C.A.S.E.

CAUCASUS ACADEMY
OF SECURITY EXPERTS

HACKING THE US ELECTIONS

EXIT STRATEGY FOR DEMOCRATS?

LASHA PATARAIA

[This page intentionally left blank]

FROM THE AUTHOR

Before going into details about "Hacking the US Elections", I will give you a short intro about me. I am the founder and director of the Caucasus Academy of Security Experts. Instructor in cyber security and national security courses for the academy as well as for the Ministry of Foreign Affairs of Georgia (Diplomatic Training Center) and Ministry of Justice of Georgia (Training Center of Justice). I wrote the very first book on cyber security in Georgia which included research on Russian cyber security capabilities as well as the cyber war report of 2008. For those who are not yet aware, in 2008 during Russo-Georgian war, Russians used weaponized software and sophisticated cyber attacks against Georgia which was the very first cyber war. It was the first time in history when any form of cyber attack was combined in conventional military operations and kinetic attacks. During that period I was working in Israeli's security company as a contractor of Ministry of Defense of Georgia and I was a team leader and cyber security analyst working on exactly the same case. Of course, Russia did not stop there, after the cyber war they have designed and spread sophisticated malware throughout the Georgian governmental networks. Russian state sponsored cyber intelligence activities were focal points of my work during my career in various security positions. I think this kind of experience gives to my research value of what many would call the Insider's eye. This is an issue of special importance for me as I had the opportunity to watch tangible cyber aspects of Russian-Georgian War of 2008 from inside. I tried to put some of the pieces of my research in a way that could respond to the current hot topic and at the same time make it easy to follow for anyone despite their technical background.

CONTENTS

INTRODUCTION

I've been researching Russian cyber capabilities for almost ten years and for all that time it was underestimated along with the soft power that Russia's intelligence services use around the globe. After November 2016 US Presidential election it got deserved attention, but with completely wrong page. Which lead us to today's hottest topic - "Hacking the US Elections".

Given story is the biggest story ever happened to the cyber space and therefore conversations on this thesis should be evidence based. Considering that Russians could hack the US elections and influence on results in favor of Donald Trump means at least two things: First, it says that with the Cyber attacks you can decide world's balance and second, that Russians have such kind of influence.

This special report is dedicated to answer on following questions: Was that the cyber attack? were the Russian intelligence services behind it? and if not, then what was really happened? Suspicious events during the elections and even after are included in this report and analyzed not only in cyber security aspects, but within a counterintelligence point of view as well.

I things in cyber security and in national security domains will change dramatically and as the 9/11 became a water shield in the field of counter terrorism, events of a recent presidential election will also leave its trace on the US intelligence community and on their way of responding cyber threats as well as confronting informational warfare. It is vital for the US to take it as a wake-up call. United States has almost 600 billion USD of military budget, which is a biggest military budget on earth and adversaries are choosing cyber attacks and informational warfare against as it is cheaper or even free, anonymous and widely available. Therefore attack vectors against US will extend to cyber space and more and more events will occur in future. In the cyber security communities, professionals agree that US is great at offensive cyber security, but lacking cyber defense.

This campaign already made cyber security the hottest domain because of a well known e-mail scandal and as Donald Trump was stressing it from day one. After elections, we have also witnessed unprecedented attention to this topic on confirmation hearings of CIA's current director as well at the hearing of General James Mattis US Secretary of Defense. In February President Trump will sign an executive order on cyber security and this will accelerate things in this domain as never before.

CURRENT SECURITY LANDSCAPE

To understand the nature of ongoing cyber operations and alleged “Russian Hack” we should start with the basics and better understand the role of cyber security in today’s global security environment. For decades our biggest threats were radical groups, terrorists, criminal organizations, intelligence agencies and military regimes. And the weapons that scared every security organization around the globe, were weapons of mass destruction, Chemical, Biological, Radioactive and Nuclear weapons. But there’s been a big shift in the threat landscape; we had nuclear arms race between Russia and the United States for decades. The whole world was threatened by so called “Nuclear Powers” and now we are facing new reality, where these dominant countries went from nuclear to cyber powers. While cyber capabilities are not so visible, traditional weapons are already more or less under control. These modern weapons are hidden and can be used by anybody. So as the technology advanced, new threats have emerged. And now we are facing the 5th dimensional warfare - The Silent War.

Cyber operations are cheap or even free, widely available, less visible or even fully stealthy and have the element of plausible deniability!

