

**SpiderLabs**  
Worst of the Best of  
the Best

 **Trustwave®**

**Kevin Stadmeyer  
Garrett Held**



# Worst of the Best of the Best





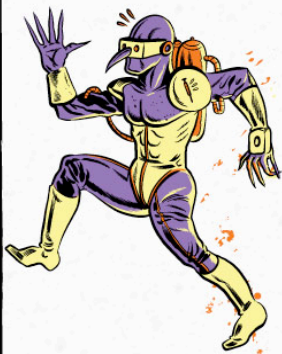
# Agenda

- Motives
- Goals
- Awards Overview
- Example of Serious Flaws in the System
- Lies, Damned Lies, and Awards
- What Awards Really Mean
- Better Ways





# Motives and Goals





## Motives

---

- Yes, it's obvious this is about marketing
- Any product will probably contain vulnerabilities
- Awarding dangerous security practices is much worse
- Public records give an incomplete picture





## Goals

- Highlight a product that's an example of this problem, and why vulnerability statistics do not accurately reflect product security
- Attempt to use publicly available statistics that come up with a model that does work





# Awards Overview

| Name                          | Nomination         | Choosing A Winner            |
|-------------------------------|--------------------|------------------------------|
| Info Security Products Guide  | Pay for Nomination | No official public criteria. |
| SC Magazine                   | Unknown            | Popular vote                 |
| Techworld.com                 | Unknown            | Unknown                      |
| Information Security Magazine | Editor Chosen      | Popular vote                 |





# Product X and Vendor Y

Why public statistics aren't a complete picture







# Product X

---

It's a Secret shhh! Hi Lawyers!

- Provides a web service/interface on a network appliance





# Product X: Findings

- A manual application security review was performed on the device without access to the source code
- The following vulnerabilities were found:
  - Eight high-risk issues
  - Six medium-risk issues
  - Nine low-risk issues





# Product X: Serious Findings

This is a subset of the High and Medium risk issues found:

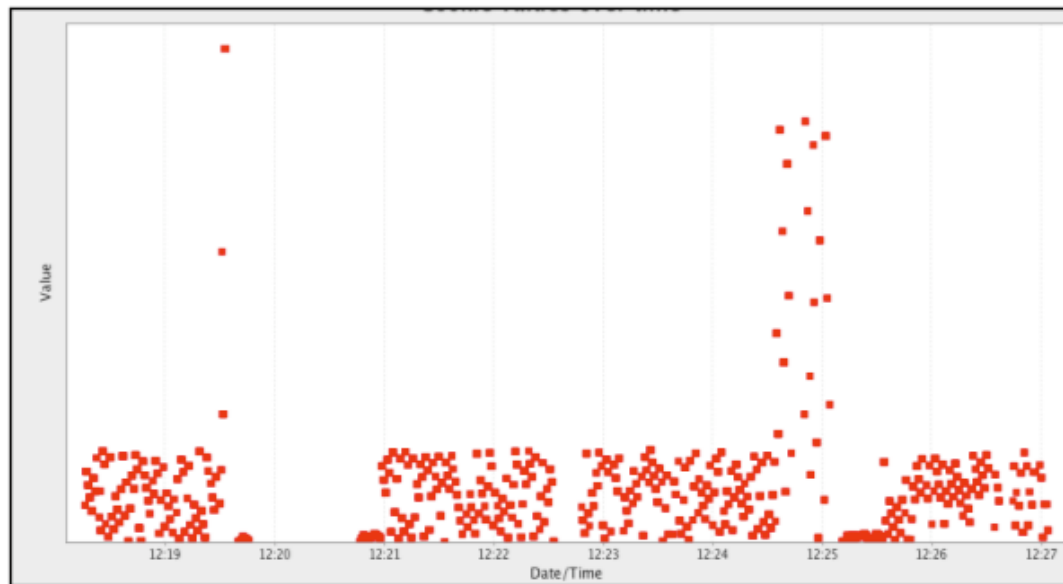
- **Systemic Cross-Site Scripting**
  - Almost any variable was vulnerable, including variables stored by the application (Persistent Cross-Site Scripting)
- **Privilege Escalation**
  - Browser-supplied user ID while in a valid session could be changed, using an easily predictable method, for privilege escalation.
- **Custom Web Server**
  - Re-inventing the wheel and introducing bugs such as arbitrary system file access, including the password file.





