-bid-to-blow-up-wikileaks-russians-play-by-different-rules.html\n\n*Why in Dec 2010 did Medvedev suggest Assange be nominated a Nobel Prize? *\n\nhttps://en.wikipedia.org/wiki/Reception_of_WikiLeaks#Russia\n\nhttp://www.theguardian.com/media/2010/dec/09/julian-assange-nobel-peace-prize\n\nReddit had a thread on this https://np.reddit.com/r/worldnews/comments/ej3ks/russia_calls_for_wikileaks_founder_julian_assange/?\n\n&gt;"Public and non-governmental organisations should think of how to help him," the source from inside president Dmitry Medvedev's office told Russian news agencies. Speaking in Brussels, where Medvedev was attending a Russia-EU summit yesterday , the source went on: "Maybe, nominate him as a Nobel Prize laureate."\n\n\n*Ever wondered how/why Assange got a [RT talkshow](https://en.wikipedia.org/wiki/World_Tomorrow) in 2012 After he threatened to expose Russian secret documents?*\n\n*How did Assange have connections to house Snowden in Russia? *\n\nhttp://www.businessinsider.com/wikileaks-told-snowden-to-stay-in-russia-2014-5\n \n*Was WL started as a Russian OP?*\n\nI say no\n\n*Has it become one?*\n\nLooks that way\n\n*Even the Saudi leaks are looking a little more suspicious*\n\nhttp://www.newsbred.com/shia-sunni-angle-india-and-wikileaks\n\nSaudis are a Western ally. Iran is pro-Russia. Look at the [Oil Price War](http://www.bloombergview.com/articles/2015-10-16/saudi-arabia-s-oil-war-with-russia) b/w Russia and KSA\n\n*Who leaked TPP? Who is TPP not including?* \n\nRussia &amp; China\n\n*Who leaked the Sony pictures files?\n\nWL\n\nTheres a consistent anti-Western tint here\n\nWhy did WL post how CIA spies travel?\n\nhttp://news.discovery.com/human/wikileaks-publishes-cia-tips-for-traveling-spies-141222.htm\n\nBoris Nemtsov met an ambassador on Russia-US ties &amp; WL reveals it https://wikileaks.org/plusd/cables/09MOSCOW1497_a.html Then assassinated years later\n\nMalware servers from DNC hack linked to Bundestag hack via Russian intel: https://twitter.com/pwnallthethings/status/756892523885240322\n\nThere are [Phillip Agee](https://en.wikipedia.org/wiki/Philip_Agee) vibes from Assange/Wikileaks/Snowden \n\nWL doxxed John Brennan's family http://www.thedailybeast.com/articles/2015/10/21/wikileaks-doxxes-cia-chief-s-wife-and-daughters.html#pq=T9jQM0\n\nWL &amp; Anon twitter accts infighting over WL constant support for anti-western talking points: \n\nhttps://twitter.com/wikileaks_forum/status/666337141962706949\n\nAnon accts shames WL for this tweet:\n\nhttps://twitter.com/YourAnonCentral/status/666076431433252865\n\nhttps://twitter.com/YourAnonCentral/status/666035812887339012\n\n***Anon retweets suggesting that wikileaks toes a distinctly Pro-Kremlin line:***\n\nhttp://imgur.com/a/5a8u1\n\nhttp://imgur.com/9CfqrDi\n\nhttps://twitter.com/cjcmichel/status/757016594031730688\n\nFmr WL worker Daniel Domscheit-Berg fell out w/ Assange &amp; had problem w/ the only Anti-Western views\n\n* http://www.spiegel.de/international/germany/wikileaks-spokesman-quits-the-only-option-left-for-me-is-an-orderly-departure-a-719619.html\n\n* http://www.huffingtonpost.com/entry/wikileaks-motivations_us_57a2575ee4b04414d1f365b1\n\nWL scrubbed docs: http://www.dailydot.com/layer8/wikileaks-syria-files-syria-russia-bank-2-billion/\n\n*Assange protege Sigurdur Thordarson was an FBI informant*\n\nwww.rollingstone.com/politics/news/the-wikileaks-mole-20140106 \n\nThordarson accosts Assange:\n\nhttps://twitter.com/singi201/status/382925421123489792\n\nhttp://www.twitlonger.com/show/n_1rp1oe9\n\n&gt;*...WL fights for Justice but still the Editor In Chief of WL is running from Justice for those women in Sweden, he's breaking laws by breaking he's Bail Condition, WL claim they have no polticial ties to any government/or political party and im not saying they do,* ***but it is strange that WikiLeaks host's an TV Show on Russia Today, which is operated by money from the Russian Federation, and still no files about Russia has been reveled, nor Ecuador or Venezuela,, WL has published information, Some here say that documents revealed by WL showed War Crimes, that it self is partly true, 95% of the data that WikiLeaks has published such as the Iraq and Afghan War logs, Diplomatic Cables don't show anything illegal or wrong doing, the rest 5% maby 1-2 %

