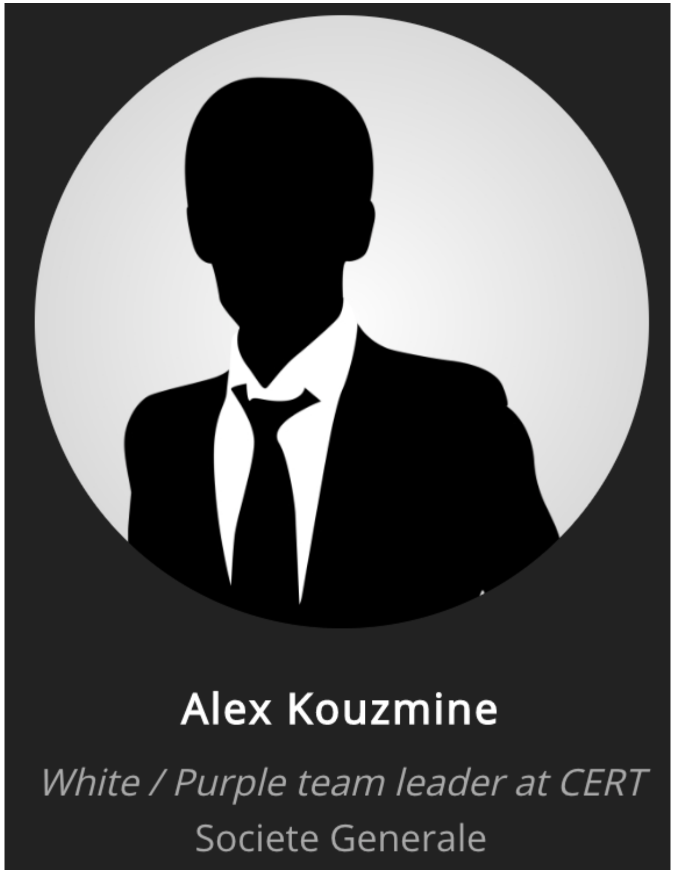
Let’s create a Readteam mission!

CERT

Societe Generale

whoami



Alex Kouzmine

White / Purple team leader at CERT

Societe Generale

CERT SOCIETE GENERALE

Who are WE

CERT | SOCIETE GENERALE

- 1st French Banking CERT team
- For the Entire Group
- Report to Group CISO
- Governed by a Group Instruction

RED TEAM

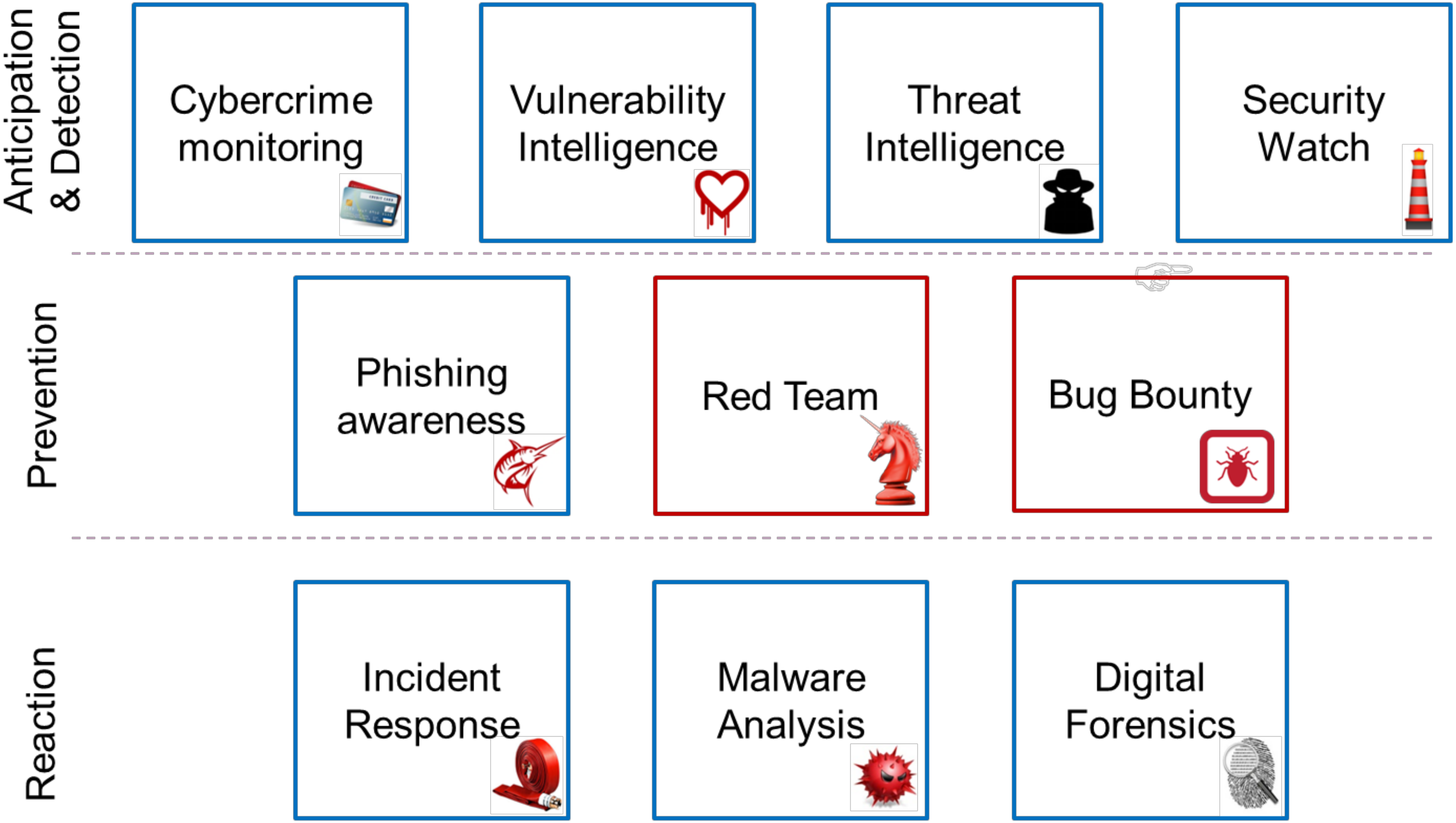
- Offensive Security Team
- For the Entire Group
- Report to Group CISO
- Mission by a sponsor

A team in charge of intelligence, detection and reaction on cyber security incidents

Purple team oversees both teams

A team to evaluate the maturity of your security controls and improve the abilities of Blue Team

