Threat Actor Profiling:

- **Threat Actor:** Midnight Blizzard
- **Other Names:** NOBELIUM, APT29, UNC2452, Cozy Bear
- **Country:** Russia
- **Affiliation:** Foreign Intelligence Service of the Russian Federation (SVR)
- **Motivation:** Espionage and intelligence collection
- **Active Since:** 2018

Techniques:

1. **Social Engineering:** Uses credential theft phishing lures sent as Microsoft Teams chats.
2. **Compromise of Microsoft 365 Tenants:** Uses previously compromised Microsoft 365 tenants to create new domains that appear as technical support entities for further phishing attacks.
3. **MFA Prompt Bombing:** Engages users to approve MFA prompts via social engineering messages.
4. **Token Theft:** Regularly utilizes token theft techniques for initial access.
5. **Password Spraying:** Uses password spray attacks tailored to avoid detection.
6. **Authentication Spear-Phishing:** Utilizes spoofed identity/credential phishing attempts.
7. **Supply Chain Attacks:** Exploits trusted relationships between service providers and downstream customers.
8. **OAuth Application Abuse:** Misuses OAuth applications to maintain access and conduct post-compromise activity.
9. **Advanced Techniques to Compromise Authentication Mechanisms:** Includes exploitation of AD FS via FOGGYWEB and MAGICWEB malwares.
10. **HTML Smuggling:** Hides first-stage JavaScript dropper in malicious HTML attachments.

Commonly Used Malware:

- FOGGYWEB
- MAGICWEB
- ROOTSAW (EnvyScout)
- WINELOADER
- GraphicalProton
- TEARDROP
- GoldMax

Report Excerpts:

- **Activity Date:** Late May 2023
    - **Title:** Highly Targeted Social Engineering Attacks
    - **Details:** Used credential theft phishing lures via Microsoft Teams, leveraging previously compromised tenants for further attacks targeting MFA approval.
- **Activity Date:** September 6, 2023
    - **Title:** Exploitation of TeamCity Vulnerability
    - **Details:** Leveraged CVE-2023-42793 to conduct remote code execution and post-exploitation activities using GraphicalProton malware.
- **Activity Date:** January 12, 2024
    - **Title:** Credential Theft and Post-Compromise Activities
    - **Details:** Detected and mitigated an extensive phishing campaign targeting Microsoft systems, involving OAuth abuse and password spray attacks.
- **Activity Date:** February 2024
    - **Title:** Phishing Campaign Targeting German Political Parties

    - **Details:** Used ROOTSAW to deliver WINELOADER backdoor, representing a shift to targeting political entities alongside traditional diplomatic targets.

- **Activity Date:** Late February 2024
    - **Title:** Increased Phishing Operations in Ukraine
    - **Details:** Targeted foreign embassies in Ukraine, including Moscow·s partners, with phishing emails to collect intelligence amidst Ukraine's counteroffensive.

Attribution:

- **Government:**
    - US Government
    - UK Government
- **Security Organizations:**
    - Microsoft Threat Intelligence
    - Mandiant
    - Recorded Future

Targets:

- Government Entities
- Diplomatic Entities
- Non-Governmental Organizations (NGOs)
- IT Service Providers
- Technology Sector
- Discrete Manufacturing
- Media Sector
- Political Parties

Recommendations:

- Enable and enforce MFA for all user accounts.
- Regularly audit and restrict OAuth applications.
- Reinforce social engineering detection training among users.
- Implement robust password policies to defend against password spray attacks.
- Monitor for suspicious MFA prompt activity and other login anomalies.
- Update software and systems to patch known vulnerabilities promptly.

Hunting Actions:

- **Credential Theft Phishing Lures via Microsoft Teams**
    - Identify and track phishing lures sent via Microsoft Teams chats.
    - Detect new domain creation by compromised small business tenants.
    - Monitor for requests to create new onmicrosoft.com subdomains.
    - Alert for MFA prompt engagement requests initiated by external users.
- **Credential Attack Campaigns**
    - Detect token theft techniques for initial access.
    - Monitor for signs of authentication spear-phishing, password spray, brute force, and other credential attacks.
    - Identify activity using Microsoft 365 tenants owned by small businesses for malicious purposes.

