Ãttàck Brief: Pàtchwörk APT

What is the Patchwork APT?

First observed in December 2015, the Patchwork APT is made of several code segments, each taken from an online forum. It has infected approximately 2,500 high-profile targets worldwide.

Once the APT had already been detected and stopped on a compromised host, security tools were installed to explore the attack process. Based on the timing and activity of the attack, it is plausible that the attackers are Indian or pro-Indian.

What does the attack do?

Targets are primarily military and political staff dealing with Southeast Asia and the South China Sea. Compromised computers have their documents leaked and activity read.

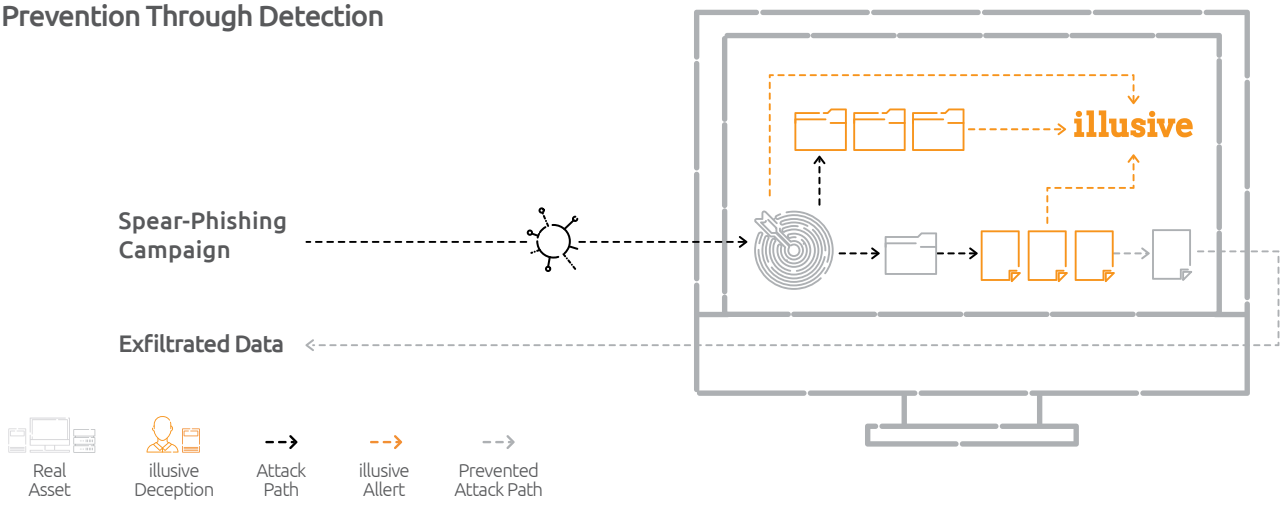
How does the attack operate?

As part of a phishing scheme, documents (generally PowerPoint presentations with subjects relating to China or pornography) are sent to targets. When opened, the malware uses known exploits and common attack tools (such as Sandworm, UACME, and Meterpreter) to scan the host, escalate privileges, exfiltrate files of predefined types from the local drive.

If the uploaded files are deemed valuable, the attackers deploy a second executable that scans the compromised hard disk and enables remote access. During this second stage, attackers exfiltrate additional local data and use existing connections to access further locations.

How would illusive detect the attack before the payload-launch?

Prevention Through Detection



The illusive Deceptions Everywhere® solution keeps sensitive data safe by detecting attacks like Patchwork before valid data is reached. Advanced attacks are caught in real-time and source-based forensics are instantly delivered.

- illusive deploys deceptions that appear as shared drives and files, distracting and diverting attackers while detecting attacks with high-fidelity. As they are not seen (or accessed) by valid users and tools, they cause zero false-positive alerts.
- illusive detects unauthorized scans and active malicious processes, as well as attempted access to malicious locations. These alerts allow Incident Response teams to understand the attack and quarantine it immediately.