# Executive Summary:

## Assets:

|  |  |  |  |
| --- | --- | --- | --- |
| Hosts | IPv4 | IPv6 | Details |
| WINDMILLDC | 10.10.200.6 | fe80:0:0:0:397e:3b48:f27a:d3cc |  |
| KARIM | 10.10.200.11 | - |  |
| BRURYA-PC | 10.10.200.16 | - |  |
| METUSHELAH-PC | 10.10.200.20 | - |  |
| YEHOSHPHAT | 10.10.200.24 | - |  |
| DESKTOP-VOA929U | 10.10.200.26 | - |  |
| BOYDEM | 10.10.180.6 | - | Shared Drive |

## Users:

|  |  |  |
| --- | --- | --- |
| Domain/Local PC | User | Details |
| BRURYA-PC | Administrator |  |
| WINDMILL | aadi |  |
| WINDMILL | Administrator |  |
| WINDMILL | fabian |  |
| WINDMILL | fatima |  |
| WINDMILL | hican |  |
| WINDMILL | it |  |
| WINDMILL | nancyn |  |
| WINDMILL | vladg |  |
| Window Manager | DWM-1 |  |
| Window Manager | DWM-2 |  |
| Window Manager | DWM-3 |  |
| Window Manager | DWM-4 |  |
| Window Manager | DWM-5 |  |
| Window Manager | DWM-6 |  |
| Window Manager | DWM-7 |  |
| Window Manager | DWM-8 |  |
| YEHOSHPHAT | Administrator |  |

## IOCs:

|  |  |  |
| --- | --- | --- |
| Binary | Hash Value (SHA1) | Details |
| PAExec-4300-DESKTOP-VOA929U.exe | 820DEE796573B93F154CFA484C35354E41EF7A51 | Hacktool |
| PAExec-1272-DESKTOP-VOA929U.exe | 820DEE796573B93F154CFA484C35354E41EF7A51 | Hacktool |
| xlbwvnv.exe | E6285770991890378CC3176E63D0230AB5AC9F1C | Password Dumping tool |
| nmuxssiml.exe | E6285770991890378CC3176E63D0230AB5AC9F1C | Password Dumping Tool |
| hsjdove.exe | E6285770991890378CC3176E63D0230AB5AC9F1C | Password Dumping tool |
| AtomPortable.exe | 4700B8EF0B890D80268979F98D8F6F701DC7E30F | Portable Text Editor |
| polarclock3.exe | B7182ABD084C1962F7E91F4F07104C56B2DB2277 | Trojan |
| SecurityScan\_Release.exe | 5fb57acb3e2b845da0ca24a28bba2c66bb4e222e |  |

## Timeline of attack:

# Detailed Findings:

## Initial Detection:

Investigation Notes:

Failed Attempts:

From our observations, our initial detection was from a query on failed logons from detected suspicious activity at 20/3/2017 4:16:17 pm UTC and 20/3/2017 4:16:43 pm UTC of 2 failed login attempts from account james towards KARIM workstations via caller process name C:\Windows\PAExec-3992-DESKTOP-VOA929U.exe and PAExec-5260-DESKTOP-VOA929U.exe.

Drilling down to the login period to see what occurred prior to the login and to see the child processes and activities spawned. We observed that for both the failed attempts, prior to the respective events we observe the following details:

1. Prior to the events we observed that there was a local logon to KARIM with the Administrator account from DESKTOP-VOA929U (10.10.200.26)which are evident by the Windows Event ID 4776 and 4624 events.

2. We observed a user mode service, PAExec-3992-DESKTOP-VOA929U and PAExec-5260-DESKTOP-VOA929U.exe at the respective timeframe, installed on to KARIM to start manually when requested and running under Local System Account.

This is suspicious logon via this process is typically not normal, and when investigating the hash of the binary via OSINT, we detected that this is PAExec.exe. While typically a tool

designed for system administrators, like PsExec, PAExec can be exploited by malicious actors to execute unauthorized commands on remote systems. If an attacker gains access to an administrator's credentials, they could use PAExec to move laterally within a network, executing harmful scripts or installing malware without detection.

However, after the failed login attempts from the process, there were no further events or processes spawned. Hence, continuing the investigation in the next sections.

Logon 1

Investigating further on the usage of this binary, we see that there were multiple occurrences of successful logons via use of explicit credentials (Windows Event 4624 and 4648) on KARIM and WINDMILLDC. On KARIM, we observed that the account used that was successful was WINDMILL\fabian on 20/3/2017 4:17:18 pm UTC and 20/3/2017 4:35:27 pm UTC.

