On December 14, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Fortinet, Mozilla, VMware, Citrix, Adobe, Google, Apple, and Microsoft products.
CIS Security Advisories

Threat Level's explained

- **GREEN or LOW** indicates a low risk.
- **BLUE or GUARDED** indicates a general risk of increased hacking, virus, or other malicious activity.
- **YELLOW or ELEVATED** indicates a significant risk due to increased hacking, virus, or other malicious activity that compromises systems or diminishes service.
- **ORANGE or HIGH** indicates a high risk of increased hacking, virus, or other malicious cyber activity that targets or compromises core infrastructure, causes multiple service outages, causes multiple system compromises, or compromises critical infrastructure.
- **RED or SEVERE** indicates a severe risk of hacking, virus, or other malicious activity resulting in widespread outages and/or significantly destructive compromises to systems with no known remedy or debilitates one or more critical infrastructure sectors.

WEEKLY IT SECURITY BULLETIN
16 December 2022

In The News This Week

The FBI's Cybersecurity Program for Critical Infrastructure Was Hacked

A database with contact information for elite cybersecurity professionals is now being sold on the dark web to the highest bidder - A hacker has breached an FBI program dedicated to critical infrastructure cybersecurity and is now selling access to its data on the dark web. Security blogger Brian Krebs reports that InfraGard, an information-sharing program maintained by the bureau, was compromised earlier this month by a cybercriminal who goes by the moniker "USDoD." After swiping an internal database that contained contact information for "tens of thousands" of InfraGard members, the hacker proceeded to post its contents for sale on the dark web marketplace "Breached," where anybody can now buy the info for $50,000. The hacker told Krebs that the high price set for the data was a negotiating tactic: "I don't think someone will pay that price, but I have to [price it] a bit higher to [negotiate] the price that I want," they said. Read the rest of the article by Lucas Ropek here: Gizmodo

Uber Hacked Again? – Data from Uber and Uber Eats Published on Hacking Forums

Uber has been the subject of a new cyberattack. Early on Saturday morning, a threat actor going by the name of "UberLeaks" began publishing information on a hacking forum known for revealing data breaches. Employee email addresses, company reports, and data on IT assets that were stolen from a third-party vendor are all included in the attack. Numerous archives that claim to be source code for mobile device management platforms (MDM) used by Uber, Uber Eats, and other third-party vendor services are among the disclosed data. The 'UberLeak' hacker created four different topics on the hacker forum, for each MDM platform deployment it had breached... Read the full story by Guru here: Cyber Security News

Albanian Government Workers Facing Seven Years in Prison for Not Updating Software

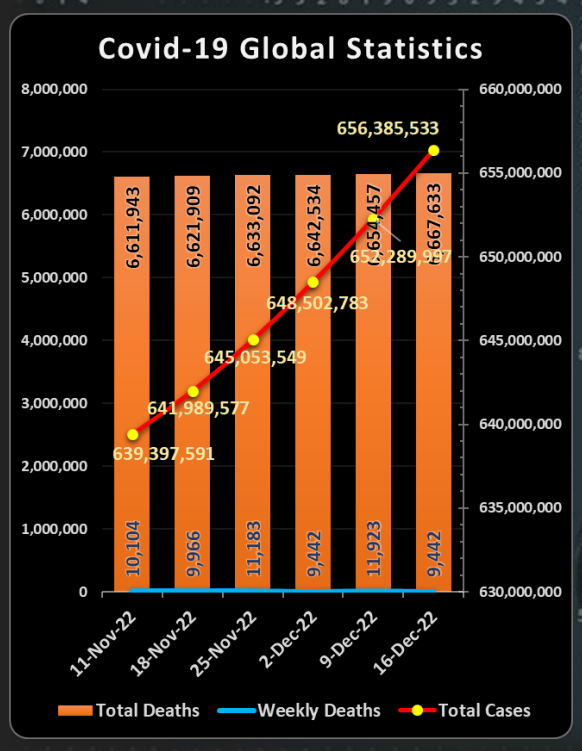
It's not unheard of for government officials to lose their jobs following high-profile breaches. But it's something else entirely for employees who did not deliberately help intruders breach their employers' computer systems to be charged with any kind of crime purely because of security negligence. That's exactly what happened in late November, when Albanian prosecutors requested that five government IT officials in the public administration department be placed under house arrest for failing to update the antivirus software on government computers. The Albanian IT officials are reportedly accused of "abuse of post," which can carry penalties of up to seven years in prison, according to the Associated Press. It raises an important question: Does prison time for mistakes incentivize good security practices, or just disincentivize anyone from entering the field in the first place. In July, Albania was hit by a cyberattack that took down many of the government's websites and online services. The country's National Agency for Information Society, known as AKSHI, announced it had been forced to shut down several government computer systems until the attacks could be "neutralized." The U.S. government, Microsoft, and NATO all supported Albania's efforts to investigate and remediate the attack in the following months...
Read the article by Josephine Wolff here: Slate

