

RSA®Conference2018

San Francisco | April 16 – 20 | Moscone Center

SESSION ID: EXP-W14

HACKING EXPOSED: THINK BEYOND (NEXTGEN AI POWERED)



#RSAC

Stuart McClure

CEO, Co-Founder
Cylance Inc.

Paul Mehta

Chief Architect
Cylance Inc.

Brian Wallace

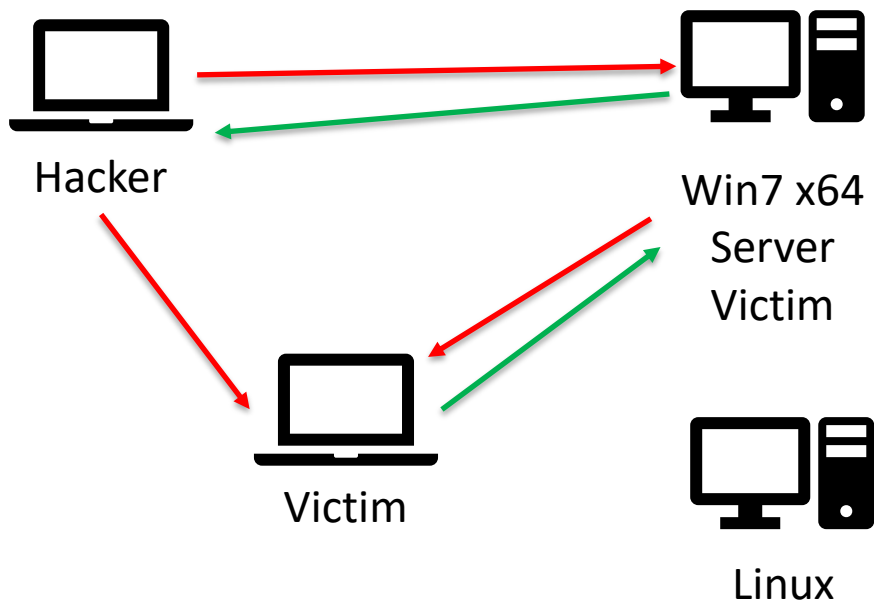
Lead Security Data Scientist
Cylance Inc.

Agenda



- Network hack: Server
 - EternalBlue->Doublepulsar
 - Password dumping the Server
 - Update->Dump Credentials
- Drive-by download: Spectre and Meltdown
 - Spectre (User) – Demo on Windows
 - Dump memory from a scripting language (without reading memory)
 - Meltdown (Kernel) – Demo on Linux
 - The cure, worst than the disease on Windows 7 x64
- SpearPhish: Operation Shaheen
 - Email->DOC->Crypto attack (with an unusual twist)

Hack Map



RSA®Conference2018



#RSAC

HACK #1

SERVER OVER NETWORK HACK

ETERNELBLUE->DOUBLEPULSAR

Is the backdoor locked?



#RSAC

```
.data:000000000001D75D      db 0FEh ; b
.data:000000000001D75E      db 0FEh ; b
.data:000000000001D75F      db 0FEh ; b
.data:000000000001D760      SrvTransaction2DispatchTable dq offset SrvSmbOpen2
.data:000000000001D760      ; DATA XREF: ExecuteTransaction+BE4r
.data:000000000001D768      dq offset SrvSmbFindFirst2
.data:000000000001D770      dq offset SrvSmbFindNext2
.data:000000000001D778      dq offset SrvSmbQueryFsInformation
.data:000000000001D780      dq offset SrvSmbSetFsInformation
.data:000000000001D788      dq offset SrvSmbQueryPathInformation
.data:000000000001D790      dq offset SrvSmbSetPathInformation
.data:000000000001D798      dq offset SrvSmbQueryFileInformation
.data:000000000001D7A0      dq offset SrvSmbSetFileInformation
.data:000000000001D7A8      dq offset SrvSmbFindNotify
.data:000000000001D7B0      dq offset SrvSmbIoctl2
.data:000000000001D7B8      dq offset SrvSmbFindNotify
.data:000000000001D7C0      dq offset SrvSmbFindNotify
.data:000000000001D7C8      dq offset SrvSmbCreateDirectory2
.data:000000000001D7D0      dq offset SrvTransactionNotImplemented
.data:000000000001D7D8      dq offset SrvTransactionNotImplemented
.data:000000000001D7E0      dq offset SrvSmbGetDfsReferral
.data:000000000001D7E8      dq offset SrvSmbReportDfsInconsistency
.data:000000000001D7F0      SrvWtTransactionDispatchTable dq 0 ; DATA XREF: ExecuteTransaction+1FB4r
.data:000000000001D7F8      dq offset SrvSmbCreateWithSdOrEa
.data:000000000001D800      dq offset SrvSmbNtIoctl
.data:000000000001D808      dq offset SrvSmbSetSecurityDescriptor
.data:000000000001D810      dq offset SrvSmbNtNotifyChange
.data:000000000001D818      dq offset SrvSmbNtRename
.data:000000000001D820      dq offset SrvSmbQuerySecurityDescriptor
.data:000000000001D828      dq offset SrvSmbQueryQuota
.data:000000000001D830      dq offset SrvSmbSetQuota
.data:000000000001D838      dq offset SrvSmbCreateWithExtraOptions
.data:000000000001D840      SrvApiDispatchTable dq 0 ; DATA XREF: sub_68FC4+B94r
.data:000000000001D848      db 0
.data:000000000001D849      db 0
```

Hack Steps



- Windows 7 x64 server
- Vulnerable SMBv1 running
- EternalBlue (the exploit) delivering Doublepulsar (the payload)
- Controlled by fb.py, FuzzBunch, an NSA Tool for exploits and implants
- Upload files as part of a campaign

RSA®Conference2018



HACK #1

DEMO

(praise to the live demo gods!)

Preventing EternelBlue



- Patching is about it...

