SERVICE DESCRIPTION

SpiderLabs Red Team Testing

Service Scope

Trustwave's SpiderLabs team have over 10 years' experience of operating Red Team engagements and are one of the world's leading threat simulation groups. We focus on replicating real-world scenarios based on a mixture of experience, OSINT and threat intelligence gathering. We build our teams on an ad hoc basis, choosing the most suitable red teamers from our global pool of over 100 testers (also utilizing our core red team specialists to run the engagement). We have an extremely broad capability, with subject matter experts in all conceivable disciplines. In our assessment we utilize our world-renowned research team to provide real-world intelligence, resulting in bleeding edge techniques, scenarios and tools (including custom RAT and implant frameworks). All of our Red Team clients are assigned an attack manager early on in the process, who will be the interface with the SpiderLabs team and serve as a point of contact throughout.

Outline of the Engagement Model

Following conversations with the RfP steering committee, we have decided to take a 'goal orientated' approach to our assessment, with elements of playbook testing and 'purple teaming' centered on OSINT and threat intelligence precursors. This means that our engagement will have multiple elements and include deliverables as described below. Currently, we have limited data regarding the test's scope and focal points, therefore, we have outlined a prescriptive (and somewhat atypical) approach. However, it should be noted that we can easily reconfigure almost all elements of our approach.

The following model demonstrates the typical workflow of our service model.

- Initial meeting to discuss high level goals
- Risk analysis and legal requirements
- Scoping and asset identification
  - Highlight 'worst-case' scenarios
  - Define escalation points and paths
- Agreement of Terms
  - Agree KPIs
  - Define process for if something goes wrong during testing
  - Define and agree on risk ratings

- Onboarding processes (with assigned attack manager)
- Attack period begins
  - Scenario finalization
  - Execution chain initiated
  - Clean-up
  - Post attack scenario report delivered
  - Post attack round-table session
- End of service wrap-up
  - Maturity report and modelling (Purple team option)
  - Future works discussion
  - Close-out

SpiderLabs Execution Chain

Our execution chain describes the high-level approach that we will take in order to compromise the targets in a phased and secure manner.

- Reconnaissance
  - This can combine OSINT with stealthy attempts to profile the organizations' estate and people. This should be a follow-up with the client to understand how much of this was detected.
- Scenario Ideation (second round and validation, adjustments if required)
  - The creation of realistic scenarios for attack execution based on the OSINT, Threat Intelligence, Reconnaissance phase and experience of the team.
- Tooling
  - Appropriate toolsets, RATs and exploits will be collated, and selections made for the attack.
- Execution
  - This is the launching of attacks after the previous planning phases.
- C2 (Command and Control)
  - One of the key objectives of the assessment is to have control over multiple hosts within the victim organization.
- Persistence
  - Once a host is compromised, this phase is used to gain a foothold within the network.
- P2 (Pivoting and Proliferation)
  - Once we're confident that we have persistent access to the target network, we can try and 'pivot' further into it.
- Gains
  - At this stage, we start executing our high-level goals, such as data exfiltration to demonstrate the effectiveness of our attack.
- Exit strategy

    - It's important that we exit the operation in a stealthy fashion and try to get out within triggering any alerts or disrupting services.
- Exploit Selection

  When selecting (or developing) exploits, Trustwave ensure that every care is taken to launch the exploit safely and handle the communications appropriately. To ensure that this is done, we follow the following selection criteria:

    - Specific intelligence on appropriateness (i.e. Windows 7 exploit for Windows 7 boxes)
    - We select only exploits that can be controlled (and we have tested ourselves)
    - We select exploits that we can track and audit
    - We select exploits that we can clean up after
    - We select exploits that are reliable and infrequently cause system crashes or undesirable states, such as DoS.

Physical Testing Elements

It has been noted through the RfP process that social engineering is deemed out-of-scope. However, we have included this as supplementary information in case this changes.

A physical penetration test is conducted by a group of subject matter experts from various physical security disciplines, who will launch a campaign of attacks against organizational and human-related processes. They will act as a resourceful adversary using a controlled, realistic and interactive techniques during the testing window.

