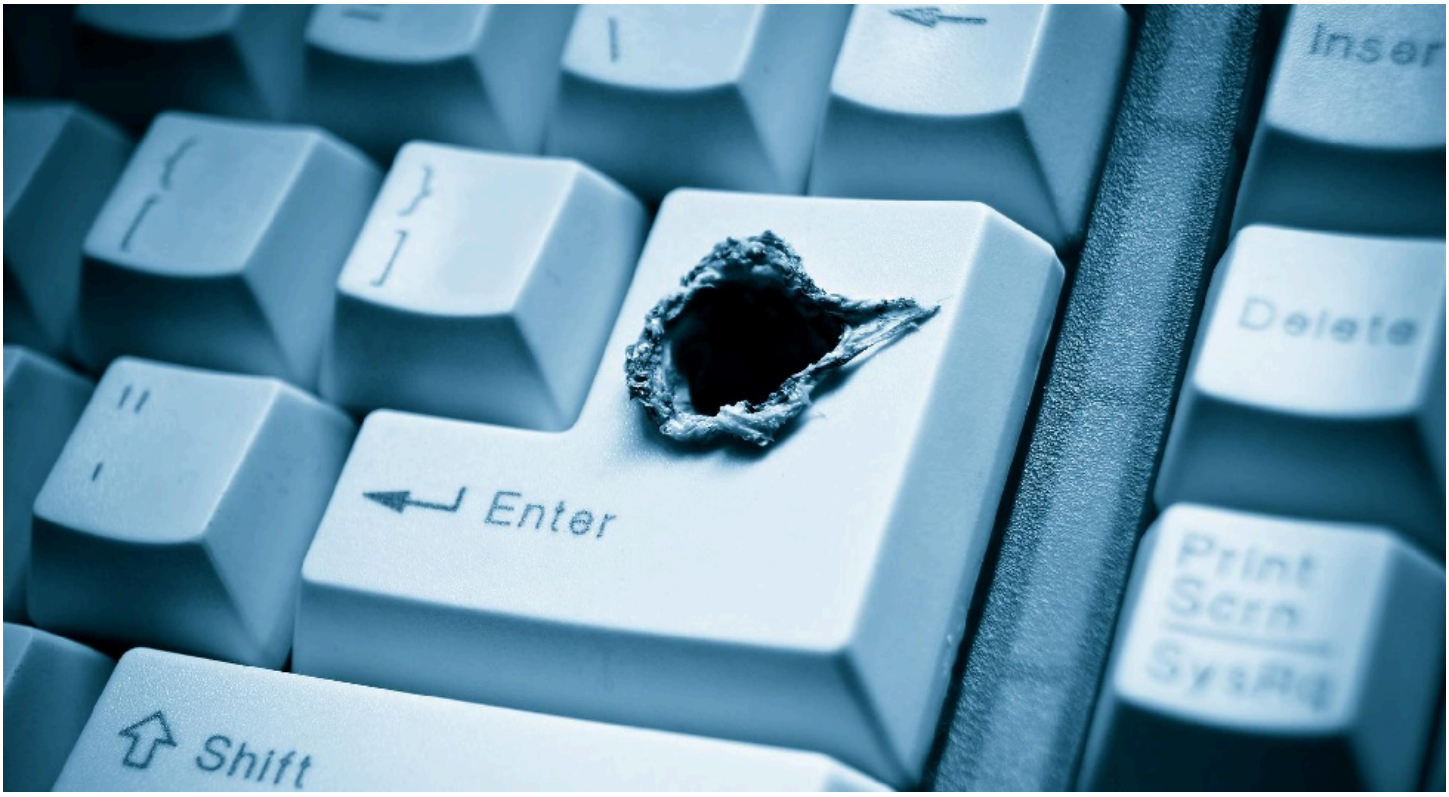
# Unknown Title

⋮ 10/8/2025




Cyber Threats

# RondoDox: From Targeting Pwn2Own Vulnerabilities to Shotgunning Exploits

Trend™ Research and ZDI Threat Hunters have identified a large-scale RondoDox botnet campaign exploiting over 50 vulnerabilities across more than 30 vendors, including flaws first seen in Pwn2Own contests.

By: Deep Patel, Ashish Verma, Simon Dulude, Peter Girnus October 09, 2025 Read time: 9 min (2515 words)

**Key takeaways**

- The campaign exposes organizations to the risks of data exfiltration, persistent network compromise, and operational disruption for organizations with exposed infrastructure.

- Organizations operating internet-facing network devices are at heightened risk. Active exploitation has been observed globally since mid-2025, with several CVEs now included in CISA's Known Exploited Vulnerabilities (KEV) catalog.
- Prioritize patching of all listed vulnerabilities, especially those in the KEV catalog. Conduct regular vulnerability assessments, segment networks to limit lateral movement, and continuously monitor devices for anomalous activities. Trend Micro solutions already provide protection against vulnerabilities and flaws exploited in this campaign, helping organizations mitigate exposure while patching efforts are underway.

