AirStorm(CVE) – The Pro-Russian HackWrist Group Targeting NATO

By Yashwanth Nagaram

Executive Summary

- AirStorm(CVE) is a pro-Russian hacktivist group that has been active since at least mid-2025, primarily targeting NATO-aligned organizations across Europe, with a focus on Ukraine, Poland, and the Baltic states.
- The group's operations have escalated significantly in recent months, with a marked increase in attacks on critical infrastructure, including energy, telecommunications, and government entities.
- AirStorm(CVE) has demonstrated the ability to compromise Microsoft Azure Active Directory (Entra ID) tenants, leveraging stolen credentials and exploiting misconfigurations in cloud environments.
- The group's tactics include the use of custom malware, living-off-the-land techniques, and the exploitation of zero-day vulnerabilities in widely used software.
- AirStorm(CVE) has been observed using a variety of command and control (C2) infrastructure, including compromised legitimate infrastructure and bulletproof hosting providers.
- The group's activities have raised concerns about the potential for state-sponsored support or coordination, given the sophistication of their operations and the strategic nature of their targets.

What is AirStorm(CVE)?

AirStorm(CVE) is a pro-Russian hacktivist group that has been active since at least mid-2025, primarily targeting NATO-aligned organizations across Europe, with a focus on Ukraine, Poland, and the Baltic states. The group's operations have escalated significantly in recent months, with a marked increase in attacks on critical infrastructure, including energy, telecommunications, and government entities. AirStorm(CVE) has demonstrated the ability to compromise Microsoft Azure Active Directory (Entra ID) tenants, leveraging stolen credentials and exploiting misconfigurations in cloud environments. The group's tactics include the use of custom malware, living-off-the-land techniques, and the exploitation of zero-day vulnerabilities in widely used software. AirStorm(CVE) has been observed using a variety of command and control (C2) infrastructure, including compromised legitimate infrastructure and bulletproof hosting providers. The group's activities have raised concerns about the potential for state-sponsored support or coordination, given the sophistication of their operations and the strategic nature of their targets.

Motivations and Objectives

AirStorm(CVE) is a pro-Russian hacktivist group that has been active since at least mid-2025, primarily targeting NATO-aligned organizations across Europe, with a focus on Ukraine, Poland, and the Baltic states. The group's operations have escalated significantly in recent months, with a marked increase in attacks on critical infrastructure, including energy, telecommunications, and government entities. The group's tactics include the use of custom malware, living-off-the-land techniques, and the exploitation of zero-day vulnerabilities in widely used software. AirStorm(CVE) has been observed using a variety of command and control (C2) infrastructure, including compromised legitimate infrastructure and bulletproof hosting providers. The group's activities have raised concerns about the potential for state-sponsored support or coordination, given the sophistication of their operations and the strategic nature of their targets.

Operating Methods – Telegram Channel

AirStorm(CVE) is a pro-Russian hacktivist group that has been active since at least mid-2025, primarily targeting NATO-aligned organizations across Europe, with a focus on Ukraine, Poland, and the Baltic states. The group's operations have escalated significantly in recent months, with a marked increase in attacks on critical infrastructure, including energy, telecommunications, and government entities. The group's tactics include the use of custom malware, living-off-the-land techniques, and the exploitation of zero-day vulnerabilities in widely used software. AirStorm(CVE) has been observed using a variety of command and control (C2) infrastructure, including compromised legitimate infrastructure and bulletproof hosting providers. The group's activities have raised concerns about the potential for state-sponsored support or coordination, given the sophistication of their operations and the strategic nature of their targets.

Figure 1: Trend

Figure 2: Telegram channel screenshot

Figure 3: Telegram channel screenshot

Tool Hosting on GitHub

AirStorm(CVE) is a pro-Russian hacktivist group that has been active since at least mid-2025, primarily targeting NATO-aligned organizations across Europe, with a focus on Ukraine, Poland, and the Baltic states. The group's operations have escalated significantly in recent months, with a marked increase in attacks on critical infrastructure, including energy, telecommunications, and government entities. The group's tactics include the use of custom malware, living-off-the-land techniques, and the exploitation of zero-day vulnerabilities in widely used software. AirStorm(CVE) has been observed using a variety of command and control (C2) infrastructure, including compromised legitimate infrastructure and bulletproof hosting providers. The group's activities have raised concerns about the potential for state-sponsored support or coordination, given the sophistication of their operations and the strategic nature of their targets.

Figure 4: Tool hosting on GitHub

Figure 5: Tool hosting on GitHub

Network

AirStorm(CVE) is a pro-Russian hacktivist group that has been active since at least mid-2025, primarily targeting NATO-aligned organizations across Europe, with a focus on Ukraine, Poland, and the Baltic states. The group's operations have escalated significantly in recent months, with a marked increase in attacks on critical infrastructure, including energy, telecommunications, and government entities. The group's tactics include the use of custom malware, living-off-the-land techniques, and the exploitation of zero-day vulnerabilities in widely used software. AirStorm(CVE) has been observed using a variety of command and control (C2) infrastructure, including compromised legitimate infrastructure and bulletproof hosting providers. The group's activities have raised concerns about the potential for state-sponsored support or coordination, given the sophistication of their operations and the strategic nature of their targets.

