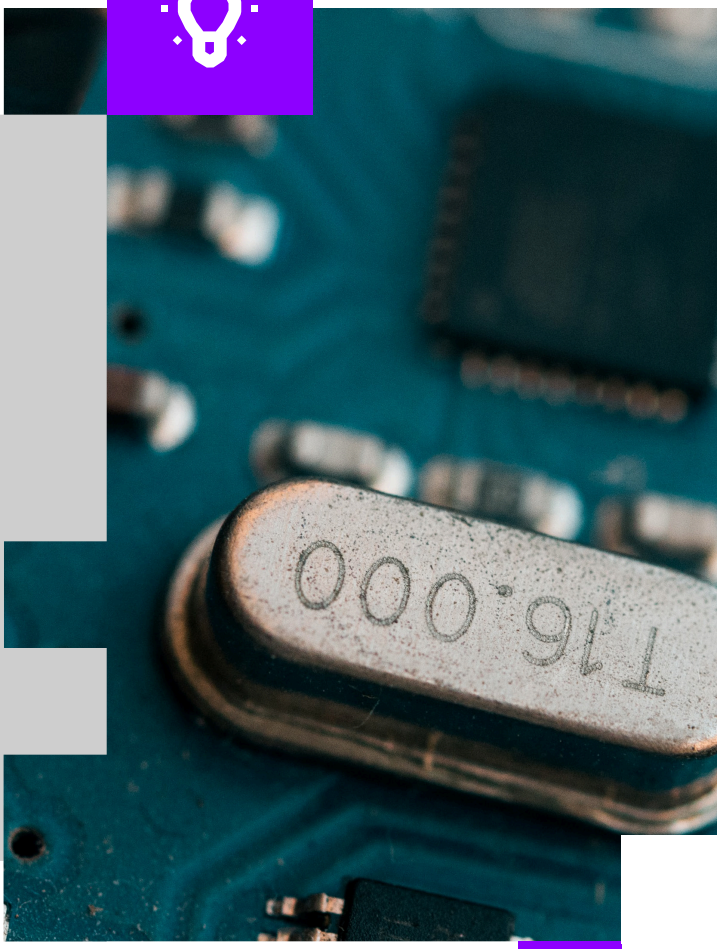
exabeam

UEBA

Advanced Analytics Use Case: Detecting Compromised Credentials

Keith Buswell, Senior Sales Engineer



Stolen credentials have been a persistent problem, and organizations have yet to effectively solve that problem. Every week, we hear about credential-stuffing attacks where a threat actor successfully steals credentials, logs in to the environment and moves laterally to gain higher-level access. All activities have a single focus: to access private data or high-value assets. The MITRE ATT&CK knowledgebase provides information about tactics, techniques and procedures used by threat actors that can help security teams build stronger security processes. Exabeam is successfully helping organizations detect these activities through analytics, including mapping the activities to MITRE. Here's an example of how I was able to help my customer with our analytics solution that is powered by machine learning.

Recently, I was working on a new Exabeam augmentation deployment on our customer's existing SIEM. Before we fully deployed Exabeam, we used a Syslog feed from the existing SIEM into our Exabeam analytics engine to start modeling the environment. During that time, Exabeam Advanced Analytics triggered a Notable User. From that point on, we saw the progression of the user's account to a compromised account through account switching and lateral movement. Here's how it unfolded.

On Thursday, May 7th Exabeam triggered a Notable User with a risk score of 93 points.

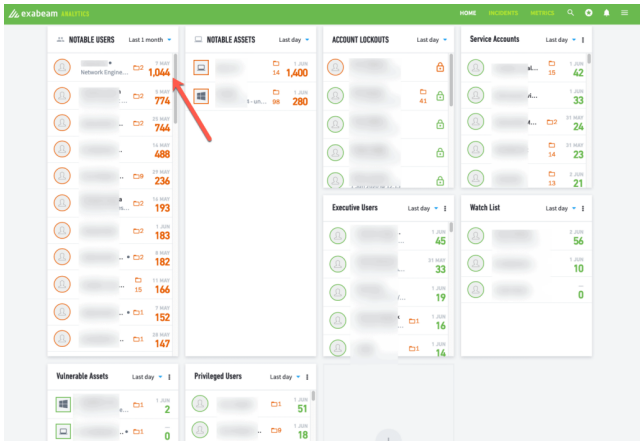


Figure 1: We first saw an unusual amount of activity for a user.

