Threat actors are ramping up efforts, to exploit the growing Coronavirus panic, across the world

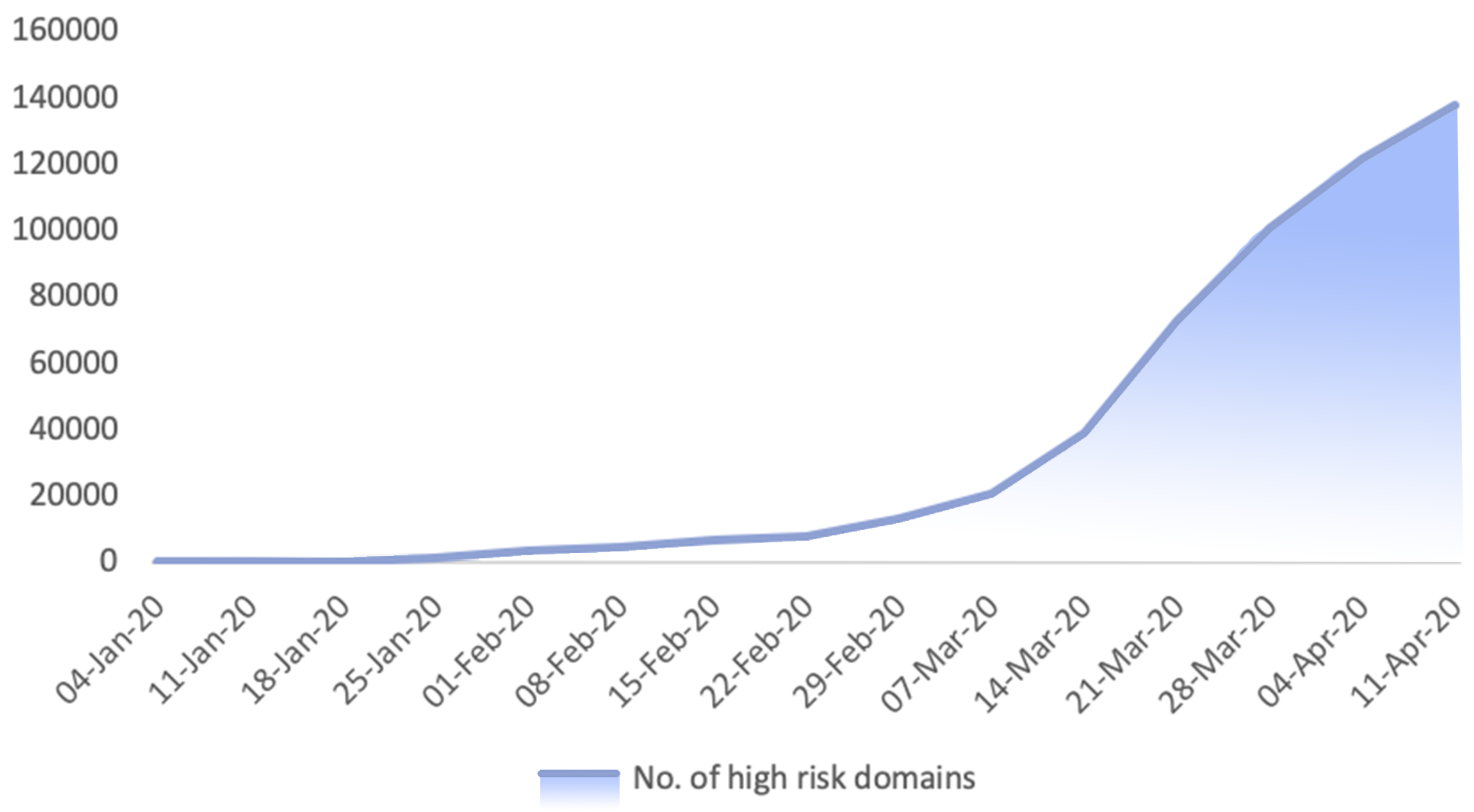
Making sense of the thousands of COVID-themed cyber threats that are detected every day

Over the past few weeks there have been reports of malware laced COVID guidance manuals, fake medical supplies for sale on the dark web, and direct attacks on hospitals and testing facilities.

