CleanINTERNET® Service Report

April 10th, 2020

REPORT PREPARED FOR: Traffic Observed Circumventing Palo Alto Firewall
REPORTING PERIOD: March 19th – April 10th

CONFIDENTIAL & PROPRIETARY — PROVIDED UNDER NDA

TURNING INTELLIGENCE INTO ACTION

Centripetal

Summary

The data behind this report was collected from **Monday, March 16th through Friday, April 10th, 2020** across the RuleGATE® protected location(s). The report reflects continuously updated risk models and policy tuning to maximize protection through the network shielding function. This is an interim weekly report. The individual events of interest which are specifically analyzed below represent a small subset (<1%) of the total collected threat data and are intended to provide insight on samples with actionable recommendations along with context.

CleanINTERNET service leverages the expertise of thousands of security analysts worldwide by harnessing their work-product: threat intelligence. The insight provided through our intelligence sources is massive and enables our ability to provide both automatic Shielding and Advanced Threat Detection on your behalf. The findings identified herein do not represent a deficiency of your security teams, but rather a deficiency of conventional security tools. This level of protection and visibility is only possible due to the RuleGATE filter technology and the real-time threat intelligence provided by up to 88 partners, 3,000+ risk-specialized feeds, and over 6 billion unique indicators of compromise.

OPERATIONAL NOTES

- This report with supporting data is located on the CleanINTERNET customer portal located at https://portal.centripetalnetworks.com
- Each highlighted event of interest has a corresponding EventID which you can use to identify the event in QuickTHREAT® analytics within the CleanINTERNET cloud portal at www.quickthreat.com
- The RuleGATE enables packet capture for each event for full traffic analysis. For data security this requires retrieval directly from the RuleGATE. Please contact us if you need assistance with the retrieval of the PCAP which is currently disabled in your environment.

ONGOING RECOMMENDATIONS

- Commence the CleanInternet service to start maximizing your Shielding posture to eliminate unneeded cyber risks and the workload associated with them.
- Evaluate the Advanced Threat Detection events presented in the report and provide feedback to your Centripetal SOC team to aid in investigation, risk profiling, and policy tuning. Please contact us if you need assistance.

