Mandiant Red Team Emulates FIN11 Tactics To Control Operational Technology Servers

mandiant.com/resources/mandiant-red-team-emulates-fin11-tactics

During the last couple of years, ransomware incidents have impacted thousands of industrial and critical infrastructure organizations. In some cases, Mandiant has observed how these intrusions disrupt industrial production chains and operational workflows as a method to incentivize the payment of ransoms. Although in most cases victims have suffered damages exclusively restricted to enterprise systems, this does not mean that operational technology (OT) systems are not at risk.

The nature of OT technology and the challenges of defending it means that many OT networks have security gaps that even less sophisticated actors can leverage. Furthermore, Mandiant has consistently highlighted that some financially motivated groups continue to deploy the same or similar tools and techniques as those used by advanced persistent threats (APTs) during high-profile cyber physical incidents.

In this blog, we describe an engagement where a Mandiant Red Team targeted a European engineering organization to understand the potential reach ransomware operators could have in their network. Our Red Team emulated the techniques used by FIN11, a financially motivated threat group that has conducted long-running ransomware distribution campaigns across multiple industries. Using FIN11's techniques to move from a corporate endpoint with regular employee credentials, obtain domain administrator rights, steal critical data, and gain access to OT servers.

Ransomware Actors Have Proven Capabilities to Access OT

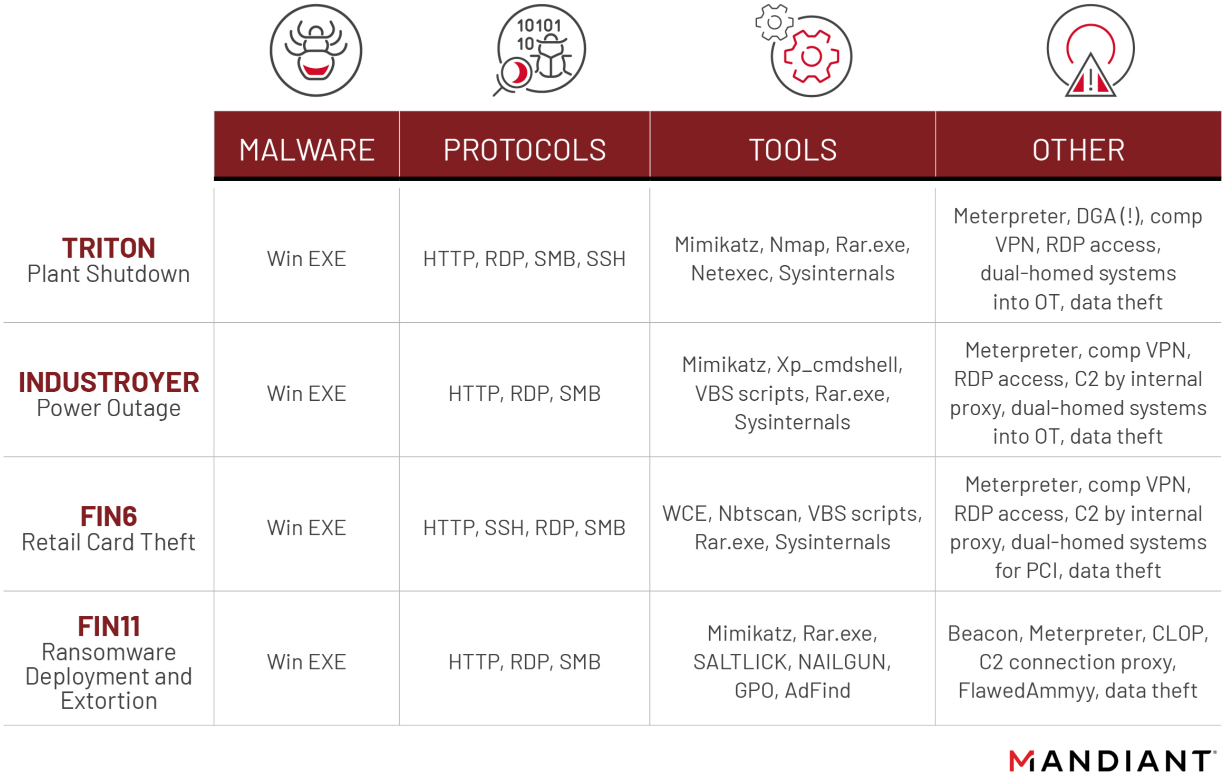
In 2020, Mandiant released a post describing how financial crime actors were expanding their reach into OT. Our assessment was based upon two process kill-lists that were deployed alongside known ransomware strains to amplify the impact of the attacks. These lists were intended to enumerate and terminate software processes, a couple of which were coincidentally related to OT. While there is limited documented information to determine the impact from these process lists, our assessment indicated that by stopping such processes the actor could have abruptly terminated and encrypted critical OT functions resulting in added damage to the victim.

