Vad händer med dina kortuppgifter?

2014-03-13 Jonas Elmqvist

Trender, intrång och forensiska utredningar

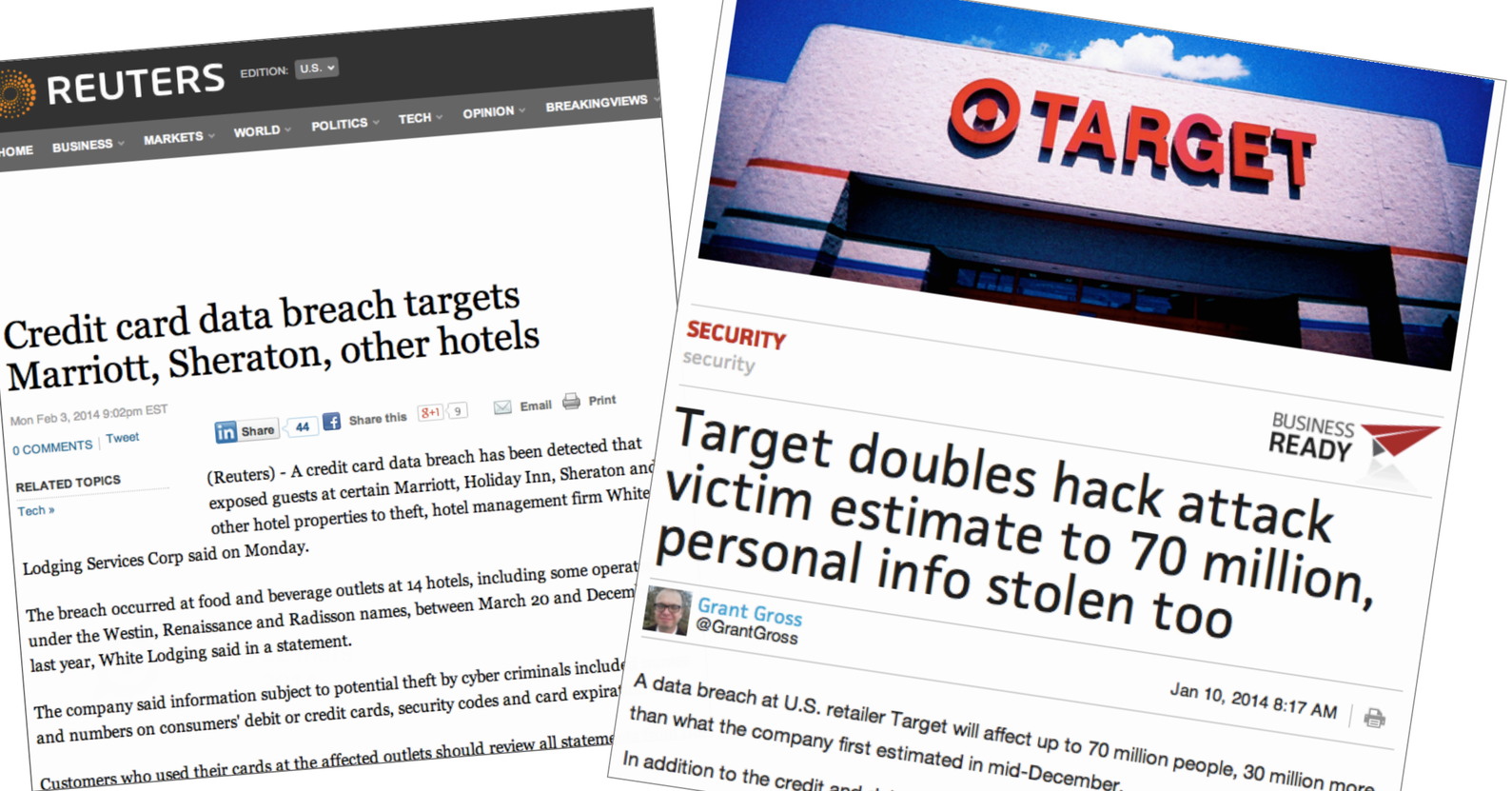
knowit

”Payment card data remains one of the easiest types of data to convert to cash, and therefore the preferred choice of criminals.”

KONTOKORTSBEDRÄGERI

37% AV ALLA AMERIKANER HAR UTSATTS

10% AV ALLA SVENSKAR HAR UTSATTS



REUTERS EDITION: U.S.

HOME BUSINESS MARKETS WORLD POLITICS TECH OPINION BREAKINGVIEWS

Credit card data breach targets Marriott, Sheraton, other hotels

Mon Feb 3, 2014 9:02pm EST

0 COMMENTS | Tweet

Share 44 Share this 9 Email Print

RELATED TOPICS

Tech »

(Reuters) - A credit card data breach has been detected that exposed guests at certain Marriott, Holiday Inn, Sheraton and other hotel properties to theft, hotel management firm White Lodging Services Corp said on Monday.

The breach occurred at food and beverage outlets at 14 hotels, including some operat under the Westin, Renaissance and Radisson names, between March 20 and Decem last year, White Lodging said in a statement.

The company said information subject to potential theft by cyber criminals includ and numbers on consumers' debit or credit cards, security codes and card expira

Customers who used their cards at the affected outlets should review all statem

TARGET

SECURITY

security

BUSINESS READY

Target doubles hack attack victim estimate to 70 million, personal info stolen too

Grant Gross
@GrantGross

Jan 10, 2014 8:17 AM

A data breach at U.S. retailer Target will affect up to 70 million people, 30 million more than what the company first estimated in mid-December.

In addition to the credit and

”Through 2016, the financial impact of cybercrime will grow 10% per year, due to the continuing discovery of new vulnerabilities.”

Gartner®

Hur ser trenden ut?

ALLA BRANSCHER

70% AV ALLA INTRÅNG UPPTÄCKS AV TREDJE PART

66% AV ALLA INTRÅNG TAR **MÅNADER** ATT UPPTÄCKA

ÖKNING AV AVANCERADE **RIKTADE** ATTACKER

SVART MARKNAD
”Hacking as a Service”

KREDITKORTSBRANSCHEN

1% AV ALLA INTRÅNG UPPTÄCKS AV ’HANDLARNA’

2013 VISA VARNAR FÖR ÖKNING AV ATTACKER MOT BETALTERMINALER

KÖP OCH SÄLJ AV KORTNUMMER

Svart marknad

”the service also offers consultation for hacking into any given Web site, with the prices varying between $1000 to $50,000”

ZERO-DAY SÅRBARHETER

ADOBE READER	$5,000–$30,000
MAC OSX	$20,000–$50,000
ANDROID	$30,000–$60,000
FLASH OR JAVA BROWSER PLUG-INS	$40,000–$100,000
MICROSOFT WORD	$50,000–$100,000
WINDOWS	$60,000–$120,000
FIREFOX OR SAFARI	$60,000–$150,000
CHROME OR INTERNET EXPLORER	$80,000–$200,000
IOS	$100,000–$250,000

