German Task Force for COVID-19 Medical Equipment Targeted in Ongoing Phishing Campaign

securityintelligence.com/posts/german-task-force-for-covid-19-medical-equipment-targeted-in-ongoing-phishing-campaign/

Home / Incident Response

German Task Force for COVID-19 Medical Equipment Targeted in Ongoing Phishing Campaign

Incident Response June 8, 2020
By Claire Zaboeva 3 min read

During the course of ongoing research on coronavirus-related cyber activity, IBM X-Force Incident Response and Intelligence Services (IRIS) uncovered a COVID-19 related phishing campaign targeting a German multinational corporation (MNC), associated with a German government-private sector task force to procure personal protective equipment (Task Force Schutzausrüstung). The group has been commissioned to use their international contacts and expertise to obtain personal protective equipment (PPE) such as face masks and medical gear, particularly from China-based supply and purchasing chains.

IBM X-Force IRIS' research indicates that the threat actors behind this campaign targeted more than 100 high ranking executives in management and procurement roles within this organization and its third-party ecosystem. Overall, IBM X-Force IRIS observed approximately 40 organizations being targeted in this campaign. Given the extensive targeting observed of this supply chain, it's likely that additional members of the task force could be targets of interest in this malicious campaign, requiring increased vigilance. IBM X-Force IRIS has notified CERT BUND about this activity to further ensure members are aware.

This discovery represents a precision-targeting campaign exploiting the race to secure essential PPE. Based on our analysis, attackers likely intended to compromise a single international company's global procurement operations, along with their partner environments devoted to a new government-led purchasing and logistics structure.

Targeting New Medical Equipment Procurement Structures

On 30 March 2020, German government officials met with several top German MNCs to establish new 'framework agreements' to commission these nine companies to leverage their access to foreign markets to purchase and facilitate the delivery of PPE on behalf of various German Ministries.

Our research shows that, on this same date, suspicious activity from a Russia-based IP address toward the MNC began. Specifically, IBM X-Force IRIS discovered over 280 URLs tied to the suspicious Russia-based IP address 178[.]159[.]36[.]183, with more than a third including Base64 encoded email addresses belonging to suspected targets at the MNC and its third-party supply chain partners. Approximately half of the encoded email accounts belong to executives associated with operations, finance, and procurement within the targeted corporation. The remaining half belong to executives at third-party partners, including European and American companies associated with chemical manufacturing, aviation and transport, medical and pharmaceutical manufacturing, finance, oil and gas, and communications.

As of the time of publication, this campaign remains an ongoing operation.

Credential Harvesting

IBM X-Force IRIS discovered that the URLs redirect the target emailed to a fake, actor-controlled Microsoft login page designed to steal and exfiltrate user credentials to several different Yandex email accounts.

It is unclear how many of these phishing attacks were successful, however through credential harvesting, threat actors could gain access to the victims' email accounts with the potential to collect or exfiltrate data of interest, and/or move laterally through the network to fulfill other actions on objectives.

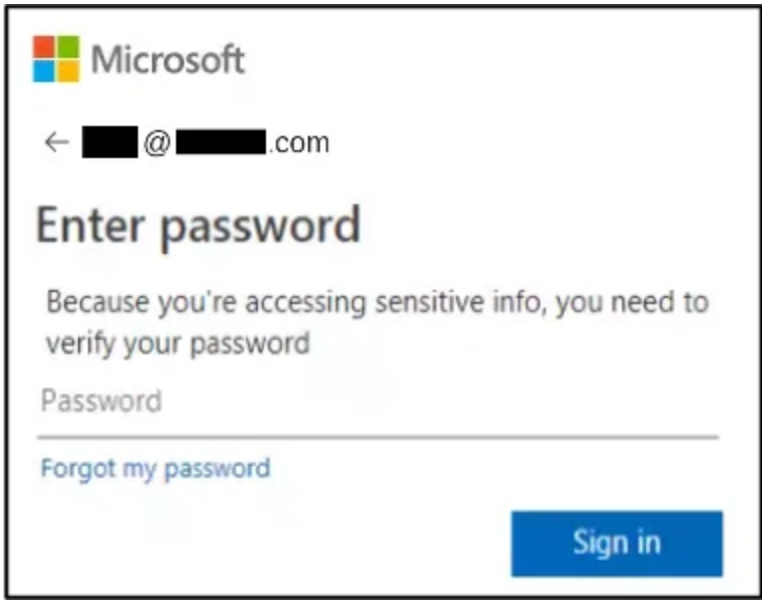


Figure 1: Fake Login Page

```
var licensekey = 'G814R78S12F5T1';
var emailkey = 'r35ul7@yandex.com';
var _$_b349=["XMLHttpRequest","ActiveXObject","Microsoft.XMLHTTP","off-v2","a","p","i",".","h",
```

