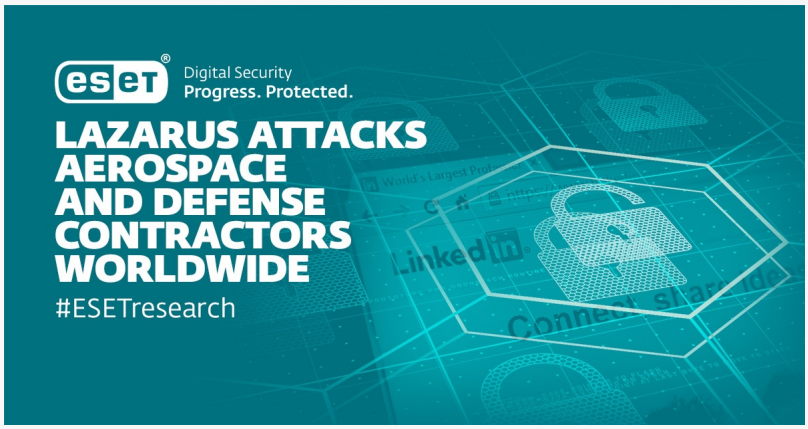
ESET Research: Lazarus attacks aerospace and defense contractors worldwide while misusing LinkedIn and WhatsApp

DUBAI, UNITED ARAB EMIRATES, June 1, 2022 /EINPresswire.com/ -- During the annual ESET World conference, ESET researchers have been presenting about a new investigation into the infamous Lazarus APT group. Director of ESET Threat Research Jean-Ian Boutin went over various new campaigns perpetrated by the Lazarus group against defense contractors around the world between late 2021 and March 2022.



In the relevant 2021-2022 attacks and according to ESET telemetry, Lazarus has been targeting companies in Europe (France, Italy, Germany, the Netherlands, Poland, and Ukraine) and Latin America (Brazil).

Despite the primary aim of this Lazarus operation being cyber-espionage, the group has also worked to exfiltrate money (unsuccessfully). “The Lazarus threat group showed ingenuity by deploying an interesting toolset, including for example a user mode component able to exploit a vulnerable Dell driver in order to write to kernel memory. This advanced trick was used in an attempt to bypass security solutions monitoring.,” says Jean-Ian Boutin.

As early as 2020, ESET researchers had already documented a campaign pursued by a sub-group of Lazarus against European aerospace and defense contractors ESET called operation In(ter)ception. This campaign was noteworthy as it used social media, especially LinkedIn, to build trust between the attacker and an unsuspecting employee before sending them malicious components masquerading as job descriptions or applications. At that time, companies in Brazil, Czech Republic, Qatar, Turkey and Ukraine had already been targeted.

ESET researchers believed that the action was mostly geared towards attacking European companies, but through tracking a number of Lazarus sub-groups performing similar campaigns against defense contractors, they soon realized that the campaign extended much wider. While

the malware used in the various campaigns were different, the initial modus operandi (M.O.) always remained the same: a fake recruiter contacted an employee through LinkedIn and eventually sent malicious components.

In this regard, they've continued with the same M.O. as in the past. However, ESET researchers have also documented the re-use of legitimate hiring campaign elements to add legitimacy to their fake recruiters' campaigns. Additionally, the attackers have used services such as WhatsApp or Slack in their malicious campaigns.

In 2021, the U.S. Department of Justice charged three IT programmers for cyberattacks as they were working for the North Korean military. According to the U.S. government, they belonged to the North Korean military hacker unit known in infosec community as Lazarus Group.

Along with the new Lazarus research, ESET has been presenting about the "Past and Present Cyberwar in Ukraine" during the annual conference. ESET researcher Robert Lipovský has taken an in-depth look at the cyber war during the Russia's war against Ukraine - including the latest attempt to disrupt the country's power grid using Industroyer2 and various wiper attacks.

Alongside ESET Research at ESET World, former Commander of the International Space Station, Canadian astronaut Chris Hadfield, and key figure in ESET's Progress Protected campaign has joined ESET CEO Richard Marko to discuss the intricacies of technology, science and life.

About ESET
For more than 30 years, ESET® has been developing industry-leading IT security software and services to protect businesses, critical infrastructure and consumers worldwide from increasingly sophisticated digital threats. From endpoint and mobile security to endpoint detection and response, as well as encryption and multifactor authentication, ESET's high-performing, easy-to-use solutions unobtrusively protect and monitor 24/7, updating defenses in real time to keep users safe and businesses running without interruption. Evolving threats require an evolving IT security company that enables the safe use of technology. This is backed by ESET's R&D centers worldwide, working in support of our shared future. For more information, visit www.eset.com or follow us on LinkedIn, Facebook, and Twitter.

Sanjeev Kant
Vistar Communications
+971 55 972 4623
email us here

in today's world. Please see our Editorial Guidelines for more information.