The Network is the Battlefield

Why Defense and Offense Must Merge in Modern Network Security

A S M Shamim Reza

TheTeamPhoenix
Machine Secures Machines

[~]$whoami

A S M **Shamim** Reza

– Founder & Chief of Research, *TheTeamPhoenix*

– SME & CT at *APNIC, Australia*

– ex-CTO, *Pipeline Inc. Japan*

– 12+ years, worked for *Link3 Technologies Limited*

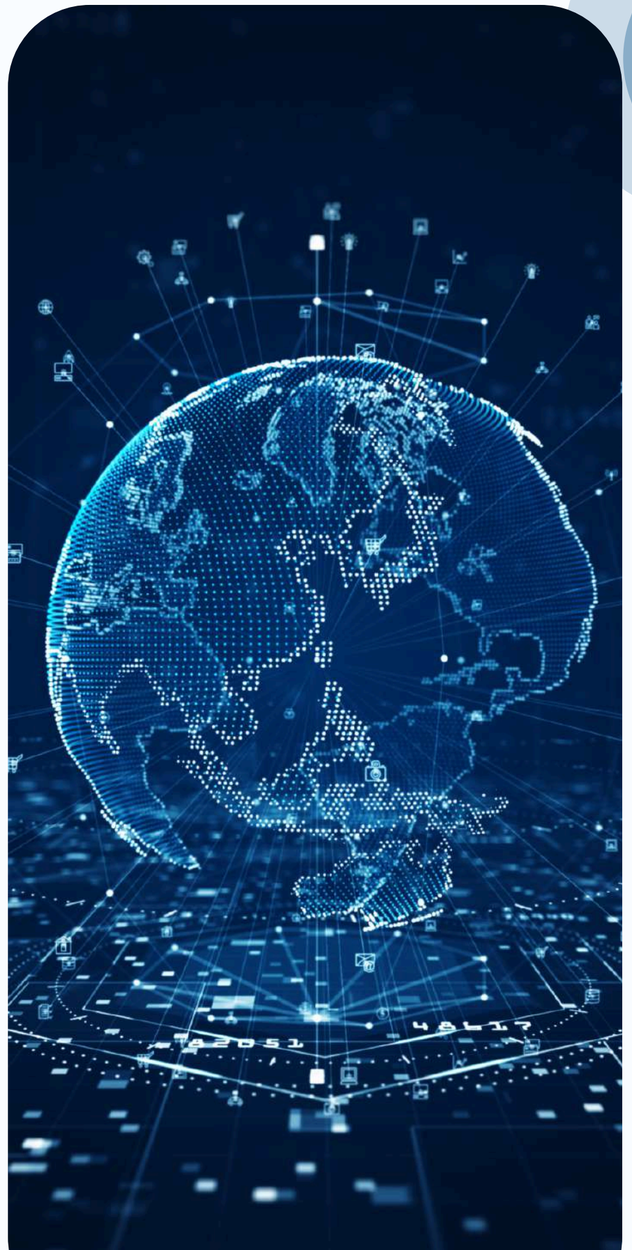
– PC Member, AI & Data Foundation, *Open Source Summit - North America*

– PC Member, *btNOG, APNIC 60.*

– Ambassador, *Wazuh, USA*

@asmshamimreza on **Linkedin**
@shamimrezasohag on **Twitter**
@ShamimRezaCNB on **Facebook**

TheTeamPhoenix
Machine Secures Machines

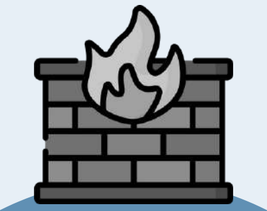


Agenda

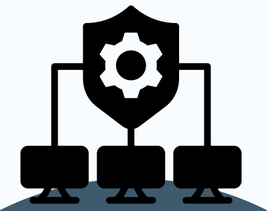
- Network Defense is broken by Design
- Real-World Offensive Network TTPs
- Why Internal Threats are still Thriving
- Case Study: Red Teaming a "Compliant" Network
- Recommendations for Resilient Network Architecture

TheTeamPhoenix
Machine Secures Machines

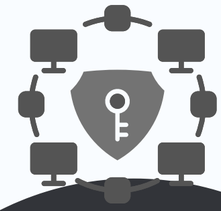
Legacy Network Defense is Failing



Network design is often decades old, even there is no inventory.



Internal lateral movement frequently goes undetected.



Firewalls protect the edge, but attackers operate inside the network.