Security Bricks



Anticipation & Detection

Cybercrime monitoring

Vulnerability Intelligence

Threat Intelligence

Security Watch

Prevention

Phishing awareness

Red Team

Bug Bounty

Reaction

Incident Response

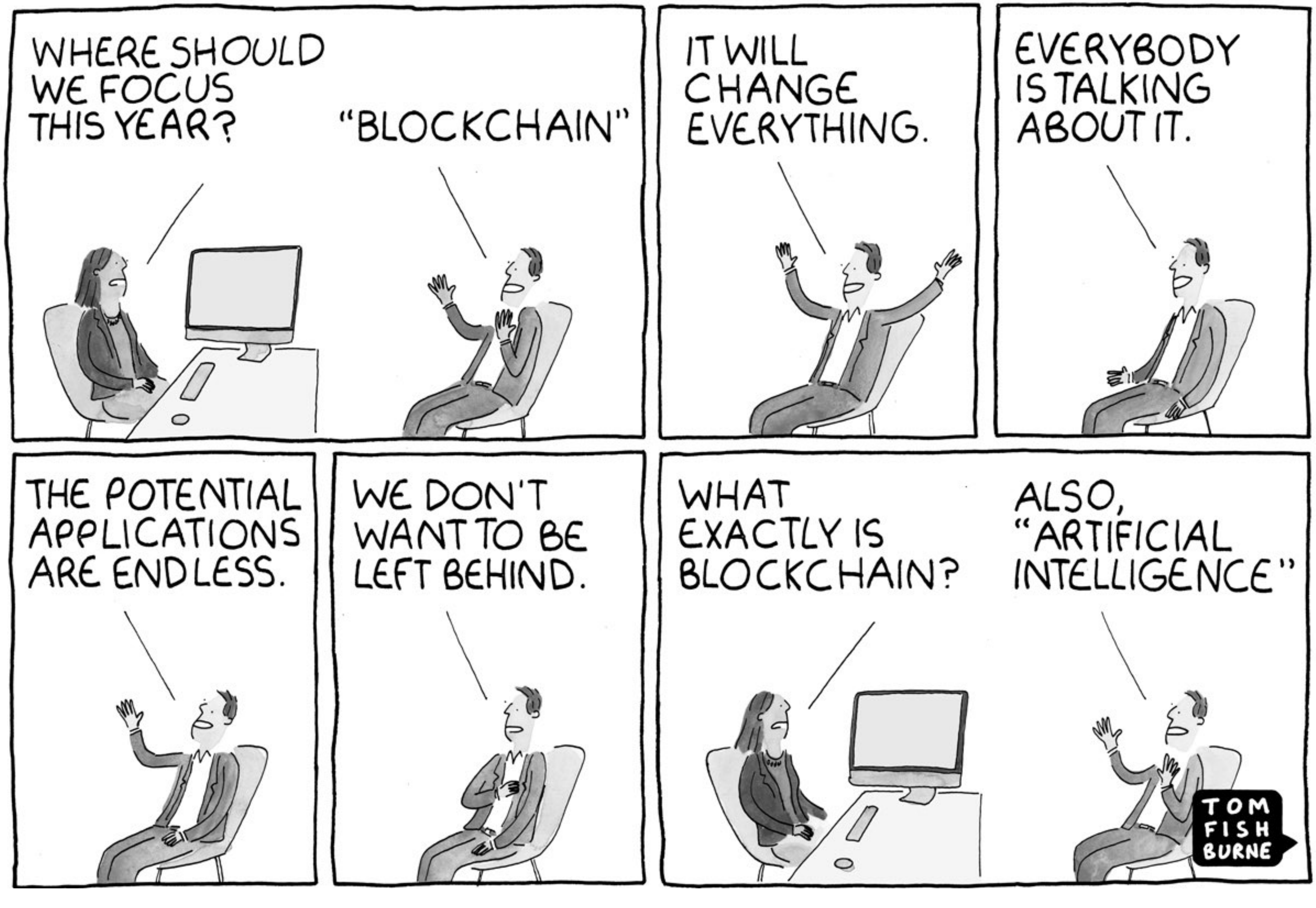
Malware Analysis

Digital Forensics

Why Redteaming?

The reasoning behind the implementation

It’s all about the

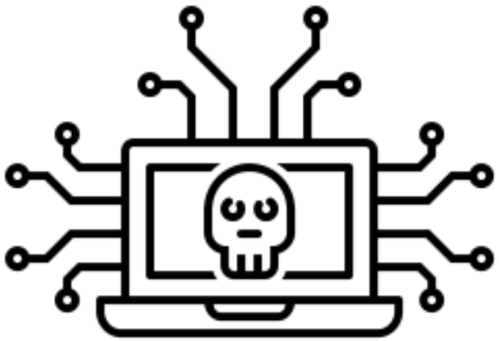

WHERE SHOULD WE FOCUS THIS YEAR?
"BLOCKCHAIN"
IT WILL CHANGE EVERYTHING.
EVERYBODY IS TALKING ABOUT IT.
THE POTENTIAL APPLICATIONS ARE ENDLESS.
WE DON'T WANT TO BE LEFT BEHIND.
WHAT EXACTLY IS BLOCKCHAIN?
ALSO, "ARTIFICIAL INTELLIGENCE"
TOM FISHBURNE

Why going Red?

To Make America Great Again

New Threats Bring Up New Needs

- Assess the maturity of your information system security make resilient to real-life threats;



- Introduce a decisional tool to anticipate and the worst and avoid it altogether!

« Your best enemy who wants you to get better »

-Sun Tsu

(could have come up with a slogan like that)

Pentest vs. Redteam

	PENTEST	REDTEAM
Objectives	**Vulnerabilities assessment**	**Test resilience against APT attackers**
Scope	•Limited and defined scope •Application only	•Large scope, better overview of the Group IT architecture •Continuous discovery/supervision of critical, exposed or attractive assets for attackers •Focus on incident detection and response
Mission duration	Short (1-2 weeks)	Long (1-3+ months)
Methodology	Static, predefined (OWASP…)	Focus on realistic scenarios Flexibility
Techniques	Discovery, active scan, exploitation	Tactics, Techniques and Procedures of known attackers (APT, cybercriminals)
Post-Exploitation	None or limited	Total, focus on the “price” to obtain
Periodicity	Integrated inside project life cycle	Tailored, out of project life

