THE FURRY AND THE SOUND

A mock disaster security vulnerability fable

CRob
Manager, Product Security Program Management
May 2, 2017

....with apologies to Faulkner

AGENDA

- A brief introduction
- What is an Incident and how do I know if I’m having one?
- 2017 The fury and the sound! Incident
- Questions

WHO IS THIS GUY?

CRob *(pronounced krobe)*

@RedHatCRob

Cat Herder

Red Hat Inc.

(actual title Manager, Product Security Program Management, but I'm like an Ambassador of Red Hat Security)

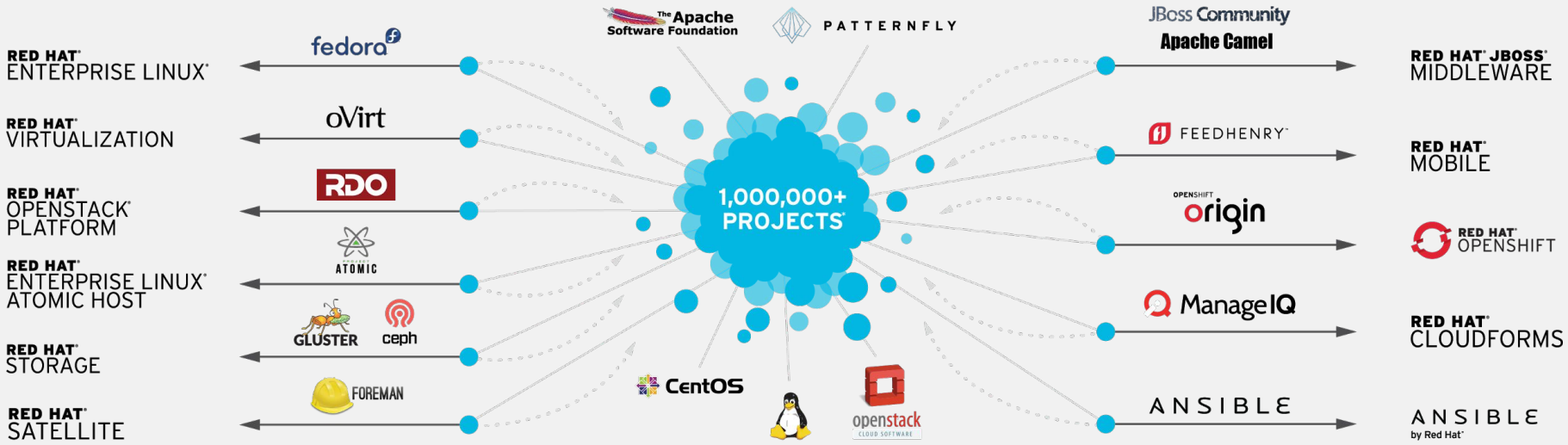
President, (ISC)2 CLE Chapter

CISSP, ITILv3, TOGAF9.1, MA, BS-er

Pirate and Security-enthusiast

19 years of Enterprise-class Operations, Engineering, and Security experience

COMMUNITY POWERED SECURITY



RH0064-3

WHY SHOULD I CARE ABOUT "INCIDENTS?"

“FUN” CYBERSECURITY FACTS

ANYONE CAN BE A TARGET

NO, YOU’RE NOT TOO SMALL. NO YOU DO NOT HAVE TO HAVE ANYTHING OF VALUE.

