Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

Raptor Train Paradox: A Multi-Tiered Botnet Phenomenon

Date of Publication	Admiralty Code	TA Number
October 3, 2024	A1	TA2024378

Summary

Attack Commenced: May 2020
Threat Actor: Flax Typhoon (aka Ethereal Panda, RedJuliett)
Malware: Nosedive, Raptor Train
Attack Region: Worldwide
Targeted Industries: Military, Government, Higher Education, Telecommunications, Defense, Information Technology
Attack: The Raptor Train botnet framework, active since mid-2020, has evolved into a sophisticated, multi-tiered network primarily targeting small office/home office (SOHO) networks and Internet of Things (IoT) devices. Likely operated by Chinese nation-state cybercriminals known as Flax Typhoon, the botnet had expanded significantly by June 2024, with its database growing to over 1.2 million compromised devices globally, including more than 385,000 unique U.S. victims. Linked to four major cyber campaigns, this ever-evolving botnet highlights the increasing complexity and persistence of nation-state cyberattacks.

Attack Timeline

May 2020 to April 2022

Crossbill campaign: maintained tens of thousands of compromised devices at any time. By mid-2021, botnet operations began gaining momentum.

July 2022 to June 2023

Finch campaign: Approximately 60,000 devices were compromised in June 2023 alone.

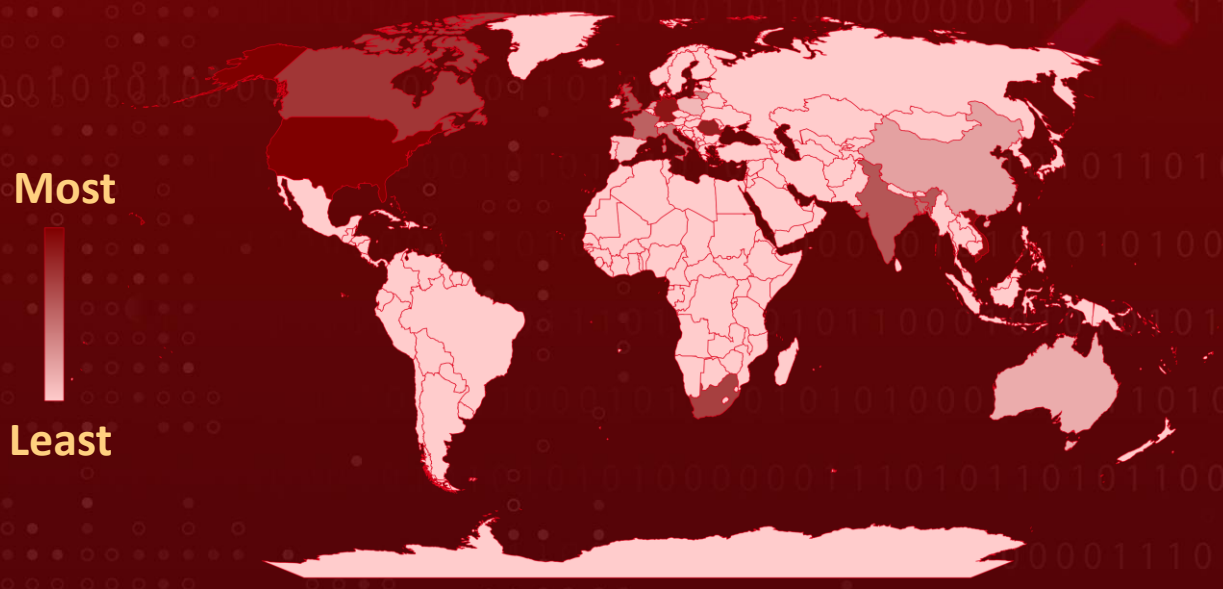
May 2023 to August 2023

Canary campaign: At least 16,000 devices were compromised. The primary targets were the ActionTec PK5000 modems, ASUS routers, Hikvision IP cameras, and Shenzhen TVT NVRs.

June 2023 to September 2024

Oriole campaign: The botnet had grown to over 260,000 compromised devices globally by mid-2024.

Attack Regions



Attack Details

#1 The Raptor Train botnet framework has continuously evolved since mid-2020, reflecting over four years of ongoing development. This sophisticated, multi-tiered botnet primarily targets small office/home office (SOHO) networks and Internet of Things (IoT) devices, with subtle indications that it is operated by Chinese nation-state threat actors identified as Flax Typhoon.

