Defensive InfoSec

Marc Silver
Discovery Limited
@bsdkid

Defensive InfoSec

Why we need to Think Differently

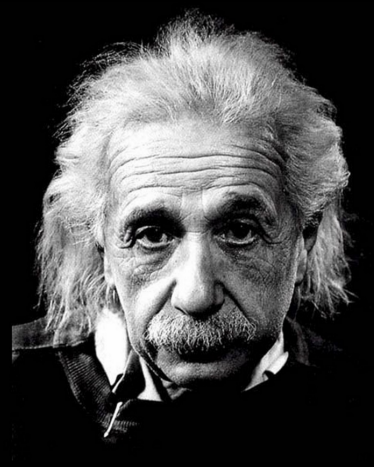
Hello
my name is

Marc Silver (@bsdkid)

Sysadmin Background, InfoSec Obsession

Information Security @ Discovery Limited

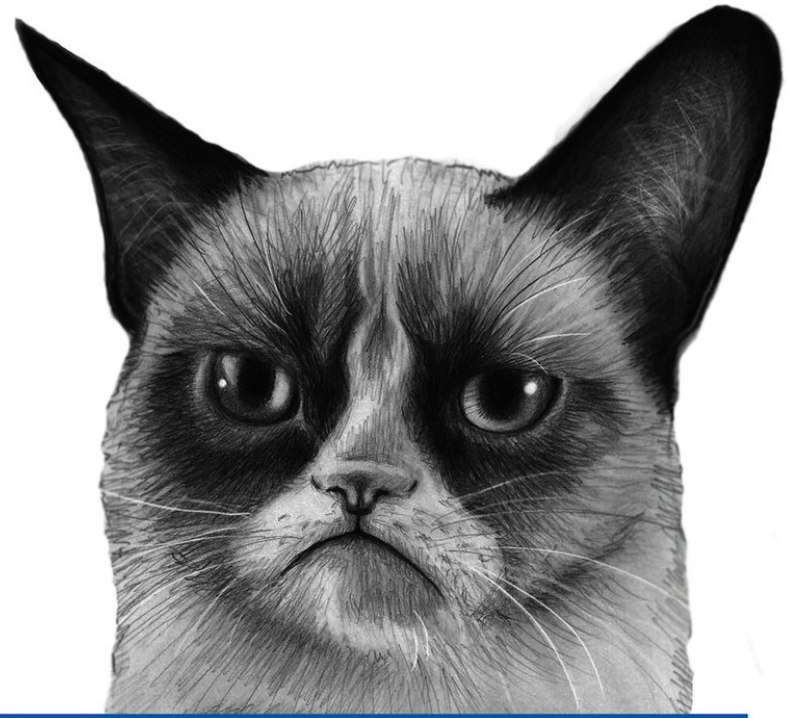
What’s wrong with our current approach?



Insanity: doing the same thing over and over and expecting different results.

- Albert Einstein

You're a 10x hacker and it must be someone else's fault.



Blaming the User

Pocket Reference

O RLY?

@ThePracticalDev

Let’s just be honest

- One of these files contains malware…

Name	Date modified	Type	Size
what_could_go_wrong.pdf	12/10/2015 10:48 ...	Adobe Acrobat D...	3,502 KB
totally_legit.pdf	9/9/2010 3:13 PM	Adobe Acrobat D...	6,176 KB

- What chance do your users have?

Even technical users are at risk

The Linux Mint Blog

News from the Mint Team

« Monthly News – January 2016 |

Beware of hacked ISOs if you downloaded Linux Mint on February 20th!

Written by **Clem** on Sunday, February 21st, 2016 @ 1:44 am | Main Topics

Tweet Share 1981 Like 2K

I'm sorry I have to come with bad news.

We were exposed to an intrusion today. It was brief and it shouldn't impact many people, but if it impacts you, it's very important you read the information below.

What happened?

Hackers made a modified Linux Mint ISO, with a backdoor in it, and managed to hack our website to point to it.

While we're being honest

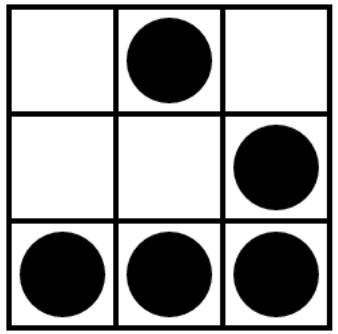
Security is not easy, and it's not convenient. Users implicitly trust their IT departments to keep them safe. And we're failing them dismally…

Still, $$$

Richard Thieme @neuralcowboy

"My job," said an infosec guru, "is to keep orgs from getting owned. They all get owned so I guess I pretty much suck at my job." still, $$$

24 Likes	**26** Retweets
11 Feb 2016 at 23:24	via **Twitter Web Client**



“Hacker Culture”

The **hacker culture** is a subculture of individuals who enjoy the intellectual challenge of creatively overcoming and circumventing limitations of systems to achieve novel and clever outcomes.