TheTeamPhoenix
Machine Secures Machines

Legacy Network Defense is Failing

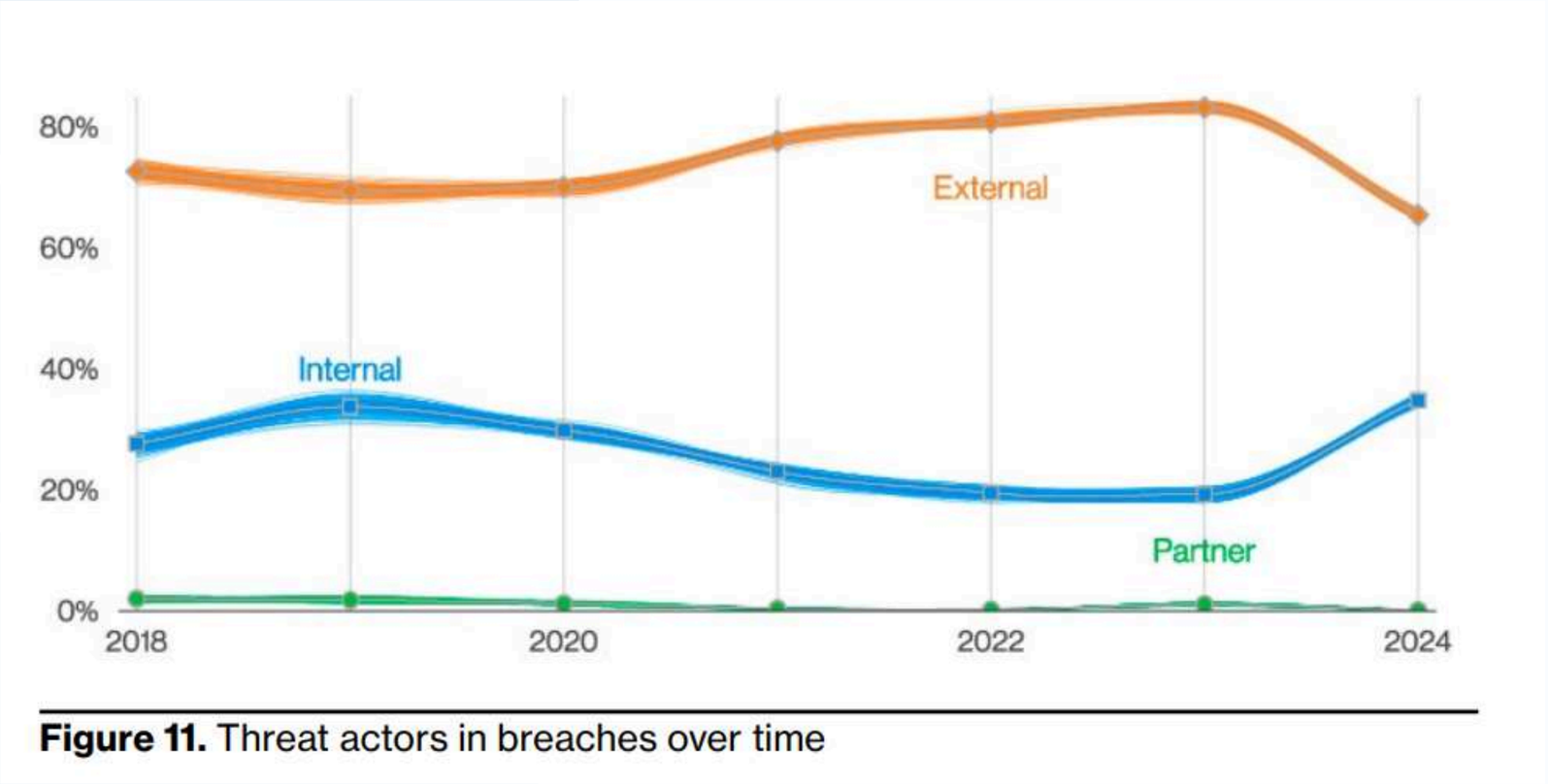


Figure 11. Threat actors in breaches over time

35% of breaches originate from internal network layers – Verizon DBIR 2024

TheTeamPhoenix
Machine Secures Machines

Common Network Security Gaps

Unsegmented internal traffic presents a risk to network security.

When internal network segments are not properly isolated, it increases vulnerability to lateral movement by attackers.

Lack of east-west visibility hinders threat detection.

Without tools like NetFlow or PCAP, monitoring internal traffic becomes challenging, leaving gaps in security visibility.

Using SNMPv2 community strings in plaintext is a significant security flaw.

Plaintext community strings can be easily intercepted, granting unauthorized access to network devices.

Default credentials on switches and routers create exploitable weaknesses.

Leaving default credentials unchanged provides an easy entry point for attackers into the network.

Absence of Layer 3 ACLs between VLANs allows unrestricted access.

Without Layer 3 Access Control Lists, traffic between VLANs can be manipulated by unauthorized users.

