

Lazarus Group: 5.56%

[Lazarus Group](<https://attack.mitre.org/groups/G0032>) is a North Korean state-sponsored cyber threat actor.

Type: "intrusion-set"

Domains: "enterprise-attack, ics-attack"

Aliases: "Lazarus Group, Labyrinth Chollima, HIDDEN COBRA, Guardians of Peace, ZINC, NICKEL"

x_mitre_version: "4.0"

External references: [{"Source Name": "mitre-attack", "URL": "[https://attack.mitre.org/groups/G0032](\"https://attack.mitre.org/groups/G0032\")"}]

Related Attack Patterns: [{"Exploitation": [{"ID": "T1059.003", "Name": "Windows Command Shell", "T": "T1059.003", "Name": "Windows Command Shell"}]}

Tools and Malware used by group: [{"ID": "S0364", "Name": "RawDisk", "Type": "tool", "Description": "RawDisk is a tool used to access raw disk data. It is often used by malware to retrieve sensitive information from a disk, such as passwords, emails, and other personal data. RawDisk is a command-line tool that can be used to access raw disk data from a remote system. It is often used by malware to retrieve sensitive information from a disk, such as passwords, emails, and other personal data. RawDisk is a command-line tool that can be used to access raw disk data from a remote system."}]

Campaigns attributed to group: [{"ID": "C0022", "Name": "Operation■Dream Job", "Type": "campaign",

Sandworm Team: 5.56%

[Sandworm Team](<https://attack.mitre.org/groups/G0034>) is a ■ destructive threat group that has been

Domains: "enterprise-attack, ics-attack, mobile-attack"

Aliases: "Sandworm Team, ELECTRUM, Telebots, IRON VIKING, BlackEnergy█(Group), Quedagh, V

x_mitre_version: "4.0"

External references: [{"Source Name": "mitre-attack", "URL": "█https://attack.mitre.org/groups/G0034"}]

Related Attack Patterns: [{"Weaponization": [{"ID": "T1588.006", "Name": "Vulnerabilities", "Type": "at

Tools and Malware used by group: [{"ID": "S0002", "Name": "Mimikatz", "Type": "tool", "Description": "Mimikatz is a tool used to extract plaintext passwords, API keys, and other sensitive information from memory. It is often used by attackers to gain unauthorized access to systems and networks."}]

Campaigns attributed to group: [{"ID": "C0028", "Name": "2015 Ukraine█Electric Power Attack", "Type": "Cyber", "Status": "Active", "Priority": "High", "Description": "A series of cyberattacks targeting the Ukrainian power grid in 2015, resulting in a major blackout. The attacks were attributed to a group of hackers known as 'Electric Blue'."}]

APT38: 5.56%

[APT38](<https://attack.mitre.org/groups/G0082>) is a North Korean state-sponsored threat group that s

Type: "intrusion-set"

Domains: "enterprise-attack, ics-attack"

Aliases: "APT38, NICKEL GLADSTONE, BeagleBoyz, Bluenoroff, Stardust, Chollima, Sapphire Sleet,

x_mitre_version: "3.0"

External references: [{"Source Name": "mitre-attack", "URL": "[https://attack.mitre.org/groups/G0082](\"https://attack.mitre.org/groups/G0082\")"}]

Related Attack Patterns: [{"Action On Objectives": [{"ID": "T1486", "Name": "Data Encrypted for Impact"}]}

Tools and Malware used by group: [{"ID": "S0039", "Name": "Net", "Type": "tool", "Description": "The"}]

APT37: 5.56%

[APT37](https://attack.mitre.org/groups/G0067) is a North Korean state-sponsored cyber espionage group

Type: "intrusion-set"

Domains: "enterprise-attack"

Aliases: "APT37, InkySquid, ScarCruft, Reaper, Group123, TEMP.Reaper, Ricochet Chollima"

x_mitre_version: "2.0"

External references: [{"Source Name": "mitre-attack", "URL": "https://attack.mitre.org/groups/G0067"}]

Related Attack Patterns: [{"Installation": [{"ID": "T1547.001", "Name": "Registry Run Keys / Startup Folder"}]}]

Tools and Malware used by group: [{"ID": "S0657", "Name": "BLUELIGHT", "Type": "malware", "Desc

FIN7: 5.56%

[FIN7](https://attack.mitre.org/groups/G0046) is a financially-motivated threat group that has been ac

Type: "intrusion-set"

Domains: "enterprise-attack, ics-attack"

Aliases: "FIN7, GOLD NIAGARA, ITG14, Carbon Spider, ELBRUS, SangriaTempest"

x_mitre_version: "4.0"

External references: [{"Source Name": "mitre-attack", "URL": "https://attack.mitre.org/groups/G0046"}]

Related Attack Patterns: [{"Exploitation": [{"ID": "T1204.001", "Name": "Malicious Link", "Type": "attac

Tools and Malware used by group: [{"ID": "S0002", "Name": "Mimikatz", "Type": "tool", "Description": "Mimikatz is a tool used to extract plaintext passwords from the memory of local and remote systems. It is often used by attackers to gain unauthorized access to systems and networks."}]