ATD Event — Possible Brute Force Login against Enterprise Remote Access System

Classification:
Possible Exploitation

Matching Policies:
BDE-blocklist_de-ip

Observed Risk:
HIGH

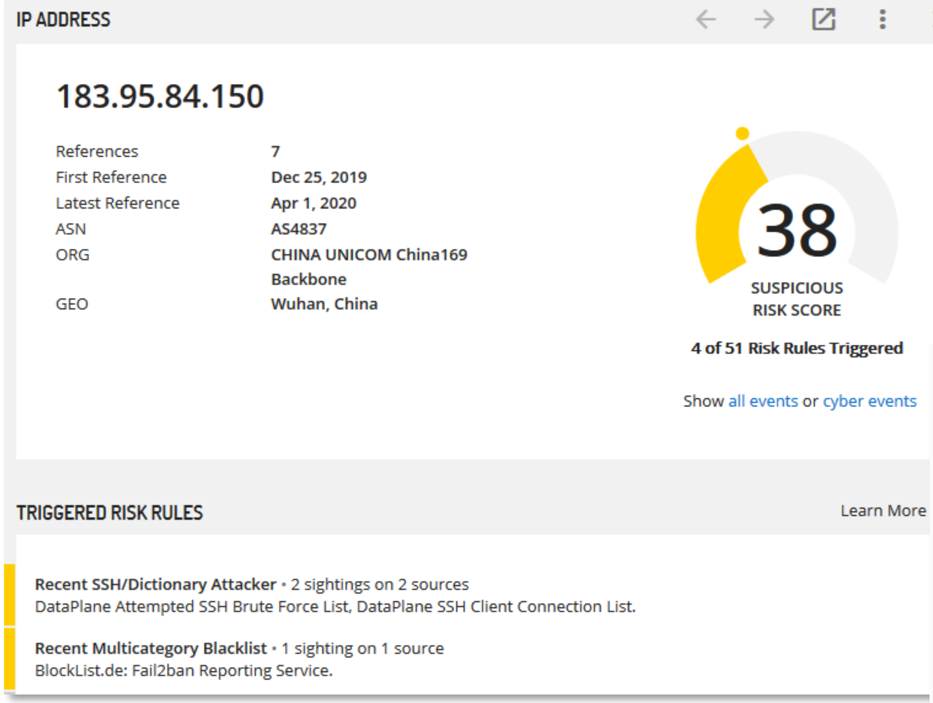
Notable EventID:
97EA0AD289

Client IP:
[redacted]

Trigger:
183.95.84.150

On **April 6th, 2020** between **03:39:23.900 UTC** and **05:15:07.600 UTC** the RuleGATE identified 14 allowed inbound events from the triggering IP to the client IP. These events were observed establishing a full TCP connection and were seen transferring anywhere from **111 to 361 packets per event, indicating that an authenticated session existed**. Unsuccessful SSH brute forcing events are expected to have less than 20 packets, as SSH servers terminate connections after three invalid logins. The extended packet counts, and matching threat intelligence are suspicious and deserve further investigation.

The triggering IP is **well known for brute forcing attacks across the Internet** (Figs. 1 & 2). There are reports on AbuseIPDB as recent as three hours ago stating that this IP is continuing to brute force connections. The combination of suspicious packet counts and known intelligence for the triggering IP suggests that there may have been unauthorized SSH logins.



IP ADDRESS

183.95.84.150

References	7
First Reference	Dec 25, 2019
Latest Reference	Apr 1, 2020
ASN	AS4837
ORG	CHINA UNICOM China169 Backbone
GEO	Wuhan, China

38
SUSPICIOUS
RISK SCORE

4 of 51 Risk Rules Triggered

Show all events or cyber events

TRIGGERED RISK RULES

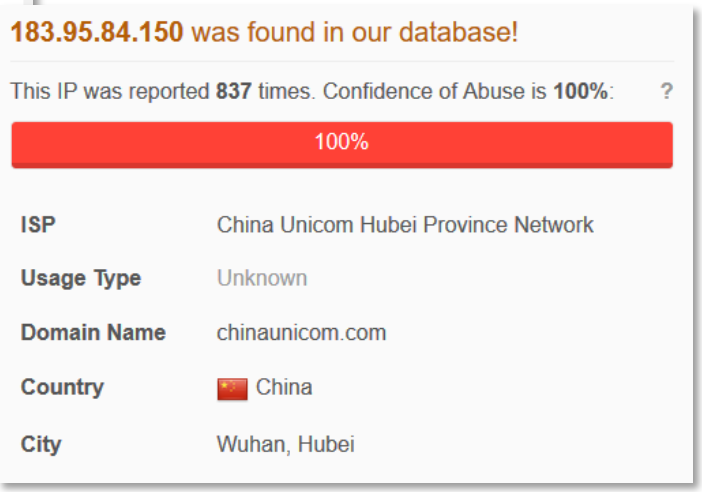
Learn More

Recent SSH/Dictionary Attacker • 2 sightings on 2 sources
DataPlane Attempted SSH Brute Force List, DataPlane SSH Client Connection List.

Recent Multicategory Blacklist • 1 sighting on 1 source
BlockList.de: Fail2ban Reporting Service.

Fig 1 | **Recorded Future analysis of the triggering IP**

Fig 2 | **AbuseIPDB analysis of the triggering IP**



183.95.84.150 was found in our database!

This IP was reported **837** times. Confidence of Abuse is **100%**: ?

