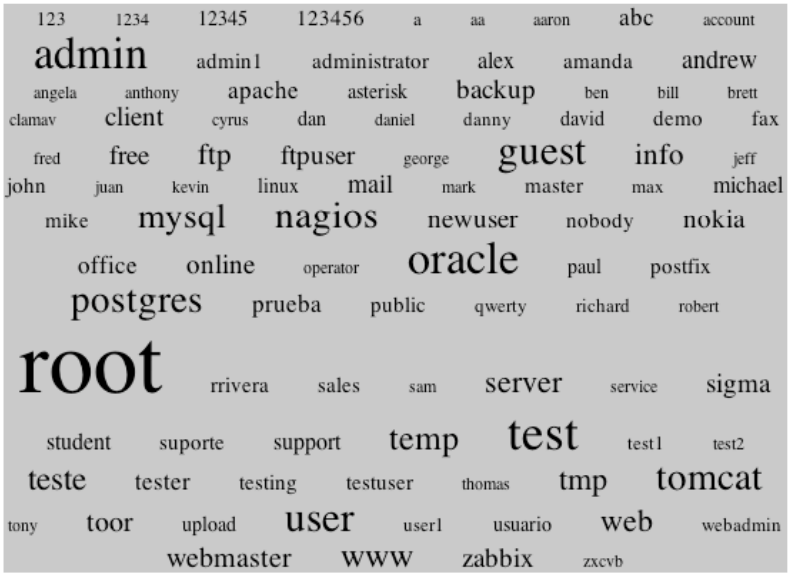
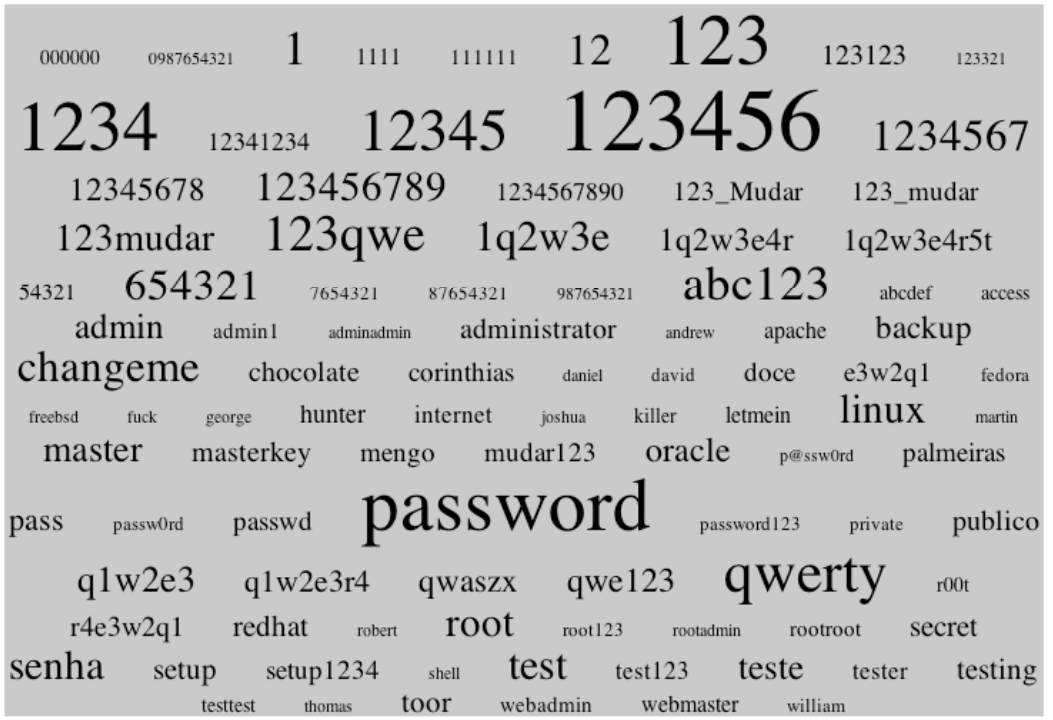
DRG SSH Username and Password Authentication Tag Clouds

