Turla Details
Vectra Mitre Att&CK

Threat Group Turla

Turla Description

Turla is a Russian-based threat group that has infected victims in over 45 countries, spanning a range of industries including government, embassies, military, education, research and pharmaceutical companies since 2004. Heightened activity was seen in mid-2015. Turla is known for conducting watering hole and spearphishing campaigns and leveraging in-house tools and malware. Turla's espionage platform is mainly used against Windows machines, but has also been seen used against macOS and Linux machines.(Citation: Kaspersky Turla)(Citation: ESET Gazer Aug 2017)(Citation: CrowdStrike VENOMOUS BEAR)(Citation: ESET Turla Mosquito Jan 2018)

MITRE ATT&CK T-Numbers

This section will list all the T-Numbers known to be used by the group Turla and associated detections within Vectra Cognito Detect that will monitor for activity seen to be utilising the method.

Collection

T1005	Hidden DNS Tunnel
	Suspicious Relay
	External Remote Access
	Vectra Match
	Hidden HTTP Tunnel
	Hidden HTTPS Tunnel
T1025	Hidden DNS Tunnel
	Suspicious Relay
	External Remote Access
	Hidden HTTP Tunnel
	Hidden HTTPS Tunnel
T1213	Smash and Grab
	M365 Suspicious Download Activity
	M365 Suspicious Teams Application
	M365 Exfiltration Before Termination
	M365 Suspicious Sharing Activity
	Data Smuggler
	Data Gathering
T1560	Smash and Grab
	Data Gathering
	Hidden HTTP Tunnel
	Data Smuggler
	Hidden HTTPS Tunnel

Command-And-Control

T1071	
	Hidden DNS Tunnel
	Stealth HTTP Post
	Suspicious Relay
	Multi-home Fronted Tunnel
	External Remote Access
	Vectra Match
	Peer-To-Peer
	Suspicious HTTP
	Vectra Threat Intelligence Match
	Hidden HTTP Tunnel
	Hidden HTTPS Tunnel
T1090	
	TOR Activity
	Suspicious Relay
	Azure AD TOR Activity
	External Remote Access
	Vectra Match
	AWS TOR Activity
T1102	Hidden HTTP Tunnel
	Suspicious Relay
	M365 Power Automate HTTP Flow Creation
	Hidden HTTPS Tunnel
T1105	Internal Stage Loader
	Hidden DNS Tunnel
	Stealth HTTP Post
	Suspicious Relay
	Multi-home Fronted Tunnel

Turla Details
Vectra Mitre Att&CK

Command-And-Control

	External Remote Access
	Vectra Match
	Peer-To-Peer
	Suspicious HTTP
	Vectra Threat Intelligence Match
	Hidden HTTP Tunnel
	Hidden HTTPS Tunnel

Credential-Access

T1110	
	Azure AD Successful Brute-Force
	Kerberos Brute-Sweep
	Kerberos Brute-Force
	Brute-Force
	SMB Brute-Force
	Vectra Match
	Azure AD Brute-Force Attempt
T1555	Privilege Anomaly: Unusual Host
	Privilege Anomaly: Unusual Service from Host
	Privilege Anomaly: Unusual Service
	Privilege Anomaly: Unusual Service - Insider
	Privilege Anomaly: Unusual Trio
	Privilege Anomaly: Unusual Account on Host

Defense-Evasion

T1027	
T1055	
T1078	Privilege Anomaly: Unusual Host
	Suspicious Admin
	AWS Suspect Privilege Escalation
	Azure AD Newly Created Admin Account
	Privilege Anomaly: Unusual Service from Host
	Privilege Anomaly: Unusual Service - Insider
	Privilege Anomaly: Unusual Account on Host
	AWS Suspect Admin Privilege Granting
	AWS Suspicious Credential Usage
	Azure AD Suspected Compromised Access
	Azure AD Admin Account Creation
	Privilege Anomaly: Unusual Service
	AWS Root Credential Usage
	Privilege Anomaly: Unusual Trio
	Azure AD Login Attempt to Disabled Account
	Suspicious Remote Desktop
	Azure AD Privilege Operation Anomaly
	Azure AD Suspicious Sign-On
	Suspicious Remote Execution
T1112	
T1134	
T1140	
T1553	
T1562	M365 Log Disabling Attempt
	AWS MFA Disabled

Defense-Evasion

	AWS Logging Modified
	Azure AD Change to Trusted IP Configuration
	AWS Logging Disabled
	Azure AD MFA Disabled
	AWS Security Tools Disabled
	AWS Suspect Public EC2 Change
	M365 Disabling of Security Tools

