Chapter 1

M-Trends 2015 Report

1.1 Intro

1.1.1 Targets

Retailers are the main targets, because of their potential credentials possession. New emergent target: business and professional services, healthcare, and government and international organisations.

1.1.2 Detection

Surprisingly only 30 percent of the victims discover the breach internally, 70 percent are notified by external entities.

1.1.3 Phising

78 percent of phising impersonate an IT department. and 70 percent of those mails were sent between Tuesday and Friday.

1.2 Trends

1.2.1 Struggling with disclosure(act of making something known)

More victims are publicly disclosing breaches and finding themselves in the media spotlight. The press, customers, and partners are beginning to realise that security breaches are inevitable. But at the same time, they are demanding more information and asking more detailed questions. To prepare, organisations need an effective communication strategy. The best strategies are guided and informed by facts determined from a thorough investigation of the incident.

Steps of an investigation

Questions we should ask ourselves when conducting an investigation:

- How did they get access ?
- How did they maintain access?
- Storyline of the attack ?
- What data has been stolen ?
- Is the incident contained ?

1.2.2 Retail in the crosshairs

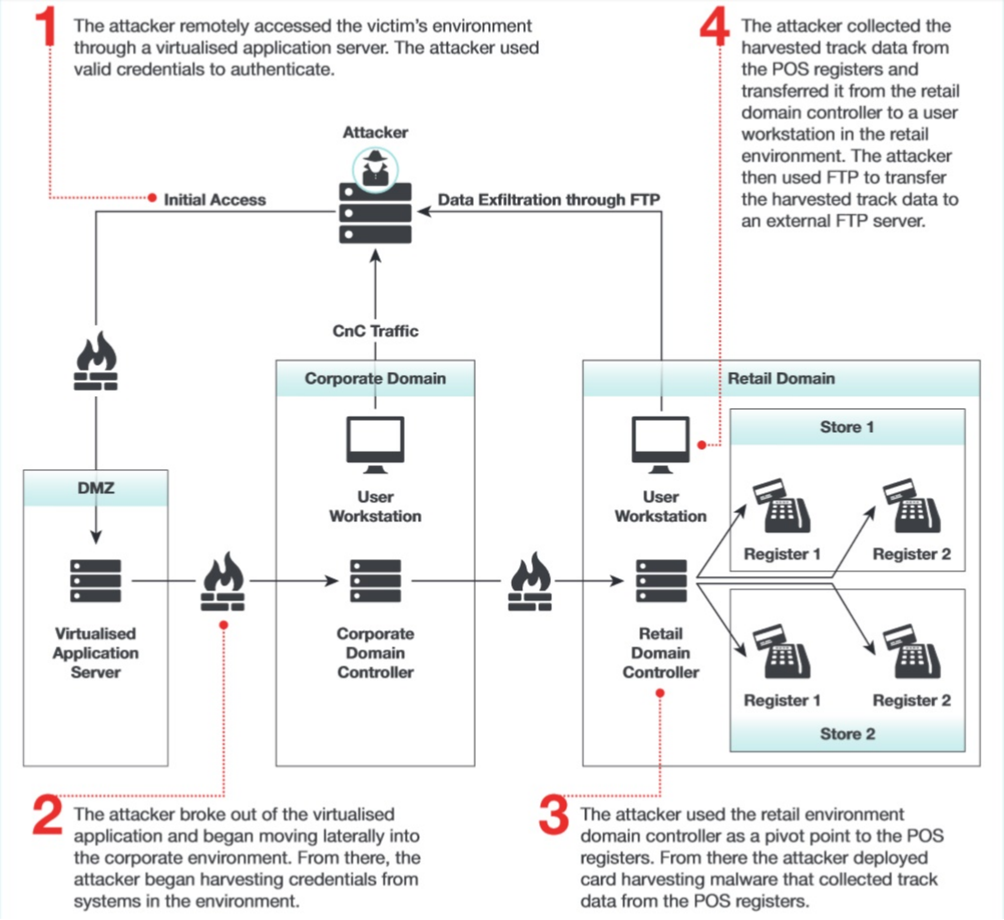
(running the gamut = to include everything within a group or type) Many application run on virtual machines which should make it impossible for attackers to gain access to the main server, but a slight error in the configuration can leave gaps.
Even if chip and PIN authentication should make it more difficult for attackers, the attacks against the technologies have increased.

