Iron Tiger: How hackers have stolen terabytes of confidential data from US high-tech firms

(HTTP://WWW.TRIPWIRE.COM/STATE-OF-SECURITY/CONTRIBUTORS/GRAHAM-CLULEY/)

GRAHAM CLULEY (HTTP://WWW.TRIPWIRE.COM/STATE-OF-SECURITY/CONTRIBUTORS/GRAHAM-CLULEY/)

SEP 17, 2015 |

IT SECURITY AND DATA PROTECTION (HTTP://WWW.TRIPWIRE.COM/STATE-OF-SECURITY/TOPICS/SECURITY-DATA-PROTECTION/)

(http://www.tripwire.com/state-of-security/security-data-protection/iron-tiger-data-us-firms/)

A new report claims that in 2013, a group of China-based hackers switched their attention from targeting victims in Asia-Pacific to stealing terabytes of confidential data from US high-tech firms and government contractors.

The report, “Operation Iron Tiger: Exploring Chinese Cyber-Espionage Attacks on United States Defense Contractors” (http://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/operation-iron-tiger-chinese-cyber-espionage-attacks-on-us-defense-contractors), claims that a hacking gang named “Emissary Panda” (where do security firms get these names from?) initially launched a cyberespionage campaign in 2010, spying on politicians and government agencies in China, Hong Kong, the Philippines and Tibet.

However, two years ago, the campaign dubbed “Iron Tiger” is said to have shifted its sights to US government contractors working in the aerospace, energy, intelligence, telecoms and nuclear industries.

Researchers at Trend Micro have described the hacking group as “highly competent and sophisticated”, claiming that up to 58 GB worth of data was stolen just from a single target.

In all, terabytes of confidential data has potentially been exfiltrated by the attackers, who have abused legitimate services such as Blogspot and the Google Cloud Platform to aid them in their criminal endeavours.

A key component of attacks launched as part of the Iron Tiger campaign are targeted spear-phishing emails, zeroing-in on government officials, executives, engineers and PR teams, often using names that are likely to pique the interest of the recipient, such as the BBC or AFP news agencies.

Although sometimes generic subject lines are used in the emails, other times professional or personal subjects are chosen – depending on what the attacker feels might work best with their targeted victim. Samples of subject lines include "Shanghai mayor Han Zheng visits Taipei to promote World Expo," "Han Zheng stays at Regent Pan—Housing protest held in advance," and "Sino-US cooperation on maritime security seminar neighborhoods."

And it may not even be obvious that the email is malicious, as in some cases there is no visible evidence of a malicious link or attachment to the casual observer.

In the above example, for instance, a "web bug" hidden image embedded inside the email won't be seen by many users – but is scooping up information about the recipient's IP address, operating system and browser details. Other emails may contain obfuscated code that runs remote scripts on the targeted computer.

Although attribution in internet attacks is always a tricky area, the report concludes that those involved are Chinese based upon a number of factors:

- The VPN servers were mostly located in China like those provided by BAIGE VPN.
- The file names and passwords used were Chinese.
- Some text resources and language IDs used in malware binaries were set to simplified Chinese.
- HUC Packet Transmit Tool (HTran) is frequently used by Chinese threat actors.
- Whois data revealed that related domains like shangxian.info were registered with physical addresses in China.
- The other related resources (QQ, Lofter, 163.com) are popularly used in China.

But Trend Micro goes further than that, claiming to have identified a man named Guo Fei, who resides in Shanghai, as a key member of the gang's operations team – after investigating various virtual aliases related to the Iron Tiger campaign.

Whoever might be responsible for the Iron Tiger cyberespionage campaign, one thing is certain. Government organisations and companies need to do everything in their power to reduce the chances of a successful attack, deploying a layered defence to protect their systems rather than relying upon a single solution.

If you want to catch the Iron Tiger before it causes you any harm, it makes sense to build a series of traps.

CATEGORIES Featured Articles (http://www.tripwire.com/state-of-security/topics/featured/), IT Security and Data Protection (http://www.tripwire.com/state-of-security/topics/security-data-protection/)

TAGS China (http://www.tripwire.com/state-of-security/tag/china/), Iron Tiger (http://www.tripwire.com/state-of-security/tag/iron-tiger/), malware (http://www.tripwire.com/state-of-security/tag/malware/)

COMMENTS

Login

There are no comments posted yet. Be the first one!

POST A NEW COMMENT

Enter text right here!

Comment as a Guest, or login:

NAME

Displayed next to your comments.

EMAIL

Not displayed publicly.

WEBSITE (OPTIONAL)

If you have a website, link to it here.

Subscribe to

None

Submit Comment

About Graham Cluley

(http://www.tripwire.com/state-of-security/contributors/graham-cluley/)

Graham Cluley (http://www.tripwire.com/state-of-security/contributors/graham-cluley/) has contributed 52 posts to The State of Security.

