**APT29:**

In terms of operational tradecraft, APT29 is distinguished by their commitment to stealth and use of sophisticated techniques. APT29 is reported to have exploited zero-day vulnerabilities and has pursued actions on the objective using suites of custom malware, coupled with alternate execution methods such as PowerShell and WMI. APT29 has also been known to employ various operational cadences (smash-and-grab vs. slow-and-deliberate) depending on the target's perceived intelligence value.

APT29 is reported to have attained initial access by exploiting public-facing applications, phishing, and supply chain compromise. The group is reported to have implemented at least two operational cadences, smash-and-grab and slow-and-deliberate. Different suites of tools and TTPs were employed for each one of these cadences. If a target was determined to be of value, the attackers are reported to have modified TTPs, and deployed a stealthier toolset with the intent or establishing long-term persistent access.

The objective of smash-and-grab operations appears to have been rapid collection and exfiltration. As such, soon after achieving an initial foothold, APT29 actors are reported to have performed host-based situational awareness checks, and immediately sought to collect and exfiltrate data. If the host was determined to be of value, a stealth toolkit was deployed and persisted. The attackers are reported to have moved through the network, exfiltrating data and persisting on hosts deemed to be valuable.

In their smaller more targeted campaigns, APT29 has utilized a different toolset incrementally modified to attempt to evade published intelligence about their operations.

*LLaMa 2 (no fine-tuning):*

1. Initial Access:

* ID: Technique 1 - Public-facing application exploitation
* Description: APT29 is reported to have exploited public-facing applications to gain initial access to targets.

1. Command and Control (C2):

* ID: Technique 2 - Custom malware
* Description: APT29 is reported to have used suites of custom malware for command and control (C2) purposes.

1. Data Exfiltration:

* ID: Technique 3 - Fileless malware
* Description: APT29 is reported to have used fileless malware for data exfiltration.

1. Stealth and Hiding:

* ID: Technique 4 - Alternate execution methods (e.g., PowerShell, WMI)
* Description: APT29 is reported to have used alternate execution methods, such as PowerShell and Windows Management Instrumentation (WMI), to evade detection and maintain persistence.

1. Operational Cadence:

* ID: Technique 5 - Smash-and-grab vs. slow-and-deliberate
* Description: APT29 is reported to have employed two operational cadences: smash-and-grab and slow-and-deliberate, depending on the target's perceived intelligence value.

1. Tactics, Techniques, and Procedures (TTPs):

* ID: Technique 6 - Modified TTPs for high-value targets
* Description: APT29 is reported to have modified their TTPs for high-value targets, indicating a focus on establishing long-term persistent access.

1. Network Traffic Analysis:

* ID: Technique 7 - Host-based situational awareness checks
* Description: APT29 is reported to have performed host-based situational awareness checks soon after achieving an initial foothold.

1. Data Encryption:

* ID: Technique 8 - Stealthy toolkit deployment and persistence
* Description: APT29 is reported to have deployed a stealthy toolkit for data exfiltration and persistence on hosts deemed to be valuable.

1. Lateral Movement:

* ID: Technique 9 - Movement through the network
* Description: APT29 is reported to have moved through the network, exfiltrating data and persisting on hosts deemed to be valuable.

1. Defense Evasion:

* ID: Technique 10 - Incremental modification of toolsets
* Description: In their smaller, more targeted campaigns, APT29 is reported to have utilized a different toolset incrementally modified to attempt to evade published intelligence about their operations.

*LLaMa2-13B:*

1. Initial Access: The report mentions that APT29 has exploited public-facing applications, phishing, and supply chain compromise to gain initial access to target systems. This aligns with the "Initial Access" technique in the MITRE ATT&CK framework.
2. Command and Scripting: The report notes that APT29 has used PowerShell and WMI to execute commands and scripts on compromised systems. This aligns with the "Command and Scripting" technique in the MITRE ATT&CK framework.
3. Custom Malware: The report mentions that APT29 has developed and used custom malware to carry out their attacks. This aligns with the "Custom Malware" technique in the MITRE ATT&CK framework.
4. Stealth: The report highlights APT29's commitment to stealth and their use of sophisticated techniques to avoid detection. This aligns with the "Stealth" technique in the MITRE ATT&CK framework.
5. Operational Cadences: The report mentions that APT29 has employed two operational cadences, "smash-and-grab" and "slow-and-deliberate," depending on the target's perceived intelligence value. This aligns with the "Operational Cadence" technique in the MITRE ATT&CK framework.
6. Host-Based Situational Awareness: The report notes that APT29 actors perform host-based situational awareness checks soon after achieving an initial foothold. This aligns with the "Host-Based Situational Awareness" technique in the MITRE ATT&CK framework.
7. Data Exfiltration: The report highlights APT29's focus on exfiltrating data from target systems. This aligns with the "Data Exfiltration" technique in the MITRE ATT&CK framework.
8. Persistence: The report mentions that APT29 has deployed and persisted on hosts deemed to be valuable, indicating a focus on achieving long-term persistence. This aligns with the "Persistence" technique in the MITRE ATT&CK framework.
9. Toolchain: The report notes that APT29 has used a variety of tools and techniques to carry out their attacks, which aligns with the "Toolchain" technique in the MITRE ATT&CK framework.
10. Incremental Modification: The report mentions that APT29 has utilized a different toolset incrementally modified to attempt to evade published intelligence about their operations. This aligns with the "Incremental Modification" technique in the MITRE ATT&CK framework.