Case Study: 1 attacker, millions of credit cards

Entering remotely a VM with credentials acquired priorly to the attack. Escalating privileges thanks to a misconfiguration and accessing system, using a windows FTP to dl password dumping tool,escalating to root privileges, same admin access for the whole environment.
(Amid = Parmi)
Recommendation:

- secure remote access(2 way authentification + monitoring of logons)
- secure access to PCI(payment card inductry) environment
- deploy app-whitelisting on critical assets
- Manage privilege accounts

Where money goes, criminals will follow. Retailers have always been in the crosshairs of financially motivated cyber criminals. We saw no change to this in 2014. While attackers used some new techniques and grabbed more headlines, their playbook remained largely consistent with what we have observed over the last few years.

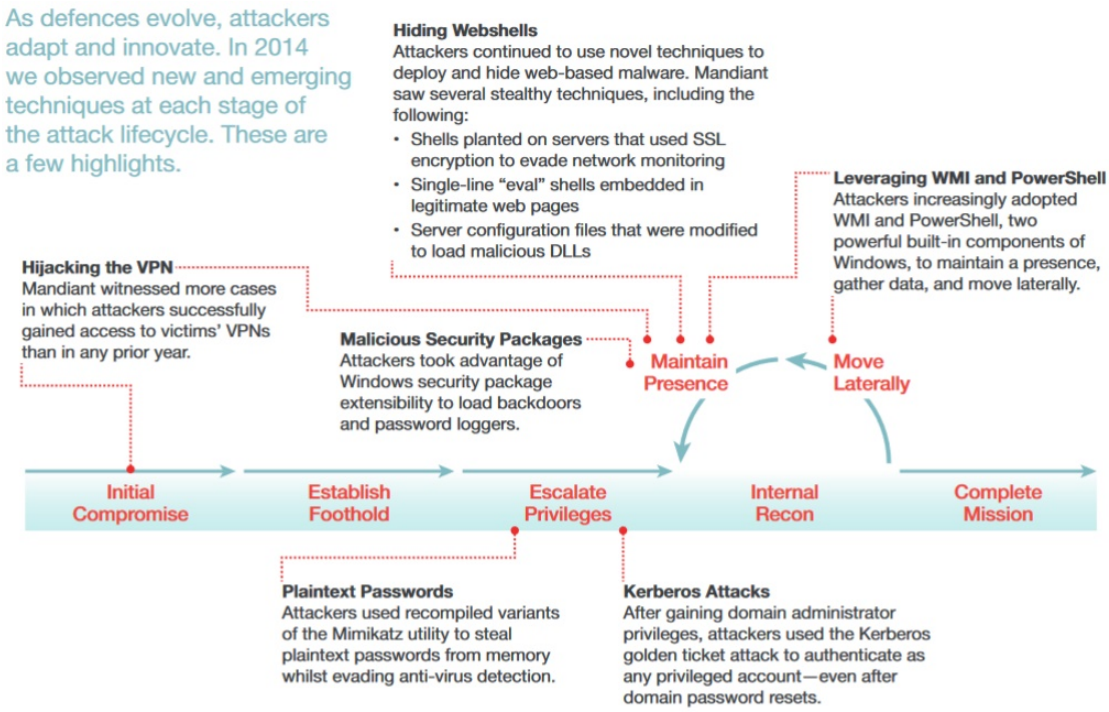

1
The attacker remotely accessed the victim's environment through a virtualised application server. The attacker used valid credentials to authenticate.
4
The attacker collected the harvested track data from the POS registers and transferred it from the retail domain controller to a user workstation in the retail environment. The attacker then used FTP to transfer the harvested track data to an external FTP server.
Attacker
Initial Access
Data Exfiltration through FTP
CnC Traffic
Corporate Domain
Retail Domain
DMZ
User Workstation
User Workstation
Store 1
Register 1
Register 2
Virtualised Application Server
Corporate Domain Controller
Retail Domain Controller
Register 1
Register 2
Store 2
2
The attacker broke out of the virtualised application and began moving laterally into the corporate environment. From there, the attacker began harvesting credentials from systems in the environment.
3
The attacker used the retail environment domain controller as a pivot point to the POS registers. From there the attacker deployed card harvesting malware that collected track data from the POS registers.

