



# NJCCIC

NJ CYBERSECURITY AND COMMUNICATIONS INTEGRATION CELL

## Advanced Cyber Threats Succeed Using Simplest of Tactics

August 12, 2015

TLP: **WHITE** | For several years, cybersecurity firms and the U.S. intelligence community have warned of the increasing frequency and scope of targeted cyber-attacks conducted by state-sponsored actors and sophisticated cyber-criminal groups – often referred to as Advanced Persistent Threats, or APTs. These groups are known to be well-resourced and composed of highly-skilled computer experts capable of penetrating the networks of the most hardened corporations and governments around the world. Yet, reports resulting from forensic investigations of high-profile data breaches consistently reveal the use of basic tactics to initiate attacks, including spear-phishing emails and rudimentary algorithms that crack weak passwords. In fact, according to [Verizon](#), the majority of data breaches in 2014 were carried out without the use of malware. ***The NJCCIC assesses that APTs will continue to target user credentials by exploiting basic human tendencies that result in weak email and web-browsing security, as well as poor authentication practices. To reduce the likelihood of account compromises and socially-engineered spear-phishing campaigns, the NJCCIC recommends implementing two-factor authentication (2FA) when possible***, particularly for remote access applications such as VPNs and web portals, email services like Microsoft Outlook Web Access, and cloud storage applications such as Google Drive, Dropbox, and Microsoft OneDrive.

- Last week, the Joint Staff of the Department of Defense provided new details on a breach of their unclassified email network that began with a malicious spear-phishing email, similar to breaches of the White House and State Department networks in the Fall of 2014. According to consistent media reporting citing unnamed U.S. officials, these federal breaches have all been attributed to espionage actors acting on behalf of the Russian government.
- One cybersecurity firm that regularly reports on the most current tactics, techniques and procedures (TTPs) of active Russian and Chinese APTs, CrowdStrike, recently produced a [white paper](#) detailing the prevalence of malware-free attacks that seek to establish undetected, long-term access on networks, often by compromising insider credentials. The report examined a prolonged state-sponsored attack on a large U.S. defense contractor in which the attackers compromised the Virtual Private Network (VPN) and were able to sustain their attack using seemingly legitimate credentials and network activity, thereby limiting indicators of compromise.
- On 1 August 2015, Dell SecureWorks released a [report](#) detailing a Chinese cyber-espionage group they refer to as TG-3390, or EMISSARY PANDA. This espionage group has targeted at least fifty organizations, many in the U.S. and U.K., spanning the aerospace, energy, law and pharmaceutical industries, as well as defense contractors and those involved in international relations, including embassies and non-governmental organizations. While EMISSARY PANDA employs a range of advanced tools and tactics, they rely heavily on stolen credentials to carry out their intrusions, ultimately seeking to obtain privileged access and move laterally throughout networks to achieve their objectives.

In today's cyber threat landscape, organizations and home users face a barrage of threats and constant notification of new vulnerabilities affecting the most common software used for day-to-day business, commerce, and communication. While a proactive and agile cybersecurity posture requires comprehensive strategies that address the enterprise's people, processes, and technology, there are also low-cost, high-impact solutions that can greatly decrease cyber risk and elevate the barriers for malicious actors.

- In addition to implementing 2FA, organizations should set minimum requirements to enforce complex passwords and regular password resets, remove local administrator rights, implement the principle of least privilege, and update all operating systems, software applications, and web services as soon as patches become available.

Traffic Light Protocol: **WHITE** information may be distributed without restriction.