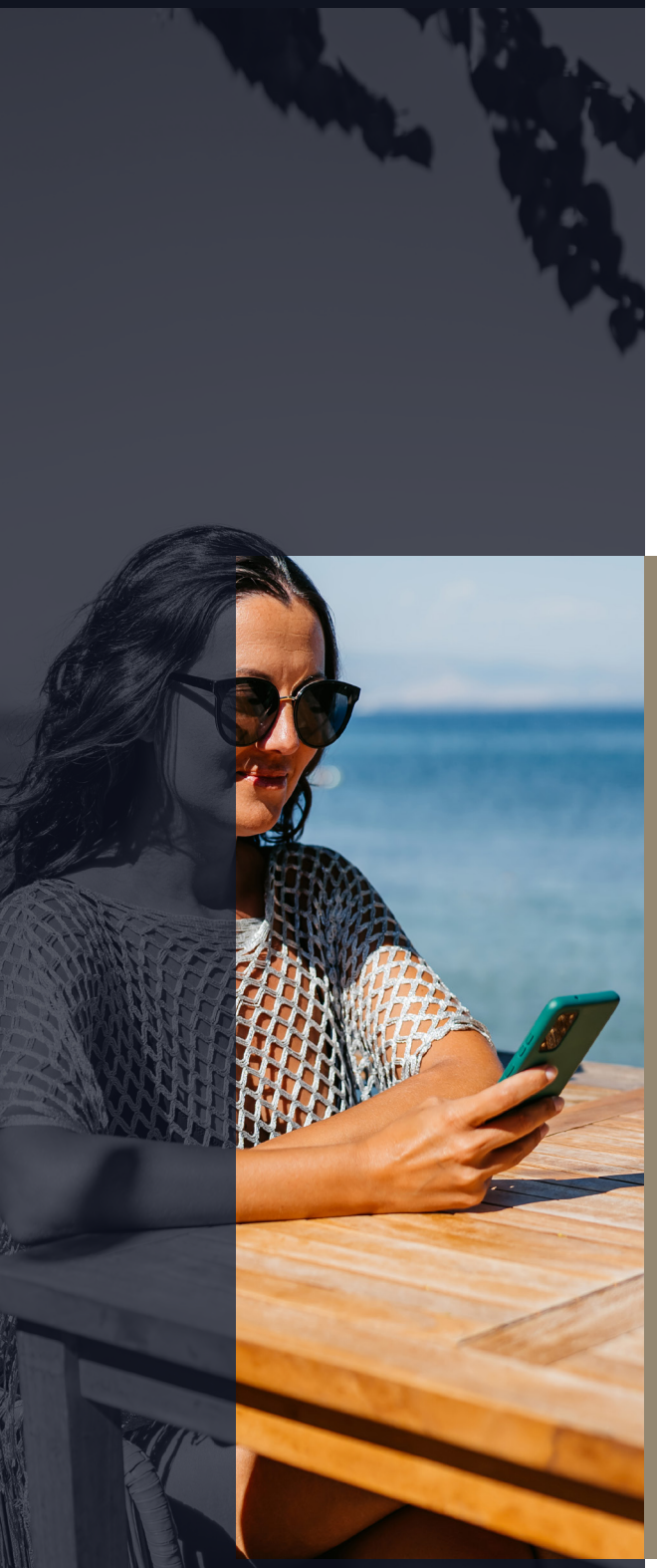
BLACKCLOAK®

Cyber Paradise Lost

BlackCloak Discovers Critical Vulnerabilities at Tropical Haven

Leading Cybersecurity Firm to High-Net-Worth Clients Sounds the Alarm on Severe Vulnerabilities Lurking on a Paradise Island



In the heart of this affluent island community where billionaires, celebrities, athletes, and politicians outnumber the miles of pristine coastline, a silent threat is lurking.

BlackCloak, uncovered disturbing vulnerabilities through its specialized vulnerability scanning of a client's home network (aka penetration testing). What was a retreat for the rich and famous has become a digital battleground of equipment forbidden from the U.S., an open island infrastructure,and even potential weaknesses that might affect sea-going travel.

Here, the elite find their lives unknowingly vulnerable to malicious cyber activities as they drop anchor in harbors far removed from the safeguards and high standards of security they are accustomed to in their home nations.

