ExploitChance

~~vs~~ and

CrowdStrike

March 2022

Crowdstrike Mantra:

“*Breaches Stop Here*”

Machine Learning, Behavioral Analytics, Exploit Mitigation, Sandboxing & Isolation, Detection & Response

Machine Learning

Effective against: New, modified or packed malware

Primary benefit: Anti-malware efficacy and system performance

Behavioral Analitics

Effective against: Web shells and other advanced infections (e.g. stolen passwords & abuse of legit tools), Ransomware, Lateral movement, Persistence, Data access and exfiltration

Primary benefit: Coverage for malware-free attacks and polymorphic malware

Exploit Mitigation

Effective against: Exploits - Hugely prevalent exploit kits

Primary benefit: System hardening

SandBoxing & Isolation

Effective against: Exploits - Hugely prevalent exploit kits

Primary benefit: Impact reduction

Detection & Response

Effective against: Advanced threats, zero days, APT activity, insider threat, abuse of legit tools

Primary benefit: Visibility

What is the common requirement to all the techniques used by Crowdstrike to stop attackers?

They need an attack.

Unless an attack is ongoing, Crowdstrike can't help the company.

In other words Crowdstrike is like a **RESERVE PARACHUTE** for corporate security.

Reserve parachute saves the pilot when there's a malfunction.

Malfunction

verb

1. (of a piece of equipment or machinery) fail to function normally.
   "the unit is clearly malfunctioning"

   Similar: **crash, go wrong, break down, break, act up, fail, fall over, play up, pack up**

noun

1. a failure to function normally.
   "a computer malfunction"

   Similar: **crash, breakdown, fault, failure, defect, flaw, collapse, impairment, glitch**

The pilot will never require the reserve parachute until there's a malfunction.

The company will never require CrowdStrike until there's a ***security malfunction***.

Meet Bob.

He likes skydiving, he uses standard skydiving equipment (parachute).

Anyway, John likes to fly very close to the mountains (proximity) and don't follow any "security" rules…

Stats say John has (lot) more chances of dying than a standard skydiver.

Meet Bob: Habits

John also works at Big Corp and has very bad habits: he usually do not follows corporate security best practices.

John thinks everything is “under control”. He is self confident.

Meet Bob: Access Level

John has access to very sensible data/systems at Big Corp…

Meet Bob: Computer

John was able to convince IT management to have local admin rights so he can install custom apps he “really needs”.

Meet Alice.

She likes skydiving, she uses standard skydiving equipment.

Anyway, Alice prefers to fly far from Earth and strictly follows security rules.

Statistically Alice will survive Bob.

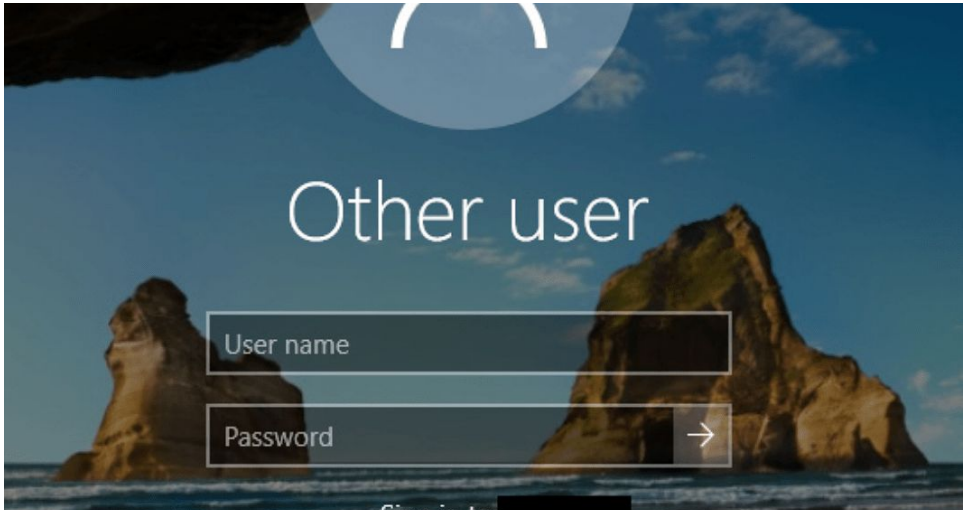
Meet Alice: Habits

Alice also works at Big Corp. She strictly follows corporate security best practices.