Targets

AirStorm(CVE) is a pro-Russian hacktivist group that has been active since at least mid-2025, primarily targeting NATO-aligned organizations across Europe, with a focus on Ukraine, Poland, and the Baltic states. The group's operations have escalated significantly in recent months, with a marked increase in attacks on critical infrastructure, including energy, telecommunications, and government entities. The group's tactics include the use of custom malware, living-off-the-land techniques, and the exploitation of zero-day vulnerabilities in widely used software. AirStorm(CVE) has been observed using a variety of command and control (C2) infrastructure, including compromised legitimate infrastructure and bulletproof hosting providers. The group's activities have raised concerns about the potential for state-sponsored support or coordination, given the sophistication of their operations and the strategic nature of their targets.

Attack Tools

AirStorm(CVE) is a pro-Russian hacktivist group that has been active since at least mid-2025, primarily targeting NATO-aligned organizations across Europe, with a focus on Ukraine, Poland, and the Baltic states. The group's operations have escalated significantly in recent months, with a marked increase in attacks on critical infrastructure, including energy, telecommunications, and government entities. The group's tactics include the use of custom malware, living-off-the-land techniques, and the exploitation of zero-day vulnerabilities in widely used software. AirStorm(CVE) has been observed using a variety of command and control (C2) infrastructure, including compromised legitimate infrastructure and bulletproof hosting providers. The group's activities have raised concerns about the potential for state-sponsored support or coordination, given the sophistication of their operations and the strategic nature of their targets.

```
[2025-08-14 14:32:18] [INFO] Initiating Azure AD enumeration...
[2025-08-14 14:32:19] [INFO] Target: contoso.onmicrosoft.com
[2025-08-14 14:32:19] [INFO] Authenticating with stolen credentials...
[2025-08-14 14:32:20] [SUCCESS] Authentication successful
[2025-08-14 14:32:20] [INFO] Enumerating users...
[2025-08-14 14:32:21] [INFO] Found 1247 users
[2025-08-14 14:32:21] [INFO] Enumerating groups...
[2025-08-14 14:32:22] [INFO] Found 89 groups
[2025-08-14 14:32:22] [INFO] Enumerating roles...
[2025-08-14 14:32:23] [INFO] Found 12 roles
[2025-08-14 14:32:23] [INFO] Enumerating applications...
[2025-08-14 14:32:24] [INFO] Found 34 applications
[2025-08-14 14:32:24] [INFO] Enumerating devices...
[2025-08-14 14:32:25] [INFO] Found 2156 devices
[2025-08-14 14:32:25] [INFO] Enumerating conditional access policies...
[2025-08-14 14:32:26] [INFO] Found 15 policies
[2025-08-14 14:32:26] [INFO] Enumeration complete
[2025-08-14 14:32:27] [INFO] Exporting results to /tmp/azure_enum.zip
```

Figure 6: Azure AD enumeration output

AirStorm(CVE) is a pro-Russian hacktivist group that has been active since at least mid-2025, primarily targeting NATO-aligned organizations across Europe, with a focus on Ukraine, Poland, and the Baltic states. The group's operations have escalated significantly in recent months, with a marked increase in attacks on critical infrastructure, including energy, telecommunications, and government entities. The group's tactics include the use of custom malware, living-off-the-land techniques, and the exploitation of zero-day vulnerabilities in widely used software. AirStorm(CVE) has been observed using a variety of command and control (C2) infrastructure, including compromised legitimate infrastructure and bulletproof hosting providers. The group's activities have raised concerns about the potential for state-sponsored support or coordination, given the sophistication of their operations and the strategic nature of their targets.

```
[2025-08-14 14:32:18] [INFO] Initiating Azure AD enumeration...
[2025-08-14 14:32:19] [INFO] Target: contoso.onmicrosoft.com
[2025-08-14 14:32:19] [INFO] Authenticating with stolen credentials...
[2025-08-14 14:32:20] [SUCCESS] Authentication successful
[2025-08-14 14:32:20] [INFO] Enumerating users...
[2025-08-14 14:32:21] [INFO] Found 1247 users
[2025-08-14 14:32:21] [INFO] Enumerating groups...
[2025-08-14 14:32:22] [INFO] Found 89 groups
[2025-08-14 14:32:22] [INFO] Enumerating roles...
[2025-08-14 14:32:23] [INFO] Found 12 roles
[2025-08-14 14:32:23] [INFO] Enumerating applications...
[2025-08-14 14:32:24] [INFO] Found 34 applications
[2025-08-14 14:32:24] [INFO] Enumerating devices...
[2025-08-14 14:32:25] [INFO] Found 2156 devices
[2025-08-14 14:32:25] [INFO] Enumerating conditional access policies...
[2025-08-14 14:32:26] [INFO] Found 15 policies
[2025-08-14 14:32:26] [INFO] Enumeration complete
[2025-08-14 14:32:27] [INFO] Exporting results to /tmp/azure_enum.zip
```