#2 As of June 2024, the Raptor Train botnet had surged to encompass over 1.2 million compromised devices globally, including more than 385,000 unique U.S. victims, historically and currently exploited. Its operators control this extensive and varied network through distributed payload and command-and-control (C2) servers, centralized by a Node.js backend and managed via a cross-platform Electron-based front-end application called Sparrow.

#3 This infrastructure functions as a competent, enterprise-grade control system, designed to manage over 60 C2 servers and their infected devices simultaneously. The structure of Flax Typhoon's infrastructure facilitates a range of malicious activities. These include scalable bot exploitation, **vulnerability and exploit management**, remote control of C2 infrastructure, file transfers, remote command execution, and the deployment of large-scale IoT-based distributed denial-of-service (DDoS) attacks.

#4 A degree of automation aids in managing the C2 network, ensuring the seamless collection of logs and bot data to enhance operators' situational awareness. Tasks within the Raptor Train network originate from Tier 3 Sparrow management nodes. These tasks are then relayed through Tier 2 C2 and Exploitation servers before reaching the bots in Tier 1, creating a structured hierarchy for efficient botnet operations.

#5 The primary implant found across most compromised devices is known as "Nosedive," a custom variant of the Mirai malware. Nosedive is designed to be compatible with all major SOHO and IoT architectures. It is typically deployed from Tier 2 payload servers using a unique URL encoding technique and domain injection method.

#6 Once deployed, Nosedive operates entirely in-memory, allowing the botnet operators to execute commands, transfer files, and conduct DDoS attacks on the compromised devices. At least four distinct campaigns have been linked to the evolving Raptor Train botnet framework, each distinguished by the root domains utilized and the devices targeted.

#7 The Crossbill campaign relied on the C2 root domain k3121[.]com. The Finch campaign utilized the C2 root domain b2047[.]com. The Canary campaign also used the b2047[.]com domain but relied on multi-stage droppers for its operations. Finally, the ongoing Oriole campaign has shifted to the C2 root domain w8510[.]com and its associated subdomains.

Recommendations

Disable Unused Services and Ports: Ensure unnecessary services and ports are disabled on routers and IoT devices. Features like Universal plug-and-play (UPnP), remote management, and file-sharing protocols can be exploited by threat actors to gain initial access or spread malware. If these features are not required for operational functionality, they should be turned off.

Regularly Apply Patches and Updates: Maintain a proactive approach to cybersecurity by regularly applying software and firmware updates. Patching known vulnerabilities significantly reduces risks. Utilize automatic update channels from trusted sources whenever possible and avoid trusting unsolicited email updates or attachments from unknown websites.

Replace End-of-Life Equipment: Upgrade and replace devices that have reached their end-of-life status and are no longer supported by their vendors. Utilizing devices under active support plans ensures that they receive necessary security updates and patches, reducing vulnerabilities.

Plan for Device Reboots: Schedule regular reboots of devices to terminate all running processes, which may help eliminate certain types of malware, including fileless malware. This is particularly effective against Mirai variants like Nosedive, a final payload that lacks persistence. To minimize disruption, choose preferred times for reboots, and be prepared for service interruptions. For unresponsive compromised devices, a physical reboot may be necessary.

Monitor for Abnormal Network Traffic: Establish monitoring protocols for high network traffic volumes, as DDoS attacks from botnets can mimic normal traffic patterns. Implement firewalls and intrusion detection systems to define and monitor for abnormal traffic behaviors. Consider deploying proxy solutions to help mitigate the effects of DDoS incidents.

Implement Network Segmentation: Utilize network segmentation to isolate IoT devices within a larger network, minimizing their risk exposure. By applying the principle of least privilege, assign only the essential connectivity needed for each device to perform its designated functions, reducing potential attack surfaces.