Trophies for Awareness

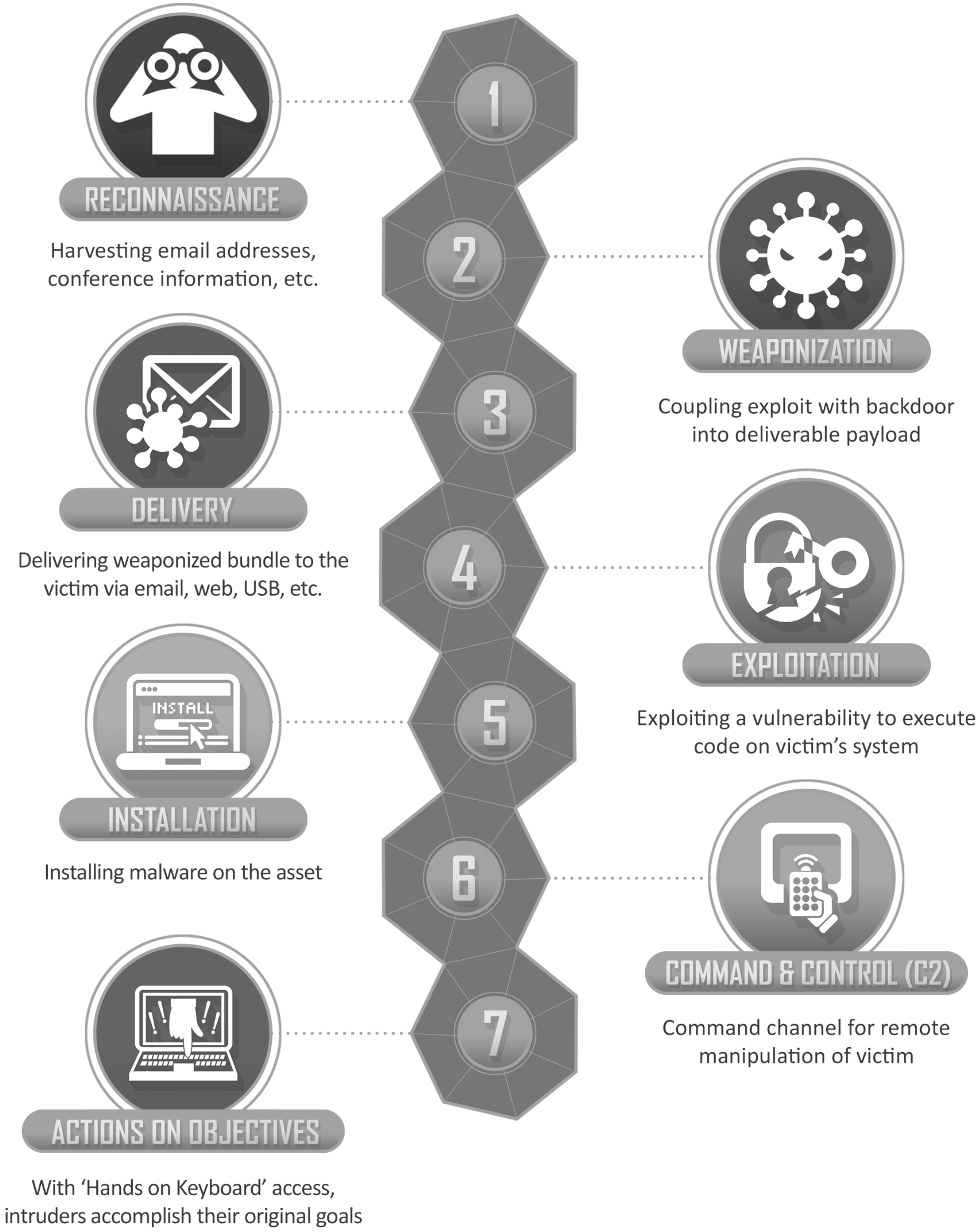
Red Team focuses on getting specific trophies:

- Confidential data
- Financial analysis reports
- Get foothold on critical systems (i.e. SWIFT, Bigdata)
- Get privileges on Active Directory and other critical assets

Trophies are defined with the tested entity

RESPONSIBILITY IS KEY
FOCUS ON SAFETY
WHILE PROMOTING SECURITY IMPROVEMENTS

Killchain all things



1 RECONNAISSANCE

Harvesting email addresses, conference information, etc.

2 WEAPONIZATION

Coupling exploit with backdoor into deliverable payload

3 DELIVERY

Delivering weaponized bundle to the victim via email, web, USB, etc.

4 EXPLOITATION

Exploiting a vulnerability to execute code on victim's system

5 INSTALLATION

Installing malware on the asset

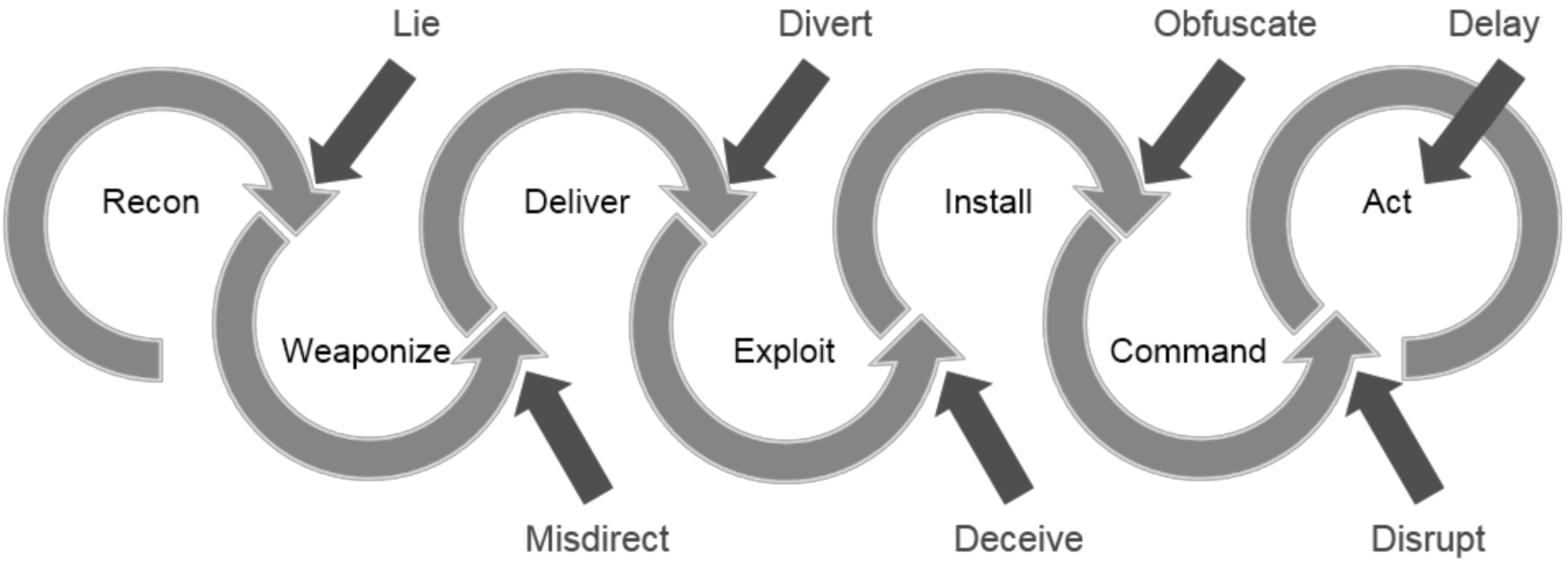
6 COMMAND & CONTROL (C2)

