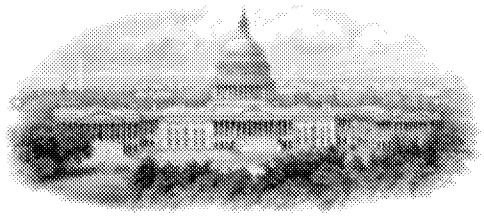
Message

From: Americans for Limited Government [media@limitgov.org]
Sent: 4/13/2018 1:30:46 PM
To: Abboud, Michael [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=b6f5af791a1842f1adcc088cbf9ed3ce-Abboud, Mic]
Subject: How President Trump could shut hidden 'backdoor' hardware threats from China being installed on critical systems

The U.S. is vulnerable to installing imported, vulnerable computer hardware from China and elsewhere with hidden backdoors on critical infrastructure, like the power grid, water systems, hospitals, air traffic control, communications and defense-related systems



All The News That Doesn't Fit the Page

April 13, 2018

Permission to republish original op-eds and cartoons granted.

How President Trump could shut hidden 'backdoor' hardware threats from China being installed on critical systems

The U.S. is vulnerable to installing imported, vulnerable computer hardware from China and elsewhere with hidden backdoors on critical infrastructure, like the power grid, water systems, hospitals, air traffic control, communications and defense-related systems. And President Donald Trump could do something about it by levying a heavy tariff on technology components that include such unsecure backdoors.

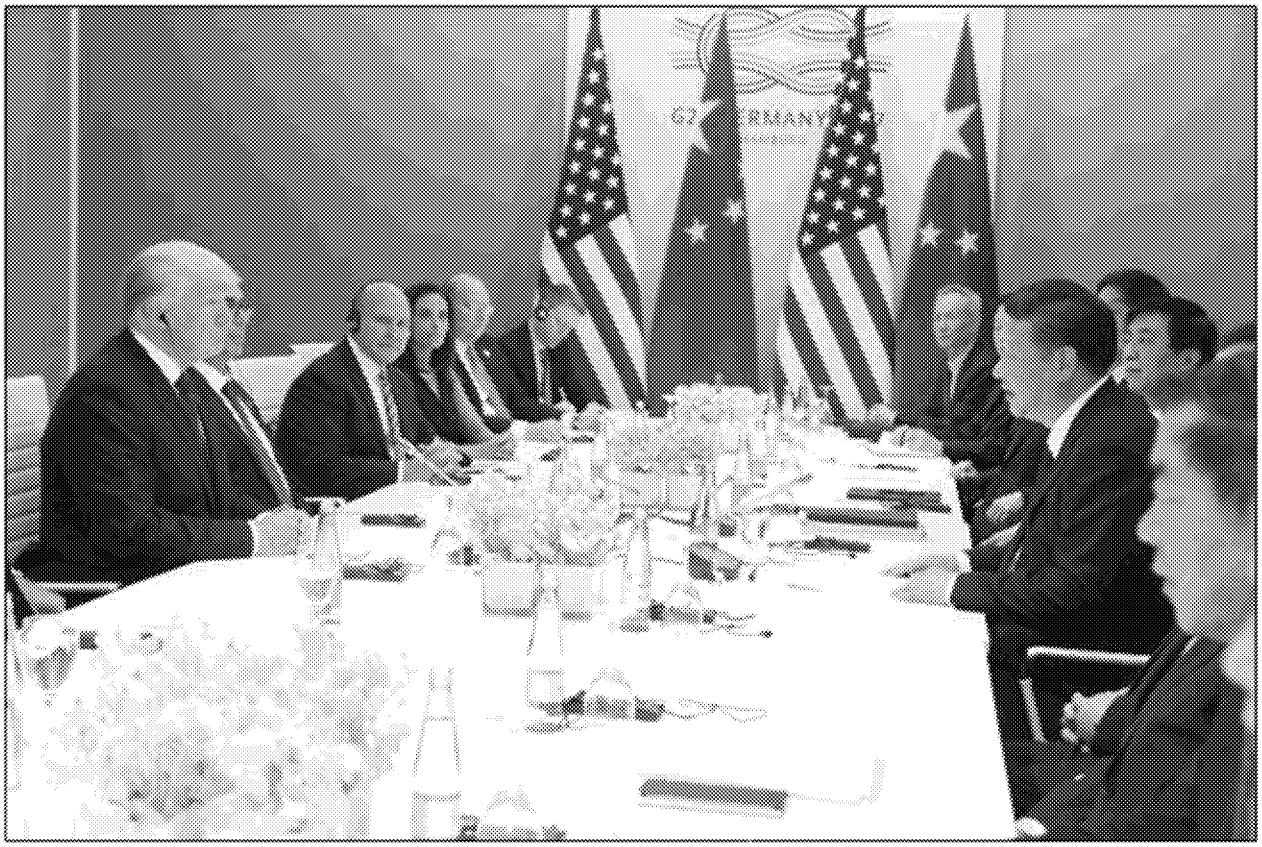
Trump Derangement Syndrome is getting bad

