A Journey Into…
IT SECURITY RISK & COMPLIANCE
… aka the coming of age of the credentials

Philippe Alcoy

Technical Director APAC

RAPID7

ISC 2014 中国互联网安全大会

360互联网安全中心

China Internet Security Conference 2014

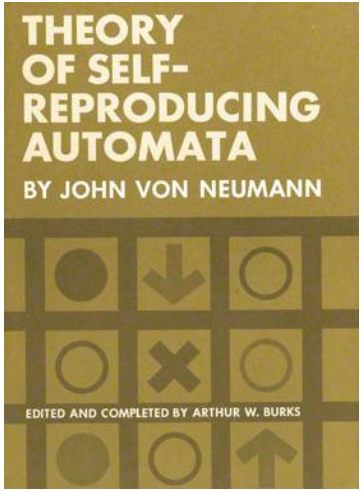
2014中国互联网安全大会

YESTER~~DAY~~YEAR

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

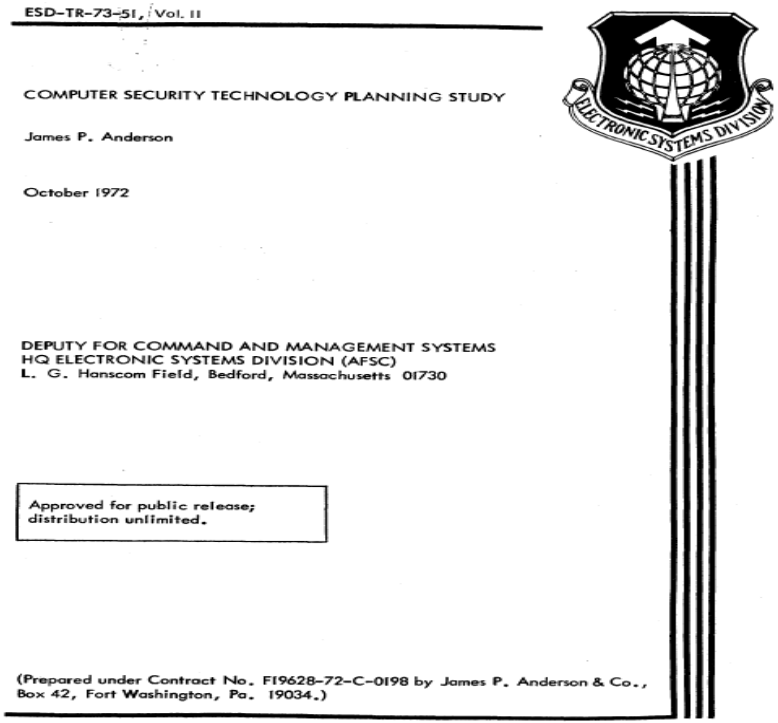
Experiments

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.

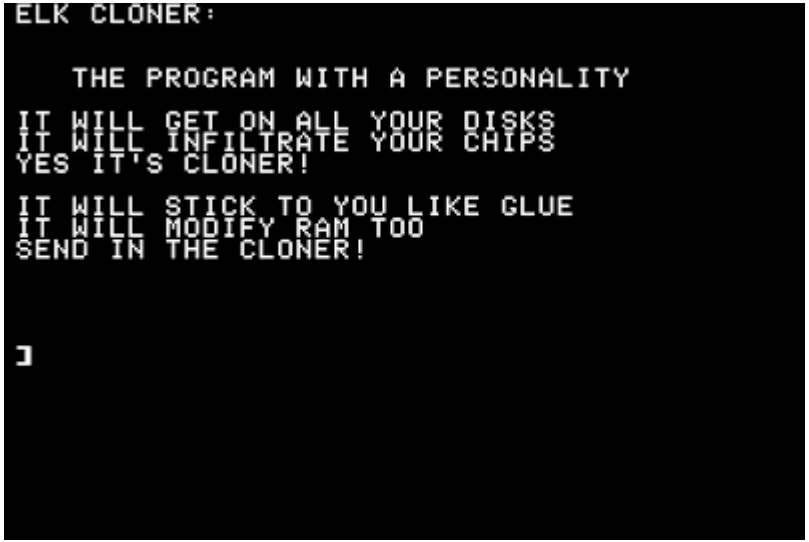
(Prepared under Contract No. F19628-72-C-0198 by James P. Anderson & Co., Box 42, Fort Washington, Pa. 19034.)