https://en.wikipedia.org/wiki/Hacker_culture

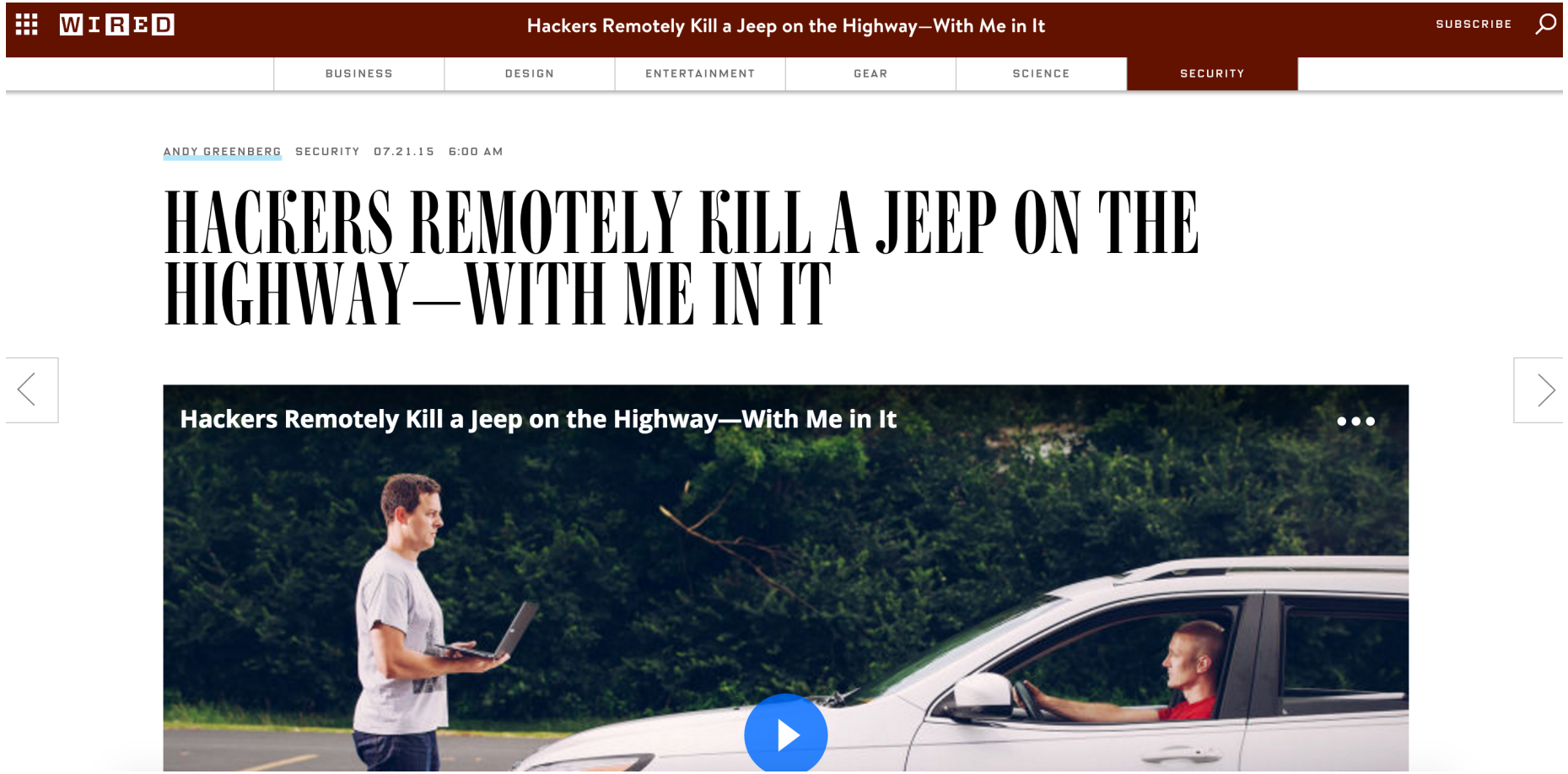
So why does that matter?

Defense is Hard

It seems to me that NSA does not yet have much expertise in computer security. Rather, we are expert in computer insecurity. We do much better in finding security vulnerabilities in any computer complex than in proposing security architectures for them. Somehow, the attack seems more challenging (fun) than the defense, and this seems true in the general business of cryptosystem design as well. A spin-off of this syndrome manifests itself when a security modification is needed for an existing crypto-equipment. In my experience, most design engineers would *much* rather attack a brand new problem – meet a new and difficult requirement – starting from scratch, pushing the electronic state of the art, exercising opportunities for innovation, and so on than go through the drudgery of a mere "fix" accepting all the constraints of configuration and technology in some pre-existing piece of hardware.

A History of U.S. Communications Security, David Boake, NSA (1973)
http://www.governmentattic.org/18docs/Hist_US_COMSEC_Boak_NSA_1973u.pdf

Offense is just cooler…



Defenders Challenges

Defenders conundrum

- Defenders are required to protect everything *equally*.
- Attackers do not play by the same rules; they require a single weak point to gain entry.
- Attacks are developed faster than defensive techniques.

Defenders conundrum

- Security products are sold around the latest hype-cycle.

- Defenders hold cards too close to their chests in many cases; knowledge sharing is still relatively poor.

Gaining access is trivial

Photo Credit:
Kim Zetter

Even nation states don’t need 0day

Another common attack vector is common vulnerabilities and exposures (CVEs) that haven’t been patched, he said. Companies need to make automatic patching the norm to protect themselves against nation-state hackers he warned. As for zero-day flaws, he said they are overrated.

“A lot of people think that nation states are running their operations on zero days, but it’s not that common,” he said. “For big corporate networks persistence and focus will get you in without a zero day; there are so many more vectors that are easier, less risky, and more productive.”

As for the NSA’s own collection of zero-day exploits, Joyce said that in fact the agency had very few and each new one was discovered was evaluated by an outside committee to see when software manufacturers should be informed to build a patch. The NSA doesn’t have the final decision on this, he claimed.

Rob Joyce, NSA chief of Tailored Access Operations (2015)

- 0 day vulnerabilities are available (some at a reasonable price), but attackers don’t need them anyway.

Or to put it better…

the grugq @thegrugq

Give a man an 0day and he'll have access for a day, teach a man to phish and he'll have access for life.

594 Faves	**1 010** Retweets
07 Feb 2015 at 09:35	via **Tweetbot for iOS**

Our own tools can work against us

Tavis Ormandy @taviso

@unixgeekem @flameeyes The problem isn't bypassing, the problem is that AV software is dangerously insecure and makes things worse.

16 Faves	**10** Retweets
26 Jan 2016 at 17:55	via **Twitter Web Client**

It’s easy to feel hopeless;

Defenders are on the back foot…


The gold standard?

A look at the financial sector

- Average time in financial sector to apply security patches is 176 days.*
- Massive reliance on perimeter technologies to protect us. **
- InfoSec budgets are typically 8-10% of total IT spend.
- Much focus is still spent on stopping external threats.

* http://www.zdnet.com/article/financial-sector-takes-176-days-on-average-to-patch-security-vulnerabilities/
** https://www.sans.org/reading-room/whitepapers/analyst/security-spending-preparedness-financial-sector-survey-36032

Gold standard?

ars technica

MAIN MENU MY STORIES: 25 FORUMS SUBSCRIBE JOBS

RISK ASSESSMENT / SECURITY & HACKTIVISM

Billion dollar Bangladesh hack: SWIFT software hacked, no firewalls, $10 switches

The Bangladesh Bank's internal network security was sorely lacking.

by **Peter Bright** - Apr 26, 2016 12:15am SAST

Share Tweet Email 69

The Bangladesh central bank had no firewall and was using a second-hand $10 network when it was hacked earlier this year. Investigation by British defense contractor BAE Systems has also shown that the SWIFT software used to make payments was compromised, enabling the hackers to send money around the world without leaving any trace in Bangladesh.

… so with attacks (seemingly) on the increase we don’t seem to be getting better at the basics...

Attacks will technically be perpetrated internally – either by actual staff members, or by attackers who are using staff credentials and who have control of staff assets.

that said...

Attackers have challenges of their own…

“He who makes war without any mistakes
has not made war very long”

-- Napoleon Bonaparte

Analysis of an attack

- We all *know* the Lockheed Martin kill chain. *zzzzzz*
- As defenders, we should be learning from attackers. Unless we understand their methods, we are doomed to fail.
- Attackers leave traces. And they make mistakes…

Windows

- Box gets owned.
- cmd.exe typically used and system profiling generally occurs (systeminfo etc).
- Tasklist, netstat, net use, reg query etc.

