
NORMEN

Windows Defender Antivirus has detected malware or other potentially unwanted software.
For more information please see the following:
https://go.microsoft.com/fwlink/?linkid=37020&name=Trojan:Win32/Meterpreter.O&threa

Name: Trojan:Win32/Meterpreter.O
ID: 2147729928
Severity: Severe
Category: Trojan
Path:
Detection Origin: Local machine
Detection Type: Concrete
Detection Source: Real-Time Protection

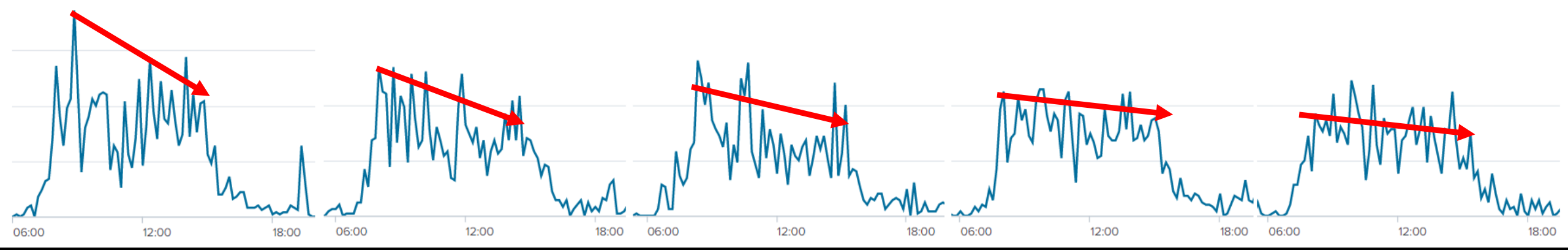

Honeywell
FLIGHT
RECORDER
DO NOT OPEN
BITE ATE (CAUTION: 115V)

6,513,146,544

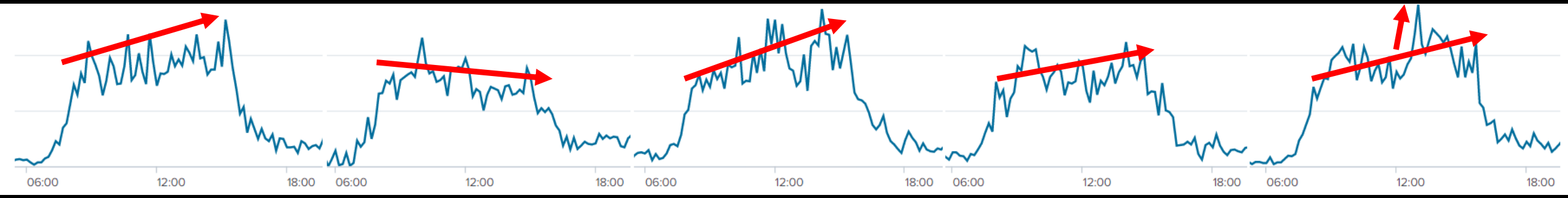
output: (user=root user_loginuid=-1 k8s.ns=fuf k8s.pod=ztagent-deployment-85f5bfc57f-kl8xx container=9875b8b3dbe6 process=sshd parent=sshd cmdline=sshd -R terminal=0 container_id=9875b8b3dbe6 image=nhnreg.azurecr.io/zerotier-agent fd.name=::1:35504->::1:22 fd.num=0 fd.type=ipv6 fd.sip=808d:f1d9:ff7f:0:2100::) k8s.ns=fuf k8s.pod=ztagent-deployment-85f5bfc57f-kl8xx container=9875b8b3dbe6 k8s.ns=fuf k8s.pod=ztagent-deployment-85f5bfc57f-kl8xx container=9875b8b3dbe6

