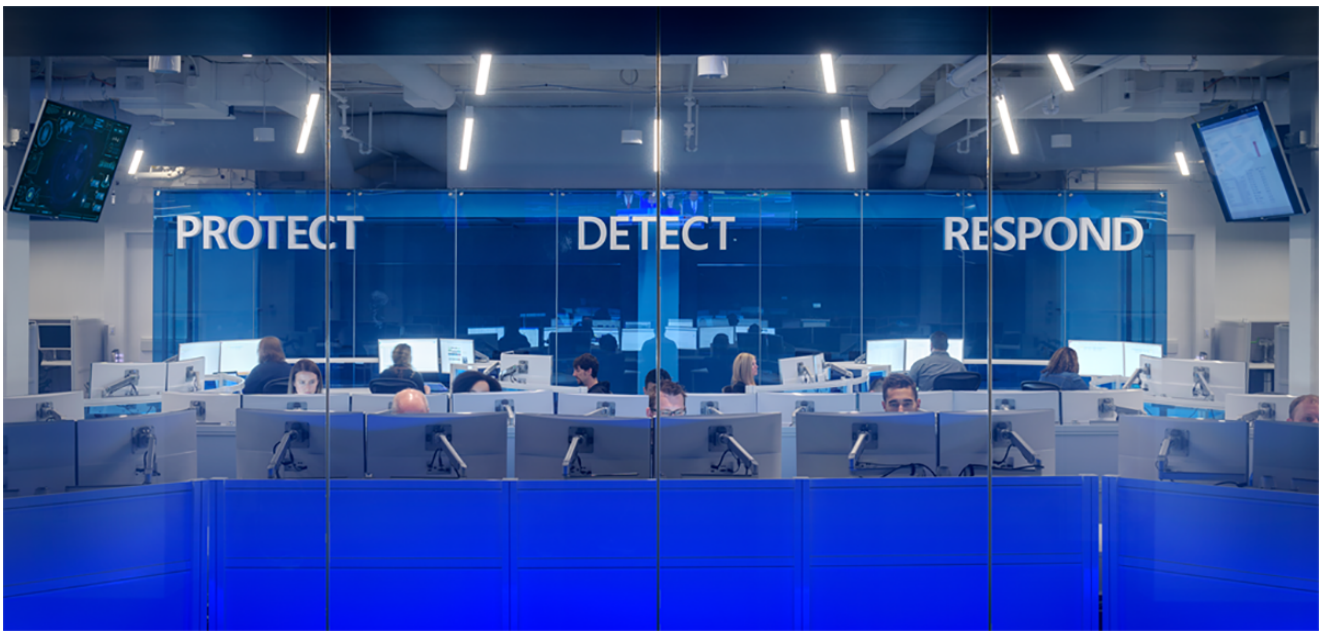
STRONTIUM: Detecting new patterns in credential harvesting

microsoft.com/security/blog/2020/09/10/strontium-detecting-new-patters-credential-harvesting/

September 10, 2020



Microsoft has tied STRONTIUM to a newly uncovered pattern of Office365 credential harvesting activity aimed at US and UK organizations directly involved in political elections. Analysts from Microsoft Threat Intelligence Center (MSTIC) and Microsoft Identity Security have been tracking this new activity since April 2020. Credential harvesting is a known tactic used by STRONTIUM to obtain valid credentials that enable future surveillance or intrusion operations. Subsequent analysis revealed that between September 2019 and June 2020, STRONTIUM launched credential harvesting attacks against tens of thousands of accounts at more than 200 organizations. In the two weeks between August 18 and September 3, the same attacks targeted 6,912 accounts belonging to 28 organizations. None of these accounts were successfully compromised.

Not all the targeted organizations were election-related. However, we felt it important to highlight a potential emerging threat to the 2020 US Presidential Election and future electoral contests in the UK.

