FORTRA

Threat Scenarios

PLAYBOOK

An Offensive Security Guide to Understanding, Emulating, and Testing against Modern Targeted Attacks

Table of Contents

Featuring 11 real-world threat scenarios by nation-state actors, ransomware groups, and cybercriminal organizations, this playbook shows how security teams can use **Cobalt Strike**, **Outflank Security Tooling**, and **Core Impact** to test defenses against the tactics adversaries use every day.

The scenarios span the full attack lifecycle, covering In Phase initial access, Through Phase post-compromise activity, and Out Phase objectives such as data theft and exfiltration. They also address cloud-focused attacks and emerging AI-driven threats, providing a practical way to emulate real-world operations and measure security readiness across modern environments.

Threat Actors – Geography

Global Cyber-Criminal Syndicates

- Conti / LockBit / BlackCat (ALPHV) – ransomware operations
- FIN7, FIN11 – financial crime and data theft
- Cl0p – data-extortion campaigns.
- Scattered Spider / ShinyHunters – Identity compromise, social engineering and data extortion

- APT28 (Fancy Bear) – military/ government espionage
- APT29 (Cozy Bear) – intelligence collection;
- Sandworm / Voodoo Bear – disruptive / ICS attacks
- EvilCorp – financially motivated.

- Lazarus Group – espionage & cryptocurrency theft
- APT38 / Bluenoroff – financial theft operations
- Kimsuky – intelligence collection.

- APT33 (Elfin) – aerospace & energy espionage
- APT34 (OilRig) – credential harvesting & espionage
- APT42 – cyber-espionage supporting domestic surveillance.

- APT10 (Stone Panda) – global IP theft
- APT31 (Zirconium) – espionage & credential theft
- APT41 (Double Dragon) – espionage + financially motivated ops;
- Volt Typhoon – critical infrastructure targeting.

Threat Actors – Industry Sectors

Defense

- APT28 / APT29 (Russia), APT31 (China), APT33 (Iran), Lazarus (North Korea)
- Espionage, influence ops, theft of classified or geopolitical data. Use spear phishing, zero-days, credential theft, and lateral movement.

Healthcare & Life Sciences

- APT42 (Iran), UNC1878 (Ryuk), Conti / LockBit / ALPHV ransomware groups
- Data theft and extortion. Target hospitals, pharma, biotech for sensitive patient/IP data. Low tolerance for downtime makes ransomware effective.

Financial Services

- APT38 (North Korea), FIN7, FIN11, EvilCorp, Scattered Spider
- Financial theft, extortion, fraud. Heavy use of social engineering, remote access tools, and credential compromise.

Technology & Telecommunications

- APT41 (China), Mustang Panda, Scattered Spider, Lapsus$
- IP theft and access to customer environments. Exploit managed service providers (MSPs) and cloud platforms. Heavy social engineering.