However, these individual occurrences don't capture the complete scale and volume of the cyber attacks.

In this report, we look at the combined scope and impact of the growing number of cyber threats, ranging from malicious COVID-related domains, to phishing campaigns and malware attacks.

100,000+ COVID related domains registered since Jan' 2020



Data Source: Domain Tools

Thousands of COVID domains registered every day

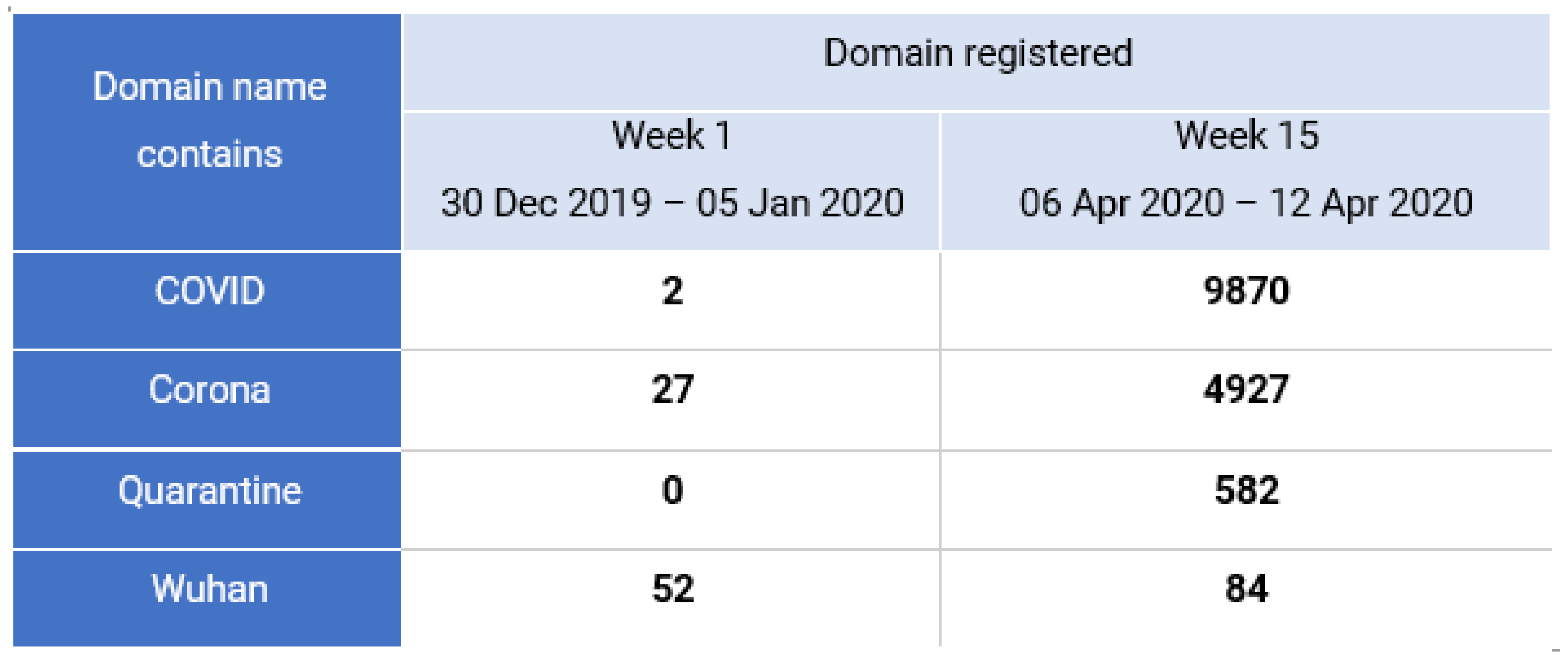
While not all the registered sites are malicious, there are thousands of active threats among them. These domains are being used to orchestrate **scams**, **deliver malware** and ransomware payloads, send **phishing emails**, and **steal data** that can be sold on the dark web. This graph shows the domains registered every week, since the 1st week of Jan' 2020, which have a risk score >70.

COVID related domains more likely to be malicious

Coronavirus-related domains are 50% more likely to be malicious than other domains registered during the same period.