Vulnerability Management: Implement a robust vulnerability management process to ensure that software and systems are regularly assessed for vulnerabilities and updated with the required security patches. Prioritize critical vulnerabilities identified by security advisories and vendors to mitigate the risk of exploitation by threat actors.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0005 Defense Evasion
TA0007 Discovery	TA0008 Lateral Movement	TA0009 Collection	TA0011 Command and Control
TA0010 Exfiltration	TA0040 Impact	TA0042 Resource Development	T1210 Exploitation of Remote Services

T1059 Command and Scripting Interpreter	**T1059.003** Windows Command Shell	**T1068** Exploitation for Privilege Escalation	**T1071** Application Layer Protocol
T1505 Server Software Component	**T1005** Data from Local System	**T1571** Non-Standard Port	**T1190** Exploit Public-Facing Application
T1204.002 Malicious File	**T1027** Obfuscated Files or Information	**T1496** Resource Hijacking	**T1202** Indirect Command Execution
T1016 System Network Configuration Discovery	**T1046** Network Service Discovery	**T1104** Multi-Stage Channels	**T1203** Exploitation for Client Execution
T1584.005 Botnet	**T1584** Compromise Infrastructure	**T1498** Network Denial of Service	**T1588.006** Vulnerabilities
T1588 Obtain Capabilities	**T1588.001** Malware	**T1587** Develop Capabilities	**T1587.001** Malware

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	114[.]255[.]70[.]20, 5[.]188[.]33[.]135, 202[.]182[.]109[.]151, 5[.]188[.]33[.]228, 185[.]14[.]45[.]160, 185[.]207[.]154[.]253, 14[.]1[.]98[.]223, 223[.]98[.]159[.]112, 210[.]61[.]186[.]117, 104[.]244[.]89[.]157, 114[.]255[.]70[.]30, 140[.]82[.]14[.]222, 45[.]32[.]196[.]165, 66[.]42[.]118[.]156,

TYPE	VALUE
IPv4	85[.]90[.]216[.]178, 85[.]90[.]216[.]184, 149[.]28[.]98[.]243, 66[.]42[.]83[.]4, 45[.]91[.]82[.]49, 45[.]91[.]82[.]78, 66[.]42[.]101[.]23, 92[.]223[.]30[.]61, 92[.]223[.]30[.]95, 216[.]128[.]183[.]154, 37[.]61[.]229[.]163, 37[.]61[.]229[.]171, 45[.]32[.]185[.]75, 45[.]65[.]9[.]216, 45[.]65[.]9[.]235, 45[.]65[.]9[.]28, 92[.]223[.]30[.]82, 216[.]128[.]128[.]245, 195[.]234[.]62[.]188, 195[.]234[.]62[.]192, 85[.]90[.]216[.]69, 195[.]234[.]62[.]184, 89[.]44[.]198[.]200, 207[.]148[.]68[.]131, 108[.]61[.]177[.]81, 45[.]80[.]215[.]149, 45[.]92[.]70[.]111, 45[.]13[.]199[.]140, 45[.]13[.]199[.]152, 45[.]13[.]199[.]207, 45[.]13[.]199[.]84, 45[.]13[.]199[.]96, 45[.]13[.]199[.]104, 45[.]13[.]199[.]45, 45[.]135[.]117[.]136, 45[.]10[.]58[.]133, 45[.]10[.]58[.]130, 85[.]90[.]216[.]111, 5[.]8[.]33[.]26, 45[.]10[.]58[.]128, 195[.]234[.]62[.]197, 45[.]92[.]70[.]68, 5[.]45[.]184[.]68, 195[.]234[.]62[.]198, 92[.]38[.]185[.]47, 92[.]38[.]185[.]43,

TYPE	VALUE
IPv4	85[.]90[.]216[.]112, 45[.]10[.]58[.]129, 5[.]181[.]27[.]219, 92[.]38[.]185[.]44, 45[.]135[.]117[.]131, 85[.]90[.]216[.]110, 37[.]61[.]229[.]17, 37[.]9[.]35[.]89, 85[.]90[.]216[.]116, 37[.]61[.]229[.]15, 92[.]38[.]185[.]46, 45[.]80[.]215[.]186, 85[.]90[.]216[.]115, 45[.]10[.]58[.]132, 92[.]38[.]185[.]45, 45[.]92[.]70[.]71, 207[.]148[.]122[.]69, 91[.]216[.]190[.]154, 23[.]236[.]68[.]193, 91[.]216[.]190[.]247, 91[.]216[.]190[.]74, 45[.]80[.]215[.]47, 139[.]180[.]137[.]219, 149[.]248[.]51[.]22, 65[.]20[.]97[.]251, 45[.]77[.]231[.]209, 78[.]141[.]238[.]97, 155[.]138[.]133[.]56, 92[.]38[.]178[.]232, 92[.]223[.]30[.]233, 92[.]38[.]135[.]146, 92[.]223[.]30[.]232, 92[.]223[.]30[.]241, 155[.]138[.]151[.]225, 5[.]181[.]27[.]19, 5[.]181[.]27[.]6, 195[.]234[.]62[.]18, 45[.]80[.]215[.]153, 45[.]80[.]215[.]154, 45[.]80[.]215[.]156, 92[.]38[.]176[.]156, 45[.]80[.]215[.]151, 5[.]181[.]27[.]21, 45[.]92[.]70[.]113, 45[.]92[.]70[.]115, 195[.]234[.]62[.]19,

