LetsDefend

Official Incident Report

Event ID: 139

Rule Name: SOC189 - VBScript Suspicious Behavior Detected

Table of contents

Alert

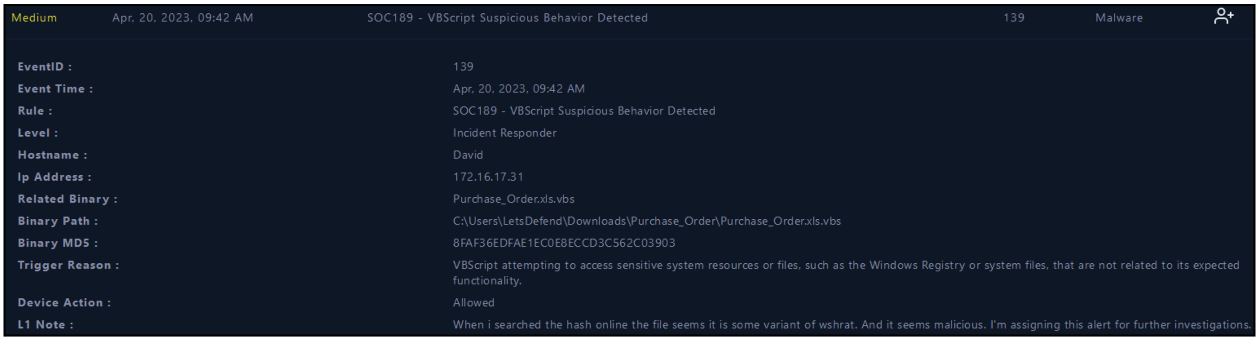
Based on the information that alert provided, it appears that there is some malicious VBScript executed on a system named "**David**" with an IP address of **172.16.17.31**. The Alert is triggered by a **SOC139 rule for VBScript Suspicious Behavior Detected**.

> *VBScript is used to give functionality and interaction to web pages. VBScript can be used for **client-side scripting**.*

The L1 analyst observed that the vbs file seems to be a part of WSHRAT family based on its behavior and has been flagged by multiple antivirus engines on Virustotal. The file path is identified as:
"**C:\Users\LetsDefend\Downloads\Purchase_Order\Purchase_Order.xls.vbs**"
The device action is marked as "allowed", indicating that no action was taken by the device to prevent or block the execution of the file.

> *WSHRAT, also known as "Windows Script Host Remote Administration Tool," is a type of malware that allows a hacker to remotely access to the victim's computer through the use of malicious VBscripts. WSHRAT is a variant of Houdini worm and has vbs and js variants.*

According to the trigger reason provided, the VBScript attempts to access sensitive system resources or files, such as the Windows Registry or system files, that are not related to its expected functionality.



Medium Apr, 20, 2023, 09:42 AM SOC189 - VBScript Suspicious Behavior Detected 139 Malware

EventID :	139
Event Time :	Apr, 20, 2023, 09:42 AM
Rule :	SOC189 - VBScript Suspicious Behavior Detected
Level :	Incident Responder
Hostname :	David
Ip Address :	172.16.17.31
Related Binary :	Purchase_Order.xls.vbs
Binary Path :	C:\Users\LetsDefend\Downloads\Purchase_Order\Purchase_Order.xls.vbs
Binary MD5 :	8FAF36EDFAE1EC0E8ECCD3C562C03903
Trigger Reason :	VBScript attempting to access sensitive system resources or files, such as the Windows Registry or system files, that are not related to its expected functionality.
Device Action :	Allowed
L1 Note :	When i searched the hash online the file seems it is some variant of wshrat. And it seems malicious. I'm assigning this alert for further investigations.

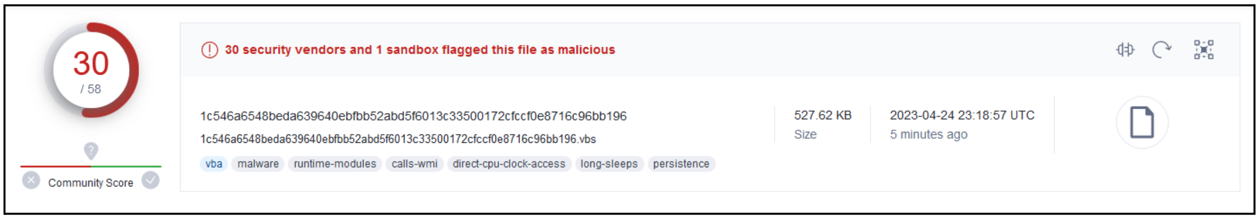
Overall, it appears that there may be malicious activity occurring on the system, and further investigation is needed to identify the extent of the activity and determine any necessary actions to remediate the situation.

Detection

Verify

As an incident responder, one of the first steps we take to verify the alert and determine whether it is a false positive or a true positive incident is to analyze the logs collected from the host by our security products.

The first step we can take to investigate the hash value of the suspicious file is to use online threat intelligence platforms such as VirusTotal, Hybrid Analysis, and MalwareBazaar.



30 / 58

Community Score

30 security vendors and 1 sandbox flagged this file as malicious

1c546a6548beda639640ebfbb52abd5f6013c33500172cfccf0e8716c96bb196
1c546a6548beda639640ebfbb52abd5f6013c33500172cfccf0e8716c96bb196.vbs

vba malware runtime-modules calls-wmi direct-cpu-clock-access long-sleeps persistence

527.62 KB
Size

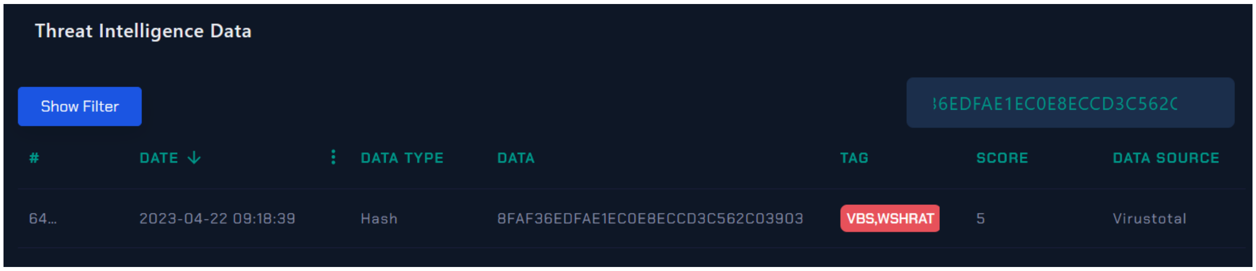
2023-04-24 23:18:57 UTC
5 minutes ago

Based on the information provided by VirusTotal, it appears that the suspicious file has been flagged as malicious by **30 out of 58** antivirus engines. The file has been labeled as "RAT - TROJAN, Malware, Persistence" which indicates that it is likely a type of malware that is designed to create persistence on the host machine.

Persistence refers to the ability of malware to maintain its presence on an infected system even after the system has been restarted or the malware process has been terminated.

VBS malware can achieve persistence by creating startup entries in the Windows registry, creating scheduled tasks, or modifying system files.

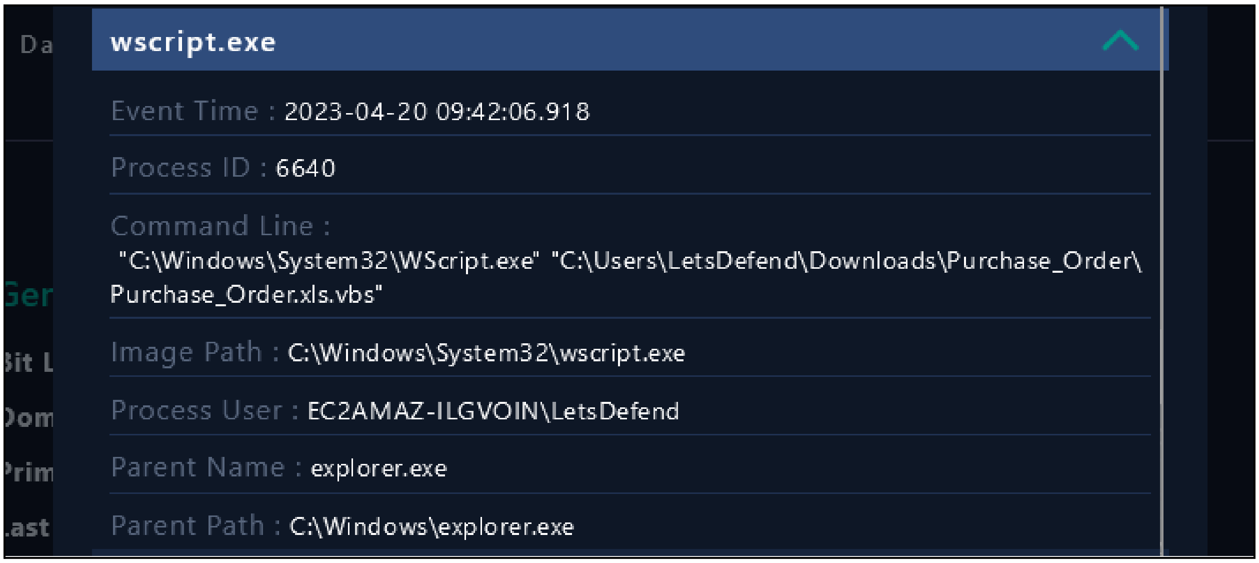
Also when we check the “Threat Intel” tab we see that the hash is flagged as malicious.