RSA®Conference2018



#RSAC

HACK #2

DRIVE-BY DOWNLOAD

SPECTRE AND MELTDOWN

Global Meltdown



UPDATE

Meltdown and Spectre FAQ: How the critical CPU flaws affect PCs and Macs

It varies widely depending on your hardware, operating system, and workload.



By Brad Chacos and Michael Simon

PCWorld | FEB 22, 2018 7:14 AM PT

Pure Power

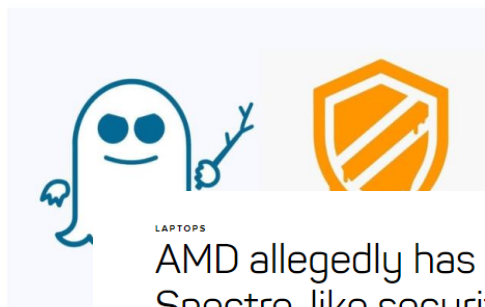
HP Smart Buy EliteDesk 705 G3 delivers uncompromising performance, security, manageability, and Ryzen™ Pro processors.

LEARN MORE



Connection

we solve IT



LAPTOPS

AMD allegedly has its own Spectre-like security flaws

Researchers say they've found 13 flaws in AMD's Ryzen and EPYC chips, which could let attackers install malware on highly guarded parts of the processor.

MORE LIKE THIS



How to protect your PC from the Meltdown and Spectre CPU flaws



AMD processors will get a firmware update for the Spectre CPU exploit, but...



Nvidia updates graphics

AMD Releases Updated Risk Guidance on Meltdown, Spectre

By Joel Hruska on January 11, 2018 at 5:39 pm 41 Comments

f t G+ Y 64 SHARES



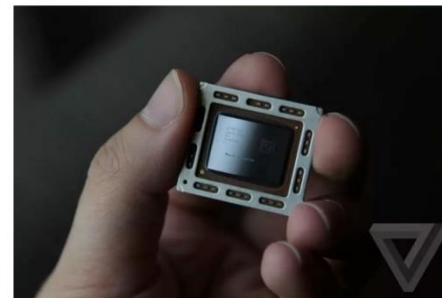
With Meltdown and Spectre now unveiled contain the problems they represent and Different vendors have released their ov Meltdown, ARM has some limited vulner quiet, apart from its initial statement last

Microsoft halts AMD Meltdown and Spectre patches after reports of unbootable PCs

Microsoft blames AMD's documentation

By Tom Warren | @tomwarren | Jan 9, 2018, 2:50am EST

f t SHARE



NOW TRE

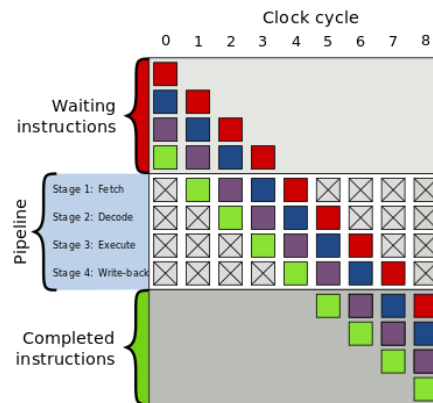


RSAConference2018

Instruction Pipelines



- One of the ways that modern processors increase speed is by pipelining
- Pipelining allows instructions to execute faster and in parallel
- What about branch instructions?
 - This is where **Speculative Execution** comes in



Speculative execution



- A vulnerable processor encounters a **branch**, if it's really not sure which branch to take...
- The **Branch** is *both taken and not taken*.
- Once determined, the other branch is discarded.
- Observe side effects from the discarded work. Wait, what?
 - *The branch not taken is discarded, so how can the effects be observed?*

The Crux

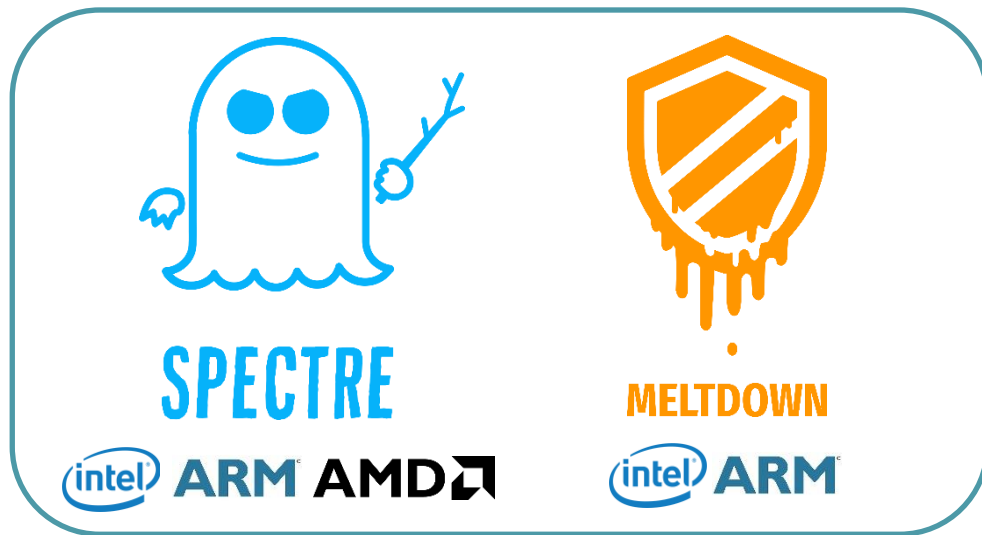


- The effects of touching memory will remain in the CPU cache.
- Cache hits are faster than misses.
- By measuring memory access this time, an attacker can infer memory.
- Repeating many times increases reliability.

Hack Steps



- Windows 7 desktop
- Vulnerable Windows and Linux version running
- User goes to website
 - Run Spectre
 - Show User memory
- User runs meltdown
 - Show Kernel memory



RSA®Conference2018



#RSAC

HACK #2

DEMO: SPECTRE AND MELTDOWN

(praise to the live demo gods!)

Total meltdown!