1949 1971 1972 1978 1982 1987

Boot Sector Galore

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

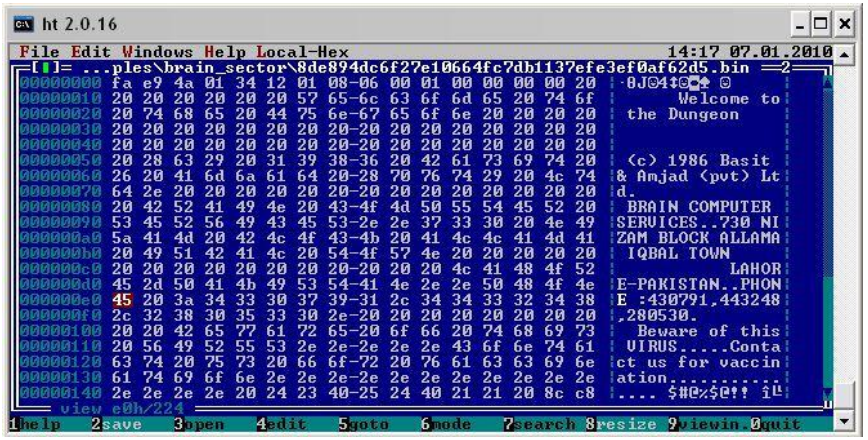
“ARF, ARF, GOTCHA”
Joke viruses, grandfathers of “YOU JUST GOT PWNED!” website hack meme!