One of the two process kill lists was deployed alongside a CLOP ransomware sample, which we then attributed to a cybercrime actor known as FIN11. The group has monetized their operations using point-of-sale (POS) malware, CLOP ransomware, and traditional extortion.

FIN11 has shown no indication of having specialized OT expertise and there is no evidence indicating that the process kill list they deployed resulted in significant impacts to any victim OT environments. However, the actor's use of a process kill list containing some OT processes brings up further questions about the extent of their capabilities and how they might impact OT in the future.

In the past, financially motivated actors—such as FIN11—have used tactics, techniques and procedures (TTPs) that are comparable to those used by state-sponsored actors to support the early stages of the OT targeted attack lifecycle. This includes using publicly available tooling, living –off-the-land techniques, known exploitation frameworks, and tailored malware to compromise victims.

Figure 1 illustrates some overlaps in techniques used during the TRITON and INDUSTROYER incidents with techniques used by FIN11 and another cybercrime actor, FIN6 for ransomware deployment and extortion and retail card theft.



	MALWARE	PROTOCOLS	TOOLS	OTHER
TRITON Plant Shutdown	Win EXE	HTTP, RDP, SMB, SSH	Mimikatz, Nmap, Rar.exe, Netexec, Sysinternals	Meterpreter, DGA (!), comp VPN, RDP access, dual-homed systems into OT, data theft
INDUSTROYER Power Outage	Win EXE	HTTP, RDP, SMB	Mimikatz, Xp_cmdshell, VBS scripts, Rar.exe, Sysinternals	Meterpreter, comp VPN, RDP access, C2 by internal proxy, dual-homed systems into OT, data theft
FIN6 Retail Card Theft	Win EXE	HTTP, SSH, RDP, SMB	WCE, Nbtscan, VBS scripts, Rar.exe, Sysinternals	Meterpreter, comp VPN, RDP access, C2 by internal proxy, dual-homed systems for PCI, data theft
FIN11 Ransomware Deployment and Extortion	Win EXE	HTTP, RDP, SMB	Mimikatz, Rar.exe, SALTLICK, NAILGUN, GPO, AdFind	Beacon, Meterpreter, CLOP, C2 connection proxy, FlawedAmmyy, data theft

MANDIANT

Figure 1: TTP overlaps among state-sponsored and financially motivated actors

The overlaps in TTPs across the four cases likely exist because reaching target assets—both in IT and OT—often requires an actor to follow a process of lateral movement and escalation of privileges across corporate and/or production networks. As ransomware operators have significantly evolved over the past couple of years, the main difference that remains is that some state-sponsored actors have also invested significant resources to develop OT-tailored payloads to disrupt physical processes.

Mandiant Red Team Used FIN11 Techniques to Move Across a Target's Enterprise Network and Reach OT Servers

The MandiantRed Team supported a European engineering organization to visualize the possible impact of a financially motivated actor deploying ransomware in their environment. The engagement pursued three goals, all of which were successfully accomplished:

- Emulate a ransomware attacker in the IT environment
- Propagate from IT to separate OT network segments
- Emulate multi-faceted extortion by accessing confidential information to steal and redistribute

Figure 2 illustrates the two paths Mandiant pursued to reach OT targets:

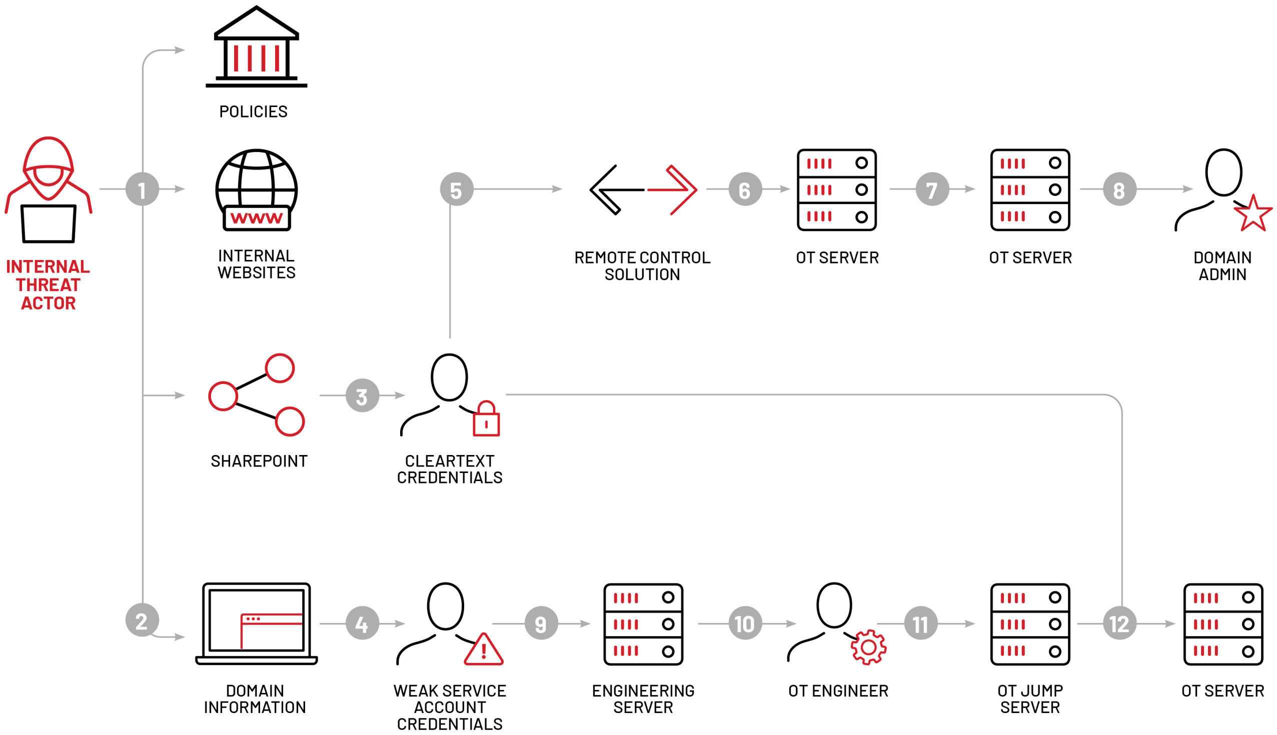


Figure 2: Red Team attack path using FIN11 techniques

For this engagement, Mandiant adopted an "assumed breach" approach, starting from a standard employee account and device on the target's enterprise domain. Mandiant then utilized commonly seen FIN11 techniques to continue the intrusion moving across endpoints in different security zones (see the Appendix). Some of the techniques we used to achieve our objectives in IT and OT included:

- *Reconnaissance of web and internal applications*

  Mandiant discovered several documents that contained cleartext credentials, information on IT architecture, network information, and other confidential data on internal shares and knowledge sharing web applications and wikis.
- *Reconnaissance of Active Directory infrastructure*

  Mandiant used a variation of the public tool BloodHound to gather user, group, group policy objects (GPO), and machine information to build up data structures that describe the target's Active Directory (AD) infrastructure. Mandiant then encrypted and exfiltrated this information to track compromised users and strategize the next steps for the attack.
- *Privilege escalation through CVE-2021-36934*, *aka "SeriousSAM"*

  Mandiant discovered a number of devices vulnerable to CVE-2021-36934. Exploiting this vulnerability, Mandiant downloaded the Security Account Manager (SAM) databases of these devices and utilized the Impacket library to extract secrets from it, including the password hashes for local accounts, computer account passwords, and cached domain credentials.

- *Lateral movement through silver ticket*

  Mandiant forged Silver tickets – Kerberos Ticket Granting Service (TGS) tickets necessary for user authentication – using the ticketer.py script from the Impacket library. This enabled the Red Team to impersonate any user on the victim service (including administrative accounts) to escalate privileges on specific endpoints in the IT network.
- *Privilege escalation through Active Directory Certificate Services abuse*

  Mandiant discovered that the target's AD Certificate Services (CS) configuration contained at least one misconfiguration in a Certificate Template, which allowed the requesting entity to request certificates for other principals in the target's AD domains. Mandiant enumerated the AD CS configuration using the public Certify tool.

Pivoting to OT on Multiple Fronts

Using the information and privileges gathered through the enterprise network compromises, Mandiant identified the best paths to reach the target OT servers. Mandiant focused on reaching two different specific targets: an isolated legacy OT network and a global OT network with connections across different regions.

