Dark Pink: New APT group targets governmental, military organizations in APAC, Europe

Media Center → Press Releases

January 11, 2023 · 8 min to read

APAC APT group Europe Threat Intelligence

Group-IB, one of the global cybersecurity leaders, has today **published its findings into Dark Pink**, an ongoing advanced persistent threat (APT) campaign launched against high-profile targets in **Cambodia, Indonesia, Malaysia, Philippines, Vietnam**, and **Bosnia and Herzegovina** that we believe, with moderate confidence, was launched by a new threat actor. To date, Group-IB's **Threat Intelligence** has been able to attribute **seven successful attacks** to this particular group from June-December 2022, with targets including military bodies, government ministries and agencies, and religious and non-profit organizations, although the list of victims could be significantly longer. Group-IB also noted one unsuccessful attack on a European state development body based in Vietnam.

Group-IB analysis discovered that the initial access vector for the campaign of **Dark Pink** (name given by Group-IB) was targeted **spear-phishing emails**, and the core goal of the threat actors, who leverage an almost-entirely custom toolkit, is **corporate espionage**, as they attempt to **exfiltrate files, microphone audio**, and **messenger data** from infected devices and networks. Group-IB, in line with its zero-tolerance policy to cybercrime, has issued proactive notifications to all potential and confirmed targets of Dark Pink. Our researchers are continuing to uncover and analyze all the details behind this particular APT campaign.

Dark Pink goes to the core

To date, Group-IB has been unable to attribute this campaign, which leverages custom tools and some rarely seen tactics and techniques, to any known threat actor. As a result, Group-IB believes that Dark Pink's campaign in the second half of 2022 is the activity of an entirely new threat actor group, which has also been termed Saaiwc Group by Chinese cybersecurity researchers. This new APT group is notable due to their specific focus on attacking branches of the military, and government ministries and agencies. Group-IB discovered that, as of December 2022, Dark Pink APT breached the security defenses of six organizations in five APAC countries (**Cambodia, Indonesia, Malaysia, Philippines, and Vietnam**), and one organization in Europe (**Bosnia and Herzegovina**). The first successful attack took place this past June, when the threat actors gained access to the network of a **religious organization in Vietnam**. Following this particular breach, no other attack attributable to Dark Pink was registered until August 2022, when Group-IB analysts discovered that the threat actors had gained access to the network of a **Vietnamese non-profit organization**.

Dark Pink's activity ramped up in the final four months of the year. Group-IB's Threat Intelligence Team uncovered attacks on a branch of the Philippines military in September, a Malaysian military branch in October, two breaches in November, with the victims being government organizations in Bosnia & Herzegovina and Cambodia, and finally, in early December, an Indonesian governmental agency. Group-IB's Threat Intelligence also discovered an unsuccessful attack on a European state development agency based in Vietnam in October.

Figure 1: Dark Pink APT's timeline and affected organizations

While the first Dark Pink breach, as confirmed by Group-IB, took place in June 2022, there are clues to suggest that the group was active as far back as mid-2021. Group-IB found that the threat actors, upon infection of a device, were able to issue commands to the infected computer to download malicious files from **Github**, with these resources uploaded by the threat actors themselves. Interestingly, the threat actors have used **the same Github account** for uploading malicious files for the **entire duration of the APT campaign** to date, which could suggest that they have been able to operate without detection for a significant period of time.

Figure 2: Screenshot detailing activity on Github account attributed to Dark Pink APT in 2021 (above) and 2022 (below)

Sharpen those custom tools

Dark Pink utilizes a set of custom tools and sophisticated tactics, techniques and procedures (TTPs) that have made a major contribution to their successful attacks over the past seven months. In their research into Dark Pink, Group-IB analysts detail the entire victim journey from initial infection to data exfiltration.

The threat actors launch their attack with targeted spear-phishing emails. Group-IB was able to find the original email sent by the threat actors in one unsuccessful attack. In this instance, the attackers posed as a job seeker applying for the position of PR and Communications Intern. In the email, the threat actor mentions that they found the vacancy on a jobseeker site, which could suggest that the **threat actors scan job** boards and craft a **unique phishing email** relevant to the organization that they find.

