Ãttàck Brief: Sony “Dêstóver” Attåck

Who was attacked?

Sony Pictures Entertainment (SPE) is a motion picture and television production/distribution company. Based in the USA, SPE owns several film- and television-studios.

What was the attack-narrative?

In late November 2014, the Sony Pictures Entertainment IT network was knocked offline for a week, with terabytes of data mysteriously erased and massive amounts of sensitive information leaked on the internet. Leaked information included confidential company data (contracts, executive salaries…); IT data (plaintext credentials, server and access details); and employees’ personal data (social security numbers, credit card information, emails…).

Both SPE and the FBI have concluded that the North Korean government was behind the attack, named “Destover.”

How did the attack operate?

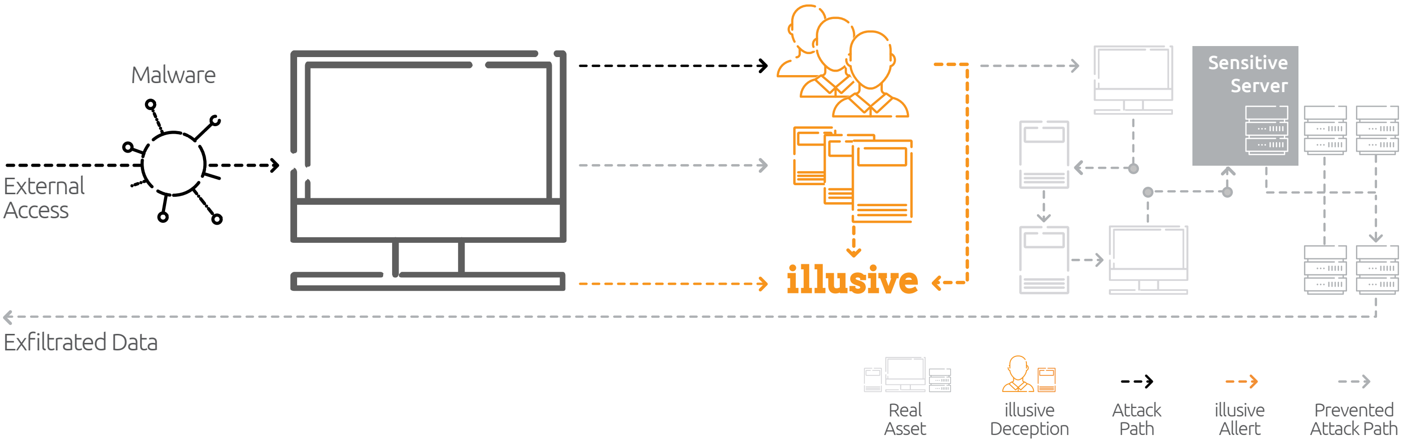
The targeted nature of the attack proves that attackers gained intimate knowledge of the network; the names of sensitive servers were hard-coded in the malware, meaning that attackers spent time and energy making lateral movements on the network, mapping and exploring assets.

To deploy malware, the attackers used administrator credentials, which are commonly retrieved from the memory of compromised hosts. The malware sought sensitive data and exfiltrated it via an internal server and third-party seeding platforms. While the malware used Windows management and file-sharing tools to propagate, shut down, and reboot assets, it used a commercial program to wipe data without being in admin mode.

How would illusive have detected the attack before the payload-launch?

Prevention Through Detection

Sony Detection



The illusive Deceptions Everywhere® solution detects advanced attacks in real-time and immediately collects forensics from compromised hosts, enabling Incident Response teams to prevent attackers from reaching sensitive data.

- illusive coats hosts with deceptive credentials, shared drives, and website-connections, ensuring that attackers reveal themselves as they attempt lateral movements.
- illusive detects unauthorized scans, used by attackers to discover saved connections.