LetsDefend

Official Incident Report

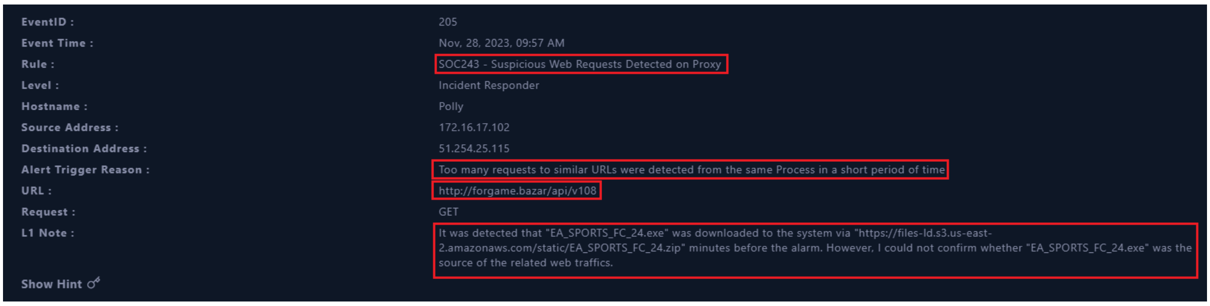
Event ID: 205

Rule Name: SOC243 - Suspicious Web Requests Detected on Proxy

Table of contents

Alert

The alert was triggered due to too many requests from the same process to similar URLs in a short period of time on the system. The alert hit the SOC243 - Suspicious Web Requests Detected on Proxy rule.



EventID :	205
Event Time :	Nov, 28, 2023, 09:57 AM
Rule :	SOC243 - Suspicious Web Requests Detected on Proxy
Level :	Incident Responder
Hostname :	Polly
Source Address :	172.16.17.102
Destination Address :	51.254.25.115
Alert Trigger Reason :	Too many requests to similar URLs were detected from the same Process in a short period of time
URL :	http://forgame.bazar/api/v108
Request :	GET
L1 Note :	It was detected that "EA_SPORTS_FC_24.exe" was downloaded to the system via "https://files-ld.s3.us-east-2.amazonaws.com/static/EA_SPORTS_FC_24.zip" minutes before the alarm. However, I could not confirm whether "EA_SPORTS_FC_24.exe" was the source of the related web traffics.

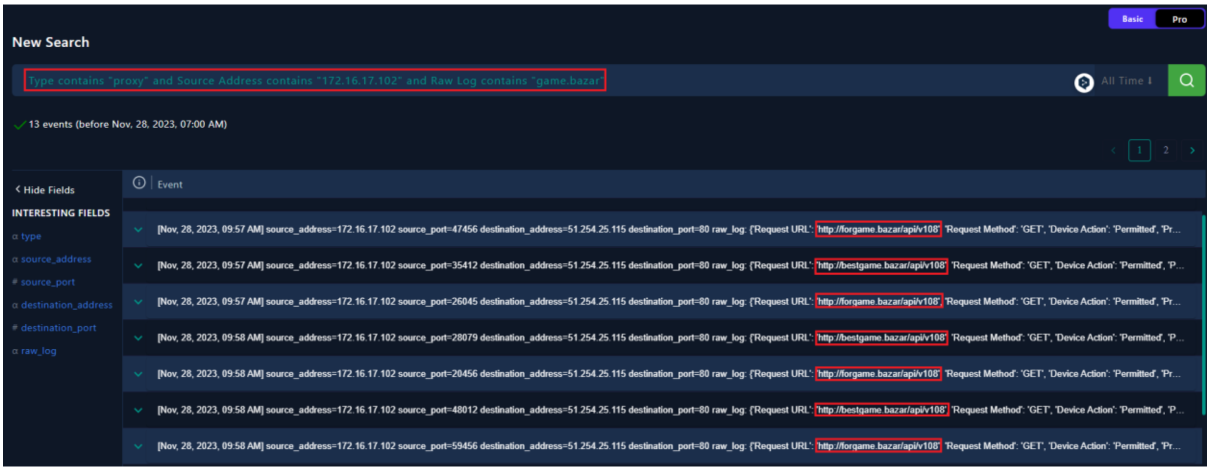
First, the alert should be verified by checking the available logs, then the source of this traffic should be investigated and it should be confirmed whether it is legitimate or not.

Detection

Verify

In Log Management, search for the source IP address (172[.]16.17.102) in the alert and examine the logs among the results. This way, both Proxy, Firewall, OS, and DNS logs of the relevant IP were seen.

You should check the proxy logs in detail to confirm the alert. For this, you can search on Log Management as follows. The relevant search shows the URL “hxxp://forgame.bazar/api/v108” in the alert as below. Similar to the related URL, many requests were seen towards “hxxp://bestgame.bazar/api/v108”. Thus, the alert matches the trigger reason. It was confirmed that requests to similar URLs were made in a short time. It can be said that the alert is True Positive.



```
Type contains "proxy" and Source Address contains "172.16.17.102" and Raw Log contains "game.bazar"
```