63% OF ALL ATTACKS IN 2016 WERE A RESULT OF

PASSWORD GUESSING/REUSING CREDENTIALS

PHISHING IS THE GO-TO ATTACK VECTOR

IF YOU HAVE A VALID EMAIL, CHANCES ARE THAT YOU’VE BEEN PHISHED

84% OF BREACHES TAKE MONTHS OR YEARS TO DISCOVER

SADLY, ~80% OF THOSE BREACHES ARE REPORTED TO YOU VIA AN EXTERNAL ENTITY
LAW ENFORCEMENT OF CUSTOMERS

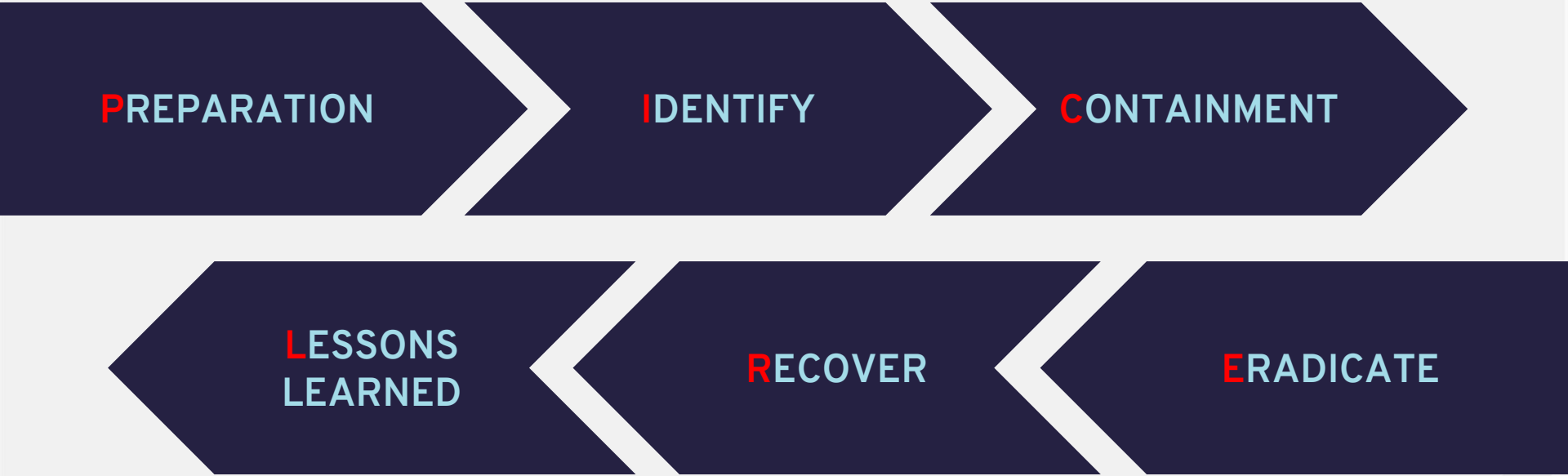
“HALF OF ALL EXPLOITATIONS HAPPEN BETWEEN

10 AND 100 DAYS AFTER THE VULNERABILITY IS PUBLISHED

http://www.verizonenterprise.com/resources/reports/rp_dbir-2016-executive-summary_xg_en.pdf

A CYBER-INCIDENT FABLE

THE STAGES OF AN INCIDENT - “PICERL”



https://www.sans.org/reading-room/whitepapers/incident/incident-handling-process-small-medium-businesses-1791

WHAT IS OUR COMPANY?

SportsBall.org.com

Our tagline:

"All your balls R belong to us."

Who are we?:

A hip social-sports-fantasysports-gaming-chill-dating-video-chat-micro/macroblogging spot

Source: http://memecrunch.com

THE PLAYERS

PRODUCT MANAGEMENT
Hey man, he's got a deadline to hit.

OUR CEO
Rags-to-riches-to MORE-riches story. She's the brainchild of our ideas and the charismatic figure behind the company.

SECURITY ARCHITECTURE
Highly technical, not highly-social. Yeah, he's THAT guy

IT OPS
The unsung heroes, keeping the place held together with bubblegum and popsicle sticks.

BUT WAIT... WE HAVE ONE MORE SEAT...

FOR YOU... YOU WILL BE OUR BOARD OF DIRECTORS

WHAT'S SPORTSBALL.ORG.COM'S RISK PROFILE?

- We're a young, energetic internet startup that isn't opposed to cut a few corners to meet a deadline.
- Our whole toolchain, infrastructure and application, exclusively runs on FOSS.
- Our "***SPortal!!!***" or Sports-Portal, is a mash-up of many different tools and apps (and is completely **EXTREME!**).
- *Sportsball.org.com* does deal with PII, and is toying with the idea of a for-fee service to access premium content.

Source: http://memecrunch.com

WHERE IS OUR PROBLEM?

Just days before the launch of an update to our flagship app into our SPortal!!!, *SportsBaller!!!* (It's **EXTREME!!!**), something strange happens to our CEO…..