TheTeamPhoenix
Machine Secures Machines

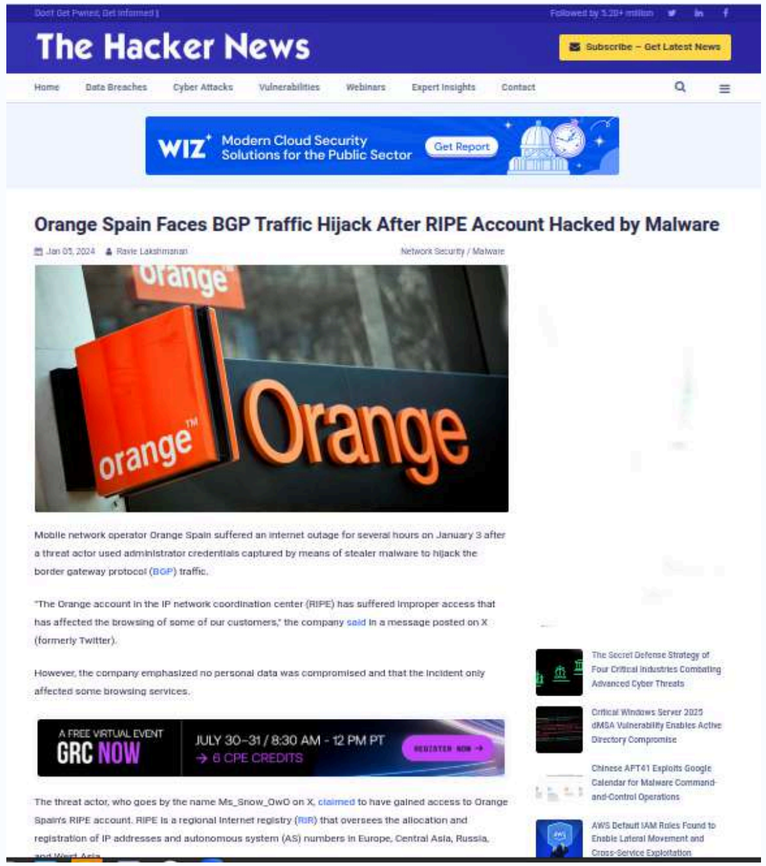
Network Security is more than Routing Hygiene

- BGP controls (MANRS, ROAs, RPKI) ≠ internal security
- The myth of segmentation: VLANs ≠ true isolation
- Modern attacks operate inside the perimeter

TheTeamPhoenix
Machine Secures Machines

Network Security is more than Routing Hygiene

- BGP controls (MANRS, ROAs, RPKI) ≠ internal security
- The myth of segmentation: VLANs ≠ true isolation
- Modern attacks operate inside the perimeter



Orange Spain Faces BGP Traffic Hijack After ***RIPE Account Hacked*** by Malware in ***2024***

TheTeamPhoenix
Machine Secures Machines

What MANRS & ROAs Solve vs. What you still Need

ROA, RPKI, MANRS is mendatory, but dont cover all

Security Layer	Example Attack	Covered by MANRS/ROAs?	Needed Detection / Mitigation
Inter-domain routing	BGP route hijack	✅	ROAs, RPKI, MANRS
Intra-domain routing	OSPF injection	❌	OSPF auth, NetFlow, Zeek
Data-link (L2)	ARP spoofing	❌	ARPWatch, Zeek, 802.1X, NAC
DHCP layer	Rogue DHCP server	❌	DHCP snooping, NAC
App-layer exfil	East-West Exfiltration (DNS/HTTPS)	❌	Egress Filtering, TLS JA3, Proxy Inspection
Network hardening	SNMPv2 leaks	❌	Enforce SNMPv3, audit ACLs
VLAN isolation	Misconfigured trunks	❌	ACLs, NetBox audit, NAC
Network hardening	Unauthorized Lateral Access	❌	NetFlow/sFlow + Role-Based Access

TheTeamPhoenix
Machine Secures Machines

FireEye Red Team tools (2020)

FireEye Red Team tools have been stolen

Posted date 10/12/2020
08/12/2020

FireEye, one of the world's leading cybersecurity companies dedicated to vulnerability analysis and prevention, has reported being the victim of a cyberattack through which its Red Team pentesting tools were stolen.

The cybercriminal, a highly sophisticated threat actor, has gotten to steal data ranging from simple scripts to entire frameworks similar to CobaltStrike and Metasploit. There are no 0-Day exploits among the above, nor been any leakage of client data.

In response to this incident, FireEye has issued over 300 countermeasures to protect its clients from stolen Red Team tools, and has also shared them with partners and government agencies to limit their ability to exploit them.

