

# Hackaday

## Securing by the Crowd

Kok Tin Gan

Partner, Cybersecurity and Privacy  
PwC Hong Kong's Dark Lab



# 2022 Cyber threats in overview

🔒 Ransomware Attack

✉️ Business E-mail Compromise (BEC)

👤 APT Group



**January 2022**

LockBit 2.0 exploits Fortigate SSL VPN vulnerability (CVE-2018-13379) to compromise local financial services associations

**2022**



**January 2022**

Threat actor exploited Log4Shell (CVE-2021-44228) hours after POC was released; remained stealthy for 2+ months to exfiltrate data



**July 2022**

ALPHV/BlackCat compromised non-profit organisation via an exposed RDP; likely initial access broker (IAB) as next hands-on action was one week later



**April 2022**

Active exploitation of VMware WorkSpace ONE server-side injection vulnerability (CVE-2022-22954) to exfiltrate sensitive data...



**March 2022**

LockBit 2.0 affiliate leveraged 0-day on SonicWall SSLVPN to circumvent MFA – Dark Lab awarded CVE-2022-22279



**July 2022**

...and institute compromised again 3+ months later via CMS; per DFIR/TI, the same threat actor obtained access from an IAB



Mass exploitation of Zimbra Collaboration injection vulnerability (CVE-2022-27924) observed days after POC was publicly available – over 15+ victims in Hong Kong

**October 2022**



**September 2022**

Hong Kong and Singapore citizens targeted by global smishing campaign impersonating Hongkong Post and SingPost; shift towards B2C



**September 2022**

Multi-million dollar loss through business email compromise (BEC) on global payment service provider; threat actor persisted for 2+ months to identify and target higher-profile users



**November 2022**

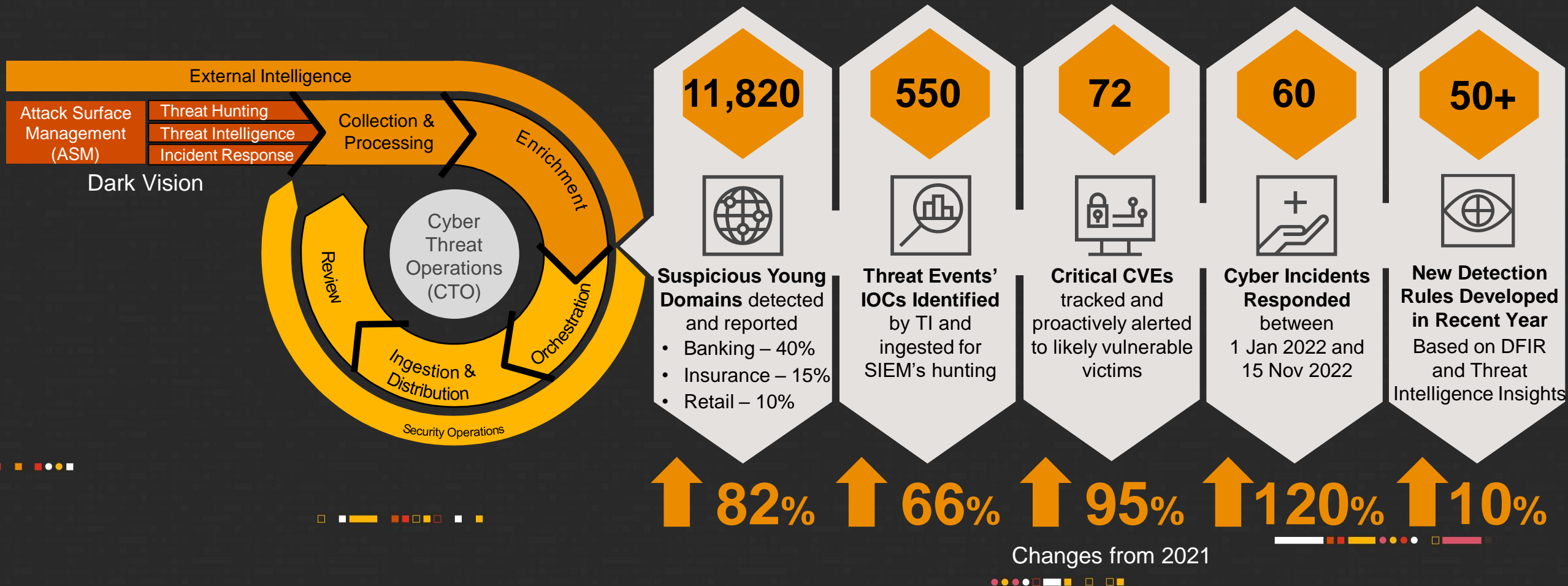
Mass exploitation of FortiOS authentication bypass vulnerability (CVE-2022-40684) observed days after POC was available with 10+ compromised – Cyber Vigilante?