Microsoft CVP Customer Security and Trust, Tom Burt provided some additional details on this campaign in his recent *On The Issues* blog post. The purpose of this post is to provide defenders in any organization, but especially those directly or indirectly affiliated with electoral systems, insight into the technical nature of this activity. By providing these details, we hope to enable better defense against future attacks and share best practices for securing cloud environments against this type of activity.

Tactical Details

STRONTIUM relied heavily upon spear phishing in its credential harvesting efforts leading up to the 2016 US presidential election. In 2016, spear-phishing was the most common tactic for stealing credentials from targeted accounts. This time around, STRONTIUM appears to be taking a different approach, namely, brute-force/password-spray tooling. This shift in tactics, also made by several other nation-state actors, allows them to execute large-scale credential harvesting operations in a more anonymized manner. The tooling STRONTIUM is using routes its authentication attempts through a pool of approximately 1,100 IPs, the majority associated with the Tor anonymizing service. This pool of infrastructure has evolved over time, with an average of approximately 20 IPs added and removed from it per day. STRONTIUM's tooling alternates its authentication attempts amongst this pool of IPs approximately once per second. Considering the breadth and speed of this technique, it seems likely that STRONTIUM has adapted its tooling to use an anonymizer service to obfuscate its activity, evade tracking, and avoid attribution.

During the two-week period, August 19 – September 3, STRONTIUM's credential harvesting tooling utilized a daily average of 1,294 IPs associated with 536 netblocks and 273 ASNs. Of these netblocks, some were much more heavily utilized by the tooling than others, both in terms of the total number of authentications attempted from them and the total number of IPs utilized within them. Figure 1 below represents the 5 netblocks from which the highest number of total auth attempts were observed. As highlighted in the table, several of these netblocks had much higher IP utilization rates than the rest. This observed behavior indicates that the underlying anonymization services providing the infrastructure backbone for STRONTIUM auth attempts are, in a sense, over-serving IPs in these specific netblocks.

Netblock	Netblock Country	Netblock Owner	Netblock ASN	IPs Available in Netblock	IPs in Netblock Utilized by Tooling	Netblock Utilization Percentage
199.249.230.0/24	[US]	[QUINTEX, US]	[62744]	256	72	28.125000
185.220.101.0/24	[DE]	[ASMK, NL]	[208294]	256	65	25.390625
23.129.64.0/24	[US]	[EMERALD-ONION, US]	[396507]	256	36	14.0625
109.70.100.0/24	[AT]	[APPLIEDPRIVACY-AS, AT]	[208323]	256	23	8.984375
185.220.102.0/24	[DE]	[ZWIEBELFREUNDE, AT]	[60729]	256	19	7.421875

Figure 1: Highest volume netblocks used in STRONTIUM auth attempts.

The fact that the anonymization service is over-serving specific netblocks gives defenders an opportunity to hunt for activity associated both with this STRONTIUM activity or other malicious tooling that is utilizing the same anonymization service. The following Azure

Sentinel query (GitHub link) is designed to identify failed authentication attempts from the three highest-signal, highest-utilization netblocks highlighted above, and group the results by UserAgent.

```
let lookBack = 30d;
OfficeActivity
| where TimeGenerated > ago(lookBack)
| where RecordType in ("AzureActiveDirectoryAccountLogon", "AzureActiveDirect
oryStsLogon")
| where Operation != 'UserLoggedIn'
| extend UserAgent = iff(parse_json(ExtendedProperties)[0].Name =~ "UserAgent
", extractjson("$[0].Value", ExtendedProperties, typeof(string)),"")
| mv-expand parse_json(ExtendedProperties)
| where ExtendedProperties.Name =~ "RequestType"
| extend RequestType = ExtendedProperties.Value
| where ClientIP startswith "185.220.101." or ClientIP startswith "199.249.23
0." or ClientIP startswith "23.129.64."
| summarize authAttempts=dcount(TimeGenerated), firstAttempt=min(TimeGenerate
d), lastAttempt=max(TimeGenerated), uniqueIPs=dcount(ClientIP), uniqueAccount
s=dcount(UserId), attemptedAccounts=make_set(UserId) by UserAgent
| sort by uniqueAccounts
```

