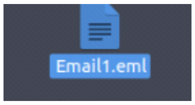
Analyzing a suspicious emails (Tryhackme)

Tuesday, October 31, 2023 3:03 PM

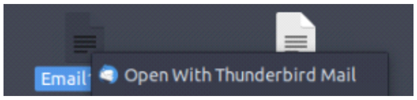
This is a part of my Threat Intelligence Tools Practices

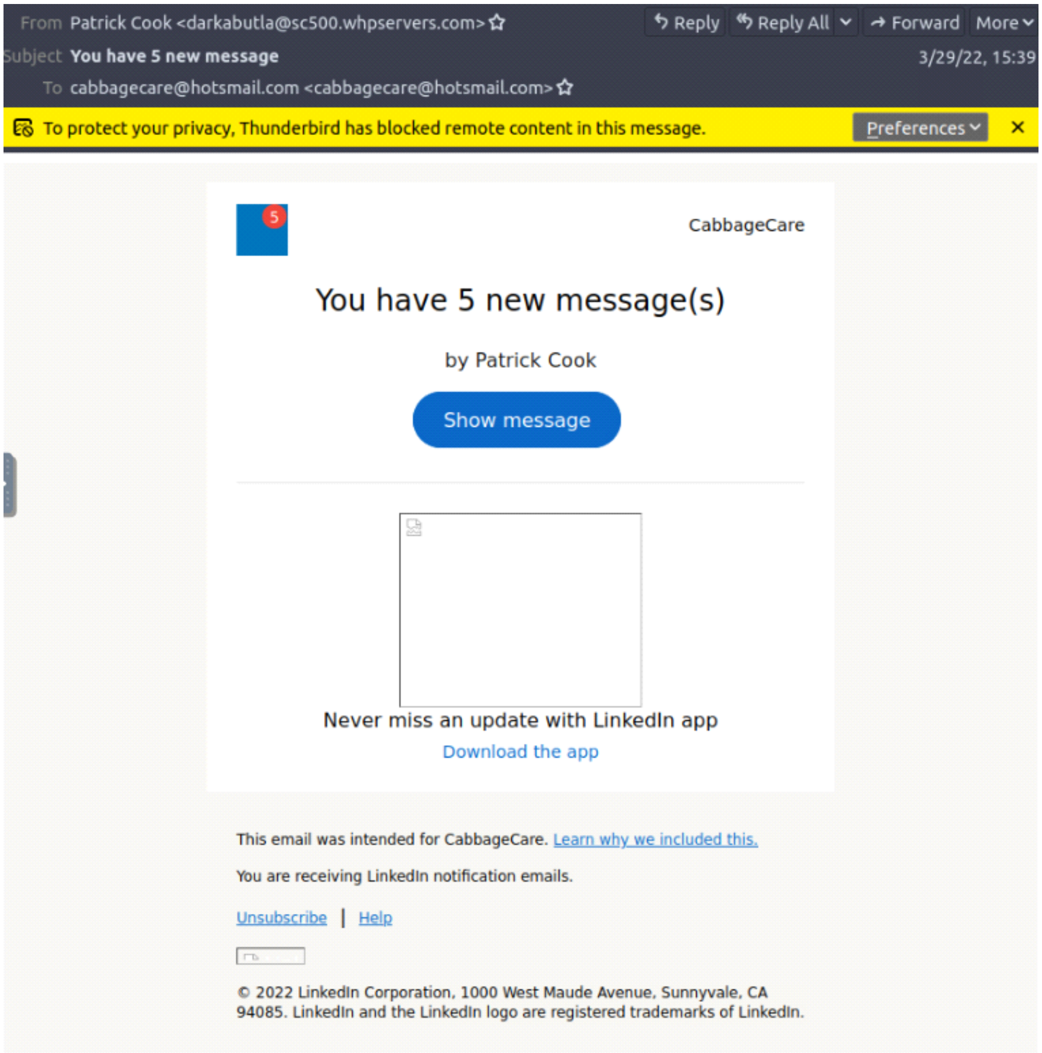
I am tasked to analyze 3 suspicious emails and reply to few questions :

Email 1



First I opened the file Using Thunderbird on My VM Machine





From Patrick Cook <darkabutla@sc500.whpservers.com>

Subject **You have 5 new message**

3/29/22, 15:39

To cabbagecare@hotmail.com <cabbagecare@hotmail.com>

To protect your privacy, Thunderbird has blocked remote content in this message.