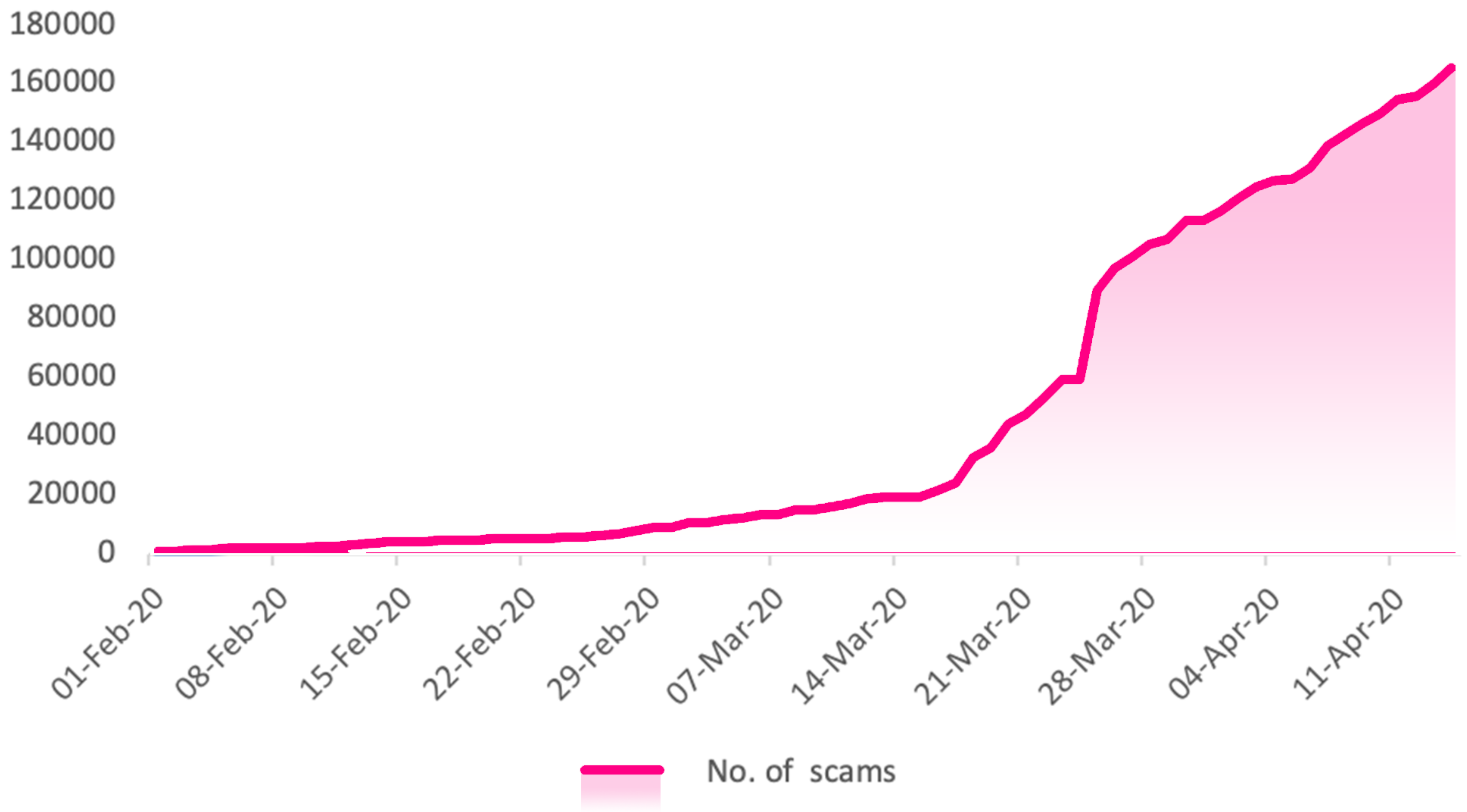
- Check Point

Trend of COVID related domains



Domain name contains	Domain registered	
	Week 1 30 Dec 2019 – 05 Jan 2020	Week 15 06 Apr 2020 – 12 Apr 2020
COVID	**2**	**9870**
Corona	**27**	**4927**
Quarantine	**0**	**582**
Wuhan	**52**	**84**

The internet is teeming with 150,000+ COVID related scams



Data Source: CheckPhish

Scams are piggybacking on COVID fears

Threat actors are orchestrating scams that exploit the shortage of medical supplies, and the demands of remote work. On the dark web, masks and vaccines are being sold at exorbitant prices. And on the surface web, the thousands of COVID related domains registered, are hosting fake charities and conferencing tools. This graph shows the number of scams detected every day, since 01 Feb' 2020.