Currently, cyber capabilities have a vital role in Intelligence gathering and even conducting the military operations. And the threats from cyber space can create a real, lethal damage in real life. The key players in global security were countries with nuclear power, but from nuclear these countries have gone to more effective, cyber powers. Why more effective? Well nuclear weapons in war history were only used twice. In Hiroshima and Nagasaki, while cyber attacks are happening every day and massive operations can occur anytime and anywhere. Nuclear weapons can not be as invisible as cyber, they need resources that are easy to track and they also need to do test detonations. The global security environment and balance extremely relies on Russian, Chinese and Iranian military and now also cyber capabilities. For decades the above-mentioned countries were named as the Nuclear Powers, but nowadays it’s really hardly that threatening, as it requires huge resources, related to lethal risks for their own nations and it’s also transparent. You can’t have those kind of toys and stay in the shadow. So, it makes no sense to me… But cyber capabilities can be really invisible, have the same lethal results (e.g.: “Stuxnet"), cost little or even nothing.

Here are the key groups in cyber space:

NATION STATE

NON-STATE

HACTIVISTS

RUSSIAN CYBER OFFENSIVE AND DEFENSIVE CAPABILITIES

FANCY BEAR
Аквариум
Аквариум

Tattoo on the right hand represented in famous hacking group's logo says: AQUARIUM (Russian title: АКВАРИУМ) There is an old book about the GRU (Russian Main Intelligence Service) Aquarium by Viktor Suvorov, who was one of the first revealing GRU. In that book Aquarium is a name of GRU headquarters.

The first thing to know on Russian cyber capabilities is that most of them are not that cyber at all. Because "Securitization" scale in the Russian government state sponsored cyber crime involves almost every law enforcement agency and special services. Also, private companies, criminal organizations, NGOs, academia, expert community, activists and individuals are responsible not only in cyber space, but in the extensive propaganda campaigns. And it all started long time ago with these three letters: KGB.

We should understand that Russia has an incredible intelligence collection system which was underestimated many times. But it is growing and sharpening from the times of KGB, which by itself was the strongest intelligence agency by that time.

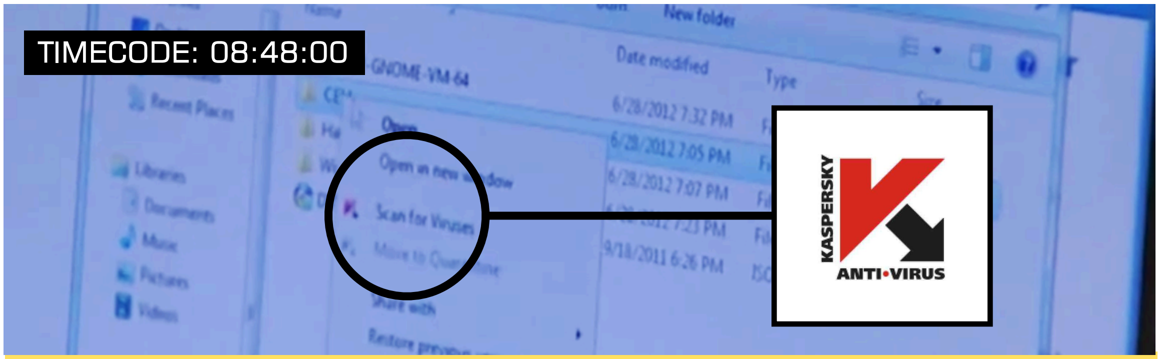
So, what exactly is Russia's defensive and offensive cyber capabilities?

Great examples besides very popular "Cosy Bear" / APT29 and"Fancy Bear" / APT28 could be youth activists "Nashi", one of the worlds biggest Anti-Virus company "Kaspersky, Russian private company RBN - Russian Business Network and many others. There are even IT companies which cover whole CIS countries that are also a tool for Russia's intelligence services for gathering very useful real time raw data. One more example could be the popular ISP in Moscow "Degunino" - Russian internet service provider, which is an ultimate tool for defensive and offensive purposes. It can stand as an alternative and very powerful communication channel with lots of features if something goes wrong, and as an attack tool since by its structure all the customers of this ISP are like individual bots which can be used to launch powerful cyber attacks such as Layer 7 with some new innovative technical manipulations that was never seen in cyber space before. But there are some ready-made software for that purpose in the Russian hacking underground which is the separate topic for research. Again, during the years of my research I have listed hundreds of such organizations, but above-mentioned organizations are the key players and more importantly relevant to ongoing Russian cyber offensive operations. The Unite States must understand philosophy behind the Russian cyber capabilities. There is a different mentality of conducting cyber operations by the Eastern versus Western players.

In the western way of conducting cyber operations these players are government and military affiliated. While in the eastern way we see non-state players, such as the RBN, the Syrian electronic army and Iran. The point is that non-state actors have no proven link to a government entity. The West is using it as a governmental asset, while the East maintains the plausible deniability.

