

Hacker's Fingerprints pt. 4

Data Theft Through Credentials
Compromise

Pavel Minarik

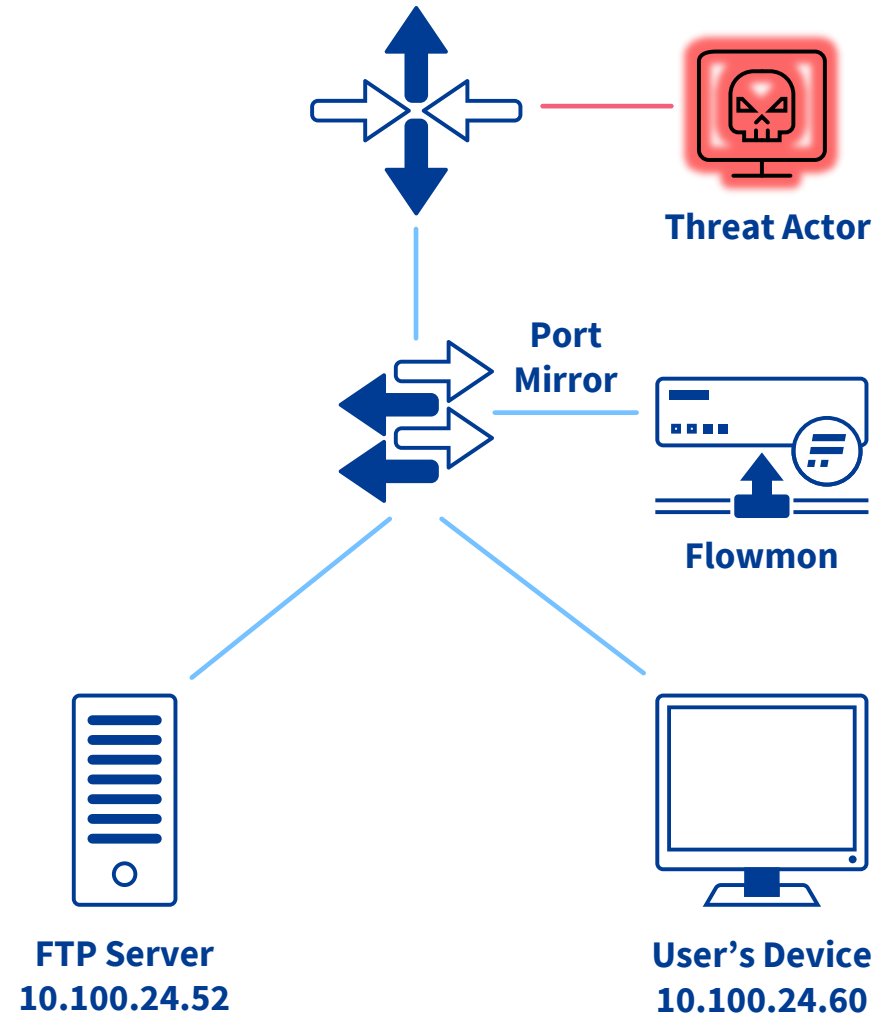
VP Technology

24th Sept 2024, AFCEA KB12



Data Theft Through Credentials Compromise

- Tricked by malicious login prompt, a user provided credentials not secured with MFA
- Full scenario replicated in lab environment
- All network activity recorded and made available for education purposes
- **Actors:**
 - User's device (10.100.24.60)
 - FTP server (10.100.24.52)
- **Objectives:**
 - Get access to company network
 - Locate and steal sensitive company data



Malicious Login Prompt

When accessing social networks, user is tricked by “malvertising” and redirected to fake Microsoft login page

The image shows a screenshot of the TikTok mobile application interface. On the left, the navigation menu includes 'For You', 'Following', 'Explore', 'LIVE', and 'Profile'. A 'Log in' button is visible below the menu. The main feed displays two videos. The first video, by user 'hanicka.9', has the caption '#judge #fyp' and 2.3M likes. The second video, by user 'kazma_kazmitch', has the caption 'I've dropped a million dollars out of helicopter to people...' and 1.6M likes. A large, semi-transparent overlay on the right side of the screen displays a fake Microsoft login page. The overlay features the Microsoft logo, the text 'Sign in', an email input field containing 'jim.smith@example.com', and buttons for 'Back' and 'Next'. Below the overlay, there is a 'Sign-in options' section with a key icon.