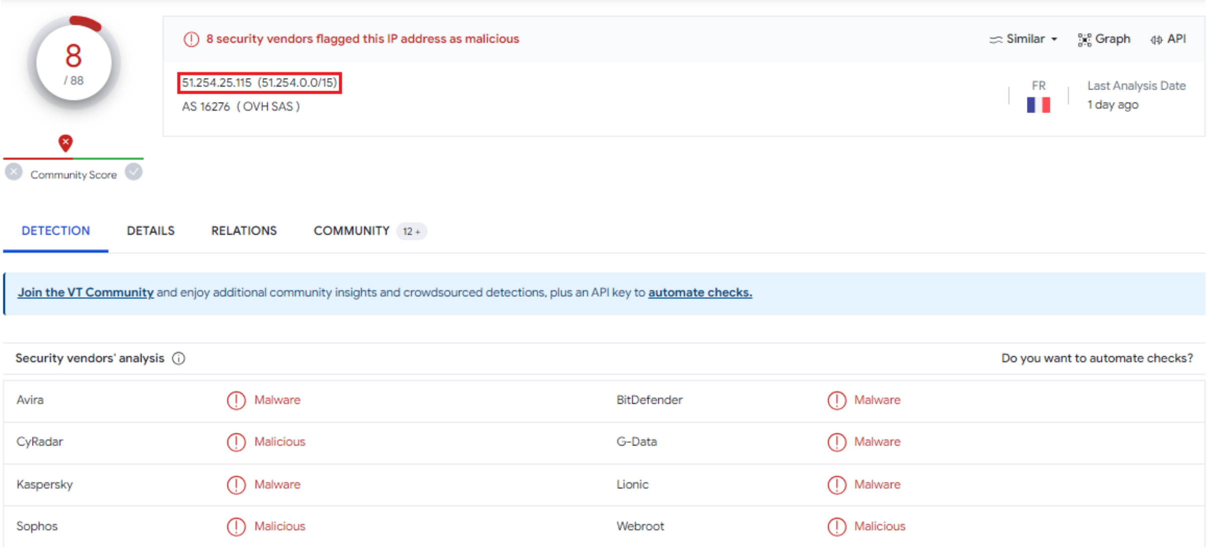
13 events (before Nov, 28, 2023, 07:00 AM)

```
[Nov, 28, 2023, 09:57 AM] source_address=172.16.17.102 source_port=47456 destination_address=51.254.25.115 destination_port=80 raw_log: {'Request URL': 'http://forgame.bazar/api/v108' 'Request Method': 'GET', 'Device Action': 'Permitted', 'Pr...
[Nov, 28, 2023, 09:57 AM] source_address=172.16.17.102 source_port=35412 destination_address=51.254.25.115 destination_port=80 raw_log: {'Request URL': 'http://bestgame.bazar/api/v108' 'Request Method': 'GET', 'Device Action': 'Permitted', 'P...
[Nov, 28, 2023, 09:57 AM] source_address=172.16.17.102 source_port=26045 destination_address=51.254.25.115 destination_port=80 raw_log: {'Request URL': 'http://forgame.bazar/api/v108', 'Request Method': 'GET', 'Device Action': 'Permitted', 'Pr...
[Nov, 28, 2023, 09:58 AM] source_address=172.16.17.102 source_port=28079 destination_address=51.254.25.115 destination_port=80 raw_log: {'Request URL': 'http://bestgame.bazar/api/v108' 'Request Method': 'GET', 'Device Action': 'Permitted', 'P...
[Nov, 28, 2023, 09:58 AM] source_address=172.16.17.102 source_port=20456 destination_address=51.254.25.115 destination_port=80 raw_log: {'Request URL': 'http://forgame.bazar/api/v108' 'Request Method': 'GET', 'Device Action': 'Permitted', 'Pr...
[Nov, 28, 2023, 09:58 AM] source_address=172.16.17.102 source_port=48012 destination_address=51.254.25.115 destination_port=80 raw_log: {'Request URL': 'http://bestgame.bazar/api/v108' 'Request Method': 'GET', 'Device Action': 'Permitted', 'P...
[Nov, 28, 2023, 09:58 AM] source_address=172.16.17.102 source_port=59456 destination_address=51.254.25.115 destination_port=80 raw_log: {'Request URL': 'http://forgame.bazar/api/v108' 'Request Method': 'GET', 'Device Action': 'Permitted', 'Pr...
```

Analysis

Reputation Check

You can perform reputation checks of the France-based IP "51[.]254.25.115" mentioned in the alert details. In addition, the URLs “hxxp://forgame.bazar/api/v108” and “hxxp://bestgame.bazar/api/v108” in proxy traffic should also be checked. You should also check the reputation of the hash value of "EA_SPORTS_FC_24.exe" which was stated to be downloaded to the system in the L1 analyst note.



8 security vendors flagged this IP address as malicious

51.254.25.115 (51.254.0.0/15)
AS 16276 (OVH SAS)

FR

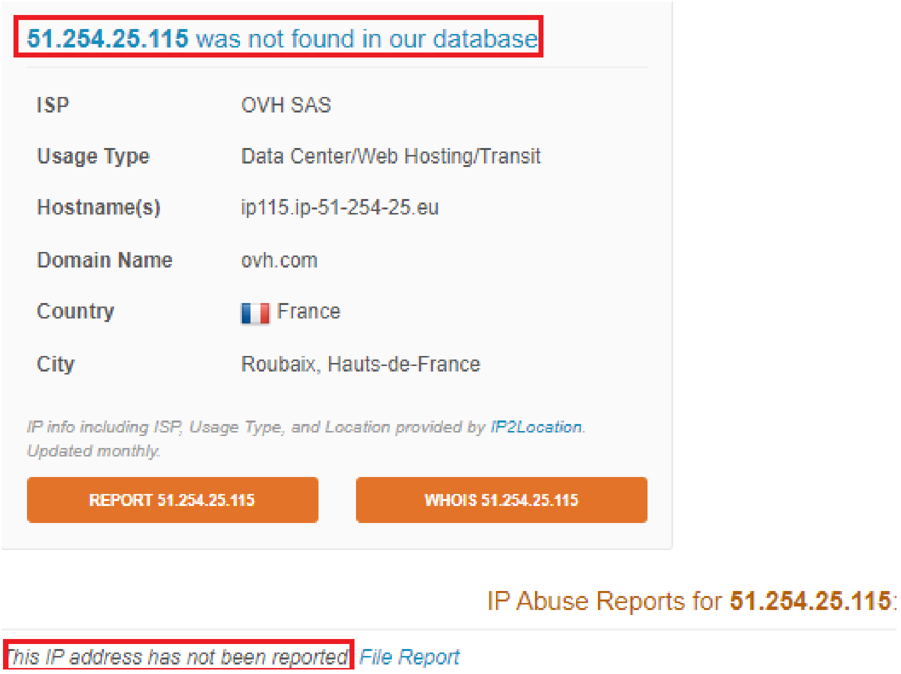
Last Analysis Date
1 day ago

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis — Do you want to automate checks?