Figure 2: Actor-owned email account embedded in the HTML

Global Race for Resources

A global rush to obtain essential PPE for health care personnel has resulted in an unprecedented leap in prices and competition for now-critical medical resources. To secure vital supplies, nations across the globe have launched a bevy of national buying programs, emergency state export statutes, and contracting initiatives to acquire the essential equipment to address the rapid spread of coronavirus.

Given the worldwide spread of COVID-19 and fears of a pending second wave of infection, it is highly likely criminal and state-sponsored actors alike will seek to exploit global procurement and supply chains with the intention of either profiting from the crisis or supporting the acquisition activities of their host nation.

Preparation, Planning and Practice

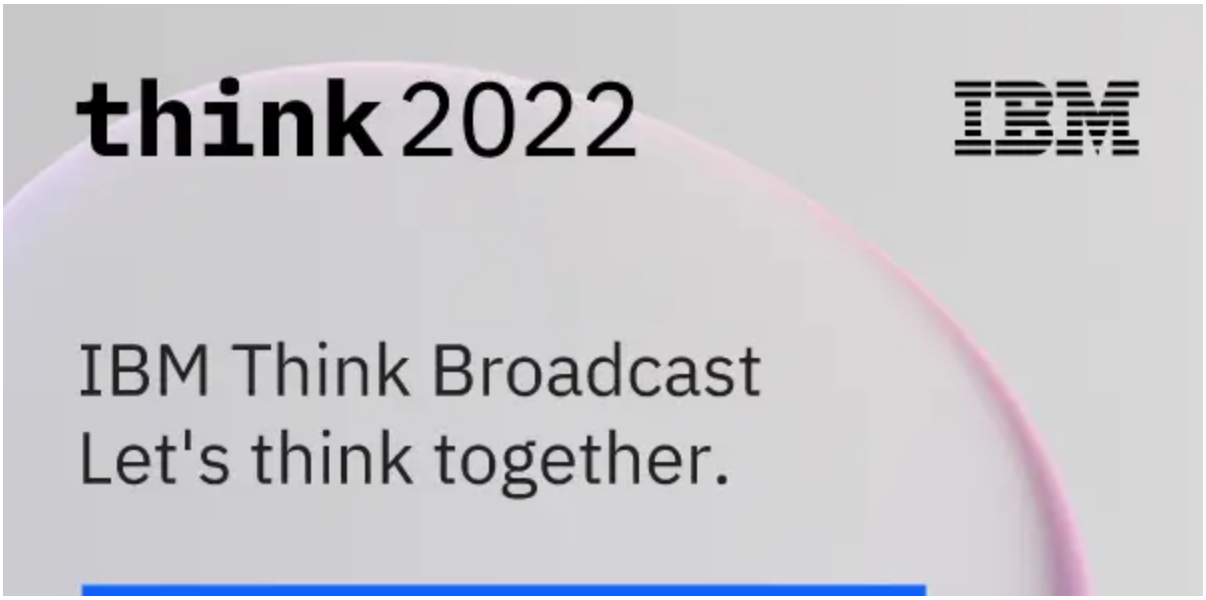
In this extraordinary time, many organizations across the globe are being called upon to perform essential tasks to outfit, equip and support medical professionals on the frontlines of a global crisis. These companies are now part of an emerging high value target group whose reliance on digital technology to enable business practices provides a potential means of compromise to malicious cyber actors. Now, perhaps more than ever, businesses must have an actionable Incident Response Plan in place to prevent, react and recover from a cyber emergency.

