RAPID7

HACKING HOTEL KEYS

And Point of Sale Systems



Security Consultant
TWITTER, LinkedIN @westonhecker
Rapid7 www.rapid7.com



“A Little Bit About Myself”

- ✓ Senior Security Engineer/Senior Pentester/ Security Researcher.
- ✓ About 11 years pen-testing, Security Research, Speaker at Defcon 22, 23 and 24 Las Vegas, HOPE 11, TakedownCON 2016,B-sides Boston, Blackhat 2016, Enterprise Connect 2016, ISC2, SC Congress Toronto.
- ✓ 12 years programming and Reverse Engineering.
- ✓ Side projects Department of Home Land Security. Attacking 911 centers / Malware Analysis Ransomware. Hacking ATM’s, Cars, Point of Sale Systems, Hotel Key Systems - Property Management Software.



What Is This Talk About?

- ✓ Explain magstrip readers Magspoofer. Difference from RFID
- ✓ Explain Modification to device.
- ✓ Hotel back ends explained, POS systems Explained
- ✓ Process of key checkout check in. Different parts of hotels.
- ✓ Attacks on Privileged Keys. Maids, Service , Fireman
- ✓ Encryption is just encoded.



What Is This Talk About?

- ✓ What lead to research on POS from hotel keys.
- ✓ How Do POS systems use magstripe readers.
- ✓ Trigger events and when the Reader listening and what is it listening for.
- ✓ Management cards on POS/card readers on the screen.
- ✓ How is a magstripe reader Used as a HID keyboard?.
- ✓ Injecting 102-US and proprietary keyboard layouts into binary data.
- ✓ Cash tend/Check tend attack.
- ✓ Attacking OS SQL injection CMD Drive by attack
- ✓ Restaurant attacks/other mag readers/Rewards programs and players cards on slot machines

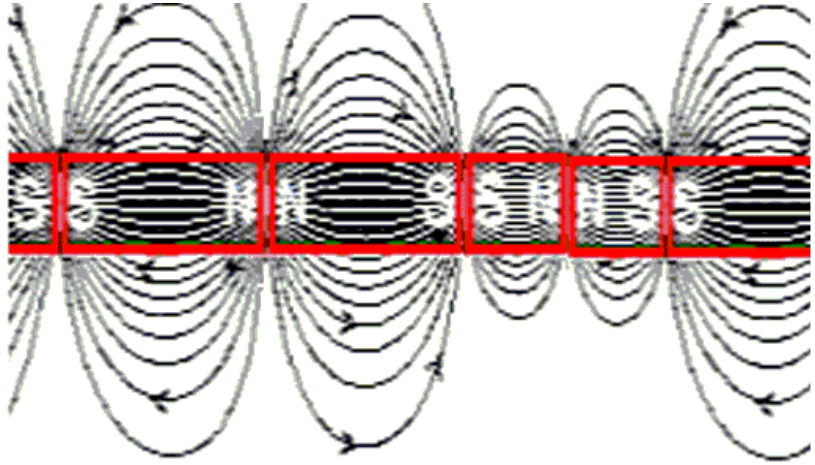
Thanks to Samy Kamkar for his work.

- What is Magspoofer

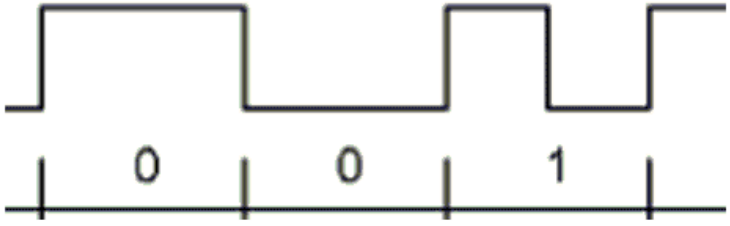




How does a Magstipe Reader work









How magspoofer works what is SMT

- Explanation of Magspoofer+ and EM fields and how they interact w ith Heads on magnetic head read er this is not RFID Cards!!!.