Threat Intelligence Data

#	DATE ↓	DATA TYPE	DATA	TAG	SCORE	DATA SOURCE
64...	2023-04-22 09:18:39	Hash	8FAF36EDFAE1EC0E8ECCD3C562C03903	VBS,WSHRAT	5	Virustotal

Now that we have determined that the file is malicious, the next step is to investigate whether the file has been executed on the host system. To do this, we can check the **Process List** from the **Endpoint Security** tab to see if the file has been run on the system by looking at running processes is a quick and straightforward method for identifying any active instances of the file.



wscript.exe

Event Time : 2023-04-20 09:42:06.918

Process ID : 6640

Command Line :
"C:\Windows\System32\WScript.exe" "C:\Users\LetsDefend\Downloads\Purchase_Order\Purchase_Order.xls.vbs"

Image Path : C:\Windows\System32\wscript.exe

Process User : EC2AMAZ-ILGVOIN\LetsDefend

Parent Name : explorer.exe

Parent Path : C:\Windows\explorer.exe

As seen above, the file has been run on the system.

It appears that the Windows Script Host (Wscript.exe) was used to execute a Visual Basic Script file called "Purchase_Order.xls.vbs". The command line used to execute the script indicates that the script file is located in the "**C:\Users\LetsDefend\Downloads\Purchase_Order**" directory.

The parent process of Wscript.exe was explorer.exe, which is the default Windows shell. This means the process was executed by a user called "LetsDefend" on the machine.

WScript is a Windows Script Host (WSH) engine that allows you to execute scripts written in various scripting languages on Windows operating systems.

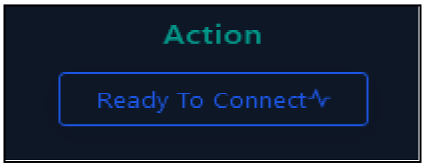
Based on our analysis, we have confirmed that the alert is a **true positive (TP)**, and the labeled "**RAT-TROJAN**" malware has **executed** on the system. This incident warrants further investigation and an appropriate response.

Analysis

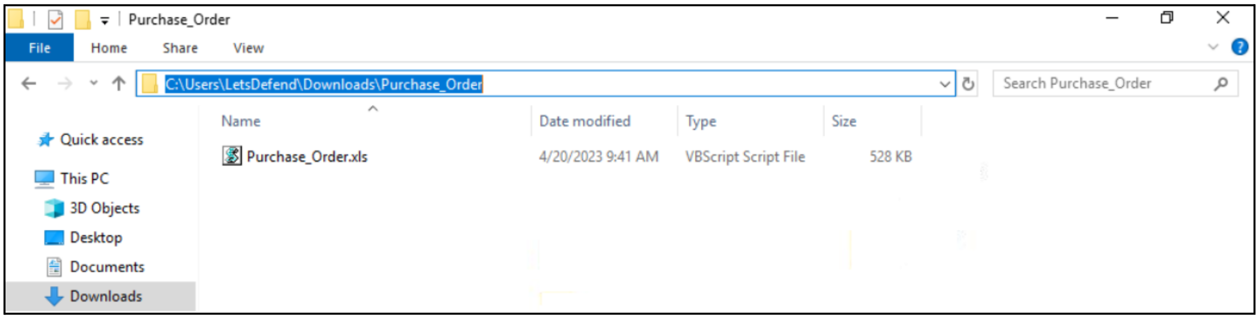
Initial Access

The presence of malicious files on the computer should make us think about initial access. It is crucial to investigate the initial access point of the attacker in order to determine how they were able to gain unauthorized access to the system.

We can proceed with connecting to the host machine for further analysis. This can easily be done from the Endpoint Security tab by searching for the hostname or IP address and clicking the "Connect" button.



We have identified that the suspicious file is located in the downloads folder in alert details. When we checked the related path, we found that the file still exists.

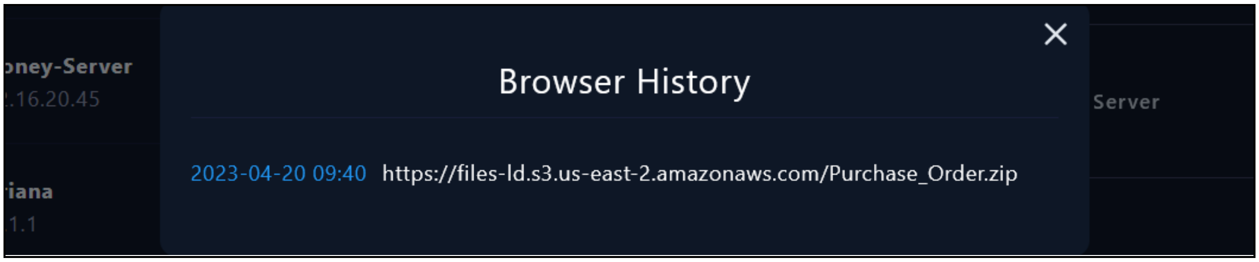


C:\Users\LetsDefend\Downloads\Purchase_Order

Name	Date modified	Type	Size
Purchase_Order.xls	4/20/2023 9:41 AM	VBScript Script File	528 KB

To begin our investigation, we will review the logs under the Endpoint security tab and cross-reference them with the information we gathered from the alert page.

On the "**Browser History"** its seen that the **Purchase_Order.zip** was downloaded from the address **hxxps[:]//files-ld.s3.us-east-2.amazonaws[.]com/Purchase_Order.zip** on **2023-04-20 09:40**

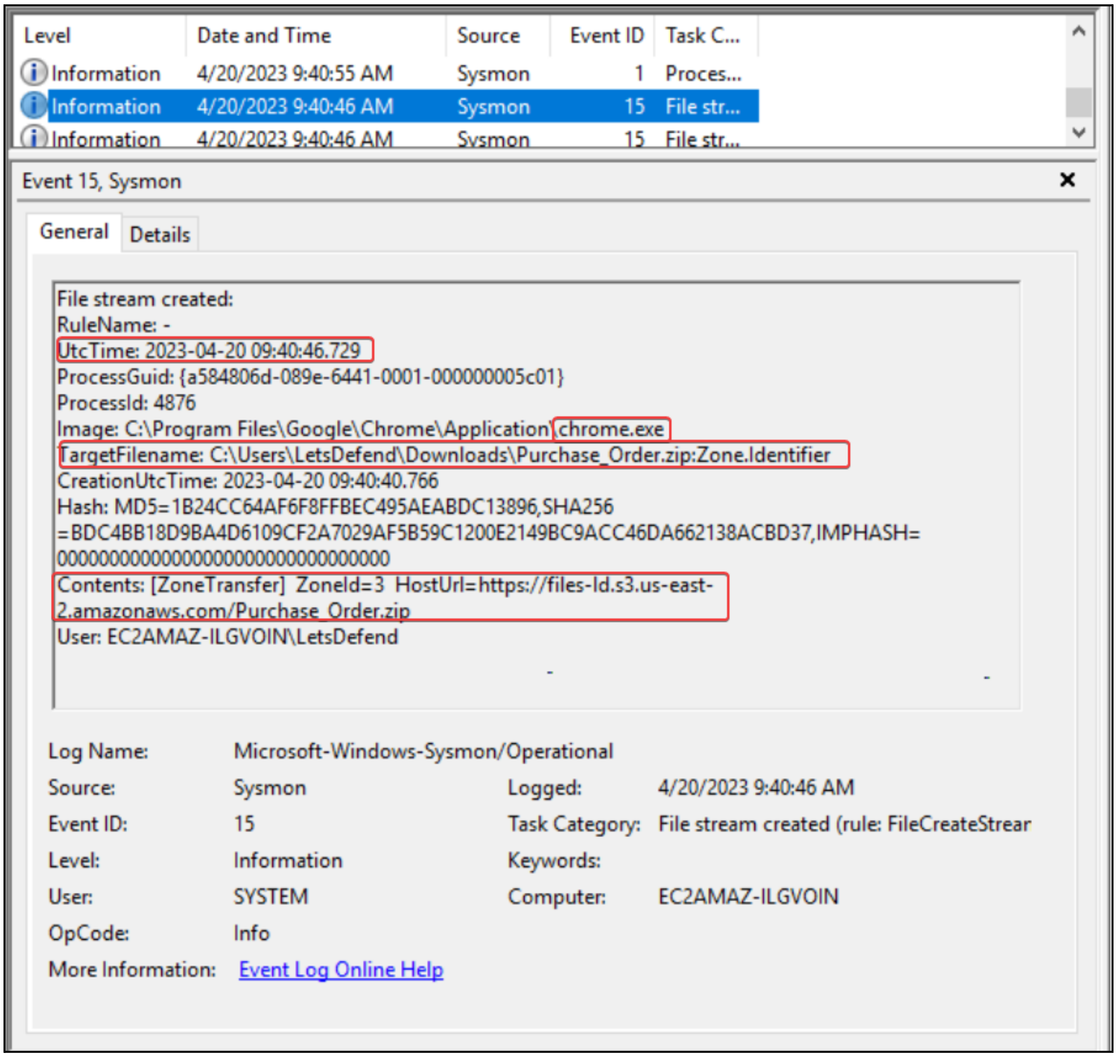


Browser History

2023-04-20 09:40 https://files-ld.s3.us-east-2.amazonaws.com/Purchase_Order.zip

We can simply verify this by connecting to the host machine and analyzing the Sysmon Event ID: 15 logs.

