ECHO
CYBER THREAT INTELLIGENCE

SECTORAL REPORT 2023

ATTACKS ON THE AVIATION SECTOR IN THE SECOND HALF OF THE YEAR

@echocti

@echocti

echocti.com

Contents

Executive Summary

This report summarises the key developments in cyber security observed in the second half of 2023. The events reported under the relevant headings provide an analysis of specific cyber threats and key trends in the industry.

Phishing, malware attacks and ransomware attacks were among the prominent cyber threats during this period. Malicious actors increased phishing attacks to manipulate users and access sensitive information. Similarly, malware and ransomware attacks posed serious risks by negatively affecting the activities of organisations.

In 2023, the activities of certain cyber threat actors were observed. These actors distinguished themselves by using complex and variable attack techniques. At the same time, certain countries and sectors were more exposed to attacks. This situation emphasises that cyber security strategies need to be handled more carefully, especially on a sectoral and geographical basis.

Significant data breaches have compromised organisations' sensitive information and demonstrated once again that vulnerabilities are critical. These breaches highlighted the need to strengthen and improve cyber defence strategies.

Finally, the significant vulnerabilities discovered clearly demonstrated the vulnerabilities in our systems. It has become a critical priority to identify and fix these vulnerabilities and to create a stronger defence mechanism against future attacks.

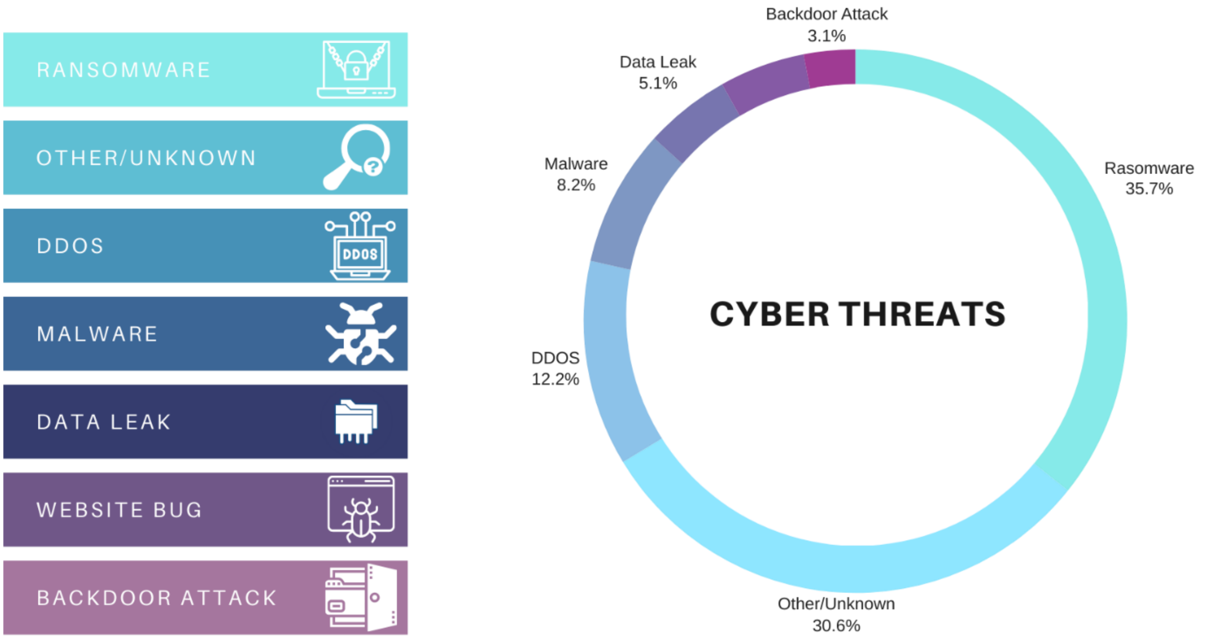
Cyber security threats are constantly evolving, and as an organisation, we focus on updating and improving our security strategies. This report summarises the key cyber security trends for the second half of 2023 and aims to provide guidance for building a more robust security infrastructure for the coming year.

Cyber Threads on Aviation Industry

The aviation industry is a sector open to cyber threats as an area where technology is developing rapidly and digitalisation is widespread. In this article, we will focus on the nature and effects of cyber threats encountered in the aviation industry and security measures in the sector.

