ECHO

CYBER THREAT INTELLIGENCE

İNTELLİGENCE REPORT 2023

ATTACK REPORT ON THE ENERGY SECTOR

Content

Executive Summary

This executive summary addresses the significance and impacts of cyberattacks targeting the energy sector. In recent years, cyberattacks in the energy sector have become a significant threat to businesses. These attacks target critical areas such as the infrastructure of energy companies, energy production systems, distribution networks, and even energy trading platforms.

The energy sector is in a vulnerable position when it comes to cyberattacks. The protection of critical infrastructure and data in the sector is of utmost importance for ensuring the continuity of energy production and energy security. Cyberattacks can lead to serious consequences, including data theft, operational disruptions, and jeopardizing the energy supply.

In recent years, there has been a noticeable increase in the number of cyberattacks in the energy sector. This increase underscores the need for energy companies to be better prepared to counter cyber threats. According to Eurocontrol reports, cyberattacks have increased by at least 530% annually over the past four years. This demonstrates the necessity of implementing comprehensive security measures to enhance the security of the energy sector.

Cyber attackers continuously evolve their techniques and tactics to overcome security measures. These attackers are motivated by various goals, including financial gain, disrupting energy supply, engaging in espionage activities, or showcasing their cyberattack capabilities.

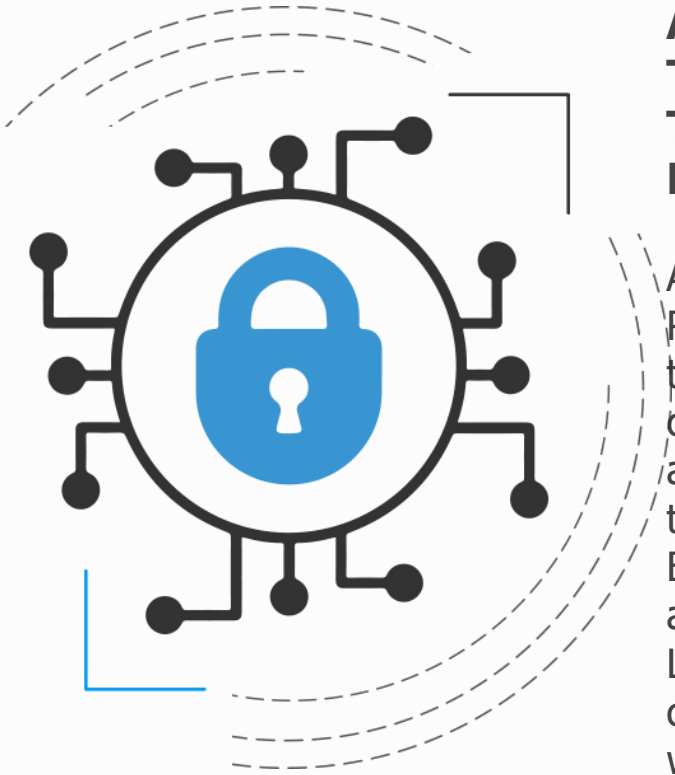
The energy sector is an area where cybersecurity must continually stay up to date. To prevent future threats, the sector must regularly review its security policies, invest in personnel training, and closely monitor technological developments.

This report aims to raise awareness among executives in the energy sector about the threats posed by cyberattacks and to assist them in taking the necessary measures to protect their companies and the sector as a whole. Cybersecurity must become a top priority for the energy sector to ensure its continuity and security.

Incidents and Events in 2023

Cyber Attack Attempt on Ukraine's Energy Sector

Ukraine's critical energy infrastructure was effectively defended against a cyber attack attempt orchestrated by the Russian threat actor known as APT28, by the Computer Emergency Response Team of Ukraine (CERT-UA). It was reported that the attack, which began with a phishing email containing a malicious ZIP archive, involved remote command execution.



A Malicious Software Family Targeting the Energy and Telecom Sectors Detected on LinkedIn – RedEnergy –

A new malicious software named RedEnergy has been discovered, aiming to maximize damage to victims by combining data theft with encryption in attacks targeting the energy, oil, gas, telecom, and machinery sectors in Brazil and the Philippines. Threat actors, who reached out through LinkedIn profiles, were found to conduct a phishing campaign with fake web browser updates.

