RSAC Studio

Connect to Protect

Think Like an Operative: Protect Sensitive Data

Tyler Cohen Wood

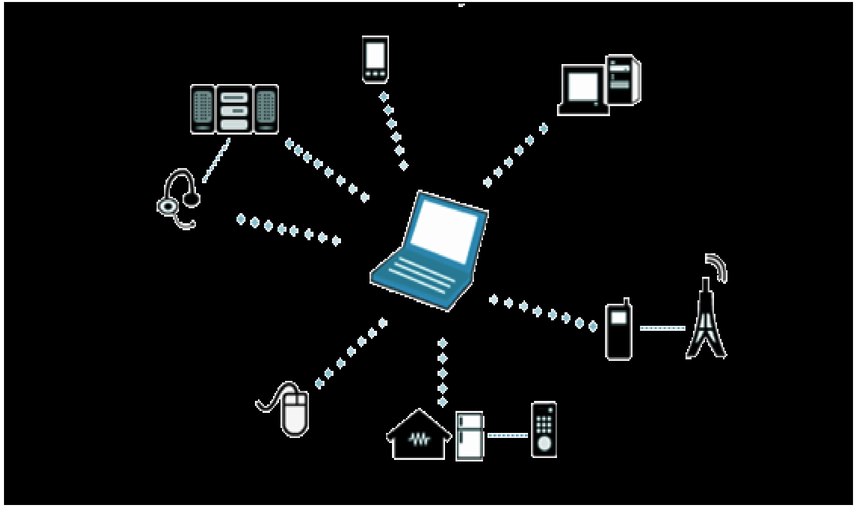
Cyber Security Advisor and Media Spokesperson
Inspired eLearning

