

RSAC Studio



Connect **to**
Protect

The First 12

**An Hour-by-Hour Breakdown of a
Threat Actor Inside Your Environment**

ARMOR™

Dr. Chase Cunningham
ECSA, LPT

HEAD OF THREAT RESEARCH
& DEVELOPMENT, ARMOR

@CynjaChaseC



#RSAC



0100 HOURS

Target Observation & Selection

Finding the
Slow Gazelle

Hour 2



#RSAC

0200 HOURS

Do the
Homework

Map & Detail
the Network,
Users & Data
Points



0300 HOURS

Plot the
Operations

Dropping the
Crosshairs



0400 HOURS

Begin the
Attack

Poking Away
at Easy
Access Points



0500 HOURS

Find
Weakness
in the
Defense

Unlocking
the Door

Hour 6



#RSAC

0600 HOURS

Gain
Glorious
Access

Let the
Data Flow



RSA[®]Conference2016



0700 HOURS

Become
Just
Another
User

Hiding
Inside the
Network
Shadows



0800 HOURS

Plot the
Exfiltration

Planning the
Escape with
Your Data

Hour 9



#RSAC

0900 HOURS

Steal
Everything

It's Not
Bolted
Down?
Take it.

Hour 10



#RSAC

1000 HOURS

Set Up
Future
Access

The Lucrative
Link to
Unfettered
Entry



1100 HOURS

Walk Out
the Front
Door

The Silent
Exit



1200 HOURS

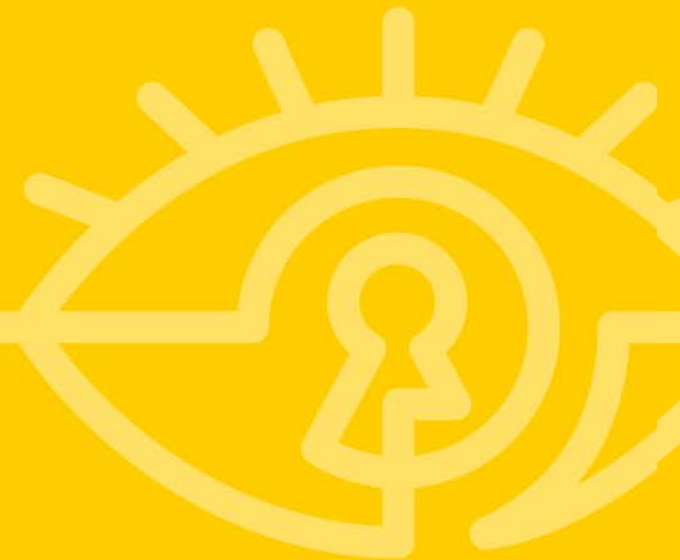
Sell Your
Secrets

Cashing In
on the
Breach



Steps You Can Take So This Doesn't Happen To You

ARMOR™



Find a Leader

Place someone in charge of cybersecurity who has the backing of the CEO.

Patch Everything

Update all patches across the board; out-of-date systems represent the most common security vulnerabilities.

Five Long-Term Objectives



Know Your Data

Design and implement a data classification program.
You can't defend what you don't understand.



Five Long-Term Objectives



Build a VTM Plan

Build a thorough vulnerability and threat management (VTM) program that will keep patches constantly updated and identify points of risk.



Create the Culture

Make security a culture change. Educating employees is more than sending one email a year with a simple multiple-choice test.

Five Long-Term Objectives



Layer Up

Implement a multilayered security environment that not only identifies and defeats inbound threats, but also watches and mitigates outbound traffic.



Five Long-Term Objectives



Be Honest

Decide if this is a war you can win with in-house resources. If there is even a little doubt, outsource to proven and trusted cybersecurity experts.



RSA[®]C Studio



Connect **to**
Protect

The First 12

**An Hour-by-Hour Breakdown of a
Threat Actor Inside Your Environment**

ARMOR[™]

Dr. Chase Cunningham
ECSA, LPT

HEAD OF THREAT RESEARCH
& DEVELOPMENT, ARMOR

@CynjaChaseC



#RSAC

RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center



Connect **to**
Protect

How Hacks Happen

James Lyne

General Reprobate, Global Head of
Security Research, Sophos and
Instructor, SANS.

