Summary of Coverage:

Black Lotus Labs Discovers ZuoRAT – a new malware targeting home routers

Release date: June 28, 2022

Overview

On Tuesday, June 28, 2022, Black Lotus Labs issues a press release to announce a research blog detailing the discovery of ZuoRAT, a highly complex remote access trojan that targets home routers and appears to be the work of a nation-state actor.

The project team responsible for producing and publicizing this blog includes:

- Danny Adamitis – Principal Security Researcher
- Suzanne Dawe – Senior Lead PR Manager
- Mark Dehus – Director, Black Lotus Labs
- Elizabeth Green – Sr. Project Manager, Marketing
- Michelle Lee – Director, Black Lotus Labs
- Kaitlyn McIntyre – Senior Lead Marketing Manager
- Stephanie Walkenshaw – Lead Security Professional

The data in this report are current as of July 13.

Quick Numbers

- 17,064 blog views
- 5,859 press release views
  - 64 views from credentialed journalists using PR Newswire for Journalists
  - 111 views on prnewswire.com from identifiable organizations (based on IP addresses)
- 14,945 click-throughs from the press release to:
  - ZuoRAT blog – 4,913
  - Lumen newsroom – 1,977
  - Konni blog – 1,798
  - ReverseRAT blog – 1,784

Media Outreach

- We offered the blog under embargo[1] to 29 journalists and it was accepted by:
  - CNN, Cyberwire, Hacker News, HelpNet Security, Reuters, SC Magazine and Zero Day.
- Interdependence PR pitched an additional 47 journalists after the release crossed the wire.
- We responded to several media inquiries including:
  - Written questions from ArsTechnica, Dark Reading, the Hacker News and Tech Republic
  - Phone interviews with Fierce Telecom and Decipher
  - Podcast recording for RiskyBiz

Media Placements

- Media relations efforts for this blog were the **most successful to date** for Black Lotus Labs.
- We had **330 exact matches** of the press release that ran on outlets such as Yahoo Finance, AP News, etc. These outlets have a **combined reach of 217 million**.
- As of July 13, the outreach generated **67 unique articles** in English. (Jump to the full list.)
  - A search for news articles that include the term “ZuoRAT” (which did not exist before June 28) yields 11,000 results.

[1] When journalists accept an embargo, we provide the content several days before the publication date, and they agree not to run the story until our release crosses the wire. The purpose is to give journalists time write the story in advance so it’s ready to publish at the time of the release.

- The ZuoRAT story ran worldwide in **more than 25 languages** including Arabic, Bengali, Bulgarian, Chinese, Czech, Danish, Dutch, Filipino, Finnish, French, German, Greek, Gujarati, Hindi, Indonesian, Italian, Japanese, Korean, Norwegian, Polish, Portuguese, Russian, Spanish, Swedish, Tamil and Vietnamese.

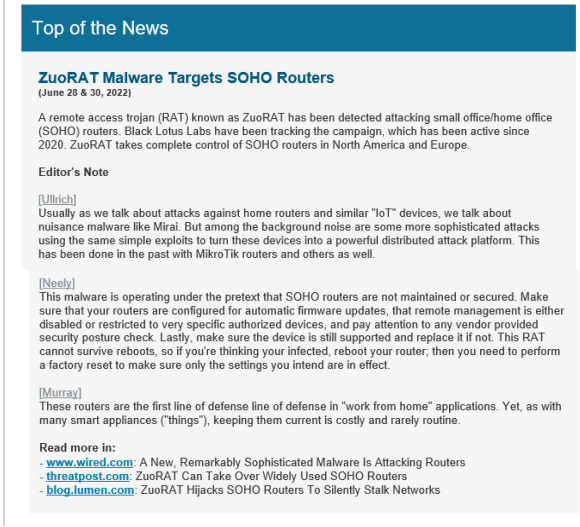
Notable placements/mentions

- Apple News ran the TechSpot story in its feed: https://apple.news/AKRw6UKAvSnGHh1zRVRj03w
- General interest publications that covered ZuoRat include Mashable and Wired
- All the major security publications covered the research including ArsTechnica, Bleeping Computer, CyberWire, Dark Reading, Hacker News, HelpNet Security, Malware Bytes, the Register, SANS News Bites, SC Magazine, Security Week, ThreatPost, ZDNet
- MentalOutlaw's YouTube overview has 218,000 views
- Danny Adamitis recorded for the RiskyBiz podcast (the oldest and one of the top security podcasts)
- ZuoRAT was the subject line and top story in two of the leading security newsletters:

The Hacker News – June 29

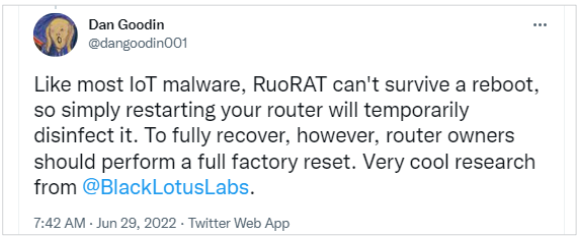


SANS News Bites – July 8

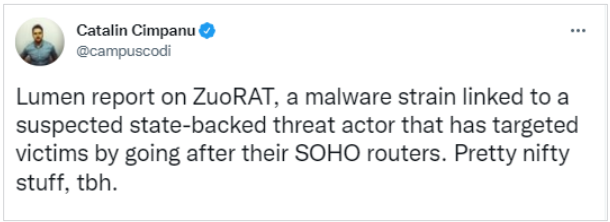


- Most journalists and/or their publications tweeted the ZuoRAT stories.
  - Dan Goodin (ArsTechnica) called ZuoRAT "the most important IoT discovery since 2018" and "very cool research from @BlackLotusLabs"





  - Catalin Cimpanu (RiskyBiz) said the research is "pretty nifty stuff, to be honest"



Questions

For questions or comments about this report, please contact Suzanne Dawe.

Appendix A: Full list of unique media placements

Publication	Link	Date
AI Tech Park	Black Lotus Labs discovers remote access trojan (RAT) called ZuoRAT	28-Jun
ArsTechnica	A wide range of routers are under attack by new, unusually sophisticated malware	28-Jun
Bleeping Computer	New ZuoRAT malware targets SOHO routers in North America, Europe	28-Jun
Cyber Physical-Systems Virtual Organization	Researchers Uncover ZuoRAT Malware Targeting Home-Office Routers	28-Jun
fCybrary	CTIG Coverage of Black Lotus Labs' ZuoRAT Report	28-Jun
Helpnet Security	Researchers uncover ZuoRAT malware targeting home-office routers	28-Jun
MSSP Alert	Hackers use remote access trojan to target home office routers	28-Jun
NewsBoardforMe	Researchers discover ZuoRAT malware aimed at home office routers	28-Jun
NewsPostTalk	ZuoRAT Malware Hijacking Home-Office Routers to Spy on Targeted Networks	28-Jun
RiskyBiz newsletter	APTs and cyber-espionage	28-Jun
Security Affairs	ZuoRAT malware hijacks SOHO Routers to spy on victims	28-Jun
The Cybersecurity News	ZuoRAT Malware Hijacking Home-Office Routers to Spy on Targeted Networks	28-Jun
The Hacker News	ZuoRAT Malware Hijacking Home-Office Routers to Spy on Targeted Networks	28-Jun
The Tech Outlook	A new multistage remote access trojan ZuoRAT has been targeting SOHO routers in North America and Europe	28-Jun
2-spyware	A multistage ZuoRAT has been targeting a wide range of SOHO routers	29-Jun
CyberIntelMag	Home-Office Routers Hijacked by ZuoRAT Malware to Sneak on Specific Networks	29-Jun
CyberWire	SOHO routers under attack.	29-Jun
Dark Reading	ZuoRAT Hijacks SOHO Routers from Cisco, Netgear	29-Jun
Decipher	ZUORAT MALWARE FOUND HITTING HOME ROUTERS	29-Jun
Fierce Telecom	Lumen says Cisco, Netgear routers could be targets for newly discovered malware	29-Jun
Silicon Angle	New 'ZuoRAT' malware targets routers in Europe and North America	29-Jun
ZDNet	This sophisticated malware is targeting routers to break into networks	29-Jun
PC Perspective	THERE MIGHT BE A ZUORAT IN YOUR SOHO ROUTER, INFECTING YOUR MACHINES	29-Jun
SOC Prime	ZuoRAT Malware Detection	29-Jun
Broadcom	ZuoRAT Hijacking SOHO Routers	29-Jun
RIskyBiz podcast	RiskyBiz podcast	29-Jun
TechSpot	Routers from Asus, Netgear, and Cisco are being targeted by a sophisticated malware campaign	29-Jun
Techzine	A new, highly sophisticated malware strain threatens various routers	29-Jun
Digital Trends	Oh great, new malware lets hackers hijack your Wi-Fi router	30-Jun
IT News	Sophisticated ZuoRAT attack targets home workers	30-Jun
Malware Bytes	ZuoRAT is a sophisticated malware that mainly targets SOHO routers	30-Jun
ReviewGeek	New ZuoRAT Malware Attacks Routers and Hijacks Connected Devices	30-Jun
Schneier on Security	ZuoRAT Malware Is Targeting Routers	30-Jun
Secure Team	ZuoRAT Malware Targets Home-Office Routers	30-Jun
Integral Defense	ZuoRAT Malware Hijacking Home-Office Routers to Spy on Targeted Networks	30-Jun
Planet Concerns	Hackers are hijacking Wi-Fi routers with zuoRAT malware	30-Jun
Free Digital Spirit	ZuoRAT hijacks SOHO routers from Cisco, Netgear	30-Jun
Mashable	A new trojan malware, ZuoRAT, is hijacking home-office routers: Report	30-Jun