TYPE	VALUE
IPv4	92[.]38[.]176[.]131, 45[.]92[.]70[.]112, 45[.]80[.]215[.]150, 45[.]80[.]215[.]155, 89[.]44[.]198[.]195, 45[.]80[.]215[.]152, 89[.]44[.]198[.]254, 91[.]216[.]190[.]2, 91[.]216[.]190[.]80, 23[.]236[.]68[.]213, 23[.]236[.]69[.]82, 23[.]236[.]68[.]161, 23[.]236[.]69[.]110, 23[.]236[.]68[.]229, 208[.]85[.]16[.]100, 222[.]186[.]48[.]201, 222[.]186[.]48[.]204, 37[.]9[.]35[.]91
Domains	hy92[.]com, hy830[.]com, hy529[.]com, hy229[.]com, hy324[.]com, hy1025[.]com, hy42[.]com, hy619[.]com, hy424[.]com, hy811[.]com, hy30[.]com, zdacasdc[.]w8510[.]com, zdacxzd[.]w8510[.]com, zasdfgasd[.]w8510[.]com, bzbatflwb[.]w8510[.]com, qacassdfawemp[.]w8510[.]com, apdfhhjcxcb[.]w8510[.]com, dftiscasdwe[.]w8510[.]com, lyblqwesfawe[.]w8510[.]com, ocmnusdjdik[.]w8510[.]com, kliscjaisdjhi[.]w8510[.]com, mjiudwajhkf[.]w8510[.]com, wmllxwkg[.]w8510[.]com, awbpxtpi[.]w8510[.]com, aewreiuicajo[.]w8510[.]com, tuisasdcxzd[.]w8510[.]com, kuyw[.]b2047[.]com,

TYPE	VALUE
Domains	xxqw[.]b2047[.]com, hume[.]b2047[.]com, oklm[.]b2047[.]com, ayln[.]b2047[.]com, abpi[.]b2047[.]com, amushuvfikjas[.]b2047[.]com, firc[.]b2047[.]com, voias[.]b2047[.]com, acgtjkiufde[.]b2047[.]com, awerdasvbjgrt[.]b2047[.]com, xaqw[.]k3121[.]com, lfdx[.]k3121[.]com, xbqw[.]k3121[.]com, dfgh[.]k3121[.]com, oklm[.]k3121[.]com, hyjk[.]k3121[.]com, mail[.]k3121[.]com, axqw[.]k3121[.]com, api[.]k3121[.]com, awqx[.]k3121[.]com, hnai[.]k3121[.]com, qwsd[.]k3121[.]com, wsxe[.]k3121[.]com, nulp[.]k3121[.]com, hyddh[.]com, blepmhnay[.]com, dkuwbcen[.]com, ftcexq[.]com, eufcj[.]com, saoadlg[.]com, gmhrxhc[.]com, vbbrfvhrg[.]com, wndaoyk[.]com, ecvkiehs[.]com, hfsdln[.]com, osiso[.]com, bcdkwwuah[.]com, cvmnomvxm[.]com, cvgeuwo[.]com, lofeuq[.]com, lznmihdej[.]com, fajxtg[.]com, grntjr[.]com, oploz[.]com, mudvw[.]com, amdord[.]com,