The Trend Zero Day Initiative™ (ZDI) Threat Hunting and Trend™ Research teams have identified a significant RondoDox botnet campaign that targets a wide range of internet-exposed infrastructure. This campaign consists of over 50 exploits, including unpatched router flaws across over 30 vendors, targeting vulnerabilities found in routers, digital video recorders (DVRs), network video recorders (NVRs), CCTV systems, web servers, and various other network devices. While the exploits specifically exploit vulnerabilities in routers, DVRs, NVRs, CCTV systems, web servers, and networking equipment, the latest RondoDox campaign uses an "exploit shotgun", using multiple exploits and seeing what hits.

# From Pwn2Own to active in-the-wild exploitation

Our first RondoDox intrusion attempt began on June 15, 2025, when we identified a familiar vulnerability from our Pwn2Own Toronto event. This vulnerability, tracked as CVE-2023-1389, targets the WAN interface of the TP-Link Archer AX21 Wi-Fi router.

We previously reported on a Mirai campaign that exploited CVE-2023-1389 back in 2023, shortly after the Pwn2Own event. Vulnerabilities presented at our Pwn2Own consumer event continue to be popular with botnet operators.

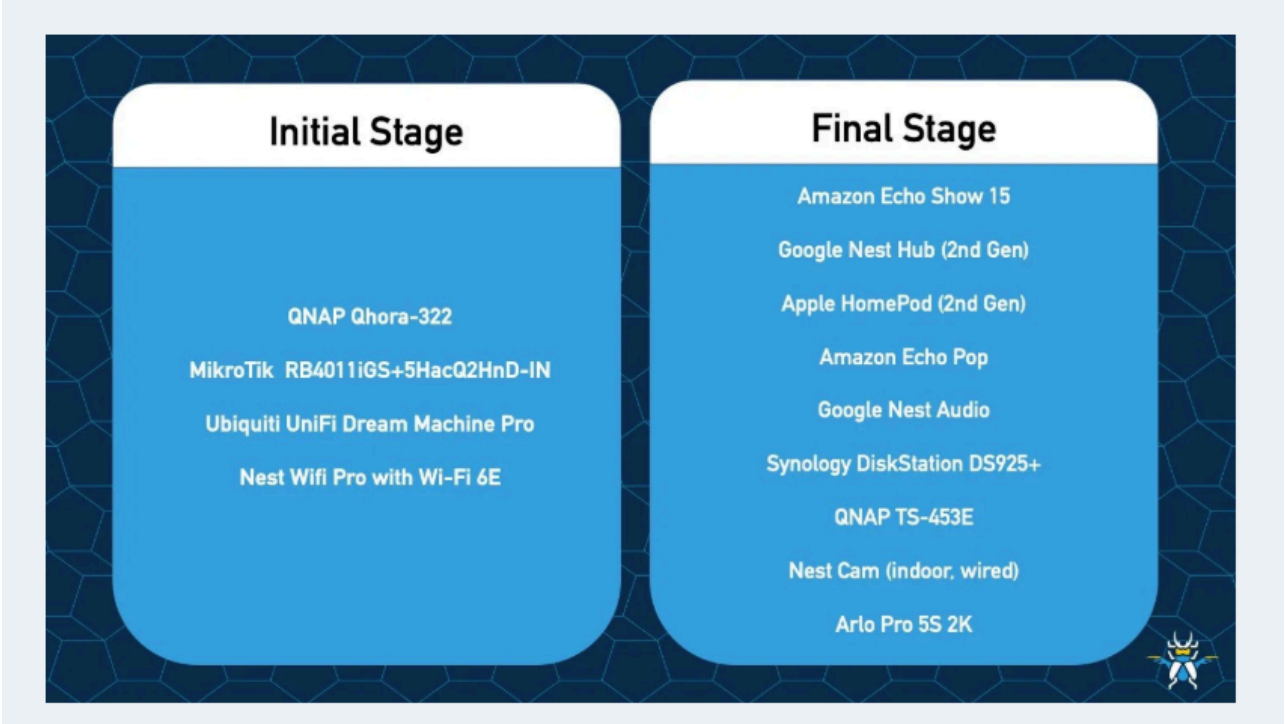



Figure 1. Pwn2Own Ireland target list in the SOHO Smashup event including multiple networking devices
download

Trend customers can be reassured that they have been protected against vulnerabilities like CVE-2023-1389 since it was disclosed at Pwn2Own.