How To Handle Over Heating

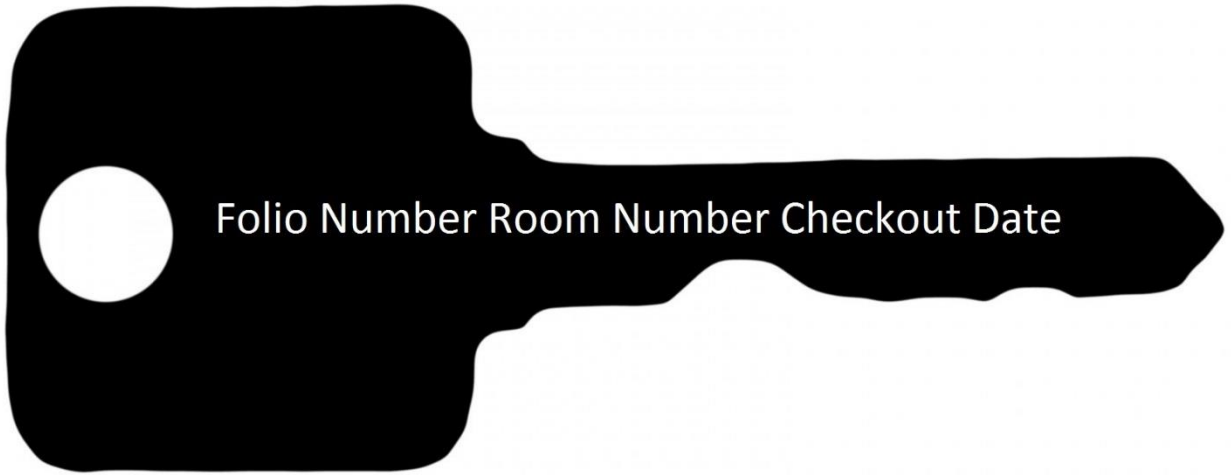


100s of Cards = Heat

Explanation of PMS

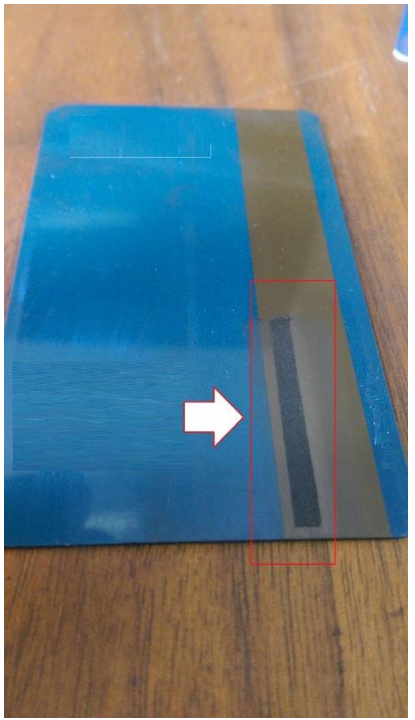


Explanation of proprietary card readers and security behind hotel keys.



Collecting information from keys and reissued keys.



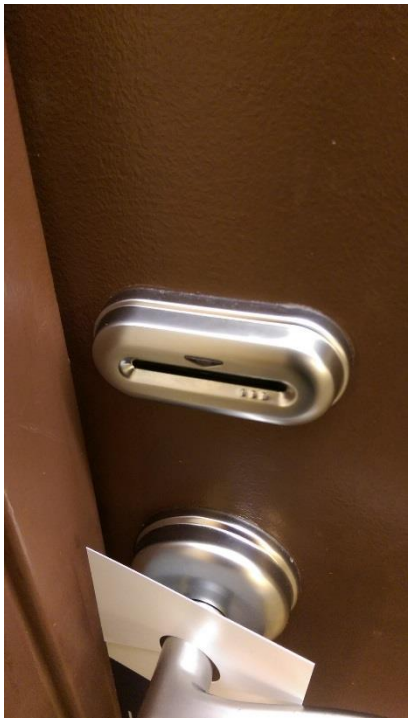


Interactions with different readers your door vs elevator external access and pool access.



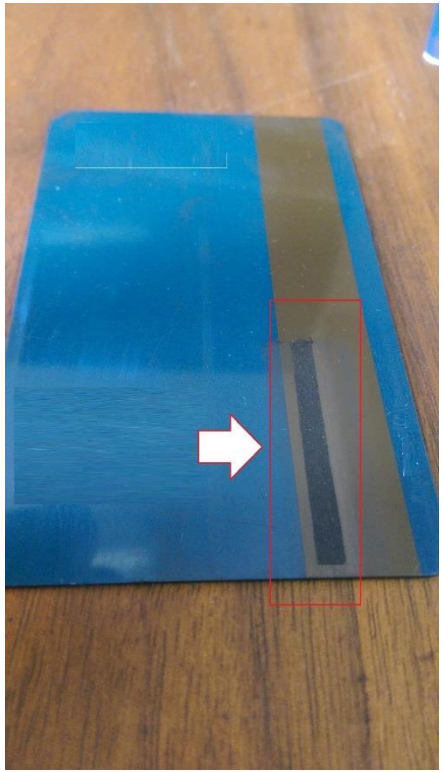


Privileged cards Management, Maids, Service, Fireman law enforcement.

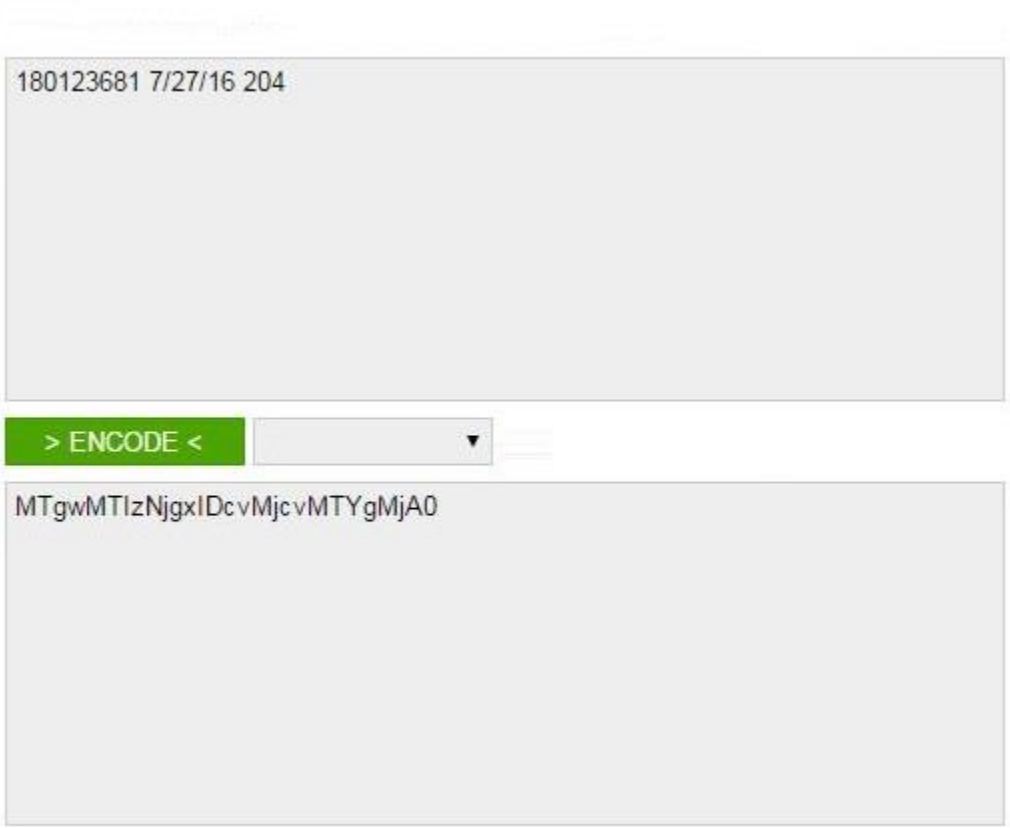


Examples of card Dumps Raw data fr om track 3 other tracks restaurant an d Resort functions.