Energy & Critical Infrastructure

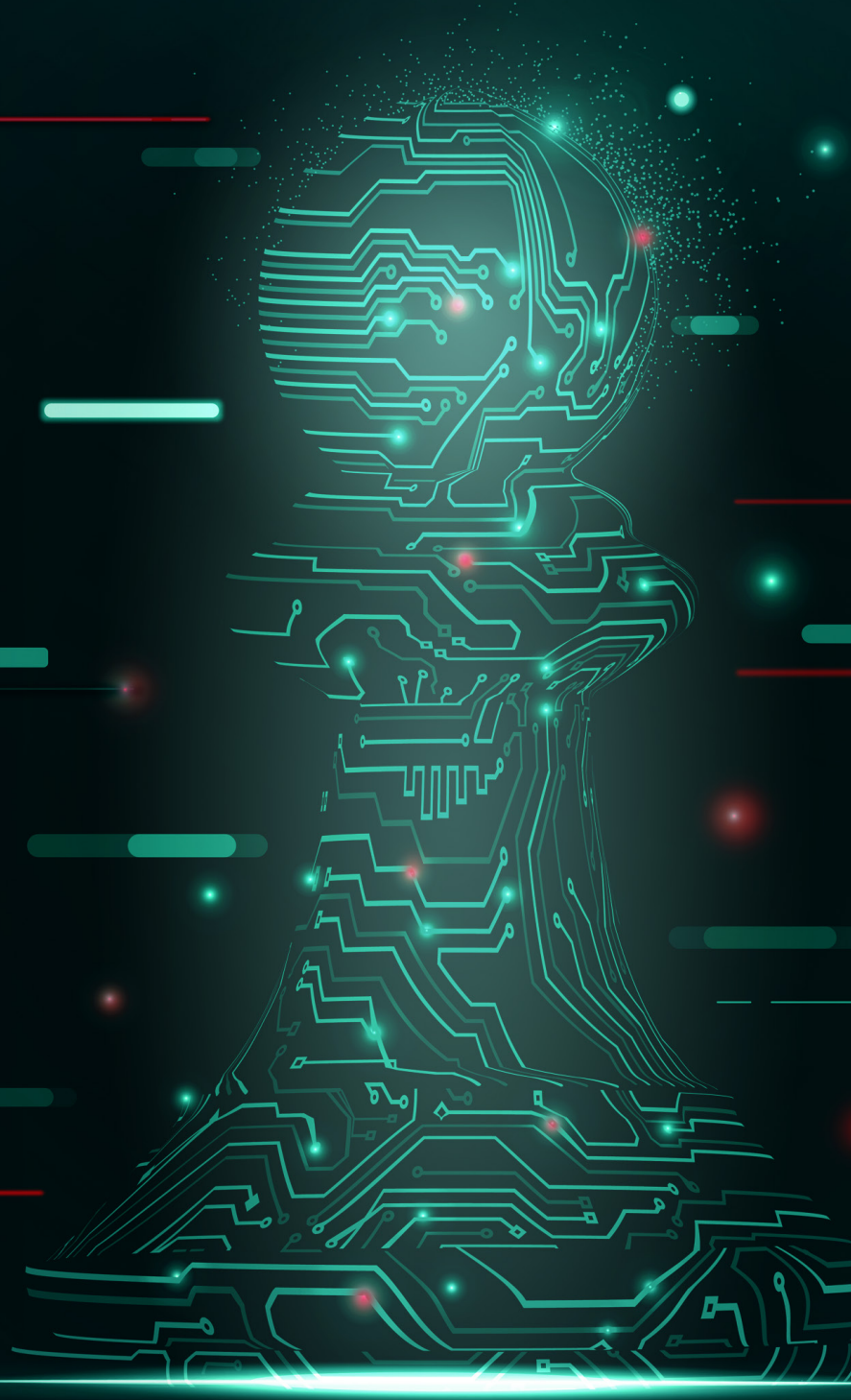
- Sandworm / Berserk Bear (Russia), Volt Typhoon (China), APT33 (Iran)
- Disruption and espionage. Focus on ICS/SCADA environments, supply chain infiltration, and prepositioning for potential disruption.

Public Sector / Local Government

- Conti, REvil, LockBit, Scattered Spider
- Ransomware and disruption. Often exploit legacy systems and poor segmentation.

Threat Scenarios

Emulate real threat actor capabilities to test your defenses



Covert Post Exploitation

Cobalt Strike Adversarial C2 Implementations

(In Phase)

Threat Scenario

- Threat actors are known for covert post exploitation using C2 Frameworks.
- Examples include rogue implementations of C2 Frameworks such as Vermillion Strike.
- These threat actors are also known to develop their own BOF and Loader implementations.

KNOWN TO BE USED BY

Threat Actors

- APT29 (Cozy Bear)
- FIN7
- APT41 (Wicked Panda)
- REvil (Sodinokibi)
- APT37

HOW FORTRA CAN SUPPORT YOU

Fortra's Solutions

- Cobalt Strike Out of the Box.
- Cobalt Strike's customizable malleable C2 Profile, which can be used mimic APT behaviors or use existing profiles of known APTs.
- Extend functionality and behavior using BOFs and Scripts to emulate specific malware behaviors.

Modern EDR Evasion

OST's PE Payload Generator

(In Phase)

Threat Scenario

- Organizations depend on Endpoint Detection and Response (EDR) solutions to identify and mitigate nefarious activities.
- However, threat actors utilize state-of-the-art evasion techniques to bypass modern EDRs impacting their effectiveness.
- Once initial access is obtained, attackers look to achieve their operational objectives.