Scams are targeting remote workers across the world

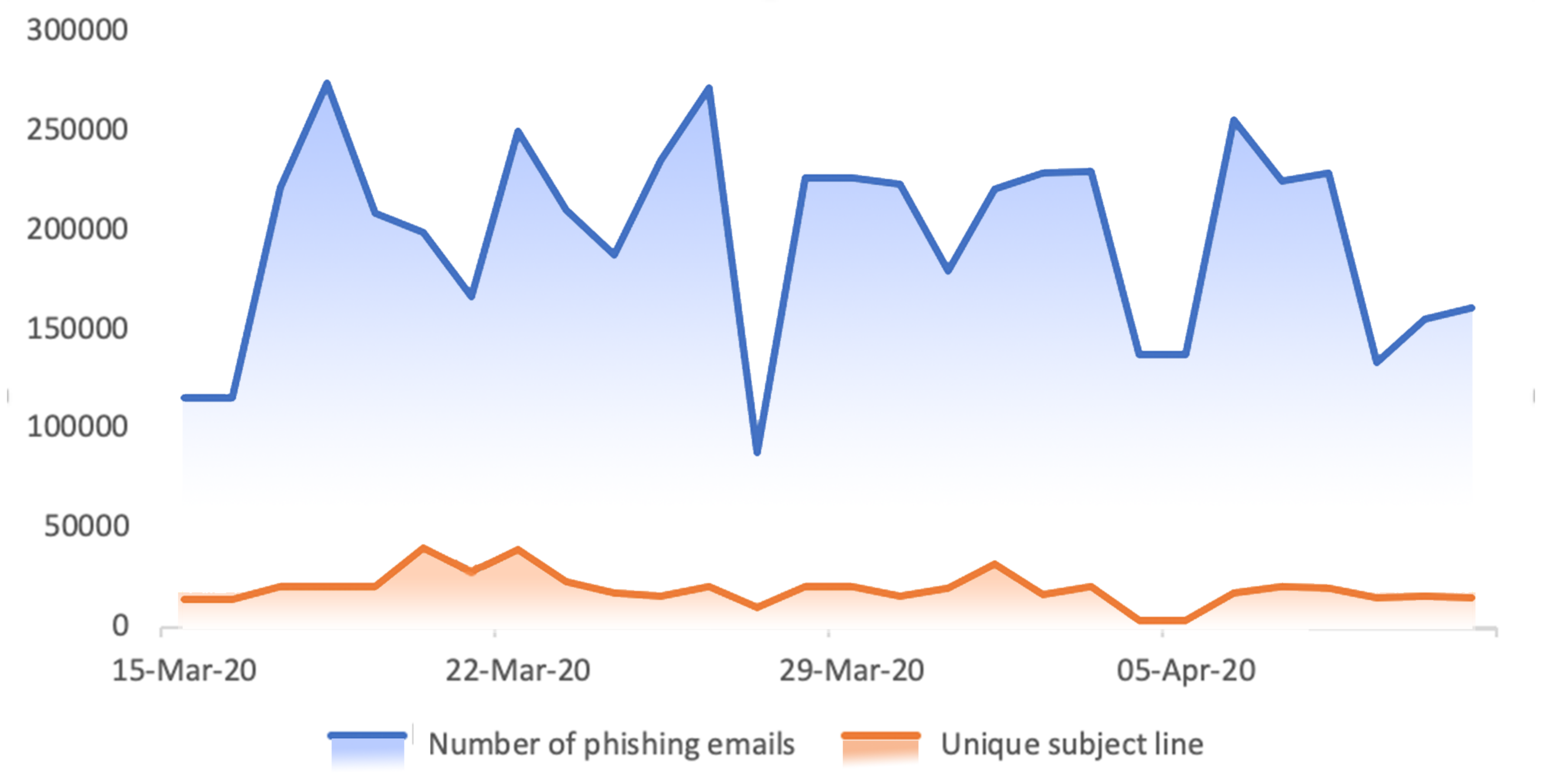
- Scam sites targeting Microsoft's cloud tools have increased 72% from January to March.
- Skype counterfeiting has increased 31% from February to March.