YoroTrooper: Cyber Espionage Campaign Targeting Government and Energy Sectors Uncovered

YoroTrooper, an unidentified cyber threat actor, has been operating as part of a sophisticated cyber espionage campaign targeting governments, the energy sector, and international organizations in Europe since June 2022. Among the data stolen in successful attacks are identity information, browser histories and cookies, system details, and screen captures.

NikoWiper Malware Targeting Ukraine's Energy Sector Uncovered

It has been determined that the cyber threat actor known as Sandworm, associated with Russia, used a wiper malware named NikoWiper as part of an attack targeting an energy sector company in Ukraine. These attacks appear to share similar targets with missile strikes by the Russian armed forces on Ukraine's energy infrastructure, indicating a concerning alignment of objectives.

Iranian Government-Backed Hacker Group Targets U.S. Energy and Transportation Systems

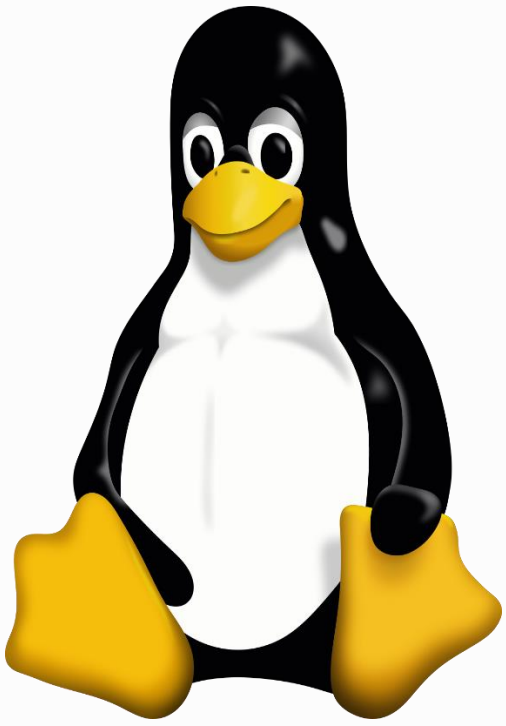
An Iran government-backed threat actor known as Mint Sandstorm has been linked to attacks targeting the critical infrastructure of the United States from late 2021 to the middle of 2022. According to an analysis by the Microsoft Threat Intelligence team, this Mint Sandstorm sub-group exhibits technical and operational sophistication, the capability to develop custom tools, and a rapid ability to exploit N-day (zero-day) vulnerabilities. They have demonstrated agility in alignment with Iran's national priorities in their operational focus.

Security Vulnerabilities in Industrial Control Systems on the Rise: Over One-Third Unpatched in 2023

Approximately 34% of security vulnerabilities affecting industrial control systems (ICS) reported in the first half of 2023 have no fixes or patches available. This represents a significant increase from the 13% reported the previous year. In the first half of 2023 alone, a total of 670 ICS product vulnerabilities were reported through the U.S. Cybersecurity and Infrastructure Security Agency (CISA).

Space Pirates Launches Cyber Campaign in Russia and Serbia]

The threat actor known as Space Pirates has been associated with attacks against at least 16 organizations in Russia and Serbia over the past year, employing new tactics and drawing attention by adding new cyber weapons to their arsenal. Targets include government agencies, educational institutions, private security companies, aerospace manufacturers, agricultural producers, defense, energy, and



ChamelDoH: New Linux Backdoor Utilizing DNS-over-HTTPS Tunneling for Covert CnC

The threat actor known as ChamelGang has been observed expanding its capabilities by deploying an undocumented implant to establish a backdoor on Linux systems. This malicious software, named ChamelDoH, is a tool developed in the C++ language that communicates via DNS-over-HTTPS (DoH) tunneling. It first emerged in September 2021 and has been detailed in attacks targeting the fuel, energy, and aerospace manufacturing industries in Russia, the United States, India, Nepal, Taiwan, and Japan.]

APT28 Targets Ukrainian Government Institutions with Fake "Windows Update" Emails

The Computer Emergency Response Team of Ukraine (CERT-UA) has issued a warning regarding cyber attacks carried out by Russian state-sponsored hackers targeting various government institutions in the country. This phishing campaign was conducted by the APT28 group. It was found that the subject line of the attack emails was "Windows Update" and they contained Ukrainian-language instructions, allegedly instructing recipients to execute a PowerShell command under the guise of security updates.