> When a file is downloaded from the internet it is saved to the local system. File streams are recorded by **Event ID: 15** on sysmon logs.



Level	Date and Time	Source	Event ID	Task C...
Information	4/20/2023 9:40:55 AM	Sysmon	1	Proces...
Information	4/20/2023 9:40:46 AM	Sysmon	15	File str...
Information	4/20/2023 9:40:46 AM	Sysmon	15	File str...

Event 15, Sysmon

```
File stream created:
RuleName: -
UtcTime: 2023-04-20 09:40:46.729
ProcessGuid: {a584806d-089e-6441-0001-000000005c01}
ProcessId: 4876
Image: C:\Program Files\Google\Chrome\Application\chrome.exe
TargetFilename: C:\Users\LetsDefend\Downloads\Purchase_Order.zip:Zone.Identifier
CreationUtcTime: 2023-04-20 09:40:40.766
Hash: MD5=1B24CC64AF6F8FFBEC495AEABDC13896,SHA256
=BDC4BB18D9BA4D6109CF2A7029AF5B59C1200E2149BC9ACC46DA662138ACBD37,IMPHASH=
00000000000000000000000000000000
Contents: [ZoneTransfer]  ZoneId=3  HostUrl=https://files-ld.s3.us-east-
2.amazonaws.com/Purchase_Order.zip
User: EC2AMAZ-ILGVOIN\LetsDefend
```

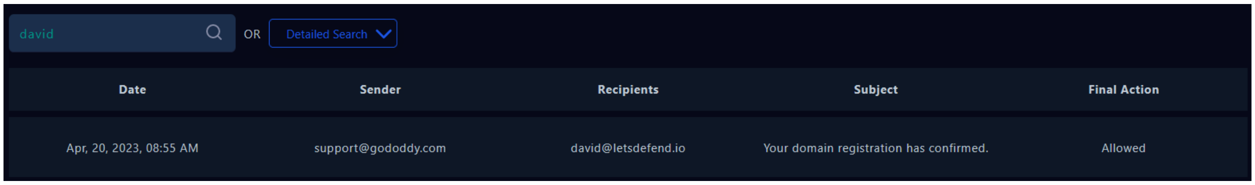
Log Name:	Microsoft-Windows-Sysmon/Operational		
Source:	Sysmon	Logged:	4/20/2023 9:40:46 AM
Event ID:	15	Task Category:	File stream created (rule: FileCreateStrear
Level:	Information	Keywords:	
User:	SYSTEM	Computer:	EC2AMAZ-ILGVOIN
OpCode:	Info		
More Information:	Event Log Online Help		

Our investigation has revealed that the **Purchase_Order.zip** file, which contains the malicious **Purchase_Order.xls.vbs** file, was downloaded from the **Chrome browser** to the compromised system.

This suggests that the initial infection vector was likely a malicious website or a phishing email that tricked the user into downloading and running the file.

As part of our investigation, we will review the Email Security tab on LetsDefend to check if any phishing emails were sent to the user.

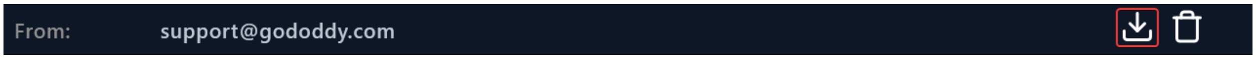
On the email security tab we can simply filter the username to see what emails that **David** received or sent. We see that **David** received an email from **support@gododdy.com** with the subject of “**Your domain registration has confirmed**”.



Date	Sender	Recipients	Subject	Final Action
Apr, 20, 2023, 08:55 AM	support@gododdy.com	david@letsdefend.io	Your domain registration has confirmed.	Allowed

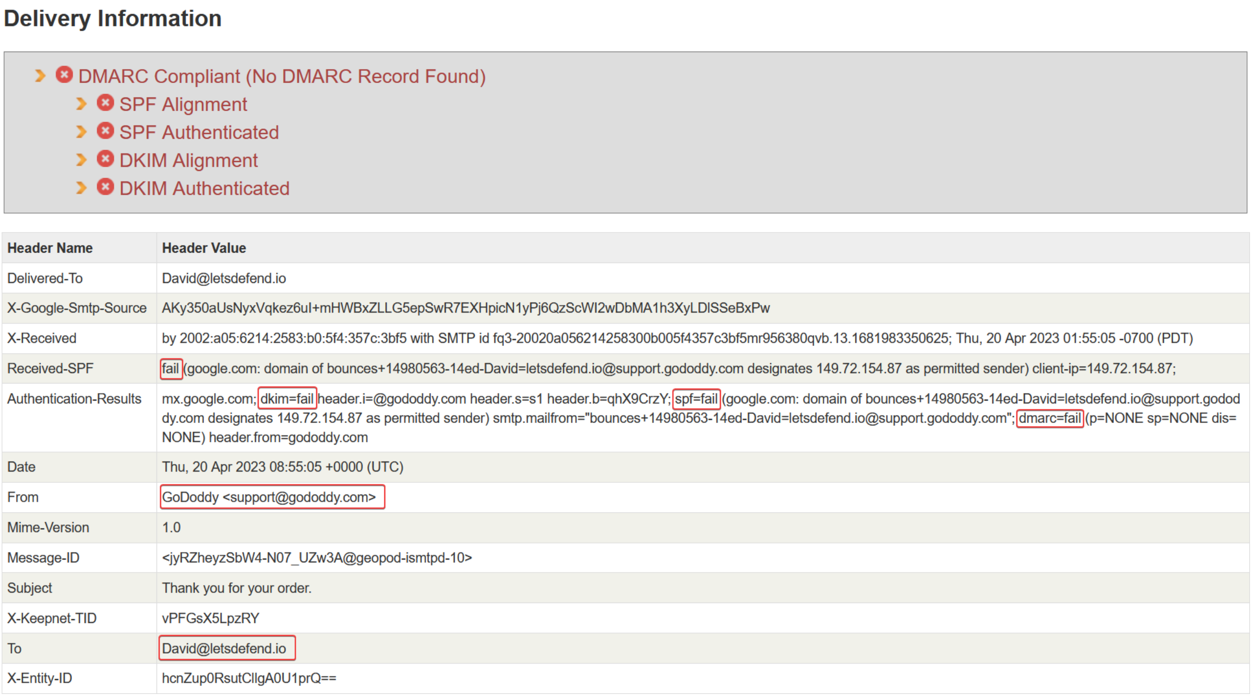
This is highly suspicious as the sender is attempting to imitate a legitimate domain (godaddy.com) in order to trick the user into opening the email and clicking on any links or attachments contained within it.

To determine whether this email is a phishing email or not, we can download it in EML format and carefully analyze its content and headers.



From: support@gododdy.com

To do header analysis, we can use tools such as mxtoolbox email header analyzer. https://mxtoolbox.com/EmailHeaders.aspx

