Sign Up   Log I

info security
STRATEGY | INSIGHT | TECHNOLOGY

Latest
Tackling The Impact Of Fraud By Utilising Machine Learning Tactics

🏠   News   Topics   Features   Webinars   White Papers   Events & Conferences   Directory   🔍

17 DEC 2015   NEWS

NATO and Symantec Tie Knot on Info Sharing Agreement

Phil Muncaster UK / EMEA News Reporter , Infosecurity Magazine
Email Phil Follow @philmuncaster

NATO and Symantec have signed an information sharing agreement which will see both parties exchange threat intelligence to build resilience to cyber attacks.

The agreement, signed within the framework of the NATO Industry Cyber Partnership (NICP), will see information flow two ways between the security giant and the NATO Communications and Information (NCI) Agency.

According to NATO, effective info sharing on threats can be the best way to improve resilience and incident handling and mitigate vulnerabilities.

"Today's agreement is as an excellent and concrete example of how NATO and Industry can work side by side to confront difficult challenges in the cyber domain," said ambassador Sorin Ducaru, assistant secretary general of NATO's Emerging Security Challenges Division.

"When it comes to the cyber threat, none of us acting alone can address these challenges as effectively as if we act together. Increased information sharing translates into better cyber defense for NATO, allies and our industry partners such as Symantec."

NCI general manager, Koen Gijsbers, added that NATO is facing "new and increasingly dangerous threats to cybersecurity."

"To avoid it, NCI Agency strongly believes in rapid and early information sharing on threats and vulnerabilities with leading companies worldwide, such as Symantec," he added. "Trust is the key to success."

The NATO Industry Cyber Partnership was ratified at the organization's Wales Summit in September 2014.

The idea is to improve the sharing of cybersecurity "expertise, information and experience" and enhance NATO's cyber defenses.

It's also hoped the NICP will help improve understanding of cyber risks, build "access and trust" between NATO and the private sector and boost cyber defense education and training.

NATO has been a very public target for nation state hackers over the years—especially those from Russia and China.
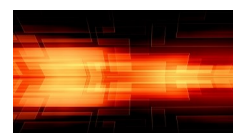
Why Not Watch?

22 OCT 2015
The Kick Inside – Dealing with Threats from Within Your Firm

25 JUN 2015
Meeting the New Challenges of Enterprise Security

9 JUL 2015

8 OCT 2015

The group known as "Pawn Storm" (aka APT28)—which has been linked to the Kremlin—was one of the most recent to attack the military coalition.

Photo © Gilmanshin

Recommended for you

The Funny Face of Information Sec...
www.infosecurit...

Target Breach Affecting 40 Mill...
www.infosecurit...

Saudi Aramco Cyber Attacks a '...
www.infosecurit...

New Version of ISO/IEC 27001 Te...
www.infosecurit...

+ AddThis

0 Comments   **Infosecurity Magazine**   💬 **Login** ▾

♥ Recommend   ↱ Share   Sort by Best ▾

Start the discussion…

Be the first to comment.

ALSO ON **INFOSECURITY MAGAZINE**   WHAT'S THIS?

Touchnote Postcard Service Hacked, Affecting Millions
1 comment • a month ago
  Paul German — Another breach! These security breaches are happening far too frequently and businesses are still failing …

Happy Hour for Hackers as Wetherspoons Suffers Data Breach
1 comment • 14 days ago
  Paul German — The fact that it took JD Wetherspoons nearly six months to detect that a hack had taken place is simply far …

UK and China Shake Hands on Cyber IP-Theft Deal
1 comment • 2 months ago
  Crom! — Why does the victim, the UK, have to agree with the burglar, China, to an agreement? China is the one stealing …

Biometrics: A Next Wave of Banking Authentication
1 comment • 23 days ago
  IASSecPro — What makes Mobey Forum, the financial industry association think that banks are able to protect the …

✉ Subscribe   Ⓓ Add Disqus to your site Add Disqus Add   🔒 Privacy   **DISQUS**

How Outsiders Become Insiders: Understanding and Combating Today's Threats

Fighting Cyber-Attacks Through Security Intelligence

Related to This Story

NATO admits to ongoing hacking attempts, spark info-sharing discussions

Stuxnet has been attacking Iran since 2005

Five-month malvertising campaign serves up sile infections

Spam epidemic spreading via fake government websites

Faux BlackHole 2.0 kit exploits hackers

What's Hot on Infosecurity Magazine?

| Read | Shared | Watched | Editor's Choice |

1 16 DEC 2015 NEWS
80% of Companies Had a Security Incident in 2015

2 16 DEC 2015 NEWS
Mobile Banking Trojans: A Top-10 Threat for the First Time

3 17 DEC 2015 NEWS
Users Warned of Info-Stealing Christmas-Themed Malware

4 17 DEC 2015 NEWS FEATURE
Six Months Later, Find Out If The OF Breach Affected You

5 17 DEC 2015 NEWS
NATO and Symantec Tie Knot on In Sharing Agreement

6 17 DEC 2015 NEWS
Verizon: 90% of Industries Suffer Patient Data Breaches