100%

ISP	China Unicom Hubei Province Network
Usage Type	Unknown
Domain Name	chinaunicom.com
Country	China
City	Wuhan, Hubei

CENTRIPETAL RECOMMENDATIONS | **Promote the matching policy to shielding. Check authentication logs for unauthorized logins. Change passwords for compromised accounts.**

ATD Event — TOR Traffic Identified

Classification:
TOR
Bad Web Traffic
Potential Infection (TorBot)

Matching Policies:
TOR-Active_Relays_24_Hours-md

Observed Risk:
HIGH

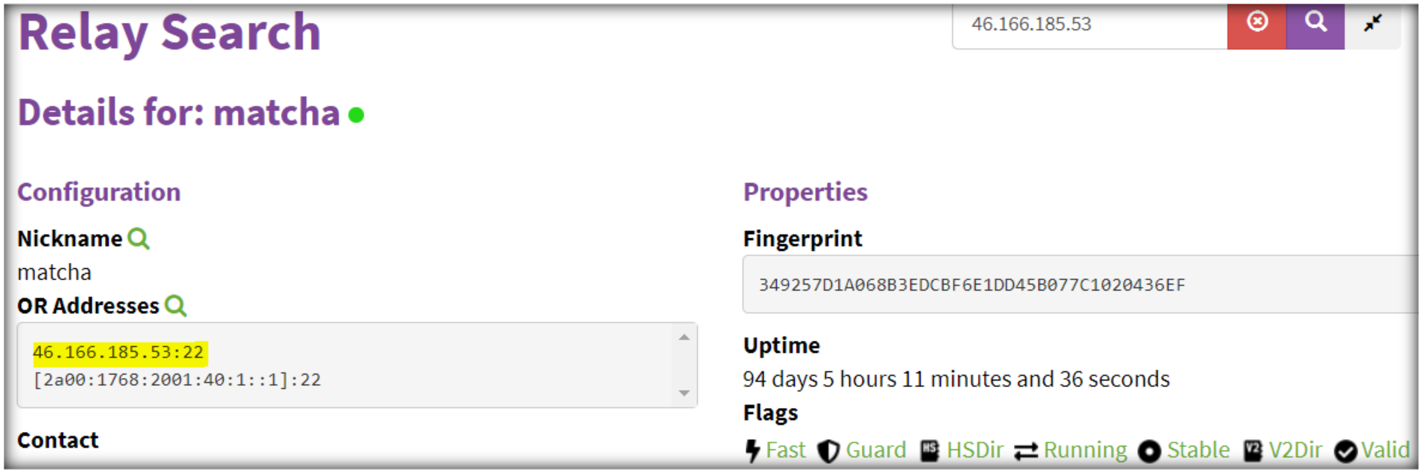
Notable EventID:
97E9C7A570

Client IPs:
XX.XX.XX.XX

Trigger:
95.216.118.16:**4223**
46.28.207.107:**443**
46.166.185.53:**22**

Starting at 11:59am on Thursday March 12th and continuing until the last event on Friday March 13th at 7:57pm, the RuleGATE observed **49 events of bi-directional traffic** from the listed client IPs to the listed TCP socket combinations. Analysis of the TCP handshakes as well as domain information in the event show **full sessions were established**. The triggering IPs are known to be active TOR relays within 24 hours of detection, which Centripetal has verified against at least one other list (Fig 1). When inspected in VirusTotal the triggering IPs have **several recent records** of malicious Windows executables communicating, including generic **trojan downloaders** and **Win32/TorBot**.

TOR is frequently abused by malicious actors to perform command and control functions, and by users inside the enterprise to circumvent web content filtering and other security measures. It is **typically prohibited in enterprise environments**.