Command channel for remote manipulation of victim

7 ACTIONS ON OBJECTIVES

With 'Hands on Keyboard' access, intruders accomplish their original goals

Killchain all things



Lie

Divert

Obfuscate

Delay

Recon

Deliver

Install

Act

Weaponize

Exploit

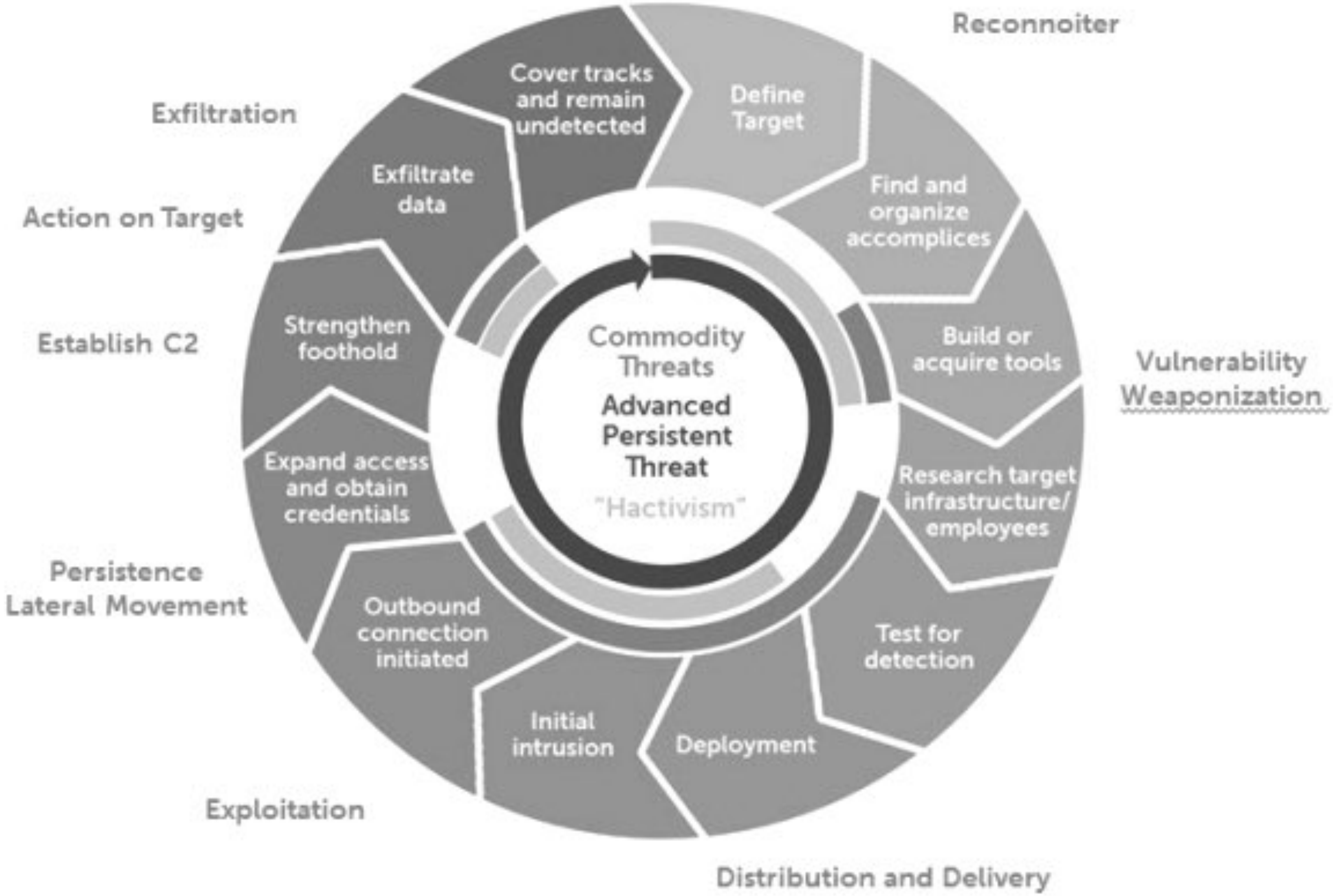
Command

Misdirect

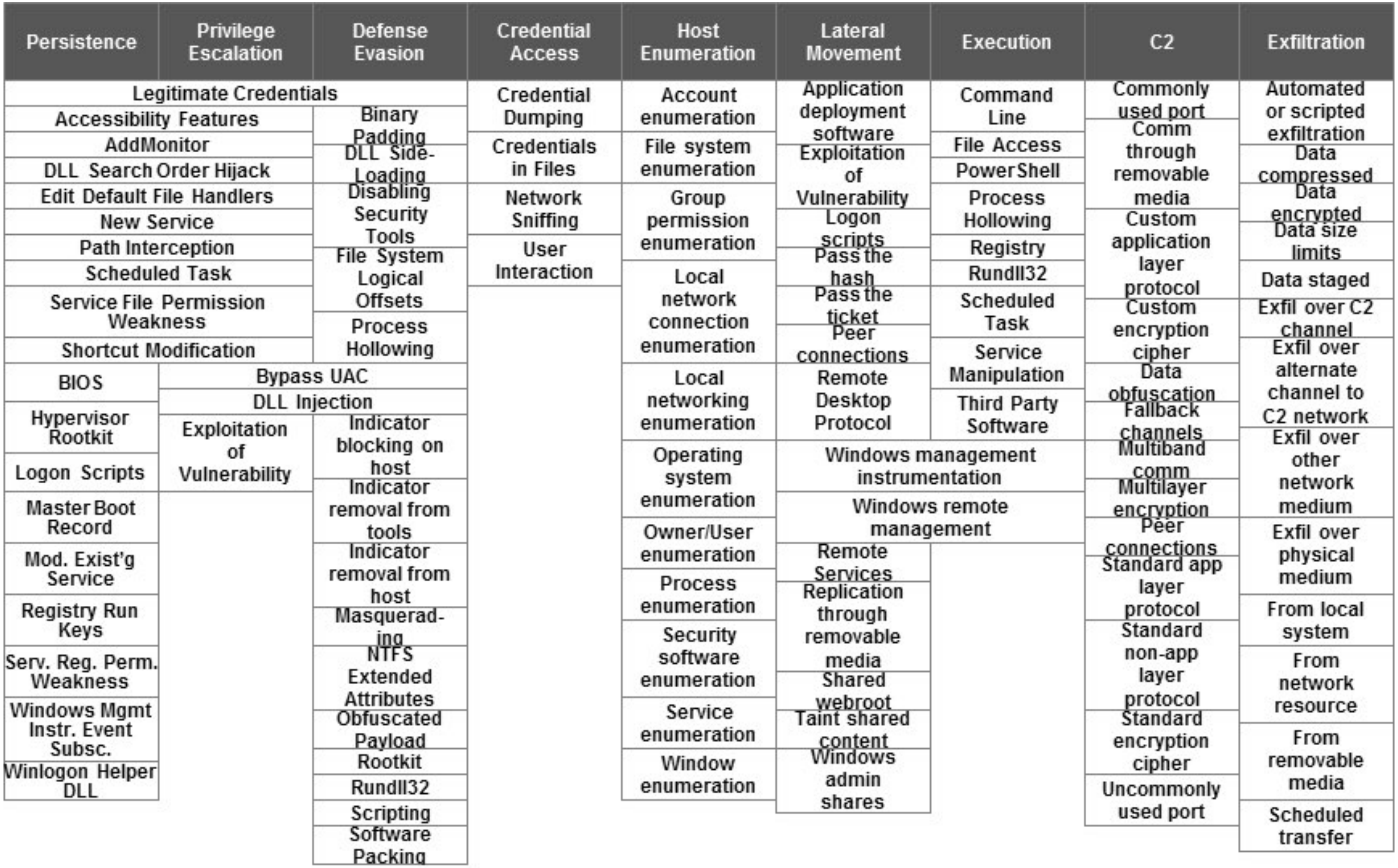
Deceive

Disrupt

Killchain all things


Reconnoiter
Define Target
Find and organize accomplices
Build or acquire tools
Vulnerability Weaponization
Research target infrastructure/ employees
Test for detection
Deployment
Distribution and Delivery
Initial intrusion
Outbound connection initiated
Exploitation
Expand access and obtain credentials
Persistence Lateral Movement
Strengthen foothold
Establish C2
Exfiltrate data
Action on Target
Cover tracks and remain undetected
Exfiltration
Commodity Threats
Advanced Persistent Threat
"Hactivism"