Avira	Malware	BitDefender	Malware
CyRadar	Malicious	G-Data	Malware
Kaspersky	Malware	Lionic	Malware
Sophos	Malicious	Webroot	Malicious

https://www.virustotal.com/gui/ip-address/51.254.25.115/detection



51.254.25.115 was not found in our database

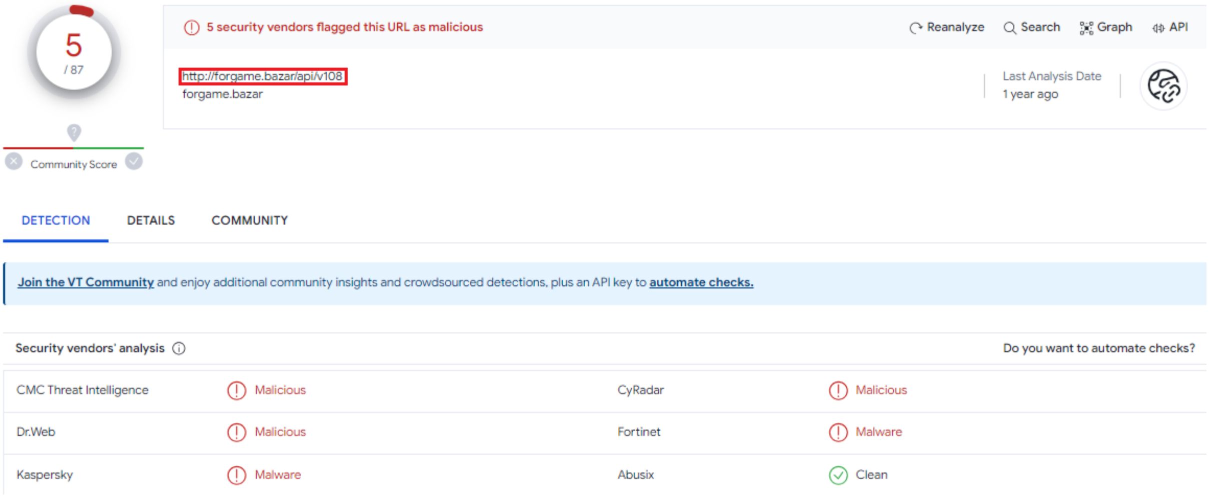
ISP	OVH SAS
Usage Type	Data Center/Web Hosting/Transit
Hostname(s)	ip115.ip-51-254-25.eu
Domain Name	ovh.com
Country	France
City	Roubaix, Hauts-de-France

IP info including ISP, Usage Type, and Location provided by IP2Location. Updated monthly.

IP Abuse Reports for **51.254.25.115**:

This IP address has not been reported File Report

https://www.abuseipdb.com/check/51.254.25.115



5 security vendors flagged this URL as malicious

http://forgame.bazar/api/v108
forgame.bazar

Last Analysis Date
1 year ago

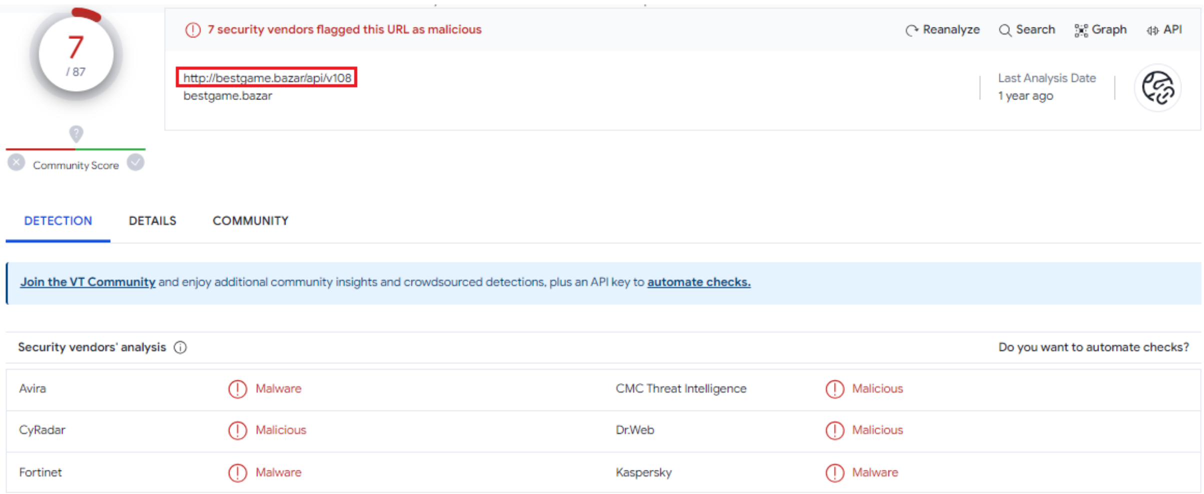
Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to **automate checks.**

Security vendors' analysis

Do you want to automate checks?

CMC Threat Intelligence	Malicious	CyRadar	Malicious
Dr.Web	Malicious	Fortinet	Malware
Kaspersky	Malware	Abusix	Clean

https://www.virustotal.com/gui/url/ce059fb571647d351e85e11c5d7ac2c67e1ea68ecbf1e6815a26d17e327a3016



7 security vendors flagged this URL as malicious

http://bestgame.bazar/api/v108
bestgame.bazar

Last Analysis Date
1 year ago

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

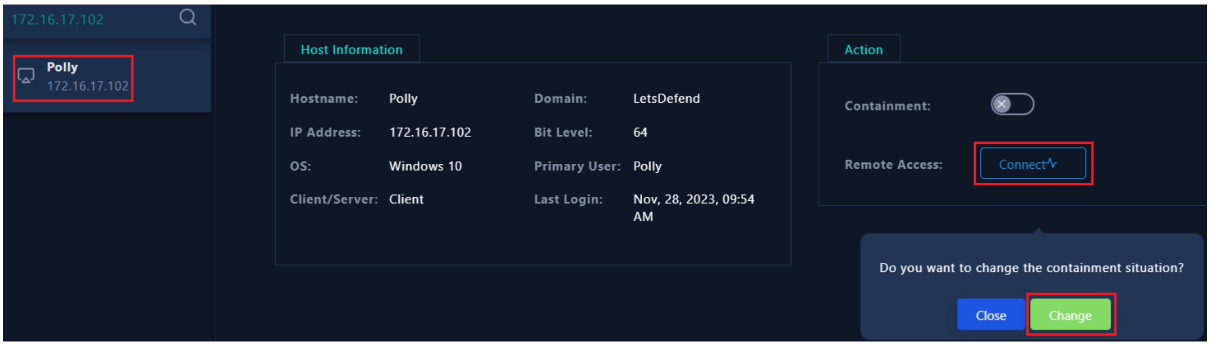
Do you want to automate checks?

