Proliferation of Foreign Commercial Spyware Drives Increasing Counterintelligence Risk

Market-leading foreign commercial spyware firms sell advanced capabilities worldwide, including to hostile foreign governments, which have used these technologies to target U.S. interests. Foreign governments purchase these spyware tools because they are often more affordable and effective than what governments can develop indigenously. Some spyware firms try to evade scrutiny and resist diplomatic, economic, and legal efforts to constrain their activities.[a]

Advanced Capabilities

Spyware developed by these firms provides the capability to collect audio, data, and location information from targeted devices. It infects devices using either one-click tactics that entice the victim to click on a malicious web link or download a malicious application or by using zero-click methods that require no victim interaction. Spyware and supporting infrastructure evolve in response to software updates from device vendors and evade detection by antivirus software, device users, and forensic analysis. Some civil society groups have been able to glean technical insights into the tools by analyzing targeted devices.

Opaque Controls

Some firms claim to vet potential clients and investigate allegations of misuse to mitigate the risks of their technology being misused to undermine human rights. Other firms claim no ability to investigate based on a lack of backdoor access to the system once installed. In addition, some firms claim to restrict their customers' ability to target U.S.-registered phone numbers and devices located in the United States.

Obfuscated Business Practices

Some firms take advantage of complex business structures to mask their activities and insulate their operations against government action by using global resellers, shell companies, and subsidiaries.

Access to Capital

Some firms have attracted capital from private investors, venture capital firms, and existing technology or security corporations looking to expand into new markets.

Civil Society Groups Offer Insight

Civil society groups have done significant work documenting the proliferation of commercial spyware, resulting in a body of knowledge readily available to the public.

[a]The term "commercial spyware" is defined here as per Executive Order 14093, "Prohibition on Use by the United States Government of Commercial Spyware that Poses Risks to National Security." This report does not address commercial lawful intercept capabilities, geolocation systems, or intercept devices for wireless networks.

Proliferation of Foreign Commercial Spyware Drives Increasing Counterintelligence Risk

COUNTERINTELLIGENCE RISKS

U.S. officials and citizens abroad face the risk that foreign powers—some without indigenous technical intelligence expertise—could use commercial spyware capabilities to target their locally registered devices. Foreign powers may seek to use collected data for intelligence recruitment purposes, to jeopardize the safety of government personnel, or to undermine other U.S. equities. Moreover, developments in artificial intelligence (AI), including generative AI, will exacerbate the counterintelligence threat, allowing foreign governments to be more sophisticated in their deployment of spyware capabilities. Incorporating AI into their products may allow spyware developers to better and more rapidly deploy new products and product versions capable of exploiting a broader range of victims. Advancing generative AI capabilities may allow firms to easily customize products for users and rapidly craft and deploy highly targeted lures.

MITIGATION BEST PRACTICES

The Intelligence Community has published best practices and recommended actions that individuals, including U.S. Government employees, can take to partially mitigate the threat from commercial spyware. Mitigation steps include keeping devices updated; regularly restarting them; disabling location tracking; always behaving as if the device is compromised; and being mindful of sensitive content, even in encrypted messaging applications.

For further information, please see the following publications:

ODNI

Protect Yourself: Commercial Cyber Intrusion Tools

https://www.dni.gov/files/NCSC/documents/SafeguardingOurFuture/FINAL_Jan-7-2022_Protect_Yourself_Commercial_Surveillance_Tools.pdf

NSA

Mobile Device Best Practices

https://media.defense.gov/2021/Sep/16/2002855921/-1/-1/0/Mobile_Device_Best_Practices_FINAL_V3%20-%20copy.pdf

Cyber Threat Intelligence Integration Center (CTIIC)

CTIIC analyzes and integrates cyber intelligence for decisionmakers so they can act on the identified threats. CTIIC works closely with the National Security Council, National Intelligence Council, and partners across the IC.

Visit our website at www.dni.gov/ctiic