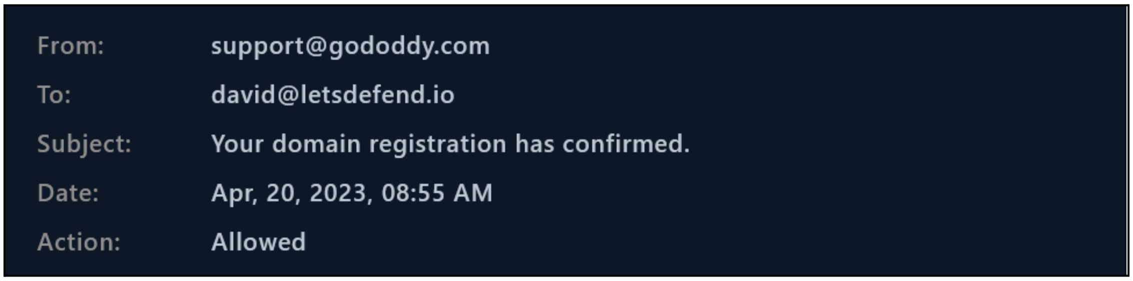


Delivery Information

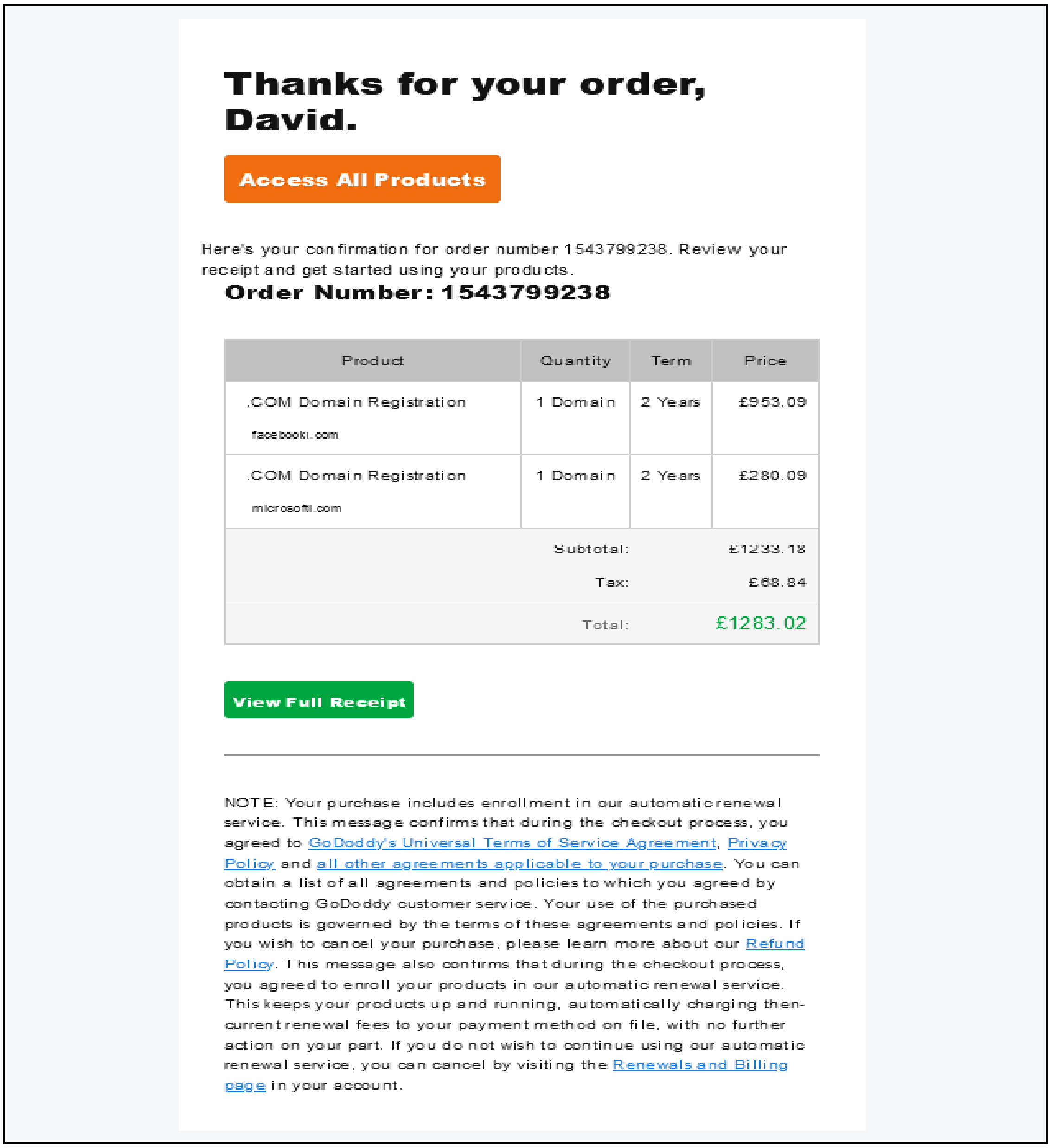
- DMARC Compliant (No DMARC Record Found)
  - SPF Alignment
  - SPF Authenticated
  - DKIM Alignment
  - DKIM Authenticated

Header Name	Header Value
Delivered-To	David@letsdefend.io
X-Google-Smtp-Source	AKy350aUsNyxVqkez6ul+mHWBxZLLG5epSwR7EXHpicN1yPj6QzScWI2wDbMA1h3XyLDlSSeBxPw
X-Received	by 2002:a05:6214:2583:b0:5f4:357c:3bf5 with SMTP id fq3-20020a056214258300b005f4357c3bf5mr956380qvb.13.1681983350625; Thu, 20 Apr 2023 01:55:05 -0700 (PDT)
Received-SPF	fail (google.com: domain of bounces+14980563-14ed-David=letsdefend.io@support.gododdy.com designates 149.72.154.87 as permitted sender) client-ip=149.72.154.87;
Authentication-Results	mx.google.com; dkim=fail header.i=@gododdy.com header.s=s1 header.b=qhX9CrzY; spf=fail (google.com: domain of bounces+14980563-14ed-David=letsdefend.io@support.gododdy.com designates 149.72.154.87 as permitted sender) smtp.mailfrom="bounces+14980563-14ed-David=letsdefend.io@support.gododdy.com"; dmarc=fail (p=NONE sp=NONE dis=NONE) header.from=gododdy.com
Date	Thu, 20 Apr 2023 08:55:05 +0000 (UTC)
From	GoDoddy <support@gododdy.com>
Mime-Version	1.0
Message-ID	<jyRZheyzSbW4-N07_UZw3A@geopod-ismtpd-10>
Subject	Thank you for your order.
X-Keepnet-TID	vPFGsX5LpzRY
To	David@letsdefend.io
X-Entity-ID	hcnZup0RsutCllgA0U1prQ==

The email that David received from **support@gododdy.com** with the subject "Your domain registration has confirmed" contained the following message:



From:	support@gododdy.com
To:	david@letsdefend.io
Subject:	Your domain registration has confirmed.
Date:	Apr, 20, 2023, 08:55 AM
Action:	Allowed



Thanks for your order, David.

Here's your confirmation for order number 1543799238. Review your receipt and get started using your products.

Order Number: 1543799238

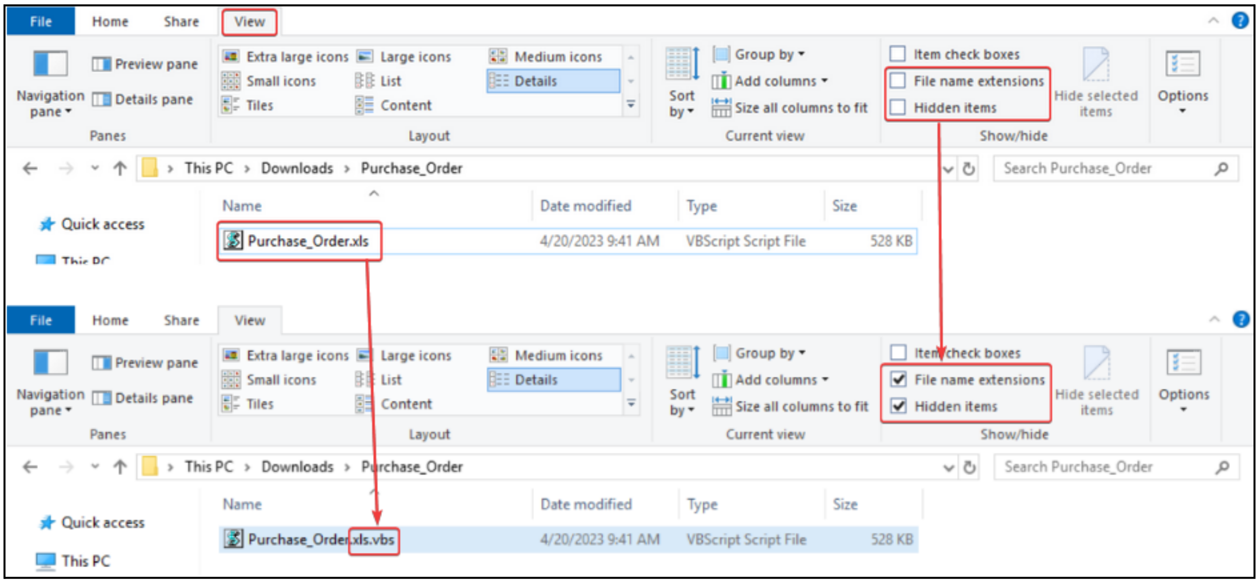
Product	Quantity	Term	Price
.COM Domain Registration facebooki.com	1 Domain	2 Years	£953.09
.COM Domain Registration microsoftl.com	1 Domain	2 Years	£280.09
	Subtotal:		£1233.18
	Tax:		£68.84
	Total:		£1283.02

NOTE: Your purchase includes enrollment in our automatic renewal service. This message confirms that during the checkout process, you agreed to GoDoddy's Universal Terms of Service Agreement, Privacy Policy and all other agreements applicable to your purchase. You can obtain a list of all agreements and policies to which you agreed by contacting GoDoddy customer service. Your use of the purchased products is governed by the terms of these agreements and policies. If you wish to cancel your purchase, please learn more about our Refund Policy. This message also confirms that during the checkout process, you agreed to enroll your products in our automatic renewal service. This keeps your products up and running, automatically charging then-current renewal fees to your payment method on file, with no further action on your part. If you do not wish to continue using our automatic renewal service, you can cancel by visiting the Renewals and Billing page in your account.

This message is a classic example of a **phishing email** that tries to trick the user into clicking on a malicious link or downloading a malware-infected attachment.

The phishing email containing the attachment "**Purchase_Order.zip**" was designed to trick the user into executing the malicious file "**Purchase_Order.xls.vbs**," which in turn led to the execution of a malware on the host machine.