EXAMPLE OF US CYBER DEFENSE

In next chapters of this report we will extend discussion on US cyber defense capabilities with recent cases, but for comparative analysis it is worth mention, that US has a big problem balancing cyber offensive and defensive operations. US has the world's most advanced and finest technology in offensive cyber capabilities, but has a huge gaps in cyber defense. One of the brightest examples is the: 39th IOS - The Information Operations Squadron under the US Air Force. Not so long ago on the DOD's official Youtube channel was published a short documentary named: "The Making of a Cyber Warrior". If you look carefully you can see: despite the key message of the video that US is increasing its cyber capabilities by raising cyber defense and exercising ultimate cyber tools, they use famous Russian anti-virus software which is well known for its ties to FSB and other Russian intelligence services. This says a lot about cyber defense approaches and how US is underestimating Russian cyber capabilities.



Students and staff at the Air Force's Information Operations School at Hurlbert Field, FL explore training for battle on the new front lines of cyberspace. Views are available at https://www.dvidshub.net/video/286915/making-cyber-warrior or DOD's channel on Youtube at: https://www.youtube.com/watch?v=WbmTqzLHBGA

THE HACK

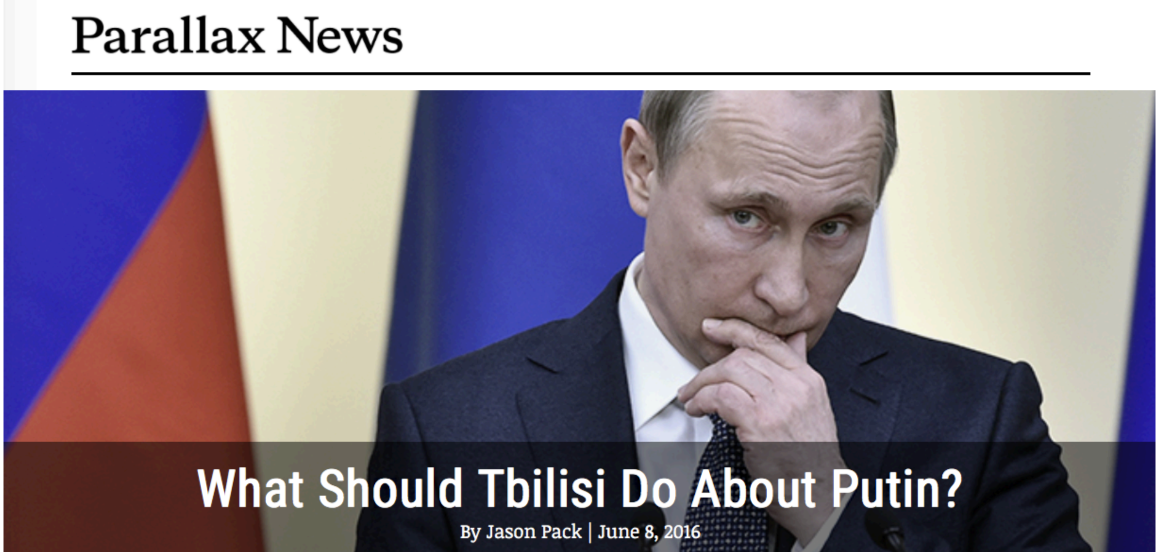
Is this a hacking or is it a classic intelligence operation? Is this a cyber attack or informational propaganda? I would take the latter one, but I think of it as ongoing informational warfare which by itself is part of Cold War. In my recent interview with Jason Pack I came with this unpopular idea that the Cold War never even ended. And I stand on my words. All the indicators if you carefully analyze them, will lead you to the same exact conclusion.

Speaking of a Cold War: I want to share with you a piece of that interview which you can see on Parallax.news

“Those who assume the Cold War ended with the Soviet collapse in 1991 are deluding themselves. Countries that border Russia will continue to remain targets for subversion, invasion, irredentism, and even outright annexation. The Cold War never ended. We are currently fighting the same war that our parents and grandparents fought against the Soviets. All that happened is that the name of our opponent has changed. The period 1991-2003 was merely a brief ceasefire while the Russians regrouped.”

Full version of the interview is available here:

http://parallax.news/what-should-tbilisi-do-about-putin



Parallax News

What Should Tbilisi Do About Putin?

By Jason Pack | June 8, 2016

Cyber attacks are happening every day and the major target for state sponsored cyber crime is the US. And suddenly it became a big story. I guess, the only reason for all of this is that the Democrats needed a solid excuse why they lost the election. That is why I called this report Exit Strategy for Democrats.

All this story is full of unverifiable claims, obsession to delegitimize Donald Trump as a president and intent to mislead. But let’s try to decipher all this “Russian Hack”.

