ON2IT AND AMS-IX PRESENT: THREAT TALKS

Threat Talks
Advanced Persistent Threats

The silent threats behind major breaches

What if a cyberattack could stay hidden in your systems for months without a trace? What if it wasn't just about stealing data, but gaining long-term access and control? These are the questions that define Advanced Persistent Threats, or APTs.

APTs are not your average cyber threats. They're highly targeted, stealthy, and often backed by nation-states. Instead of quick attacks, APTs are designed for long-term infiltration. Threat actors behind these campaigns use a mix of social engineering, zero-day exploits, and built-in system tools to breach defenses and quietly maintain access.

These groups typically aim at high-value targets–government bodies, energy infrastructure, defense contractors, and major enterprises–seeking sensitive data or positioning themselves for future disruptions. APTs are also a key tool in cyber-espionage and geopolitical conflict.

71%
of APT attacks target **the public sector and critical infrastructure**

Source: IBM X-Force Threat Intelligence Index 2024

211
the average dwell time for an APT attack is **211 days**

Source: Mandiant M-Trends 2023 Report

43%
of APTs use **stolen credentials** as their **initial access vector**

Source: Verizon Data Breach Investigations Report 2023

150
at least **150 distinct APT groups** are being tracked globally by threat intelligence analysts

Source: MITRE ATT&CK

APT Handala

Anti-Israeli hacktivists

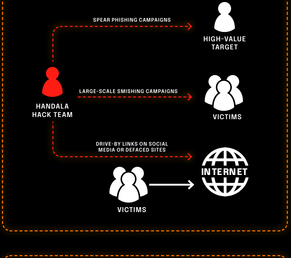
APT Handala, also known as the 'Handala Hack Team', is a politically motivated hacktivist group with a strong pro-Palestinian and anti-Israeli narrative. They are known for disruptive cyber operations including wiper malware attacks, data leaks, and website defacements.

mSOC condidence score	**Confirmed**
Threat category	**APTs Profiling**
Severity	**Nation-State**

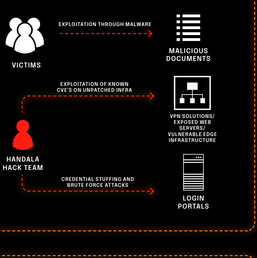
Attack Strategy	Evasion	Complexity	Target Type
Mostly relatively simplistic attacks like high volume phishing, SMS spam and spearphishing of high-value personnel in target organizations. They've also been observed exploiting known vulnerabilities	Custom phishing message content, often written in Hebrew/Arabic. Or malicious macros embedded in documents.	Medium	Israeli-backed (government) organizations

Attack vector	Detection	Threat level	Threat Actor Type
Publicly known personnel from target organizations, determined via various OSINT techniques.	Employee phishing awareness training. URL Filtering and endpoint protection.	Low	Politically Motivated Hacktivists

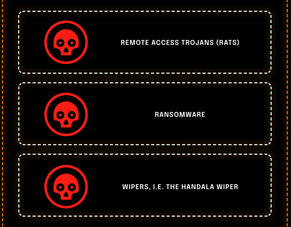
1 Delivery



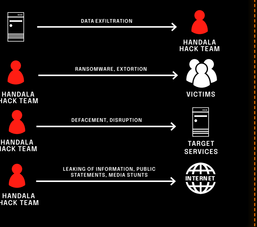
2 Exploitation



3 Installation



4 Act on Objectives



Delivery

1. Handala Hack Team targets personnel with spear phishing, smishing, or drive-by links on social media/defaced sites. Their phishing often uses macro-infected documents to install backdoors or ensure persistence.

M. User awareness campaigns, anti-spam, and mail security solutions are key defenses. Disabling scripting and macros on endpoints further reduces risk. Awareness training is especially effective against phishing.

Exploitation

2. The team exploits targets through phishing-delivered malware, unpatched CVEs, or credential stuffing/brute forcing. Malware is mainly used to access personal files for potential exfiltration, while the latter two methods typically target web servers for defacement.

M. Patch management, especially for edge infrastructure, is critical. Handala Hack Team hasn't used zero-days but exploits known vulnerabilities for access. Mail security and anti-spam solutions help block phishing-delivered malware.

Installation

3. Handala Hack Team typically deploys common trojans/RATs, sometimes slightly customized. They also use ransomware or wipers, including their own "Handala Wiper." RATs help them assess access to sensitive data for possible exfiltration.

M. EDR solutions on all endpoints are crucial to defend against ransomware, wipers, and data exfiltration. Network segmentation with Zero Trust strategies further protects the network if edge servers are compromised.

Acting on Objectives

4. Handala aims to harm targets' services or reputation, commonly through data exfiltration, ransomware, web defacement, public leaks, or endpoint wiping for disruption.

M. EDR/XDR on servers and endpoints defends against ransomware, wipers, and data exfiltration. Strict network policies, limiting outbound access from sensitive sources, further protect against data leaks.

threat-talks.com

ON2IT ZERO TRUST INNOVATORS

amsix

CONTACT US