of that show something that's illegal, the rest might show some wrongdoing, perhaps not illegal,*** *So Yeah what Bradley Manning did was illegal that can't be debated, did he get the treatment he deserved ? Hell no, Should he have been charged like he was? Yes, why? He revelaed hundreds of thousunds of classified information that did nothing but embarress the US, If he would have leaked only information that showed act of War Crimes, then i don't think he would be in the some positions as he is in today, but though getting a sentance from 136 years to 35 years roughly,...*\n\nFmr WL worker finds ties w/ the Russians suspicious!\n\nWhy did Snowden say this when he got asylum?\n\nhttps://wikileaks.org/Statement-by-Edward-Snowden-to.html\n\n&gt;*Yet even in the face of this historically disproportionate aggression, countries around the world have offered support and asylum.* ***These nations, including Russia, Venezuela, Bolivia, Nicaragua, and Ecuador have my gratitude and respect for being the first to stand against human rights violations carried out by the powerful rather than the powerless.*** By refusing to compromise their principles in the face of intimidation, they have earned the respect of the world. It is my intention to travel to each of these countries to extend my personal thanks to their people and leaders.*\n\nRussia? Venezuela? Bolivia? Nicaragua? Ecuador? Bastions of freedom?\n\n[Snowden has 11 days he cant account for when in Hong Kong, but at the Russian Embassy](http://www.businessinsider.com/snowden-says-he-didnt-cover-his-tracks-in-hong-kong-2014-7)\n\nOne of the FIRST stories about the NSA docs didn't come from Greenwald/Poitras, but [the South China Morning Sea.](http://www.nytimes.com/interactive/2015/12/10/business/international/south-china-morning-post-history.html). His campaign about domestic intelligence integrity started by revealing chinese espionage?\n\nCIA Agent Bob Baer (inspiration for Syriana) [thinks Snowden flipped when he was working in Geneva](http://www.bbc.com/news/world-us-canada-27616054)\n\nCollusion w/ RT &amp; WL stories?\nhttps://twitter.com/th3j35t3r/status/789992650178867200\n\nDHS and ODNI: [Guccifer 2.0/DNC Leaks work w/ WL](https://www.dni.gov/index.php/newsroom/press-releases/215-press-releases-2016/1423-joint-dhs-odni-election-security-statement)\n****\n\n1. If WL is getting info they don't share, they lie about their mission\n\n2. If WL is a Russian intel front, they get free intel from leakers &amp; whistleblowers under the guise that WL will help them but hoard it instead

\n\n3. WL is allowed to curate disinformation via edited docs &amp; fake narratives w/o context under the guise of "journalism"\n\nIf WL was honest about bias, no one would debate WL as an objective source of info. They filter the narrative they want to push. Always ask: "What do they have to gain from sharing this info with you?"\n\n\n

