RED TEAM TOOLKIT

The Red Team Toolkit is a compilation of advanced offensive security tools to aid red teams deliver advanced attack simulations. The purchase of a yearly subscription service comes with a current version of the Toolkit, which includes all the updates released during that year, and is offered with our top support services.

OVERVIEW

Cyber adversaries are dedicated to devoting their full focus and time researching and weaponizing new attack techniques that defeat enterprise security products. They also build complex command and control infrastructure that can prevent takedown and remain undetected for long periods of time.

Mossé Security's Red Team Toolkit (RTT) is a subscription service that allows us to provide you with up-to-date tools and techniques as if you were a real adversary group.

The subscription comes with our top support services. We can also develop custom capabilities specific to your needs.

As a result, your security team can focus on testing and defending your networks without the challenges of researching, building, testing, documenting and maintaining advanced cyber security tools.

FEATURES

- **Fully Featured:** RTT comes with attack tools to simulate all types of attacks. Tools for espionage campaigns, ransomware, targeted spear phishing, and theft of large amount of data are all included.
- **C2 Infrastructure:** RTT uses a fully encrypted custom C2 protocol that can be encapsulated over any standard network protocol.
- **Custom Malware:** RTT contains custom malware in open source format that can be compiled and modified to fit your needs.
- **Resilience:** RTT offers numerous automated techniques to defeat anti-virus software, endpoint detection and prevention, prevent takedowns and detect if the blue team's investigating your C2 infrastructure.
- **Memory-Only:** RTT contains many memory-only tactics and techniques to run malware and execute payloads.
- **N-Day Vulnerabilities:** RTT comes with several "n-day" attack techniques that are not yet properly detected and blocked by security vendors.

BENEFITS:

Reduced Costs:

The Red Team Toolkit provides organisations with advanced attack simulation capabilities at a fraction of the cost of building it themselves. Given that the toolkit is open source and fully automated, your junior tech employees can also use it.

Full Coverage:

The Red Team Toolkit includes everything your testers need to act like a true adversary group. Custom network protocols and malware, n-day vulnerabilities, memory-only attacks, and anti-takedown capabilities are amongst the meany features that are included.

Demonstrated Defence:

Organisations that can consistently detect, takedown and disrupt security testers armed with the Red Team Toolkit, will have demonstrated serious defensive capabilities against advanced threat actors.

Mossé Security, 454 Collins Street. Melbourne, 3000, Victoria, Australia
www.mosse-security.com contact@mosse-security.com