OT Compromise #1 – Establish Foothold and Privilege Escalation in Legacy OT Network

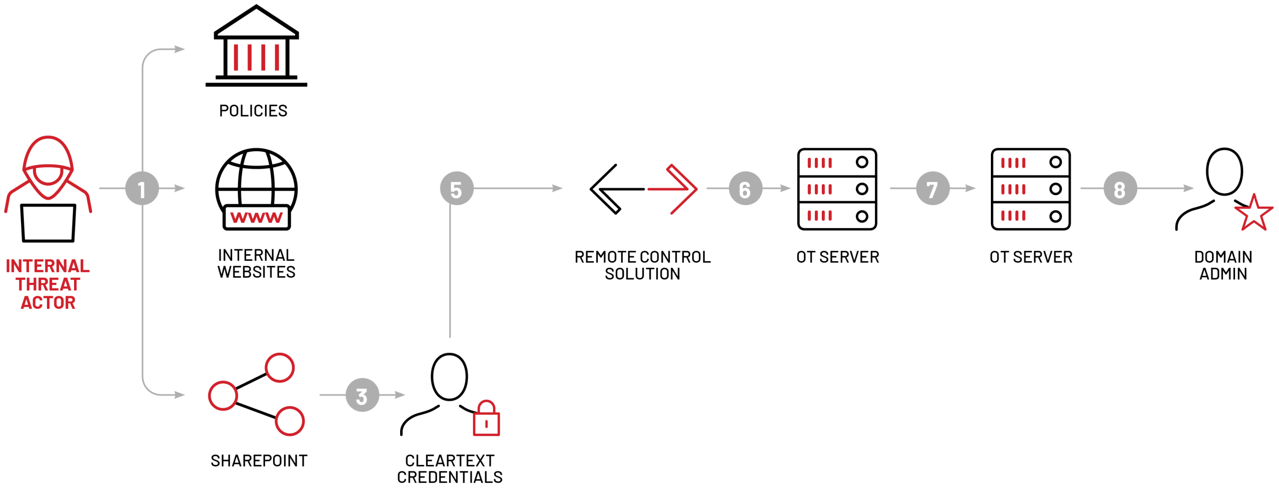


Figure 3: Red Team attack path for OT Compromise #1

Mandiant used the same credentials and documentation acquired during initial phases in the corporate network to gain access to remote management software installed on a host with access to the OT network. Mandiant then enumerated the host's network defenses and observed that it did not utilize SSL/TLS inspection, which allowed the Red Team to launch an implant that utilized domain fronting as a means for command and control (C&C).

Further network enumeration uncovered that the account accessed via the remote management software also had administrative privileges on other hosts in the OT network. Mandiant used the remote desktop protocol (RDP) to access multiple hosts, enumerate their defenses, and upload a custom crafted C&C implant payload via Server Message Block (SMB) protocol and RDP. Mandiant then executed these payloads via remote service creation, Windows Management Instrumentation (WMI) command execution, and manual execution. Given that these protocols and services were also being utilized by legitimate users, it is unlikely that such activity would raise any alerts, making the lateral movement blend into background traffic and decreasing the likelihood of discovery by network sensors.

In total, Mandiant accessed eight servers within the OT network, one of which was a Human Machine Interface (HMI). Access to this system would allow an attacker to maliciously interact with the physical control process using native commands. Once Mandiant established a foothold and had administrative access, the focus shifted to privilege escalation.

- Mandiant dumped the SAM database on one of the hosts to retrieve local account password hashes, which we cracked using a dictionary attack. This revealed the cleartext password for one of the local administrator accounts.
- Utilizing local administrator credentials Mandiant created a memory dump of the Local Security Authority Subsystem Service (LSASS) process on another OT host using the Task Manager application.
- Mandiant exfiltrated a memory dump file and retrieved the contained credentials using a specifically packed version of the public tool Mimikatz. The recovered credentials contained the NTLM hash for a Domain Administrator account on the OT network domain.
- Mandiant then completed the objective by utilizing the Domain Administrator account password hash and executing our custom payload on the OT domain controller via remote service creation.