- On Windows 7 x64, this patch introduced a larger security hole...
 - The user/supervisor bit was set to user
 - Allowed user-mode code access to the page tables... oops
- This means userland code can access page tables and dump kernel memory with ease at 100MB+/s

```
C:\Users\Paul\Desktop\bin>pcileech.exe dump -out memorydump.raw -device totalmeltdown -v -force

TOTALMELTDOWN: Successfully exploited for physical memory access.
Memory Map:
START      END      #PAGES
0000000000001000 - 000000000000e000 00000000
000000000000e000 - 000000000000ffff 0003fff0

Current Action: Dumping Memory
Access Mode:  DMA (hardware only)
Progress:      1024 / 2048 (50%)
Speed:         146 MB/s
Address:       0x0000000040000000
Pages read:    262046 / 524288 (49%)
Pages failed:  98 (0%)
```


Prevention: Meltdown Patch.....?



- Microsoft released a patch for Meltdown in January
- Kb4056897 implemented “Kernel Page Table Isolation”, or KPTI to mitigate Meltdown
 - On every context switch, page tables are swapped back and forth between kernel and userland.
 - *As you know*, page tables map virtual memory to physical memory.
 - Patch does not prevent Meltdown from leaking memory so much as it prevents the memory from being present.
- This was fixed in the March patch



HACK #3

DEMO: CURE WORSE THAN THE DISEASE?

(praise to the live demo gods!)

RSA®Conference2018



#RSAC

HACK #4

SPEARPHISHING OPERATION SHAHEEN

APT group attacking Pakistani Nuclear Power Plant

SpearPhishing: Operation Shaheen



- We were looking for similar documents related to an APT from another group.
- Led us to a hacked Belgian Company site.
 - The hacked site was being used as a platform to distribute exploits.



Exploit Document



- The exploit contained dl/exec shellcode which pulled a payload from the Government website.
- The military engineering organization, and one of the major science and technology commands of a nation state Army.

Document attack



- This document was downloaded from an IP address
- C&C domain resolution using web services and attacks against Asian targets.
- Which for a period of a week resolved to this IP: 1**.2**.1**.1**.
 - resolved to a subdomain of a completely unrelated topic.

Evolution



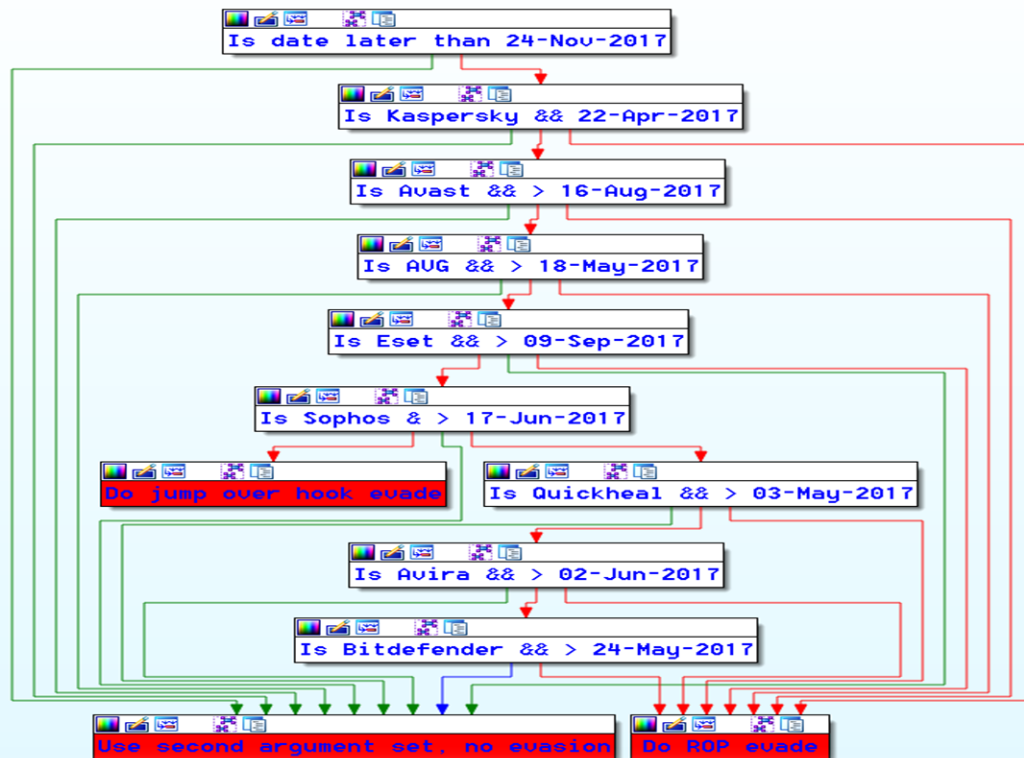
- The shellcode has evolved over time.
 - Earlier exploit docs contained basic download & execute shellcode.
 - More recent examples use multi-stage embedded payloads.
- Our samples matched based on source of the payload as well as shellcode similarities, known as code-sharing.

Evasion Capabilities



- They used a relatively unique means of obfuscating function calls to evade Kaspersky.
- They went through a lot of trouble to do this among other evasions, only to stop in sync.

Evasion: Antivirus?



RSA®Conference2018



#RSAC

HACK #4

DEMO: SPEARPHISH SHAHEEN

(praise to the live demo gods!)

Prevention: Operation Shaheen



- Office 2010 SP2 patch, July 2013

RSA®Conference2018



HACK #5

ADVERSARIAL AI

Adversarial AI



- The practice of pitting AI against AI to improve the original classification mode
- Build classification model
- Search for Interesting Results
- Build adversarial generated deceptive samples to trick our model into missing those results
- Harden the model against attacks by training it with samples generated to attack it

Shodan – Scans/Archives public IP space



The screenshot shows the Shodan website homepage. At the top, there's a navigation bar with links like 'Shodan', 'Emergencies', 'Back', 'View All', and a search bar. Below the navigation bar, the main heading reads 'The search engine for Webcams' with a subtext 'Shodan is the world's first search engine for Internet-connected devices.' There are two buttons: 'Create a Free Account' and 'Getting Started'. Below this, there are four feature sections: 'Explore the Internet of Things' (with a cloud icon), 'Monitor Network Security' (with an eye icon), 'See the Big Picture' (with a globe icon), and 'Get a Competitive Advantage' (with a magnifying glass icon). Each section has a brief description of its capabilities. At the bottom, there's a blue banner with two statistics: '56% of Fortune 100' and '1,000+ Universities', followed by a world map and the text 'Analyze the Internet in Seconds'.

