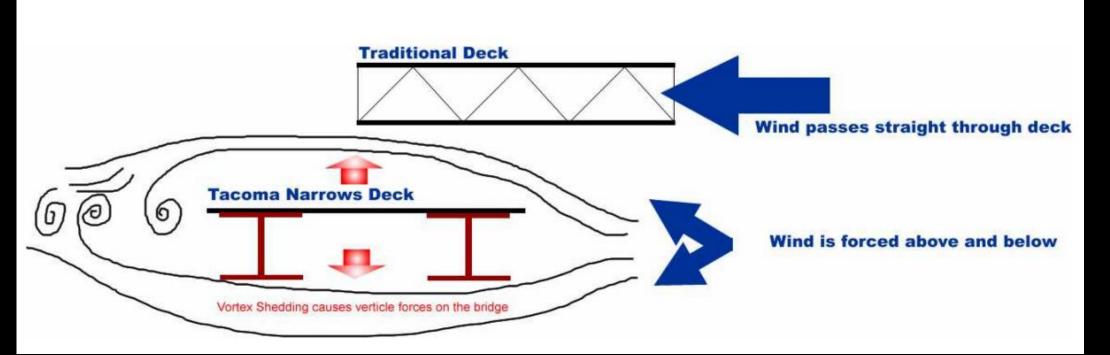
November 7th 1940

Tacoma Washington USA









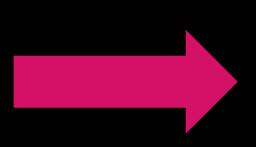


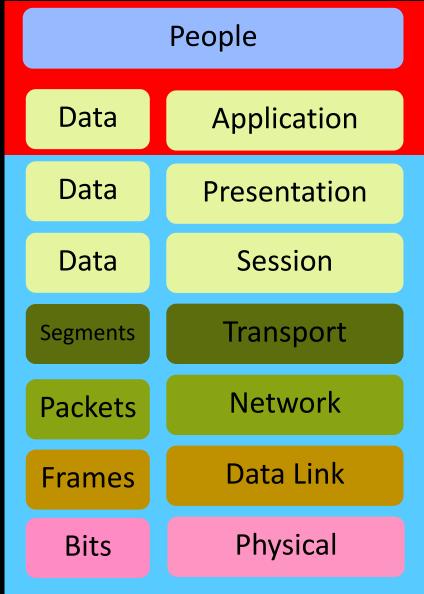
Have we learned from our past?



The Wild West

Foundation of the Internet







Lessons learned from the Check Point Incident Response Team in 2019







Management needs to embrace security

Security can no longer be:
Ignored
Partially implemented
Fully outsourced

Cloud is not automatic security

Cloud requires a lot of planning and hard work





293.6 billion emails per day

347.3 billion by 2023

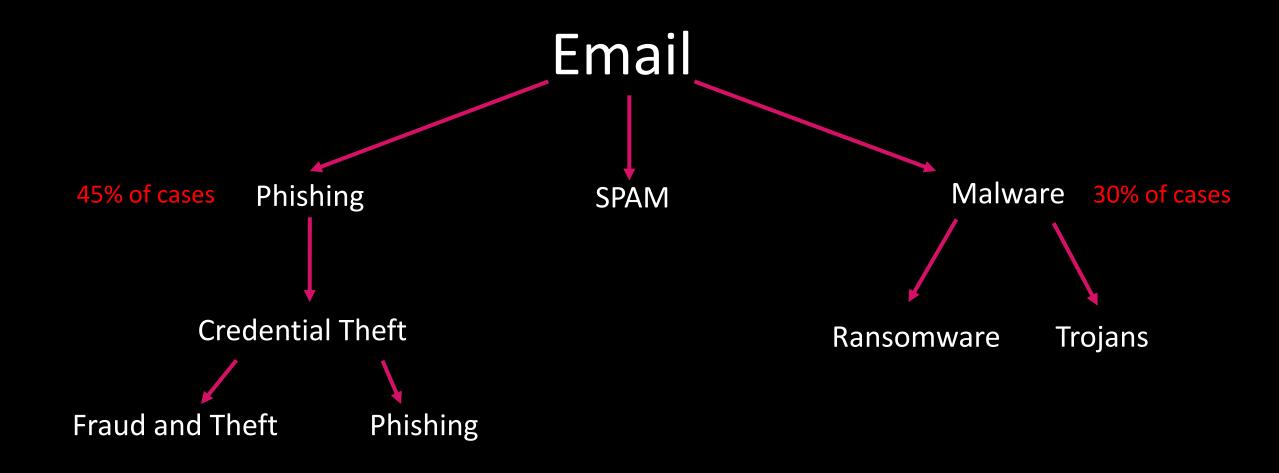
55% of all email are spam

The average office worker receives 120 emails per day

Email marketing ROI: 3,200%

An emoji in the subject line will boost your open rate • **!!