CabbageCare

You have 5 new message(s)

by Patrick Cook

Show message

Never miss an update with LinkedIn app

Download the app

This email was intended for CabbageCare. Learn why we included this.

You are receiving LinkedIn notification emails.

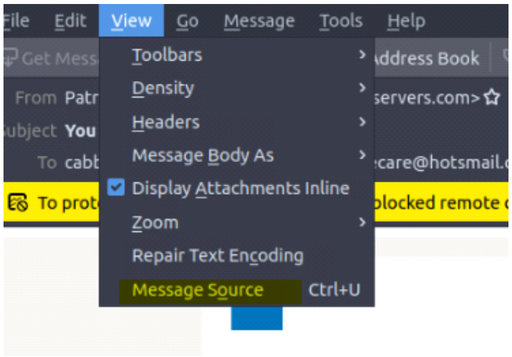
Unsubscribe | Help

© 2022 LinkedIn Corporation, 1000 West Maude Avenue, Sunnyvale, CA 94085. LinkedIn and the LinkedIn logo are registered trademarks of LinkedIn.

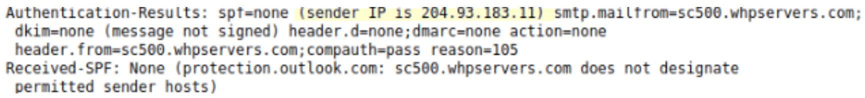
Question1:

What is the Originating IP address? Defang the IP address.

First open The Message Source:



And look for the Sender IP



```
Authentication-Results: spf=none (sender IP is 204.93.183.11) smtp.mailfrom=sc500.whpservers.com;
 dkim=none (message not signed) header.d=none;dmarc=none action=none
 header.from=sc500.whpservers.com;compauth=pass reason=105
Received-SPF: None (protection.outlook.com: sc500.whpservers.com does not designate
 permitted sender hosts)
```

Now Defang it: I prefer using a simple python script

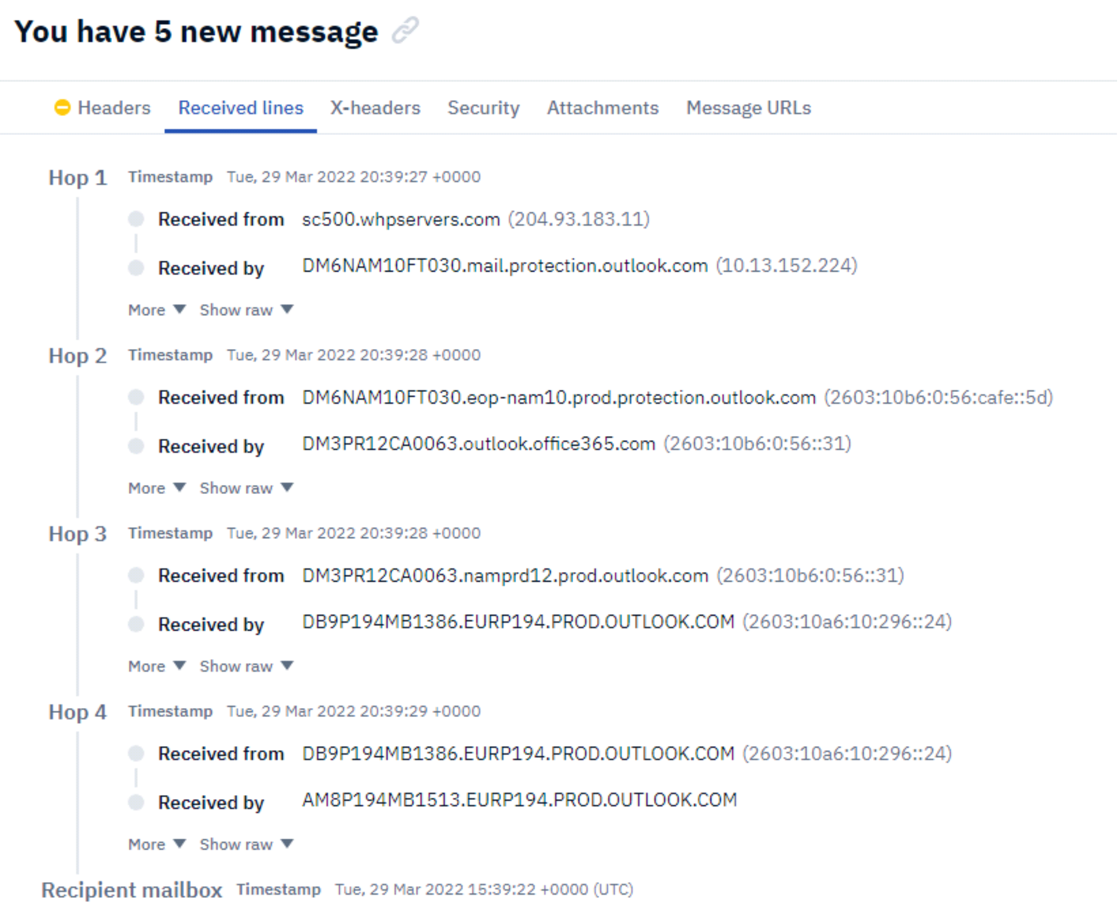
```
import re
def Defanged_IP(Str):
    x=re.sub("[.]","[.]",Str)
    print(x)
Str="1.1.1.2"
Defanged_IP(Str)
S = "204.93.183.11"
Defanged_IP(S)
```