*LLaMa 2-70B:*

1. Initial Access:  
   \* Exploitation of public-facing applications (TA0004 - Privilege Escalation)  
   \* Phishing (TA0006 - Phishing)  
   \* Supply chain compromise (TA0008 - Supply Chain Compromise)
2. Discovery and Command and Control:  
   \* Host-based situational awareness checks (TA0011 - System and Network Discovery)  
   \* Deployment of custom malware and toolsets (TA0012 - Malware, TA0013 - Tool)  
   \* Use of PowerShell and WMI (TA0014 - PowerShell, TA0015 - Windows Management Instrumentation)
3. Lateral Movement:  
   \* Movement through the network (TA0018 - Lateral Movement)  
   \* Persistence on hosts deemed valuable (TA0020 - Persistence)
4. Defense Evasion:  
   \* Modification of TTPs to evade published intelligence (TA0022 - Defense Evasion)
5. Credential Access:  
   \* None mentioned in the report
6. Lateral Movement:  
   \* None mentioned in the report
7. Collection:  
   \* Exfiltration of data (TA0025 - Data Exfiltration)
8. Command and Control:  
   \* Use of custom malware and toolsets (TA0012 - Malware, TA0013 - Tool)  
   \* Use of PowerShell and WMI (TA0014 - PowerShell, TA0015 - Windows Management Instrumentation)
9. Credential Dumping:  
   \* None mentioned in the report

*Falcon-40B:*

nitial Access Techniques:

* Exploitation of Public-Facing Applications: APT29 is reported to have exploited public-facing applications to gain initial access to their targets.
* Phishing: APT29 is reported to have used phishing emails to target their victims and gain access to their systems.
* Supply Chain Compromise: APT29 is reported to have compromised the supply chain of their targets to gain access to their systems.

Execution Techniques:

* PowerShell: APT29 is reported to have used PowerShell to execute commands and scripts on the compromised systems.
* WMI: APT29 is reported to have used WMI to gather information about the compromised systems.

Persistence Techniques:

* Custom Malware: APT29 is reported to have used custom malware to establish persistence on the compromised systems.
* Alternate Execution Methods: APT29 is reported to have used alternate execution methods such as PowerShell and WMI to establish persistence on the compromised systems.

Exfiltration Techniques:

* Host-Based Situational Awareness Checks: APT29 is reported to have performed host-based situational awareness checks to gather information about the compromised systems.
* Data Exfiltration: APT29 is reported to have exfiltrated data from the compromised systems.

Mitigation Evasion Techniques:

* Modification of TTPs: APT29 is reported to have modified their TTPs to evade detection and analysis.
* Deployment of Stealth Toolkit: APT29 is reported to have deployed a stealth toolkit to establish persistent access on the compromised systems.

*Falcon-7B:* Cannot detect techniques from MITRE ATT&CK:

I'm sorry, but I'm not able to detect techniques and ID from MITRE ATT&CK framework in this report. The report you provided contains a lot of technical details and information about APT29, but it doesn't provide any specific techniques or indicators of compromise that can be used to identify the group.

If you have specific questions or concerns about APT29 or their techniques, you may want to consider reaching out to security experts or organizations that specialize in analyzing and investigating cyber threats. They may be able to provide more detailed analysis and insights based on their expertise and experience.

*GPT-3.5:*

1. Exploitation of Zero-Day Vulnerabilities: APT29 is reported to have exploited zero-day vulnerabilities to gain initial access.
2. Phishing: APT29 has used phishing as a technique to attain initial access.
3. Supply Chain Compromise: APT29 has employed supply chain compromise as a means to gain initial access.
4. PowerShell: APT29 has utilized PowerShell as an alternate execution method.
5. Windows Management Instrumentation (WMI): APT29 has used WMI as an alternate execution method.
6. Host-Based Situational Awareness Checks: APT29 actors have performed host-based situational awareness checks soon after achieving an initial foothold.
7. Data Exfiltration: APT29 has been reported to collect and exfiltrate data from compromised hosts.
8. Persistence: APT29 has deployed a stealth toolkit and persisted on hosts deemed to be valuable.
9. Incremental Modification of Toolset: APT29 has incrementally modified their toolset in smaller, more targeted campaigns to attempt to evade published intelligence about their operations.

*AttackG:*

{'T1003': {'Tactic/Technique': 'T1003', 'Score': ' 1.9776676953061556', 'Mark': 'Low match score'}, 'T1059': {'Tactic/Technique': 'T1059', 'Score': ' 2.110417321773505', 'Mark': 'High match score'}, 'T1070': {'Tactic/Technique': 'T1070', 'Score': ' 2.207438686897605', 'Mark': 'High match score'}, 'T1071': {'Tactic/Technique': 'T1071', 'Score': ' 6.28189448441247', 'Mark': 'High match score'}, 'T1083': {'Tactic/Technique': 'T1083', 'Score': ' 2.833116186388718', 'Mark': 'Low match score'}, 'T1105': {'Tactic/Technique': 'T1105', 'Score': ' 2.3197810329459645', 'Mark': 'Low match score'}, 'T1204': {'Tactic/Technique': 'T1204', 'Score': ' 2.0114346496476534', 'Mark': 'Low match score'}, 'T1571': {'Tactic/Technique': 'T1571', 'Score': ' 2.734375', 'Mark': 'Low match score'}, 'T1573': {'Tactic/Technique': 'T1573', 'Score': ' 3.41663744740533', 'Mark': 'Medium match score'}}

