Adaptive Defense at work...

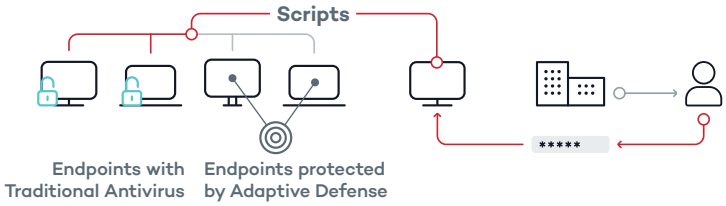
An Ex-employee tries to Extort his Former Company.

1 The employee is fired

But his credentials were not revoked, so he still can remotely access his computer.

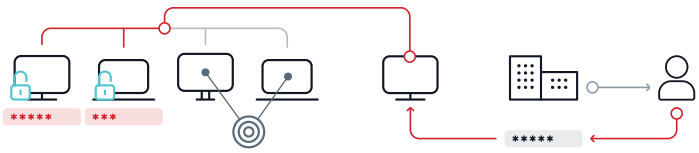
2 Detailed profiling

Thanks to several OS tools, the employee gets the list of endpoints connected to the network.
He launches a script with a MS command to find out the users of the domain.



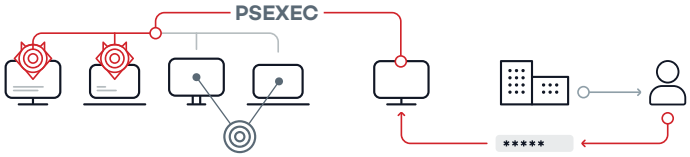
3 Brute-force attacks

Within the following days, he deployed brute-force attacks and finally got access to several endpoints.



4 Ransomware attack

He creates a ransomware, which is compiled the day before it is deployed. From his former computer, and by executing PSEXEC, he launches a script to remove all the existing backups and then copies and executes the ransomware.



☆ Attack discovered by the Threat Hunting team

Adaptive Defense blocked the attack in all the machines where it was installed. After the first attack attempt on an endpoint protected by Adaptive Defense, the Threat Hunting team investigated all the processes and behaviors, which revealed all the details of the attack and the identity of the attacker.