The search engine for Webcams
Shodan is the world's first search engine for Internet-connected devices.

[Create a Free Account](#) [Getting Started](#)

Explore the Internet of Things
Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.

Monitor Network Security
Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.

See the Big Picture
Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!

Get a Competitive Advantage
Who is using your product? Where are they located? Use Shodan to perform empirical market intelligence.

56% of Fortune 100
Shodan is used around the world by researchers, security professionals, large enterprises, CERTs and everybody in between.

1,000+ Universities

Analyze the Internet in Seconds
Shodan has servers located around the world that crawl the Internet 24/7 to provide the latest Internet intelligence. Who buys Smart TVs? Which countries are building the most wind farms? What companies are affected by Heartbleed? Shodan provides the tools to answer questions at the Internet scale.

[Sample Report on Heartbleed](#)

Show Admin | Show API Key | Help Center

SHODAN

[Search]
[+]
Explore
Downloads
Reports
Developer Pricing
Enterprise Access
Contact Us
My Account

Exploits
 Maps
 Share Search
 Download Results
 Create Report

TOTAL RESULTS

68,153

TOP COUNTRIES

COUNTRY	RESULTS
United States	68,153

TOP SERVICES

HTTP	43,068
HTTPS	17,933
8081	3,581
HTTP (8080)	2,171
HTTP (8443)	361

TOP ORGANIZATIONS

Enix Corporation	17,995
Dino Solutions	7,168
Colocation America Corporation	4,791
Consew LLC	3,504
Certified Hosting	2,800

TOP OPERATING SYSTEMS

Linux 3.x	3,506
Linux 2.6.x	162
Windows 7 or 8	86
Linux 2.4-2.6	27
FreeBSD 9.x	23

TOP PRODUCTS

Apache httpd	66,497
Apache Tomcat/Coyote JSP engine	1,109
nginx	4

Matt Ventura's blog

203.141.136.176
[bserve1.mattventura.net](#)
FranTech Solutions
 Added on 2019-04-05 17:38:57 GMT
United States, Las Vegas
 Technologies: PHP
 DoubleClick Ad Exchange (ADX)
 Details

```

HTTP/1.1 200 OK
Date: Thu, 05 Apr 2018 17:34:03 GMT
Server: Apache/2.2.22 (Debian)
X-Powered-By: PHP/5.4.45-0+deb7u8
Link: <http://mattventura.net/wp-json/?rel=https://api.w.org/>
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8
X-Pad: avoid browser bug
          
```

170.130.14.203

192.229.225.26
[enixcorp.revelate.com](#)
Enix Corporation
 Added on 2019-04-05 17:36:03 GMT
United States, Las Vegas
 Details

```

HTTP/1.1 200 OK
Date: Thu, 05 Apr 2018 17:33:21 GMT
Server: Apache/2.2.18 (Unix) mod_ssl/2.2.18 OpenSSL/1.0.0-fips DAV/2 PHP/5.3.4
Last-Modified: Sat, 20 Nov 2004 20:16:24 GMT
ETag: "bb1141-2c-3e9554c23b600"
Accept-Ranges: bytes
Content-Length: 44
Content-Type: text/html

<html><body><h1...
          
```

Louisiana Tech Bulldogs Football Tickets - Louisiana Tech Bulldogs - Louisiana Tech Tickets

192.229.225.26
[webhost.presenter.com](#)
Consew LLC
 Added on 2019-04-05 17:33:59 GMT
United States, Las Vegas
 Details

```

HTTP/1.1 200 OK
Date: Thu, 05 Apr 2018 17:33:56 GMT
Server: Apache
Content-Length: 34829
Content-Type: text/html; charset=UTF-8
          
```

