THREAT SIMULATION
OF THE MOMENT

UPDATE

APT 29

aka Cozy Bear / Nobelium / Midnight Blizzard

B|ACKNO|SE

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 APT 29

APT29, also known as Cozy Bear, is a Russian cyber espionage group linked to the SVR. It employs advanced tactics to gather sensitive data, particularly government, military, and economic information. The group gained attention for the SolarWinds breach in 2020.

>_ WHY PLAY THIS SIMULATION ?

Active threat

To address this kind of threat, you must validate your capabilities to detect the following technical adversary behaviors in a short time frame, and validate the effectiveness of your investigation & reaction strategy. It helps to adjust security policies, such as detection rules, network segmentation or privilege management, in the face of advanced attack behaviors.

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

🟥 4 high severity events

🟨 24 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 :

- Network Service Discovery: Command Execution Slow TCP SYN Scan
- Network Service Discovery: Web TCP Connect Scan
- Network Service Discovery: Windows TCP SYN Scan
- Active Scanning: Web Vulnerability Scanning
- Brute Force: SMB password guessing & password spraying
- Brute Force: RDP password guessing & password spraying
- Brute Force: SSH password guessing & password spraying
- Session Creation: SMB Password Authentication
- Session Creation: WMI Password Authentication
- Impair Defenses: Disable Defender AMSI
- Impair Defenses: Disable Defender ATP
- Masquerading: Rename Powershell Executable
- Process Discovery
- OS Credential Dumping: Security Account Manager
- Steal or Forge Kerberos Tickets: Kerberos Ticket Dump
- Session Creation: WMI Pass-the-Ticket Authentication
- Ingress Tool Transfer: SysInternals Suite
- Scheduled Task/Job: Create Local Account
- Registry IFEO Debugger Persistence
- Account Discovery: Local Account
- System Information Discovery
- Account Discovery: Local & Domain Account
- Account Discovery: Domain Account
- Account Discovery: Domain Account
- Steal or Forge Kerberos Tickets: Kerberoasting

>_ STRENGTHEN YOUR DETECTION CAPABILITIES

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

- Configure IDS/IPS (e.g., Snort or Suricata): Identify frequent SYN scans indicative of port scanning.
- Set Alerts for SMB, RDP, and SSH Behavior: Enforce limits on login attempts per user per minute using tools like fail2ban or firewall rules.
- Enable Advanced PowerShell Logging: Activate `ScriptBlockLogging` and Module Logging to track PowerShell activities.
- Monitor Anomalous Commands: Use SIEM solutions to detect unusual commands, such as attempts to disable AMSI or ATP.
- Detect Extensive WMI Usage: Identify unusual task executions via tools like Sysmon (`ID 11` for scheduled task creation).
- Enable Kerberos Event Logging:
  - Monitor Event `4769` (Kerberos Service Ticket Request) to identify suspicious requests (e.g., Kerberoasting).
  - Monitor Event `4771` (Failed Kerberos Pre-authentication) to detect brute force attacks.
- Monitor for Suspicious Tool Usage: Track the use of `certutil.exe`, `bitsadmin.exe`, and `PsExec.exe`. Block and log the use of SysInternals tools if unnecessary

For additional technical recommendations, visit the BlackNoise platform or contact us for more information.

BLACKNOISE
NEVER TRUST. ALWAYS **CHECK**.

CONTACT
contact@blacknoise.co