ISCANN GROUP EXAMINES OPEN SOURCE INTELLIGENCE THREATS TO NATIONAL SECURITY

WHITEPAPER: OSINT THREATS TO NATIONAL SECURITY

LONDON, UNITED KINGDOM, March 3, 2021 /EINPresswire.com/ -- IScann Group, an open-source intelligence agency that enables companies to counter an array of modern threats,

ISCANN | GROUP

IScann logo

today announced the release of its whitepaper - OSINT Threats to National Security, researched and written by its Senior Advisor, Rich Coyne. The paper provides an in-depth examination of how the aggregation of seemingly innocuous online data presents a significant deception risk for people who handle sensitive technologies destined for national security purposes.

> "
>
> Many of these high-level, well-hidden people may be readily exploited as an entry vector for attackers to acquire sensitive material."
>
> *Andrew Vasko, Managing Director of IScann Group*

Remote penetration of networks (or "hacking") is nothing particularly new, with attempts to gain access to enemy networks having occurred for decades. A more recent threat, however, has arisen with mass public adoption of the internet and the proliferation of both personal and professional data. Thus, it has become easy via OSINT ("Open Source Intelligence") to identify persons with access to the information that the attacker needs – an attacker who may achieve their aims through deception or outright

coercion at little to no cost.

The whitepaper provides a series of case studies exhibiting the ease and very serious threat that cyber espionage holds, particularly when it comes to military personnel and as a result, national security. It highlights how spear-phishing is used to identify the weakest link in a company; coercion and blackmail through the dark web are used to exploit staff in the military supply chain; and how top, private military personnel can be identified from the digital shadow of the people closest to them.

"Rich Coyne has brought to light the issues of how simple it is to acquire concealed data through

open-source, passive means. Many of these high-level, well-hidden people may be readily exploited as an entry vector for attackers to acquire sensitive material. This is a severe risk and an issue that is important for every company big or small to take seriously, especially as it is increasingly evident that the national security secrets of tomorrow are the corporate intellectual property of today," says Andrew Vasko, Managing Director of IScann Group.

The body of open source-accessible data available to organisations and staff will only grow exponentially over time. The tools and know-how to access the data will also become more readily available. There are opportunities for mitigation, including proactively searching for vulnerabilities in one's own organisation and awareness training of personnel digital footprints and digital shadows.

For more information visit www.iscanngroup.com

--END--

About IScann Group

IScann Group is an open-source intelligence service that enables companies to understand and counter an array of modern threats. By utilising proprietary methodologies, the Group monitors global security trends, tracks social media and is at the forefront of exploiting digitalisation. The group is managed by Andrew Vasko.

More information: www.iscanngroup.com

Media Contacts

REDHILL (for IScann Group)
Tien Ma
tien@redhill.world

Tien Ma
REDHILL
email us here