

Watering Hole Attacks:

Detect End-User Compromise
Before the Damage is Done



Garrett Gross

Sr. Technical Product Marketing Manager

Victor Obando

Technical Sales Engineer



ALIEN VAULT

About AlienVault

AlienVault has unified the security products, intelligence and community essential for mid-sized businesses to defend against today's modern threats



Agenda

- 👁️ How Watering Hole attacks work
- 👁️ What attackers do next to infiltrate the network
- 👁️ Why detecting these attacks is tricky
- 👁️ Demo: How to detect Watering Hole attacks with AlienVault USM

Watering Hole Attack in 4 Easy Steps

1. Determine target group

- Attacker identifies websites to target based on observation or guessing
- Compromises a well-known, legitimate site to avoid blacklist issues

2. Identify vulnerabilities on those websites

- Test web servers, ad servers, web apps, etc for vulnerabilities to exploit

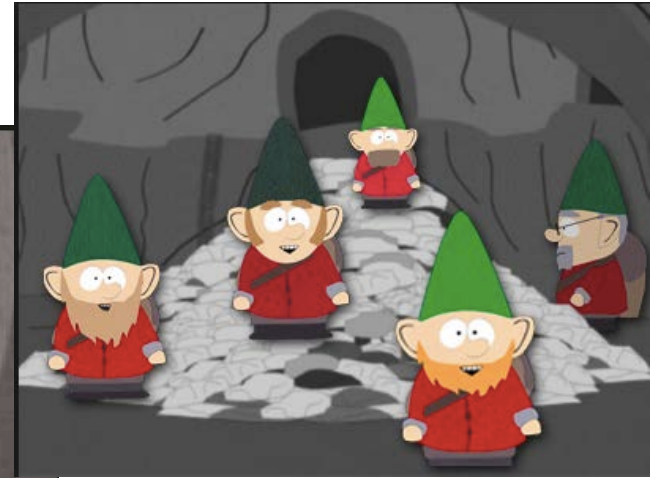
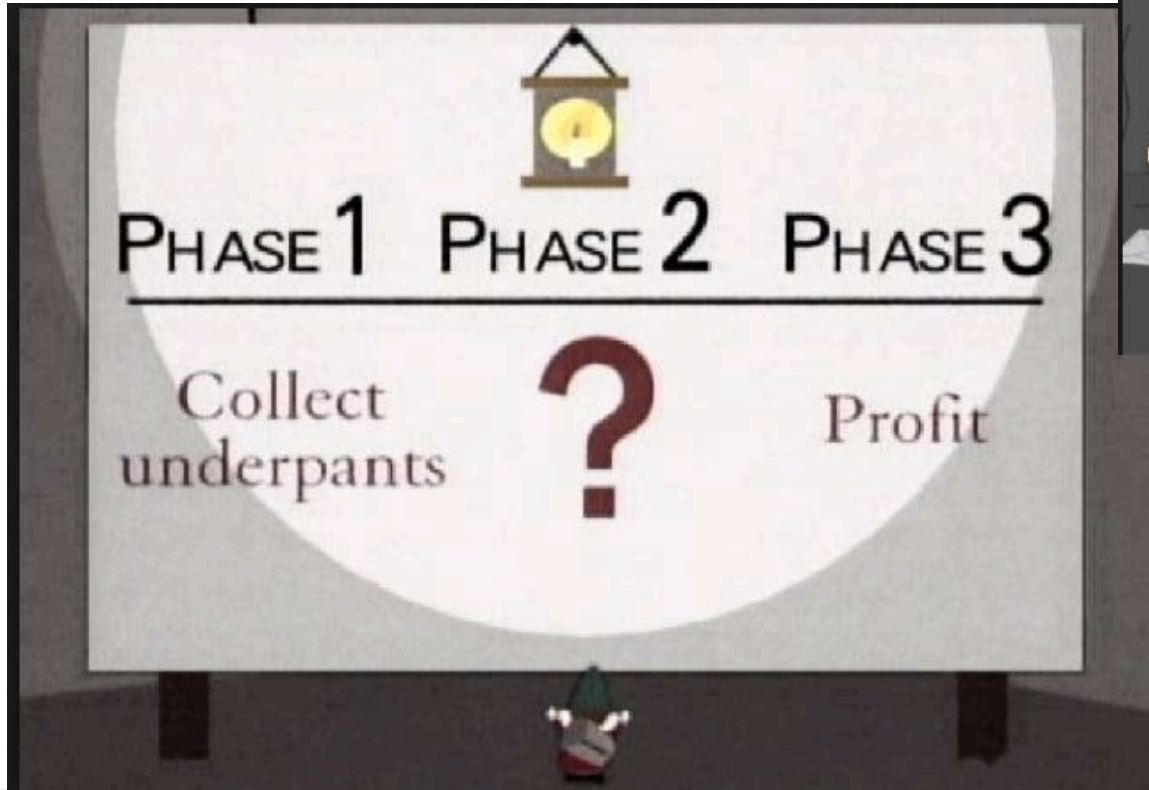
3. Inject threat into website

- For example, inject HTML or JavaScript to redirect victims to sites hosting malware




4. Sit in the tall grass and wait for targets

- Redirected from compromised site
- Eventually compromised by download of malware
- Even more effective with e-mail spear-phishing campaign

What happens next?






No seriously, what happens next??

-  Grab credentials of current user
-  Browse the domain
-  Exfiltrate data

How do you detect this?