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

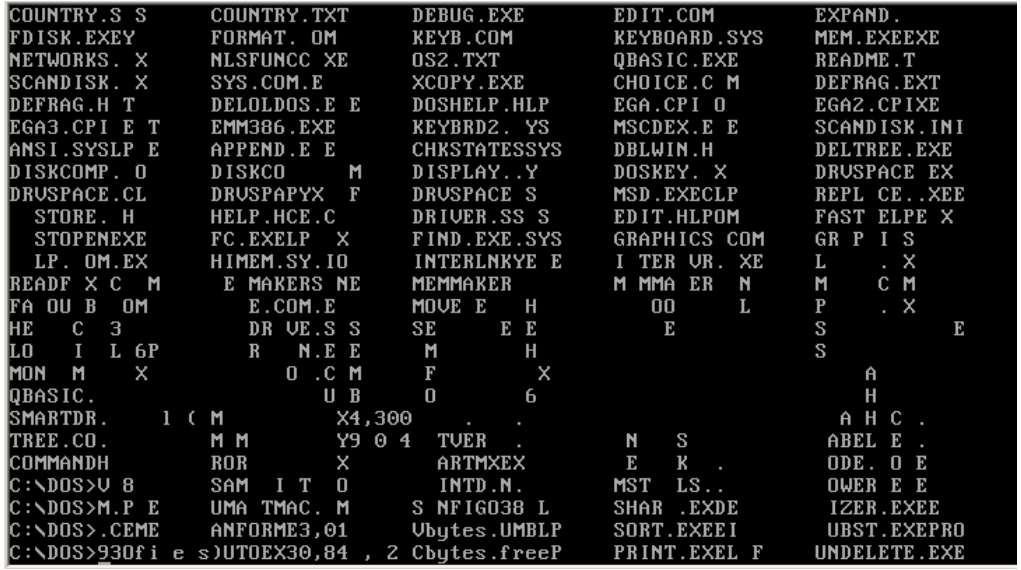
1994

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

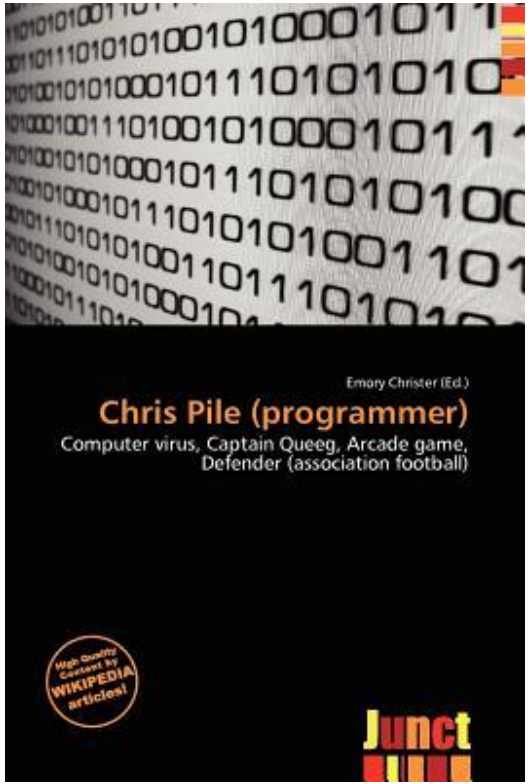
1988 1989 1990 1991 1993 1994

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

Buffer Overflow
Thomas Lopatic step-by-step NCSA HTTPd exploit
Mudge ‘How to write Buffer Overflows’
Aleph1 ‘Smashing the Stack for Fun & Profit’