Avira	Malware	CMC Threat Intelligence	Malicious
CyRadar	Malicious	Dr.Web	Malicious
Fortinet	Malware	Kaspersky	Malware

https://www.virustotal.com/gui/url/d57425705a70379958f77f12d9f958ca11b8f6881e057b93d43734f630d6de2e

It is found that the relevant URL and IP are reported as malicious on sources such as Virus Total and AbuseIPDB.

You should isolate the system from the network until the system is analyzed in detail due to repeated requests to malicious URLs from the same source in a short time. For the relevant process, go to Endpoint security and isolate it via Containment as follows.



Hostname: Polly
Domain: LetsDefend
IP Address: 172.16.17.102
Bit Level: 64
OS: Windows 10
Primary User: Polly
Client/Server: Client
Last Login: Nov, 28, 2023, 09:54 AM

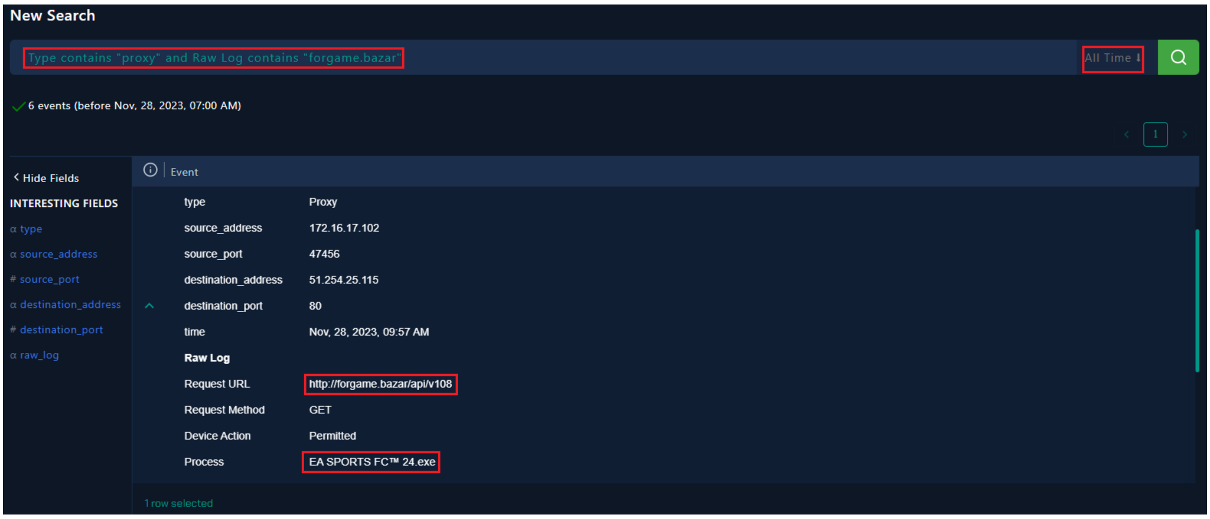
Containment:
Remote Access:

Do you want to change the containment situation?

Initial Access

The L1 Analyst note indicates that the file “EA_SPORTS_FC_24.zip” was downloaded to the system via the address “hxxps://files-ld.s3.us-east-2.amazonaws.com/static/EA_SPORTS_FC_24.zip”. First of all, the connection of the file with the repeated URL traffic should be confirmed.

For the related control, you can look at the details of the proxy log on Log Management as shown below. As can be seen in the log, the source process of the related traffic is “EA SPORTS FC™ 24.exe”. It is highly likely that the relevant application is in the EA_SPORTS_FC_24.zip file downloaded to the system. However, this can be confirmed by checking the file create(EventID:11) logs.

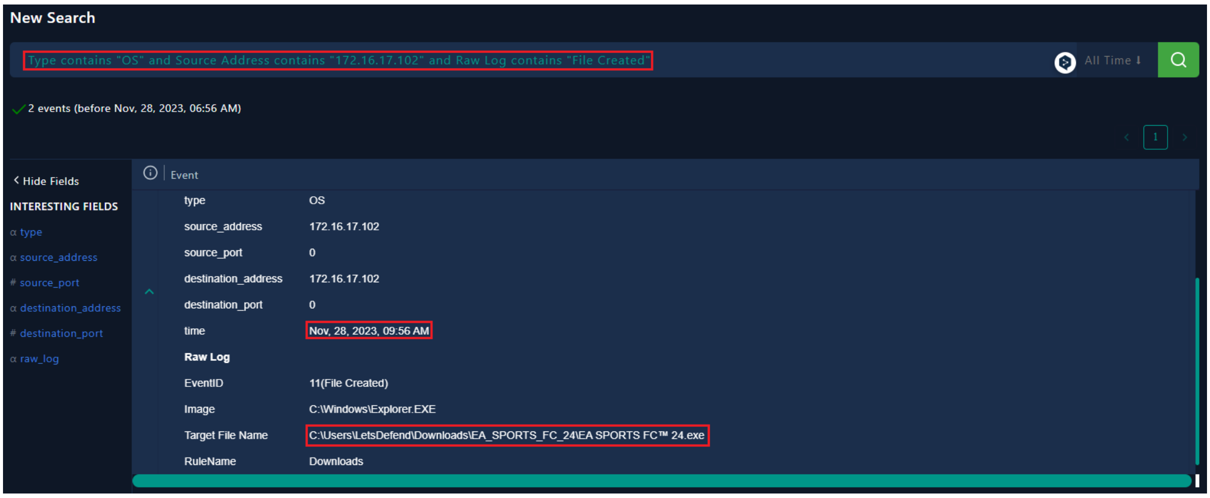


Type contains "proxy" and Raw Log contains "forgame.bazar"

6 events (before Nov, 28, 2023, 07:00 AM)

type	Proxy
source_address	172.16.17.102
source_port	47456
destination_address	51.254.25.115
destination_port	80
time	Nov, 28, 2023, 09:57 AM
Raw Log	
Request URL	http://forgame.bazar/api/v108
Request Method	GET
Device Action	Permitted
Process	EA SPORTS FC™ 24.exe

You can perform a search on Log Management as follows to provide the relevant check. As can be seen in the log detail, “EA SPORTS FC™ 24.exe” was created under the file “C:\Users\LetsDefend\Downloads\EA_SPORTS_FC_24” at 09:56 AM.

