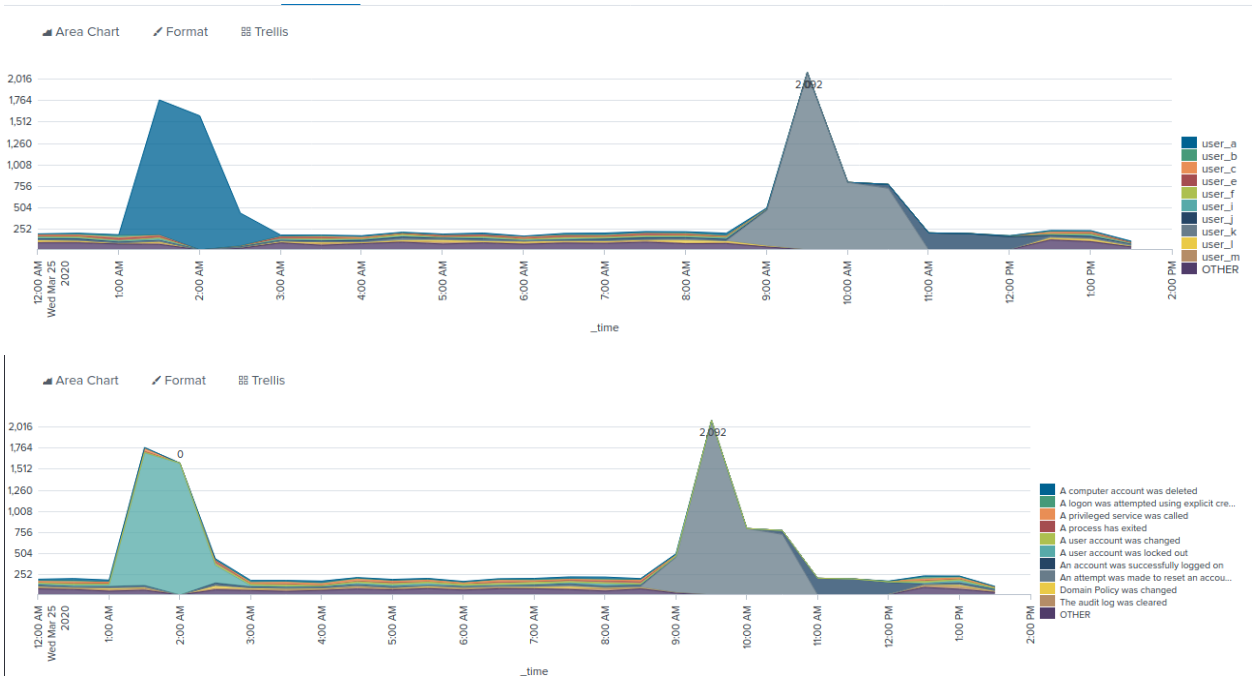
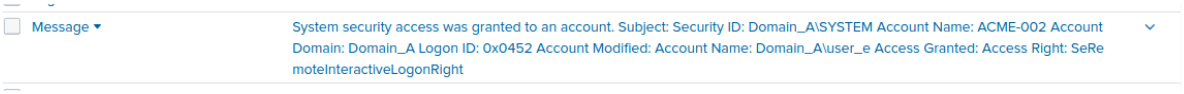
Cameron Wright

Splunk Project Part 2

Part 1 Windows Server Attack
User K - Over the period of approximately 2 hours after the users account was successfully logged on there were over 2000 attempts to reset the users password.



Most Importantly there was system security granted to an account by user_k for the Domain_A where Access was granted for Remote Interactive Logon.



To mitigate against this I would suggest implementing an access control list and remove user privilege to be able to make changes to system security settings.

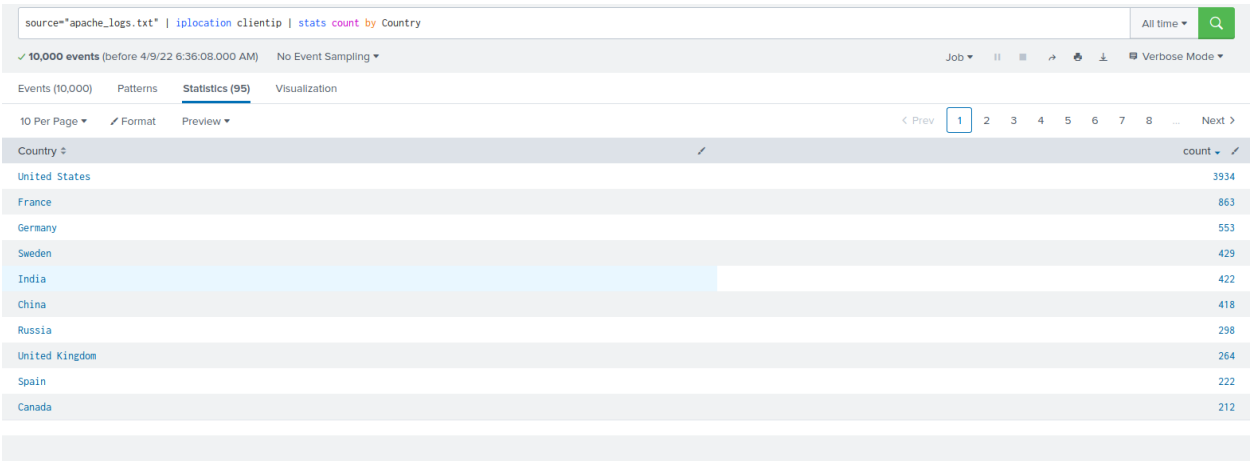
User A
The Majority of attacks that the account of User A were involved in was to do with the user account being locked out. Although this points to some sort of password security policy already being in place, however the amount of times the account was locked out in the matter of a few hours was cause for concern. I believe if a user account see's more then 10 lockouts within an hour then they should need to use alternative means to authenticate before access is granted.