StackPatch
Solar Designer NX stack

StackGuard
Cowan & al stack canaries

1995 1997 1998 2010

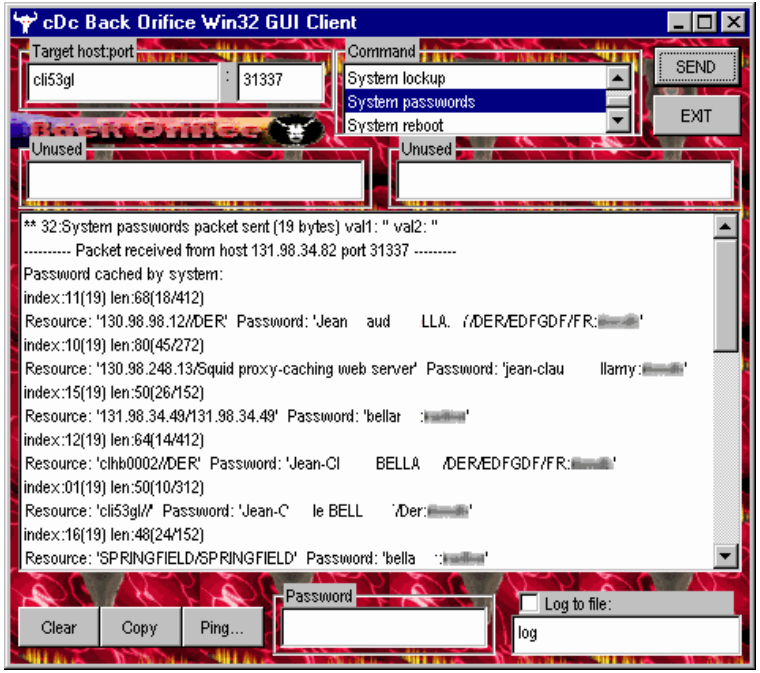
Backdoors

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

NH농협은행

LOTTE CARD

KB

CFO apologises to Congress for breach

TARGET®

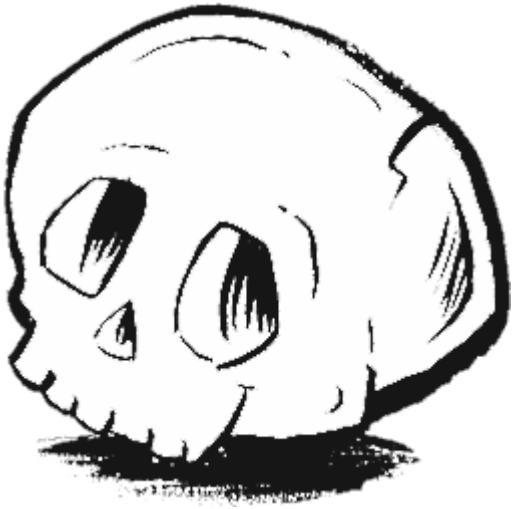
- Nov 27th to Dec 15th 2013
- 110m holiday shoppers affected
- 40m credit cards stolen
- CIO Beth Jacob resigns