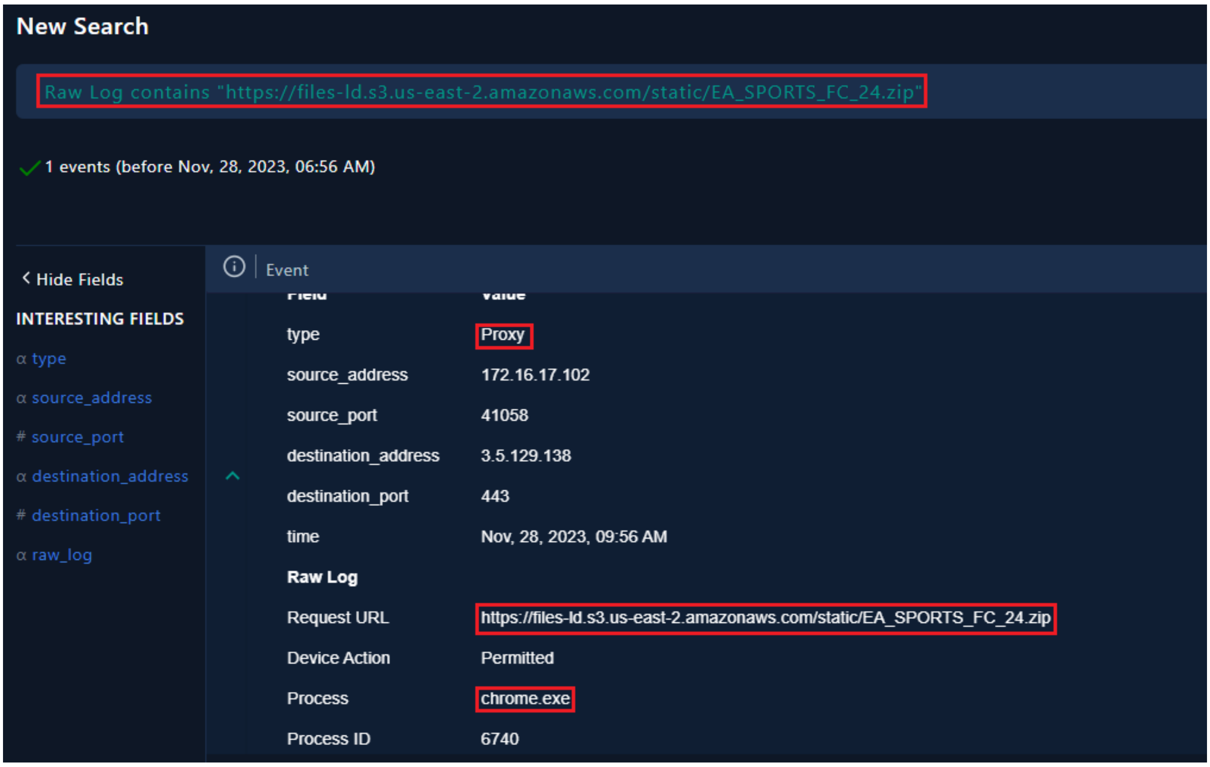


Type contains "OS" and Source Address contains "172.16.17.102" and Raw Log contains "File Created"

2 events (before Nov, 28, 2023, 06:56 AM)

type	OS
source_address	172.16.17.102
source_port	0
destination_address	172.16.17.102
destination_port	0
time	Nov, 28, 2023, 09:56 AM
Raw Log	
EventID	11(File Created)
Image	C:\Windows\Explorer.EXE
Target File Name	C:\Users\LetsDefend\Downloads\EA_SPORTS_FC_24\EA SPORTS FC™ 24.exe
RuleName	Downloads

You should also check how the relevant application was downloaded to the system. For this, you can check the proxy logs for the URL mentioned in the L1 analyst's note.



New Search

Raw Log contains "https://files-ld.s3.us-east-2.amazonaws.com/static/EA_SPORTS_FC_24.zip"

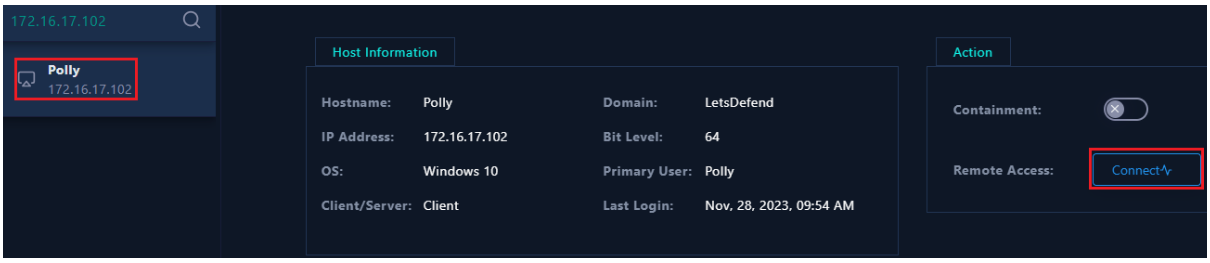
✓ 1 events (before Nov, 28, 2023, 06:56 AM)

Field	Value
type	Proxy
source_address	172.16.17.102
source_port	41058
destination_address	3.5.129.138
destination_port	443
time	Nov, 28, 2023, 09:56 AM
Raw Log	
Request URL	https://files-ld.s3.us-east-2.amazonaws.com/static/EA_SPORTS_FC_24.zip
Device Action	Permitted
Process	chrome.exe
Process ID	6740

As can be seen above, there is a request to the “hxxps://files-ld.s3.us-east-2.amazonaws.com/static/EA_SPORTS_FC_24.zip” address via Chrome. The alert occurred in the system due to malware via Malicious Link. At this point, initial access can be both Phishing and Drive-by Compromise. It should be checked whether the relevant link has reached the victim by 3rd party persons via e-mail or other means. If the relevant mail did not reach “Polly” by any user, it can be said that “Drive-by Compromise” technique was used for the initial access. You should search the URL on Email Security for the relevant check. As can be seen, the relevant mail does not appear in any mail. Thus, it can be said that “Drive-by Compromise” technique was used for initial access instead of "Phishing".