Initial Access

User accesses TikTok social network where attacker is gathering credentials

Type Communication with blacklisted hosts (BLACKLIST)













Subtype Application
Reports devices that communicate with blacklisted applications.

Detail TikTok (TikTok), attempts: 11, uploaded: 31.72 KiB, downloaded: 8.23 MiB, frequently used ports: 443.

Detection time	2024-01-03 16:11:13	Event source	 10.100.24.60	Probability	100 %
Last update	2024-01-03 16:16:13	Captured source hostname	N/A	False positive	No
First flow	2024-01-03 16:10:53	MAC address	00:50:56:bf:a0:2f	Detected by instance	Default
		User identity	N/A	Data feed	Default

TARGETS (4) COMMENTS (0) CATEGORIES (0) ATTRIBUTES EVENT EVIDENCE RELATED IDS EVENTS (245)

ALL IP ADDRESSES BY COUNTRY BY IP BY APPLICATION

   2.16.1.34	   23.76.204.5	   129.158.250.181	   1.37.42.235
---	---	---	--


Initial Access

User was redirected to a phishing site, provided credentials and attacker has now open access to the network

Type Communication with blacklisted hosts (BLACKLIST)


Subtype Web
Reports devices that communicate with a blacklisted website. This may indicate that the device is compromised or takes part in malicious activities depending on the category of the blacklisted HTTP hostname or SNI. The detection is performed using HTTP hostname or SNI string from an encrypted communication.

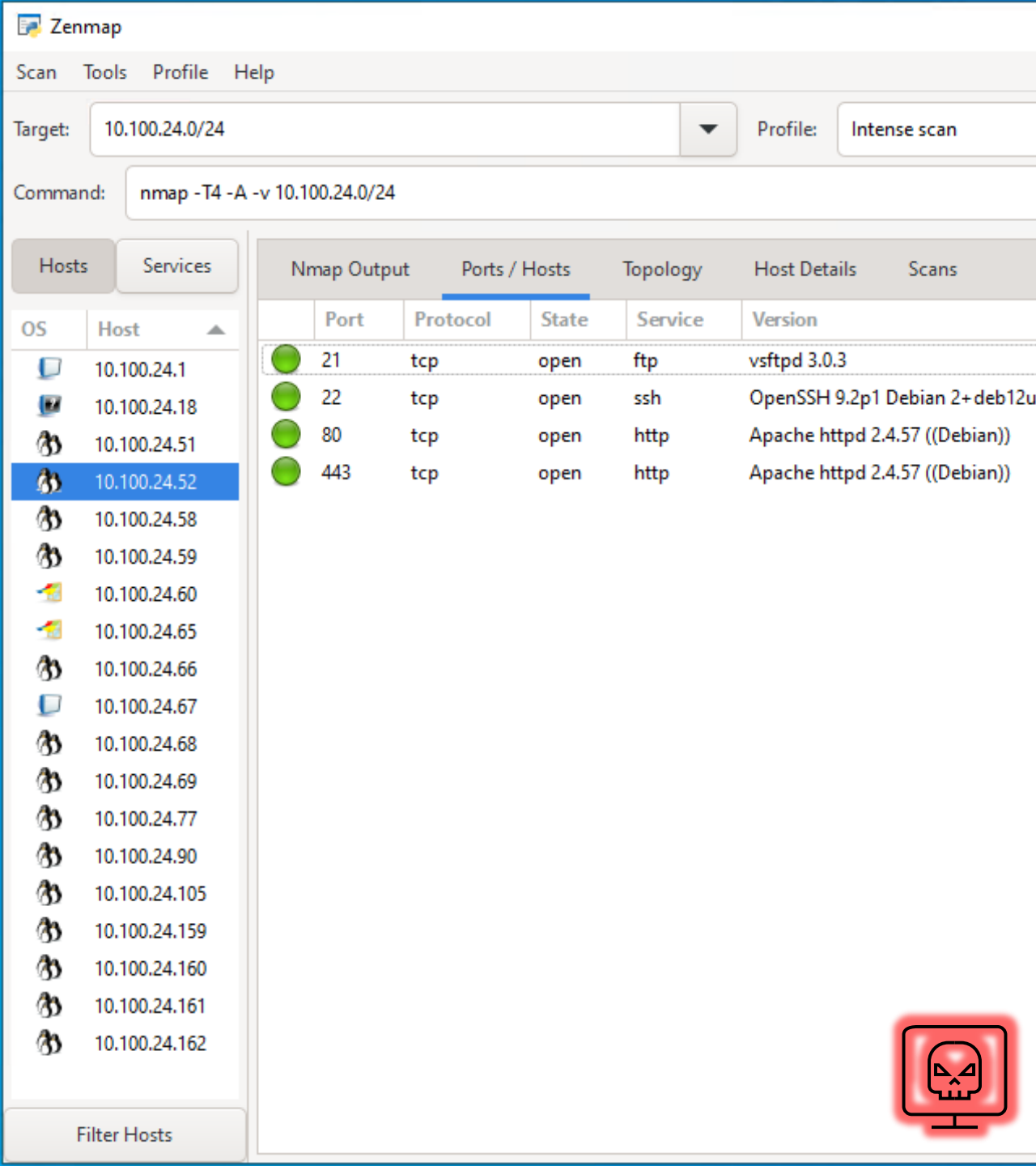
Detail Phishing (02e4675179a3.godaddysites.com / Known M365 phishing domain), attempts: 1, uploaded: 1.98 KiB, downloaded: 6.14 KiB, frequently used ports: 443.