May 7, 22:20

The Trend Timeline gave a pretty clear indication that this was quite abnormal for the user.

Figure 2: Viewing this activity on the Trend Timeline shows the spike in contrast to normal activity for the user.

Using the dynamic KPIs, we can also see that in all of the previous days of activity the user does not normally generate this level of risk, use this many accounts or access this many assets.

Figure 3 and 4: Looking back at the user's behavior over the past days we can see there is no level of risk compared to the alerts we are seeing.

Drilling into the user details, we could quickly see a summary of why the user had become notable, but we clicked on the Timeline view to understand more of what happened.

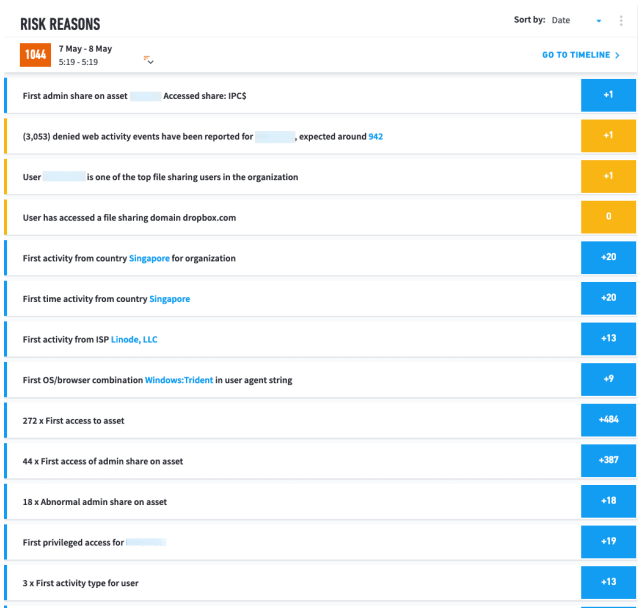


Figure 5: Looking more closely we can see how the risk reasons add up to a score of 1044.

Looking through the Timeline, at 21:15 we could see that Exabeam flagged 20 points of risk for the user VPNing in from Singapore. Since this has never been seen before from the user or anyone in the entire organization, it triggered an additional 20 points of risk. This user additionally received 22 more points of risk because they connected from an ISP that has never been observed before from them along with connecting from a user-agent string that's never been associated with them prior.

The MITRE ATT&CK techniques used at this stage were External Remote Services (**T1133**) and Valid Accounts (**T1078**).

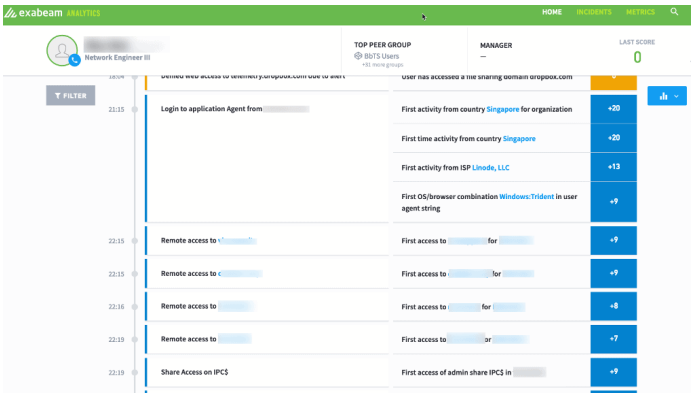


Figure 6: Exabeam flagged the user with 20 points of risk as they were VPNing in from Singapore, another 20 points since neither the user nor anyone in the entire organization had this activity and added 22 more points for connecting from a new ISP.

Drilling into the data model shows that we've clearly seen them typically connect from a Windows machine using Mozilla, but never Trident, which is why this risk was applied to their timeline.