It was confirmed that there has been repeated traffic to malicious URLs via the "EA SPORTS FC™ 24.exe" application. It was also determined that the application was downloaded to the system through the user's error. You can connect to the system to obtain the hash values of the relevant application. You should always check the hash values on the original file/.exe if possible.

To connect to the system, go to Endpoint Security and press the “connect” button as below.



172.16.17.102

Polly
172.16.17.102

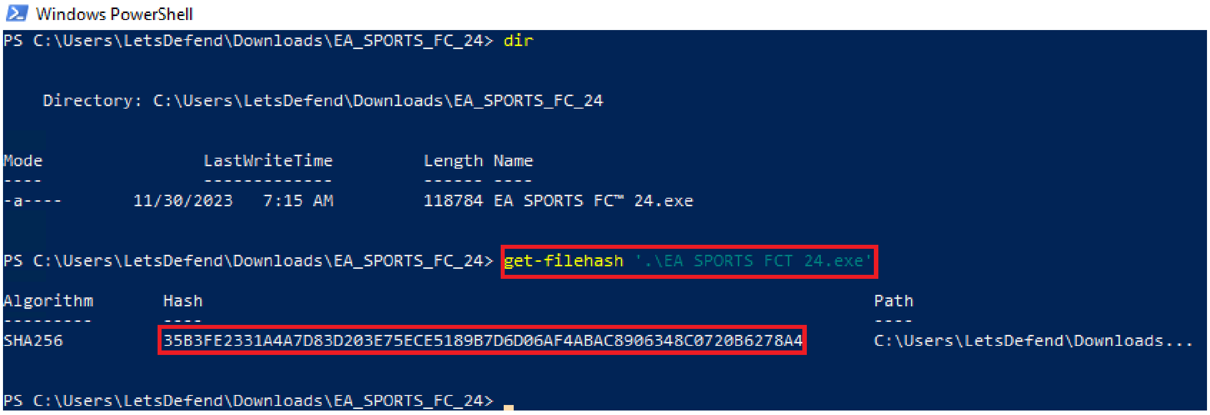
Host Information

Hostname: Polly
IP Address: 172.16.17.102
OS: Windows 10
Client/Server: Client
Domain: LetsDefend
Bit Level: 64
Primary User: Polly
Last Login: Nov, 28, 2023, 09:54 AM

Action

Containment:
Remote Access: Connect

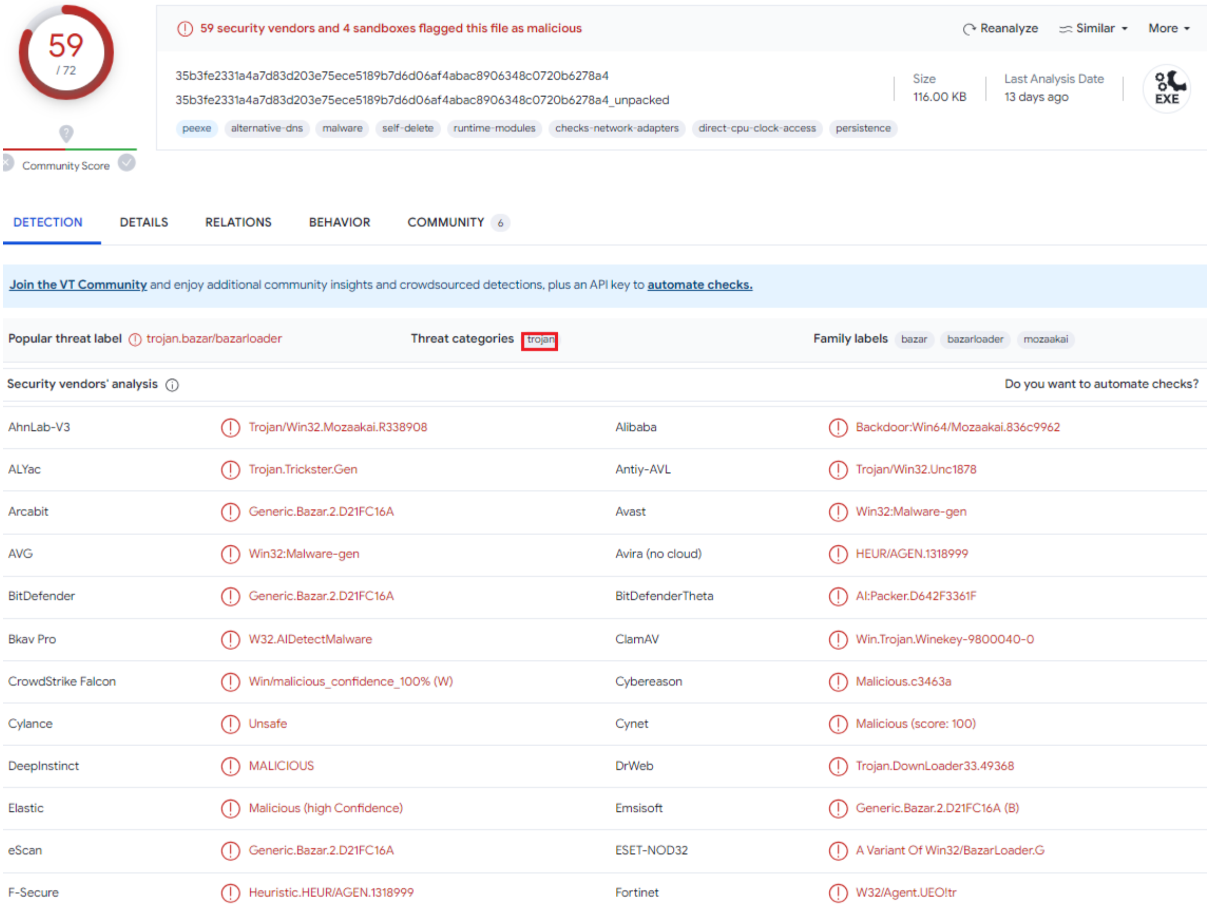
After connecting to the system, you can open PowerShell for hash checking. The hash value is obtained via PowerShell as follows.



```
PS C:\Users\LetsDefend\Downloads\EA_SPORTS_FC_24> dir


    Directory: C:\Users\LetsDefend\Downloads\EA_SPORTS_FC_24


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        11/30/2023   7:15 AM         118784 EA SPORTS FC™ 24.exe


PS C:\Users\LetsDefend\Downloads\EA_SPORTS_FC_24> get-filehash '.\EA SPORTS FCT 24.exe'

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
SHA256          35B3FE2331A4A7D83D203E75ECE5189B7D6D06AF4ABAC8906348C0720B6278A4       C:\Users\LetsDefend\Downloads...


PS C:\Users\LetsDefend\Downloads\EA_SPORTS_FC_24>
```