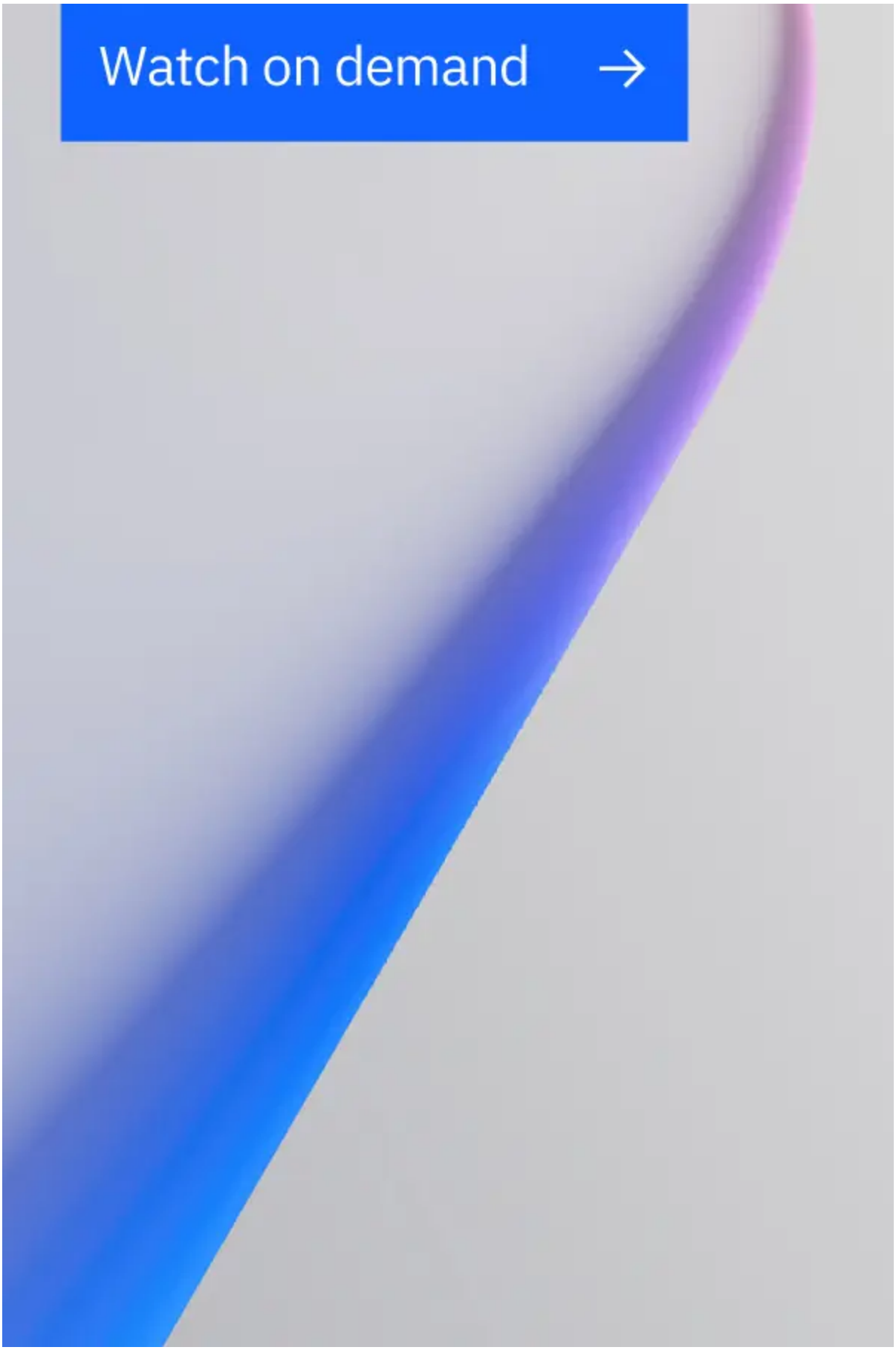
IOCs associated with this campaign are available via our Enterprise Intelligence Management platform.

This campaign also underscores the need for organizations to address the risks from phishing attacks. Phishing was the initial infection vector in nearly one-third of all cyber incidents we investigated last year. Please read our previously published blog "State of the Phish: IBM X-Force Reveals Current Phishing Attack Trends" to review ways to help mitigate this threat.

Phishing | X-Force
Claire Zaboeva
Senior Strategic Cyber Threat Analyst, IBM

Claire is a Senior Strategic Cyber Threat Analyst on the Threat Hunt & Discovery Team within IBM X-Force. Claire has over 10 years of analytic experience...




Watch on demand