#RSAC

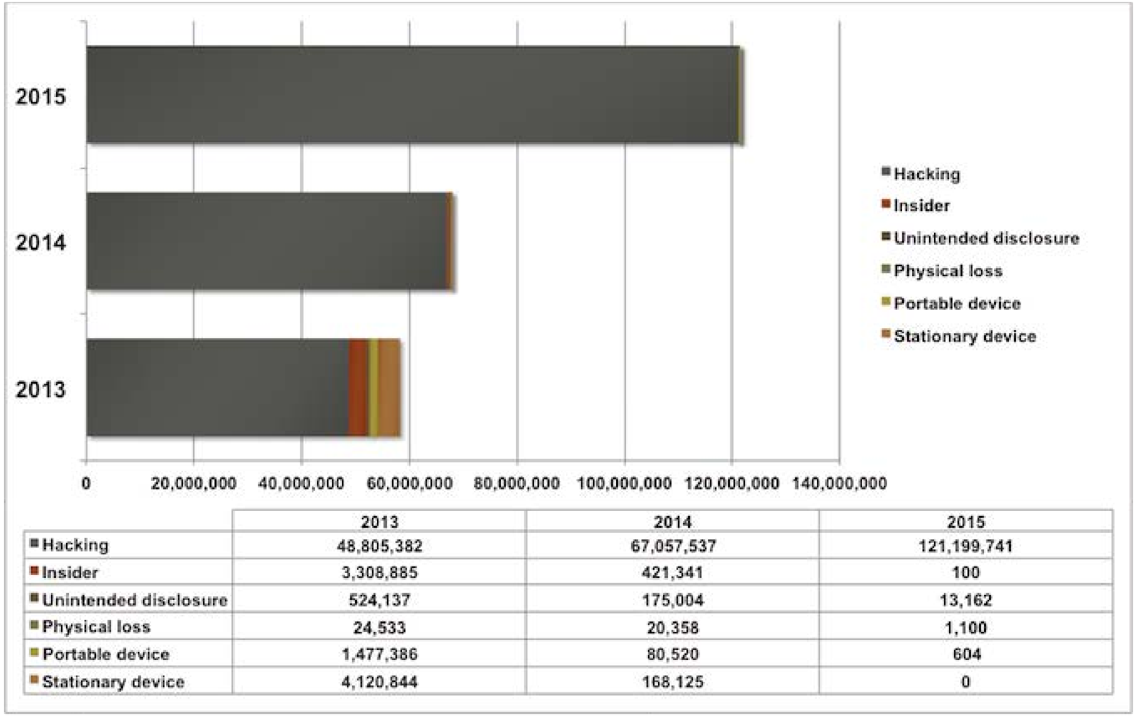
How We Got Here

The Old Days

Today

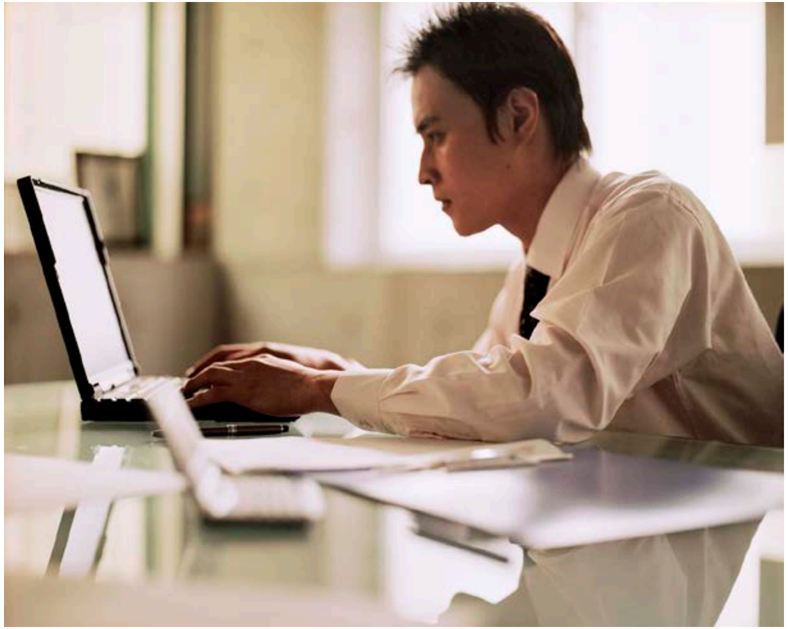


Data Breaches - 2013-2015



	2013	2014	2015
■ Hacking	48,805,382	67,057,537	121,199,741
■ Insider	3,308,885	421,341	100
■ Unintended disclosure	524,137	175,004	13,162
■ Physical loss	24,533	20,358	1,100
■ Portable device	1,477,386	80,520	604
■ Stationary device	4,120,844	168,125	0

What Causes Most Data Breaches?



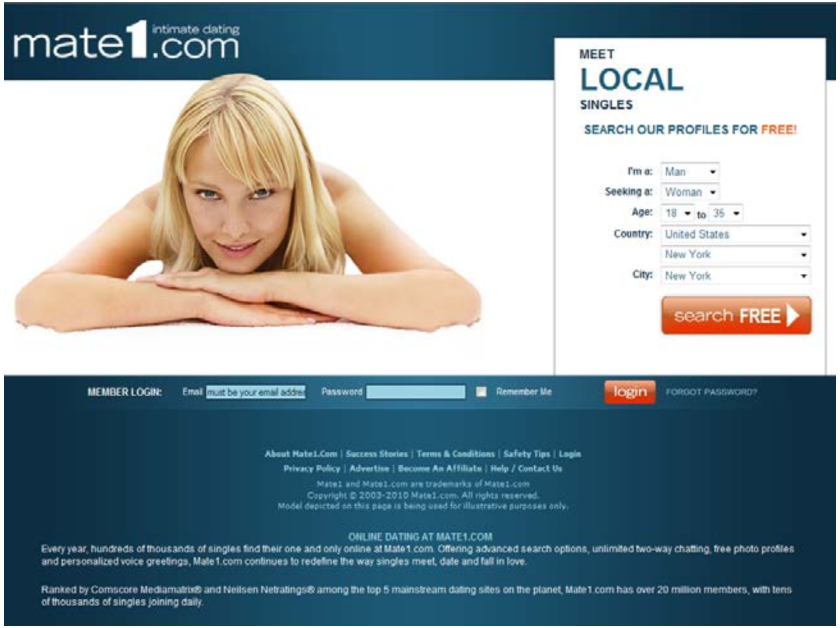
Mindshift: Think Like an Operative

Challenge: Find John Doe

John Doe’s Dating Site Profile

Indicators

- “High powered executive at X company”
- “No one ever thought I’d make it out of X and become a success”
- “I make well over six figures”
- “Every Thursday you can find me at X for happy hour”
- “We could meet for coffee at X”
- Photos of John and John’s new house



MEET LOCAL SINGLES

SEARCH OUR PROFILES FOR FREE!

I'm a: Man
Seeking a: Woman
Age: 18 to 35
Country: United States
New York
City: New York

MEMBER LOGIN: Email must be your email addre Password ☐ Remember Me

About Mate1.Com | Success Stories | Terms & Conditions | Safety Tips | Login
Privacy Policy | Advertise | Become An Affiliate | Help / Contact Us

Mate1 and Mate1.com are trademarks of Mate1.com
Copyright © 2003-2010 Mate1.com. All rights reserved.
Model depicted on this page is being used for illustrative purposes only.

ONLINE DATING AT MATE1.COM

Every year, hundreds of thousands of singles find their one and only online at Mate1.com. Offering advanced search options, unlimited two-way chatting, free photo profiles and personalized voice greetings, Mate1.com continues to redefine the way singles meet, date and fall in love.

Ranked by Comscore Mediamatrix® and Neilsen Netratings® among the top 5 mainstream dating sites on the planet, Mate1.com has over 20 million members, with tens of thousands of singles joining daily.

Building a Pattern of Life

What Can We Get From This?

- Blogs
- Social media
- Public records
- Photos

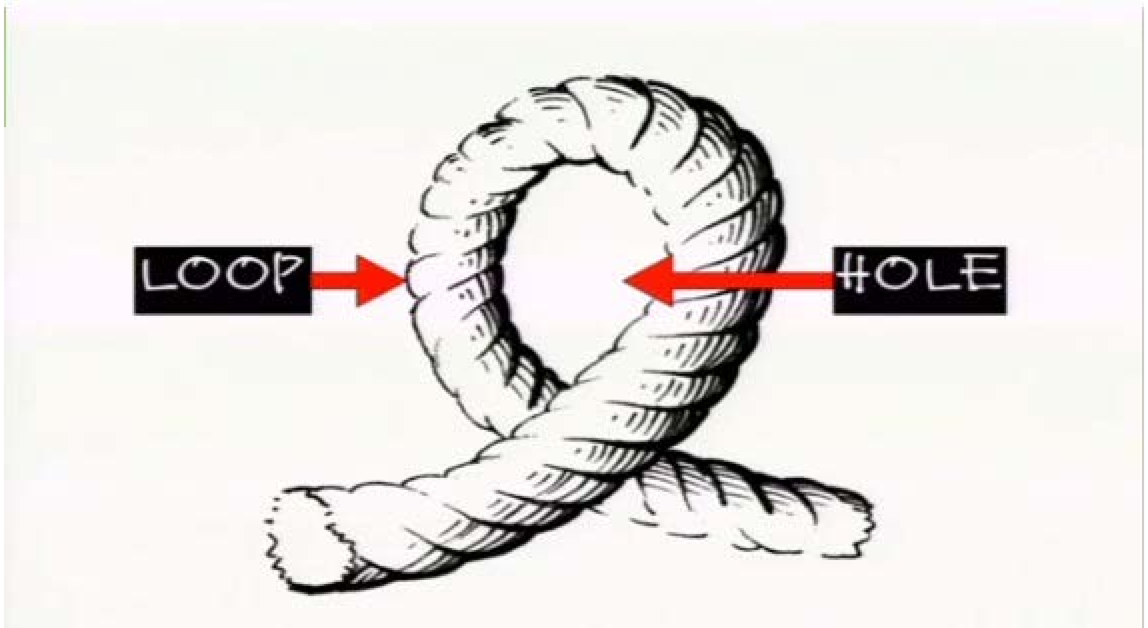
Which Tells Us John's:

- Name
- Home address
- Family
- Friends
- Politics
- Schools attended
- Hobbies
- Places of Interest
- Work location/coworkers
- Accounts/passwords

Attack Vectors

- Phishing/spearphishing
- Link attack
- Smart Phone hack
- Steal usernames/passwords for wireless attack

How Could John Have Thought Like an Operative?



How Can You Think Like an Operative?

- Assume there is always a loophole
- Don’t use same image on public sites that you use on hidden sites
- Educate yourself and company on threats
- Be aware that what you read isn’t always true
- Understand technical attacks
- Work together as a team

RSAC Studio

Connect to Protect

Think Like an Operative: Protect Sensitive Data

Tyler Cohen Wood

Cyber Security Advisor and Media Spokesperson

Inspired eLearning

#RSAC

RSAC Studio

Connect to Protect

Your Organization Is What It Eats - Software Supply Chain Analysis

Michael F. Angelo – CRISC, CISSP

Chief Security Architect
Micro Focus | NetIQ
@mfa0007

About Me...

YOUR LEISURE READING

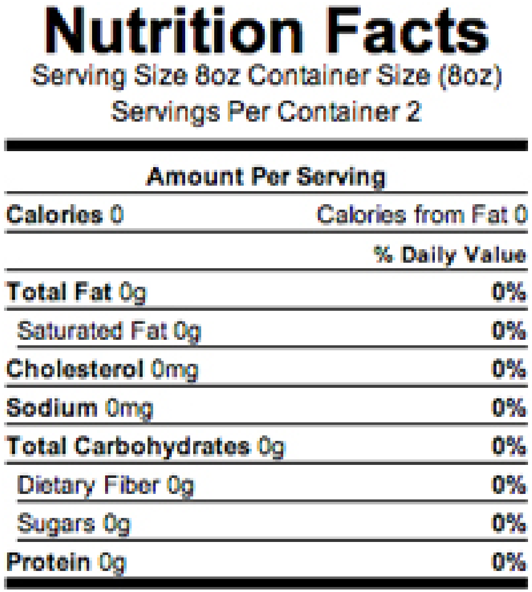
Michelangelo virus attacks P.C. data worldwide

Widespread

Gambling fever takes its toll in Australia

You Are What You Eat

Good Water

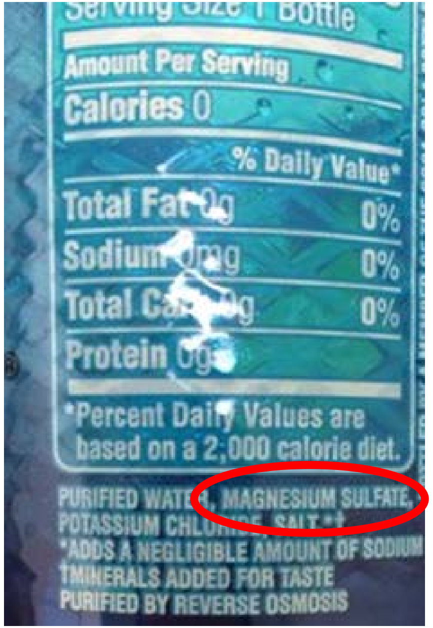


Nutrition Facts

Serving Size 8oz Container Size (8oz)
Servings Per Container 2

Amount Per Serving	
Calories 0	Calories from Fat 0
	% Daily Value
Total Fat 0g	**0%**
Saturated Fat 0g	**0%**
Cholesterol 0mg	**0%**
Sodium 0mg	**0%**
Total Carbohydrates 0g	**0%**
Dietary Fiber 0g	**0%**
Sugars 0g	**0%**
Protein 0g	**0%**

Good Water



Serving Size 1 Bottle

Amount Per Serving	
Calories 0	
	% Daily Value*
Total Fat 0g	0%
Sodium 0mg	0%
Total Carb 0g	0%
Protein 0g	

*Percent Daily Values are based on a 2,000 calorie diet.

PURIFIED WATER, MAGNESIUM SULFATE, POTASSIUM CHLORIDE, SALT.*†
*ADDS A NEGLIGIBLE AMOUNT OF SODIUM
†MINERALS ADDED FOR TASTE
PURIFIED BY REVERSE OSMOSIS

How is this Relevant?

- We consume software
  - Software is written for functionality, NOT security
  - Unknown vulnerabilities
  - Hacks are ultimately against software
- What you don’t know about….