KNOWN TO BE USED BY

Threat Actors

- APT29 (Cozy Bear)
- APT41 (Wicked Panda)
- Scattered Spider
- FIN7

HOW FORTRA CAN SUPPORT YOU

Fortra's Solutions

- OST's Payload Generator is a binary payload builder/transformer focussed on OPSEC safety.
- Payloads are enhanced with expertly researched techniques for antiforensics and EDR evasion.
- Red Teams can now focus on other aspects of the kill-chain, ultimately helping build cyber resilience over the long-term.

Weaponized File Formats

Builder

(In Phase)

Threat Scenario

- Threat actors are known to use weaponize various file formats types which appear to be legitimate business files i.e., malicious office documents.
- Users are more likely to trust and click in these documents to view them.
- This allows attackers to run hidden shellcode, gain initial access, and establish a foothold within the environment.

KNOWN TO BE USED BY

Threat Actors

- APT28 (Fancy Bear)
- APT29 (Cozy Bear)
- Lazarus Group
- FIN7
- Financially motivated
- cybercrime groups

HOW FORTRA CAN SUPPORT YOU

Fortra's Solutions

- OST's Builder provides a myriad of different weaponize file format options for initial access.
- These formats can be customized with various OPSEC options and converted multiple times to support evasion.
- Legitimate looking files are then used to deliver the payload and compromise the user.

Steganography

OST's Stego Loader

(In Phase)

Threat Scenario

- Threat actors are known to use steganography to hide malicious payloads within seemingly innocuous files such as images.
- Users are less likely to be suspicious of these infected images that appear legitimate.
- Attackers can then evade detection, blend in with normal traffic, and quietly communicate with compromised systems once in the network.

KNOWN TO BE USED BY

Threat Actors

- Lazarus Group
- APT29 (Cozy Bear)
- APT28 (Fancy Bear)
- Fin7

HOW FORTRA CAN SUPPORT YOU

Fortra's Solutions

- OST's Stego Loader was designed to embed payloads to images without corrupting the image.
- Once on the victim's environment, the payload will be decoded from the image and executed, giving access to the user's desktop.

Vulnerability Exploitation

Core Impact Certified Exploit Library

(In Phase)

Threat Scenario

- Modern threat actors are increasingly using exploits for initial access.
- Public facing services, network and web application vulnerabilities are actively exploited by attackers.
- Ultimately allowing attackers code execution on the target and establishing a foothold within the environment.

KNOWN TO BE USED BY

Threat Actors

- APT28 (Fancy Bear)
- CL0P
- Lazarus Group
- FIN7
- Financially motivated cybercrime groups

HOW FORTRA CAN SUPPORT YOU

Fortra's Solutions

- Core Impact's Certified Exploit Library releases on average a new exploit every 1-2 weeks.
- These exploits are rigorously tested and go through a release-cycle before being published.
- Core Impact's exploits are written by the same developers of Impacket and consider several factors from criticality to prevalence in enterprise environments.

Browser Based Attacks

OST's Chromeo

(Through Phase)

Threat Scenario

- Modern browsers store credentials, authentication tokens and session cookies, making them a high-value target for attackers.
- Threat actors increasingly use browser-based malware and infostealers to hijack authenticated sessions and bypass MFA.
- Compromised browser sessions enable attackers to access sensitive resources without the user's password.

KNOWN TO BE USED BY

Threat Actors

- APT29 (Cozy Bear)
- Fin7
- Scattered Spider
- Lazaruss Group

HOW FORTRA CAN SUPPORT YOU

Fortra's Solutions

- OST's Chromeo is a Chrome DevTools Remote Injection and Interaction toolset for post-exploitation.
- Allows the operator to dump cookies, history, bookmarks, passwords directly from the browser.
- AITM capabilities on targeted domains (remote network interception).

Ransomware

OST's Fake Ransom

(Out Phase)

Threat Scenario

- Threat Actors are known to use Ransomware to extort organizations by encrypting sensitive data.
- A screen takeover message is shown to the victim with details of the data encrypted, ransom amount and contact address of Threat Actor to pay ransom often in cryptocurrency.

