China-based Cyber Attacks On US Military Are 'Advanced, Persistent And Ongoing': Report

SEP 17, 2015 @ 02:22 AM 3,776 VIEWS

Lisa Brownlee
CONTRIBUTOR

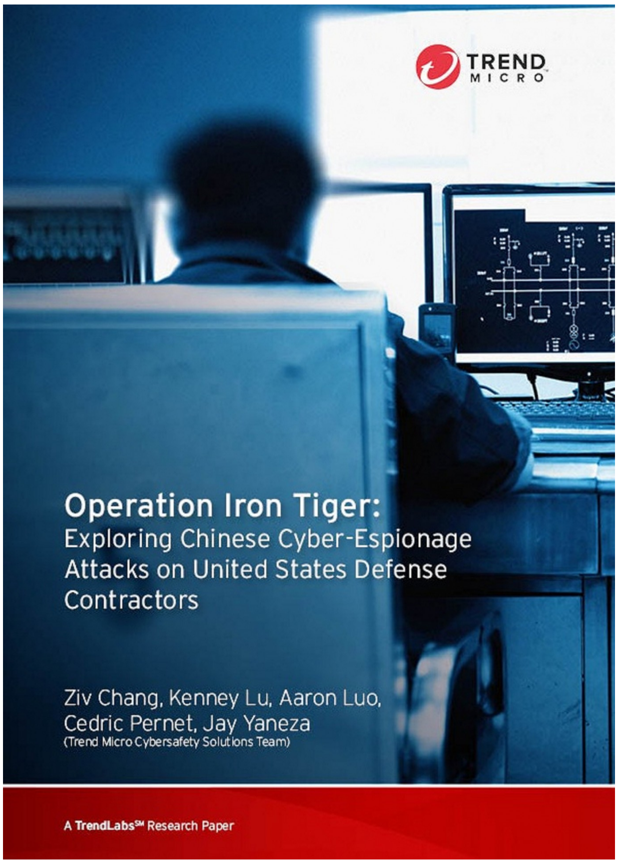
FOLLOW ON FORBES (8)

Opinions expressed by Forbes Contributors are their own.

FULL BIO

A high-level hacking group dubbed Iron Tiger has been observed stealing trillions of bytes of confidential data from the United States government, US defense contractors and related companies in the United States and abroad, security company Trend Micro reports in its research paper posted Tuesday, *Operation Iron Tiger: Exploring Chinese Cyber Espionage Attacks on U.S. Defense Contractors.*

Numerous U.S.-based security tech intensive companies were hacked and continuously monitored since 2013 until this year, Trend Micro reports. Dr. Ziv Chang, Sr. Director, Cyber Safety Solutions, Core Technology at Trend Micro and first author on the report, informed me by direct message (confirmed by email) that the attackers' aims to target very important persons, engineers, and public relations/communication officers was evidenced even as recently as February 17, 2015, when mail of a corporate strategic director at Westinghouse Electric Company was breached. Dr. Chang informed me that he believes that "China based Iron Tiger hacking group is a highly active, continuous advanced persistent threat that continues to attack the U.S."



TREND MICRO

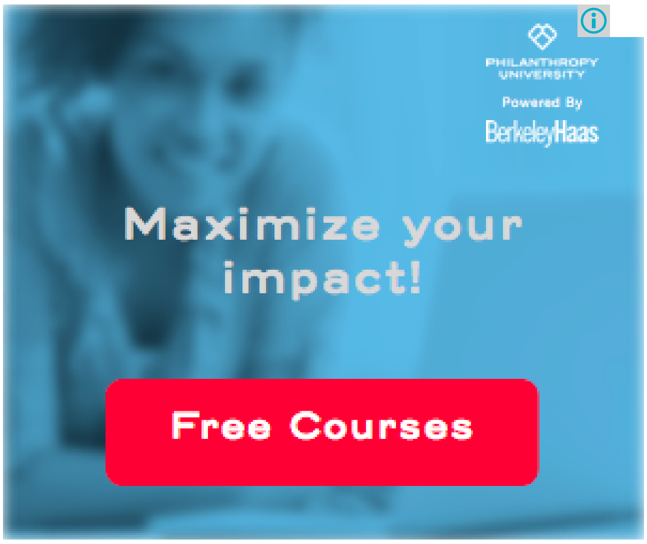
Operation Iron Tiger:
Exploring Chinese Cyber-Espionage Attacks on United States Defense Contractors

Ziv Chang, Kenney Lu, Aaron Luo,
Cedric Pernet, Jay Yaneza
(Trend Micro Cybersafety Solutions Team)

A TrendLabs℠ Research Paper

China based Iron Tiger hacking group is a highly-active, continuous advanced persistent threat that continues to attack the US.

In its blog announcing the paper, Trend Micro stated that "Operation Iron Tiger is a targeted attack campaign discovered to have stolen trillions of bytes of data from defense contractors in the U.S., including stolen emails, intellectual property, and strategic planning documents." The report further details that targets of Iron Tiger included military defense contractors, intelligence agencies, FBI-based partners, and the U.S. government. The private entities were tech-based government contractors in the electric, aerospace, intelligence, telecommunications, energy, and nuclear engineering industries.



Iron Tiger was observed exfiltrating up to 58GB worth of data from a single target, more than was stolen in the Sony attack. It could have potentially stolen up to terabytes of data in total, Trend Micro reports. It is highly environmentally adaptive and otherwise sophisticated and well organized, potentially merely an arm of a larger, multi-teamed operation with various targets.

China is convincingly Iron Tiger's home base

The primary situs of China as the operatives' home base was convincingly evidenced by the facts that the operatives used virtual private network (VPN) servers that only accepted China-based registrants, used Chinese file names and passwords, and operated from China-registered domains, according to the report. Some of Iron Tiger's actions were also attributed Iron to an individual physically located in China.

Iron Tiger transformed from Emissary Panda in huge geographical and target shift

Iron Tiger is believed to be a transformation of a hacking group known since 2010 as Threat Group 3390 or “Emissary Panda.” The threat actors shifted their focus from east Asian political targets to United States government and defense industry targets. “The actors have stolen emails, full Active Directory dumps, intellectual property, strategic planning documents, and budget- or finance-related content—all of which can be used to sabotage target governments’ or private organizations’ plans,” the report states.

Update Sept 17, 2015 04:00 EDT: This report comes less than week before high-level US-China diplomatic meetings including China President Xi’s first state visit. It also follows intense private cyber security meetings that concluded with the Obama administration indicating that it would hold off on previously-threatened cyber sanctions.

PAGE 1 / 2 Continue >

Comment on this story

✎ Report Corrections

Reprints & Permissions

SEE ALSO

UNITED	MILITARY
GO ARMY	TOP
US	ARMY
US	MILITARY