Threat Analysis of APT40 vs USNA

By Alexander Miller, Tyler Crosby, Joshua Bunce

THREAT:
APT40

Aliases: TEMP.Periscope & TEMP.Jumper

Prior Activity: US Navy UUV

Motivation: Support Chinese Naval Operations

Methods: Cyber Espionage & Data Exfiltration

Resources: China (China's People's Liberation Army)

Exploits Commonly Leveraged

CVE-2012-0158

CVE-2017-0199

CVE-2017-8759

CVE-2017-118821

The HOW?

1. Establish a Foothold
2. Escalate Privileges
3. Internal Reconnaissance
4. Lateral Movement
5. Maintain Presence
6. Profit?

UNITED STATES NAVAL ACADEMY

The **United States Naval Academy** (also known as **USNA**, **Annapolis**, or simply **Navy**) is a four-year coeducational federal service academy adjacent to Annapolis, Maryland. Established on 10 October 1845, under Secretary of the Navy George Bancroft, it is the second oldest of the United States' five service academies, and educates officers for commissioning primarily into the United States Navy and United States Marine Corps.

The Process - People

Reza Malek-Madani

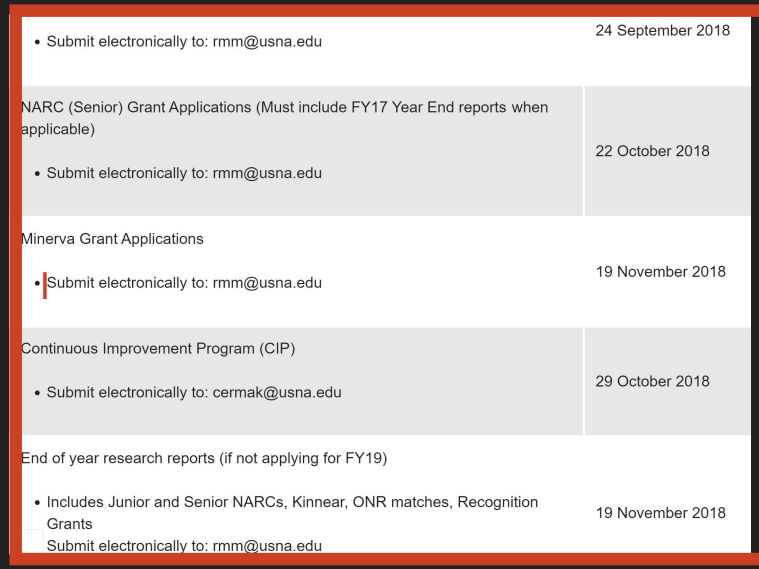
Department of Mathematics, Chauvenet Hall 301
The United States Naval Academy
572 Holloway Road, Annapolis, MD 21402
rmm@usna.edu
(410) 293-2504

Katherine Cermak

cermak@usna.edu
ADPA - Academic Dean & Provost Staff
Dr. Katherine A. Cermak
Dr. Katherine A. Cermak
Associate Dean for Planning and Assessment

Who Is Important

Due to the nature of the APT-40 to attack research departments of maritime educational facilities, teachers and faculty become the primary target due to the ability to move laterally and get to the certain department,



• Submit electronically to: rmm@usna.edu	24 September 2018
NARC (Senior) Grant Applications (Must include FY17 Year End reports when applicable) • Submit electronically to: rmm@usna.edu	22 October 2018
Minerva Grant Applications • Submit electronically to: rmm@usna.edu	19 November 2018
Continuous Improvement Program (CIP) • Submit electronically to: cermak@usna.edu	29 October 2018
End of year research reports (if not applying for FY19) • Includes Junior and Senior NARCs, Kinnear, ONR matches, Recognition Grants Submit electronically to: rmm@usna.edu	19 November 2018

Determine Cyber Threats to Those Assets

Both of these individuals have their personal emails listed in their publicly facing website. This is extremely dangerous.

Develop Potential Attack Strategies Against Those Targets

An attacker could spoof their email address to be a @usna.edu email and send a email to both of these emails with the title as the Continuous Improvement Program, or any of the other programs that you must submit a document to, and include a malicious pdf with the same title as the subject line.

Prioritize Mitigations and Countermeasures

The way that students electronically submit these. The email for submitting these documents should be changed to an email address that is created in a sandbox environment outside of the normal network of the institution, and on a device that has zero information regarding the individuals within the institution, or the institution at all. The device should solely be used for the purpose of receiving and reviewing the submitted documents in a safe environment.

More Mitigation

- Students are provided laptops, electronic device/ cell phone restriction in sensitive areas
- Disable Peripherals
- Rules on what personal devices are and aren't allowed.
- Teachers are also supplied work laptops.
-

Resources:

F. Plan, N.Fraser, J. O'Leary, V. Cannon, B. Read, March 4, 2019, "APT40: Examining a China-Nexus Espionage Actor", https://www.fireeye.com/blog/threat-research/2019/03/apt40-examining-a-china-nexus-espionage-actor.html

Photos:

Obtained and provided by Tyler Crosby