Detection time	2024-01-03 16:11:31	Event source	 10.100.24.60	Probability	100 %
Last update	2024-01-03 16:11:31	Captured source hostname	N/A	False positive	No
First flow	2024-01-03 16:10:58	MAC address	00:d2:b1:95:9d:d5	Detected by instance	Default
		User identity	N/A	Data feed	Default

TARGETS (1) COMMENTS (0) CATEGORIES (0) ATTRIBUTES EVENT EVIDENCE RELATED IDS EVENTS (245)

ALL IP ADDRESSES BY COUNTRY BY IP BY APPLICATION

 13.248.243.5



Reconnaissance & Discovery

Attacker has logged into VPN using the stolen credentials, gained access to the user's device and begins to scan the environment from there



Reconnaissance & Discovery

Attacker has logged into VPN using the stolen credentials, gained access to the user's devices and begins to scan the environment from there

Type Port scanning (SCANS)

Subtype TCPSYN
Reports scanning of the services using the TCP protocol. Only the flows with the set SYN flag are used for detection. Port scanning is a technique used to map the network environment and identify potential victims for subsequent attacks.

Detail Chaotic TCP SYN scan (attempts with response: 5300, attempts without response: 21806, targets: 830, port(s): 443, 22, 179, 3389, 1, 7999, 30, 19, 33, 37, ...).

MITRE ATT&CK

- Tactic Discovery >> Technique Network Service Discovery, Technique Network Share Discovery
- Tactic Reconnaissance >> Technique Active Scanning

Detection time	2024-01-03 16:11:57	Event source	10.100.24.60	Probability	100 %
Last update	2024-01-03 16:16:57	Captured source hostname	N/A	False positive	No
First flow	2024-01-03 16:10:58	MAC address	00:50:56:bf:a0:2f	Detected by instance	Default
		User identity	N/A	Data feed	Default

TARGETS (830) COMMENTS (0) CATEGORIES (0) ATTRIBUTES EVENT EVIDENCE RELATED IDS EVENTS (245)

