

A Journey Into... IT SECURITY RISK & COMPLIANCE

... aka the coming of age of the credentials



Philippe Alcoy
Technical Director APAC

RAPID7



中国互联网安全大会



360互联网安全中心

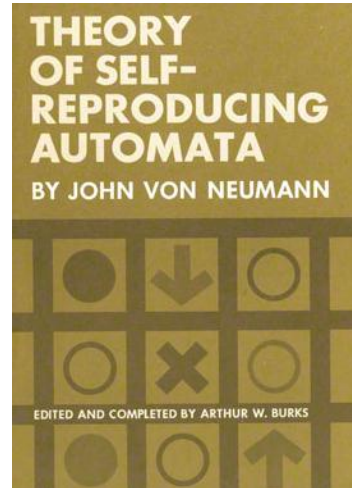
China Internet Security Conference 2014
2014中国互联网安全大会

YESTERDAYYEAR

Theoretical Years

John Von Neumann

Preliminary work compiled in one article based on lectures given at University Illinois in 1949



1949

1987

Experiments

Creeper/Reaper

First experiment of self-replicating virus on the ARPANET! Reaper created to hunt and destroy “Creeper”, ie. first AV!

ANIMAL

First game “Trojan”!

XEROX Alto Research

First mistake worm for calculus!



1949

1971

1972

1978

1982

1987

Experiments

CSTPS

Memory errors first publicly discussed.

"The code performing this function does not check the source and destination addresses properly, permitting portions of the monitor to be overlaid by the user. This can be used to inject code into the monitor that will permit the user to seize control of the machine."

page 61

ESD-TR-73-51, Vol. II

COMPUTER SECURITY TECHNOLOGY PLANNING STUDY

James P. Anderson

October 1972

DEPUTY FOR COMMAND AND MANAGEMENT SYSTEMS
HQ ELECTRONIC SYSTEMS DIVISION (AFSC)
L. G. Hanscom Field, Bedford, Massachusetts 01730

Approved for public release;
distribution unlimited.

(Prepared under Contract No. F19628-72-C-0198 by James P. Anderson & Co.,
Box 42, Fort Washington, Pa. 19034.)



1949

1971

1972

1978

1982

1987

Boot Sector Galore

ELK CLONER

First “in the wild” MS-DOS/Apple virus!

“ARF, ARF, GOTCHA”

Joke viruses, grandfathers of “YOU JUST GOT PWNED!” website hack meme!

ELK CLONER:

THE PROGRAM WITH A PERSONALITY

IT WILL GET ON ALL YOUR DISKS
IT WILL INFILTRATE YOUR CHIPS
YES IT'S CLONER!

IT WILL STICK TO YOU LIKE GLUE
IT WILL MODIFY RAM TOO
SEND IN THE CLONER!

▯

1949

1978

1982

1987

Business Explorations

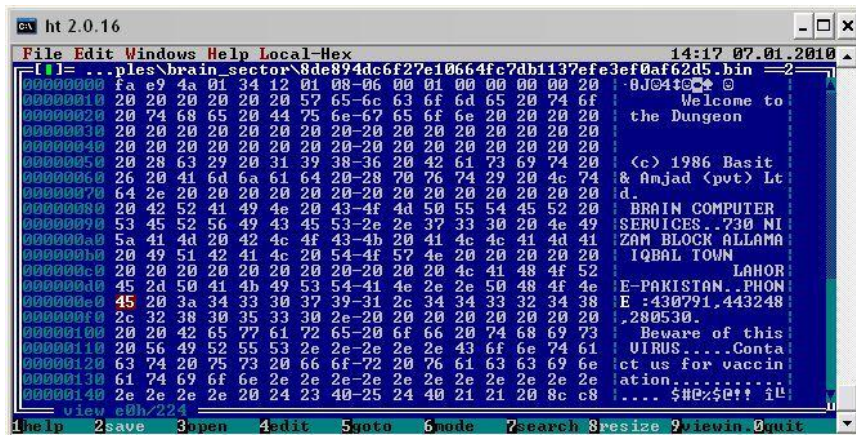
BRAIN

First commercial virus, allegedly gave birth to McAfee AV company!



Lehigh

First memory resident virus infecting command.com and deleting disk after 4 infections (accidental suicide)



1949

1986 1987

Internet Worm

Robert Tappan “Morris” Jr. Worm

First Internet worm requiring no user interaction, exploiting a buffer overflow in fingerd.