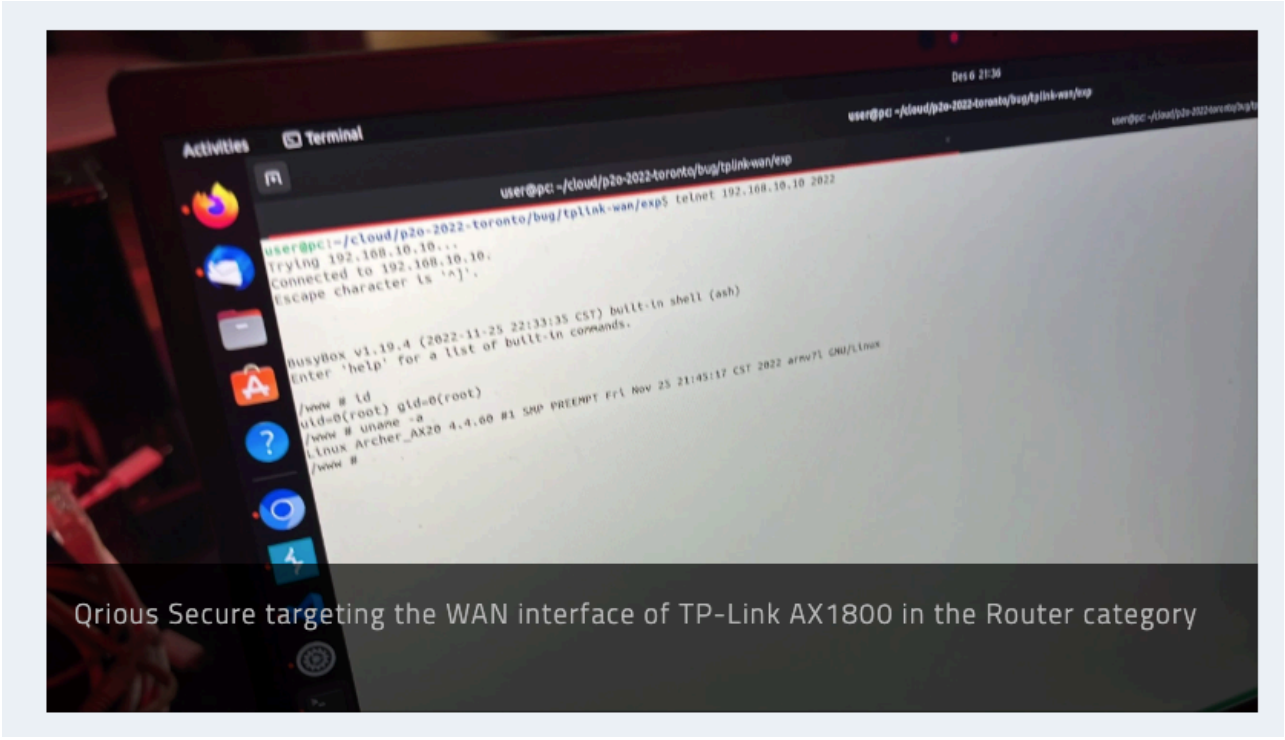



Figure 2. Tri Dang and Bien Pham (@bienpnn) from Qrious Secure were able to exploit two bugs (authentication bypass and command injection) at Pwn2Own Toronto 2022
download

# RondoDox background: a new botnet emerges

RondoDox first surfaced publicly in mid-2025 as a stealthy botnet campaign that weaponizes longstanding command-injection flaws in internet-facing routers, DVRs, NVRs, CCTV systems, and other networking equipment to gain shell access and, ultimately, to drop multiarchitecture payloads. The initial RondoDox analysis authored by FortiGuard Labs highlighted an initial campaign, which focused on TBK DVRs and Four-Faith routers, through the exploitation of CVE-2024-3721 and CVE-2024-12856.

More recently, RondoDox broadened its distribution by using a "loader-as-a-service" infrastructure that co-packages RondoDox with Mirai/Morte payloads — making detection and remediation more urgent.