PCI DSS COMPLIANT

RAPID7

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

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%

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

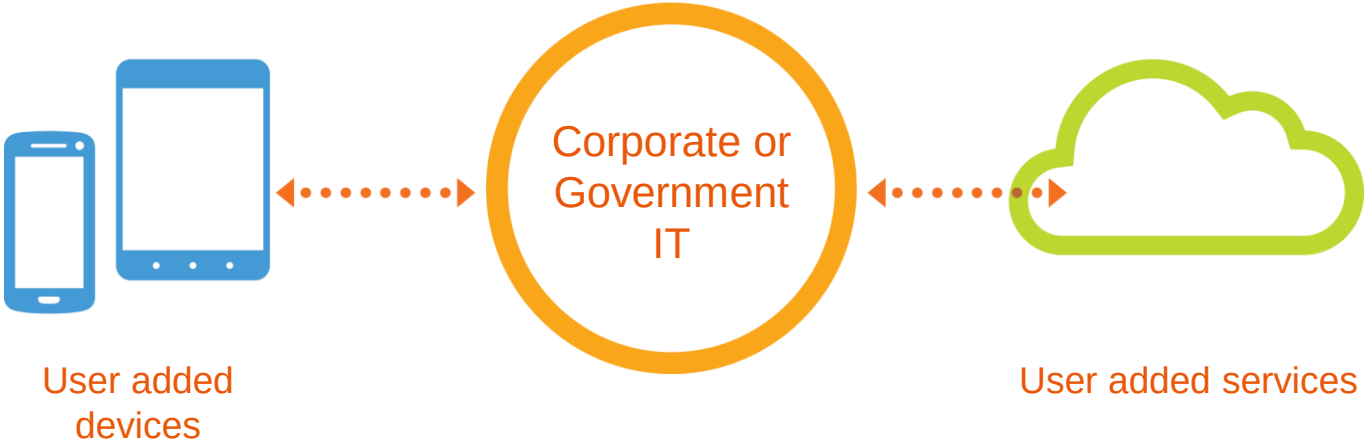
A determined attacker can always get in

60%

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

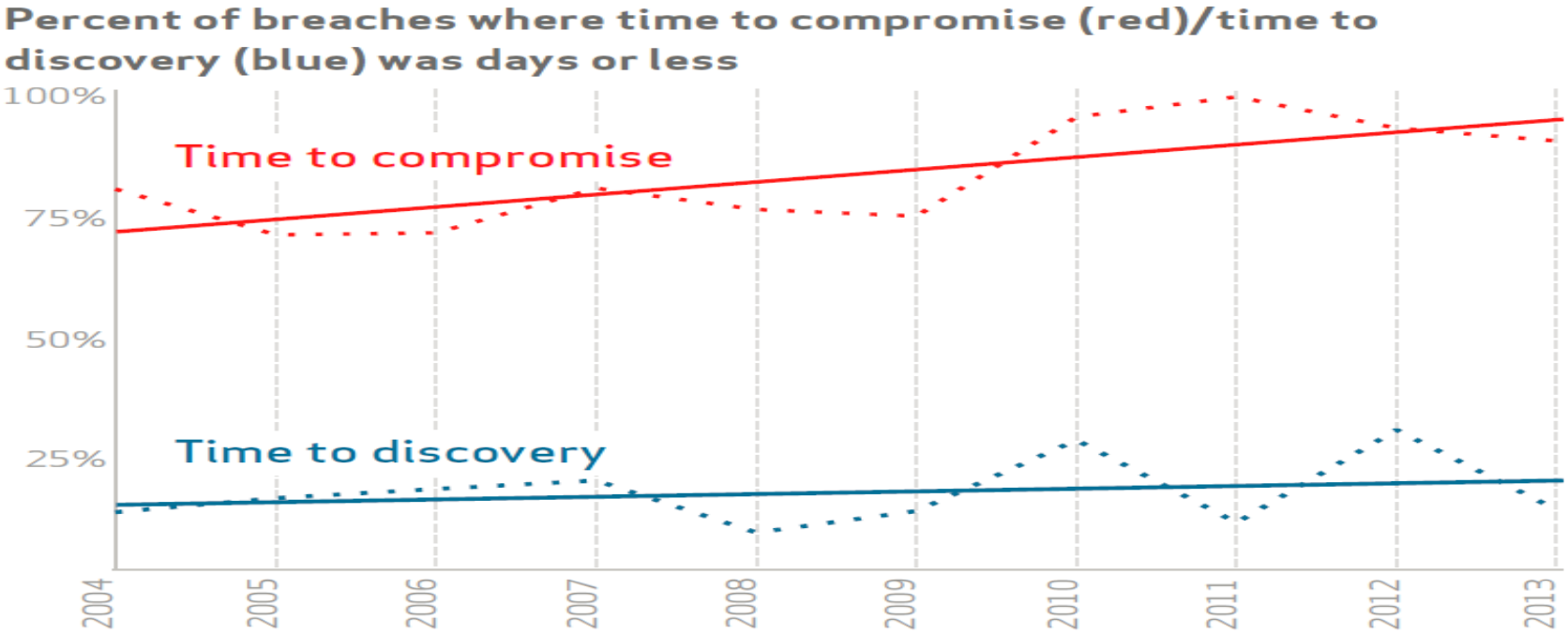
Information Economy

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



Verizon 2014 Data Breach Investigations Report

TOMORROW?