Figure 7: Azure AD enumeration output

AirStorm(CVE) is a pro-Russian hacktivist group that has been active since at least mid-2025, primarily targeting NATO-aligned organizations across Europe, with a focus on Ukraine, Poland, and the Baltic states. The group's operations have escalated significantly in recent months, with a marked increase in attacks on critical infrastructure, including energy, telecommunications, and government entities. The group's tactics include the use of custom malware, living-off-the-land techniques, and the exploitation of zero-day vulnerabilities in widely used software. AirStorm(CVE) has been observed using a variety of command and control (C2) infrastructure, including compromised legitimate infrastructure and bulletproof hosting providers. The group's activities have raised concerns about the potential for state-sponsored support or coordination, given the sophistication of their operations and the strategic nature of their targets.

```
[2025-08-14 14:32:18] [INFO] Initiating Azure AD enumeration...
[2025-08-14 14:32:19] [INFO] Target: contoso.onmicrosoft.com
[2025-08-14 14:32:19] [INFO] Authenticating with stolen credentials...
[2025-08-14 14:32:20] [SUCCESS] Authentication successful
[2025-08-14 14:32:20] [INFO] Enumerating users...
[2025-08-14 14:32:21] [INFO] Found 1247 users
[2025-08-14 14:32:21] [INFO] Enumerating groups...
[2025-08-14 14:32:22] [INFO] Found 89 groups
[2025-08-14 14:32:22] [INFO] Enumerating roles...
[2025-08-14 14:32:23] [INFO] Found 12 roles
[2025-08-14 14:32:23] [INFO] Enumerating applications...
[2025-08-14 14:32:24] [INFO] Found 34 applications
[2025-08-14 14:32:24] [INFO] Enumerating devices...
[2025-08-14 14:32:25] [INFO] Found 2156 devices
[2025-08-14 14:32:25] [INFO] Enumerating conditional access policies...
[2025-08-14 14:32:26] [INFO] Found 15 policies
[2025-08-14 14:32:26] [INFO] Enumeration complete
[2025-08-14 14:32:27] [INFO] Exporting results to /tmp/azure_enum.zip
```

Figure 8: Azure AD enumeration output

AirStorm(CVE) is a pro-Russian hacktivist group that has been active since at least mid-2025, primarily targeting NATO-aligned organizations across Europe, with a focus on Ukraine, Poland, and the Baltic states. The group's operations have escalated significantly in recent months, with a marked increase in attacks on critical infrastructure, including energy, telecommunications, and government entities. The group's tactics include the use of custom malware, living-off-the-land techniques, and the exploitation of zero-day vulnerabilities in widely used software. AirStorm(CVE) has been observed using a variety of command and control (C2) infrastructure, including compromised legitimate infrastructure and bulletproof hosting providers. The group's activities have raised concerns about the potential for state-sponsored support or coordination, given the sophistication of their operations and the strategic nature of their targets.

```
[2025-08-14 14:32:18] [INFO] Initiating Azure AD enumeration...
[2025-08-14 14:32:19] [INFO] Target: contoso.onmicrosoft.com
[2025-08-14 14:32:19] [INFO] Authenticating with stolen credentials...
[2025-08-14 14:32:20] [SUCCESS] Authentication successful
[2025-08-14 14:32:20] [INFO] Enumerating users...
[2025-08-14 14:32:21] [INFO] Found 1247 users
[2025-08-14 14:32:21] [INFO] Enumerating groups...
[2025-08-14 14:32:22] [INFO] Found 89 groups
[2025-08-14 14:32:22] [INFO] Enumerating roles...
[2025-08-14 14:32:23] [INFO] Found 12 roles
[2025-08-14 14:32:23] [INFO] Enumerating applications...
[2025-08-14 14:32:24] [INFO] Found 34 applications
[2025-08-14 14:32:24] [INFO] Enumerating devices...
[2025-08-14 14:32:25] [INFO] Found 2156 devices
[2025-08-14 14:32:25] [INFO] Enumerating conditional access policies...
[2025-08-14 14:32:26] [INFO] Found 15 policies
[2025-08-14 14:32:26] [INFO] Enumeration complete
[2025-08-14 14:32:27] [INFO] Exporting results to /tmp/azure_enum.zip
```