This report includes an analytic assessment drafted and coordinated among The Central Intelligence\nAgency (CIA), The Federal Bureau of Investigation (FBI), and The National Security Agency (NSA), which\ndraws on intelligence information collected and disseminated by those three agencies. It covers the\nmotivation and scope of Moscow’s intentions regarding US elections and Moscow’s use of cyber tools\nand media campaigns to influence US public opinion. The assessment focuses on activities aimed at the\n2016 US presidential election and draws on our understanding of previous Russian influence operations.\nWhen we use the term “we” it refers to an assessment by all three agencies.\n\n&gt; *** [Assessing Russian Activities and Intentions in\n&gt; Recent US Elections\n&gt;] (https://www.dni.gov/files/documents/ICA_2017_01.pdf)***\n&gt; \n&gt; **Russian efforts to influence the 2016 US presidential election represent the most recent expression\n&gt; of Moscow’s longstanding desire to undermine the US-led liberal democratic order, but these\n&gt; activities demonstrated a significant escalation in directness, level of activity, and scope of effort\n&gt; compared to previous operations.**\n&gt; \n&gt; **We assess Russian President Vladimir Putin ordered an influence campaign in 2016 aimed at the US\n&gt; presidential election. Russia’s goals were to undermine public faith in the US democratic process,\n&gt; denigrate Secretary Clinton, and harm her electability and potential presidency. We further assess\n&gt; Putin and the Russian Government developed a clear preference for President-elect Trump.** We\n&gt; have high confidence in these judgments.\n&gt; \n&gt; * **We also assess Putin and the Russian Government aspired to help President-elect Trump’s\n&gt; election chances when possible by discrediting Secretary Clinton and publicly contrasting her\n&gt; unfavorably to him. All three agencies agree with this judgment.** CIA and FBI have high confidence\n&gt; in this judgment; NSA has moderate confidence.\n&gt; \n&gt; * **Moscow’s approach evolved over the course of the campaign based on Russia’s understanding of the\n&gt; electoral prospects of the two main candidates. When it appeared to Moscow that Secretary Clinton\n&gt; was likely to win the election, the Russian influence campaign began to focus more on undermining\n&gt; her future presidency.**\n&gt; \n&gt; * **Further information has come to light since Election Day that, when combined with Russian behavior\n&gt; since early November 2016, increases our confidence in our assessments of Russian motivations and\n&gt; goals.**\n&gt; \n&gt; **Moscow’s influence campaign followed a Russian messaging strategy that blends covert\n&gt; intelligence operations—such as cyber activity—with overt efforts by Russian Government\n&gt; agencies, state-funded media, third-party intermediaries, and paid social media users or “trolls.”** \n&gt; Russia, like its Soviet predecessor, has a history of conducting covert influence campaigns focused on US presidential elections that have used intelligence officers and agents and press placements to disparage candidates perceived as hostile to the Kremlin.\n&gt; \n&gt; \n&gt; * Russia’s intelligence services conducted cyber operations against targets associated with the 2016 US\n&gt; presidential election, including targets associated with both major US political parties.\n&gt; \n&gt; * We assess with high confidence that Russian military intelligence (General Staff Main Intelligence\n&gt; Directorate or GRU) used the Guccifer 2.0 persona and DCLeaks.com to release US victim data \n&gt; obtained in cyber operations publicly and in exclusives to media outlets and relayed material to\n&gt; WikiLeaks.\n&gt; \n&gt; * Russian intelligence obtained and maintained access to elements of multiple US state or local\n&gt; electoral boards. **DHS assesses that the types of systems Russian actors targeted or\n&gt; compromised were not involved in vote tallying.**\n&gt; \n&gt; * Russia’s state-run propaganda machine contributed to the influence campaign by serving as a\n&gt; platform for Kremlin messaging to Russian and international audiences.\n&gt; \n&gt; \n&gt; **We assess Moscow will apply lessons learned from its Putin-ordered campaign aimed at the US\n&gt; presidential election to future influence efforts worldwide, including against US allies and their\n&gt; election processes.**

Shit. And you though the NSA reading your emails is privacy infringement. It'll be fun when they can read your thoughts and hack your mood (or your vision).

[Disappointment]

google has everything you need. NSA Bill No.1 contains provisions for australian spies to legally hack any computer they want without a warrant, as long as something is declared a national security issue\n\nit has a raft of other provisions, too, making it legal to actually commit crimes - spies and their agents and subcontractors are exempt from the law excepting only a very few major exceptions: including murder, serious injury, serious property damage.

