NAWA Media

Online Threats to Journalists: Case Study

Section: 3.3

Online Threats for Journalists

Research by UNESCO reveals how media practitioners across the world face the threat of surveillance, software and hardware exploits without the knowledge of the target phishing attacks, intimidation, harassment, disinformation and smear campaigns, and data storage and mining.

Link to the report:
unesdoc.unesco.org/ark:/48223/pf0000232358

Online Threats for Journalists: Case Study

"Journalists might also be targeted with a 'zero day attack' – when an adversary exploits a vulnerability in software or hardware when there is no prior knowledge of the flaw in the general information security community, and therefore no fix or software patch available yet. This is done to gain access to a target's device in order to deliver malware. Once an adversary has access to someone's computer, he or she can then install software to monitor the communications on that computer, such as keystroke logging, remote webcam/microphone access, email monitoring, file extraction, etc. It also allows the attacker to bypass encryption. This is especially important given the increase in encrypted traffic over recent years."

Link to the report:
unesdoc.unesco.org/ark:/48223/pf0000232358

Online Threats for Journalists: Case Study

"Journalists and news organizations can be targeted for surveillance through phishing or spearphishing campaigns. These targeted 'phishing' or 'spearphishing' campaigns often use links or attachments laden with malware that are sent via email or social media. Although malware differs in its capabilities, one of the most malevolent forms of malware that has been known to affect journalists' work is a Remote Access Trojan (RAT). The more sophisticated a RAT is, the more likely it is to avoid detection by anti-virus software. If clicked on or downloaded, these RATs allow the attacker to gather anything they want on the compromised computer. 'If the computer can do it for you, they can make it do it for them, or work differently for their needs, like re-routing traffic for a Man-in-the-Middle attack,' says Seamus Tuohy. Other times, these attacks take the guise of a fake domain (website). The site silently collects account information that the journalist enters on the site, thinking that it is legitimate."

Link to the report:
unesdoc.unesco.org/ark:/48223/pf0000232358

Online Threats for Journalists: Case Study

”A common phishing attack is when a journalist receives an email that appears to be from someone they know. It might be from a familiar email address and/or written as if it comes from an acquaintance. This fraudulent correspondence then lures the recipient into clicking on a link or an attachment that downloads malware onto his or her computer. According to Bill Marczak, a researcher with Citizen Lab and a doctoral candidate in computer science at University of California, Berkeley in the USA, journalists assisted by Citizen Lab researchers continued to be repeatedly targeted via attachments, despite warnings from researchers at Citizen Lab to open attachments only in the cloud (such as offered via several webmail service providers). Marczak believes that harm could be reduced by 85 per cent if journalists would stop directly opening attachments.”

Link to the report:
unesdoc.unesco.org/ark:/48223/pf0000232358

Online Threats for Journalists: Case Study

"Phishing campaigns and the subsequent installation of surveillance technology on a journalists' device can:

- Compromise a journalist's personal information, data and sources often without the journalist ever finding out,
- Result in blackmail by misuse of personal information, and
- Lead to self-censorship."

Link to the report:
unesdoc.unesco.org/ark:/48223/pf0000232358

Online Threats for Journalists

Whistle-blower Edward Snowden revealed how the National Security Agency (NSA) of the US had a surveillance programme to tap into the telephonic conversations of citizens in the name of security. Snowden lives in Moscow and faces espionage charges in the US, where after seven years the US Court of Appeals has ruled that the surveillance programme was illegal.

These programs can be used to surveil and monitor journalists working on stories and journalism that is critical of the state. Surveillance can put the safety of their colleagues, family and friends in addition to themselves at risk. Surveillance or threat of surveillance is also known to result in self-censorship.

Furthermore reading: “Journalism After Snowden: The Future of the Free Press in the Surveillance State”, Edited by Emily Bell and Taylor Owen. With Smitha Khorana and Jennifer R. Henrichsen, Columbia University Press, 2017.

NAWA Media

In the **next** section, we will emphasize the importance of backing up data!

BCMCR | Birmingham Centre for Media and Cultural Research

BIRMINGHAM CITY University

MEEDAN

Check

Sida