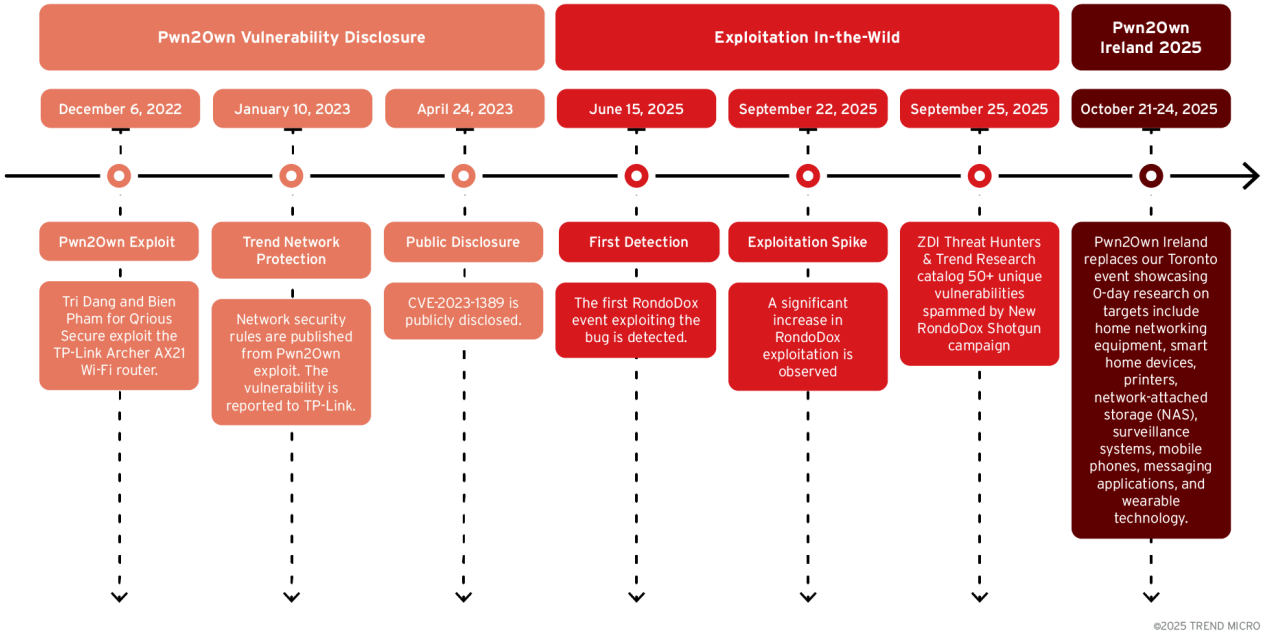



Figure 3. A timeline of the RondoDox vulnerability, from initial disclosure and first detection in 2025 to eventual widespread exploitation in large-scale campaigns
download

Below is the timeline showing key events in the RondoDox vulnerability, from discovery to exploitation:

- **December 6, 2022:** Tri Dang and Bien Pham (@bienpnn) from Qrious Secure exploit the WAN interface of TP-Link AX1800 at Pwn2Own Toronto 2022.
- **January 10, 2023:** Trend Network Security publishes rule 42150: HTTP: TP-Link AX1800 locale controller Command Injection Vulnerability (ZDI-23-451).
- **January 15, 2023:** Pwn2Own vulnerability is reported to TP-Link. Coordinated public disclosure of CVE-2023-1389 with vendor.
- **June 15, 2025:** First RondoDox event detected inside Trend Telemetry utilizing Pwn2Own Toronto 2022 bug, CVE-2023-1389.
- **September 22, 2025**: Trend Threat Research triages a RondoDox exploitation spike inside Trend telemetry.

- **September 25, 2025:** CloudSEK publishes a follow-up showing rapid growth via a loader-as-a-service model that distributes RondoDox alongside Mirai/Morte, with evidence of large-scale, rotated infrastructure.

# Exploit shotgun: RondoDox's expanded arsenal

Building on CVE-2023-1389 and other vulnerabilities, such as CVE-2024-3721 and CVE-2024-12856, RondoDox's expanded arsenal now includes several additional CVEs and exploitation patterns observed in the wild. It's a clear signal that the campaign is evolving beyond single-device opportunism into a multivector loader operation.

Notably, researchers tied the active exploitation of CVE-2024-3721 (TBK DVR) and CVE-2024-12856 (Four-Faith routers) to RondoDox activity, and a subset of the newly observed vulnerabilities was added to CISA's Known Exploited Vulnerabilities (KEV) catalog, elevating them to immediate, high-priority patching targets for defenders.

Below we list the fresh CVEs researchers have seen in RondoDox campaigns, summarizing how each is being weaponized:

**RondoDox targeted vulnerabilities**

- Total Vulnerabilities: 56
- No CVE Assigned: 18
- CVE Assigned: 38
- Command Injection (CWE-78): 50
- Path Traversal (CWE-22): 2
- Buffer Overflow (CWE-120): 1
- Authentication Bypass (CWE-287): 1
- Memory Corruption (CWE-119): 1

| Vendor | Product | CVE ID | CWE | Type |
|---|---|---|---|---|
| D-Link | DNS-343 ShareCenter / goAhead Web Server | N/A | CWE-78 | No CVE |
| TVT | NVMS-9000 Digital Video Recorder (DVR) | N/A | CWE-78 | No CVE |
| LILIN | DVR (Variant A) | N/A | CWE-78 | No CVE |
| LILIN | DVR (Variant B) | N/A | CWE-78 | No CVE |
| Fiberhome | Router SR1041F RP0105 | N/A | CWE-78 | No CVE |
| Linksys | Router apply.cgi (Variant A) | N/A | CWE-78 | No CVE |
| Linksys | Router apply.cgi (Variant B) | N/A | CWE-78 | No CVE |
| BYTEVALUE | Intelligent Flow Router | N/A | CWE-78 | No CVE |
| D-Link | DIR-645 & DIR-815 | N/A | CWE-78 | No CVE |
| Unknown | wlan_operate endpoint | N/A | CWE-78 | No CVE |
| Unknown | resize_ext2 endpoint | N/A | CWE-78 | No CVE |
| ASMAX | 804 Router | N/A | CWE-78 | No CVE |