Discovery

T1007	
T1012	
T1016	
T1018	Port Sweep
	Vectra Match
	Port Scan
	RDP Recon
	Internal Darknet Scan
T1049	AWS External Network Discovery
T1057	
T1069	AWS Suspect Escalation Reconnaissance
	RPC Recon
	RPC Targeted Recon
	Vectra Match
T1082	
T1083	RPC Recon
	File Share Enumeration
	M365 Unusual eDiscovery Search
	M365 Suspect eDiscovery Usage
	Vectra Match
T1087	RPC Recon
	AWS User Permissions Enumeration
	Kerberos Account Scan
	SMB Account Scan
	RPC Targeted Recon

Discovery

	Vectra Match
	Azure AD Brute-Force Attempt
T1120	
T1124	
T1201	
T1518	
T1615	RPC Recon
	RPC Targeted Recon
	Vectra Match
	Suspicious LDAP Query

Execution

T1059	M365 Power Automate HTTP Flow Creation
	Hidden DNS Tunnel
	Suspicious Relay
	Azure AD Unusual Scripting Engine Usage
	Suspicious HTTP
	Hidden HTTP Tunnel
	Hidden HTTPS Tunnel
T1106	
T1204	Custom Models
	M365 Malware Stage: Upload
	M365 DLL Hijacking Activity

Exfiltration

T1567	Smash and Grab
	M365 Suspect Power Automate Activity
	M365 Suspicious Download Activity
	M365 External Teams Access
	M365 Suspicious Power Automate Flow Creation
	M365 Suspicious Sharing Activity
	Data Smuggler

Turla Details

Vectra Mitre Att&CK

Initial-Access

T1078	Privilege Anomaly: Unusual Host
	Suspicious Admin
	AWS Suspect Privilege Escalation
	Azure AD Newly Created Admin Account
	Privilege Anomaly: Unusual Service from Host
	Privilege Anomaly: Unusual Service - Insider
	Privilege Anomaly: Unusual Account on Host
	AWS Suspect Admin Privilege Granting
	AWS Suspicious Credential Usage
	Azure AD Suspected Compromised Access
	Azure AD Admin Account Creation
	Privilege Anomaly: Unusual Service
	AWS Root Credential Usage
	Privilege Anomaly: Unusual Trio
	Azure AD Login Attempt to Disabled Account
	Suspicious Remote Desktop
	Azure AD Privilege Operation Anomaly
	Azure AD Suspicious Sign-On
	Suspicious Remote Execution
T1189	
	Vectra Match
	Vectra Threat Intelligence Match
T1566	
	Vectra Match

Lateral-Movement

T1021	Privilege Anomaly: Unusual Host
	Privilege Anomaly: Unusual Service from Host
	Privilege Anomaly: Unusual Service
	Privilege Anomaly: Unusual Service - Insider
	Novel Access to SMB Admin Share
	Novel Admin Protocol Usage
	Privilege Anomaly: Unusual Trio
	Suspicious Remote Desktop
	Vectra Match
	Azure AD Privilege Operation Anomaly
	Privilege Anomaly: Unusual Account on Host
T1570	Custom Models
	Vectra Match
	Internal Stage Loader

Turla Details

Vectra Mitre Att&CK

Persistence

T1055	
T1068	
T1078	Privilege Anomaly: Unusual Host
	Suspicious Admin
	AWS Suspect Privilege Escalation
	Azure AD Newly Created Admin Account
	Privilege Anomaly: Unusual Service from Host
	Privilege Anomaly: Unusual Service - Insider
	Privilege Anomaly: Unusual Account on Host
	AWS Suspect Admin Privilege Granting
	AWS Suspicious Credential Usage
	Azure AD Suspected Compromised Access
	Azure AD Admin Account Creation
	Privilege Anomaly: Unusual Service
	AWS Root Credential Usage
	Privilege Anomaly: Unusual Trio
	Azure AD Login Attempt to Disabled Account
	Suspicious Remote Desktop
	Azure AD Privilege Operation Anomaly
	Azure AD Suspicious Sign-On
	Suspicious Remote Execution
T1134	
T1546	
T1547	