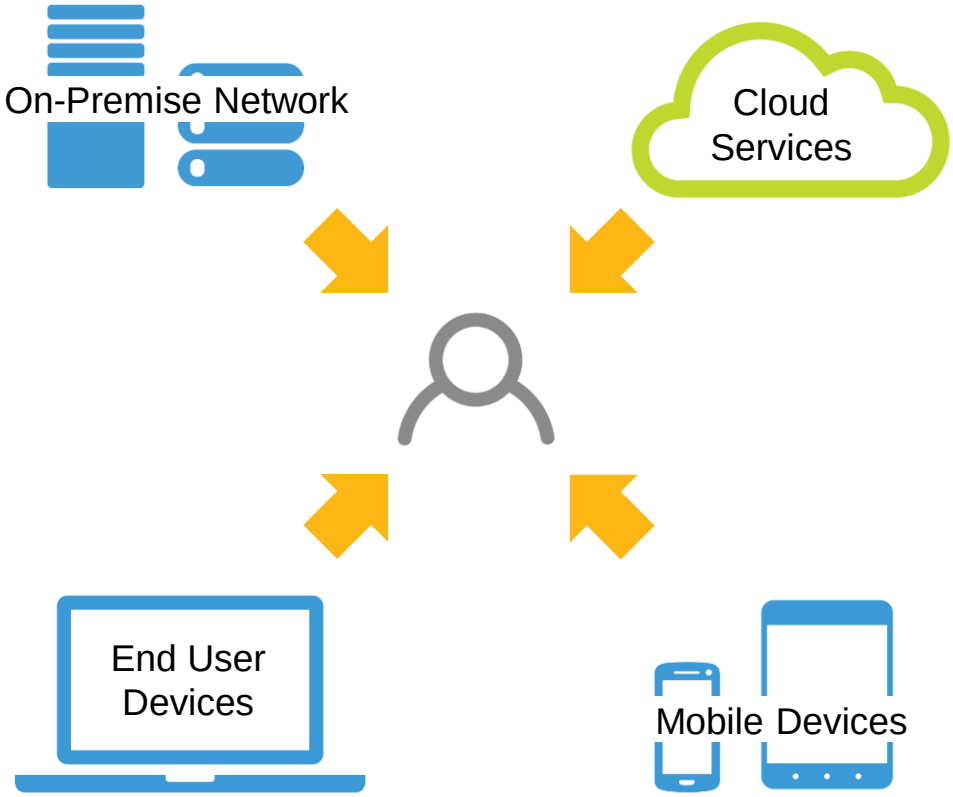
Focus on the most dangerous threats

Targeting users is now the most common attack method

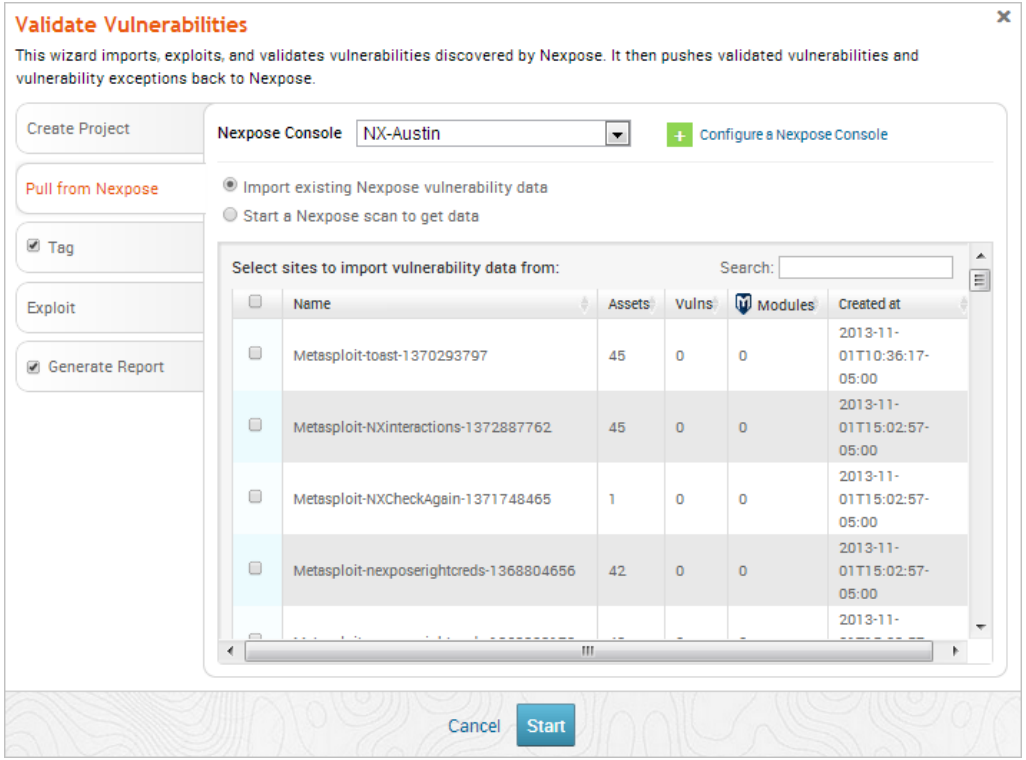
Compromise web-based environments are on the rise

Increasing number of vulnerabilities (60,000 and counting)

