nccgroup

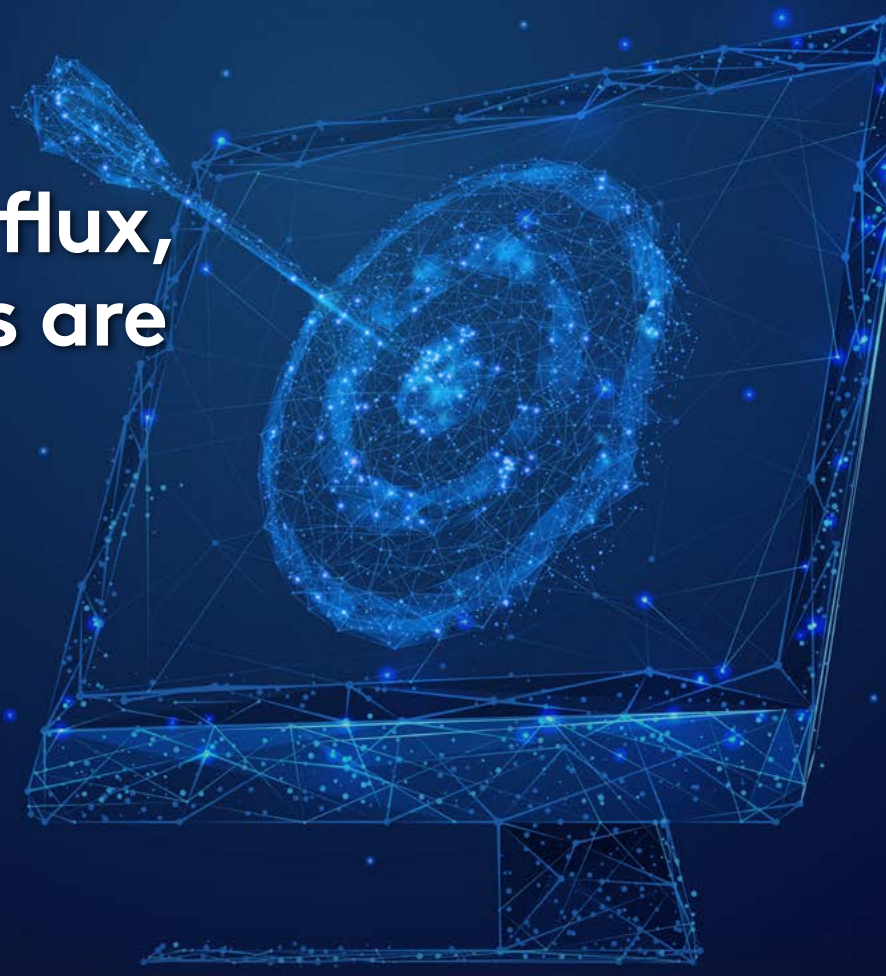
FOX IT
part of nccgroup

# Insights

**Pragmatic cyber security advice for senior executives**

# The threat landscape is in flux, and OT systems are a prime target

Threat intel report



**Matt Hull**
NCC Group's Global Head of Threat Intelligence

**Global. Transformative. Resilient.**

# The threat landscape is in flux, and OT systems are a prime target

Matt Hull, NCC Group's Global Head of Threat Intelligence, discusses the current threat landscape and the disastrous fallout of recent high profile attacks on OT systems.

**Matt Hull**
NCC Group's Global Head of Threat Intelligence

Once again, 2022 is shaping up to be an interesting year with regards the criminal threat landscape, particularly the use of ransomware. We continue to see Ransomware-as-a-Service (RaaS) as one of the most significant threats to organisations around the globe, despite several prominent ransomware operators disbanding and rebranding.

In the first half of this calendar year, 65% of all of our incident response cases across the globe have involved the deployment of ransomware . In most cases, this has also involved the release of sensitive corporate data on so called 'leak sites' which are used by ransomware operators as part of 'double-extortion' campaigns.

Last year there were concerns around the targeting of operational technology (OT) environments by criminal groups, something which rose to prominence following the Colonial Pipelines breach. This year, we are seeing more and more incidents involving the OT space. In 2022, the industrials sector has been the victim of 45% of all double extortion ransomware incidents. It shows that weaknesses in legacy OT environments, which may have been overlooked for many years, are an obvious and easy target for criminal groups.

**65%**

of all of our incident response cases across the globe have involved the deployment of ransomware

**45%**

of all double extortion ransomware incidents in 2022 have affected industrials sector

> Ransomware-as-a-Service (RaaS) is one of the most significant threats to organisations around the globe.

# Threat Intel Report

OT systems support the critical infrastructure we depend on: electrical grids, water, transport networks, fuel and power plants, food and product manufacturing. As OT networks become increasingly connected to IT systems, attacks can be highly disruptive – a threat to not only organisations, but a country's economy and national security. We have seen that operational and production disruption is possible, with detrimental consequences for processes and safety. The stakes at play for organisations are high, with financial loss, data loss and compromised human safety at risk.

The terrifying potential of an attack against an OT environment was realised in June this year. The threat actor 'Predatory Sparrow' was able to demonstrate the true impact of a cyber-kinetic attack, which resulted in a large fire in an Iranian steel plant. Interestingly, the group claim to have deliberately launched the attack in a manner which did not cause injury to innocent people.

So, as we expect that OT environments will continue to be a priority target for a plethora of threat groups over the coming years, investment in the security of these must be a key priority for organisations and global governments alike.

As OT networks become increasingly connected to IT systems, attacks can be highly disruptive



**The impact of 'Predatory Sparrow', a cyber-kinetic attack**

OT environments will continue to be a priority target for a plethora of threat groups over the coming years.

# About Insights

Insights is a program designed for sharing pragmatic cyber security insights with senior executives. You can expect a magazine and interactive online event about a trending topic each quarter. Register here for the free virtual Insights event: Growing Threats.

# About NCC group

It's a new era of risk. Defy it with NCC Group's end-to-end cyber security and resilience solutions, and confidently embrace technology to support sustainable growth and success.

From governments to tech giants, financial institutions to expanding businesses, for over 30 years we have proudly provided them with strong security solutions...and with a global team of over 2,400 experts, we're ready to do the same for you.

With NCC Group, take your business to the next level. Unleash innovation without the obstacle of cyber threats.

## More than a solution. **A partner.**

You're not alone on your security journey. NCC Group is your partner. Be it rolling up our sleeves with your in-house team or developing strategy with your board, we help you have control over your appropriate level of security. Yes, we deliver industry leading security solutions, but we'll also reduce stress, save your business time, and help you prepare for, or even face, a crisis together.

www.nccgroup.com

UNI106269