After almost 50 years email is still the most prolific source of threats







The Case:

Business Email Compromise Resulting in Fraudulent Wire Transfers



THE TARGET

Financial sector- Investment Company

Location – Anywhere there is money

Losses - \$1.5 Million

Customer did not know how the attack worked

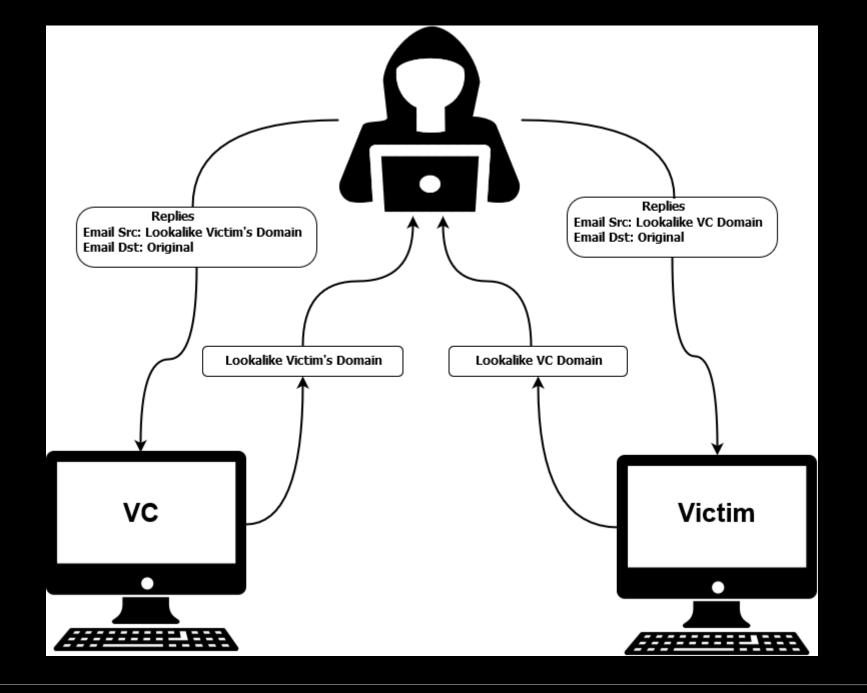
Called Check Point Incident Response Team to investigate