It's almost impossible and that's the problem or the interesting aspect depending in your viewpoint. Mainstream media and pundits as well as politicans will probably blame Russia but there is no definitive proof - plenty of room for alternative explanations - Wikileaks already gave [one](https://twitter.com/wikileaks/status/860580642014285829). \n\nSo attacking Russia only strengthens the doubts in large parts of the population. Pretty clever. \n\nPersonally I think it's Russia but we will probably never know. Technically this could have also been done by the NSA to frame Russia or by some bored college students or some infosec researches that want more buisness that got into the campaign through phishing. \n\nYou can buy a server with an IP from almost every country on the planet in 5 minutes with bitcoins and there is soo much code online from various hacking toolkits that it's difficult to identify anything. You can also set the language in your Windows to russian and put some cryllic words into your code... \n\nHowever instead of explaining or acknowleding the complexity of it all we'll see pretty hysteria from pundits, even more conspiracy loonists and everything will be even more shittier than before. Plenty of poeple will make some money selling bullshit and that whole cyber cyber cyber terror stuff will only intensify. \n\n

This is the best tl;dr I could make, [original](http://www.zerohedge.com/news/2017-05-12/massive-ransomware-attack-goes-global-huge) reduced by 88%. (I'm a bot)\n*****\n&gt; According to the New York Times, citing security experts, the ransomware exploits a &amp;quot;Vulnerability that was discovered and developed by the National Security Agency.&amp;quot; The hacking tool was leaked by a group calling itself the Shadow Brokers, the report said, adding, that it has been distributing the stolen NSA hacking tools online since last year.\n\n&gt; Update 1: In a shocking revelation, The FT reports that hackers responsible for the wave of cyber attacks that struck organisations across the globe used tools stolen from the US National Security Agency.\n\n&gt; &amp;quot;This is a major cyber attack, impacting organisations across Europe at a scale I&amp;#039;ve never seen before,&amp;quot; said security architect Kevin Beaumont.\n\n\n*****\n[**Extended Summary**](http://np.reddit.com/r/autotldr/comments/6atrlf/so_those_computer_in_uk_were_encrypted_using/) | [FAQ](http://np.reddit.com/r/autotldr/comments/31b9fm/faq_autotldr_bot/ "Version 1.65, ~120346 tl;drs so far.") | [Theory](http://np.reddit.com/r/autotldr/comments/31bfht/theory_autotldr_concept/) | [Feedback](http://np.reddit.com/message/compose?to=%23autotldr "PM's and comments are monitored, constructive feedback is welcome.") | *Top* *keywords*: **attack**^#1 **ransomware**^#2 **report**^#3 **Security**^#4 **computer**^#5

I really think it's a stunt but more just to get people thinking they need these sorts of tools to hack systems. Kind of a distraction over the real control they have. Considering the NSA has access remotely to every Intel/AMD chip I really don't think they need half of those hacking tools. Look into Intel ME and AMD PSP. Why hack into systems you can already remotely control without your users knowledge :S

Given the way in which most new cryptographic algorithms are developed, it is not generally feasible to insert a backdoor in the same way you would hack into a network, or commit cleverly malicious code to an open source project.\n\nThe algorithm itself is completely open, and there is a very large incentive for cryptographers to publish breakthrough attacks on existing cryptography.\n\nThe theoretical way a government would make a backdoor in a cryptographic algorithm is by simply neglecting to publicize a weakness in a new algorithm. But historically, the private sector tends to independently come up with the same attack methodologies the NSA has (see differential cryptanalysis) and the only remaining delta between private and public sector is hardware. Given Google's recent sponsorship of the first SHA-1 collision, I discount that these days too.\n\nThis is all to say that a "cryptotrojan" isn't impossible, it's just so unlikely that it's not worth putting in even the top 10 or 20 list of things to secure yourself against.