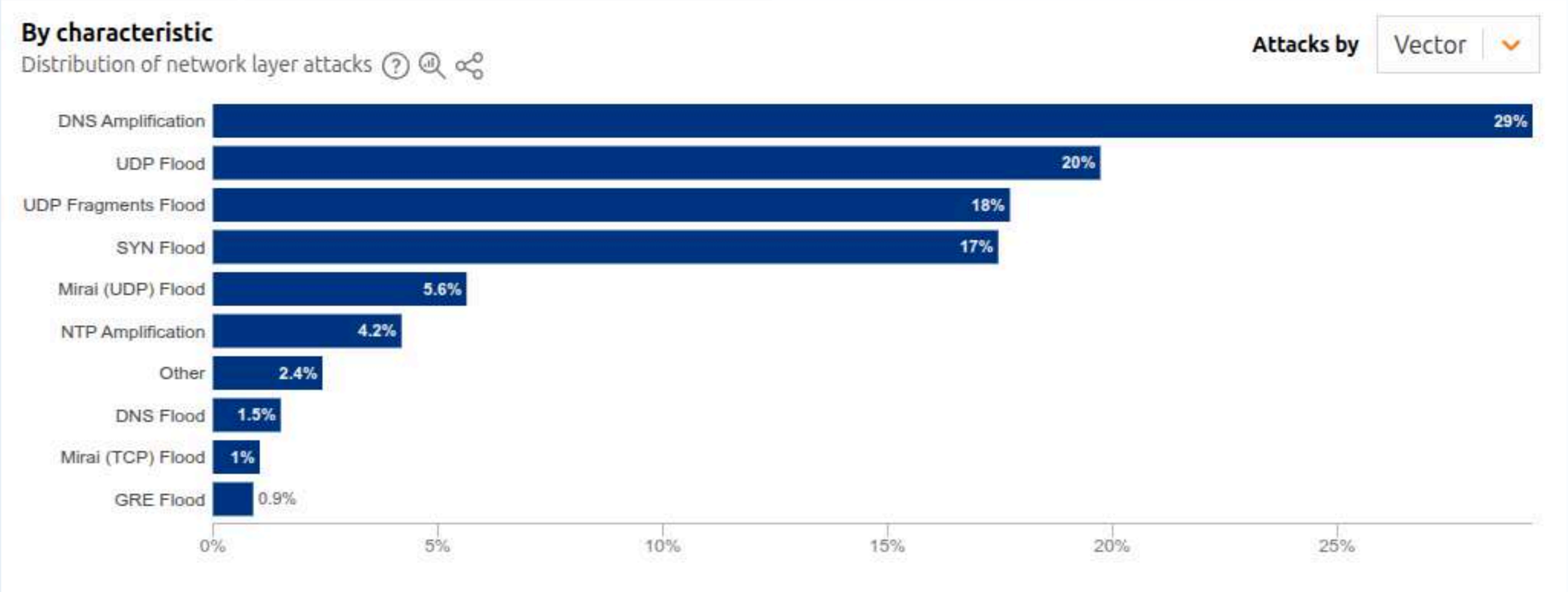
At present, there is no evidence that the stolen tools have been distributed or used, and a monitoring is maintained.

[Update 12/15/2020] Kevin Mandia, CEO of FireEye, has posted a blog entry updating the information provided on FireEye's Red Team tool theft. In the post, he states that they have identified a global campaign that engages the networks of public and private organizations throughout the software supply chain, using updates to an IT infrastructure management software widely used by various organizations, called the SolarWinds Orion Platform. In addition, a SolarWinds briefing note to the U.S. Securities and Exchange Commission (SEC) details that there has been significant media coverage of attacks on U.S. government agencies and other companies, and many of these reports attribute these attacks to a vulnerability in Orion products. SolarWinds continues to investigate, in collaboration with the FBI and other US government agencies, whether and to what extent the vulnerability in Orion products was successfully exploited in any of the reported attacks.