The aviation industry uses a wide range of technological infrastructure from aircraft systems to ground services in the digitalisation process. However, the complexity of this infrastructure can make the industry vulnerable to cyber threats. Cyber threats can lead to serious consequences such as data leaks, interference with air traffic control systems, manipulation of flight systems.

Top Cyber Threads



In the researches conducted, it has been observed that the aviation sector is mostly targeted by ransomware attacks. You can review our previous report on this subject, Ransomware in 2023.

Important Events

Cyber attack on US aerospace company detected

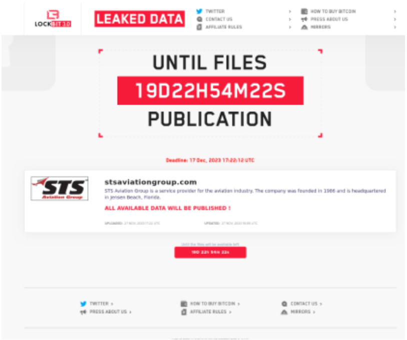
Iranian hackers have been revealed to have infiltrated a US aviation organisation using ManageEngine and Fortinet bugs. Threat groups have not yet been named, but USCYBERCOM has indicated that Iran is associated with the exploit efforts. The breach took place by exploiting vulnerabilities in Zoho ManageEngine ServiceDesk Plus and the Fortinet firewall. The attackers have been on the organisation's network since January, and after infiltrating the network, they established persistence. It was determined that the attack was carried out using devices with unpatched vulnerabilities.

Rosaviatsia Aviation Company Hacked

The intelligence service of the Ukrainian Ministry of Defence claims to have hacked Rosaviatsia, the Russian Federal Air Transport Agency. Ukraine says that the stolen data revealed the problematic situation of the Russian aviation sector. Rosaviatsia has not yet made a statement on the subject.

LockBit ransomware group has added STS Aviation Group to its list of victims.

STS Aviation Group is a service provider for the aviation industry, founded in 1986. On November 27, 2023, the LockBit 3.0 ransomware group reported that the organization in question had been exposed to the ransomware and that the data would be published if the ransom was not paid.



UNTIL FILES
19D22H54M22S
PUBLICATION

Deadline: 17 Dec, 2023 17:22:12 UTC

stsaviationgroup.com

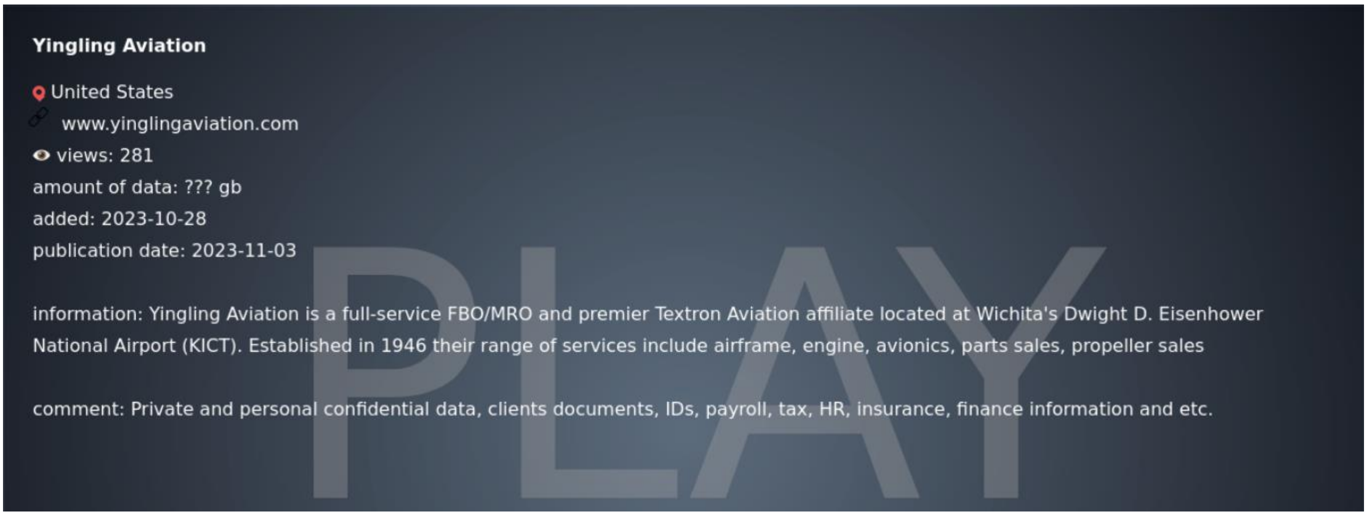
STS Aviation Group is a service provider for the aviation industry. The company was founded in 1986 and is headquartered in Jensen Beach, Florida.