Figure 3: Screenshot of original spear-phishing email sent by Dark Pink APT, containing a link to an ISO image hosted on a file-sharing site.

The spear-phishing emails contain a shortened URL linking to a free-to-use file sharing site, on which the victim is presented with the option to download a malicious ISO file that always contains three specific file types: **a signed executable file**, a **nonmalicious decoy document** (some ISO files seen by Group-IB had more than one), and a **malicious DLL file**. However, these file types can differ in their content and functionality, and Group-IB analysts uncovered three separate kill chains, underscoring the sophistication of this particular APT group.

The first kill chain analyzed by Group-IB sees the threat actors pack all of the described above files, including a malicious DLL, onto the ISO itself, and after mounting, the DLL will be run using the attack known as **DLL Side-Loading**. The second kill chain sees the threat actors leverage Github

after initial access, allowing them to automatically download a template document that contains **macro codes** that are responsible for running the threat actors' malware. Finally, the third, and most recent kill chain leveraged by the threat actors (in December 2022) sees their malware launched with the assistance of an **XML file**, which contains an MSBuild project that includes a task to execute .NET code in order to launch their custom malware.

The sophistication of Dark Pink's attacks is also underlined by the custom malware and stealers in the threat actors' arsenal. They created two custom modules, named by Group-IB as **TelePowerBot** and **KamiKakaBot**, which are written in PowerShell and .NET, respectively. These two pieces of malware are designed to read and execute commands from a **threat actor-controlled Telegram channel via Telegram bot**. Group-IB researchers noted that all communication between the devices of the threat actors and victims was based entirely on **Telegram API**, and they utilized numerous evasion techniques, including **Bypass User Account Control**, to remain undetected.

The threat actor also created two custom stealers, dubbed **Cucky** and **Ctealer** by Group-IB. When launched on the victims' device, the stealers are able to steal passwords, history, logins, and cookies from dozens of web browsers. In this campaign, the threat actors also wrote script that allowed them to **transfer their malware to USB devices** connected to the compromised machine, and also spread their malware across **network shares**.

The threat actors also leveraged a custom utility, dubbed **ZMsg** by Group-IB, to exfiltrate data from the **Zalo** messenger on victims' devices. Researchers found evidence that the APT group could steal data from the **Viber** and **Telegram** messengers as well. One of the only off-the-shelf tools that the threat actors utilized was the publicly available PowerSploit module **Get-MicrophoneAudio**, which is loaded onto the victim's device via download from Github. This module, which the threat actors customized to ensure they were able to bypass antivirus software, allowed them to record audio input and later **exfiltrate these recordings via their Telegram bot**. Group-IB analysts noted that the custom script added to this PowerSploit module was changed multiple times, after several unsuccessful attempts to record the microphone audio on infected devices.

Dark Pink exfiltrated data from victims via three specific pathways: via **Telegram, Dropbox** and **email**. In fact, the name Dark Pink comes from a hybrid of two of the email addresses (blackpink.301@outlook[.]com and blackred.113@outlook[.]com) used by the threat actors during data exfiltration via the latter pathway.

Andrey Polovinkin
Malware Analyst at Group-IB

"Group-IB's analysis of Dark Pink is of major significance, as it details a highly complex APT campaign launched by seasoned threat actors. The use of an

almost entirely custom toolkit, advanced evasion techniques, the threat actors' ability to rework their malware to ensure maximum effectiveness, and the profile of the targeted organizations demonstrate the threat that this particular group poses. Group-IB will continue to monitor and analyze both past and future Dark Pink attacks with the aim of uncovering those behind this campaign."

Dark Pink APT's recent campaign is yet another example of how individuals' interactions with spear-phishing emails can result in the penetration of the security defenses of even the most protected organizations. Group-IB recommends solutions, such as its proprietary **Business Email Protection**, that can counter this threat effectively and stop malicious emails from ending up in employees' inboxes. That said, Group-IB urges organizations to foster a culture of cybersecurity and educate their employees on how to identify phishing emails. Group-IB's **Threat Intelligence** platform led the analysis into Dark Pink, and can help organizations shore up their security posture by equipping them with the latest insights into emerging threats.