@jameslyne



#RSAC



Computer Geek



Mac User
(Eternal Cult
Of Turtlenecks)



Researcher
Linux User
(Eccentric)



TED Speaker
(Lots of
Photoshop)

Courtesy of @Steph3nSims



#RSAC





“Our users, the people that depend on us for advice, actually **cling on to ideas long after they are still good ideas.**”

– *Me (like 2 months ago whilst eating a club sandwich)*



“Sometimes we, this industry, are guilty of the same.”

– *Me (shortly after the original quote, maybe during dessert but I don't recall)*

The Cybercrime World We Know



- Mass use of drive by downloads
- Heavy reliance on exploits
 - Often with clever bypasses of novel anti-exploit controls
- Still plenty of spam and phishing, links to infected sites
- Hacked legitimate sites used as a majority distribution mechanism

Industrialized Processing



#RSAC

CC Autoshop | AlphaBay Market - Tor Browser

CC Autoshop | Alpha... x Someone has your pa... x V-M.NAME x

pwoah7foa6au2pul.onion/autoshop.php?a_bin=&a_city=&a_state=&a_zip=&a_countryname=United+Kingdom&: x Search

AlphaBay Market

Autoshop Logout

Home • Sales • Messages • Listings • Balance • Orders • Feedback • Forums • Contact

USD 411.00 CAD 538.04 EUR 372.28 AUD 575.73 GBP 265.88

CC Autoshop

Welcome to the CC autoshop! This section allows you to search for credit cards or fults in the most convenient way possible. Be careful when using checkers, as they can have side effects on the cards.

Buy Cards Buy Accounts My Purchased Cards My Purchased Accounts

BIN: City: State: Zip: Country: United Kingdom

DOB: (Any) SSN: (Any) Birth Year: 0000 to 9999 Price: 0.01 to 999.99 Seller: (Any)

Bank: (Any) Type: (Any) Credit: (Any) Level: (Any) Search

Clear All

BIN	Exp.	Seller	Name	City	State	Zip	Country	DOB	SSN	Price
<input type="checkbox"/> 465859	12 / 15	dimples (24%)	Joe Ma...	Bury St Edmunds	Suffolk		United Kingdom	N/A	N/A	\$8.90
<input type="checkbox"/> 465946	2 / 16	dimples (24%)	Simon ...	Crouch End	N/A		United Kingdom	N/A	N/A	\$8.90
<input type="checkbox"/> 454742	12 / 15	dimples (24%)	David ...	Barnstaple	Devon		United Kingdom	N/A	N/A	\$8.90
<input type="checkbox"/> 454742	12 / 15	dimples (24%)	dan go...	bracknell	berkshire		United Kingdom	N/A	N/A	\$8.90
<input type="checkbox"/> 465901	9 / 19	dimples (24%)	karyn ...	southampton	hampshire		United Kingdom	N/A	N/A	\$8.90
<input type="checkbox"/> 475117	6 / 18	dimples (24%)	DEREK ...	aberdeeen	Aberdeenshire		United Kingdom	N/A	N/A	\$8.90
<input type="checkbox"/> 475111	3 / 16	dimples (24%)	STEPHE...	Belfast	Down		United Kingdom	N/A	N/A	\$8.90
<input type="checkbox"/> 465942	9 / 19	dimples (24%)	Laura ...	Basingstoke	N/A		United Kingdom	N/A	N/A	\$8.90
<input type="checkbox"/> 454313	11 / 16	cc-king (24%)	Mr T G...	Hampshire	Hampshire		United Kingdom	N/A	N/A	\$8.90
<input type="checkbox"/> 446291	3 / 18	cc-king (24%)	Mrs Ja...	Upton	Dorset		United Kingdom	N/A	N/A	\$8.90
<input type="checkbox"/> 446291	2 / 18	cc-king (24%)	Mrs C ...	Scarborough	North Yorkshire		United Kingdom	N/A	N/A	\$8.90
<input type="checkbox"/> 475117	1 / 17	cc-king (24%)	Mrs J ...	Alloa	Clackmannshire		United Kingdom	N/A	N/A	\$8.90
<input type="checkbox"/> 465901	4 / 18	cc-king (24%)	Mr K L...	Gloucestershire	Gloucestershire		United Kingdom	N/A	N/A	\$8.90
<input type="checkbox"/> 465901	3 / 17	cc-king (24%)	Mr R H...	Maldstone	Kent		United Kingdom	N/A	N/A	\$8.90
<input type="checkbox"/> 465901	11 / 17	cc-king (24%)	Mrs M ...	Welling	Greater London		United Kingdom	N/A	N/A	\$8.90
<input type="checkbox"/> 454313	1 / 16	cc-king (24%)	Mrs M ...	Rochford	Essex		United Kingdom	N/A	N/A	\$8.90
<input type="checkbox"/> 454313	1 / 16	cc-king (24%)	Jonath...	Dilton Priors, Bridgnor	Shropshire		United Kingdom	N/A	N/A	\$8.90

