GROUP-IB

EXECUTIVE SUMMARY

BEHIND THE BREACH

How OPERA1ER seized millions from fraudulent transactions

The CISO's guide

The threat actor "OPERA1ER" has repeatedly attacked banks with a basic toolset to execute fraudulent transactions as a part of their phishing campaign. Although African banks were the most frequent victims, highly targeted campaigns have also been observed against many other industry verticals in different geographic regions. Organizations should take steps to mitigate the threat of this highly replicable attack.

Stats

Threat actor	OPERA1ER
Activity	2016 - present
Confirmed attacks	30
Countries attacked	14
Confirmed fraud	$11 million
Estimated fraud	$30+ million

About the attack

Analysis of the attacks shows that most start with spear phishing emails carrying Remote Access Trojans (RATs) and other tools to collect user credentials. The spear phishing emails were highly targeted, with content tailored for specific audiences of as few as 18 people. The stolen credentials were used to gain administrator privileges on the domain controllers and the banking back-office systems.

From initial access, the average dwell time was 3-12 months, at which point money would be stolen. During this time the threat actor would study the victims' network, often using well-known tools and vulnerabilities. Through analysis of the attacks, Group-IB discovered that vulnerabilities as old as 3 years had been utilised by OPERA1ER, and in at least one case, an antivirus update server within the network had been used as a pivot point to compromise other systems.

The final phase of the attack would often take place on a weekend, OPERA1ER would utilise the banking infrastructure to fraudulently transfer money from the bank's customers' accounts to the mule accounts. Mules, hired by OPERA1ER would conduct "cash out" exercises, withdrawing money from numerous ATMs.

Timeline

2019
The threat actor began operating

2020
Group-IB began an investigation into the attacks

Further analysis revealed that the attacks most likely started with spear phishing emails carrying Remote Access Trojans (RATs) and other tools.

3-6 month
before fraud, OPERA1ER begins recruiting mules that would withdraw money during the final stage.

May 2020
To carry out more detailed investigations, CERT Orange reached out to Group-IB's team

Group-IB was able to identify more than 30 attacks carried out by OPERA1ER and manage incidents in Africa.

Group-IB tracked the infrastructure of the threat actor and created a detailed report containing hunting tricks and Indicators of Compromise (IoCs).

Striking twice

Many of the victim organizations were attacked twice, which shows the importance of engaging experienced and competent digital forensics and incident response teams to avoid repeated hacking.

How to mitigate the attack?

There are several actionable steps that organizations can take to mitigate attacks by OPERA1ER.

Action		Best practices
OPERA1ER often initiates attacks by sending highly targeted emails to specific teams within the organizations. Therefore, it is vital to analyze all incoming emails for malicious attachments.	→	Detonate incoming malware and identify phishing links with Group-IB Business Email Protection. The built-in sandbox can be configured to look like your environment, overcoming threat actors' evasion techniques.
Once within the network, OPERA1ER often deploys malware. So, organizations need to conduct an infrastructure audit to identify RATs, Metasploit Meterpreter and Cobalt Strike beacons within the corporate perimeter. Also, search for IoCs of OPERA1ER's activity.	→	Automatically detect suspicious activity occurring on infrastructure with Group-IB XDR. Use threat hunting features to proactively search for activity by skilled threat actors'. Utilise Group-IB Threat Intelligence high fidelity threat landscape to prioritize hunting activities.
There are no zero-day threats in OPERA1ER's arsenal, and the attacks often use exploits for vulnerabilities discovered three years ago. To mitigate threats, updating infrastructure and installing security patches would be a good practice.	→	Enhance your patch prioritization program with Group-IB Threat Intelligence. Automatically monitor for vulnerabilities, track active exploitation by threat actors, and detect discussions about the vulnerabilities on underground forums.

Stay off OPERA1ER's hook

Incessant tracking by Group-IB of OPERA1ER's malicious activities revealed that they often **operate during weekends and public holidays**. Improve your security posture by having complete visibility into the threat actor's insights.

To identify and protect yourself from cyber intrusions, build a response plan with Group-IB's kill chain.

LEARN MORE

VISIT GROUP-IB

Group-IB's mission:
Fight against cybercrime

Group-IB is a leading provider of innovations and solutions for detecting and preventing cyberattacks, eliminating fraud, and protecting brands from digital risks worldwide.

About Group-IB

1,300+ successful investigations	**600+** employees	**550+** enterprise customers
60 countries	**120+** patents and applications	**4** regions with research centers

Global partnerships

INTERPOL

Europol

Recognized by top industry experts

FORRESTER®

kuppingercole ANALYSTS

Gartner

IDC

FROST & SULLIVAN

Preventing and investigating cybercrime since 2003

FIGHT AGAINST CYBERCRIME

GROUP-IB.COM
INFO@GROUP-IB.COM

APAC
+65 3159 3798

EU & NA
+31 20 226 90 90

MEA
+971 4 508 1605