OVERWATCH

"The advancement and diffusion of knowledge is the only guardian of true liberty."
-James Madison

THE JOURNAL OF THE MARINE CORPS INTELLIGENCE OVERSIGHT DIVISION

Volume 10 Issue 2 Spring 2021

A projection of cyber code on a hooded man is pictured in this illustration picture taken on May 13, 2017. REUTERS/Kacper Pempel/Illustration

IN THIS ISSUE, FEATURED ARTICLE: RANSOM GROUP LINKED TO COLONIAL PIPELINE HACK IS NEW BUT EXPERIENCED

Inspector General of the Marine Corps

The Inspector General of the Marine Corps (IGMC) will promote Marine Corps combat readiness, institutional integrity, effectiveness, discipline, and credibility through impartial and independent inspections, assessments, inquiries, investigations, teaching, and training.

The Intelligence Oversight Division

To ensure the effective implementation of Marine Corps-wide oversight of Intelligence, Counterintelligence, Sensitive activities (to include USMC support to law enforcement agencies, special operations, and security matters), and Special Access Programs. To establish policy and ensure their legality, propriety and regulatory compliance with appropriate Department of Defense/ Department of the Navy guidance.

Contact Information

Mail:

Director, Intelligence Oversight
Inspector General of the Marine Corps
Headquarters U.S. Marine Corps
701 South Courthouse Road
Building 12, Suite 1J165
Arlington, VA 22204

Intelligence Oversight Division Staff

GS15 Edwin T. Vogt, Director
LtCol David Lasseter, Deputy Director
VACANT-Sensitive Activities Officer

Inside This Issue

Web Links

Senior Intelligence Oversight Official (SIOO)
https://dodsioo.defense.gov/

Marine Corps Inspector General
https://www.hqmc.marines.mil/igmc//

Naval Inspector General
https://www.secnav.navy.mil/ig

A Message from the Director

Greetings from the Office of the Inspector General for the Marine Corps, Oversight Division. This edition of *Overwatch* is the second of calendar year 2021. As always, the articles provided in this issue do not represent the opinion of Intelligence Oversight Division or the Inspector General's Office. **Please be aware of the release of MARADMIN 134/21, Annual Operations Security Training Requirements, which outlines annual requirements for OPSEC training. This training applies to all active and reserve Marines, Government Civilians and contractors, and other assigned or supporting personnel. https://www.marines.mil/News/Messages/Messages-Display/Article/2531451/annual-operations-security-training-requirements/.**

Also, on April 19, 2021 the Department of Defense issued an update to Directive-type Memorandum (DTM) 13-008 incorporating Change 5. This administrative change updates the title of the Under Secretary of Defense for Intelligence to the Under Secretary of Defense for Intelligence and Security in accordance with Public Law 116-92. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dtm/DTM-13-008.pdf?ver=VxROPIbAMgpYCv8NnHDHBg%3d%3d

The first article was written by Raphael Satter of Reuters. The article discusses Darkside a relatively new player in the "hacking for ransom" community while also highlighting the very public ramifications of this attack.

The second article by Maggie Miller discusses U.S. intelligence community leaders pushing for measures to encourage the private sector to report breaches and to deter malicious hackers from attacking critical infrastructure.

Next, on April 2, 2021 the Privacy and Civil Liberties Board released a public report on its initial oversight review of Executive Order 12333.

The last article, by Dina Temple-Ralston, discusses how Russian Federation intelligence services used the guise of a routine software update to conduct one of the most devastating cyberattacks in American history.

Semper Fidelis,

Edwin T. Vogt
Director, Intelligence Oversight Division
Office of the Inspector General of the Marine Corps
Ph: 703-604-4518 DSN: 664-4518
Email: Edwin.Vogt@usmc.mil

Featured Article

Ransom Group Linked to Colonial Pipeline Hack is new but experienced

By Raphael Satter
Reuters
May 10, 2021

The ransomware group linked to the extortion attempt that has snared fuel deliveries across the U.S. East Coast may be new, but that doesn't mean its hackers are amateurs.

Who precisely is behind the disruptive intrusion into Colonial Pipeline hasn't been made officially known and digital attribution can be tricky, especially early on in an investigation. A former U.S. official and two industry sources have told Reuters that the group DarkSide is among the suspects.

Cybersecurity experts who have tracked DarkSide said it appears to be composed of veteran cybercriminals who are focused on squeezing out as much money as they can from their targets.
"They're very new but they're very organized," Lior Div, the chief executive of Boston-based security firm Cybereason, said on Sunday.