Transferring data from pwoah7foa6au2pul.onion...

User expectations



#RSAC

*From: Frank Young <xxxxx@xxxxx.com>
To: xxxxx@xxxxx.com
Subject: Time travelers PLEASE HELP!!!!!!
Date: 10 Jan 2002 20:43:53 +0100*

If you are a time traveler or alien disguised as human and or have the technology to travel physically through time I need your help!

My life has been severely tampered with and cursed!!

I have suffered tremendously and am now dying!

I need to be able to:

Travel back in time.

Rewind my life including my age back to 4.

Be able to remember what I know now so that I can prevent my life from being tampered with again after I go back.

I am in very great danger and need this immediately!

I am aware that there are many types of time travel, and that humans do not do well through certain types.

I need as close to temporal reversion as possible, as safely as possible. To be able to rewind the hands of time in such a way that the universe of now will cease to exist.

I know that there are some very powerful people out there with alien or government equipment capable of doing just that.

If you can help me I will pay for your teleport or trip down here, Along with hotel stay, food and all expenses. I will pay top dollar for the equipment. Proof must be provided.

Also if you are one of the very few beings with the ability to edit the universe PLEASE REPLY!!!

Only if you have this technology and can help me please send me a (SEPARATE) email to:

xxxxxx@aol.com

Please do not reply if your an evil alien!

Thanks

<no subject>



Sandrine Nzi <nzisandrine37@gmail.com> sent by martinartin9@gmail.com <martinartin9@gmail.com>

Tuesday, 1 March 2016 at 07:39

To:

Dear Friend,

My name is Sandrine Nzi, Personal attorney to my late client who died of heart attack in 2009. He deposited \$15,500,000.00 in a Bank here. He died without any registered next of kin as he was long divorced and had no child. The bank contacted me and said that they will confiscate his account and money if i fail to present any of his relative. I contacted you because you can perfectly handle this transaction and fit in as his next of kin, We can work together to claim this money and share it 50/50.

Kindly reply me through this email address for more details (sandrine_nzi2010@yahoo.co.jp)










Yours Sincerely,
Sandrine Nzi.


https://github.com/jameslyne/SSET



#RSAC

[Home](#) [Generate Code](#) [Stats](#)

Browser	User ↓	IP Address ↓	Group ↓	Time ↓
 46.0.2490.80	-	-	Marketing - Campaign A	2015-11-02 11:00:02
 46.0.2490.80	-	-	First Attempt	2015-10-30 08:04:56
 46.0.2490.80	-	-	First Attempt	2015-10-29 14:54:32
 2.0	-	-	First Attempt	2015-10-23 15:08:36
 0.1	-	-	First Attempt	2015-10-23 15:08:34
 1.0	-	-	First Attempt	2015-10-23 15:07:05
 40.0	-	-	First Attempt	2015-10-23 14:31:23
 7.0	-	-	First Attempt	2015-10-23 14:29:36
 46.0.2490.71	-	-	First Attempt	2015-10-23 14:28:56



SIMPLE SOCIAL ENGINEERING TRACKER

[Home](#) [Generate Code](#) [Stats](#)

