Cyber Threat Intelligence

Rabbani

15 March 2025

AGENDA

01 Introduction

- Whoami
- What is CTI
- Why it's Important
- Application

02 CTI Life Cycle

- Collection
- Processing
- Analysis
- Dissemination

03 Cyber Kill Chain

- Reconnaissance
- Weaponization
- Delivery
- Exploitation
- Installation
- Command and Control
- Actions on Objectives

04 Data Classification

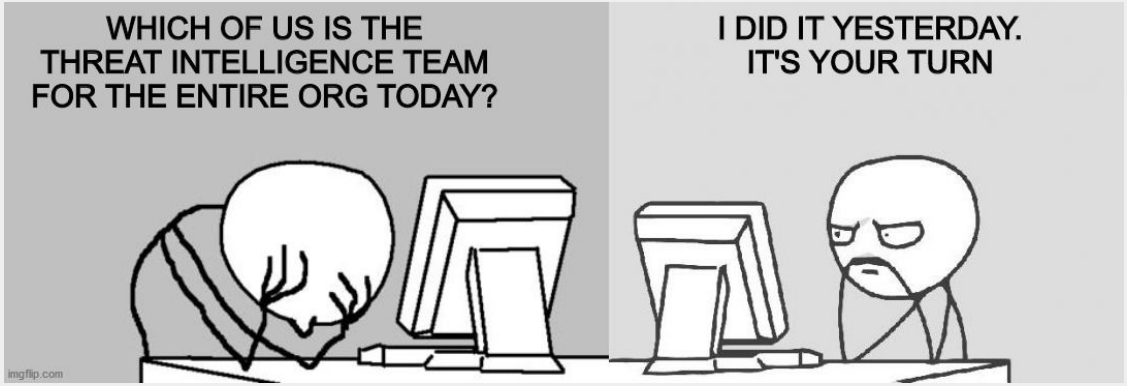
- Business
- US Government
- Traffic Light Protocol

05 Case Study - Fancy Bear

- APT Report Template
- XAgent

whoami

- Rabbani
- Worked with CTI for 2 years +
- Certification - CREST Practitioner Threat Intelligence Analyst (CPTIA)
- Cyber security enthusiast
- cyber673[.]com



What is CTI?

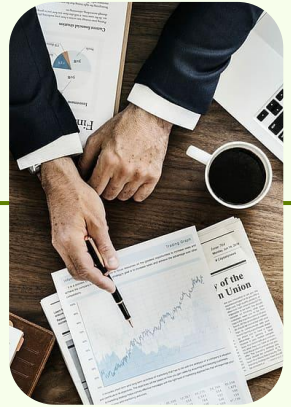
- What is CTI?
  - Analyzed data about threats, attackers and tactics. It is actionable data that can helps organisations improve their cyber security.
- Why is CTI important?
  - Helps organisations strengthen their defenses and make informed, evidence based decisions, reducing financial losses, safeguarding reputation, and ensuring business continuity.
- CTI applications?
  - Make informed decisions
  - Enhance cyber defense
  - Identify emerging threats
  - Incident response
  - Risk assessment

Planning and Direction

This initial phase coordinates intelligence activities to meet consumer needs. It involves significant interaction between consumers and producers to define **(1) Intelligence Requirements (IRs)** and **(2) Priority Intelligence Requirements (PIRs)**.

Collection

The process of gathering relevant data from various sources. Effective collection requires identifying reliable sources that provide timely and actionable information while filtering out irrelevant data.



Processing and Analysis

Raw data is analyzed to produce intelligence. Analysts use qualitative and quantitative methods to assess significance, identify patterns, and ensure accuracy. Source reliability is also evaluated to support informed decision-making.

Dissemination

Intelligence is delivered in a timely and appropriate format to consumers. Feedback helps refine IRs, restarting the cycle.

CTI Lifecycle

Structured process to create CTI.

Cyber Kill Chain

A framework developed by Lockheed Martin to describe the stages of a cyber attack.

(1) Reconnaissance: Identify potential targets, typically organisations with valuable data and weak security.
(2) Weaponization: Creating custom malware.
(3) Delivery: Deliver malware to the victim's environment.
(4) Exploitation: User executes a malware.
(5) Installation: Deploying backdoors.
(6) Command and Control (C2): Maintain remote access and receive attacker commands.
(7) Action on Objectives: Activate malware remotely to steal data for example.

Data Classification

To protect sensitive information, ensuring regulatory compliance, mitigating security risks.

Business	• **Public**: No security risk if exposed (e.g., marketing content). • **Internal:** Limited to employees, low risk (e.g., internal reports). • **Confidential**: Potential damage to the business (e.g., customer data, contracts). • **Restricted: Highly Sensitive** Severe impact if exposed (e.g., encryption keys, trade secrets).
US Government	• **Top Secret**: Grave damage to national security if disclosed. • **Secret:** Serious damage to national security. • **Confidential:** Some damage to national security. • **Unclassified:** No significant risk but still controlled.
Traffic Light Protocol	• **RED:** Restricted, named recipients only. • **AMBER:** Limited to the recipient's organisation. • **GREEN**: Can be shared within trusted communities. • **WHITE**: Publicly shareable information.

Case Study - Fancy Bear

Executive Summary
Fancy Bear is a highly sophisticated cyber threat group from Russia, believed to be linked to Russia's military intelligence agency (GRU). They are known for targeting government and political entities. The group employs advanced malware such as X-Agent to infiltrate networks, steal credentials, and maintain persistence. Organisations should follow recommendations to enhance their cyber security.

