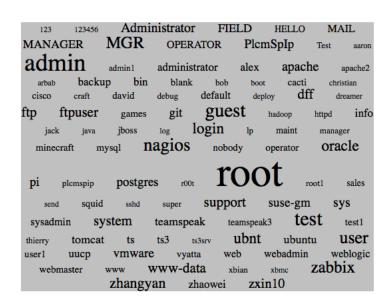


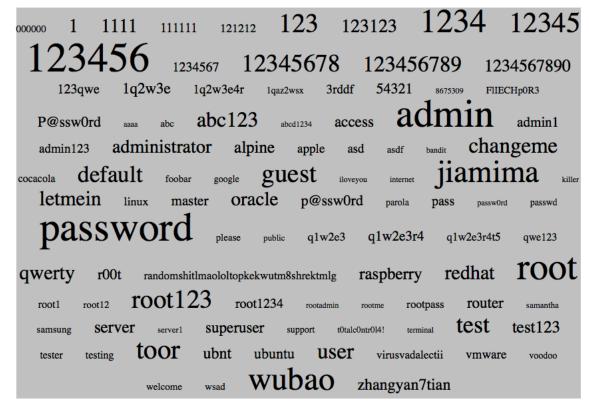
## **DRG SSH Username and Password Authentication Tag Clouds**

2015-04-01 15:40:40 - 2015-04-08 15:40:40

most popular passwords



most popular usernames



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

## Local ICSI hosts contacted via SSH by remote hosts

Tues Apr 7, 2015

# Local			
Hosts	Remote Host		
512	blade-server.leasevps.c	om	
512	61.182.227.182		
512	43.255.191.163		
512	43.255.191.141		1:000 000
512	43.255.190.60	440	li618-127.members.linode.com
512	222.236.44.115	410	218.200.188.213
512	222.215.230.216	401	netscan.gtisc.gatech.edu
512	222.186.56.101	322	134.213.58.205
512	221.235.188.213	264	185.35.56.47.venomit.com
512	183.136.216.7	245	111.204.175.8
512	122.228.207.76	244	222.186.34.242
512	118.244.136.200	241	211.154.6.101
512	117.6.133.229	240	222.186.129.101
512	113.98.255.48	222	94.79.33.21
511	117.21.225.165	218	cloud1.brainhost.com
510	43.255.191.170	214	www.compumir.ru
509	222.186.42.175	214	183.56.129.146
505	221.235.188.210	211	researchscan273.eecs.umich.edu
502	43.255.191.168	208	185.7.182.177
500	218.77.79.43	207	182.100.67.115
497	43.255.191.165	206	218.87.109.60
495	43.255.191.161	206	73.30.65.218.broad.xy.jx.dynamic.163data.com.cn
489	112.253.2.180	205	researchscan433.eecs.umich.edu
485	43.255.191.166	204	91.236.74.164
485	211.153.66.43	204	researchscan160.eecs.umich.edu
477	218.7.37.194	203	23.30.65.218.broad.xy.jx.dynamic.163data.com.cn
474	61.240.144.66	203	122.228.207.77
455	221.235.188.212	[208 >= 10	local elided]

Order	Password	Occurences	Percentage				
1	123456		3.11				
2	111111	322	1.77				
3	123123	200	1.1				
4	qwerty	196	1.08				
5	123321	157	0.86				
6			0.68				
7	6 123456789 12 7 12345 10		0.57				
8	666666		0.53				
9	1234567	80	0.44				
10	0	0 65					
11	7777777	60	0.36 0.33				
12	121212	58					
13	1234567890	54	0.3				
14	159753	53					
15	555555	48					
16	12345678	46					
17	112233	45					
18	q1w2e3		0.23				
19	qweqwe	41					
20	123qwe	40	0.22				
21	123	40	0.22				
22	life777	40	0.22				
23	654321	36					
24	qazwsx	31	0.17				
25	gfhjkm	30	0.16				

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

----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

\_AirBears UID 1051850 will be blocked, per the SNS notice associated with tracking number [SNS #902375].

