Tropic Trooper APT targets Taiwanese Government and companies in the energy sector

November 23, 2016 By Pierluigi Paganini

The Tropic Trooper APT continues to target Asia, this time government Taiwanese organizations and companies in the energy sector.

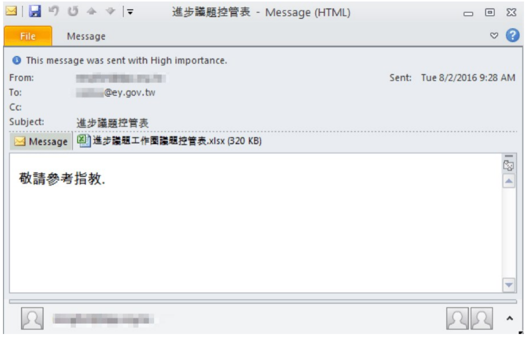
The Tropic Trooper APT that has been active at least since 2012, it was first spotted last year by security experts at Trend Micro when it targeted government ministries and heavy industries in Taiwan and the military in the Philippines.

Now researchers from Palo Alto Networks targeted the secretary general of Taiwan's Executive Yuan and a fossil fuel provider with a strain of malware called Yahoyah. The attackers leverage an exploit for the CVE 2012-0158 vulnerability, the same flaw was exploited by many other APT groups, including Lotus Blossom, NetTraveller, and The Four Element Sword ATP.

Palo Alto Networks discovered that the group used Poison Ivy for his campaigns, a circumstance that emerged in the analysis of TrendMicro.

"The attacks in this case are associated with a campaign called Tropic Trooper, which has been active since at least 2011 and is known for heavily targeting Taiwan. One of the attacks used their known Yahoyah malware, but the other attack deployed the widely available Poison Ivy RAT." state the ***report*** *published by Palo Alto Networks. "This confirms the actors are using Poison Ivy as part of their toolkit, something speculated in the original Trend Micro report but not confirmed by them. Further analysis uncovered a handful of ties indicating the actors may also be using the PCShare malware family, which has not been previously tied to the group."*

The hackers launched a spear-phishing campaign to trick victims into opening specially crafted decoy documents. The Excel file sent to the Executive Yuan purports to come from a staff member at the Democratic Progressive Party, the document is related to political issues.



This message was sent with High importance.

From: [redacted]

Sent: Tue 8/2/2016 9:28 AM

To: [redacted]@ey.gov.tw

Cc:

Subject: 進步議題控管表

Message 進步議題工作團議題控管表.xlsx (320 KB)

敬請參考指教.

[redacted]

After infecting the target machine, the malware displays to the victim a clean document that contains the content of interest.

"All of the text uses Traditional Chinese, in contrast to Simplified Chinese, which is the official written language of the People's Republic of China. Traditional Chinese is used in Taiwan, Hong Kong, Macau, and many overseas Chinese communities. The overarching theme of the spreadsheet is documenting protestor activity and/or progressive reform attempts in progress across Taiwan and the tone of the spreadsheet suggests it was compiled by progressive supporters." continues the report.

If you are interested in more info on Tropic Trooper APT, including IoC for its malware give a look at the report.

Pierluigi Paganini

(Security Affairs – Tropic Trooper APT, cyber espionage)

Share this...

SHARE ON

Pierluigi Paganini

Pierluigi Paganini is member of the ENISA (European Union Agency for Network and Information Security) Threat Landscape Stakeholder Group and Cyber G7 Group, he is also a Security Evangelist, Security Analyst and Freelance Writer. Editor-in-Chief at "Cyber Defense Magazine", Pierluigi is a cyber security expert with over 20 years experience in the field, he is Certified Ethical Hacker at EC Council in London. The passion for writing and a strong belief that security is founded on sharing and awareness led Pierluigi to find the security blog "Security Affairs" recently named a Top National Security Resource for US. Pierluigi is a member of the "The Hacker News" team and he is a writer for some major publications in the field such as Cyber War Zone, ICTTF, Infosec Island, Infosec Institute, The Hacker News Magazine and for many other Security magazines. Author of the Books "The Deep Dark Web" and "Digital Virtual Currency and Bitcoin".

PREVIOUS ARTICLE
Credit cards stolen from Madison Square Garden venues in the last year

NEXT ARTICLE
Registral Function of the State Mexico (FREM) hacked. Shad0wS3C is back

Back to top