FBI DIRECTOR RECOMMENDS HILLARY CLINTON NOT BE INDICTED IN EMAIL INVESTIGATION

FBI DIRECTOR RECOMMENDS HILLARY CLINTON NOT BE INDICTED IN EMAIL INVESTIGATION

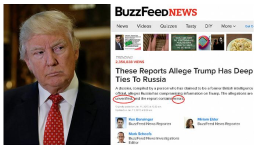
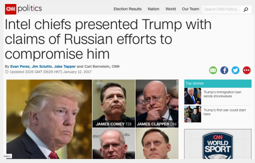
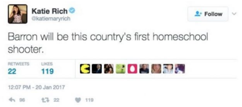
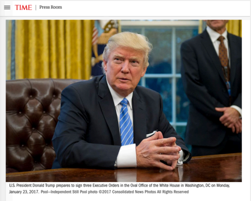
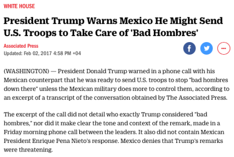
If you look at the chronology of events within this story, it started with Hillary Clinton and John Padesta's email scandal. Then spreading classified records via Wikileaks and involving whole informational warfare at the level that the US has never seen. But all this happened by ignoring all security measures and acting in such a negligent manner that eventually they gave access to tons of classified data. That could happen also deliberately as the Federal Bureau of Investigation officially confirmed that they had warned the DNC before the hack about the threat and official investigation was conducted after the leak. It seems like the US always had a huge gap in cyber security, while Russia is extensively developing its cyber offensive capabilities and cyber security became the #1 topic only after it could serve as the best excuse for the Democrats losing the election and blaming Russia and hackers in order to stay on ground and continue informational warfare. Every country on earth at the moment is developing its cyber capabilities and especially Russia. There are some players in cyber space which are not even on the radar yet and could be more powerful that anyone we ever knew. So it is what they do and what to expect. In today's world being hacked is not really someone else's fault, but mostly yours as we know we are dealing with hackers from all around the globe! That's a nature of cyber crime. You you have clicked the wrong button, you have responded to the wrong email, you have visited the wrong link. That's what it takes for most of the time to get hacked! Even the FBI tells you officially that "you are going to be hacked, have a plan!" FBI cyber division chief Joseph Demarest.

The United States government, former President Obama in particular took it to a completely new level by putting new sanctions against Russia and linking this to alleged cyber attack. But later, in his last press-conference, he confirmed that Russia sanctions were in response to invasion of Ukraine. If we are talking about what Russia wants in this game, it is obvious that they want to divide the United States, weaken its security, use the moment to increase their influence around the globe and assure Russian people with such overrated conspiracies that Russia's intelligence services are back to the level of KGB and they are as strong as half a century ago.

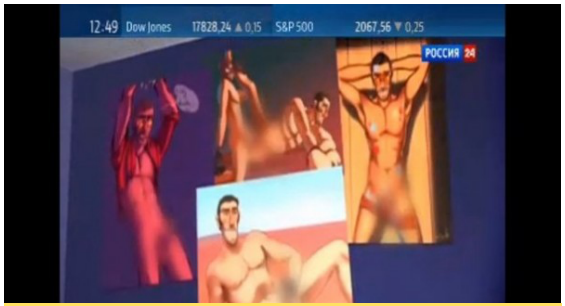
CYBER ATTACK OR PROPAGANDA?

From day one the mainstream media was conducting the biggest informational warfare, heavy propaganda against President Trump in favor of Hillary Clinton. After they lost it was obvious that they did not had plan B for Trump and all this propaganda that they conducted after only gave gave an upper hand to the Russian government. We saw fake news from the biggest broadcasters, campaigns from big sharks in social media, leaks from government's most secure agencies and role plays from top government officials.
This is an unprecedented campaign not only from foreign, but also by the domestic groups in the US. The mainstream media is deliberately engaged in false reporting, social attacks even on President Trump's family members. Propaganda campaign become so nasty that it even attacks the sovereignty of the US. Every aspect of this informational warfare indicates that it is very well organized and managed. All this can lead to very serious, devastating consequences as the radical wing is also talking about military coup.
Some of the unverified and fake news that took place in informational campaign against President Trump:

CHRONOLOGY OF THE MAJOR FAKE NEWS & CAMPAIGNS

 BuzzFeed NEWS News Videos Quizzes Tasty DIY More TRENDING 2,356,838 VIEWS These Reports Allege Trump Has Deep Ties To Russia A dossier, compiled by a person who has claimed to be a former British intelligence official, alleges Russia has compromising information on Trump. The allegations are unverified, and the report contains errors. Originally posted on Jan. 11, 2017, at 12:20 a.m. Updated on Jan. 11, 2017, at 2:09 a.m. Ken Bensinger BuzzFeed News Reporter Miriam Elder BuzzFeed News Reporter Mark Schoofs BuzzFeed News Investigations Editor	**These Reports Allege Trump Has Deep Ties To Russia**	Buzzfeed www.buzzfeed.com	Jan. 11, 2017
 CNN politics Election Results Nation World Our Team Intel chiefs presented Trump with claims of Russian efforts to compromise him By Evan Perez, Jim Sciutto, Jake Tapper and Carl Bernstein, CNN Updated 2226 GMT (0626 HKT) January 12, 2017 JAMES COMEY FBI JAMES CLAPPER DNI Top stories Trump's immigration ban sends shockwaves Trump's first war could start here CNN WORLD SPORT	**Intel chiefs presented Trump with claims of Russian efforts to compromise him**	CNN Evan Perez, Jim Sciutto, Jake Tapper and Carl Bernstein	Jan. 12, 2017
 Katie Rich @katiemaryrich Follow Barron will be this country's first homeschool shooter. RETWEETS 22 LIKES 119 12:07 PM - 20 Jan 2017 96 22 119	**SNL Writer's Tweet Saying Barron Trump Will be America's 'First Homeschool Shooter'**	SNL Katie Rich	Jan. 20, 2017
 TIME | Press Room U.S. President Donald Trump prepares to sign three Executive Orders in the Oval Office of the White House in Washington, DC on Monday, January 23, 2017. Pool—Independent Still Pool photo ©2017 Consolidated News Photos All Rights Reserved	**Martin Luther King Jr. bust had been removed from the Oval Office after President Donald Trump moved in.**	TIME magazine Zeke Miller White House pool reporter	Jan. 20, 2017
 WHITE HOUSE President Trump Warns Mexico He Might Send U.S. Troops to Take Care of 'Bad Hombres' Associated Press Updated: Feb 02, 2017 4:58 PM +04 (WASHINGTON) — President Donald Trump warned in a phone call with his Mexican counterpart that he was ready to send U.S. troops to stop "bad hombres down there" unless the Mexican military does more to control them, according to an excerpt of a transcript of the conversation obtained by The Associated Press. The excerpt of the call did not detail who exactly Trump considered "bad hombres," nor did it make clear the tone and context of the remark, made in a Friday morning phone call between the leaders. It also did not contain Mexican President Enrique Pena Nieto's response. Mexico denies that Trump's remarks were threatening.	**President Trump Warns Mexico He Might Send U.S. Troops to Take Care of 'Bad Hombres'**	Associated Press	Feb. 2, 2017

All these efforts reminded me the Kremlin style propaganda campaigns.



Russian fake version represented in “Rossya 1” TV

Original footage used in fake version

Like the Russian state television channel “Russia 1” falsified the video to claim that the young American boy had the pictures of naked men in his bedroom. The US company responsible for the advert: Fathead - which it would not tolerate the manipulation of its material for a "hateful, bigoted, and outrageous attack on the gay community as well as children”.

Journalists should try to be neutral in their observations, but unfortunately in this game too much powerful groups are involved dictating extreme rules. We see celebrities, Hollywood actors and activists groups involved in extensive campaign against democratically elected president and therefore against sovereignty of their own country.

TROLLING TO SHAPE PUBLIC OPINION

In this world when feeling safe is more important than being protected: authors of this entire propaganda campaign used two very special ingredients to give an extra sweet flavor to given dish by including classic Russian threat factor and the Mysterious Cyber Intrusion Theory. We see an unprecedented trolling activities which aim to shape public opinion, millions of fake news which attack social media users, propaganda from some of the biggest mainstream media actors and most importantly we see the trend. Trend inspired by all of the above mentioned activities, accelerated with involving social influencers and raised to confrontational level. There is a great research and theory which applies very well to this phenomenon called “The Structure and Dynamics of Organizations and Groups” by Eric Berne. If we are talking about sophisticated cyber conspiracies than this conversation also can have a window for discussion of ultimate psychological practices that are undivided part of such campaigns and are exercised by almost every intelligence agency on earth. From the counterintelligence perspective which combines all the attack vectors, methods and tools in analysis: there are same patterns in ongoing campaigns as it is in many Russian cases, but this time the Russian Federation could be the least problem for the US. Russia just needs a moment to take a breath after the Ukraine, while the US is left with radical wing fighting for power and revenge. Russia will have more time and space to work in his neighborhood by pushing his agenda to rebuild the USSR and extending its influence in CIS countries.

