











Investigation - ALERT! Crypto mining [Critical]










User: [suman_chanthati@](#)

Hostname: GOL012702

Apex Central TM

- We have observed multiple alerts on TM Apex Central regarding <https://agafurretor.com> which are getting blocked under Web Violation.
- We are getting similar logs from May 2021; no action was taken till date.

Security Threat Details						
	Security Threat	Category	File Path / Email Subject / Rule Name	Action	Logged by	Time
	https://agafurretor.com/event	Web violation	Malware Accomplish	Block	Apex One	05/26/2021 22:45:11
	https://agafurretor.com/event	Web violation	Malware Accomplish	Block	Apex One	05/26/2021 22:45:11
	https://agafurretor.com/event	Web violation	Malware Accomplish	Block	Apex One	05/26/2021 22:41:40
	https://agafurretor.com/event	Web violation	Malware Accomplish	Block	Apex One	05/26/2021 22:41:39
	https://agafurretor.com/iwant-show?3.1.293	Web violation	Malware Accomplish	Block	Apex One	05/26/2021 22:41:37
	https://agafurretor.com/iwant?3.1.293	Web violation	Malware Accomplish	Block	Apex One	05/26/2021 22:41:36
	https://agafurretor.com/iwant?3.1.293	Web violation	Malware Accomplish	Block	Apex One	05/26/2021 22:41:34
	https://cdn.betgorebysson.club/apu.php?zoneid=3897490	Web violation	Scam	Block	Apex One	05/26/2021 22:06:10
	https://cdn.betgorebysson.club/apu.php?zoneid=3897490	Web violation	Scam	Block	Apex One	05/26/2021 22:05:18

Security Threat Details						
	Security Threat	Category	File Path / Email Subject / Rule Name	Action	Logged by	Time
	https://agafurretor.com/iw-ant-check?3.1.297	Web violation	Malware Accomplice	Block	Apex One	07/07/2021 21:33:06
	https://agafurretor.com/iw-ant-check?3.1.297	Web violation	Malware Accomplice	Block	Apex One	07/07/2021 21:32:51
	https://agafurretor.com/iw-ant-check?3.1.297	Web violation	Malware Accomplice	Block	Apex One	07/07/2021 21:32:39
	https://agafurretor.com/iw-ant-check?3.1.297	Web violation	Malware Accomplice	Block	Apex One	07/07/2021 21:09:05
	https://agafurretor.com/iw-ant-check?3.1.297	Web violation	Malware Accomplice	Block	Apex One	07/07/2021 12:59:38
	https://agafurretor.com/iw-ant-check?3.1.297	Web violation	Malware Accomplice	Block	Apex One	07/07/2021 12:59:38
	https://agafurretor.com/iw-ant-check?3.1.297	Web violation	Malware Accomplice	Block	Apex One	07/07/2021 12:58:14
	https://agafurretor.com/iw-ant-check?3.1.297	Web violation	Malware Accomplice	Block	Apex One	07/07/2021 12:58:02

What is Agafurretor?

Agafurretor.com is part of an advertising service that website publishers can use to generate revenue on their sites. Unfortunately, there are malicious programs that are redirecting users to these Agafurretor.com ads without the permission of the publisher to generate revenue. When Agafurretor.com redirects a browser to an advertisement, the ads are typically for unwanted chrome extensions, surveys, adult sites, online web games, fake software updates, and unwanted programs.


Impact:

Once Agafurretor.com lands on your computer, it modifies the settings of your browser (Mozilla Firefox, Google Chrome, or Internet Explorer) and changes its home page to Agafurretor.com. As with most browser hijackers, it starts displaying unwanted pop-up ads which will disturb your browsing routine.

The main purpose of Agafurretor.com Virus is to generate traffic on its main page, monetizing it in various ways such as pay-per-click schemes profiting from infected visitors to the home page.

Zscaler

- We have checked that Zscaler was installed on Thu Jul 08, 2021
- User was using Bitcoin/Trading and advertisement Websites as checked in browsing history and logs.

Zscaler Client Connector Registered Device Details 

REGISTRATION DETAILS

User ID suman_chanthati@██████████	Policy Name Production Users App Profile
Device ID 24720873	Last Registration Time Thu Jul 08 2021 16:28:16 GMT+0530 (India ...)
Last Unregistration Time Unavailable	Zscaler Client Connector Version 3.4.0.124
Tunnel Version Tunnel 2.0 with DTLS Protocol	