Privilege-Escalation

T1055	
T1068	
T1078	Privilege Anomaly: Unusual Host
	Suspicious Admin
	AWS Suspect Privilege Escalation
	Azure AD Newly Created Admin Account
	Privilege Anomaly: Unusual Service from Host
	Privilege Anomaly: Unusual Service - Insider
	Privilege Anomaly: Unusual Account on Host
	AWS Suspect Admin Privilege Granting
	AWS Suspicious Credential Usage
	Azure AD Suspected Compromised Access
	Azure AD Admin Account Creation
	Privilege Anomaly: Unusual Service
	AWS Root Credential Usage
	Privilege Anomaly: Unusual Trio
	Azure AD Login Attempt to Disabled Account
	Suspicious Remote Desktop
	Azure AD Privilege Operation Anomaly
	Azure AD Suspicious Sign-On
	Suspicious Remote Execution
T1134	
T1546	
T1547	

Resource-Development

T1583	
T1584	
T1587	
T1588	

MITRE ATT&CK T-Number Descriptions

This section describes the MITRE Techniques known to be used by the group Turla.

T-Number	Description
T1005	Adversaries may search local system sources, such as file systems or local databases, to find files of interest and sensitive data prior to Exfiltration. Adversaries may do this using a Command and Scripting Interpreter, such as cmd, which has functionality to interact with the file system to gather information. Some adversaries may also use Automated Collection on the local system.
T1007	Adversaries may try to get information about registered services. Commands that may obtain information about services using operating system utilities are "sc," "tasklist /svc" using Tasklist, and "net start" using Net, but adversaries may also use other tools as well. Adversaries may use the information from System Service Discovery during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions.
T1016	Adversaries may look for details about the network configuration and settings of systems they access or through information discovery of remote systems. Several operating system administration utilities exist that can be used to gather this information. Examples include Arp, ipconfig/ifconfig, nbtstat, and route. Adversaries may use the information from System Network Configuration Discovery during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions.
T1018	Adversaries may attempt to get a listing of other systems by IP address, hostname, or other logical identifier on a network that may be used for Lateral Movement from the current system. Functionality could exist within remote access tools to enable this, but utilities available on the operating system could also be used such as Ping or net view using Net. Adversaries may also use local host files (ex: C:\Windows\System32\Drivers\etc\hosts or /etc/hosts) in order to discover the hostname to IP address mappings of remote systems.
T1021	Adversaries may use Valid Accounts to log into a service specifically designed to accept remote connections, such as telnet, SSH, and VNC. The adversary may then perform actions as the logged-on user. In an enterprise environment, servers and workstations can be organized into

T-Number	Description
	domains. If an adversary is able to obtain a set of valid domain credentials, they could login to many different machines using remote access protocols such as secure shell (SSH) or remote desktop protocol (RDP).
T1049	Adversaries may attempt to get a listing of network connections to or from the compromised system they are currently accessing or from remote systems by querying for information over the network. An adversary who gains access to a system that is part of a cloud-based environment may map out Virtual Private Clouds or Virtual Networks in order to determine what systems and services are connected. Utilities and commands that acquire this information include netstat, "net use," and "net session" with Net. In Mac and Linux, netstat and lsof can be used to list current connections. who -a and w can be used to show which users are currently logged in, similar to "net session".
T1057	Adversaries may attempt to get information about running processes on a system. Information obtained could be used to gain an understanding of common software/applications running on systems within the network. Adversaries may use the information from Process Discovery during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions. In Windows environments, adversaries could obtain details on running processes using the Tasklist utility via cmd or Get-Process via PowerShell. Information about processes can also be extracted from the output of Native API calls such as CreateToolhelp32Snapshot. In Mac and Linux, this is accomplished with the ps command. Adversaries may also opt to enumerate processes via /proc.
T1059	Adversaries may abuse command and script interpreters to execute commands, scripts, or binaries. These interfaces and languages provide ways of interacting with computer systems and are a common feature across many different platforms. Most systems come with some built-in command-line interface and scripting capabilities. There are also cross-platform interpreters such as Python, as well as those commonly associated with client applications such as JavaScript and Visual Basic. Adversaries may abuse these technologies in various ways as a means of executing arbitrary commands. Commands and scripts can be embedded in Initial Access payloads delivered to victims as lure documents or as secondary payloads downloaded from an existing C2. Adversaries may also execute commands through interactive terminals/shells.
T1069	Adversaries may attempt to find group and permission settings. This information can help adversaries determine which user accounts and