Relay Search

46.166.185.53

Details for: matcha ●

Configuration

Nickname
matcha

OR Addresses

```
46.166.185.53:22
[2a00:1768:2001:40:1::1]:22
```

Contact

Properties

Fingerprint

```
349257D1A068B3EDCBF6E1DD45B077C1020436EF
```

Uptime
94 days 5 hours 11 minutes and 36 seconds

Flags
Fast Guard HSDir Running Stable V2Dir Valid

Fig 1 | **Relay Verified at TorProject.org**

Table 1 | **Top 10 Domains Recorded**

Day	Time (EST)	Source IP	Dest. IP	Port	Domain
3/12/2020	11:59:29	*[Redacted]*	46.28.207.107	443	www.xxvzaulovgbc4k3.com
3/12/2020	12:52:29	*[Redacted]*	95.216.118.16	4223	www.5pstkicd7bsrksxd.com
3/12/2020	14:35:29	*[Redacted]*	46.28.207.107	443	www.36fucus62nqyose7gl2g3e.com
3/12/2020	16:05:29	*[Redacted]*	95.216.118.16	4223	www.e4yttwols.com
3/12/2020	17:24:29	*[Redacted]*	95.216.118.16	4223	www.5x6zib7pvo5m.com
3/12/2020	19:29:29	*[Redacted]*	46.28.207.107	443	www.2vb7qrj.com
3/12/2020	20:08:35	*[Redacted]*	46.166.185.53	22	www.hol4vrnzdo.com
3/12/2020	20:09:29	*[Redacted]*	46.28.207.107	443	www.kjepi27kg25rh4.com
3/12/2020	20:50:29	*[Redacted]*	95.216.118.16	4223	www.tmia5sj2ey45ibd2sf7p2eh.com
3/12/2020	22:24:29	*[Redacted]*	46.166.185.53	22	www.s7qcm.com

CENTRIPETAL RECOMMENDATIONS | Promote the matching policy to Shielding. Identify the internal host and run a full AV scan.

ATD Event — Internal Hosts Participating in Possible Botnet C2

Classification:
Command and Control
Potential Botnet Infection

Matching Policies:
ThreatSTOP-BOTNET2E_block-ip
XF-Bots_Block-ip
14 Others

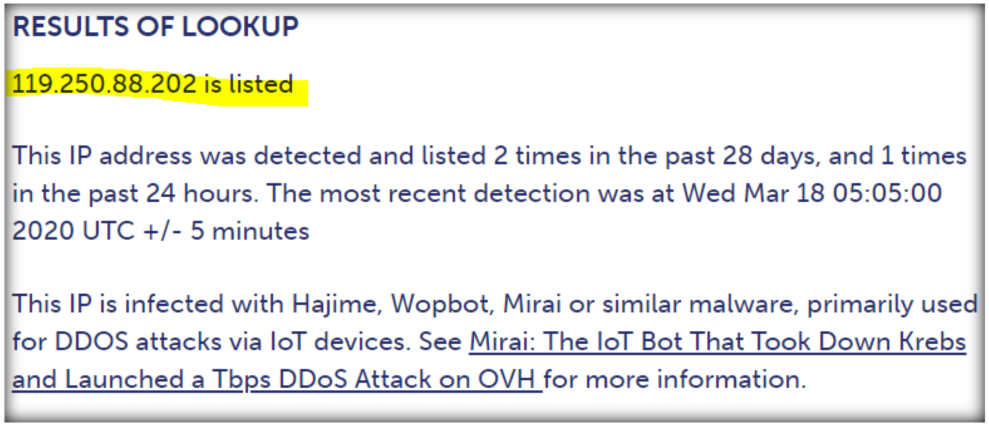
Observed Risk:
HIGH

Notable EventID:
97E9CE91C9
97E9C91345

Client IPs:
10.59.82.162
10.64.28.9
10.76.89.1
10.76.89.2
10.76.89.3
10.76.89.5
10.76.89.7

Trigger:
95.171.210.66:**26881**
584 Other Unique IPs

Since installation, the RuleGATE has observed 5,371 events of unsolicited outbound traffic on **TCP and UDP ports 26881 and 26882** which fits the profile for ZBot C2. This communication occurs to **known botnet hosts** in seventeen threat intelligence feeds and forty-eight different countries including Tanzania, Niger, Vietnam, Venezuela and others. The triggering IPs are in threat intelligence for observed botnet activity such as service scanning, SSH brute forcing, and emitting spam. Approximately **85% of all outbound TCP communications** are blocked by the client firewall; one of these blocked hosts Centripetal identified as a **compromised HikVision DVR** (See red trigger in table 1). **Successfully established sessions were detected by Geo only**, with the triggering IPs not being in any sort of threat intelligence, blacklists, or public abuse reports.



