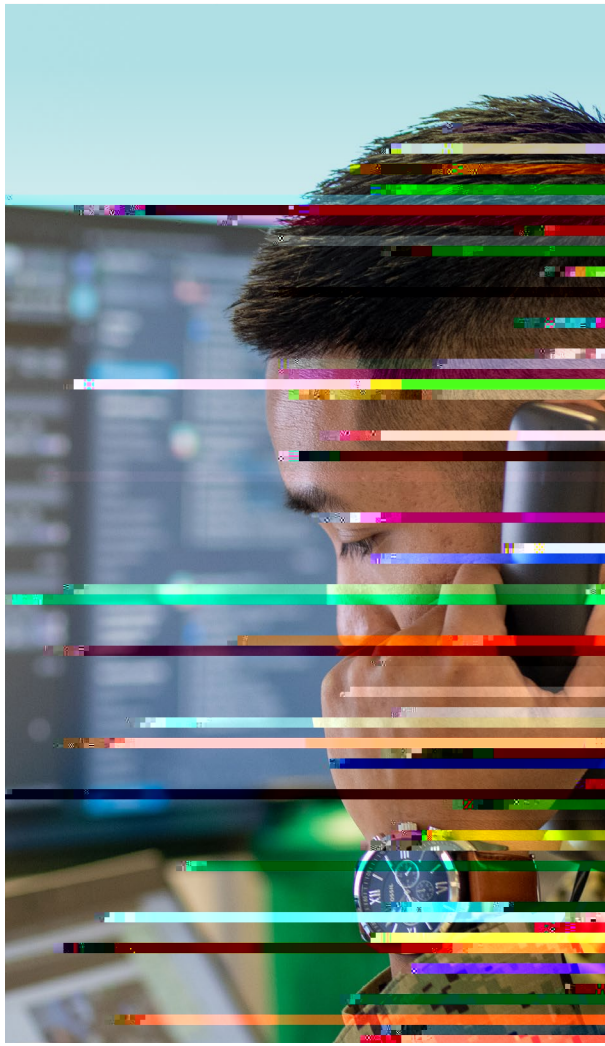
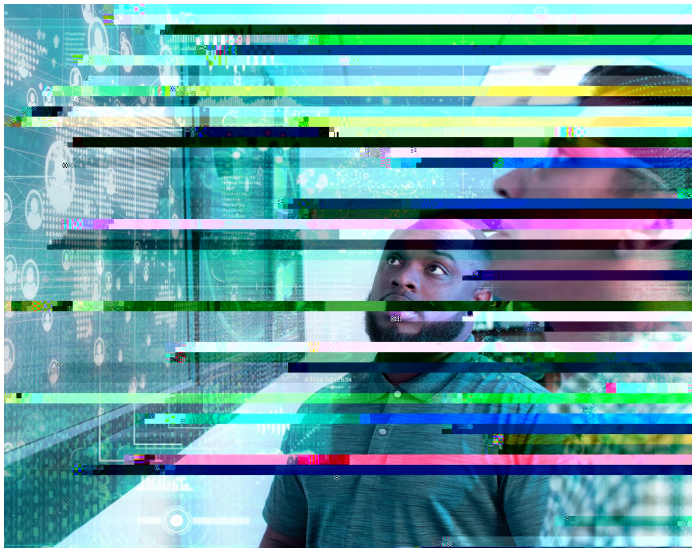

B ILDING MI ION-DRI EN

# BUILDING MISSION-DRIVEN 5G SECURITY WITH ZERO TRUST





| NETWORK EFFECTS | INITIAL ACCESS | CREDENTIAL ACCESS | PERSISTENCE | PRIVILEGE ESCALATION | LATERAL MOVEMENT | COLLECTION | IMPACT |
|---|---|---|---|---|---|---|---|
| o f ce, a sophisticated threat actor gains access to a nearby 5G small cell and confgures the small cell to enable 4G spoofng, which allows the attacker to downgrade the attached devices to a more vulnerable 4G technology and exploit legacy SS7/Diameter vulnerabilities. | Using intelligence gains from espionage, the malicious actor secretly modifes legitimate 5G software used by government and industry, resulting in a software supply chain compromise. This advances a scheme to undermine U.S. defense capabilities. | To further undermine a misconfgured standalone 5G network, the threat actor exploits a packet fow control protocol (PFCP) vulnerability to redirect / intercept communications—with the added power to delete session data or deny service at will. The enemy steals credentials. | Aiming to exploit vulnerabilities in order to craft attack vectors through the attack surface to reach assets, the attacker compromises credentials, gaining access a virtual machine (VM) on the core cloud, part of a customized virtual network function (VNF). | The adversary, an expert at crafting attack vectors on 5G architecture, conducts a hypervisor/ container breakout to gain access to the underlying virtual resources, and subsequently the other underlying infrastructure used by a defense contractor. | The adversary pivots to the underlying host infrastructure used by a defense contractor to steal and manipulate sensitive data. | The adversary is postured to scrape sensitive data,pivot to other infrastructure components, or disrupt/degrade the environment Ă ` ʐ o The adversar Ă ` ʐ oe r̃ aul " ] ɹ manipu ` ar˜ Ml " $ " ^ ` ʐ odB sgne = l e l l' ṅ e t | |

## ENDNOTES:

U.S. President, Executive Order, "Executive Order 14028 of May 12, 2021," Federal Register Vol. 86, no. 93 (May 17, 2021), https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity; U.S. National Security Agency, Embracing a Zero Trust Security Model (Maryland, 2021), https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.pdf

U.S. Department of Defense, Department of Defense 5G-Strategy Implementation Plan (Washington, DC, 2020), https://www.cto.mil/wp-content/uploads/2020/12/DOD-5G-Strategy-Implementation-Plan.pdf

Ibid.

Ibid.

[5] U.S. Government Accountability O f ce, Internet of Things: Enhanced Assessments and Guidance Are Needed to Address Security Risks in DOD, GAO-17-668, (Washington, DC, 2017), https://www.gao.gov/products/gao-17-668

U.S. Government Accountability O f ce, 5G Wireless: Capabilities and Challenges for an Evolving Network, GAO-21-26SP, (Washington, DC, 2020), https://www.gao.gov/products/gao-21-26sp

[7] Ibid.

## About Booz Allen

BoozAllen.com/5G