To avoid being blocked from the Airbears network, you must go to the link below and login with your Calnet id and password:

http://auth.berkeley.edu/cas/login/?service=https%3A%2F%2Fsecurity.berkeley.edu%2Flogin%2Fcas

The blocking will be suspended if valid Calnet id and password have been provided no later than 23:59 on Mar 24.

System and Network Security

-----BEGIN PGP SIGNATURE-----Version: GnuPG v2.0.22 (FreeBSD)

iD8JJIlid+8923ljsdwWTf6yM0oJEJOljwenfiOIEIFFXOwefhliuuNSACeLXka EJUlyJEoe992webRAURx4xbx= =6Nch

----END PGP SIGNATURE-----

mandrillapp.com/track/click/30563913/auth.berkeley.netne.net?p=eyJzIjoiSFA3M1ZvenB5WFRPX094dUozdkpudENM...Zjg3NDA1NjNjZjQ5N1wiLFwidXJsX2lkc1wiOltcImIzN2RiO

						Usab	ility		Dep	loyal	bility	l		Securi	ty	1
The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes												tion	g sing	ion -Verifiers		
University of Cambridge Microsoft Research Cambridge, UK Redmond, WA, USA jcb82@cl.cam.ac.uk cormac@microsoft.com	Ottawa, ON, Canada paulv@scs.carleton.ca fro	Frank Stajano <sup>†</sup> Iniversity of Cambridge Cambridge, UK unk.stajano@cl.cam.ac.uk	in section		-Effortless -Users	arry Ifortless	rn Jse	Infrequent-Errors Easy-Recovery-from-Loss	Accessible Negligible-Cost-per-User	vatible npatible	tarv	Physical-Observation Targeted-Impersonation	Resilient-to-Throttled-Guessing Resilient-to-Unthrottled-Guessing	Internal-Observation Leaks-from-Other-Verifiers	Theft	No-1 nisted-1 nird-rary Requiring-Explicit-Consent Unlinkable
http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-817.pdf  Category Scheme			Described in	Reference	Memorywise-Effortless Scalable-for-Users	Nothing-to-Carry Physically-Effortless	Easy-to-Learn Efficient-to-Use	Infrequent-Errors Easy-Recovery-fro	Accessible Negligible-C	Server-Compatible Browser-Compatible	Mature Non-Proprietary	Resilient-to-	Resilient-to- Resilient-to-	Resilient-to- Resilient-to-	Resilient-to-Theft	No-1 rustea-1 tura-rarty Requiring-Explicit-Con Unlinkable
	(Incumbent)	Web passwords		[13]		•	• •	0 •	• •	• •	• •	0	)		•	• • •
	Password managers		IV-A		0 0	0 0	••	•	• •	•	••	0 0				• • •
	Proxy		IV-B	[42] [5] [23]	•	00		0		0		0 0		0		
	Federated	Impostor OpenID Microsoft Passport Facebook Connect BrowserID OTP over email	IV-C		0 0	• 0 • 0 • 0	0 • • • • • • • • • • • • • • • • • • •		•	0	0	0 0	00			
	Graphical	PassGo		[7] [47]		:	• 0 • 0	0 •			0		0	•		
	Cognitive	GrIDsure (original) Weinshall Hopper Blum Word Association		[48] [49] [50]		:	• •	0 0				0		•		
	Paper tokens	S/KEY PIN+TAN		[32] [51]				0 0	•					::	0	
	Visual crypto  Hardware tokens	PassWindow RSA SecurID Yubikey Ironkey CAP reader Pico	IV-G	[52] [34] [53] [54] [55] [8]	0 0	0	• 0 • 0 • 0	0 0 0 0	•			0 0		0		
	Phone-based			[36] [56] [6]	• •		• 0		0					0 0	0	
		Fingerprint Iris Voice	IV-I	[38] [39] [40]	::	• 0	• 0 • 0		0 0 0 0			•	0			• O
	Recovery	Personal knowledge Preference-based Social re-auth.		[58] [59] [60]	0	:	• •	0 • • 0	::	:	0	0	)	00		• <u>0</u>