T-Number	Description
	groups are available, the membership of users in particular groups, and which users and groups have elevated permissions.
T1071	Adversaries may communicate using application layer protocols to avoid detection/network filtering by blending in with existing traffic. Commands to the remote system, and often the results of those commands, will be embedded within the protocol traffic between the client and server. Adversaries may utilize many different protocols, including those used for web browsing, transferring files, electronic mail, or DNS. For connections that occur internally within an enclave (such as those between a proxy or pivot node and other nodes), commonly used protocols are SMB, SSH, or RDP.
T1078	Adversaries may obtain and abuse credentials of existing accounts as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion. Compromised credentials may be used to bypass access controls placed on various resources on systems within the network and may even be used for persistent access to remote systems and externally available services, such as VPNs, Outlook Web Access and remote desktop. Compromised credentials may also grant an adversary increased privilege to specific systems or access to restricted areas of the network. The overlap of permissions for local, domain, and cloud accounts across a network of systems is of concern because the adversary may be able to pivot across accounts and systems to reach a high level of access (i.e., domain or enterprise administrator) to bypass access controls set within the enterprise.
T1078	Adversaries may obtain and abuse credentials of existing accounts as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion. Compromised credentials may be used to bypass access controls placed on various resources on systems within the network and may even be used for persistent access to remote systems and externally available services, such as VPNs, Outlook Web Access and remote desktop. Compromised credentials may also grant an adversary increased privilege to specific systems or access to restricted areas of the network. The overlap of permissions for local, domain, and cloud accounts across a network of systems is of concern because the adversary may be able to pivot across accounts and systems to reach a high level of access (i.e., domain or enterprise administrator) to bypass access controls set within the enterprise.
T1078	Adversaries may obtain and abuse credentials of existing accounts as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion. Compromised credentials may be used to bypass access controls placed on various resources on systems within the

T-Number	Description
	network and may even be used for persistent access to remote systems and externally available services, such as VPNs, Outlook Web Access and remote desktop. Compromised credentials may also grant an adversary increased privilege to specific systems or access to restricted areas of the network. The overlap of permissions for local, domain, and cloud accounts across a network of systems is of concern because the adversary may be able to pivot across accounts and systems to reach a high level of access (i.e., domain or enterprise administrator) to bypass access controls set within the enterprise.
T1078	Adversaries may obtain and abuse credentials of existing accounts as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion. Compromised credentials may be used to bypass access controls placed on various resources on systems within the network and may even be used for persistent access to remote systems and externally available services, such as VPNs, Outlook Web Access and remote desktop. Compromised credentials may also grant an adversary increased privilege to specific systems or access to restricted areas of the network. The overlap of permissions for local, domain, and cloud accounts across a network of systems is of concern because the adversary may be able to pivot across accounts and systems to reach a high level of access (i.e., domain or enterprise administrator) to bypass access controls set within the enterprise.
T1082	An adversary may attempt to get detailed information about the operating system and hardware, including version, patches, hotfixes, service packs, and architecture. Adversaries may use the information from System Information Discovery during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions. Infrastructure as a Service (IaaS) cloud providers such as AWS, GCP, and Azure allow access to instance and virtual machine information via APIs. Successful authenticated API calls can return data such as the operating system platform and status of a particular instance or the model view of a virtual machine.
T1083	Adversaries may enumerate files and directories or may search in specific locations of a host or network share for certain information within a file system. Adversaries may use the information from File and Directory Discovery during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions. Many command shell utilities can be used to obtain this information. Examples include dir, tree, ls, find, and locate. Custom tools may also be used to gather file and directory information and interact with the Native API.

Turla Details
Vectra Mitre Att&CK

T-Number	Description
T1087	Adversaries may attempt to get a listing of accounts on a system or within an environment. This information can help adversaries determine which accounts exist to aid in follow-on behavior.
T1090	Adversaries may use a connection proxy to direct network traffic between systems or act as an intermediary for network communications to a command and control server to avoid direct connections to their infrastructure. Adversaries use these types of proxies to manage command and control communications, reduce the number of simultaneous outbound network connections, provide resiliency in the face of connection loss, or to ride over existing trusted communications paths between victims to avoid suspicion. Adversaries may chain together multiple proxies to further disguise the source of malicious traffic. Adversaries can also take advantage of routing schemes in Content Delivery Networks (CDNs) to proxy command and control traffic.
T1105	Adversaries may transfer tools or other files from an external system into a compromised environment. Files may be copied from an external adversary controlled system through the command and control channel to bring tools into the victim network or through alternate protocols with another tool such as FTP. Files can also be copied over on Mac and Linux with native tools like scp, rsync, and sftp.
T1110	Adversaries may use brute force techniques to gain access to accounts when passwords are unknown or when password hashes are obtained. Without knowledge of the password for an account or set of accounts, an adversary may systematically guess the password using a repetitive or iterative mechanism. Brute forcing passwords can take place via interaction with a service that will check the validity of those credentials or offline against previously acquired credential data, such as password hashes.
T1124	An adversary may gather the system time and/or time zone from a local or remote system. The system time is set and stored by the Windows Time Service within a domain to maintain time synchronization between systems and services in an enterprise network. System time information may be gathered in a number of ways, such as with Net on Windows by performing net time \hostname to gather the system time on a remote system. The victim's time zone may also be inferred from the current system time or gathered by using w32tm /tz. This information could be useful for performing other techniques, such as executing a file with a Scheduled Task/Job, or to discover locality information based on time zone to assist in victim targeting (i.e. System Location Discovery).