- **Post-compromise Activities**
  - Alert on information theft indicators from compromised Microsoft 365 tenants.
  - Monitor attempts to add new devices to the organization as managed devices via Microsoft Entra ID.
  - Log any anomalous device additions or policy circumvention attempts.
- **OAuth Application Abuse**
  - Track and alert on malicious OAuth application creation or modification within a tenant.
  - Flag excessive or unusual permission grants to OAuth applications.
  - Monitor OAuth application's suspicious API activity.
- **Remote Code Execution via CVE-2023-42793**
  - Detect unauthorized access to vulnerable JetBrains TeamCity versions.
  - Monitor application and system logs for signs of exploitation.
  - Track IP addresses and commands executed remotely on vulnerable servers.
  - Watch for attempts to install or execute malicious DLL files.
- **Custom Exploit Script Usage**
  - Detect the use of Nuclei vulnerability scanner templates targeting CVE-2023-42793.
  - Alert on HTTP requests indicative of exploitation attempts.
  - Monitor for indicators of multiple threat actors exploiting the same vulnerability.
- **WINELOADER and ROOTSAW Campaigns**
  - Track spear-phishing emails containing malicious links or attachments.
  - Monitor HTTP requests to domains like 'waterforvoiceless[.]org' for payload downloads.
  - Inspect downloaded payloads for file and directory creation activities.
  - Watch for execution of Windows binaries by malicious JavaScript payloads.
- **GraphicalProton Malware Usage**
  - Detect malicious DLL files with indicators matching GraphicalProton Yara rules.
  - Observe execution of suspicious scheduled tasks invoking malicious DLLs.
  - Monitor network connections to malicious C2 servers or unexpected services like Microsoft OneDrive and Dropbox.

MITRE ATT&CK Matrix:

- **Reconnaissance:**
  - Active Scanning
  - Search Open Technical Databases
  - Search Open Websites/Domains
- **Resource Development:**
  - Compromise Accounts
  - Compromise Infrastructure
- **Initial Access:**
  - Exploit Public-Facing Application
  - External Remote Services
  - Phishing
  - Replication Through Removable Media
  - Supply Chain Compromise

  - Trusted Relationship
  - Valid Accounts

- **Execution:**
  - Command and Scripting Interpreter
  - Inter-Process Communication
  - Native API
  - Scheduled Task/Job
  - Shared Modules
  - System Services
  - Windows Management Instrumentation

- **Persistence:**
  - Create Account
  - Event Triggered Execution
  - Hijack Execution Flow
  - Scheduled Task/Job
  - Server Software Component

- **Privilege Escalation:**
  - Access Token Manipulation
  - Hijack Execution Flow
  - Scheduled Task/Job

- **Defense Evasion:**
  - Deobfuscate/Decode Files or Information
  - Execution Guardrails
  - Hijack Execution Flow
  - Indicator Removal
  - Masquerading
  - Obfuscated Files or Information
  - System Binary Proxy Execution

- **Credential Access:**
  - Brute Force
  - Credentials from Password Stores
  - OS Credential Dumping
  - Steal Application Access Token
  - Steal Web Session Cookie

- **Discovery:**
  - Domain Trust Discovery
  - File and Directory Discovery
  - Network Service Discovery
  - Process Discovery
  - Query Registry
  - System Information Discovery
  - System Network Configuration Discovery
  - System Owner/User Discovery
  - System Service Discovery

- **Lateral Movement:**
  - Exploitation of Remote Services
  - Remote Services

    - Remote Service Session Hijacking
    - Replication Through Removable Media
    - Software Deployment Tools
    - Use Alternate Authentication Material

- **Collection:**
    - Browser Session Hijacking
    - Clipboard Data
    - Data from Information Repositories
    - Email Collection
    - Input Capture

- **Command and Control:**
    - Application Layer Protocol
    - Data Encoding
    - Data Obfuscation
    - Dynamic Resolution
    - Encrypted Channel
    - Protocol Tunneling
    - Proxy
    - Remote Access Software

- **Exfiltration:**
    - Exfiltration Over C2 Channel
    - Transfer Data to Cloud Account

- **Impact:**
    - Data Destruction
    - Data Encrypted for Impact