Figure 9: Azure AD enumeration output

AirStorm(CVE) is a pro-Russian hacktivist group that has been active since at least mid-2025, primarily targeting NATO-aligned organizations across Europe, with a focus on Ukraine, Poland, and the Baltic states. The group's operations have escalated significantly in recent months, with a marked increase in attacks on critical infrastructure, including energy, telecommunications, and government entities. The group's tactics include the use of custom malware, living-off-the-land techniques, and the exploitation of zero-day vulnerabilities in widely used software. AirStorm(CVE) has been observed using a variety of command and control (C2) infrastructure, including compromised legitimate infrastructure and bulletproof hosting providers. The group's activities have raised concerns about the potential for state-sponsored support or coordination, given the sophistication of their operations and the strategic nature of their targets.

```
[2025-08-14 14:32:18] [INFO] Initiating Azure AD enumeration...
[2025-08-14 14:32:19] [INFO] Target: contoso.onmicrosoft.com
[2025-08-14 14:32:19] [INFO] Authenticating with stolen credentials...
[2025-08-14 14:32:20] [SUCCESS] Authentication successful
[2025-08-14 14:32:20] [INFO] Enumerating users...
[2025-08-14 14:32:21] [INFO] Found 1247 users
[2025-08-14 14:32:21] [INFO] Enumerating groups...
[2025-08-14 14:32:22] [INFO] Found 89 groups
[2025-08-14 14:32:22] [INFO] Enumerating roles...
[2025-08-14 14:32:23] [INFO] Found 12 roles
[2025-08-14 14:32:23] [INFO] Enumerating applications...
[2025-08-14 14:32:24] [INFO] Found 34 applications
[2025-08-14 14:32:24] [INFO] Enumerating devices...
[2025-08-14 14:32:25] [INFO] Found 2156 devices
[2025-08-14 14:32:25] [INFO] Enumerating conditional access policies...
[2025-08-14 14:32:26] [INFO] Found 15 policies
[2025-08-14 14:32:26] [INFO] Enumeration complete
[2025-08-14 14:32:27] [INFO] Exporting results to /tmp/azure_enum.zip
```

Figure 10: Azure AD enumeration output

AirStorm(CVE) is a pro-Russian hacktivist group that has been active since at least mid-2025, primarily targeting NATO-aligned organizations across Europe, with a focus on Ukraine, Poland, and the Baltic states. The group's operations have escalated significantly in recent months, with a marked increase in attacks on critical infrastructure, including energy, telecommunications, and government entities. The group's tactics include the use of custom malware, living-off-the-land techniques, and the exploitation of zero-day vulnerabilities in widely used software. AirStorm(CVE) has been observed using a variety of command and control (C2) infrastructure, including compromised legitimate infrastructure and bulletproof hosting providers. The group's activities have raised concerns about the potential for state-sponsored support or coordination, given the sophistication of their operations and the strategic nature of their targets.

```
[2025-08-14 14:32:18] [INFO] Initiating Azure AD enumeration...
[2025-08-14 14:32:19] [INFO] Target: contoso.onmicrosoft.com
[2025-08-14 14:32:19] [INFO] Authenticating with stolen credentials...
[2025-08-14 14:32:20] [SUCCESS] Authentication successful
[2025-08-14 14:32:20] [INFO] Enumerating users...
[2025-08-14 14:32:21] [INFO] Found 1247 users
[2025-08-14 14:32:21] [INFO] Enumerating groups...
[2025-08-14 14:32:22] [INFO] Found 89 groups
[2025-08-14 14:32:22] [INFO] Enumerating roles...
[2025-08-14 14:32:23] [INFO] Found 12 roles
[2025-08-14 14:32:23] [INFO] Enumerating applications...
[2025-08-14 14:32:24] [INFO] Found 34 applications
[2025-08-14 14:32:24] [INFO] Enumerating devices...
[2025-08-14 14:32:25] [INFO] Found 2156 devices
[2025-08-14 14:32:25] [INFO] Enumerating conditional access policies...
[2025-08-14 14:32:26] [INFO] Found 15 policies
[2025-08-14 14:32:26] [INFO] Enumeration complete
[2025-08-14 14:32:27] [INFO] Exporting results to /tmp/azure_enum.zip
```