There are limitations on characters you can enter



Breaking the complex encryption of hotel keys... o it’s simple encoding never mind.



Checking into your own hotel room KIOSK research.



Point of Sale Systems

- What lead to this research after
- hotel keys?

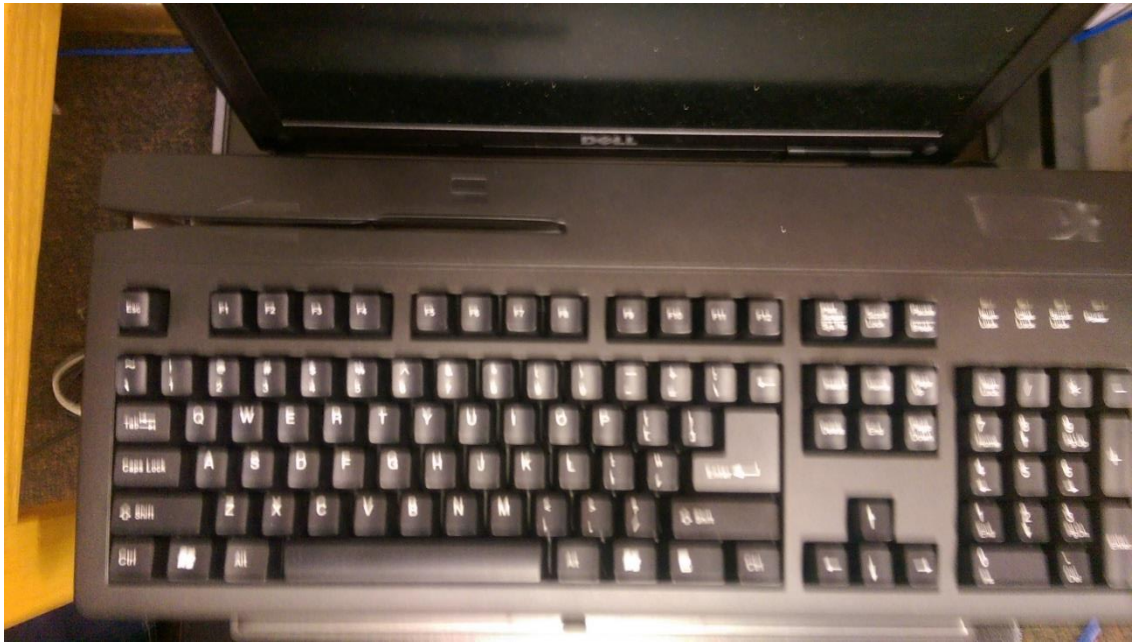




How do POS systems use magstripe readers?







Trigger events and when the Reader listening and what is it listening for.





- Management cards on
- POS/card readers on the screen.





How is a magstripe reader Used as a HID keyboard?



ASCII control characters

00	NULL	(Null character)
01	SOH	(Start of Header)
02	STX	(Start of Text)
03	ETX	(End of Text)
04	EOT	(End of Trans.)
05	ENQ	(Enquiry)
06	ACK	(Acknowledgement)
07	BEL	(Bell)
08	BS	(Backspace)
09	HT	(Horizontal Tab)
10	LF	(Line feed)
11	VT	(Vertical Tab)
12	FF	(Form feed)
13	CR	(Carriage return)
14	SO	(Shift Out)
15	SI	(Shift In)
16	DLE	(Data link escape)
17	DC1	(Device control 1)
18	DC2	(Device control 2)
19	DC3	(Device control 3)
20	DC4	(Device control 4)
21	NAK	(Negative acknowl.)
22	SYN	(Synchronous idle)
23	ETB	(End of trans. block)
24	CAN	(Cancel)
25	EM	(End of medium)
26	SUB	(Substitute)
27	ESC	(Escape)
28	FS	(File separator)
29	GS	(Group separator)
30	RS	(Record separator)
31	US	(Unit separator)
127	DEL	(Delete)

ASCII printable characters

32	space	64	@	96	`
33	!	65	A	97	a
34	"	66	B	98	b
35	#	67	C	99	c
36	$	68	D	100	d
37	%	69	E	101	e
38	&	70	F	102	f
39	'	71	G	103	g
40	(	72	H	104	h
41	)	73	I	105	i
42	*	74	J	106	j
43	+	75	K	107	k
44	,	76	L	108	l
45	-	77	M	109	m
46	.	78	N	110	n
47	/	79	O	111	o
48	0	80	P	112	p
49	1	81	Q	113	q
50	2	82	R	114	r
51	3	83	S	115	s
52	4	84	T	116	t
53	5	85	U	117	u
54	6	86	V	118	v
55	7	87	W	119	w
56	8	88	X	120	x
57	9	89	Y	121	y
58	:	90	Z	122	z
59	;	91	[	123	{
60	<	92	\	124	|
61	=	93	]	125	}
62	>	94	^	126	~
63	?	95	_		