Clean Bill of Cyber Health?

Where Does ~~Water~~ Software Come From?

Doesn’t Matter

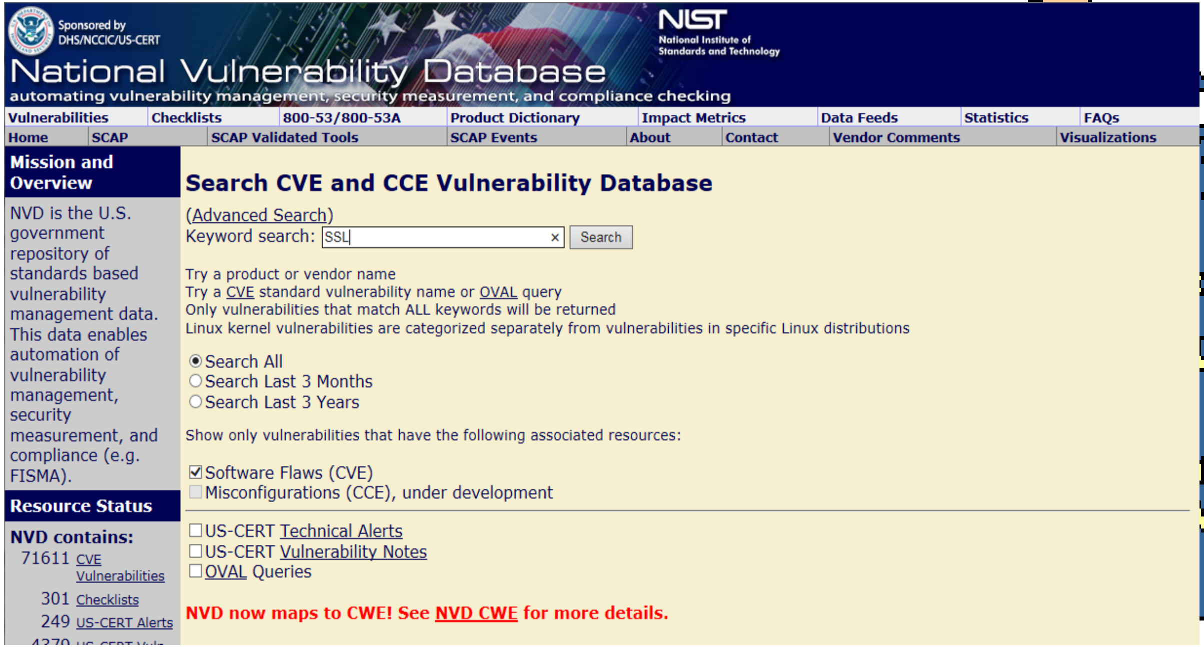
What Matters: Is It Secure?

© Martin Allen – 'The Rebel' http://www.differentaspects.com

Successful Software

Since 2013,
612 Java
Vulnerabilities

Good News - NVD



Sponsored by DHS/NCCIC/US-CERT

NIST National Institute of Standards and Technology

National Vulnerability Database

automating vulnerability management, security measurement, and compliance checking

Mission and Overview

NVD is the U.S. government repository of standards based vulnerability management data. This data enables automation of vulnerability management, security measurement, and compliance (e.g. FISMA).

Resource Status

NVD contains:

71611 CVE Vulnerabilities

301 Checklists

249 US-CERT Alerts

4370 US-CERT Vuln

Search CVE and CCE Vulnerability Database

(Advanced Search)

Keyword search: SSL

Try a product or vendor name

Try a CVE standard vulnerability name or OVAL query

Only vulnerabilities that match ALL keywords will be returned

Linux kernel vulnerabilities are categorized separately from vulnerabilities in specific Linux distributions

● Search All

○ Search Last 3 Months

○ Search Last 3 Years

Show only vulnerabilities that have the following associated resources:

☑ Software Flaws (CVE)

□ Misconfigurations (CCE), under development

□ US-CERT Technical Alerts

□ US-CERT Vulnerability Notes

□ OVAL Queries

NVD now maps to CWE! See NVD CWE for more details.

Reported Vulnerabilities - Past 5 Years

Year	CVEs
2011	4150
2012	5278
2013	5174
2014	7903
2015	6500

Other Successful Applications

- 2015[1] - 902,997,800 web servers
- 2014 CNN $\frac{2}{3}$ web servers - OpenSSL