On WINDMILLDC, we can also see that there were 5 successful logins with WINDMILL\administrator account between 20/3/2017 4:47:44 pm UTC and 20/3/2017 4:50:07 pm UTC.

From KARIM workstation, we drilled down to the login period to see what occurred prior to the login and to see the child processes and activities spawned.

Prior to the event, we observed that there was a local logon to KARIM with the Administrator account from DESKTOP-VOA929U (10.10.200.26) at 20/3/2017 4:17:17 pm UTC, evident by the Windows Event ID 4776 and 4624 events.

After the logon event, at 20/3/2017 4:17:18 pm UTC, we observed a user mode service, PAExec-4380-DESKTOP-VOA929U, installed on to KARIM to start manually when requested and running under Local System Account.

Sequentially, at the same timing we had the following observations:

1. Command C:\Windows\PAExec-4380-DESKTOP-VOA929U.exe -service was automatically ran to start up the service.

2. Kerberos Authentication Ticket (TGT) (Event ID 4768) and Kerberos Service Ticket (Event ID 4769) were requested towards windmill.local domain for user account fabian towards WINDMILLDC from KARIM.

3. Occurrence of successful logons via use of explicit credentials (Windows Event 4624 and 4648) with user WINDMILL\fabian

This leads us up to the detection we had where WINDMILL\fabian successfully logon on 20/3/2017 4:17:18 pm UTC via PAExec-4380-DESKTOP-VOA929U.exe process.

Event that triggered sequentially after are as follows:

1. Multiples Kerberos Authentication Ticket (TGT) (Event ID 4768) and Kerberos Service Ticket (Event ID 4769) requested with varying TicketOptions towards WINDMILLDC from KARIM.

2. Multiple successful logon events with fabian account on WINDMILL domain towards WINDMILLDC from KARIM.

3. From the PAExec-4380-DESKTOP-VOA929U.exe binary, it triggered a command qwinsta, likely to perform reconnaissance activities since it can display all active Remote Desktop sessions on the local machine.

4. Multiple subsequent SMB requests towards WINDMILLDC, which is potentially an attempt to perform lateral movement to the domain controller to establish control.

Logon 2

Continuing with the investigation, we decided to add an additional focus on any login attempts from DESKTOP-VOA929U as an indicator and we observed that 20/3/2017 4:20:38 pm UTC, there was another logon from DESKTOP-VOA929U with KARIM\Administrator user.

This time we observed another service installed in a similar manner, hsjdove.exe, after the logon. We observed a ProcessCreate event (Sysmon ID 1) for the binary hsjdove.exe followed by CreateRemoteThread event (Sysmon ID 8) at the same timestamp where the binary is creating a thread within the lsass.exe process.

This is highly suspicious because of the fact that hsjdove.exe (a non-standard executable name) is creating a thread in lsass.exe and since lsass.exe handles sensitive operations related to authentication, compromising it can allow attackers to steal credentials or perform other malicious actions.

Additionally, checking the binary on OSINT, we confirm with high confidence that this is a Password Dumping tool. It is likely that the Threat Actor is attempting to perform collect passwords through this malicious binary.

Logon 3

Next logon attempt from DESKTOP-VOA929U was detected on 20/3/2017 4:32:01 pm UTC with KARIM\Administrator.

Similar to the previous logon, we saw another service installed in a similar manner, nmuxssiml.exe, after the logon. We observed a ProcessCreate event (Sysmon ID 1) for the binary hsjdove.exe followed by CreateRemoteThread event (Sysmon ID 8) at the same timestamp where the binary is creating a thread within the lsass.exe process.

Checking the hash value of this binary, we can confirm nmuxssiml.exe and hsjdove.exe are the same, both reported on OSINT as a Password Dumping tool. It is likely that the Threat Actor is attempting to perform collect passwords through this malicious binary as well.

Logon 4:

On 20/3/2017 4:35:26 pm UTC, we observed similar sequential events to the first successful logon event observed.

1. A local logon to KARIM with the Administrator account from DESKTOP-VOA929U (10.10.200.26) at 4:35:26 pm UTC, evident by the Windows Event ID 4776 and 4624 events.

2. Observed a user mode service, PAExec-956-DESKTOP-VOA929U, installed on to KARIM to start manually when requested and running under Local System Account.

