Operation Wilted Tulip – Exposing a Cyber Espionage Apparatus – ClearSky Cyber Security

Published: 2017-07-25 · Archived: 2026-04-06 02:10:53 UTC

CopyKittens is a cyberespionage group that has been operating since at least 2013. In November 2015, ClearSky and Minerva Labs published the first public report exposing its activity [1]. In March 2017, ClearSky published a second report exposing further incidents, some of which impacted the German Bundestag [2].

In this report, Trend Micro and ClearSky expose a vast espionage apparatus spanning the entire time the group has been active. It includes recent incidents as well as older ones that have not been publicly reported; new malware; exploitation, delivery and command and control infrastructure; and the group's modus operandi. We dubbed this activity **Operation Wilted Tulip.**

Targetting

CopyKittens is an active cyber espionage actor whose primary focus appears to be foreign espionage on strategic targets. Its main targets are in countries such as Israel, Saudi Arabia, Turkey, The United States, Jordan, and Germany. Occasionally individuals in other countries are targeted as well as UN employees.

Targeted organizations include government institutions (such as Ministry of Foreign Affairs), academic institutions, defense companies, municipal authorities, sub-contractors of the Ministry of Defense, and large IT companies. Online news outlets and general websites were breached and weaponized as a vehicle for watering hole attacks.

For example, a malicious email was sent from a breached account of an employee in the Ministry of Foreign Affairs in the Turkish Republic of Northern Cyprus, trying to infect multiple targets in other government

organizations worldwide. In a different case, a document likely stolen from the Turkish Ministry of Foreign affairs was used as decoy. In other cases, Israeli embassies were targeted, as well as foreign embassies in Israel.

Victims are targeted by watering hole attacks, and emails with links to malicious websites or with malicious attachments. Fake Facebook profiles have been used for spreading malicious links and building trust with targets. Some of the profiles have been active for years.

Malware

CopyKittens use several self-developed malware and hacking tools that have not been publicly reported to date, and are analyzed in this report: TDTESS backdoor; Vminst**,** a lateral movement tool; NetSrv, a Cobalt Strike loader; and ZPP, a files compression console program. The group also uses Matryoshka v1, a self-developed RAT analyzed by ClearSky in the 2015 report, and Matryoshka v2 which is a new version, albeit with similar functionality.

The group often uses the trial version of Cobalt Strike, a publicly available commercial software for "Adversary Simulations and Red Team Operations." Other public tools used by the group are Metasploit, a well-known free and open source framework for developing and executing exploit code against a remote target machine; Mimikatz, a post-exploitation tool that performs credential dumping; and Empire, "a PowerShell and Python post-exploitation agent." For detection and exploitation of internet-facing web servers, CopyKittens use Havij, Acunetix and sqlmap.

A notable characteristic of CopyKittens is the use of DNS for command and control communication (C&C) and for data exfiltration. This feature is available both in Cobalt Strike and in Matryoshka.

Most of the infrastructure used by the group is in the U.S., Russia, and The Netherlands. Some of it has been in use for more than two years.

Read the full report: Operation Wilted Tulip
Indicators of compromise: indicators-wilted_tulip.csv (also available on PassiveTotal)
Yara rules: yara-apt_wilted_tulip.txt (courtesy of Florian Roth)
Samples: Live samples can be downloaded from the following link: https://ln.sync[.]com/dl/f6772eb20/d8yt6kez-9q7eef3m-ai27ebms-8zcufi5f (Please email info@clearskysec.com to get the password.)

Acknowledgments

This research was facilitated by PassiveTotal for threat infrastructure analysis, and by MalNet for malware research.

[1] https://www.clearskysec.com/report-the-copykittens-are-targeting-israelis/
[2] https://www.clearskysec.com/copykitten-jpost/