| | | | | |
|---|---|---|---|---|
| D-Link | DIR-X4860 | N/A | CWE-78 | No CVE |
| Unknown | File Upload (upgrade form) | N/A | CWE-78 | No CVE |
| Brickcom | IP Camera | N/A | CWE-78 | No CVE |
| IQrouter | IQrouter 3.3.1 | N/A | CWE-78 | No CVE |
| Ricon | Industrial Cellular Router S9922XL | N/A | CWE-78 | No CVE |
| Unknown | Shell endpoint | N/A | CWE-78 | No CVE |
| Nexxt | Router Firmware | CVE-2022-44149 | CWE-78 | N-Day |
| D-Link | DIR-645 Wired/Wireless Router | CVE-2015-2051 | CWE-78 | N-Day |
| Netgear | R7000 / R6400 Router | CVE-2016-6277 | CWE-78 | N-Day |
| Netgear | Multiple Routers (mini_httpd) | CVE-2020-27867 | CWE-78 | N-Day |
| Apache | HTTP Server | CVE-2021-41773 | CWE-22 | N-Day |
| Apache | HTTP Server | CVE-2021-42013 | CWE-22 | N-Day |
| TBK | Multiple DVRs | CVE-2024-3721 | CWE-78 | N-Day |
| TOTOLINK | Router (setMtknatCfg) | CVE-2025-1829 | CWE-78 | N-Day |
| Meteobridge | Web Interface | CVE-2025-4008 | CWE-78 | N-Day |
| D-Link | DNS-320 | CVE-2020-25506 | CWE-78 | N-Day |
| Digiever | DS-2105 Pro | CVE-2023-52163 | CWE-78 | N-Day |
| Netgear | DGN1000 | CVE-2024-12847 | CWE-78 | N-Day |
| D-Link | Multiple Products | CVE-2024-10914 | CWE-78 | N-Day |
| Edimax | RE11S Router | CVE-2025-22905 | CWE-78 | N-Day |
| QNAP | VioStor NVR | CVE-2023-47565 | CWE-78 | N-Day |
| D-Link | DIR-816 | CVE-2022-37129 | CWE-78 | N-Day |
| GNU | Bash (ShellShock) | CVE-2014-6271 | CWE-78 | N-Day |
| Dasan | GPON Home Router | CVE-2018-10561 | CWE-287 | N-Day |
| Four-Faith | Industrial Routers | CVE-2024-12856 | CWE-78 | N-Day |
| TP-Link | Archer AX21 | CVE-2023-1389 | CWE-78 | N-Day |
| D-Link | Multiple Products | CVE-2019-16920 | CWE-78 | N-Day |
| Tenda | Router (fromNetToolGet) | CVE-2025-7414 | CWE-78 | N-Day |
| Tenda | Router (deviceName) | CVE-2020-10987 | CWE-78 | N-Day |
| LB-LINK | Multiple Routers | CVE-2023-26801 | CWE-78 | N-Day |
| Linksys | E-Series Multiple Routers | CVE-2025-34037 | CWE-78 | N-Day |
| AVTECH | CCTV | CVE-2024-7029 | CWE-78 | N-Day |
| TOTOLINK | X2000R | CVE-2025-5504 | CWE-78 | N-Day |
| ZyXEL | P660HN-T1A | CVE-2017-18368 | CWE-78 | N-Day |
| Hytec Inter | HWL-2511-SS | CVE-2022-36553 | CWE-78 | N-Day |
| Belkin | Play N750 | CVE-2014-1635 | CWE-120 | N-Day |
| TRENDnet | TEW-411BRPplus | CVE-2023-51833 | CWE-78 | N-Day |
| TP-Link | TL-WR840N | CVE-2018-11714 | CWE-78 | N-Day |
| D-Link | DIR820LA1_FW105B03 | CVE-2023-25280 | CWE-78 | N-Day |
| Billion | 5200W-T Router | CVE-2017-18369 | CWE-78 | N-Day |
| Cisco | Multiple Products | CVE-2019-1663 | CWE-119 | N-Day |
| TOTOLINK | Router (setWizardCfg) | CVE-2024-1781 | CWE-78 | N-Day |

Table 1. CVEs seen in RondoDox campaigns

# Proactive strategies for effective vulnerability management

The latest RondoDox botnet campaign represents a significant evolution in automated network exploitation, demonstrating how threat actors continue to weaponize both publicly disclosed vulnerabilities and zero-day exploits discovered at security competitions like Pwn2Own.

The campaign's shotgun approach of targeting more than 50 vulnerabilities across over 30 vendors underscores the persistent risks facing organizations that maintain internet-exposed network infrastructure without adequate security controls.

The timeline presented in this analysis reveals an uncomfortable truth about the vulnerability lifecycle. Even when security researchers responsibly disclose flaws and vendors issue patches, the window between public disclosure and widespread exploitation continues to shrink, while the lifecycle of n-day exploits remain a perennial challenge to devices and their vendors. Organizations that delay patching or fail to maintain comprehensive asset inventories of their network edge devices create opportunities for campaigns like RondoDox to establish persistent footholds within their infrastructure.

Moving forward, defenders must adopt a proactive security posture that includes regular vulnerability assessments, network segmentation to limit lateral movement, restrict internet exposure, and continuous monitoring for signs of compromise.

We look forward to seeing great research at Pwn2Own Ireland 2025!

## Proactive security with Trend Vision One™

Trend Vision One™ is the only AI-powered enterprise cybersecurity platform that centralizes cyber risk exposure management, security operations, and robust layered protection. This holistic approach helps enterprises predict and prevent threats, accelerating proactive security outcomes across their respective digital estate. Eliminate security blind spots, focus on what matters most, and elevate security into a strategic partner for innovation, especially in the cases of novel malware threats as in the one discussed in this blog entry.