RESULTS OF LOOKUP

119.250.88.202 is listed

This IP address was detected and listed 2 times in the past 28 days, and 1 times in the past 24 hours. The most recent detection was at Wed Mar 18 05:05:00 2020 UTC +/- 5 minutes

This IP is infected with Hajime, Wopbot, Mirai or similar malware, primarily used for DDOS attacks via IoT devices. See Mirai: The IoT Bot That Took Down Krebs and Launched a Tbps DDoS Attack on OVH for more information.

Fig 1 | **Botnet Tracking from Spamhaus CBL for triggering IP**

Trigger	Blacklists	Abuse Reports	Known Botnet	Event Count
124.236.56.233	4	11	Yes	11
221.194.160.35	3	4	Yes	9
119.250.88.202	3	12	Yes	8
101.20.221.136	2	10	Yes	7
101.230.193.200	2	6 (aged)	Yes	7
103.17.213.98	5	179	Yes	7
113.160.117.28	6	1	Yes	7
117.187.12.126	5	1,922	Yes	7
125.234.116.6	2	0	No	7
49.231.5.82	0	1	No	7

Table 1 | **Threat Intelligence Stats for Top 10 Destination IPs Port 26881 and 26882 Traffic**

CENTRIPETAL RECOMMENDATIONS | Promote the matching policy to Shielding. Allow Centripetal to pull PCAP, if available. Identify the internal host and run a full AV scan.