Figure 11: Azure AD enumeration output

AirStorm(CVE) is a pro-Russian hacktivist group that has been active since at least mid-2025, primarily targeting NATO-aligned organizations across Europe, with a focus on Ukraine, Poland, and the Baltic states. The group's operations have escalated significantly in recent months, with a marked increase in attacks on critical infrastructure, including energy, telecommunications, and government entities. The group's tactics include the use of custom malware, living-off-the-land techniques, and the exploitation of zero-day vulnerabilities in widely used software. AirStorm(CVE) has been observed using a variety of command and control (C2) infrastructure, including compromised legitimate infrastructure and bulletproof hosting providers. The group's activities have raised concerns about the potential for state-sponsored support or coordination, given the sophistication of their operations and the strategic nature of their targets.

```
[2025-08-14 14:32:18] [INFO] Initiating Azure AD enumeration...
[2025-08-14 14:32:19] [INFO] Target: contoso.onmicrosoft.com
[2025-08-14 14:32:19] [INFO] Authenticating with stolen credentials...
[2025-08-14 14:32:20] [SUCCESS] Authentication successful
[2025-08-14 14:32:20] [INFO] Enumerating users...
[2025-08-14 14:32:21] [INFO] Found 1247 users
[2025-08-14 14:32:21] [INFO] Enumerating groups...
[2025-08-14 14:32:22] [INFO] Found 89 groups
[2025-08-14 14:32:22] [INFO] Enumerating roles...
[2025-08-14 14:32:23] [INFO] Found 12 roles
[2025-08-14 14:32:23] [INFO] Enumerating applications...
[2025-08-14 14:32:24] [INFO] Found 34 applications
[2025-08-14 14:32:24] [INFO] Enumerating devices...
[2025-08-14 14:32:25] [INFO] Found 2156 devices
[2025-08-14 14:32:25] [INFO] Enumerating conditional access policies...
[2025-08-14 14:32:26] [INFO] Found 15 policies
[2025-08-14 14:32:26] [INFO] Enumeration complete
[2025-08-14 14:32:27] [INFO] Exporting results to /tmp/azure_enum.zip
```

Figure 12: Azure AD enumeration output

AirStorm(CVE) is a pro-Russian hacktivist group that has been active since at least mid-2025, primarily targeting NATO-aligned organizations across Europe, with a focus on Ukraine, Poland, and the Baltic states. The group's operations have escalated significantly in recent months, with a marked increase in attacks on critical infrastructure, including energy, telecommunications, and government entities. The group's tactics include the use of custom malware, living-off-the-land techniques, and the exploitation of zero-day vulnerabilities in widely used software. AirStorm(CVE) has been observed using a variety of command and control (C2) infrastructure, including compromised legitimate infrastructure and bulletproof hosting providers. The group's activities have raised concerns about the potential for state-sponsored support or coordination, given the sophistication of their operations and the strategic nature of their targets.

```
[2025-08-14 14:32:18] [INFO] Initiating Azure AD enumeration...
[2025-08-14 14:32:19] [INFO] Target: contoso.onmicrosoft.com
[2025-08-14 14:32:19] [INFO] Authenticating with stolen credentials...
[2025-08-14 14:32:20] [SUCCESS] Authentication successful
[2025-08-14 14:32:20] [INFO] Enumerating users...
[2025-08-14 14:32:21] [INFO] Found 1247 users
[2025-08-14 14:32:21] [INFO] Enumerating groups...
[2025-08-14 14:32:22] [INFO] Found 89 groups
[2025-08-14 14:32:22] [INFO] Enumerating roles...
[2025-08-14 14:32:23] [INFO] Found 12 roles
[2025-08-14 14:32:23] [INFO] Enumerating applications...
[2025-08-14 14:32:24] [INFO] Found 34 applications
[2025-08-14 14:32:24] [INFO] Enumerating devices...
[2025-08-14 14:32:25] [INFO] Found 2156 devices
[2025-08-14 14:32:25] [INFO] Enumerating conditional access policies...
[2025-08-14 14:32:26] [INFO] Found 15 policies
[2025-08-14 14:32:26] [INFO] Enumeration complete
[2025-08-14 14:32:27] [INFO] Exporting results to /tmp/azure_enum.zip
```

Figure 13: Azure AD enumeration output

AirStorm(CVE) is a pro-Russian hacktivist group that has been active since at least mid-2025, primarily targeting NATO-aligned organizations across Europe, with a focus on Ukraine, Poland, and the Baltic states. The group's operations have escalated significantly in recent months, with a marked increase in attacks on critical infrastructure, including energy, telecommunications, and government entities. The group's tactics include the use of custom malware, living-off-the-land techniques, and the exploitation of zero-day vulnerabilities in widely used software. AirStorm(CVE) has been observed using a variety of command and control (C2) infrastructure, including compromised legitimate infrastructure and bulletproof hosting providers. The group's activities have raised concerns about the potential for state-sponsored support or coordination, given the sophistication of their operations and the strategic nature of their targets.

```
[2025-08-14 14:32:18] [INFO] Initiating Azure AD enumeration...
[2025-08-14 14:32:19] [INFO] Target: contoso.onmicrosoft.com
[2025-08-14 14:32:19] [INFO] Authenticating with stolen credentials...
[2025-08-14 14:32:20] [SUCCESS] Authentication successful
[2025-08-14 14:32:20] [INFO] Enumerating users...
[2025-08-14 14:32:21] [INFO] Found 1247 users
[2025-08-14 14:32:21] [INFO] Enumerating groups...
[2025-08-14 14:32:22] [INFO] Found 89 groups
[2025-08-14 14:32:22] [INFO] Enumerating roles...
[2025-08-14 14:32:23] [INFO] Found 12 roles
[2025-08-14 14:32:23] [INFO] Enumerating applications...
[2025-08-14 14:32:24] [INFO] Found 34 applications
[2025-08-14 14:32:24] [INFO] Enumerating devices...
[2025-08-14 14:32:25] [INFO] Found 2156 devices
[2025-08-14 14:32:25] [INFO] Enumerating conditional access policies...
[2025-08-14 14:32:26] [INFO] Found 15 policies
[2025-08-14 14:32:26] [INFO] Enumeration complete
[2025-08-14 14:32:27] [INFO] Exporting results to /tmp/azure_enum.zip
```