BlackCloak's Intelligence and Threat Hunting Teams Sounded the Alarm

"The wealthy and influential often find themselves in remote locales, which can take them outside of the protective bubble of their home nations. This weakness hasn't escaped the notice of cyber criminals and foreign adversaries who intentionally exploit these gaps to wreak digital havoc,"
said **Daniel Floyd**, Chief Information Security Officer at BlackCloak.

Threat Actors can probe the defenses of the rich and powerful, searching for cracks in the armor from anywhere, whether it's a line of-site Wi-Fi vulnerability from a passing boat or an over-the-horizon attack from the other side of the globe. Each yacht and villa forms part of an open network, easily exploitable, individually named, and significantly escalating the risk of intrusion and surveillance of private communications.

BlackCloak's Threat Intelligence Team Skillfully Unveiled the Achilles' Heel of this Island Nation

There are two additional aspects of this situation that are unique.

01. First, these vulnerabilities can take on greater significance considering the prevalence of less secure equipment otherwise prohibited in the United States. Unaddressed equipment flaws can pave the way for unauthorized entry, data leaks, and critical service interruptions.

02. And second, the use of a shared IP address on a network loop in private communities and popular vacation spots further intensifies privacy risks. Wealthy individuals inevitably become coveted targets, especially in small enclaves where they are less able to blend in, jeopardizing both their personal and professional lives.

Uncovering a Critical Weakness

During a vulnerability assessment into a “High-Value-Target”member’s residence at their overseas community, BlackCloak discovered a critical weakness in a networking device that delivered all of the Internet services to the entire island community, their yachts, and other communication points. The silver lining is that our team found the misconfigurations and architecture design problems and was able to responsibly disclose the weaknesses, risks, and potential solutions. The networking device provided the entire island with “last mile” fiber to home (FTTH) connections driving internet connectivity including voice, data, and video services that spanned multiple residents, the central club facility, private dock slips, and potentially a navigation system. Altogether, the threats found allowed any malicious actor or nation state the opportunity to compromise not only the families on the island, but also their corporate networks or data if malware was able to be deployed.

Conducting Comprehensive Scans

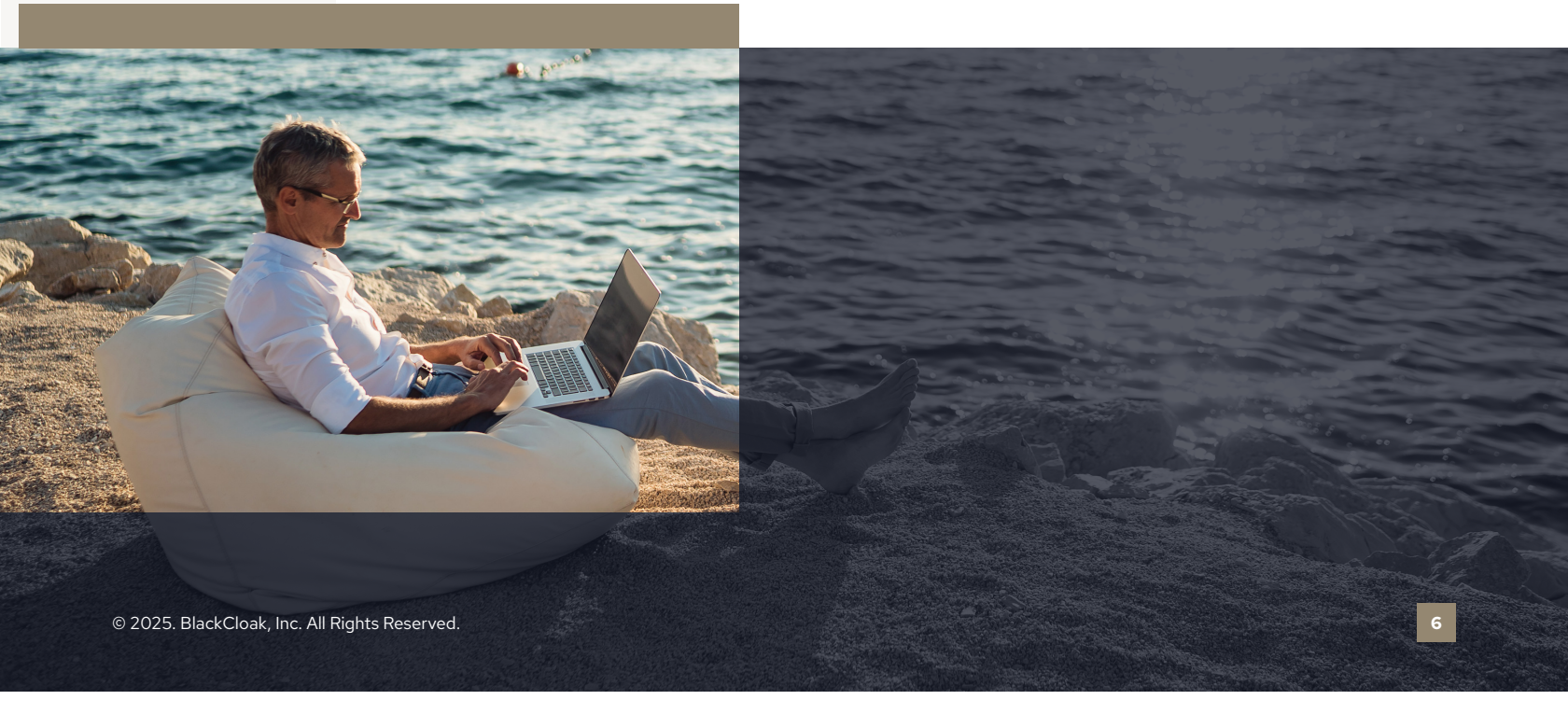
In our investigation, BlackCloak conducted comprehensive network scans of the member’s residence public IP address. This examination revealed open TCP Ports 443, 2343, and 10000. Further scrutiny with service-level discovery scans revealed that TCP port 2343 harbored a telnet daemon linked to a Chinese-made GPON (Gigabit Passive Optical Network) switch/router. This crucial networking device, functioning as both a layer 2 switch and layer 3 router catered not only to the member’s home but potentially served other residences. The results returned data that disclosed not one large home network, but rather dozens of homes and yachts all tied together on one flat network and configuration files that referenced names of many potential owners