So the answer is: **204[.]93[.]183[.]11**

Question2:

How many hops did the email go through to get to the recipient?

I used PhishTool



You have 5 new message

Hop 1 Timestamp Tue, 29 Mar 2022 20:39:27 +0000
Received from sc500.whpservers.com (204.93.183.11)
Received by DM6NAM10FT030.mail.protection.outlook.com (10.13.152.224)

Hop 2 Timestamp Tue, 29 Mar 2022 20:39:28 +0000
Received from DM6NAM10FT030.eop-nam10.prod.protection.outlook.com (2603:10b6:0:56:cafe::5d)
Received by DM3PR12CA0063.outlook.office365.com (2603:10b6:0:56::31)

Hop 3 Timestamp Tue, 29 Mar 2022 20:39:28 +0000
Received from DM3PR12CA0063.namprd12.prod.outlook.com (2603:10b6:0:56::31)
Received by DB9P194MB1386.EURP194.PROD.OUTLOOK.COM (2603:10a6:10:296::24)

Hop 4 Timestamp Tue, 29 Mar 2022 20:39:29 +0000
Received from DB9P194MB1386.EURP194.PROD.OUTLOOK.COM (2603:10a6:10:296::24)
Received by AM8P194MB1513.EURP194.PROD.OUTLOOK.COM

Recipient mailbox Timestamp Tue, 29 Mar 2022 15:39:22 +0000 (UTC)

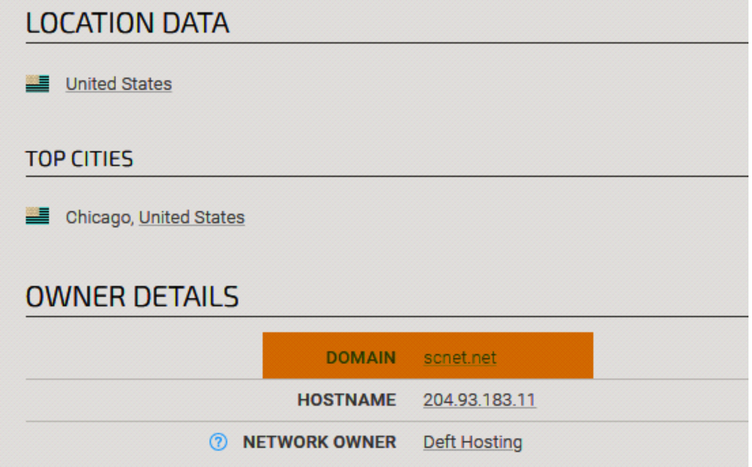
So the answer is: **4**

Ps: hop count is an important concept in networking and cybersecurity. It is used to analyze network topology, assess routing behavior, implement access controls, and monitor network performance. Understanding hop counts can help identify and address potential security risks and anomalies in a network.

Question3:

What is the listed domain of the Sender IP address?