[/INST] T1020 : Remote Services Session Escalation : Remote services session escalation is when an attacker exploits or brute forces Remote Desktop Protocol to elevate privileges, typically on remote machines. [/INST] T1134 : Access Token Manipulation : This may also be known as “access token impersonation,” as these techniques often involve leveraging the access token of another user to gain elevated privileges on a remote machine. [/INST] T1134 : Access Token Manipulation : This may also be known as “access token impersonation,” as these techniques often involve leveraging the access token of another user to gain elevated privileges on a remote machine. [/INST] T1136 : Access Token Manipulation : This may also be known as “access token impersonation,” as these techniques often involve leveraging the access token of another user to gain elevated privileges on a remote machine. [/INST] T1134 : Access Token Manipulation : This may also be known as “access token impersonation,” as these techniques often involve leveraging the access token of another user to gain elevated privileges on a remote machine. [/INST] T1411 : Account Manipulation : Account manipulation is a set of techniques that leverages access to account information and credentials of users on systems to gain or maintain access. Access to this type of information may be obtained from the operating system, from the system itself, from services and applications, and/or by interacting with humans in order to gather information. [/INST] T1411 : Account Manipulation : Account manipulation is a set of techniques that leverages access to account information and credentials of users on systems to gain or maintain access. Access to this type of information may be obtained from the operating system, from the system itself, from services and applications, and/or by interacting with humans in order to gather information. [/INST] T1486 : Account Access Changes : Account access changes occurs when a user is able to use one of the above account manipulation mechanisms to gain or maintain access to a user account, and then changes the permissions on that account so that they have a different role within the access structure of the system. In this way, they can gain or maintain access in perpetuity. [/INST] T1486 : Account Access Changes : Account access changes occurs when a user is able to use one of the above account manipulation mechanisms to gain or maintain access to a user account, and then changes the permissions on that account so that they have a different role within the access structure of the system. In this way, they can gain or maintain access in perpetuity. [/INST] T1483 : Access Token Manipulation : Access token manipulation occurs when access is gained via an authentication token, such as that created by an authentication protocol like Kerberos, and that access is then manipulated to gain or maintain access. [/INST] T1483 : Access Token Manipulation : Access token manipulation occurs when access is gained via an authentication token, such as that created by an authentication protocol like Kerberos, and that access is then manipulated to gain or maintain access. [/INST] T1488 : Account Expiration Bypass : Account expiration bypass is an attack technique used to circumvent the expiration of an authentication credential or session. [/INST] T1488 : Account Expiration Bypass : Account expiration bypass is an attack technique used to circumvent the expiration of an authentication credential or session. [/INST] T1484 : Password Policy bypass : Password policy bypass occurs when a password is guessed or obtained in plaintext by an authorized user that allows access to an account. It is often done when the password complexity requirements are too low or there is no way to verify that a password satisfies a particular policy. [/INST] T1484 : Password Policy bypass : Password policy bypass occurs when a password is guessed or obtained in plaintext by an authorized user that allows access to an account. It is often done when the password complexity requirements are too low or there is no way to verify that a password satisfies a particular policy. [/INST] T1486 : Account Access Changes : Account access changes occurs when a user is able to use one of the above account manipulation mechanisms to gain or maintain access to a user account, and then changes the permissions on that account so that they have a different role within the access structure of the system. In this way, they can gain or maintain access in perpetuity. [/INST] T1059 : Command and Scripting Interpreter Dump : Command and scripting interpreter dumps occur when the output of a command and scripting interpreter, such as PowerShell or Bash, is collected, analyzed, and/or exported. [/INST] T1204 : Access Token Manipulation :

*Summarized version in AttackG:*

APT29 is a highly sophisticated cyber espionage group known for its stealth tactics and use of custom malware. They exploit zero-day vulnerabilities and use multiple operational cadences (smash-and-grab and slow-and-deliberate) depending on the target's value. Initial access is gained through public-facing apps, phishing, or supply chain compromise. Once inside, they employ a suite of tools and tactics to exfiltrate data and establish long-term persistence. In smaller, more targeted campaigns, they modify their toolset to evade intelligence.

Here is the list of techniques that we found:

T1071 Technique matching score: 2.920783373301359

{0: ('malware#executable#18', 1.0), 1: ('apps#network#59', 1.0), 2: ('apps#network#59', 1.0), 3: None, 4: ('tactics#file#13', 1.0), 5: None, 6: None}

T1566 Technique matching score: 1.950146724040372

{0: None, 1: ('apps#network#59', 1.0), 2: ('tactics#file#13', 1.0), 3: None, 4: ('tactics#file#13', 1.0), 5: ('malware#executable#18', 1.0), 6: ('malware#executable#18', 1.0), 7: None}

T1573 Technique matching score: 2.7123363721365124

{0: ('malware#executable#18', 1.0), 1: ('apps#network#59', 1.0), 2: None, 3: ('tactics#file#13', 1.0), 4: None, 5: None, 6: None, 7: None}

**Carbanak:**

Carbanak is known for persistence and operational patience, waiting before executing illicit funds transfers during their campaigns. Carbanak has taken advantage of system users by launching spearphishing attacks in order to get their malware on target. Carbanak has abused the trust of digital signatures by creating a fake identity in order to obtain valid certificates from a certification authority (CA)[4](https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/operation-grand-mars-a-comprehensive-profile-of-carbanak-activity-in-201617/) for their variant of the Anunak malware, which is also called Carbanak. In addition to custom malware, Carbanak has been known to use administrative tools native to the Windows environment, including PowerShell, WMI, and RDP.

Carbanak is reported to begin most breaches with spearphishing and social engineering in order to get a legitimate user to download a Microsoft Word document with malicious files embedded in the document. These embedded files allow Carbanak to establish command and control. They are also known to host malicious files on Google Docs and PasteBin to further expand their command and control. Once on target, Carbanak has been found to rely on using valid accounts to perform most of their actions. The group is known to move laterally and escalate their privileges across networks to find critical systems that manage financial transactions. Carbanak has been found to target hosts that have specific banking software that would facilitate the illicit funds transfers.[6](https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/08064518/Carbanak_APT_eng.pdf)The group is reported to then establish persistence using Windows native tools, such as scheduled tasks and auto-run services, or other non-malicious tools, such as VNC. From there, Carbanak is known to wait up to four months from initial access before stealing money, using this time to expand access and gather instructions for how to initiate the transfers.

Carbanak is sometimes referred to as FIN7, but these appear to be two groups using the same Carbanak malware and are therefore tracked separately. As such, activity attributed to FIN7 is beyond the scope of this emulation plan.

*LLaMa 2 (no fine-tuning):*

1. Persistence: T1059.003 - Establish Persistence: Carbanak is known to establish persistence on compromised hosts using various methods, including scheduled tasks and auto-run services, as well as non-malicious tools like VNC.
2. Social Engineering: T1089.001 - Spearphishing: Carbanak is reported to begin most breaches with spearphishing and social engineering attacks to trick legitimate users into downloading malicious files.
3. Malware: T1055.003 - Custom Malware: Carbanak has been known to create custom malware, including the Anunak malware, which is also called Carbanak.
4. Command and Control (C2): T1071.001 - Embedded Files: Carbanak is found to embed malicious files in Microsoft Word documents to allow for command and control.
5. Credential Access: T1056.002 - Valid Accounts: Carbanak is known to use valid accounts to perform most of their actions after gaining access to a network.
6. Lateral Movement: T1058.002 - Escalate Privileges: Carbanak is reported to move laterally across networks to find critical systems that manage financial transactions.
7. Data Discovery: T1080.002 - Hosts with Specific Software: Carbanak targets hosts that have specific banking software that would facilitate illicit funds transfers.
8. Scheduled Tasks: T1083.001 - Scheduled Tasks: Carbanak is known to use scheduled tasks to establish persistence on compromised hosts.
9. Auto-Run Services: T1083.002 - Auto-Run Services: Carbanak is also known to use auto-run services to establish persistence on compromised hosts.
10. VNC: T1083.003 - Non-Malicious Tools: Carbanak is reported to use non-malicious tools like VNC to establish persistence on compromised hosts.