Finding U.S.-Banned Networking & Security Devices

Another noteworthy detail emerged during the scans - the networking device, recently banned by the U.S. Federal Communications Commission, was in commonplace use on this island and potentially other islands and communities in other locations. While there were architecture problems with the island network and substantial misconfiguration issues with the device, the fact that a device controlling traffic for F100 executives was unexpected. All in, this essentially equated to a lowered drawbridge complete that could be exploited not just by cybercriminals, but by nation-state intelligence agents as well.

Potential Access to Private Data

Sadly, the team was able to penetrate the home of its client by using default scanning techniques part of CWE-1392: Use of Default Credentials. This entailed detecting and utilizing the device's default credentials to authenticate access to what was believed to be one client home. The BlackCloak team successfully infiltrated the telnet daemon, gaining entry to the network and began its client alerting and remediation process. Unbeknownst to the team, the network device held a trove of data beyond what was expected - encompassing full resident names, address information, ship vessel details, and even dock slip numbers.



Mitigating Further Risks

Given the potential risks to its client and as it turns out other new clients to the island community, the decision to act to disclose the event was immediate. Moreover, given the potential connection of architecture to seagoing navigation systems, the team needed to ensure responsible disclosure was effective. The prospect of cybercriminals being able to seize control of the entire network could have had wide-ranging consequences including:

Traffic Dumps and Network Sniffing: Exploiting the device's support for monitor ports and traffic captures, an attacker could orchestrate a comprehensive traffic dump, intercepting and collecting all data flowing through a VLAN or port. From eavesdropping on voice communications transmitted through VoIP phones to capturing unencrypted web traffic and email exchanges, the attacker gains an unsettling window into sensitive information.

Traffic Routing: Armed with layer 2 and layer 3 access, an attacker can manipulate end-user traffic, redirecting it through malevolent networks, proxies, or VPNs. This enables them to engage in spoofing, sniffing, intercepting, and tampering with data or launching targeted attacks against vulnerable end-user devices.

Endpoint Malware: Capitalizing on their control over traffic routes, DNS, and DHCP, an attacker can implant malware. They gain direct access through enabled services like SSH, SMB, or RDP. Alternatively, they exploit Man-in-the-Middle (MiTM) and other redirection tactics, deceiving users into unwittingly installing malicious software that can wreak havoc.

