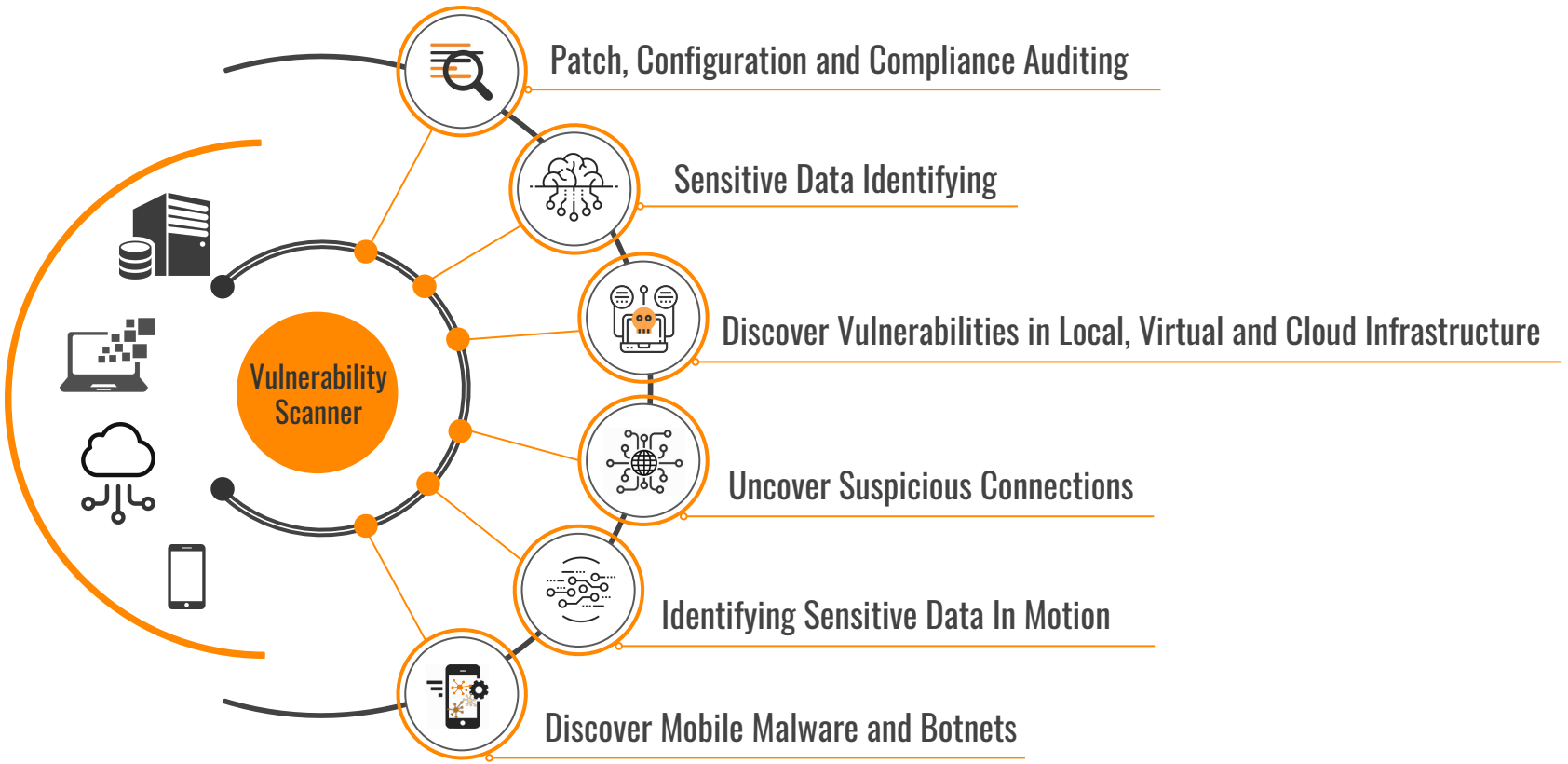
Case Study 2018

UNDER DEFENSE
CyberSecurity Solutions
Protecting your business

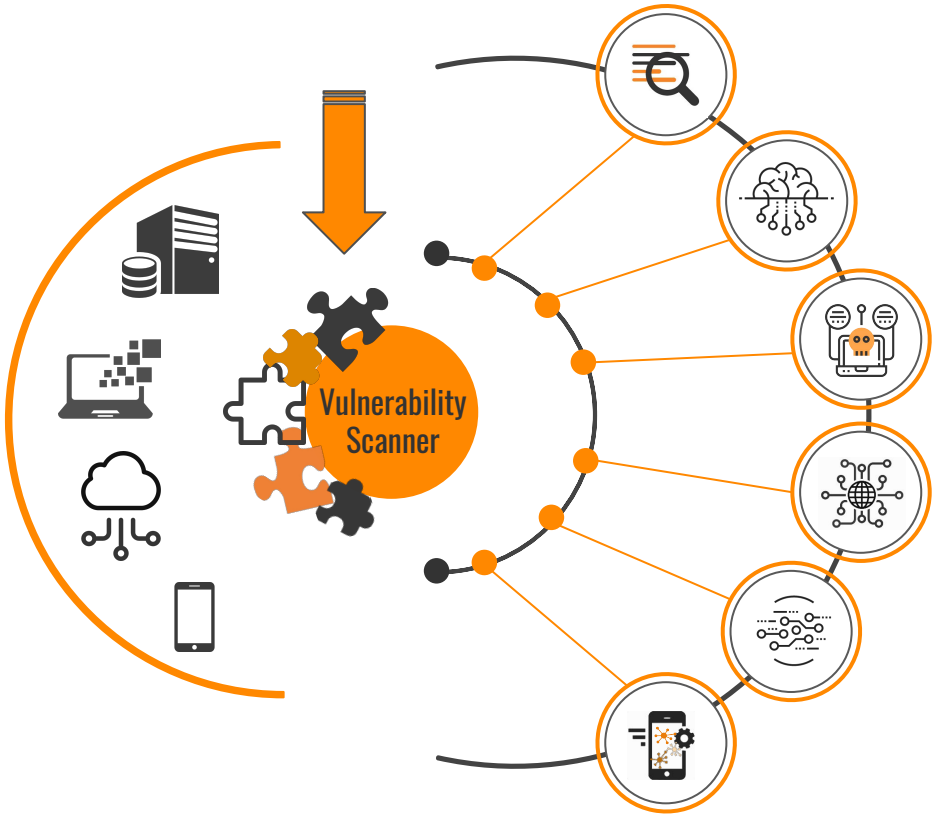
Patch & Vulnerability Management

Solution/Service Title	Vulnerability Management & Vulnerability Assessment
Client Industry	Cybersecurity, Vulnerability Assessment and Management, Network Security
Client Overview	WorldWide company which solutions help businesses and governments improve their network and application security
Client Challenge	Creating programs (plugins) for vulnerability scanner engine to run tests, scan networks or remote targets, rapidly identify software vulnerabilities in IT environment.