Threat Actor Details
APT28, also known as Fancy Bear, Pawn Storm, the Sednit Gang, and Sofacy, is a Russian state-sponsored advanced persistent threat (APT) group believed to be linked to Russia's military intelligence agency (GRU). is a highly sophisticated cyber threat group recognized for its disruptive operations, notably against the U.S. Democratic National Committee (DNC). Public reports indicate that APT28 has previously utilized tools such as X-Tunnel, X-Agent, and CompuTrace to infiltrate target networks. These tools enable the group to hook into system drivers, retrieve local passwords, and access the LDAP server.

APT28's known capabilities include logging keystrokes and mouse movements, gaining access to webcams and USB drives, modifying local files, and maintaining persistent network connections.

Technical Details
X-AGENT is a modular Remote Access Trojan (RAT) designed for second-stage attacks. It is compatible with Windows, iOS, and Unix-based operating systems. Its capabilities include keylogging and file extraction. Typically, X-AGENT is deployed following first-stage malware like CORESHELL or GAMEFISH and is often used alongside XTUNNEL and CompuTrace/Lojack.

Recommendations
- Layer phishing defence
- Deploy Sysmon
- Manage office macros carefully
- Set up security monitoring capability

IOCs

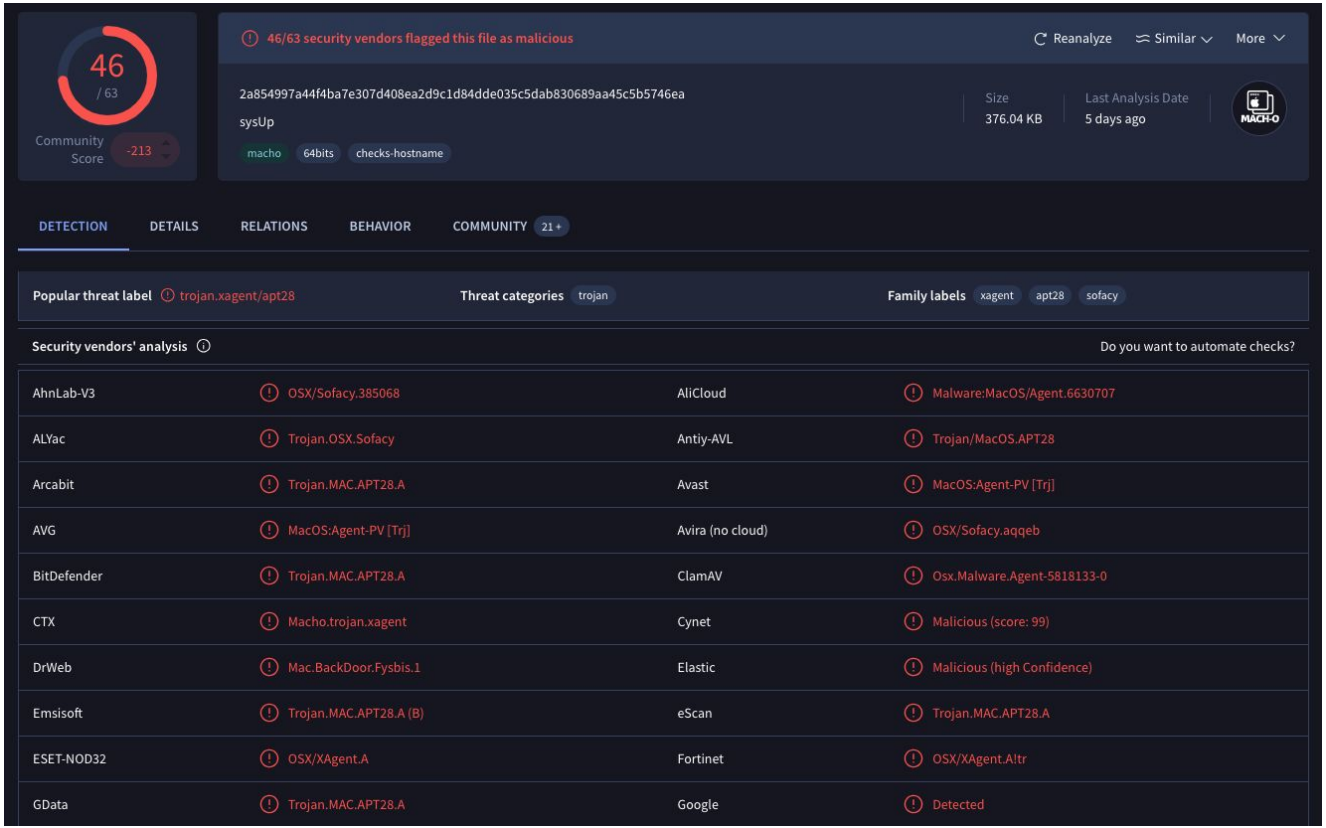
Type	IOCs	Description
SHA256	2a854997a44f4ba7e307d408ea2d9c1d84dde035c5dab830689aa45c5b5746ea	Malware, aka Xagent_FancyBear, .exe or .dll
MD5	4fe4b9560e99e33dabca553e2eeee510	Malware, aka Xagent_FancyBear, .exe or .dll
Website	thepiratecinemaclub[.]org	C2 server
IP	185[.]181.102.204	C2 Server

Reference

- https://www[.]crowdstrike.com/en-us/blog/who-is-fancy-bear/
- https://www[.]mandiant.com/sites/default/files/2021-09/APT28-Center-of-Storm-2017.pdf
- https://www[.]crowdstrike.com/adversaries/fancy-bear/
- https://www[.]ncsc.gov.uk/news/indicators-of-compromise-for-malware-used-by-apt28
- https://www[.]wired.com/story/russias-fancy-bear-hack-us-federal-agency/

X-AGENT as seen on VirusTotal

Sophisticated malware developed by the Russian cyber espionage group APT28 (Fancy Bear).



THANK YOU

Rabbani