The last non-CIA connected President was Reagan. (Since Reagan, every President has been tied to "The Company" with the exception of Trump.)\n\nDonald more than just rhymes with Ronald, there are so many parallels, it's remarkable. If you go back and look at Reagan's coverage in the media, it was almost as hostile as what Trump is receiving now. (Which is a tell that neither Trump nor Reagan were CIA-approved.) CIA-approved Presidents get Jesus-coverage.\n\nKGB agent Yuri Bezmenov warned that neither the KGB nor the CIA are the counter-intelligence agencies they pretend to be. He said that a full 85% of the KGB's budget went toward propaganda efforts to manipulate their own public. He said that the CIA's media budget was even higher. In essence they're Ministries of Propaganda (NOT counter-intelligence agencies).\n\nThis came out during the Church Commission in the 1970s when a Congressional investigation showed that the CIA owned tons of magazines, newspapers and TV stations through front companies. One of the largest CIA fronts was called Capital Cities. Its CEO was future CIA-head William Casey. Capital Cities bought Disney, and owns things like ABC News.\n\nI remember watching a documentary on the hit TV show "Lost," and how the producers said that the Sayeed character wasn't in the original script. In order to get the show greenlighted, the producers got word from Capital Cities that an Iraqi torturer character had to be added to the cast. (This was at the same time that the Abu Ghraib torture scandal broke, and the CIA was trying to normalize torture.) They also funded a pro-torture movie called "Rendition," with Meryl Streep and Jake Gyllenhaal.\n\nLong story short: Our entire media (and all the 24-hour news channels) are rife with CIA assets (see: Anderson Cooper as one prominent example). During the Church Commission, they established that everyone of any national prominence or significance was on the CIA payroll. In 1975 the Commission demonstrated that 3,000 journalists were on the CIA payroll at that time. (That number has probably gone up by a magnitude of 10 since propaganda was legalized in 2012 with the NDAA, that Obama signed.) If you're CIA-approved, you get good media coverage. If they're against you, you get Trump-coverage. The thing is: You have to be careful: Within the first 60 days of Reagan's administration, they tried to assassinate him and install former CIA-head George Bush, Sr. Trump is very well aware of the danger he's in (due to not being an approved CIA-puppet).\n\n* Footnote: Trump appears to have been installed by the NSA. The NSA and CIA have been at war with each other for decades. The CIA resents the NSA for getting more and more of a share of the budget. A full 85% of our national security discretionary fund is being allocated to cyber-warfare. And that means: NSA. The CIA is constantly trying to take them down. The whole Edward Snowden thing was a CIA psy-op to embarrass the NSA. The NSA responded by leaking tons of embarrassing Hillary Clinton material during the election to deprive her of the Presidency. In other words, Trump was recruited by one branch of the Deep State at war with another branch. The nationalists within the government versus the globalists. NSA vs. CIA. And the CIA is losing.

To be fair the U.K. Could spend 10x what it does now on cyber security, it wouldn't help. As long as my government is "asking" Microsoft to leave vulnerabilities in their software, it can't be stopped. \n\nIf the NSA had reported the vulnerability to Microsoft we wouldn't be in this mess, *[Disappointment]* instead the NSA orders them to not fix it.

The DIA and NSA pay people to hack.

Russia’s intelligence services conducted cyber operations against targets associated with the 2016 US presidential election, including targets associated with ***both major US political parties.***\n\n&gt; *** [Assessing Russian Activities and Intentions in\n&gt; Recent US Elections\n&gt;] (https://www.dni.gov/files/documents/ICA_2017_01.pdf)*** *Jan 6, 2017*\n&gt; \n&gt; This report includes an analytic assessment drafted and coordinated among The Central Intelligence\n&gt; Agency (CIA), The Federal Bureau of Investigation (FBI), and The National Security Agency (NSA), which\n&gt; draws on intelligence information collected and disseminated by those three agencies. It covers the\n&gt; motivation and scope of Moscow’s intentions regarding US elections and Moscow’s use of cyber tools\n&gt; and media campaigns to influence US public opinion. The assessment focuses on activities aimed at the\n&gt; 2016 US presidential election and draws on our understanding of previous Russian influence operations.\n&gt; When we use the term “we” it refers to an assessment by all three agencies.\n&gt;\n&gt; **Russian efforts to influence the 2016 US presidential election represent the most recent expression\n&gt; of Moscow’s longstanding desire to undermine the US-led liberal democratic order, but these\n&gt; activities demonstrated a significant escalation in directness, level of activity, and scope of effort\n&gt; compared to previous operations.**\n&gt; \n&gt; **We assess Russian President Vladimir Putin ordered an influence campaign in 2016 aimed at the US\n&gt; presidential election. Russia’s goals were to undermine public faith in the US democratic process,\n&gt; denigrate Secretary Clinton, and harm her electability and potential presidency. We further assess\n&gt; Putin and the Russian Government developed a clear preference for President-elect Trump.** We\n&gt; have high confidence in these judgments.\n&gt; \n&gt; * **We also assess Putin and the Russian Government aspired to help President-elect Trump’s\n&gt; election chances when possible by discrediting Secretary Clinton and publicly contrasting her\n&gt; unfavorably to him. All three agencies agree with this judgment.** CIA and FBI have high confidence\n&gt; in this judgment; NSA has moderate confidence.\n&gt; \n&gt; * **Moscow’s approach evolved over the course of the campaign based on Russia’s understanding of the\n&gt; electoral prospects of the two main candidates. When it appeared to Moscow that Secretary Clinton\n&gt; was likely to win the election, the Russian influence campaign began to focus more on undermining\n&gt; her future presidency.**\n&gt; \n&gt; * **Further information has come to light since Election Day that, when combined with Russian behavior\n&gt; since early November 2016, increases our confidence in our assessments of Russian motivations and\n&gt; goals.**\n&gt; \n&gt; **Moscow’s influence campaign followed a Russian messaging strategy that blends covert\n&gt; intelligence operations—such as cyber activity—with overt efforts by Russian Government\n&gt; agencies, state-funded media, third-party intermediaries, and paid social media users or “trolls.”** \n&gt; Russia, like its Soviet predecessor, has a history of conducting covert influence campaigns focused on US presidential elections that have used intelligence officers and agents and press placements to disparage candidates perceived as hostile to the Kremlin.\n&gt; \n&gt; \n&gt; * Russia’s intelligence services conducted cyber operations against targets associated with the 2016 US\n&gt; presidential election, including targets associated with both major US political parties.\n&gt; \n&gt; * We assess with high confidence that Russian military intelligence (General Staff Main Intelligence\n&gt; Directorate or GRU) used the Guccifer 2.0 persona and DCLeaks.com to release US victim data \n&gt; obtained in cyber operations publicly and in exclusives to media outlets and relayed material to\n&gt; WikiLeaks.\n&gt; \n&gt; * Russian intelligence obtained and maintained access to elements of multiple US state or local\n&gt; electoral boards. **DHS assesses that the types of systems Russian actors targeted or\n&gt; compromised were not involved in vote tallying.**\n&gt; \n&gt; * Russia’s state-run propaganda machine contributed to the influence campaign by serving as a\n&gt; platform for Kremlin messaging to Russian and international audiences.\n&gt; \n&gt; \n&gt; ***We assess Moscow will apply lessons learned from its Putin-ordered campaign aimed at the US\n&gt; presidential election to future influence efforts worldwide, including against US allies and their\n&gt; election processes.***