"It looks like someone who's been there, done that."
DarkSide is one of a number of increasingly professionalized groups of digital extortionists, with a mailing list, a press center, a victim hotline and even a supposed code of conduct intended to spin the group as reliable, if ruthless, business partners.
Experts like Div said DarkSide was likely composed of ransomware veterans and that it came out of nowhere in the middle of last year and immediately unleashed a digital crime wave.

"It's as if someone turned on the switch," said Div, who noted that more than 10 of his company's customers have fought off break-in attempts from the group in the past few months.

Ransom software works by encrypting victims' data; typically, hackers will offer the victim a key in return for cryptocurrency payments that can run into the hundreds of thousands or even millions of dollars. If the victim resists, hackers are increasingly threatening to leak confidential data in a bid to pile on the pressure.

DarkSide's site on the dark web hints at their hackers' past crimes, claims they previously made millions from extortion and that just because their software was new "that does not mean that we have no experience and we came from nowhere."

The site also features a Hall of Shame-style gallery of leaked data from victims who haven't paid up, advertising stolen documents from more than 80 companies across the United States and Europe.

Reuters was not immediately able to verify the group's various claims but one of the more recent victims featured on its list was Georgia-based rug maker Dixie Group Inc (DXYN.O) which publicly disclosed a digital shakedown attempt affecting "portions of its information technology systems" last month.
A Dixie executive did not immediately return a message seeking further comment.

In some ways DarkSide is hard to distinguish from the increasingly crowded field of internet extortionists. Like many others it seems to spare Russian, Kazakh and Ukrainian-speaking companies, suggesting a link to the former Soviet republics.

It also has a public relations program, as others do, inviting journalists to check out its haul of leaked data and claiming to make anonymous donations to charity. Even its tech savvy is nothing special, according to Georgia Tech computer science student Chuong Dong, who published an analysis of its programming.

According to Dong, DarkSide's code was "pretty standard ransomware." Div said that what does set them apart is the intelligence work they carry out against their targets beforehand.

Typically, "they know who the manager is, they know who they're speaking with, they know where the money is, they know who is the decision maker," said Div.

In that respect, Div said that the targeting of Colonial Pipeline, with its potentially massive knock-on consequences for Americans up and down the Eastern seaboard - may have been a miscalculation. "It's not good for business for them when the U.S. government becomes involved, when the FBI becomes involved," he said. "It's the last thing they need."

As for DarkSide, which usually isn't shy about putting out press releases and promises registered journalists "fast replies within 24 hours," the group has stayed uncharacteristically silent.

The reason is not clear. Requests for comment Reuters left via its main site and their media center have gone unanswered.

Intelligence Leaders Push for Mandatory Breach Notification Law

By Maggie Miller
The Hill
April 14, 2021

The leaders of the nation's intelligence agencies on Wednesday joined bipartisan members of the Senate Intelligence Committee in pushing for measures to encourage the private sector to report breaches and to deter malicious hackers from attacking critical infrastructure.

The discussion came as Congress is under increasing pressure to act after the discovery of both the SolarWinds hack, in which likely Russian hackers compromised nine federal agencies, and new vulnerabilities in a Microsoft email application exploited by a Chinese state-sponsored hacking group to breach thousands of companies.

"We are troubled in terms of being able to understand the depth and breadth of an intrusion based upon the fact that, for a number of good reasons, some of them obviously legal, that much of the private sector does not share this information readily," Gen. Paul Nakasone, the director of the National Security Agency and commander of U.S. Cyber Command, testified during the Senate Intelligence Committee's annual worldwide threats hearing.

Both Director of National Intelligence Avril Haines and FBI Director Christopher Wray also argued in favor of breach notification legislation, particularly following the SolarWinds hack. The breach was first discovered and reported publicly by cybersecurity group FireEye, not the federal government, something FireEye had no legal requirement to do.

"The reality is that adversaries try to use U.S. infrastructure for a variety of reasons," Wray testified. "The private sector controls 90 percent of the infrastructure and an even higher percentage of our PII [personally identifiable information] and innovation. It has the key dots as part of the overall connecting of the dots phenomenon."

Wray noted that some type of mandatory breach notification law to encourage the private sector to report cyberattacks would help to "further strengthen the glue between the private sector and the intelligence community and the rest of the government," which he said would be "the key ingredient to any long-term solution."

