illusive

Ãttàck Brief: Snowden NSA Attåck

Who was attacked?

The **National Security Agency** (NSA) is a part of the US government responsible for global intelligence and counterintelligence. It is also tasked with protection of US government communication and information systems.

How did the attack operate?

Given only contractor permissions, basic-terminal access, and SSH keys to authenticate and manage systems, Snowden reportedly obtained dozens of usernames and passwords from hosts.

Using these credentials, Snowden must have incrementally searched hosts for sensitive connections. The NSA stated that he manipulated found credentials and generated SSH keys to access restricted locations.

To avoid detection, he allegedly encrypted data before exfiltrating it.

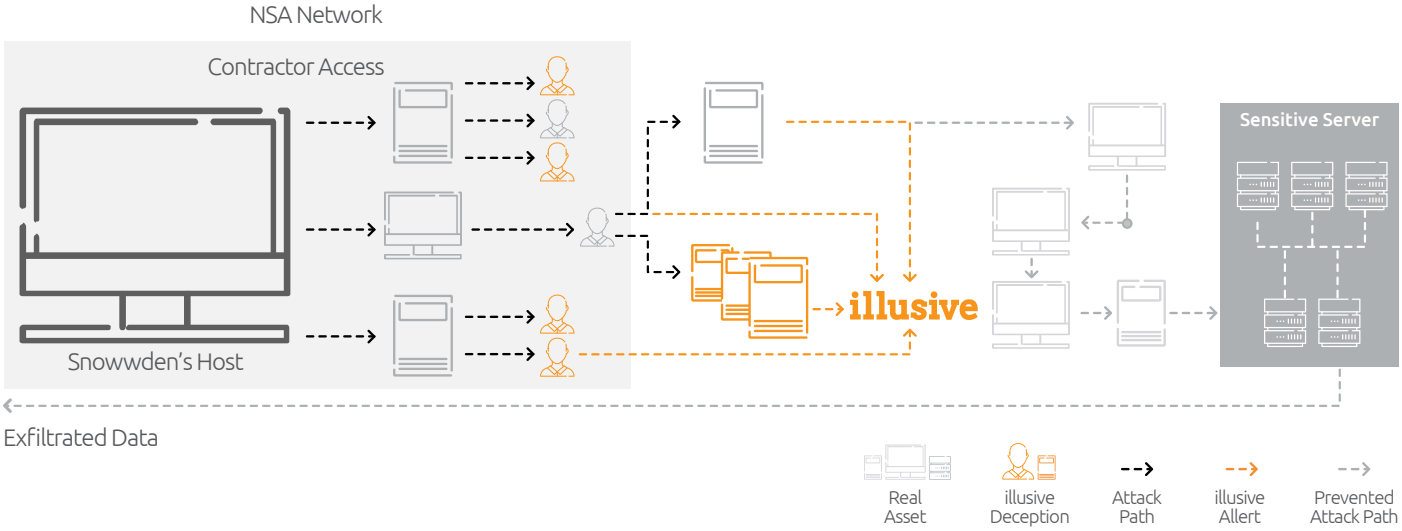
What was the attack narrative?

Edward Snowden, a former CIA employee, was contracted to work as a System Administrator for the NSA in 2013. He gained access to unknown amounts of classified information and leaked documents to reporters.

Leaked information included details of NSA programs that compromise the privacy of US citizens, world leaders, and several countries' communications.

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

Prevention Through Detection



Attacks like this require attackers who take time to locate and explore credentials and locations. The illusive Deceptions Everywhere® solution detects these lateral movements before sensitive data is reached. Real-time, source-based forensics enable compromises to be stopped in their infancy.

- illusive credential-deceptions cause attackers to reveal themselves as attackers use stored credentials to execute lateral movements.
- illusive SSH-server deceptions lead attackers to show themselves while seeking sensitive locations.
- illusive detects unauthorized network-scans, used by attackers to identify lateral-movement targets.
- The illusive Attacker View™ reveals attack-vectors, including network segmentation faults, identifying admin-credentials that can be used to breach network boundaries.