OT Compromise #2: Move Laterally from IT to Global OT Network

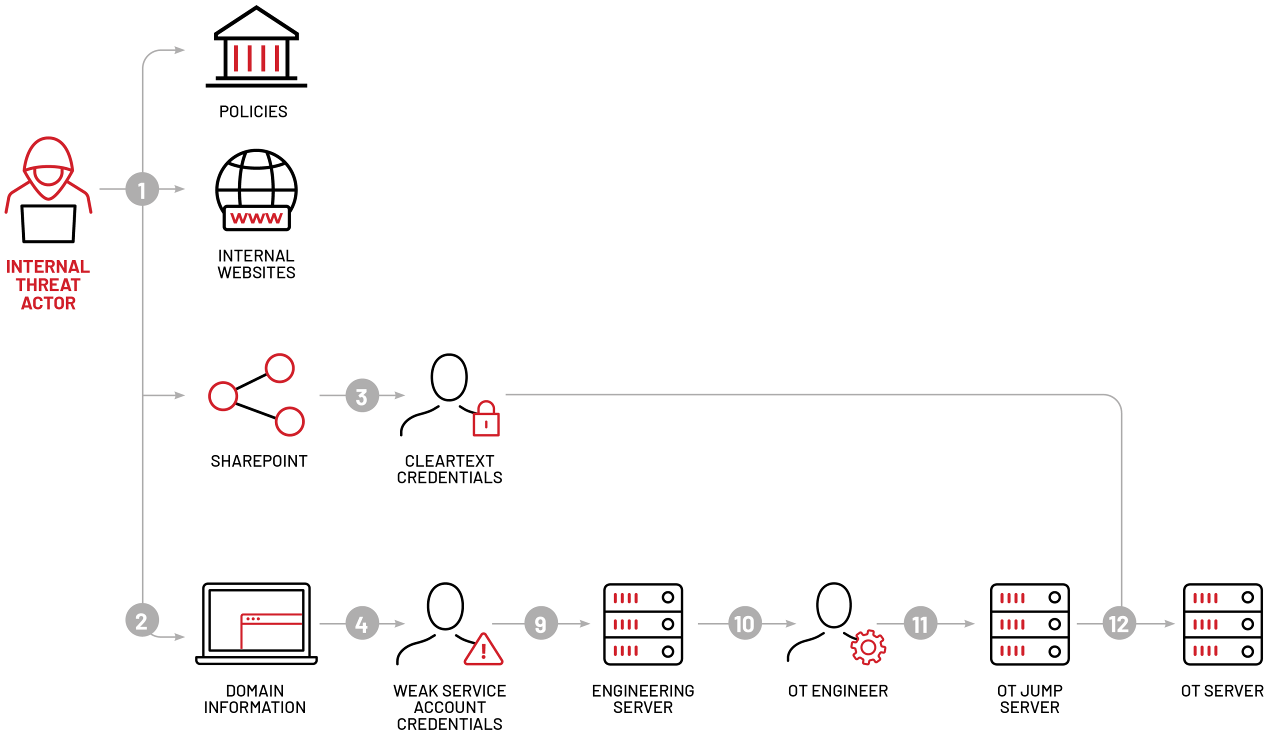


Figure 4: Red Team attack path for OT Compromise #2

For the second attack path, Mandiant escalated privileges within the target's enterprise domain with an "AS-REP roast" attack using the Impacket library to recover multiple user account password hashes. Mandiant cracked password hashes using a dictionary attack, which revealed the cleartext password for one of the accounts. The user account and credentials had RDP privileges onto an additional host, allowing Mandiant to move laterally within the enterprise environment.

The accessed host contained engineering software, which indicated it was likely a jumphost or an application server for engineers. Additionally, the engineering application installed on the host used shortcuts on the desktop that pointed to batch (BAT) files in a directory writeable by non-privileged users. This allowed Mandiant to alter the content of the BAT files to launch unauthorized applications when users clicked the shortcut on the desktop.

Multiple users fell victim to this attack. One of these users was a member of several AD groups and had RDP privileges to various OT jump hosts. Mandiant used the Rubeus tool to extract the user's Kerberos Ticket Granting Ticket (TGT) from an active session on the compromised host. This allowed Mandiant to import the TGT on a system that was already controlled by the Red Team and then request a TGS for the "TERMSRV/<HOST>" service, which can be used to connect via RDP to a target host using Remote Credential Guard or Restricted Admin Mode. Finally, Mandiant launched the Remote Desktop session via the "mstsc /remoteGuard" command to connect to several OT jumphosts via RDP.

To complete the objective, Mandiant again used credentials acquired during the reconnaissance phase to authenticate to an OT server from one of the OT jumphosts. The OT server ran a client/server-based SCADA software solution which was fully accessible and already active on the machine; however due to operational impact concerns, the Red Team refrained from interacting with the application. Access to this type of software could potentially allow an attacker to perform in-depth reconnaissance of the OT environment, exfiltrate sensitive information, deploy additional payloads (e.g., ransomware), or even degrade the victim's ability to monitor or control the process.