Enabling "**file name extensions**" is a crucial step for forensic investigators, as it allows for better identification and analysis of file types, which can help uncover potential security breaches and malicious activities on a system.



□ Item check boxes
□ File name extensions
□ Hidden items

Name	Date modified	Type	Size
Purchase_Order.xls	4/20/2023 9:41 AM	VBScript Script File	528 KB

□ Item check boxes
☑ File name extensions
☑ Hidden items

Name	Date modified	Type	Size
Purchase_Order.xls.vbs	4/20/2023 9:41 AM	VBScript Script File	528 KB

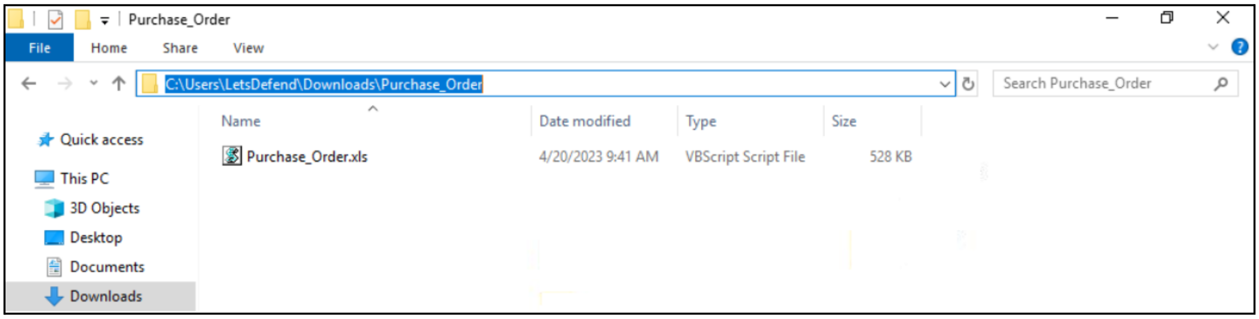
As observed, the apparent **XLS** file was actually a **VBS** file disguised with a double extension, indicating that the attacker used a common **masquerading** technique to conceal the true nature of the file from the user. This highlights the importance of educating users on how to identify suspicious file types and avoid falling victim to similar attacks in the future.

Upon further investigation, it is discovered that the initial compromise was achieved through a successful **phishing attack**, which enabled the attackers to gain access to the host machine.

PHISHING T1566

Persistence

Once an attacker gains initial access, they may try to establish persistence to ensure continued access to the system or network, even if their initial access is discovered and removed.



C:\Users\LetsDefend\Downloads\Purchase_Order

Name	Date modified	Type	Size
Purchase_Order.xls	4/20/2023 9:41 AM	VBScript Script File	528 KB

Once we have confirmed the presence of the malware, our next step should be to investigate any potential **persistence** by the attacker.
In terms of malware persistence, attackers may use a variety of techniques to maintain access to a compromised system, such as **adding a new service** or **scheduled task**, **modifying startup folders**, or **installing a rootkit**.
Here are some registry common autorun registry keys for persistence.

Common Autorun Registry Keys

- **Active Setup**
HKLM\Software\Microsoft\Active Setup\Installed Components\%APPGUID%

- **AppInit_DLLs**
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Windows\AppInit_DLLs

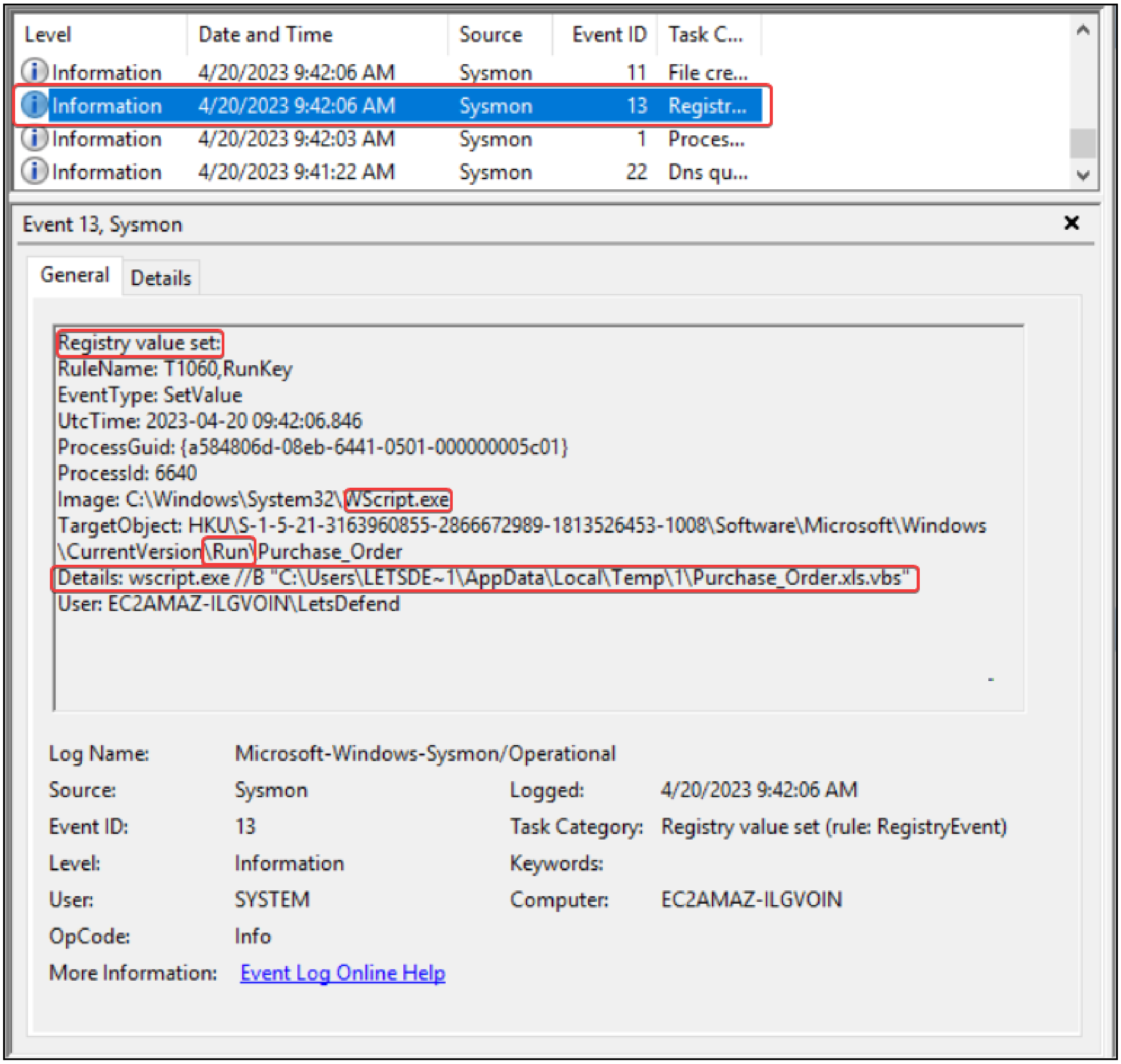
- **Run Keys**
HKLM\Software\Microsoft\Windows\CurrentVersion\Run, RunOnce

- **Services and ServiceDLLs**
HKLM\System\ControlSet###\Services\<Servicename>,<ImagePath>
HKLM\System\ControlSet###\Services\<Servicename>\Parameters,<servicedll>

- **Shell Extensions**
HKLM\Software\Microsoft\Windows\CurrentVersion\Shell Extensions

- **UserInit**
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\UserInit

To do this we can start by analyzing the tracks of malware on sysmon logs.
Analyzing sysmon logs can be an effective way to identify indicators of compromise (IoCs) related to malware persistence.



```
Level          Date and Time          Source    Event ID  Task C...
Information    4/20/2023 9:42:06 AM   Sysmon          11  File cre...
Information    4/20/2023 9:42:06 AM   Sysmon          13  Registr...
Information    4/20/2023 9:42:03 AM   Sysmon           1  Proces...
Information    4/20/2023 9:41:22 AM   Sysmon          22  Dns qu...
```