Trustwave typically target the following vectors during a penetration test:

- Survey and collect information on the physical perimeter and security controls
- Derive methods of attack and penetration methods for facility
- Carry out stated attacks on facility to include, but not limited to:
- Lock Picking
- Magnetic Door brute forcing
- Alarm system avoidance
- Ventilation system entrance
- Social engineering
- Tail-gating
- Procurement of badged access
- Solicitation
- Access System bypass
- Video Camera System redirection
- Gathering of onsite sensitive information by utilizing network access, physical collection, shoulder surfing, and photographs.
- Gaining access to protected areas such as server facility or datacenter
- Recording possible penetration points as well as cataloguing all information collected.

OSINT and Threat Intelligence

We have included the optional elements of threat intelligence collection, as a precursor to our attack simulations. In some cases, this is a useful exercise to map threats and correlate these to attack scenarios.

Service Description

Trustwave SpiderLabs perform an open source intelligence investigation to identify readily accessible information in the public domain. Following this initial discovery activity, a detailed and contextual analysis of the data is performed, and the overall security risks related to unnecessary or unauthorized leakage of potentially sensitive data.

We also extend this search to the threat landscape and provide narrative around the general threat actors within your market vertical. This provides key insights into real-world attack scenarios and helps us achieve more realistic simulations.

Scope and Project Phases

Following an initial pre-engagement kick-off meeting that would determine the specific focus areas of the assessment, the assessment consists of two phases (discovery and analysis).

Discovery

The discovery phase involves utilizing the same tools and techniques that malicious individuals would use to profile an organization and its data leakage footprint, including:

- Identification of legacy assets
- Search engine content discovery
- News groups and mailing lists trawling
- Querying of Public Registration records

The following additional data sources are utilized for the collation of potentially useful data:

- Trustwave SpiderLabs Forensic Investigations
- Trustwave SpiderLabs Malware Reverse Engineering and Analysis
- Trustwave SpiderLabs Vulnerability Research
- Trustwave SpiderLabs Security Testing and Analysis
- Trustwave Managed Security Services (e.g. Global managed SIEM data points)
- Trusted information sharing relationships through:
- Worldwide law enforcement agencies;
- Industry vendors;
- Private and public vulnerability disclosures.

Analysis

Following the initial discovery phase each potentially interesting record, document or piece of information is reviewed within the wider context of the focus areas for the assessment and the particular line of business of the target organization. Each confirmed item of data exposure is risk rated and catalogued for inclusion in the final report on findings.

Deliverables

Following the conclusion of the engagement, findings will be made available. The deliverables will be both strategic and tactical in nature, presented in a format that is highly accessible to both management and operational staff. Each finding will have a risk scoring associated with it as well as contain detailed technical information pertaining to the nature of the finding. Each finding will also be presented with clear guidance on how to remediate the issue.

Threat Intelligence Report

This report is derived from the collation, analysis and evaluation of intelligence from numerous data sources. The report is human written and will describe the threat landscape as applicable to the client.

Attack Scenario Report

An attack scenario report will be created following the assessment. The style of this report is similar to a traditional penetration testing report, but with additional narrative around the steps that led to the compromise. It will combine all elements of the attacks and not be limited to the ‘cyber’ realm. Should the client require any specific scoring systems or formatting, this should be discussed during the scoping meetings.

Post Attack Round-table Meeting

This comprises a one-day session with all relevant stakeholders and is led by the SpiderLabs attack manager. The purpose of this meeting is to discuss the findings, methods and remediation requirements of the client. It is essential that the client have fully read and understood the report in advance of this meeting in order to get full benefit.

Purple Teaming (Optional)

Purple teaming is becoming a lot more popular 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 whilst the client’s internal blue teams hunt, defend and respond to the simulated threats. 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.

Maturity Report and Modelling (Optional)

In conjunction with the SpiderLabs incident response team, we will provide a report discussing the maturity of the client and the high-level context of the engagement and how well the internal teams performed. This will assess the organization’s ability to resist and recover from a direct assault. This report is the main written deliverable of this type of assessment. However, reporting for our ‘purple team’ engagements are typically heavily customized.