1.2.3 The evolving attack lifecycle

Hijacking VPN, huge grow of interest for the VPN's, and here are the 2 methods used to acquire this access:

- Single factor authentication (reuse of stolen usernames/passwords)
- Certificate-based two-factor authentication: tools are used to extract the Certificates or obtained by careless exchange of these.

Here is the usual cycle



As defences evolve, attackers adapt and innovate. In 2014 we observed new and emerging techniques at each stage of the attack lifecycle. These are a few highlights.

Hiding Webshells
Attackers continued to use novel techniques to deploy and hide web-based malware. Mandiant saw several stealthy techniques, including the following:

- Shells planted on servers that used SSL encryption to evade network monitoring
- Single-line "eval" shells embedded in legitimate web pages
- Server configuration files that were modified to load malicious DLLs

Leveraging WMI and PowerShell
Attackers increasingly adopted WMI and PowerShell, two powerful built-in components of Windows, to maintain a presence, gather data, and move laterally.

Hijacking the VPN
Mandiant witnessed more cases in which attackers successfully gained access to victims' VPNs than in any prior year.

Malicious Security Packages
Attackers took advantage of Windows security package extensibility to load backdoors and password loggers.

Plaintext Passwords
Attackers used recompiled variants of the Mimikatz utility to steal plaintext passwords from memory whilst evading anti-virus detection.

Kerberos Attacks
After gaining domain administrator privileges, attackers used the Kerberos golden ticket attack to authenticate as any privileged account—even after domain password resets.

Advanced threat actors continue to evolve their tools and tactics to reduce the forensic footprint of their activities and evade detection. Targeted organisations need to ensure that they maintain capabilities for both real-time monitoring and "look-back" forensics capabilities across endpoint systems, log sources, and network devices. Establishing a baseline of normal activity in an environment, and proactively hunting for deviations from this baseline, are essential to stay a step ahead of intruder's efforts.

1.2.4 Blurred lines-criminal and APT actors take a page from each other's playbook

As the tools, techniques, and procedures of criminal and APT actors coalesce, you must scrutinise actors' intent and motivations. Only then can you properly assess the potential impacts of security incidents, respond appropriately, and create a security strategy appropriate for the threats you face.

1.3 Conclusion

Far too many organisations were unprepared for the inevitable breach, allowing attackers to linger far too long in compromised environments.
No one can prevent every breach. But by preventing, detecting, analysing, and responding to the most advanced threats quickly and effectively, you can protect yourself, your customers, and your partners from the headline-generating consequences.

Chapter 2

McAfee Threats Report

2.1 Summary

...

2.2 Key Reports

2.2.1 The equation group: hard disk and solid state drive firmware

2.2.2 Ransomware

2.2.3 Adobe Flash

2.3 Threat Statistics

Chapter 3

Hacking human OS(social engineering)

3.1 Intro

3.2 Social engineering

3.3 Attacks

3.4 Attacks Lifecycle

3.5 Channels of attack

3.6 Defence ?

3.7 Conclusion

Chapter 4

DPI (deep packet inspection) and data protection law

4.1 Confidentiality of communications (Art.5)(EUROPE)

Member States shall ensure the confidentiality of communications and the related traffic data. Meaning they have to prohibit listening, tapping, storage or other kinds of interception or surveillance.

4.2 Principle of erasure of traffic data (Art.6)

4.2.1 paragraph 1

Traffic data relating to subscribers and users must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication.
Traffic data = any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof.

