Trustwave®

Trustwave SpiderLabs® Red Teaming

RESEARCH AND INTELLIGENCE-LED ATTACK SIMULATIONS

Red Teaming is one of the most advanced and interesting services performed by the SpiderLabs team. We have three permanent Red Teams: 'Missing Sector', 'Redbacks' and 'Huntsman' with core hubs in the US, Australia and the UK. These core teams are augmented by a pool of over 160 penetration testers, security researchers, malware reverse engineers and incident responders globally.

Our Red teams comprise members sourced from more than 16 countries globally, with each team member having an average of 12 years' experience. Each year we conduct more than 50 Red Team engagements and over 4000 manual penetration tests. Our team have experience of testing in a multitude of countries around the world, meaning we always understand local legislations and cultural nuances. Our Red Team service is largely based on our experience of CREST STAR and CBEST frameworks from the UK (developed inline with the UK Banking Industry), coupled with our years of experience providing offensive capability to our clients in the US and Australia.

Our Red Team is backed by our world-renowned research team. The research team have access to billions of security events, multiple threat database feeds and years of cumulative experience discovering 0-day vulnerabilities. Combined with our core Red Teams, the research team assist in building bleeding edge custom implants / RATs and various other toolsets. We regularly involve our Incident Response team in preparation exercises for our clients, creating bespoke 'Purple Team' engagements to give maximum learning outcomes for our clients and to ensure they're ready for advanced adversaries (or next years' Red Team assessment!).

Intelligence Driven Assessment

Our Red Teaming engagements are driven by threat intelligence. We gather this information by aggregating our Research team's data with manually collated Open Source Intelligence (OSINT), Human Intelligence gathering (HUMINT) and search engine (meta)data. We often incorporate client data into the reconnaissance phase of our methodology to further enhance the accuracy. Once we have the data we require, we begin to process the information with close interaction with the client. The information gathered is utilized to create various scenarios that form the basis of the engagement.

SpiderLabs Credentials

SpiderLabs Memberships

- CREST (SpiderLabs were the First Global Member)
- Member of the Forum of Incident Response and Security Teams
- Qualified Payment Card Industry Forensic Investigator (PFI)

Individual Qualifications

- Offensive Security (OSCP, OSCE, OSWP)
- CREST (CCT APP, CCT INF, CRT)
- SANS (GXPN, GPEN, GWAPT, GAWN)
- Cisco (CCNP, CCNA)
- ISC2 (CISSP)
- ISACA (CISA, CISM)
- EC-Council (CEH)
- CompTIA (Security+)
- SCO (CUSA, Master ACE)
- Academic (PhD, MSc, BSc (Hons), MRes)

Research Programs

- MAPP – Microsoft Active Protections Program
- Facebook Threat Exchange
- ii (Incidents & Insights)
- Ops-Trust
- Microsoft DCC – The Digital Crime Consortium
- MUTE – The Malware URL Tracking and Exchange
- OWASP
- APWG
- Project HoneyPot

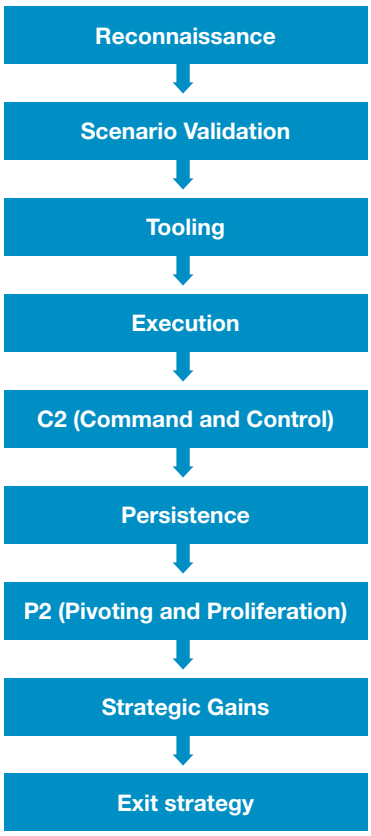
Trustwave® SpiderLabs®

Our Approach

The SpiderLabs Execution Chain describes our operation during the Attack phase of the engagement. Each phase of the execution chain is linked to the previous and forms an iterative process. Our testers will start by discovering targets and aim to gain and foothold and eventually persistence within the target network. Following this, data exfiltration will be attempted with high levels of stealth. We'll ultimately leave the network undetected.

Our attack simulation methodology is bespoke to SpiderLabs. We have augmented our approach by applying our own subject matter expertise and open source frameworks, such as the Mitre Att&ck™ model. Our approach centers on utilizing previously gathered threat intelligence and launches into reconnaissance phases to gain a holistic view of the target organization before we being the Cyber assault. We utilize the Mitre Att&ck Matrix™ as a starting point to chart our execution of various scenarios, and build upon this to create detailed attack chains.

SpiderLabs Execution Chain



Managing the Risks

The worst thing that can happen during a Red teaming assessment is that the organization conducting the test loses control of the simulation. This can often lead to a financial impact to your business and downtime for your customers. This can be mitigated by having the right assessment partner, with the right experience, processes and controls. Our Red teamers have years of experience of conducting these types of engagements and undergo training that focuses specifically on risk mitigation strategies. We also assign an attack manager at the start of the engagement who creates a customized risk mitigation document that addresses common concerns.

Get Prepared to Resist!

Purple Teaming

Purple teaming is growing in popularity as an approach for security assessments, as it allows education to happen during a real-world simulation. This approach involves live access to our incident response experts during certain periods of the assessment, where we run various attack plays (scenarios) whilst the client's internal blue teams (or SOC) detect, defend and respond to the simulated attacks. Typically, we will begin with more simple threats and increase the stealth of our attempts as the engagement progresses. The main goal of this is for the team to learn new techniques and 'feel' what it's like to be pitted against a live onslaught of skilled attackers.

Trustwave®

For more information: www.trustwave.com