KNOWN TO BE USED BY

Threat Actors

- Conti / Royal / BlackCat (ALPHV)
- LockBit
- REvil / Sodinokibi
- Scattered Spider
- Financially Motivated Threat Actor Groups

HOW FORTRA CAN SUPPORT YOU

Fortra's Solutions

- Outflank Security Tooling (OST) Fake Ransom is a fake yet real-life like ransomware.
- Fake Ransom hijacks the screen as an attacker would with a full ransom notice.
- The message can be customized to simulate a real-stress test of the incident response processes of an organization.

Financial Malware

OST's Hidden Desktop

(Out Phase)

Threat Scenario

- Threat actors are known to use hidden desktop techniques to secretly monitor and interfere with user activity without being noticed.
- Examples include banking malware, which use this method to capture login details and manipulate online banking sessions.

KNOWN TO BE USED BY

Threat Actors

- TA505 – Dridex
- TA542 – Gozi (Ursnif)
- Trickbot
- Financially motivated cybercrime groups

HOW FORTRA CAN SUPPORT YOU

Fortra's Solutions

- Users of OST can take advantage of Hidden Desktop, this allows invisible control of the client computer, a feature in top-tier financial malware.
- Hidden Desktop allows access to fat-client applications, the ability to watch the victim's desktop as they are working or even access sensitive data.

RMM Abuse

Outflank Security Tooling (Payload Generator + Hidden Desktop)

(Out Phase)

Threat Scenario

- Big Game Hunting Affiliates are known for aggressive social engineering campaigns.
- Through an initial phish unsuspecting users download what looks to be legitimate RMM software.
- Threat actor then takes control of the end users' session.

KNOWN TO BE USED BY

Threat Actors

- Scattered Spider (UNC3944)
- Mangled Spider / Punk Spider / Bitwise Spider
- Black Basta Ransomware Group
- Qakbot / Qbot Affiliates / LockBit

HOW FORTRA CAN SUPPORT YOU

Fortra's Solutions

- Outflank Security Tooling (OST) has built in EDR evasion payload generation capabilities through the Payload Generator.
- A payload can be masqueraded as RMM software and executed on the victim's machine.
- Users of OST can also use Hidden Desktop, for invisible control of the client computer whilst emulating a threat actor appearing as IT support.

Cloud Phishing

OST's PhisherPrice and RoadTune

(Cloud)

Threat Scenario

- Organizations are increasingly moving resources into the cloud to create business efficiencies.
- Attackers are taking advantage of this by compromising identities.
- Once compromised attackers can establish persistence, escalate privileges, and exfiltrate data.

KNOWN TO BE USED BY

Threat Actors

- APT29 (Cozy Bear)
- Fin7
- Scattered Spider
- Cloud Focused Cyber Crime Groups

HOW FORTRA CAN SUPPORT YOU

Fortra's Solutions

- OST's PhisherPrice abuses the EntraID Device Code Flow.
- A rogue phishing website is created, luring the user to provide their device code.
- With OST's RoadTune, this stolen token can be used to impersonate a managed device and infiltrate the corporate network and extract sensitive data.

AI Enabled Adversary

Cobalt Strike REST API/MCP + Aggressor AI

(AI)

Threat Scenario

- With the rise of AI, Threat Actors are utilizing both LLMs and AI agents in their attacks.
- From hyper-personalized phishing e-mails to actual AI enabled offensive operations.
- This has reduced both the time of attack and complexity bottlenecks which had previously hindered threat actors.

KNOWN TO BE USED BY

Threat Actors

- APT29 (Cozy Bear)
- Fin7
- Scattered Spider
- Various state sponsored and financially motivated Threat Actors

HOW FORTRA CAN SUPPORT YOU

Fortra's Solutions

- Cobalt Strike 4.13 brings the REST API, MCP server and Aggressor AI.
- Red Teams can utilize Cobalt Strike's integrations for AI enabled operations from streamlining tasks to generating OPSEC safe commands.
- With Cobalt Strike's flexibility, Organizations can now test how their defenses hold up against AI empowered threat actors.

Fortra's Offensive Security Solutions help you determine how your security defenses hold up against real attacks.

Learn more at fortra.com

(fta-g-0826-r2-am)