How Gufficer The Hacker Accidentally Destroyed Silicon Valley Corruption

- GUCCIFER The Hacker Opened The Door For China To Take All Of Kleiner Perkins Political Bribery Files

- He went deep inside John Doerr's digital door and then left that door propped open for the rest of the world's hackers

- He got to gut the biggest secrets of the most famous insiders because someone else left “back-doors” in those famous people's networks

The “Guccifer” hacking spree began in late-2012 with the ransacking of e-mail accounts of Bush family members and friends. Lazar’s victims would eventually grow to include dozens of public figures, including former Secretary of State Colin Powell; CBS sportscaster Jim Nantz; authors Candace Bushnell and Kitty Kelley; billionaire venture capitalist John Doerr; journalists Carl Bernstein and Tina Brown; actress Mariel Hemingway; former Nixon aide John Dean; three members of Britain’s House of Lords; and numerous U.S. military officials, including a former member of the Joint Chiefs of Staff.

But the Lazar e-mail incursion with the most serious repercussions was his March 2013 hacking of the AOL account of Sidney Blumenthal, the Clinton family confidant.

While in control of the AOL account, Lazar (seen at left) copied Blumenthal’s e-mails, including dozens of messages sent to Hillary Clinton, who was then Secretary of State. Blumenthal’s e-mails to Clinton--many of which included detailed memos about international affairs--were not sent to her government address, but rather to hdr22@clintonemail.com.

The clintonemail.com domain was registered on January 13, 2009, as Clinton's Senate confirmation hearings were about to commence.

The revelation that Clinton used her personal e-mail account for Department of State business--and that her e-mail was housed on a “home brew” server--prompted a sprawling FBI investigation that is examining, among other things, whether classified material was improperly sent and stored via the unsecure system.

Though locked up 5000 miles away, Lazar stays abreast of U.S. events by watching CNN all day. Along with Clinton’s Iowa caucus tally, the hacker is up to speed on the Democratic presidential candidate’s e-mail travails. “Of course I know,” he said. “There are 100 FBI agents working on that server.”

Asked about his role in prompting the e-mail probe that now shadows Clinton, Lazar replied, “Yeah, it’s because of me.”

Guccifer stormed into Silicon Valley and Bohemian Club servers and opened the floodgates on John Doerr's and Eric Schmidt's bribery of White House and Department of Energy officials in order to get them to throw all of the "Green Energy Cleantech" taxpayer cash to Doerr, a felony class crime.

Guccifer claims to just be a Lulz hacker who hacks for fun but he happened to have hacked the biggest pack of political insiders and cross-dealing insiders in the world. Now, in an election year, his work may hold the biggest shockers of the American 2016 elections.

Cyber criminals focus on the super-wealthy

Hugo Greenhalgh, Wealth Correspondent

- 

©Anna Gordon

Doubles match: Potential recruits jump from site to site when considering a career move

Cyber criminals are trawling through wealth managers’ websites as well as social media networks to target the super-rich and trick them into parting with hundreds of millions of pounds a year, security experts say.

Kroll, the security group, said it had seen an increase in the number of cyber attacks against the very wealthy and those who manage their private investments. Organisations that list details of senior staff online and networking sites such as LinkedIn are being filleted by criminals to find people with board-level job titles.

-

More

On this topic

- ‘Hacker’: an imprecise term that is loaded with menace
- Analysis Surge in Israeli cyber security launches
- Investors cautious over security start-ups
- FireEye bulks up for ‘cyber arms race’

*First*FT is our new essential daily email briefing of the best stories from across the web

“The methods of attack are as varied as they are against any other commercial enterprise being subjected to cyber crime, with attacks via social media featuring prominently,” said Andrew Beckett, Kroll’s managing director.

“Individually, attacks we have investigated range from a few hundred thousand pounds in value to multimillion-pound scams. Collectively each year, this probably runs to hundreds of millions.”

The Office for National Statistics reported last year that nine in every 1,000 people had been the victim of unauthorised use of their personal information. In the UK alone, the cost of cyber crime to the national economy has been estimated at more than £30bn.

Many attacks involve hacking email accounts or creating fake ones, with criminals posing either as wealth managers contacting their clients or vice versa. Instead of old-fashioned “phishing” exercises — sending out thousands of anonymous emails in the hope of a response — criminals are specifically targeting the wealthy. “The term we use for this is ‘whaling’,” said Orla Cox, director of Symantec Security Response.

“Whereas in the past we might have seen cyber criminals go for mass attacks, they are now trying to target individuals and trick them into transferring money.”

Mustafa Al-Bassam, a former hacker who received a 20-month suspended sentence in 2013 for “computer misuse”, warned most people — rich or poor — were simply unaware of the risks of sharing their information online. “LinkedIn is a very good tool to find out people’s job titles,” he told the Financial Times. “People post a lot of publicly available information about themselves online that is very useful [for criminals].”

Special inspector James Phipson, commercial director of the Economic Crime Directorate at City of

London Police, said wealth managers and similar roles in the financial services industry had become particular favourites.

In depth

Cyber warfare

As online threats race up national security agendas and governments look at ways of protecting their national infrastructures a cyber arms race is causing concern to the developed world

But, he added, the nature of the super-wealthy had changed. For instance, he said: “There are some pensioners, now with [full] access to their pensions, who have enormous amounts at their disposal”.

In one instance, Mr Phipson said, a victim’s email account was cloned and funds were transferred on instructions sent from that address without the victim or his wealth manager knowing anything about it.

Neil Deakin, compliance manager at Brooks Macdonald, the Aim-listed wealth manager, said the firm had noticed a rise in attacks on its clients’ email accounts. “We are receiving quite a lot of fraudulent requests to withdraw money out of their investment account to their bank account purporting to be in their own name — or to go to cash businesses like Western Union,” he said.

Liz Field, chief executive of the Wealth Management Association, said the scale of the problem heightened the need for companies to report cyber crime. “We all need to be more alert to the severity of this threat,” she said. “As the UK is an international hub for financial services, we are a very desirable target.”

LinkedIn said it always investigated suspected violations of its terms of service, including the creation of false profiles, and took immediate action when violations were uncovered.

Related Topics

- Cyber Security,
- United Kingdom,
- Wealth Management,
- Data protection