Technologies	Nessus Attack Scripting Language (NASL). CVE databases, NVD database
Key Benefits	UnderDefense has helped client in extending its product capabilities with the research and development of the latest vulnerability and exploitation techniques, and providing significant enhancements to Vulnerability Scanner
Results	Over 500 .nasl plugins covering vulnerabilities released in 2017-2018(Q1, Q2) including most disruptive and notorious threats.

Inputs and Outcomes of Vulnerability Assessment



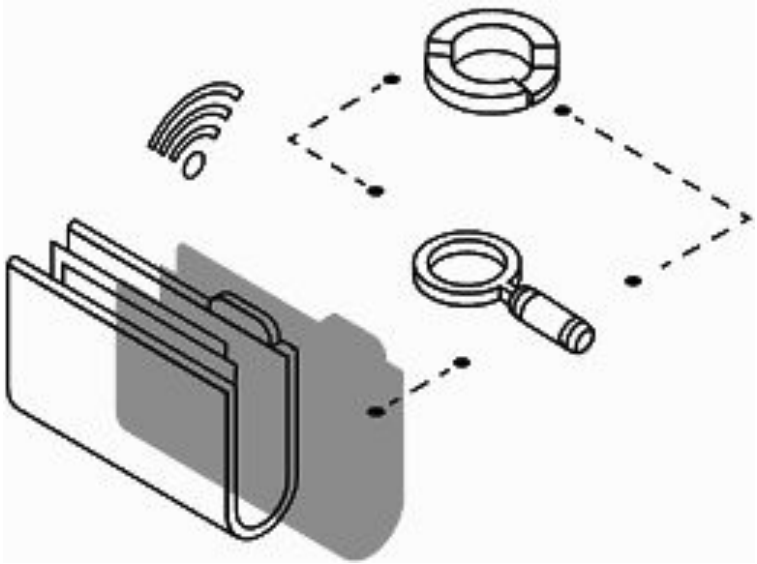
UnderDefense Role



Our task was to develop, test and deploy plugins for the vulnerability scanner.