Linux

- Box gets owned.
- Shell gets spawned and system profiling occurs.
- netstat, iptables, lsof etc.

Persistence?

Persistence

- Download toolkit/malware for persistence.
- Ensure service, registry or other mechanism to auto-start.
- Escalate privileges (assuming not done already).
- Lots of places to look; windows services, registry, DLL search order hijacking, GPO, AT, WMI…

Lateral movement and exfiltration

- Browse at attackers leisure gathering data.
- Exfil…
- Repeat ad-infinitum until complete, discovered or bored.

Attackers Conundrum

- Defenders have the upper hand; this is **your** environment.
- Attackers need to tread carefully so as not to set off alarm bells (assuming you have any).
- Attackers need varying amounts of time to perform many actions – and they are vulnerable during these times.

This presents us with opportunities for detection…

Current methods of detection

Threat Feeds

Anti Virus

IDS / IPS / HIPS

Proxy technologies (URL filtering etc.)

Signature detection is failing us

DLP

SSL is helping (and hurting) us…

Log correlation and SIEM

Still the proverbial needle

Pen Tests

Current methods are not 100% effective…

We are still squishy on the inside...

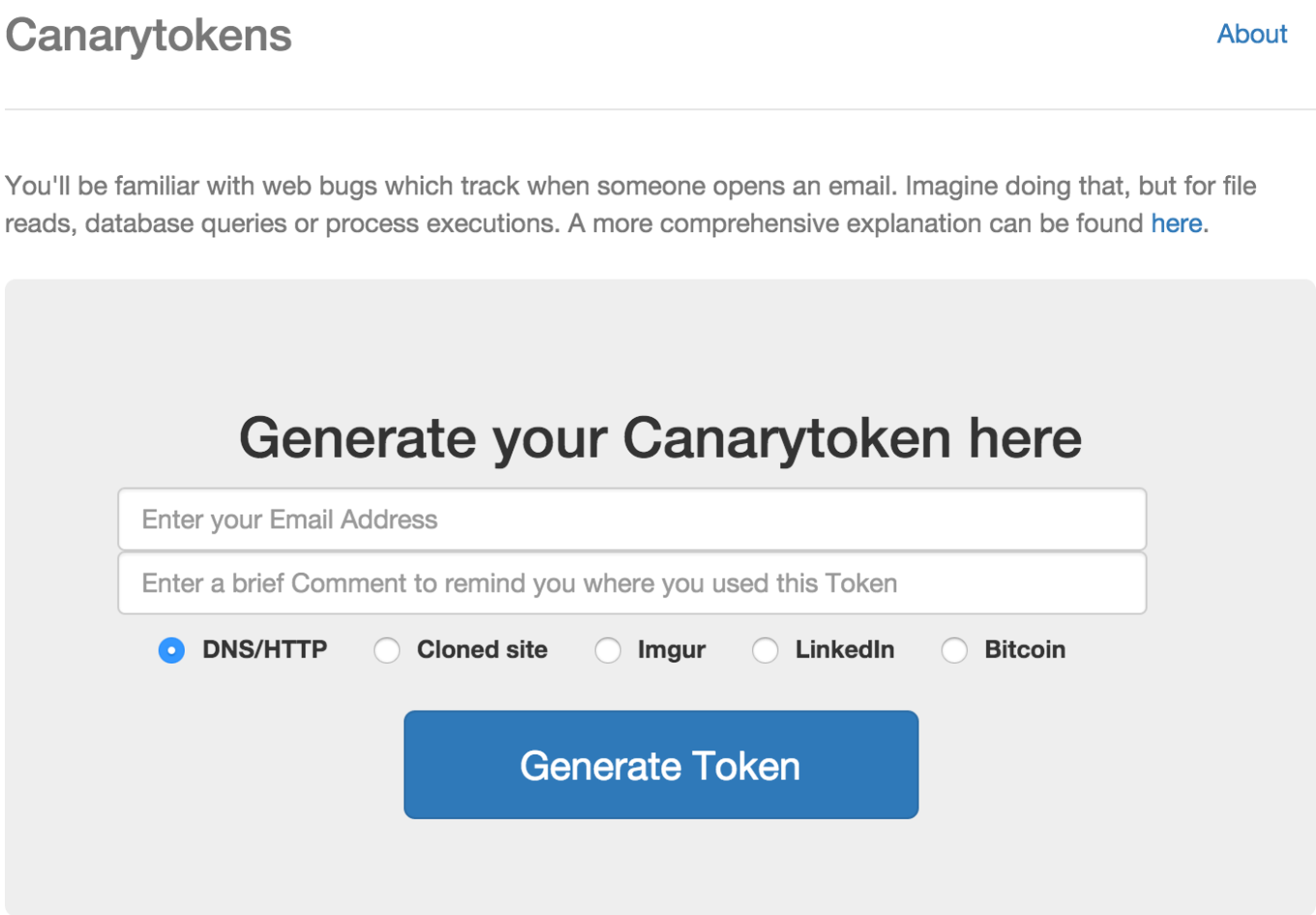
So should you be getting rid of what you have?


NOPE

Promising new technologies

Canary

Canary Tokens



Endpoint Detection & Machine Learning

Thinking a bit differently…

Your best defense

Your staff and their l33t skillz


Enthusiasm is important


INNOVATE NEVER
IMITATE!

Let’s look at some examples

Configuration management

CFEngine

SALTSTACK

puppet labs®

CHEF

Configuration management

```
Running 05-sshd-config...
 Checking '/etc/ssh/sshd_config' ... [OK]
Module runtime: 0 seconds

Running 06-ssh-config...
 This module only applies to RHEL7 currently
Module runtime: 0 seconds

Running 10-selinux...
 Checking '/etc/selinux/config'... [OK]
 Checking current selinux status... [OK]
Module runtime: 0 seconds

Running 11-logrotate...

Module runtime: 0 seconds

Running 12-ulimits...
 Checking '/etc/security/limits.d' ... [OK]
 Checking '/etc/security/limits.d/99-limits-tisec.conf' ... [OK]
Module runtime: 0 seconds

Running 20-bash-customisations...
Module runtime: 0 seconds
```

Configuration management

```
Running 60-user-provision...
 Checking '/home/          ' ... [OK]
 Checking '/home/          /.ssh' ... [OK]
 Checking '/home/          /.ssh/authorized_keys' ... [OK]
 Checking '/home/            ... [OK]
 Checking '/home/          .ssh' ... [OK]
 Checking '/home/          .ssh/authorized_keys' ... [OK]
 Checking '/home/            ... [OK]
 Checking '/home/          .ssh' ... [OK]
 Checking '/home/          .ssh/authorized_keys' ... [OK]
 Checking '/home/          er' ... [OK]
 Checking '/home/          er/.ssh' ... [OK]
 Checking '/home/          er/.ssh/authorized_keys' ... [OK]
 Checking '/home/          ctivity' ... [OK]
 Checking '/home/          ctivity/.ssh' ... [OK]
 Checking '/home/          ctivity/.ssh/authorized_keys' ... [OK]
Module runtime: 0 seconds

Running 70-motd...
 Checking '/etc/motd' ... [OK]
Module runtime: 0 seconds

Running 80-cloud-init...
 This module only applies to aws, exiting... [OK]
```

These tools can be especially useful when combined with something like process accounting or auditd….