ALL IP ADDRESSES BY COUNTRY BY IP **BY APPLICATION**

Unknown (830)

```
# hydra -L users.txt -P common_pas
16 by van Hauser/THC - Please do n

.org/thc-hydra) starting at 2024-0
er 1 server, overall 64 tasks, 700
vice ftp on port 21
/min, 275 tries in 00:01h, 6725 to
/min, 808 tries in 00:03h, 6192 to
0.24.52 login: anonymous passw
0.24.52 login: anonymous passw
0.24.52 login: anonymous passw
0.24.52 login: anonymous passw
0.24.52 login: anonymous passw
0.24.52 login: anonymous passw
0.24.52 login: anonymous passw
0.24.52 login: anonymous passw
0.24.52 login: anonymous passw
0.24.52 login: anonymous passw
hydra.restore was written. Type h
```



Credential Access

Attacker was able to find a way how to log into the company FTP server through brute force attack

Now the attacker can start to work on the objective and exfiltrate the data

Credential Access

Attacker is brute forcing an FTP server found in the company infrastructure

Type Dictionary attacks (DICTATTACK)

Subtype FTPProtocol
Reports the password-guessing attacks (dictionary or brute-force based) on an FTP server. This may indicate an attacker's activity to get unauthorized access to a service or a misconfigured device that is continuously trying to authenticate to a service unsuccessfully.

Detail FTP dictionary attack, attempts: 439, port(s): 21, attack duration: 4 min 49 s 20 ms, average time between attempts: 658 ms.

MITRE ATT&CK Tactic: Credential Access >> Technique: Brute Force: Password Guessing

Detection time	2024-01-03 16:21:01	Event source	10.100.24.60	Probability	100 %
Last update	2024-01-03 16:26:01	Captured source hostname	N/A	False positive	No
First flow	2024-01-03 16:20:01	MAC address	00:50:56:bf:bb:f1	Detected by instance	Default
		User identity	N/A	Data feed	Default

TARGETS (1) COMMENTS (0) CATEGORIES (0) ATTRIBUTES EVENT EVIDENCE RELATED IDS EVENTS (248)

ALL IP ADDRESSES BY COUNTRY BY IP BY APPLICATION

10.100.24.52

Lateral Movement

Attacker is moving the sensitive data from company FTP server over the local network

Type High volume of transferred data (HIGHTRANSF)

Subtype General
Reports devices within the monitored network that transfer large amounts of data within a short period. This may indicate an unexpected overload of the network (e.g. due to backup process or similar large data transfers). Such activity could be considered as legitimate depending on devices and services involved.

Detail Transferred: 688.86 MiB, top peer transfer: 688.86 MiB.

MITRE ATT&CK Tactic: Lateral Movement >> Technique: Lateral Tool Transfer

Detection time	2024-01-03 16:25:59	Event source	10.100.24.52 ▾	Probability	100 %
Last update	2024-01-03 16:31:00	Captured source hostname	N/A	False positive	No
First flow	2024-01-03 16:20:01	MAC address	00:50:56:92:50:c3 ▾	Detected by instance	Default
		User identity	N/A	Data feed	Default

TARGETS (1) COMMENTS (0) CATEGORIES (0) ATTRIBUTES EVENT EVIDENCE RELATED IDS EVENTS (25)

ALL IP ADDRESSES BY COUNTRY BY IP BY APPLICATION

10.100.24.60 ▾

Command and Control

Attacker is using evasion techniques such as resolving domain names using DNS over HTTPS

Type Communication with DoH servers (DOHDET)

Subtype KnownServers
Reports devices in the monitored network that use DNS over HTTPS (DoH) protocol to resolve domain names. This detection was performed based on the regularly updated list of publicly known DoH servers. The DoH protocol aims to increase privacy and security by performing the process of domain resolution via an encrypted channel. It uses the same port as HTTPS protocol to hide DoH traffic inside the regular HTTPS traffic. From the monitoring perspective, it is impossible to determine which domains a device resolves when it uses this protocol. Therefore, the protocol may be misused to bypass network security policy or hide malicious malware activities.