DHCP Attack: Leveraging their dominance over the compromised networking device, an attacker can manipulate DHCP server settings, tampering with DNS configurations, routes, and other network options assigned to connected devices. This surreptitious control can enable various forms of data manipulation and interception.

Traffic Dumps and Network Sniffing: Exploiting the device's support for monitor ports and traffic captures, an attacker could orchestrate a comprehensive traffic dump, intercepting and collecting all data flowing through a VLAN or port. From eavesdropping on voice communications transmitted through VoIP phones to capturing unencrypted web traffic and email exchanges, the attacker gains an unsettling window into sensitive information.

Traffic Routing: Armed with layer 2 and layer 3 access, an attacker can manipulate end-user traffic, redirecting it through malevolent networks, proxies, or VPNs. This enables them to engage in spoofing, sniffing, intercepting, and tampering with data or launching targeted attacks against vulnerable end-user devices.

Endpoint Malware: Capitalizing on their control over traffic routes, DNS, and DHCP, an attacker can implant malware. They gain direct access through enabled services like SSH, SMB, or RDP. Alternatively, they exploit Man-in-the-Middle (MiTM) and other redirection tactics, deceiving users into unwittingly installing malicious software that can wreak havoc.

DHCP Attack: Leveraging their dominance over the compromised networking device, an attacker can manipulate DHCP server settings, tampering with DNS configurations, routes, and other network options assigned to connected devices. This surreptitious control can enable various forms of data manipulation and interception.

Safeguarding the Elite: A Mandate for Diligence

BlackCloak proactively collaborated with the IT administrator and with the community management firm to solve the vulnerability, discussed the risks of its flat architecture network loop for all residents, yacht slips, and navigational equipment, and was able to alert our corporate client CISO/CSOs of the risks to their executives. Further testing confirmed that the device in question could no longer be accessed after the credentials were changed and also that our clients' homes were in a safe state. The scenario encountered during the penetration test, unfortunately, is not unique to the exotic island location but can occur in any country with an immature cybersecurity infrastructure, regardless of the exclusivity of the community.

While BlackCloak successfully mitigated the critical risk, addressing cybersecurity issues in areas with less robust standards requires a multifaceted approach.

To address future challenges, members are counseled on how to exercise heightened diligence when traveling or on remote networks, and BlackCloak leads the way to collaborate with other technology companies and authorities to create a culture of cybersecurity vigilance. A collective effort raises awareness of operational security (OPSEC) best practices to foster cybersecurity ecosystems that can transcend national boundaries.

The home is the new battleground. It has always been a weakness exploited by cybercriminals and nation-states, but what our team has been discovering more and more are fundamental weaknesses in the overall security posture of the world's wealthiest individuals.

Recommendations for CISOs and CSOs

It remains a challenge for CISOs and CSOs to mitigate the security risks associated with executive and board members' home security systems when they are visiting vacation homes outside of the United States. There are three key approaches:

01. An essential first step is to conduct a risk assessment that considers the local security landscape, geopolitical risks, and the infrastructure of the nation.

02. Second, ensuring the home network is architected correctly, network and smarthome systems are updated and secured, and home systems cannot be accessed externally is critical.

03. Finally, since most home networks and cameras can be controlled via mobile devices, security leaders should encourage executives and board members to secure their personal devices with biometrics or strong passwords, multifactor authentication, and keep them updated with the latest operating system/security patches.

BLACKCLOAK®

BlackCloak secures the personal digital lives of corporate executives, high-net-worth individuals, and their families. We tailor our cutting-edge technology, expertise and support to protect clients from evolving threats, safeguarding reputations, finances, and peace of mind in an increasingly connected world. Used by Fortune 500 companies, recommended by wealth management firms, and trusted by private family offices, the BlackCloak Platform is an award-winning holistic cybersecurity solution, complete with 24/7 personalized support. With BlackCloak, executives and high-profile individuals get peace of mind knowing their family, privacy, reputation, and finances are secured, while CISOs and CSOs can be confident that their people, brand, intellectual property, data, and finances are protected without invading their executives' personal lives.

Learn more at www.blackcloak.io

@BlackCloakCyber

BlackCloak

info@blackcloak.io

www.blackcloak.io