Datasheet

Bitdefender Global Leader In Cybersecurity

Bitdefender Offensive Services: Phishing

Over the years, as technology has evolved, so too have the attack paths and tactics used by threat actors. One constant, however, is phishing — an enduring and pervasive form of social engineering that remains a top attack vector. Despite cybersecurity being a key focus in modern digital ecosystems, the human element continues to be a critical vulnerability due to negligence and lack of awareness.

Bitdefender provides tailored phishing simulation campaigns, designed to replicate real-world threat actor tactics. Our CREST-accredited cybersecurity consultants methodically scope each engagement with an objective-driven approach, ensuring realistic attack scenarios that expose weaknesses and drive security awareness.

With best-in-class service delivery, these simulations help organizations strengthen their defenses against one of the most persistent cyber threats.

The lifecycle of a phishing engagement would be as below:

- **Research & Target Identification:**
  Bitdefender consultants design a highly targeted phishing campaign, mirroring the tactics and techniques of real-world threat actors.

- **Phishing Simulation:**
  The campaign is executed with deployed infrastructure, testing how employees respond. The engagement identifies both victims and those who successfully report the phishing attempt through official IT/Security channels.

- **Assessment & Risk Mitigation:**
  The collected data is analyzed to measure the impact across the organization, identifying areas of weakness. Insights from the engagement inform actionable strategies to mitigate future risks and improve security awareness.

At-a-Glance

Bitdefender Offensive Services deliver realistic phishing simulations that mirror real-world adversary tactics, providing organizations with a true-to-life social engineering experience. Our approach equips you with a comprehensive view of your organization's resilience against phishing attacks through detailed campaign analytics. Additionally, we provide targeted training to enhance user awareness, empowering employees to recognize and respond to phishing threats effectively. Ultimately, this strengthens the organization's overall security culture, reducing risk and reinforcing cyber resilience.

Key Benefits

- **Enhanced Awareness**:
  Educates users on phishing risks and tactics, reinforcing their ability to identify and avoid threats.

- **Hands-on Experience**:
  Exposure to realistic phishing scenarios helps employees recognize the telltale signs of an attack in real-world conditions.

- **Reduced Risk of Data Breaches**:
  Proactive phishing simulations minimize the likelihood of successful attacks and compromised data.

- **Strengthened Security Culture**:
  Reinforces user vigilance while testing and improving cybersecurity reporting channels and response processes.

- **Improved Incident Response**:
  By simulating real-world attacks, organizations can assess user and team readiness, enabling faster, more effective responses to actual threats.

When it comes to campaign specifications, the following options are offered by Bitdefender:

Scenario Crafting:

- **Client has a scenario in mind:** Bitdefender consultants will understand the client's scenario and evaluate its feasibility in terms of success and setup.
- **Client has no scenario in consideration:** Bitdefender consultants will craft 2-3 phishing scenarios to choose from.

Type of Campaign:

- **Click-Only Campaign:** The campaign will only allow the target users to click the phishing link. Submission of credentials will not be a part of the campaign.
- **Click & Credential Gathering Campaign:** The campaign entices the victim to submit credentials after clicking the phishing link. Usually in the form of a spoofed SSO login page *(e.g. Microsoft, Google, Okta)*. Only usernames and masked passwords will be harvested.
- **Malware-based Campaign:** The campaign entices the target users to download malware via attachment or certain URLs. Only the IP and authenticated usernames/hostnames will be harvested.

End of Campaign:

- **Education Page:** After credential submission, the target users will be presented with an education page (e.g. Mandatory Security Awareness Training). The target users will be notified that it is a phishing exercise after completing the flow of the campaign.
- **Proper Final Page:** A final page will be designed to complete and fit the phishing scenario. This minimizes the chances of the target users realizing that it is a phishing exercise.

After gathering all relevant data and findings, we conduct a detailed analysis of the phishing campaign's outcomes. The final report includes key insights and actionable intelligence, featuring:

- **Response Time Analysis:** Measures the time taken for target users to recognize a phishing attempt and report it through official channels.
- **Resiliency Assessment:** Evaluates the ratio of employees who successfully reported the phishing attempt versus those who fell victim, providing a clear resilience metric.
- **Industry Benchmarking:** Compares the organization's phishing susceptibility rate against industry peers of similar size, offering valuable context.
- **Departmental Risk Analysis:** Identifies the top three departments with the highest phishing susceptibility rates, enabling targeted security awareness initiatives.

Romania HQ
Orhideea Towers
15A Orhideelor Road,
6th District,
Bucharest 060071

T: +40 21 4412452

US HQ
6301 NW 5th Way,
#4300,
Fort Lauderdale,
FL, 33309

T: +1 954-776-6262