Alice understands employees are responsible of security so she tries to do her best by having good habits.

Meet Alice: Access Level

Even if Alice has a relevant role at Big Corp, she has not access to very sensible data/systems.



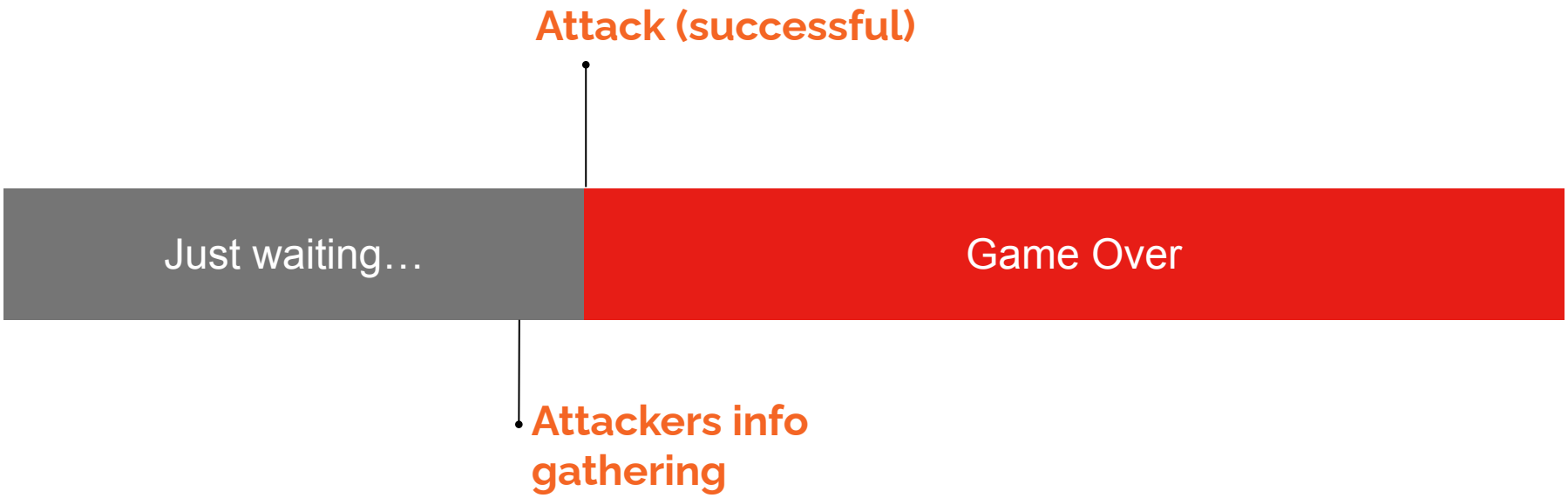
Meet Alice: Computer

Alice has a standard local account. She only uses corporate apps and is unable to install anything.