Detail A device that uses DNS over HTTPS (DoH) protocol was detected. Data downloaded: 5.7 KiB, uploaded: 3.37 KiB. Domain names of the used DoH services: dns.quad9.net.

MITRE ATT&CK Tactic: Command and Control >> Technique: Protocol Tunneling

Detection time	2024-01-03 16:33:01	Event source	10.100.24.60	Probability	100 %
Last update	2024-01-03 16:33:01	Captured source hostname	N/A	False positive	No
First flow	2024-01-03 16:25:22	MAC address	00:d8:61:fb:fd:32	Detected by instance	Default
		User identity	N/A	Data feed	Default

TARGETS (1) COMMENTS (0) CATEGORIES (0) ATTRIBUTES EVENT EVIDENCE RELATED IDS EVENTS (125)

ALL IP ADDRESSES BY COUNTRY BY IP BY APPLICATION

9.9.9.9

Command and Control

Attacker is using evasion techniques such as dynamic resolution to avoid detection

Type Random domain name (RANDOMDOMAIN)

Subtype General
Reports the usage of randomly generated domain names. This kind of domain names may be used by malware for communication with its Command and Control servers.

Detail Access to randomly generated domains was detected. Domains: rc49h14cwhsj36craqtprhve61.com.

MITRE ATT&CK Tactic: Command and Control >> Technique: Dynamic Resolution

Detection time	2024-01-03 16:26:15	Event source	10.100.24.60	Probability	100 %
Last update	2024-01-03 16:31:16	Captured source hostname	N/A	False positive	No
First flow	2024-01-03 16:25:52	MAC address	00:50:56:bf:a0:2f	Detected by instance	Default
		User identity	N/A	Data feed	Default

TARGETS (1) COMMENTS (0) CATEGORIES (0) ATTRIBUTES EVENT EVIDENCE RELATED IDS EVENTS (125)

ALL IP ADDRESSES BY COUNTRY BY IP BY APPLICATION

3.220.158.139

Exfiltration

Attacker has exfiltrated the company data via an encrypted communication channel

Type Data upload anomaly (UPLOAD)

Subtype General
Reports devices that excessively upload data outside of the allowed network segment. This may indicate the use of services outside of the allowed network segment or even malicious activity (e.g. data exfiltration).

Detail Uploaded: 1.47 GiB, downloaded: 1.75 MiB, port(s): 443, 43365.

MITRE ATT&CK Tactic Exfiltration >> Technique Automated Exfiltration

Detection time	2024-01-03 16:27:54	Event source	10.100.24.60	Probability	100 %
Last update	2024-01-03 16:27:54	Captured source hostname	N/A	False positive	No
First flow	2024-01-03 16:25:52	MAC address	00:50:56:92:50:c3	Detected by instance	Default
		User identity	N/A	Data feed	Default

TARGETS (1) COMMENTS (0) CATEGORIES (0) ATTRIBUTES EVENT EVIDENCE RELATED IDS EVENTS (125)

ALL IP ADDRESSES BY COUNTRY BY IP BY APPLICATION

3.220.158.139


Backdoor Leftover

Attacker has implanted a malware/backdoor for easy access in the future


Type Malware Command and Control Activity Detected (2044254)

Detail ET MALWARE Win32/WhiskerSpy - FTP - Observed Creds

References <http://www.threatexpert.com/report.aspx?md5=cdf9e79b37ae70fb19b504f81e655d2a>

Detection time	2024-01-03 16:27:09	Event source	 10.100.24.60	Log source interface	idsp_eth2_out
Last update	2024-01-03 16:27:09	User identity	N/A	Log source IP	127.0.0.1
First flow	2024-01-03 16:27:05	Source port	41680		
		Destination port	21		

TARGETS (1) RELATED FLOWS ATTRIBUTES RELATED IDS EVENTS (3)

  3.220.158.139

Attack Summary

Hacker's fingerprints left in the network detected as events and interpreted through the lens of MITRE ATT&CK