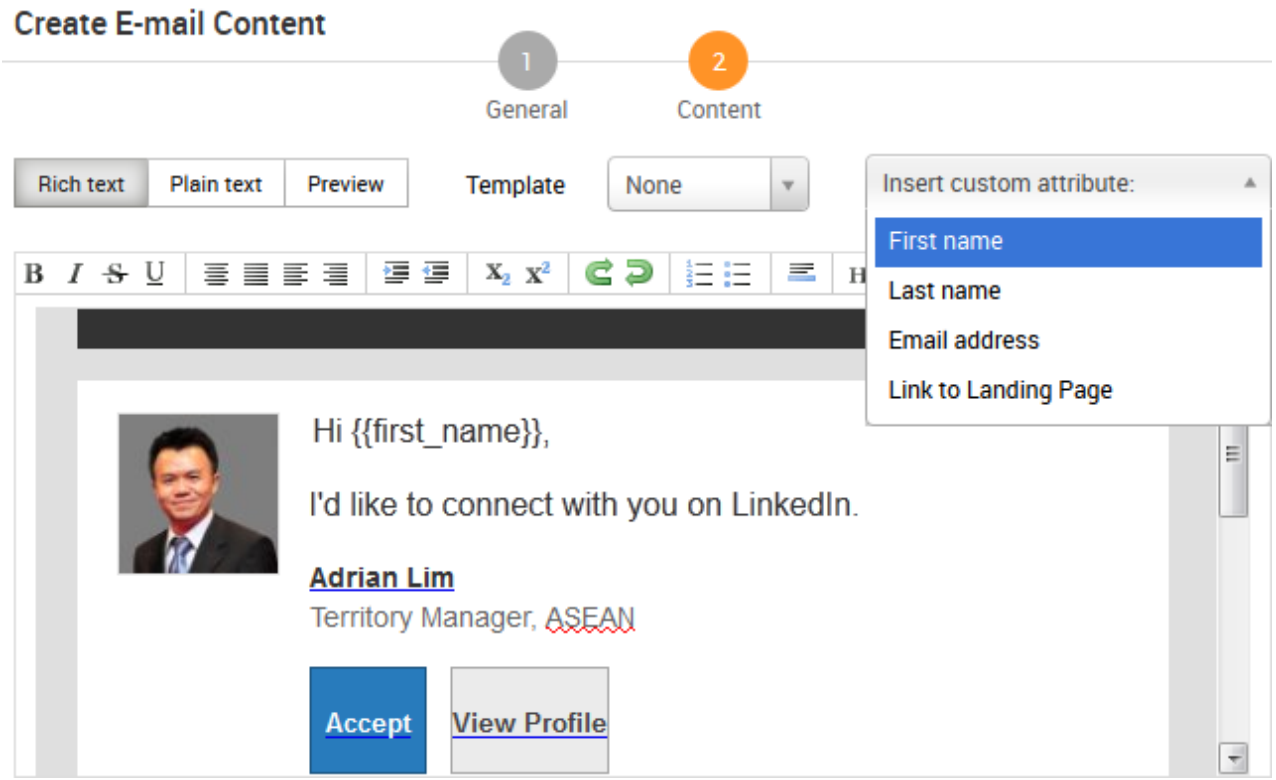
Putting users at the centre of your defenses