ATD Event —Partial Indicator Identifies Potential Ransomware

Classification:
Potential Ransomware Command and Control

Matching Policies:
ET-CnC_Block-fqdn

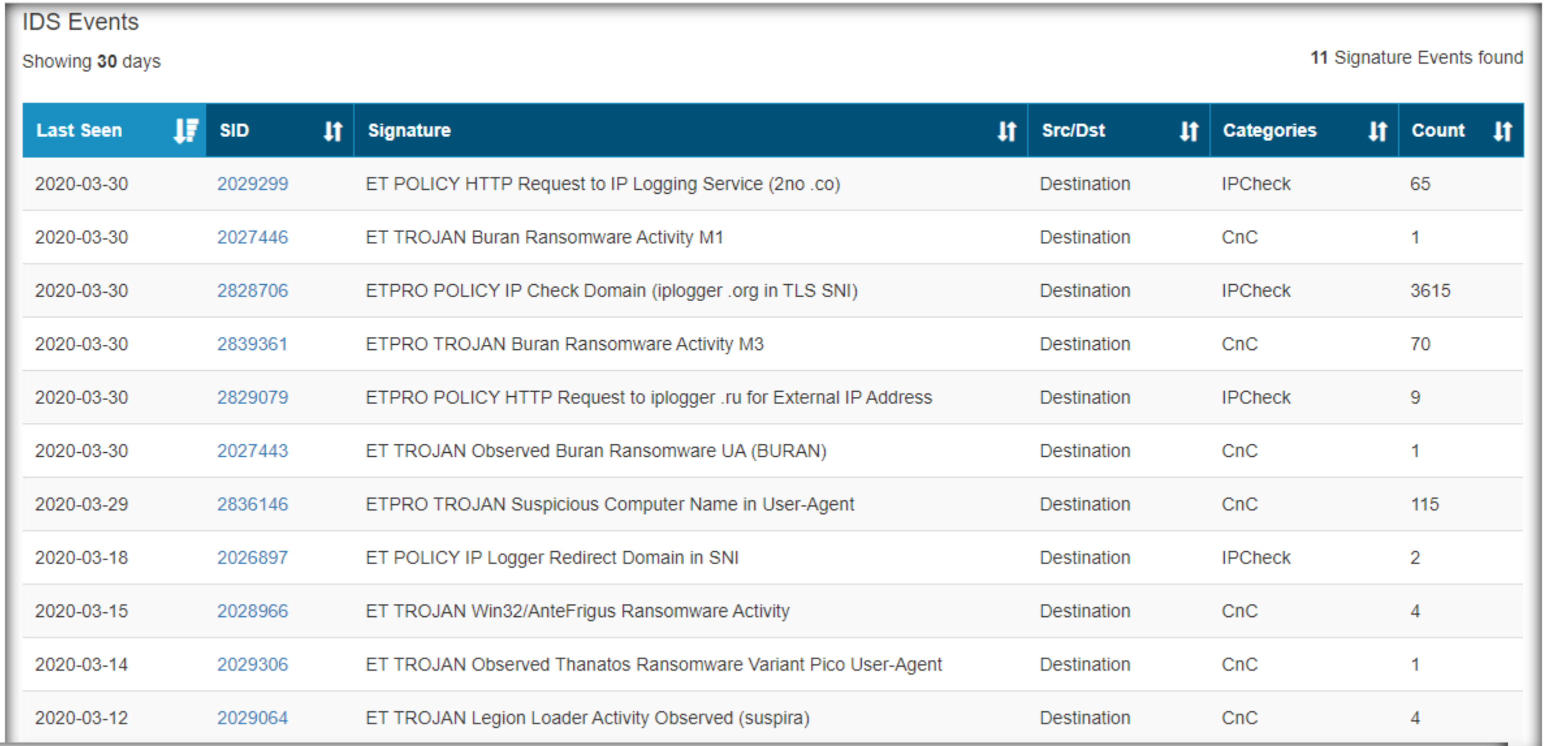
Observed Risk:
HIGH

Notable EventIDs:
97E9EDB0B8
97E9EDB0B9

Client IPs:
10.56.92.11

Trigger:
IPLogger[.]org

On **Thursday March 26th at 10:51:26.400am EST**, the RuleGATE observed an outbound session between the listed client IP and triggering domain on TCP port 443. This traffic represents an aberration against the site baseline as this service has **never been previously contacted.** The triggering domain is listed by threat intelligence partner Emerging Threats as being observed in **IDS hits for several ransomware family C2 activity**. Pivoting to other intelligence shows that **Recorded Future's threat hunting group, Insikt, released a flash report** based on research from ThreatPost and LastLine Security which also lists the triggering domain as an IoC for a new variant of Paradise Ransomware's C2[1, 2].