STULNA KORTNUMMER

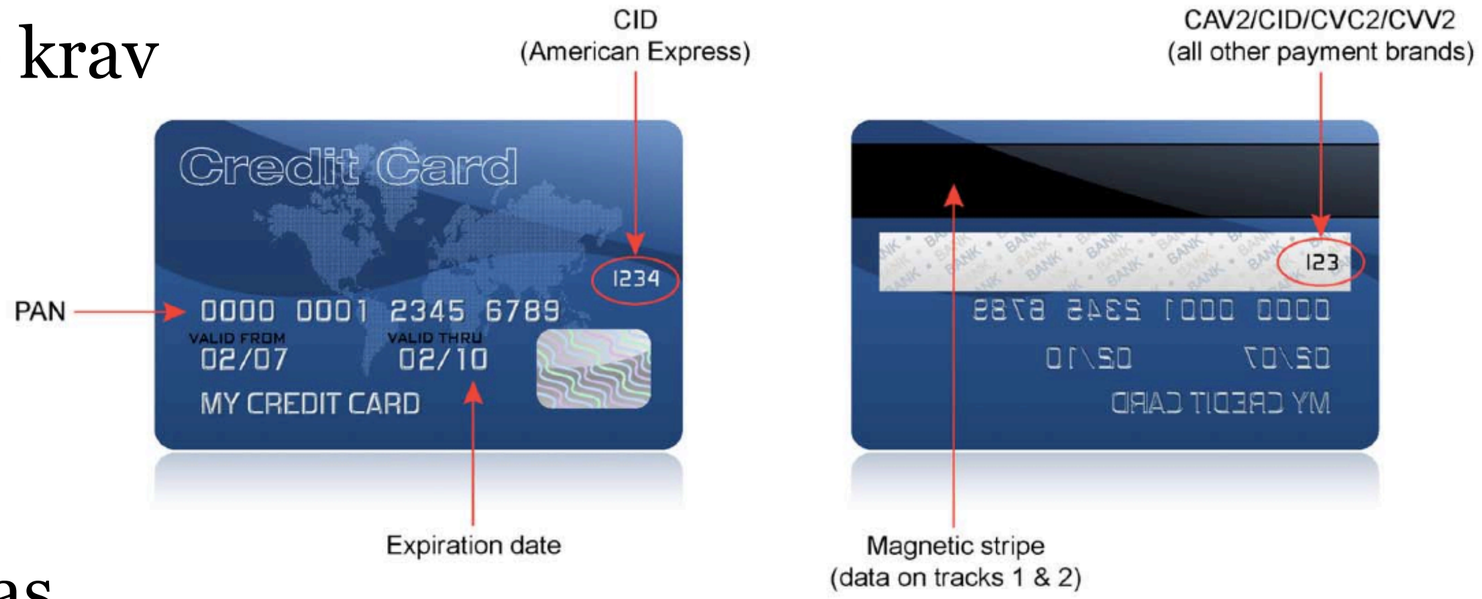
	US			EU		
Visa Classic	$15	$80		$40	$150	
Master Card Standard		$90			$140	
Visa Gold/Premier	$25	$100	$200	$45	$160	$250
Visa Platinum	$30	$110		$50	$170	
Business/Corporate	$40	$130		$60	$170	
Purchasing/Signature	$50	$120		$70		
Infinite				$130	$190	
Master Card World		$140				
AMEX	$40			$60		
AMEX Gold	$70			$90		
AMEX Platinum	$50					

Hur fungerar kreditkortsbranchen?

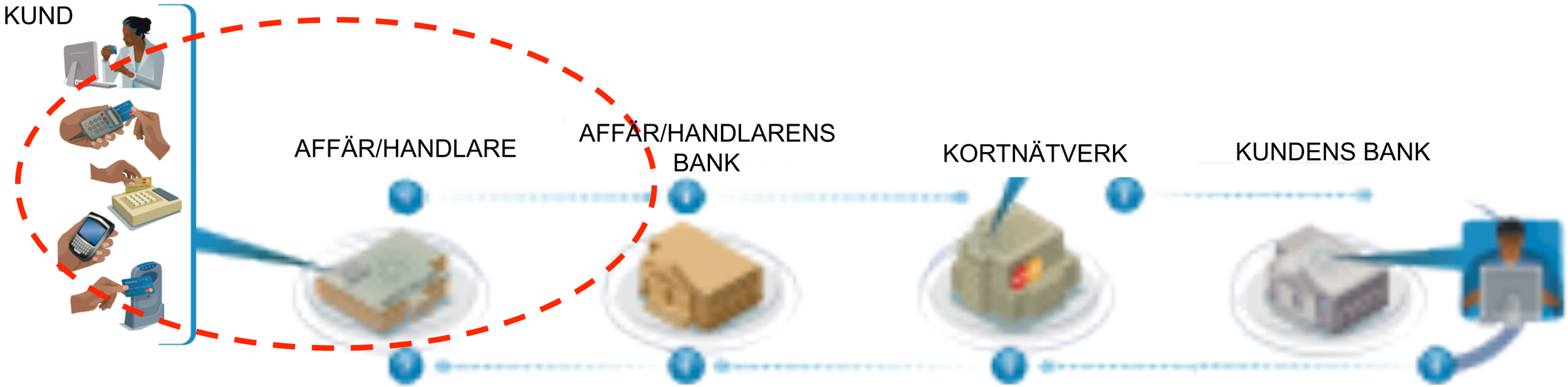
- Payment Card Industry (PCI)
- Regleras av PCI Data Security Standard
- 12 kravområden, ca 280 krav