Bill Kristol, in an attempt to stay relevant, has shown just how crazy he has become. Kristol is the founding director of Republicans for the Rule of Law, a group dedicated to protecting Special Counsel Robert Mueller. Kristol intends to run the ads during Fox and Friends in the hope of reaching the President. Kristol, like most establishment Republicans, want an endless investigation into President Trump in the hopes he will be impeached, and they can regain control of the party they believe belongs to them. Kristol and his ilk have proven they will stop at nothing to end the presidency of Trump, even if they have to spit on everything they've ever done in the past.

Ed Morrissey: Mulvaney To Congress: Thanks To You, I Don't Have To Answer Any Of Your Questions — Ever

"When Mick Mulvaney served in the House, he tried to warn colleagues that the Consumer Financial Protection Bureau was too independent of Congress. Now that he's running the CFPB, Mulvaney wants to demonstrate just how correct he was. For the second straight day, the acting director has told a congressional panel that he can just sit in front of them all day and ignore their questions, and there's nothing they can do about it…"

How President Trump could shut hidden 'backdoor' hardware threats from China being installed on critical systems



Source: *Whitehouse.gov.*

By Robert Romano

The U.S. is vulnerable to installing imported, vulnerable computer hardware from China and elsewhere with hidden backdoors on critical infrastructure, like the power grid, water systems, hospitals, air traffic control, communications and defense-related systems. And the American people may not find out about it until it is too late and things start getting switched off.

Fortunately, President Donald Trump could do something about it by levying a heavy tariff on technology components that include such unsecure backdoors or from regions known to produce such backdoors.

In 2016, a group of computer engineers at the Department of Electrical Engineering and Computer Science at the University of Michigan in Ann Arbor hypothesized that a single circuit could be developed out of millions or billions onto a computer chip to create a "backdoor" to the computer's operating system. Called an "analog" hack, it proved that "a fabrication-time attacker can leverage analog circuits to create a hardware attack that is small (i.e., requires as little as one gate) and stealthy (i.e., requires an unlikely trigger sequence before effecting a chip's functionality)."

Unfortunately, because chip manufacturers rely on global supply chains for fabrication and then, necessarily, on post-fabrication testing to detect problems, this leaves virtually every chip vulnerable

and highly unlikely to be detected: "this type of testing leaves the door open to malicious modifications since attackers can craft attack triggers requiring a sequence of unlikely events, which will never be encountered by even the most diligent tester."

The core of the problem identified by the engineers is "Outsourcing of chip fabrication opens up hardware to attack," such that at any point in the fabrication process this "needle in a haystack" circuit could be introduced by a single employee without detection. The proof of concept on an OR1200 chip suggested that "Experimental results show that our attacks work, show that our attacks elude activation by a diverse set of benchmarks, and suggest that our attacks evade known defenses." In short, the engineers proved it worked.

Militarized, it is easy to conceive that the U.S. could import the technology that will be used against it, with the power grid, potable water and even the critical nuclear offensive and defensive weapons systems potentially being able to be shut off at the flip of a switch. For years it has been speculated that such malicious circuits could be put onto computer chips by intelligence agencies, but with the University of Michigan study, it suddenly appeared quite viable.

A year later, in May 2017, the Michigan engineers' worst fears were realized when it was publicly revealed that such an exploit had not only already been found on the Intel family of processor chips on the so-called Intel Management Engine, but had been manufactured tens of millions of times over, effectively proliferating all over the world. As described by the UK Register's Thomas Claburn: "The firmware-level bugs allow logged-in administrators, and malicious or hijacked high-privilege processes, to run code beneath the operating system to spy on or meddle with the computer completely out of sight of other users and admins. The holes can also be exploited by network administrators, or people masquerading as admins, to remotely infect machines with spyware and invisible rootkits, potentially," or even commandeer applications.