Extended ASCII characters

128	Ç	160	á	192	└	224	Ó
129	ü	161	í	193	┴	225	ß
130	é	162	ó	194	┬	226	Ô
131	â	163	ú	195	├	227	Ò
132	ä	164	ñ	196	─	228	õ
133	à	165	Ñ	197	┼	229	Õ
134	å	166	ª	198	ã	230	µ
135	ç	167	º	199	Ã	231	þ
136	ê	168	¿	200	╚	232	Þ
137	ë	169	®	201	╔	233	Ú
138	è	170	¬	202	╩	234	Û
139	ï	171	½	203	╦	235	Ù
140	î	172	¼	204	╠	236	ý
141	ì	173	¡	205	═	237	Ý
142	Ä	174	«	206	╬	238	¯
143	Å	175	»	207	¤	239	´
144	É	176	░	208	ð	240	≡
145	æ	177	▒	209	Ð	241	±
146	Æ	178	▓	210	Ê	242	‗
147	ô	179	│	211	Ë	243	¾
148	ö	180	┤	212	È	244	¶
149	ò	181	Á	213	ı	245	§
150	û	182	Â	214	Í	246	÷
151	ù	183	À	215	Î	247	¸
152	ÿ	184	©	216	Ï	248	°
153	Ö	185	╣	217	┘	249	¨
154	Ü	186	║	218	┌	250	·
155	ø	187	╗	219	█	251	¹
156	£	188	╝	220	▄	252	³
157	Ø	189	¢	221	¦	253	²
158	×	190	¥	222	Ì	254	■
159	ƒ	191	┐	223	▀	255	nbsp

www.
theASCIIcode
.com.ar

most consulted

ñ	ényе, n with tilde	(alt + 164)
■	black square	(alt + 254)
2	superscript two, square	(alt + 253)
°	degree symbol	(alt + 248)
'	apostrophe, single quote	(alt + 39)
µ	letter Mu, micro, micron	(alt + 230)
©	copyright symbol	(alt + 184)
®	registered trademark	(alt + 169)
3	superscript three, cube	(alt + 252)
á	a with acute accent	(alt + 160)

frequently-used (spanish language)

ñ	alt + 164
Ñ	alt + 165
@	alt + 64
¿	alt + 168
?	alt + 63
¡	alt + 173
!	alt + 33
:	alt + 58
/	alt + 47
\	alt + 92

vowels acute accent (spanish language)

á	alt + 160
é	alt + 130
í	alt + 161
ó	alt + 162
ú	alt + 163
Á	alt + 181
É	alt + 144
Í	alt + 214
Ó	alt + 224
Ú	alt + 233

vowels with diaresis

ä	alt + 132
ë	alt + 137
ï	alt + 139
ö	alt + 148
ü	alt + 129
Ä	alt + 142
Ë	alt + 211
Ï	alt + 216
Ö	alt + 153
Ü	alt + 154

mathematical symbols

½	alt + 171
¼	alt + 172
¾	alt + 243
¹	alt + 251
³	alt + 252
²	alt + 253
ƒ	alt + 159
±	alt + 241
×	alt + 158
÷	alt + 246

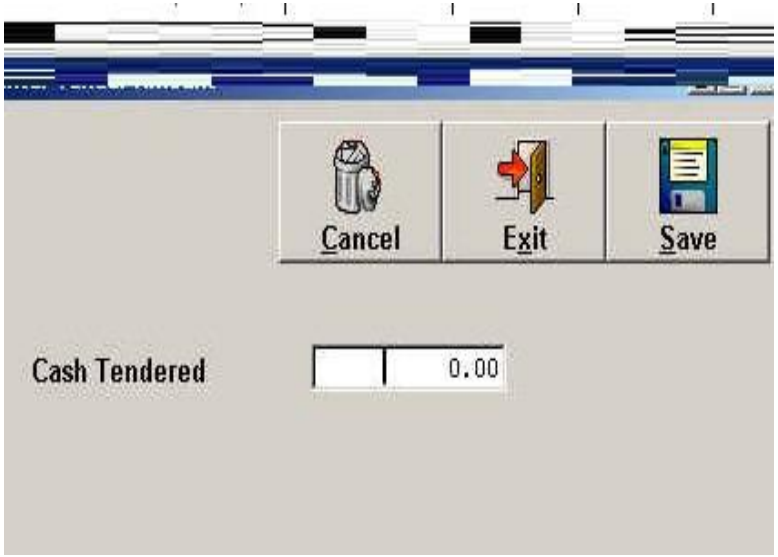
commercial / trade symbols

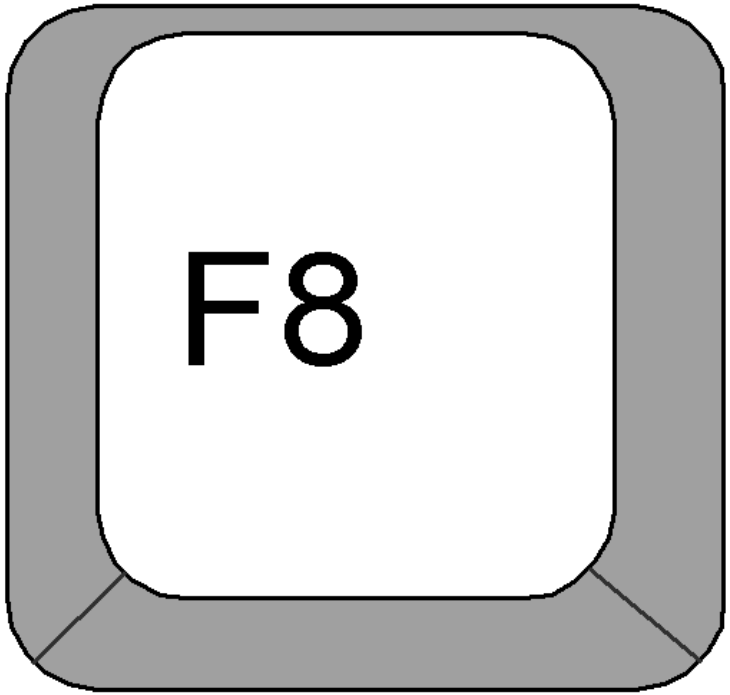
$	alt + 36
£	alt + 156
¥	alt + 190
¢	alt + 189
¤	alt + 207
®	alt + 169
©	alt + 184
ª	alt + 166
º	alt + 167
°	alt + 248