Source: http://memecrunch.com

THE FURY AND THE SOUND

THE OPENING BELL

Malware can come in many forms. Infected image/video files are a "new" vector to think about. Our attack here is cross-platform and exploits a flaw in a mediaplayer demuxer.

*Do you *KNOW* what your users' permissions really are? How many executives "delegate" authority to assistants or grant proxy via mail/calendaring or other systems or even just give them their passwords?*

Frank McFrankface, assistant to Jane Everywoman, CEO of ***Sportsball.org.com*** receives and email from an old colleague. Attached to it is an amusing video featuring a cuddle kitty saying "Hey." He immediately plays the file in a popular mediaplayer.

https://www.youtube.com/watch?v=QNmjEPZBkDA
https://www.youtube.com/watch?v=sLCH1ZspSZw

THE ANATOMY OF A MODERN PHISH

This is how our attack today works….

One phish utilizing multiple vectors:

- Shortened url with redirects that try to beefhook the browser before going to content.
- "smb" url that attempts to get username & NTLM password hash (who filters ports 137, 138, 445?)
- Regular link if media can't be played, try it here: url
- Custom video content on the website
  - Links in the customer video content to malicious site(s)
  - Buffer overflow with exploit code: *note what it can do in memory*
  - Process injection
  - Purely Memory Resident

SHARING IS CARING

What are you doing for spam-filtering/phishing protection?

Most desktop controls are heuristic-based and cannot stop the latest attacks for days possibly even weeks.

Jane Everywoman is contacted by her close friend, Sally MacDevALot, thanking her for forwarding along an amusing cat video, but is curious why Sportsball.org.com sent her an invoice for $42.78?

Source: http://imgflip.com

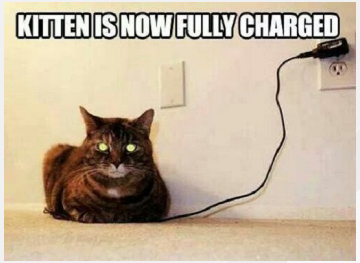
THUNDER IN THE DISTANCE?

Do you have a CI database of all devices, services running on them, and permitted connections to other devices/networks?

Do you know what your typical network traffic baseline is to know when it's different?

Bob Awesome, Sys Admin, RHCE, and Tiny House-enthusiast, is notified by his alerting/monitoring system of a significant uptick of access to the payroll and invoicing server from the CEO's workstation.

Petey Paranoid, Security Manager, gets a report from his Intrusion Detection System that there is a significant amount of network activity coming from an IP address that is NOT in the corporate configuration management system.



Source: http://images.google.com

THAT ESCALATED QUICKLY!

What are your organization's objectives in the event of a cyber-incident: Prosecute or Eradicate? - each has a very different reaction.

Do you have a cyber-incident response plan? What are your corporate and legal obligations when it comes to possible exposure of customer data?

Cathy Customerservice, manager of the *Sportsball.org.com* call center, sees calls coming in from customers asking about invoices. The Premium for-fee services have not officially been launched.

Jane Everywoman gets a call from someone named “L33Th@x0rVL@d421” telling her that her workstation has been encrypted, and for a small donation of 13 bitcoins he can give her the passcode to unlock it.

Source: http://images.google.com

LIGHT ON THE HORIZON

How do you get alerts from your vendors? What are YOUR business/operational priorities?

What are your emergency testing procedures?

Do you have hardening in place that could have avoided some of this?

Do you have SELinux on? (The default SELinux "out of the box" config blocks many of the high-profile attacks out today in traditional and cloud deployments)?

Bob Awesome is notified by his Linux vendor, Brown Shoe, of a severe issue impacting a popular media player.

There is no patch yet, but they offer a few mitigations and they have a Prancible script that could be used to push out the mitigations.

Source: http://images.google.com

WAT?

How do you manage traffic to/from your servers?

Can anyone log into anything on the network?

How would you KNOW if something was going on?

Bob Awesome using his automation tool, Prancible, pushes out the mitigation.

Hours after the initial fix is in place previously affected machines start experiencing high network loads almost as if they were being DDoS'ed from inside the network.

Source: http://images.google.com

(UN)SPREADING THE DISEASE

Can anyone install devices on your network?

What network access controls do you have in place?

How are you evaluating and then managing "Of Things" devices that are slipping into your networks?

