California Senators Contract Hackers To Attack Opponents And Manipulate Government Records

Numerous Congressional reports, IT staff reports and security industry reports have verified that agency servers and files, including those upon which Plaintiffs records were housed, have been hacked, moved, deleted and edited by outside third parties including Chinese and Russian hackers, bored teens and hired opposition research operatives and that the hardware level back-doors for SPECTRE and many other incursion sets still exist in agency Cisco, Intel, Juniper Networks and other Network devices now connected to government file networks at DOE, SSA, FEC, and other agencies and this fact is indisputable.

Certain "LOST" Lois Lerner, Hillary Clinton, SSA, DOE and other files are neither lost nor unrecoverable. The notorious Kleiner Perkins and Greylock corruption case files are neither lost nor unrecoverable. At the very least, China, Russian or Brazilian teen hackers have them up for sale on the Dark Web. The NSA certainly has copies of them.

Per the FBI, DOJ, FCC and Congressional investigators:

It is widely verified by the U.S. DOJ that hackers such as Wang Dong, Sun Kailiang, Wen Xinyu, Huang Zhenyu, and Gu Chunhui, who were officers in Unit 61398 of the Third Department of the Chinese People’s Liberation Army (PLA) and Aleksei Sergeyevich Morenets, 41, Evgenii Mikhaylovich, Serebriakov, 37, Ivan Sergeyevich Yermakov, 32, Artem Andreyevich Malyshev, 30, and Dmitriy Sergeyevich Badin, 27, who were each assigned to Military Unit 26165, and Oleg Mikhaylovich Sotnikov, 46, and

Alexey Valerevich Minin, 46, who were also GRU officers, and hackers-for-hire including Kevin David Mitnick, Adrian Lamo, Albert Gonzalez, Matthew Bevan, Richard Pryce, Jeanson James Ancheta, Michael Calce, Kevin Poulsen, Jonathan James, The hacker known as ASTRA, The hacker known as GUCIFER, The hacker known as ANON 4CHAN and THOUSANDS of other individuals had free acess and free reign throughout NSA, FBI, SSA, DOJ, OPM, CIA and other government servers via the SPECTRE, EMOTET, PRIME ROOTKIT, SERCOMM BACKDOOR, NOTPETYA, MELTDOWN, MASTERKEY, RYZENFALL, FALLOUT, CHIMERA, and hundreds of other back doors and penetration vulnerabities in Cisco, Intel, Juniper Networks, AMD, and other equipment. Additionally, all of the core server penetration tools used by the CIA and the NSA were hacked by foreign nations and their core source code posted on the internet for all to use.

It is ludicrous for any agency to state that any government servers, prior to 2020, were not widely penetrated and manipulated. The hackers are all known to have sold, or provided the results of their work to famous politicians for use against their competitors.

Nancy Pelosi is an owner of the hacking manipulation firm: CROWDSTRIKE. Crowdstrike and famous California Senators had the easy means, the motivations, the staffing, the resources and the known engagement of services to manipulate SSA, DOJ, SEC, FTC and other agency decisions and filing records in order to harm Plaintiffs, reporters and whistle-blowers who reported their crimes and corruptions.

(http://www.opensecrets.org/personal-finances/nancy-pelosi/net-worth?cid=N00007360&year=2011)

(
https://www.realclearinvestigations.com/articles/2020/10/09/pelosi_takes_big_stake_in_crowdstrike_democrat-tied_linchpin_of_russiagate_125557.html)

(https://dailycaller.com/2019/11/07/feinstein-fusion-gps-steele/)

(https://thefederalist.com/2018/04/27/confirmed-former-feinstein-staffer-hired-fusion-gps-christopher-steele/)

(https://en-volve.com/2018/01/11/democrats-should-question-feinsteins-mental-health-after-recent-fusion-gps-doc-release/)

(https://dailycaller.com/2017/06/24/crowdstrike-five-things-everyone-is-ignoring-about-the-russia-dnc-story/)

The hackers, daily, use the common tools of:

A. Injection. Injection flaws, such as SQL, NoSQL, OS, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.

B. Broken Authentication. Application functions related to authentication and session management are often implemented incorrectly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities temporarily or permanently.

C. Sensitive Data Exposure. Many web applications and APIs do not properly protect sensitive data, such as financial, healthcare, and PII. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data may be compromised without extra protection, such as encryption at rest or in transit, and requires special precautions when exchanged with the browser.

D. XML External Entities (XXE). Many older or poorly configured XML processors evaluate external entity references within XML documents. External entities can be used to disclose internal files using the file URI handler, internal file shares, internal port scanning, remote code execution, and denial of service attacks.

E. Broken Access Control. Restrictions on what authenticated users are allowed to do are often not properly enforced. Attackers can exploit these flaws to access unauthorized functionality and/or data, such as access other users' accounts, view sensitive files, modify other users' data, change access rights, etc.

F. Security Misconfiguration. Security misconfiguration is the most commonly seen issue. This is commonly a result of insecure default configurations, incomplete or ad hoc configurations, open cloud storage, misconfigured HTTP headers, and verbose error messages containing sensitive information. Not only must all operating systems, frameworks, libraries, and applications be securely configured, but they must be patched/upgraded in a timely fashion.

G. Cross-Site Scripting XSS. XSS flaws occur whenever an application includes untrusted data in a new web page without proper validation or escaping, or updates an existing web page with user-supplied data using a browser API that can create

HTML or JavaScript. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.

H. Insecure Deserialization. Insecure deserialization often leads to remote code execution. Even if deserialization flaws do not result in remote code execution, they can be used to perform attacks, including replay attacks, injection attacks, and privilege escalation attacks.

I. Using Components with Known Vulnerabilities. Components, such as libraries, frameworks, and other software modules, run with the same privileges as the application. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications and APIs using components with known vulnerabilities may undermine application defenses and enable various attacks and impacts.

J. Insufficient Logging & Monitoring. Insufficient logging and monitoring, coupled with missing or ineffective integration with incident response, allows attackers to further attack systems, maintain persistence, pivot to more systems, and tamper, extract, or destroy data. Most breach studies show time to detect a breach is over 200 days, typically detected by external parties rather than internal processes or monitoring.