Led to the creation of the US CERT/CC.



1988

1994

Birth of Cyber Criminality

Vienna

First polymorphic virus!

Dark Avenger

Random overwrite of HDD sectors

AIDS

Trojan would replace autoexec.bat and encrypt HDD after 90 reboots

EICAR
Foundation

Bugtraq
Started

```
COUNTRY.S S      COUNTRY.TXT      DEBUG.EXE      EDIT.COM      EXPAND.
FDISK.EXEY      FORMAT. OM      KEYB.COM      KEYBOARD.SYS  MEM.EXEEXE
NETWORKS. X     NLSFUNCC XE    OS2.TXT      QBASIC.EXE    README.T
SCANDISK. X     SYS.COM.E     XCOPY.EXE    CHOICE.C M    DEFRAG.EXT
DEFRAG.H T      DELOLDOS.E E  DOSHELP.HLP  EGA.CPI O     EGA2.CPIXE
EGA3.CPI E T    EMM386.EXE    KEYBRD2. YS  MSCDEX.E E    SCANDISK.INI
ANSI.SYSLP E    APPEND.E E    CHKSTATESSYS DBLWIN.H      DELTREE.EXE
DISKCOMP. O     DISKCO        M    DISPLAY.Y     DOSKEY. X     DRUSPACE EX
DRUSPACE.CL     DRUSPAPYX F   DRUSPACE S    MSD.EXECLP    REPL CE..XEE
STORE. H        HELP.HCE.C    DRIVER.SS S  EDIT.HLPOM    FAST ELPE X
STOPENEXE      FC.EXELP X    FIND.EXE.SYS GRAPHICS.COM   GR P I S
LP. OM.EX       HIMEM.SY.IO   INTERLNKYE E I TER UR. XE  L . X
READF X C M     E MAKERS NE  MEMMAKER      M MMA ER N    M C M
Fa OU B OM      E.COM.E      MOVE E H      OO L          P . X
HE C 3          DR UE.S S    SE E E        E          S E
LO I L 6P       R N.E E     M H          S
MON M X         O C M     F X          A
QBASIC.         U B         O 6          H
SMARTDR. 1 ( M   X4,300      .          A H C .
TREE.CO. M M    Y9 0 4    TVER.      N S          ABEL E .
COMMANDH ROR X   ARTMXEX  E K .       ODE. O E
C:\DOS>U B      SAM I T O    INTD.N.    MST LS..     OWER E E
C:\DOS>M.P E    UMA TMAC. M  S NF1G038 L  SHAR .EXDE   IZER.EXEE
C:\DOS>.CEME    ANFORME3,01 Ubytes.UMBLP  SORT.EXEEI   UBST.EXEPRO
C:\DOS>930fi e s)UTOEX30,84 , 2 Cbytes.freeP PRINT.EXEL F UNDELETE.EXE
```

1988

1989

1990

1991

1993

1994

Arrival of the Toolkits

MtE

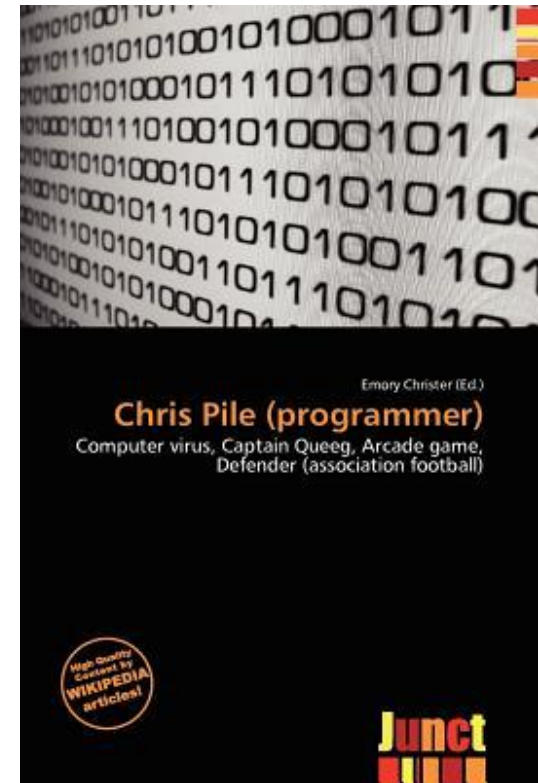
Dark Avenger's self mutating engine

Multi-vector Viruses

Boot sector, partition tables & files

Smeg.(Pathogen| Queeg)