- CheckPhish

Common scams

- Fake N95 and medical grade masks and purported vaccines.
- Malware and ransomware apps and maps that claim to provide COVID updates.
- Trojanized versions of remote working tools, antivirus, and website plugins.

Phishing emails impersonate reliable entities to lure victims



Data Source: RiskIQ

Phishing emails adapt to exploit the pandemic

Phishing emails have been especially successful in initiating large scale malware and ransomware attacks, even on already stressed healthcare providers. From impersonating organizations such as CDC and WHO, to blackmail and extortion, we have observed a wide range of phishing campaigns. This graph shows the phishing emails detected every day, since 15 Mar' 2020.

Types of phishing emails

Scams: **54%**

Brand impersonation attacks: **34%**

Blackmail: **11%**

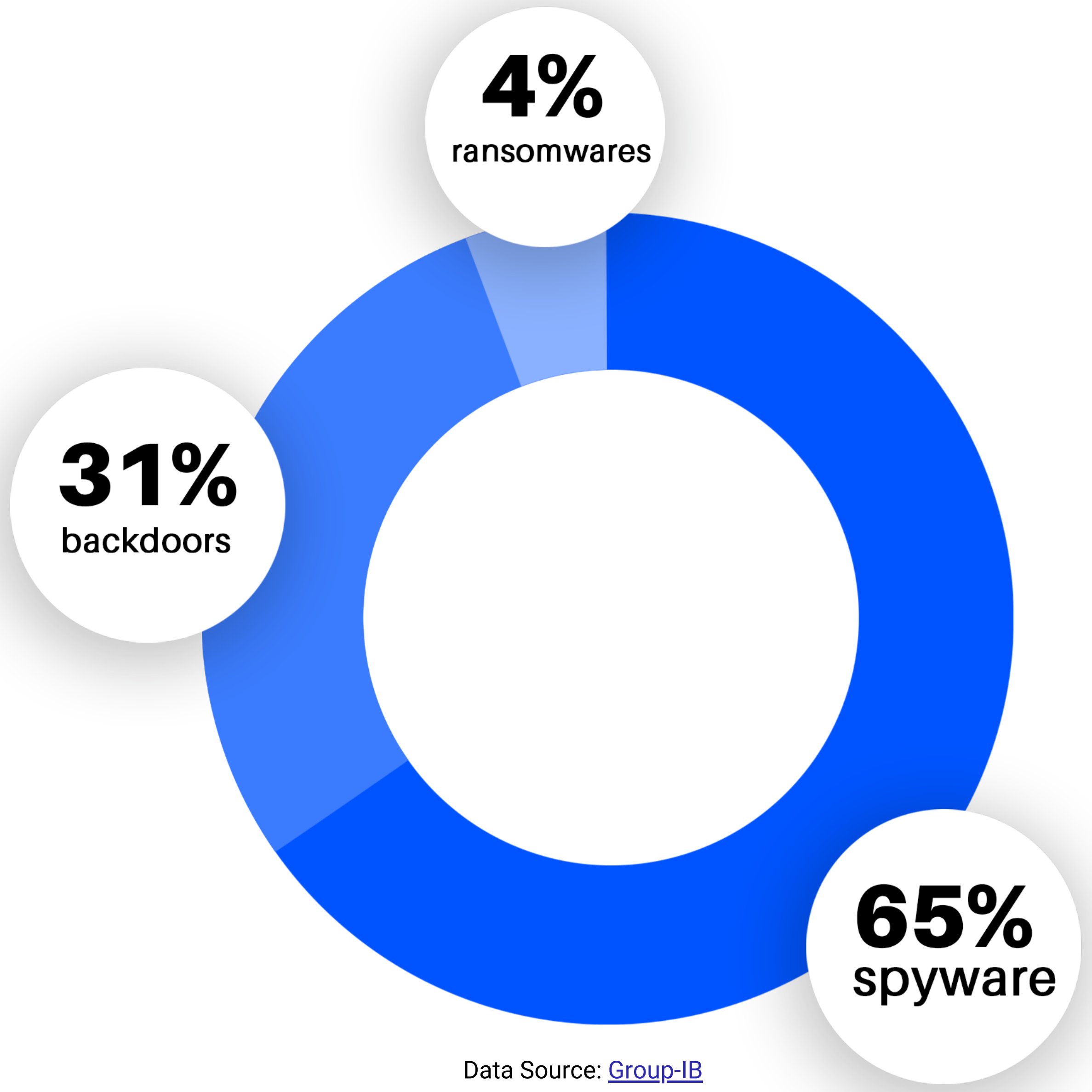
Business email compromise: **1%**

- Baracuda

Common phishing email lures

- COVID-19 advisories and updates from reliable organizations such as WHO and CDC.
- Extortion campaigns that threaten to infect the email recipient with Coronavirus.
- Relief efforts or benefits from the Government or the recipients employer.

Malware attacks target hospitals and COVID testing facilities



Data Source: Group-IB

Common malware families

Agent Tesla	45%
Netwire	30%
LokiBot	8%
Hawk Eye	7%
Unclassified spyware	4%
Aurora	3%
Hakbit	2%
Formbook	1%

Data Source: Group-IB

Phishing lures and scams are entry points for malware

Phishing email attachments, which pretend to be COVID guidelines or WHO advisories, are intended to deliver malware payloads to the victims' systems. They have been seen to steal data, credentials, and deliver other malware or ransomware. This graph shows the top malware classes that have been spread via COVID related lures.

Recent attacks on hospitals and research firms

- COVID vaccine testing firm Hammersmith Medicines Research (HMR) was the victim of a ransomware attack that exfiltrated their data.
- COVID research firm 10x Genomics, was hit by the Sodinokibi ransomware and data theft.
- Cyber attack on Czech COVID-19 testing lab and hospital caused surgeries to be postponed and patients to be sent to another hospital.

8x increase in cyber attacks