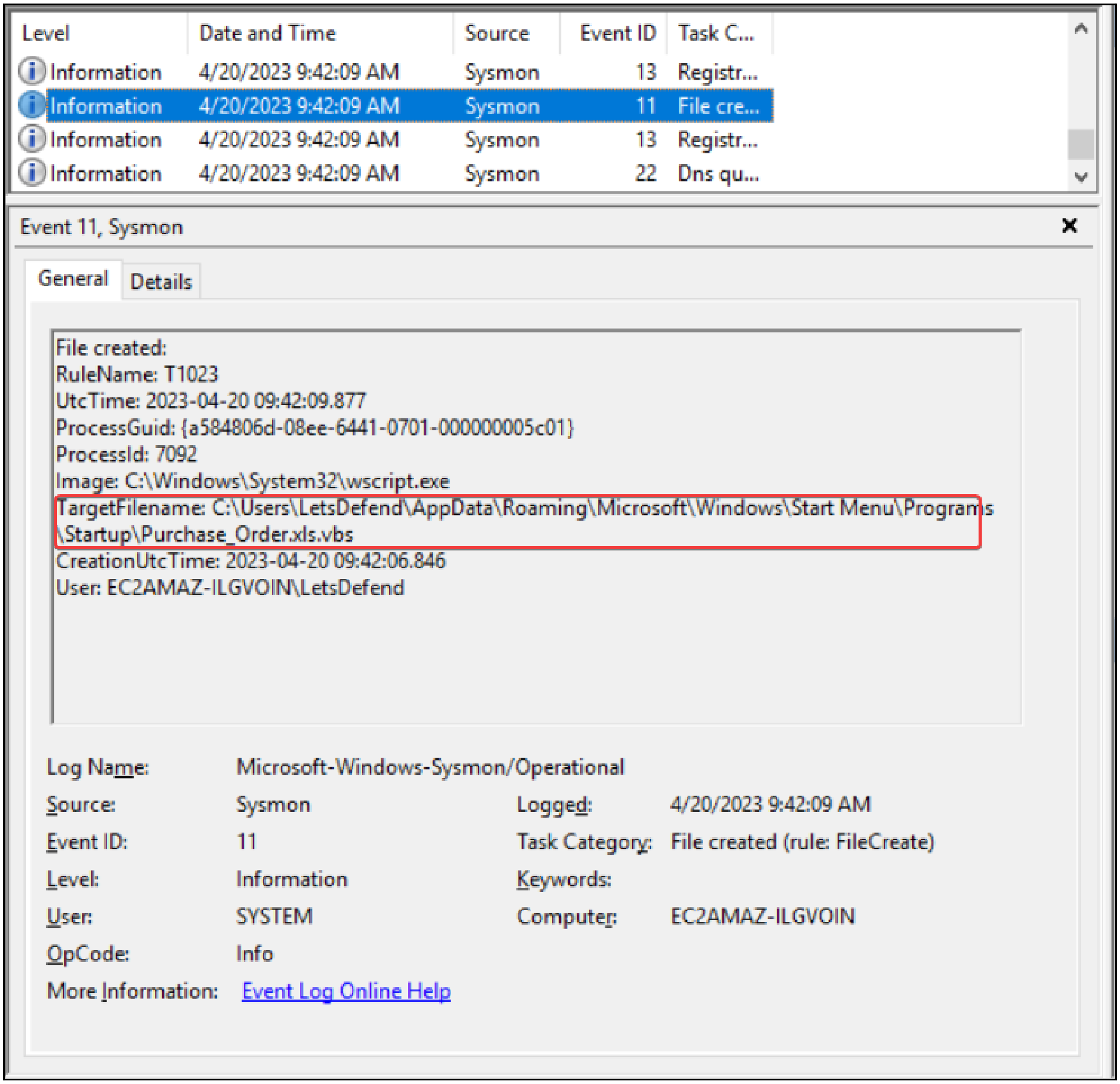
Event 13, Sysmon

```
Registry value set:
RuleName: T1060,RunKey
EventType: SetValue
UtcTime: 2023-04-20 09:42:06.846
ProcessGuid: {a584806d-08eb-6441-0501-000000005c01}
ProcessId: 6640
Image: C:\Windows\System32\WScript.exe
TargetObject: HKU\S-1-5-21-3163960855-2866672989-1813526453-1008\Software\Microsoft\Windows
\CurrentVersion\Run\Purchase_Order
Details: wscript.exe //B "C:\Users\LETSDE~1\AppData\Local\Temp\1\Purchase_Order.xls.vbs"
User: EC2AMAZ-ILGVOIN\LetsDefend
```

Log Name:	Microsoft-Windows-Sysmon/Operational		
Source:	Sysmon	Logged:	4/20/2023 9:42:06 AM
Event ID:	13	Task Category:	Registry value set (rule: RegistryEvent)
Level:	Information	Keywords:	
User:	SYSTEM	Computer:	EC2AMAZ-ILGVOIN
OpCode:	Info		
More Information:	Event Log Online Help		

In this sysmon log it is seen that the malware achieves persistence by adding itself to "**HKU\S-1-5-21-3163960855-2866672989-1813526453-1008\Software\Microsoft\Windows\CurrentVersion\Run\Purchase_Order.xls.vbs**" registry the Run key.

Further analysis shows that the malware also adds itself to the startup too. **C:\Users\LetsDefend\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Purchase_Order.xls.vbs**



Level	Date and Time	Source	Event ID	Task C...
Information	4/20/2023 9:42:09 AM	Sysmon	13	Registr...
Information	4/20/2023 9:42:09 AM	Sysmon	11	File cre...
Information	4/20/2023 9:42:09 AM	Sysmon	13	Registr...
Information	4/20/2023 9:42:09 AM	Sysmon	22	Dns qu...

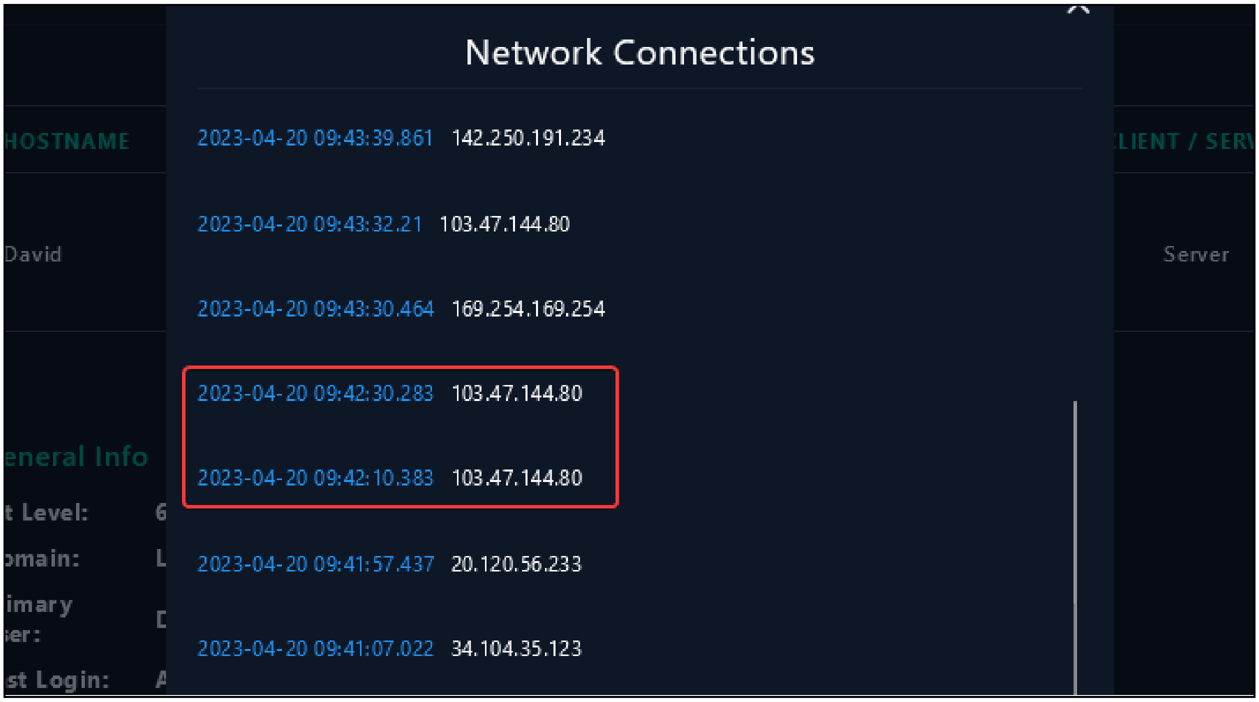
Event 11, Sysmon

```
File created:
RuleName: T1023
UtcTime: 2023-04-20 09:42:09.877
ProcessGuid: {a584806d-08ee-6441-0701-000000005c01}
ProcessId: 7092
Image: C:\Windows\System32\wscript.exe
TargetFilename: C:\Users\LetsDefend\AppData\Roaming\Microsoft\Windows\Start Menu\Programs
\Startup\Purchase_Order.xls.vbs
CreationUtcTime: 2023-04-20 09:42:06.846
User: EC2AMAZ-ILGVOIN\LetsDefend
```

Log Name:	Microsoft-Windows-Sysmon/Operational		
Source:	Sysmon	Logged:	4/20/2023 9:42:09 AM
Event ID:	11	Task Category:	File created (rule: FileCreate)
Level:	Information	Keywords:	
User:	SYSTEM	Computer:	EC2AMAZ-ILGVOIN
OpCode:	Info		
More Information:	Event Log Online Help		

Placing a program within a startup folder will also cause that program to execute when a user logs in. There is a startup folder location for individual user accounts as well as a system-wide startup folder that will be checked regardless of which user account logs in.