Black Baron sentenced to prison in England



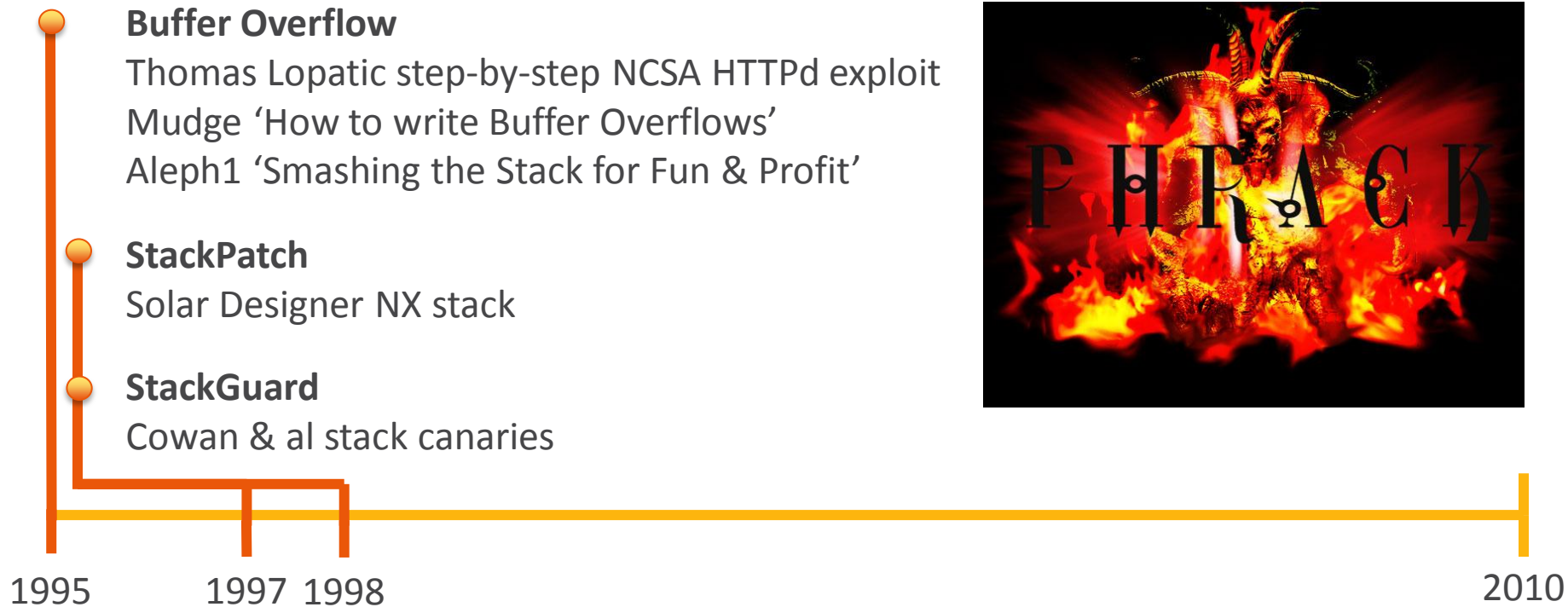
1988

1991

1992

1994

Memory Errors Bonanza



Backdoors

NetBus & BackOrifice

Microsoft internal network hit by BO in 2000

Heap Overflow

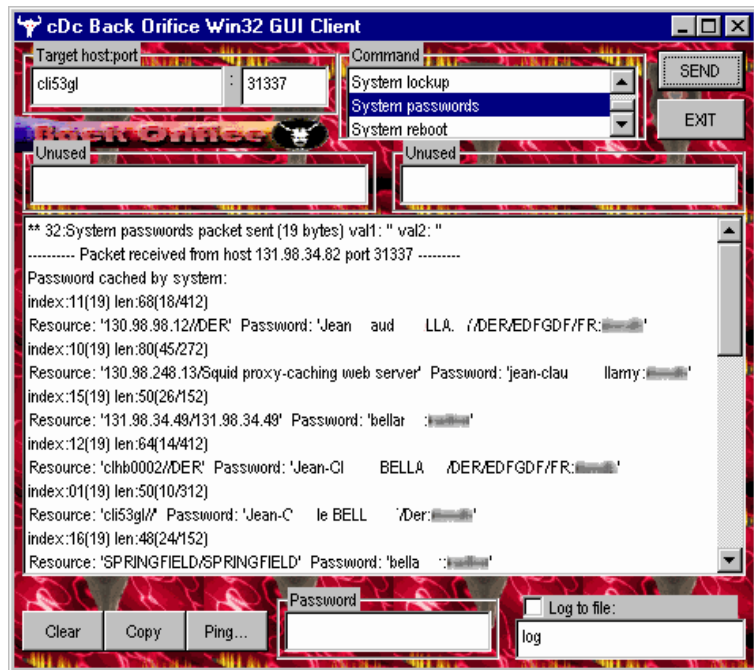
Conover & w00w00 exploitation paper

Format String

Tim Twillman's exploit against ProFTP

Melissa & ILOVEYOU

Biggest Outlook & most malicious email worms



1995

1998

1999

2000

2010

Buffer Overflows

- **CodeRed & Nimda**
First IIS BOF worm targeting White House DOS.
No user interactions.
- **PaX Team ASLR Linux Kernel Patch**
NULL/Dangling Pointer Dereference Attack
- **SQL Slammer, Blaster, Nachi & Sasser**
Most successful worms in history



Sven Jaschan

1995

2001

2004

2010

Organised Criminal Rings

Trojans #1 Weapons

Password, credit cards & personal information

Botnet, Zombies & CC for hire

NULL Pointer Exploitation

Arbitrary Code Execution

Conficker, Stuxnet & CryptoLocker

Most notorious malwares ever created



1995

2004

2008

2010

TODAY

Disgraced CEOs make joint public apology