ALL AVAILABLE DATA WILL BE PUBLISHED !

UPLOADED: 27 NOV, 2023 17:22 UTC UPDATED: 27 NOV, 2023 18:00 UTC

19D 22h 54m 22s

Yingling Aviation hit by ransomware attack



Yingling Aviation

United States

www.yinglingaviation.com

views: 281

amount of data: ??? gb

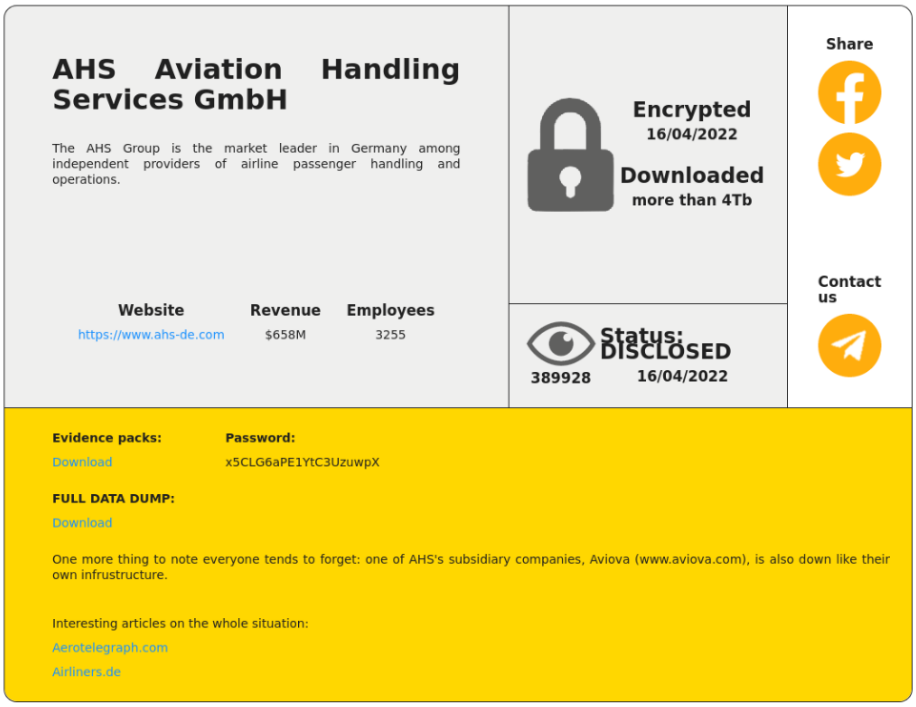
added: 2023-10-28

publication date: 2023-11-03

information: Yingling Aviation is a full-service FBO/MRO and premier Textron Aviation affiliate located at Wichita's Dwight D. Eisenhower National Airport (KICT). Established in 1946 their range of services include airframe, engine, avionics, parts sales, propeller sales

comment: Private and personal confidential data, clients documents, IDs, payroll, tax, HR, insurance, finance information and etc.

Since 1946, Yingling Aviation, which has been serving in many areas such as airframe, engine, avionics, parts sales, propeller sales, has been subjected to Play ransomware attack. On October 28, 2023, the Play ransomware group announced that they had infected the organization with ransomware and stolen some private information. This information includes: private and personal confidential data, customer documents, IDs, payroll, tax, HR, insurance, financial information, etc.



AHS Aviation Handling Services GmbH

The AHS Group is the market leader in Germany among independent providers of airline passenger handling and operations.