Gus Grumpydba is called out of bed to restore possible/probable corrupt databases.

Bob Awesome uses his Hindsights hosted service to evaluate his affected devices and then his Sputnik managed server to get a list of devices managed that are exposed to the flaw.

Petey Paranoid works with Alice Arrogant, network engineer, and discovers that the Hospitality team recently installed several BlueberryCakes (a small *nix device) to manage the video displays in the corporate office and the EXTREME! Breakrooms. These devices were not entered into the CI system and are running a very old version of BluOS. The device has been found actively port-scanning the network now.

… BUT THEN

Backups and Patch Management - two of the MOST fundamental processes you MUST have.

Are they working well in your organization?

Do you have an Emergency Patching procedure?

How/where will you test fixes to ensure there are no regressions in YOUR environment?

Have you planned for personnel-related issues during a crisis?

Gus Grumpydba reports that the database backups have been failing for weeks. “It must be the server team’s fault,” he mutters as he logs off the Crisis Call. He doe not answer subsequent calls to his home or cell phone.

Bob Awesome gets the fixes from Brown Shoe and, after testing them in his test environment, starts scheduling updates.

Source: http://images.google.com

LESSONS LEARNED

Sportsball.org.com is on their way back to recovery. You saw how they did. How would YOU do if you were in this position?

Source: http://images.google.com

WRAPPING IT ALL UP...

Source: http://images.google.com

10 PRINCIPLES OF INCIDENT RESPONSE

Assign an executive responsible for the plan	Maintain relationships with SLAs and relationships with breach-remediation providers/experts
Develop a taxonomy of risks, threats and potential failure modes	Ensure the documented response plan is available to the entire organization
Develop easily accessible quick-response guides for each likely scenario	Make sure staff members understand their roles and responsibilities
Establish processes making major decisions	Identify individuals who are critical for incident response and ensure redundancy
Maintain relationships with key external stakeholders, such as law enforcement	Train, practice and run simulation breaches

RED HAT SUMMIT

THANK YOU

plus.google.com/+RedHatSupport

facebook.com/RedHatSupport

linkedin.com/company/red-hat

twitter.com/RedHatSecurity

youtube.com/user/RedHatVideos

APPENDIX

AGENDA

- A brief introduction
- What is an incident and how do I know I’m having one?
- 2017 The fury and the sound! incident
- Questions

Who is this guy?

CROB

@RedHatCRob

Cat Herder

Red Hat Inc.

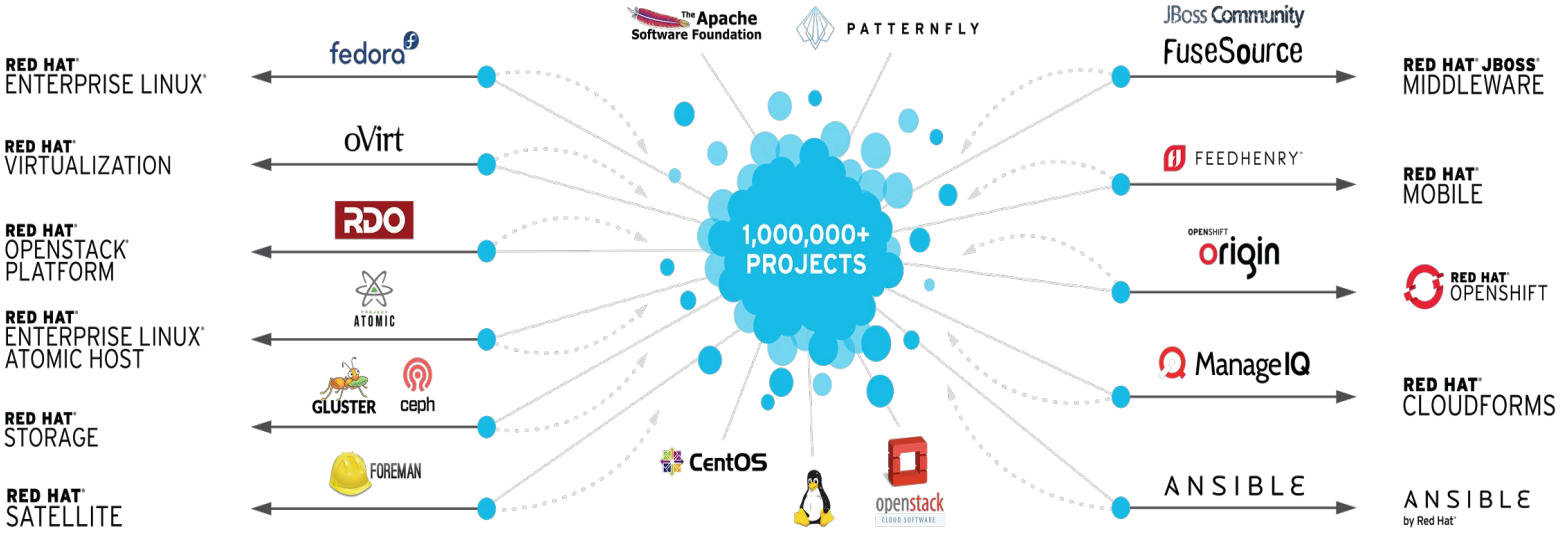
(actual title Manager, Product Security Program Management, but I'm like an Ambassador of Red Hat Security)