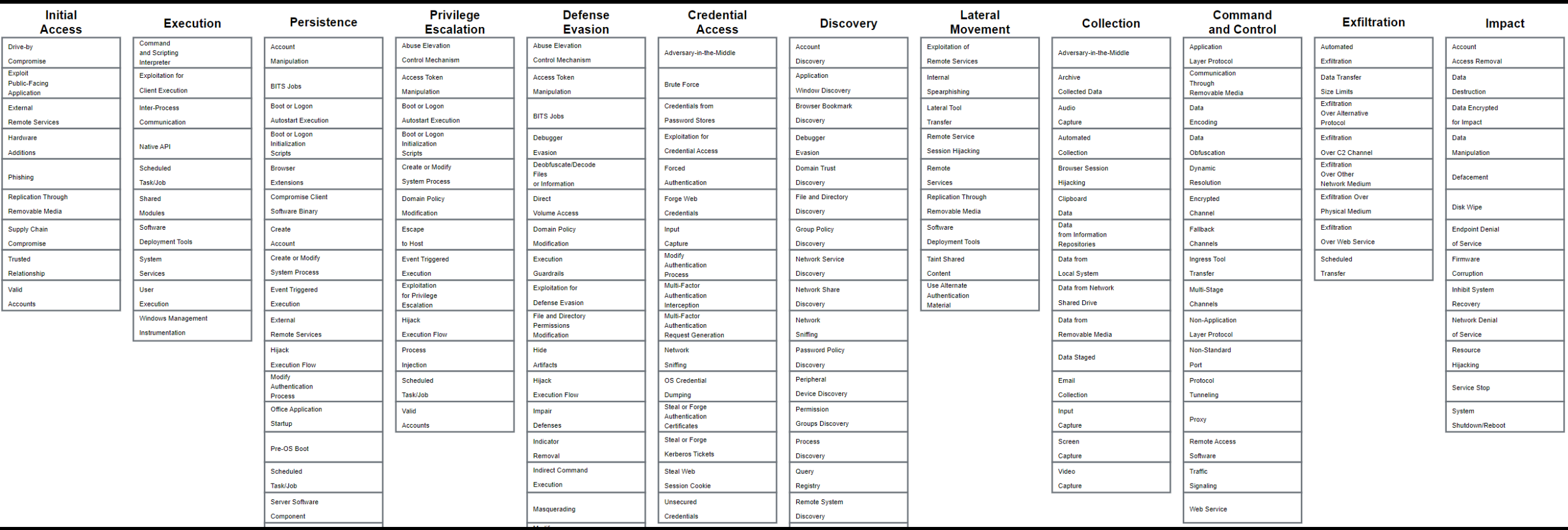
output: Warning Redirect stdout/stdin to network connection

