Pwned! (or not?)

The need for and effectiveness of Cyber Deception

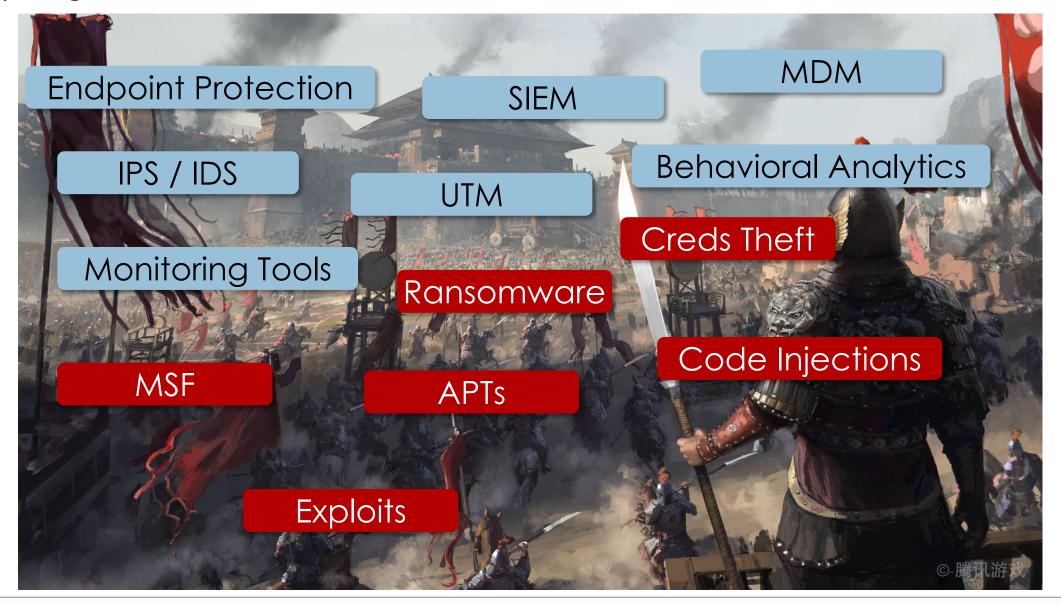
April 2019



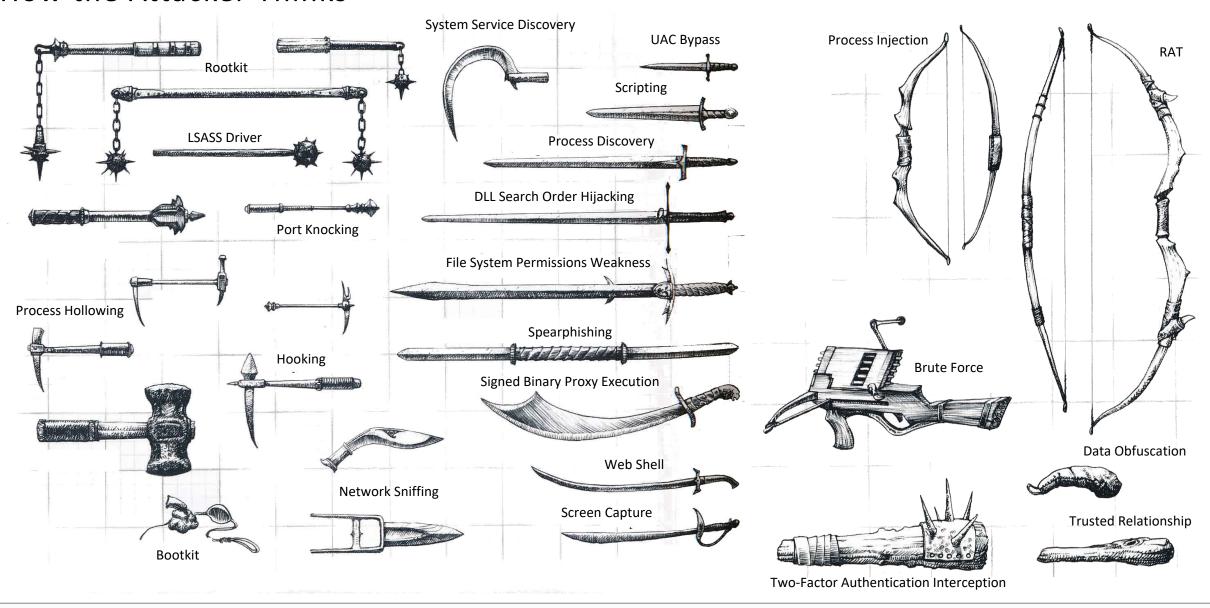




Every Single Network is a Battlefield



How the Attacker Thinks



How the Defender Thinks





The Attacker Tactics and Weapons

Recon

Gain Access

Escalate
Privileges

Persistence
Movement

Exfiltration

PRE-ATT&CK

- Priority Definition Planning
- Priority Definition Direction
- Target Selection
- Information Gathering
 - Technical
 - People
 - Organizational
- Weakness Identification
 - Technical
 - People
 - Organizational