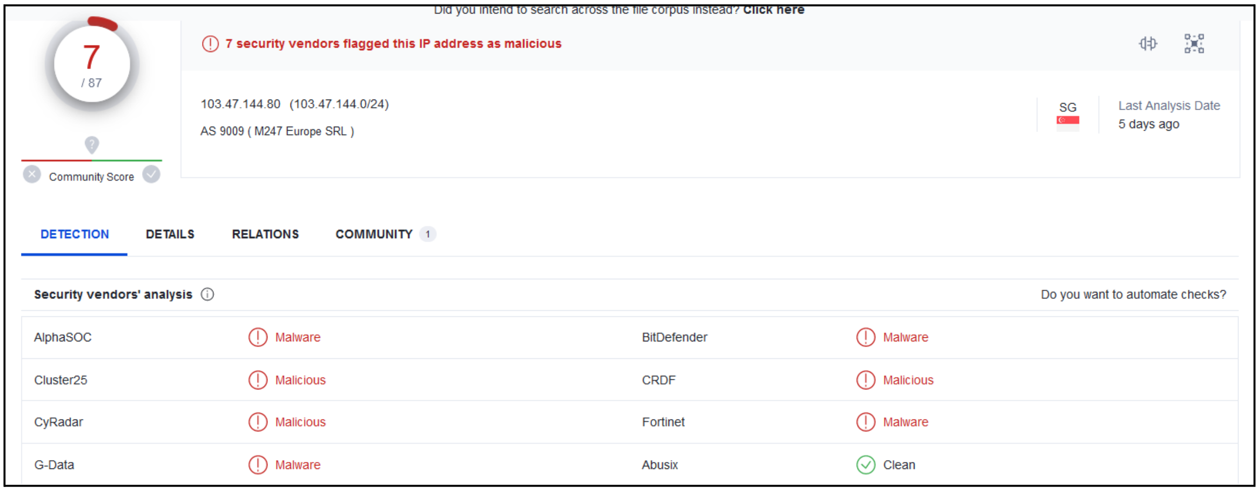
Furthermore, we should review the host's **Network Connections** on Endpoint Security tab to identify any communication with external servers.



Network Connections

```
2023-04-20 09:43:39.861   142.250.191.234
2023-04-20 09:43:32.21   103.47.144.80
2023-04-20 09:43:30.464   169.254.169.254
2023-04-20 09:42:30.283   103.47.144.80
2023-04-20 09:42:10.383   103.47.144.80
2023-04-20 09:41:57.437   20.120.56.233
2023-04-20 09:41:07.022   34.104.35.123
```

It is seen some suspicious outbound connections have been made from the infected host machine. These connections were made to external IP addresses and domains that are known to be associated with malware.



Did you intend to search across the file corpus instead? **Click here**

7 security vendors flagged this IP address as malicious

103.47.144.80 (103.47.144.0/24)
AS 9009 (M247 Europe SRL)

SG

Last Analysis Date
5 days ago

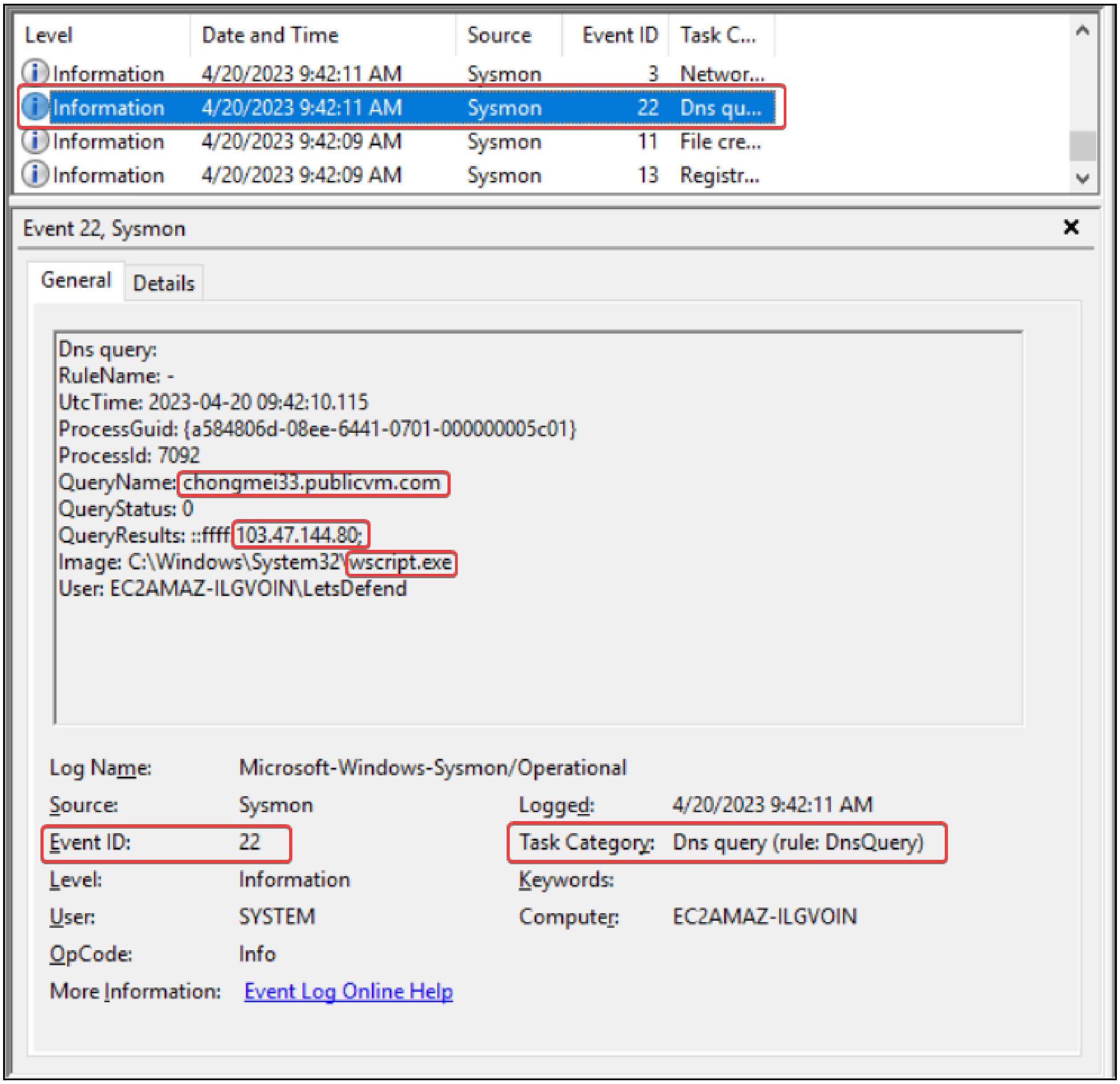
Security vendors' analysis

Do you want to automate checks?

AlphaSOC	Malware	BitDefender	Malware
Cluster25	Malicious	CRDF	Malicious
CyRadar	Malicious	Fortinet	Malware
G-Data	Malware	Abusix	✓ Clean

And flagged as malicious on virustotal.

It can also be seen in the sysmon logs that the malware makes requests to the **chongmei33[.]publicvm[.]com** which resolves to related malicious ip address **103[.]47[.]144[.]80**



Level	Date and Time	Source	Event ID	Task C...
Information	4/20/2023 9:42:11 AM	Sysmon	3	Networ...
Information	4/20/2023 9:42:11 AM	Sysmon	22	Dns qu...
Information	4/20/2023 9:42:09 AM	Sysmon	11	File cre...
Information	4/20/2023 9:42:09 AM	Sysmon	13	Registr...

Event 22, Sysmon

```
Dns query:
RuleName: -
UtcTime: 2023-04-20 09:42:10.115
ProcessGuid: {a584806d-08ee-6441-0701-000000005c01}
ProcessId: 7092
QueryName: chongmei33.publicvm.com
QueryStatus: 0
QueryResults: ::ffff:103.47.144.80;
Image: C:\Windows\System32\wscript.exe
User: EC2AMAZ-ILGVOIN\LetsDefend
```

Log Name:	Microsoft-Windows-Sysmon/Operational		
Source:	Sysmon	Logged:	4/20/2023 9:42:11 AM
Event ID:	22	Task Category:	Dns query (rule: DnsQuery)
Level:	Information	Keywords:	
User:	SYSTEM	Computer:	EC2AMAZ-ILGVOIN
OpCode:	Info		
More Information:	Event Log Online Help		

Based on our analysis, we have identified that the malware used **Boot or Logon Autostart Execution** technique to remain persistent on the host machine.

T1547 Boot or Logon Autostart Execution

Privilege Escalation

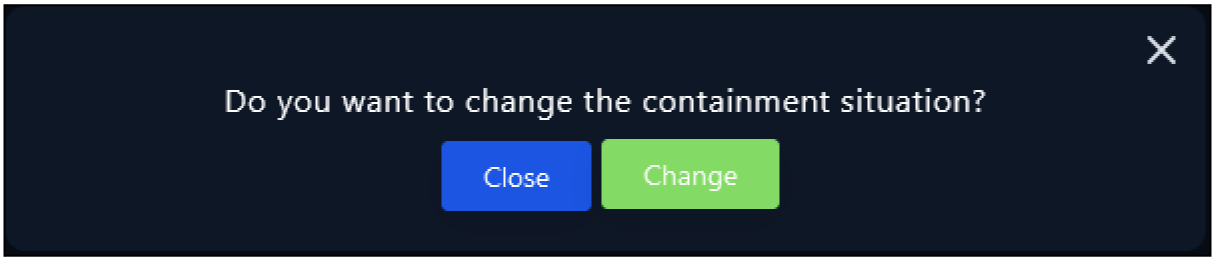
We reviewed system logs, analyzed running processes, and checked for any suspicious system changes, but did not find any evidence of attempts to gain elevated access or escalate privileges.
Based on the analysis there were no privilege escalation indicators.