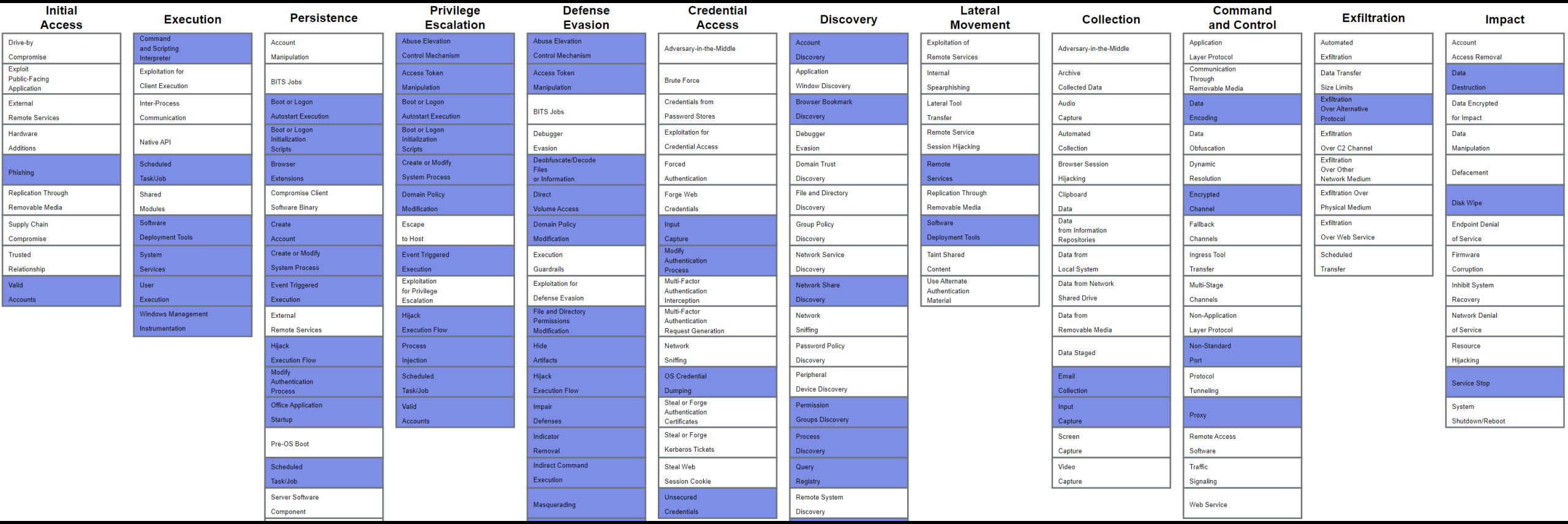
VG


06:00
12:00
18:00
06:00
12:00
18:00
06:00
12:00
18:00
06:00
12:00
18:00
06:00
12:00
18:00