404 Not Found

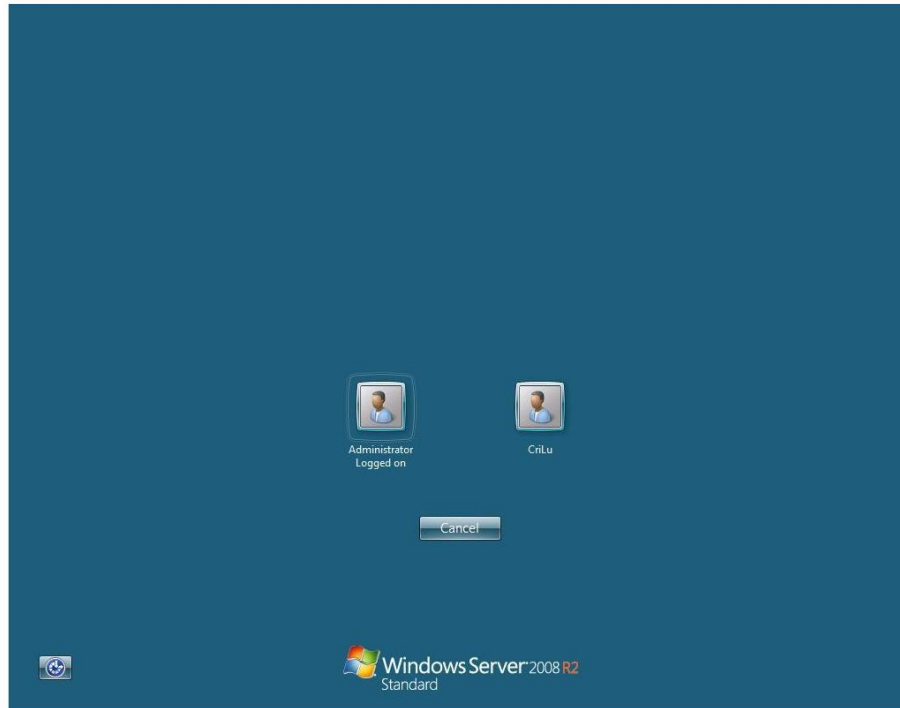
170.130.140.91
[lery05.pircadian.com](#)
Enix Corporation
 Added on 2019-04-05 17:33:29 GMT
United States, Las Vegas
 Details

```

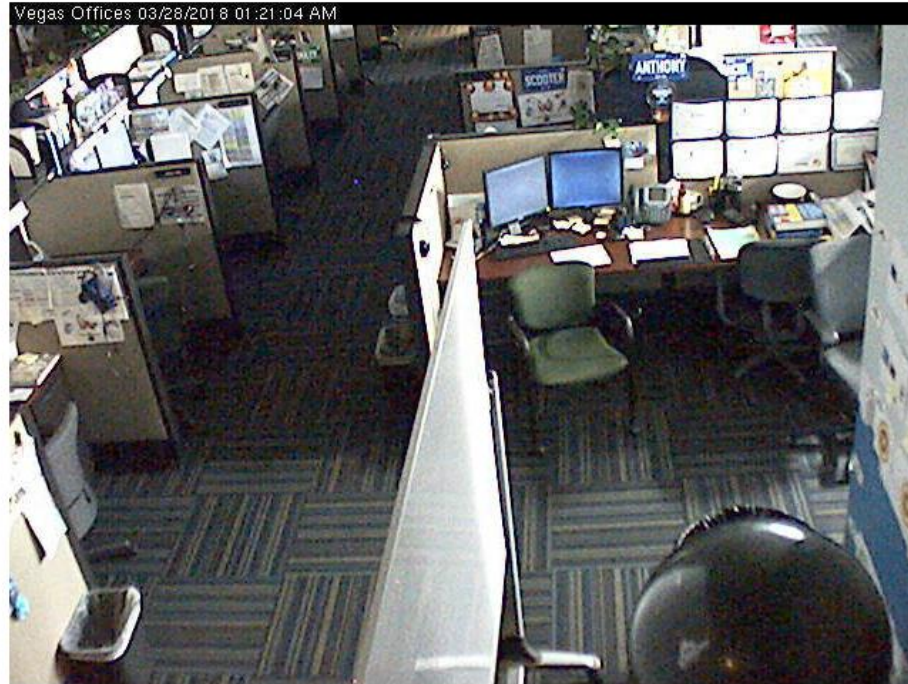
HTTP/1.1 200 OK
Date: Thu, 05 Apr 2018 17:33:28 GMT
Server: Apache/2.2.15 (CentOS)
X-Powered-By: PHP/5.6.22
Content-Length: 203
Content-Type: text/html; charset=UTF-8
          
```