View all posts by Graham Cluley (http://www.tripwire.com/state-of-security/contributors/graham-cluley/) >

Follow @gcluley

Latest Security News (/state-of-security/topics/latest-security-news/)

Banks Allowed to Bring Class Action Suit Against Target for 2013 Breach SEP 17, 2015

Over 21 Million New Types of Malware Created in Q2 2015, Report Finds SEP 16, 2015

Russian Hacker Pleads Guilty to Stealing 160M Credit Cards SEP 16, 2015

DHS Forces Public Library to Shut Down Tor Exit Relay SEP 15, 2015

Report: Cyber Insurance Market Expected to Reach $7.5 Billion By 2020 SEP 14, 2015

POPULAR | FEATURED | RECENT

(http://www.tripwire.com/state-of-security/security-data-protection/cyber-security/most-suspicious-tlds-revealed-by-blue-coat-systems/)

Most Suspicious TLDs Revealed by Blue Coat Systems (http://www.tripwire.com/state-of-security/security-data-protection/cyber-security/most-suspicious-tlds-revealed-by-blue-coat-systems/)

SEPTEMBER 13, 2015

(http://www.tripwire.com/state-of-security/latest-security-news/excellus-bluecross-blueshield-hacked-over-10-million-members-affected/)

Excellus BlueCross BlueShield Hacked, Over 10 Million Members Affected (http://www.tripwire.com/state-of-security/latest-security-news/excellus-bluecross-blueshield-hacked-over-10-million-members-affected/)

SEPTEMBER 10, 2015

(http://www.tripwire.com/state-of-security/latest-security-news/fireeye-filed-injunction-against-security-firm-to-protect-intellectual-property/)

FireEye Filed Injunction Against Security Firm to Protect Intellectual Property (http://www.tripwire.com/state-of-security/latest-security-news/fireeye-filed-injunction-against-security-firm-to-protect-intellectual-property/)

SEPTEMBER 11, 2015

(http://www.tripwire.com/state-of-security/security-data-protection/cyber-security/sakawa-scams-spread-to-the-uk/)

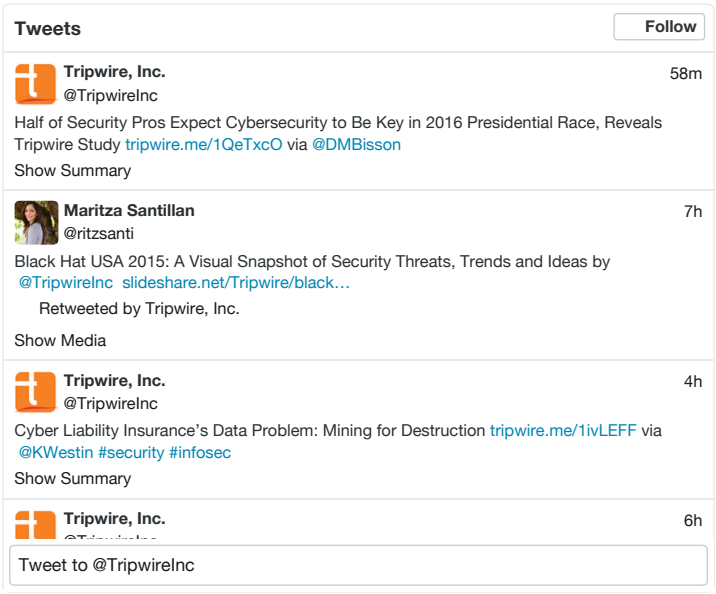
Sakawa Scams Spread to the UK (http://www.tripwire.com/state-of-security/security-data-protection/cyber-security/sakawa-scams-spread-to-the-uk/)

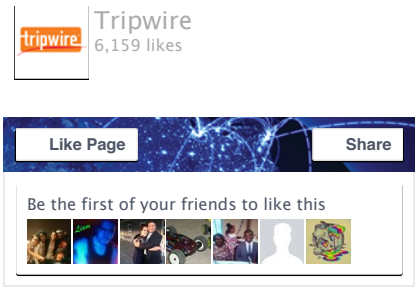
SEPTEMBER 10, 2015

Will Quantum Computers Threaten Modern Cryptography? (http://www.tripwire.com/state-of-security/featured/will-quantum-computers-threaten-modern-cryptography/)

SEPTEMBER 14, 2015

(http://www.tripwire.com/state-of-security/featured/will-quantum-computers-threaten-modern-cryptography/)





Topics (/state-of-security/topics/)

- Government
- Incident Detection
- IT Security and Data Protection
- Latest Security News
- Off Topic
- Regulatory Compliance
- Risk-Based Security for Executives
- Security Awareness
- Security Slice
- This Week in Security
- Tripwire News
- Vulnerability Management

FOLLOW US