TheTeamPhoenix
Machine Secures Machines

Network Layer Attacks

by Country - Bangladesh

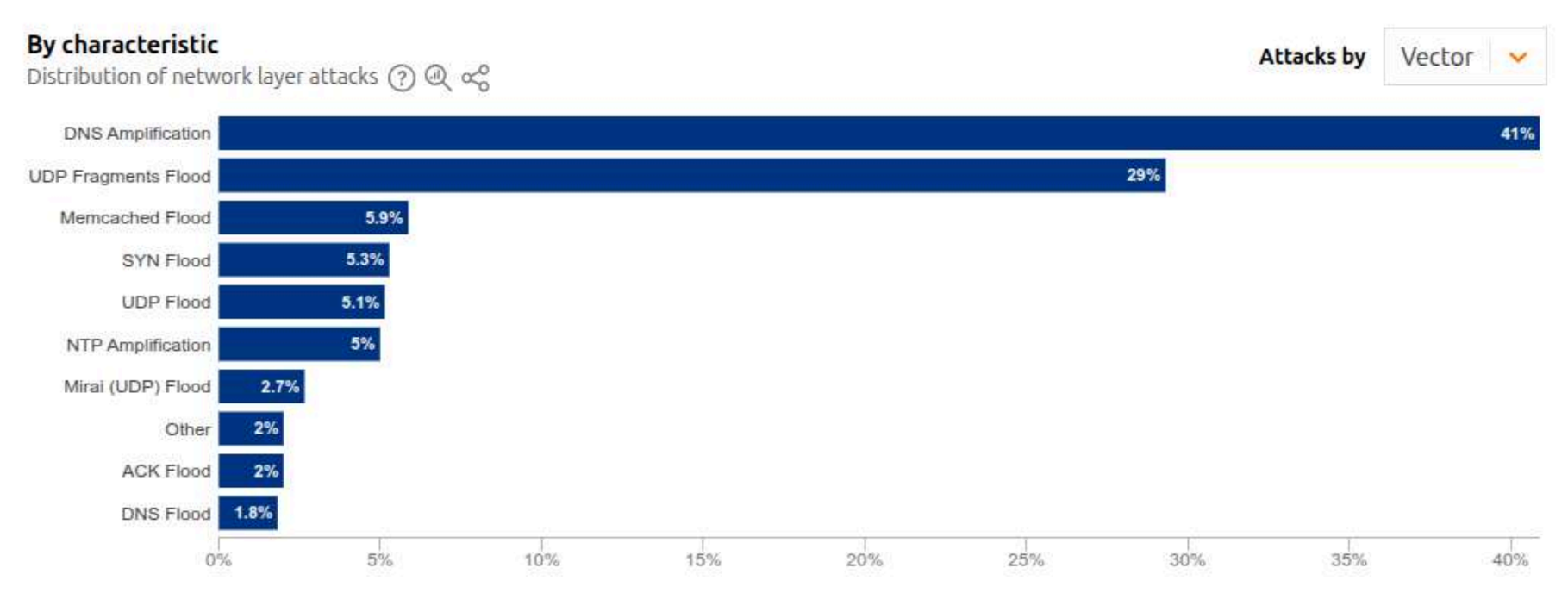


https://radar.cloudflare.com/

TheTeamPhoenix
Machine Secures Machines

Network Layer Attacks

by Country - Nepal

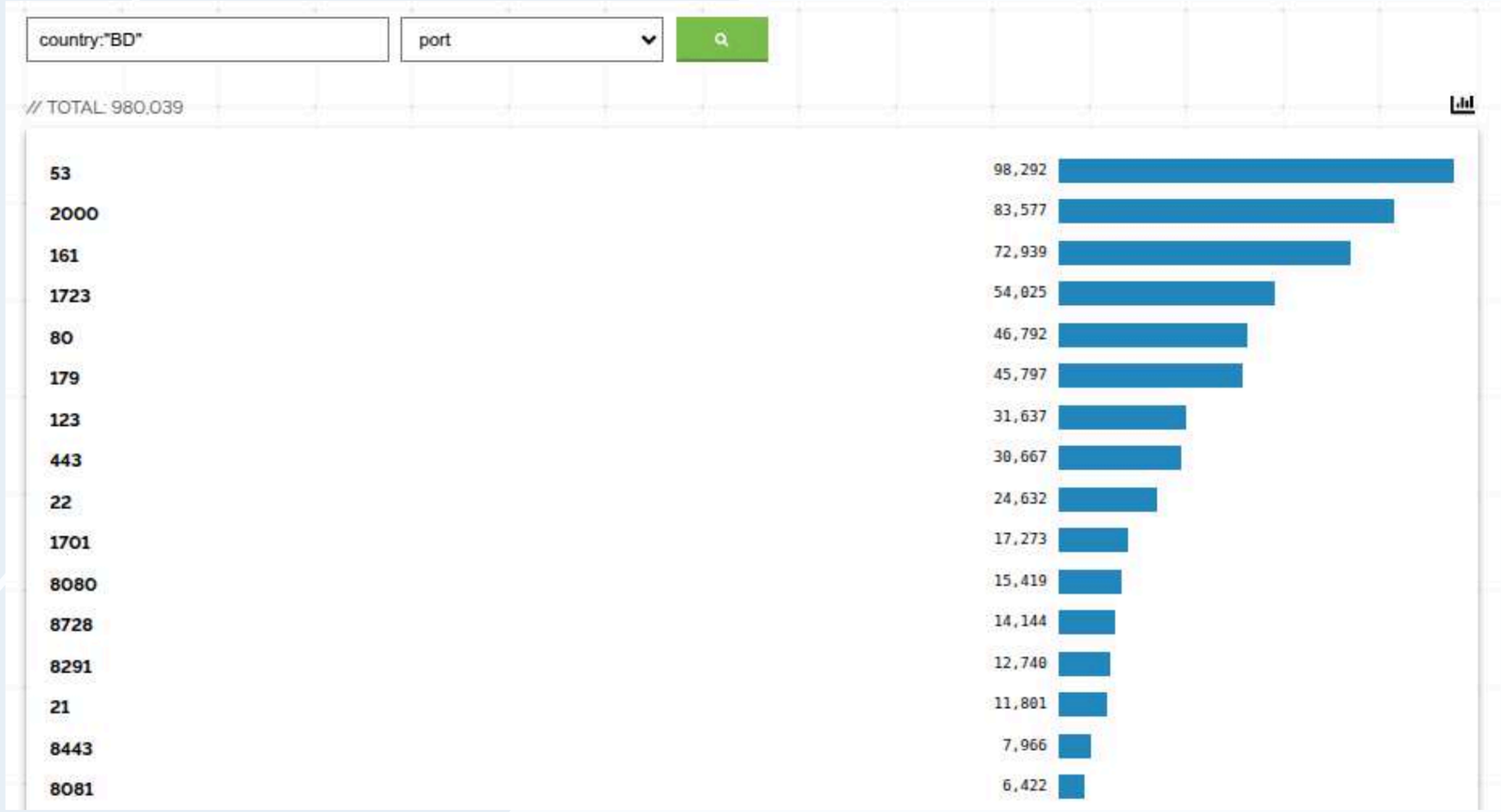


https://radar.cloudflare.com/

TheTeamPhoenix
Machine Secures Machines

Helping the Attackers?