Enter group name

Group	Link
Marketing - Campaign A	http://192.168.41.129/secure?secure_id=563740d061c2e
Another group	http://192.168.41.129/secure?secure_id=562a12496cee5
First Attempt	http://192.168.41.129/secure?secure_id=562a0ba69988e

A small measure of phish



“Tax Refund”

8 people

A small measure of phish



“Here is my resume”

217 people / 194 people

A small measure of phish



“Amazon package”

116 people / 7 people

A small measure of phish



“Payment advice”

304 people / 87 people

A small measure of phish



“Bruh, do you even click my links? <<URL>>”

19 people



#RSAC



THIRD PARTY FACE PALM

For when there is so much fail.... you need that extra bit of outside help..

What I learned

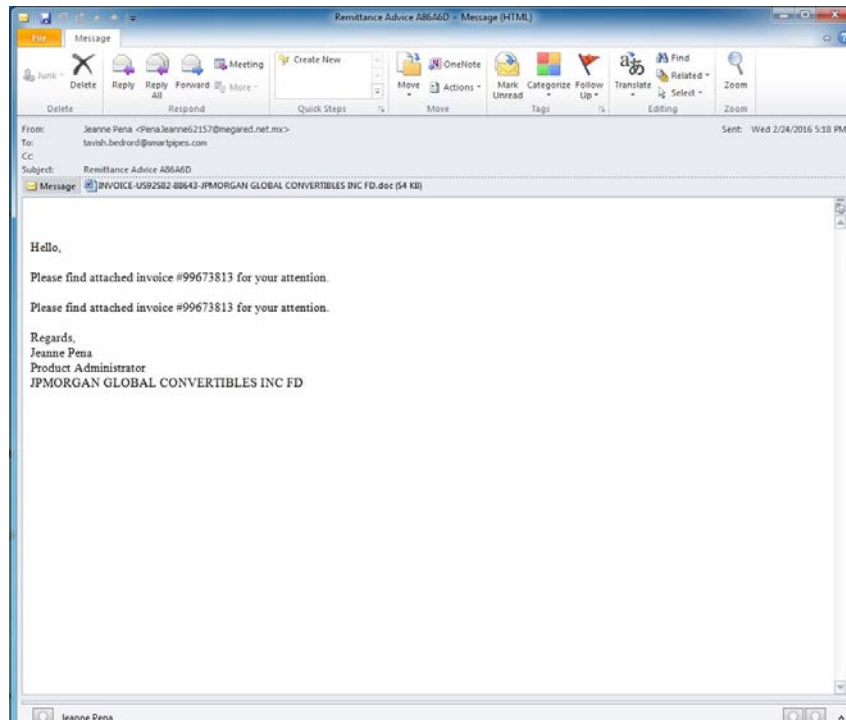
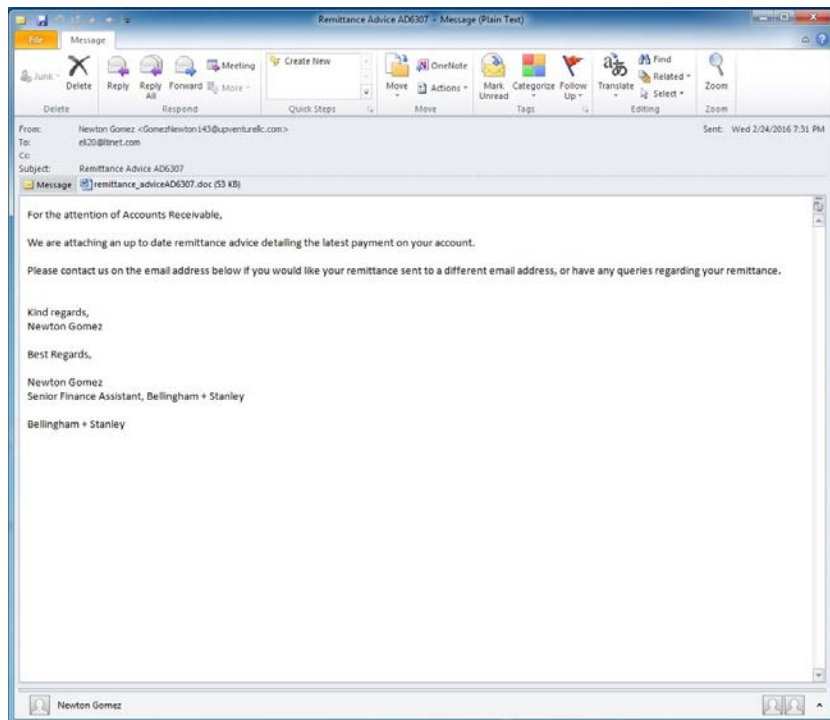


