New York State Intelligence Center

Cyber Intelligence Bulletin

CAU@nysic.ny.gov
1-866-48-NYSIC (866-486-9742)

May 1, 2024 **NYSIC-CYB-24-01**

ATTN: Critical Infrastructure Partners

SUBJECT: **Increased Potential for Cyber Attacks Amidst International Conflicts**

OVERVIEW: As international conflicts continue in Eastern Europe and the Middle East, numerous socio-political hacktivist groups and state-sponsored advanced persistent threats (APTs) have declared a widening scope and lowered threshold for potential victims whom they feel are not aligned with their beliefs or are perceived as antagonists. These groups are typically ideologically motivated, and the scope, scale and impact of their operations can vary. Hacktivist groups are typically associated with unsophisticated activity that requires limited technical skill, such as Distributed Denial of Service (DDoS) attacks, doxing, and website defacements. The goal of such activity is usually to spread messaging to potential supporters and/or to intimidate victims. APT groups have a high degree of technical skill, more resources, and can engage in extended campaigns with funding by the nation-states they support. More sophisticated attacks by APT groups may include disruption or destruction of critical infrastructure and key resources (CIKR).

BACKGROUND: A sampling of recent cyber events across the continental United States have included website defacements, DDoS attacks, and attacks on public-facing ICS/SCADA systems in CIKR facilities. All of these incidents have been linked to ideologically-motivated actors who used the attacks to call attention to their cause or beliefs.

RECOMMENDATIONS: Any agency that falls victim to a cyberattack and receives notification that the malicious actors intend to release data for sale should immediately contact law enforcement. Entities should validate the necessity of public-facing components, ensure all software and hardware is updated and patched, and review all user accounts and permissions.

REPORTING: The NYSIC CAU is requesting contact from any entity impacted by a cyberattack from a known APT or ideologically motivated actor. The CAU is interested in all Indicators of Compromise (IOCs) related to the incident. Please contact the CAU by phone 518-786-2191 or email: cau@nysic.ny.gov.

As a reminder, non-executive NYS Agencies and Critical Infrastructure and Key Resource (CIKR) entities within New York State can report suspicious cyber activity or request assistance from the NYS Division of Homeland Security and Emergency Services Cyber Incident Response Team (DHSES CIRT) via 1-844-OCT-CIRT / 1-844-628-2478.

Please note that some of this information describes first amendment protected activities. The NYSIC recognizes that Americans have constitutionally protected rights to assemble, speak, and petition the government. The NYSIC safeguards these rights and only reports on First Amendment protected activities, although no violence or criminality has been observed, this information is provided for operational planning in the interest of assuring the safety and security of the demonstrators and the public.

Requirements: NY-SIN- 1.1, 1.2, 1.3, 1.4, 1.5, 1.8 & 1.10

ADDITIONAL RESOURCES:

- https://www.ic3.gov/ - FBI Internet Crime Complaint Center (IC3)
- https://www.cisa.gov/stopransomware - CISA Stop Ransomware
- https://www.cisa.gov/news-events/alerts/2024/05/01/cisa-and-partners-release-fact-sheet-defending-ot-operations-against-ongoing-pro-russia-hacktivist - CISA and Partners Release Fact Sheet on Defending OT Operations Against Ongoing Pro-Russia Hacktivist Activity
- https://www.dhs.gov/publication/resources-individuals-threat-doxing - Resources for Individuals on the Threat of Doxing

For general inquiries, contact the NYSIC main line at 866-48-NYSIC (866-486-9742). Report suspicious activity of a physical threat nature to 866-SAFE-NYS (866-723-3697) while utilizing 911 for emergencies.

For further information regarding the content of this bulletin, please contact cau@nysic.ny.gov.

Please note that some of this information describes first amendment protected activities. The NYSIC recognizes that Americans have constitutionally protected rights to assemble, speak, and petition the government. The NYSIC safeguards these rights and only reports on First Amendment protected activities, although no violence or criminality has been observed, this information is provided for operational planning in the interest of assuring the safety and security of the demonstrators and the public.

Requirements: NY-SIN- 1.1, 1.2, 1.3, 1.4, 1.5, 1.8 & 1.10