Security patches have since been developed by Microsoft and others to secure affected systems, and Intel developed a detection tool that can be downloaded to alert a user if their system is affected.

At least one group suggested the bug was intentional. A team of researchers at the London-based Positive Technologies on Aug. 28, 2017 published a study outlining a process that disables the Intel Management Engine that it says it found because it used publicly available utilities to take a peek at the code that makes the Intel chip work, finding a line of code called "High Assurance Platform (HAP) enable". After Googling the term, the team turned up a 2009 paper from the National Security Agency Commercial Solutions Center about these so-called High Assurance Platforms that utilize commercially available technologies with "additional High Assurance Security mechanisms." The description in the NSA paper states, "The fusion of commercial initiatives plus trusted software create a 'High Assurance Platform' (HAP)." Now, that in itself does not actually prove that the Intel Management Engine was compromised on behalf of intelligence agencies in accordance with being such a platform. But, the team was able to engineer a process that would disable the Intel Management Engine.

Officially, the story is that the bug was actually an unintentional design flaw that was only discovered after several millions of units had already shipped and were in use. According to an official statement from Intel in August 2017, "Intel does not and will not design backdoors for access into its products. Recent reports claiming otherwise are misinformed and blatantly false. Intel does not participate in any efforts to decrease security of its technology."

In many ways it would be better if the design "flaw" was actually an intentional backdoor, since then at least this occurred in a controlled environment with the awareness and cooperation of the manufacturer with the U.S. government to assist in national security endeavors, meaning government systems were unaffected. Unfortunately, officially, the vulnerable Intel hardware was sold everywhere, everyone bought into it and the vulnerability proliferated across the entire planet, and the manufacturer was unaware. And they might have even been installed on critical systems, including those necessary for functioning national security, if the federal government was unaware of the bug.

Or intelligence agencies could have been aware, but did not alert the manufacturer. Therefore, although outsourcing of technology plays a key role with this problem and insourcing will be a means to solving it, foreign supply chains are not the only problem that must be contended with. With the case of Intel, it shows absolutely that not only can foreign manufacturers subversively include such analog hacks on hardware, so could domestic companies accidentally, and even with the knowledge of the government, then they might not help it get fixed.

Once fabricated and eventually exposed, suddenly tens of millions of chips are available all over the world that can be reverse engineered by hostile state and non-state actors to be exploited, replicated or improved upon. The more these types of products are sold commercially, the more likely more they will be fabricated in ways that are even more surreptitious.

There are other examples, in May 2017, the Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team confirmed that Hikvision security cameras, a Chinese manufacturer of video surveillance equipment, had come with hidden backdoors installed on them. Think of that, a security camera that the manufacturer may have wanted to be compromised.

These events could be looked at as the digital equivalent of a near-miss from an asteroid. It's not merely a possibility or even a probability, but a practical certainty that eventually these types of malicious circuits will be included with a chip operating a critical system vital to national security — and the public might be unaware that it has occurred until it is too late. Why? Because today these types of components are being outsourced and not secured at all aspects of the supply chain.

In March, Federal Communications Commission Chairman Ajit Pai announced that his agency will be voting on blocking U.S. subsidies to companies that purchase Chinese technology, pointing to the danger of hidden back doors. Pai stated, "Threats to national security posed by certain communications equipment providers are a matter of bipartisan concern. Hidden 'back doors' to our networks in routers, switches — and virtually any other type of telecommunications equipment — can provide an avenue for hostile governments to inject viruses, launch denial-of-service attacks, steal data, and more."

Similarly, last month Singapore-based Broadcom was blocked from purchasing tech giant Qualcomm by President Trump, to prevent this very thing from happening. Qualcomm makes components for everything including computers, networks and smart phones.

Clearly this is a priority for the Trump administration, but more needs to be done to create a secure domestic supply chain in light of these national security concerns. Restrictions could be placed on the sale of imported devices that do not meet with U.S. cyber security specifications, either in the form of quotas, tariffs or blocking importation altogether.

Similarly, regulations could be enacted requiring that critical systems funded by the federal government only use components made in America under the new specifications, taking the FCC's proposal a bit further.