## Product X: Serious Findings (Cont.)

- Session Hijacking
  - Poor implementation resulted in users able to steal sessions of users logging in around the same time of day.
- Custom, Weak Session ID Algorithm
  - Without getting into details that would give it away:





# Product X: Reaction

---

# So What?





## Vendor Y

---

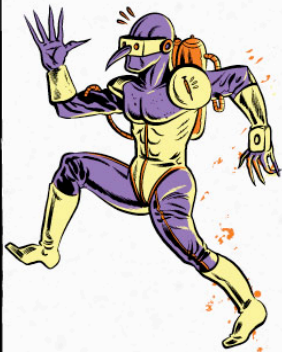
- Major software vendor
- Two independently discovered vulnerabilities, medium or higher
- One occurs on their own servers (still)

Vendor Response: \*Crickets\*





# Lies, Statistics, and Awards





# What Awards Really Mean

---

## Problems with gathering statistics

- FUD
- Sources
- Lack of History







# Sample Statistics

---

## Methodology

- Three Categories
- Two Awards
- Competitors
- Variety of Sources





# Awards: Anti-Malware

| Award                        | Product                       | Highs | Mediums | Lows |
|------------------------------|-------------------------------|-------|---------|------|
| SC Magazine                  | Symantec End-Point Protection | 4     | 0       | 0    |
| Info Security Products Guide | CoreTrace - Bouncer 4.0       | 0     | 0       | 0    |
|                              | Nod32 Anti-Virus              | 2     | 1       | 2    |
|                              | Proventia Network Scanner     | 0     | 0       | 0    |
|                              | Radware Defense Pro           | 0     | 0       | 0    |
|                              | Vipre                         | 0     | 0       | 0    |
|                              | Websense                      | 1     | 2       | 1    |





# Awards: Endpoint Security

| Award                        | Product                             | Highs | Mediums | Lows |
|------------------------------|-------------------------------------|-------|---------|------|
| SC Magazine                  | McAfee Security Center              | 2     | 0       | 1    |
| Info Security Products Guide | Parity v4.0.1                       | 0     | 0       | 0    |
|                              | Checkpoint for Endpoint Security    | 0     | 2       | 2    |
|                              | Cisco NAC                           | 1     | 1       |      |
|                              | F5 Firepass Remote Access Solutions | 5     | 2       | 18   |
|                              | Symantec Endpoint Protection        | 0     | 0       | 0    |





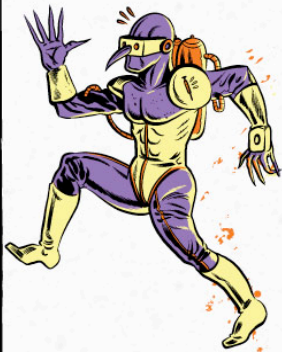
# Awards: IPSec/SSL VPN

| Award                        | Product                             | Highs | Mediums | Lows |
|------------------------------|-------------------------------------|-------|---------|------|
| SC Magazine                  | Cisco ASA 5500                      | 3     | 0       | 4    |
| Info Security Products Guide | NCP Secure Enterprise Solution      | 0     | 0       | 2    |
|                              | Checkpoint Connectra                | 0     | 0       | 2    |
|                              | Citrix Access Gateway               | 1     | 1       | 0    |
|                              | F5 Firepass Remote Access Solutions | 5     | 2       | 17   |
|                              | Stonesoft Stonegate VPN             | 0     | 0       | 0    |





# What Awards Really Mean





# What Awards Really Mean

## Awards Are Marketing

- Unclear
- Too Many
- Press Releases
- Pointless



**SPIDERLABS**

# Better Ways



Trustwave®





# Better Ways

---

## Credible Award Requirements

- Open Process
- Established Products
- Audit Product Patch Process
- Relevant Criteria







# Better Ways

---

## Alternative Evaluation Criteria


- References
- History of Security
- Talk to Developers



**SPIDERLABS**

**Questions?**



 Trustwave®