Configuration management

1. bash

```
mdworker32 -S      marcs    __         0.17 secs Fri May 20 16:57 (0:14:29.38)
sudo       -S      root     ttys000    0.00 secs Fri Mar 25 15:09 (0:00:00.00)
lsof       -FX     marcs    ttys000    0.00 secs Fri May 20 17:10 (0:00:02.53)
lsof       -X      marcs    ttys000    0.20 secs Fri May 20 17:10 (0:00:02.53)
man        -       marcs    ttys000    0.00 secs Fri May 20 17:10 (0:00:27.50)
sh         -       marcs    ttys000    0.00 secs Fri May 20 17:10 (0:00:27.48)
sh         -F      marcs    ttys000    0.00 secs Fri May 20 17:10 (0:00:27.48)
sh         -F      marcs    ttys000    0.00 secs Fri May 20 17:10 (0:00:27.48)
less       -       marcs    ttys000    0.00 secs Fri May 20 17:10 (0:00:27.48)
groff      -       marcs    ttys000    0.00 secs Fri May 20 17:10 (0:00:00.03)
grotty     -       marcs    ttys000    0.00 secs Fri May 20 17:10 (0:00:00.03)
troff      -       marcs    ttys000    0.02 secs Fri May 20 17:10 (0:00:00.03)
tbl        -       marcs    ttys000    0.00 secs Fri May 20 17:10 (0:00:00.00)
ocspd      -S      root     __         0.33 secs Fri Mar 25 14:30 (0:37:42.00)
vim        -       marcs    ttys000    0.02 secs Fri May 20 17:09 (0:00:01.28)
Python     -       marcs    ttys000    0.03 secs Fri May 20 17:09 (0:00:05.28)
git        -       marcs    ttys000    0.00 secs Fri May 20 17:09 (0:00:00.02)
sudo       -S      root     ttys000    0.00 secs Fri Mar 25 15:07 (0:00:00.02)
sudo       -S      root     ttys000    0.00 secs Fri Mar 25 15:07 (0:00:00.00)
sudo       -S      root     ttys000    0.00 secs Fri Mar 25 15:06 (0:00:00.00)
sudo       -S      root     ttys000    0.00 secs Fri Mar 25 15:06 (0:00:02.97)
find       -SX     root     ttys000    0.84 secs Fri Mar 25 15:06 (0:00:02.95)
com.apple. -SX     marcs    __         0.00 secs Fri May 20 15:47 (1:20:47.00)
com.apple. -SX     marcs    __         0.03 secs Fri May 20 15:47 (1:20:47.00)
com.apple. -SX     marcs    __         0.00 secs Fri May 20 15:47 (1:20:47.00)
```

Some Examples

- SSH Tunnels.
- netcat, nmap, etc.
- Detection of newly installed packages/running processes.
- Service restarts, modifications to files/folders, kernel params.

Configuration management

Purrtecting IP information

Status	Host Name	IP	OS	Checkin	SVN Rev	Run Time	Message	action
			RHEL6 x86_64	2016-03-11 17:03:34	425	5	2346	Disable
			SLES11 x86_64	2016-03-12 07:49:06	425	6	379764	Disable
			SLES11 x86_64	2016-03-12 07:47:37	425	4	398985	Disable
			RHEL6 x86_64	2016-03-12 07:49:31	425	7	1484626	Disable
			RHEL6 x86_64	2016-03-12 07:48:20	425	6	2345053	Disable
			RHEL6 x86_64	2016-03-12 07:47:50	425	5	346088	Disable
			RHEL6 x86_64	2016-03-12 07:44:10	425	6	1693115	Disable
			RHEL6 x86_64	2016-03-12 07:47:45	425	5	2438976	Disable
			RHEL6 x86_64	2016-03-12 07:49:04	425	6	1024842	Disable
			RHEL6 x86_64	2016-03-12 07:46:18	425	5	1028134	Disable
			RHEL6 x86_64	2016-03-12 07:47:04	425	6	1025182	Disable
			UNSUPPORTED i686	2016-03-12 07:44:01	425	6	60628149	Disable
			RHEL6 x86_64	2016-03-12 07:48:38	425	5	212655	Disable
			RHEL6 x86_64	2016-03-12 07:40:35	425	5	60867	Disable
			RHEL7 x86_64	2016-03-12 07:45:17	425	8	935061	Disable
			RHEL7 x86_64	2016-03-12 07:44:44	425	4	1884853	Disable
			RHEL7 x86_64	2016-03-12 07:46:56	425	16	1451347	Disable
			RHEL7 x86_64	2016-03-12 07:48:38	425	7	262881	Disable
			RHEL7 x86_64	2016-03-12 07:48:36	425	7	272954	Disable
			RHEL7 x86_64	2016-03-12 07:46:20	425	7	261278	Disable

Possible on Windows too

https://technet.microsoft.com/en-us/sysinternals/sysmon

TechNet | Products | IT Resources | Downloads | Training | Support

United States (English) Sign in

Windows Sysinternals

Search TechNet with Bing

Home | Learn | Downloads | Community

Windows Sysinternals > Downloads > Security Utilities > Sysmon

Utilities

- Sysinternals Suite
- Utilities Index

- File and Disk Utilities
- Networking Utilities
- Process Utilities
- Security Utilities
- System Information Utilities
- Miscellaneous Utilities

Additional Resources

- Forum
- Site Blog
- Sysinternals Learning
- Mark's Webcasts
- Mark's Blog
- Software License
- Licensing FAQ

Sysmon v3.21

By Mark Russinovich and Thomas Garnier

Published: February 4, 2016

Download Sysmon
(641 KB)

Rate:

Share this content

Introduction

System Monitor (*Sysmon*) is a Windows system service and device driver that, once installed on a system, remains resident across system reboots to monitor and log system activity to the Windows event log. It provides detailed information about process creations, network connections, and changes to file creation time. By collecting the events it generates using Windows Event Collection or SIEM agents and subsequently analyzing them, you can identify malicious or anomalous activity and understand how intruders and malware operate on your network.

Note that *Sysmon* does not provide analysis of the events it generates, nor does it attempt to protect or hide itself from attackers.