- 104m credit card account details stolen
- 40% South Korea population
- 3 dozen financial executives resign



CFO apologises to Congress for breach

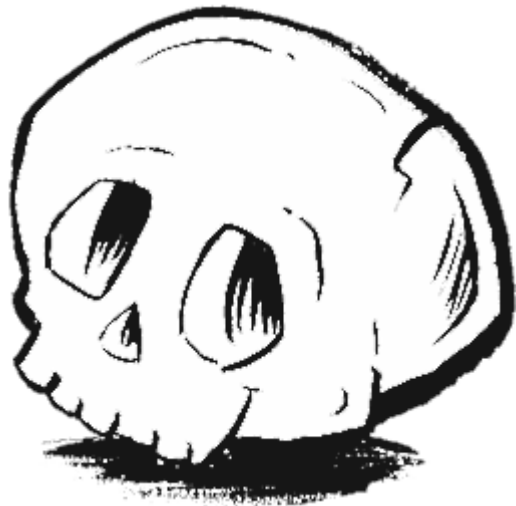


- Nov 27th to Dec 15th 2013
- 110m holiday shoppers affected
- 40m credit cards stolen
- CIO Beth Jacob resigns



CHALLENGES

To Comply, or not to Comply



PCI DSS provides a baseline of technical and operational requirements designed to protect cardholder data

PCI Documentation

- **Standards neither can keep up with attackers**
- **Nor they are intended to**

Compliance is not Security

A blue chain with a brass padlock and a rope knot. The chain is made of thick, blue links. A brass padlock is attached to one of the links. A rope is tied in a knot around the chain.

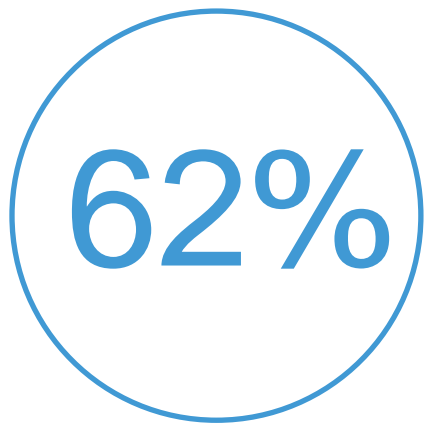
Compliance

is adherence to standards, regulations and industry requirements

Security

is the degree of protection against danger, damage, loss and crime

Overall volume of attacks continue to grow



62% increase in successful breaches and 23% increase in web-based attacks in 2013