Hash:35B3FE2331A4A7D83D203E75ECE5189B7D6D06AF4ABAC8906348C0720B6278A4

The reputation of the hash is seen in Virus Total as below. It was reported as “Malicious”, “Trojan” and “Unsafe” multiple times by different sources.



59 security vendors and 4 sandboxes flagged this file as malicious

35b3fe2331a4a7d83d203e75ece5189b7d6d06af4abac8906348c0720b6278a4

35b3fe2331a4a7d83d203e75ece5189b7d6d06af4abac8906348c0720b6278a4_unpacked

peexe alternative-dns malware self-delete runtime-modules checks-network-adapters direct-cpu-clock-access persistence

Size 116.00 KB

Last Analysis Date 13 days ago

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label trojan.bazar/bazarloader

Threat categories trojan

Family labels bazar bazarloader mozaakai

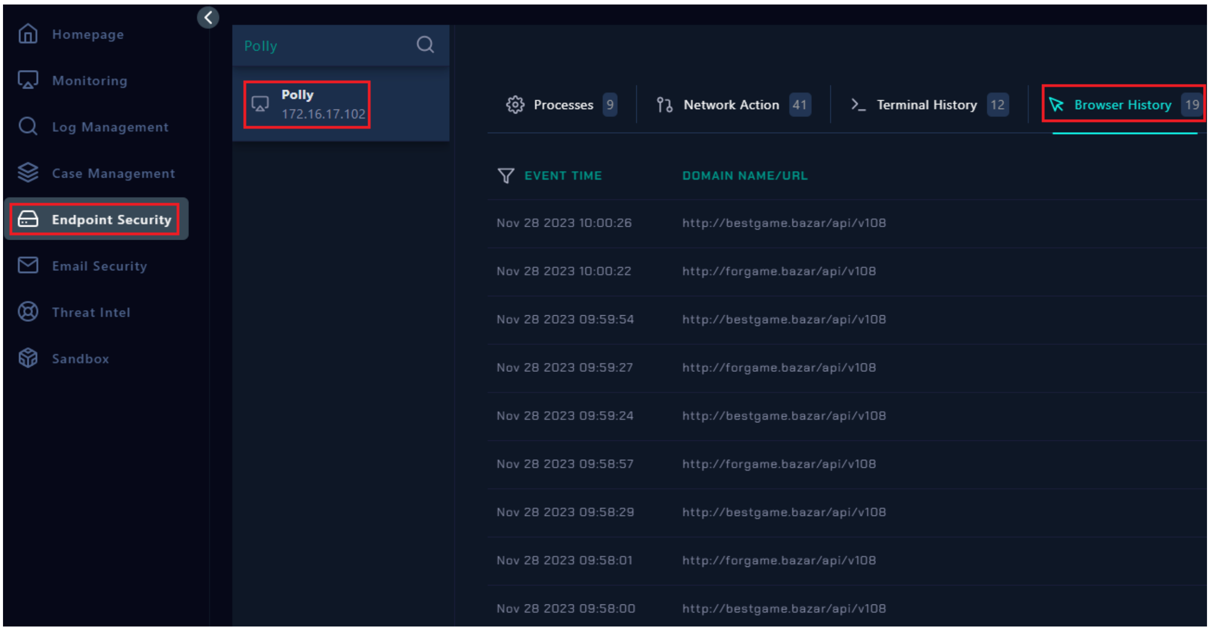
Security vendors' analysis

Do you want to automate checks?

AhnLab-V3	Trojan/Win32.Mozaakai.R338908	Alibaba	Backdoor:Win64/Mozaakai.836c9962
ALYac	Trojan.Trickster.Gen	Antiy-AVL	Trojan/Win32.Unc1878
Arcabit	Generic.Bazar.2.D21FC16A	Avast	Win32:Malware-gen
AVG	Win32:Malware-gen	Avira (no cloud)	HEUR/AGEN.1318999
BitDefender	Generic.Bazar.2.D21FC16A	BitDefenderTheta	AI:Packer.D642F3361F
Bkav Pro	W32.AIDetectMalware	ClamAV	Win.Trojan.Winekey-9800040-0
CrowdStrike Falcon	Win/malicious_confidence_100% (W)	Cybereason	Malicious.c3463a
Cylance	Unsafe	Cynet	Malicious (score: 100)
DeepInstinct	MALICIOUS	DrWeb	Trojan.DownLoader33.49368
Elastic	Malicious (high Confidence)	Emsisoft	Generic.Bazar.2.D21FC16A (B)
eScan	Generic.Bazar.2.D21FC16A	ESET-NOD32	A Variant Of Win32/BazarLoader.G
F-Secure	Heuristic.HEUR/AGEN.1318999	Fortinet	W32/Agent.UEO!tr

https://www.virustotal.com/gui/file/35b3fe2331a4a7d83d203e75ece5189b7d6d06af4abac8906348c0720b6278a4

Analyses revealed how and by what means the malware gained access to the system. However, the exact purpose and target of the malware could not be understood. The analysis so far showed that the malware sent repeated requests to similar URLs in a short period of time. To see the URLs in one place, you can check browser history in Endpoint Security.