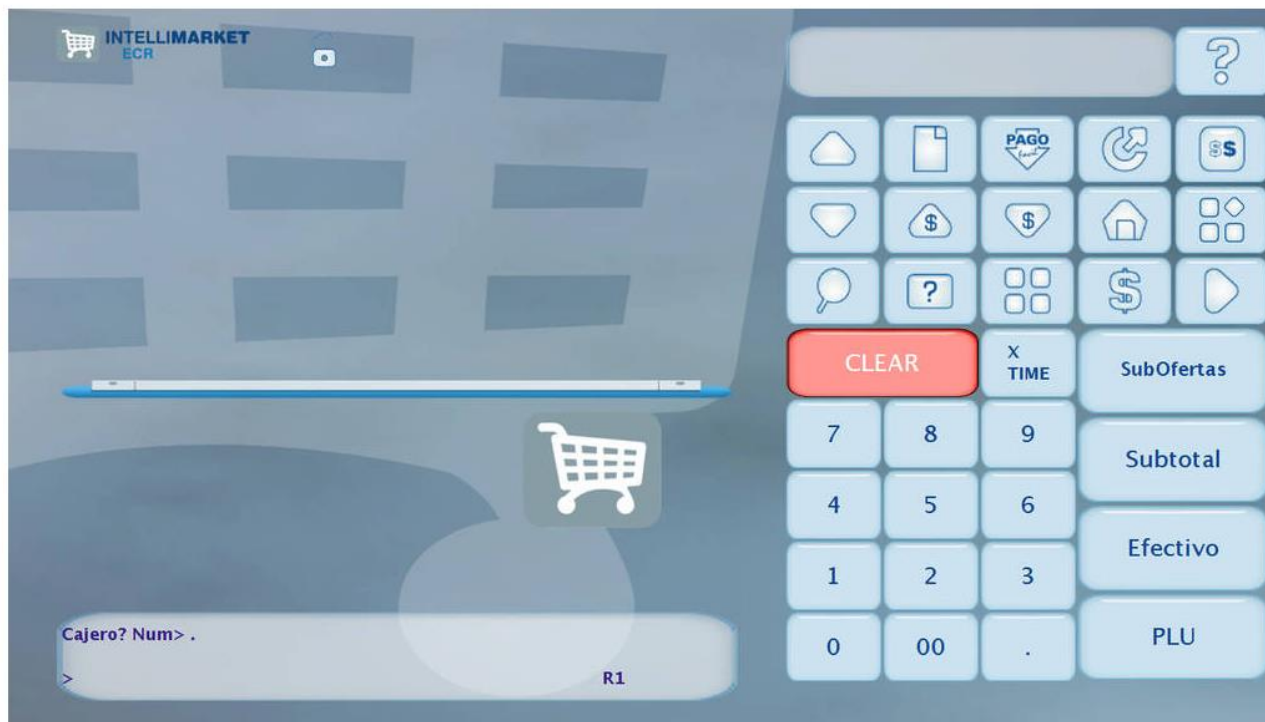
Shodan Grabs Screenshots



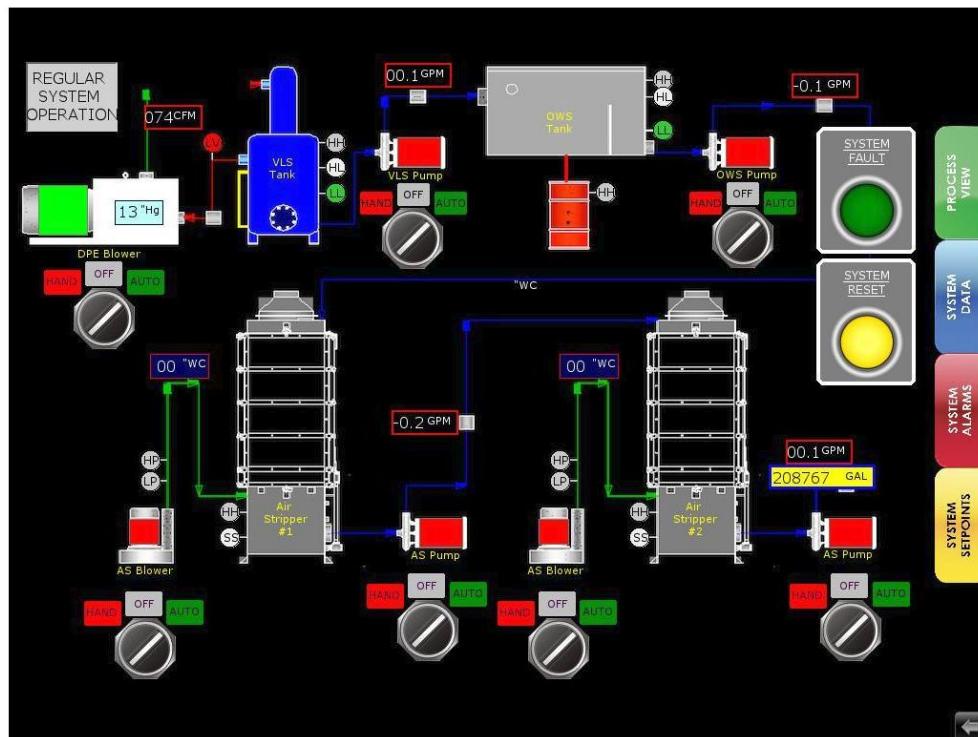
Shodan Sees Security Cams



Shodan Sees POS



Shodan Sees ICS



[illegible]

Shodan Sees Logged in Desktops



#RSAC

Navigateur Web Firefox

militaria radio en vente | eBay - Mozilla Firefox

https://www.ebay.fr/sch/l.html?_si= suitcase spy radio ww2 ebay

Les plus visités • Getting Started • Latest Headlines • Page de démarrage M...

Bienvenue ! Connectez-vous ou inscrivez-vous | Bons Plans | Vendre | Aide

Mon eBay

ebay Parcourir les catégories

militaria radio

Toutes les catégories Rechercher Recherche approfondie

Recherches associées: militaria radio militaire radios militaires radio

☐ Inclure la description

Tout Enchères Achat immédiat

Trier : Durée : nouveaux objets Afficher :

1 335 résultats pour militaria radio Enregistrer cette recherche

CES PRODUITS DEVRAIENT VOUS INTÉRESSER ! Aide [x]

- [1. SOMFY Relais radio SOMFY PROTECT - 2401495](#)
- [2. NEW ONE Radio reveil Analogique Tuner FM alarme](#)
- [3. NEW ONE Radio reveil Analogique Tuner PLL/FM](#)
- [4. NEW ONE Radio reveil Analogique Tuner FM alarme](#)

Tous les produits Vita Habitat
Profitez des prix chocs sur Rasoir-Service
Prix imbattables sur Rasoir-Service
Les meilleures offres de Rasoir-Service