by Country - Bangladesh

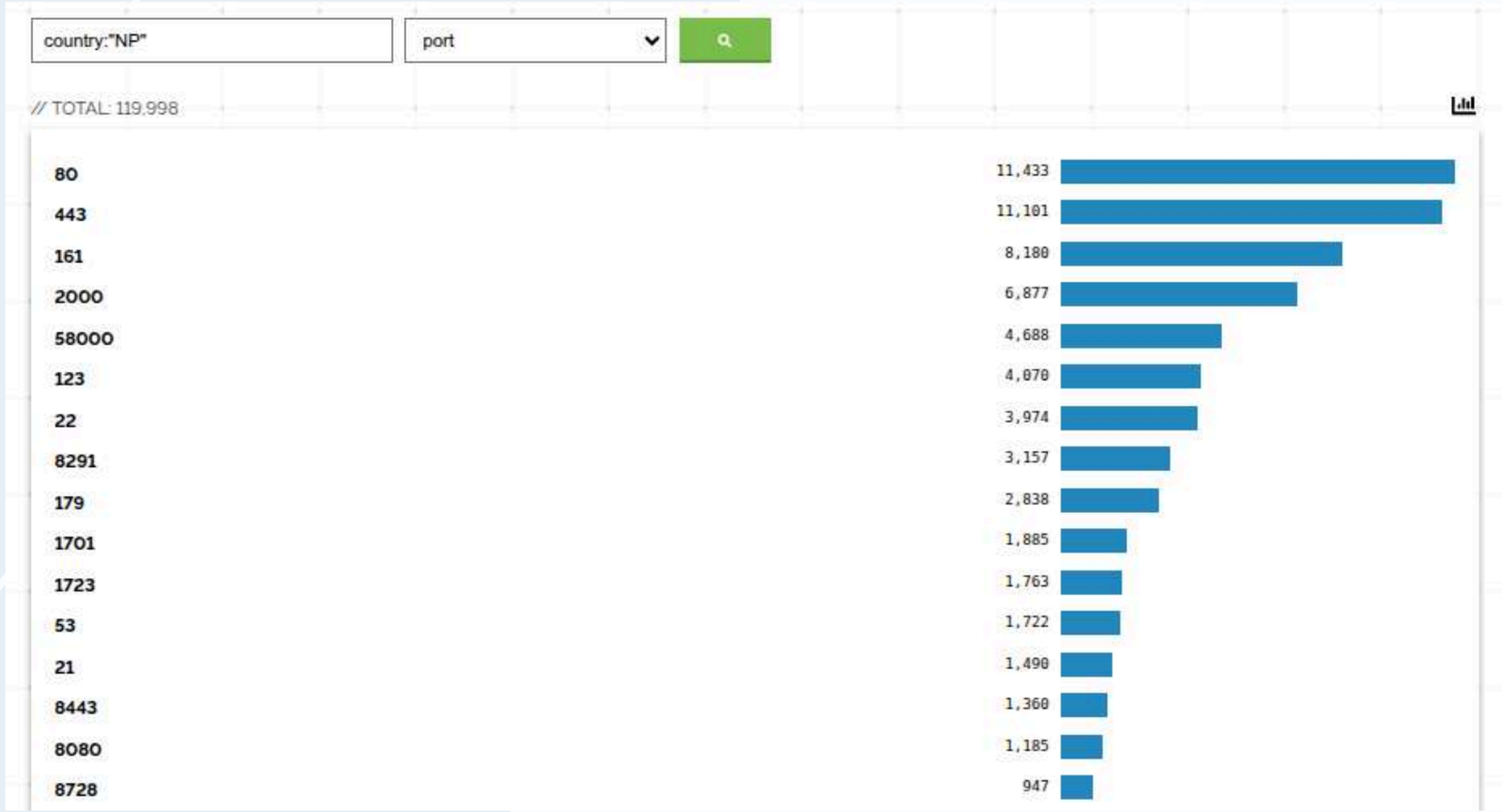


https://www.shodan.io/

TheTeamPhoenix
Machine Secures Machines

Helping the Attackers?

by Country - Nepal



https://www.shodan.io/

TheTeamPhoenix