Overview of Sysmon Capabilities

Sysmon includes the following capabilities:

- Logs process creation with full command line for both current and

Download

Download Sysmon
(641 KB)

Detailed information

Event Properties - Event 1, Sysmon

General | Details

Friendly View | XML View

+ **System**

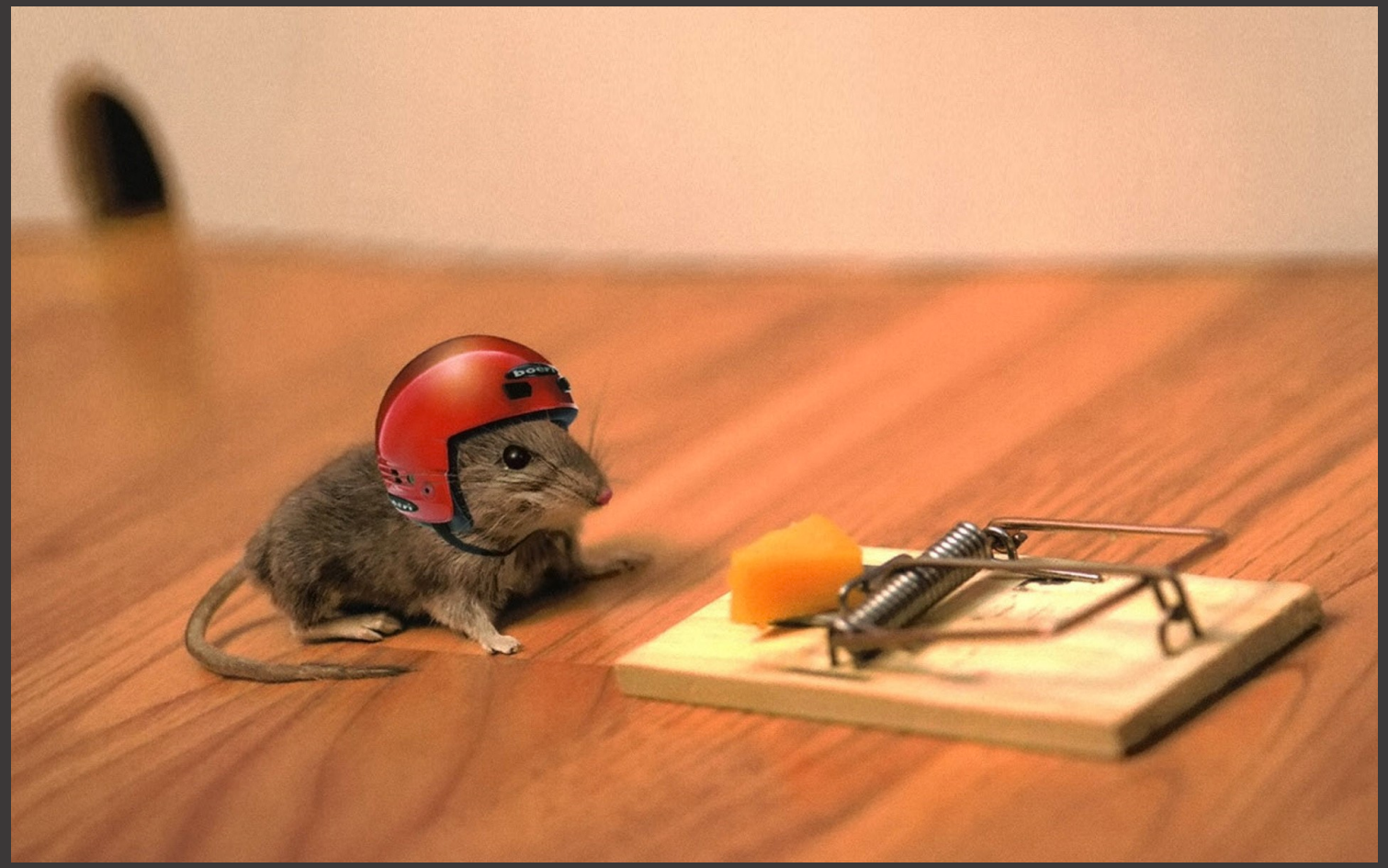
- **EventData**

UtcTime	8/10/2014 12:51 AM
ProcessGuid	{00000642-C228-53E6-0000-00107C7E0A00}
ProcessId	2784
Image	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
CommandLine	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe ("H4sIACjF5lMCA7VW/2+iSBT/uU32fyAbEyC1iq3b222yyQ0IitVW (New-Object IO.StreamReader(New-Object IO.Compression.GzipS
User	ACMELABS\Administrator
LogonId	0x3b462
TerminalSessionId	2
IntegrityLevel	High
HashType	SHA1
Hash	5330FEDAD485E0E4C23B2ABE1075A1F984FDE9FC
ParentProcessGuid	{00000642-C227-53E6-0000-0010D86C0A00}
ParentProcessId	3068
ParentImage	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
ParentCommandLine	powershell.exe -nop -enc WwBTAHkAcwB0AGUAbQAuAE4AZQB0AC4AUwBlAHIAdgBp

Copy | Close

K.I.S.S.

Persistence



Attacker challenges

- Attackers (usually) need to download some code to execute to gain persistence.
- They (usually) have a reliance on some tool to download that code for them.

Potential detection

- Tool of choice for most attackers would be wget or curl which are installed by default on most *nix machines.
- You *could* uninstall these, but why not use them against the attacker?
- If they're available, they will be used.

Wrapping of curl/wget

```bash
#!/bin/bash

$CURL = "/usr/bin/curl.874jgk"

echo 'args="'"$@"'"' | $CURL -s -d @- http://xxxx/curl-wget-activity.php
$CURL "$@"
```

```php
<?php

include_once("../notify_functions.php");

if($_POST) {
    if(isset($_POST["args"])) {
        send_alert($_SERVER["remote_ip"], $_POST["args"]);
    }
}

function send_alert($server, $args) {
    plain_text_mail("wget|curl initiated on {$server} with args {$args}");
}

?>
```

The same principle can be applied in other places too… even Windows

Exfiltration

Attacker challenges

- Attackers need to collate and collect data.
- Typically stored somewhere centrally to easily get out.

Simple potential detection

- Windows: forfiles /P c:\ /M *.* /S /D +”DD/MM/YYYY" /C "cmd /c if @fsize gtr <XX bytes> echo @path @fsize @fdate @ftime”

- *Nix: find / -mtime 0 -size +XXG

Digital Forensic Tools

File Name	Folder	Recovery Options	Document Type	File Type
Default.rdp	C:\Users\m...	Instant Unprotection	Remote Desktop Connection Docu...	Remote Desktop Connection
Discovery Dropbox L...	C:\Users\m...	Instant Unprotection, File patching req...	Acrobat 8.0	Adobe Acrobat Document
Discovery Dropbox Si...	C:\Users\m...	Instant Unprotection, File patching req...	Acrobat 8.0	Adobe Acrobat Document
FTP Account Reques...	C:\Users\m...	Instant Unprotection, File patching req...	MS Excel 97-2003	Microsoft Excel 97-2003 Workshee
QNJ0054479.pdf	C:\Users			
Inv 11407 20 Dec 201...	C:\Users			
Inv 11477 19 Feb 201...	C:\Users			
Inv 11498 27 Feb 201...	C:\Users			
Inv Discovery Dec 20...	C:\Users			
Inv Discovery Head ...	C:\Users			
Invoice 11478 20 Feb ...	C:\Users			
Staff Salaries.xlsx	C:\Users			
MS - 2015-12 Incenti...	C:\Users			
LETTER OF OFFER - ...	C:\Users			
LETTER OF OFFER - L...	C:\Users			
Server Request Form ...	C:\Users			

Select filter conditions.

