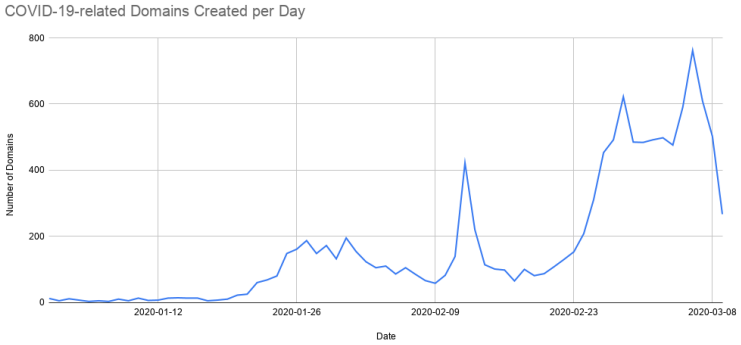
Protecting Against Remote Workforce Threats

Evaluating Cyber Threats With Recorded Future

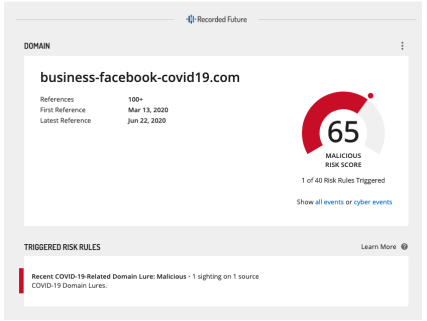
IN TODAY'S RAPIDLY CHANGING AND STEALTHY THREAT ENVIRONMENT, KNOWING WHAT'S HAPPENING INSIDE YOUR ORGANIZATION IS NOT ENOUGH.

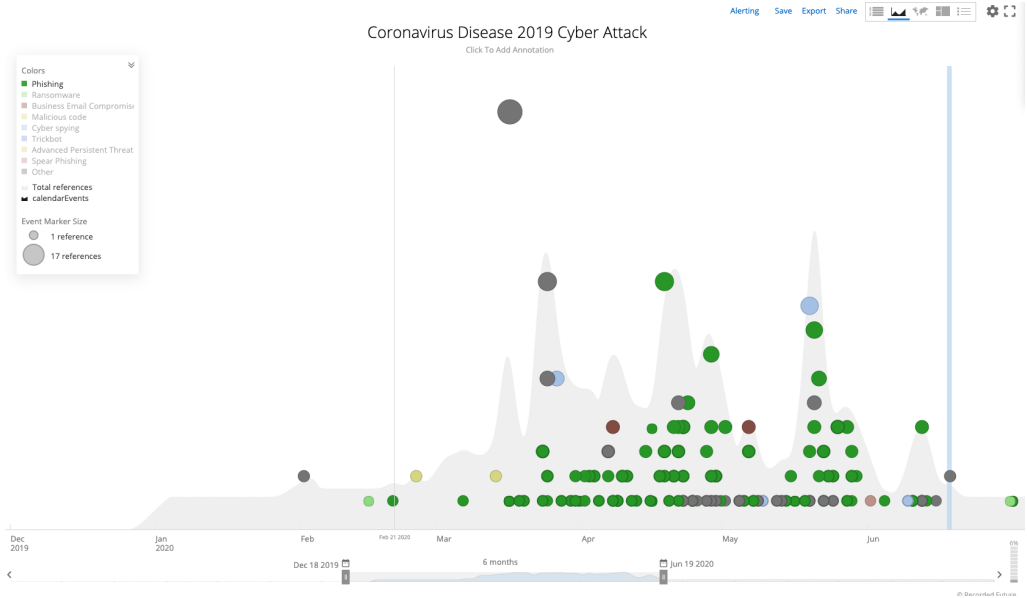
Recorded Future®

Phishing attacks During Covid 19 Period



Graph showing the registrations of COVID-19-related domains per day in 2020. Recorded Future analysts created a query to find domain registrations of URLs containing "corona," "covid19" or "covid2019."