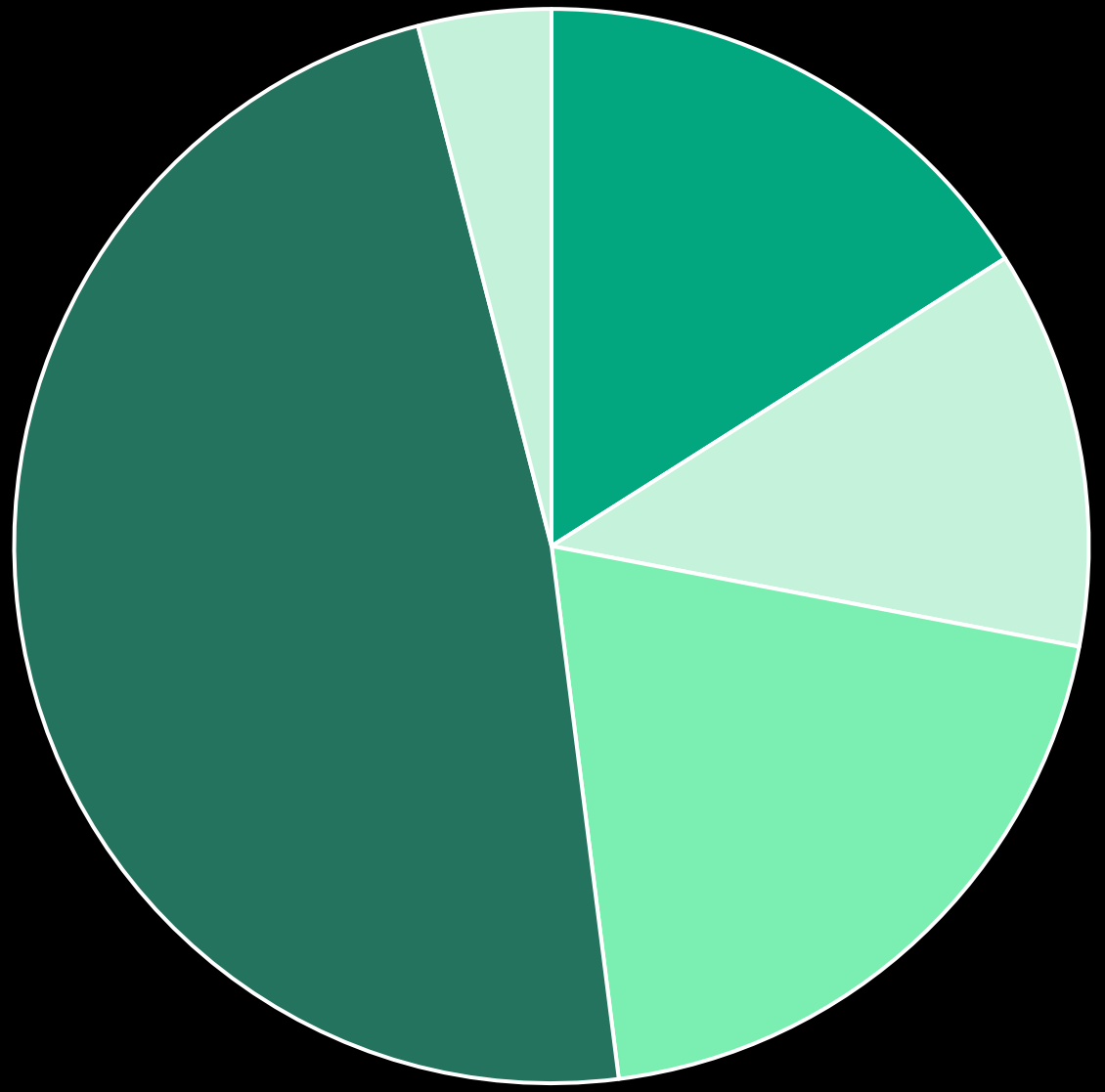
Youtube


06:00
12:00
18:00
06:00
12:00
18:00
06:00
12:00
18:00
06:00
12:00
18:00
06:00
12:00
18:00