quotes and parenthesis

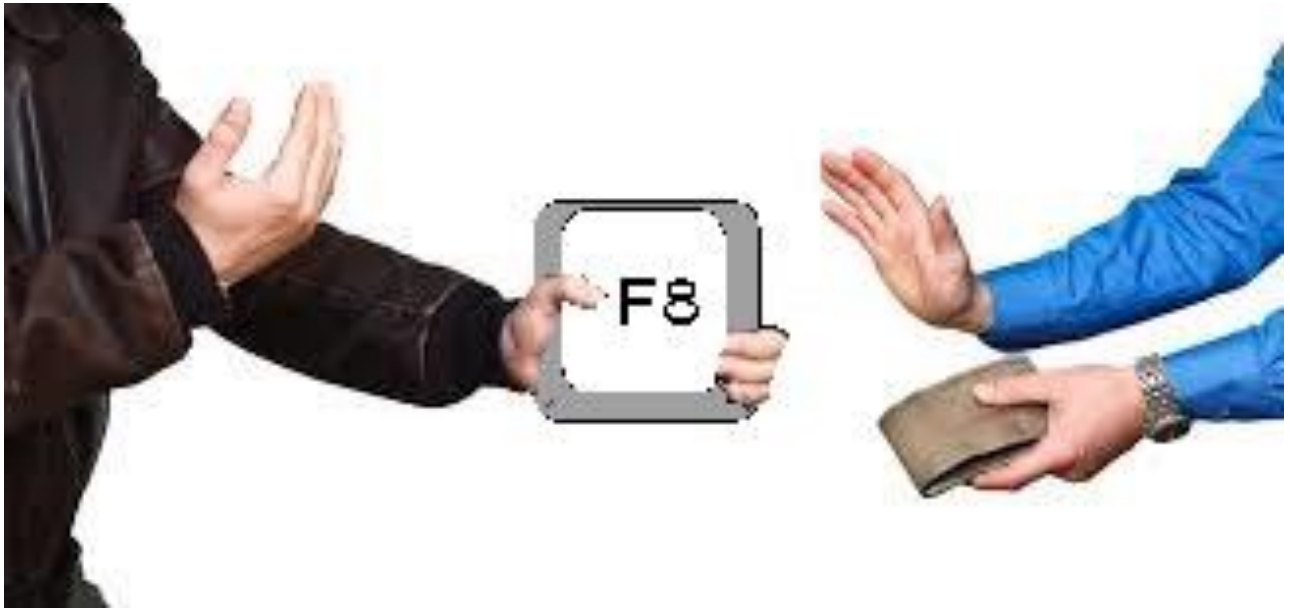
"	alt + 34
'	alt + 39
(	alt + 40
)	alt + 41
[	alt + 91
]	alt + 93
{	alt + 123
}	alt + 125
«	alt + 174
»	alt + 175

Injecting 102-US and proprietary keyboard layouts into binary data.

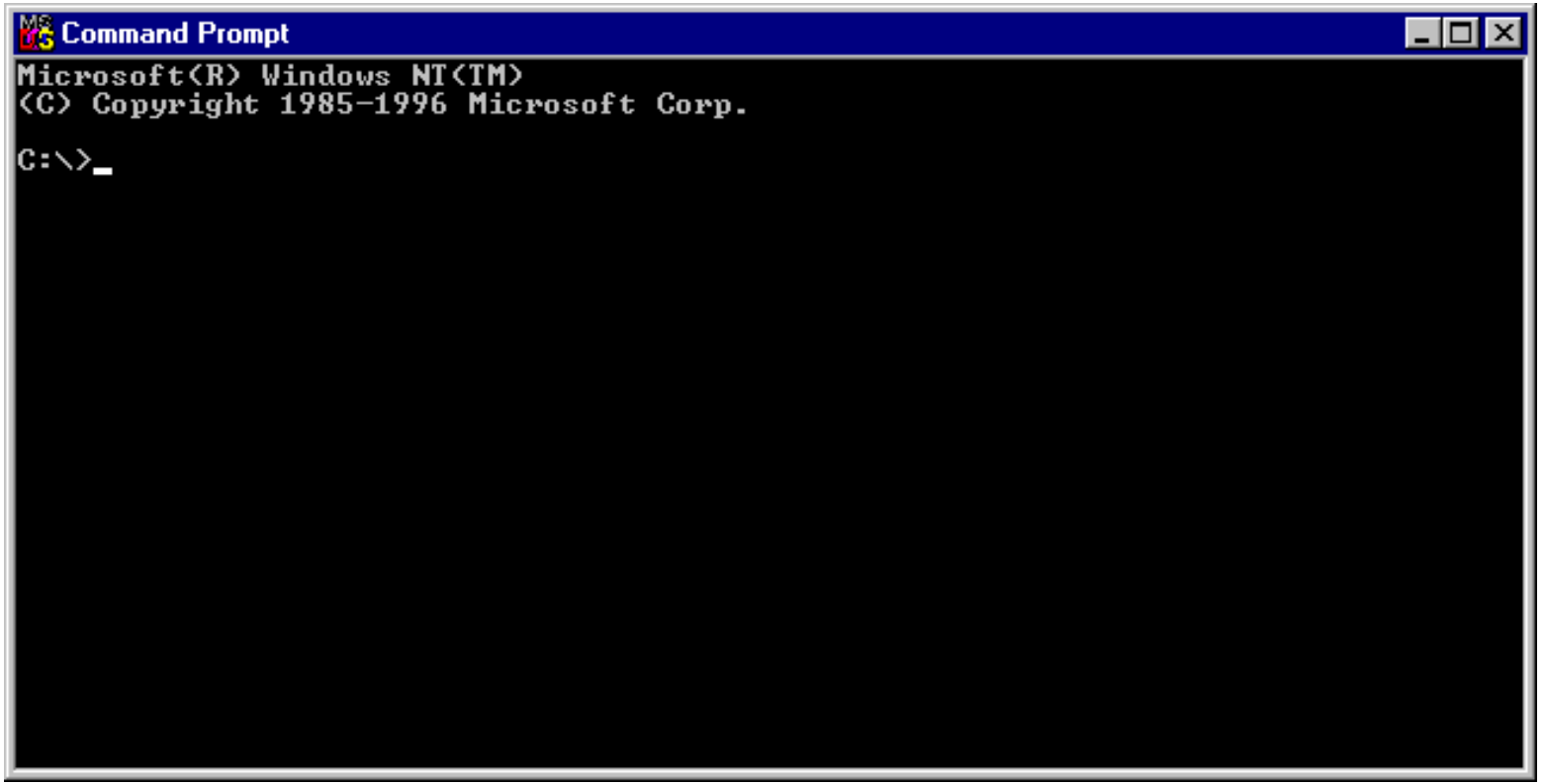




Cash tend/Check tend attack.



