encode
cyber threat management

Datasheet

Extrusion Testing™

Targeted Cyber Attack Simulation

The Threat Landscape

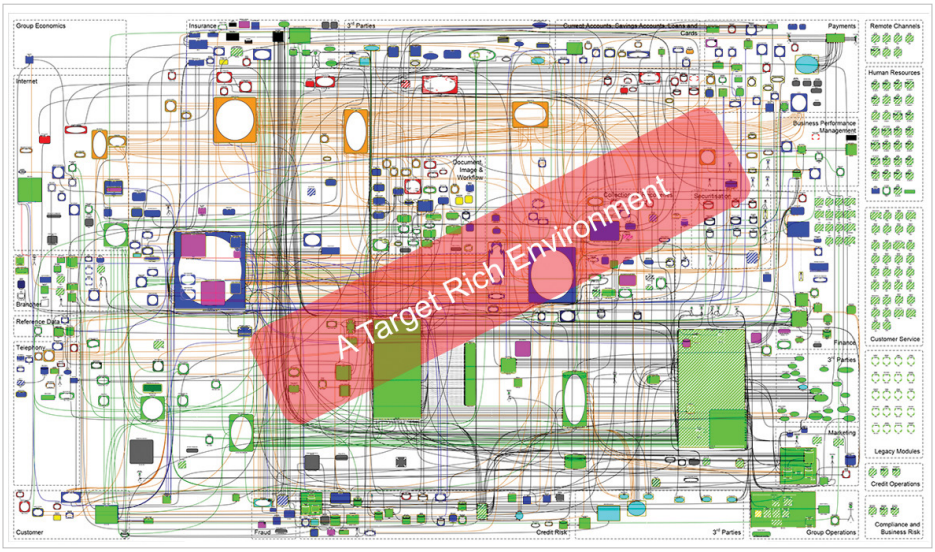
The target

The ever-growing reliance on digital technology in business operations, customer interactions, and data storage is creating increased risk for companies working to ensure information and system assets remain available 24/7 and, more importantly, uncompromised.

As cyber threats evolve and spread across multiple industries targeting more and more businesses, the protection of critical digital information assets from both internal and external threats is crucial.

IT System for a single Mortgage System at a Major High street bank

Organizations with valuable intellectual property or other critical data are facing a colossal challenge of how to share and allow the usage of confidential and proprietary information by colleagues and trading partners whilst protecting this information from internal and external threats.



Source: Computer Weekly, Karl Finders, 18th June 2015

Attack Surface

Every digitised business will have an attack surface. An attack surface is essentially a function of IT complexity which in turn is a function of the range of applications, technologies, Operating systems and digital access channels such as public, employee, BYOD, partner and vendor access. This attack surface in a growing business represents opportunity and choice for a determined attacker.

The Targeted Attack: the Advanced Persistent Threat (APT)

The most potent threat any digitised business faces today is the Targeted Cyber Attack. It is characterised by a highly motivated, skilled, well resourced, Threat Actor with strategic goals who is expressly targeting your business. This Threat Actor will dedicate weeks or months to breaching the business, persisting undetected whilst gathering intelligence and slowly extruding information and compromising system assets. Such a low and slow Targeted cyber attack is commonly known as an "Advanced Persistent Threat or APT.

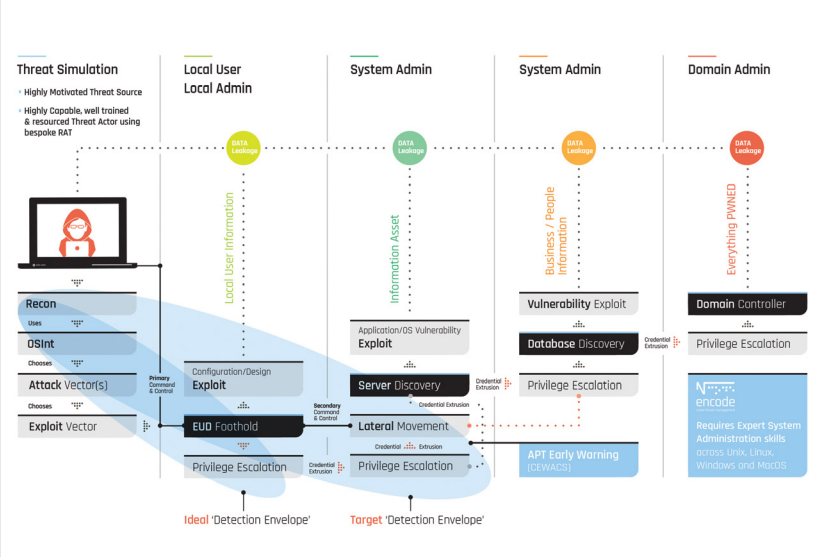
Targeted APT attacks hurt

Such targeted cyber-attacks that evade current security controls have become an epidemic and a priority for the security industry. They affect enterprises and organizations of any size, with far-reaching impacts. It's no longer unusual to exceed $100 million in damages for a single incident.