Global Solution.
I think the safest and most efficient method of further preventing this type of attack in the future and to secure the company assets and users would be to implement some sort of multi factor

authentication. I also believe there needs to be access rights given to the intended employee's and not just every user.

2.
The easiest solution would be to whitelist employees by IP, block attempted attacker IP address and to implement multifactor authentication so the attackers would not lockout the accounts by only entering a bad password.

Part 2 Apache Webserver Attack
Q1. As you can see from both logs below the only real difference between the normal logs and the attack logs were Ukraine, from this data I would add a firewall rule that would 'Block all incoming traffic from any IP address located in the Country Ukraine"
Normal Logs

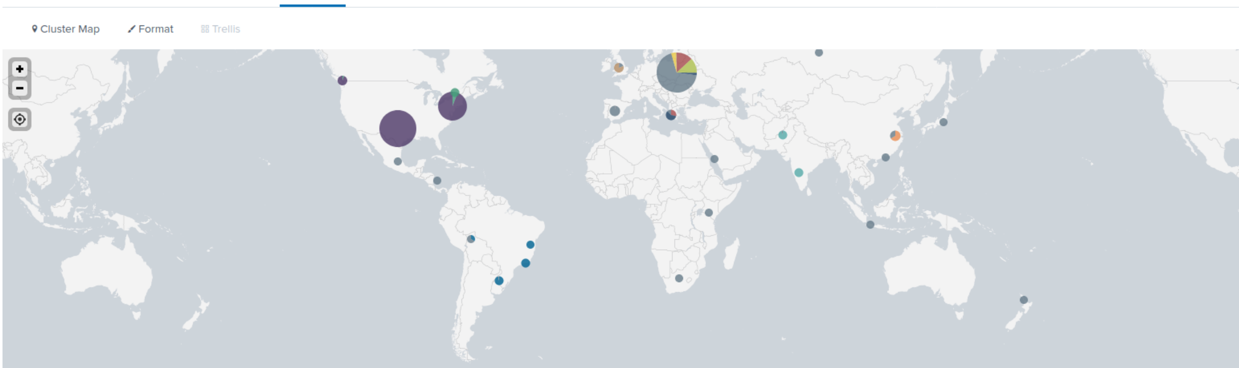


Country	count
United States	3934
France	863
Germany	553
Sweden	429
India	422
China	418
Russia	298
United Kingdom	264
Spain	222
Canada	212

Attack Logs

Country	count
United States	2027
Ukraine	877
France	195
Sweden	192
Germany	154
Spain	108
Canada	82
Italy	77
United Kingdom	69
Brazil	67

Attack Logs



Q2. The only other similarities i could find were the user_agent being used

Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; SV1; .NET CLR 2.0.50727987787; InfoPath.1)

The number of bytes 65748

The req_time 25/Mar/2020:20:05:59 +0000

These three things were all consistent with traffic originating from Ukraine. The only problem is that there was a lot of traffic coming from the United States with the same values. First I would need to assure that the traffic originating in the United States was safe. If this was true then I would create the following rules

“Block all HTTP traffic with the user_agent = Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; SV1; .NET CLR 2.0.50727987787; InfoPath.1),”

“Block all HTTP traffic which Byte size = 65748”

“Block all HTTP traffic which req_time = 25/Mar/2020:20:05:59 +000”

If I was certain that the traffic matching these values that originated in the United States was safe then I would add “Except from the Country=United States” for each rule.

>	3/25/20 8:05:59.000 PM	apache_attack_logs.txt	-	Ukraine	25/Mar/2020:20:05:59 +0000	65748	-	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; SV1; .NET CLR 2.0.50727987787; InfoPath.1)
>	3/25/20 8:05:59.000 PM	apache_attack_logs.txt	-	Ukraine	25/Mar/2020:20:05:59 +0000	65748	-	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; SV1; .NET CLR 2.0.50727987787; InfoPath.1)
>	3/25/20 8:05:59.000 PM	apache_attack_logs.txt	-	Ukraine	25/Mar/2020:20:05:59 +0000	65748	-	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; SV1; .NET CLR 2.0.50727987787; InfoPath.1)
>	3/25/20 8:05:59.000 PM	apache_attack_logs.txt	-	United States	25/Mar/2020:20:05:59 +0000	65748	-	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; SV1; .NET CLR 2.0.50727987787; InfoPath.1)
>	3/25/20 8:05:59.000 PM	apache_attack_logs.txt	-	United States	25/Mar/2020:20:05:59 +0000	65748	-	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; SV1; .NET CLR 2.0.50727987787; InfoPath.1)