Incident: Supply chain attack

NANGIJALA INTERNATIONAL AIRPORT

July-27-2018

On July 27th, Nangijala International Airport was targeted by supply chain attack. Attack was carried out by yet unknown threat actor. Threat actor used unpatched vulnerability on suppliers (HaiTek) operating system, and used existing VPN- service to gain access to airports systems.

Based on our findings, threat actor managed to penetrate into the AirPortSys database with administrative permissions. To achieve this, threat actor most likely used information found on HaiTek's compromised system (ex. List of passwords or otherwise weak credentials), since method of breach required only handful of attempts with few different usernames.

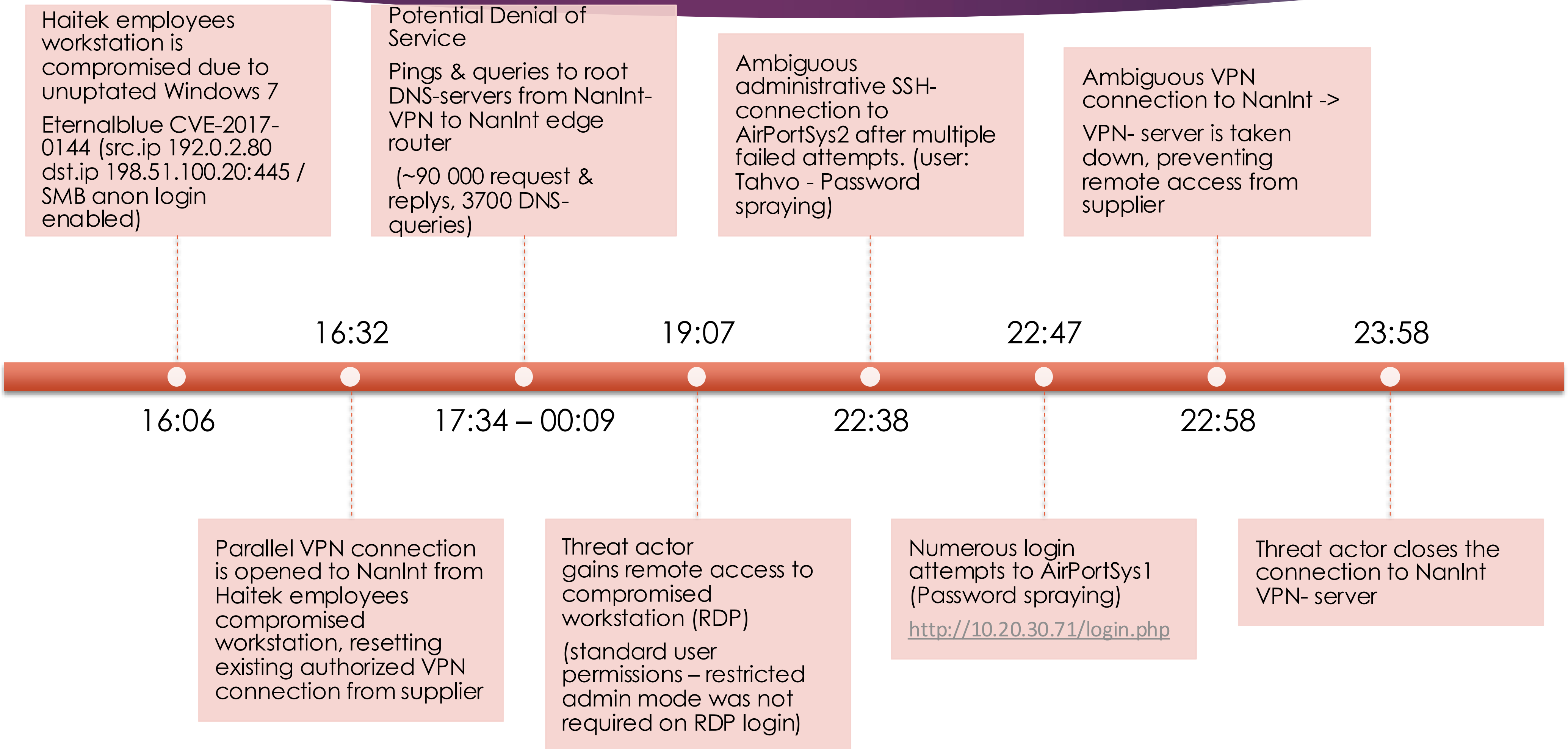
Initial investigation didn't conclude if the threat actor was able to exfiltrate data. However high amounts of TLS- encrypted traffic (due to VPN) was captured between C2 channel of airport to compromised HaiTek system.

Currently threat actor poses low threat. Airports operational capabilities remain unaffected, isolation and eradication can still be done with minimal effort. If left unchecked, threat actor can potentially create strong persistence, and move laterally to more critical systems.

At this time, TTPs of the threat actor suggest that the main goal was to gain access to AirPortSys1, that manages the presentation of info-boards, making them viable target for hacktivists to gain exposure. However more malicious intent is possible and shouldn't be overlooked. Further lateral movement from the compromised systems has not been detected.

TLP:AMBER+STRICT

Timeline of suspected breach



16:06

Haitek employees workstation is compromised due to unuptated Windows 7

Eternalblue CVE-2017-0144 (src.ip 192.0.2.80 dst.ip 198.51.100.20:445 / SMB anon login enabled)

16:32

Parallel VPN connection is opened to NanInt from Haitek employees compromised workstation, resetting existing authorized VPN connection from supplier

17:34 – 00:09

Potential Denial of Service

Pings & queries to root DNS-servers from NanInt-VPN to NanInt edge router

(~90 000 request & replys, 3700 DNS-queries)

19:07

Threat actor gains remote access to compromised workstation (RDP)

(standard user permissions – restricted admin mode was not required on RDP login)

22:38

Ambiguous administrative SSH-connection to AirPortSys2 after multiple failed attempts. (user: Tahvo - Password spraying)

22:47

Numerous login attempts to AirPortSys1 (Password spraying)

http://10.20.30.71/login.php

22:58

Ambiguous VPN connection to NanInt ->

VPN- server is taken down, preventing remote access from supplier

23:58

Threat actor closes the connection to NanInt VPN- server

TLP:AMBER+STRICT

Incident Response & Urgent Actions

- Containment & Eradication
  - Block the malicious address from suppliers side
  - Isolate Affected systems (AirPortSys2, NanInt-vpn)
  - Reduce attack-surface by temporarily disabling AirPortSys1
  - Check affected systems for possible footholds & persistence
  - Remediate vulnerabilities in supply chain
    - Urgent updates to OS (supplier-side)
    - Security best-practises for SMB & RDP (ex. no anonymous logins)

- Recovery
  - Restore the systems carefully to their pre-incident stage (if backupped)
  - Validate systems
  - Apply security patches & harden systems (Defence In Depth)

- Other Notes
  - Consider increasing the budget for your cybersecurity posture – We at LouTek care about our partners and provide you with 24/7 monitoring and technical support to prevent attacks, ensure resilience and enhance response time.