Website	Revenue	Employees
https://www.ahs-de.com	$658M	3255

Encrypted 16/04/2022

Downloaded more than 4Tb

Status: DISCLOSED 16/04/2022

389928

Evidence packs: Download

Password: x5CLG6aPE1YtC3UzuwpX

FULL DATA DUMP:
Download

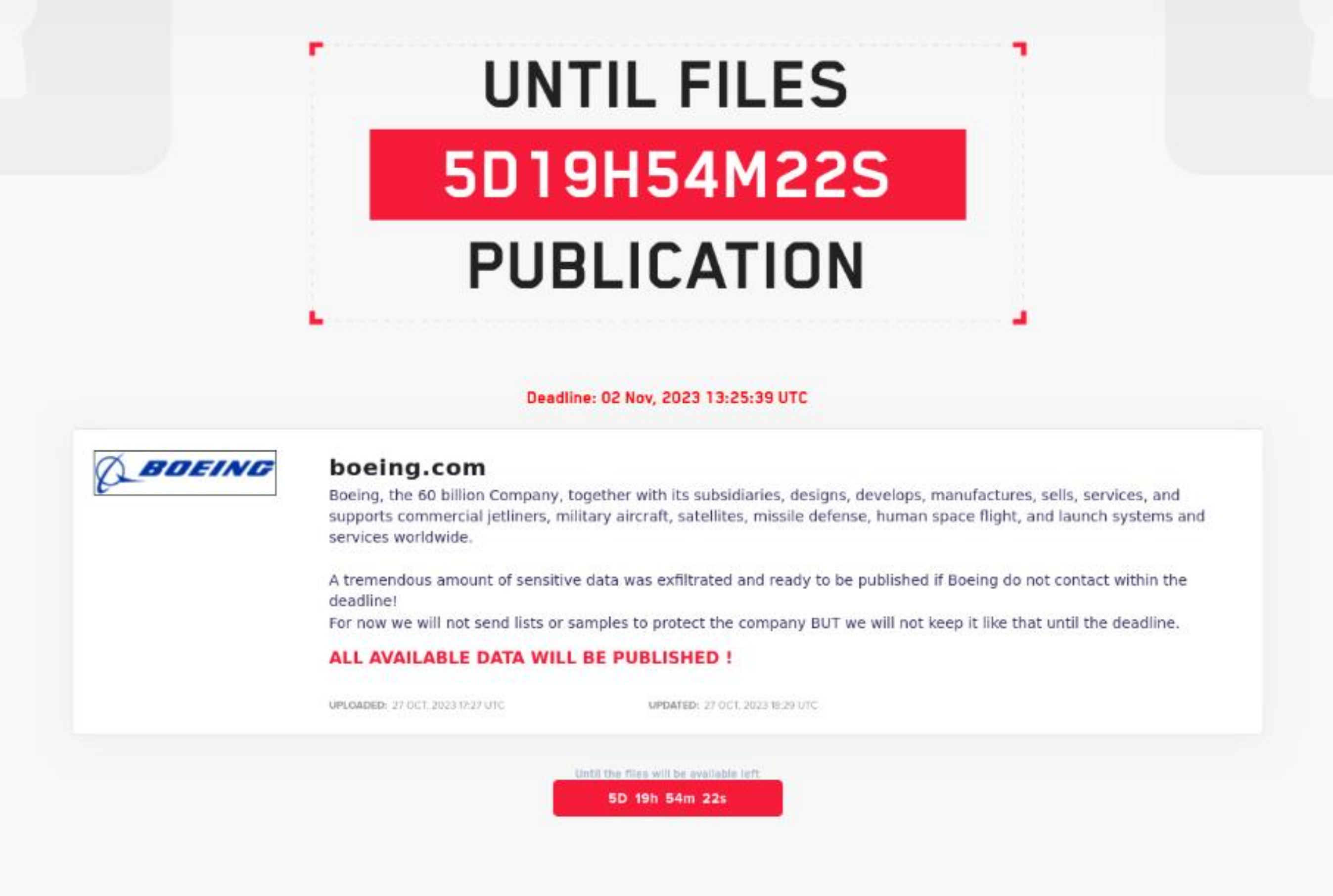
One more thing to note everyone tends to forget: one of AHS's subsidiary companies, Aviova (www.aviova.com), is also down like their own infrustructure.