There has been an 8x increase in cyber attacks, thanks to remote work, loosened security controls to support it, and the menace of COVID themed scams.

WFH Cyber risks

Given the severity of the COVID-19 outbreak, remote work is the new normal. However, being outside your secure office networks increases your vulnerability to cyber-attacks. Despite VPNs and Firewalls, leakage of source codes, confidential data, and credentials, is an imminent threat.

Know more >>

60% chance of Third-party Vendor leaks

A 2018 study shows that nearly 60% of the companies surveyed, experienced data breached due to their third party vendors.

Third Party Vendor Leaks

When your third-party vendors have access to your confidential data and networks, it drastically increases the risk of your organization being targeted by cyber attacks. Third-party vendors give threat actors an unsecured point of entry to your organization, via which they can initiate and carry out attacks.

Know more >>

How CloudSEK can help ?

CloudSEK's 'XVigil' is an AI-powered SaaS-based platform that provides specific, actionable, and timely warnings that help you intervene and take swift action, thus preventing costly breaches and losses.By deploying comprehensive security scans and monitors, XVigil gives you unified supervision, of credential disclosures and data leaks, across the surface web, deep web, and dark web.

Source code leak Monitor

XVigil monitors code sharing services, to detect repositories and code files, which are leaking sensitive information related to your organization.

Confidential Data Leak monitor

XVigil alerts you to detect leaked emails, SMSs andother PII data.

Dark web monitor

XVigil identifies user credentials, in leaked databases and dumps, that have your organization's email domainor personal emails.

Infrastructure monitor

(multiple modules) to help you detect vulnerabilitiesyou might have exposed as you loosened your securitycontrols and firewalls to support WFH.

Quick Deployment

Since XVigil is SaaS-based, your dashboard will be up and running in 30 minutes.

Remote Setup

Having no in-person requirements means your XVigil account can be set-up and configured remotely.

Free for 1 month

Offering XVigil Free for 1 month. No Commitments, Just as simple as that.

Request a Demo

No commitments