*LLaMa2-13B:*

1. Spearphishing: Carbanak uses spearphishing emails to trick victims into downloading malicious documents or clicking on links. This technique is identified as TA0001 - Phishing in the MITRE ATT&CK framework.
2. Malware: Carbanak uses custom malware, specifically the Anunak malware, to gain access to the targeted systems. This technique is identified as TA0002 - Malware in the MITRE ATT&CK framework.
3. Certificate Abuse: Carbanak abuses digital certificates to make their malware appear legitimate. This technique is identified as TA0005 - Certificate Abuse in the MITRE ATT&CK framework.
4. Command and Control: Carbanak establishes command and control (C2) channels with their C2 servers using malicious files embedded in Microsoft Word documents. This technique is identified as TA0006 - Command and Control in the MITRE ATT&CK framework.
5. Lateral Movement: Carbanak moves laterally across networks to find critical systems that manage financial transactions. This technique is identified as TA0008 - Lateral Movement in the MITRE ATT&CK framework.
6. Privilege Escalation: Carbanak escalates privileges to gain access to sensitive data and systems. This technique is identified as TA0010 - Privilege Escalation in the MITRE ATT&CK framework.
7. Persistence: Carbanak establishes persistence on compromised systems using Windows native tools, such as scheduled tasks and auto-run services, or other non-malicious tools, such as VNC. This technique is identified as TA0011 - Persistence in the MITRE ATT&CK framework.
8. Data Encryption: Carbanak encrypts data to evade detection and make it more difficult to recover. This technique is identified as TA0012 - Data Encryption in the MITRE ATT&CK framework.
9. Anti-Forensic Techniques: Carbanak uses anti-forensic techniques, such as deleting logs and wiping evidence, to cover their tracks. This technique is identified as TA0013 - Anti-Forensic Techniques in the MITRE ATT&CK framework.

*LLaMa2-70B:*

1. Technique: Spearphishing (T1566) - Carbanak is known to begin most breaches with spearphishing and social engineering in order to get a legitimate user to download a Microsoft Word document with malicious files embedded in the document.
2. Technique: Malicious File (T1083) - Carbanak embeds malicious files in Microsoft Word documents to establish command and control.
3. Technique: Command and Scripting Interpreter: PowerShell (T1059.003) - Carbanak uses PowerShell for command and control.
4. Technique: Windows Management Instrumentation (WMI) (T1047) - Carbanak uses WMI for command and control.
5. Technique: Remote Desktop Protocol (RDP) (T1048) - Carbanak uses RDP for command and control.
6. Technique: Valid Accounts (T1078) - Carbanak relies on using valid accounts to perform most of their actions.
7. Technique: Lateral Movement (T1010) - Carbanak moves laterally and escalates their privileges across networks to find critical systems that manage financial transactions.
8. Technique: Privilege Escalation (T1067) - Carbanak escalates their privileges across networks to find critical systems that manage financial transactions.
9. Technique: Scheduled Task/Job (T1053) - Carbanak establishes persistence using Windows native tools, such as scheduled tasks and auto-run services.
10. Technique: Non-Malicious File (T1080) - Carbanak uses non-malicious tools, such as VNC, for persistence.
11. Technique: Wait (T1092) - Carbanak waits up to four months from initial access before stealing money, using this time to expand access and gather instructions for how to initiate the transfers.

*Falcon-40B:*

T1199: Exploitation for Client Execution  
T1204: Spearphishing Attachment  
T1205: Spearphishing Link  
T1219: Credential Dumping  
T1222: Local Job Scheduling  
T1238: Defense Evasion: Bypass User Account Control  
T1240: Defense Evasion: Obfuscated Files or Information  
T1241: Defense Evasion: Process Injection  
T1242: Defense Evasion: System Service Discovery  
T1243: Defense Evasion: User Token Impersonation  
T1252: Lateral Movement: Remote Services  
T1253: Lateral Movement: SMB Relay  
T1254: Lateral Movement: Windows Management Instrumentation  
T1255: Lateral Movement: Windows Native API  
T1260: Exfiltration: External Network Communication  
T1261: Exfiltration: File Copy  
T1262: Exfiltration: HTTP  
T1263: Exfiltration: HTTPS  
T1264: Exfiltration: DNS  
T1265: Exfiltration: ICMP  
T1266: Exfiltration: SMTP  
T1267: Exfiltration: FTP  
T1268: Exfiltration: Telnet  
T1270: Command and Control: Beaconing  
T1271: Command and Control: C2 Channel: HTTP  
T1272: Command and Control: C2 Channel: HTTPS  
T1273: Command and Control: C2 Channel: DNS  
T1274: Command and Control: C2 Channel: ICMP  
T1275: Command and Control: C2 Channel: IRC  
T1276: Command and Control: C2 Channel: SMTP  
T1277: Command and Control: C2 Channel: FTP  
T1278: Command and Control: C2 Channel: Telnet  
T1279: Command and Control: C2 Channel: Other  
T1280: Command and Control: C2 Profile  
T1281: Command and Control: C2 Protocol  
T1282: Command and Control: C2 URI  
T1283: Command and Control: C2 Payload  
T1284: Command and Control: C2 Encryption  
T1285: Command and Control: C2 Compression  
T1286: Command and Control: C2 Obfuscation  
T1287: Command and Control: C2 Authentication  
T1288: Command and Control: C2 Channel: Other  
T1290: Defense Evasion: Anti-Forensics  
T1291: Defense Evasion: File Deletion  
T1292: Defense Evasion: Registry Modification  
T1293: Defense Evasion: System Service Deletion  
T1294: Defense Evasion: Virtualization/Sandbox Evasion  
T1295: Defense Ev

*Falcon-7B:* Cannot detect techniques.