TYPE	VALUE
Domains	mvxnspcqr[.]com, adjsn[.]com, ttcyci[.]com, glxxet[.]com, nmfagp[.]com, rnjca[.]com, woaba[.]com, bxgtbv[.]com, ykcmewapc[.]com, tvcvhzyk[.]com, sreudcnb[.]com, vgbgwzmr[.]com, jgnsqihc[.]com, dvujvkfu[.]com, clqqknzb[.]com, sbuybjv[.]com, lomuzs[.]com, hersrr[.]com, Ifzupr[.]com, zuszr[.]com, jkwxcc[.]com, obqlibg[.]com, omviak[.]com, qjknpv[.]com, wvsezu[.]com, ysubryfv[.]com, nhcmdikkd[.]com, kmgzbowwg[.]com, qsxgzu[.]com, oicdsgjxz[.]com, iycwqot[.]com, ujrtkw[.]com, bkhqwfhtu[.]com, aqakffj[.]com, acqv[.]w8510[.]com, asdvxzzxvza[.]w8510[.]com, cansqra[.]w8510[.]com, canwtrow[.]w8510[.]com, cccasdqawer[.]w8510[.]com, ccccasdasdq[.]w8510[.]com, cccvbsdfsdf[.]w8510[.]com, ccmmkmnkna[.]w8510[.]com, cpooooim[.]w8510[.]com, dvasrdftqgqg[.]w8510[.]com, iiiiopasdfcasd[.]w8510[.]com, iikljhg[.]w8510[.]com,

TYPE	VALUE
Domains	iuyrdfvv[.]w8510[.]com, iyasdasfda[.]w8510[.]com, Ikljjhidjaiwd[.]w8510[.]com, Ikopiyut[.]w8510[.]com, mmjkjiu[.]w8510[.]com, mmnajsdh[.]w8510[.]com, mnbghjj[.]w8510[.]com, oiuiasdads[.]w8510[.]com, pllkkoasdko[.]w8510[.]com, poiaqqrjk[.]w8510[.]com, pojkkaka[.]w8510[.]com, poooooiioasd[.]w8510[.]com, ppppoiiua[.]w8510[.]com, qmmklou[.]w8510[.]com, qwertdvvaaz[.]w8510[.]com, ssacawfafwa[.]w8510[.]com, testate[.]w8510[.]com, testateone[.]w8510[.]com, uqooapp[.]w8510[.]com, uuiyiyasd[.]w8510[.]com, zda4g4[.]w8510[.]com, zda896[.]w8510[.]com, zda9ol[.]w8510[.]com, zdaaac[.]w8510[.]com, zdaasdafq[.]w8510[.]com, zdabnv[.]w8510[.]com, zdacasc[.]w8510[.]com, zdacawca[.]w8510[.]com, zdacccz[.]w8510[.]com, zdacppao[.]w8510[.]com, zdacscswc[.]w8510[.]com, zdacvb[.]w8510[.]com, zdacvbzzs[.]w8510[.]com, zdacwaca[.]w8510[.]com, zdacwrf[.]w8510[.]com, zdacx46[.]w8510[.]com, zdacxdawdas[.]w8510[.]com, zdaczcaaw[.]w8510[.]com, zdaczcvs1[.]w8510[.]com, zdaczsc[.]w8510[.]com, zdaczvs[.]w8510[.]com, zdaczxc1[.]w8510[.]com, zdafaa[.]w8510[.]com, zdamkl[.]w8510[.]com, zdaplm[.]w8510[.]com, zdapoi[.]w8510[.]com,

TYPE	VALUE
Domains	zdapoq[.]w8510[.]com, zdaqggh[.]w8510[.]com, zdaqwfasf[.]w8510[.]com, zdavva[.]w8510[.]com, zdaxcxzc[.]w8510[.]com, zdazzz[.]w8510[.]com, zdcacaw[.]w8510[.]com, zdcawca[.]w8510[.]com, zdpoa[.]w8510[.]com, zdpog[.]w8510[.]com, zdqqqqwe[.]w8510[.]com, zdzvbs[.]w8510[.]com, zzxnjiq[.]w8510[.]com, zzzcmsq[.]w8510[.]com
SHA256	2aa12e5989065951be84ce932b65bd197dd6be3fa987838bad48536c0c74d145, c6fe1748e68923f278926ee8679aaee22800b9c93c38641d12ea0e945e116bb0, 546390a3a296154e36051dda745b573658311f9831789bb1faca411a3803a9bb

CVEs

The adversary strategically exploited the following vulnerabilities to not only seize new botnet victims but also empower the botnet framework to extend its reach by targeting additional victims through the compromised devices. For easy reference, the patches for the exploited CVEs are hyperlinked to the checkmarks marked under 'Patch Link.'