Behind every strong man is a strong woman and behind ever POS there is a outdated OS.

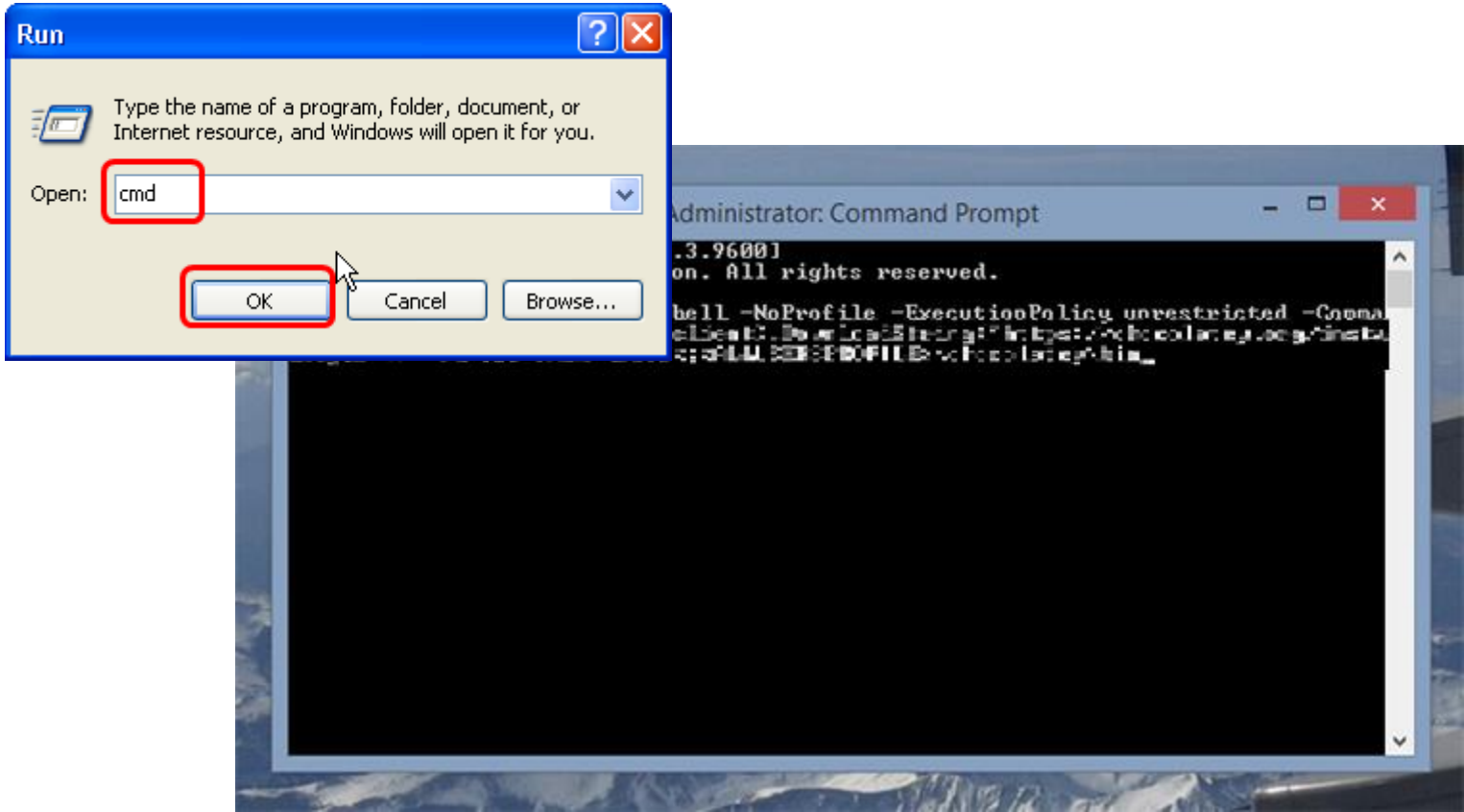


Exiting POS Software.