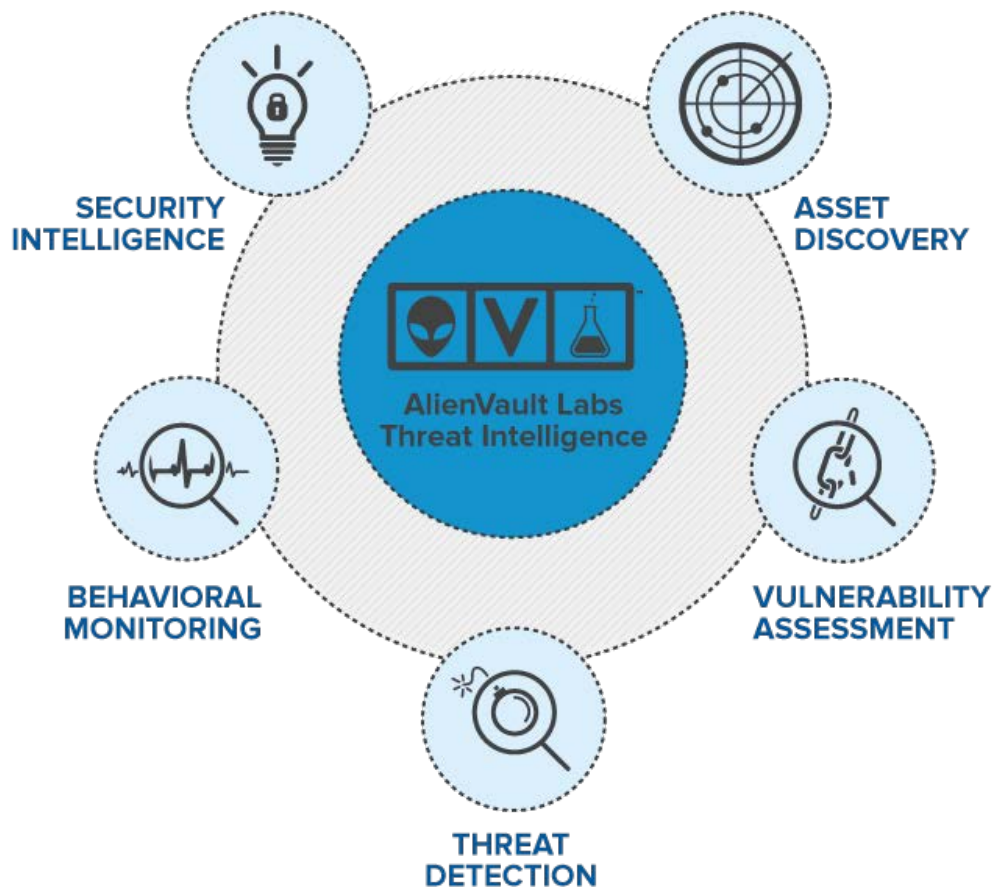
Tricky to detect because...

-  Firewall won't catch it
 - Attack is executed via an existing, permitted session
-  Anti-virus is unlikely to catch it
 - 82,000 new malware variants released every day*
-  Won't leave a trace in the system logs
 - Occurs through a web-browser which doesn't result in any log entries

So, what will catch it?

-  Network Intrusion Detection and effective correlation

AlienVault USM™



Asset Discovery

- Active Network Scanning
- Passive Network Scanning
- Asset Inventory
- Host-based Software Inventory

Vulnerability Assessment

- Network Vulnerability Testing
- Remediation Verification

Threat Detection

- Network IDS
- Host IDS
- Wireless IDS
- File Integrity Monitoring

Behavioral Monitoring

- Log Collection
- Netflow Analysis
- Service Availability Monitoring

Security Intelligence

- SIEM Event Correlation
- Incident Response

The logo is a large, light gray watermark in the background. It consists of a rounded rectangle divided into two equal squares. The left square contains a stylized alien head profile, and the right square contains a large, bold letter 'V'.

Now Lets See
It In Action

TM

ALIEN VAULT

Thank You! Any Questions?

Test Drive AlienVault USM

👾 Download a Free 30-Day Trial <http://www.alienvault.com/free-trial>

👾 Try Our Product Sandbox <http://www.alienvault.com/live-demo-site>



The screenshot shows the AlienVault USM website. At the top, it says "Detecting Threats Has Never Been Easier (or Faster)". Below that, it says "Meet AlienVault USM!" and "Within minutes, you'll be able to detect:". A list of threats is shown: Malware infections, Command and control activity, Known Vulnerability (CVE) Exploits, Bruteforce Attacks, and SQL Injection & XSS Attacks. A green button says "DOWNLOAD A FREE TRIAL ►". On the right, there's a laptop displaying a dashboard with a large play button and a price tag that says "FROM \$3600!". At the bottom, there are five icons representing different features: Asset Discovery, Vulnerability Assessment, Threat Detection, Behavioral Monitoring, and Security Intelligence.

Detecting Threats Has Never Been Easier (or Faster)

Meet AlienVault USM!

Within minutes, you'll be able to detect:

- ✓ Malware infections
- ✓ Command and control activity
- ✓ Known Vulnerability (CVE) Exploits
- ✓ Bruteforce Attacks
- ✓ SQL Injection & XSS Attacks

DOWNLOAD A FREE TRIAL ►

FROM \$3600!

ASSET DISCOVERY

VULNERABILITY ASSESSMENT

THREAT DETECTION

BEHAVIORAL MONITORING

SECURITY INTELLIGENCE

More Questions?
Email Hello@AlienVault.com