Exempel

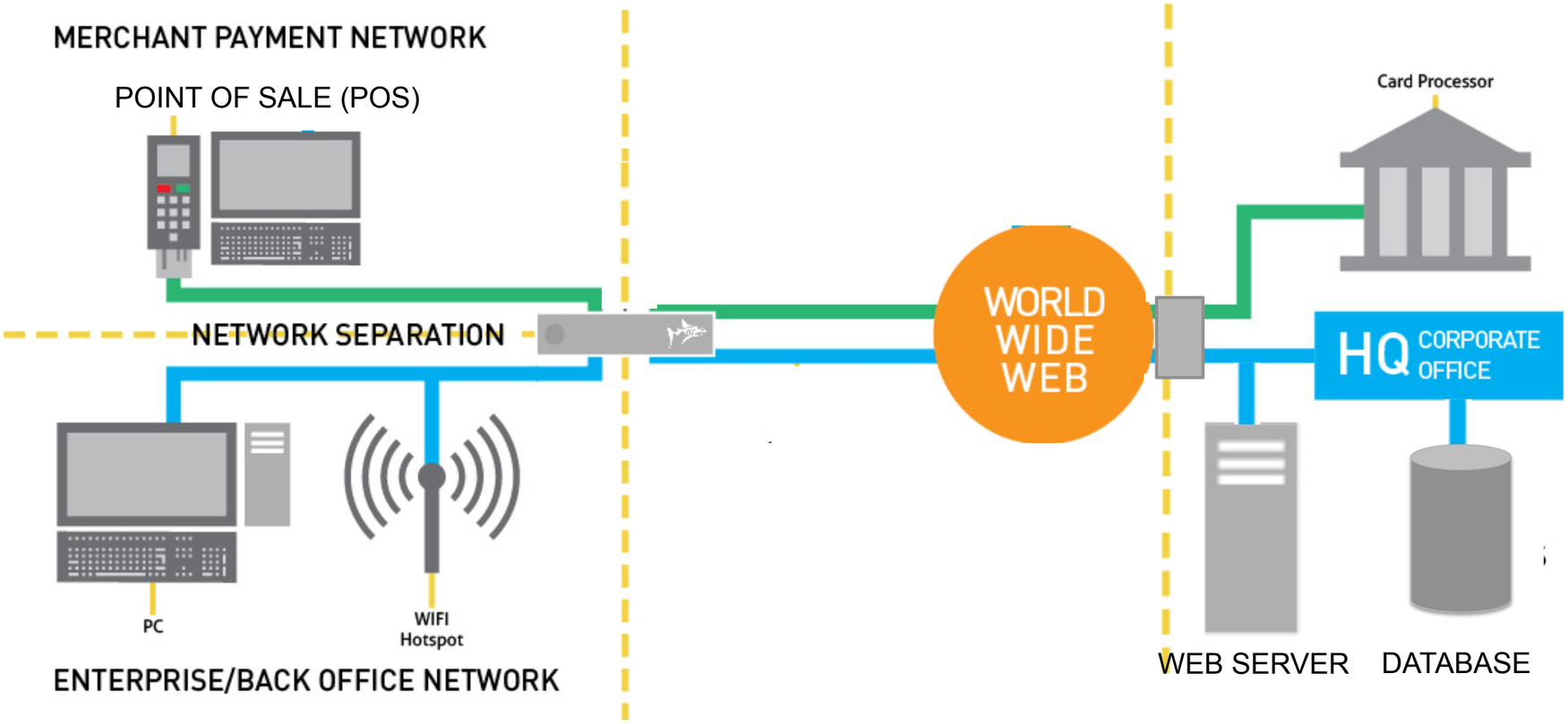
- Ansvar och roller
- Rutiner
- Hur miljön ska se ut
- Hur kortdata får hanteras



Hur sker en betalning?



Card Data Environment (CDE)



VANLIGA ATTACKVEKTORER

- WIFI
- Malware
- Fjärråtkomst (leverantör)
- Dåliga lösenord
- Osäkera webbapplikationer
- Lagring av kortdata i klartext
- POS
- Ej uppdaterade system

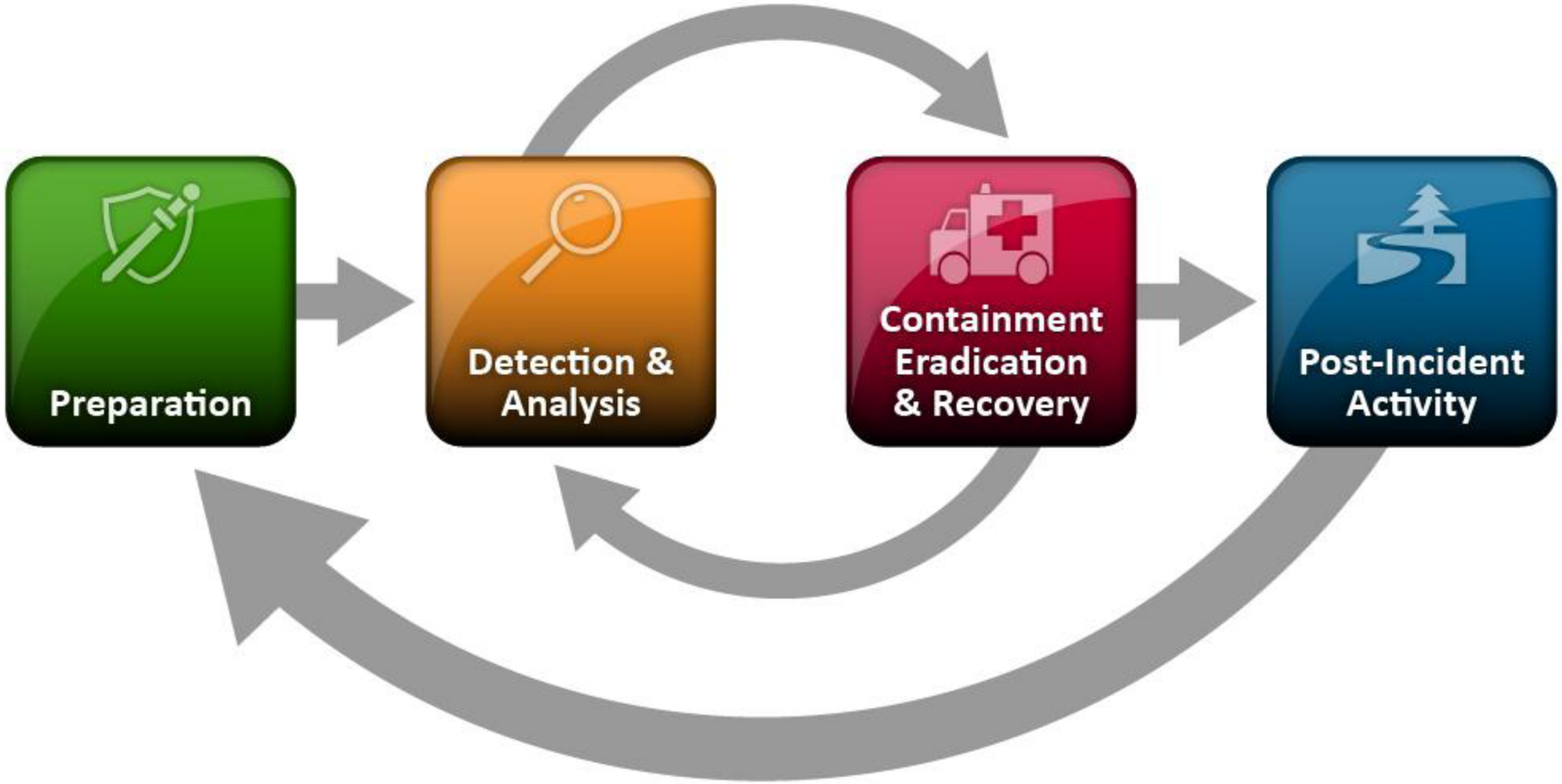
När och hur görs utredningar?

