Vajra Daily APT Cloud Scan

An Introduction

Cyber Security & Privacy Foundation Pte Ltd

CYBER SECURITY & PRIVACY FOUNDATION

Contact-director@cysecurity.co

The Problem

CYBER SECURITY & PRIVACY FOUNDATION

Hacking Incidents

Persistent global hacking incidents on US Govt & Fortune 100 firms. BFSI organization recently compromised and regulators have taken strict action

Points of infiltration (APT):

- External web application /services/mobile application – insecure
- SQL injection/XSS/IDOR/File upload/Broken authentication
- 0 day vulnerabilities on exposed services
- Default passwords on frameworks/application/devices
- Lateral movement through Pivoting - from exposed interfaces
- Existing Cyber Security Structure not able to address these infiltration points

The Solution

CYBER SECURITY & PRIVACY FOUNDATION

REEJA VAJRA
Daily APT Cloud Scan

Daily APT Cloud Scan

Anti-Fraud module extending to Anti– Phishing, Anti-Malware and Anti– Spam (APMS). Protect against Reputational, Financial & IP loss. Secure against Trojan Horses, Ransom Demands

Web Security scanner scans for vulnerabilities on web portal/web services

APMS Corporate

Web Reputation & Security Scan (WRSS)

Automated Vulnerability Assessment

Advanced intrusive model including external VA of network for protective and compliance requirements

DF 24

Defacement monitor for customer facing web portals. Includes Android mobile app/Windows SOC desktop app (for quick alerts)

Deliverables

CYBER SECURITY & PRIVACY FOUNDATION

Daily APMS report to customer

Weekly AVA/WRSS report with Bugtrack report

All critical/high vulnerabilities from automated WRSS/AVA and manual apt testing that need addressing are exported into Bugtrack in the portal

Prioritize vulnerability and work with SOC/Vendor (network/ application level) to fix them

Strive to ensure no exploitable vulnerability is present

APMS–Anti Phishing, Malware, Spamming Module (Anti Fraud Service)
Non-intrusive monitoring - protection from Reputation, Financial & IP loss

- Exhaustive scan of global phishing and spamming databases to cross-check potential compromises of customer's domain/s
- Sandbox application to browse customer's site/sand check if iframe, malware, java driveby can be downloaded to infect the machines of the end users of a bank's website or an e-commerce portal
- Automated daily scan and report generation
- Phishing complaints reporting system
- Anti viruses check for web portal infections by crawling through all known paths
- DNS Hijack Detection via cross checking with 450 odd DNS servers from across the world
- Similarly named websites detection using a) Advanced heuristics algorithm (even a 5 % match generates alert) and b) Automated "Electronic Eye", a recognition and comparison engine to scan screen shots
- AP 24 – Uses phishing feeds on24/7 basis to detect logo spoofing; image processing engine incorporates machine learning; Use of feedsfrom certificate transparency logs (CTL) for comparison and monitoring of logo misuse

WRSS–Web Reputation and Security Scan Module

- Security Scan of Web portals
- Protect customers/clients, employees, suppliers, distributors
- Automated scan and report generation
- Advanced shell detector module to identify stealth shell-codes
- Web reputation scan is non-intrusive testing while security scan is intrusive testing

AVA–Automated Vulnerability Assessment for IP Address

- Identification, quantification, and prioritisation of vulnerabilities
- Security scans of external IP addresses
- Charts for easy human interpretations
- Delta reporting of vulnerabilities (calculates difference in vulnerability reports)
- Scanner finds vulnerabilities for CMS system
- False positive & Ignore list for each device/server/web portal
- Dedicated Monitoring – partner with customer to fix vulnerabilities proactively
- Reports vetted by security researchers and cyber defense experts who are listed on Hall of Fame of firms such as Google, Microsoft, Apple and Facebook among others
- In built Cyber Defense Access Point (allows Cyber Defense experts to manually & securely insert access point) for cloud scanning of vulnerabilities

DF24-Defacement monitor for customer facing web portals

- DF24 monitors key homepage(s) for defacement and instantly raises a flag upon detection of defacements
- Separate servers for monitoring defacements and scan of key homepage(s) every 2 hours.
- Should DF24 detect a home page modification, an instant alert is transmitted - Windows app for SOC, Android app for CISO and IT mgr
- Allows companies and organisations to detect defacements and take corrective measures before others such as the media and regulators discover it.
- DF24 uses technology of word match algorithm and source code analysis. Calculating unique signature for main pages of URL, any change beyond 20% is immediately sent for review. The mobile app runs in two modes (review/CISO mode). Reviewer gets first level alert, once defacement is confirmed, an escalation to CISO follows for immediate action.