Cyber Threat Reports 01 May - 15 May 2017

James Twist
Army Cyber Institute, contact.cyber@usma.edu

Follow this and additional works at: https://digitalcommons.usmalibrary.org/aci_rp

Recommended Citation
https://digitalcommons.usmalibrary.org/aci_rp/24
JCC Bomb Hoaxer Charged With Vast List of Offenses

*Items of Interest: DCO / Profiling Hackers / Cyber-Psychology*

Israel on Monday filed a massive laundry list of criminal charges against an Israeli-American teenager accused of making thousands of bomb threat calls and other violent threats to Jewish institutions, schools, hospitals and airlines all over the world. His alleged threats caused fighter jets to scramble, planes to dump fuel and make emergency landings, large numbers of schools to evacuate, and numerous other chaotic consequences. In some cases, he allegedly threatened to execute children he claimed to be holding hostage.>> [Massive List of Crimes From One Hacker.](#)

New Dok Mac Malware Gets Complete Access to Victim's Traffic, Even If Encrypted.

*Items of Interest: Malware / Operating Systems / Detection*

A new Mac malware was discovered in the wild - the malware affects all OSX versions and is virtually undetectable on VirusTotal. What makes matters worse is that the malware is signed with a valid developer certificate authenticated by Apple. Once the infection is complete, the attackers manage to gain complete access to all victim communications, including those encrypted by SSL.>> [OSX Malware Does It All to Take Control of Your Computer.](#)

U.S. Warns of 'Emerging' Global Cyber-Espionage Campaign by China.

*Items of Interest: APTs / Chinese Cyber Threat / Campaigns*

An “emerging” international cyber-espionage campaign by a group with suspected ties to the Chinese government is affecting a growing number of companies globally, according to a warning from the U.S. government. Cybersecurity researchers and intelligence analysts have been tracking the hacker group known as APT10 or MenuPass Group since at least 2009. In the past, the group has targeted construction, engineering, aerospace and telecom companies as well as government agencies in the U.S., Europe and Japan.>> [MenuPass / APT 10 Hacking Campaign Successful Across Many Sectors.](#)

US Intelligence Agencies Fear Insiders As Much As Spies.

*Items of Interest: Insider Threats / Third Party Access / Cybersecurity*

Forget about spies. It’s rogue insiders that cause heartburn at US intelligence agencies these days. Few spy cases have broken in the past decade and a half. In contrast, a proliferation of US intelligence and military insiders have gone rogue and spilled secrets to journalists or WikiLeaks, the anti-secrecy group. The leaks are as damaging as any major spy case, perhaps more so. And they have underscored the ease of stealing secrets in the modern age, sometimes with a single stroke of a keyboard.>> [Continuous Plague of U.S. Insider Threats.](#)