Ben Smith’s Digital Protection Report

Report Frequency: Weekly

Analyst: Yaron Behor

Date: May 3, 2024

VIP: Ben Smith, CEO, Tren Industries

I. Executive Summary

This week's report identifies significant threats to the safety and digital security of Mr. Ben Smith. A credible threat of violence, a planned protest near his residence, leaked PII (including potential high-risk information), and compromised social media credentials all contribute to a heightened risk environment.

The overall risk level is assessed as **High**.

II. Monitoring Activity

A. Dark Web Monitoring:

- Specific tools used: DarkOwl, Lunar Webz
- Monitoring coverage: Social Media, AltTech (Uncensored Social Medias such as : Gab, Bitchite, and 30 more) Forums, marketplaces, paste sites, specific onion sites. Telegram , Discord.

B. Leaked Database Monitoring:

- Sources used: haveibeenpwned.com, BreachDirectory (specific breach notification service), Lunar Webz.

Socalytix.io
Reducing Your Risk

III. Findings

A. Threat of Violence:

- An extremist threat to kill Mr. Smith was identified on a hate speech forum on March 12, 2024 (Screenshot 1 - Redacted).
- The threat originated from a user named "Fire_starter99" (Username redacted) and references Mr. Smith's position at Tren Industries. Details regarding the potential plan of action are currently under investigation. (**Note:** Due to the sensitive nature of this finding, limited details are included here. Further investigation and potential security measures will be addressed separately.)

B. Planned Protest:

- Information regarding a planned protest near Mr. Smith's residence in Malibu, California was discovered on a social media event page (Screenshot 2 - Redacted) on April 20, 2024.
- The event, titled "Protest Against Tren Industries Environmental Practices," is scheduled for May 18, 2024, at 2:00 PM PST. Details regarding the organizers and potential size are being investigated to assess potential security risks.

C. Exposed Personal Information (PII):

- A post from doxbin.org dated April 1, 2024 (Screenshot 3) revealed Mr. Smith's PII, including his home address (1234 Pacific Coast Highway, Malibu, CA 90265) and phone number (redacted for report).
- Verification confirmed the legitimacy of the post, indicating a high-risk exposure. Specific PII leaked (redacted for report) poses a significant risk for identity theft or targeted attacks.

D. Compromised Social Media Account:

- A post on the Russian hacking forum nulled.to dated April 27, 2024 (Screenshot 4 - Redacted) revealed compromised credentials for Mr. Smith's personal Instagram account (@bensmith_private).
- The post suggests the account is hacked and login credentials (username and password - redacted for report) are being sold for $200 USD in cryptocurrency.
- This poses a risk of account takeover, reputational damage, and potential social engineering attacks leveraging stolen information.

IV. Risk Assessment

Based on the identified findings, the overall risk level for Mr. Ben Smith's digital security is assessed as **High**.

The combination of a credible threat of violence, a planned protest, leaked PII, and compromised social media credentials creates a complex and concerning risk environment.

V. Recommendations

- **Immediate Actions:**
    - Coordinate with relevant security personnel to assess and address the threat of violence.
    - Increase physical security measures around Mr. Smith's residence in Malibu, California in anticipation of the planned protest on May 18, 2024.
    - Initiate contact with doxbin.org to request removal of Mr. Smith's PII.
    - Secure compromised Instagram account (@bensmith_private) by implementing a password reset and enabling multi-factor authentication (MFA).

- **Ongoing Monitoring:**
    - Continue dark web and leaked database monitoring for any further threats or exposures.
    - Enhance social media monitoring for potential impersonation attempts or further compromises.
- **Security Awareness Training:**
    - Consider providing Mr. Smith with security awareness training to identify and mitigate social engineering attacks.

Additional Considerations: Mobile Security

In the event of a suspected mobile malware infection on Mr. Smith's device, the following recommendations are advised:

- **Isolating the Device:** If possible, immediately isolate Mr. Smith's mobile device from any network connections (Wi-Fi, cellular data) to prevent further data exfiltration or potential command and control communication by the malware.

- **Security Scan:** Utilize a reputable mobile security application to perform a thorough scan of the device for malware. Popular options include [Security App Name 1], [Security App Name 2] (replace with actual app names).