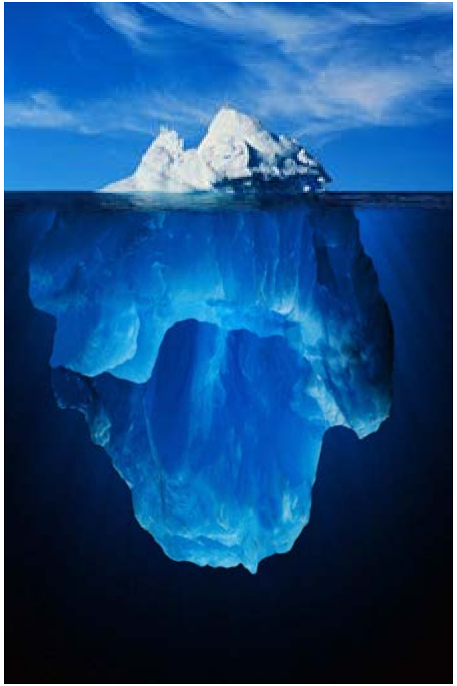
1 Potential Impact = ~602 Million

Year	CVE
2010	13
2011	7
2012	16
2013	12
2014	32
2015	35

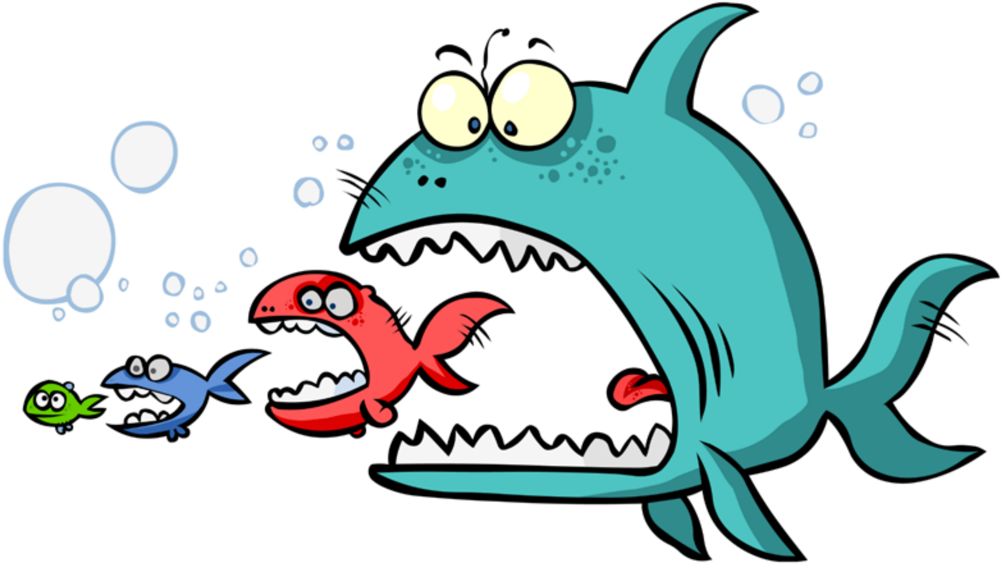
[1] http://news.netcraft.com/archives/2015/11/16/november-2015-web-server-survey.html

Next Problem….

- Products tested & analyzed for vulnerabilities
- Products consist of Components
  - Components are not visible
  - Vulnerabilities may not be visible at test time
- 2014, CVE spike was because of products with OpenSSL



Problem With Components



Proposed Solutions

- Government Approach
- Technical Approach

Technical Approach: Identify Software

- National Software Reference Library
  - http://www.nsrl.nist.gov/Downloads.htm
  - SHA1, MD5, and SHA256
- Online Queries
  - Nsrlsvr (http://rjhansen.github.io/nsrlsvr/)
  - Nsrllookup (http://rjhansen.github.io/nsrllookup/)

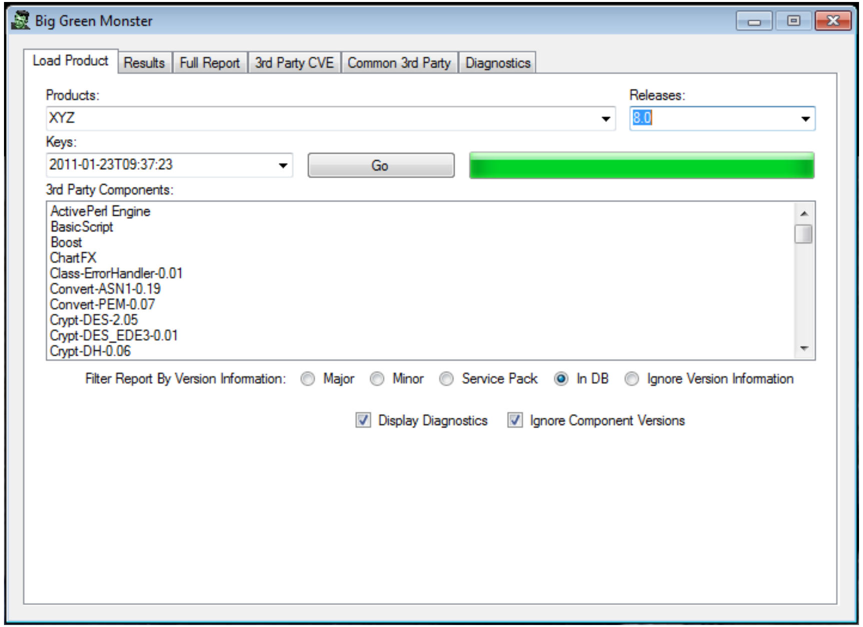
Technical Approach: Product Analysis

- Identify components in products
  - Copyright / Trademark / Version information
  - 3rd party license files
  - Hashes
- Assuming all components are identified
  - Name, Origin, Version
  - Can associate to product

Need Tools

- To *Identify* software, and associated components, in your environment
- Then the tool can
  - cross reference software to vulnerability in databases
  - raise awareness
  - provide sufficient information to enable you to test the PSV