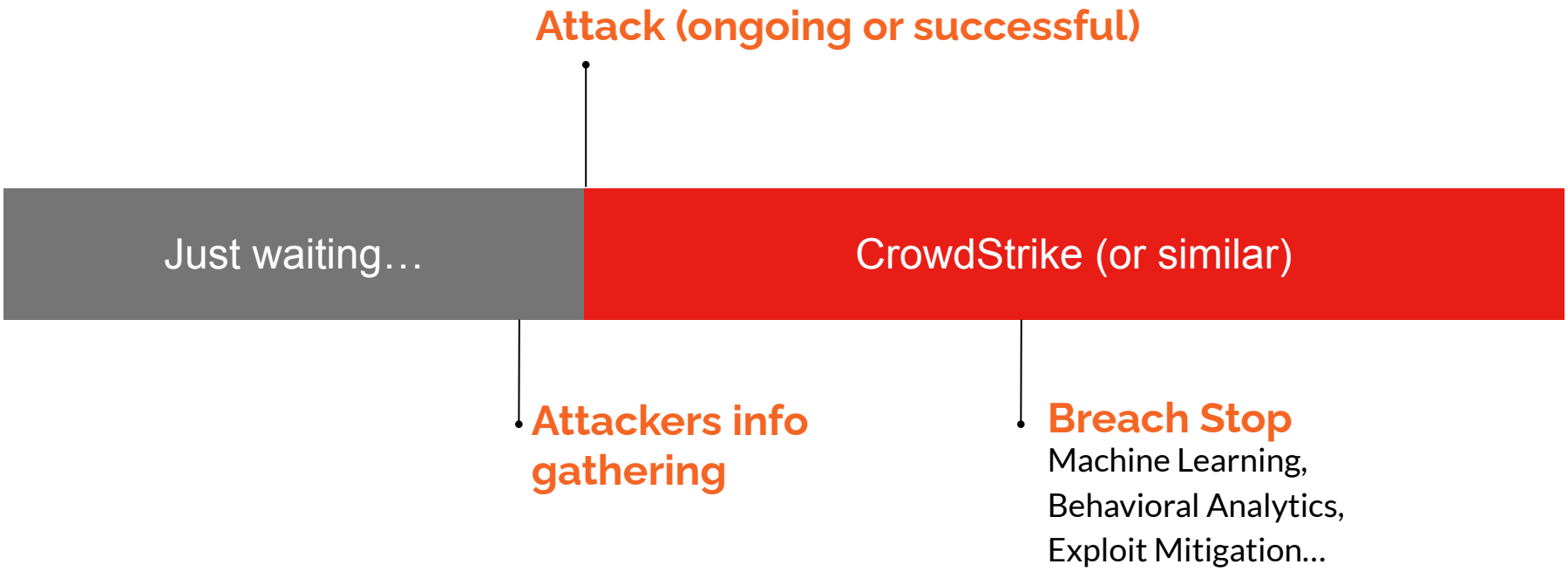
If you were an attacker, which one will you target: Alice or Bob…?

Wouldn’t be nice to know in advance that Bob’s computer has more chances of being exploited to take preventive actions?

Time Line without any protection



Time Line with just CrowdStrike (or similar)



Time Line with ExploitChance (best case)

ExploitChance info gathering

Technology Usage, Habits, Computer Config, Access Level (Via Zero Trust)

Attack (failed)

Thanks to Security Design Changes

Security Design Changes

Devices Hardening, Zero Trust, Users Training,...

Attackers info gathering

Time Line with ExploitChance (worst case)

ExploitChance info gathering

Technology Usage, Habits, Computer Config, Access Level (Via Zero Trust)

Attack (ongoing or successful)

Despite Security Design Changes

Security Design Changes

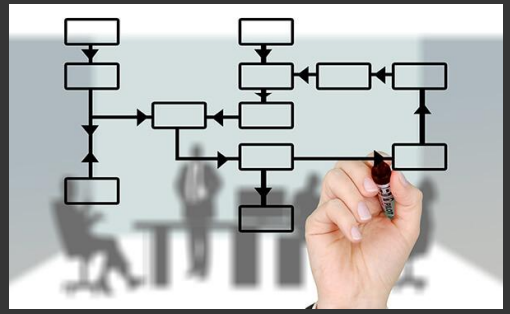
Devices Hardening, Zero Trust, Users Training,...