4.2.2 paragraph 2-4 (exceptions)

1. Traffic data necessary for the purposes of subscriber billing and interconnection payments may be processed

2. Traffic data necessary for the purpose of marketing electronic communications services or for the provision of value added services may be processed but consent of users required.
   Value added service = any service which requires the processing of traffic data or location data other than traffic data beyond what is necessary for the transmission of a communication or the billing thereof

4.2.3 paragraph 5

Processing of traffic data, in accordance with paragraphs 1, 2, 3 and 4, must be restricted to persons acting under the authority of providers of the public communications networks and publicly available electronic communications services handling billing or traffic management, customer enquiries, fraud detection, marketing electronic communications services or providing a value added service, and must be restricted to what is necessary for the purposes of such activities.
This means that is possible to process traffic data for traffic management purposes without users consent(NOT IN UK).

4.3 Questions

This raises an important question: If it is possible to process traffic data for traffic management and network security purposes :

1. How deep can you go?
2. What can you do with the data?
3. Can ISPs retain the data?

It would seem that the answer from the CJEU(Court of Justice of the European Union) is that the systematic retention of traffic data, location data and the related data necessary to identify the subscriber or user = Interference with the right to respect for private life! This means this systematic retention is illegal ?

Chapter 5

From porn to cyber security passing by copyright: How mass surveillance technologies are gaining legitimacy... The case of Deep packet inspection technologies

5.1 Intro

pervasive = spread throughout.
Monitoring of traffic data is becoming more and more common. This paper has 2 objectives that wants to discuss:

1. At the same rate people are becoming more aware of the power of the ISP's, DPI is gaining legal legitimacy.
2. Review European data protection laws and privacy rights to include the discussion of DPI.

The pervasive monitoring by governments agencies and states has increased the interest in this field.
Deep Packet Inspection (DPI) technologies are able to make anything that happens on a network visible and recordable. Therefore they can be considered as surveillance. If you consider all the traffic it might be impossible to analyse but if focused on specific patterns then we have to fear for privacy!!

5.2 Types of DPI

5.3 Content regulation

5.3.1 Private experiments

5.3.2 EU framework

5.3.3 National interpretations

5.4 Data protection

5.4.1 The Lawful processing of personal data through the means of DPI(lawful = allowed or permitted by law)

5.4.2 The confinement of the processing of personal data through the means of DPI (confinement = hidding)

5.5 Conclusions

Chapter 6

How To Break Anonymity of the Netflix Prize Dataset

6.1 Intro

As part of the Netflix Prize contest, Netflix—the world's largest online movie rental service—publicly released a dataset containing movie ratings of 500,000 Netflix subscribers. The dataset is intended to be anonymous, and all personally identifying information has been removed. They demonstrated that by crossing the data with the IMDB (Internet Movie DB) they were able to find the identities and therefore deanonymise the huge dataset.
What is more incredible is that what a person watches is really telling about the life of this person, It's like a self-portrait in movie titles: Nowhere else is cultural desire so nakedly on display.

The contest had the following specifications: 1M$ for improving their movie recommendation service. To aid contestants, Netflix publicly released a dataset containing 100,480,507 movie ratings, created by 480,189 Netflix subscribers between December 1999 and December 2005.
Cases of deanonimyzation excited before showing that removing the identifying information isn't enough because with the help of auxiliary dataset the information could be reconnected.
The interesting **question** to ask is the following: How much does the attacker need to know about a Netflix subscriber in order to identify her record in the dataset, and thus learn her complete movie viewing history. The answer is **VERY LITTLE**. This will be proven in the following arguments.

6.2 Walkthrough the attacker mindset

6.3 Does privacy of Netflix ratings matter?

The question asked isn't right, the right one is: Are there any Netflix subscribers whose privacy can be compromised by analyzing the Netflix Prize datase?
Interesting aspect, even if in the present this privacy breach might not seem

important this can be studied as forward secrecy which can have hue impact in someone's future privacy! Plus even if this person creates anonymous virtual identities elsewhere, if any attacker is able to link the discovered data with the latter identity she won't be anonymous anymore.

Chapter 7

a firm foundation for Private Data analysis

7.1 Interesting points

1. query monitoring is computationally infeasible and that the refusal to respond to a query may itself be disclosive.