Credential Access

Based on investigations of logs there weren't any Credential Access methods used by the attacker.

Containment

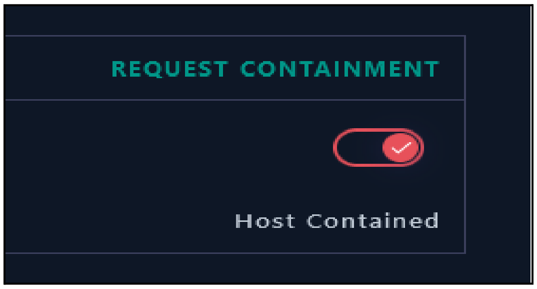
Based on the information gathered during the investigation, it is highly likely that the system has been compromised. To prevent further data loss or unauthorized access, it is recommended to isolate the system from the network immediately.



Do you want to change the containment situation?

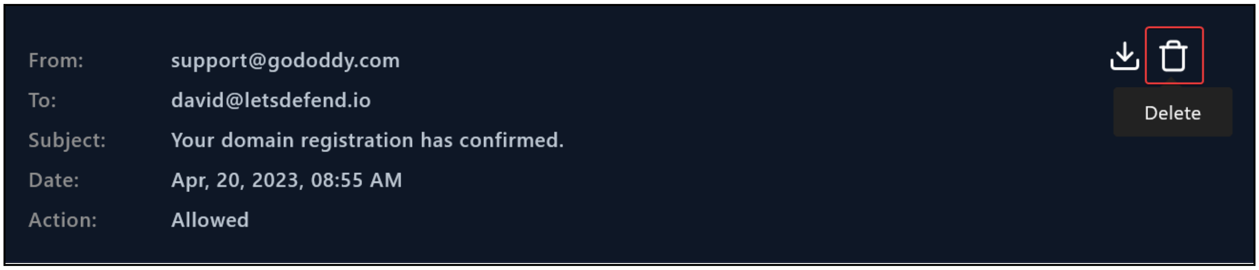
Isolation of the host can be made from the endpoint security tab.

Hostname	David
IP Address	172.16.17.31



Additionally, we should delete the phishing email from the user's mailbox to prevent any accidental or intentional re-execution of the malware. The user should also be educated on how to identify and avoid phishing emails in the future to minimize the risk of similar incidents occurring.

Deletion of mail can be made from the Email Security tab.



From:	support@gododdy.com
To:	david@letsdefend.io
Subject:	Your domain registration has confirmed.
Date:	Apr, 20, 2023, 08:55 AM
Action:	Allowed

Lesson Learned

- Educate users on identifying files with double file extensions to prevent malicious files from being delivered to target systems.

- Report phishing emails to the IT/security team immediately upon identification to prevent further damage.

- Educate users on common characteristics of phishing emails, such as urgent language and suspicious links or attachments, to help them better identify and report such emails.

Remediation Actions

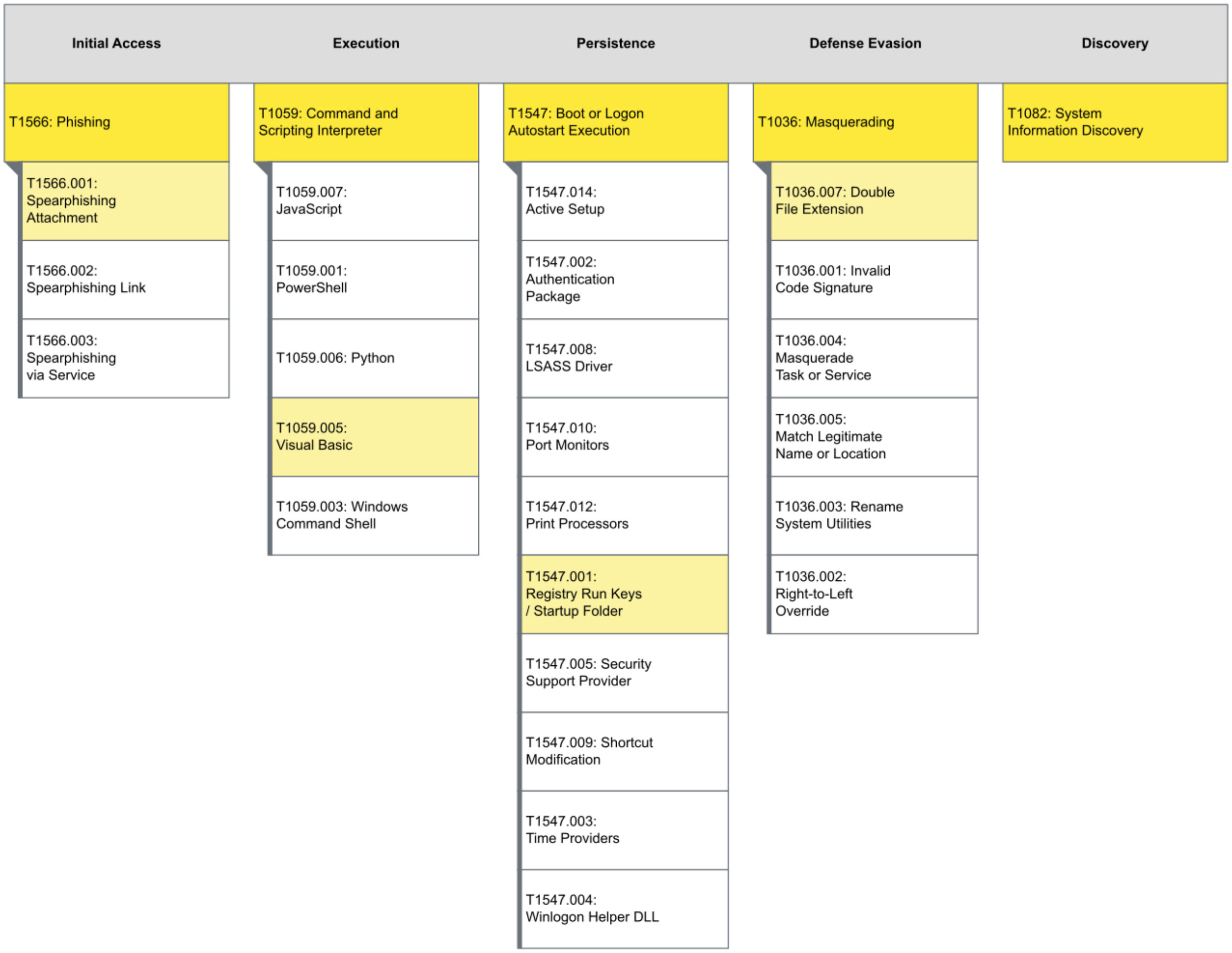
- Delete the malicious VBS file on the compromised computer to prevent further execution and damage.

- Delete the phishing email from the affected user's mailbox to prevent further access by the attacker.

- Isolate the compromised machine from the network to prevent the attacker from accessing other resources and systems within the organization.

Appendix

MITRE ATT&CK



Initial Access	Execution	Persistence	Defense Evasion	Discovery
T1566: Phishing	T1059: Command and Scripting Interpreter	T1547: Boot or Logon Autostart Execution	T1036: Masquerading	T1082: System Information Discovery
T1566.001: Spearphishing Attachment	T1059.007: JavaScript	T1547.014: Active Setup	T1036.007: Double File Extension	
T1566.002: Spearphishing Link	T1059.001: PowerShell	T1547.002: Authentication Package	T1036.001: Invalid Code Signature	
T1566.003: Spearphishing via Service	T1059.006: Python	T1547.008: LSASS Driver	T1036.004: Masquerade Task or Service	
	T1059.005: Visual Basic	T1547.010: Port Monitors	T1036.005: Match Legitimate Name or Location	
	T1059.003: Windows Command Shell	T1547.012: Print Processors	T1036.003: Rename System Utilities	
		T1547.001: Registry Run Keys / Startup Folder	T1036.002: Right-to-Left Override	
		T1547.005: Security Support Provider		
		T1547.009: Shortcut Modification		
		T1547.003: Time Providers		
		T1547.004: Winlogon Helper DLL		

MITRE Tactics	MITRE Techniques
Initial Access	T1566 Phishing
Execution	T1059 Command and Scripting Interpreter
Persistence	T1547 Boot or Logon Autostart Execution
Defense Evasion	T1036 Masquerading
Discovery	T1062 System Information Discovery

Artifacts

Filename	SHA256 Value
Purchese_Order	1c546a6548beda639640ebfbb52abd5f6013c33500172cfccf0e8716c96bb196

IOC TYPE	VALUE
Domain	chongmei33.publicvm.com
IPv4	103.47.144.80
URL	http://chongmei33.publicvm.com:7045/is-ready