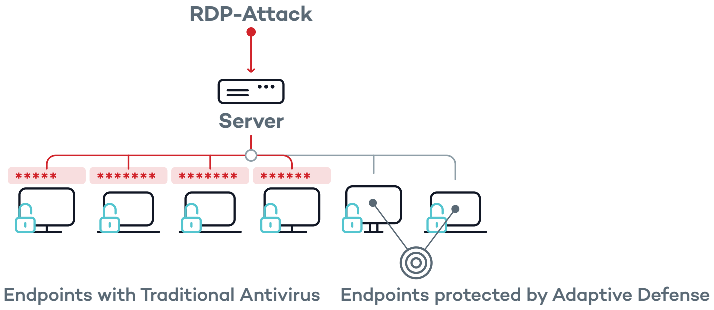
Adaptive Defense at work...

A Malware-less Attack, and two ways to monetize it.

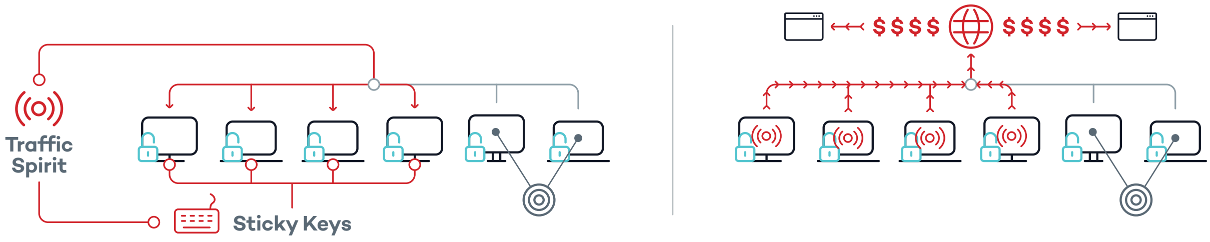
1 Gaining access and persistence

Attacker scans the Internet looking for potential victims with Remote Desktop enabled.
When found, he uses a brute-force attack to login into the system. Once in the system, he gets persistence by modifying the Sticky Keys feature registry entry. When Sticky Keys is activated (e.g. pressing CAPS 5 times) it will open a backdoor to the victim's computer that allows the attacker to access it even if Remote Desktop credentials are changed.


RDP-Attack
Server
*****
****
****
******
Endpoints with Traditional Antivirus
Endpoints protected by Adaptive Defense

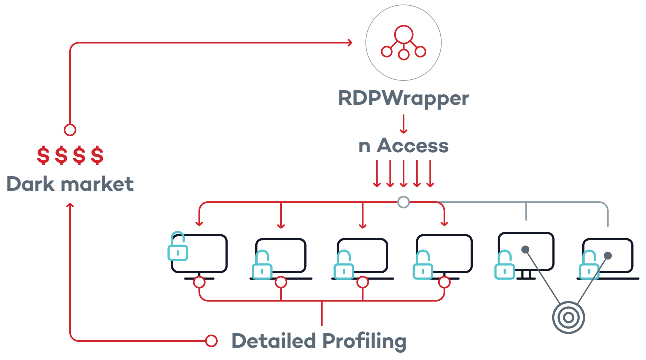
2.1 Monetization of the compromised endpoints: Generating online traffic

The hacker downloads "Traffic Spirit", a "legal" traffic generator application which is used to make extra money off of the compromised computers. There is no malicious program in this attack.



2.2 Monetization of the compromised endpoints: Selling the access to the machines

Once the attackers get the access, they carry out a detailed profiling of all the computers. They then offer access to these machines on the black market for different purposes (extortion, data leak, make them zombies, bots, etc.).



Attack discovered by Threat Hunting team

The attack is discovered thanks to continuous monitoring and visibility of all activities at the endpoint. That data shown to Panda Threat Hunters indicated an abnormal behavior at endpoints that were compromised with a brute-force attack (hundreds of login tries in a short period of time).
The customer was advised to close RDP access over the internet, to remove Traffic Spirit from the endpoints and restore the registry entry for Sticky Keys.

panda

pandasecurity.com