TEAR DROP

Machine Learning Backed Red Team Automation, Adversary Simulation Software

How Tear Drop Helps Your Organization?

The goal of Tear Drop is to prepare network defense staff for the highly sophisticated targeted attacks their organization may face. It helps you to answer three key questions:

- What are your weak sides from the attacker point of view?
- What could a targeted attacker do with access to your environment?
- How effective is your current security posture at preventing, detecting, and responding to a targeted attack?

Our goal is to give your organization the experience of a sophisticated targeted attack, without the actual damage that accompanies a real incident. Tear Drop shows you how it reached your sensitive data and related methods that can help you prevent future attacks.

To make Tear Drop as realistic as possible, we constantly update our approach to mirror the current adversary methods. Tear Drop consists of different MITRE ATT&CK™ methods and knows how to combine them to make a successful attack. We leverage Tear Drop intelligence team to keep pace with changes in different adversary groups' tactics used to target organizations. The result is a test of your defenses that replicates real-world tactics, techniques, and procedures, often relying on the same tools the attackers use themselves.

Benefits

Be Your Own Attacker

Automate your red team engagements with Tear Drop. It enables your organization to close all the internal security gaps before the real attack occurs.

SOC Maturity Assessment

Use Tear Drop's simulation module to determine how effective your SOC is at detecting, analyzing and responding to adversary tactics.

Easy Penetration Testing

Tear Drop provides you the most necessary penetration testing modules which can be used via the web interface. Tear Drop makes it easy to automate all phases of a penetration test.

Fully Automated Red Team Activities

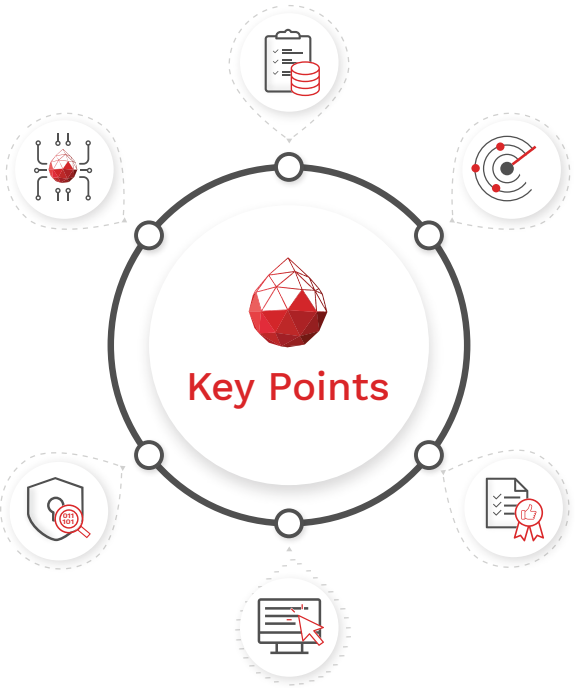
Finds weaknesses in your Active Directory environment, escalates privileges, laterally moves around the network and finds valuable data.

Machine Learning Technology

Analyze your network and detects the best communication method and attack paths.

Zero False-Positives, Always

Works with a proof-based approach. It only reports a vulnerability if it successfully exploits it.



Asset Discovery

Discover your internal or internet-faced assets, identify running services and their version, get screenshots easily.

Exploit Software Vulnerabilities

Detects vulnerabilities on your machines and exploits them safely to carry the attack to new phases. Do you use a scanner for vulnerability detection? No Problem. Upload it's report to Tear Drop and start exploitation.

One-click Modules

Do you want to take the wheel? No problem. Most necessary penetration testing tools are one-click ahead. Tear Drop provides you with easy to use spear-phishing panel with ready to use domain names and lots of post-exploitation modules for different operating systems.

TEAR SECURITY

32 Wigmore Street (1st Floor) London W1U 2RP United Kingdom
info@tearsecurity.com

TEAR DROP

Key Features

Visualized Attack Maps

Tear Drop provides you dashboard, exportable reports which focuses only on important points. All your weaknesses will be crystal clear. Tear Drop includes:

Attack Map: You can observe when and how Tear Drop reached your sensitive data

Vulnerability Report: You can get classic vulnerability report to see the vulnerabilities across your network and mitigation devices.