3. Command C:\Windows\PAExec-956-DESKTOP-VOA929U.exe -service was automatically ran to start up the service.

4. Kerberos Authentication Ticket (TGT) (Event ID 4768) and Kerberos Service Ticket (Event ID 4769) were requested towards windmill.local domain for user account fabian towards WINDMILLDC from KARIM.

5. WINDMILL\fabian successfully logon on 4:35:27 pm UTC via PAExec-956-DESKTOP-VOA929U.exe process.

6. Multiples Kerberos Authentication Ticket (TGT) (Event ID 4768) and Kerberos Service Ticket (Event ID 4769) requested with varying TicketOptions towards WINDMILLDC from KARIM.

7. Multiple successful logon events with fabian account on WINDMILL domain towards WINDMILLDC from KARIM.

8. Next, we observed that command ""c:\temp\sysmon.exe" -x \\10.10.200.6 -u windmill.local\it -p !qaz2wsX " being run as a child process of the command C:\Windows\PAExec-956-DESKTOP-VOA929U.exe -service. This is suspicious because there is an attempt to run Sysmon on WINDMILLDC with the credentials windmill.local\it and its password. So far, we do not see signs of which this is successful on the logs.

9. We can continue to see multiple logons with WINDMILL\fabian account to KARIM evident by the Windows Event ID 4776 and 4624 events.

10. Multiple subsequent SMB requests towards WINDMILLDC, which is potentially an attempt to perform lateral movement to the domain controller to establish control.

At 4:37:41 pm UTC, on KARIM, we observed a logon type 11 from process consent.exe with account WINDMILL\it and at 4:37:54 pm UTC, we observed another logon type 11 from process consent.exe with account WINDMILL\Administrator.

We can see that at 4:37:54 pm UTC SystemPropertiesRemote.exe was run with the same logonID 0x2223A5C for WINDMILL\Administrator. While there were no resultant actions, potentially it could be to test the privilege level of the account.

Logon Type 11, which is categorized as CachedInteractive, it specifically refers to a scenario where a user logs on using cached credentials rather than contacting a domain controller and consent.exe process plays a role in managing UAC prompts for actions requiring elevated privileges after such logins. This is likely an indicator which the Threat Actor is collecting the cached credentials for privileged accounts.

At 4:38:35 pm UTC and 4:38:58 pm UTC, you can see that 2 logon failures were observed (Event ID 4625) from DESKTOP-VOA929U\fabian and DESKTOP-VOA929U\Administrator on KARIM. However, it is likely when testing the account credentials, either through a script or through the Threat Actor actions, change to the account domain was not done.

At 20/3/2017 4:39:26 pm UTC and 20/3/2017 4:39:27 pm UTC, logon was tested again on WINDMILL account domain with the Administrator account on KARIM, and this time logon was successful on Logon Type 3, evidently by Windows Event ID 4776 and 4624 events.

We can confirm that the WINDMILL\Adminstrator account has been compromised at this point.

This is critical because essentially the Threat Actor can use this account to access any assets managed by the domain controller and the domain controller itself.

At this point we can also consider KARIM compromised.

Looking at between 20/3/2017 4:39:34 pm UTC and 20/3/2017 5:09:35 pm UTC on KARIM, we can see the WINDMILL\Administrator login on logon id 0x2231DBF, there are various commands being run likely to attempt to hide the malicious activities being performed on the host and to get ready to perform the next phase of the compromise.

Some notable commands ran potentially by the Threat Actor are as follows:

1. Rdpclip at 20/3/2017 4:39:34 pm UTC which allows clipboard synchronization between devices in a remote desktop session likely to copy something from between KARIMe and then paste it into his own device.

2. sysmon.exe -x \\10.10.200.6 at 20/3/2017 4:40:50 pm UTC from C:\Temp\ folder, where looks like an attempt to run sysmon with parameters related to remote execution or configuration on WINDMILLDC.

We are also suspicious of certain applications being used at the same time on KARIM such as the ones we observed below:

1. At 20/3/2017 4:39:47 pm UTC, we see ServerManager.exe being used in the same logon session, and subsequently we see a successful logon attempt on WINDMILLDC.

2. Command "C:\Program Files\VMware\VMware Tools\vmtoolsd.exe" -n vmusr ran at 20/3/2017 4:39:57 pm UTC as well, and subsequently see another successful logon attempt on WINDMILLDC.