APT attacks are Intelligence driven

A targeted (APT) attack is essentially an intelligence driven exercise whose initial strategic goals are to discover exploitable trust relationships, leverage these to evade perimeter and endpoint defences and then quickly assume a trusted insider user role. When these initial goals are achieved, the business has a very serious (if not critical) problem of which, in almost all cases, it will be unaware.

Example Attack Profile



Cyber Attack Logic - it's a process

An APT based Cyber attack follows a certain intuitive or logical set of phases. The first phase involves intelligence gathering (i.e. reconnaissance) with the aim of discovering exploitable trust relationships. These in turn drive the choice of attack and exploit vectors to achieve target foothold establishment, privilege escalation and lateral movement phases. The compromise of an environment is therefore related sets of chained or loosely coupled Attack and Exploit vectors to achieve specific compromise goals. Each compromise goal enables the next and so on.

Extrusion Testing™

"Know your enemy"...proactively

Encode offers a real life Targeted Attack Simulation that directly assesses your organization's exposure to targeted cyber-attacks. It effectively battle-tests your critical capabilities around defending, detecting and responding to such attacks.

Encode unveiled its active APT active simulation testing service, namely "Extrusion Testing™", back in 2003 with the objective to bridge gaps that infrastructure and application penetration testing services could not address. Extrusion Testing™ puts an organization's cyber security control environment to the test against common Tactics, Techniques and Procedures (TTPs) used by advanced and determined adversaries.

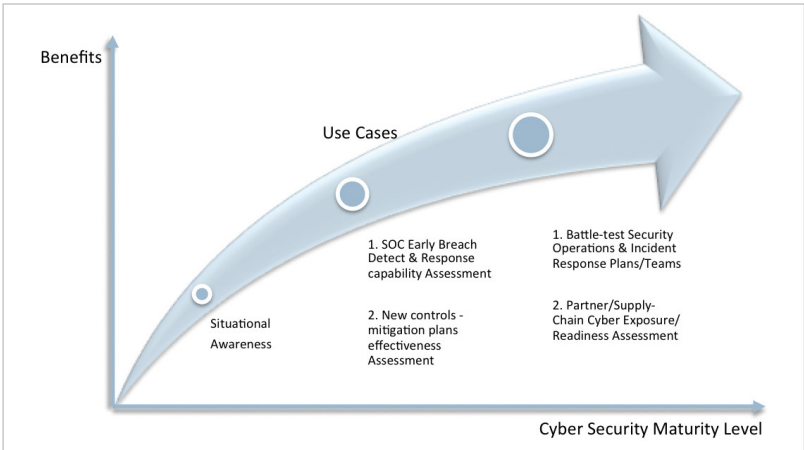
Targeted Cyber Attack Simulation

During such an exercise, our Red Team actively reproduces an actual targeted cyber-attack covering all attack kill chain stages: from reconnaissance, delivery and foothold(s) establishment, to attack escalation and objective realization. This is a unique opportunity to get to "know your enemy", without sustaining the damage you would normally experience during a real attack.

Extrusion Testing

Benefits

- Determine your business' ability to detect, respond and contain a breach early enough before damage is caused
- Raise C-level awareness around the APT problem and its implications
- Assess your current capabilities for handling APT based targeted attacks
- Assess User Security Awareness, Security Monitoring and Incident Response practices
- Identify and get expert remediation advice on critical vulnerabilities and security issues identified



Final thoughts - IT Security Investment Validation

A key issue for many companies is how do they validate that their investment in security products and services is being realized? Extrusion Testing™ provides that validation; enabling a company to determine whether they have the right solutions, and if so, are they correctly configured and monitored. If they are using external services to monitor their network then regular audits are essential to assess the service delivery.

Encode's Extrusion Testing™ is therefore an ideal audit mechanism not only for validating investment in security products but also a means of calibrating the end-to-end IT Security solution - i.e. fine tuning the defense–in-depth and monitoring environment. Ensuring your monitoring environment can detect, respond and contain a breach early in the cyber attack is critical since it

> Encode's Extrusion Testing™ is an ideal audit mechanism not only for validating investment in security products but also a means of calibrating the end-to-end IT Security solution

Encode's track record

Over the last decade, Encode have performed over 200 Extrusion Testing™ assignments across a range of customers and sectors.

During this time, our Extrusion Testing™ product has kept pace with the evolving Cyber Threat Landscape. Encode's Threat Lab team continually improves and develops new tactics, techniques,

encodegroup.com
+44 (0)207 0388305
info@encodegroup.com
Level 33, 25 Canada Square,
London E145LB