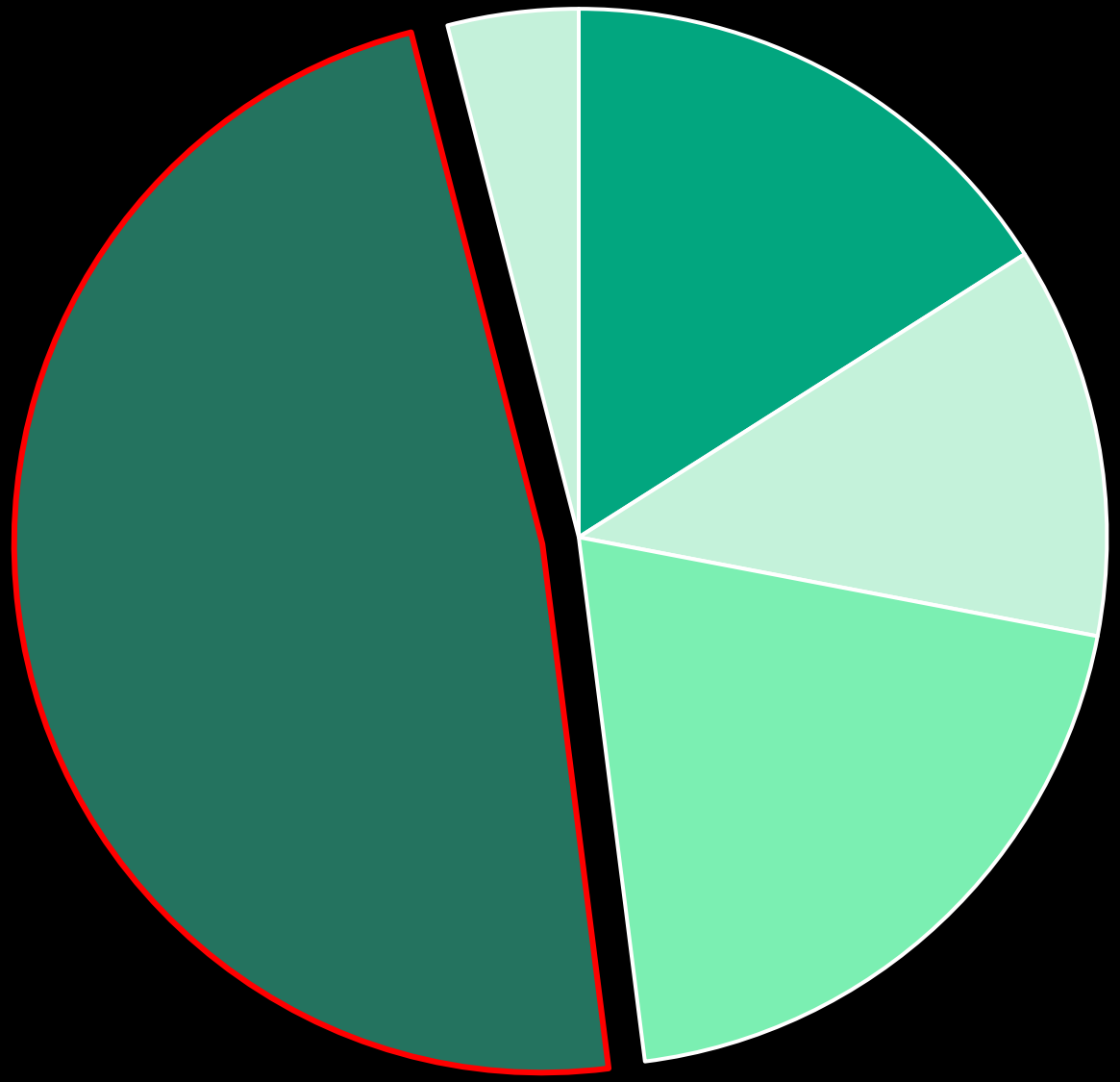

Initial Access
Drive-by Compromise
Exploit Public-Facing Application
External Remote Services
Hardware Additions
Phishing
Replication Through Removable Media
Supply Chain Compromise
Trusted Relationship
Valid Accounts
Execution
Command and Scripting Interpreter
Exploitation for Client Execution
Inter-Process Communication
Native API
Scheduled Task/Job
Shared Modules
Software Deployment Tools
System Services
User Execution
Windows Management Instrumentation
Persistence
Account Manipulation
BITS Jobs
Boot or Logon Autostart Execution
Boot or Logon Initialization Scripts
Browser Extensions
Compromise Client Software Binary
Create Account
Create or Modify System Process
Event Triggered Execution
External Remote Services
Hijack Execution Flow
Modify Authentication Process
Office Application Startup
Pre-OS Boot
Scheduled Task/Job
Server Software Component
Privilege Escalation
Abuse Elevation Control Mechanism
Access Token Manipulation
Boot or Logon Autostart Execution
Boot or Logon Initialization Scripts
Create or Modify System Process
Domain Policy Modification
Escape to Host
Event Triggered Execution
Exploitation for Privilege Escalation
Hijack Execution Flow
Process Injection
Scheduled Task/Job
Valid Accounts
Defense Evasion
Abuse Elevation Control Mechanism
Access Token Manipulation
BITS Jobs
Debugger Evasion
Deobfuscate/Decode Files or Information
Direct Volume Access
Domain Policy Modification
Execution Guardrails
Exploitation for Defense Evasion
File and Directory Permissions Modification
Hide Artifacts
Hijack Execution Flow
Impair Defenses
Indicator Removal
Indirect Command Execution
Masquerading
Credential Access
Adversary-in-the-Middle
Brute Force
Credentials from Password Stores
Exploitation for Credential Access
Forced Authentication
Forge Web Credentials
Input Capture
Modify Authentication Process
Multi-Factor Authentication Interception
Multi-Factor Authentication Request Generation
Network Sniffing
OS Credential Dumping
Steal or Forge Authentication Certificates
Steal or Forge Kerberos Tickets
Steal Web Session Cookie
Unsecured Credentials
Discovery
Account Discovery
Application Window Discovery
Browser Bookmark Discovery
Debugger Evasion
Domain Trust Discovery
File and Directory Discovery
Group Policy Discovery
Network Service Discovery
Network Share Discovery
Network Sniffing
Password Policy Discovery
Peripheral Device Discovery
Permission Groups Discovery
Process Discovery
Query Registry
Remote System Discovery
Lateral Movement
Exploitation of Remote Services
Internal Spearphishing
Lateral Tool Transfer
Remote Service Session Hijacking
Remote Services
Replication Through Removable Media
Software Deployment Tools
Taint Shared Content
Use Alternate Authentication Material
Collection
Adversary-in-the-Middle
Archive Collected Data
Audio Capture
Automated Collection
Browser Session Hijacking
Clipboard Data
Data from Information Repositories
Data from Local System
Data from Network Shared Drive
Data from Removable Media
Data Staged
Email Collection
Input Capture
Screen Capture
Video Capture
Command and Control
Application Layer Protocol
Communication Through Removable Media
Data Encoding
Data Obfuscation
Dynamic Resolution
Encrypted Channel
Fallback Channels
Ingress Tool Transfer
Multi-Stage Channels
Non-Application Layer Protocol
Non-Standard Port
Protocol Tunneling
Proxy
Remote Access Software
Traffic Signaling
Web Service
Exfiltration
Automated Exfiltration
Data Transfer Size Limits
Exfiltration Over Alternative Protocol
Exfiltration Over C2 Channel
Exfiltration Over Other Network Medium
Exfiltration Over Physical Medium
Exfiltration Over Web Service
Scheduled Transfer
Impact
Account Access Removal
Data Destruction
Data Encrypted for Impact
Data Manipulation
Defacement
Disk Wipe
Endpoint Denial of Service
Firmware Corruption
Inhibit System Recovery
Network Denial of Service
Resource Hijacking
Service Stop
System Shutdown/Reboot