Next Step: Build a Proof of Concept



Products: XYZ

Releases: 8.0

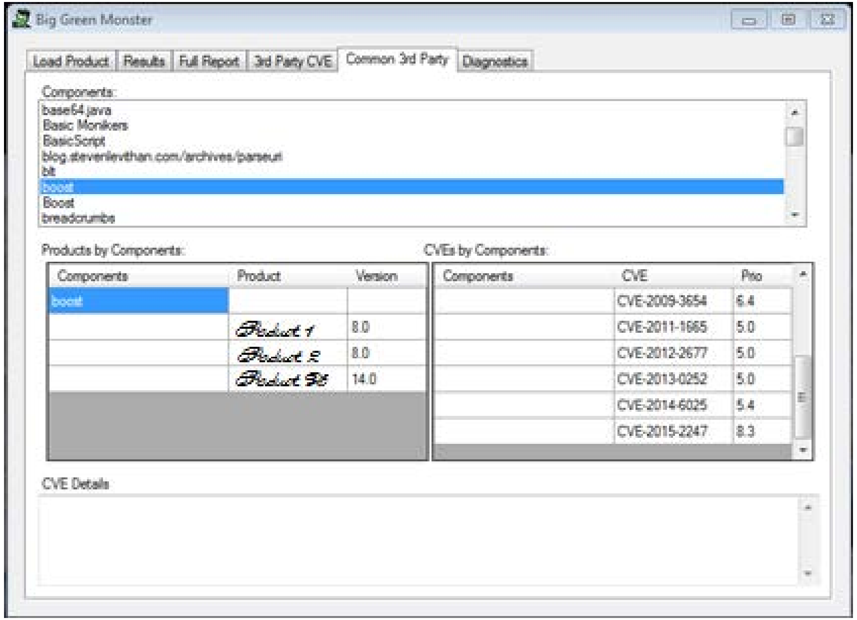
Keys: 2011-01-23T09:37:23

3rd Party Components:

- ActivePerl Engine
- BasicScript
- Boost
- ChartFX
- Class-ErrorHandler-0.01
- Convert-ASN1-0.19
- Convert-PEM-0.07
- Crypt-DES-2.05
- Crypt-DES_EDE3-0.01
- Crypt-DH-0.06

Filter Report By Version Information: ○ Major ○ Minor ○ Service Pack ● In DB ○ Ignore Version Information

☑ Display Diagnostics ☑ Ignore Component Versions



Components:

- base64.java
- Basic Monikers
- BasicScript
- blog.stevenlevithan.com/archives/parseuri
- bit
- boost
- Boost
- breadcrumbs

Products by Components:

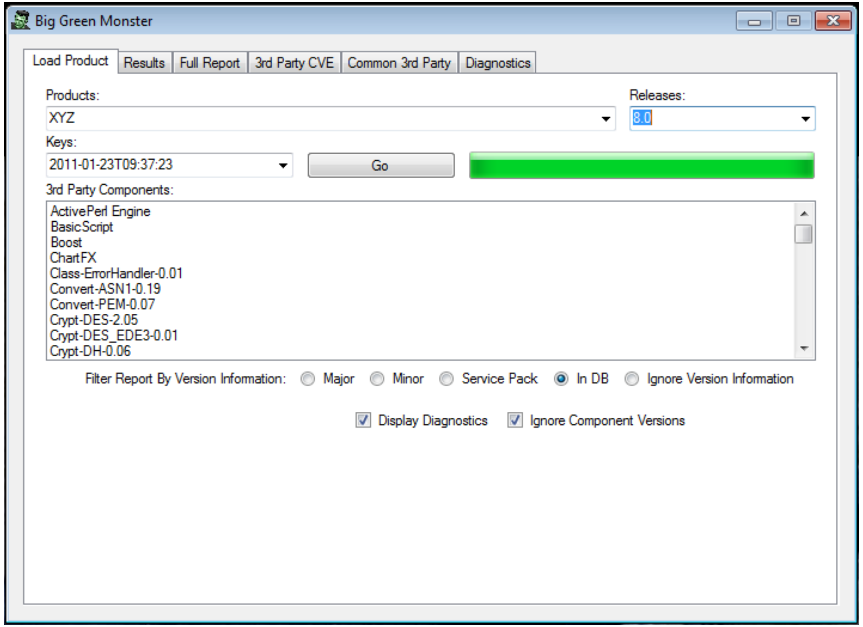
Components	Product	Version
boost		
	Product 1	8.0
	Product 2	8.0
	Product 98	14.0

CVEs by Components:

Components	CVE	Prio
	CVE-2009-3654	6.4
	CVE-2011-1665	5.0
	CVE-2012-2677	5.0
	CVE-2013-0252	5.0
	CVE-2014-6025	5.4
	CVE-2015-2247	8.3

CVE Details

Next Step: Build a Proof of Concept


Big Green Monster
Load Product | Results | Full Report | 3rd Party CVE | Common 3rd Party | Diagnostics
Go

Products: XYZ

Releases: 8.0

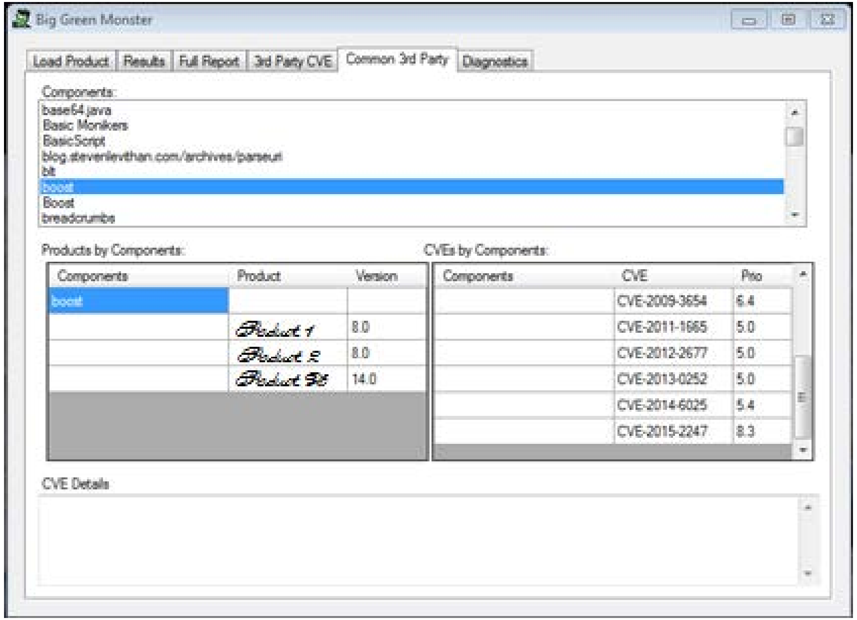
Keys: 2011-01-23T09:37:23

3rd Party Components:

ActivePerl Engine
BasicScript
Boost
ChartFX
Class-ErrorHandler-0.01
Convert-ASN1-0.19
Convert-PEM-0.07
Crypt-DES-2.05
Crypt-DES_EDE3-0.01
Crypt-DH-0.06

Filter Report By Version Information: ○ Major ○ Minor ○ Service Pack ● In DB ○ Ignore Version Information

☑ Display Diagnostics ☑ Ignore Component Versions


Big Green Monster
Load Product | Results | Full Report | 3rd Party CVE | Common 3rd Party | Diagnostics

Components:

base64.java
Basic Monikers
BasicScript
blog.stevenlevithan.com/archives/parseuri
blt
boost
Boost
breadcrumbs

Products by Components:

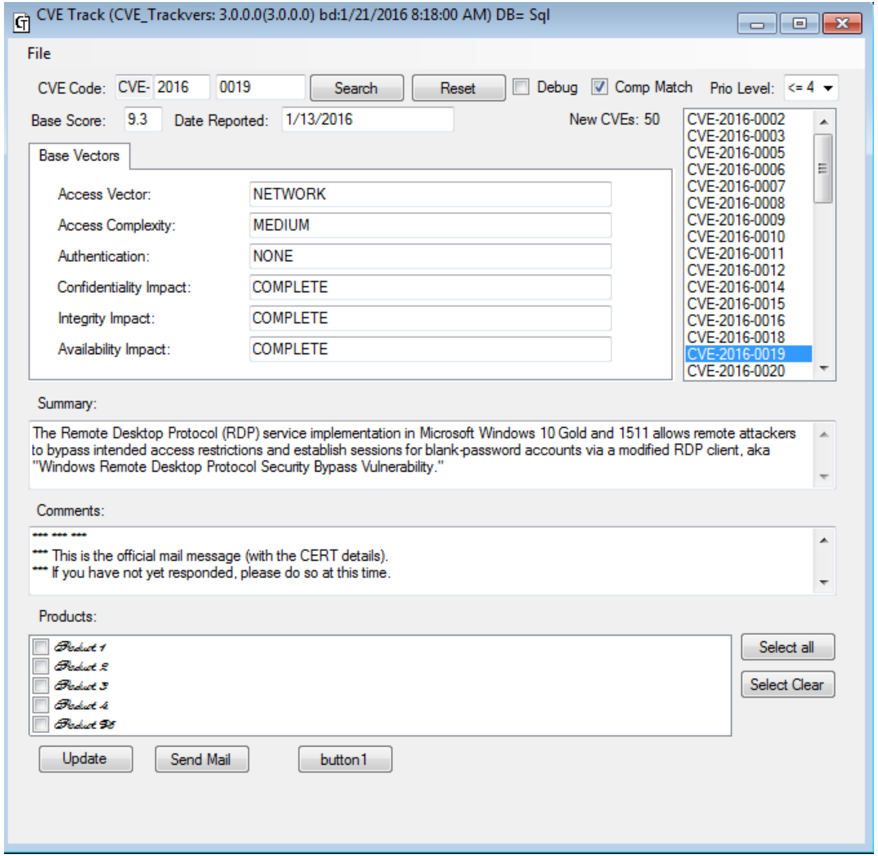
Components	Product	Version
boost		
	Product 1	8.0
	Product 2	8.0
	Product 98	14.0

CVEs by Components:

Components	CVE	Prio
	CVE-2009-3654	6.4
	CVE-2011-1665	5.0
	CVE-2012-2677	5.0
	CVE-2013-0252	5.0
	CVE-2014-6025	5.4
	CVE-2015-2247	8.3

CVE Details

Eventually…



CVE Track (CVE_Trackvers: 3.0.0.0(3.0.0.0) bd:1/21/2016 8:18:00 AM) DB= Sql

CVE Code: CVE- 2016 0019

□ Debug ☑ Comp Match Prio Level: <= 4

Base Score: 9.3 Date Reported: 1/13/2016

New CVEs: 50

CVE-2016-0002
CVE-2016-0003
CVE-2016-0005
CVE-2016-0006
CVE-2016-0007
CVE-2016-0008
CVE-2016-0009
CVE-2016-0010
CVE-2016-0011
CVE-2016-0012
CVE-2016-0014
CVE-2016-0015
CVE-2016-0016
CVE-2016-0018
CVE-2016-0019
CVE-2016-0020

Base Vectors

Access Vector:	NETWORK
Access Complexity:	MEDIUM
Authentication:	NONE
Confidentiality Impact:	COMPLETE
Integrity Impact:	COMPLETE
Availability Impact:	COMPLETE

Summary:

The Remote Desktop Protocol (RDP) service implementation in Microsoft Windows 10 Gold and 1511 allows remote attackers to bypass intended access restrictions and establish sessions for blank-password accounts via a modified RDP client, aka "Windows Remote Desktop Protocol Security Bypass Vulnerability."