- 2014 Internet Security Threat Report, Symantec

Different Types of Attackers



Hacktivists



State Sponsored



Insider Threat



Cyber Criminals

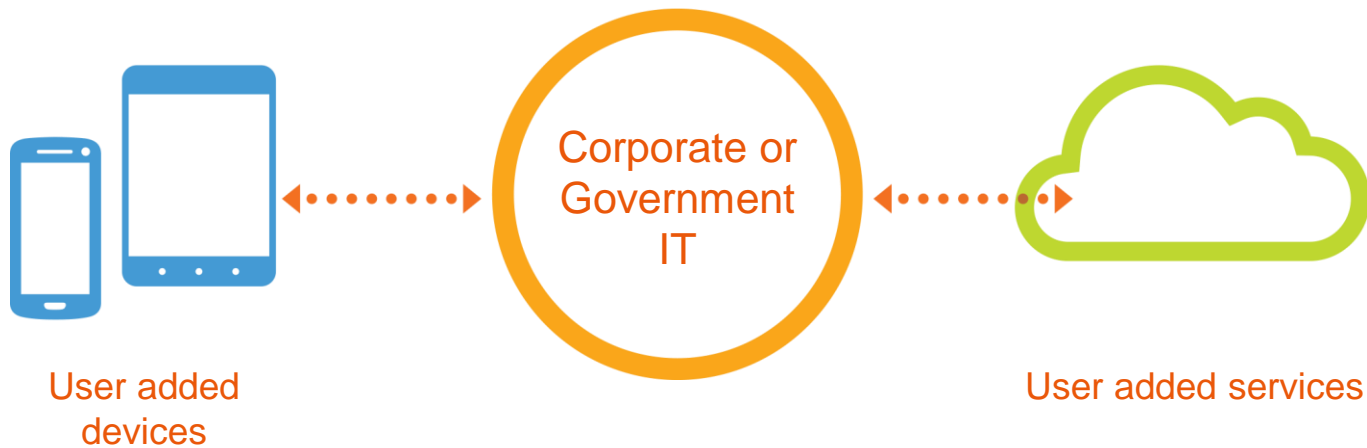
A determined attacker can always get in



60% of organisations were
affected by successful attacks
in 2013

2014 CyberDefense Report, CyberEdge Group

Expanding Attack Surface



Today's attackers are more deceptive

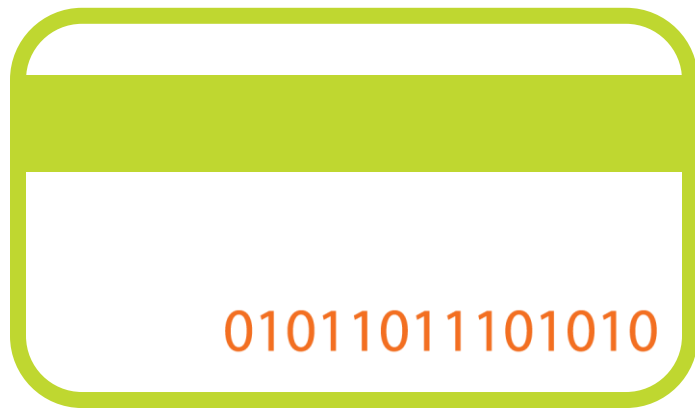


- Stolen credentials is the #1 threat action
 - 76% of network intrusions exploited weak or stolen credentials
- Phishing is the #3 threat action
 - 18% of targeted users will click on phishing link; 9% will open an attachment or fill in a web form