Machine Secures Machines

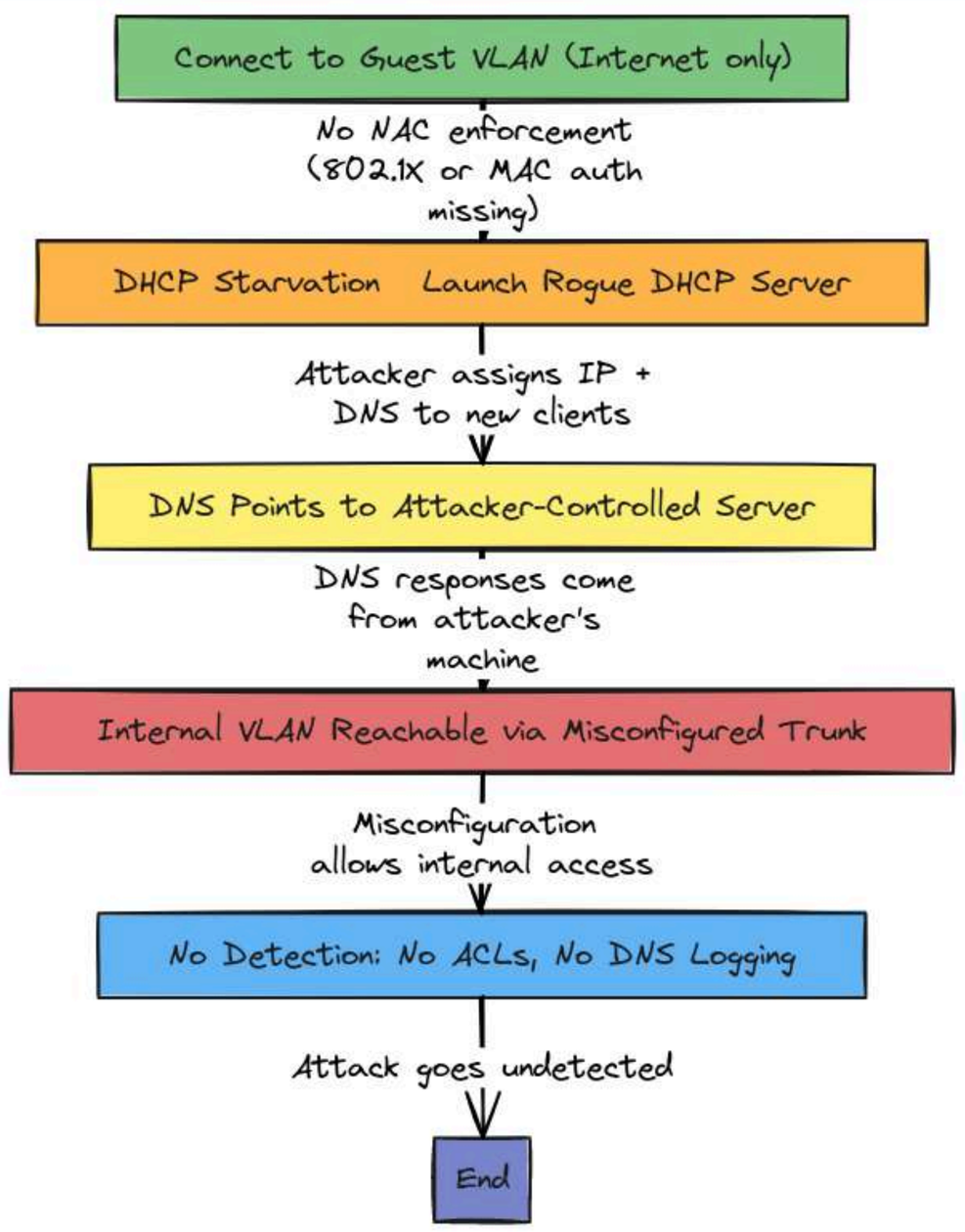
Offensive TTPs on Enterprise Networks

Understanding common Tactics, Techniques, and Procedures (TTPs) used by red teams to identify network vulnerabilities.