- Adversary OPSEC
- Establish & Maintain Infrastructure
- Persona Development
- Capabilities
 - Build
 - Test
 - Stage

ATT&CK™

- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion

- Credential Access
- Discovery
- Lateral Movement
- Collection
- Exfiltration
- Command and Control

The Attacker Weak Points

Keep Cost Low (Expense vs Gain)

- Time
- Money
- Effort
- Resources

Hide Attack Details (Do not expose)

- Path
- Strategy
- Tactics
- Evidence



Deception: A key component in warfare

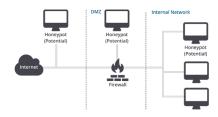






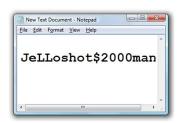
Cyber Deception Evolution





2016

Enterprise-Grade Deception Platforms



1990's Honeypots 2003 Honey tokens



2000

Honeynet



2012

Honeypot Scaling with Virtualization, Containers, Cloud, etc...





Illicium Cyber Deception Platform

- An original Neurosoft product
- From Scratch, not a modification of other software
- New software, not a stack of other tools
- Cooperation of three departments across two directorates:
 - Security Software Development
 - Cyber Security Services (Penetration Testers, Security Analysts)
 - ICT
 (System Administrators, Network Engineers)
- Mature (initiated in 2016)
- Installations in Major Companies (undisclosed)





Cyber Deception Platform

ILLI CIUM Features and Benefits

Functionality Features

- Full stack deception
- Attack Analysis
- Attacker Tracking
- Delay Attacker
- Detects attacks with very high confidence

Architectural Features

- Baits fully integrated to real systems
- Lightweight
- Full Simulation NO Emulation
- Isolation
- Custom Baits



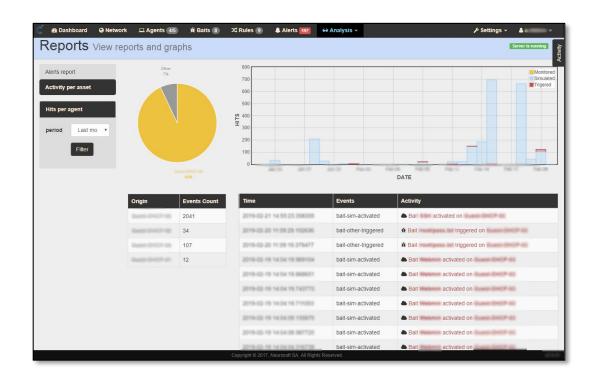


Identify <u>O-days</u>, <u>APTs</u>, and <u>Targeted Attacks</u>

Calculate <u>Attacking Trends</u>

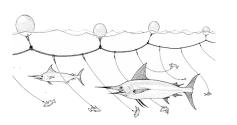
Assist on design of *Effective Defensive Measures*

Reduce <u>Detect and Response Times</u>



Deception Effectiveness is a Function of Maturity









Primitive

Free / Open Source

Academic Research

Basic logging

Emulates reality

No Customizations

Mostly Effective in Reconnaissance

Basic

Scalable

Based on baits

Customizable

Normal

Dynamically managed

deployment

Simulates reality

Forensics-enabled

Rules

Machine learning

Attack visualization

SIEM integration

Advanced

Control the attacker

Containment

More integrations...



Andreas Ntakas

Product Manager - Illicium

Email: a.ntakas@neurosoft.gr







NeuroSoft S.A.

466 Irakliou Ave. & Kiprou 141 22 Iraklio, Athens Greece

Neurosoft Analytics & Cyber Solutions Ltd.

5th floor 1 Connaught Place W22ET London United Kingdom

Neurosoft Cyprus Ltd.

2 Sophouli Street The Chanteclair House, 1096, Nicosia Cyprus

Rep Office UAE

Dubai Silicon Oasis, Headquarters PO Box 341568 Dubai, United Arab Emirates