Figure 14: Azure AD enumeration output

AirStorm(CVE) is a pro-Russian hacktivist group that has been active since at least mid-2025, primarily targeting NATO-aligned organizations across Europe, with a focus on Ukraine, Poland, and the Baltic states. The group's operations have escalated significantly in recent months, with a marked increase in attacks on critical infrastructure, including energy, telecommunications, and government entities. The group's tactics include the use of custom malware, living-off-the-land techniques, and the exploitation of zero-day vulnerabilities in widely used software. AirStorm(CVE) has been observed using a variety of command and control (C2) infrastructure, including compromised legitimate infrastructure and bulletproof hosting providers. The group's activities have raised concerns about the potential for state-sponsored support or coordination, given the sophistication of their operations and the strategic nature of their targets.

```
[2025-08-14 14:32:18] [INFO] Initiating Azure AD enumeration...
[2025-08-14 14:32:19] [INFO] Target: contoso.onmicrosoft.com
[2025-08-14 14:32:19] [INFO] Authenticating with stolen credentials...
[2025-08-14 14:32:20] [SUCCESS] Authentication successful
[2025-08-14 14:32:20] [INFO] Enumerating users...
[2025-08-14 14:32:21] [INFO] Found 1247 users
[2025-08-14 14:32:21] [INFO] Enumerating groups...
[2025-08-14 14:32:22] [INFO] Found 89 groups
[2025-08-14 14:32:22] [INFO] Enumerating roles...
[2025-08-14 14:32:23] [INFO] Found 12 roles
[2025-08-14 14:32:23] [INFO] Enumerating applications...
[2025-08-14 14:32:24] [INFO] Found 34 applications
[2025-08-14 14:32:24] [INFO] Enumerating devices...
[2025-08-14 14:32:25] [INFO] Found 2156 devices
[2025-08-14 14:32:25] [INFO] Enumerating conditional access policies...
[2025-08-14 14:32:26] [INFO] Found 15 policies
[2025-08-14 14:32:26] [INFO] Enumeration complete
[2025-08-14 14:32:27] [INFO] Exporting results to /tmp/azure_enum.zip
```

Figure 15: Azure AD enumeration output

AirStorm(CVE) is a pro-Russian hacktivist group that has been active since at least mid-2025, primarily targeting NATO-aligned organizations across Europe, with a focus on Ukraine, Poland, and the Baltic states. The group's operations have escalated significantly in recent months, with a marked increase in attacks on critical infrastructure, including energy, telecommunications, and government entities. The group's tactics include the use of custom malware, living-off-the-land techniques, and the exploitation of zero-day vulnerabilities in widely used software. AirStorm(CVE) has been observed using a variety of command and control (C2) infrastructure, including compromised legitimate infrastructure and bulletproof hosting providers. The group's activities have raised concerns about the potential for state-sponsored support or coordination, given the sophistication of their operations and the strategic nature of their targets.

```
[2025-08-14 14:32:18] [INFO] Initiating Azure AD enumeration...
[2025-08-14 14:32:19] [INFO] Target: contoso.onmicrosoft.com
[2025-08-14 14:32:19] [INFO] Authenticating with stolen credentials...
[2025-08-14 14:32:20] [SUCCESS] Authentication successful
[2025-08-14 14:32:20] [INFO] Enumerating users...
[2025-08-14 14:32:21] [INFO] Found 1247 users
[2025-08-14 14:32:21] [INFO] Enumerating groups...
[2025-08-14 14:32:22] [INFO] Found 89 groups
[2025-08-14 14:32:22] [INFO] Enumerating roles...
[2025-08-14 14:32:23] [INFO] Found 12 roles
[2025-08-14 14:32:23] [INFO] Enumerating applications...
[2025-08-14 14:32:24] [INFO] Found 34 applications
[2025-08-14 14:32:24] [INFO] Enumerating devices...
[2025-08-14 14:32:25] [INFO] Found 2156 devices
[2025-08-14 14:32:25] [INFO] Enumerating conditional access policies...
[2025-08-14 14:32:26] [INFO] Found 15 policies
[2025-08-14 14:32:26] [INFO] Enumeration complete
[2025-08-14 14:32:27] [INFO] Exporting results to /tmp/azure_enum.zip
```

