ASM is easy, ASD is harder

Attack Surface Management made easy with Attack Surface Discovery

Patrice AUSSFRET, founder & CTO

patrice.auffret@onyphe.io
Who am I?

- Patrice Auffret
  - Cybersecurity engineer
  - 20+ years of experience

- Different positions
  - Offensive security
    - Pentests, Web application audits
  - Defensive security
    - Collect and analysis of information system events (SIEM)
  - Trainer
    - Big data (Splunk, Elastic Stack)
  - Speaker
    - SSTIC, TROOPERS, Hack.lu, UYBHYS, ekoparty, EuSecWest, ...

- ONYPHE founder & CTO

Photo: Michel François Salmon
Agenda

- Introduction
- Current state of defensive cybersecurity
- ASD + ASM Demo
- Conclusion
Introduction

What is ONYPHE?
ONYPHE company

- Created in 2017
  - Pioneer in Attack Surface Management
  - French company
  - Self-financed (read: no investor)

- One main goal
  - Fight ransomware exposure

- Own technology
  - 100% in-house development
  - Data stored on dedicated servers
What is ONYPHE?

- Cyber Defense Search Engine
  - Attack Surface Discovery
  - Attack Surface Management

- Collected by
  - Active probing
  - Passive listening
  - Downloading

- Data is split into
  - 20 categories

- Everything is stored
  - Normalization
  - Correlation

- Data searchable from
  - A Web search form
  - An API
Attack Surface Discovery (1st step)

- Attack Surface Discovery solution
  - Domain-based approach
  - Protocol-based identification
  - Device classification

- Scanning different networks every month
  - IP addresses: 3.8B+ IPv4, 130M+ IPv6
  - URL scanning: 300M+
  - Dark Net scanning: 22k+

- Find unknown assets
Top threats in 202x

- External initial access vectors
  - Software vulnerabilities
  - Brute-force credential attacks
  - Previously compromised creds

- 46% of all intrusions

https://unit42.paloaltonetworks.com/incident-response-report/
Top threats in 202x

- External initial access vectors
  - Phishing for valid creds
  - Password spraying/guessing creds
  - Vulnerability exploitation

- ~50% of all intrusions

https://www.cisa.gov/sites/default/files/2023-06/aa23-165a_understanding_TA_LockBit_0.pdf
Attack Surface Management (2\textsuperscript{nd} step)

- **Attack Surface Management solution**
  - Risk baseline approach
  - Focus on most critical risks
  - Continuous monitoring

- **Identify initial access vector risks**
  - Exposed RDP/VNC/SSH/Telnet services
  - Exposed VPN servers
  - Critical vulnerabilities: 60+ CVEs

- **Cut ransomware risk upfront**
Data stored for historical searches

- **Historical data**
  - Up-to 12-month
  - Go back in the past
  - Forensic analysis

- **DNS enumeration**
  - Starting from a single domain

- **Data lake**
  - Best leveraged from our numerous APIs
Current state of defensive cybersecurity

About decades of security failures
What is **Attack Surface Management**?
- Term coined by Gartner somewhere in 2020
- New tool in defensive cybersecurity arsenal for organizations

**Goal**
- Help organizations have a better view on exposed assets

**But how to find the unknown?**
- **Attack Surface Discovery** to the rescue
Decades of patch management failures

- Traditional approach
  - Using a vulnerability scanner

- Vulnerability scanners objective
  - To have a vulnerability report with content
  - Every vulnerability should be listed
    - Even those not exploitable or useless from an attacker’s perspective

- Conclusion
  - Remediation fatigue
  - Impossible to patch everything
On vulnerability scoring systems

- Decades of trying to « score » a vulnerability danger
  - CVSS - Common Vulnerability Scoring System
  - EPSS - Exploit Prediction Scoring System
    - [https://www.first.org/epss/](https://www.first.org/epss/)

- It just doesn’t work anymore

- Let’s define a **binary scoring system**
  - A vulnerability is exploited to commit crime
  - Or it is not

- CISA Known Exploited Vulnerability catalog
  - [https://www.cisa.gov/known-exploited-vulnerabilities-catalog](https://www.cisa.gov/known-exploited-vulnerabilities-catalog)
Pentesting as a complementary approach

« Let’s pentest the service before it is put online »
- Scope-based
- Best scenario
  - IP addresses list
  - Hostnames list

Cybercriminals are scope agnostic

Why should legitimate pentests be scope-based
- While illegitimate “pentests” performed by criminals are not?
Last note on how to define a scope

- **Scope should be**
  - Domain names
  - Related « pivots »
  - IP addresses

- Should also include
  - Subsidiaries
  - Suppliers

- If subsidiaries and/or suppliers handle your data
  - They are part of YOUR attack surface
Demo

Attack Surface Discovery & Attack Surface Management
Conclusion

Key takeaways
Statistics against demo’ed scopes

- VPN servers
  - 100%

- RDP exposure
  - 100%

- SSH exposure
  - 100%

- Critical vulnerability
  - 67%
To sum it up

- **Vulnerability scanners don’t work**
  - They MUST find something, even useless
  - Good for KPIs and colorful dashboards, not for operational cyberdefense

- **Patch management doesn’t work**
  - Decades of patch management programs failures
  - Remediation fatigue **HAS** a human cost

- **ASM is the easy part, ASD is the hard part**
  - Identify the unknown that has to be managed
  - ASD can also be used to feed a vulnerability scanner
To sum it up

- **Don’t rely solely on IP addresses inventory**
  - IP addresses are subject to change, not domain names
  - Rebuild your inventory every month

- ** Doesn’t matter if an asset is on-prem or in the cloud**
  - Criminals don’t care
  - Assets handling your data are your responsibility, no matter what
Focus is key

- Put your efforts on what matters most
  - Exposed RDP/VNC/SSH/Telnet services
  - Exposed VPN Servers
  - Critical vulnerabilities

- Identify the unknown
  - Implement an attack surface discovery program

- Doing that will reduce ransomware risk tremendously
  - Then, handle remaining issues
Merci.

Twitter: @ONYPHE, @PatriceAuffret
Register: https://www.onyphe.io/signup
Pricing: https://www.onyphe.io/pricing
Github: https://github.com/onyphe