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH LINK
CVE-2024-5217	ServiceNow Incomplete List of Disallowed Inputs Vulnerability	ServiceNow Platform	✗	✓	✓
CVE-2024-4577	PHP-CGI OS Command Injection Vulnerability	PHP Group PHP	✗	✓	✓
CVE-2024-29973	Zyxel Command Injection Vulnerability	Zyxel NAS326, NAS542	✗	✓	✓

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH LINK
CVE-2024-29269	Telesquare Unauthorized Remote Command Execution Vulnerability	Telesquare TLR-2005Ksh	✗	✗	✗
CVE-2024-21762	Fortinet FortiOS Out-of-Bound Write Vulnerability	Fortinet FortiOS	✓	✓	✓
CVE-2023-50386	Apache Arbitrary File Upload Vulnerability	Apache Solr	✗	✗	✓
CVE-2023-47218	Qnap Os Command Injection Vulnerability	QNAP QTSQuTS heroQuTScloud	✗	✗	✓
CVE-2023-46747	F5 BIG-IP Configuration Utility Authentication Bypass Vulnerability	F5 Big-IP	✗	✓	✓
CVE-2023-46604	Apache ActiveMQ Deserialization of Untrusted Data Vulnerability	Apache Apache ActiveMQ	✗	✓	✓
CVE-2023-43478	Telstra Root Code Execution Vulnerability	Telstra Smart Modem Gen 2	✗	✗	✓
CVE-2023-4166	Tongda OA SQL injection Vulnerability	Tongda OA Tongda2000	✗	✗	✓
CVE-2023-38646	Metabase Arbitrary Command Execution Vulnerability	Metabase and Metabase Enterprise	✗	✗	✓
CVE-2023-3852	Openrapid Arbitrary File Upload Vulnerability	OpenRapid Yuque RapidCMS	✗	✗	✓
CVE-2023-38035	Ivanti Sentry Authentication Bypass Vulnerability	Ivanti MobileIron Sentry (MICS Admin Portal)	✓	✓	✓
CVE-2023-37582	Apache Remote Command Execution Vulnerability	Apache RocketMQ	✗	✗	✓

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH LINK
CVE-2023-36844	Juniper Junos OS EX Series PHP External Variable Modification Vulnerability	Juniper Juniper Junos	✗	✓	✓
CVE-2023-36542	Apache Code Injection Vulnerability	Apache NiFi	✗	✗	✓
CVE-2023-35885	Cloudpanel Insecure File-Manager Cookie Authentication Vulnerability	CloudPanel 2	✗	✗	✓
CVE-2023-35843	Nocodb Path Traversal Vulnerability	NocoDB	✗	✗	✓
CVE-2023-3519	Citrix NetScaler ADC and NetScaler Gateway Code Injection Vulnerability	Citrix Netscaler Gateway, Application Delivery Controller (ADC)	✓	✓	✓
CVE-2023-35081	Ivanti Endpoint Manager Mobile (EPMM) Path Traversal Vulnerability	Ivanti Endpoint Manager Mobile (EPMM)	✓	✓	✓
CVE-2023-34960	Chamilo Command Injection Vulnerability	Chamilo	✗	✗	✓
CVE-2023-34598	Gibbonedu Local File Inclusion (LFI) Vulnerability	Gibbonedu Gibbon	✗	✗	✓
CVE-2023-3368	Chamilo Command Injection Vulnerability	Chamilo LMS	✗	✗	✓
CVE-2023-33510	WordPress Read Arbitrary Files Vulnerability	WordPress Jeecg P3 Bix Chat	✗	✗	✗
CVE-2023-30799	Mikrotik Privilege Escalation Vulnerability	MikroTik RouterOS	✗	✗	✓
CVE-2023-28771	Zyxel Multiple Firewalls OS Command Injection Vulnerability	Zyxel ZyWALL/USG series	✗	✓	✓