Common Point of Purchase

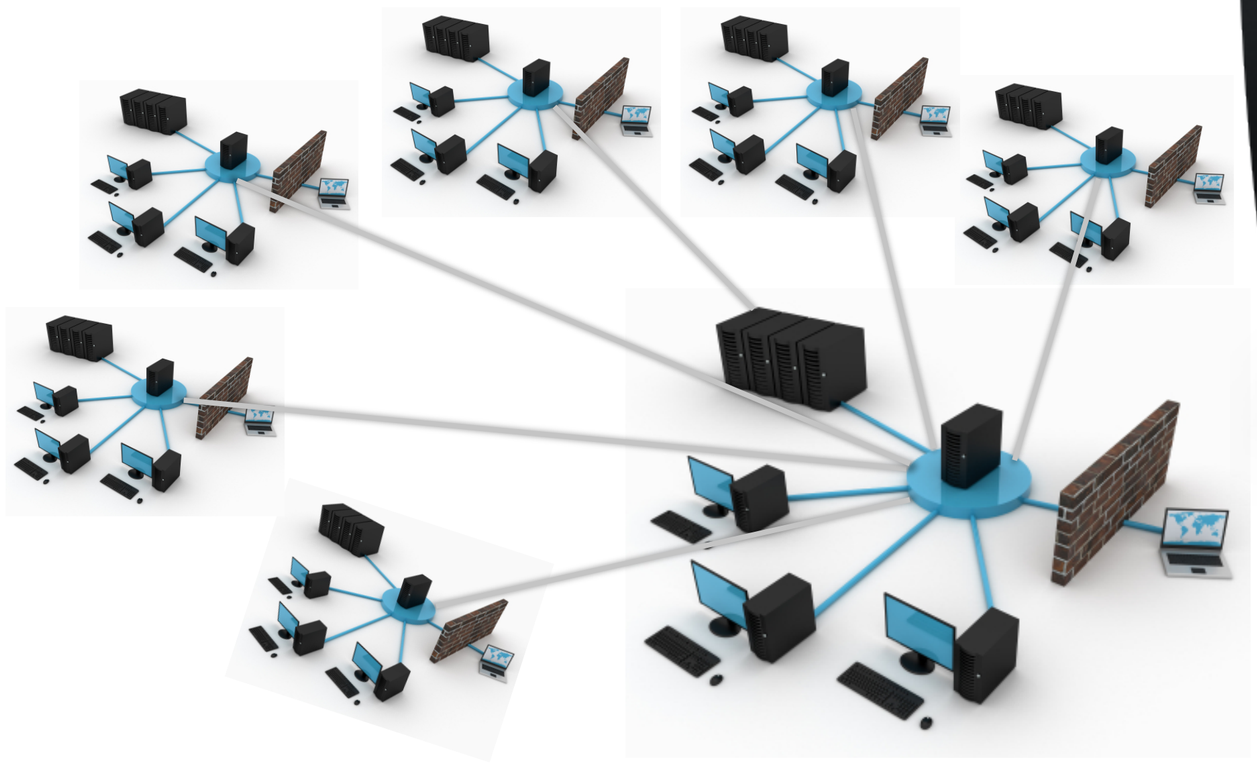
Misstänkt stulna kort

Köpställen

IT-forensik - metodik

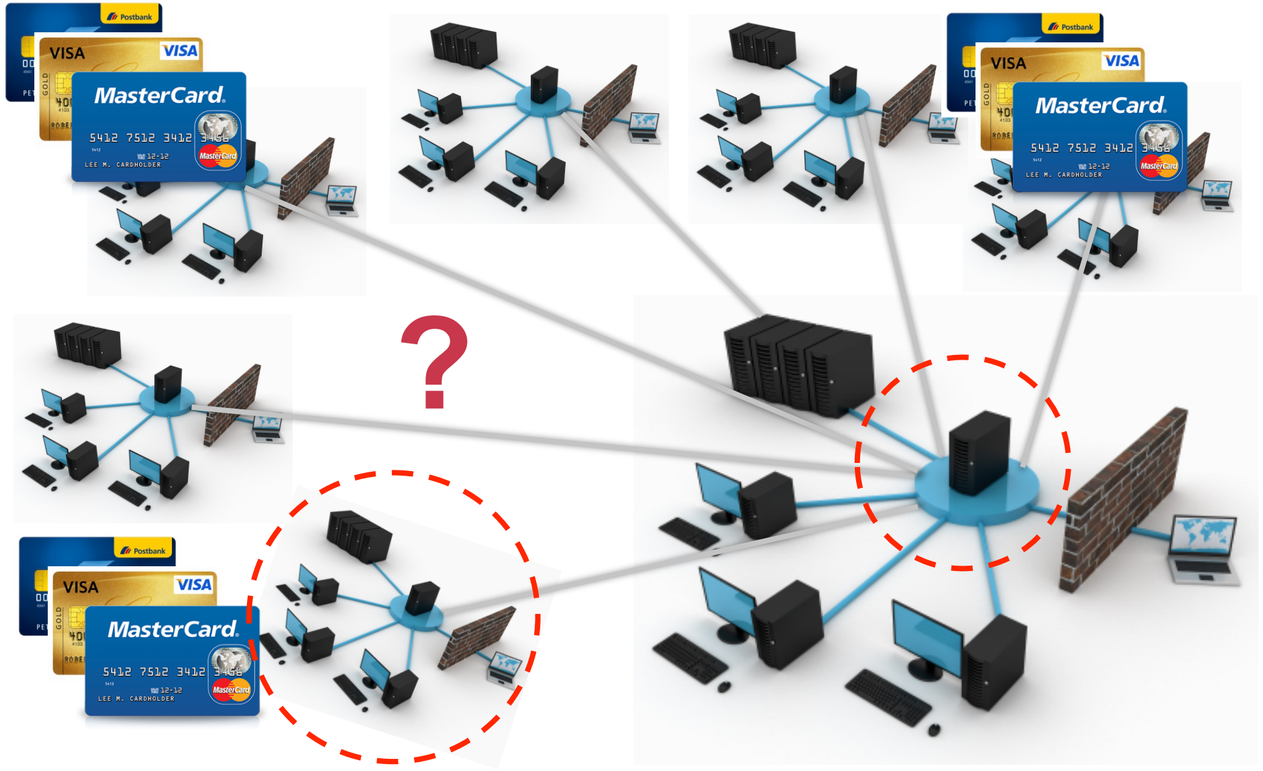


Kund_X




FORENSIC INVESTIGATION
CLASSIFIED
CASE: CREDIT CARD FRAUD
VICTIM: KUND_X
#STORES: +50
COUNTRY: SOUTHERN EUROPE
START: 20xx-12-24 12:21:37+01.00

