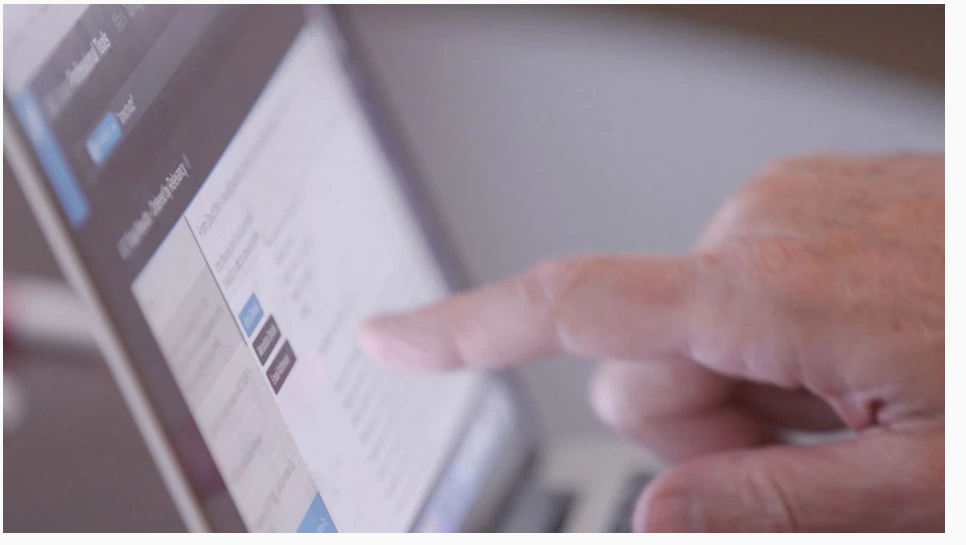
BUSINESS › TECHNOLOGY

Defense agencies top list of U.S. government with stolen data on darknet, Denver company finds

Denver's Owl Cybersecurity finds U.S. Navy has largest footprint on darknet



Vince Chandler, The Denver Post

Owl Cybersecurity monitors the darknet.

By **TAMARA CHUANG** | tchuang@denverpost.com | The Denver Post
August 8, 2017 at 6:11 pm

The Darknet Index: U.S. Government Edition

Ranking U.S. government agencies using darknet intelligence

Introduction

One measure of cybersecurity risk involves assessing how much data is available on the darknet about a company or organization that can be misused by hackers or criminals. A greater availability of data implies a higher risk profile, as more attack vectors are available for use against the organization.

OWL Cybersecurity recently reranked the companies of the Fortune 500 based on their darknet footprints[1]. We then ranked the largest commercial entities in Germany[2].

In this report, we address how prominent U.S. government agencies, departments, and the U.S. military fare on the darknet as compared to commercial enterprises. We examine 59 large divisions of the U.S. Government to see whether they have a markedly different darknet footprint than the Fortune 500. Unfortunately, the results reveal that the U.S. Government has the largest collective darknet footprint of all of our darknet indices.

By comparing how much compromised data was available on these numerous private networks, forums and channels, and running this information through our proprietary algorithm, we reached some key takeaways about the differences and similarities between the U.S. Government and large U.S. commercial entities.

Intelligence gained from monitoring the darknets (Tor and other interconnected sources including IRC, I2P, ZeroNet, other hacker forums), as well as FTP servers, select paste sites, high-risk surface internet sites and more, constitutes what OWL Cybersecurity calls DARKINT™, or darknet intelligence. These locations attract threat actors seeking to safely sell, purchase or expose stolen data.

1. https://www.owlcyber.com/owl-cybersecurity-darknet-index
2. https://www.owlcyber.com/german-darknet-index

TABLE OF CONTENTS

OWL CYBERSECURITY OWLCYBER.COM 303-376-6265

Read the OWL Cybersecurity Darknet Index: U.S. Government edition

U.S. defense agencies ranked higher than non-defense agencies for the amount of stolen data available in the online underworld where cyber criminals often hawk stolen credit cards, according to a new report by Denver's Owl Cybersecurity.

From employee passwords to intellectual property, the amount of compromised data surprised Owl cyber sleuths who analyze data captured from private networks known as the darknet. Data linked to the U.S. Navy, U.S. Army and Department of Defense had the three largest footprints on the darknet, though they were smaller than those of some major corporations scored in an earlier study.

"It wasn't a surprise that it was out there. But what was surprising was the volume of data out there. It was also surprising that defense (agencies) had the highest amount," said Andrew Lewman, Owl's vice president who previously worked as executive director the Tor Project. "They're very good at protecting our shores. … But they're not so great about protecting their credentials."

In many cases, defense workers reused work email addresses and passwords across military and personal accounts, like Pinterest, he said.

The U.S. Navy has not responded to a request for comment.

Owl, which helps customers secure their systems, said that it shared the results with the government agencies before the report became public on Tuesday. Some agencies expressed interest in learning more, he said.

Overall, 59 U.S. government agencies had compromised data on the darknet. By comparison, non-defense units like the Office of Personnel Management ranked at number 27. The same office had a massive data breach in 2015, when 21.5 million current and former federal government workers learned that Social Security numbers, fingerprints and other personal information were stolen.

And in an earlier Owl report of Fortune 500 companies, Amazon topped the list with a "Darknet Index Score" of 19.16. That score tallies up total compromised data, its frequency and a proprietary "Hackishness" rating. Amazon also outscored the U.S. Navy, which had a score of 16.59.

To protect your own data, Lewman said sign up for credit monitoring if your data was compromised. And don't use the same password for everything — use a password manager to create longer, complicated passwords.

"The enemy only needs one way in and they'll take whatever they can get," Lewman said.

TAGS: **CREDIT CARDS**, **CYBERSECURITY**, **DEPARTMENT OF HOMELAND SECURITY**, **HACKING**, **INTERNAL REVENUE SERVICE**, **MORE BUSINESS NEWS**, **SOCIAL SECURITY**, **U.S. ARMY**, **U.S. DEPARTMENT OF JUSTICE**, **U.S. NAVY**, **VETERANS**

Tamara Chuang

Tamara Chuang covers personal technology and local tech news for The Denver Post. She loves figuring out how things work and explaining them either through words, graphics or video. Find out how to contact her at dpo.st/tamara

Follow Tamara Chuang **@gadgetress**