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH LINK
CVE-2023-28365	Ubiquiti Arbitary Code Execution Vulnerability	Ubiquiti UI UniFi	✗	✗	✓
CVE-2023-27997	Fortinet FortiOS and FortiProxy SSL-VPN Heap-Based Buffer Overflow Vulnerability	Fortinet FortiOS and FortiProxy	✓	✓	✓
CVE-2023-27524	Apache Superset Insecure Default Initialization of Resource Vulnerability	Apache Apache Superset	✗	✓	✓
CVE-2023-26469	Jorani Path Traversal Vulnerability	Jorani	✗	✗	✗
CVE-2023-25690	Apache HTTP Request Smuggling Vulnerability	Apache HTTP Server	✗	✗	✓
CVE-2023-24229	DrayTek Command Injection Vulnerability	DrayTek Vigor2960 (EOL)	✗	✗	✗
CVE-2023-23333	Contec Command Injection Vulnerability	Contec SolarView Compact	✗	✗	✗
CVE-2023-22527	Atlassian Confluence Data Center and Server Template Injection Vulnerability	Confluence Data Center and Server	✗	✓	✓
CVE-2023-22515	Atlassian Confluence Data Center and Server Broken Access Control Vulnerability	Confluence Data Center and Server	✓	✓	✓
CVE-2022-42475	Fortinet FortiOS Heap-Based Buffer Overflow Vulnerability	Fortinet FortiOS and FortiProxy	✓	✓	✓
CVE-2022-40881	Contec Command Injection Vulnerability	Contec SolarView Compact	✗	✗	✓
CVE-2022-3590	WordPress Unauthenticated Blind SSRF Vulnerability	WordPress	✗	✗	✗

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH LINK
CVE-2022-31814	Netgate OS Command Injection Vulnerability	Netgate pfSense pfBlockerNG	✗	✗	✓
CVE-2022-30525	Zyxel Multiple Firewalls OS Command Injection Vulnerability	Zyxel USG FLEX, ATP, and VPN series firmware	✗	✓	✓
CVE-2022-26134	Atlassian Confluence Server and Data Center Remote Code Execution Vulnerability	Atlassian Confluence Data Center/Confluence server	✓	✓	✓
CVE-2022-20707	Cisco Remote Code Execution Vulnerability	Cisco Small Business Series Routers	✗	✗	✓
CVE-2022-1388	F5 BIG-IP Missing Authentication Vulnerability	F5 BIG-IP	✗	✓	✓
CVE-2021-46422	Telesquare OS Command Injection Vulnerability	Telesquare SDT-CW3B1	✗	✗	✗
CVE-2021-45511	NETGEAR Authentication Bpass Vulnerability	NETGEAR	✗	✗	✓
CVE-2021-44228	Log4shell (Apache Log4j2 Remote Code Execution Vulnerability)	Apache Log4j2	✓	✓	✓
CVE-2021-36260	Hikvision Improper Input Validation	Hikvision Web servers firmware	✗	✓	✓
CVE-2021-28799	QNAP NAS Improper Authorization Vulnerability	QNAP Systems Inc. Hybrid Backup Sync (HBS) 3	✗	✓	✓
CVE-2021-20090	Arcadyan Buffalo Firmware Path Traversal Vulnerability	Buffalo WSR, Arcadyan Arcadyan firmwareArcadyan Arcadyan firmware	✗	✓	✓
CVE-2021-1473	Cisco OS Command Injection Vulnerability	Cisco Small Business RV Series Routers	✗	✗	✓

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH LINK
CVE-2021-1472	Cisco Arbitrary Code Execution Vulnerability	Cisco Small Business Series Routers firmware	✗	✗	✓
CVE-2020-8515	Multiple DrayTek Vigor Routers Web Management Page Vulnerability	DrayTek Vigor	✓	✓	✓
CVE-2020-4450	IBM Arbitrary Code Execution Vulnerability	IBM WebSphere Application Server	✗	✗	✓
CVE-2020-35391	Tenda Malformed HTTP Request Header Processing Vulnerability	Tenda F3 Firmware	✗	✗	✗
CVE-2020-3452	Cisco ASA and FTD Read-Only Path Traversal Vulnerability	Cisco Adaptive Security Appliance (ASA) and Firepower Threat Defense (FTD) Software	✗	✓	✓
CVE-2020-3451	Cisco Remote Code Execution Vulnerability	Cisco Small Business Series Routers Firmware	✗	✗	✓
CVE-2020-15415	DrayTek Command Injection Vulnerability	DrayTek Vigor Firmware	✗	✗	✓
CVE-2019-7256	Nice Linear eMerge E3-Series OS Command Injection Vulnerability	Linear eMerge E3-Series	✗	✓	✗
CVE-2019-19824	TOTOLINK Realtek OS Command Injection Vulnerability	TOTOLINK Realtek SDK based routers	✗	✗	✗
CVE-2019-17621	D-Link DIR-859 Router Command Execution Vulnerability	D-Link DIR-859 Wi-Fi router 1.05 and 1.06B01 Beta01	✗	✓	✓
CVE-2019-12168	Four-Faith Remote Code Execution Vulnerability	Four-Faith Wireless Mobile Router F3x24	✗	✗	✗
CVE-2019-11829	Synology OS Command Injection Vulnerability	Synology Calendar before 2.3.1-0617	✗	✗	✓