Steg 1: Incident response



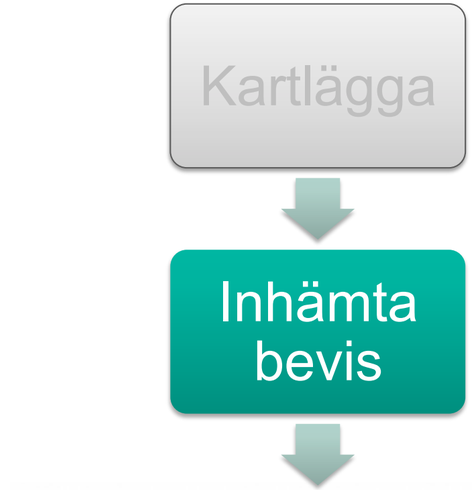
Kartlägga

Inhämta bevis

Analysera data

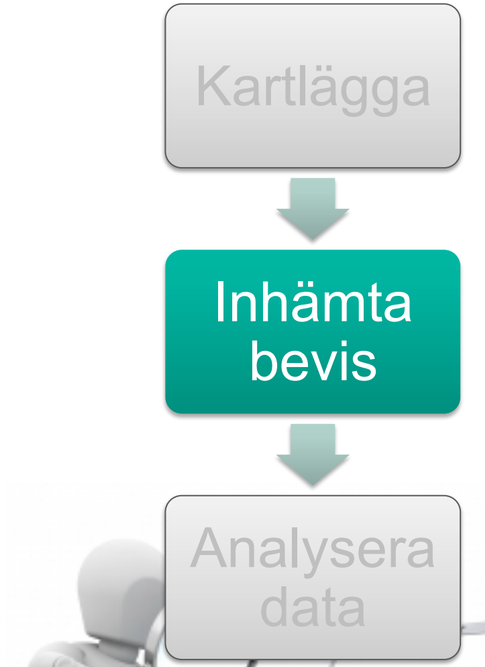
Steg 2: Samla in bevismaterial

- ”First Responders Toolkit”
  - Verktyg för inhämtning
  - Syfte: inhämta bevis med minimal påverkan
- Nätverkskomponenter, servrar, klienter, POS
- Insamling av minne, cache, register
  - Systeminformation, upptid
  - Tid
  - Kommandohistorik
  - Processer som körs
  - Inloggade användare
  - DLL:er
  - Nätverksanslutningar



Steg 2: Samla in bevismaterial

- Kopiera hårdiskar, bit-by-bit
- Chain of custody
  - Dokumentation
  - Märkning
  - Säker hantering

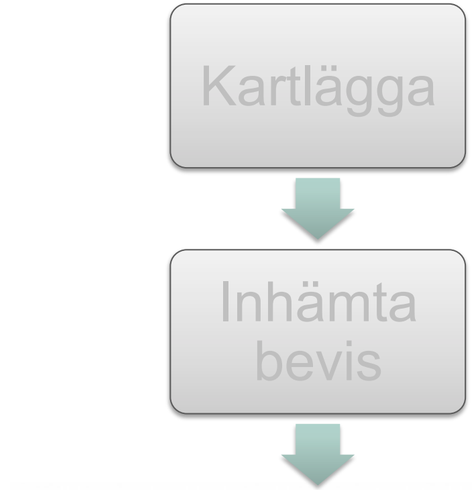


Steg 3: Analysera data

- Samla på sig indikatorer
  - Kända malware (md5)
  - IP-nummer
  - Kreditkortsnummer
  - Viktiga datum

Analys av minne

- Analysera processer och trådar
- Analysera DLLs
- Analysera nätverksanslutningar

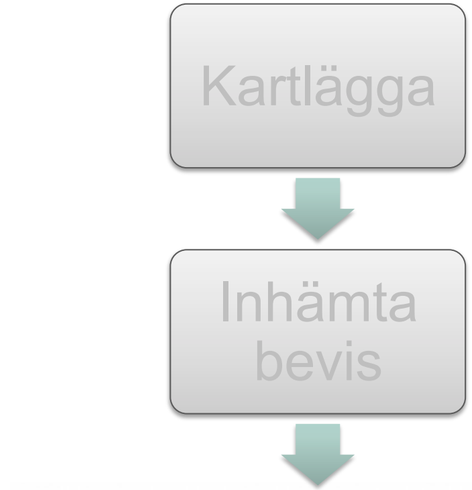


Steg 3: Analysera data

- Extrahera filer (.exe och .dll) - md5 lookup
- Kör antivirus-scan på image

Timeline Analysis

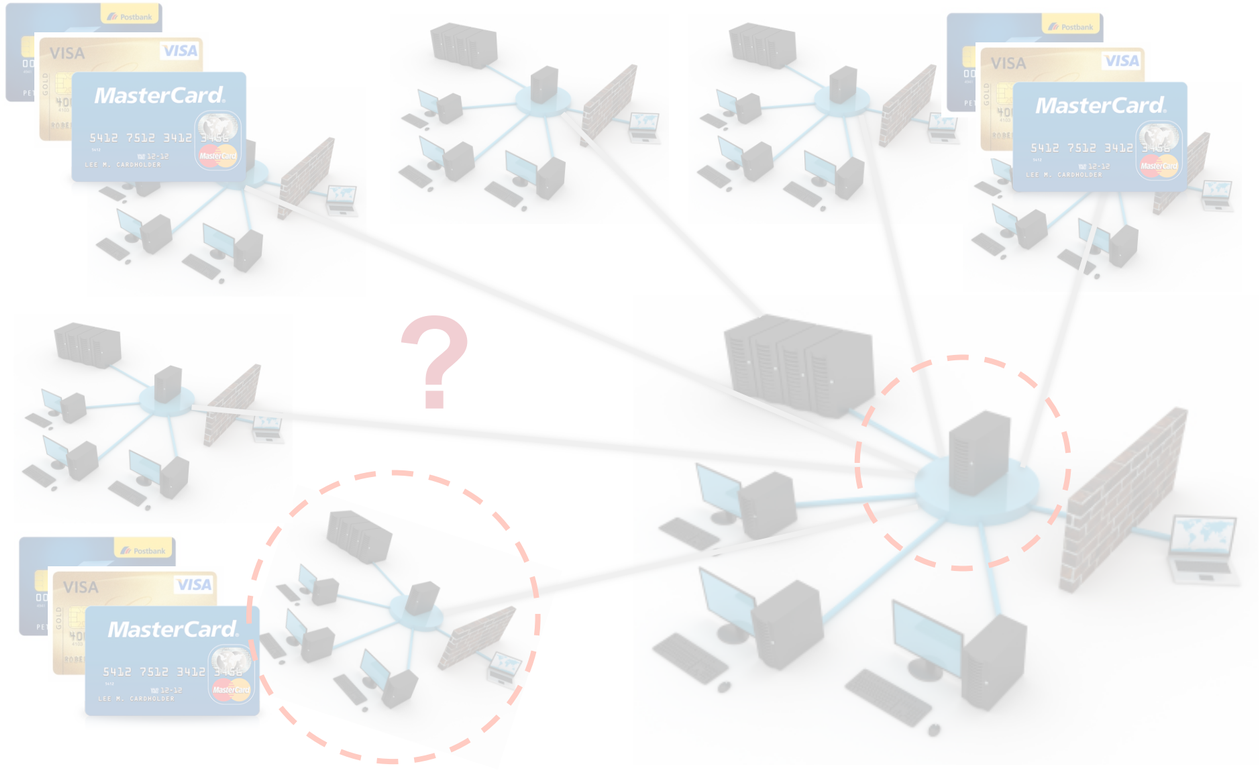
- Filsystem, processer
- Loggar
- Installerade program
- **Alla händelser läggs i tidsordning**