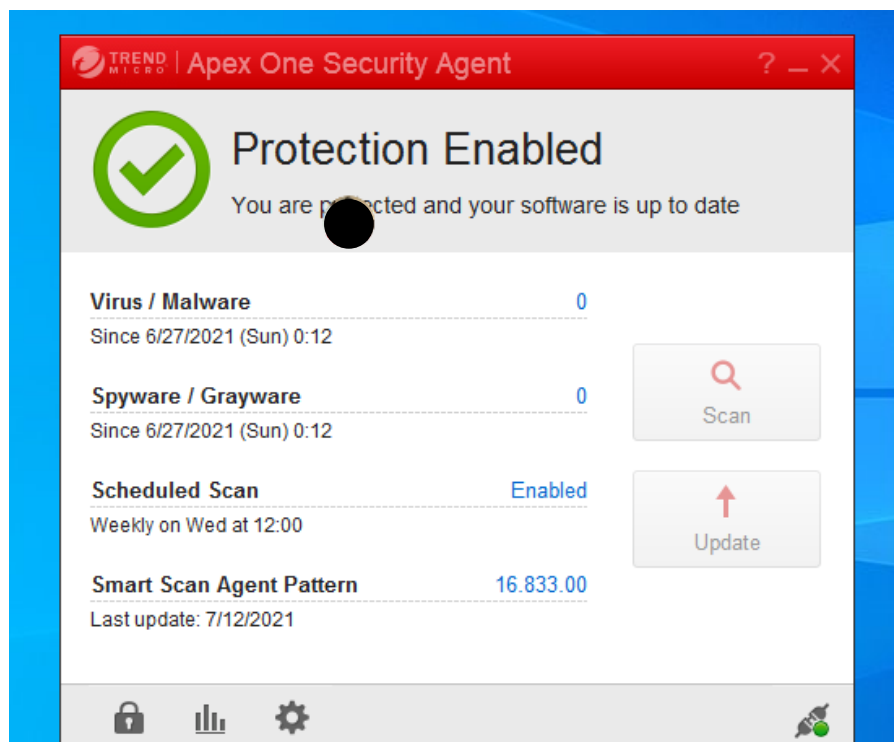
DEVICE DETAILS

Owner suman_chanthati	Machine Hostname ██████████
---------------------------------	---------------------------------------

Insights Logs						
			Jul 11, 2021 10:54:26 PM - Jul 11, 2021 11:26:05 PM			
			29 Log Records Found			
No...	Event Time	User	Policy Action	Location	URL	
1	Sunday, July 11, 2021 10:54:26 PM	suman_chanthati@...	IPS block: cryptomining traffic	Road Warrior	freebitco.in:443	
2	Sunday, July 11, 2021 10:54:26 PM	suman_chanthati@...	IPS block: cryptomining traffic	Road Warrior	static1.freebitco.in:443	
3	Sunday, July 11, 2021 10:54:26 PM	suman_chanthati@...	IPS block: cryptomining traffic	Road Warrior	freebitco.in:443	
4	Sunday, July 11, 2021 10:54:26 PM	suman_chanthati@...	IPS block: cryptomining traffic	Road Warrior	static1.freebitco.in:443	
5	Sunday, July 11, 2021 10:54:28 PM	suman_chanthati@...	IPS block: cryptomining traffic	Road Warrior	freebitco.in:443	
6	Sunday, July 11, 2021 10:54:28 PM	suman_chanthati@...	IPS block: cryptomining traffic	Road Warrior	freebitco.in:443	
7	Sunday, July 11, 2021 10:54:29 PM	suman_chanthati@...	IPS block: cryptomining traffic	Road Warrior	freebitco.in:443	
8	Sunday, July 11, 2021 10:54:29 PM	suman_chanthati@...	IPS block: cryptomining traffic	Road Warrior	static1.freebitco.in:443	
9	Sunday, July 11, 2021 10:54:29 PM	suman_chanthati@...	IPS block: cryptomining traffic	Road Warrior	freebitco.in:443	
10	Sunday, July 11, 2021 10:54:29 PM	suman_chanthati@...	IPS block: cryptomining traffic	Road Warrior	static1.freebitco.in:443	
11	Sunday, July 11, 2021 10:54:30 PM	suman_chanthati@...	IPS block: cryptomining traffic	Road Warrior	freebitco.in:443	