Microsoft Threat Protection (MTP) also provides a platform for users to identify failed authentication attempts. The following query will give MTP users the ability to hunt and address these threats as well:

```
IdentityLogonEvents
| where Timestamp > ago(30d)
| where ActionType == "LogonFailed"
| where IPAddress startswith "185.220.101." or IPAddress startswith "199.249.230."
or IPAddress startswith "23.129.64."
| summarize authAttempts=dcount(Timestamp), firstAttempt=min(Timestamp), lastAtt
empt=max(Timestamp), uniqueIPs=dcount(IPAddress), uniqueAccounts=dcount(Account
ObjectId), attemptedAccounts=make_set(AccountObjectId)
by DeviceType, OSPlatform
| sort by uniqueAccounts
```

MSTIC has observed that the STRONTIUM tooling operates in two modes when targeting accounts: brute-force and password-spray.

In **password-spray mode**, the tooling attempts username: password combinations in a 'low-'n-slow' manner. Organizations targeted by the tooling running in this mode typically see approximately four authentication attempts per hour per targeted account over the course of several days or weeks, with nearly every attempt originating from a different IP address.

In **brute-force mode**, the tooling attempts many username: password attempts very rapidly for a much shorter time period. Organizations targeted by the tooling running in this mode typically see over 300 authentication attempts per hour per targeted account over the course of several hours or days.

Tooling Operating Mode	Avg ## of Attempts Per Account Per Hour	Avg # Of IPs Utilized for Auth Attempts Per Account Per Hour	Avg Length of Attack
Password-Spray	4	4	Days-Weeks
Brute-Force	335	200	Hours-Days

Organizations targeted by STRONTIUM using this tooling saw auth attempts against an average of 20% of their total accounts. In some instances, MSTIC assesses the tooling may have discovered these accounts simply by attempting authentications against a large number of possible account names until it found ones that were valid.

Guidance: Proactive defense

There are some very simple steps businesses and targeted individuals can take to significantly improve the security of their accounts and make these types of attacks much more difficult.

1. Enable multi-factor authentication

We have seen clear proof that enabling multi-factor authentication (MFA) across both business and personal email accounts successfully thwarts the majority of credential harvesting attacks. Our colleagues in Azure Active Directory put it more precisely—

> "… doing any form of MFA takes you out of reach of most attacks. MFA (using any mechanism) is just too costly to break – unless a highly motivated attacker is after *that* high-value account or asset."
>
> Blog: Your password doesn't matter—but MFA does!

However, most enterprise accounts have not implemented this simple protection:

> *"When we evaluate all the tokens issued with MFA claims, we see that **less than 10% of users use MFA per month in our enterprise accounts** (and that includes on-premises and third-party MFA). Until MFA is more broadly adopted, there is little reason for attackers to evolve."*
>
> Blog: All your creds are belong to us!

2. Actively monitor failed authentications

When monitoring login activity in your accounts, look for any type of discernable patterns in these failed authentications and track them over time. Password spray is an increasingly common tactic of nation-state actors.

You can also maintain broader visibility into behavioral anomalies like failed login attempts by running detections and monitoring using Microsoft Cloud App Security (MCAS) which monitors user sessions for third-party cloud apps, including G-Suite, AWS, and Salesforce. The MCAS detection engine looks for anomalous user activity for indicators of compromise. One indicator, “multiple failed login attempts,” can be used to create a dynamic baseline per user, across the tenant, and alert on anomalous login behavior that may represent an active brute force or password spray attack.

Microsoft Threat Protection (MTP) can help to automatically track and rebuild the Incident view of all the compromised identities by password-spray leveraged later by the attacker to expand the breach to endpoint or cloud assets.

3. Test your organization’s resilience

Attack Simulator in Office 365 ATP lets you run realistic, but simulated phishing and password attack campaigns in your organization. Pick a password and then run the campaign against as many users as you want. The results will let you know how many people are using that password. Use the data to train users and build your custom list of banned passwords.