Group-IB report: hacker gang OPERA1ER stole $11 million from African companies

Media Center → Press Releases

November 3, 2022 · 6 min to read

OPERA1ER Report Rustam Mirkasymov Threat Intelligence

Group-IB, one of the global leaders in cybersecurity headquartered in Singapore, has today issued a new report, "OPERA1ER. Playing God without permission," in collaboration with the researchers **from Orange CERT Coordination Center**. The report takes a deep dive into financially motivated attacks of the prolific French-speaking threat actor, codenamed OPERA1ER. Despite relying solely on known "off-the-shelf" tools, the gang managed to carry out more than **30** successful attacks against banks, financial services, and telecommunication companies mainly located **in Africa** between 2018 and 2022. OPERA1ER is confirmed to have stolen at least **$11 million**, according to Group-IB's estimates. One of OPERA1ER's attacks involved a vast network of **400 mule accounts** for fraudulent money withdrawals. Researchers from the Group-IB European Threat Intelligence Unit identified and reached out to **16 affected organizations** so they could mitigate the threat and prevent further attacks by OPERA1ER.

This report was completed in 2021 while the threat actor remained active. OPERA1ER noticed Group-IB's increasing interest in his activity and reacted by deleting their accounts and changing some TTPs to cover their tracks. Group-IB decided to suspend publishing the report and wait until the threat actor resurfaced again, which happened in 2022. Therefore, the report contains the Indicators of Compromise (IOCs) relevant for the period of 2019-2021. The latest IOCs and OPERA1ER's targets can be found in Group-IB's blog post. The changes are small and don't impact the overall findings. Through threat intelligence and resource sharing, Orange-CERT-CC and Group-IB were able to better understand the threat actor's modus operandi. All findings have been compiled into the report so that the cybersecurity community could better track OPERA1ER's activity and prevent their attacks in the future.

Smooth OPERA1ER

Digital forensics artifacts analyzed by Group-IB and Orange following more than 30 successful intrusions of OPERA1ER between 2018 and 2022 helped to trace down affected organizations in **Ivory Coast, Mali, Burkina Faso, Benin, Cameroon, Bangladesh, Gabon, Niger, Nigeria, Paraguay, Senegal, Sierra Leone, Uganda, Togo, Argentina**. Many of the victims identified were successfully attacked twice, and their infrastructure was then used to attack other organizations. According to Group-IB's evaluation, between 2018 and 2022, OPERA1ER managed to steal at least **$11 million**, and the actual amount of damage could be as high as **$30 million**.

OPERA1ER, also known under the names DESKTOP-group and Common Raven (SWIFT ISAC Security Bulletin, 23 June 2021), traces its roots back to 2016 when they registered their oldest known domain. In the new report, Group-IB was able to identify previously unrecognized elements of the gang's infrastructure, including their newly deployed Command and Control servers (C&C) domains and IP addresses. Based on one of the accounts frequently used by the gang now to register domains, Group-IB codenamed the threat actor OPERA1ER.

"Detailed analysis of the gang's recent attacks revealed an interesting pattern in their modus operandi: OPERA1ER conducts attacks mainly during the weekends or public holidays," says **Rustam Mirkasymov**, head of cyber threat research at Group-IB Europe. *"It correlates with the fact that they spend from 3 to 12 months from the initial access to money theft. It was established that the French-speaking hacker group could operate from Africa. The exact number of the gang members is unknown."*

No rush to cash in

A distinct feature of the group is the use of off-the-shelf open-source programs, malware freely available on the dark web, and popular red teaming frameworks, such as **Metasploit** and **Cobalt Strike**. In at least two incidents in different banks, the attackers deployed Metasploit servers inside compromised infrastructure. Because the gang relies solely on public tools, they have to think outside the box: in one incident, analyzed by Group-IB and Orange, OPERA1ER used an antivirus update server deployed in the infrastructure as a pivoting point.

OPERA1ER start their attacks with high-quality spear phishing emails targeting a specific team within an organization. Most of their messages are written in French, ranging from fake notifications from government tax offices to hiring offers from BCEAO (The Central Bank of West African States). Under the guise of legitimate attachment, OPERA1ER distributes Remote Access Trojans, such as **Netwire, bitrat, venomRAT, AgentTesla, Remcos, Neutrino, BlackNET, Venom RAT**, as well as password sniffers and dumpers. After gaining access, OPERA1ER exfiltrate emails and internal documents to use them in further phishing attacks. They take time to study internal documentation carefully to better prepare for the cashing out stage, as most of OPERA1ER's victims used a complex digital money platform.

The platform has a three-tiered architecture of distinct accounts to allow different types of operations. To compromise these systems, OPERA1ER would require specific knowledge about key people involved in the process, protection mechanisms in place, and links between back-end platform operations and cash withdrawals. The gang could have obtained this knowledge directly from the insiders or themselves by slowly and carefully inching their way into the targeted systems.

Digital forensic findings indicate that OPERA1ER harvested credentials for three accounts with different access levels to perform fraudulent operations.

The threat actors targeted operator accounts that contained large amounts of money. Then using the stolen credentials transferred money into Channel User accounts and after that, moved the stolen funds into subscriber's accounts which they control. Finally, the funds were withdrawn from the system in cash via a network of ATMs. In one case studied by the researchers, a network of more than **400 subscriber accounts** controlled by money mules hired by OPERA1ER was used to enable the cashing out of the stolen funds, mostly done overnight via ATMs. Group-IB and Orange researchers discovered that money mules had been recruited three months in advance by analyzing the activity on the subscriber accounts used in illicit money withdrawals.

Other findings indicate that at least in two banks, OPERA1ER managed to get access to the SWIFT messaging interface software (presumably Alliance Access) running on the banks' computers. The software is used to communicate the details of financial transactions. It is important to note that SWIFT was not compromised, but the attackers were able to break into the systems inside the banks where this software was installed.

In one bank, the threat actor took control of an SMS server that could have been used to bypass anti-fraud or cash out money via payment or mobile banking systems. However, it is unknown whether the threat actor managed to steal money in any of those attacks.

For the first time, Group-IB described OPERA1ER complete Tactics, Techniques, Procedures, tools, and kill chain obtained from investigations of incidents involving the gang. The **report** will be helpful for corporate cybersecurity teams as it contains hunting tricks and Indicators of Compromise (IoCs), which can be used to check the networks for traces of OPERA1ER, prevent their future attacks, and take proactive measures to defend the perimeter.

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

EU & NA: +31 20 226 90 90

MEA: +971 4 568 1785

info@group-ib.com