Researchers stymied by hackers who drop fake clues

December 10 2014, byRaphael Satter

It's a hacker whodunit. Researchers say they have a wealth of clues—but no clear answers—as to the identity of those behind a series of newly discovered cyberattacks targeting Russian and Eastern European embassies, oil companies and military officers.

"The level of misdirection is impressive," said Hugh Thompson, a security strategist at Blue Coat Systems, Inc., which is publishing a report on the malware campaign Wednesday.

Blue Coat says the malware—nicknamed "Inception" after the complex dream heist movie starring Leonardo DiCaprio—has been attacking mainly Russian or Eastern European targets in the fields of diplomacy, energy and finance.

The Blue Coat report says researchers found signs hinting at the hackers' identity, but that they're all over the map.

For example, some of the malicious code carries words in Arabic and Hindi. Another piece of code carries the words, "God Save The Queen." A third clue, suggesting Chinese involvement, appears to have been left on purpose after the attackers realized they were being watched.

Kaspersky Lab researcher Costin Raiu, who is familiar with the malware, links the code to "Red October," a Russia-focused campaign his company uncovered early last year. Raiu points to similarities in the attackers' "philosophy and style" and says several of the same targets

were hit.

Blue Coat malware researcher Waylon Grange says that connection is possible, but that he is reserving judgment in light of the hackers' trickiness. And he says the new campaign is a good reminder that suggestive words or phrases found hiding in malicious code aren't necessarily smoking guns.

"A lot of these, as this malware illustrates, can be made up, and can lead you astray," he said.

More information: Blue Coat's report on "Inception": www.bluecoat.com/documents/dow … 0f-b89e-e40b2f8d2088