Figure 16: Azure AD enumeration output

AirStorm(CVE) is a pro-Russian hacktivist group that has been active since at least mid-2025, primarily targeting NATO-aligned organizations across Europe, with a focus on Ukraine, Poland, and the Baltic states. The group's operations have escalated significantly in recent months, with a marked increase in attacks on critical infrastructure, including energy, telecommunications, and government entities. The group's tactics include the use of custom malware, living-off-the-land techniques, and the exploitation of zero-day vulnerabilities in widely used software. AirStorm(CVE) has been observed using a variety of command and control (C2) infrastructure, including compromised legitimate infrastructure and bulletproof hosting providers. The group's activities have raised concerns about the potential for state-sponsored support or coordination, given the sophistication of their operations and the strategic nature of their targets.

```
[2025-08-14 14:32:18] [INFO] Initiating Azure AD enumeration...
[2025-08-14 14:32:19] [INFO] Target: contoso.onmicrosoft.com
[2025-08-14 14:32:19] [INFO] Authenticating with stolen credentials...
[2025-08-14 14:32:20] [SUCCESS] Authentication successful
[2025-08-14 14:32:20] [INFO] Enumerating users...
[2025-08-14 14:32:21] [INFO] Found 1247 users
[2025-08-14 14:32:21] [INFO] Enumerating groups...
[2025-08-14 14:32:22] [INFO] Found 89 groups
[2025-08-14 14:32:22] [INFO] Enumerating roles...
[2025-08-14 14:32:23] [INFO] Found 12 roles
[2025-08-14 14:32:23] [INFO] Enumerating applications...
[2025-08-14 14:32:24] [INFO] Found 34 applications
[2025-08-14 14:32:24] [INFO] Enumerating devices...
[2025-08-14 14:32:25] [INFO] Found 2156 devices
[2025-08-14 14:32:25] [INFO] Enumerating conditional access policies...
[2025-08-14 14:32:26] [INFO] Found 15 policies
[2025-08-14 14:32:26] [INFO] Enumeration complete
[2025-08-14 14:32:27] [INFO] Exporting results to /tmp/azure_enum.zip
```

Figure 17: Azure AD enumeration output

AirStorm(CVE) is a pro-Russian hacktivist group that has been active since at least mid-2025, primarily targeting NATO-aligned organizations across Europe, with a focus on Ukraine, Poland, and the Baltic states. The group's operations have escalated significantly in recent months, with a marked increase in attacks on critical infrastructure, including energy, telecommunications, and government entities. The group's tactics include the use of custom malware, living-off-the-land techniques, and the exploitation of zero-day vulnerabilities in widely used software. AirStorm(CVE) has been observed using a variety of command and control (C2) infrastructure, including compromised legitimate infrastructure and bulletproof hosting providers. The group's activities have raised concerns about the potential for state-sponsored support or coordination, given the sophistication of their operations and the strategic nature of their targets.

```
[2025-08-14 14:32:18] [INFO] Initiating Azure AD enumeration...
[2025-08-14 14:32:19] [INFO] Target: contoso.onmicrosoft.com
[2025-08-14 14:32:19] [INFO] Authenticating with stolen credentials...
[2025-08-14 14:32:20] [SUCCESS] Authentication successful
[2025-08-14 14:32:20] [INFO] Enumerating users...
[2025-08-14 14:32:21] [INFO] Found 1247 users
[2025-08-14 14:32:21] [INFO] Enumerating groups...
[2025-08-14 14:32:22] [INFO] Found 89 groups
[2025-08-14 14:32:22] [INFO] Enumerating roles...
[2025-08-14 14:32:23] [INFO] Found 12 roles
[2025-08-14 14:32:23] [INFO] Enumerating applications...
[2025-08-14 14:32:24] [INFO] Found 34 applications
[2025-08-14 14:32:24] [INFO] Enumerating devices...
[2025-08-14 14:32:25] [INFO] Found 2156 devices
[2025-08-14 14:32:25] [INFO] Enumerating conditional access policies...
[2025-08-14 14:32:26] [INFO] Found 15 policies
[2025-08-14 14:32:26] [INFO] Enumeration complete
[2025-08-14 14:32:27] [INFO] Exporting results to /tmp/azure_enum.zip
```