The result Using **Talos Intelligence :**



LOCATION DATA

United States

TOP CITIES

Chicago, United States

OWNER DETAILS

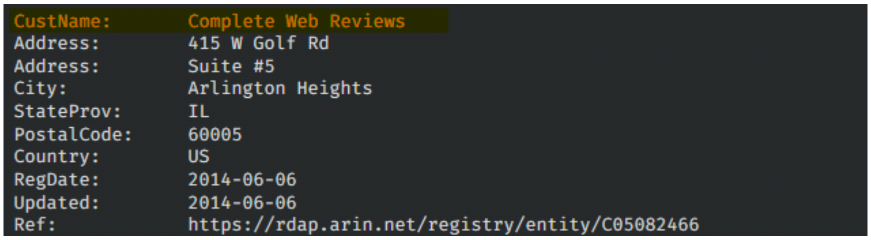
DOMAIN	scnet.net
HOSTNAME	204.93.183.11
NETWORK OWNER	Deft Hosting

So the domain name is**: scnet.net**

Question4:

What is the customer name of the IP address?

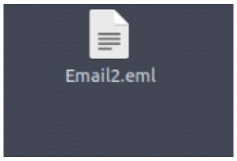
Using the same tool **Talos Intelligence :**



```
CustName:       Complete Web Reviews
Address:        415 W Golf Rd
Address:        Suite #5
City:           Arlington Heights
StateProv:      IL
PostalCode:     60005
Country:        US
RegDate:        2014-06-06
Updated:        2014-06-06
Ref:            https://rdap.arin.net/registry/entity/C05082466
```

So the name is**: Complete Web Reviews**

Email 2

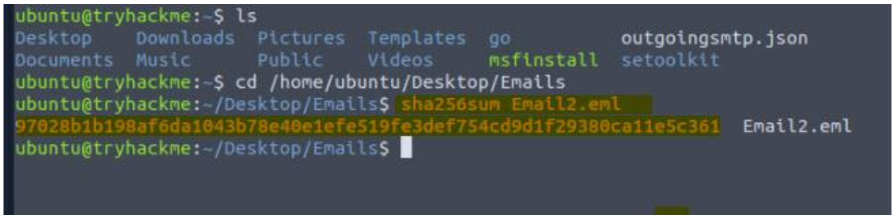


(The same previously used steps to open the File)

Question:

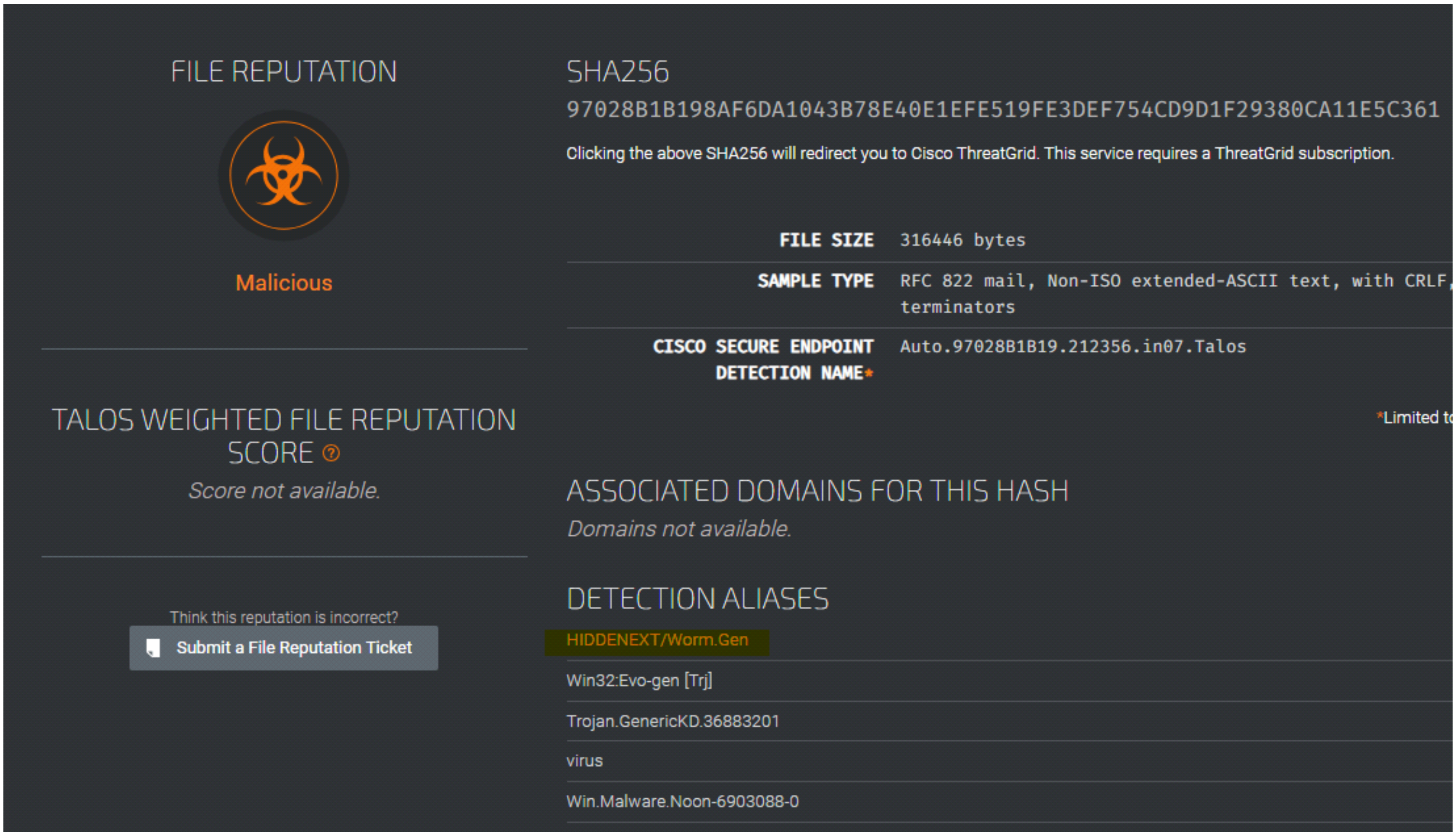
From Talos Intelligence, the attached file can also be identified by the Detection Alias that starts with an H…