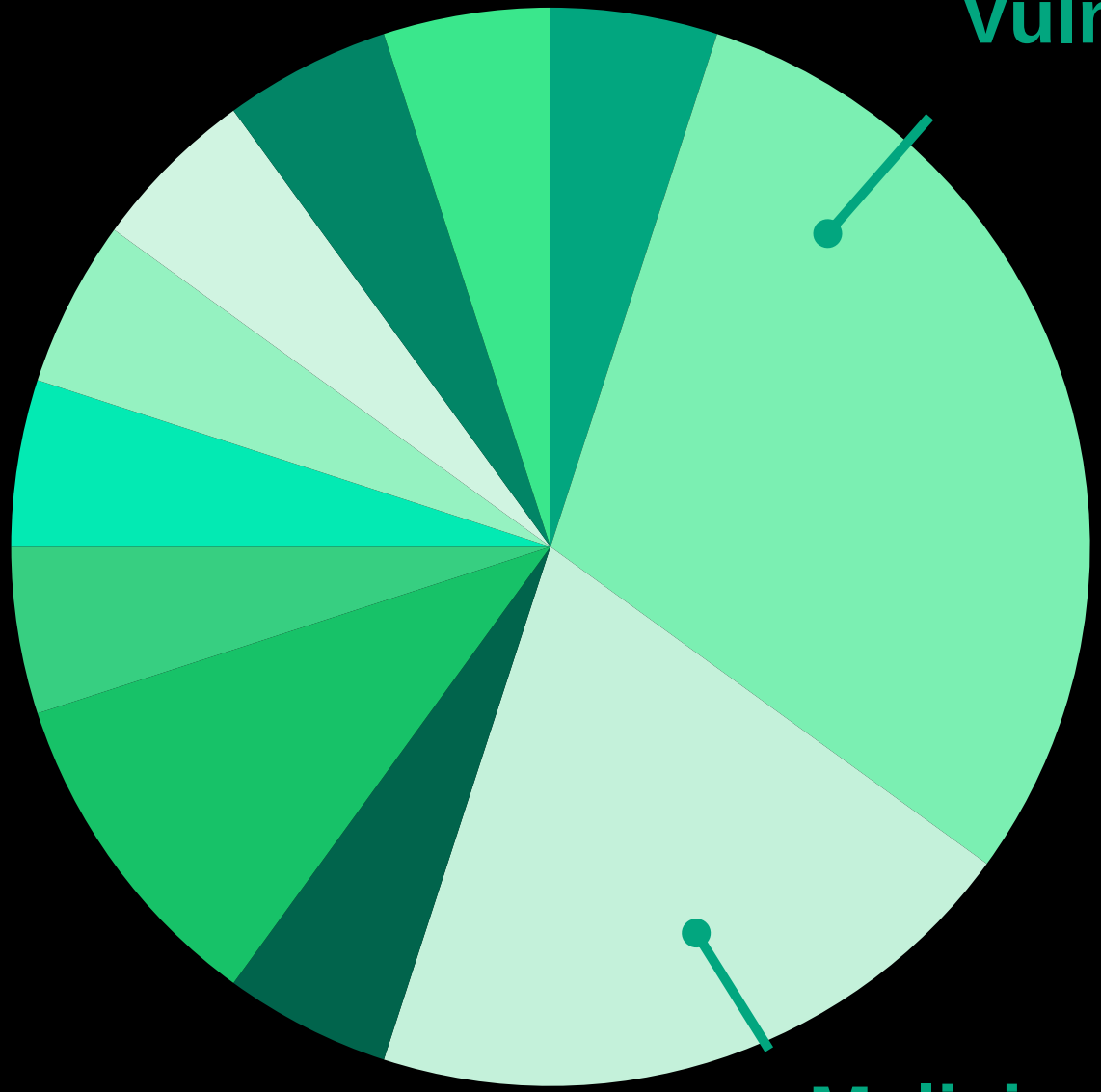

Initial Access
Drive-by Compromise
Exploit Public-Facing Application
External Remote Services
Hardware Additions
Phishing
Replication Through Removable Media
Supply Chain Compromise
Trusted Relationship
Valid Accounts
Execution
Command and Scripting Interpreter
Exploitation for Client Execution
Inter-Process Communication
Native API
Scheduled Task/Job
Shared Modules
Software Deployment Tools
System Services
User Execution
Windows Management Instrumentation
Persistence
Account Manipulation
BITS Jobs
Boot or Logon Autostart Execution
Boot or Logon Initialization Scripts
Browser Extensions
Compromise Client Software Binary
Create Account
Create or Modify System Process
Event Triggered Execution
Exploitation for Privilege Escalation
External Remote Services
Hijack Execution Flow
Modify Authentication Process
Office Application Startup
Pre-OS Boot
Scheduled Task/Job
Server Software Component
Privilege Escalation
Abuse Elevation Control Mechanism
Access Token Manipulation
Boot or Logon Autostart Execution
Boot or Logon Initialization Scripts
Create or Modify System Process
Domain Policy Modification
Escape to Host
Event Triggered Execution
Exploitation for Privilege Escalation
Hijack Execution Flow
Process Injection
Scheduled Task/Job
Valid Accounts
Defense Evasion
Abuse Elevation Control Mechanism
Access Token Manipulation
BITS Jobs
Debugger Evasion
Deobfuscate/Decode Files or Information
Direct Volume Access
Domain Policy Modification
Execution Guardrails
Exploitation for Defense Evasion
File and Directory Permissions Modification
Hide Artifacts
Hijack Execution Flow
Impair Defenses
Indicator Removal
Indirect Command Execution
Masquerading
Credential Access
Adversary-in-the-Middle
Brute Force
Credentials from Password Stores
Exploitation for Credential Access
Forced Authentication
Forge Web Credentials
Input Capture
Modify Authentication Process
Multi-Factor Authentication Interception
Multi-Factor Authentication Request Generation
Network Sniffing
OS Credential Dumping