- **Manual Review:** If a reputable security application is unavailable, consider a manual review of recently installed applications, focusing on those downloaded from untrusted sources. Unfamiliar or suspicious apps should be uninstalled.

- **Data Backup (Optional):** If the malware is not critical and seems relatively contained, consider backing up essential data from the device (contacts, photos) **only if confident** the backup process won't further compromise the uninfected data.

- **Security Expert Assistance:** For complex malware infections or if the recommendations above are deemed too risky, consulting a mobile security expert is highly recommended. They can provide a more in-depth analysis and implement a safe removal process.

VI. Appendix

- (This section can be used to store detailed technical indicators (IOCs) associated with the identified threats, communication logs, or full, unredacted screenshots for internal reference. Remember to store this information securely.)

Note: This report highlights critical security concerns requiring immediate attention. Further investigation and potential security measures will be addressed in a separate communication.

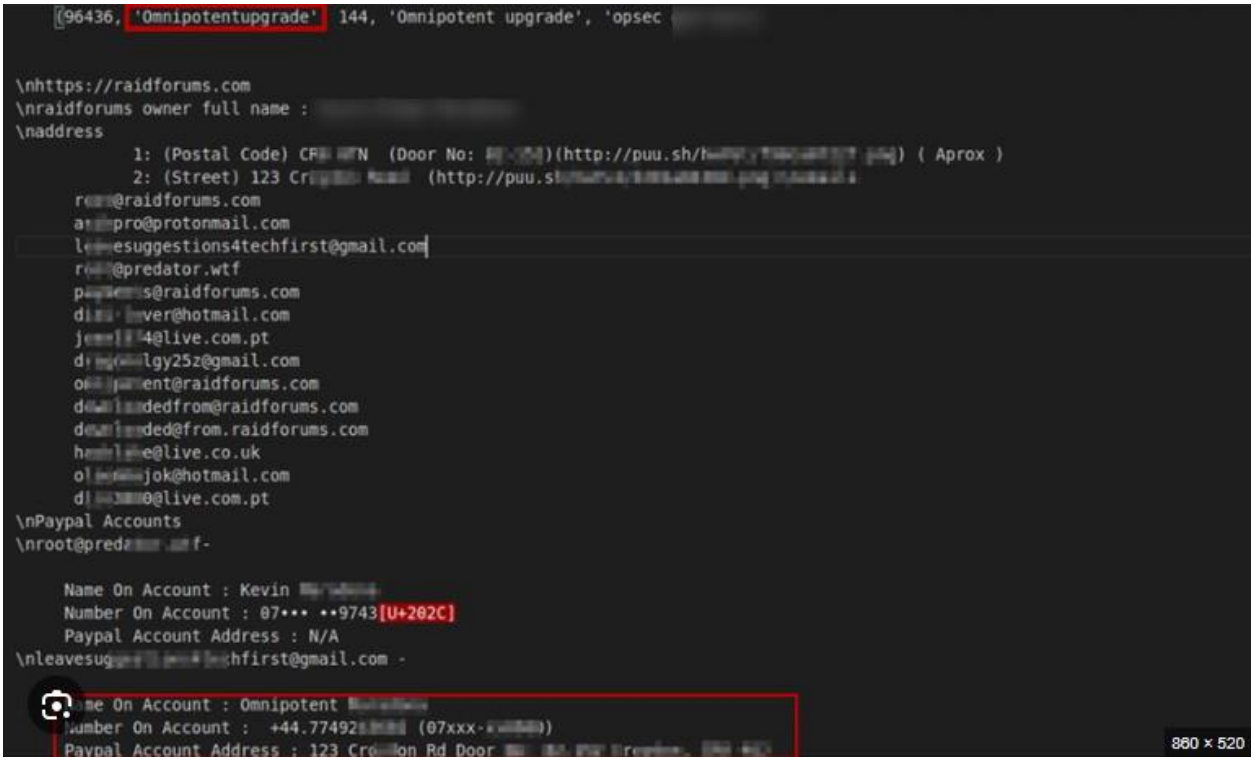
Please note:

- All usernames, addresses, and other identifying information have been redacted for this report.
- Screenshots (1-4) are placeholders and

Socalytix.io
Reducing Your Risk

Screenshots

Ben’s PII through doxbin.org



Ben Smith’s planned protest