RECENT CASES OF MAJOR CYBER ATTACKS ON THE US GOVERNMENT

Year	Target
2009	US Electrical Grid
2009	Pentagon’s Joint Strike Fighter Project
2012	NASA
2013	Department of Energy
2013	Federal Election Commission
2014	US Postal Service
2014	National Oceanic And Atmospheric Administration
2014	White House
2014	State Department
2015	Department of Defense
2015	Internal Revenue Service
2015	Office of Personnel Management
2016	Federal Bureau of Investigation

I want to bring your attention to OPM case: Office of Personnel Management of the USA was breached resulting in leaking millions (Approx. 23 mln. files) of personal data starting from the 1990’s to present time. Including background check information and personal details for the US military and law enforcement personnel, that opens up tons of other vulnerabilities. The attack suspected but not proven to be by the Chinese. In terms of cyber security it is a classic hacking and yet probably the biggest leaks in the history of the United States. Even after two years the United States government did not provide any evidences to the public. In the cyber security field, especially when we are talking about the state sponsored cyber crime, it is very hard to attribute attack to somebody and prove, but this case shows that US is lacking the cyber defense, while its cyber offensive capabilities remain as the finest in the world.

To extend current cyber story this is the chronology of events that took place during the elections:

Date	Cyber Events
Jun. 14, 2016	DNC Hacked
Jun. 15, 2016	Guccifer 2.0 sent hacked data to Wikileaks
Jun. 22, 2016	Wikileaks published around 20,000 emails linked to DNC
Jul. 1, 2016	DC Leaks also published same kind of emails
Aug. 29, 2016	DCCC (Democratic Congressional Campaign Committee) gets hacked
Oct. 7, 2016	Wikileaks published other 50,000 emails of John Padesta
Nov. 4, 2016	According to Guccifer 2.0 he hacked the Federal Election Commission

The state sponsored cyber espionage is one of the biggest problems in the field. Hacking itself is the most useful tool in the hands of criminals, intelligence agencies, corporate espionage and even for the politicians and media. They are successfully using this tool to gather information, fabricate facts and gain an impact within certain informational campaigns. It is a tool that can give a great advantage both in government or corporate sector. As I mentioned already cyber tools are available, cheap or even free, most of them are anonymous and very effective. If in the past intelligence agencies needed to use human intelligence resources, agents, money and a lot of time, nowadays it is very easy.

The most commonly used software in cyber espionage is a so called RAT (Remote Access Trojan). This is far newer version actual Trojan Horse story which is known from the ancient Greek mythology, but the principle is actually the same. For instance we had in my country (Georgia) classic cyber intelligence case involving RAT. “GEORBOT" which penetrated most of the government networks and was stealing information with pre-defined keywords related to the Russian government or national security. Very sophisticated malware which lead us to rethink our cyber defense as a nation state.

The key player in this domain is Russia with its ambitions to rebuild the USSR and aggressive foreign policy. Key step in exposing Russian cyber intelligence activities in CIS countries was catching the Cyber intelligence as the intelligence itself will remain daily routine for every intelligence agency around the globe, because it is what they exist for. Every intelligence agency is made to gather an intelligence, would it be a classic human intelligence, signals intelligence or cyber intelligence we should not be surprised that these actions are conducted, but rather think about the defense in the new domain, which we are still discovering.

There are many vectors of cyber attacks but at the same time not every of them necessarily has to be cyber. You can have the best security software and hardware that money can buy, but the human factor will always be the weakest link and it can crash down your organization despite all technical measures. Hackers, corporate espionage and intelligence agencies mostly target insiders when they want to get the data. There are lots of techniques exploiting human factor in organizations: human ego, ideology, finances and compromising them. There is already science called social engineering to exploit human vulnerabilities and manipulate them. It uses basic human factors, such as fear, trust, will of help and curiosity. Social engineering is a discipline of human deception transforming outsiders to insiders. But even without social engineering, data can be breached by insiders themselves based on human ego, fatigue or insomnia, subjective mental workload, psychological factors, tolerance, cultural factors, mood, influence, drugs, hormones and so on.

So, when we are assessing events of such an extend we should consider not only cyber security, but informational security, operational security and even counterintelligence aspects when it comes to a nation states.

WHAT SHOULD THE US DO TO DETER CYBER THREATS

During the recent events cyber defense became the highest consideration for the United States and it become obvious that the US is lacking it. During his confirmation speech current CIA director Mike Pompeo officialy stated that US government does not has a policy of cyber defense. So, the first step would be to design an adequate policy which will be based on sophisticated risk assessments and research of critical infrastructure and cyber capabilities of its adversaries. This seems to be starting soon as Donald Trump is going to sign an executive order on cyber security within February. But we should understand that giving importance to cyber security is not enough as it has to be effectively placed in the grid of national security as it is an interdisciplinary domain and should be linked to counterintelligence. Other recommendations would be stressing the importance of cyber security and raising the cyber awareness not only in governmental, but also in private sector as well, because nowadays big part of critical infrastructure are run by the private companies; Cyber security needs to be addressed in academia as well, because even current job market in US lacks more then one million specialist and job openings are not fulfilled. More researches on cyber security from local and international sources; Establishing new ways of public private partnership in cyber security on the international level; Re-assessing cyber security capabilities, threats and vulnerabilities of the critical infrastructure; Putting more on cyber defensive capabilities and combining cyber security with classic counter-intelligence operations rather then taking it as separate domain.