All Any Filter enabled

Field	Operation	Values	Remove
File extension	ends with	zip	Remove
File size (byt...	greater than	23000	Remove
Mime type	any of	"application/zip" "application/x-rar-compressed ...	Remove
Last modifie...	equal to	Day: 27 Month: 3 Year: 2(	Remove
<Please sele...			Remove

Load filter... Save filter... Apply Cancel

Things I ran out of time for…

- Detection of large disk usage changes over X periods of time.
- Using netstat to detect connections that exist for longer than Y period of time.

MISINFORMATION

1 + 1 = 3

NOT advocating attacking techniques

Fishing === Phishing

- End-users are sometimes more stupid than saltwater fishes
  - Fishes do evolve: you have to use smaller hooks and Fluorocarbon lines for increased stealth
  - Humans apparently do not evolve: we're doing phishing with 15 years old attacks that still work
    - MS Office macros
    - HTA files
    - Custom .exe files

Phish Net

- Lovingly written (and titled) by one of my team members.
- Designed to make the life of phishers a little more difficult.
- Looks to fill the phishers net with garbage data.

Investigation

- Detection of phishing attack via various methods.
- We spin up an offsite VM and browse the malicious site; choose your provider of choice.
- Search for phishing kits to obtain the source if possible.

Fire up BURP

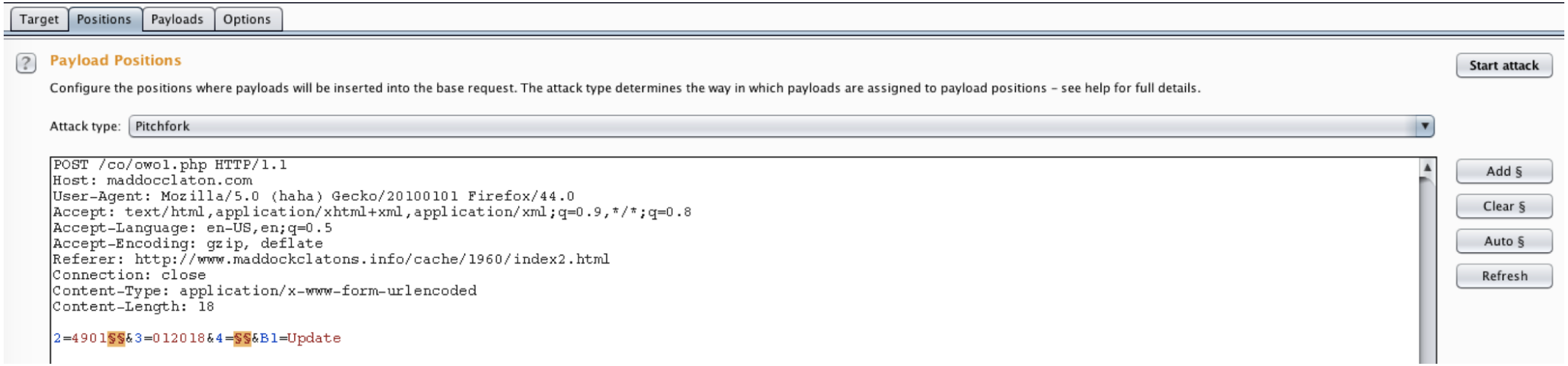
Intercept | HTTP history | WebSockets history | Options

Filter: Showing all items

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	SSL	IP
2	http://maddocclaton.com	POST	/co/owo1.php	☑	☐	302	274	HTML	php			☐	84.40.2.227
3	http://www.maddockclatons.info	GET	/cache/1960/processing.html	☐	☐	200	20254	HTML	html	Discovery Card		☐	107.180.1.12
4	http://www.maddockclatons.info	GET	/static/discovery/img/responsive/...	☐	☐	404	4346	HTML	png	Error: 404 Category n...		☐	107.180.1.12

Analysis of the app to determine where data is being POST'd.

Misinformation Payload



Now we can choose to either route through TOR or AWS, Google Compute etc.

Give the attacker moar data

Intruder attack 2

Attack Save Columns

Results | Target | Positions | Payloads | Options

Filter: Showing all items

Request	Payload1	Payload2	Status	Error	Timeout	Length	Comment
0			404			328	
1	117032242357	883	404			328	
2	826518096079	532	404			328	
3	311506337286	894	404			328	
4	295687020049	917	404			328	
5	065836936410	862	404			328	
6	260541040489	973	404			328	
7	862246350484	257	404			328	
8	742225877700	477	404			328	
9	379198779679	171	404			328	
10	782009268832	190	404			328	
11	457606947939	200	404			328	
12	693416917833	735	404			328	
13	886982290461	468	404			328	
14	027576497742	178	404			328	

Request | Response

Raw | Params | Headers | Hex

```
POST /co/owo1.php HTTP/1.1
Host: maddocclaton.com
User-Agent: Mozilla/5.0 (haha) Gecko/20100101 Firefox/44.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.maddockclatons.info/cache/1960/index2.html
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 43

2=49011170322423 57&3=012018&4=883&B1=Update
```

Feed the phisher with data that looks real…

The desired effect

Has it worked?

- We have had great success with this.
- Timing is important; too soon vs. too late.
- Gains are (hopefully) made more difficult for the attacker.

Helping and Enabling Users

Monitor for your users

GitHub, Inc. [US] https://github.com/jordan-wright/dumpmon

dumpmon

Twitter-bot (@dumpmon) which monitors paste sites for interesting content

For more overview, check out the blog post here.