Each plugin contains vulnerability information, a simplified set of remediation actions and the algorithm to test for the presence of the security issue.

Cases



Case 1: **Equifax incident**. Introduction

143

Million accounts breached on Equifax

Equifax confirmed that their high profile, high impact data breach was due to an exploit of a vulnerability in an open source component, Apache Struts CVE-2017-5638.

Equifax is a global information solutions company that uses unique data, innovative analytics, technology and industry expertise to power organizations and individuals around the world by transforming knowledge into insights that help make more informed business and personal decisions.

Apache Struts

CVE-2017-5638

The Jakarta Multipart parser in Apache Struts 2 2.3.x before 2.3.32 and 2.5.x before 2.5.10.1 has incorrect exception handling and error-message generation during file-upload attempts, which allows remote attackers to execute arbitrary commands via a crafted Content-Type, Content-Disposition, or Content-Length HTTP header

Apache Struts is a mainstream web framework, widely used by Fortune 100 companies in education, government, financial services, retail and media.

Case 1: **Equifax incident**. Actions

After python proof-of-concept exploit code had been published, we immediately analysed the exploit. Then we implemented detection technique in NASL plugin for the vulnerability scanner.

1

2

Successfully tested plugin and discovered Remote Code Execution vulnerability on preconfigured Apache Tomcat web server with Apache Struts 2.5.12 installed.

3

Delivered plugin file to customer's repository and helped them to be ready to detect such a critical threat in time.

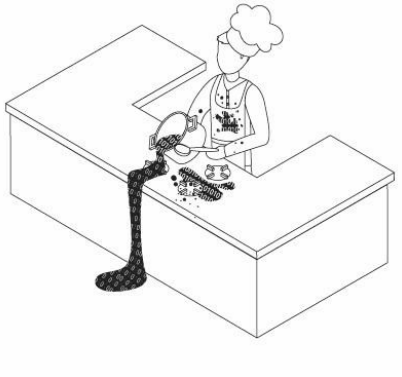
Case 1: **Equifax incident**. Conclusions

This breach highlights the need for visibility and control into the open source in use at organizations of all sizes.

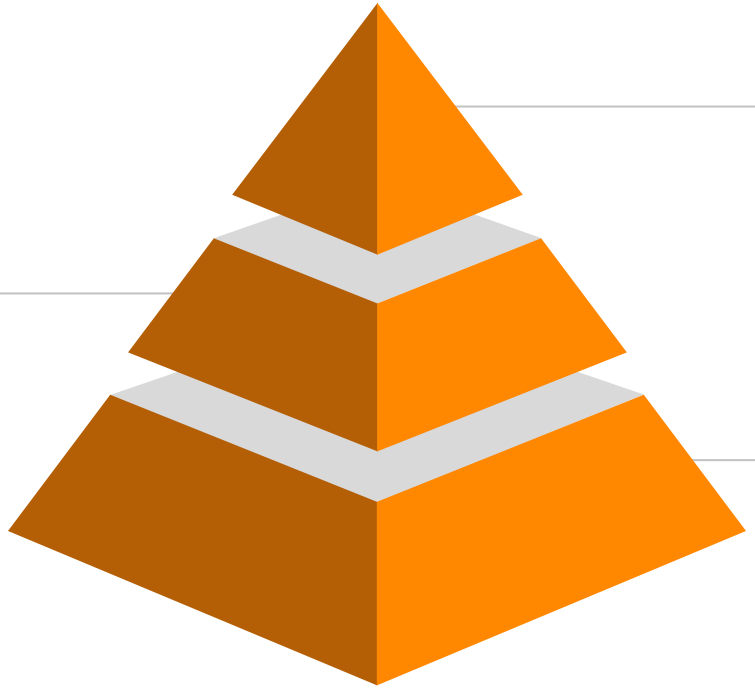
As the Equifax incident shows, open source security breaches can have devastating impacts for your users as well as your brand reputation, legal exposure, and revenue.

