U.S. cyber spies prepared to send Russia or China “back to the stone age” with hacks and cyber counter-attacks.

Fri, 26 Jun 2015 17:00:00, newstips66, [category: energy-dept-slush-fund, category: google-alphabet, post_tag: key-stories, post_tag: u-s-cyber-spies-prepared-to-send-russia-or-china-back-to-the-stone-age-with-hacks-and-cyber-counter-attacks, category: worldnews]

U.S. cyber spies prepared to send Russia or China “back to the stone age” with hacks and cyber counter-attacks.

When the bad guys decided to attack the United States with cyber warfare, they forgot that it was the U.S. who invented the concept.

Snowden, Greenwald, Assange, Onion project, and others, now say that U.S. cyber war capabilities exceed that of anything seen in even the most apocalyptic dystopian science fiction film. A nuclear bomb can wipe out 90 square miles of a country. A Cyber attack can wipe out 2000 square miles of a country. You can see a nuclear missile coming, and probably shoot it down. You can never see a Mega Cyber Attack coming and there is almost nothing you can do to stop it.

With the push of a button, the nuclear power plants, transit systems, street lights, gas mains, dam water release valves all go Kaplooie. Everything that can go wild and release death and destruction; will. Everything that you want to keep working will stop. From turning off power to every phone to making everything with a speaker emit horrific screaming sounds to melting all the ice cream across their nations. Within a 3 minute time span, all power in Moscow, Peking, Beijing and every other adversary mega-city can be made to disappear, like a scene from “Close Encounters”. Every factory can be shut down in seconds, causing billions of dollars in losses per hour. Huge cross-pacific commodity freighters can be hacked and made to ram each other and sink billions of dollars of oil and trade goods. Every Tesla and Lexus in their country can be hacked and made to swerve into on-coming traffic. This sort of cyber counter attack could be mind boggling and is now very easily launched.

The bad guys used to think they could just blow up pre-placed charges on all of the transatlantic cables and cut off the lines but that plan has gone with the wind. Satellites, drones, USB sticks and millions of pre-staged “internet bots”, already in position, preclude any physical attempts to cut the phone lines.

Why would china, Russia and smaller states like Iran and Korea, toy with such potential devastation? Because of Justin Beiber!

Yes, you heard it right. Beiber, could be the cause of the end of the world as we know it. Why?

Because all of the generals in the bad guy countries are old men who don’t really understand the internet, they think of it as a toy and have no idea who the internet-created Beiber, and his culture, is/are. Their cyber warriors, though, are kids in their 20’s who are not grown up enough to understand the full implications of their actions. To them, when they go to work each day at their government sponsored troll farms, and hacker warehouses, it is no different than going in to get paid to play a video game. They see it as a giant game of “Call of Duty”. The old generals do not know what Justin Beiber is, nor understand how his fan-base thinks, or how the internet even actually works. The young fan-base class cyber hackers do know how to hack and work the web but are not mature enough to visualize consequences. They cannot see that a fun hack on the entire privacy of the OPM in Washington can cause such emotional feelings of rape for U.S. generals that it could get their whole country electronically wiped out in retribution.

As Congress screams at federal lackey’s, in committee sessions, for a total failure to protect the system, while FBI agents even jump up to assist in the condemnations, the reality emerges. The size of the latest Mega Hack reveals numbers that almost defy comprehension. It is like a bad version of: The Matrix or The Terminator movies.

Every major agency, that was supposed to be locked up tight, was as wide open as a fishnet, for years, while over-sea hackers raided, grabbed and sifted through those agencies with impunity. They appear to have gotten quite a large part of “the good stuff”.

Hence all of the madness in the world right now: Everybody now knows everybody’s secrets.

A CIA/In-Q-Tel Company, and major press, have now revealed that they have found the latest humiliation deployed by the hackers. All of the core network login information for the biggest parts of the U.S. Government have been sprayed across the entire internet, and posted on all of the average hackers favorite bulletin boards, so that any bored 20 year old ,can try their hand at finding the secret alien files at NASA, the “who really killed Kennedy” files at the DOJ or all of the Oil Company secrets at the Department of Energy.