2010-11-03 17:00:24 - 2010-11-10 17:00:24

most popular usernames



most popular passwords



http://www.dragonresearchgroup.org/insight/sshpwauth-cloud.html

Local ICSI hosts contacted via SSH by remote hosts

Weds Nov 10, 2010 - 1AM-11AM

# Local Hosts	Remote Host
512	202.148.2.22
140	95.155.122.12
140	161-96-207-82.ip.ukrtel.net
140	80.224.43.54.static.user.ono.com
140	adsl-074-238-205-245.sip.mem.bellsouth.net
140	adsl-70-247-71-201.dsl.hrlntx.swbell.net
140	nc-65-40-234-248.sta.embarqhsd.net
140	ip-62-129-164-36.evc.net
140	222.107.61.161
140	217-220-124-90-static.albacom.net
140	informatika.brkk.hu
140	208.124.238.246
140	166.129.109.202.dial.nc.jx.dynamic.163data.com.cn
140	201.227.239.11
140	200.182.126.166
140	static-adsl190-29-2-204.une.net.co
140	190.254.98.18
140	190.253.223.162
140	static-adsl190-248-8-19.une.net.co
140	190.144.81.234
140	189-210-153-50.static.axtel.net
140	189-20-68-59.customer.tdatabrasil.net.br
140	187.53.57.247
140	180.168.5.184
140	150.162.10.60
140	147.subnet125-160-246.speedy.telkom.net.id
140	124.193.106.231
140	122.229.6.189
140	122.224.135.163
140	115-186-131-75.nayatel.pk
140	115-186-131-106.nayatel.pk
139	dsl-202-173-145-182.qld.westnet.com.au

To: vern@ee.lbl.gov
Subject: RE: Russian spear phishing attack against .mil and .gov employees
From: jeffreyc@cia.gov
Date: Wed, 10 Feb 2010 19:51:47 +0100

Russian spear phishing attack against .mil and .gov employees

A "relatively large" number of U.S. government and military employees are being taken in by a spear phishing attack which delivers a variant of the Zeus trojan. The email address is spoofed to appear to be from the NSA or InteLink concerning a report by the National Intelligence Council named the "2020 Project". It's purpose is to collect passwords and obtain remote access to the infected hosts.

Security Update for Windows 2000/XP/Vista/7 (KB823988)

About this download: A security issue has been identified that could allow an attacker to remotely compromise a computer running Microsoft Windows and gain complete control over it. You can help protect your computer by installing this update from Microsoft. After you install this item, you may have to restart your computer.

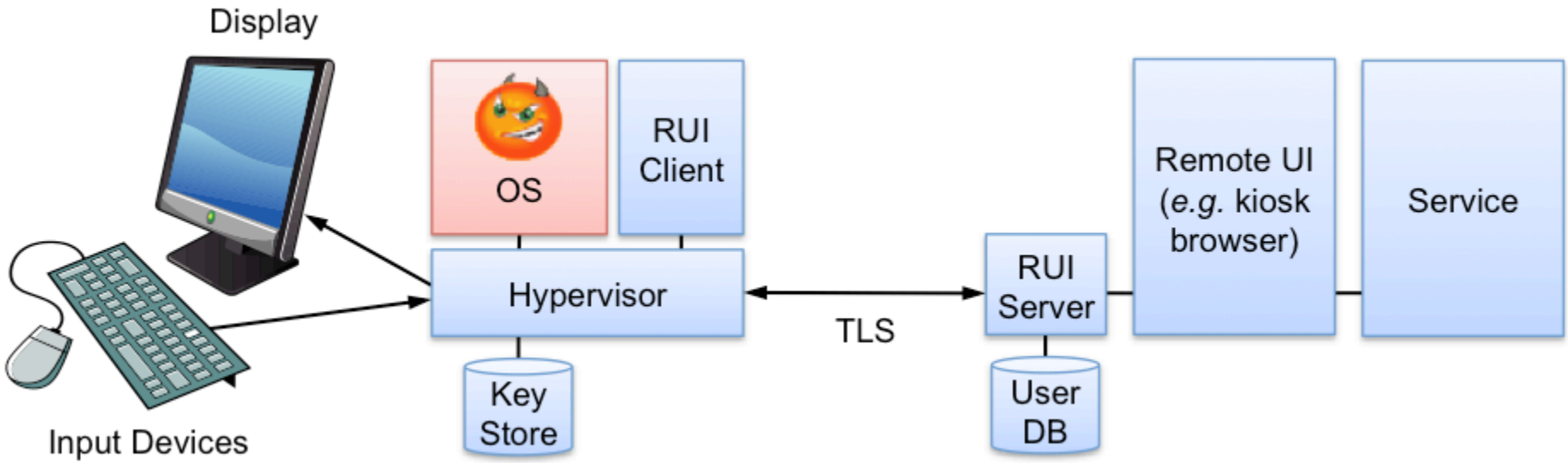
Download:

http://mv.net.md/update/update.zip

or

http://www.sendspace.com/file/xwc1pi

_____
Jeffrey Carr is the CEO of GreyLogic, the Founder and Principal Investigator of Project Grey Goose, and the author of "Inside Cyber Warfare".
jeffreyc@greylogic.us


Display
OS
RUI Client
Hypervisor
Key Store
Input Devices
TLS
RUI Server
User DB
Remote UI (e.g. kiosk browser)
Service