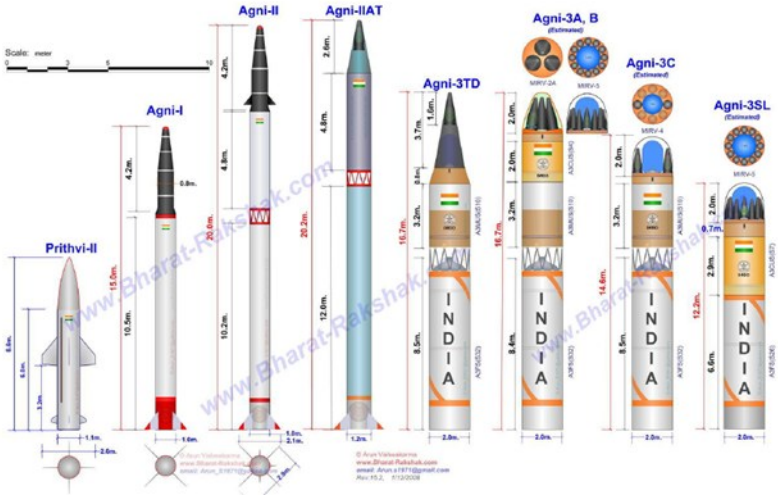
OPERATION HANGOVER | Executive Summary



Unveiling an Indian Cyberattack Infrastructure

This report details a sophisticated cyberattack infrastructure that appears to originate from India, conducted by private threat actors with no evidence of state-sponsorship. It has likely been in operation for over three years, primarily as a platform for surveillance against targets of national security interest that are mostly based in Pakistan and possibly in the United States. It is also used for industrial espionage against the Norwegian telecom corporation Telenor and other civilian corporations. Evidence points to professional project management and outsourcing of key tasks, including some by freelance programmers.

On March 17, 2013 a Norwegian newspaper reported that the country's telecommunications giant Telenor had filed a criminal police case for an unlawful computer intrusion. Spear phishing emails targeting upper management appeared to be the source of the infection

Through extensive analysis, security analysts at Norman Shark in conjunction with our partners, quickly uncovered a previously unknown and sophisticated infrastructure for targeted attacks.

norman

Cyberattack Objectives

The primary purpose of this long-running, global command-and-control network appears to be surveillance against national security interests. Private-sector industrial espionage in fields as diverse as natural resources, telecommunications, law, food & restaurants, and manufacturing is likely a secondary purpose of this network.

Target Selection

Based on analysis of IP addresses collected from criminal data stores discovered during the investigation, it appears that potential victims have been targeted in over a dozen countries, most heavily represented by Pakistan, Iran, and the United States. Targets include government, military, and civilian organizations

Highly-Targeted Social Engineering Tactics

Spear phishing to carefully-selected target individuals was the primary attack vector identified in the investigation. The attackers went to great lengths to make the social engineering aspects of the attack appear as credible and applicable as possible.

In many cases, decoy files and websites were used, specifically geared to the particular sensibilities of regional targets including cultural and religious subject matter. Victims would click on what appeared to be an interesting document, and begin the long-running infection cycle.

Exploit Tools and Techniques

Despite all of the recent media attention on so-called "zero-day" exploits encompassing brand new, never-before-seen attack methods, Operation Hangover appears to have relied exclusively upon well-known, previously identified vulnerabilities in Java, Word documents, and web browsers.

Favored methods include documents infected with malicious code, along with direction to malicious websites with names deliberately similar to legitimate government, entertainment, security related, and commercial sites. Often the user would be presented with a legitimate document or software download they were expecting to see, along with an unseen malicious download.

Infrastructure Development

Operation Hangover utilizes a very extensive and sophisticated command-and-control infrastructure, likely developed over many months or years by numerous developers. Our investigation revealed evidence of professional project management practices used to design frameworks, modules, and sub-components. Individual malware authors were assigned certain tasks, and components were "outsourced" to what appear to be freelance programmers.

Attribution of Responsibility

In recent months, much focus has been on China – including both state-sponsored and individual actors – but Operation Hangover contains notable hallmarks of originating exclusively in India. We base this attribution with a very high degree of confidence on our extensive analysis of IP addresses, website domain registrations, and text-based identifiers contained within the malicious code itself. All indications point to private syndicates of threat actors following their own motivations, with no direct evidence of state-sponsorship by the Indian government or by any other nation.

ATTACK OVERVIEW

. . .

Discovery of a security breach at Norway-based Telenor uncovered a long running, sophisticated global cyberattack infrastructure that likely continues to this day.

Cyberattack Objectives

- National security interests
- Industrial espionage

Target Selection

- Primarily Pakistani and US-based targets
- Business targets

Highly-Targeted Social Engineering Tactics

- Executables disguised as documents
- Malicious web downloads

Exploit Tools and Techniques

- Known vulnerabilities only
- No use of zero-day exploits

Infrastructure Development

- Evidence of professional project management
- Outsourcing of development

Attribution of Responsibility

- Individual actors likely based in India
- Private data security firms hired to build specific infrastructure components
- No evidence of state-sponsored activity

Contact information:

Gary Thompson, 925.768.2400
Tim Johnson, 415.385.9537
norman@claritycommunications.us

norman