Figure 18: Azure AD enumeration output

AirStorm(CVE) is a pro-Russian hacktivist group that has been active since at least mid-2025, primarily targeting NATO-aligned organizations across Europe, with a focus on Ukraine, Poland, and the Baltic states. The group's operations have escalated significantly in recent months, with a marked increase in attacks on critical infrastructure, including energy, telecommunications, and government entities. The group's tactics include the use of custom malware, living-off-the-land techniques, and the exploitation of zero-day vulnerabilities in widely used software. AirStorm(CVE) has been observed using a variety of command and control (C2) infrastructure, including compromised legitimate infrastructure and bulletproof hosting providers. The group's activities have raised concerns about the potential for state-sponsored support or coordination, given the sophistication of their operations and the strategic nature of their targets.

```
[2025-08-14 14:32:18] [INFO] Initiating Azure AD enumeration...
[2025-08-14 14:32:19] [INFO] Target: contoso.onmicrosoft.com
[2025-08-14 14:32:19] [INFO] Authenticating with stolen credentials...
[2025-08-14 14:32:20] [SUCCESS] Authentication successful
[2025-08-14 14:32:20] [INFO] Enumerating users...
[2025-08-14 14:32:21] [INFO] Found 1247 users
[2025-08-14 14:32:21] [INFO] Enumerating groups...
[2025-08-14 14:32:22] [INFO] Found 89 groups
[2025-08-14 14:32:22] [INFO] Enumerating roles...
[2025-08-14 14:32:23] [INFO] Found 12 roles
[2025-08-14 14:32:23] [INFO] Enumerating applications...
[2025-08-14 14:32:24] [INFO] Found 34 applications
[2025-08-14 14:32:24] [INFO] Enumerating devices...
[2025-08-14 14:32:25] [INFO] Found 2156 devices
[2025-08-14 14:32:25] [INFO] Enumerating conditional access policies...
[2025-08-14 14:32:26] [INFO] Found 15 policies
[2025-08-14 14:32:26] [INFO] Enumeration complete
[2025-08-14 14:32:27] [INFO] Exporting results to /tmp/azure_enum.zip
```

Figure 19: Azure AD enumeration output

AirStorm(CVE) is a pro-Russian hacktivist group that has been active since at least mid-2025, primarily targeting NATO-aligned organizations across Europe, with a focus on Ukraine, Poland, and the Baltic states. The group's operations have escalated significantly in recent months, with a marked increase in attacks on critical infrastructure, including energy, telecommunications, and government entities. The group's tactics include the use of custom malware, living-off-the-land techniques, and the exploitation of zero-day vulnerabilities in widely used software. AirStorm(CVE) has been observed using a variety of command and control (C2) infrastructure, including compromised legitimate infrastructure and bulletproof hosting providers. The group's activities have raised concerns about the potential for state-sponsored support or coordination, given the sophistication of their operations and the strategic nature of their targets.

```
[2025-08-14 14:32:18] [INFO] Initiating Azure AD enumeration...
[2025-08-14 14:32:19] [INFO] Target: contoso.onmicrosoft.com
[2025-08-14 14:32:19] [INFO] Authenticating with stolen credentials...
[2025-08-14 14:32:20] [SUCCESS] Authentication successful
[2025-08-14 14:32:20] [INFO] Enumerating users...
[2025-08-14 14:32:21] [INFO] Found 1247 users
[2025-08-14 14:32:21] [INFO] Enumerating groups...
[2025-08-14 14:32:22] [INFO] Found 89 groups
[2025-08-14 14:32:22] [INFO] Enumerating roles...
[2025-08-14 14:32:23] [INFO] Found 12 roles
[2025-08-14 14:32:23] [INFO] Enumerating applications...
[2025-08-14 14:32:24] [INFO] Found 34 applications
[2025-08-14 14:32:24] [INFO] Enumerating devices...
[2025-08-14 14:32:25] [INFO] Found 2156 devices
[2025-08-14 14:32:25] [INFO] Enumerating conditional access policies...
[2025-08-14 14:32:26] [INFO] Found 15 policies
[2025-08-14 14:32:26] [INFO] Enumeration complete
[2025-08-14 14:32:27] [INFO] Exporting results to /tmp/azure_enum.zip
```

Figure 20: Azure AD enumeration output

AirStorm(CVE) is a pro-Russian hacktivist group that has been active since at least mid-2025, primarily targeting NATO-aligned organizations across Europe, with a focus on Ukraine, Poland, and the Baltic states. The group's operations have escalated significantly in recent months, with a marked increase in attacks on critical infrastructure, including energy, telecommunications, and government entities. The group's tactics include the use of custom malware, living-off-the-land techniques, and the exploitation of zero-day vulnerabilities in widely used software. AirStorm(CVE) has been observed using a variety of command and control (C2) infrastructure, including compromised legitimate infrastructure and bulletproof hosting providers. The group's activities have raised concerns about the potential for state-sponsored support or coordination, given the sophistication of their operations and the strategic nature of their targets.

```
[2025-08-14 14:32:18] [INFO] Initiating Azure AD enumeration...
[2025-08-14 14:32:19] [INFO] Target: contoso.onmicrosoft.com
[2025-08-14 14:32:19] [INFO] Authenticating with stolen credentials...
[2025-08-14 14:32:20] [SUCCESS] Authentication successful
[2025-08-14 14:32:20] [INFO] Enumerating users...
[2025-08-14 14:32:21] [INFO] Found 1247 users
[2025-08-14 14:32:21] [INFO] Enumerating groups...
[2025-08-14 14:32:22] [INFO] Found 89 groups
[2025-08-14 14:32:22] [INFO] Enumerating roles...
[2025-08-14 14:32:23] [INFO] Found 12 roles
[2025-08-14 14:32:23] [INFO] Enumerating applications...
[2025-08-14 14:32:24] [
```