BlueVoyant

CASE STUDY:
EXTERNAL VULNERABILITY ASSESSMENT

Defense in Depth starts at the perimeter

1. MALICIOUS OUTSIDERS ARE CONSTANTLY LOOKING FOR HOLES

Attackers are constantly checking if the front door is unlocked and the windows are open. Automated scanning and exploitation tools are rapidly developed for new internet facing vulnerabilities.

2. NETWORKS ARE NO LONGER STATIC AND ENCLOSED

As businesses maximize the value of the connected world, they are also opening themselves up to more vulnerabilities. With cloud migrations, changes in network topology, and product upgrades, organizational networks are constantly changing.

3. EDGE VULNERABILITIES POSE A SIGNIFICANT RISK

Footholds in organizations enable malicious outsiders to conduct fraudulent activities which may go unnoticed. From proxies for malicious traffic to dynamic redirects on compromised websites, attacks continue to innovate monetization of unauthorized access at the expense of the organization.

EXTERNAL VULNERABILITY ASSESSMENT

Our external vulnerability assessments identify the security weaknesses of which attackers will take advantage in your publicly facing networks, systems, and applications. Vulnerabilities are prioritized based on criticality with detailed descriptions of impact and affected hosts. When paired alongside our MSS offering, the external vulnerability assessment adds organizational context to event detection and resolution while highlighting network segments which will benefit from customize detection and analytics.

Critical
Issue indicates a vulnerability whose exploitation will lead to direct and immediate access to sensitive or critical internal resources; degradation or inaccessibility to critical resources for an extended period of time.

High
Issue indicates a vulnerability whose exploitation will lead to direct or indirect access to sensitive or critical internal resources; degradation or inaccessibility to critical resources for a period of time.

Medium
Issue indicates a vulnerability whose exploitation has the potential to provide direct or indirect access to sensitive or critical internal resources; degradation or inaccessibility to critical resources for a period of time.

Low
Issue indicates a vulnerability whose existence will degrade currently implemented security mechanisms.

Risk Rating: High	**Open SSH MaxAuthTries Bypass**
Description of Risk	The remote SSH server is affected by a security bypass vulnerability due to a flaw in the keyboard-interactive authentication mechanisms. The kbdint_next_device() function in auth2-chall.c improperly restricts the processing of keyboard-interactive devices within a single connection.
Potential Impact	A threat actor can exploit this vulnerability, via a crafted keyboard-interactive devices string, to bypass the normal restriction of 6 login attempts (MaxAuthTries), resulting in the ability to conduct a brute-force attack or cause a denial of service condition.
Affected Host(s)	[HOST6]; TCP Port [PORT]
Recommendation	Upgrade to OpenSSH 7.0 or later. Alternatively, this vulnerability can be mitigated on some Linux distributions by disabling the keyboard-interactive authentication method. This can be done on Red Hat Linux by setting ChallengeResponseAuthentication to no in the /etc/ssh/sshd_config configuration file and restarting the sshd service.

CASE STUDY

Client Challenges

A small client engagement was affected by a ransomware attack and realized the need for updated security measures. While upgrading to our managed SIEM offering, the organization also wanted to validate perimeter security.

Approach

Unknown Vulnerabilities Discovered
Our vulnerability scans identified 3 high vulnerabilities in externally facing servers.

Enhanced Detection

As new detection controls were implemented, additional focus was given to vulnerable network segments.

Results

The organization discovered their externally facing website was compromised and embedded with a malicious code snippet which redirected users to malicious websites. The organization was able to resolve the issue before any damage was cause to their business or reputation.

For more information please visit:
www.bluevoyant.com

Secure your business now:
sales@bluevoyant.com

About BlueVoyant

BlueVoyant is an analytic-driven cybersecurity company whose mission is to protect businesses of all sizes against agile and well-financed cyber attackers by providing unparalleled visibility, insight, and responsiveness. BlueVoyant provides Advanced Threat Intelligence, Managed Security Services and Incident Response through offices in the United States, the United Kingdom, Israel, and Spain.