Share article

About Group-IB

Founded in 2003 and headquartered in Singapore, Group-IB is a leading creator of cybersecurity technologies to investigate, prevent, and fight digital crime. Combating cybercrime is in the company's DNA, shaping its technological capabilities to defend businesses, citizens, and support law enforcement operations.

Group-IB's Digital Crime Resistance Centers (DCRCs) are located in the Middle East, Europe, Central Asia, and Asia-Pacific to help critically analyze and promptly mitigate regional and country-specific threats. These mission-critical units help Group-IB strengthen its contribution to global cybercrime prevention and continually expand its threat-hunting capabilities.

Group-IB's decentralized and autonomous operational structure helps it offer tailored, comprehensive support services with a high level of expertise. We map and mitigate adversaries' tactics in each region, delivering customized cybersecurity solutions tailored to risk profiles and requirements of various industries, including retail, healthcare, gambling, financial services, manufacturing, crypto, and more.

The company's global security leaders work in synergy with some of the industry's most advanced technologies to offer detection and response capabilities that eliminate cyber disruptions agilely.

Group-IB's Unified Risk Platform (URP) underpins its conviction to build a secure and trusted cyber environment by utilizing intelligence-driven technology and agile expertise that completely detects and defends against all nuances of digital crime. The platform proactively protects organizations' critical infrastructure from sophisticated attacks while continuously analyzing potentially dangerous behavior all over their network.

The comprehensive suite includes the world's most trusted Threat Intelligence, The most complete Fraud Protection, AI-powered Digital Risk Protection, Multi-layered protection with Managed Extended Detection and Response (XDR), All-infrastructure Business Email Protection, and External Attack Surface Management.

Furthermore, Group-IB's full-cycle incident response and investigation capabilities have consistently elevated industry standards. This includes the 77,000+ hours of cybersecurity incident response

completed by our sector-leading DFIR Laboratory, more than 1,400 successful investigations completed by the High-Tech Crime Investigations Department, and round-the-clock efforts of CERT-GIB.

Time and again, its solutions and services have been revered by leading advisory and analyst agencies such as Aite Novarica, Gartner®, Forrester, Frost & Sullivan, KuppingerCole Analysts AG, and more.

Being an active partner in global investigations, Group-IB collaborates with international law enforcement organizations such as INTERPOL, EUROPOL and AFRIPOL to create a safer cyberspace. Group-IB is also a member of the Europol European Cybercrime Centre's (EC3) Advisory Group on Internet Security, which was created to foster closer cooperation between Europol and its leading non-law enforcement partners.

Read next

March 19, 2026

Group-IB Partners with Copy Cat Group to Strengthen Intelligence-Led Cybersecurity Across East Africa

March 13, 2026

Group-IB Supports INTERPOL's Operation Synergia III, Contributing Intelligence to Global Cybercrime Takedown

March 12, 2026

Group-IB Expands into the Americas with Launch of Digital Crime Resistance Center in Chile

March 3, 2026

Group-IB and Nebrija University Strengthen Cybersecurity Education Through MOU and Threat

Intelligence Integration

February 26, 2026

Group-IB Partners with Savex Technologies to Advance Predictive Threat Intelligence and Cyber Fraud Protection Across India and SAARC

February 16, 2026

National Polytechnic University of Armenia and Group-IB sign strategic partnership to strengthen cybersecurity education and research in Armenia

Go to all Press Releases →

Partners

Partner Program

MSSP and MDR Partner Program

Technology Partners

Partner Locator

Company

About Group-IB

Team

CERT-GIB

Careers

Internship

Academic Aliance

Sustainability

Media Center

Contact

Subscription plans →

Services →

Resource Center →

Contact

APAC: +65 3159 3798

EU & NA: +31 20 226 90 90

MEA: +971 4 568 1785

info@group-ib.com

Subscribe to stay up to date with the latest cyber threat trends