Apex Central Security Agent

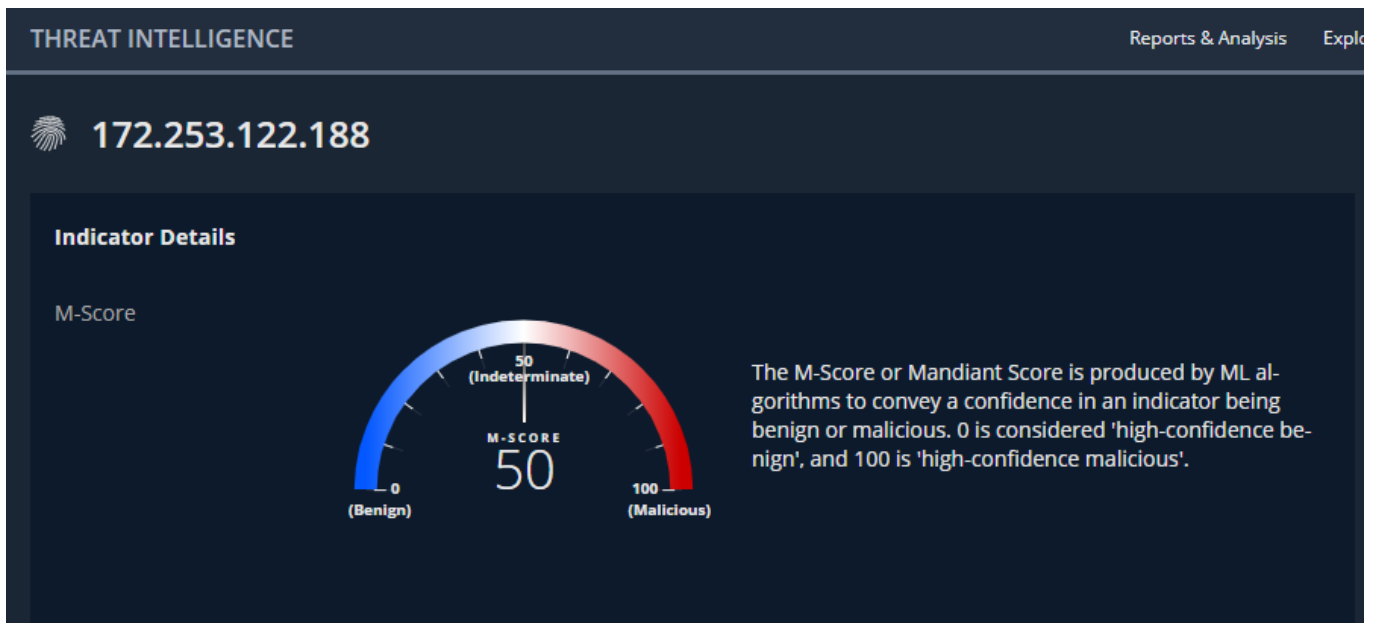
- As checked Agent was up to date



TCP Connections

- We have observed Suspicious IP communications towards Remote Port 5228 and Remote IP 172.253.122.188
- As checked IP belongs to Google but on Threat Intelligence it is showing Malicious.

[Time Wait]		TCP	Time Wait	192.168.0.38	50277	52.114.75.79	443		
PanGPA.exe	14556	TCP	Established	127.0.0.1	55941	127.0.0.1	4767	7/12/2021 12:13:53 AM	PanGPA.exe
python.exe	22776	TCP	Established	127.0.0.1	60376	127.0.0.1	5050	7/12/2021 12:35:22 PM	python.exe
chrome.exe	24156	TCP	Established	192.168.0.38	55216	172.253.122.188	5228	7/12/2021 12:35:48 PM	chrome.exe
[Time Wait]		TCP	Time Wait	192.168.0.38	56385	10.96.114.31	8443		
javaw.exe	17848	TCP	Established	10.223.224.77	56380	10.96.114.31	8443	7/12/2021 1:12:10 PM	javaw.exe
javaw.exe	17848	TCP	Established	10.223.224.77	56381	10.96.114.31	8443	7/12/2021 1:12:14 PM	javaw.exe
javaw.exe	17848	TCP	Established	10.223.224.77	56382	10.96.114.31	8443	7/12/2021 1:12:15 PM	javaw.exe
javaw.exe	17848	TCP	Established	10.223.224.77	56386	10.96.114.31	8443	7/12/2021 1:12:19 PM	javaw.exe
javaw.exe	17848	TCP	Established	10.223.224.77	56387	10.96.114.31	8443	7/12/2021 1:12:20 PM	javaw.exe
javaw.exe	17848	TCP	Established	10.223.224.77	56388	10.96.114.31	8443	7/12/2021 1:12:24 PM	javaw.exe



Browser History

- Multiple Bitcoin, Cryptocurrency, Gambling and Movies websites were accessed.
- This indicates that Adware Virus was possibly installed on User System while accessing such websites.

1532	16256	6/24/2021	17:06:32	Free Bitcoin	https://freebit.co.in/	1	1 typed
1846	16085	6/21/2021	17:43:12	Best Casino Bonuses India Free No Deposit Bonus ₹650K+	https://casinobetting.live/in/casino-b	1	0 link
2162	15925	6/17/2021	11:02:58	Top 20 Free Bitcoin Sites & Bitcoin Games	https://btc-sites.com/	3	0 link
2163	15925	6/17/2021	11:02:58	Top 20 Free Bitcoin Sites & Bitcoin Games	https://btc-sites.com/	3	0 link
2164	15925	6/17/2021	11:02:52	Top 20 Free Bitcoin Sites & Bitcoin Games	https://btc-sites.com/	3	0 link
2185	15898	6/16/2021	21:30:57	Command Center Gamehag	https://gamehag.com/	2	0 reload
2188	15898	6/16/2021	21:29:24	Command Center Gamehag	https://gamehag.com/	2	0 link
2202	15898	6/16/2021	21:27:02	Command Center Gamehag	https://gamehag.com/	2	0 link
7455	12645	5/20/2021	14:37:05	agoodmovietowatch What to Watch on Streaming	https://agoodmovietowatch.com/	1	0 link

Action Taken

- Killed all the process contributing to alerts.
- Removed Adware Virus – agafurretor from HOST.
- Reinstalled Google Chrome Browser to avoid similar alerts in future.
- After taking preventive measures no similar alerts has been observed and we have kept User system under monitoring.