Lazarus X_TRADER Attack Extends Beyond 3CX Breach, Impacts Electrical and Energy Sectors' Electrocritical Infrastructures]

Lazarus, the renowned hacking group from North Korea, was behind a series of supply chain attacks targeting 3CX, and additionally, it impacted two critical infrastructure organizations and two businesses engaged in financial transactions using the Trojanized X_TRADER application.

Iranian Government-Backed Hackers Found to Target U.S. Energy and Transportation Systems

An actor known as Mint Sandstorm, supported by the Iranian government, has been linked to attacks on critical infrastructure in the United States from late 2021 to the middle of 2022. Targeted institutions include seaports, energy companies, transportation systems, and a major U.S. energy and gas company. These activities are believed to have been carried out in retaliation for attacks on maritime, railway, and gas station payment systems between May 2020 and the end of 2021.

CISA Issues Warning About Critical ICS Vulnerabilities Affecting Hitachi Energy, mySCADA, ICL, and Nexx Products

The United States Cybersecurity and Infrastructure Security Agency (CISA) has issued eight Industrial Control Systems (ICS) advisories, disclosing critical vulnerabilities affecting products from Hitachi Energy, mySCADA Technologies,

Microsoft Outlook Vulnerability Exploited in Attacks Targeting Government Institutions

Threat actors believed to be supported by the Russian government targeted numerous government institutions in the energy, military, and transportation sectors using the "CVE-2023-23397" Outlook vulnerability, which allows for the retrieval of NTLM

ESXiArgs Ransomware Attack Targets Numerous Institutions in Europe

The ESXiArgs ransomware has caused damage in a total of 14 energy institutions by targeting computers using outdated ESXi versions or failing to apply security updates.

Lazarus Targets Unpatched Zimbra Devices

North Korea's Lazarus Group-affiliated cyber attackers have initiated a new cyber espionage campaign by targeting Zimbra devices without security updates. The attacks were organized to infiltrate supply chains of the energy, research, defense, and healthcare sectors. It is estimated that the attackers may have stolen approximately 100 GB of data by targeting these devices without the updates.

Large-Scale QR Code Phishing Attack Targets Energy Companies

Beginning in May 2023, a large-scale phishing campaign utilizing QR codes is targeting leading energy companies in the United States. The attack aims to steal users' Microsoft credentials using QR codes, with the energy sector prominently featured in this campaign. The use of QR codes can provide an advantage in bypassing anti-phishing solutions, contributing to the campaign's growth of over 2,400% since May. The misuse of QR codes in this manner indicates that cyber threat actors are experimenting with new tactics.

Australian Software Provider ENERGY ONE Falls Victim to Cyberattack

Australian software provider Energy One has disclosed that it fell victim to a cyberattack affecting specific corporate systems. Following the incident, the company initiated an investigation and provided information to the Australian Cyber Security Centre and relevant UK authorities. In response to the attack, the company disabled some connections between corporate and customer-focused systems. The initial vector of the attack and the identity of the attackers remain undetermined, and it is uncertain whether threat actors gained access to customer data as a result of the attack.

Critical Vulnerability Exploited in Energy Sector: CVE-2022-29303

The security vulnerability CVE-2022-29303 found in the solar energy monitoring product Contec SolarView continues to pose a potential threat to organizations in the energy sector. Observations indicate that a new variant of the Mirai botnet is also targeting this vulnerability. Using Shodan, over 615 SolarView installations were found on the internet, with 425 of them running vulnerable versions. As a result, the number of affected organizations in the energy sector continues to grow day by day.

Schneider Electric and Siemens Energy Fall Victim to MOVEit Attack]

The Clop ransomware group has added five new MOVEit (CVE-2023-34362) attack victims, including industry giants like Schneider Electric and Siemens Energy, to a dark web leak site. The list of leaked victims includes:

- werum.com
- Schneider Electric (http://se.com)
- Siemens Energy (http://siemens-energy.com)
- UCLA (http://ucla.edu)
- Abbie (http://abbvie.com)

