WELCOME TO

Systems
Engineering &
Administration
Technology
User
Group

January 27, 2014

bringing IT together℠

Agenda

- 6:00pm Tech-talk & Networking
- 6:30pm Introduction /
  Tools and Industry news
- 6:45pm 5 Ways Corporate IT Enables Cybercrime
- 7:30 Deep Dive on Cryptolocker
- 8:00 Highlights of Verizon DBIR
- ?:?? Post Meeting Networking

SEA-TUG

bringing IT together℠

What is SEA-TUG?

- Founded in 2001 by Steve Noel and Rob Bergin to create a collegial group of IT professionals willing to share their knowledge. We aim to create an open and collaborative forum for the e-Coast.

- This is YOUR user group – help us make it better. What topics do you want covered? What resources can you contribute? Please help spread the word!

- 400 local IT pros on the mailing list – if you have not joined, email caretaker@sea-tug.com

SEA-TUG

bringing IT together℠

Worst Passwords of 2013

http://www.symantec.com/connect/blogs/worst-passwords-2013

Rank	Password	Change from 2012
1	123456	*Up 1*
2	password	*Down 1*
3	12345678	*Unchanged*
4	qwerty	*Up 1*
5	abc123	*Down 1*
6	123456789	*New*
7	111111	*Up 2*
8	1234567	*Up 5*
9	iloveyou	*Up 2*
10	adobe123	*New*
11	123123	*Up 5*
12	admin	*New*
13	1234567890	*New*
14	letmein	*Down 7*
15	photoshop	*New*
16	1234	*New*
17	monkey	*Down 11*
18	shadow	*Unchanged*
19	sunshine	*Down 5*
20	12345	*New*
21	password1	*Up 4*
22	princess	*New*
23	azerty	*New*
24	trustno1	*Down 12*
25	000000	*New*

Also see:
The worst 500 passwords of all time

http://www.symantec.com/connect/blogs/top-500-worst-passwords-all-time

SEA-TUG

bringing IT together sm

Tools

- Algosec firewall policy analyzer
- Archive.org
- MXToolbox.com
- Whois.sc
- Postlayer.com / MXGuardDog.com
- Securelist.com
- Threatpost.com
- Live.sysinternals.com
- PermissionsAnalyzer
- Extrahop / Riverbed Cascade
- Lucid8
- Windows 8 To-Go

bringing IT together sm

Industry News

- **Airwatch sold to Vmware for $1,540,000,000**
  - http://www.rethink-wireless.com/2014/01/22/vmware-pays-hefty-15bn-airwatch.htm
- **Windows Server Disaster Recovery Preparation**
  - http://blogs.technet.com/b/askpfeplat/archive/2012/02/13/disaster-recovery.aspx
- **Why .com.com should scare you**
  - https://blog.whitehatsec.com/why-com-com-should-scare-you/
- **NIST guidance on securing virtual environments**
  - http://csrc.nist.gov/publications/nistpubs/800-125/SP800-125-final.pdf
- **Scott Hanselman's 2014 Ultimate Developer and Power Users Tools for Windows**
  - http://www.hanselman.com/blog/ScottHanselmans2014UltimateDeveloperAndPowerUsersToolListForWindows.aspx

SEA-TUG

bringing IT together sm

Resources you should know…

- Microsoft Security Incident Review
  - http://www.microsoft.com/security/sir/default.aspx
- Symantec Annual Threat Report
  - http://www.symantec.com/security_response/publications/threatreport.jsp
- Verizon Data Breach Investigation Report
  - http://www.verizonenterprise.com/DBIR/
- Mandiant APT Report
  - http://intelreport.mandiant.com/
- ISC² Storm Center Daily Diary
  - http://isc.sans.edu
  - http://www.securingthehuman.org/resources/newsletters/ouch

bringing IT together℠

More SANS Resources

There are a number of other blogs hosted by SANS:

- Digital Forensics Blog - http://computer-forensics.sans.org/blog
- Penetration Testing and Ethical Hacking Blog - http://pen-testing.sans.org/blog
- Software Security Blog - http://software-security.sans.org/blog
- IT Audit Blog - http://it-audit.sans.org/blog
- Cloud Security Blog - http://www.sans.org/cloud

Some other SANS related sites, although not blogs, also host some excellent free security resources:

- The SANS/GIAC Reading Room - http://www.sans.org/reading_room/
- Securing the Human - http://www.securingthehuman.org/
- STI and Faculty Research - http://www.sans.edu/research/
- Windows Security blog - http://www.sans.org/windows-security

bringing IT together sm

Breach Info

Chronology of Data Breaches Security Breaches 2005 - Present

- http://www.privacyrights.org/data-breach

State of NH catalog of data breaches involving NH citizens:

- http://doj.nh.gov/consumer/security-breaches/

Department of State Bureau of Diplomatic Security (OSAC)

- https://www.osac.gov/Pages/CategoryHome.aspx?CategoryId=7

SEA-TUG

bringing IT together sm

Cryptolocker – your money or your life webcast

- Short presentation / lots of Q&A
  - http://www.viddler.com/v/7cc149f6

bringing IT together℠

Tonight's Presentation

1. **5 Ways Corporate IT Enables Cybercrime**
   Mark Villinski | Kaspersky Lab

2. **Deep Dive on CryptoLocker**
   Andrey Pozhogin | Kaspersky Lab

3. **Verizon Data Breach Investigation Report Highlights**
   Angelo Cianci | Verizon

KASPERSKY lab

verizon

SEA-TUG

bringing IT together℠