First I need to generate the file hash



```
ubuntu@tryhackme:~$ ls
Desktop    Downloads  Pictures  Templates  go           outgoingsmtp.json
Documents  Music      Public    Videos     msfinstall  setoolkit
ubuntu@tryhackme:~$ cd /home/ubuntu/Desktop/Emails
ubuntu@tryhackme:~/Desktop/Emails$ sha256sum Email2.eml
97028b1b198af6da1043b78e40e1efe519fe3def754cd9d1f29380ca11e5c361  Email2.eml
ubuntu@tryhackme:~/Desktop/Emails$ 
```

Now I search for the file reputation in **Talos Intelligence**



FILE REPUTATION

Malicious

TALOS WEIGHTED FILE REPUTATION SCORE

Score not available.

Think this reputation is incorrect?

Submit a File Reputation Ticket

SHA256

97028B1B198AF6DA1043B78E40E1EFE519FE3DEF754CD9D1F29380CA11E5C361

Clicking the above SHA256 will redirect you to Cisco ThreatGrid. This service requires a ThreatGrid subscription.

FILE SIZE	316446 bytes
SAMPLE TYPE	RFC 822 mail, Non-ISO extended-ASCII text, with CRLF, terminators
CISCO SECURE ENDPOINT DETECTION NAME*	Auto.97028B1B19.212356.in07.Talos

*Limited to

ASSOCIATED DOMAINS FOR THIS HASH

Domains not available.

DETECTION ALIASES

HIDDENEXT/Worm.Gen

Win32:Evo-gen [Trj]

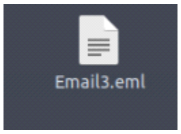
Trojan.GenericKD.36883201

virus

Win.Malware.Noon-6903088-0

So the answer is**:** **HIDDENEXT/Worm.Gen**

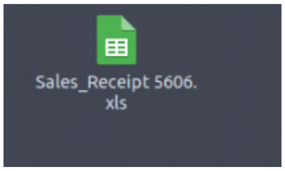
Email 3



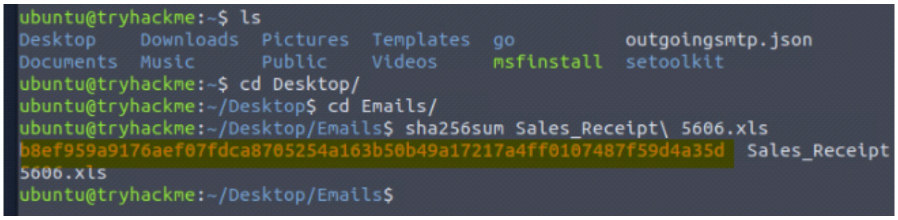
Question:

What malware family is associated with the attachment on Email3.eml?