Verizon 2014 & 2013 Data Breach Investigations Report

Evolution of Attackers: Market & Economics

Credit Card Economy



Information Economy



The Cyber Crime Economy

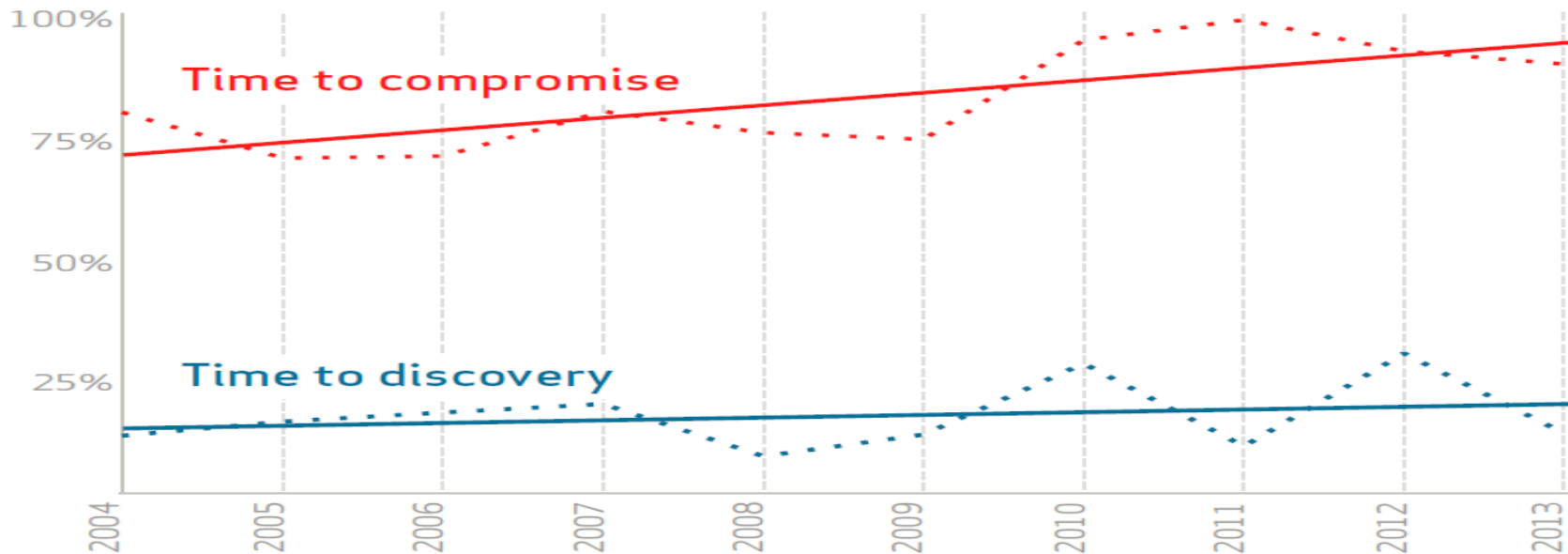


- Credit card numbers & CVV – US\$15 to \$18
- Credit card & track data – US\$28
- Fullz (identity & financial info) – US\$30 to \$40
- Bank account details – US\$300 and less
- Infected computers – US\$20 to \$250

- The Underground Hacking Economy is Alive and Well, SecureWorks

First In, Last Out

Percent of breaches where time to compromise (red)/time to discovery (blue) was days or less



Verizon 2014 Data Breach Investigations Report

TOMORROW?