Timeline analysis (exempel)

39649	0.06115	MACB	Email PST	Email Read	Message 114: Attachment m57biz.xls Opened
7/20/2008	1:27:40	MACB	XP Prefetch	Last run	EXCEL.EXE-1C75F8D6.pf: EXCEL.EXE was executed
7/20/2008	1:27:40	.AC.	NTFS $MFT	$SI [.AC.] time	C:/Program Files/Microsoft Office/Office/EXCEL.EXE
7/20/2008	1:27:40	.AC.	UserAssist key	Time of Launch	UEME_RUNPATH:C:/PROGRA~1/MICROS~2/Office/EXCEL.EXE
7/20/2008	1:28:03	..CB	Shortcut LNK	Created	C:/Documents and Settings/Jean/Desktop/m57biz.xls
7/20/2008	1:28:043	MACB	NTFS $MFT	$SI [MACB] time	C:/Documents and Settings/Jean/Application Data/Microsoft/Office/Recent/Desktop.LNK
7/20/2008	1:28:03	MACB	FileExts key	Extension Change	File extension .xls opened by EXCEL.EXE
7/20/2008	1:28:03	MACB	NTFS $MFT	$SI [MACB] time	C:/windows/system32/winsvchost.exe
7/20/2008	1:28:03		SOFTWARE key	Last Written	SOFTWARE\Microsoft\Windows\CurrentVersion\Run
7/20/2008	1:27:40		Memory Process	Process Started	winsvchost.exe|1556|1032||0x02476768
7/20/2008	1:27:40		Memory Socket	Socket Opened	4|134.182.111.82:443|Protocol: 6 (TCP)|0x8162de98|||
7/20/2008	1:27:40		XP Prefetch	Last run	WINSVCHOST.EXE-1C75F8D6.pf: EXCEL.EXE was executed
7/20/2008	1:28:03	..CB	Shortcut LNK	Created	C:/Documents and Settings/Jean/Desktop/m57biz.xls
7/20/2008	1:28:03	.A..	Shortcut LNK	Access	C:/Documents and Settings/Jean/Desktop/m57biz.xls
7/20/2008	1:28:04	MAC.	NTFS $MFT	$SI [MAC.] time	C:/Documents and Settings/Jean/Application Data/Microsoft/Office/Recent/m57biz.LNK
7/20/2008	1:28:04	..C.	NTFS $MFT	$SI [..C.] time	C:/Documents and Settings/Jean/Local Settings/History/History.IE5/MSHist01200807202008
7/20/2008	1:28:04	..C.	NTFS $MFT	$SI [..C.] time	C:/Documents and Settings/Jean/Local Settings/History/History.IE5/MSHist01200807202008