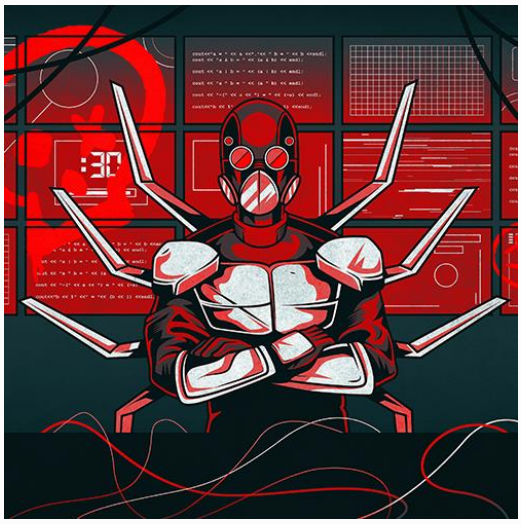
Energy Company Suncor Hit by Cyberattack at Petro-Canada Gas Stations in Canada]

Suncor Energy experienced a cyberattack that affected payment transactions at Petro-Canada gas stations in Canada. Customers at the affected gas stations were unable to make payments with credit cards. Suncor took immediate steps to investigate the incident with the assistance of third-party experts.

APT Groups Targeting the Energy Sector in 2023

Our team's investigations have revealed that several APT groups have been targeting the energy sector since the beginning of this year. For informational purposes, the following information about these APT groups is included in the report.

Bitwise SPIDER



Bitwise Spider APT Group: Bitwise Spider is an APT group that primarily targets government agencies, large corporations, and countries with critical infrastructures, especially in the defense, energy, communication, and technology sectors.

Vulnerabilities and attack techniques employed in their attacks:

- Active Directory
- Shadow copy
- UAC Bypass
- ESXI

Bitwise Spider infiltrates target networks using advanced attack vectors, including phishing emails, exploiting security vulnerabilities, injecting malware, employing social engineering tactics, and utilizing advanced process hijacking techniques.

The Bitwise Spider APT group employs customized malicious software tailored for espionage activities, often making it challenging to detect using advanced malware analysis methods. There are two known malware families developed by the Bitwise Spider group: LockBit Ransomware and StealBit InfoStealer Malware.

The impacts of the Bitwise Spider APT group on organizations include:

1. Data Theft
2. Reputational Damage
3. Financial Losses
4. Reduced Competitive Advantage
5. Increased Attack Costs

For IoC's, please click here.

Berserk Bear

Berserk Bear, also known as Energetic Bear or Dragonfly, is an Advanced Persistent Threat (APT) group engaged in cyber espionage activities.

The primary focus of Berserk Bear's operations is organizations within the energy sector, particularly energy grids, oil and gas companies, and other critical infrastructure providers.

By gaining unauthorized access to these systems, the group aims to gather intelligence, disrupt operations, and establish control over vital resources.

Berserk Bear employs various advanced techniques and tactics to achieve its objectives. These include spear-phishing campaigns where carefully crafted emails, often containing malicious attachments or links, are sent to specific individuals. The group also resorts to watering hole attacks, compromising legitimate websites frequented by their target organizations to deliver malware or exploit vulnerabilities.

Notably, Berserk Bear is known for its ability to exploit vulnerabilities in software and systems used in industrial control systems (ICS). This capability to breach critical infrastructure poses significant risks to the targeted organizations and the overall stability of affected sectors.

The group gained international attention for its role in disrupting Ukraine's energy grids in 2015 and 2016, highlighting its capabilities and potential impact. While the energy sector remains its primary focus, Berserk Bear's attacks on organizations in other sectors and countries, including the United States and Europe, are also documented.

Due to the need for operational secrecy, detailed information about Berserk Bear is often limited and closely guarded. Security researchers and government agencies continue to monitor the group's activities to understand and counter the threats posed by this persistent and highly capable APT group.

APT28

APT28, also known as "Fancy Bear" or "Sofacy Group," is an advanced cyber espionage and cyberattack group associated with Russia.

The activities of this group are often alleged to have connections to the Russian government or Russian intelligence agencies.

APT28 is known as a group that has been active since 2007, and it has carried out complex cyberattacks targeting various objectives.

APT28, also known as "Fancy Bear" or "Sofacy Group," is an advanced cyber espionage and cyberattack group associated with Russia. While it's unclear exactly which Russian agency APT28 is linked to, this group may have connections with separate units that use Russia's cyber espionage capabilities. APT28 has been active since 2007 and has been involved in various international incidents.

Areas of Operation:

APT28 is known for cyberattacks targeting regions of strategic interest to Russia, including NATO countries, European governments, Ukraine, and Georgia. They have also been active in attempting to interfere in international politics and elections, including efforts to interfere in U.S. elections.

