Guidance On an Ongoing Hacktivist Operation #Opspatuk Conducted by The Malaysian Hacktivist Threat Group 'DragonForce' Against Indian Organizations | FortiGuard Labs

Published: 2022-06-15 · Archived: 2026-04-02 12:24:34 UTC

The 'OpsPatuk' operation began on June 6, 2022. That’s when the Malaysian hacktivist group known as DragonForce began targeting India in retaliation for controversial comments made by a BJP spokesperson.

At the time of writing, this operation has compromised over 102 websites and continues to list new targets on various social media platforms, including Telegram, Twitter, and their own DragonForce website.

Widely targeted sectors include financial organizations, government entities, and educational institutions. FortiGuard Threat Research Team has also observed hosting providers being one of their main targets, enabling attackers to compromise their customers' websites. Additionally, the threat group has also encouraged other hackers to join the operation.

Hacktivism uses computer-based civil disobedience strategies such as hacking to advocate a political agenda or social change on the Internet. While the roots of hacktivism can be traced back to the 1990s, people worldwide have recently begun to adopt this strategy on a vast scale, thanks to the expanding age of digitization and the paradigm shift brought about by the worldwide pandemic.

Our team is proactively monitoring the OpsPatuk event and will release timely updates as events develop. In addition, the following advisory contains details about the operation and steps that can be taken to mitigate risks.

What is #OpsPatuk?

#OpsPatuk, aka Operation Patuk, is an ongoing operation led by a Malaysia-based hacktivist group dubbed 'DragonForce.' June 6, 2022, witnessed one of the first activities by the group that framed cyberattacks as retribution for controversial remarks made by a BJP spokesperson (now suspended). BJP (Bharatiya Janata Party) is one of India's two major political parties.

What are the most common attack vectors observed?

So far, DragonForce and its supporters have predominantly targeted victims using the following techniques:

- DDoS
- Website defacement
- Compromising VPN portals with stolen credentials
- Targeting web application vulnerabilities
- Exploiting the recent Atlassian Confluence vulnerability (CVE-2022-26134)

The group has also publicly released sensitive information about several organizations on its official website.

Who are the targets?

At the time of writing, FortiGuard Threat Research could identify over 100+ Indian websites targeted by the group. They seem to be primarily targeting the government, technology, financial services, manufacturing, and education sectors.

What steps should an enterprise take to mitigate its risk?

Hacktivist groups like DragonForce often respond to specific events and therefore need to be expeditious in attacking their targets to get their message across as quickly as possible. Due to this time constraint, driven by the need to create immediate awareness, they rely on relatively simple but highly visible activities like DDoS attacks and website defacements. However, we expect other common methods, such as public exploits and stolen credentials, will likely be utilized by these groups in the near future.

As a result, we propose that organization(s) review the following recommendations for mitigating the most common attack vectors to further strengthen their response to acts of hacktivism.

- Carry out robust threat hunting based on the compromised account. Check AV/EDR and SIEM logs to identify any malicious activities.
- Once the infected system is identified, isolate the system and perform reimaging.
- Change the passwords of compromised users.
- Notify users about the activity and inform them to change the passwords on all other public profiles and enable two-factor authentication wherever possible.
- Organizations should conduct periodic security awareness training, which will help to improve the operational security of their employees. Such training should ensure that users:
    - are aware of the risks of online fraud
    - are aware they should never share OTPs
    - understand the techniques used by malicious actors
    - are conscious of any suspicious activity on their systems and understand who they should report this to within the organization

Fortinet Protections

As multiple techniques are being used in this operation to make the quickest and most high-profile impact, the list of Fortinet protections covers many areas. Customers should assess the risk to their organization and implement appropriate security controls where needed. Here is a selection of ways Fortinet can help.

DDoS attacks

Organizations should monitor for spikes in incoming network traffic and scale accordingly to mitigate downtime caused by such increases in traffic.

- Organizations can deploy server redundancy and network segmentation proactively, ensuring FortiGate firewalls, FortiADC load balancers, and other network devices have all necessary rules/ACLs in place.
- To mitigate against large-scale DDoS, ML-enabled FortiDDoS can be employed.

Public exploits

Organizations should implement a risk-based vulnerability management process for their IT infrastructure to ensure that critical vulnerabilities and security misconfigurations are identified and prioritized for remediation.

- FortiRecon Digital Risk Prevention Service can help organizations gain control and visibility of their attack surface before attacks occur.
- FortiGate Next-Generation Firewall with FortiGuard IPS can be deployed to 'virtually patch' and block exploits against vulnerabilities before critical systems can be remediated – including against the Atlassian Confluence RCE vulnerability (CVE-2022-26134) being targeted.
- FortiGuard Outlook Alerts enables rapid visibility across your Fortinet estate to identify if you have been impacted/protected by 0-day activity such as the Atlassian Confluence RCE vulnerability (CVE-2022-26134).
- Deploy FortiEDR on company-managed devices to prevent malware and ransomware based on the behavior of malicious files.

Web application vulnerabilities

- FortiWeb Web Application Firewall can be deployed on-prem or in the cloud to secure web-facing Services and APIs as a compensating control for code sanitization deficiencies.
- Longer-term, to identify code issues, FortiDevSec and FortiPenTest can be employed to detect flaws in web applications before they reach production.

Leaked credentials

To prevent credential stuffing attacks caused by the inevitability of users re-using passwords across multiple sites, organizations must enforce Multi Factor Authentication (MFA) for all logins.

- FortiToken can provide MFA for your FortiGate SSL-VPN and, when combined with FortiAuthenticator, can deliver MFA-enabled Single Sign On for all your applications.
- To prevent credential stuffing into your web applications, enable credential stuffing defense on your FortiWeb Appliance or Cloud service and use FortiRecon External Attack Service Management to identify user credential risks to your organization.

User awareness

- The FortiPhish Phishing Simulation Service uses real-world simulations to help organizations test user awareness and vigilance to phishing threats and to train and reinforce proper practices when users encounter targeted phishing attacks.
- We also suggest that organizations have their end users undergo our free NSE training: NSE 1 – Information Security Awareness. It includes a module on Internet threats designed to help end-users learn how to identify and protect themselves from various types of phishing attacks.

Attack remediation and incident response

FortiGuard Incident Response Services deliver critical services before/during/after a security incident. Our experts arm your team with fast detection, investigation, containment, and return to safe operation.

IOCs

These threat actors are using multiple techniques to achieve their goals. The known exploits being used include the following recently publicized exploits. However, organizations are cautioned that this list is expected to grow.

Atlassian Confluence vulnerability CVE-2022-26134 (Outbreak Alert)

Java/Websh.D!tr
HTML/Agent.D71B!trW32/Filecoder.1104!tr.ransom
ELF/BitCoinMiner.HF!tr
ELF/Mirai.A!tr
Linux/Agent.PZ!tr
Linux/CVE_2021_4034.G!tr
Riskware/CoinMiner
Adware/Miner

MSDT Follina CVE-2022-30190 (Outbreak Alert)

WSO2 vulnerability (CVE-2022-29464)

W64/Agent.CY!tr
ELF/Agent.AR!tr
ELF/BitCoinMiner.HF!tr
Java/Agent.AUJ!tr
Java/Webshell.E!tr
Java/Webshell.0CC4!tr
Riskware/Generic.H2
Malicious_Behavior.SB

Learn more about Fortinet's FortiGuard Labs threat research and intelligence organization and the FortiGuard Security Subscriptions and Services portfolio.