Attackers info gathering

Breach Stop

Machine Learning, Behavioral Analytics, Exploit Mitigation…

Feature	ExploitChance	CrowdStrike
Pre-Attack risk analysis	YES	**NO**
Legitimate User Behavior analytics (Thanks to Zero Trust)	YES	**NO**
FW (Native + Cloud)	YES	**NO** (Only Native)
Zero Trust	YES	YES (**Partial**, not enforced by Virtual Apps/Endpoints)
SaaS + On-Premises	YES	**NO** (Only SaaS)
Mathematically Proven TCB (seL4)	YES	**NO**
Single Product for All Features	YES	**NO**
Virtual Apps/Endpoints	*Not Yet*	**NO**



Best/Worst case examples of Attackers, EC and Crowdstrike working flow

Ex. 1: Phase Info Gathering

Attackers get information about employees that usually receive email attachments, employees that are easy to trick, employees with heavy use of Internet, etc. ExploitChance already provided this (and much more) information to the customer.

- **Attackers**: **POTENTIAL TARGETS**
- **ExploitChance**: **POTENTIAL TARGETS**
- **CrowdStrike**: **NONE**

Ex. 1: Malware Attack (best case)

Attackers are able to reach an employee device with malware. Thanks to specific employee education malware is never executed.

- **Attackers**: **TARGET ATTACK**
- **ExploitChance**: **NONE**
- **CrowdStrike**: **NONE**

Ex. 1: Malware Attack (worst case)

Attackers are able to reach an employee device with malware. Even with specific employee education malware is executed. CrowdStrike stops the attack.

- **Attackers**: TARGET ATTACK
- **ExploitChance**: **NONE**
- **CrowdStrike**: BREACH STOP

Ex. 2: Phase Info Gathering

Attackers get information about key employees that have remote access to engineering network.

- **Attackers**: **POTENTIAL TARGETS**
- **ExploitChance**: **POTENTIAL TARGETS**
- **CrowdStrike**: **NONE**

Ex. 2: Lat. Movement (best case)

Attackers try to use a stolen device to access engineering network to jump to other system. Thanks to employee profile hardening, the attackers laptop requires physical token to boot and attack fails.

- **Attackers**: **POTENTIAL TARGETS**
- **ExploitChance**: **NONE**
- **CrowdStrike**: **NONE**

Ex. 2: Lat. Movement (worst case)

Attackers use a stolen device to access engineering network and and are able to jump to other systems even if laptop hardware token was in place, attackers are able to use the laptop to access de remote network. CrowdStrike detects anomalous behavior and stops attack.

- **Attackers**: **POTENTIAL TARGETS**
- **ExploitChance**: **NONE**
- **CrowdStrike**: **BREACH STOP**

Ex. 3: Info Gathering

Attackers get information about key employees that has remote access to a specific critical system.

- **Attackers**: **POTENTIAL TARGETS**
- **ExploitChance**: **POTENTIAL TARGETS**
- **CrowdStrike**: **NONE**

Ex. 3: Legit. Access (best case)

Attackers use a stolen device and token to legitimately access a critical system. ExploitChance warned about this potential target and target user was very trained and able to manually rise an alert when s/he detected the attack. The attack failed or just partially succeeded.

- **Attackers**: **POTENTIAL TARGETS**
- **ExploitChance**: **NONE**
- **CrowdStrike**: **NONE**

Ex. 3: Legit. Access (worst case)

Attackers use a stolen device and token to legitimately access a critical system. ExploitChance warned about this potential target and target user was very trained anyway, s/he didn't detected the attack. The attack succeeded.

- **Attackers**: **POTENTIAL TARGETS**
- **ExploitChance**: **NONE**
- **CrowdStrike**: **NONE**

What you get with EC

Extended range awareness and risk management that integrates with existing EDR

Added security capabilities with Design Change capabilities: Zero Trust, Virtual Apps/Endpoints,..

Verified TCB (seL4), trusted design, etc beyond most DoD requirements.