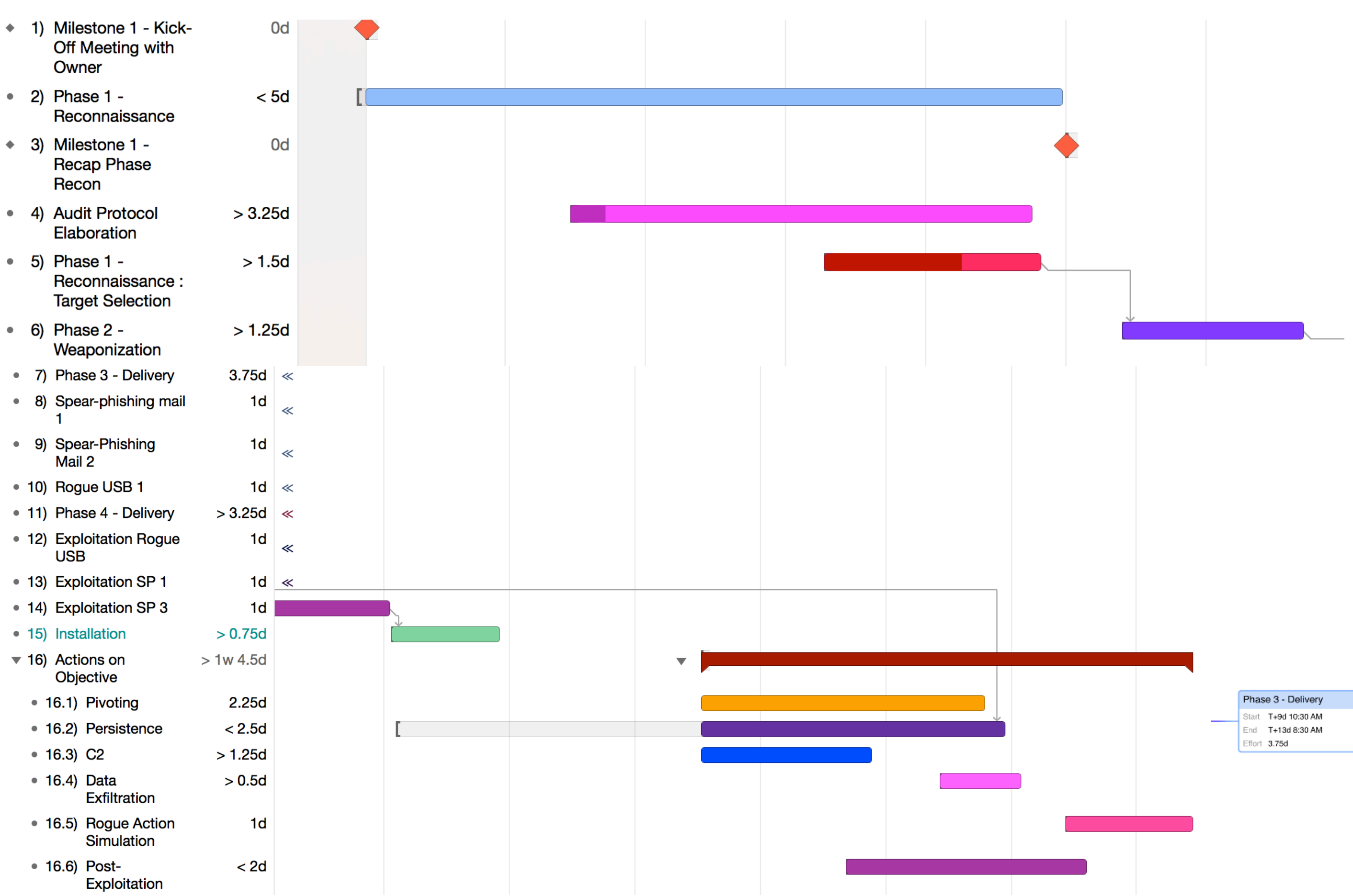
Killchain all things



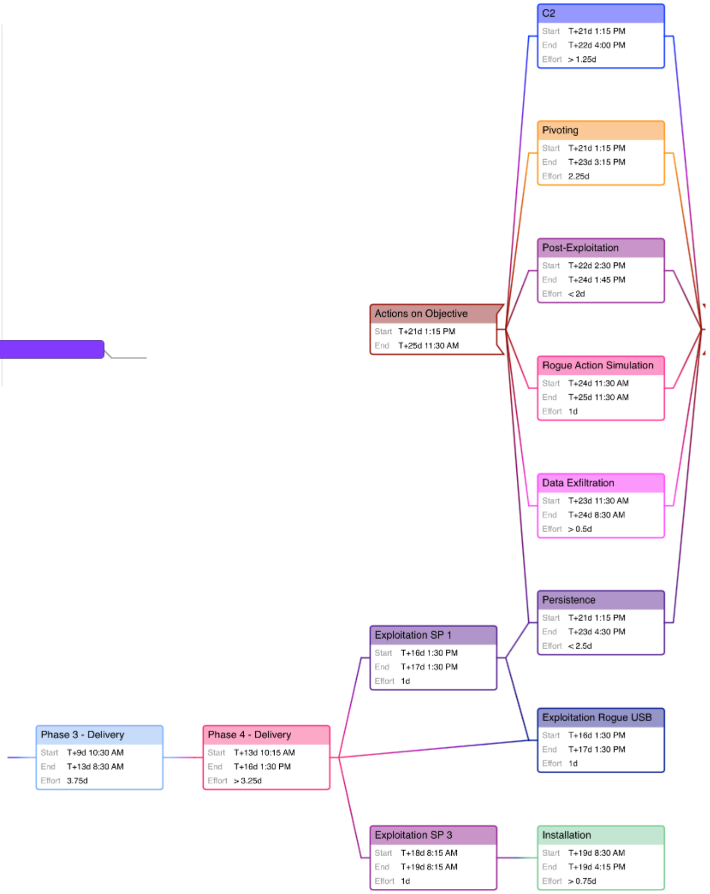
Persistence	Privilege Escalation	Defense Evasion	Credential Access	Host Enumeration	Lateral Movement	Execution	C2	Exfiltration
Legitimate Credentials			Credential Dumping	Account enumeration	Application deployment software	Command Line	Commonly used port	Automated or scripted exfiltration
Accessibility Features		Binary Padding	Credentials in Files	File system enumeration	Exploitation of Vulnerability	File Access	Comm through removable media	Data compressed
AddMonitor		DLL Side-Loading	Network Sniffing	Group permission enumeration	Logon scripts	PowerShell	Custom application layer protocol	Data encrypted
DLL Search Order Hijack		Disabling Security Tools	User Interaction	Local network connection enumeration	Pass the hash	Process Hollowing	Custom encryption cipher	Data size limits
Edit Default File Handlers		File System Logical Offsets		Local networking enumeration	Pass the ticket	Registry	Data obfuscation	Data staged
New Service		Process Hollowing		Operating system enumeration	Peer connections	Rundll32	Fallback channels	Exfil over C2 channel
Path Interception				Owner/User enumeration	Remote Desktop Protocol	Scheduled Task	Multiband comm	Exfil over alternate channel to C2 network
Scheduled Task				Process enumeration		Service Manipulation	Multilayer encryption	Exfil over other network medium
Service File Permission Weakness				Security software enumeration		Third Party Software	Peer connections	Exfil over physical medium
Shortcut Modification				Service enumeration	Windows management instrumentation		Standard app layer protocol	From local system
	Bypass UAC			Window enumeration	Windows remote management		Standard non-app layer protocol	From network resource
	DLL Injection				Remote Services		Standard encryption cipher	From removable media
BIOS	Exploitation of Vulnerability	Indicator blocking on host			Replication through removable media		Uncommonly used port	Scheduled transfer
Hypervisor Rootkit		Indicator removal from tools			Shared webroot			
Logon Scripts		Indicator removal from host			Taint shared content			
Master Boot Record		Masquerading			Windows admin shares			
Mod. Exist'g Service		NTFS Extended Attributes						
Registry Run Keys		Obfuscated Payload						
Serv. Reg. Perm. Weakness		Rootkit						
Windows Mgmt Instr. Event Subsc.		Rundll32						
Winlogon Helper DLL		Scripting						
		Software Packing						