Attack Techniques:

APT28 employs advanced and sophisticated cyberattack techniques. They excel in methods like spear phishing (targeted fake emails), malware delivery, and penetration techniques. They also have the ability to monitor the networks of targeted organizations over extended periods, enabling them to gather intelligence and understand their targets more effectively.

Known Attacks:

APT28 has been involved in a series of high-profile attacks worldwide. Their attempts to interfere in the 2016 U.S. presidential elections garnered significant attention. Additionally, they have been associated with attacks on Ukraine, cyberattacks against NATO institutions, and espionage activities in the European energy sector.

Purpose and Targets:

The motivations and objectives of APT28 are debated, but they are generally believed to serve Russia's national interests or support the political goals of the Russian government. This group operates to gather strategic, military, and political intelligence and can use this information for various purposes.

For IoC's, please click here.

APT31

APT31, also known as Zirconium, is an advanced persistent threat (APT) group.

This group is believed to be predominantly China-based and is a sophisticated cyber espionage group.

APT31 operates with the purpose of cyber espionage, information gathering, and conducting other cyber attacks.

Key Features:

1. Association with the Chinese Government: APT31 is known as a cyber espionage group associated with the Chinese government, although the Chinese government often denies such relationships.
2. Sophisticated Attacks: APT31 conducts sophisticated and complex attacks against its targets. These attacks can involve advanced malware, zero-day exploits, and intricate network penetration techniques.
3. Information Gathering: The group operates to gather information, particularly from companies in technology, energy, aerospace, and military sectors. This information can be used to support the strategic interests of the Chinese government.
4. Long-Term Operations: APT31 works towards long-term objectives and has the capability to monitor organizations' networks over extended periods. This allows them to better understand their targets.

Known Attacks:

APT31 is believed to have been involved in various high-profile attacks worldwide. It is particularly associated with intellectual property theft, cyber espionage against technology companies, and intelligence operations against foreign governments.

Purpose and Targets:

The primary motives and targets of APT31 are believed to align with the national interests of China or to support the political goals of the Chinese government. The group operates to steal strategic information and technology.

For IoC's, please click here.

APT34

APT34, also known as OILRIG, is an advanced persistent threat (APT) group based in Iran.

This group is considered an intelligence unit conducting cyber espionage and cyber attacks to support Iran's strategic interests.

APT34 has the capability to conduct cyber attacks across various sectors and is believed to be backed by the Iranian government.

Key Features:

1. Connection to the Iranian Government: APT34 is closely associated with the Iranian government and operates as a cyber espionage group to support Iran's strategic interests.
2. Diverse Range of Targets: APT34 carries out attacks on various sectors, including energy, defense, telecommunications, finance, and government. Targets often include foreign governments, companies, and countries with strategic positions.
3. Social Engineering Skills: The group uses social engineering tactics to infiltrate its targets. This can involve manipulation and fraud to gain the trust of victims and spread malicious software.
4. Malware Expertise: APT34 is skilled in the use of malicious software. It particularly employs various types of malware to infiltrate its targets.

Known Attacks:

One of APT34's most notable attacks is the Phosphorus campaign, which targeted numerous governments and private sector organizations worldwide. This campaign involves cyber espionage and information-gathering operations targeting specific entities.

Purpose and Targets:

APT34 operates to protect and advance the strategic interests of the Iranian government. Its targets include foreign governments, the energy sector, military defense, and strategic information.

For IoC's, please click here.

Mint Sandstorm

Mint Sandstorm, also known as an advanced persistent threat (APT) group, is a cyber attack group engaged in cyber espionage activities.

This group primarily targets high-profile entities such as governments, military institutions, and large enterprises in the Asia-Pacific region.

Mint Sandstorm is known as a disciplined actor that conducts sophisticated and targeted cyber attacks.

Key Features:

1. Asia-Pacific Focus: Mint Sandstorm primarily focuses on targets in the Asia-Pacific region. This region includes governments, defense institutions, and economic powers of strategic importance to the group.
2. Government and Defense Targets: The group targets military and government entities for the purpose of cyber espionage. This includes gathering information on government policies, military strategies, and national security-related data.
3. Sophisticated Attacks: Mint Sandstorm conducts targeted and custom-tailored cyber attacks that involve the use of advanced malware and cyber espionage tools.
4. Stealth Capabilities: The group often keeps its activities covert for extended periods and employs various methods to avoid detection.