Interesting articles on the whole situation:
Aerotelegraph.com
Airliners.de

AHS Aviation Handling Services Subjected to Ransomware Attack

AHS Group, the market leader in Germany, was reportedly hit by the RansomHouse ransomware attack on August 18, 2023. Ransomware group claimed to have stolen more than 4TB of data.

Boeing exposed to LockBit 3.0 ransomware



UNTIL FILES

5D19H54M22S

PUBLICATION

Deadline: 02 Nov, 2023 13:25:39 UTC

boeing.com

Boeing, the 60 billion Company, together with its subsidiaries, designs, develops, manufactures, sells, services, and supports commercial jetliners, military aircraft, satellites, missile defense, human space flight, and launch systems and services worldwide.

A tremendous amount of sensitive data was exfiltrated and ready to be published if Boeing do not contact within the deadline!
For now we will not send lists or samples to protect the company BUT we will not keep it like that until the deadline.

ALL AVAILABLE DATA WILL BE PUBLISHED !

UPLOADED: 27 OCT, 2023 17:27 UTC

UPDATED: 27 OCT, 2023 18:29 UTC

Until the files will be available left

5D 19h 54m 22s

Boeing, which develops, manufactures and services commercial aircraft, defense products and space systems, was hit by the LockBit 3.0 ransomware attack on October 27, 2023. The LockBit 3.0 ransomware group claimed to have stolen 40GB of data.

Most Active Threat Actors

As a result of the investigations conducted by our team, it has been determined that some APT groups targeted the aviation sector in the second half of this year. For the informative purpose of this report, information on these APT groups is provided below.

MuddyWater

The MuddyWater APT group is an advanced persistent threat (APT) group that has carried out attacks against various national and international targets.

This group was first detected in 2017 and is known to be active in attacks against public institutions, telecommunication companies, universities and other sectors, usually in the Middle East and Asian countries.

MuddyWater's attacks often involve advanced social engineering techniques, sophisticated malware attacks and targeted phishing campaigns. This group attempts to infiltrate target systems through seemingly trustworthy messages, such as fake documents, Word or Excel files. In its attacks, it tries to avoid detection by using advanced stealth and cloaking techniques.

MuddyWater's objectives may include information gathering, espionage, information exfiltration and gaining control of networks. This group is known to be an expert actor capable of carrying out sophisticated attacks and is constantly evolving its tactics and techniques.

The MuddyWater APT group is closely monitored and analyzed by information security experts and cyber security teams. In this way, information about new attack trends and methods is obtained and defense strategies are tried to be created.

APT-33

APT33, also known as Cozy Bear, is an Advanced Persistent Threat (APT) group affiliated with Russia.

This group is commonly known for state-sponsored cyber espionage and attacks against strategic targets such as the governments of various countries, the defense industry and the energy sector.

Main Features

1. **State Sponsored Operations:** APT33 is known as a group believed to be linked to the Russian government. As such, its activities are often in the strategic interests of the Russian state.

2. **Sophisticated Cyber Operations**: The group has the capability to conduct advanced and sophisticated cyber operations. It specializes in infiltrating target systems, espionage activities and using long-term attack strategies.

3. **Target Diversity:** APT33 operates on a wide range of targets. These targets include government agencies, defense industry, energy sector and other strategic sectors.

Known Attacks:

Attacks against Politicians and Government Agencies: APT33 is known for sophisticated phishing campaigns and espionage operations against politicians and government agencies of various countries.

Energy Sector Targets: The group conducts attacks against energy facilities and infrastructure. These attacks are planned to have long-term effects.

Aims and Objectives:

APT33 often operates to support the strategic interests of the Russian government. The group aims to gather political, military and economic information through cyber espionage and attacks on various sectors. It also aims to undermine the defense capabilities of hostile countries by conducting state-sponsored cyber operations to create long-term effects.

APT-27

APT27, also known as Emissary Panda or Threat Group-3390, is an advanced persistent threat (APT) group based in China. The group is a threat actor that targets its victims using strategic web compromises.

The group has been active since at least 2010 and has targeted organisations operating in the aerospace, government, defence, technology, energy, manufacturing and gambling/betting sectors.