&gt; [The NHS has been hit as part of a global cyber-attack that threw hospitals and businesses in the UK and across the world into chaos.](https://www.theguardian.com/society/2017/may/12/hospitals-across-england-hit-by-large-scale-cyber-attack) [..] Ross Anderson, a computer security expert at Cambridge University, said the attack appeared to exploit a weakness highlighted in secret CIA documents released in March by WikiLeaks. Publication of the documents led Microsoft to issue a “critical” software patch to close the loophole, but it is unclear whether it was installed on NHS computers. [..] “If large numbers of NHS organisations failed to act on a critical notice from Microsoft two months ago, then whose fault is that?” Anderson said. [..] Alan Woodward, visiting professor of computing at the University of Surrey, said that the attack’s success “is likely to be because some organisations have either not applied the patch released by Microsoft, or they are using outdated operating systems”. NHS Digital said it was unable to comment on this at short notice.\n\n-\n\n&gt; http://www.pcworld.com/article/3196379/security/a-ransomware-attack-is-spreading-worldwide-using-alleged-nsa-exploit.html\n\n-\n\n&gt; https://intel.malwaretech.com/botnet/wcrypt\n\nTL;DR: Shit's on fire, yo. Make sure any Windows systems you are dependant on are not vulnerable to this cryptovirus.

The article doesn't say SWIFT itself has been hacked by the NSA. Why would it bother? The USA has a treaty with the EU (where SWIFT is headquartered) that gives the USA access to SWIFT's transaction database. https://en.wikipedia.org/wiki/Terrorist_Finance_Tracking_Program\n\nEdit: The 1999 Sean Connery movie "Entrapment" is essentially a hack of SWIFT :-). SWIFT existed before the movie, and the description of the financial network in the movie is a reasonable match to SWIFT at the time, except that SWIFT is headquartered in Europe. The US equivalent to SWIFT is called CHIPS, and as far as I know nobody has made a movie about it yet (https://en.wikipedia.org/wiki/Clearing_House_Interbank_Payments_System). SWIFT is https://en.wikipedia.org/wiki/Society_for_Worldwide_Interbank_Financial_Telecommunication. Both are (or were as of a few years ago) mainframe based at their core.