Known Attacks:

Specific details about the attacks conducted by the Mint Sandstorm APT group are limited because the group is typically very careful to avoid detection. However, it is known that the group has conducted cyber espionage operations, particularly against military and government targets in the Asia-Pacific region.

Purpose and Objectives:

The primary goal of Mint Sandstorm is to understand political and strategic developments in the Asia-Pacific region and gain access to valuable information about the activities of governments, military institutions, and large corporations. The group uses this information to achieve strategic advantages.

For IoC's, please click here.

ALPHA SPIDER

Alpha Spider APT group is an advanced persistent threat (APT) group known for engaging in cyberattacks and possessing stealth capabilities.

Alpha Spider's attacks typically focus on strategic sectors such as government agencies, military organizations, energy companies, and financial institutions.

This group employs advanced targeted attack techniques to infiltrate systems and aims to exfiltrate sensitive data.

Alpha Spider is known for its cyber espionage activities and often pursues objectives such as information gathering, intellectual property theft, and leaking strategic information. The group uses advanced malware tools, exploits, and social engineering tactics in its cyberattacks. Additionally, it possesses advanced privacy and evasion techniques to remain undetected.

The Alpha Spider APT group consistently evolves and updates its attack tactics and techniques. Therefore, cybersecurity experts and security teams continuously analyze their activities to track them and update defense strategies.

Gaining more information about Alpha Spider APT group's objectives and attack methods is crucial for strengthening information security and implementing more effective measures against their attacks.

For IoC's, please click here.

Cosmic Wolf

Cosmic Wolf APT group is an advanced persistent threat (APT) group known for engaging in cyberattacks. This group conducts complex and sophisticated attacks against targets across various sectors and is typically operated by cybercriminals.

Cosmic Wolf's targets often include government agencies, military units, large corporations, and critical infrastructure, among other strategically important organizations. The group may launch attacks for financial gain, espionage, or political purposes.

Cosmic Wolf APT group aims to infiltrate target systems using advanced attack techniques. This group undergoes an extensive intelligence gathering process to identify target organizations and discover vulnerabilities. They then breach target systems using specially crafted malware, exploits, and social engineering methods.

Cosmic Wolf employs advanced evasion and camouflage techniques both before and after their attacks to hide traces in the compromised networks. This makes detection more difficult and tracking their activities and preventing attacks becomes more challenging.

This APT group continually evolves and updates its attack techniques. They engage in advanced research and development efforts to renew themselves, attempting to bypass defense measures. Therefore, security experts and cybersecurity teams work constantly to monitor Cosmic Wolf's activities, detect their attacks, and update their protective strategies.

Understanding the activities of the Cosmic Wolf APT group and strengthening defense measures is of great importance to targeted organizations. Collaboration and information sharing within the security community are essential to access up-to-date information and to thwart their attacks.

For IoC's, please click here.

Lazarus

Lazarus, a sophisticated advanced persistent threat (APT) group with origins attributed to North Korea, conducts operations worldwide. This cyberattack group is known for various cyber espionage, financial crimes, and cyber sabotage operations.

Lazarus is recognized as a group that carries out highly complex and targeted cyberattacks. They focus on high-profile targets globally, including governments, financial institutions, and large corporations.

Key Features:

1. North Korean Connection: Lazarus APT group is attributed to North Korea, and therefore, it is believed to be a state-sponsored group.
2. Cyber Espionage and Financial Crimes: The group is known for its cyber espionage operations as well as its capabilities in financial crimes. They have previously carried out bank heists, cryptocurrency thefts, and ransomware attacks.
3. High-Profile Targets: Lazarus targets high-profile entities such as governments, financial institutions, and large corporations. Attacks on the financial sector, in particular, stand out as a means for the group to gain financial profit.
4. Complex Malware: The group uses complex malware and cyber espionage tools, making it difficult to detect their attacks.

Known Attacks:

One of Lazarus APT group's most famous attacks is the 2014 Sony Pictures hack. The group has also executed numerous major attacks targeting financial institutions. These include the 2016 Bangladesh Bank heist and the 2017 WannaCry ransomware attack.

Purpose and Targets:

Lazarus APT group's main purpose is to operate in alignment with various objectives of the North Korean government. These objectives encompass financial gain, espionage, and safeguarding national interests. The group attempts to generate income by targeting the international financial system while concurrently focusing on gathering intelligence through espionage operations.

For IoC's, please click here.

ECHO

CYBER THREAT INTELLIGENCE