From: Executive Communications <executivecommunications@iansresearch.com>
Sent: Monday, October 7, 2019 8:57 AM
To: Client <client@company.com>
Subject: [External] IANS Executive Communications: Monday, October 7

IANS Executive Communications: **Monday, October 7**

==========

Today's top takeaways:

- Phosphorous targets Trump campaign.
- Ransomware hackers see small hospitals as choice targets.
- FBI warns universities on Chinese IP theft.

==========

Compilation: Iranian Hackers Target Trump Re-Election Campaign
WSJ: Presidential Campaign Targeted by Suspected Iranian Hackers, Microsoft Says
Reuters: Trump Re-election Campaign Targeted by Iran-Linked Hackers: Sources

What it Says:

- An Iranian hacking group targeted a U.S. presidential campaign between Aug-Sept 2019, according to Microsoft:
    - Microsoft would not identify the targeted campaign, but President Trump is the only contending candidate whose campaign uses Microsoft's cloud email service.
    - Phosphorous -- the hacking group -- used spear-phishing emails and fake LinkedIn profiles to trick potential victims into clicking on malicious links.

What to Communicate to Executives:

- Through spear-phishing, Iranian hackers target campaign officials' email to both gather intel and potentially disrupt the 2020 election.
- *Corporate* executives are targeted by spear-phishing as well -- used in 65% of attacks by sophisticated hackers last year. To protect executives:
    - Do not have administrative rights on any corporate device.
    - Use two-factor authentication:
        - Consider moving to a physical security key (Google's Titan) for accounts with high-value information.
    - Never re-use credentials between accounts (especially professional and personal).
    - Comply with company requirements around password length/complexity:
        - Consider a password manager (LastPass, 1Password).

Relevant Document [Subscription might be required]:
Overview of Targeted Attacks in 2018

==========

Compilation: Small Healthcare Providers Ripe Targets for Ransomware
WSJ: Smaller Medical Providers Get Burned by Ransomware
AP: Report: Alabama Hospitals Pay Hackers in Ransomware Attack

What it Says:

- Small healthcare providers are increasingly targeted by ransomware attackers due to their computer networks' criticality and poor patching:

- Alabama's DCH Health Systems -- which operates three hospitals -- suffered a ransomware attack last week and was forced to stop admitting patients.
- California's Wood Ranch Medical was forced to permanently close after suffering an attack:
  - "Unfortunately, the damage to our computer system was such that we are unable to recover the data stored there and, with our backup system encrypted as well, we cannot rebuild our medical records."

What to Communicate to Executives:

- Small healthcare providers (often rural) have become a choice target for ransomware hackers because they must quickly restore their systems to serve their communities.
- Executives must develop a ransomware position prior to an incident:
  - *Pay the ransom*: Consider paying if the compromised data could lead to loss of life or cause substantial harm if deleted (birth certificates, child custody).
  - *Don't pay*: Paying doesn't guarantee that the data will be recovered and it funds hackers' future activities.

Relevant Document [Subscription might be required]:
8 Ransomware Payment Considerations

==========

AP: US Researchers on Front Line of Battle Against Chinese Theft

What it Says:

- The FBI is warning U.S. universities about the growing threat of Chinese researchers pilfering their technology and trade secrets:
  - Universities targeted: Illinois-Urbana-Champaign, Washington, Oklahoma State, Kansas, Minnesota, Colorado, Texas A&M, others.
  - "Existentially, we look at China as our greatest threat from an intelligence perspective, and they succeeded significantly in the last decade from stealing our best and brightest technology," asserted William Evanina, director of the U.S. Counterintelligence and Security Center.

What to Communicate to Executives:

- China steals between $225-$600 billion in IP from the U.S. every year:
  - "No country poses a broader, more severe intelligence collection threat than China," stated FBI director Christopher Wray. "China has pioneered a societal approach to stealing innovation…"
- The Chinese actively pilfer IP focused on bolstering China's "Made in China 2025" program, with an emphasis on:
  - Artificial intelligence, IoT, aerospace, medicine/medical devices, ocean engineering, high-tech ships and quantum computing.

Relevant Document [Subscription might be required]:
Overview of China's Targeting of U.S. Intellectual Property

==========

==========