Haines also expressed support for a breach notification bill, asking members of the committee to support potential legislation.

"Something that would create, as I understand it, an obligation on companies to provide information when there are attacks, much like FireEye did in the context of SolarWinds ... that is something that I think would be useful. That is obviously one piece of the puzzle," Haines testified.

Support for breach notification legislation has been steadily increasing in both the House and Senate following the SolarWinds breach.

The bipartisan leaders of both the House Homeland Security and the House Oversight and Reform panels, which are carrying out a joint investigation into the Solar Winds breach, in February expressed their support for the introduction of legislation to enable and encourage the private sector to report breaches.

Key private sector groups have also been supportive of the idea, including the leaders of FireEye and Microsoft during a previous hearing on the Solar Winds breach held by the Senate Intelligence Committee.

Committee members, including Chairman Mark Warner (D-Va.), on Wednesday pushed for introduction of this legislation, with bipartisan agreement that it could assist intelligence agencies in responding to breaches faster.

"As we have discussed in a broadly bipartisan way, we have taken the lessons from our Solar Winds hearing, and I think we may have at least a partial response where, with appropriate liability protections, there would be some level of incident reporting to an enterprise that would include public and private together so that we could potentially close some of these gaps," Warner said.

"We are looking through a soda straw at some of the threats," Sen. John Cornyn (R-Texas) said in summing up the current visibility of the federal government into major cyber breaches.

Beyond breach notification legislation, both the intelligence leaders and senators highlighted concerns that foreign hackers, particularly those in China and Russia, continue to target the U.S. in cyberspace due to a lack of effective deterrence.

"Adversaries also have the capability to undertake destructive attacks of critical infrastructure," Warner said. "In order to deter these intrusions, we will need to accurately attribute them and hold our adversaries accountable."

Senate Intelligence Committee ranking member Marco Rubio (R-Fla.) also called for action.

"As a government, we need to have a more explicit deterrence policy that will clearly set expectations for accepted cyber behavior, and delineate very clear responses when those lines are crossed," Rubio said Wednesday. "Today's technology environment allows adversaries to wreak havoc, and they often do so at a minimal cost."

Nakasone stressed that while the federal government was working "every single day" to tackle cyber threats, "our adversaries continue to get better at what they're doing."

"I think it's fair to say that it's not as effective as we'd like it to be," Haines added.

PCLOB Board Members Ed Felten and Travis LeBlanc's Statement on Executive Order 12333 Public Report

PCLOB Official Statement
April 2, 2021

Today, the Privacy and Civil Liberties Oversight Board ("PCLOB" or "the Board") brings to conclusion its initial oversight review of Executive Order 12333 ("E.O. 12333") through release of a public report.

We thank the PCLOB staff and the Intelligence Community ("IC") for their diligence in working to support the PCLOB's efforts on this report. In general, Executive Order 12333 establishes the overarching framework for United States intelligence activities and outlines "general principles . . . intended to achieve the proper balance between the acquisition of essential information and protection of individual interests." It is then the responsibility of the 17 individual IC elements to implement E.O. 12333 and apply its general principles to each element's specific intelligence activities.

Accordingly, as the project progressed, it unfortunately proved difficult and impractical for the Board to address the full framework of counterterrorism activities governed by E.O. 12333. Additionally, as noted in the report, most of the Board's work on E.O. 12333 remains classified.

Accepting these facts, we voted to approve this report for two primary reasons. First, this report is the only public, unclassified document released by PCLOB regarding our initial review of the privacy and civil liberties implications of counterterrorism activities undertaken pursuant to E.O. 12333. The Board completed three additional deep dive reviews of

activities conducted under E.O. 12333 by the CIA (2) and NSA (1) that have been provided to Congress and the respective agencies. We found that those classified deep dive reviews ultimately were more meaningful and impactful regarding our balancing of privacy and civil liberties with national security value compared to what we could say publicly in an unclassified manner about E.O. 12333.

Second, our Board is a relatively small agency with limited resources. When presented with the option to carry on with a very broad oversight review of E.O. 12333, balanced against our need also to work on other timely, critical, and impactful issues affecting the privacy and civil liberties of Americans, we decided that there are other important issues today that demand our attention. We believe the Board now can and should focus its resources on other projects, which likely will continue to include oversight of specific counterterrorism activities conducted under E.O. 12333.