Case 2: **Cisco Smart Install**. Introduction

Embedi, a security firm, has discovered a major security flaw in the Cisco Smart Install code. According to Embedi and Cisco, “A vulnerability in the Smart Install feature of Cisco IOS Software and Cisco IOS XE Software could allow an unauthenticated, remote attacker to trigger a reload of an affected device, resulting in a denial of service (DoS) condition, or to execute arbitrary code on an affected device.”



Case 2: **Cisco Smart Install**. Actions



3 **Delivered plugin file to the customer's repository.**

2 Successfully tested plugin on preconfigured vulnerable target.

1 After Embedi's proof-of-concept exploit code had been published we immediately analysed the exploit. Then we composed detection algorithm and implemented it in NASL plugin for vulnerability scanner.

Case 3: **IP Cameras**. Introduction

Leaving IP cameras default passwords is dangerous and makes it easy for even inexperienced attackers to take control, brick or watch your video feed. To make things worse, since many cameras are made available over the Internet (often because of another risky practice, port forwarding or because the manufacturer defaulted UPnP on), the cameras may be attacked from anywhere in the world.

Shodan's query results with ~ 165,000 publicly accessed and potentially vulnerable ip cameras.

Case 3: **IP Cameras**. Actions

Client requested rule for detecting misconfiguration in the world's largest video surveillance manufacturer device firmware.

1

We have created delicate test scenario and implemented it in plugin which would gently discover misconfiguration and inform user in detail about following solutions of problem

2

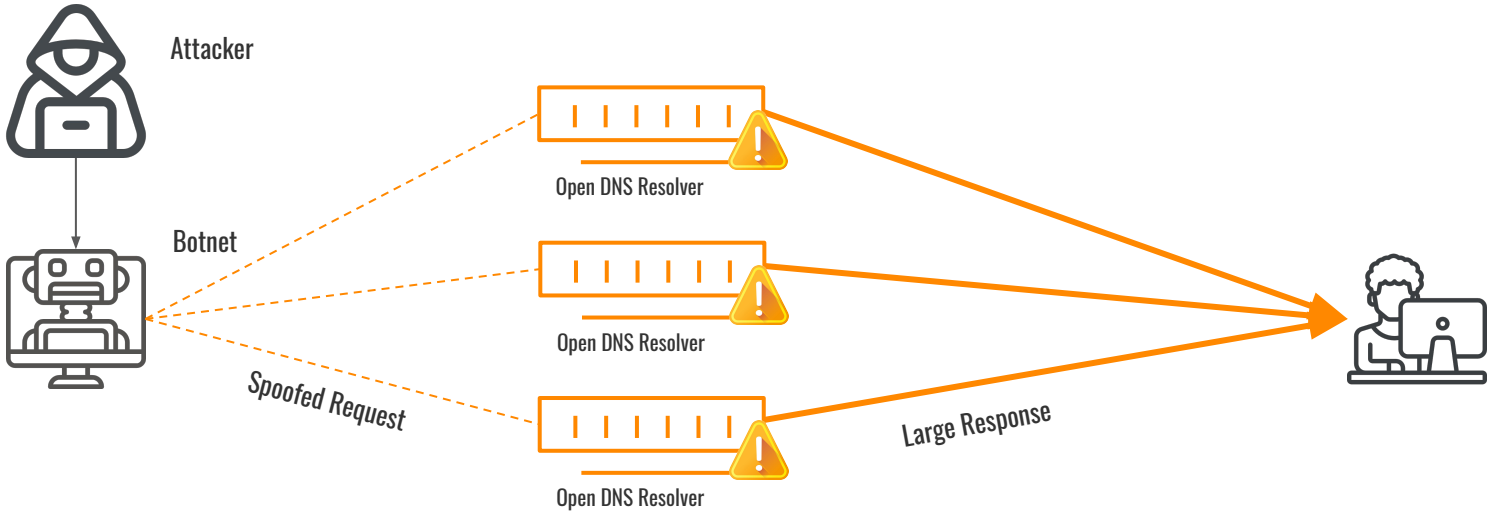
Successfully tested plugin on preconfigured vulnerable target

3

Delivered rule plugin to customer’s repository.

Case 4: **DNS amplification attack**. Introduction

This DDoS attack is a reflection-based volumetric distributed denial-of-service (DDoS) attack in which an attacker leverages the functionality of open DNS resolvers in order to overwhelm a target server or network with an amplified amount of traffic, rendering the server and its surrounding infrastructure inaccessible.