EVENT TIME	DOMAIN NAME/URL
Nov 28 2023 10:00:26	http://bestgame.bazar/api/v108
Nov 28 2023 10:00:22	http://forgame.bazar/api/v108
Nov 28 2023 09:59:54	http://bestgame.bazar/api/v108
Nov 28 2023 09:59:27	http://forgame.bazar/api/v108
Nov 28 2023 09:59:24	http://bestgame.bazar/api/v108
Nov 28 2023 09:58:57	http://forgame.bazar/api/v108
Nov 28 2023 09:58:29	http://bestgame.bazar/api/v108
Nov 28 2023 09:58:01	http://forgame.bazar/api/v108
Nov 28 2023 09:58:00	http://bestgame.bazar/api/v108

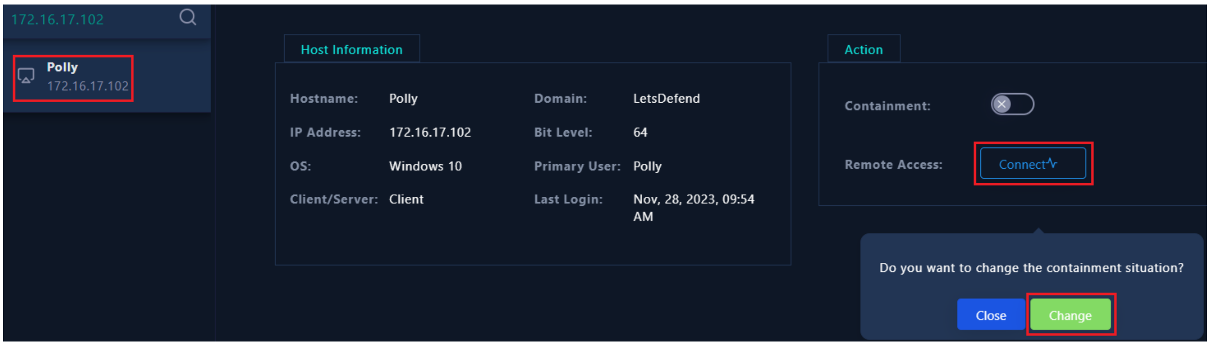
As can be seen above, there has been repeated traffic to "hxxp://forgame.bazar/api/v108" and "hxxp://bestgame.bazar/api/v108" addresses on the system. Another noteworthy point here is that the requests are thrown sequentially. If the relevant URLs are considered as C2s, it means that the malware was trying to access the relevant C2s in order. It can be said that “Fallback Channels” was used as a MITRE technique. Because the malware may be aiming to use an alternative second channel in communication with the C2.

#####Fallback Channels
Adversaries may use fallback or alternate communication channels if the primary channel is compromised or inaccessible in order to maintain reliable command and control and to avoid data transfer thresholds.

https://attack.mitre.org/techniques/T1008/

Containment

It was detected that there were repeated requests to malicious URLs from the same source in a short time. It was observed that the repetitive traffic belongs to the malware trying to communicate with C2. Therefore, it is necessary to isolate the system from the network. For the related process, go to Endpoint security and isolate the system via Containment as follows.



Hostname: Polly
Domain: LetsDefend
IP Address: 172.16.17.102
Bit Level: 64
OS: Windows 10
Primary User: Polly
Client/Server: Client
Last Login: Nov, 28, 2023, 09:54 AM

Containment:
Remote Access:

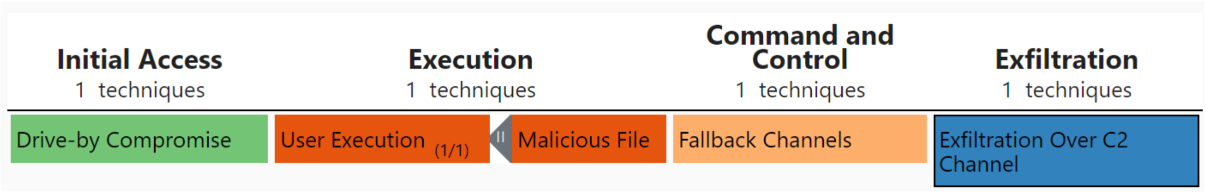
Do you want to change the containment situation?

Lesson Learned

- End users should be trained periodically to increase information security.
- Applications of unknown origin and credibility should not be downloaded and installed on the system.
- For inside-out traffic, whitelisting method should be applied to the rules on the Firewall.
- EDR products must be enabled in the systems and their signatures must be up to date.

Appendix

MITRE



Initial Access
1 techniques
- Drive-by Compromise

Execution
1 techniques
- User Execution (1/1)
- Malicious File

Command and Control
1 techniques
- Fallback Channels

Exfiltration
1 techniques
- Exfiltration Over C2 Channel

MITRE Tactics	MITRE Techniques
Initial Access	● Drive-by Compromise
Execution	● User Execution: Malicious File
Command and Control	● Fallback Channels
Exfiltration	● Exfiltration Over C2 Channel

Artifacts

Field	Value
IPs	● 172[.]16.17.102 ● 51[.]254.25.115 ● 3[.]5.129.138
Files/Exe	● EA_SPORTS_FC_24.zip ● EA SPORTS FC™ 24.exe
Hash	● 35B3FE2331A4A7D83D203E75ECE5189B7D6D06AF4ABAC8906348C0720B6278A4
User	● polly[@]letsdefend[.]io
URL	● hxxps://files-ld.s3.us-east-2.amazonaws.com/static/EA_SPORTS_FC_24.zip ● hxxp://bestgame.bazar/api/v108 ● hxxp://forgame.bazar/api/v108