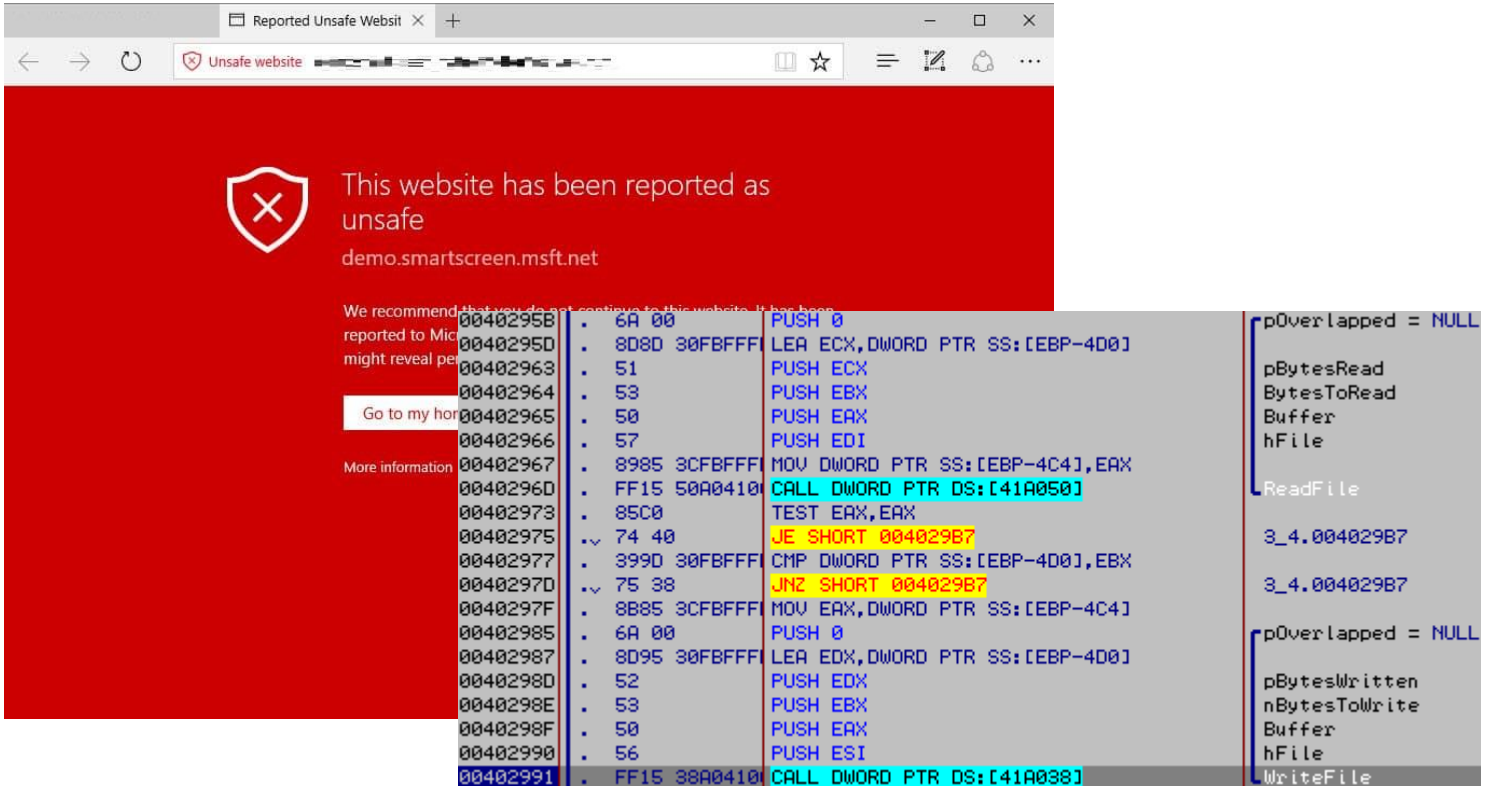




Popping CMD downloading payload.



Payload overview what the bad guys would load.

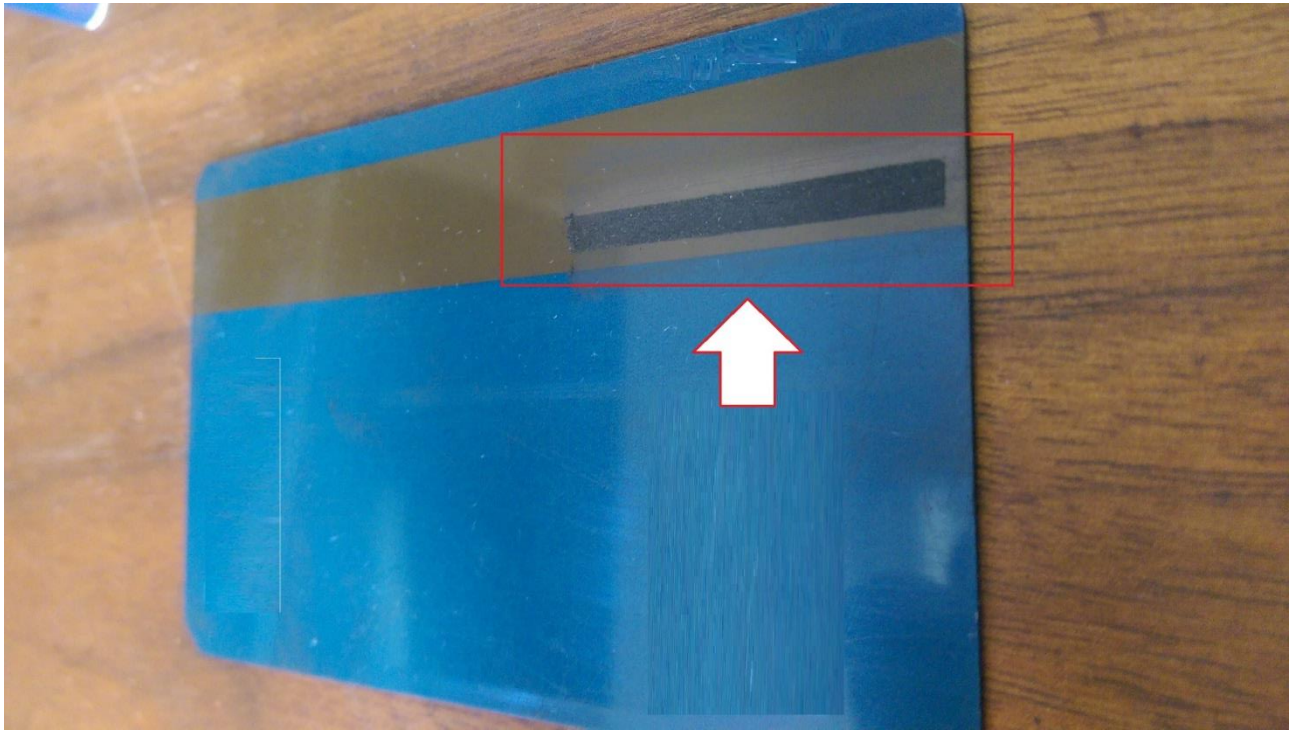


Locked down and custom Dev'ed environments.