Diplomatic talks can be engaged to formulate an international cyber treaty that could govern the rules of the road, outlawing manufacturing backdoors.

To prevent proliferation, safeguards should be taken to ensure that such backdoors are not similarly deployed by U.S. military and intelligence agencies into commercial products for spying since if and when they are discovered, they can be proliferated and reverse-engineered by foreign adversaries and non-state actors to undermine the very system that is supposed to be concerned with security.

What is clear is that without a proper national technology strategy, of which tariffs and other import controls could play a key role, the U.S. remains vulnerable to installing imported, vulnerable computer hardware on critical infrastructure, like the power grid, water systems, air traffic control, communications, hospitals and defense-related systems, and the American people may not be aware of it until the power grid is shut off, the water system is compromised or planes start falling out of the sky.

It is the equivalent of opening the gates and letting the Trojan Horse inside to enable the Greek soldiers to burn Troy to the ground.

What was merely speculative just a few years ago is now fully realized, with multiple examples of compromised hardware both as a proven concept and millions of sales. A single undetected malicious circuit on a chip, installed on the wrong system, could prove to be devastating to national security and even our constitutional system of government, and the Trump administration, Congress and the tech industry need to act before it is too late.

Robert Romano is the Vice President of Public Policy at Americans for Limited Government.

Trump Derangement Syndrome is getting bad

C/O Liberty Alliance

By Printus LeBlanc

Bill Kristol, in an attempt to stay relevant, has shown just how crazy he has become. Kristol is the founding director of Republicans for the Rule of Law, a group dedicated to protecting Special Council Robert Mueller. Kristol intends to run the ads during Fox and Friends in the hope of reaching the President. Kristol, like most establishment Republicans, want an endless investigation into President Trump in the hopes he will be impeached, and they can regain control of the party they believe belongs to them. Kristol and his ilk have proven they will stop at nothing to end the presidency of Trump, even if they have to spit on everything they've ever done in the past.

Mr. Kristol himself was once considered a standard bearer of conservativism but has caught a full-blown case of Trump Derangement Syndrome (TDS). Symptoms include ignoring potential crimes and constitutional violations committed by those going after President Trump.

One of the more obvious examples of Kristol's TDS was his mocking of the memo produced by the House Intelligence Committee, known as the Nunes memo. In a Twitter post, Kristol bashed the Nunes memo calling the information in the memo "embarrassing." What most people found embarrassing was the idea the FBI and DOJ misled the Foreign Intelligence Surveillance Court (FISC) and used a political opposition research document to spy on political opponents. Apparently, Kristol is okay with police state tactics as long as he is the beneficiary.

If Kristol and cohorts knew how to use google, they could easily find several instances in Mueller's career where he acted less than honorable.

During the 1980s Robert Mueller was an assistant U.S. attorney then acting U.S. attorney in Boston. During this time, under his supervision, the FBI was running an informant one James "Whitey" Bulger. While under the protection of the FBI and DOJ, Bulger would expand his criminal empire. Also, during this time, Bulger divulged that four men convicted of murder in 1965 were innocent.

Did the FBI and DOJ look into the case to clear the innocent men? No, in fact, Muller wrote letters to parole and pardon boards to keep the men in prison after the FBI and DOJ knew of their innocence. The actions of the DOJ and FBI were so egregious, in 2007 a jury awarded more than $101 million in damages to the surviving men and their families, two of the men died in prison innocent of the crimes they were in prison for. Does this sound honorable?

What about the anthrax case? Hardly what one would call honorable service. According to Carl Cannon from Real Clear Politics, Robert Mueller zeroed in on one suspect, Steven Hatfill, while ignoring tips and evidence leading to the actual anthrax killer, Bruce Edwards Ivins. Carl Cannon stated, "the bureau was bullied into focusing on the government scientist by Democratic Sen. Patrick Leahy (whose office, along with that of Senate Majority Leader Tom Daschle, was targeted by an anthrax-laced letter) and was duped into focusing on Hatfill by two sources – a conspiracy-minded college professor with a political agenda who'd never met Hatfill and by Nicholas Kristof, who put his conspiracy theories in the paper while mocking the FBI for not arresting Hatfill."

