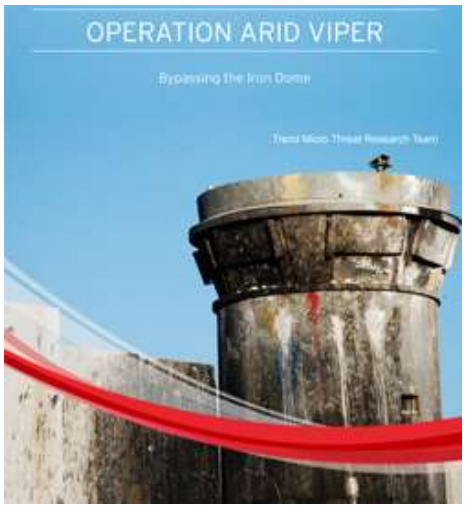
Operation Arid Viper: Bypassing the Iron Dome

16 de febrero de 2015



View research paper

strong Arab ties possibly located in the Gaza Strip. The first operation, Operation Arid Viper, is responsible for highly targeted cyber attack against five Israeli-based organizations (government, transport/ infrastructure, military, academia, and transport) and one organization based in Kuwait. The threat actors behind this operation have shown the capability to employ sophisticated attacks on key individuals with the goal of exfiltrating sensitive and confidential data, and it is believed that the operation has been ongoing since mid-2013.

While monitoring the C&C infrastructure (hosted in Germany) it connects to, our researchers found another operation, Advtravel led by Egyptian hackers. Our investigation reveals that these Egyptian hackers seem to be particularly interested in the images stored in its victim's machine. We can surmise that they are looking for incriminating or compromising images for blackmail purposes. Unlike the threat actors of Operation Arid Viper, the motivation of the group behind operation Advtravel is neither financial nor espionage-related. Interestingly, when we checked advtravel[dot]info, the attacker has left the directory structure of the server completely open to the public. This leads us to believe that the attackers behind Advtravel have less technical knowledge and is attacking other Egyptians in less purposeful attacks.

Infection Chains for Operation Arid Viper and Advtravel

A spear phishing email was used as a delivery mechanism by Operation Arid Viper that contained an email attachment. The said attachment has a .RAR file that automatically extracts an .SCR file that drops two files when executed.

The first file is a pornographic video clip, which serves as a social engineering bait while the second file is the actual malware connecting to the C&C servers. Once the second-stage malware is in the system, it sets itself to autorun each time the systems reboot, even posing as an Internet communication software. In addition, the other C&C servers have been hosted in IP addresses

.

Although the malware involved in operation Advtravel is different from that of Operation Arid Viper, both operations still have a few similarities, such as sharing the same server and having the domains used in Advtravel registered with the same emails as the Operation Arid Viper. Notably, the same server and site registration details suggest the existence of a supra-organization, a forum or an influential sponsor could be providing various hacking groups with the means to pursue their ends.

Aside from the technical details of both campaigns and its targets, the research paper **Operation Arid Viper: Bypassing the Iron Dome** also discusses the attribution or details on certain individuals that seem to be tied to these campaigns.

[Read: **Arid Viper: Gaza vs Israel Cyber Conflict**]

Publicado en Cyber Attacks, Research, Targeted Attacks

Artículos Relacionados

- Exposing Earth Berberoka: A Multiplatform APT Campaign Targeting Online Gambling Sites
- The Far-Reaching Attacks of the Void Balaur Cybermercenary Group
- Zloader Campaigns at a Glance
- Earth Baku Returns: Uncovering the Upgraded Toolset Behind the APT Group's New Cyberespionage Campaign
- Cambiando el rumbo: Predicciones de seguridad de Trend Micro para 2021

Artículos Recientes

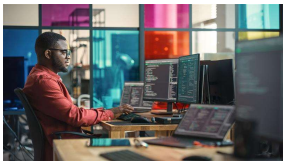
- Distributed Energy Generation Gateway (In)Security
- Threat Modeling API Gateways: A New Target for Threat Actors?
- Rising Security Weaknesses in the Automotive Industry and What It Can Do on the Road Ahead

Nosotros recomendamos

MQTT and M2M: Do You Know Who Owns Your Machine's Data?

Addressing CAPTCHA-Evading Phishing Threats With Behavior-Based AI Protection

A Deep Dive into the Packet Reflection Vulnerability Allowing Attackers to Plague Private 5G Networks



Understanding the Kubernetes Security Triad: Image Scanning, Admission Controllers, and Runtime Security

Mining Through Mountains of Information and Risk: Containers and Exposed Container Registries

Exposed Container Registries: A Potential Vector for Supply-Chain Attacks

Ransomware Spotlight: Trigona

Ransomware Spotlight: Akira

LockBit, BlackCat, and Clop Prevail as Top RAAS Groups: Ransomware in 1H 2023

Alexa and Google Home Devices can be Abused to Phish and Eavesdrop on Users, Research Finds

Mirai Variant Spotted Using Multiple Exploits, Targets Various Routers

A Look Into the Most Noteworthy Home Network Security Threats of 2017

2024 is poised to be a hotbed for new challenges in cybersecurity as the economic and political terrains continue to undergo digitization and enterprises increasingly leverage artificial intelligence and machine learning (AI/ML), the cloud, and Web3 technologies.
View the 2024 Trend Micro Security Predictions

Trend Micro 2023 Midyear Cybersecurity Threat Report

from behaviors and patterns observed in the threat landscape to stay ahead and prepare for risks in the second half of the year.

View the report

Empresas