Approved for Public Release; Distribution Unlimited. Case Number 15-1288

White Mode Killchain



1) Milestone 1 - Kick-Off Meeting with Owner	0d
2) Phase 1 - Reconnaissance	< 5d
3) Milestone 1 - Recap Phase Recon	0d
4) Audit Protocol Elaboration	> 3.25d
5) Phase 1 - Reconnaissance : Target Selection	> 1.5d
6) Phase 2 - Weaponization	> 1.25d
7) Phase 3 - Delivery	3.75d
8) Spear-phishing mail 1	1d
9) Spear-Phishing Mail 2	1d
10) Rogue USB 1	1d
11) Phase 4 - Delivery	> 3.25d
12) Exploitation Rogue USB	1d
13) Exploitation SP 1	1d
14) Exploitation SP 3	1d
15) Installation	> 0.75d
16) Actions on Objective	> 1w 4.5d
16.1) Pivoting	2.25d
16.2) Persistence	< 2.5d
16.3) C2	> 1.25d
16.4) Data Exfiltration	> 0.5d
16.5) Rogue Action Simulation	1d
16.6) Post-Exploitation	< 2d



C2
Start T+21d 1:15 PM
End T+22d 4:00 PM
Effort > 1.25d

Pivoting
Start T+21d 1:15 PM
End T+23d 3:15 PM
Effort 2.25d

Post-Exploitation
Start T+22d 2:30 PM
End T+24d 1:45 PM
Effort < 2d

Actions on Objective
Start T+21d 1:15 PM
End T+25d 11:30 AM

Rogue Action Simulation
Start T+24d 11:30 AM
End T+25d 11:30 AM
Effort 1d

Data Exfiltration
Start T+23d 11:30 AM
End T+24d 8:30 AM
Effort > 0.5d

Persistence
Start T+21d 1:15 PM
End T+23d 4:30 PM
Effort < 2.5d

Exploitation SP 1
Start T+16d 1:30 PM
End T+17d 1:30 PM
Effort 1d

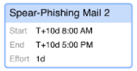
Phase 3 - Delivery
Start T+9d 10:30 AM
End T+13d 8:30 AM
Effort 3.75d

Phase 4 - Delivery
Start T+13d 10:15 AM
End T+16d 1:30 PM
Effort > 3.25d

Exploitation Rogue USB
Start T+16d 1:30 PM
End T+17d 1:30 PM
Effort 1d

Exploitation SP 3
Start T+18d 8:15 AM
End T+19d 8:15 AM
Effort 1d

Installation
Start T+19d 8:30 AM
End T+19d 4:15 PM
Effort > 0.75d



Spear-Phishing Mail 2
Start T+10d 8:00 AM
End T+10d 5:00 PM
Effort 1d

Let’s model!

TI-based Modelling

Why Modelling?

Why: to inform business needs and technology owners of prioritized threats as they relate to the cybercontrols and processes in place - within the context of business processes of technologies.

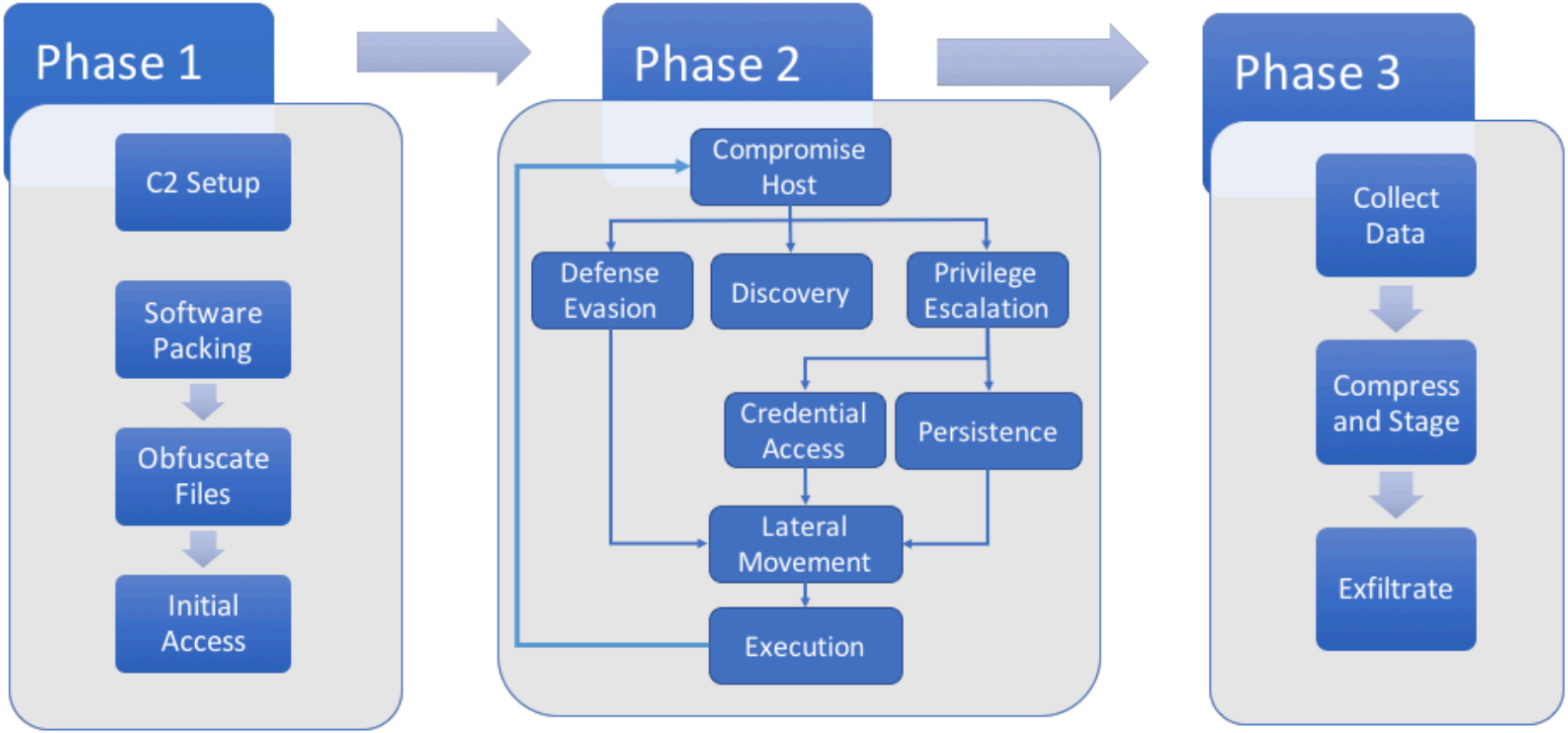
How: Common threat assessment implies creating a common view of cyber threat landscape

How (external view): By assessing active threats to the company / industry / geography

How (internal view): By assessing existing defensive postures within the tested scopes: implemented controls, security monitoring, employee responsiveness

In order to: To prioritize financial and HR allocation vs acceptable defensive posture against the current threats.