Mental Outlaw (YouTube)	ZuoRAT Malware is Infecting Routers and Taking Over Entire Networks	30-Jun
SC Magazine	ZuoRAT targets home-office routers in Europe and North America	30-Jun
Security Week	SOHO Routers in North America and Europe Targeted With 'ZuoRAT' Malware	30-Jun
Tech Radar	Attackers are infiltrating routers to take control of connected devices	30-Jun
Tech Republic	SOHO routers used as initial point of compromise in stealth attack campaign	30-Jun
Threat Post	ZuoRAT Can Take Over Widely Used SOHO Routers	30-Jun
Wired	A New, Remarkably Sophisticated Malware Is Attacking Routers	30-Jun
ESecurityPlanet	Highly Sophisticated Malware Attacks Home and Small Office Routers	1-Jul
InfoSec Today	ZuoRAT Can Take Over Widely Used SOHO Routers	1-Jul
OodaLoop	SOHO routers used as initial point of compromise in stealth attack campaign	1-Jul
HiTech Wiki	Do you have your own WiFi router? Dangerous malware is spreading	2-Jul
HT Tech	Wifi routers getting hacked with complicated malware. Here's how to stay safe	2-Jul
Swords Today	Security Warning ZuorAT, A New Sophisticated Malware, Steals Data Through Wi-Fi Routers.	2-Jul
ITIGC	ZuoRAT, the malware that has hijacked thousands of routers	2-Jul
The Register	Google location tracking to forget you were ever at that medical clinic ... and more	2-Jul
Information Security Buzz	ZuoRAT Malware Targets SOHO Routers In North America, Europe – Expert Comment	3-Jul
This Week in Security	Routers under attack by unusually sophisticated malware (Zack Whittaker)	3-Jul
CyberDaily	Home office routers are being used by the malware ZuoRAT to spy on specific networks	4-Jul
Cyware	ZuoRAT Malware with Hallmarks of a State-Backed Threat Actor	5-Jul
TWiT (This week in tech Vlog)	The ZuoRAT	5-Jul
Gibson Research	The ZuoRAT	5-Jul
Security Boulevard	What is ZuoRAT?	6-Jul
Allot	What is ZuoRAT?	6-Jul
ID Strong	ZuoRAT Capable of Overtaking SOHO Routers	6-Jul
IT Security Wire	ZuoRAT Malware, State-Backed Threat Actor Targeting SOHO Routers	6-Jul
SANS News Bites	ZuoRAT Malware Targets SOHO Routers	8-Jul
Secure Zoo	ZuoRAT targets SOHO devices to launch sophisticated multi-stage cyber attacks	8-Jul
Titan Tech	Malware Highlight: ZuoRAT	9-Jul
CompCiti	A Complex Hacking Group: ZuoRAT Malware Attacks SOHO Routers	11-Jul