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2018-18852	Cerio OS Command Injection Vulnerability	Cerio Cerio Dt-300N Firmware and Cerio Dt-300n	✗	✗	✗
CVE-2017-7876	QNAP Command Injection Vulnerability	QNAP QTS	✗	✗	✓
CVE-2015-7450	IBM WebSphere Application Server and Server Hypervisor Edition Code Injection.	IBM Tivoli Common Reporting	✗	✓	✓

References

https://assets.lumen.com/is/content/Lumen/raptor-train-handbook-copy

https://www.ic3.gov/Media/News/2024/240918.pdf

https://www.justice.gov/opa/pr/court-authorized-operation-disrupts-worldwide-botnet-used-peoples-republic-china-state

https://www.cyber.gov.au/about-us/view-all-content/alerts-and-advisories/peoples-republic-china-linked-actors-compromise-routers-and-iot-devices-botnet-operations

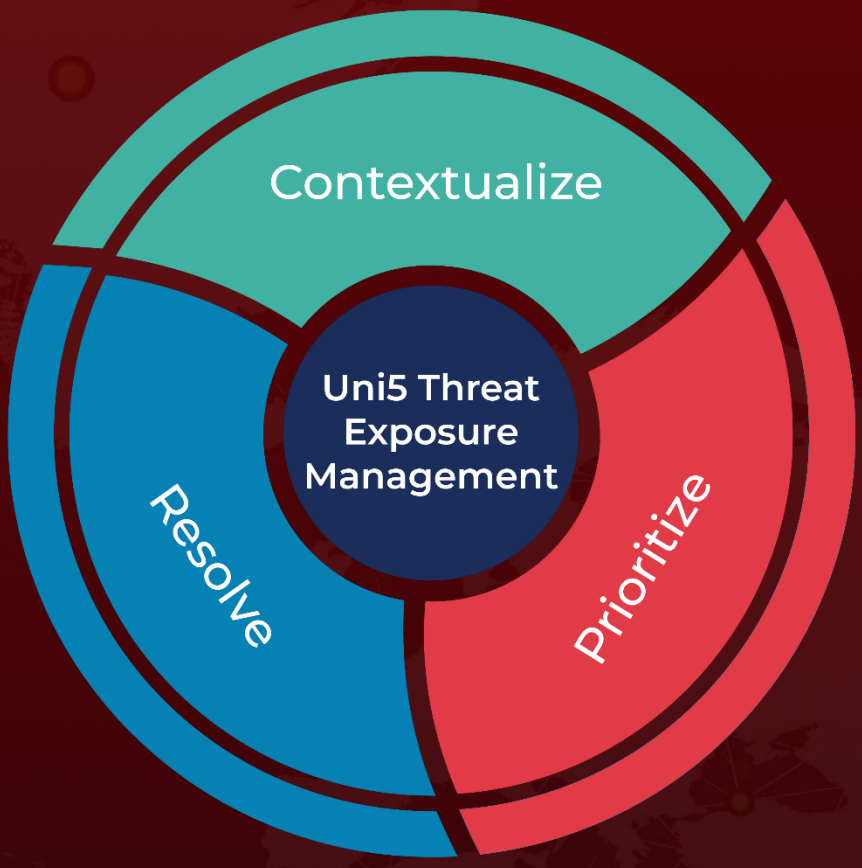
https://hivepro.com/threat-advisory/cybercriminals-forge-alliances-via-compromised-routers/

https://hivepro.com/threat-advisory/cuttlefish-malware-silent-stalkers-of-router-traffic/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

October 3, 2024 • 9:30 PM

More at www.hivepro.com