TTP	What It Is	Impact	Common Tools
ARP Spoofing / MITM	Redirects network traffic by falsifying ARP messages.	Intercepts, reads, and modifies data (credential theft, session hijacking).	bettercap
DHCP Starvation / Rogue DHCP	Starvation: Exhausts DHCP IP pool. Rogue: Sets up malicious DHCP server.	DoS attacks or attacker-controlled configurations.	dhcpd, yersinia
DNS Poisoning	Injects false DNS records into a resolver's cache.	Redirects users to malicious sites for phishing or malware distribution.	dnschef, mitm6
OSPF/BGP Injection	Manipulates routing protocols (OSPF internally, BGP externally).	Reroutes core traffic for surveillance, interception, or access.	Advanced/custom tools
NAC Bypass via MAC Spoofing	Impersonates an authorized device by spoofing its MAC address.	Bypasses Network Access Control (NAC) to gain unauthorized access.	OS utilities, macchanger

TheTeamPhoenix
Machine Secures Machines

Red Team Use Case: Guest VLAN to DNS Control



TheTeamPhoenix
Machine Secures Machines

Red Team Use Case: Guest VLAN to DNS Control

Why This Is Powerful

- No exploits: Just misconfig and default behavior
- Common: Many guest networks have basic firewalling but allow DHCP
- Undetected: If DNS logs aren't monitored or ACLs don't block rogue DHCP, it slips through

Layer	Tool	Signal
DHCP	Zeek	Unknown DHCP IP
DNS	Zeek	Short TTL, mismatched A
L2	ARPWatch	MAC/IP anomalies

“Prevention is ideal, but DETECTION is a must!

“Knowing your Offense is the best defense!

TheTeamPhoenix
Machine Secures Machines

Detection Engineering: Network Layer

Layer	Tool	Detection Use
L2	ARPWatch, Zeek	Detect spoofing
L3	NetFlow, ACL logs	Lateral movement
L4	Suricata	Traffic signature
L7	Zeek scripting	DNS tunnels, C2

TheTeamPhoenix
Machine Secures Machines

The Purple Loop: Offense Drives Network Resilience

Red Team Action	Blue + NetOps Response
Rogue DHCP → Attacker's DNS	Enable DHCP snooping + Zeek DHCP script
DNS Poisoning with dnschef	Zeek rule for TTL/mismatch + SIEM alert
WPAD / NTLM credential hijack	Block WPAD in DNS + add responder alerting

TheTeamPhoenix
Machine Secures Machines

Recommended Network Security Tools

Tool	Use Case
Zeek	L7 protocol analysis
Suricata	IDS/IPS
Arkime	Full PCAP inspection
NetBox + NMAP	Infra discovery & validation
NetFlow/sFlow	L3+ visibility
NAC (802.1X)	Access enforcement

TheTeamPhoenix
Machine Secures Machines

Recommended Practice

Network Resilience Requires Adversarial Thinking; DO Quarterly

- Simulate rogue DHCP or DNS
- Evaluate switch/router auth (SNMPv3, ACLs)
- Don’t just patch BGP — patrol your internal traffic; Deploy Zeek on internal SPAN/TAPs
- Capture 24–48 hrs of east-west NetFlow
- Check firewall rules between internal VLANs
- Connect with Intel from CloudFlare Radar and Shodan.
- Work with DNSRPZ/Pi-Hole project to work with DNS-based IOCs.
- Update your system and application with the latest patch.

“If your network is flat, your security is fantasy.”

Reference

- Verizon Data Breach Investigations Report (DBIR) 2024 – for breach stats.
- MITRE ATT&CK & D3FEND – for structured adversary techniques and defensive mapping.
- CISA “Known Exploited Vulnerabilities” Catalog – for trending network layer risks.
- FireEye/Mandiant Reports – for Red Team tactics.
- ENISA Threat Landscape Reports – for regulatory and European network defense posture.
- https://www.shodan.io/search/facet?query=country%3A%22NP%22&facet=port
- https://radar.cloudflare.com/security/network-layer/np?dateRange=24w
- https://thehackernews.com/2024/01/orange-spain-faces-bgp-traffic-hijack.html