CONCLUSION

No proof that it was a "Hack" nor that it was "RIS" (Russia's Intelligence Services)

Hacking the US elections to interfere elections in favor of specific candidate is the loudest title ever existed in media about cyber space. such controversial statement needs a hard data for evidence, especially when former VP of the United States Joe Biden has offered response to Russia's cyber attacks during his vice presidency. Despite of such importance of world's one of the most popular topic, we only have two official sources about it. First is a Grizzly Steppe Report on Russian Malicious Cyber Activity By the US-CERT which is not directly targeted to the current campaign of alleged Russian Hack, but it is a part of the story as it was published right after the Donald Trump won. And the second is a DNI report: Assessing Russian Activities and Intentions in Recent US Elections which is a declassified version of the Office of the Director of National Intelligence and was extensively reflected in mainstream media as the final and official proof of hacking that allegedly took place. In its Key Judgements section of the report following was stated:

"DHS assesses that the types of systems Russian actors targeted or compromised were not involved in vote tallying."

Well, in a world of cyber space it is extremely hard and sometimes even impossible to attribute cyber attack to someone as it is very complicated and complex domain. Hackers, especially the ones that are conducting state sponsored cyber crime are even better in hiding their tracks, than designing high caliber weaponized software.
Report was more about the informational campaigns even though it was dedicated to explain alleged cyber activities.

"Russia's state-run propaganda machine contributed to the influence campaign by serving as a platform for Kremlin messaging to Russian and international audiences."

Was this a hacking?
All this campaign in general was more informational propaganda campaigns than cyber attacks and that is why I would say it was not a hacking. But of course during that period specific cyber events took place which could defined as a small tools such as more of a social engineering level.

What Russia behind these events?

Sure, it was a part of all this theatre, but not the only one. These events were multifaceted and involved various groups of interests. Russia as well as every country's intelligence services whether or not they are adversaries will be interested gaining intelligence and even conducting some actions, because that is what they are made for. People of intelligence community are very well aware of this as well as the politicians, but confusion that it has created in society is not innocuous and has all signs of being orchestrated.

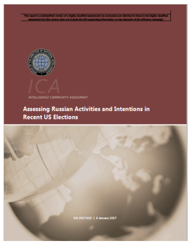
We should also understand that intelligence agencies can maintain data classified and therefore there can be more evidences for this thesis that are not publicly available, but given political statements, media reflections, high interest of people and nations around the world and the fact that this theory is used by various groups in attempts to delegitimize Donald Trump as a president, should be answered appropriately.

To be continued…

Lot of things are going on right now around this topic. Should it be investigations in the US, or rumors that FSB (Federal Security Service of Russia) top officials are arrested, charged with treason, the new initiatives in cyber security and so forth. Cyber security is not a growing domain anymore, it is adequately estimated already by the military and intelligence services. Every war, terrorist activities and propaganda campaigns involves the element of cyber security because the whole world is computerized. We see that governments, businesses, banking and society in general are completely depended on technology. Nowadays it is impossible to handle so much data and routine without sophisticated IT infrastructure. Individuals can't reject such comfort in communication, education and everyday life. That means that the whole world depends on technology. After so much dependence look at the critical processes here. E-government is developing on daily basis offering to citizens new services in digital space, Law enforcement and military entities are aggressively developing new technologies, Businesses are getting new software, new services, ERP, CRM, cloud solutions to enhance their productivity, cut down expenses and raise the profit. In the future things will only get more sophisticated would it be an issue of national security or privacy. So, stay tuned and enjoy the technological progress.

Lasha Pataraia

SOURCES



This report is a declassified version of a highly classified assessment; its conclusions are identical to those in the highly classified assessment but this version does not include the full supporting information on key elements of the influence campaign.