Dependencies

```
twitter library - https://pypi.python.org/pypi/twitter
$ pip install beautifulsoup4
$ pip install requests
$ pip install pymongo <-- for MongoDB support (must have mongod running!)
```

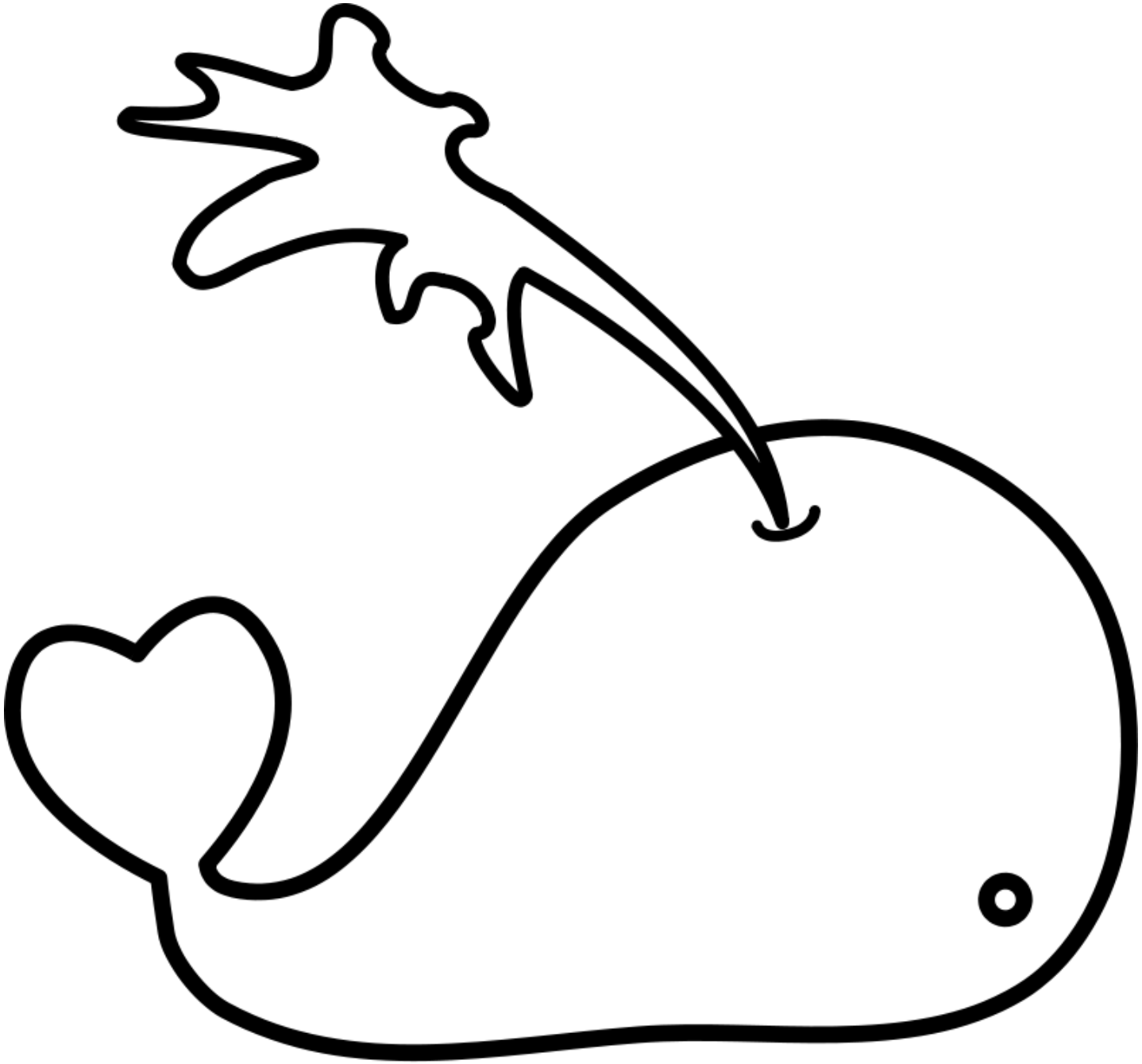
Next, edit the settings.py to include your Twitter application settings.

ASHLEY MADISON®

Life is short. Have an affair.®

How AM affected us?

- 17 addresses found in the AM database.
- Important that we get to them before attackers do.
- Enable them to deal with the threats of exposure, publicity etc.



Whaling Example

[TARGET],

I need you to put through a transaction today in form of a wire transfer. Let me know what details will be sufficient., For the last months we have been working, in coordination and under the supervision of the SEC, on acquiring a company....

This is very sensitive, so please only communicate with me through this email, in order for us not to infringe SEC regulations.