President, (ISC)2 CLE Chapter

CISSP, ITILv3, TOGAF9.1, MA, BS-er

Pirate and Security-enthusiast

19 years of Enterprise-class Operations, Engineering, and Security experience


RED HAT ENTERPRISE LINUX
RED HAT VIRTUALIZATION
RED HAT OPENSTACK PLATFORM
RED HAT ENTERPRISE LINUX ATOMIC HOST
RED HAT STORAGE
RED HAT SATELLITE
fedora
oVirt
RDO
ATOMIC
GLUSTER
ceph
FOREMAN
The Apache Software Foundation
PATTERNFLY
1,000,000+ PROJECTS
CentOS
openstack
JBoss Community FuseSource
FEEDHENRY
OPENSHIFT origin
ManageIQ
ANSIBLE
RED HAT JBOSS MIDDLEWARE
RED HAT MOBILE
RED HAT OPENSHIFT
RED HAT CLOUDFORMS
ANSIBLE by Red Hat

RH0064-3

“Fun” Cybersecurity facts….

- Anyone can be a target. No, you’re not too small and no you don’t not have anything of value.
- 63% of all attacks in 2016 were a result of password guessing/reusing valid credentials.
- Phishing (attacks via email) are the go-to attack vector; chances are if you have email, you’ve been phished.
- Most breaches (84%) take months or years to discover. Sadly, ~80% of those breaches are reported back to you via an external entity (Law Enforcement or Customers).
- “*Half of all exploitations happen between **10 and 100 days** after the vulnerability is published.*” - (VDBIR)
- “*sometimes you just can’t fix a vulnerability—be it because of a business process, a lack of a patch, or incompatibilities. At that point, for whatever reason, you may have to live with those residual vulnerabilities. It’s important to realize that mitigation is often just as useful as remediation—and sometimes it’s your only option.* “ - (VDBIR)

Source: 2016 Verizon Breach Report - http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/

Krebs on Security and his giant hand tell us….

SANS SECURING THE HUMAN

YOU ARE A TARGET

Username & Passwords

Once hacked, cyber criminals can install programs on your computer that capture all your keystrokes, including your username and password. That information is used to log into your online accounts, such as:

- *Your bank or financial accounts, where they can steal or transfer your money.*
- *Your iCloud, Google Drive, or Dropbox account where they can access all your sensitive data.*
- *Your Amazon, Walmart or other online shopping accounts where they can purchase goods in your name.*
- *Your UPS or Fedex accounts, where they ship stolen goods in your name.*

Email Harvesting

Once hacked, cyber criminals can read your email for information they can sell to others, such as:

- *All the names, email addresses and phone numbers from your contact list.*
- *All of your personal or work email.*

Virtual Goods

Once hacked, cyber criminals can copy and steal any virtual goods you have and sell them to others, such as:

- *Your online gaming characters, gaming goods or gaming currencies.*
- *Any software licenses, operating system license keys, or gaming licenses.*

Botnet

Once hacked, your computer can be connected to an entire network of hacked computers controlled by the cyber criminal. This network, called a botnet, can then be used for activities such as:

- *Sending out spam to millions of people.*
- *Launching Denial of Service attacks.*

You may not realize it, but you are a target for cyber criminals. Your computer, your mobile devices, your accounts and your information all have tremendous value. This poster demonstrates the many different ways cyber criminals can make money by hacking you. Fortunately, by taking some simple steps, you can help protect yourself and your family. To learn more, subscribe to OUCH!: a security newsletter designed to help people just like you.

www.securingthehuman.org/ouch

Identity Hijacking

Once hacked, cyber criminals can steal your online identity to commit fraud or sell your identity to others, such as:

- *Your Facebook, Twitter or LinkedIn account.*
- *Your email accounts.*
- *Your Skype or other IM accounts.*

Web Server

Once hacked, cyber criminals can turn your computer into a web server, which they can use for the following:

- *Hosting phishing websites to steal other people's usernames and passwords.*
- *Hosting attacking tools that will hack people's computers.*
- *Distributing child pornography, pirated videos or stolen music.*

Financial

Once hacked, cyber criminals can scan your system looking for valuable information, such as:

- *Your credit card information.*
- *Your tax records and past filings.*
- *Your financial investments and retirement plans.*

Extortion

Once hacked, cyber criminals can take over your computer and demand money. They do this by:

- *Taking pictures of you with your computer camera and demanding payment to destroy or not release the pictures.*
- *Encrypting all the data on your computer and demanding payment to decrypt it.*
- *Tracking all websites you visit and threatening to publish them.*

This poster is based on the original work of Brian Krebs. You can learn more about cyber criminals at his blog at http://krebsonsecurity.com

Source: https://krebsonsecurity.com/2013/01/you-are-a-target-poster-builds-on-hacked-pc-graphic/

A Cyber-Incident Fable

Source: http://images.google.com

The Stages of an Incident

Preparation
Identify
Containment
Eradicate
Recover
Lessons Learned

Source: http://images.google.com

Who are we today?

SportsBall.org.com

Tagline - “All your balls R belong to us”

A hip social-sports-fantasysports-gaming-chill-dating-video-chat-micro/macroblogging spot

Source: http://memecrunch.com

The Players

Source: http://images.google.com

The Players

Product Management – Hey man, he's got a deadline to hit.

Our CEO – Rags-to-Riches-to-MORE-riches story. She's the brainchild of our ideas and the charismatic figure behind the company.

Security Architecture – Highly technical, not highly-social. Yeah, he's THAT guy.

IT Ops - the unsung heroes, keeping the place held together with bubblegum and popsicle sticks.

Source: http://images.google.com

But wait...we have one more seat...

For YOU…. You will be our Board of Directors

Source: http://images.google.com

What's Sportsball.org.com's Risk Profile?

- We're a young, energetic internet startup that isn't opposed to cut a few corners to meet a deadline.
- Our whole toolchain, infrastructure and application, exclusively runs on FOSS.
- Our "***SPortal!!!***" or Sports-Portal, is a mash-up of many different tools and apps (and is completely EXTREME!).
- *Sportsball.org.com* does deal with PII, and is toying with the idea of a for-fee service to access premium content.

Source: http://images.google.com

Where is our problem?

Just days before the launch of an update to our flagship app into our SPortal!!!, *SportsBaller!!!* (It's **EXTREME!!!**), something strange happens to our CEO…..

Source: http://images.google.com

The Furry and the Sound

Source: http://images.google.com

The Opening Bell

Frank McFrankface, assistant to Jane Everywoman, CEO of *Sportsball.org.com* receives an email from an old colleague. Attached to it is an amusing video featuring a cuddle kitty saying “Hey”. He immediately plays the file in a popular mediaplayer.

https://www.youtube.com/watch?v=QNmjEPZBkDA
https://www.youtube.com/watch?v=sLCH1ZspSZw

Malware can come in many forms. Infected image/video files are a “new” vector to think about. Our attack here is cross-platform and exploits a flaw in a mediaplayer demuxer.

*Do you *KNOW* what your users’ permissions really are? How many executives “delegate” authority to assistants or grant proxy via mail/calendaring or other systems or even just give them their passwords?*

Source: http://images.google.com

The Anatomy of a modern Phish

This is how our attack today works….