**Trend Vision One™ Threat Intelligence**

To stay ahead of evolving threats, Trend customers can access Trend Vision One™ Threat Insights which provides the latest insights from Trend™ Research on emerging threats and threat actors.

**Trend Vision One Threat Insights**

- Emerging Threats: RondoDox: From Targeting Multiple Vulnerabilities to Shotgunning Exploits

**Trend Vision One Intelligence Reports (IOC Sweeping)**

- RondoDox: From Targeting Multiple Vulnerabilities to Shotgunning Exploits

Hunting Queries

**Trend Vision One Search App**

Trend Vision One customers can use the Search App to match or hunt the malicious indicators mentioned in this blog post with data in their environment.

- *RondoDox Infection Payloads (Post Exploitation)*

eventSubId:2 AND (processCmd:"#!/bin/sh" AND processCmd:"chmod 777" AND processCmd:"service apparmor stop" AND processCmd:rondo.)

# Threat Hunting Queries & Detection Logic

Generic splunk query example:

- *index="<index_name>" | spath <json_field> | search <json_field>="*rondo.**"

**Generic Network Detection**

index=proxy OR index=web OR index=firewall | search user_agent="*bang2012@protonmail.com*" OR User-Agent="*bang2012@protonmail.com*" | table _time src_ip dest_ip url user_agent | sort -_time

# RondoDox Email

Common Proton email address found in numerous exploitation samples.

```
rule ZTH_Malware_RondoDox_Email{
meta:
description = "Detects patterns associated with rondo malware"
date = "2025-09-29"
author = "Peter Girnus (@gothburz)"
strings:
$s0 = "bang2012@protonmail.com" ascii
$s1 = "makenoise@tutanota.de" ascii

condition:
any
}
```

RondoDox Loader

Detects attempts to fetch infection payloads. This happens POST exploitation of the above mentioned vulnerabilities.

```
rule ZTH_Malware_RondoDox_Loader_A {
meta:
description = "Detects patterns associated with the RondoDox post exploitation."
date = "2025-09-29"
author = "Peter Girnus (@gothburz) with Trend Zero Day Initiative."
strings:
$s0 = "#!/bin/sh" ascii
$s1 = "chmod 777" ascii
$s2 = "service apparmor stop" ascii
$r1 = /\brondo\./ nocase
condition:
all of them
}
```

# Trend Solutions

Trend Micro customers have been protected from threats mentioned in the blog entry via the following rules and filters:

**Trend Micro Cloud One - Network Security & TippingPoint Filters**

- 1125 - HTTP: ../.. Directory Traversal
- 16797 - HTTP: GNU Bash URI Parameter Remote Code Execution Vulnerability
- 16798 - HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability
- 16800 - TCP: Non-Standard Function Declaration
- 16801 - HTTP: GNU Bash URI Remote Code Execution Vulnerability
- 16806 - UDP: Non-Standard Function Declaration
- 16811 - DHCP: GNU Bash Remote Code Execution Vulnerability
- 17463 - TCP: Linux/ShellshockCampaign.DDOSBot Random Byte Flood CnC Server Message
- 17466 - TCP: Linux/ShellshockCampaign.DDOSBot HOLD TCP Flood CnC Server Message
- 19677 - HTTP: Belkin Play N750 login.cgi Buffer Overflow Vulnerability
- 20005 - HTTP: D-Link Multiple Devices HNAP Command Injection Vulnerability
- 21687 - TCP: Linux/ShellshockCampaign.DDOSBot Scanner CnC Server Message
- 22228 - TCP: Linux/ShellshockCampaign.DDOSBot Terminate Process CnC Server Message
- 26943 - IPP: CUPS Code Injection Vulnerability
- 27492 - HTTP: NetGear Multiple Routers Command Injection Vulnerability
- 31938 - HTTP: Dasan GPON Home Router Authentication Bypass Vulnerability
- 32909 - SMTP: GNU Bash SMTP Header Remote Code Execution Vulnerability
- 33111 - TCP: Worm.Linux.Hakai.B Runtime Detection