Ransomware Attack Emulation Provides Critical Insight on Defensive Capabilities

OT systems are critical for organizations to automate production processes. As a result, they are attractive targets for actors intending to disrupt production either for profit or to produce physical damage. The overlaps in TTPs between ransomware operators and OT-focused APTs suggest that protecting against ransomware operations also yields significant defenses against other impactful events, such as a cyber physical attack.

As of mid-2022 we have not observed financially motivated actors explicitly targeting OT networks to extort victims, however we highlight that actors have carried out ransomware attacks that impacted OT processes. Actors with access to OT assets may be empowered to disrupt the victim's control or visibility over a process in several ways. OT asset owners and operators benefit from ransomware attack emulation by confronting the latest adversary TTPs, identifying vulnerabilities in their environment and improving breach detection and response capabilities.

For more information about attack emulation and red teaming services for OT, please see our previous post on proactive security service offerings for OT. Visit our website to request more information about Mandiant services for OT, red team assessments or threat intelligence.

Appendix: FIN11 Techniques Utilized for the Red Team Engagement

Table 1: List of FIN11 techniques used for the Red Team emulation

TTP	Emulation
Initial Access	
T1192: Spear-Phishing Link	Out of Scope

T1193: Spearphishing Attachment	Out of Scope
Execution	
T1047: Windows Management Instrumentation	Yes
T1086: PowerShell	Yes
T1053: Scheduled Task	No
T1064: Scripting	Yes
T1059: Command-Line Interface	Yes
T1035: Service Execution	Yes
T1204: User Execution	Yes
Persistence	
T1133: External Remote Services	Out of Scope
T1053: Scheduled Task	No
T1060: Registry Run Keys / Start Folder	No
T1015: Accessibility Features	No
T1138: Application Shimming	No
T1004: Winlogon Helper DLL	No
T1050: New Service	Yes
T1078: Valid Accounts	Yes

T1108: Redundant Access	Yes
Privilege Escalation	
T1138: Application Shimming	No
T1055: Process Injection	Yes
T1015: Accessibility Features	No
T1050: New Service	Yes
T1053: Scheduled Task	No
T1078: Valid Accounts	Yes
T1086: Exploitation for Privilege Escalation	Yes
Defensive Evasion	
T1055: Process Injection	Yes
T1045: Software Packing	Yes
T1107: File Deletion	Yes
T1064: Scripting	Yes
T1116: Code Signing	Yes
T1112: Modify Registry	No
T1070: Indicator Removal on Host	Yes
T1027: Obfuscated Files or Information	Yes

T1202: Indirect Command Execution	Yes
T1090: Connection Proxy	Yes
T1078: Valid Accounts	Yes
T1140: Deobfuscate/Decode Files or Information	Yes
T1108: Redundant Access	Yes
Credential Access	
T1003: Credential Dumping	Yes
T1558: Kerberoasting	Yes
T1003.006: DCSync	No
Discovery	
T1082: System Information Discovery	Yes
T1057: Process Discovery	Yes
T1063: Security Software Discovery	Yes
Lateral Movement	
T1021: Remote Services	Yes
T1076: Remote Desktop Protocol	Yes
T1105: Remote File Copy	Yes
Collection	

T1125: Video Capture	No
T1113: Screen Capture	No
T1119: Automated Collection	Yes
T1005: Data from Local System	Yes
Command and Control	
T1090: Connection Proxy	Yes
T1071: Standard Application Layer Protocol	Yes
T1094: Custom C2 Protocol	No
T1105: Remote File Copy	Yes
T1032: Standard Cryptographic Protocol	Yes
T1043: Commonly Used Port	Yes
T1065: Uncommonly Used Port	No
T1219: Remote Access Tools	Yes
Exfiltration	
T1002: Data Compressed	Out of Scope
T1022: Data Encrypted	Out of Scope
T1041: Exfiltration Over C2 Channel	Out of Scope
T1048: Exfiltration Over Alternative Protocol	Out of Scope

Impact	
T1486: Data Encrypted for Impact	Out of Scope
T1529: System Shutdown/Reboot	Out of Scope
T1485: Data Destruction	Out of Scope
T1488: Disk Content Wipe	Out of Scope
T1489: Service Stop	Out of Scope