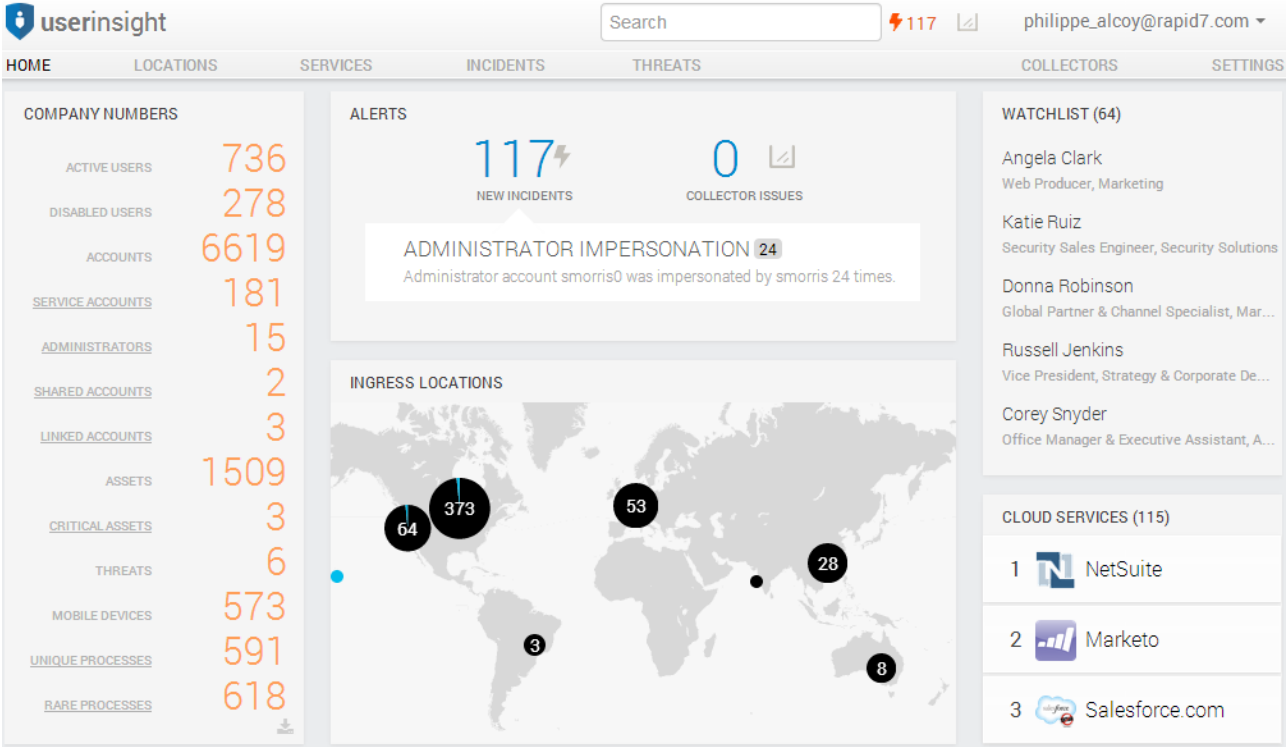
Understand The Attack



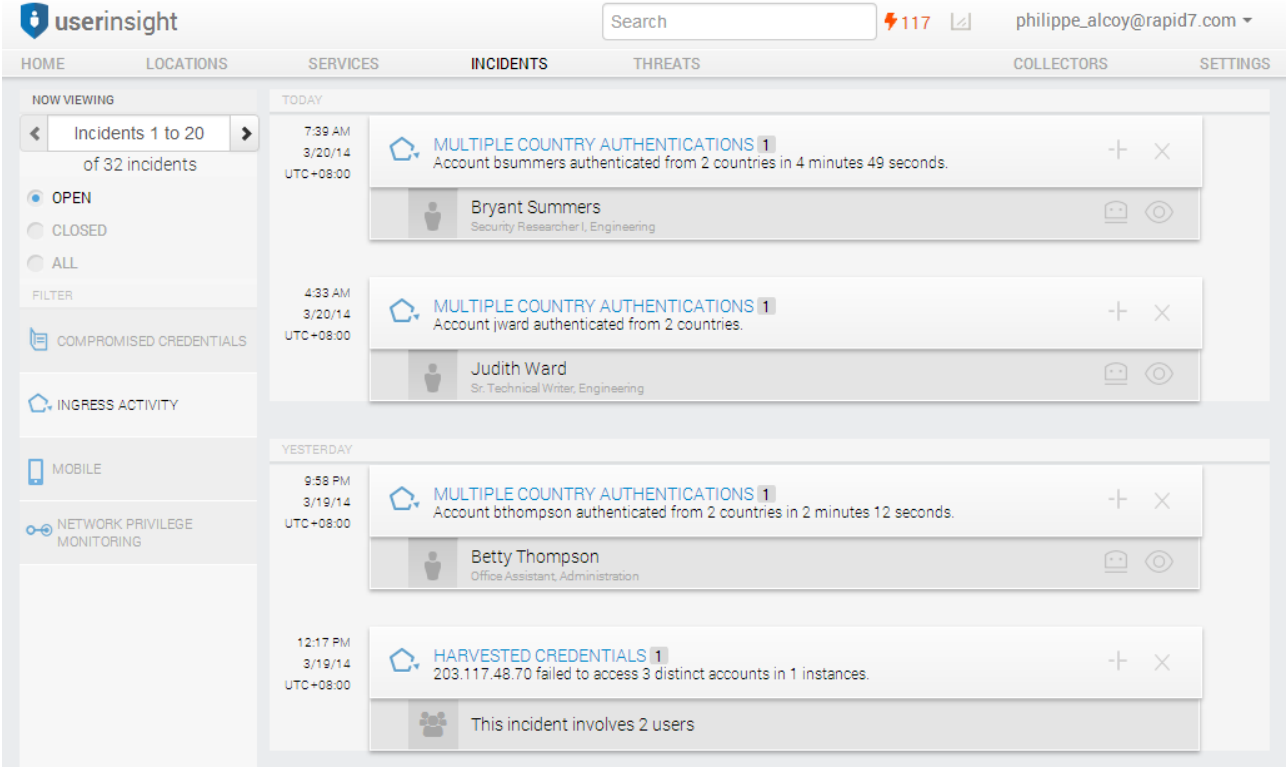
Test Your Users



Understand Activity



Understand Incidents



THANK YOU

philippe_alcoy@rapid7.com