KASPERSKY[®]



BANKING THREATS IN DEPTH BANKS ARE UNDER ATTACK 2016

Sergey Lozhkin Senior Security Researcher Kaspersky Lab Italia

GREAT: ELITE THREAT RESEARCH



- Global Research and Analysis Team, since 2008
- Threat intelligence, research and innovation leadership
- Focus: APTs, critical infrastructure threats, banking threats, sophisticated targeted attacks

IN 2014...WE PREDICTED AND WE WERE RIGHT

Escalation of ATM and PoS attacks

Attacks against cash machines (ATM) seemed to explode this year with several public incidents and a rush t law enforcement authorities globally to respond to this crisis. A corollary of this publicity is an awareness tha ATMs are ripe for the taking and cybercriminals are sure to notice. As most of these systems are running Windows XP and also suffer from frail physical security, they are incredibly vulnerable by default and, as the impersonal gatekeepers of the financial institutions' cash, cybercriminals are bound to come knocking here first.



The next stage will see attackers compromising the networks of banks to manipulate #ATM " chines in real time

The Great Bank Robbery: the Carbanak APT

By GReAT on February 16, 2015. 4:20 pm

In the revolution of these ATM attacks with the use of APT techniques to gain In machines. The next stage will see attackers compromising the networks of f access to manipulate ATM machines in real time.



THEY STARTED OPERATIONS WORLDWIDE





CASES 2015-2016

- CARBANAK 2.0
- METEL (RUSSIAN BANKS)
- GCMAN (MOSTLY RUSSIAN BANKS)
- CARBANAK 2.0 (WORLDWIDE)
- UNKNOWN (BANGLADESH)



SPEARFISHING – STILL NUMBER 1



LEGITIMATE TOOLS

- PUTTY (WHITELISTED)
- VNC
- METERPRETER(IN POWERSHELL)
- AMMY
- MIMIKATZ (IN POWERSHELL)



MONEY EXFILTRATION

- ONLINE BANKING
- E-PAYMENT SYSTEMS
- INFLATING ACCOUNT BALANCES
- DATABASE MANIPULATION
- CONTROLLING ATM'S

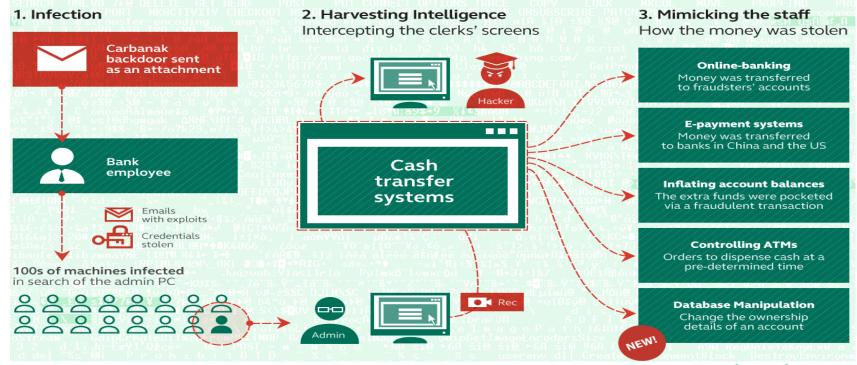


CARBANAK 2.0

- Attacks in budget deps
- Change registration data of shareholders' in depository



How the Carbanak cybergang targets financial organizations



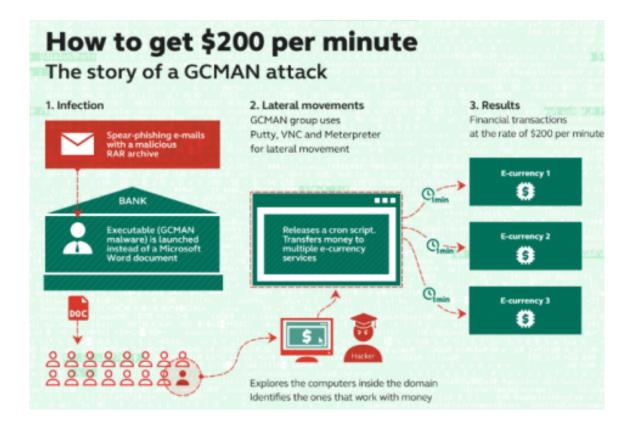


METEL – TRANSACTIONS ROLLBACK





GCMAN – 200\$ PER MINUTE AUTOSCRIPT



200 USD PER MINUTE

root@payments ~ # root@payments ~ # crontab -l # crontab for root * * * * * /bin/snitch_some_money

root@payments ~ #



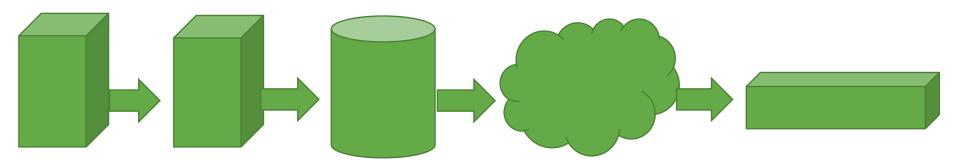


- 70 internal hosts
- 56 accounts
- 139 attack sources:

TOR and home routers



GCMAN ATTACK

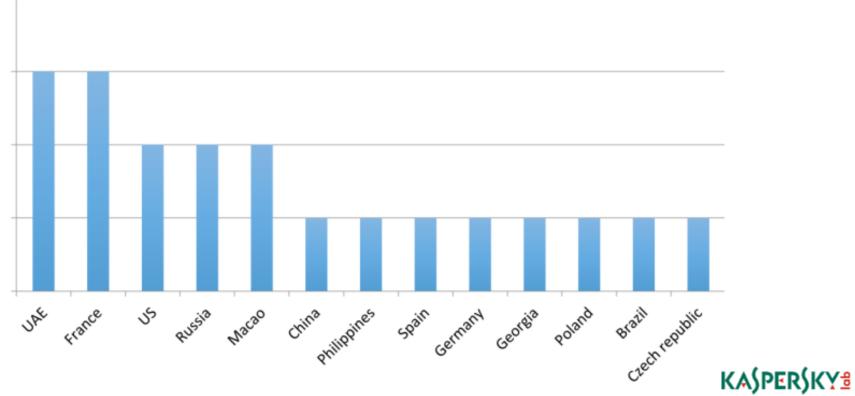


Ads Web	Corporate	Online banking	Admin's Workstations	
Server	banking	DB	VVOIKStations	
	webserver			

Processing Connection Server

KASPERSKY

ATM INFECTOR



ATM INFECTOR – XFS SERVICE PATCH

.00402036:	6A28	push	028;'('
.00402038:	68A0384000	push	0004038A01
.0040203D:	E8FA010000	call	.00040223C 2
.00402042:	33FF	xor	edi,edi
.00402044:	57	push	edi
.00402045:	FF1588304000	call	GetModuleHandleA
.0040204B:	6681384D5A	cmp	w,[eax],05A4D ;'ZM'
.00402050:	751F	jnz	.000402071 3
.00402052:	8B483C	MOV	ecx,[eax][03C]
.00402055:	03C8	add	ecx,eax
.00402057:	813950450000	cmp	d,[ecx],000004550 ;' EP'
.0040205D:	7512	jnz	.000402071 3
.0040205F:	0FB74118	MOVZX	eax,w,[ecx][018]
.00402063:	3D0B010000	cmp	eax,00000010B
.00402068:		jz	.000402089 4
.0040206A:	3D0B020000	cmp	eax,00000020B
.0040206F:	7405	jz	.000402076 5
.00402071:	897DE4	3mov	[ebp][-01C],edi
.00402074:	EB27	jmps	.00040209D 6
.00402076:	83B9840000000E	Scmp	d,[ecx][00000084],00E



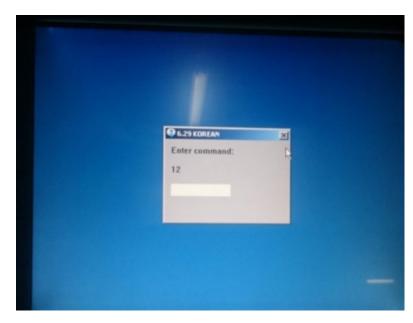
ATM INFECTOR – SPISERVICE PATCHED

.004023E0: 55	push	ebp
.004023F1: 8BEC	MOV	ebp, esp
.004023F3: 83C400	add	esp,0
.004023F6: 5D	рор	ebp
.004023F7: 6836204000	push	000402036
.004023FC: 680C244000	push	00040240C ;'C:\Program Files\Diebold\AgilisXFS\bin\SpiService.exe:netmgr.dll'
.00402401: B8771D807C	MOV	eax,07C801D77 ;' C w'
.00402406: FFD0	call	eax
.00402408: C3	retn ; -^-^-	
.00402409: 8D4000	lea	eax,[eax][0]
	2inc	ebx
.0040240D: 3A5C5072	cmp	bl.[eax][edx]*2[072]
.0040240D: 58363072	outsd	DI,[Edx][Edx]*2[0/2]
.00402412: 677261		.00040247613
.00402412: 677261	jo	.000402476
	insd	
.00402416: 204669	and	[esi][069],al
.00402419: 6C	insb	
.0040241A: 65735C	jnc	.000402479
.0040241D: 44	inc	esp
.0040241E: 6965626F6C645C	imul	esp,[ebp][062],05C646C6F;'\dlo'
.00402425: 41	inc	ecx
.00402426: 67696C6973584653	imul	ebp,[si][069],053465873 ;'SFXs'



ATM INFECTOR – MAGIC CARD

CARD 1 – INTERFACE COMMANDS CARD 2 – TRACK 2 HARDCODED





THANK YOU!

Sergey Lozhkin Senior Security Researcher Kaspersky Lab