2. In sub-sampling a subset of the rows is chosen at random and released. **Does that means that sensitive data is disclosed in those sample ??** This questions comes from this comment: "Suppose appearing in a sub-sample has terrible consequences. Then every time sub-sampling occurs some individual suffers horribly.

3. In input perturbation, either the data or the queries are modified before a response is generated. This one is pretty good but "However, an outlier(donnée aberrante est une valeur ou une observation qui est "distante" des autres) may only be protected by the unlikelihood of being in the sub-sample". Does it mean that if you have a snignifical differene from the other data your only way to stay "privat" is not to be in the sub-sample?

4. Randomized response: Randomized response was devised for the setting in which the individuals do not trust the curator, so we can think of the randomized responses as simply being published. Privacy comes from the uncertainty of how to interpret a reported value. The approach becomes untenable for complex data

5. Adding random noise to the output fails: suppose the noise has mean zero and that fresh randomness is used in generating every response. In this case, if the same query is asked repeatedly, then the responses can be averaged, and the true answer will eventually emerge.

6. Intro of differential privacy idea: What happens if the curator(Data curation is a broad term used to indicate processes and activities related to the organization and integration of data collected from various sources, annotation of the data, and publication and presentation of the data such that the value of the data is maintained over time, and the data remains

available for reuse and preservation) permits only a sub-linear number of questions?

What is a sublinear number of questions ? how to maintain privacy against a sub-linear number of counting queries, that is, queries of the form “How many rows in the database satisfy property P ?” by adding noise of order less than the sampling error to each answer.

7. the importance of taking auxiliary information into account in privacy-preserving data release.

8. auxiliary information to capture information about the respondents other than that which is obtained through the statistical database. Any priors, beliefs, or information from newspapers, labor statistics, and so on, all fall into this category.

9. Dalenius’s Desideratum: Anything that can be learned about a respondent from the statistical database should be learnable without access to the database. Which he was totally wrong unfortunately, simply explain the German height example.

10. New privacy goal: Minimize the increased risk to an individual incurred by joining (or leaving) the database. −¿ Solution: Differential Privacy!

11. differential privacy: Differential privacy will ensure that the ability of an adversary to inflict harm (or good, for that matter) of any sort, to any set of people should be essentially the same, independent of whether any individual opts in to, or opts out of, the dataset.

Chapter 8

Breaking Diffie-Hellman

The Diffie Hellman was the system used for key exchange. The idea is that both parties want to communicate, but to do so thy need a common key to encrypt their messages. This key has to be known by both but can't be known by someone intercepting their messages, this is how it works:

Diffie-Hellman Protocol

The Diffie-Hellman protocol is a method for two computer users to generate a shared private key with which they can then exchange information across an insecure channel. Let the users be named Alice and Bob. First, they agree on two prime numbers g and p, where p is large (typically at least 512 bits) and g is a primitive root modulo p. (In practice, it is a good idea to choose p such that $(p-1)/2$ is also prime.) The numbers g and p need not be kept secret from other users. Now Alice chooses a large random number a as her private key and Bob similarly chooses a large number b. Alice then computes $A = g^a(modp)$, which she sends to Bob, and Bob computes $B = g^b(modp)$, which he sends to Alice.

Now both Alice and Bob compute their shared key $K = g^(ab)(modp)$, which Alice computes as
$K = B^a(modp) = (g^b)^a(modp)$

and Bob computes as
$K = A^b(modp) = (g^a)^b(modp)$.

Alice and Bob can now use their shared key K to exchange information without worrying about other users obtaining this information. In order for a potential eavesdropper (Eve) to do so, she would first need to obtain $K = g^(ab)(modp)$ knowing only g, p, $A = g^a(modp)$ and $B = g^b(modp)$.

This can be done by computing a from $A = g^a (modp)$ and b from $B = g^b (modp)$. This is the discrete logarithm problem, which is computationally infeasible for large p. Computing the discrete logarithm of a number modulo p takes roughly the same amount of time as factoring the product of two primes the same size as p, which is what the security of the RSA cryptosystem relies on. Thus, the Diffie-Hellman protocol is roughly as secure as RSA.