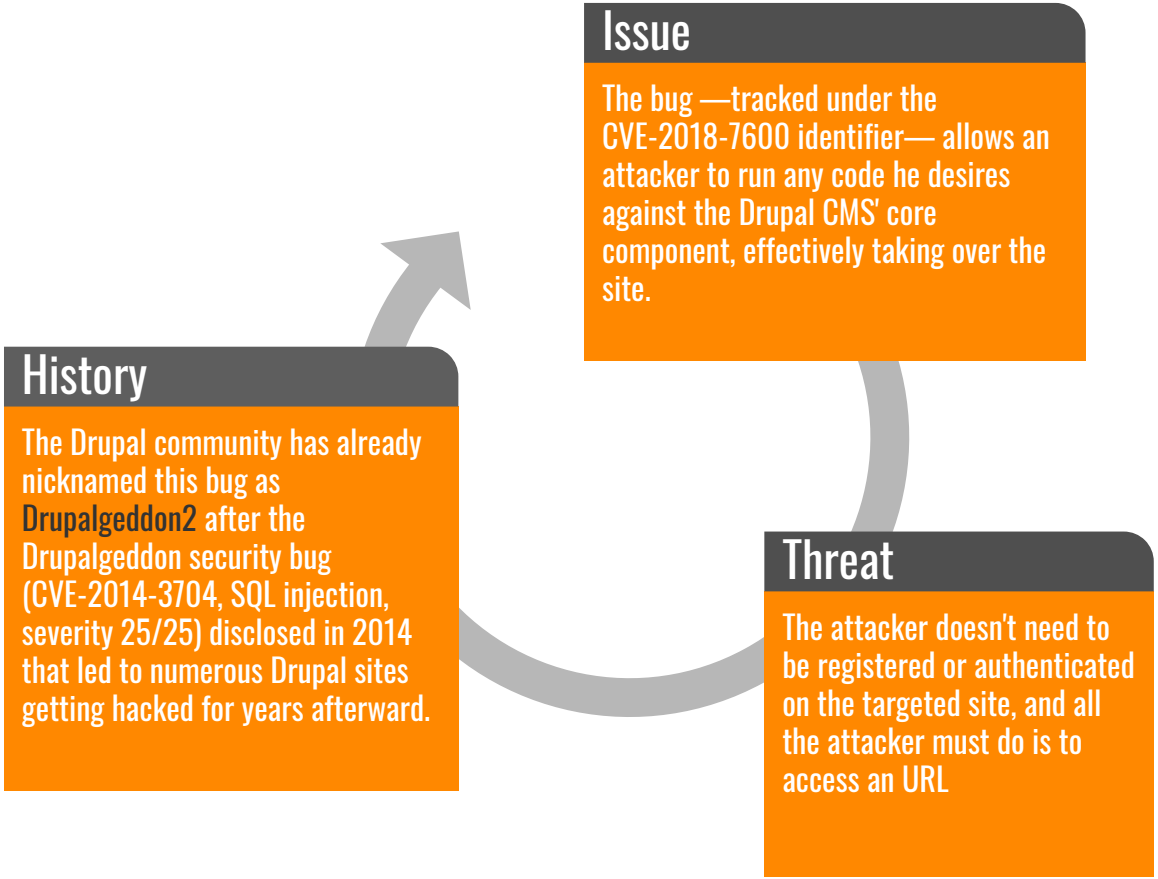


Case 4: **DNS amplification attack**. Actions

Client requested rules for 13 application-layer protocols that could be exploited to distributed reflective denial-of-service (DRDoS) attack referring to US CERT alert.

Step 1	Step 2	Step 3
We have utilized IP packet datagram forge technic in order to implement it in plugins which would discover vulnerability to DRDoS attack and provide the user with comprehensive instruction for the correct way to resolve the problem.	Successfully tested plugins on preconfigured vulnerable targets.	Delivered plugin files to customer's repository.

Case 5: **Drupal CMS**. Introduction



Case 5: **Drupal CMS**. Actions

At the moment of The Drupal CMS security flaw reporting we have immediately implemented “version check” scenario in NASL plugin for vulnerability scanner

Delivered plugin file to customer’s repository.

Successfully tested plugin on preconfigured Drupal CMS 8.5.0.

Thank you!

Call us now at +1 929 999 5101