- 35135 - HTTP: Cisco RV110W/RV130W/RV215W Routers Management Interface Command Execution Vulnerability
- 35725 - HTTP: Worm.Linux.Vampdemokre.A Runtime Detection
- 35803 - HTTP: Worm.Linux.Nekonebot.A Runtime Detection
- 36007 - HTTP: Worm.Linux.Asherposy.A Runtime Detection
- 36452 - HTTP: Worm.Linux.Ankitegg.A Runtime Detection
- 36707 - HTTP: Worm.Linux.Krasplint.A Runtime Detection
- 36923 - TCP: Worm.Linux.Momentumbotnet.A Runtime Detection
- 37015 - TCP: Trojan.Linux.Muhstik.A Runtime Detection
- 37073 - HTTP: Worm.Linux.Ayewoabot.A Runtime Detection
- 37314 - HTTP: Trojan.Linux.Kaguyabot.A Runtime Detection
- 37462 - HTTP: Trojan.Linux.Gangmirbot.A Runtime Detection
- 37508 - HTTP: Worm.Linux.Noelobot.A Runtime Detection
- 37624 - HTTP: TrueOnline Billion 5200W-T Router Command Injection Vulnerability
- 37926 - HTTP: Worm.Linux.Sorafetbot.A Runtime Detection
- 38067 - HTTP: NETGEAR Multiple Routers mini_httpd  Command Injection Vulnerability (ZDI-20-1423)
- 38405 - HTTP: Worm.Linux.Katana.A Runtime Detection
- 39550 - HTTP: Worm.Linux.Busybobot.A Runtime Detection
- 40008 - HTTP: Worm.Linux.Loudscream.A Runtime Detection
- 40064 - HTTP: D-Link Various Routers Remote Code Execution Vulnerability
- 40086 - HTTP: Worm.Linux.Frostymirbot.A Runtime Detection
- 40538 - TCP: Worm.Linux.BotenaGo.A Runtime Detection
- 40828 - HTTP: Worm.Linux.Tropimesbot.A Runtime Detection
- 41396 - HTTP: Worm.Linux.Enemybot.A Runtime Detection
- 41396 - HTTP: Worm.Linux.Enemybot.A Runtime Detection
- 41654 - HTTP: Worm.Linux.Aquamirbot.A Runtime Detection
- 42120 - HTTP: Worm.Linux.Zerobot.A Runtime Detection
- 42150 - HTTP: TP-Link AX1800 locale controller Command Injection Vulnerability (ZDI-23-451)
- 42389 - HTTP: Worm.Linux.Bratomirbot.A Runtime Detection
- 42823 - HTTP: Worm.Linux.Mirai.EV Runtime Detection (Zyxel Infection)
- 42824 - HTTP: Worm.Linux.Mirai.EV Runtime Detection (LB-Link Infection)
- 42825 - HTTP: Worm.Linux.Mirai.EV Runtime Detection (Tenda Infection)
- 42826 - HTTP: Worm.Linux.Mirai.EV Runtime Detection (Netlog Infection)
- 42836 - HTTP: LB-Link Multiple Products Command Injection Vulnerability
- 42880 - HTTP: Worm.Linux.Unhanaawbot.A Runtime Detection
- 43190 - HTTP: D-Link DIR820LA1_FW105B03 Command Injection Vulnerability
- 43357 - HTTP: Worm.Linux.Mirai.IZ1H9 Runtime Detection
- 43829 - HTTP: TP-Link Authentication Bypass Vulnerability
- 44282 - TCP: Trojan.Linux.Goldoon.A Runtime Detection
- 44287 - HTTP: Trojan-Downloader.Shell.Goldoonps.A Runtime Detection

- 44585 - HTTP: Worm.Linux.Aresmirbot.A Runtime Detection
- 45104 - TCP: Trojan.Linux.Mirai.AGIO Runtime Detection
- 45234 - HTTP: D-Link NAS OS Command Injection Vulnerability
- 45254 - IRC: Trojan.Linux.Capsaicin.A Runtime Detection
- 45270 - HTTP: Worm.Linux.XorBot.A Runtime Detection
- 45300 - HTTP: Four-Faith Industrial Router Command Injection Vulnerability
- 45615 - HTTP: Worm.Linux.BallistaBot.A Runtime Detection
- 46070 - HTTP: TBK DVR Command Injection Vulnerability

**Trend Vision One Network Sensor and Trend Micro Deep Discovery Inspector (DDI) Rules**

- 1618 - CVE-2014-6271 - Shellshock HTTP Request
- 1646 - CVE-2014-6271 - SHELLSHOCK VoIP SIP Exploit
- 1647 - CVE-2014-6271 - SHELLSHOCK DNS Exploit
- 1650 - CVE-2014-6271 - Shellshock SMTP Exploit
- 1651 - CVE-2014-6271 - Shellshock POP3 Exploit
- 1656 - CVE-2014-6271 - Shellshock DHCP Exploit
- 2941 - Possible CVE-2019-1663 CISCO RV Routers Buffer Overflow Exploit - HTTP (Request)
- 4251 - CVE-2019-16920 - D-Link RCE Exploit - HTTP (Request)
- 4633 - CVE-2021-41773 - APACHE TRAVERSAL RCE EXPLOIT - HTTP(REQUEST)
- 4839 - CVE-2023-1389 - TPLink Firmware Command Injection Exploit - HTTP (Request)
- 5441 - CVE-2024-3721 - TBK DVR RCE - HTTP (Request)
- 5522: CVE-2025-1829_HTTP_TOTOLINK_CMD_INJECTION_EXPLOIT_REQUEST
- 5523: CVE-2025-4008_HTTP_METEOBRIDGE_INJECTION_EXPLOIT_REQUEST

**Trend Vision One Endpoint Security, Trend Cloud One - Workload and Endpoint Security, Deep Security and Vulnerability Protection IPS Rules**