These 2 observations based on the application type could indicate that the Threat Actor is attempting to use other methods to attempt to hide their activities and establish persistence. For example use of Threat Actors may exploit vmtoolsd.exe to run malicious commands or scripts within a virtual machine environment. Since it operates under the context of a legitimate service, malicious activities could be obscured from standard monitoring tools and use Server Manager for remote management capabilities to manipulate systems without direct interaction.

Logon to DC:

At 4:40:50 pm UTC we start seeing multiple successful logon events from KARIM to WINDMILLDC with WINDMILL\Administrator account evident by the Windows Event ID 4776 and 4624 events.

Subsequently we start seeing the same actions being performed earlier on KARIM but this time on WINDMILLDC:

1. At 4:40:50 pm UTC, service xlbwvnv.exe installed after the logon. We observed a ProcessCreate event (Sysmon ID 1) for the binary xlbwvnv.exe followed by CreateRemoteThread event (Sysmon ID 8) at the same timestamp where the binary is creating a thread within the lsass.exe process. Checking the hash, this is the same as the earlier malicious services which were installed.

2. Multiple subsequent SMB requests from KARIM towards WINDMILLDC were observed.

3. This time round, we are seeing around 24 failed logins attempts with the Administrator account between 4:47:07 pm UTC and 4:47:44 pm UTC from DESKTOP-VOA929U, but failure is due to use of DESKTOP-VOA929U as the account domain for 22 of the failed logon events. Whereas 2 of the failed logon attempts were due to wrong password when attempting to logon with the administrator account on windmill.local account domain. This is likely a script ran by the user on DESKTOP-VOA929U but not edited properly causing such an error.

4. At 4:47:44 pm UTC, a successful login to WINDMILLDC was made from DESKTOP-VOA929U.

Initial detection was on BRURYA-PC, at 20/3/2017 11:11:02 am, where we observed a logon type 2, a local logon via Administrator account. From which, at 11:11:05 am we observed that Administrator user interacted with various files and performed various activities but most interestingly the user accessed the shared drive BOYDEM and interacted with the suspicious binary AVG\_Protection\_Free\_1606.exe.

### Process Tree:

[0]: Process ID: 516, C:\Windows\System32\winlogon.exe

[1]: Process ID: 3196, C:\Windows\System32\userinit.exe

[2]: Process ID: 1436, C:\Windows\explorer.exe

[3]: Process ID:6052, \\10.10.180.6\share\Installs\AVG\_Protection\_Free\_1606.exe

[4]: Process ID: 5884, C:\Windows\Temp\7zS4A7386A2\avgsetupx.exe

[5]: Process ID: 5884. C:\Program Files (x86)\AVG\Setup\avgsetupx.exe"

[6]: Process ID: 2440, C:\Program Files (x86)\AVG\Setup\avgsetupx.exe"

[6]: Process ID: 6344, "C:\Program Files (x86)\AVG\Setup\avgOfferTool.exe" -checkChrome -elevated

[6]: Process ID: 6488, "C:\Windows\Temp\AvgSetup\463e0055-0364-47cf-bafa-d119107c2d7a\install\fmw\avgrdsttesta.exe"

[6]: Process ID: 2992, "C:\Windows\Temp\AvgSetup\463e0055-0364-47cf-bafa-d119107c2d7a\install\fmw\avgrdsttestx.exe"

[6]: Process ID: 6680, "C:\Windows\Temp\AvgSetup\463e0055-0364-47cf-bafa-d119107c2d7a\install\bav\avg\_free\_antivirus\_setup\_online.exe

[6]: Process ID: 180, "C:\Program Files (x86)\AVG\Setup\avgsetupx.exe" /cp=82c64164-0365-47cf-bafa-d119107c2d7a

From Process ID: 6680

[6]: Process ID:

Second detection of the malicious loader was at 20/3/2017 11:13:40 am where user “it” access the shared drive BOYDEM and interacted with the malicious binary AVG\_Protection\_Free\_1606.exe with LogonId 0x487316, on host KARIM. However, it appears to not have been successful as the suspicious binary drop was not observed, hence, likely through Logon Type 11, where the Threat Actor got the network credentials of the Administrator account stored on the host on LogonID 0x1A84303, and again access the attempt to run the AVG\_Protection\_Free\_1606.exe, this time successfully interacting with the file to start the process.

0x1c96412

METH 0xcfe62