WINDSHIFT_summit_archive_1554718868

WindShift APT: Insights and Analysis

TRAILS OF WINDSHIFT

TAHA KARIM –MALWARE SPECIALIST

1

A little bit about me

!

Currently I’m founder and CTO of tephracoreTechnologies

!

Malware Analysis for more than a decade.

!

Previously worked at : Dark Matter, FireEye, Symantec ...

!

Most known for: –

Uncovering LatentBotIn 2015

–

A major carding investigation in 2016

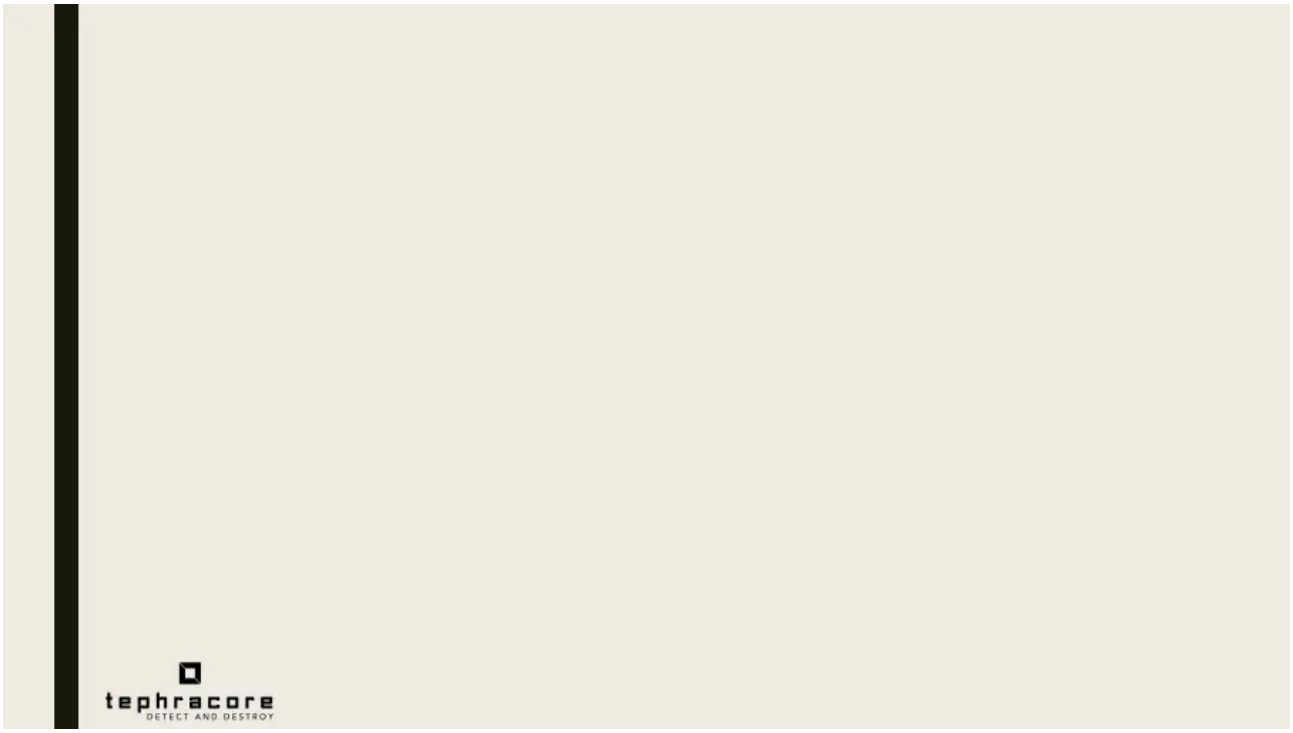
–

Multiple intelligence reports 2011-2019

–

Uncovering WindShiftAPT in 2018

2



A little bit about my company

!

In 2019, tephracoreTechnologies a cyber security startup was established in Dubai

!

With the purpose of raising the bar very high against threat actors (their job wont be easy anymore)

!

We are specialized in malware analysis, Incident Response, Vulnerability analysis, security testing, building APT deception frameworks, and red team assessments and malware analysis training courses.

!

We communicate via our technical blog see: https://tephracore.com/blog

3

Contents

!