Main Features

1. **Strategic Web Compromises:** APT27 commonly uses strategic web compromises to target its victims. This increases their ability to infiltrate target organisations using web-based vulnerabilities.
2. **Long-term Activity:** The Group has been active since at least 2010 and has adopted long-term cyber attack strategies. This tends to sustain its activities against targets on a continuous basis.
3. **Attacks on Various Sectors:** APT27 is known as a group capable of conducting attacks against a wide range of sectors such as aviation, government, defence, technology, energy, manufacturing, and gambling/betting.
4. **Relationships with Other APT Groups:** Emissary Panda has overlapping characteristics with other APT groups such as Turbine Panda, APT 26, Shell Crew, WebMasters, KungFu Kittens, and possibly UNC215. It also co-operated with TA428 in Operation StealthyTrident.

Known Attacks:

APT27 targets foreign embassies and aims to collect data from these organisations. These attacks are usually aimed at the government, defence and technology sectors.

Aims and Objectives:

APT27's main objectives include collecting strategic information from foreign governments and organisations, particularly weakening the security of organisations operating in the government, defence and technology sectors. As a China-based actor, this group aims to protect national interests and conducts cyber espionage activities.

APT-34

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

This group is considered an intelligence unit that conducts cyber espionage and cyber attacks in support of Iran's strategic interests.

APT34 is capable of conducting cyber attacks against various sectors and is supported by the Iranian government.

Main Characteristics:

1. **Iranian Government Connection:** APT34 is a cyber espionage group closely associated with the Iranian government. The group operates in support of Iran's strategic interests.
2. **Target Diversity:** APT34 conducts attacks against a range of sectors, including energy, defence, telecommunications, finance and government. Targets often include foreign governments, corporations, and strategic positions of hostile countries.
3. **Social Engineering Capabilities:** The group uses social engineering tactics to infiltrate its targets. This may include manipulation and fraud to gain the trust of victims and spread malware.
4. **Malicious Software:** APT34 specialises in the use of malware. Specifically, it uses various types of malware to infiltrate its targets.

Known Attacks:

One of APT34's most notable attacks is the Phosphorus campaign against numerous government and private sector organisations worldwide. This campaign involves cyber espionage and information gathering operations against targets.

Purpose and Target:

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

Click for IoC.

APT-28

APT28, also known as Fancy Bear or Sofacy, is a threat group that, according to an allegation published by the US Department of Justice in July 2018, was identified as a group affiliated with Russia's General Staff Intelligence Directorate (GRU).

The group reportedly targeted the Hillary Clinton campaign, the Democratic National Committee and the Democratic Congressional Campaign Committee in an attempt to interfere in the 2016 US presidential election. APT28 has been active since at least January 2007.

Main Features:

1. **Link to Russia**: APT28 is a threat group believed to be affiliated with Russia's General Staff Intelligence Directorate. According to the US Department of Justice's 2018 indictment, this group operates to collect and intercept Russian government information.
2. **Interference in American Elections:** Notorious for alleged interference in the 2016 US presidential election, APT28 targeted the Hillary Clinton campaign, the Democratic National Committee, and the Democratic Congressional Campaign Committee.
3. **Activities Focused on Eastern Europe and Georgia:** According to FireEye analysis, APT28 sought to gather information on Georgia's security and political dynamics, focusing on officials working in the Georgian Ministries of Interior and Defence.
4. **Attacks on Eastern European and European Security Organisations:** The group maintained its interest in Eastern European governments and security organisations, providing the Russian government with the ability to anticipate policy-making intentions and influence public opinion.

Known Attacks:
2016 US Presidential Election: APT28 targeted the Hillary Clinton campaign, the Democratic National Committee, and the Democratic Congressional Campaign Committee in an attempt to interfere in the United States presidential election.

Attacks Against Doping Agencies: In 2018, the United States charged five GRU Unit 26165 officers associated with APT28 with cyber operations against the World Anti-Doping Agency (WADA), the US Anti-Doping Agency, a US nuclear facility, the Organisation for the Prohibition of Chemical Weapons (OPCW), the Spiez Swiss Chemical Laboratory and other organisations between 2014 and 2018.

Aims and Objectives:
The main objectives of APT28 are to gather strategic information in the interests of the Russian government and to influence international policy. Through its targets in regions such as Eastern Europe, Georgia, and the United States, the group aims to increase Russia's political influence through information leakage and manipulation.

Click **for IoC.**

ECHO

CYBER THREAT INTELLIGENCE