First I saves the attachment

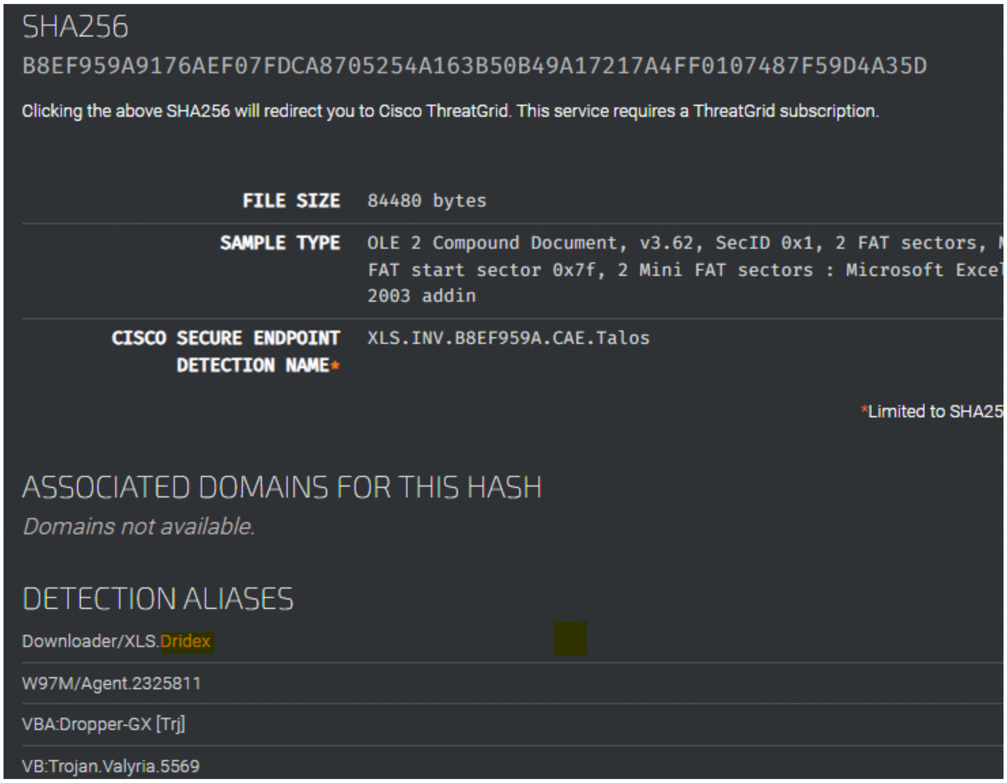


to generate the file hash



```
ubuntu@tryhackme:~$ ls
Desktop    Downloads  Pictures  Templates  go          outgoingsmtp.json
Documents  Music      Public    Videos     msfinstall  setoolkit
ubuntu@tryhackme:~$ cd Desktop/
ubuntu@tryhackme:~/Desktop$ cd Emails/
ubuntu@tryhackme:~/Desktop/Emails$ sha256sum Sales_Receipt\ 5606.xls
b8ef959a9176aef07fdca8705254a163b50b49a17217a4ff0107487f59d4a35d  Sales_Receipt
5606.xls
ubuntu@tryhackme:~/Desktop/Emails$
```

Now I search for the file reputation in **Talos Intelligence**



SHA256

B8EF959A9176AEF07FDCA8705254A163B50B49A17217A4FF0107487F59D4A35D

Clicking the above SHA256 will redirect you to Cisco ThreatGrid. This service requires a ThreatGrid subscription.

FILE SIZE	84480 bytes
SAMPLE TYPE	OLE 2 Compound Document, v3.62, SecID 0x1, 2 FAT sectors, M FAT start sector 0x7f, 2 Mini FAT sectors : Microsoft Excel 2003 addin
CISCO SECURE ENDPOINT DETECTION NAME*	XLS.INV.B8EF959A.CAE.Talos

*Limited to SHA25

ASSOCIATED DOMAINS FOR THIS HASH

Domains not available.

DETECTION ALIASES

Downloader/XLS.Dridex

W97M/Agent.2325811

VBA:Dropper-GX [Trj]

VB:Trojan.Valyria.5569

So the answer is**: Dridex**