Focus on the most dangerous threats



Targeting users is now the most common attack method

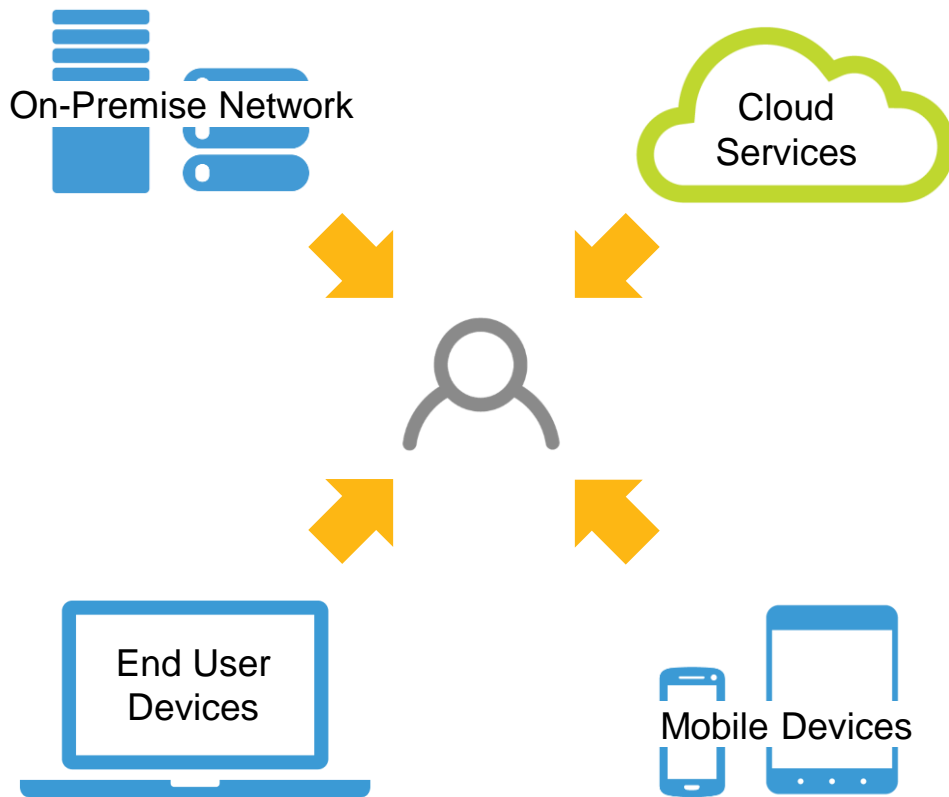


Compromise web-based environments are on the rise



Increasing number of vulnerabilities (60,000 and counting)

Putting users at the centre of your defenses



Understand The Attack

Validate Vulnerabilities

This wizard imports, exploits, and validates vulnerabilities discovered by Nexpose. It then pushes validated vulnerabilities and vulnerability exceptions back to Nexpose.

Create Project

Nexpose Console NX-Austin + Configure a Nexpose Console

Pull from Nexpose

☒ Import existing Nexpose vulnerability data
☐ Start a Nexpose scan to get data

☒ Tag

Exploit

☒ Generate Report

Select sites to import vulnerability data from:

Search:

<input type="checkbox"/>	Name	Assets	Vulns	Modules	Created at
<input type="checkbox"/>	Metasploit-toast-1370293797	45	0	0	2013-11-01T10:36:17-05:00
<input type="checkbox"/>	Metasploit-NXinteractions-1372887762	45	0	0	2013-11-01T15:02:57-05:00
<input type="checkbox"/>	Metasploit-NXCheckAgain-1371748465	1	0	0	2013-11-01T15:02:57-05:00
<input type="checkbox"/>	Metasploit-nexposerightcreds-1368804656	42	0	0	2013-11-01T15:02:57-05:00
<input type="checkbox"/>					2013-11-

Cancel

Start

Test Your Users

Create E-mail Content

1 General
2 Content

Rich text
Plain text
Preview

Template
None ▼

Insert custom attribute: ▲

- First name
- Last name
- Email address
- Link to Landing Page


B *I* ~~S~~ U

[List Icons]

x₂ x²

[Undo] [Redo]

[Align Icons]



Hi {{first_name}},

I'd like to connect with you on LinkedIn.