- No one believes they are getting a tax refund. Ever.
- People expect bad grammar in a resume/CV e-mail. Not alarming.
- People are 'better' tuned to detect commercial identity hijacks, such as Amazon/UPS/FedEx etc.
- People like money. They are optimistic about receiving it even when it looks ridiculously suspicious.
- Some people just can't be helped.

Spam! Glorious Spam!



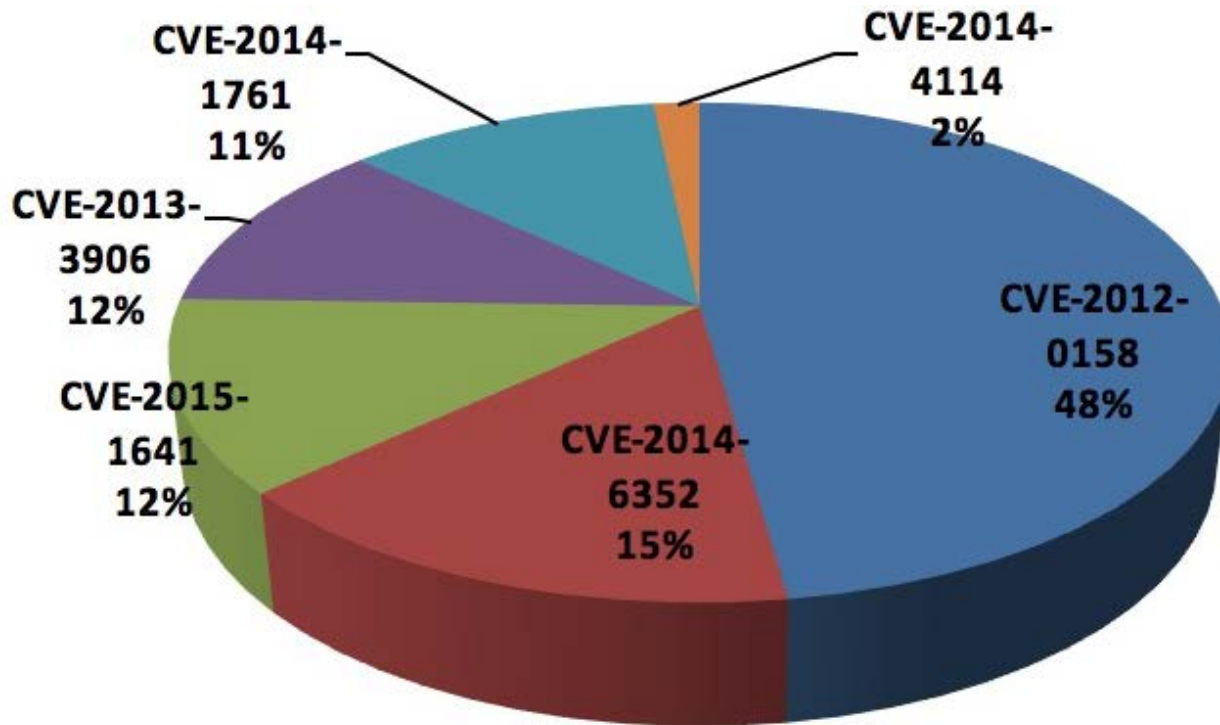
#RSAC



Old but good?