Why was it this easy? Theories abound. Many say it was because Cisco, Juniper Networks and Intel thought that spy backdoors would be easier if they just built the back-doors right into their chip-level hardware. For the sake of profit efficiency, they put something in that they couldn’t get out, once the bad guys got the keys to those doors. When the finance people at the Department of Energy were told they needed to pull out billions of dollars of Cisco routers and hardware, they said they would take a look but never actually did it.

Another theory says that some bad guys were moles at Cisco and THEY put their own back-doors in the firmware development at the network companies.

Still another theory says that the Chinese built one of the largest internet spoofing systems. This giant set of computers in Beijing grabbed all of the U.S. federal attempts to login to federal VPN’s and instantaneously created a fake clone of the login page while recording the numbers and characters of the U.S. federal officers attempts. Easy Peasey. They might have tricked the DOJ, CIA and NASA to personally hand them the keys to the kingdom.

Of course, the prevailing theory is federal incompetence and crony supplier contracts with no accountability.

How many millions more hacked files will be discovered tomorrow?

How many more times will it happen?

Will the U.S. launch the big Kahuna back at them?

Stay tuned…

nationaljournal.com/tech/cia-admits-it-improperly-hacking-sen...
More results

How hackers made minced meat of Department of Energy networks ...

A **Department of Energy** network breach earlier this year that allowed hackers to download sensitive personal information for 104,000 people was the ... The **hack** resulted in the exfiltration of more than 104,000 individuals' personally ... **CIA** Cybersecurity Guru Dan Geer Doesn't ...
arstechnica.com/security/2013/12/how-hackers-made-minced-...
More results

Government Hacked: 24,000 Files Stolen in Worst Pentagon .

The website of the U.S. Central Intelligence Agency ... Defense William Lynn said that hackers stole 24,000 sensitive defense **department** files in a single March ... that the next Pearl Harbor would be a debilitating cyber attack aimed at government networks or **energy** grids, ...

IBT ibtimes.com/government-hacked-24000-files-stolen-wors...

W en.wikipedia.org/wiki/RecordedFuture
More results

Recorded Future: Tech company finds stolen government log-ins ..link

A **CIA**-backed technology **company** has found logins and passwords for 47 government agencies strewn across the Web — ... **Recorded Future:** Tech **company** finds stolen government log-**ins** all over Web. ... The **company** says logins and passwords were found connected with the departments of Defense, ...
wptv.com/news/science-tech/recorded-future-tech-co...

Recorded Future: It's like Google Meets Nostradamus ..

... or in a decade?The founders of **Recorded**... Get It ... He wouldn't confirm where the **company** is based or when ... And while the **Recorded Future** ...
boston.com/business/technology/innoeco/2010/02/recor...

Your background checks are now available for free, online, for anybody to see...

... reported **Recorded Future**, ... **Federal** agencies exposing login and password information, technology company **finds** . June 26, 2015 | By Dibya Sarkar.
fiercegovernmentit.com/story/federal-agencies-exposing-login-and...
More results

Recorded Future: Tech company finds stolen government log-ins ...

Recorded Future: Tech company **finds** ... says in a report that login credentials for nearly every **federal** agency ... The company says logins and passwords were ...
wptv.com/news/science-tech/recorded-future-tech-co...
More results

Government cybersecurity even worse! Federal passwords are ...

Federal passwords are loose online. ... a senior analyst at **Recorded Future**] said. Next page: **Find** out more about the government's vulnerable passwords ...
K komando.com/happening-now/314109/government-cybersecu...
More results

Welcome to Recorded Future - Recorded Future

What is **Recorded Future**? **Recorded Future** allows you to explore temporal data about people, ... selected your user name and password through the registration process.
recordedfuture.com/welcome-to-recorded-future-2/
More results

Public records that can appear in your credit report |

Dear AMB, There are only three types of public records that appear in a credit report, all of them related to debts. Bankruptcy is the most obvious.
experian.com/blogs/ask-experian/2011/04/13/public-reco...
More results