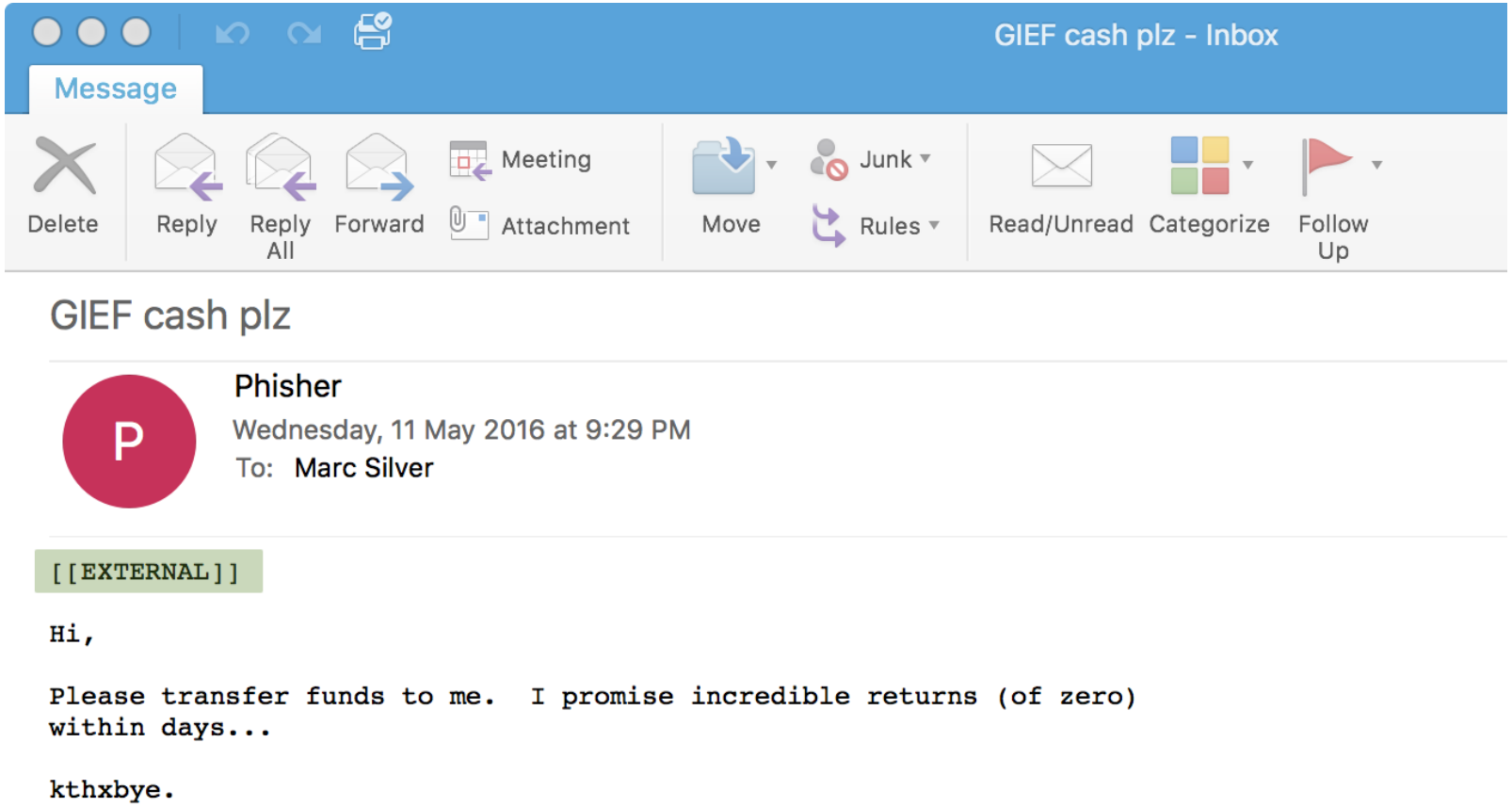
[SPOOFED NAME]
CEO – Discovery Holdings

Sent from my iPad

Enabling users to detect these mails

- Users find it challenging to determine the origin of these mails.
- We want to try and enable them to do so.
- Enabling them to do so would allow more informed decisions.

Duh?! Show them it's external?



Are these proposed solutions enough?


AW HELL NAW

If you’re going to do it,
do it right…

FireEye Appliance - Unauthorized File Disclosure

EDB-ID: 38090	**CVE:** N/A	**OSVDB-ID:** 127144
EDB Verified: ✓	**Author:** Kristian Erik Hermansen	**Published:** 2015-09-06
Download Exploit: Source Raw	**Download Vulnerable App:** N/A	

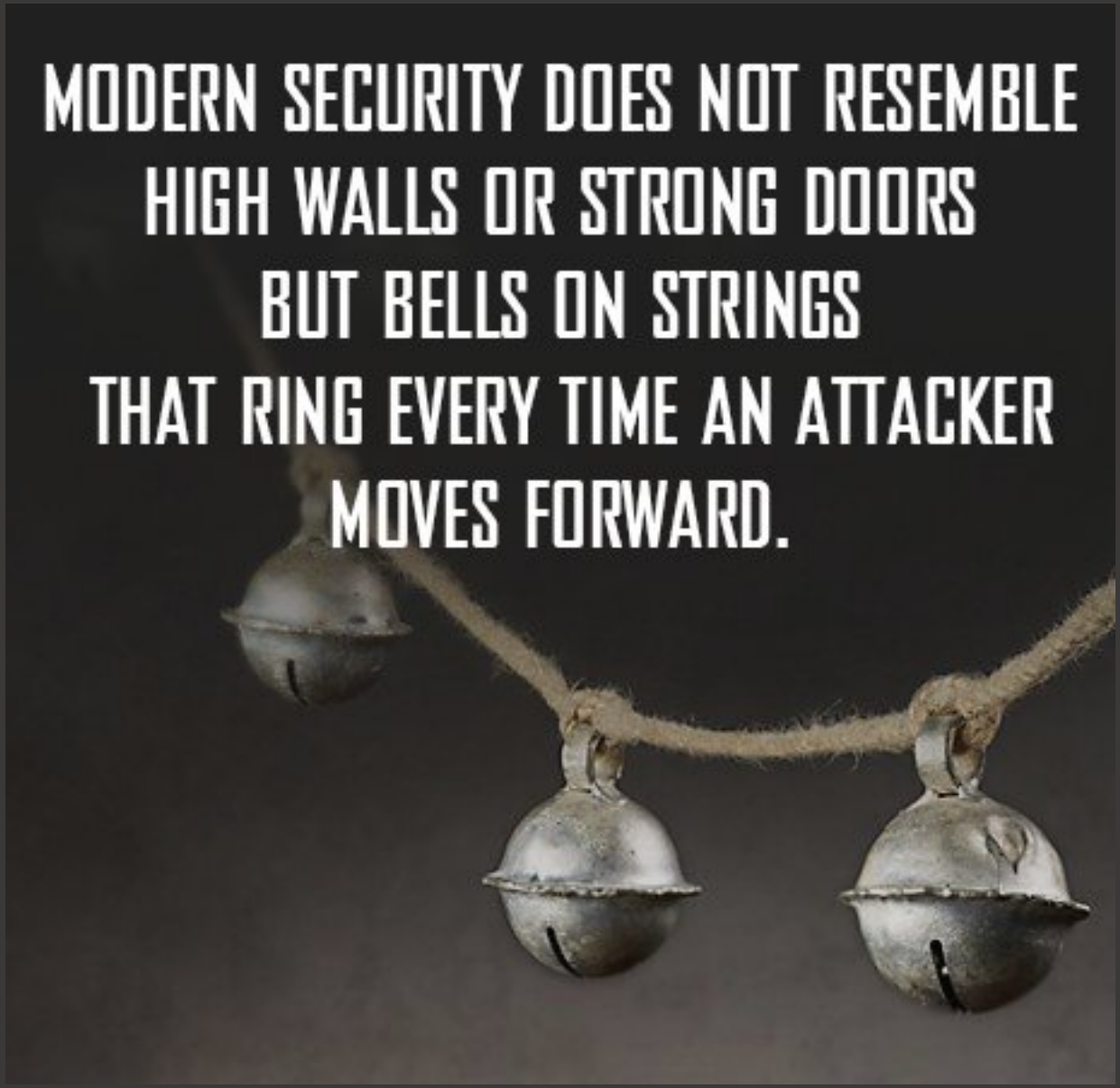
« Previous Exploit

Next Exploit »

```
Just one of many handfuls of FireEye / Mandiant 0day. Been sitting on this for more than 18 months with no fix from those securit

FireEye appliance, unauthorized remote root file system access. Oh cool, web server runs as root! Now that's excellent security f

https://fireeyeapp/script/NEI_ModuleDispatch.php?module=NEI_AdvancedConfig&function=HapiGetFileContents&name=../../../../../../..
```



Florian Roth

In Summary

People much smarter than me need to consider solutions that fall outside of traditional avenues.

In Summary….

- We need champions of Defensive Information Security.
- We need to **share** more information amongst defensive communities.
- We need to be honest with our boards about the reality on the ground.
- We need to work harder to get the basics rights.

In Summary….

- Simple solutions often provide decent detection.
- Encourage your staff to play a more active role.
- Focus more around how attackers would operate and optimize ways to detect their movement by playing to your strengths and their weaknesses;
- Encourage development of *secure* internal tools to help detect attacks.

Questions?

Thank you