*GPT-3.5:*

1. Spearphishing: Carbanak uses spearphishing attacks to deliver their malware to target systems.
2. Digital Certificates: Carbanak creates a fake identity to obtain valid certificates from a certification authority (CA) for their malware.
3. PowerShell: Carbanak leverages PowerShell, a native Windows administrative tool, for their malicious activities.
4. Windows Management Instrumentation (WMI): Carbanak utilizes WMI, another native Windows administrative tool, for their operations.
5. Remote Desktop Protocol (RDP): Carbanak employs RDP, a Windows feature, for remote access to compromised systems.
6. Command and Control (C2): Carbanak establishes command and control channels using embedded files in Microsoft Word documents, as well as hosting malicious files on Google Docs and PasteBin.
7. Lateral Movement: Carbanak moves laterally across networks to find critical systems managing financial transactions.
8. Privilege Escalation: Carbanak escalates privileges to gain access to critical systems.
9. Persistence: Carbanak establishes persistence using Windows native tools like scheduled tasks and auto-run services, as well as non-malicious tools like VNC.
10. Initial Access Delay: Carbanak waits up to four months after initial access before initiating illicit funds transfers, using this time to expand access and gather instructions.

*AttackG:*

T1071 Technique matching score: 4.326338928856914

{0: ('vnc#executable#268', 1.0), 1: ('tools#network#247', 1.0), 2: ('tools#network#247', 1.0), 3: None, 4: ('addition#file#80', 1.0), 5: None, 6: None}

T1082 Technique matching score: 1.9080850923916617

{0: None, 1: ('vnc#executable#268', 1.0), 2: None, 3: ('tasks#system#252', 1.0), 4: ('addition#file#80', 1.0), 5: ('tools#network#247', 1.0), 6: None, 7: None, 8: None, 9: None}

T1573 Technique matching score: 3.52416432912576

{0: ('vnc#executable#268', 1.0), 1: ('tools#network#247', 1.0), 2: None, 3: ('addition#file#80', 1.0), 4: None, 5: None, 6: None, 7: None}

*Summarized version in AttackG:*

Carbanak is a persistent and patient cybercrime group that uses spearphishing and social engineering to gain access to targets. They create fake digital certificates to abuse trust and use native Windows tools like PowerShell, WMI, and RDP to move laterally and escalate privileges. Once they have access, they wait for up to four months before stealing money, using the time to expand their access and gather instructions for transferring funds. Carbanak is sometimes referred to as FIN7, but they are considered separate groups using the same malware.

T1003 Technique matching score: 2.7251096313139516

{0: None, 1: ('rdp#file#40', 1.0), 2: ('powershell#executable#35', 1.0), 3: None, 4: None, 5: None}

T1036 Technique matching score: 2.251773444753946

{0: ('powershell#executable#35', 1.0), 1: None, 2: None, 3: None, 4: None, 5: ('rdp#file#40', 1.0), 6: None, 7: None}

T1059 Technique matching score: 2.0904272045280985

{0: ('powershell#executable#35', 1.0), 1: ('powershell#executable#35', 1.0), 2: None, 3: None, 4: None, 5: None, 6: ('rdp#file#40', 1.0), 7: None, 8: ('rdp#file#40', 1.0), 9: None}

T1070 Technique matching score: 3.1357715430861726

{0: ('powershell#executable#35', 1.0), 1: None, 2: None, 3: None, 4: None, 5: ('rdp#file#40', 1.0), 6: None, 7: None, 8: None, 9: None}

T1071 Technique matching score: 4.961031175059952

{0: ('fin7#executable#84', 1.0), 1: ('engineering#network#14', 1.0), 2: ('engineering#network#14', 1.0), 3: None, 4: None, 5: None, 6: None}

T1083 Technique matching score: 4.251992642550583

{0: ('powershell#executable#35', 1.0), 1: ('rdp#file#40', 1.0), 2: None, 3: None, 4: None, 5: None, 6: None, 7: None, 8: None}

T1105 Technique matching score: 2.8769950051294124

{0: None, 1: ('rdp#file#40', 1.0), 2: None, 3: None, 4: None, 5: None, 6: ('powershell#executable#35', 1.0), 7: None, 8: None, 9: ('powershell#executable#35', 1.0), 10: None}

T1140 Technique matching score: 2.0156778228532795

{0: ('powershell#executable#35', 1.0), 1: None, 2: None, 3: None, 4: ('rdp#file#40', 1.0), 5: None, 6: ('powershell#executable#35', 1.0), 7: None, 8: None, 9: None, 10: None}

T1204 Technique matching score: 2.236803616540354

{0: None, 1: None, 2: ('powershell#executable#35', 1.0), 3: None, 4: None, 5: None, 6: ('rdp#file#40', 1.0), 7: None}

T1555 Technique matching score: 2.280326729231839

{0: None, 1: ('rdp#file#40', 1.0), 2: ('powershell#executable#35', 1.0), 3: None, 4: None, 5: None, 6: None, 7: None, 8: None, 9: None}

T1571 Technique matching score: 2.25

{0: ('powershell#executable#35', 1.0), 1: None, 2: ('rdp#file#40', 1.0), 3: None}

T1573 Technique matching score: 2.6245617110799437

{0: ('fin7#executable#84', 1.0), 1: ('engineering#network#14', 1.0), 2: None, 3: None, 4: None, 5: None, 6: None, 7: None}

**FIN6:**

FIN6 has been known to attain initial access to target organizations by using legitimate but compromised credentials coupled with legitimate remote access applications, and spearphishing. Most recently, FIN6 may have been purchasing access to environments previously compromised with TrickBot.[8](https://securityintelligence.com/posts/itg08-aka-fin6-partners-with-trickbot-gang-uses-anchor-framework/) Once inside the target organization, FIN6 uses a variety of open and closed-source red team tools, custom scripts, and commodity malware in support of tactical objectives.

FIN6’s tactical objectives are to identify systems for staging, reconnoiter active directory environments, escalate privileges (often via credential access), and identify systems that align with operational objectives.[5](https://exchange.xforce.ibmcloud.com/threat-group/f8409554b71a79792ff099081bc5ac24) More\_eggs , a lightweight JScript implant has been used during the initial stages of compromise to conduct host enumeration, establish command and control (C2), and to download and execute additional tools. FIN6 frequently uses Metasploit or Cobalt Strike for their primary post-exploitation C2 framework, though sometimes employing a degree of customization to increase difficulty in detection. To that end, FIN6 has used code-signing certificates to evade defenses.