**NOW**



# Dark Lab cyber threat operations 2.0

Operationalising threat intelligence for proactive managed detection and response



# Summary of lessons learnt



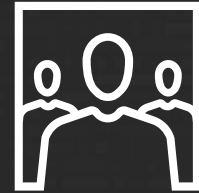
Threat actors are increasingly sophisticated – **Speed** and **Scale**



Weaponisation of CVEs  
**Occur mere hours after POCs released**  
– Either in public or dark web

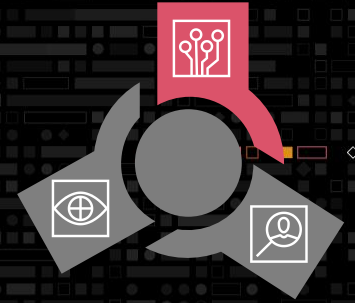


Shift in focus to exploit  
**Web-based Vulnerabilities** due to  
Increased Connectivity and Digitalisation



Threat actors are  
**Specialising and Crowdsourcing**  
**their Skillsets**

# Weaponisation of CVEs occur mere hours after POCs are released – either in public or dark web



**T-2  
days**

Dark Lab uncovers Spring4Shell CVE-2022-22965 POC on the dark web, and conducts CTO to notify potential victims prior to public news release

**8  
hours**

Log4Shell CVE-2021-44228 was weaponised, with mass automated scans and exploitation observed

**0  
days**

Threat actor releases SonicWall SSLVPN exploit code on dark web and is weaponised immediately; Dark Lab awarded CVE-2022-22279

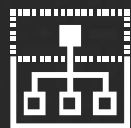
**2  
days**

Mass exploitation of Zimbra Collaboration injection vulnerability (CVE-2022-27924) observed – over 15+ victims in Hong Kong

**3  
days**

Mass exploitation of FortiOS authentication bypass vulnerability (CVE-2022-40684) observed – over 10+ victims in Hong Kong

# Threat actors are specialising and crowdsourcing their skillsets



Rise of Initial Access Brokers (IABs)

400%  
Increase in  
Listings

>20  
Days From Sale  
to Impact



Phishing-as-a-Service (PhaaS)  
Platforms

43 Bil  
Global Cost of  
BEC Attacks

B2C  
Observation Of  
Shift To Target  
Individuals



Talent Drives, Contests,  
and Rewards

2 BTC  
Prize Pool for  
Technical  
Pocs

1 Mil  
US Dollar Bug  
Bounty Awards  
by Lockbit



Speed



Impact



# Shift in focus to exploit web-based vulnerabilities due to increased connectivity and digitalisation



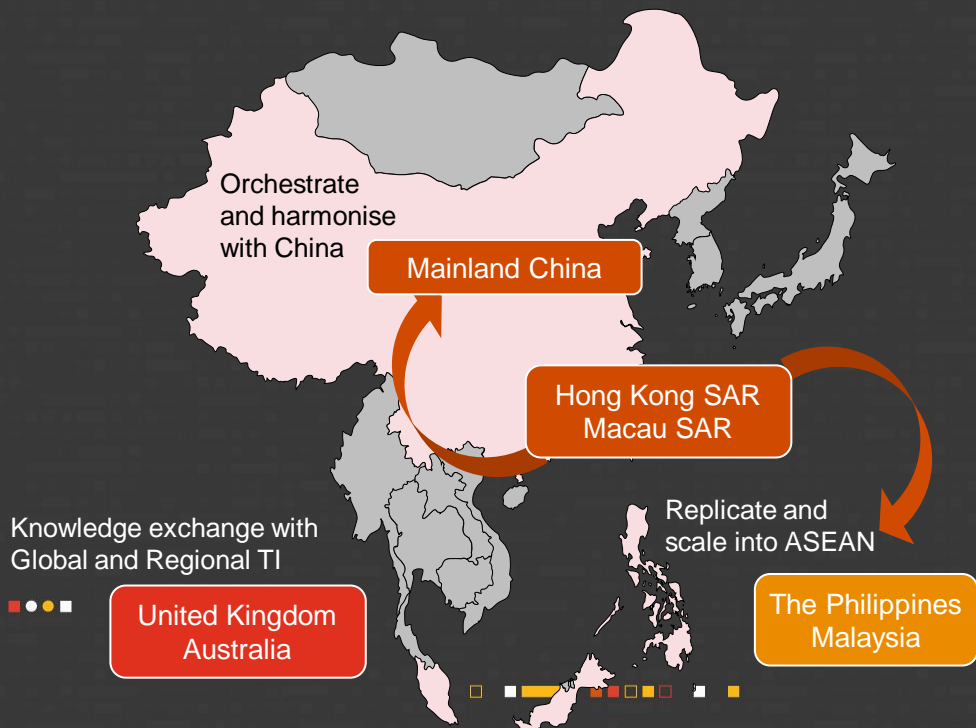
## Shift in focus to exploit web-based vulnerabilities due to increased attack surface