Clansman 320 Radio Small Centre Junction Dipole Balun 5820-99-117-7439

13,74 EUR
Achat immédiat
+9,16 EUR de frais de livraison
4 suivis

16-mars 22:20
Provenance : Royaume-Uni
Top Fiabilité

WW2 1942 US ARMY SIGNALS CORPS RADIO RECEIVER B3 357 M

79,02 EUR
Achat immédiat

16-mars 21:30
Provenance : Royaume-Uni

Format tout afficher

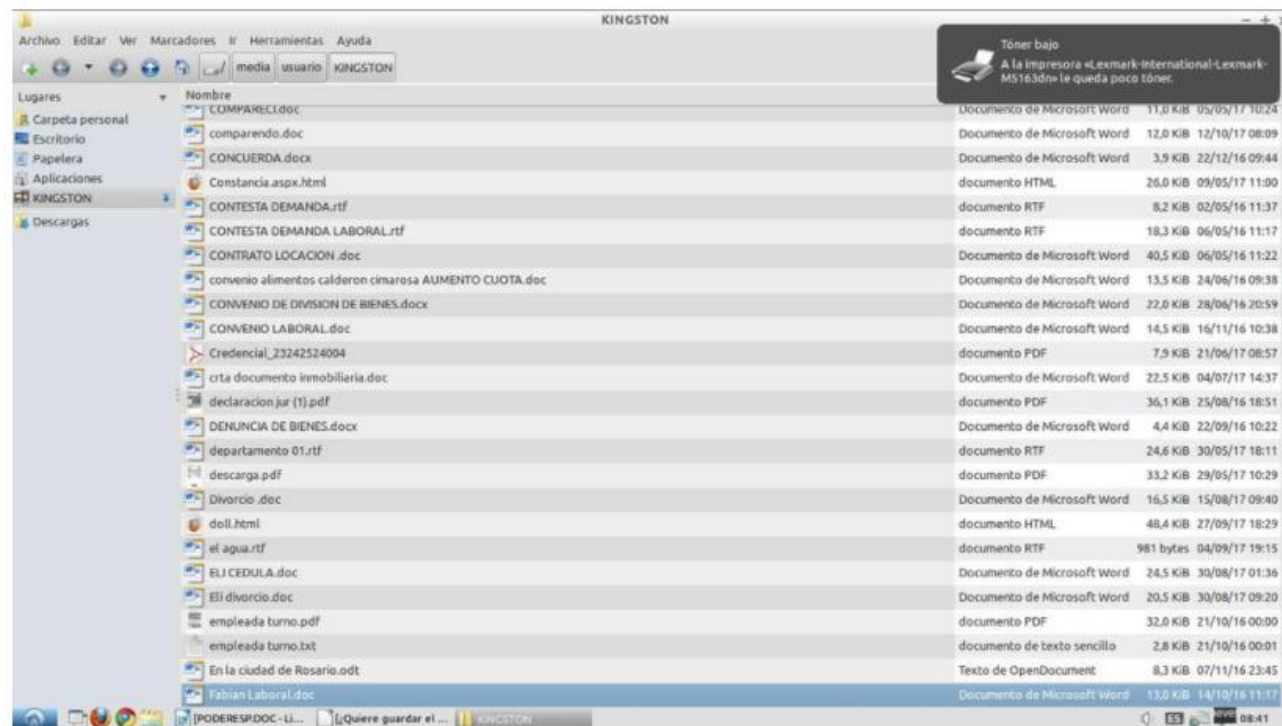
Tout Enchères Achat immédiat

Type tout afficher

Shodan Sees Logged in Desktops



#RSAC



Shodan Image Classification (SIC) Project



- Objective: Build a collection of binary classifiers to identify different traits about screen shots of Shodan services
 - Including classifiers that determine if a screen shot is a logged in desktop, ICS, POS, log in screen, security camera, etc
- Downloaded and manually labeled as many images as I could from the Shodan Developer API
- Trained two part Neural Networks using a method called “Transfer Learning”
 - Copy the top portion of a neural network trained on a large number of images
 - Only train the bottom portion based on the output from the top portion
 - Combine the two to make predictions
- Logged In Desktop classifier ends up 97.89% accurate

Logged In Desktop Classifier Findings



Computer NetTools Zenmap

Recycle Bin Ostinato

Host Name: WIN7-UNL
Machine Domain: WORKGROUP
User Name: Administrator

IP Address: 172.16.10.5
Subnet Mask: 255.255.255.0
Default Gateway: 172.16.10.1
DHCP Server: (none)
DNS Server: (none)
MAC Address: 00-C9-AA-76-9E-00

```
Administrator: Command Prompt
Reply from 172.16.1.1: bytes=32 time<1ms TTL=254
Reply from 172.16.1.1: bytes=32 time<1ms TTL=254
Reply from 172.16.1.1: bytes=32 time<1ms TTL=254
Reply from 172.16.1.1: bytes=32 time<1ms TTL=254

Ping statistics for 172.16.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\Administrator>ping 172.16.1.1

Pinging 172.16.1.1 with 32 bytes of data:
Reply from 172.16.1.1: bytes=32 time<1ms TTL=254
Reply from 172.16.1.1: bytes=32 time<1ms TTL=254
Reply from 172.16.1.1: bytes=32 time<1ms TTL=254
Reply from 172.16.1.1: bytes=32 time<1ms TTL=254

Ping statistics for 172.16.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Administrator>
```