Resultat

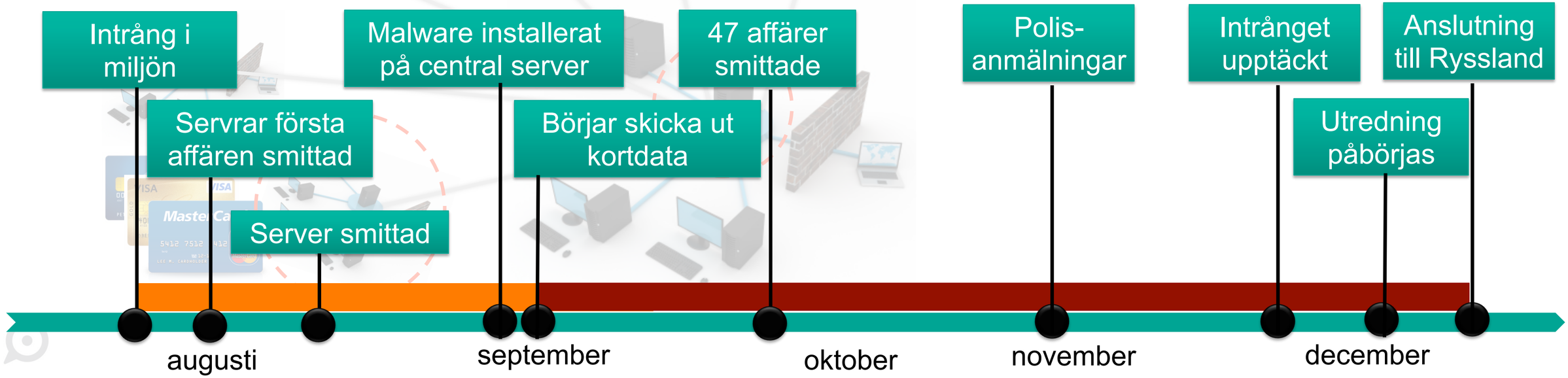


Resultat

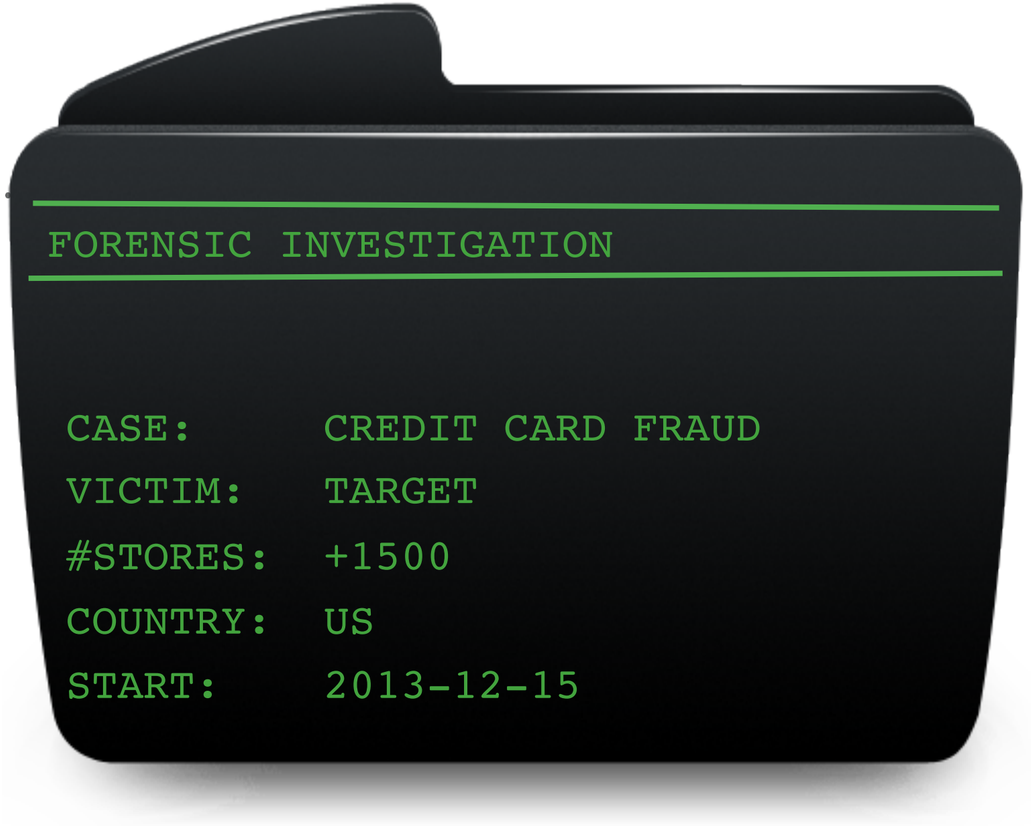
- Analys brandväggsloggar
- Analys av centrala servrar
  - Stora mängder kortdata ’gömd’
  - Ansluter till flera interna servrar
  - Laddar ned och gömmer kortdata
  - Ansluter till Command&Control
- Analys server i affär
  - Sniffer som fångar kortdata
  - Skriver på fil
  - Lyssnar på portar
- Analys av fler servrar
- Analys av datorer i affäre
  - MS08-67
  - Backdoor installerad 1 aug

Typer av malware

- Portscanners
- Backdörrar
- Återskapa raderade filer
- WinRAR
- Proxys
- Remote access
- FTP-verktyg
- Command&Control

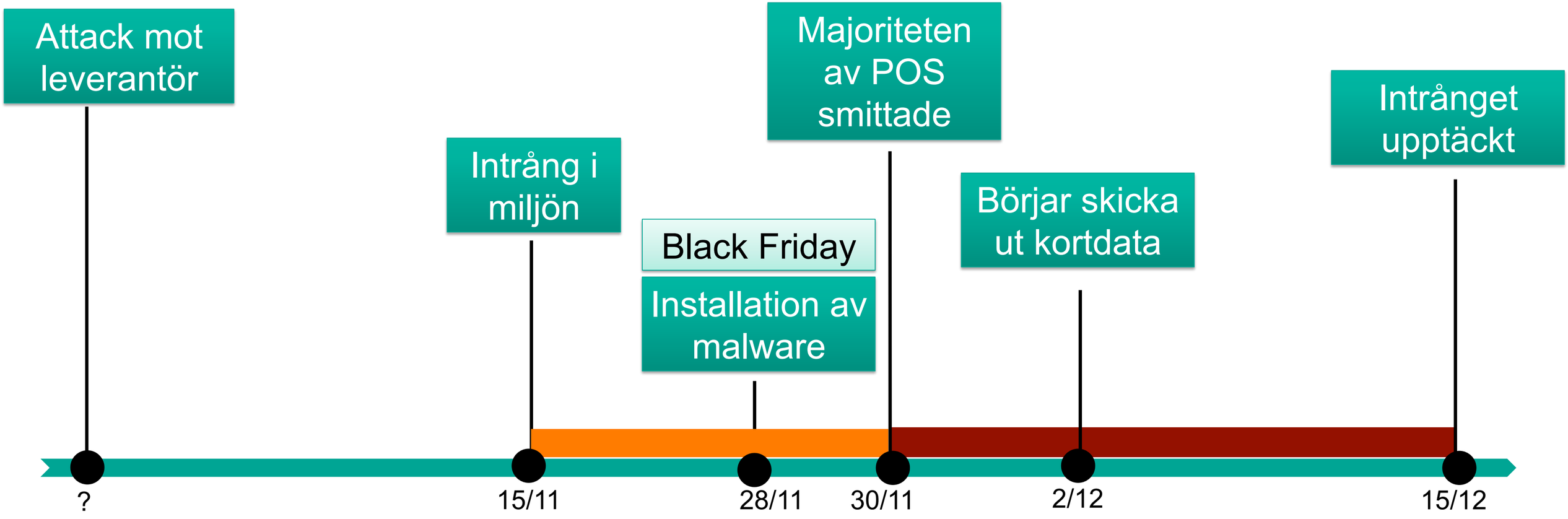


Target



22 ma
2014

Target - händelserförlopp



Malware - ’Black POS’

- Fanns att köpa för för $1800 från mars 2013
- Memory scraper
- Smittar Windowsbaserade POS
- Styrdes av Command&Control server i miljön
- C&C skickade kontinuerligt ut kortdata till olika platser via FTP

Memory Scraper

- Sorterar bort kända processer
- Väljer ut rätt processer
- Söker efter kortnummer
- Skriver till fil
- Specifika för varje system – svåra att hitta mha signaturbaserade AV

Command & Control (exempel)