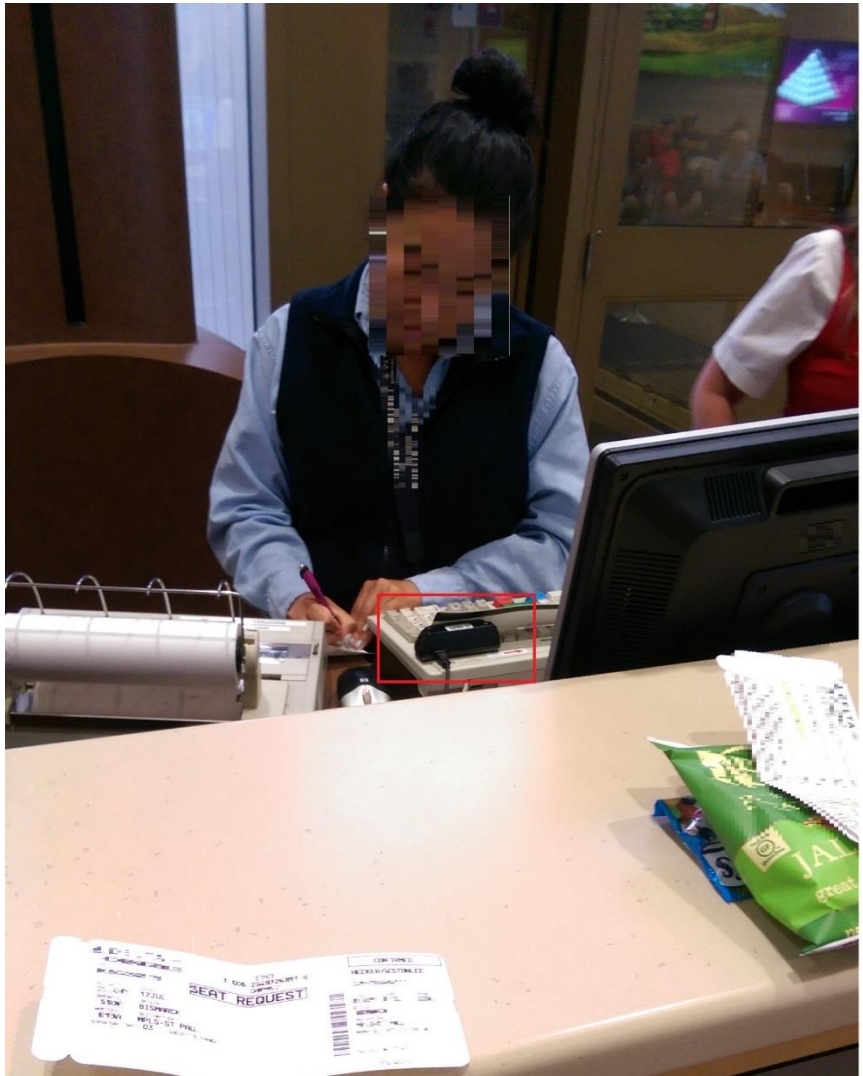


Limitations of mag injection/making a physical car d attack/ limitations of physical can you make a wa iter do your dirty work?





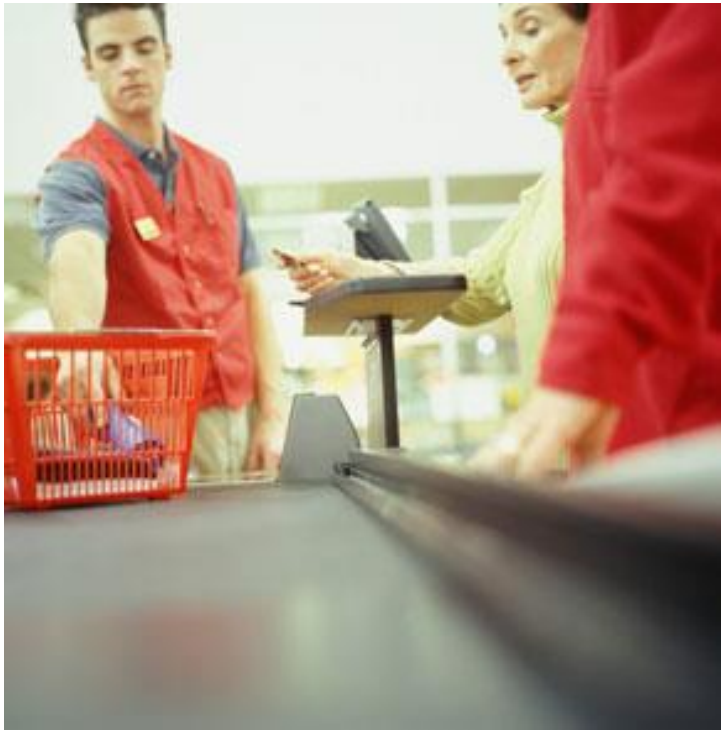
These devices Are everywhere



Injecting player rewards cards into Slot machines people already intentionally leave cards in machin e for this purpose.



Rewards card point collecting rolling 10 different accounts/ Grocery store and gas stations



Injecting into prepaid/phone card acti vation/ activate at terminal swapping systems at POS



Trigger injection attacks "Sniffing USB reader" power up wh en power up is detected it triggers the EM read. Some comp anies ask to confirm account if only you could hit the enter key some how !!



Clock-In systems never be late for work again.





Going over 2 Demos

- Going to inject the Cash Tender

- And next I'm going to Install Credit Card Skimming Software with a Spoofer.

RAPID7

THANKS FOR COMING

Stay Legal



Security Consultant
TWITTER, LinkedIN @westonhecker
Rapid7 www.rapid7.com