	Log4Shell	SonicWall SSLVPN	VMWare Workspace ONE	Zimbra Collaboration	Sitecore	Liferay Portal	Telerik UI	Microsoft SharePoint
Vulnerability	CVE-2021-44228	CVE-2022-22279	CVE-2022-22954	CVE-2022-27924	CVE-2021-42237	CVE-2020-7961	CVE-2019-18935	CVE-2019-0604
Month Observed Being Exploited in Hong Kong	December 2021	March 2022	April 2022	October 2022	August 2022	October 2022	March 2022	September 2022
Impact	RCE	Post-auth RFI – Circumvent MFA	RCE	Unauthenticated Remote Code Injection	Insecure Deserialisation Attack to RCE	RCE via JSON Web Services	RCE via .NET JSON Deserialisation Vulnerability	RCE
Potential Victims in Hong Kong *	1,000+	150	20	200	10	5	20	5
New vulnerabilities in 2022					Older but still severe vulnerabilities			

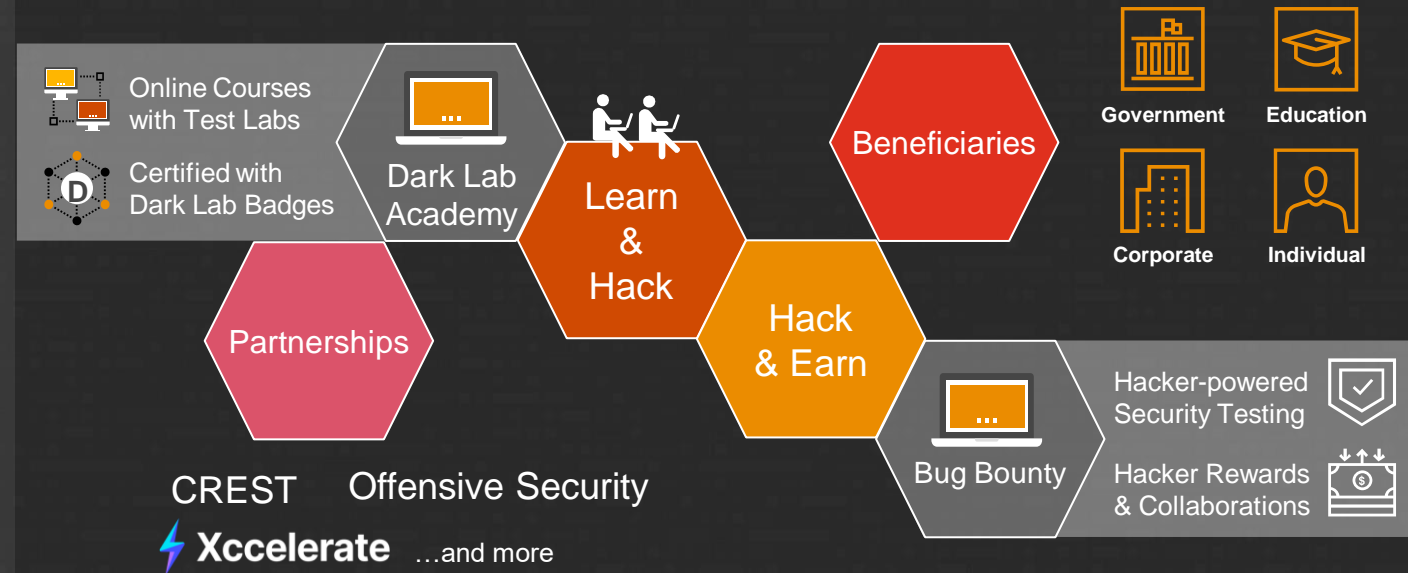
\*as of date of scan as outlined in table

# The increase in cyber incidents also taught us that we need a bigger “Crowd” to jointly secure our ecosystem...

Expand Dark Lab’s Cyber Threat Operations in HK/MO across Asia Pacific and knowledge exchange with Global