Action	UID	Version	Remote IP	Username	Computername	User Agent	OS	Architecture	Idle Time	Last Visit	Last Command	Process List
1 - Delete	e4	vTREI	*3.60.70	Administrator	T /R	Mozilla/4.0 (compatible; MSIE 6.0;	Windows XP	32 Bit	13	2 weeks 5 days	1 month, 1 week	Procs None
2 - Delete	dc	vTREI	*.232.71			Mozilla/4.0(compatible; MSIE 7.0b;			168209	1 month	1 month, 1 week	Procs None
3 - Delete	bf	vTREI	*7.218.187	Administrator	06 53-01	Mozilla/4.0(compatible; MSIE 7.0b;	Windows Server 2003	32 Bit	299255	3 weeks	3 weeks 3 days	Procs None
4 - Delete	42	vTREI	*.82.129	terminal	S ER2K3	Mozilla/4.0(compatible; MSIE 7.0b;	Windows Home Server	32 Bit	1394524	1 week 4 days	1 month 2 weeks	Procs None
5 - Delete	e5	vTREI	*.234.69	Âäìèíèñòðàòîð	T	Mozilla/4.0 (compatible; MSIE 7.0;	Windows Home Server	32 Bit	0	1 week 3 days	1 week 3 days	Procs None
6 - Delete	e1	vTREI	*.234.69	coadmin	T	Mozilla/4.0 (compatible; MSIE 7.0;	Windows Home Server	32 Bit	600	1 week 4 days	3 weeks 3 days	Procs None
7 - Delete	96	vTREI	*.136.20	administrator	K V-INT	Mozilla/4.0(compatible; MSIE 7.0b;	Windows Home Server	32 Bit	0	1 month, 1 week	1 month 2 weeks	Procs None
8 - Delete	d3	vTREI	*.136.20			Mozilla/4.0(compatible; MSIE 7.0b;			0	1 month, 1 week	1 month, 1 week	Procs None
9 - Delete	ea	vTREI	*.136.20	administrator	K ICROS-SRV	Mozilla/4.0(compatible; MSIE 7.0b;	Windows Home Server	32 Bit	0	1 month, 1 week	1 month, 1 week	Procs None
10 - Delete	67	vTREI	*.204.232	Administrator	S GROUP01	Mozilla/4.0(compatible; MSIE 7.0b;	Windows Home Server	32 Bit	0	2 days 11 hours	1 week 2 days	Procs None
11 - Delete	b0	vTREI	*.204.232	sys	S GROUP01	Mozilla/4.0(compatible; MSIE 7.0b;	Windows Home Server	32 Bit	2	4 days 20 hours	1 week 2 days	Procs Logs (2)
12 - Delete	0f	vTREI	*8.30.153	Réception	W FR21824	Mozilla/4.0(compatible; MSIE 7.0b;	Windows XP	32 Bit	0	1 month	1 month, 1 week	Procs None
13 - Delete	a1	vTREI	*2.62.193	administrator	F MILLSRV	Mozilla/4.0(compatible; MSIE 7.0b;	Windows Home Server	32 Bit	0	2 weeks, 1 day	1 month, 1 week	Procs None
14 - Delete	3c	vTREI	*0.174.98	Administrator	H 019778174	Mozilla/4.0(compatible; MSIE 7.0b;	Windows XP	32 Bit	54	1 day 8 hours	1 month, 1 week	Procs Logs (10)
15 - Delete	e2	vTREI	*.10.104	Administrador	7 KO	Mozilla/4.0(compatible; MSIE 7.0b;	Windows XP	32 Bit	6077	34 secs	3 weeks 3 days	Procs None
16 - Delete	2e	vTREI	*6.159.22	microssvc	W V8SRV	Mozilla/4.0 (compatible; MSIE 7.0;	Windows Server 2003	32 Bit	686344	1 month	1 month, 1 week	Procs None
17 - Delete	ed	vTREI	*6.159.22	Administrator	W V8SRV	Mozilla/4.0 (compatible; MSIE 7.0;	Windows Server 2003	32 Bit	368773	19 secs	1 month, 1 week	Procs None
18 - Delete	a9	vTREI	*1.41.134	Owner	P ADNA-320A0E	Mozilla/4.0 (compatible; MSIE 8.0;	Windows XP	32 Bit	0	2 weeks 4 days	1 month, 1 week	Procs None
19 - Delete	d5	vTREI	*0.68.34	ucetni	U N1	Mozilla/4.0 (compatible; MSIE 8.0;	Windows XP	32 Bit	28915	58 secs	1 month, 1 week	Procs Logs (3)
20 - Delete	69	vTREI	*.177.170	Administrator	M S-DE2HAVE	Mozilla/4.0 (compatible; MSIE 8.0;	Windows Home Server	32 Bit	277218	17 secs	1 month, 1 week	Procs None
21 - Delete	9f	vTREI	*6.45.179	User	D	Mozilla/4.0(compatible; MSIE 7.0b;	Windows XP	32 Bit	0	3 weeks	1 month, 1 week	Procs None
22 - Delete	16	vTREI	*.42.214	user1	K ALLOS-PC	Mozilla/4.0(compatible; MSIE 7.0b;	Windows XP	32 Bit	831	1 day 11 hours	1 month, 1 week	Procs Logs (4)
23 - Delete	39	vTREI	*.196.166	Administrador	S IDOR	Mozilla/4.0 (compatible; MSIE 6.0;	Windows XP	32 Bit	0	1 month	1 month, 1 week	Procs None
24 - Delete	ee	vTREI	*4.236.14	Manager	M OS	Mozilla/4.0 (compatible; MSIE 8.0;	Windows Server 2003	32 Bit	11	1 week 2 days	1 month, 1 week	Procs None
25 - Delete	b3	vTREI	*5.103.19	K	K APSV I	Mozilla/5.0 (compatible; MSIE 9.0;	Windows 7	64 Bit	29	4 hours 8 mins	1 month, 1 week	Procs Logs (9)
26 - Delete	de	vTREI	*.167.188	Administrator	P MS	Mozilla/4.0(compatible; MSIE 7.0b;	Windows Home Server	32 Bit	3571524	16 secs	1 month, 1 week	Procs None
27 - Delete	4c	vTREI	*.167.188	accountsadmin	P MS	Mozilla/4.0(compatible; MSIE 7.0b;	Windows Home Server	32 Bit	2	4 hours 8 mins	1 month, 1 week	Procs Logs (23)
28 - Delete	eb	vTREI	*.167.188	adminmmwh2008	P MS	Mozilla/4.0(compatible; MSIE 7.0b;	Windows Home Server	32 Bit	600	3 weeks, 1 day	3 weeks 3 days	Procs None

Target vs Kund_X

	TARGET
ATTACKVEKTOR	3:e partsleverantör Keylogger
TYP AV ANGREPP	Malware Memory Scraper
UTSKICK AV KORTDATA	Command&Control FTP
STULET KORTDATA	40 miljoner (+70 milj personuppgifter)

	KUND_X
ATTACKVEKTOR	Wifi? Leverantör?
TYP AV ANGREPP	Malware Network Sniffer
UTSKICK AV KORTDATA	Command&Control
STULET KORTDATA	Oklart. 100 000-tals

Sammanfattning

- Fler **avancerade** riktade attacker
- Enklare att utföra attacker
- Krävs högre säkerhet

- … och det kommer fler angrepp…

Secure Experience

Jonas Elmqvist
jonas.elmqvist@knowit.se
+4670-379 22 74

knowit

Frågor?

Secure Experience

Jonas Elmqvist
jonas.elmqvist@knowit.se
+4670-379 22 74

knowit