ICA

INTELLIGENCE COMMUNITY ASSESSMENT

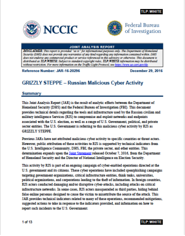
Assessing Russian Activities and Intentions in Recent US Elections

ICA 2017-01D | 6 January 2017

DNI REPORT (UNCLASSIFIED)

ASSESSING RUSSIAN ACTIVITIES AND INTENTIONS IN RECENT US ELECTIONS

Document can be downloaded from this url:
https://www.dni.gov/files/documents/ICA_2017_01.pdf



TLP:WHITE

NCCIC Federal Bureau of Investigation

JOINT ANALYSIS REPORT

DISCLAIMER: This report is provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. DHS does not endorse any commercial product or service referenced in this advisory or otherwise. This document is distributed as TLP:WHITE: Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction. For more information on the Traffic Light Protocol, see https://www.us-cert.gov/tlp.

Reference Number: JAR-16-20296 December 29, 2016

GRIZZLY STEPPE – Russian Malicious Cyber Activity

Summary

This Joint Analysis Report (JAR) is the result of analytic efforts between the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI). This document provides technical details regarding the tools and infrastructure used by the Russian civilian and military intelligence Services (RIS) to compromise and exploit networks and endpoints associated with the U.S. election, as well as a range of U.S. Government, political, and private sector entities. The U.S. Government is referring to this malicious cyber activity by RIS as GRIZZLY STEPPE.

Previous JARs have not attributed malicious cyber activity to specific countries or threat actors. However, public attribution of these activities to RIS is supported by technical indicators from the U.S. Intelligence Community, DHS, FBI, the private sector, and other entities. This determination expands upon the Joint Statement released October 7, 2016, from the Department of Homeland Security and the Director of National Intelligence on Election Security.

This activity by RIS is part of an ongoing campaign of cyber-enabled operations directed at the U.S. government and its citizens. These cyber operations have included spearphishing campaigns targeting government organizations, critical infrastructure entities, think tanks, universities, political organizations, and corporations leading to the theft of information. In foreign countries, RIS actors conducted damaging and/or disruptive cyber-attacks, including attacks on critical infrastructure networks. In some cases, RIS actors masqueraded as third parties, hiding behind false online personas designed to cause the victim to misattribute the source of the attack. This JAR provides technical indicators related to many of these operations, recommended mitigations, suggested actions to take in response to the indicators provided, and information on how to report such incidents to the U.S. Government.

1 of 13 TLP:WHITE

GRIZZLY STEPPE
RUSSIAN MALICIOUS CYBER ACTIVITY

DOCUMENT CAN BE DOWNLOADED FROM THIS URL:
https://www.us-cert.gov/security-publications/GRIZZLY-STEPPE-Russian-Malicious-Cyber-Activity

ABOUT CASE

CAUCASUS ACADEMY OF SECURITY EXPERTS
Advancing Security as a Profession!

With seven years of experience teaching law enforcement, military, corporations, diplomats and students the Caucasus Academy of Security Experts is a leading security academy in the Caucasus region. CASE is awarded by the Ministry of Justice and ICT Business Council as the Best Provider of IT Education. Along with the cyber security courses CASE was the first organization in Caucasus which designed and conducted intelligence, counterintelligence, anti-terrorism and lie-detection courses for civilians.

Caucasus Academy of Security Experts has unique and rich experience of conducting sophisticated corporate trainings including topics that never been so available before. In the whole Caucasus region we were first to launch forklift safety exploitation training, upgraded first aid training on highest level, introduced latest risk assessment training and designed hundreds of topics within occupational health and safety direction. Starting from OHS ending with cyber and physical security trainings we cover all the topics that security services, corporations and individuals are facing today. Our approach is holistic and trainings also come with expertise and advisory services. Our experience is fulfilled with thousands of hours of training biggest corporations and hundreds of students. Our team includes top notch internationally certified experts with many years of proven experience.

Besides the international networking with educational and technological institutions in our portfolio we partner with leading international corporations who trust their security to CASE. We have conducted a number of corporate training events starting from information security, to labor safety, to first aid and so on. Such trust for our academy is a strong sign of its reputation which we value most of all. It is also worth mentioning that the Caucasus Academy of Security Experts attaches a huge importance to the youth involvement in security studies. Our awareness programs include topics to motivate them for building career in various security related fields. That is why we have a successful cooperation with students' associations and universities, in the frames of which we deliver free lectures, trainings and literature.

Our analytical team conducts extensive analysis and delivers top-notch expertise that serve for better security and innovative product development in that area. All trainings are unique as they are designed by CASE and tailored according to specific needs. We have a strong, reliable and successful relationship with security, education and technology related organizations worldwide what gives us even more advantage for the best performance in our activities. In addition to training solutions, CASE delivers an adequate risk assessment and advisory services to fulfill the customers demands. CASE has an international network uniting students, alumni, members and partner organizations that gives us a very powerful position for research and analysis in different fields of security. For more information visit us http://www.globalcase.org

[This page intentionally left blank]