Steal or Forge Authentication Certificates
Steal or Forge Kerberos Tickets
Steal Web Session Cookie
Unsecured Credentials
Discovery
Account Discovery
Application Window Discovery
Browser Bookmark Discovery
Debugger Evasion
Domain Trust Discovery
File and Directory Discovery
Group Policy Discovery
Network Service Discovery
Network Share Discovery
Network Sniffing
Password Policy Discovery
Peripheral Device Discovery
Permission Groups Discovery
Process Discovery
Query Registry
Remote System Discovery
Lateral Movement
Exploitation of Remote Services
Internal Spearphishing
Lateral Tool Transfer
Remote Service Session Hijacking
Remote Services
Replication Through Removable Media
Software Deployment Tools
Taint Shared Content
Use Alternate Authentication Material
Collection
Adversary-in-the-Middle
Archive Collected Data
Audio Capture
Automated Collection
Browser Session Hijacking
Clipboard Data
Data from Information Repositories
Data from Local System
Data from Network Shared Drive
Data from Removable Media
Data Staged
Email Collection
Input Capture
Screen Capture
Video Capture
Command and Control
Application Layer Protocol
Communication Through Removable Media
Data Encoding
Data Obfuscation
Dynamic Resolution
Encrypted Channel
Fallback Channels
Ingress Tool Transfer
Multi-Stage Channels
Non-Application Layer Protocol
Non-Standard Port
Protocol Tunneling
Proxy
Remote Access Software
Traffic Signaling
Web Service
Exfiltration
Automated Exfiltration
Data Transfer Size Limits
Exfiltration Over Alternative Protocol
Exfiltration Over C2 Channel
Exfiltration Over Other Network Medium
Exfiltration Over Physical Medium
Exfiltration Over Web Service
Scheduled Transfer
Impact
Account Access Removal
Data Destruction
Data Encrypted for Impact
Data Manipulation
Defacement
Disk Wipe
Endpoint Denial of Service
Firmware Corruption
Inhibit System Recovery
Network Denial of Service
Resource Hijacking
Service Stop
System Shutdown/Reboot

Hendelser per området



Hendelser per området




Vulnerabilities
Malicious File

«Lykkelig Uvitende»

Lykkelig Vitende

Norsk helsenett