One-Click Adversary Simulation

Tear Drop consists of different MITRE ATT&CK™ techniques for Windows, Linux, and macOS operating systems. Just select the techniques you want to simulate, Tear Drop agents will handle the rest for you.

There are also 15+ different APT groups with their specific scenarios which are included in Tear Drop's simulation module.

Phishing E-mails Made Easy

Tear Drop includes all necessary functions for your phishing campaigns.

Integrated E-mail Harvester: You can find your company e-mails from public websites like Google, Twitter, LinkedIn and save them.

Integrated Domain Names: You can use domain names provided by Tear Drop to send phishing e-mails.

E-mail Templates: Tear Drop includes different phishing templates for your needs.

Integrated HTML Editor: Do you want to use your own templates? No problem! You can edit HTML templates inside Tear Drop's web panel.

PII Data Detection

Tear Drop automatically detects PII Data that can be reached by an attacker. Only masked data reaches Tear Drop's server.

Use Cases

Identifying Internal Security Gaps With Red Teaming

Red team engagements are the best way of testing your organization with full "Cyber Kill Chain" approach. However, red team engagements requires highly skilled experts, lots of different tools and time. That's why you can't do it within short periods. You are becoming vulnerable until the next red team engagement.

Solution: Tear Drop's machine learning backed algorithm analyzes your Windows domain network and creates the best attack paths like a real hacker. It extracts credentials, laterally moves around the domain network, detects valuable data and reports all important point. Tear Drop enables the organization to close all the security gaps before real attack occurs.

Penetrating Your Vulnerabilities

Vulnerability assessment became a mainstream activity for almost every organization. They are using softwares like Nessus, Nexpose, OpenVAS to find vulnerabilities in their infrastructure. But they can't be sure if those vulnerabilities are exploitable. If they are exploitable, what are the risks and impacts? To answer these questions, they need to work with penetration testing specialists. But penetration testers need lots of time, different tools to complete their mission. Therefore, organizations can't know their risks on daily basis.

Solution: Tear Drop's "Smart Exploitation Module" identifies vulnerabilities and safely exploits them if it's possible. If you already use vulnerability scanners like Nessus, Nexpose, OpenVAS, just upload their report to Tear Drop and check which vulnerabilities are exploitable. After exploitation finishes, post-exploitation part starts. If you want to take the wheel, Tear Drop provides you lots of one-click use post-exploitation modules. If you don't, just start automated red team engagement and Tear Drop handles the rest.

Defending Against Phishing E-mails

Email is an essential part of our everyday communications. It is also one of the most common methods that hackers use to attempt to gain access to your network. More than 90% of data breaches start with a phishing attack. Despite record investments in cyber security technology, phishing attacks still works! Organizations can't know if their phishing e-mail protection mechanisms works until a real attack occurs.

Solution: Tear Drop provides you almost anything that can be helpful for phishing e-mail assessments. You can find your company e-mails from public websites with "E-mail Harvester" tool. You can use our integrated domain names and e-mail templates for your phishing campaigns. Check which employee(s) have opened your malicious attachment. If anybody did it, you can start fully automated red team engagement on the network.

Analyzing Performance of Your Defensive Security Solutions

Organizations around the world are investing billions of dollars in defensive security solutions to protect their critical assets. However, when we look at the APT group attacks, those solutions are not enough to hold attackers back. Organizations can't know if their defensive solutions are good enough until the real attack occurs.

Solution: You can test defensive solution's capability with Tear Drop's Adversary Simulation module. Tear Drop consists of different MITRE ATT&CK™ techniques for Windows, Linux and macOS operating systems. There are also 15+ different APT groups with their specific scenarios are included in Tear Drop too. We leverage Tear Drop intelligence team to keep pace with changes in different adversary groups' tactics used to target organizations.

Integrations

ALIEN VAULT · Nessus · nexpose · SHODAN Computer Search Engine · OpenVAS

TEAR SECURITY

32 Wigmore Street (1st Floor) London W1U 2RP United Kingdom
info@tearsecurity.com