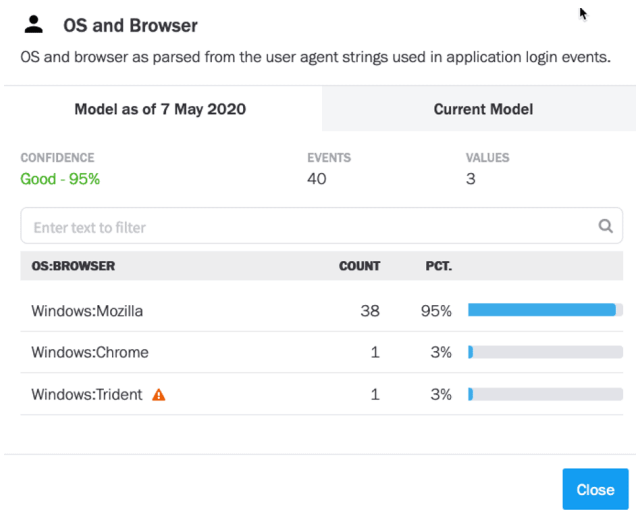


Figure 7: The activity is flagged as the user typically connects from a Windows machine using Mozilla, not Trident.

The user was now at 62 points of risk on their timeline. One hour later at 22:15, the user started accessing assets that have never been observed before for them, with each one flagging 10 points of risk. Two Assets at 22:15 added 20 more points of risk, and another at 22:16 gave this user the 93 points of risk crossing the global threshold to become notable. This is when the alert went out to investigate this individual.

At this point, 100% of the risk applied to their timeline was based on behavior deviations from the abnormal logon location to access assets they either don't normally touch or never touch.

May 8, 3:48

After hundreds of attempts to hit other assets, the user was finally able to find credentials to switch to and laterally move off the initial host. Exabeam stitched this into the timeline as an account switch activity and displayed the username that was used originally and what they switched to and which host.

The MITRE ATT&CK techniques used were Discovery (**TA0007**), Account Discovery (**T1087**), Network Share Discovery (**T1135**), Lateral Movement (**TA0008**), Remote Services: Remote Desktop Protocol (**T1021.001**)

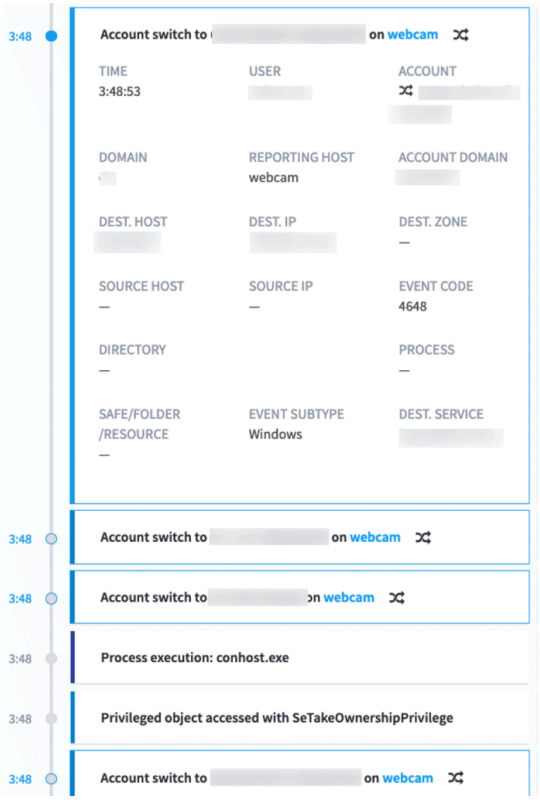


Figure 8: The user finds credentials to switch to and laterally moves off the initial host.

Unfortunately, this organization did not currently have a 24/7 SOC to manage security alerts throughout the night, and the user went on to access a total of 487 assets via 233 dumped credentials from Mimikatz, then laterally moved off the initially compromised host to another asset in the environment. Through that asset, another 60 credentials were dumped and attempted to be used throughout the environment.

Because this organization was using Exabeam Entity Analytics, they also observed the asset the user laterally moved to become notable at 03:04 the next morning, once again due to behavioral changes on the asset.

Mimikatz is a credential dumper capable of obtaining plain text account logins and passwords. This tool is detected by techniques as described in the MITRE ATT&CK framework like Account Manipulation (**T1098**), Credential Dumping (**T1003**), Rogue Domain Controller (**T1207**) and more.