Cyber-espionage group Cloud Atlas targets Russia and its supporters

The cyber-espionage group Cloud Atlas has ramped up activities targeting Russia, Belarus and disputed parts of Ukraine and Moldova since Russia's invasion this year, according to a new report. The group has been active since 2014, according to research published by Check Point last week, but since the outbreak of the war in Ukraine it has mainly attacked "high profile victims" in Russia, Belarus, Transnistria (a pro-Kremlin breakaway region of Moldova), and Russian-annexed territories of Ukraine, including Crimea, Luhansk, and Donetsk. The goals of the group are espionage and theft of confidential information, according to researchers from Positive Technologies. It is not yet clear who is behind the group. Cloud Atlas has stuck with its "simple but effective" methods, which haven't changed over time, according to Check Point. The group uses so-called template injection attacks that abuse features in Microsoft Word to deliver malicious payloads to victims. The documents are usually crafted for a particular target, which makes them almost undetectable...
Read the full story by Daryna Antoniuk here: The Record

Hacking Humans - Disinformation and verification (Podcast – 15 Mins)

Kaspars Ruklis, the Program Manager for Media Literacy from IREX sits down with Dave to talk about the very verified media literacy program. Dave and Joe share some listener followup on some of the business' common language, this week, listener Vicki asks about the term "EULA" and what it stands for. Joe's story follows a scam that is particularly alarming around the holiday's, about fake barcodes on gift cards. Dave's story is all about scammers who are getting scammed. The story follows cybercriminals who are using hacking forums to buy software exploits and stolen login details and how they keep falling for cons and are getting ripped off thousands of dollars.
Listen to Dave and Joe's podcast here: The Cyberwire



For Reporting Cyber Crime in the USA go to (IC3) , in SA go to Cybercrime, in the UK go to ActionFraud

Cyber Operations in Ukraine: Russia's Unmet Expectations

As most of us observed the conflict in Ukraine from afar and waited for the "big world-threatening " cyber war to unfold, after ten months, we realized that this is probably not going to pan out as badly as expected. This week, Gavin Wilde published a paper on the Carnegie Endowment for International Peace website that gives us some insight into why the so-called Russian Cyber War machine hardly made it to the front lines. An extract of the paper follows below.

Cyber Operations in Ukraine: Russia's Unmet Expectations - Gavin Wilde
Russia has achieved far less via cyber warfare in Ukraine than many Western observers expected. Many aspects of Moscow's approach to cyber operations have been misunderstood and overlooked.

SUMMARY
A review of academic, doctrinal, and journalistic writing covering the last three decades of Russian military theorizing on cyber-related issues yields three hypotheses that may explain the mismatch between the expectations of many Western observers and the reported impact of Russian cyber operations in the 2022 invasion of Ukraine. By exploring the unique and oft-overlooked facets of Moscow's conceptualization of "cyber," this paper provides a foundation for better assessing Russia's performance in cyberspace in Ukraine in early 2022, along with a more nuanced understanding of its capabilities and possible expectations going forward. These hypotheses are as follows:

- Russia's Information Operations Troops—a rough analog to Western military cyber commands—remains in its infancy and appears optimized more for counterpropaganda than for offensive cyber operations. The operational command structure over offensive cyber operations, meanwhile, remains murky and is possibly more political than military in nature.
- Russia's premier offensive cyber capacities are housed within agencies focused on intelligence and subversion—the key tool kits used against Ukraine since 2014—rather than combined-arms warfare.
- Moscow's secretive and poorly executed February 2022 invasion precluded optimal performance in the initial period of the war, which is particularly pivotal in Russian thinking about effectiveness in the information domain.

These are each examined through Russia's own information warfare prism, which differs in crucial ways from Western conceptions of "cyber"—foremost in that it is more expansive, encompassing and emphasizing the psychosocial impacts of information and communication technologies on both the polity and the public.