1 phish utilizing multiple vectors:

- shortened url with redirects that try to beefhook the browser before going to content.
- "smb" url that attempts to get username & NTLM password hash (who filters ports 137, 138, 445?)
- regular link if media can't be played, try it here: url
- custom video content on the website
  - links in the custom video content to malicious site(s)
  - buffer overflow with exploit code: *note what it can do in memory*
  - **Process Injection:** Process injection is simply the method to inject into an already running process. By injecting into a process, the information of the application can be hidden within a process that would normally be trusted in nature. It's very difficult for preventative measure technology to inspect running processes and can almost always hide in a different process that the application would think is a trusted one.
  - **Purely Memory Resident**: Memory resident attacks are generally the most preferred as most technologies do not inspect memory. As an attacker, finding a way to live in memory purely would be most desirable. When writing to disk, most applications will conduct scans, baselines, and other identifications of potentially malicious software. The ability to be detected when writing to disk becomes significantly greater.

Source: http://images.google.com

Sharing is Caring

Jane Everywoman is contacted by her close friend, Sally MacDevALot, thanking her for forwarded along an amusing cat video, but is curious why *Sportsball.org.com* sent her an invoice for $42.78?

What are you doing for spam-filtering/phishing protection? Most desktop controls are heuristic-based and can not stop the latest attacks for days possibly even weeks.

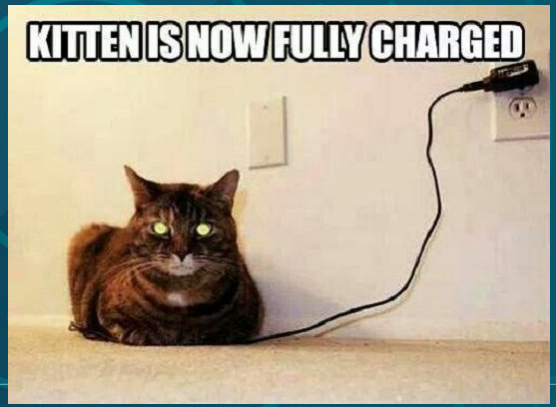
Source: http://imgflip.com

Thunder in the distance?

Bob Awesome, sysadmin, RHCE, and Tiny House-enthusiast is notified by his alerting/monitoring system of a significant uptick of access to the Payroll & Invoicing server from the CEO's workstation

Petey Paranoid, Security Manager, gets a report from his Intrusion Detection System that there is a significant amount of network activity coming from an IP address that is NOT in the corporate configuration management system

Do you have a CI database of all devices, services running on them, and permitted connections to other devices/networks? Do you know what your typical network traffic baseline is to know when it's different?



Source: http://images.google.com

THAT escalated quickly!

Cathy Customerservice, manager of the *Sportsball.org.com* call center sees calls coming in from customers asking about invoices. The Premium for-fee services have not officially been launched yet.

Jane Everywoman gets a call from someone named “L33Th@x0rVL@d421” telling her that her workstation has been encrypted, and for the small donation of 13 bitcoins he can give her the passcode to unlock it.

What are your organization's objectives in the event of a cyber-incident: Prosecute or Eradicate? - each has a very different reaction. Do you have a cyber-incident response plan? What are your corporate and legal obligations when it comes to possible exposure of customer data?

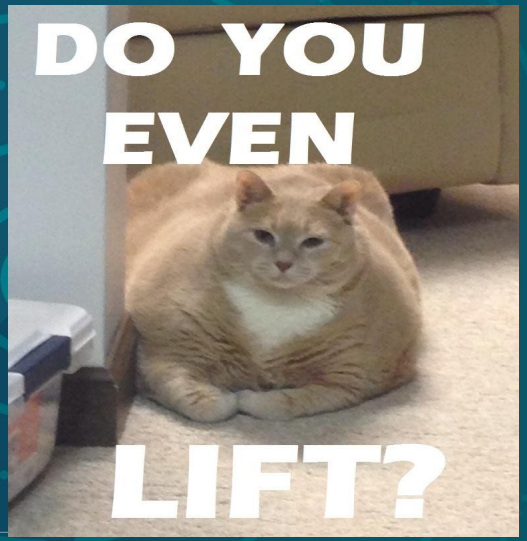
Source: http://images.google.com

Light on the Horizon

Bob Awesome is notified by his Linux vendor, Brown Shoe, of a severe issue impacting a popular media player.

