Trustwave®

DATA SHEET

Trustwave SpiderLabs® Red Teaming

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 150 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 of experience. Each year we conduct more than 50 red team engagements and over 4000 manual penetration tests. Our team has experience with testing in a multitude of countries around the world, so we have a solid understanding of local legislations and cultural nuances. Our red team service is largely based on our experience of CREST (the Council for Registered Ethical Security Testers) STAR (Simulated Target Attack & Response) and CBEST frameworks from the UK (developed in conjunction with the UK Banking Industry), coupled with our years of experience providing offensive capability to our clients in the US and Australia.

The Trustwave SpiderLabs Red Team is backed by our world-renowned research team. Our research team has access to billions of security events, multiple threat database feeds and years of cumulative experience discovering zero-day vulnerabilities. Combined with our core red team, the research team assists 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 custom 'Purple Team' engagements to give maximum learning outcomes to our clients and to ensure they are ready for advanced adversaries (or next year's red team assessment).

Intelligence Driven Assessment

Our red teaming engagements are driven by threat intelligence. We gather this information by aggregating our internally generated data (from our MSS and research team) with manually collated Open Source Intelligence (OSINT), Human Intelligence gathering (HUMINT) and our dark web indexing subsystems. 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.

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 start by discovering targets and aim to gain a foothold and eventually persistence within the target network. Following this, data exfiltration will be attempted
with a keen focus on stealth. We will ultimately leave the network undetected.

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

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 on your business and downtime for your customers and can be mitigated by having the right assessment partner, with the right experience, processes and controls. Our red teamers have many years of experience with 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 plan that addresses common concerns.

Get Prepared to Resist!

Purple Teaming

Our purple teaming service simulates threats to your organization based on real-world intelligence. We utilize our team of dedicated researchers, red teamers and blue teamers to create tactics, techniques and procedures (TTPs) that closely replicate real-world threat actors. We then coach your blue team leaders on how to resist, detect, respond and recover from attacks in your own environment. This culminates with a mini-red team assessment where your team can pit their new skills against our ethical hackers.

The idea of purple teaming is that it's used to help organizations mature and get ready to defend in their own environments, whilst simulating real attacks like Advanced Persistent Threats (APTs) and ransomware-based threats. At Trustwave SpiderLabs, we feel this is the very best way to prepare for red teaming. enhance your defensive capability and increase maturity. The way our purple teaming works is that we embed a red and blue team coach within your defensive team and run a series of drills and teaching break-outs that replicate real life attack simulations. Next, we assess the learning outcomes and team progress by running a mini-red teaming assessment at the end. Essentially, we train your team in the offensive and defensive arts.

The structure of the engagement is based around two key concepts and methodologies: The Cyber Kill Chain and the Mitre Att&ck Matrix. We utilize these frameworks to structure the sessions and to ensure coverage of common advanced attacks during both our purple and red teams. More detail is given in our methodology section.

PLANNING	MALWARE AND TOOLING				PIVOTING	DETECTION
Reconnaissance	Weaponization	Delivery	Exploitation	Installation	C2	Action on Objectives
Preparation	**Purple Teaming**					**Mini-Red Team**
1 Week	2 Weeks					1 Week

SpiderLabs Credentials

SPIDERLABS MEMBERSHIPS	INDIVIDUAL QUALIFICATIONS	RESEARCH AND TI PROGRAMS
CREST • Trustwave were the first Global member. • Founding member in USA. • STAR certified in North America. The only accreditation framework for Red Teaming. Member of the Forum of Incident Response and Security Teams Qualified Payment Card Industry Forensic Investigator (PFI	• Offensive Security (OSCP, OSCE, OSWP) • CREST (CCSAS, CCSAM, 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	• 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 • Anubis • Team Cymru • Trustwave MSS data

Trustwave®

For more information: www.trustwave.com