1.2 BILLION INTERNET CREDENTIALS DISCOVERED IN THE HANDS OF RUSSIAN CRIME RING

MARITZA SANTILLAN

AUG 5, 2014

Security researchers have reportedly found the largest collection of Internet username credentials, including passwords and more than 500 million email addresses.

According to researchers at Hold Security, the defrauded collection was found in the hands of a Russian crime ring with data gathered from about 420,000 different websites.

The collection has been confirmed to be authentic, but victims and affected companies have not been unveiled due to nondisclosure agreements.

Founder and CISO of Hold Security Alex Holden said, “Hackers did not just target U.S. companies, they targeted any website they could get, ranging from Fortune 500 companies to very small websites.” Holden warned that most of the websites compromised still remain vulnerable, making it possible for cybercriminals to continue exploiting the vulnerabilities to extract data.

As of now, it appears that the cybercriminals have sold few personal records, but are using the information to send spam on social networks paid for by other cybercrime groups.

Holden reported the Russian hackers were able to attain the billions of records by essentially “auditing the internet,” using malicious botnets to infect computers. According

to the New York Times report, when infected users visit a website, criminals command the botnet to test for vulnerabilities to SQL injection.

“The hacker enters commands that cause a database to produce its contents. If the website proves vulnerable, criminals flag the side and return later to extract the full contents of the database.”

Tripwire security researcher Ken Westin said, “This discovery is another example of how hacking is a business with your personal data as the currency. Hacking groups are finding ways to monetize compromised accounts, credit cards and other data making it a full-time job and not just a hobby for an individual. As groups become more well-funded and find a lucrative niche in the hacker ecosystems their capability also increases.”

Hold Security has begun alerting the affected organizations, but have not been able to successfully contacted every website. The security firm has previously uncovered various other renowned large-scale hacks, such as Adobe System’s massive breach in 2013.