BALOUGH LAW OFFICES, LLC

DHS and FBI Urge Organizations to Boost Cybersecurity to Avoid Russian Hackers

(January 3, 2017) The Joint Analysis Report on the Russian cyber activity in the recent election also serves as a warning to others of the need to implement best cybersecurity practices to protect computer systems.

The report by the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI) found activity by Russian civilian and military intelligence services (RIS) "is part of an ongoing campaign of cyber-enabled operations directed at the U.S. government and its citizens. These cyber operations have included spearphishing campaigns targeting government organizations, critical infrastructure entities, think tanks, universities, political organizations, and corporations leading to the theft of information."

The RIS attacks include placing malicious code that tricks victims into entering legitimate credentials and delivers remote access tools, which set up operational infrastructures to hide their source, host domains and malware, establish command and control nodes, and harvest credentials and other valuable information from their targets, the report said.

The Joint Report recommends organizations should answer the following questions about their cybersecurity:

- **Backups.** Do we backup all critical information? Are the backups stored offline? Have we tested our ability to revert to backups during an incident?
- **Risk Analysis.** Have we conducted a cybersecurity risk analysis of the organization?
- **Staff Training.** Have we trained staff on cybersecurity best practices?
- **Vulnerability Scanning and Patching.** Have we implemented regular scans of our network and systems and appropriate patching of known system vulnerabilities?
- **Application Whitelisting.** Do we allow only approved programs to turn on our networks?
- **Incident Response.** Do we have an incident response plan and have we practiced it?
- **Business Continuity.** Are we able to sustain business operations without access to certain systems? For how long? Have we tested it?
- **Penetration Testing.** Have we attempted to hack into our own systems to test the security or our systems and our ability to defend against attacks?

In addition, DHS encourages network administrators to implement seven mitigation strategies:

- Patch applications and operating systems with the latest updates to reduce the number of exploitable entry points available to an attacker.
- Apply whitelisting to allow only specified programs to run while blocking all others.
- Restrict administrative privileges to only those need for a user's duties.
- Segment and segregate the network into security zones to protect sensitive information and critical services and limit damage from network perimeter breaches.
- Input validation to sanitize untrusted user input.

- Tune anti-virus systems to the most aggressive setting possible.
- Configure firewalls to block data from certain locations while allowing relevant and necessary data through.

The report encourages organizations to contact DHS or the FBI to report an intrusion and to request incident response resources or technical assistance.

Balough Law Offices, LLC, is a Chicago-based law firm that focuses on cyberspace, intellectual property, and business law. Our homepage is balough.com.