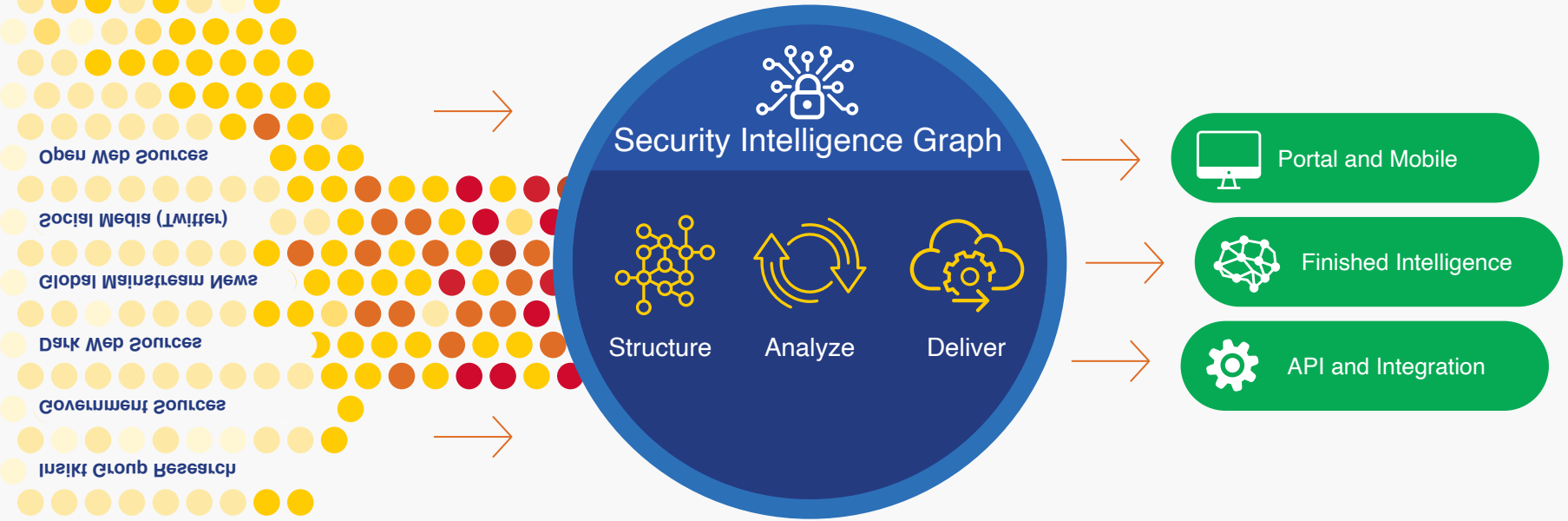


The Coronavirus Disease 2019 (COVID-19) Pandemic has created a massive cybersecurity threat by supercharging reliable attack techniques: lures that attract victims to malicious web pages by exploiting high interest in negative news and disasters.

Recorded Future

The Recorded Future® Platform

Transforming All Sources Into Actionable Intelligence



Recorded Future

COLLECTION

Automated Analysis Powered by Machine Learning

1,500+ FORUMS

Hacker, criminal, extremist, and research

65+ THREAT FEEDS

Every high-value feed available on the web

BLOGS & SOCIAL MEDIA

Security community, public Tweets, Facebook, and more

50+ PASTE SITES

Leak posts, credential breaches, corp IP

DARK WEB COLLECTION

Dark web sourcing from top tier, invite only, forums globally, including China, Russia, Brazil

ORIGINAL RESEARCH

Industry leading research at your fingertips

CODE REPOSITORIES

Code sharing, malware, C2s, POCs, app stores, vuln DBs

INTERNAL NOTES

Customer-generated intel notes and your IOC annotations

PROPRIETARY 3rd-PARTY FEEDS

Customer-exclusive internal & proprietary feeds and data

TECHNICAL COLLECTION

Shodan RAT controllers, Google dorking, domain and certificate registrations, NetFlow, GEO IP

CERTIFIED INTELLIGENCE

High-confidence, proprietary, block-grade feeds including Weaponized Domains & URLs, Command & Control, and Exploits in the Wild

DEEP LANGUAGE EXPERTISE

Automated analysis for every language with deep analysis for 12 languages

Recorded Future

Pandemic Monitoring

Evaluating a Pandemics potential effect on Business Operations

Use Cases

3rd Party Monitoring

Facility Monitoring

Global Awareness

Fraud Monitoring

Monitoring Vulnerabilities in Your Remote Access Tech Stack

FEATURES

- Real-time alerting of reported cases
- Automated Analysis for every language with deep analysis for 13 languages
- Intelligence Analysis provided by Recorded Future's Insikt Group
- Ontologies to organise and curate your organization's assets and locations
- Vulnerability risk scores based on exploitation

HOW RECORDED FUTURE HELPS

- Identify 3rd Parties affected and shutdowns.
- Monitor Facilities and locations around company assets
- Provide Global Awareness around Pandemic and its effect to operations.
- Monitor fraud such as fake mask sales, cures, etc.
- Provide risk scores on Vulnerabilities

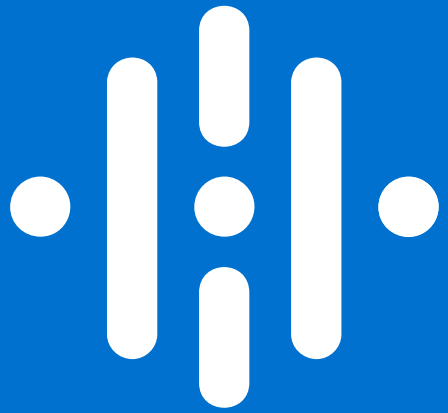
Combating these Attacks

Combating these attacks requires planning and awareness on the part of everyone in the organization. We recommend the following steps

1. IT and security teams should have a well-documented plan for working from home, as well as backup solutions
2. Combined with security controls, incident detection tools should work equally well with remote and on-premise systems.
3. Telework applications need to be prioritised for patching and configuration changes, and monitored closely for announcements about vulnerabilities, proof-of-concept (PoC) exploit code, and configuration vulnerabilities in those applications.
4. Monitor for VPN activity from strange locations. Especially with all the travel restrictions in place, there should be more homogeneity in VPN connections.
5. The increase in phishing and social engineering attacks during this period of expanded telework, communicate clearly with your workforce about the threats, what they should be looking for, and plan simulated attacks.

Source: https://www.recordedfuture.com/remote-attack-surface/

Recorded Future



End