Nurture, upskill and reskill cybersecurity talents around the world to continuously contribute back to the ecosystem





# Unboxing an incident showcasing Lockbit 2.0 affiliate's innovation and speed in March 2022

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Exploit Public-Facing Application	Command and Scripting Interpreter	Valid Accounts	Valid Accounts	Deobfuscate/Decode Files or Information	OS Credential Dumping	Account Discovery	Remote Services	Data Staged	Application Layer Protocol	Exfiltration Over Web Service	Data Encrypted for Impact
Phishing	System Services	Account Manipulation	Abuse Elevation Control Mechanism	Impair Defenses	Brute Force	File and Directory Discovery	Exploitation of Remote Services	Archive Collected Data	Data Encoding	Exfiltration Over Alternative Protocol	Inhibit System Recovery
Valid Accounts	Scheduled Task/Job	Boot or Logon Autostart Execution	Access Token Manipulation	Indicator Removal on Host	Credentials from Password Stores	Network Share Discovery	Lateral Tool Transfer	Data from Local System	Encrypted Channel	Automated Exfiltration	Service Stop
External Remote Services	Software Deployment Tools	Create or Modify System Process	Boot or Logon Autostart Execution	Masquerading	Exploitation for Credential Access	Permission Groups Discovery	Software Deployment Tools	Data from Network Shared Drive	Fallback Channels	Exfiltration Over C2 Channel	Data Destruction
Drive-by Compromise	User Execution	External Remote Services	Create or Modify System Process	Modify Registry	Steal or Forge Kerberos Tickets	Process Discovery	Use Alternate Authentication Material	Data from Cloud Storage Object	Ingress Tool Transfer		Defacement
Supply Chain Compromise	Windows Management Instrumentation	Scheduled Task/Job	Process Injection	Valid Accounts	Unsecured Credentials	Remote System Discovery		Email Collection	Protocol Tunneling		Resource Hijacking
Trusted Relationship	Exploitation for Client Execution	BITS Jobs	Scheduled Task/Job	Abuse Elevation Control Mechanism		System Information Discovery			Remote Access Software		Account Access Removal
	Native API	Boot or Logon Initialisation Scripts	Boot or Logon Initialisation Scripts	Access Token Manipulation		System Network Connections Discovery			Web Service		
		Create Account	Exploitation for Privilege Escalation	File and Directory Permissions Modification		Virtualisation/Sandbox Evasion			Remote File Copy		
		Hijack Execution Flow	Hijack Execution Flow	Obfuscated Files or Information		Application Window Discovery					
		Server Software Component		Process Injection		Domain Trust Discovery					
				System Binary Proxy Execution		Network Service Discovery					
				Virtualisation/Sandbox Evasion		Peripheral Device Discovery					
				BITS Jobs		Query Registry					
				Hide Artifacts		Software Discovery					
				Hijack Execution Flow		System Owner/User Discovery					
				Use Alternate Authentication Material		System Service Discovery					

0 day

Utilised to achieve initial access at the SonicWall SSL-VPN (CVE-2022-22279), deviating from typical Fortinet SSLVPN access vector

2 hours

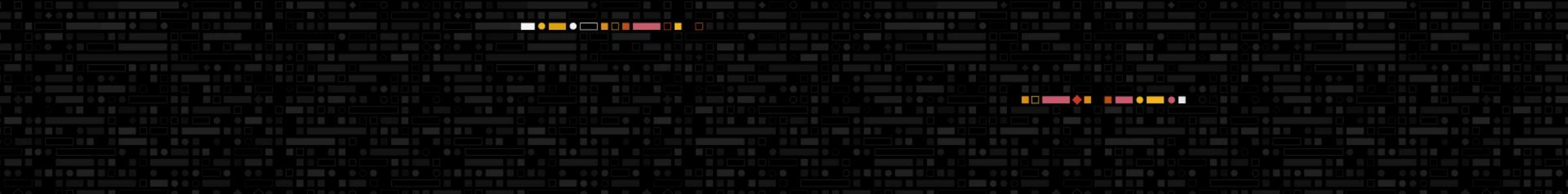
from initial access to exfiltrating data and deploying ransomware

17

MITRE ATT&CK TTPs utilised; need layered defence to prevent, detect, and respond quickly



# Thank you



© 2022 PricewaterhouseCoopers Limited. All rights reserved. Not for further distribution without the permission of PwC. PwC refers to the Hong Kong member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see [www.pwc.com/structure](http://www.pwc.com/structure) for further details. This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.