Comments:

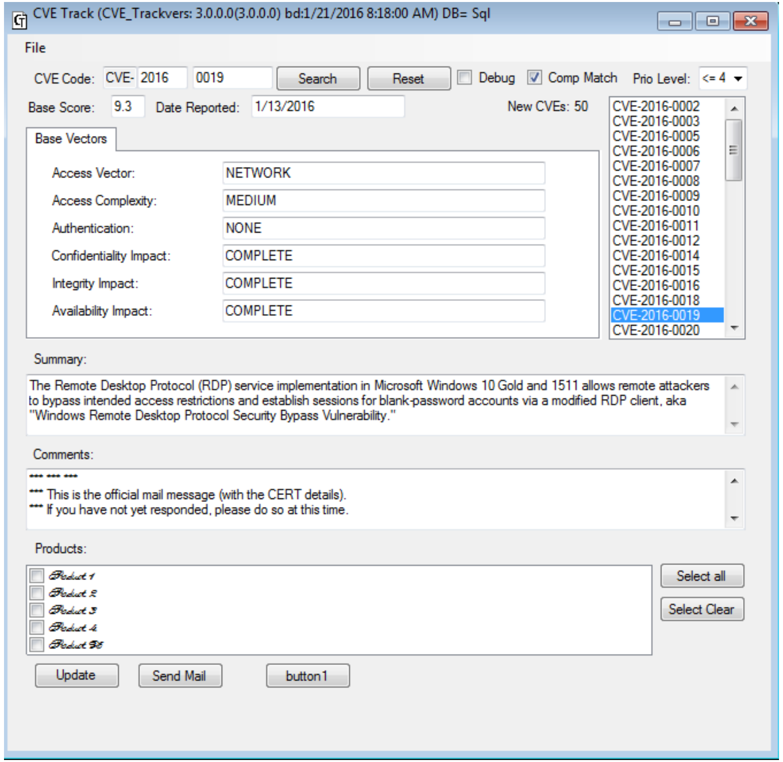
*** *** ***
*** This is the official mail message (with the CERT details).
*** If you have not yet responded, please do so at this time.

Products:

- □ Product 1
- □ Product 2
- □ Product 3
- □ Product 4
- □ Product 95

Caution

- Not every Vulnerability will be meaningful
- Every CVE would be marked as
  - Relevant, Not Relevant, Investigation
  - Mitigated, Not Mitigated, No mitigation needed



CVE Track (CVE_Trackvers: 3.0.0.0(3.0.0.0) bd:1/21/2016 8:18:00 AM) DB= Sql

CVE Code: CVE- 2016 0019 | Search | Reset | □ Debug | ☑ Comp Match | Prio Level: <= 4

Base Score: 9.3 | Date Reported: 1/13/2016 | New CVEs: 50

Base Vectors

Access Vector:	NETWORK
Access Complexity:	MEDIUM
Authentication:	NONE
Confidentiality Impact:	COMPLETE
Integrity Impact:	COMPLETE
Availability Impact:	COMPLETE

CVE-2016-0002
CVE-2016-0003
CVE-2016-0005
CVE-2016-0006
CVE-2016-0007
CVE-2016-0008
CVE-2016-0009
CVE-2016-0010
CVE-2016-0011
CVE-2016-0012
CVE-2016-0014
CVE-2016-0015
CVE-2016-0016
CVE-2016-0018
CVE-2016-0019
CVE-2016-0020

Summary:

The Remote Desktop Protocol (RDP) service implementation in Microsoft Windows 10 Gold and 1511 allows remote attackers to bypass intended access restrictions and establish sessions for blank-password accounts via a modified RDP client, aka "Windows Remote Desktop Protocol Security Bypass Vulnerability."

Comments:

```
*** *** ***
*** This is the official mail message (with the CERT details).
*** If you have not yet responded, please do so at this time.
```

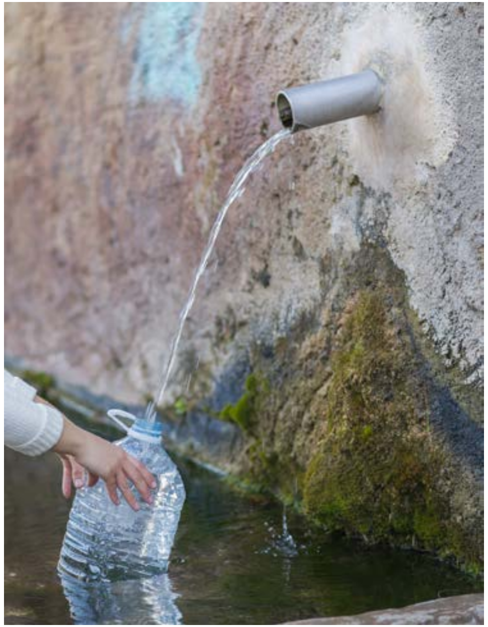
Products:

□ Product 1
□ Product 2
□ Product 3
□ Product 4
□ Product 98

Re-Cap Applying This Today

- Look at resources in this presentation
- Create a tool that:
  - Identifies components in software
  - Checks against CVE
  - Enables triage & communication of potential issues
- Spread the word & …

Remember



Don’t Poison Your Organization

Thank You

Michael F. Angelo – CRISC, CISSP
Chief Security Architect
Micro Focus | NetIQ
Michael.Angelo@Microfocus.com or Michael.Angelo@netiq.com
@mfa0007