EN 1:39 AM 23-Nov-16

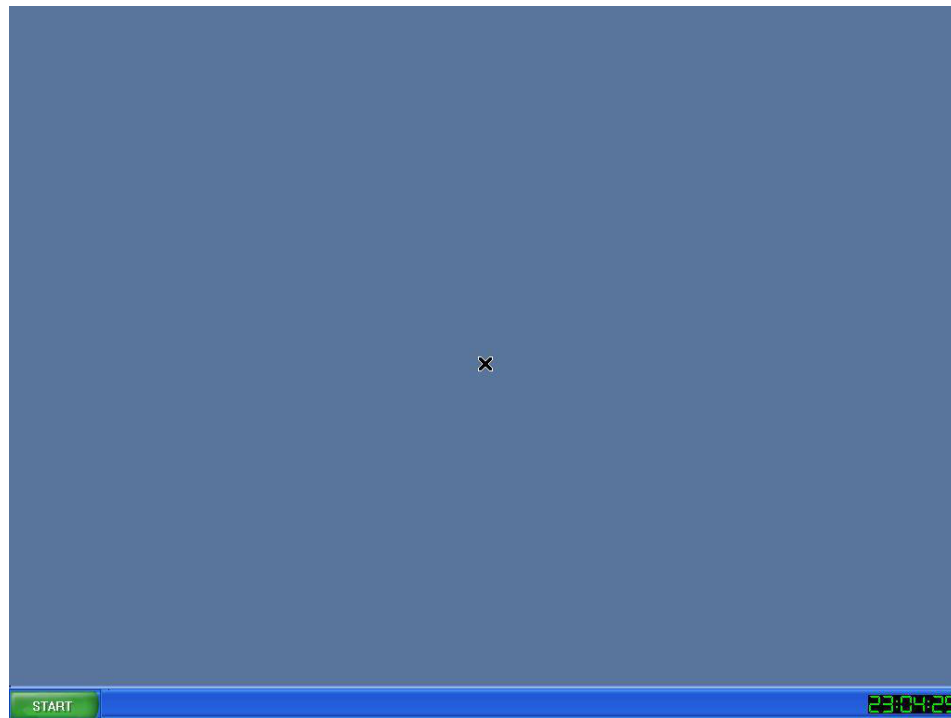
Logged In Desktop Classifier Findings



The screenshot shows a Raspberry Pi desktop with a sunset background. A terminal window is open, displaying the output of the 'ps' command. The terminal title is 'pi@lu: ~'. The output lists various system processes and user applications, including dbus-daemon, gvfsd, fuse, openbox, lxpanel, pcmanfm, ssh-agent, x11vnc, volume-monitors, menu-cache, trash, lxterminal, gnome-ptty-helper, and bash. The prompt at the bottom is 'pi@lu:~\$' followed by some characters.

```
pi@lu: ~  
Απορρίμματα  
Αρχείο Επεξεργασία Καρτέλες Βοήθεια  
760 ? Ss 0:00 /usr/bin/dbus-daemon --fork --print-pid 4 --print-add  
811 ? S1 0:00 /usr/lib/gvfs/gvfsd  
818 ? S1 0:00 /usr/lib/gvfs/gvfsd-fuse /run/user/1000/gvfs -f -o bl  
829 ? S 0:09 openbox --config-file /home/pi/.config/openbox/lxde-p  
830 ? S1 0:00 lxpolkit  
833 ? S1 26:27 lxpanel --profile LXDE-pi  
834 ? S1 0:12 pcmanfm --desktop --profile LXDE-pi  
841 ? Ss 0:00 /usr/bin/ssh-agent -s  
843 ? R 18:36 x11vnc -display :0 -forever -shared -alwaysshared -ul  
870 ? S1 0:00 /usr/lib/gvfs/gvfs-udisks2-volume-monitor  
885 ? S 0:00 /bin/sh /usr/bin/start-pulseaudio-x11  
886 ? S 0:09 /usr/bin/xprop -root -spy  
893 ? S1 0:00 /usr/lib/gvfs/gvfs-goa-volume-monitor  
897 ? S1 0:00 /usr/lib/gvfs/gvfs-mtp-volume-monitor  
901 ? S1 0:00 /usr/lib/gvfs/gvfs-afc-volume-monitor  
906 ? S1 0:00 /usr/lib/gvfs/gvfs-gphoto2-volume-monitor  
915 ? Ss1 0:00 /usr/lib/menu-cache/menu-cached /tmp/.menu-cached-:0-  
949 ? S1 0:00 /usr/lib/gvfs/gvfsd-trash --spawner :1.1 /org/gtk/gvf  
1087 ? S 0:02 /usr/lib/arm-linux-gnueabi/hf/gconf/gconfd-2  
2309 ? S1 0:09 lxterminal  
2310 ? S 0:00 gnome-ptty-helper  
2311 pts/0 Ss 0:00 /bin/bash  
17333 pts/0 R+ 0:00 ps x  
pi@lu:~$ MUJE GSM ! MUHHHAHAHAHAH
```

Logged In Desktop Classifier Findings



Logged In Desktop Classifier Findings

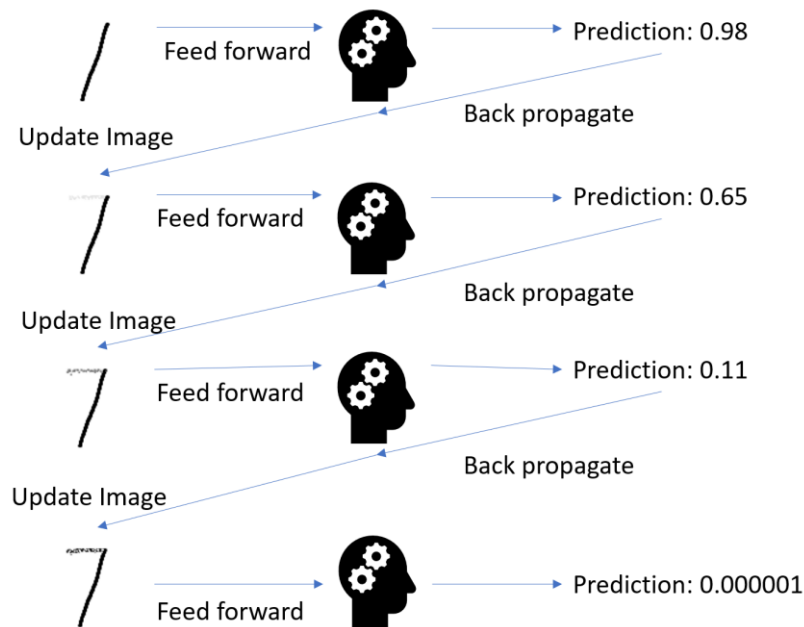


Generating Adversarial Samples



- Based on the same principals as training a neural network
- Feed in a sample to our model for classification
- Compare the output classification with the target classification we want
- Back propagate through the neural network (but not updating it) until we get to the sample
- Apply the remaining gradient to the image
- Continually repeat until the classification of the image flips

Classifier that Predicts if an Image is 1



Adversarial Sample Generation Demo



- Running in a scientific computing environment called Jupyter Lab
 - A way to run Python (and other languages) experiments, and share results
 - Pytorch is the neural networking library being used primarily
- Start by loading the sample we want use as the starting point
- Load the model we want to attack (white box attack)
- Run an attack by applying changes to the whole image
- Run an attack by applying changes to a 100x100 square of the image
- Run an attack by imprinting a desired image and attacking the area around it

RSA®Conference2018



#RSAC

HACK #5

DEMO: ADVERSARIAL AI

(praise to the live demo gods!)

Hardening Models



- Making models more robust against attacks is referred to as “model hardening”
- There are many different strategies
- The suggested is simple; generate a lot of adversarial samples and add them to your training set with the original label
- After one round of this kind of adversarial training
 - Model accuracy went from 97.89% to 98.3%
 - Adversarial sample generation went from 0/530 failures to 100/530 failures
 - Mean distance from original image went from 3.11 to 4.03 (images had to change more to trick the model)

Adversarial Machine Learning And Defenses



- There is a continual back and forth between new defenses being created, and then new attacks being created to defeat those defenses
- Similar paradigm to the security industry with red vs blue team
- Implications of the security/robustness of a machine learning model could be quite significant given how much we rely on machine learning in everything from business operations to our day to day lives
- The best way to create secure/robust models is to regularly try to find ways to attack the models you create

Thank you!



- Questions and Answers?

@hackingexposed
Monthly HE Live
sessions plus
“versus” demos...

