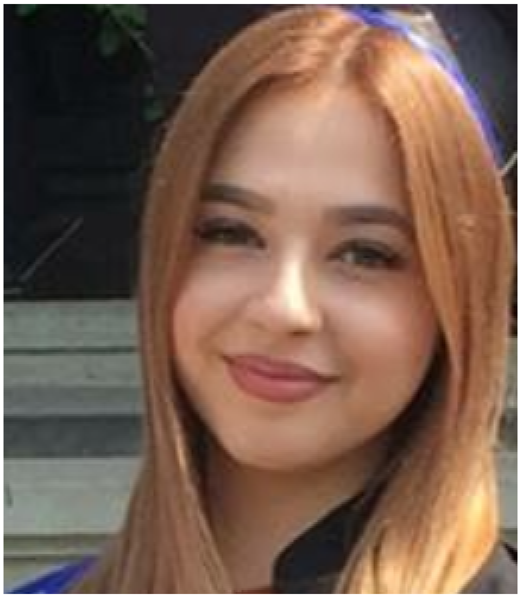
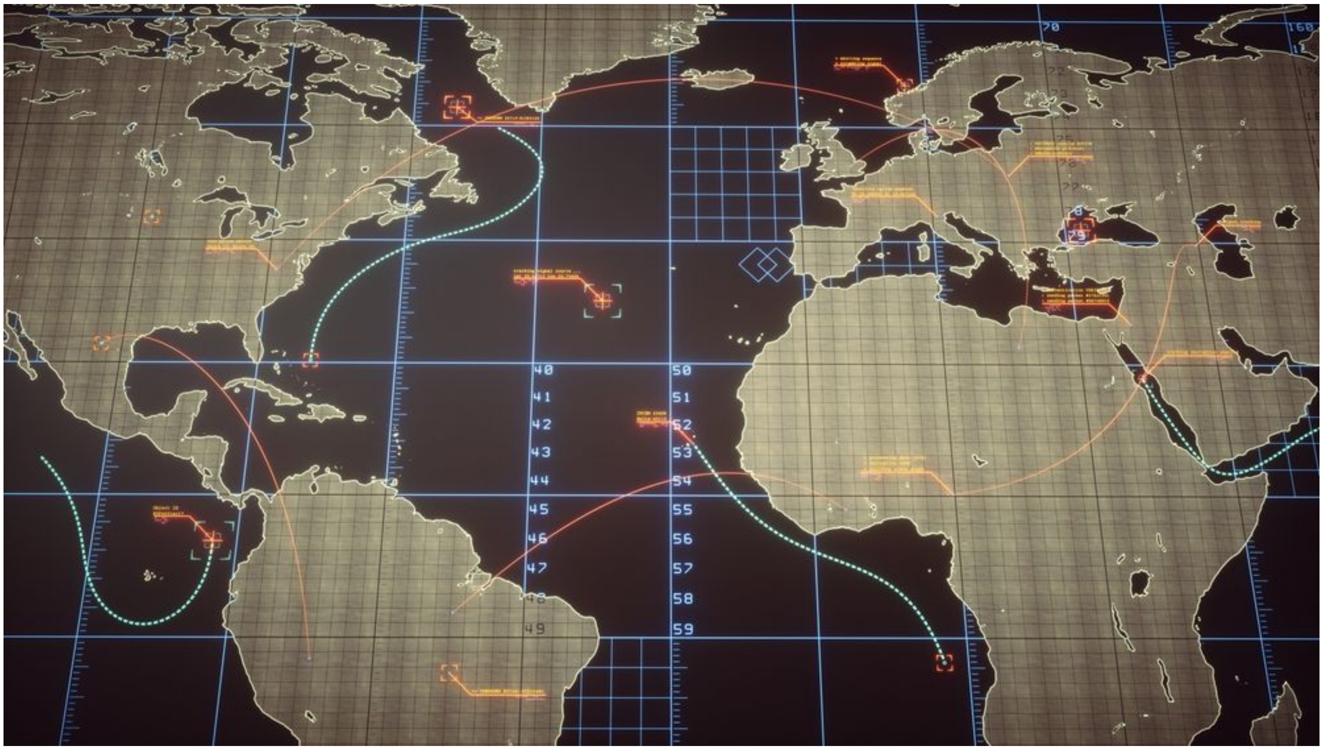
Operation PZChao: a possible return of the Iron Tiger APT

labs.bitdefender.com/2018/02/operation-pzchao-a-possible-return-of-the-iron-tiger-apt/



Ivona Alexandra CHILI

February 01, 2018



More than 30 years after the end of the Cold War, digital infrastructures worldwide have become strategic national fronts with the same importance as the geographical frontiers of air, land, sea and space.

To ensure viability in this fifth domain, cyber-attacks are growing in complexity as threat actors divide payloads in multiple modules with highly specialized uses to achieve a target's compromise. The past few years have seen high-profile cyber-attacks shift to damaging the targets' digital infrastructures to stealing highly sensitive data, silently monitoring the victim and constantly laying the ground for a new wave of attacks.

This is also the case of a custom-built piece of malware that we have been monitoring for several months as it wrought havoc in Asia. Our threat intelligence systems picked up the first indicators of compromise in July last year, and we have kept an eye on the threat ever since.

An interesting feature of this threat, which drew our team to the challenge of analyzing it, is that it features a network of malicious subdomains, each one used for a specific task (download, upload, RAT related actions, malware DLL delivery). The payloads are diversified and include capabilities to download and execute additional binary files, collect private information and remotely execute commands on the system.

In the analysis process, we managed to retrieve the malware payloads hosted on one of the command and control servers along with some statistics, such as the total number of downloads and logs containing the targeted victims. Among the most-downloaded malicious files, we found variants of Gh0st RAT used in Iron Tiger APT operation [more information about Iron Tiger is available in a research paper published by TrendMicro]. Interestingly enough, these new samples now connect to the new attack infrastructure.

This whitepaper takes an in-depth look at the the attack chain, the infrastructure used by the threat actors, the malware subdomains they control and the payloads delivered on the targeted systems, as well as other telltale signs about a possible return of the Iron Tiger APT.

Download the whitepaper

TAGS

anti-malware research whitepapers

AUTHOR

er Threat Intelligence Lab at Bitdefender. I have recently
e Alexandru Ioan Cuza University in Iasi.