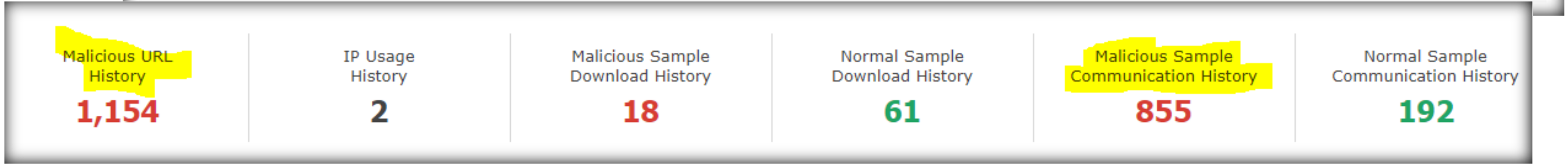
IDS Events

Showing **30** days

11 Signature Events found

Last Seen	SID	Signature	Src/Dst	Categories	Count
2020-03-30	2029299	ET POLICY HTTP Request to IP Logging Service (2no .co)	Destination	IPCheck	65
2020-03-30	2027446	ET TROJAN Buran Ransomware Activity M1	Destination	CnC	1
2020-03-30	2828706	ETPRO POLICY IP Check Domain (iplogger .org in TLS SNI)	Destination	IPCheck	3615
2020-03-30	2839361	ETPRO TROJAN Buran Ransomware Activity M3	Destination	CnC	70
2020-03-30	2829079	ETPRO POLICY HTTP Request to iplogger .ru for External IP Address	Destination	IPCheck	9
2020-03-30	2027443	ET TROJAN Observed Buran Ransomware UA (BURAN)	Destination	CnC	1
2020-03-29	2836146	ETPRO TROJAN Suspicious Computer Name in User-Agent	Destination	CnC	115
2020-03-18	2026897	ET POLICY IP Logger Redirect Domain in SNI	Destination	IPCheck	2
2020-03-15	2028966	ET TROJAN Win32/AnteFrigus Ransomware Activity	Destination	CnC	4
2020-03-14	2029306	ET TROJAN Observed Thanatos Ransomware Variant Pico User-Agent	Destination	CnC	1
2020-03-12	2029064	ET TROJAN Legion Loader Activity Observed (suspira)	Destination	CnC	4

Fig 1 | **ET IDS Hits for Triggering Domain**



Malicious URL History	IP Usage History	Malicious Sample Download History	Normal Sample Download History	Malicious Sample Communication History	Normal Sample Communication History
1,154	2	18	61	855	192

Fig 2 | **Saint Security observations for Triggering Domain**

CENTRIPETAL RECOMMENDATIONS | Promote the matching policy to Shielding. Identify the internal host and run a full AV scan.

[1] https://www.lastline.com/labsblog/iqy-files-and-paradise-ransomware/
[2] https://threatpost.com/variant-of-paradise-ransomware-targets-office-iqy-files/153559/