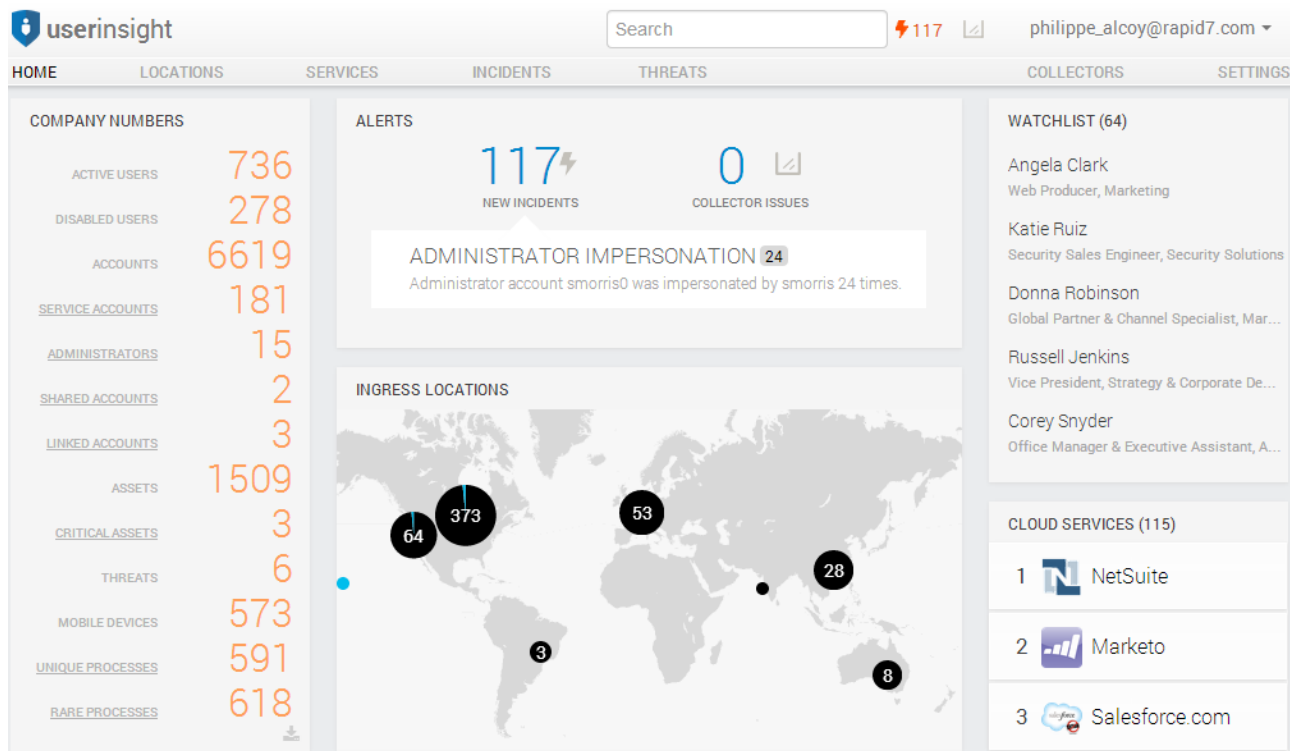
Adrian Lim

Territory Manager, ASEAN

Accept

View Profile

Understand Activity



Understand Incidents

The screenshot displays the 'userinsight' dashboard interface. At the top, there is a navigation bar with tabs for HOME, LOCATIONS, SERVICES, INCIDENTS (selected), THREATS, COLLECTORS, and SETTINGS. A search bar and a notification bell with '117' are also present. The user 'philippe_alcoy@rapid7.com' is logged in. The left sidebar, under 'NOW VIEWING', shows filters for 'Incidents 1 to 20 of 32 incidents', with 'OPEN' selected. Other filters include 'CLOSED', 'ALL', 'FILTER', 'COMPROMISED CREDENTIALS', 'INGRESS ACTIVITY', 'MOBILE', and 'NETWORK PRIVILEGE MONITORING'. The main content area is divided into 'TODAY' and 'YESTERDAY' sections. Under 'TODAY', there are two incidents: 'MULTIPLE COUNTRY AUTHENTICATIONS' at 7:39 AM and 4:33 AM, both involving accounts authenticating from 2 countries. The first incident is associated with 'Bryant Summers' (Security Researcher I, Engineering) and the second with 'Judith Ward' (Sr. Technical Writer, Engineering). Under 'YESTERDAY', there is an incident at 9:58 PM titled 'MULTIPLE COUNTRY AUTHENTICATIONS' involving 'Account bthompson' authenticating from 2 countries, associated with 'Betty Thompson' (Office Assistant, Administration). At the bottom, a summary incident at 12:17 PM titled 'HARVESTED CREDENTIALS' shows '203.117.48.70' failing to access 3 distinct accounts in 1 instance, with a note that 'This incident involves 2 users'.

Time	Incident Title	Description	User	Role
7:39 AM 3/20/14 UTC+08:00	MULTIPLE COUNTRY AUTHENTICATIONS	Account bsummers authenticated from 2 countries in 4 minutes 49 seconds.	Bryant Summers	Security Researcher I, Engineering
4:33 AM 3/20/14 UTC+08:00	MULTIPLE COUNTRY AUTHENTICATIONS	Account jward authenticated from 2 countries.	Judith Ward	Sr. Technical Writer, Engineering
9:58 PM 3/19/14 UTC+08:00	MULTIPLE COUNTRY AUTHENTICATIONS	Account bthompson authenticated from 2 countries in 2 minutes 12 seconds.	Betty Thompson	Office Assistant, Administration
12:17 PM 3/19/14 UTC+08:00	HARVESTED CREDENTIALS	203.117.48.70 failed to access 3 distinct accounts in 1 instances.	This incident involves 2 users	

THANK YOU

philippe_alcoy@rapid7.com