!

Part 2: WINDSHIFT Modus Operandi

!

Part 3: WINDSHIFT Attribution

4

Part 1: APT Myths and Definitions

!

Does APT always means Advanced?

–

Case scenario: A target using unpatched Windows XP with no AV.

!

A very advanced toolset would be an overkill and comes with an unnecessary toolset exposure, whilst a simple toolset will get the job done most of the times.

!

Modern APT’s, Re-use of available tools, think copy-cat, evading attribution.

!

Simplicity always wins over complexity. Especially when time frames are shorts and/or budgets are limited.

5

Mitre Att&ck

From Scribd9 pages17 views

Mitre Att&ck

No ratings yet

Part 1: APT Myths and Definitions

6

OPSEC

EvasionEffectivenessUniquenessStealth

Success Rate

ExfiltrationReachPersistenceIntel

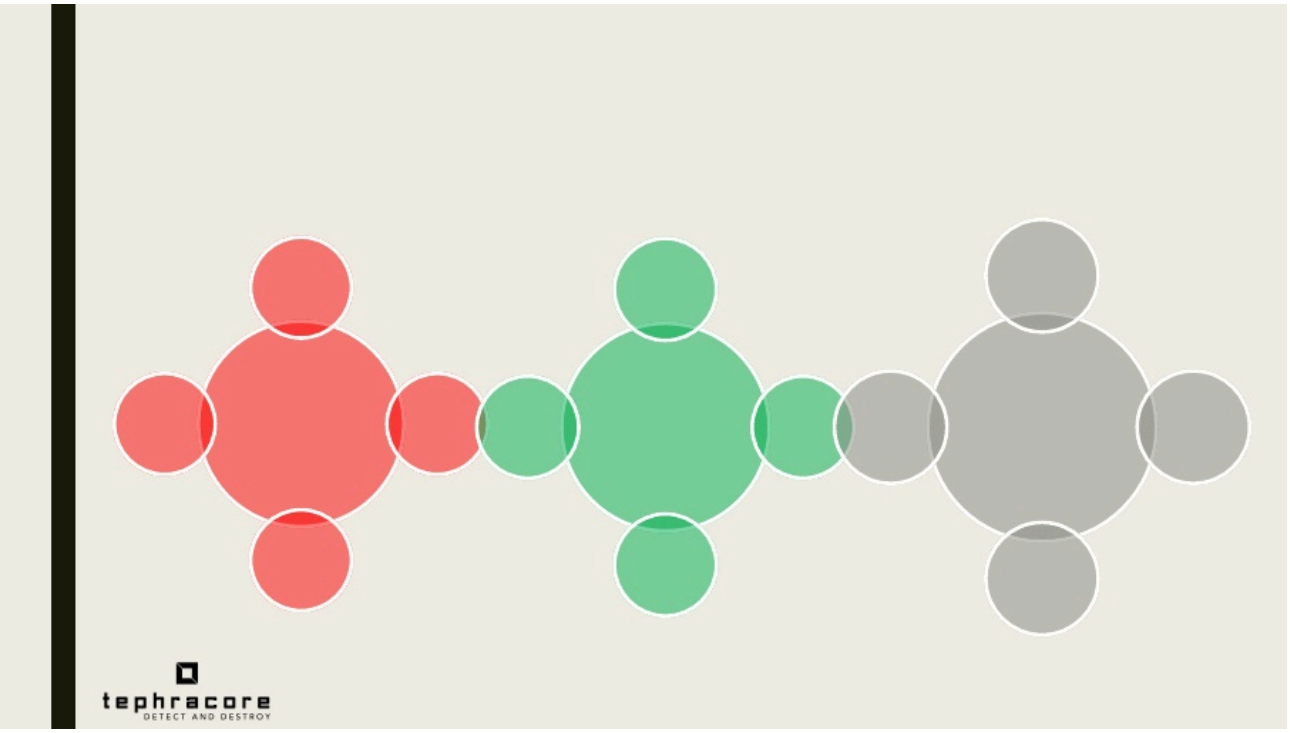
Detection

Counter measures

Predictability

AdaptabilityNoise

How to measure an APT skill level



OC1

OC1

No ratings yet