#RSAC





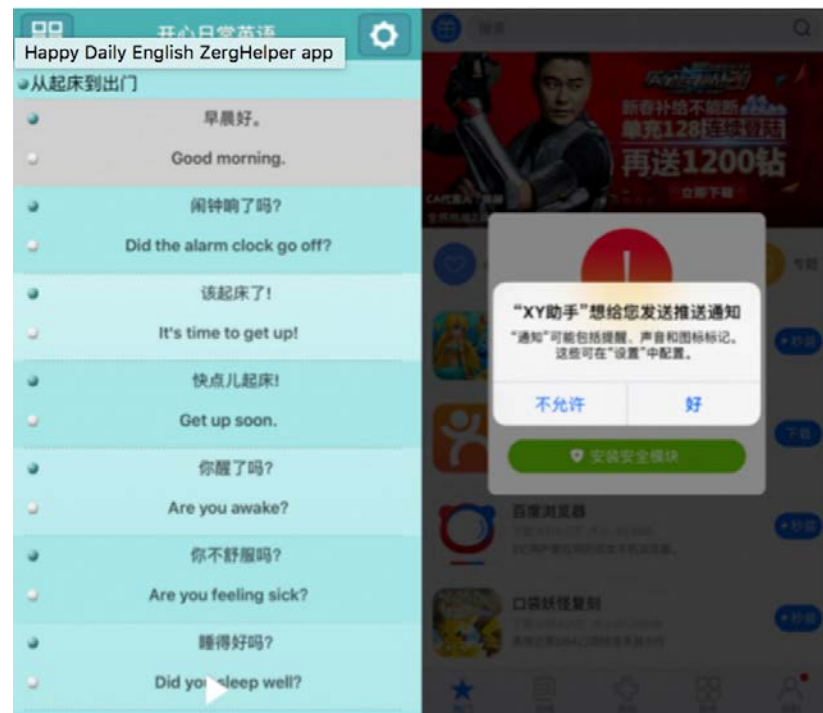
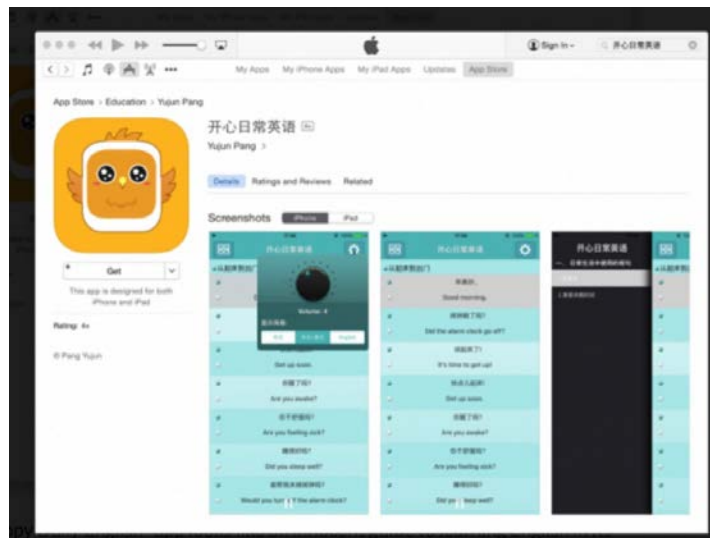


“Oh no problem, I’ll click on that on my phone to see if it is safe”

– *Unattributed remarkably typical response
(that made me choke)*



#RSAC



1002

(because 1000 would be just less awesome)

306



```
<social_block>
  <name>Twitter</name>
  <id>1</id>
  <Consumer>[REDACTED]LVES7m4Ms</Consumer>
  <Secret>MxAGEB[REDACTED]</Secret>
  <Owner>[REDACTED]/Owner>
</social_block>
```



- Document malware a specific effective focus
 - Very few 0 days – mostly old stuff, but it works!
 - Do you need Macros? Do you keep that software up to date?
- New technologies come with high expectations of trust, but often over market and don't deserve their position.
- For now cyber crime is the cyber crime we know and love with a few tweaks and altered behaviors, but we are entering a period of potential cyber crime innovation.
- A voice of reason, non hype based focus on the changes in our industry is critical. Enjoy the talks for the rest of RSAC.



Questions?

@jameslyne

ping@jameslyne.com