T-Number	Description
	Adversaries may also use knowledge of system time as part of a time bomb, or delaying execution until a specified date/time.
T1189	Adversaries may gain access to a system through a user visiting a website over the normal course of browsing. With this technique, the user's web browser is typically targeted for exploitation, but adversaries may also use compromised websites for non-exploitation behavior such as acquiring Application Access Token. Often the website used by an adversary is one visited by a specific community, such as government, a particular industry, or region, where the goal is to compromise a specific user or set of users based on a shared interest. This kind of targeted attack is referred to a strategic web compromise or watering hole attack. Typical drive-by compromise process: Unlike Exploit Public-Facing Application, the focus of this technique is to exploit software on a client endpoint upon visiting a website. This will commonly give an adversary access to systems on the internal network instead of external systems that may be in a DMZ. Adversaries may also use compromised websites to deliver a user to a malicious application designed to Steal Application Access Tokens, like OAuth tokens, to gain access to protected applications and information. These malicious applications have been delivered through popups on legitimate websites.
T1201	Adversaries may attempt to access detailed information about the password policy used within an enterprise network. Password policies for networks are a way to enforce complex passwords that are difficult to guess or crack through Brute Force. This would help the adversary to create a list of common passwords and launch dictionary and/or brute force attacks which adheres to the policy. Password policies can be set and discovered on Windows, Linux, and macOS systems via various command shell utilities such as net accounts (/domain), Get-ADDefaultDomainPasswordPolicy, chage -l , cat /etc/pam.d/common-password, and pwpolicy getaccountpolicies.
T1204	An adversary may rely upon specific actions by a user in order to gain execution. Users may be subjected to social engineering to get them to execute malicious code by, for example, opening a malicious document file or link. These user actions will typically be observed as follow-on behavior from forms of Phishing. While User Execution frequently occurs shortly after Initial Access it may occur at other phases of an intrusion, such as when an adversary places a file in a shared directory or on a user's desktop hoping that a user will click on it. This activity may also be seen shortly after Internal Spearphishing.
T1213	Adversaries may leverage information repositories to mine valuable information. Information repositories are tools that allow for storage of

T-Number	Description
	information, typically to facilitate collaboration or information sharing between users, and can store a wide variety of data that may aid adversaries in further objectives, or direct access to the target information. The following is a brief list of example information that may hold potential value to an adversary and may also be found on an information repository: policies, procedures, and standards, physical/logical network diagrams, system architecture diagrams, technical system documentation, testing/development credentials, work/project schedules, source code snippets, and links to network shares and other internal resources. Specific common information repositories include Sharepoint, Confluence, and enterprise databases such as SQL Server.
T1518	Adversaries may attempt to get a listing of software and software versions that are installed on a system or in a cloud environment. Adversaries may use the information from Software Discovery during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions. Adversaries may attempt to enumerate software for a variety of reasons, such as figuring out what security measures are present or if the compromised system has a version of software that is vulnerable to Exploitation for Privilege Escalation.
T1555	Adversaries may search for common password storage locations to obtain user credentials. Passwords are stored in several places on a system, depending on the operating system or application holding the credentials. There are also specific applications that store passwords to make it easier for users manage and maintain. Once credentials are obtained, they can be used to perform lateral movement and access restricted information.
T1560	An adversary may compress and/or encrypt data that is collected prior to exfiltration. Compressing the data can help to obfuscate the collected data and minimize the amount of data sent over the network. Encryption can be used to hide information that is being exfiltrated from detection or make exfiltration less conspicuous upon inspection by a defender. Both compression and encryption are done prior to exfiltration, and can be performed using a utility, 3rd party library, or custom method.
T1562	Adversaries may maliciously modify components of a victim environment in order to hinder or disable defensive mechanisms. This not only involves impairing preventative defenses, such as firewalls and anti-virus, but also detection capabilities that defenders can use to audit activity and identify malicious behavior. This may also span both native defenses as well as supplemental capabilities installed by users and administrators.