APT Emulation



Phase 1

C2 Setup

Software Packing

Obfuscate Files

Initial Access

Phase 2

Compromise Host

Defense Evasion

Discovery

Privilege Escalation

Credential Access

Persistence

Lateral Movement

Execution

Phase 3

Collect Data

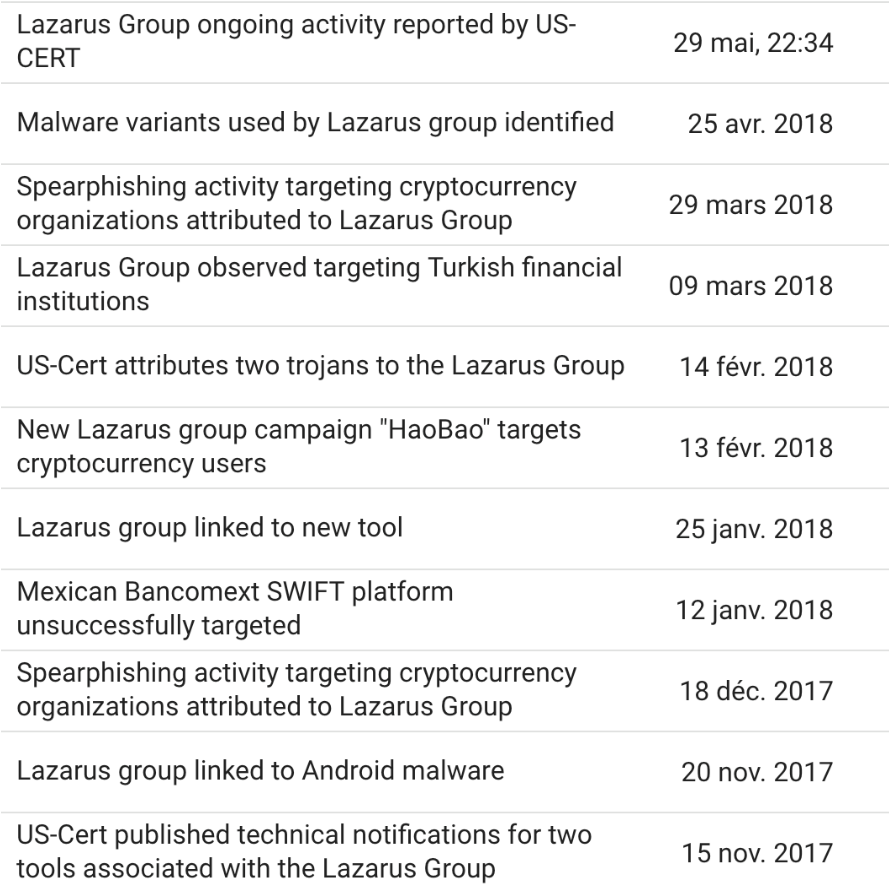
Compress and Stage

Exfiltrate

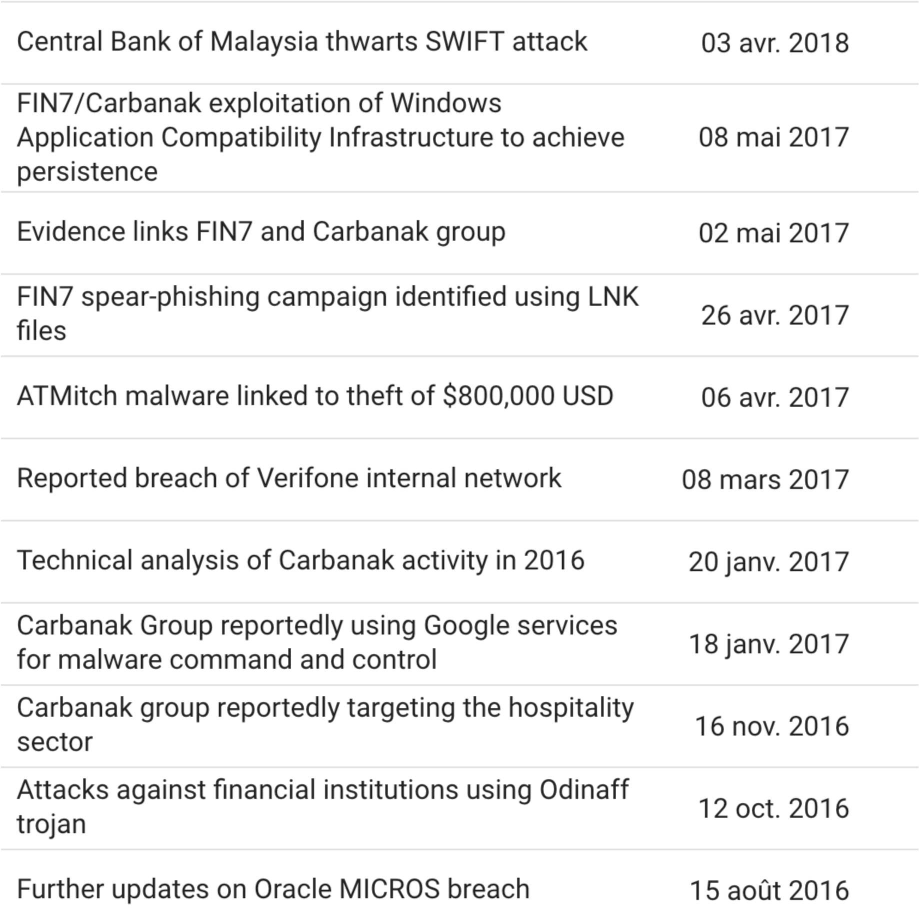
Usual Suspects

Anunak
Metel
Odinaff
Buhtrap
GCMAN
Lazarus
Bluenorof
Navigator
FIN7
Cobalt Gang
RTM

Pick one (or a few)

