ARMY CYBER
INSTITUTE

Weekly Cyber Threat Report

May 1 – May 15, 2017

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.

TECH TRENDS: Stories/Links

- **German Cybercrime Rises 80%.**
  >> Disturbing Trends in Germany.
- **Secure Execution Processor Brings Protection to IoT Devices.**
  >> Secure Execution Processor.
- **Invasion of the Hardware Snatchers**
  >> Cloned Hardware.

  The Pentagon's Seek-and-Destroy Mission for Counterfeit Electronics. >> Microscopic Chip Markers.
- **Old Windows Server Machines Can Still Fend Off Hacks.**
  >> Network Segmentation is the Answer.
- **Choking Intel Powered Broadband Modems.**
  >> Choking Intel Broadband Modems.
- **Netgear Says Sorry Four Weeks After Losing Customer Backups.**
  >> Cloud Data Evaporates.
- **Disarming Control Flow Guard Using Advanced Code Reuse Attacks. >> COOP: Code Reuse Attack.**
- **AI Might Be The Ultimate Answer To Cyber Threats.**
  >> DarkTrace: Tracking Unknown Unknowns.
- **Data Theft. Safeguard Data When Employees Leave.**
  >> Preventing Data Theft.
- **3D X-ray Tech for Easy Reverse Engineering of ICs.**
  >> Ptychography: Mapping Transistors.
- **Hacked Drones Become the Ultimate IEDs.**
  >> Cyber Control of Drones.
- **Google's New Chip Is a Stepping Stone to Quantum Computing Supremacy. >> 6 Cubit Chip Due This Year.**
- **Internet of the future via massive mobile antennae technology. >> 5G Design for Future Internet.**
  SNMP Authentication Bypass Plagues Numerous Devices
  >> 78 Models of IoT Devices Vulnerable.

Contact Us

Army Cyber Institute at West Point
2101 New South Post Road
West Point, NY 10996
Phone: 845-938-3436
Web: www.cyber.army.mil
Email: threat.cyber@usma.edu

Compilation of cyber-related media reports for the purpose of promoting situational awareness in the government. This is not vetted intelligence and does not represent the official position of the US Government or Department of Defense.