- 1006256 - GNU Bash Remote Code Execution Vulnerability
- 1006258 - GNU Bash Remote Code Execution Vulnerability Over DHCP
- 1006259 - GNU Bash Remote Code Execution Vulnerability Over SMTP
- 1006260 - GNU Bash Remote Code Execution Vulnerability Over SIP
- 1006261 - Identified Suspicious Bash ShellShock Attack
- 1011171 - Apache HTTP Server Directory Traversal Vulnerability (CVE-2021-41773 and CVE-2021-42013)

**Trend Micro Endpoint & Server Malware Pattern (VSAPI) Detection**

- CVE-2015-2051 - VSAPI-Backdoor.Linux.XorBot.A (Backdoor.Linux.XorBot.A)
- CVE-2015-2051 - VSAPI-Trojan.Linux.Capsaicin.A (Trojan.Linux.Capsaicin.A)
- CVE-2015-2051 - VSAPI-Backdoor.Linux.Aresmirbot.A (Backdoor.Linux.Aresmirbot.A)
- CVE-2015-2051 - VSAPI-Trojan-Downloader.Shell.Goldoonps.A (Trojan-Downloader.Shell.Goldoonps.A)

- CVE-2015-2051 - VSAPI-Trojan.Linux.Goldoon.A (Trojan.Linux.Goldoon.A)
- CVE-2015-2051 - VSAPI-Backdoor.Linux.Unhanaawbot.A (Backdoor.Linux.Unhanaawbot.A)
- CVE-2015-2051 - VSAPI-Backdoor.Linux.Bratomirbot.A (Backdoor.Linux.Bratomirbot.A)
- CVE-2015-2051 - VSAPI-Backdoor.Linux.Enemybot.A (Backdoor.Linux.Enemybot.A)
- CVE-2015-2051 - VSAPI-Backdoor.Linux.Tropimesbot.A (Backdoor.Linux.Tropimesbot.A)
- CVE-2015-2051 - VSAPI-Backdoor.Linux.BotenaGo.A (Backdoor.Linux.BotenaGo.A)
- CVE-2015-2051 - VSAPI-Backdoor.Linux.Hakai.B (Backdoor.Linux.Hakai.B)
- CVE-2020-25506 - VSAPI-Backdoor.Linux.Zerobot.A (Backdoor.Linux.Zerobot.A)
- CVE-2014-6271 - VSAPI-Backdoor.Linux.Kaguyabot.A (Backdoor.Linux.Kaguyabot.A)
- CVE-2018-10561 - VSAPI-Backdoor.Linux.Aquamirbot.A (Backdoor.Linux.Aquamirbot.A)
- CVE-2018-10561 - VSAPI-Backdoor.Linux.Frostymirbot.A (Backdoor.Linux.Frostymirbot.A)
- CVE-2018-10561 - VSAPI-Backdoor.Linux.Loudscream.A (Backdoor.Linux.Loudscream.A)
- CVE-2018-10561 - VSAPI-Backdoor.Linux.Busybobot.A (Backdoor.Linux.Busybobot.A)
- CVE-2018-10561 - VSAPI-Backdoor.Linux.Katana.A (Backdoor.Linux.Katana.A)
- CVE-2018-10561 - VSAPI-Backdoor.Linux.Noelobot.A (Backdoor.Linux.Noelobot.A)
- CVE-2018-10561 - VSAPI-Backdoor.Linux.Gangmirbot.A (Backdoor.Linux.Gangmirbot.A)
- CVE-2018-10561 - VSAPI-Backdoor.Linux.Ayewoabot.A (Backdoor.Linux.Ayewoabot.A)
- CVE-2018-10561 - VSAPI-Backdoor.Linux.Muhstik.A (Backdoor.Linux.Muhstik.A)
- CVE-2018-10561 - VSAPI-Backdoor.Linux.Momentumbotnet.A (Backdoor.Linux.Momentumbotnet.A)
- CVE-2018-10561 - VSAPI-Backdoor.Linux.Krasplint.A (Backdoor.Linux.Krasplint.A)
- CVE-2018-10561 - VSAPI-Backdoor.Linux.Ankitegg.A (Backdoor.Linux.Ankitegg.A)
- CVE-2018-10561 - VSAPI-Backdoor.Linux.Asherposy.A (Backdoor.Linux.Asherposy.A)
- CVE-2018-10561 - VSAPI-Backdoor.Linux.Nekonebot.A (Backdoor.Linux.Nekonebot.A)
- CVE-2018-10561 - VSAPI-Backdoor.Linux.Vampdemokre.A (Backdoor.Linux.Vampdemokre.A)
- CVE-2023-1389 - VSAPI-Backdoor.Linux.MIRAi.PUSELVIT (Backdoor.Linux.MIRAi.PUSELVIT)

**Acknowledgements**

The authors would like to acknowledge the following team members for their contributions to this project.

- William Gamazo Sanchez
- Alfredo Oliveira
- Trend Response
- Writing Team & Trend Marketing

**Indicators of compromise**

Indicators of compromise can be found here.

Tags

Latest News | Research | Articles, News, Reports | Cyber Threats