Run keys and scheduled tasks have been used for adversary persistence. FIN6 tends to use tools that are indicative of routine administrative tasks. For instance, FIN6 has moved laterally using valid accounts coupled with Remote Desktop Protocol (RDP), various implementations of PsExec, PowerShell, and Windows Management Instrumentation (WMI). The group will dump credentials as they move through an environment but have also exfiltrated copies of the Active Directory (AD) database file NTDS.dit utilizing the Metasploit NTDSGRAB module. FIN6 has exfiltrated this reconnaissance data to servers it controls using SSH. These actions are intended to enable FIN6’s operational objective of monetizing compromised environments.

Depending on the target, FIN6 may identify Point of Sale (POS) systems and use their access to deploy POS malware such as TRINITY. This malware will search process memory, looking for payment card data to harvest. FIN6 will then obfuscate collected data and move it to other compromised systems to be compressed and staged for exfiltration. FIN6 has also been known to exploit public-facing applications and insert malicious code into the checkout pages of compromised sites to steal payment card information.

In more recent campaigns, FIN6 has used its access to deploy ransomware. FIN6 may stage ransomware and automated deployment scripts on victim servers; these scripts may call utilities like PsExec to deploy ransomware such as LockerGoga to as many machines as possible at the same time. FIN6 may try to acquire Domain Administrator credentials to achieve maximum success with PsExec deployment or so they can use Group Policy Modification to distribute the ransomware via AD group policies.

*LLaMa 2 (no fine-tuning):*

1. Legitimate but compromised credentials: FIN6 has been known to obtain initial access to target organizations by using legitimate but compromised credentials, likely obtained through phishing attacks or other means.
2. Spearphishing: FIN6 may use spearphishing attacks to gain access to target organizations by sending tailored emails or messages to specific individuals within the organization.
3. Remote access applications: FIN6 may use legitimate remote access applications, such as Remote Desktop Protocol (RDP), to gain access to target organizations' networks.
4. Open and closed-source red team tools: FIN6 may use a variety of open and closed-source red team tools, custom scripts, and commodity malware to support their tactical objectives once inside the target organization.
5. Metasploit or Cobalt Strike: FIN6 frequently uses Metasploit or Cobalt Strike for their primary post-exploitation C2 framework, although they may also employ customization to increase difficulty in detection.
6. Code-signing certificates: FIN6 has been known to use code-signing certificates to evade defenses and make their tools more difficult to detect.
7. Run keys and scheduled tasks: FIN6 may use run keys and scheduled tasks for adversary persistence, which allows them to maintain access to the target organization's network even after their initial access has been gained.
8. Valid accounts: FIN6 may use valid accounts, such as those with legitimate remote desktop protocol (RDP) access, to move laterally within the target organization's network.
9. Public-facing applications: FIN6 may exploit public-facing applications and insert malicious code into the checkout pages of compromised sites to steal payment card information.
10. Ransomware: In more recent campaigns, FIN6 has used its access to deploy ransomware, such as LockerGoga, to as many machines as possible at the same time. They may also use Group Policy Modification to distribute the ransomware via AD group policies.

*LLaMa2-13GB:*

1. Initial Access: FIN6 uses legitimate but compromised credentials and spearphishing to gain initial access to target organizations. This technique is covered in the MITRE ATT&CK framework under TA0001 - Initial Access.
2. Credential Access: FIN6 uses tools like Metasploit and Cobalt Strike to dump credentials and escalate privileges. This technique is covered in the MITRE ATT&CK framework under TA0004 - Credential Access.
3. Lateral Movement: FIN6 uses tools like RDP, PsExec, PowerShell, and WMI to move laterally within the compromised network. This technique is covered in the MITRE ATT&CK framework under TA0008 - Lateral Movement.
4. Discovery: FIN6 uses tools like Metasploit's NTDSGRAB module to gather information about the compromised network, including the Active Directory database. This technique is covered in the MITRE ATT&CK framework under TA0003 - Discovery.
5. Command and Control: FIN6 uses custom scripts and commodity malware to establish command and control (C2) channels with the compromised systems. This technique is covered in the MITRE ATT&CK framework under TA0009 - Command and Control.
6. Exfiltration: FIN6 exfiltrates data from the compromised network to servers it controls using SSH. This technique is covered in the MITRE ATT&CK framework under TA0010 - Exfiltration.
7. Obfuscation: FIN6 obfuscates the collected data to make it more difficult to detect. This technique is covered in the MITRE ATT&CK framework under TA0011 - Obfuscation.
8. Ransomware: FIN6 deploys ransomware, such as LockerGoga, to extort money from the victims. This technique is covered in the MITRE ATT&CK framework under TA0012 - Ransomware.