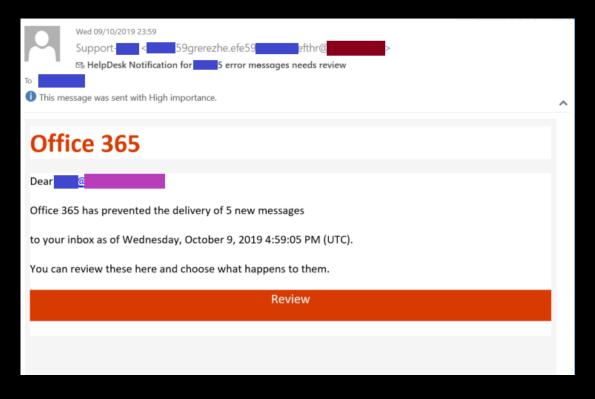
New-InboxRule -StopProcessingRules:\$True -DeleteMessage:\$True -Force:\$False -From -AlwaysDeleteOutlookRulesBlob:\$False -Name JP New-InboxRule -RecipientAddressContainsWords -AlwaysDeleteOutlookRulesBlob:\$False -Force:\$False -DeleteMessage:\$True -StopProcessingRules:\$True -Name Wq New-InboxRule -StopProcessingRules:\$False -AlwaysDeleteOutlookRulesBlob:\$False -Force:\$False -Name -MoveToFolder Note1 -SubjectOrBodyContainsWords " Supplier Payment Review - 10.12.2019 - URGENT" New-InboxRule -StopProcessingRules:\$False -AlwaysDeleteOutlookRulesBlob:\$False -Force:\$False -Name -MoveToFolder "RSS Feeds" -SubjectOrBodyContainsWords New-InboxRule -StopProcessingRules: SFalse -FromAddressContainsWords -Force: SFalse -MoveToFolder "RSS Feeds" -AlwaysDeleteOutlookRulesBlob: SFalse -Name .. -MoveToFolder "RSS Feeds" -Name ... New-InboxRule -StopProcessingRules:\$False -AlwaysDeleteOutlookRulesBlob:\$False -Force:\$False -From New-InboxRule -StopProcessingRules:\$False -FromAddressContainsWords -Force:\$False -MoveToFolder "RSS Feeds" -AlwaysDeleteOutlookRulesBlob:\$False -Name .. New-InboxRule -StopProcessingRules:\$False -AlwaysDeleteOutlookRulesBlob:\$False -Force:\$False -From I ı -MoveToFolder "RSS Feeds" -Name ... New-InboxRule -StopProcessingRules: SFalse -AlwaysDeleteOutlookRulesBlob: SFalse -Force: SFalse -Name ... -MoveToFolder "RSS Feeds" -SubjectOrBodyContainsWords New-InboxRule -StopProcessingRules:\$False -AlwaysDeleteOutlookRulesBlob:\$False -Force:\$False -From -MoveToFolder Archive -Name . New-InboxRule -StopProcessingRules:\$False -AlwaysDeleteOutlookRulesBlob:\$False -Force:\$False -From MoveToFolder Archive -Name . New-InboxRule -StopProcessingRules:\$True -AlwaysDeleteOutlookRulesBlob:\$False -Force:\$False -From I -MoveToFolder Archive -Name z New-InboxRule -StopProcessingRules: \$False -AlwaysDeleteOutlookRulesBlob: \$False -Force: \$False -Name . -MoveToFolder "RS\$ Feeds" -SubjectOrBodyContainsWords return; returned; fail; failed New-InboxRule -StopProcessingRules:\$False -FromAddressContainsWords :-Force:\$False -MoveToFolder "RSS Feeds" -AlwaysDeleteOutlookRulesBlob:\$False -Name ... New-InboxRule -StopProcessingRules:\$False -AlwaysDeleteOutlookRulesBlob:\$False -Force:\$False -Name .. -MoveToFolder "RSS Feeds" -SubjectOrBodyContainsWords New-InboxRule -StopProcessingRules:\$False -FromAddressContainsWords mazars.co.uk -Force:\$False -MoveToFolder "RSS Feeds" -AlwaysDeleteOutlookRulesBlob:\$False -Name ... New-InboxRule -StopProcessingRules:\$False -AlwaysDeleteOutlookRulesBlob:\$False -Force:\$False -From t -MoveToFolder "RSS Feeds" -Name .. New-InboxRule -StopProcessingRules:\$True -DeleteMessage:\$True -Force:\$False -From -AlwaysDeleteOutlookRulesBlob:\$False -Name . New-InboxRule -StopProcessingRules:\$False -FromAddressContainsWords r -Force:\$False -MoveToFolder "RSS Feeds" -AlwaysDeleteOutlookRulesBlob:\$False -Name ... New-InboxRule -StopProcessingRules:\$False -AlwaysDeleteOutlookRulesBlob:\$False -Force:\$False -Name .. -MoveToFolder "RSS Feeds" -SubjectOrBodyContainsWords New-InboxRule -StopProcessingRules:\$False -AlwaysDeleteOutlookRulesBlob:\$False -Force:\$False -From -MoveToFolder "RSS Feeds" -Name . -MoveToFolder "RSS Feeds" -Name . New-InboxRule -StopProcessingRules:\$False -AlwaysDeleteOutlookRulesBlob:\$False -Force:\$False -From



FullCommand



THE PHISH



Personalized for the recipient

Key personnel targeted – CEO and CFO

No massive phishing spam emails

Link is hosted on public cloud services



Reconnaissance

Attacker can spend weeks or even months reading emails, understanding how money transfers are made, key roles inside the company and the relationships with other companies.

Stage 3

Inject

During this stage the attacker will find a way to inject their fraudulent bank accounts while making sure both parties are unaware or believe this change is legitimate.

Stage 5

Repeat

At this point the attacker will continue their efforts to make more money by trying to initiate or take over another transaction.

It is also very likely that the attacker will chose their next victim out of the list of companies they learnt about from the current victim.

Phishing

Stage 1

Attacker starts with an highly targeted Phishing campaign on high profile individuals tricking them into providing their mailbox credentials.

Stage 2

Setup

Attacker starts setting up lookalike domains, mail servers and mailbox rules that will allow them to impersonate both companies and control the communications between them.



Steal

Once the company in question accepts the new banking information and agrees to perform the transaction, all is left to do is just wait for the money while still monitoring the conversations and making sure they go unnoticed.













THANK YOU