INTRODUCTION: SEEING THROUGH MOSCOW'S OWN LENS
To better understand the cyber aspects of Russia's early 2022 military incursion into Ukraine, analysts should account for the unique way in which Moscow views cyber operations and doctrinally conceptualizes success or failure in the cyber domain.

First, the very concept of "cyber" widely used in the United States and West—which largely emphasizes the technical integrity of networks—is rarely if ever used in the official Russian strategic and military lexicon. Instead, Moscow refers to "information confrontation" or "information war/warfare" to describe the range of operations—both technical and psychological, code and content—that can be deployed against adversarial systems and decision making. Drawing on Soviet fears of ideological encroachment, as well as the humiliation and siege mentality cultivated since the Soviet collapse, the preponderance of Russia's emphasis falls on what the U.S. military terms the cognitive dimension, within what U.S. officials would call information operations. Under this construct, offensive cyber operations are a subset of broader operations in the information environment designed to achieve as much a psychological impact as a technological one.

Ultimately, Russian doctrine does not make the same distinction as the West between cyber and information operations. Rather, Russia's concept entangles the physical and psychological features of interstate conflict—now heavily mediated by technology—throughout the entirety of the information space. For example, a 2011 document released by the Russian defense ministry defined information war as:

"conflict between two or more states in information space with the goal of inflicting damage to information systems, processes, and resources, as well as to critically important structures and other structures; undermining political, economic, and social systems; carrying out mass psychological campaigns against the population of a State in order to destabilize society and the government; as well as forcing a State to make decisions in the interests of their opponents."

This definition is far more expansive than what U.S. analysts call "cyber warfare." It also helps explain the self-reinforcing conspiratorialism and post-truth tendencies of Russian operations. As one Russian academic put it:

"The specific feature of "information warfare" is the implicitness of its actors. Who is the organizer of these actions? Against whom are they really directed? This ambiguity, regardless of the actors, serves to both mythologize and demonize "information warfare." One can trace, at will, a motivational chain, a "cunning plan" behind any news story or event attributable to "enemies." This, of course, does not rule out the development or execution of such plans and projects by various political and social forces—both foreign and domestic...However, the actors in "information wars" have largely become the product of interpretations and discursive practices, which, in turn, are then also regarded as "information warfare."

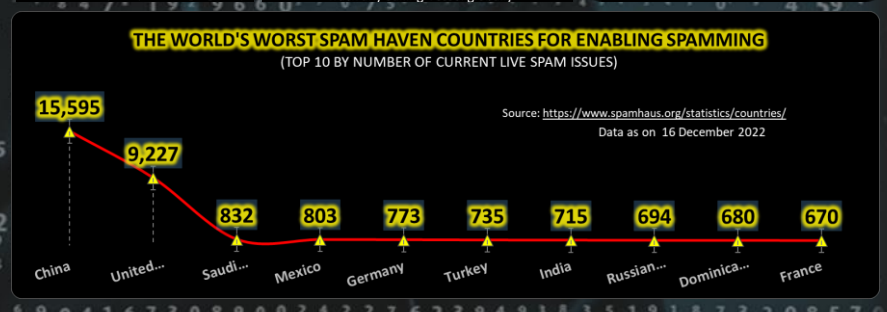
This conception also blurs the lines between foreign and domestic threats, drawing on Leninist themes of perpetual political struggle and concern over penetration by fifth columnists. The cyber-enabled tools of online surveillance and censorship within Russia's borders—and efforts to isolate Russia from the global internet—are mutually reinforcing with those deployed beyond them. Moscow's foreign policy battles are often indistinguishable from its struggle for domestic regime stability. In this regard, much of what the West views as aggression in the information space would be couched by Moscow in counteroffensive terms—chaff to drown out or distort signals from abroad that run counter to the Kremlin's preferred narratives before they can penetrate and take root within Russian society....

That is all I have space for in this post but please read Gavin's full paper on the subject here: Carnegie Endowment for International Peace

Other Interesting News and Cyber Security bits:

- Breakthrough in nuclear fusion energy announced
- Elon Musk's Twitter purchase has become a big problem for Tesla
- How The Anonymous Hacker Group Wages Cyber Warfare
- SANS Daily Network Security Podcast (Storm cast)

flightradar24 LIVE AIR TRAFFIC Track any Aeroplane in flight globally
Marine Traffic Track any Sailing Vessel globally
SatelliteXplorer Track satellites in orbit



AUTHOR: CHRIS BESTER (CISA,CISM)
chris.bester@yahoo.com