There is no patch yet, but they offer a few mitigations and they have a Prancible script that could be used to push the mitigations out.

How do you get alerts from your vendors? What are YOUR business/operational priorities? What are your emergency testing procedures? Do you have hardening in place that could have avoided some of this? Do you have SELinux on? (The default SELinux "out of the box" config blocks many of the high-profile attacks out today in traditional and cloud deployments)?



Source: http://images.google.com

wat

Bob Awesome using his automation tool, Prancible, pushes out the mitigation.

Hours after the initial fix is in place previously affected machines start experiencing high network loads almost as if they were being DDoS'ed from inside the network.

How do you manage traffic to/from your servers? Can anyone log into anything on the network? How would you KNOW if something was going on?

Source: http://images.google.com

(Un)Spreading the Disease

Bob Awesome uses his Hindsights hosted service to evaluate his affected devices and then his Sputnik management server to get a list of devices managed that are exposed to the flaw.

Gus Grumpydba is called out of bed to restore possible/probable corrupt databases.

Petey Paranoid works with Alice Arrogant, network engineer, and discovers that the Hospitality team recently installed several BlueberryCakes (a small *nix device) to manage the video displays in the corporate office and the **EXTREME!** breakrooms. These devices were not entered into the CI system and are running a very old version of BluOS. The device has been found actively port-scanning the network now.

Can anyone install devices on your network? What network access controls do you have in place? How are you evaluating and then managing "Of Things" devices that are slipping into your networks?

Source: http://images.google.com

...but then

Gus Grumpydba reports that the database backups have been failing for weeks. "It must be the server team's fault" he mutters as he logs off the Crisis Call. He does not answer subsequent calls to his home or cell phone.

Bob Awesome gets the fixes from Brown Shoe and after testing them in his test environment starts scheduling updates.

Backups and Patch Management - two of the MOST fundamental processes you MUST have. Are they working well in your organization? Do you have an Emergency Patching procedure? How/where will you test fixes to ensure there are no regressions in YOUR environment? Have you planned for personnel-related issues during a crisis?

Source: http://images.google.com

Lessons Learned?

So Sportsball.org.com is on their way back to recovery. You saw how they did, how would YOU do if you were in this position?

Source: http://images.google.com

Wrapping it all up...

Source: http://images.google.com

Threat Modeling Sportball.org.com

JUST FOR NOTES - REMOVE ONCE READY

Threat Modeling 101

$ACTORS taking $ACTIONS against $ASSETS via $VECTOR for $OUTCOMES because of $MOTIVATIONS

Threat - The term "threat" refers to the source and means of a particular type of attack. A threat assessment is performed to determine the best approaches to securing a system against a particular threat, or class of threat. **Threats (effects) generally can NOT be controlled**

Risk - The term "risk" refers to the likelihood of being targeted by a given attack, of an attack being successful, and general exposure to a given threat. A risk assessment is performed to determine the most important potential security breaches to address now, rather than later. **Risk CAN be mitigated**

Vulnerability - The term "vulnerability" refers to the security flaws in a system that allow an attack to be successful. Vulnerability testing should be performed on an ongoing basis by the parties responsible for resolving such vulnerabilities, and helps to provide data used to identify unexpected dangers to security that need to be addressed. Such vulnerabilities are not particular to technology -- they can also apply to social factors such as individual authentication and authorization policies. **Vulnerabilities CAN be treated**

Source: http://images.google.com

The 10 Principles of Incident Response

1.) Assign an executive responsible for the plan.
2.) Develop a taxonomy of risks, threats, potential failure modes.
3.) Develop easily accessible quick-response guides for likely scenario.
4.) Establish processes for making major decisions.
5.) Maintain relationships with key external stakeholders, such as law enforcement.
6.) Maintain SLAs and relationships with breach-remediation providers/experts.
7.) Ensure the documented response plan is available to the entire organization.
8.) Make sure staff members understand their roles and responsibilities.
9.) Identify individuals who are critical for incident response and ensure redundancy.
10.) Train, practice, and run simulated breaches.

Source: http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf

JUST FOR NOTES - REMOVE ONCE READY