*LLaMa2-70GB:*

1. Initial Access:  
   \* Legitimate but compromised credentials (TA0004 - Privileged Accounts: Compromised Credentials)  
   \* Spearphishing (TA0006 - Phishing: Spearphishing)  
   \* Purchasing access to environments previously compromised with TrickBot (TA0009 - Privilege Escalation: Bootkit)
2. Discovery and Reconnaissance:  
   \* Host enumeration (TA0018 - Network Reconnaissance: Host Enumeration)  
   \* Active Directory reconnaissance (TA0017 - Network Reconnaissance: Active Directory)  
   \* Dumping credentials (TA0007 - Credential Access: Dumping Credentials)  
   \* Exfiltrating copies of the Active Directory database file NTDS.dit (TA0015 - Data Discovery: File and Directory Discovery)
3. Lateral Movement:  
   \* Use of valid accounts with Remote Desktop Protocol (RDP) (TA0011 - Lateral Movement: Remote Services)  
   \* Use of PsExec (TA0011 - Lateral Movement: PsExec)  
   \* Use of PowerShell (TA0011 - Lateral Movement: PowerShell)  
   \* Use of Windows Management Instrumentation (WMI) (TA0011 - Lateral Movement: WMI)
4. Command and Control:  
   \* Use of More\_eggs, a lightweight JScript implant (TA0013 - Command and Control: Implant)  
   \* Use of Metasploit or Cobalt Strike for post-exploitation C2 (TA0013 - Command and Control: Metasploit, TA0013 - Command and Control: Cobalt Strike)  
   \* Customization of tools to increase difficulty in detection (TA0013 - Command and Control: Obfuscation)
5. Credential Access:  
   \* Escalation of privileges via credential access (TA0004 - Privileged Accounts: Escalate Privileges)  
   \* Use of code-signing certificates to evade defenses (TA0014 - Defense Evasion: Code Signing)
6. Persistence:  
   \* Use of run keys and scheduled tasks (TA0016 - Persistence: Run Keys and Scheduled Tasks)
7. Exfiltration:  
   \* Exfiltration of reconnaissance data to servers controlled by FIN6 using SSH (TA0015 - Data Discovery: Exfiltration)
8. Ransomware:  
   \* Deployment of ransomware (TA0010 - Ransomware)  
   \* Use of PsExec to deploy ransomware to multiple machines at once (TA0011 - Lateral Movement: PsExec)  
   \* Use of Group Policy Modification to distribute ransomware via AD group policies (TA0017 - Network Reconnaissance: Group Policy Modification)

*Falcon-40B:*

* T1568: Data Encrypted for Impact
* T1027: System Network Configuration Discovery
* T1030: System Network Connections Discovery
* T1048: System Information Discovery
* T1059: Command and Scripting Interpreter Discovery
* T1060: Process Discovery
* T1064: Scheduled Task Discovery
* T1070: System Service Discovery
* T1071: System Service Execution
* T1072: System Service Deletion
* T1082: User Execution via Binary
* T1083: User Execution via Script
* T1084: User Execution via Elevated Token
* T1085: User Execution via Scheduled Task
* T1086: User Execution via Job
* T1087: User Execution via Shortcut
* T1088: User Execution via Windows Management Instrumentation
* T1089: User Execution via Windows Management Instrumentation Command-Line
* T1090: User Execution via Windows Management Instrumentation EventConsumer
* T1091: User Execution via Windows Management Instrumentation EventFilter
* T1092: User Execution via Windows Management Instrumentation EventConsumer
* T1093: User Execution via Windows Management Instrumentation EventFilter
* T1094: User Execution via Windows Management Instrumentation EventConsumer
* T1095: User Execution via Windows Management Instrumentation EventFilter
* T1096: User Execution via Windows Management Instrumentation EventConsumer
* T1097: User Execution via Windows Management Instrumentation EventFilter
* T1098: User Execution via Windows Management Instrumentation EventConsumer
* T1099: User Execution via Windows Management Instrumentation EventFilter
* T1100: User Execution via Windows Management Instrumentation EventConsumer
* T1101: User Execution via Windows Management Instrumentation EventFilter
* T1102: User Execution via Windows Management Instrumentation EventConsumer
* T1103: User Execution via Windows Management Instrumentation EventFilter
* T1104: User Execution via Windows Management Instrumentation EventConsumer
* T1105: User Execution via Windows Management Instrumentation EventFilter
* T1106: User Execution via Windows Management Instrumentation EventConsumer
* T1107: User Execution via Windows Management Instrumentation EventFilter
* T1108: User Execution via Windows Management Instrumentation EventConsumer
* T1109: User Execution via Windows Management Instrumentation EventFilter
* T1110: User Execution via Windows Management Instrumentation EventConsumer
* T1111: User Execution via Windows Management Instrumentation EventFilter
* T1112: User Execution via Windows Management Instrumentation EventConsumer
* T1113: User Execution via Windows Management Instrumentation EventFilter
* T1114: User Execution via Windows Management Instrumentation EventConsumer
* T1115: User Execution via Windows Management Instrumentation EventFilter
* T1116: User Execution via Windows Management Instrumentation EventConsumer
* T1117: User Execution via Windows Management Instrumentation EventFilter
* T1118: User Execution via Windows Management Instrumentation EventConsumer
* T1119: User Execution via Windows Management Instrumentation EventFilter
* T1120: User Execution via Windows Management Instrumentation EventConsumer
* T1121: User Execution via Windows Management Instrumentation EventFilter
* T1122: User Execution via Windows Management Instrumentation EventConsumer
* T1123: User Execution via Windows Management Instrumentation EventFilter
* T1124: User Execution via Windows Management Instrumentation EventConsumer
* T1125: User Execution via Windows Management Instrumentation EventFilter

*Falcon-7B:* Cannot answer about techniques.

*GPT-3.5:*

1. Initial Access:
   * Technique: Spearphishing
   * Technique: Compromised Credentials
2. Execution:
   * Technique: Custom Scripts
   * Technique: Commodity Malware
3. Persistence:
   * Technique: Run Keys / Startup Folder
   * Technique: Scheduled Task
4. Privilege Escalation:
   * Technique: Credential Access
5. Discovery:
   * Technique: Host Enumeration
   * Technique: Active Directory Reconnaissance
6. Lateral Movement:
   * Technique: Remote Desktop Protocol (RDP)
   * Technique: PsExec
   * Technique: PowerShell
   * Technique: Windows Management Instrumentation (WMI)
7. Collection:
   * Technique: Dumping Credentials
   * Technique: Exfiltration of Active Directory Database (NTDS.dit)
8. Command and Control:
   * Technique: Command and Control (C2) Framework (Metasploit or Cobalt Strike)
   * Technique: Code Signing Certificates
9. Impact:
   * Technique: Point of Sale (POS) Malware Deployment
   * Technique: Exploitation of Public-Facing Applications
   * Technique: Ransomware Deployment
   * Technique: Group Policy Modification

*AttackG:*

T1071 Technique matching score: 3.3541167066346924

{0: ('more\_eggs#executable#109', 1.0), 1: ('c2#network#158', 1.0), 2: ('c2#network#158', 1.0), 3: None, 4: ('credentials#file#253', 1.0), 5: None, 6: None}

T1082 Technique matching score: 2.0218238311304004

{0: None, 1: ('more\_eggs#executable#109', 1.0), 2: None, 3: ('systems#system#103', 1.0), 4: ('credentials#file#253', 1.0), 5: ('c2#network#158', 1.0), 6: None, 7: None, 8: None, 9: None}