We look forward to the future where we can work with our fellow Board Members on issues such as:
1. Domestic terrorism, including implications for First Amendment-protected activities and minority groups;
2. Any use of counterterrorism authorities or resources directed at movements, protesters, demonstrations, or other public gatherings, such as the events following the killing of George Floyd last year;
3. The use of new and enhanced technologies to support counterterrorism activities, including facial recognition technology, artificial intelligence, information technology vulnerabilities, responses to changes in encryption technology, and other surveillance mechanisms;
4. Counterterrorism efforts directed at specific communities and/or narratives (such as Countering Violent Extremism programs), including First Amendment implications for speech, religion, and association; and
5. Federal government use of commercially-available or open source data (e.g., social media) for counterterrorism purposes. As terrorism threats evolve, so, too, must the Board's priorities. Fortunately, the Board's staff is comprised of innovative, dedicated, and expert individuals who every day demonstrate their commitment to the Board's mission. We are grateful for their continued diligence in safeguarding privacy and civil liberties. And we are excited about the opportunity to continue our important work in the months and years to come.

A 'Worst Nightmare' Cyberattack: The Untold Story of the Solar Winds Hack*

By Dina Temple-Raston
National Public Radio
April 16, 2021

"This release includes bug fixes, increased stability and performance improvements."
The routine software update may be one of the most familiar and least understood parts of our digital lives. A pop-up window announces its arrival and all that is required of us is to plug everything in before bed. The next morning, rather like the shoemaker and the elves, our software is magically transformed.

Last spring, a Texas-based company called Solar Winds made one such software update available to its customers. It was supposed to provide the regular fare — bug fixes, performance enhancements — to the company's popular network management system, a software program called Orion that keeps a watchful eye on all the various components in a company's network. Customers simply had to log into the company's software development website, type a password and then wait for the update to land seamlessly onto their servers.

The routine update, it turns out, is no longer so routine. Hackers believed to be directed by the Russian intelligence service, the SVR, used that routine software update to slip malicious code into Orion's software and then used it as a vehicle for a massive cyberattack against America.

"Eighteen thousand [customers] was our best estimate of who may have downloaded the code between March and June of 2020," Sudhakar Ramakrishna, Solar Winds president and CEO, told NPR. "If you then take 18,000 and start sifting through it, the actual number of impacted customers is far less. We don't

know the exact numbers. We are still conducting the investigation."

On Thursday, the Biden administration announced a roster of tough sanctions against Russia as part of what it characterized as the "seen and unseen" response to the Solar Winds breach.

NPR's months-long examination of that landmark attack — based on interviews with dozens of players from company officials to victims to cyber forensics experts who investigated, and intelligence officials who are in the process of calibrating the Biden administration's response — reveals a hack unlike any other, launched by a sophisticated adversary who took aim at a soft underbelly of digital life: the routine software update.

By design, the hack appeared to work only under very specific circumstances. Its victims had to download the tainted update and then actually deploy it. That was the first condition. The second was that their compromised networks needed to be connected to the Internet, so the hackers could communicate with their servers.

For that reason, Ramakrishna figures the Russians successfully compromised about 100 companies and about a dozen government agencies. The companies included Microsoft, Intel and Cisco; the list of federal agencies so far includes the Treasury, Justice and Energy departments and the Pentagon.

Solar Winds CEO and President Sudhakar Ramakrishna inherited the attack. He was hired shortly before the breach was discovered and stepped into the job just as the full extent of the hack became clear.

The hackers also found their way, rather embarrassingly, into the Cybersecurity and Infrastructure Security Agency, or CISA — the office at the Department of Homeland Security whose job it is to protect federal computer networks from cyberattacks.

The concern is that the same access that gives the Russians the ability to steal data could also allow them to alter or destroy it. "The speed with which an actor can move from espionage to degrading or disrupting a network is at the blink of an eye," one senior administration said during a background briefing from the White House on Thursday. "And a defender cannot move at that speed. And given the history of Russia's malicious activity in cyberspace and their reckless behavior in cyberspace that was a key concern."

