Protecting Business from Breaches: Lessons still Unlearned

christine smoley

$ whoami

- Security Engineer | Paytm Labs
- Bug Bounty Program Lead
- Threat Intelligence Lead

If there's anything I've learnt from experience...

Correlation

Bug Bounty Methodologies

Adversarial Techniques

Vulnerability Management

Known Vulnerabilities

Common Issues

Initial Compromise

1. Know your assets 2. Source intel and indentify vulnerabilities
3. Maintain control (patching)

Australian Government “Copy-Pa
Compromises”

Australian Government
Australian Signals Directorate

The actor has shown the capability to quickly leverage public exploit proof-of-concepts to target networks of interest and regularly conducts reconnaissance of target networks looking for vulnerable services, potentially maintaining a list of public-facing services to quickly target following future vulnerability releases. The actor has also shown an aptitude for identifying development, test and orphaned services that are not well known or maintained by victim organisations.

https://www.cyber.gov.au/acsc/view-all-content/alerts/copy-paste-compromises

```
The attacker used public exploits against the network

1. used scans to find vulnerable services

2. likely maintained a service /  asset inventory

3. Mapped threat intel / vulnerability releases to services
```

- Citrix
- Microsoft Internet Information Services
- Sharepoint
- Telerik UI

Australian cyber attack not 'sophisticated' – just a wake-up call for businesses, experts say

The known vulnerabilities that lead to these widely publicized breaches and compromises pose vulnerabilities to businesses of any size.

WannaCry Ransomware Attack May 2017

- Shut down 80 NHS organizations, 20,000 cancelled appointments, 5 hospitals diverting ambulances

~ $ 4 billion losses

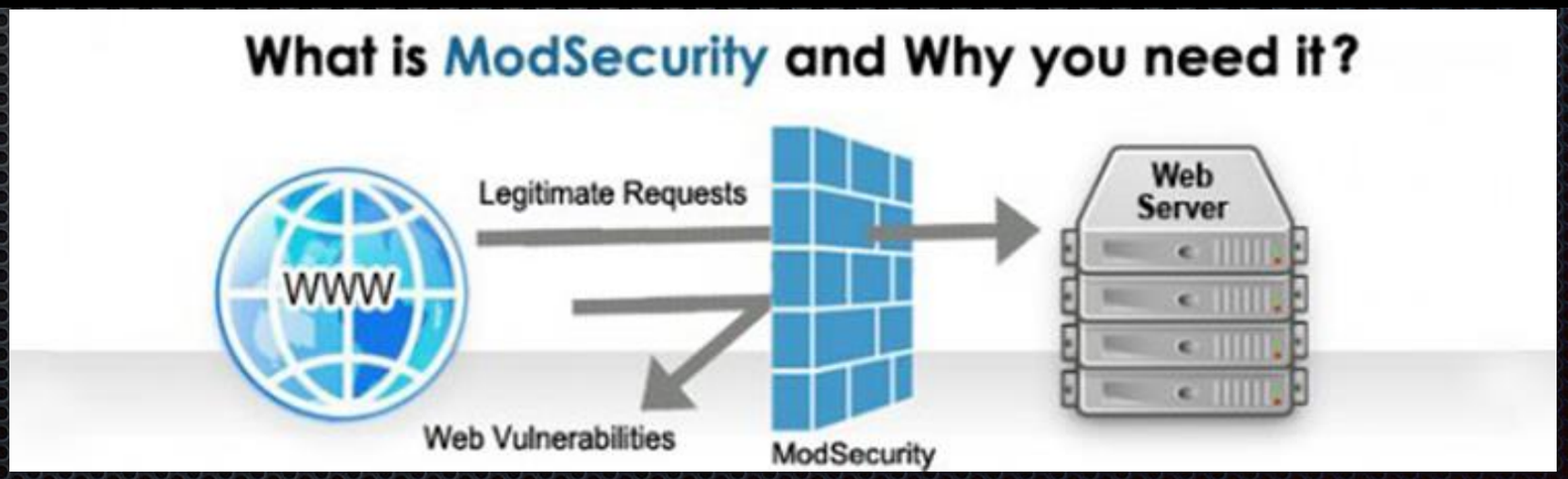
- April 2017: “Shadow Brokers” release details of Windows OS SMBv1 vulnerability.
- Believed stolen from the NSA (“Eternal Blue”)
- Microsoft produced a patch in March, tipped of that it might be made public

Capital One Breach March 2019

Server-Side Request Forgery (SSRF)

- Misconfigured open-source “ModSecurity” Web Application Firewall (WAF)
- Designed to protecting Amazon Web Services (AWS), but allowed intruder to trick the firewall into relaying requests to back-end resources (Metadata service)
- Metadata service provides credentials to access resources

Estimate cost $300 - $500 million



Accenture Cloud Leak Sept 2017

- 4 cloud-based storage servers which were publicly available and downloadable

- Amazon Web Services (AWS) S3 storage buckets can be configured for public or private access.

- In this instance they contained sensitive information about Accenture’s internal network, 40,000 passwords and client information

Equifax Breach 2017

- Unpatched web component Apache Struts - fix provided in March, breach occurred in May
- Struts used a parser with incorrect exception handling and error-message generation during file-upload attempts, which allow remote attackers to execute commands
- Consequence: 143 million consumers
- Cost: $700 million settlement alone
- Fix: simple upgrade

Lessons

- Know yourself: Asset management, cloud auditing, configuration management
- Threat intel, vulnerability assessment: know your risk
- Cyber hygiene: patch and change management processes