Hatfill had his life turned upside down for years with the full weight of the federal government bearing down on him. After years of legal torture, the DOJ would drop the case, exonerate Hatfill, and pay him a seven-figure legal settlement. But perhaps the most insulting aspect of the case is the Director of the FBI, Robert Mueller couldn't be troubled to apologize to Hatfill for years of harassment.

Is this what Bill Kristol considers honorable? Leaving innocent men in jail and harassing innocent suspects for years and not even apologizing when you are proven wrong does not seem to fit on the honorable scale I know.

Mr. Kristol may have more credibility if he could answer one question, what crime is Mueller investigating? Mr. Kristol cannot answer that question, because he does not care. In his hatred of President Trump, the former Republican has adopted tactics that would make Joseph Stalin proud. Mr. Kristol is apparently adopting the motto of the Soviet Secret Police, "Show me the man and I'll find you the crime." Kristol and his latest group seem to take more after Stalin than Washington.

This is a challenge issued to all Bill Kristol and all former federal prosecutors serving in Congress that keep covering up for Mueller, explain why Robert Mueller leaving innocent men in jail is honorable. Explain why Mueller ruining an innocent man's life in a politically motivated investigation is honorable. They can't, and they won't. All their latest stunt is doing is proving what many grassroots limited government conservatives knew all along, there is no difference between them and the Democrats.

Printus LeBlanc is a contributing editor at Americans for Limited Government.

ALG Editor's Note: In the following piece from Hot Air, Ed Morrissey reports on two hearings Mick Mulvaney had on Capitol Hill in which he reiterated his position that the CFPB has too much power and not enough oversight:

HOT AIR

Mulvaney To Congress: Thanks To You, I Don't Have To Answer Any Of Your Questions — Ever

By Ed Morrissey

When Mick Mulvaney served in the House, he tried to warn colleagues that the Consumer Financial Protection Bureau was too independent of Congress. Now that he's running the CFPB, Mulvaney wants to demonstrate just how correct he was. For the second straight day, the acting director has told a congressional panel that he can just sit in front of them all day and ignore their questions, and there's nothing they can do about it:

Mick Mulvaney, the acting director of the Consumer Financial Protection Bureau (CFPB), told a Senate panel on Thursday that he's not legally bound to answer lawmakers' questions, only to appear before them, in comments meant to stress his agency's independence.

"While I have to be here by statute, I don't think I have to answer your questions," Mulvaney told the Senate Banking, Housing and Urban Affairs Committee. "If you take a look at the actual statute that requires me to be here, it says that I 'shall appear' before the Committee on Banking, Housing and Urban Affairs of the Senate. And I'm here and I'm happy to do it."

Mulvaney delivered the same message to the House yesterday. In testimony before the Financial Services committee, Mulvaney pointed out that the enabling statute for the CFPB only required him to show up when asked. Otherwise, he could just as well twiddle his thumbs or answer e-mails rather than answering any questions from Congress:

> Mick Mulvaney took his seat before a congressional committee Wednesday for the first time since his controversial appointment to be the nation's top consumer financial watchdog and boldly declared he didn't have to say a word.
>
> "I believe it would be my statutory right to just sit here and twiddle my thumbs while you all ask questions," Mulvaney, acting director of the Consumer Financial Protection Bureau, told the House Financial Services Committee.

Jeb Hensarling found it hilarious, calling protests from his Democratic colleagues "great comic relief":

> The committee's chairman, Rep. Jeb Hensarling (R-Texas), who has been the leading opponent of the bureau, said "it is sheer irony and great comic relief to see the wailing and gnashing of teeth of many of my Democratic colleagues" about their inability to hold Mulvaney accountable.
>
> Hensarling validated Mulvaney's view that Dodd-Frank doesn't require him to answer lawmakers' questions, adding that "you could play Candy Crush for the next few hours and there would be nothing we could do about it."

This attempt to force Congress to reckon with its own bad ideas didn't just start yesterday. Mulvaney threw the first punch last week in correspondence with Sen. Elizabeth Warren (D-MA), who helped

create the agency — and its independence from Congress. The Washington Examiner covered the exchange:

Click here for the full story.

w>Normal 0 false false false EN-US X-NONE X-NONE
MM, DD, YYY

1. Headline- Subheadline

Title

Yada. yada, yada.

Americans for Limited Government
10332 Main Street # 326None
Fairfax Virginia 22030
United States