ATD Event — Observed BitTorrent Activity

Classification:
Brute Forcing
Reconnaissance

Matching Policies:
Emerging Threats P2P Block IP

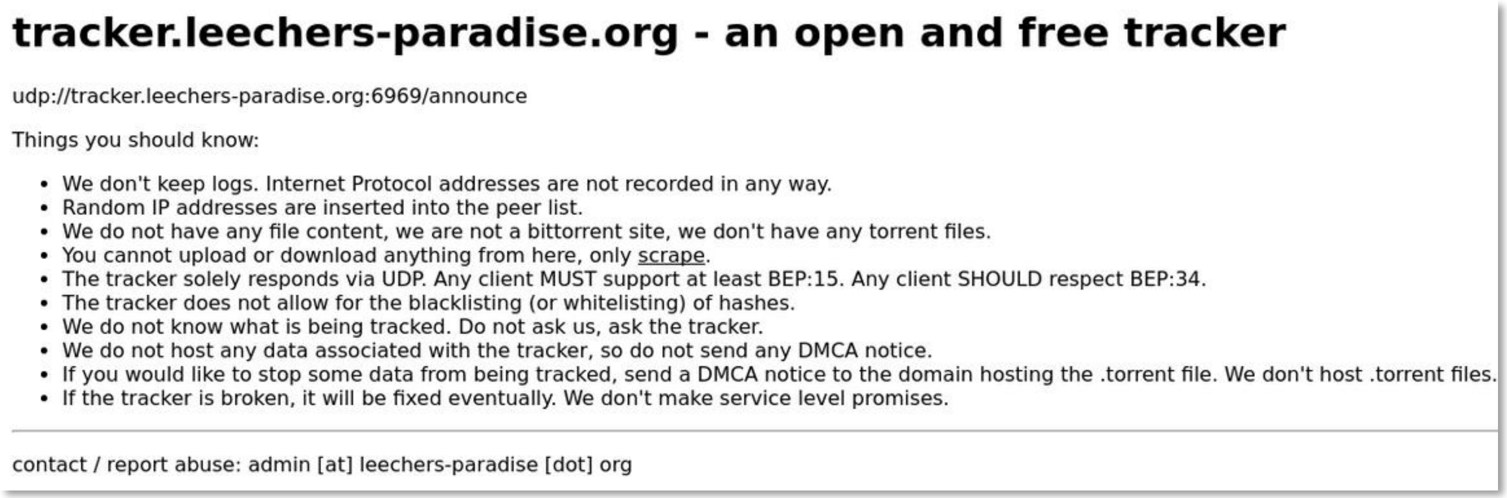
Observed Risk:
HIGH

Last EventIDs:
97E9D961AF

Client IP:
10.46.21.25
10.56.82.2
10.56.12.5
10.56.11.1

Trigger:
188.241.58.209
102.68.77.114
41.50.49.154
and 189 more

Between 2:19pm and 3:27pm EST on Thursday, March 19th the RuleGATE identified 27,294 allowed outbound events from the Client IPs to the triggering IPs. The triggering IPs are known as Peer to Peer hosts and are geo-located in **Romania, South Africa, and Kenya**. The activity was observed communicating on several different ports, with **6969 and 6881 being the most prominent**. Counter intel and open source research show that these triggering IPs are well-known for hosting BitTorrent activity (Fig. 1). Additionally, this activity showed a significant spike in event volume over this hour-long period, indicating unusual or anomalous activity (Fig. 2). **Over 97% of the traffic came from host** 10.46.21.25, while the rest of the hosts were observed only with a handful of events.



tracker.leechers-paradise.org - an open and free tracker

udp://tracker.leechers-paradise.org:6969/announce

Things you should know:

- We don't keep logs. Internet Protocol addresses are not recorded in any way.
- Random IP addresses are inserted into the peer list.
- We do not have any file content, we are not a bittorrent site, we don't have any torrent files.
- You cannot upload or download anything from here, only scrape.
- The tracker solely responds via UDP. Any client MUST support at least BEP:15. Any client SHOULD respect BEP:34.
- The tracker does not allow for the blacklisting (or whitelisting) of hashes.
- We do not know what is being tracked. Do not ask us, ask the tracker.
- We do not host any data associated with the tracker, so do not send any DMCA notice.
- If you would like to stop some data from being tracked, send a DMCA notice to the domain hosting the .torrent file. We don't host .torrent files.
- If the tracker is broken, it will be fixed eventually. We don't make service level promises.

contact / report abuse: admin [at] leechers-paradise [dot] org

Fig 1 | AbuseIPDB analysis of a triggering IP

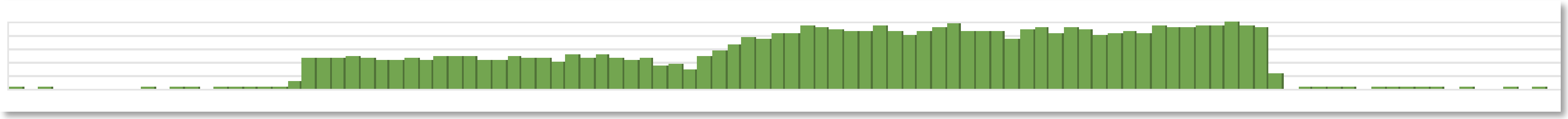


Fig 2 | Timechart showing large spike of events

CENTRIPETAL RECOMMENDATIONS | Promote matching policy to shielding, scan hosts with A/V.

About Centripetal

Centripetal is dedicated to protecting organizations from advanced threats by operationalizing intelligence-driven security. Centripetal delivers the market's only patented Threat Intelligence Gateway platform to customers via its CleanINTERNET solution, a comprehensive intelligence-led cyber service. With Centripetal, customers across every vertical and of every size can persistently prevent over 90% of known threats with applied threat intelligence, rapid correlation and automated enforcement of millions of IOC policies against live network traffic with live cyber analyst support.

Centripetal

centripetalnetworks.com

© 2019 Centripetal Networks, Incorporated. All rights reserved. Centripetal, all Centripetal logos, CleanINTERNET, QuickTHREAT, RuleGATE, and ACT are trademarks or registered trademarks of Centripetal Networks in the United States and/or other countries. All other brands, products, or trademarks are the property of their respective owners. This product / solution is subject to one or more U.S. or non-U.S. patents