* Entire story can be found at NPR.org

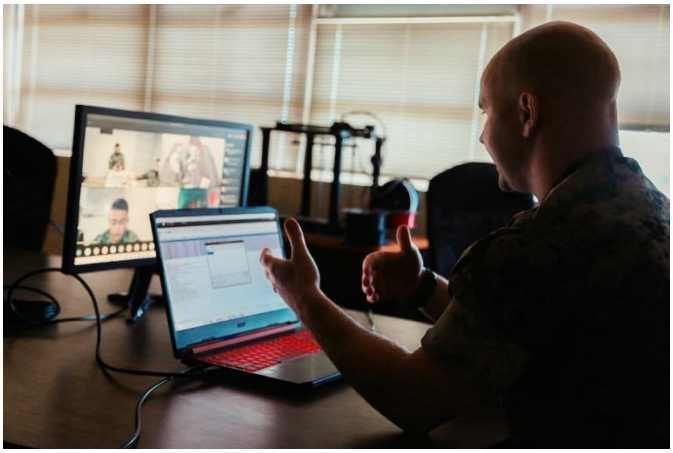
Intelligence Photographs in the News

A U.S. Marine utilizes a drone at Combined Arms Training Center, Camp Fuji, Japan, Jan. 22.

U.S. Marine Corps photo by Cpl. Savannah Mesimer/Released 210122-M-GB409-173.JPG

A U.S. Marine demonstrates Defensive Cyberspace Operations-Internal Defensive Measures capabilities during a virtual training session with members of the Philippine Marine Corps on Camp Hansen, Okinawa, Japan, April 19.

U.S. Marine Corps photo by Cpl. Nicholas Filca/Released 210419-M-SK440-001.JPG



Intelligence Oversight Division

MISSION: To ensure the effective implementation of Marine Corps-wide Oversight of Intelligence, Counterintelligence, Sensitive activities (to include USMC support to law enforcement agencies, special operations, and security matters), and special Access Programs. To establish policy and ensure their legality, propriety and regulatory compliance with appropriate Department of Defense/ Department of the Navy guidance.

Examples of sensitive activities include:

- Military support to Civil Authorities
- Lethal support/training to non-USMC agencies
- CONUS off-base training
- Covered, clandestine, undercover activities
- Intelligence collection of information on U.S. persons

SECNAVINST 5430.57G states**:**

"...personnel bearing USMC IG credentials marked 'Intelligence Oversight/Unlimited Special Access' are certified for access to information and spaces dealing with intelligence and sensitive activities, compartmented and special access programs, and other restricted access programs in which DON participates. When performing oversight of such programs pursuant to Executive Order, they shall be presumed to have a 'need to know' for access to information and spaces concerning them."

WHAT IS INTELLIGENCE OVERSIGHT?

Intelligence Oversight ensures that intelligence personnel shall not collect, retain, or disseminate information about U.S. persons unless done in accordance with specific guidelines, proper authorization, and within only specific categories (*See References*).

DEFINITIONS

i. **INTELLIGENCE OVERSIGHT (IO):** Ensures that intelligence personnel shall not collect, retain, or disseminate information about U.S. persons unless done in accordance with specific guidelines, proper authorization, and within only specific categories. References: E.O. 12333, DoD Dir 5240.01, DoD Reg 5240.1-R, SECNAVINST 3820.3F, MCO 3800.2B

ii. **INTELLIGENCE RELATED ACTIVITY**. Activities that are not conducted under the authority of Executive Order 12333 that involve the collection, retention, or analysis of information, and the activities' primary purpose is to: a. train intelligence personnel; or b. conduct research, development, or testing and evaluation for the purpose of developing intelligence-specific capabilities. Reference: SECNAVINST 5000.34G.

iii. **SENSITIVE ACTIVITIES:** Operations, actions, activities, or programs that are generally handled through special access, compartmented, or other sensitive control mechanisms because of the nature of the target, the area of the operation, or other designated aspects. Sensitive activities also include operations, actions, activities, or programs conducted or supported by any DoD component, including the DON, that, if compromised, could have enduring adverse effects on U.S. foreign policy, DoD or DON activities, or military operations; or, cause significant embarrassment to the United States, its allies, the DoD or DON. Reference: SECNAVINST 5000.34G.

iv. **SPECIAL ACCESS PROGRAM (SAP):** A program activity that has enhanced security measures and imposes safeguarding and access requirements that exceed those normally required for information at the same level. Information to be protected within the SAP is identified by a security classification guide. DoD SAPs are divided into three categories: Acquisition SAP; Intelligence SAP; or Operations and Support SAP. Reference: SECNAVINST 5000.34G.

v. **QUESTIONABLE INTELLIGENCE ACTIVITY:** Any intelligence or intelligence-related activity, when there is reason to believe such activity may be unlawful or contrary to any Executive Order, Presidential Directive, Intelligence Community Directive, or applicable DoD policy governing that activity. Reference: SECNAVINST 5000.34G.