T-Number	Description
	Adversaries could also target event aggregation and analysis mechanisms, or otherwise disrupt these procedures by altering other system components.
T1567	Adversaries may use an existing, legitimate external Web service to exfiltrate data rather than their primary command and control channel. Popular Web services acting as an exfiltration mechanism may give a significant amount of cover due to the likelihood that hosts within a network are already communicating with them prior to compromise. Firewall rules may also already exist to permit traffic to these services. Web service providers also commonly use SSL/TLS encryption, giving adversaries an added level of protection.
T1570	Adversaries may transfer tools or other files between systems in a compromised environment. Files may be copied from one system to another to stage adversary tools or other files over the course of an operation. Adversaries may copy files laterally between internal victim systems to support lateral movement using inherent file sharing protocols such as file sharing over SMB to connected network shares or with authenticated connections with SMB/Windows Admin Shares or Remote Desktop Protocol. Files can also be copied over on Mac and Linux with native tools like scp, rsync, and sftp.

Turla Details
Vectra Mitre Att&CK

Cognito's Coverage of MITRE Techniques for Group Turla

This section describes the detections within Cognito Detect that are known to trigger on techniques used by the group Turla.

Detections
Hidden DNS Tunnel
Suspicious Relay
External Remote Access
Vectra Match
Hidden HTTP Tunnel
Hidden HTTPS Tunnel
Smash and Grab
M365 Suspicious Download Activity
M365 Suspicious Teams Application
M365 Exfiltration Before Termination
M365 Suspicious Sharing Activity
Data Smuggler
Data Gathering
Stealth HTTP Post
Multi-home Fronted Tunnel
Peer-To-Peer
Suspicious HTTP
Vectra Threat Intelligence Match
TOR Activity
Azure AD TOR Activity
AWS TOR Activity

Detections

- **M365 Power Automate HTTP Flow Creation**
- **Internal Stage Loader**
- **Azure AD Successful Brute-Force**
- **Kerberos Brute-Sweep**
- **Kerberos Brute-Force**
- **Brute-Force**
- **SMB Brute-Force**
- **Azure AD Brute-Force Attempt**
- **Privilege Anomaly: Unusual Host**
- **Privilege Anomaly: Unusual Service from Host**
- **Privilege Anomaly: Unusual Service**
- **Privilege Anomaly: Unusual Service - Insider**
- **Privilege Anomaly: Unusual Trio**
- **Privilege Anomaly: Unusual Account on Host**
- **Suspicious Admin**
- **AWS Suspect Privilege Escalation**
- **Azure AD Newly Created Admin Account**
- **AWS Suspect Admin Privilege Granting**
- **AWS Suspicious Credential Usage**
- **Azure AD Suspected Compromised Access**
- **Azure AD Admin Account Creation**
- **AWS Root Credential Usage**
- **Azure AD Login Attempt to Disabled Account**
- **Suspicious Remote Desktop**
- **Azure AD Privilege Operation Anomaly**
- **Azure AD Suspicious Sign-On**
- **Suspicious Remote Execution**

Turla Details
Vectra Mitre Att&CK

Detections

- M365 Log Disabling Attempt
- AWS MFA Disabled
- AWS Logging Modified
- Azure AD Change to Trusted IP Configuration
- AWS Logging Disabled
- Azure AD MFA Disabled
- AWS Security Tools Disabled
- AWS Suspect Public EC2 Change
- M365 Disabling of Security Tools
- Port Sweep
- Port Scan
- RDP Recon
- Internal Darknet Scan
- AWS External Network Discovery
- AWS Suspect Escalation Reconnaissance
- RPC Recon
- RPC Targeted Recon
- File Share Enumeration
- M365 Unusual eDiscovery Search
- M365 Suspect eDiscovery Usage
- AWS User Permissions Enumeration
- Kerberos Account Scan
- SMB Account Scan
- Suspicious LDAP Query
- Azure AD Unusual Scripting Engine Usage
- Custom Models
- M365 Malware Stage: Upload

Detections

M365 DLL Hijacking Activity

M365 Suspect Power Automate Activity

M365 External Teams Access

M365 Suspicious Power Automate Flow Creation

Vectra Threat Intelligence Match

Novel Access to SMB Admin Share

Novel Admin Protocol Usage