THREAT SIMULATION
OF THE MOMENT

NEW

Active Directory Compomise

BLACKNOISE

PLATFORM

BlackNoise is the first European breach & attack simulation platform, and aims to assess, evaluate & improve your Cyber capabilities in real conditions.

THREAT SCENARIOS

The platform includes comprehensive presets for threat scenarios (APT, ransomware, wiper, data leak, etc.) and over 1,000 security events, with continuous updates.

>_ ABOUT AD COMPROMISE

This simulation replicates threat actor behaviors to compromise Windows domain environments; focusing on AD discovery, credential theft, privilege escalation and persistence. It assesses the ability to detect and respond to various technical actions at several stage of an attack.

>_ WHY PLAY THIS SIMULATION ?

Active threat
Active Directory (AD) remains a prime target for attackers due to its central role in managing authentication, permissions, and access across enterprise networks. Compromising AD grants threat actors broad control over critical systems, enabling lateral movement, data exfiltration, and persistence. Its widespread use and complexity make it challenging to secure fully, leaving gaps for exploitation.

Demonstrate Compliance

RGPD ☐ NIS 2 ☑ DORA ☑

Risk assessment

Espionage ☑ Destruction ☑ Data breach & leak ☑

Insider ☑ External attack ☐

Security solution assessed

EDR ☑ NDR ☑ EPP ☑

HONEY POT ☑ FW / PROXY ☑ DLP / DLD ☐

SYSTEM LOGS ☑ ID/PS ☑ SIEM ☑

SIMULATION DETAILS

>_ COMPOSITION

13 high severity events

9 low severity events

>_ TARGETS

Network, Windows, Linux, MacOs, AWS, MS Azure, Google Cloud

>_ ATTACK SCOPE

MITRE ATT&CK matrix

>_ RULES ASSOCIATED

Suricata Rules

Sigma Rules

>_ TECHNICAL DETAILS OF BLACKNOISE SIMULATION

To address this kind of threat, you must validate your capabilities to detect technical adversary behaviors in a short time frame, and validate the effectiveness of your investigation & reaction strategy. For this simulation, BlackNoise will execute the following actions :

- Session Creation: WMI Password Authentication
- System Information Discovery
- System Network Configuration Discovery
- System Service Discovery
- Account Discovery: Local Account
- Domain Information Discovery
- Account Discovery: Domain Account
- OS Credential Dumping: Security Account Manager
- OS Credential Dumping: Shadow Copy
- Steal or Forge Kerberos Tickets: Kerberos Ticket Dump
- OS Credential Dumping: Microsoft IIS App Pool
- Create Account: Local Account
- Steal or Forge Kerberos Tickets: Kerberoasting (Account Listing)
- Steal or Forge Kerberos Tickets: Kerberoasting (Ticket Request)
- Active Directory - Kerberos Constrained Delegation
- Active Directory - Kerberos Resource based constrained Delegation
- Active Directory - Kerberos Unconstrained Delegation
- Account Discovery: Domain Account
- LAPS Password Dump
- Add Computer account to Domain
- OS Credential Dumping: NTDS
- OS Credential Dumping: DCSync

>_ STRENGTHEN YOUR DETECTION CAPABILITIES

To effectively tackle this threat model, BlackNoise strongly recommends implementing the following actions:

- Enable WMI and Powershell Logging: Activate detailed logging (Event IDs `4688`, `4104`, `5861`) to monitor suspicious WMI and Powershell activities such as credential dumping and Kerberos ticket theft.
- Deploy Sysmon: Use Sysmon to capture advanced events like process creation (Event ID 1) and registry modifications, particularly for monitoring access to LSASS and NTDS.dit files.
- Monitor Kerberos Events: Track Kerberos event IDs (`4768`, `4769`, `4770`, `4771`) to detect anomalies such as Kerberoasting or ticket reuse.
- WMI Filtering: Restrict WMI usage to essential accounts and create alerts for unauthorized or excessive WMI activity.
- Account Monitoring: Enable event logging for account creation and modification (Event IDs `4720`, `4726`) to detect rogue accounts.
- LDAP Query Monitoring: Monitor LDAP traffic for high-frequency or unusual queries, especially those related to constrained delegation or account discovery.
- DCSync Detection: Monitor for DCSync behavior by setting alerts on replication
- Implement JEA (Just Enough Administration): Minimize administrative privilege misuse by restricting the scope of administrative actions.
- Process Anomaly Detection: Set up alerts for processes accessing LSASS or dumping SAM files, which indicate credential theft attempts.

For additional technical recommendations, visit the BlackNoise platform or [contact us](#).

CONTACT
contact@blacknoise.co