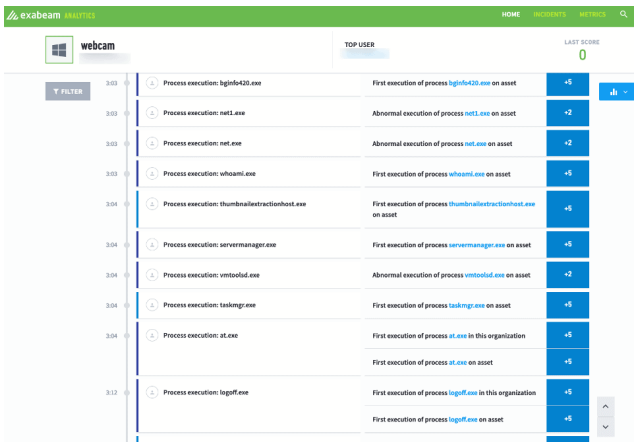


Figure 9: The compromised user continues moving through the organization.

Shortly after Exabeam triggered a Notable Asset, the customer's EDR tool lit up as well with notifications of Mimikatz tools being used. These alerts were also stitched into the Assets Timeline, further accelerating the overall risk score.

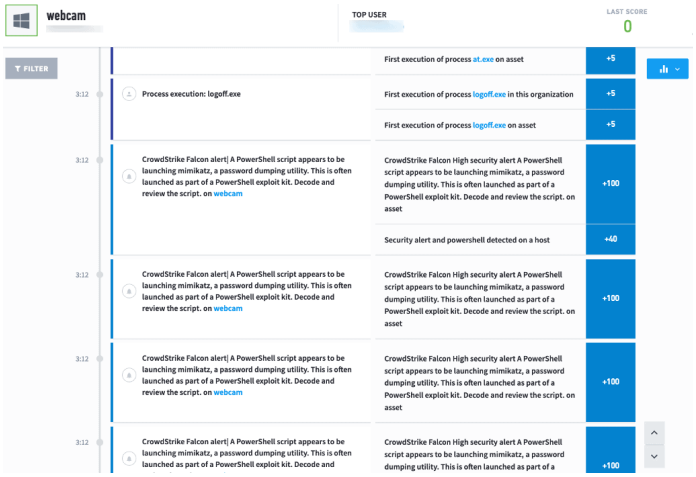


Figure 10: Alerts from the customer's EDR tool shows notifications of Mimikatz tools being used.

Exabeam Timelines and modeling were able to trigger a Notable User and Asset completely off of behavioral driven aspects, while also clearly stitching together the events to fully understand what happened while the attack was ongoing.

To recap, Exabeam Advanced Analytics detected a Notable User at 22:19. The first access with the compromised credentials happened at 21:15, which was slightly over one hour from time to detect compromised credentials. This is usually tagged as a Valid Accounts (**T1078**) technique in the MITRE ATT&CK framework, which is done together by the adversary to laterally move across different assets after gaining credentials.

The first alert the team received from their EDR tool was at 03:12 the next morning from the Mimikatz execution. Organizations that believe that you can simply send your alerts into a security orchestration, automation, and response **(SOAR) solution** and be protected would have missed the most important parts of this attack. Since the EDR only detected Mimikatz, an analyst would have needed to manually query logs to recreate this attack, including initial infection, lateral movement and credential dumping.

Per the MITRE ATT&CK framework, there are techniques used in a credential access tactic like dumping credentials in the form of a hash or clear text password (**T1003**). Once the adversary gains unauthorized access to internal systems adversaries, they can exploit remote services (**T1210**).

There was no customization to the Advanced Analytics install, and it was supported only by a straight Syslog feed from the customer's existing SIEM into Advanced Analytics for the entire chain. From my experience, it takes legacy SIEMs often days or even months to get relevant content created, even more if you have not written or created the rules on how you predict you'll be attacked.

The customer was pleased to see the sheer amount of detail on the attack, considering the solution hadn't even been customized yet. Perhaps most notable, though, was the fact that the customer, who knew very little about the environment, was able to read through the log and know exactly what had happened. They appreciated that even less senior analysts could use this software to get results immediately. The customer was able to perform their entire investigation without having to write a single query or comb through raw logs to try to answer some of the most critical questions.

About Exabeam

Exabeam helps security teams outsmart the odds by adding intelligence to their existing security tools – including SIEMs, XDRs, cloud data lakes, and hundreds of other business and security products. Out-of-the-box use case coverage repeatedly delivers successful outcomes. Behavioral analytics allows security teams to detect compromised and malicious users that were previously difficult, or impossible, to find. Automation helps overcome staff shortages by minimizing false positives and dramatically reducing the time it takes to detect, triage, investigate and respond. For more information, visit www.exabeam.com.

exabeam

To learn more about how Exabeam can help you visit exabeam.com today.