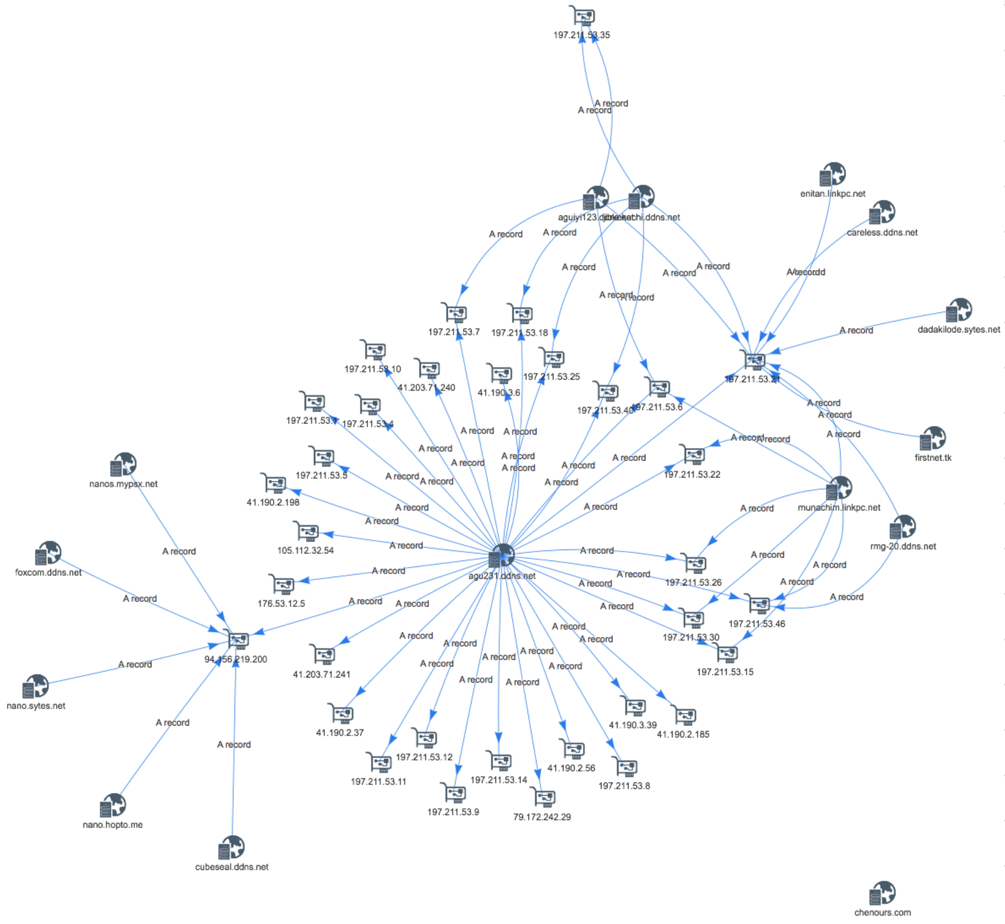


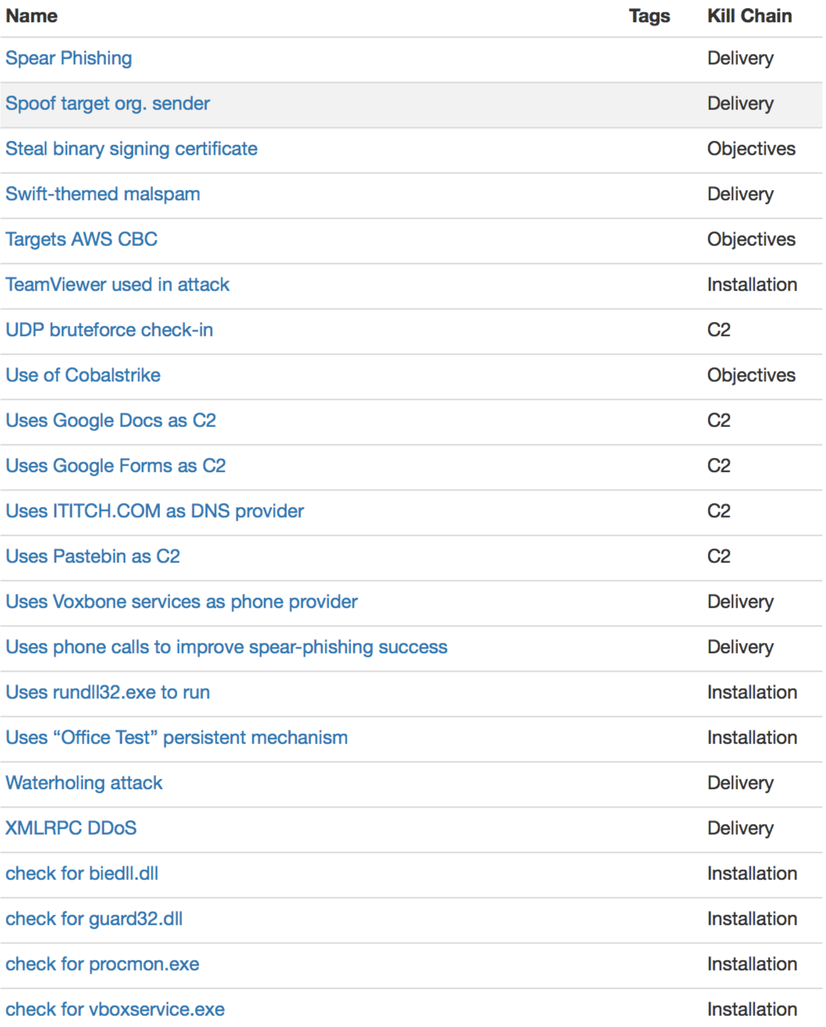
Lazarus Group ongoing activity reported by US-CERT	29 mai, 22:34
Malware variants used by Lazarus group identified	25 avr. 2018
Spearphishing activity targeting cryptocurrency organizations attributed to Lazarus Group	29 mars 2018
Lazarus Group observed targeting Turkish financial institutions	09 mars 2018
US-Cert attributes two trojans to the Lazarus Group	14 févr. 2018
New Lazarus group campaign "HaoBao" targets cryptocurrency users	13 févr. 2018
Lazarus group linked to new tool	25 janv. 2018
Mexican Bancomext SWIFT platform unsuccessfully targeted	12 janv. 2018
Spearphishing activity targeting cryptocurrency organizations attributed to Lazarus Group	18 déc. 2017
Lazarus group linked to Android malware	20 nov. 2017
US-Cert published technical notifications for two tools associated with the Lazarus Group	15 nov. 2017



Central Bank of Malaysia thwarts SWIFT attack	03 avr. 2018
FIN7/Carbanak exploitation of Windows Application Compatibility Infrastructure to achieve persistence	08 mai 2017
Evidence links FIN7 and Carbanak group	02 mai 2017
FIN7 spear-phishing campaign identified using LNK files	26 avr. 2017
ATMitch malware linked to theft of $800,000 USD	06 avr. 2017
Reported breach of Verifone internal network	08 mars 2017
Technical analysis of Carbanak activity in 2016	20 janv. 2017
Carbanak Group reportedly using Google services for malware command and control	18 janv. 2017
Carbanak group reportedly targeting the hospitality sector	16 nov. 2016
Attacks against financial institutions using Odinaff trojan	12 oct. 2016
Further updates on Oracle MICROS breach	15 août 2016

Knowledge-base it





Name	Tags	Kill Chain
Spear Phishing		Delivery
Spoof target org. sender		Delivery
Steal binary signing certificate		Objectives
Swift-themed malspam		Delivery
Targets AWS CBC		Objectives
TeamViewer used in attack		Installation
UDP bruteforce check-in		C2
Use of Cobalstrike		Objectives
Uses Google Docs as C2		C2
Uses Google Forms as C2		C2
Uses ITITCH.COM as DNS provider		C2
Uses Pastebin as C2		C2
Uses Voxbone services as phone provider		Delivery
Uses phone calls to improve spear-phishing success		Delivery
Uses rundll32.exe to run		Installation
Uses “Office Test” persistent mechanism		Installation
Waterholing attack		Delivery
XMLRPC DDoS		Delivery
check for biedll.dll		Installation
check for guard32.dll		Installation
check for procmon.exe		Installation
check for vboxservice.exe		Installation

Impersonate it

FAPT 42: « Funky Elephant »