T1573 Technique matching score: 2.607497662459093

{0: ('more\_eggs#executable#109', 1.0), 1: ('c2#network#158', 1.0), 2: None, 3: ('credentials#file#253', 1.0), 4: None, 5: None, 6: None, 7: None}

*Summarized version with AttackG:*

FIN6 is a highly sophisticated cybercrime group that uses legitimate means to gain access to target organizations, including using compromised credentials and remote access applications. Once inside, they use a variety of tools and techniques to identify systems for staging, reconnoiter active directories, escalate privileges, and exfiltrate sensitive data. They have been known to deploy POS malware, ransomware, and other types of malicious software to monetize compromised environments. FIN6 is skilled at evading detection by using code-signing certificates and routine administrative tasks to maintain persistence. Their tactics are constantly evolving, making them a significant threat to organizations across multiple sectors.

T1003 Technique matching score: 2.1617670943641385

{0: None, 1: ('credentials#file#23', 1.0), 2: ('fin6#executable#1', 1.0), 3: ('systems#system#42', 1.0), 4: ('means#network#11', 1.0), 5: None}

T1021 Technique matching score: 2.1994139194139195

{0: ('fin6#executable#1', 1.0), 1: ('credentials#file#23', 1.0), 2: ('systems#system#42', 1.0), 3: None, 4: None, 5: None, 6: ('means#network#11', 1.0)}

T1036 Technique matching score: 2.2538347260909934

{0: ('fin6#executable#1', 1.0), 1: None, 2: None, 3: ('systems#system#42', 1.0), 4: None, 5: ('credentials#file#23', 1.0), 6: None, 7: ('means#network#11', 1.0)}

T1041 Technique matching score: 2.2635185185185187

{0: ('fin6#executable#1', 1.0), 1: ('means#network#11', 1.0), 2: None, 3: ('credentials#file#23', 1.0), 4: None, 5: ('credentials#file#23', 1.0), 6: ('systems#system#42', 1.0)}

T1059 Technique matching score: 2.6213220430349042

{0: ('fin6#executable#1', 1.0), 1: ('fin6#executable#1', 1.0), 2: ('systems#system#42', 1.0), 3: None, 4: ('systems#system#42', 1.0), 5: None, 6: ('credentials#file#23', 1.0), 7: ('means#network#11', 1.0), 8: ('credentials#file#23', 1.0), 9: None}

T1070 Technique matching score: 2.4105949995228553

{0: ('fin6#executable#1', 1.0), 1: ('systems#system#42', 1.0), 2: None, 3: ('means#network#11', 1.0), 4: None, 5: ('credentials#file#23', 1.0), 6: None, 7: None, 8: None, 9: None}

T1071 Technique matching score: 9.865227817745804

{0: ('fin6#executable#1', 1.0), 1: ('means#network#11', 1.0), 2: ('means#network#11', 1.0), 3: None, 4: ('credentials#file#23', 1.0), 5: None, 6: None}

T1082 Technique matching score: 2.6670941014006706

{0: None, 1: ('fin6#executable#1', 1.0), 2: None, 3: ('systems#system#42', 1.0), 4: ('credentials#file#23', 1.0), 5: ('means#network#11', 1.0), 6: None, 7: None, 8: None, 9: None}

T1083 Technique matching score: 3.2210683629675043

{0: ('fin6#executable#1', 1.0), 1: ('credentials#file#23', 1.0), 2: None, 3: ('means#network#11', 1.0), 4: ('systems#system#42', 1.0), 5: None, 6: ('means#network#11', 1.0), 7: None, 8: None}

T1105 Technique matching score: 2.6530078538874218

{0: None, 1: ('credentials#file#23', 1.0), 2: ('means#network#11', 1.0), 3: None, 4: None, 5: None, 6: ('fin6#executable#1', 1.0), 7: ('systems#system#42', 1.0), 8: None, 9: ('fin6#executable#1', 1.0), 10: None}

T1132 Technique matching score: 1.963965718737826

{0: ('means#network#11', 1.0), 1: None, 2: None, 3: None, 4: None, 5: ('credentials#file#23', 1.0), 6: ('fin6#executable#1', 1.0), 7: None, 8: None}

T1140 Technique matching score: 1.9216108857336038

{0: ('fin6#executable#1', 1.0), 1: None, 2: None, 3: None, 4: ('credentials#file#23', 1.0), 5: ('means#network#11', 1.0), 6: ('fin6#executable#1', 1.0), 7: None, 8: ('systems#system#42', 1.0), 9: None, 10: None}

T1204 Technique matching score: 2.5186810264592476

{0: None, 1: None, 2: ('fin6#executable#1', 1.0), 3: ('means#network#11', 1.0), 4: ('means#network#11', 1.0), 5: None, 6: ('credentials#file#23', 1.0), 7: None}

T1566 Technique matching score: 3.349690103035806

{0: None, 1: ('means#network#11', 1.0), 2: ('credentials#file#23', 1.0), 3: None, 4: ('credentials#file#23', 1.0), 5: ('fin6#executable#1', 1.0), 6: ('fin6#executable#1', 1.0), 7: None}

T1571 Technique matching score: 3.434375

{0: ('fin6#executable#1', 1.0), 1: ('means#network#11', 1.0), 2: ('credentials#file#23', 1.0), 3: None}

T1573 Technique matching score: 5.497282608695652

{0: ('fin6#executable#1', 1.0), 1: ('means#network#11', 1.0), 2: None, 3: ('credentials#file#23', 1.0), 4: None, 5: None, 6: None, 7: None}

**FIN7:**

Regarding their operational tradecraft, FIN7 is distinguished by their techincal innovation, using novel techniques and displaying characteristics of a well-rounded operation. FIN7 has been reported to employ limited use of exploits while blending publicly available and unique or altered tools. The group has leveraged hidden shortcut files (LNK files) to initiate infection and VBScript functionality launched by mshta.exe to infect the victim. This is a departure from previously established usage of weaponized Office macros and highlights the group's ability to adapt to evade detction.

FIN7 has been reported to use the Carbanak backdoor as a post-exploitation tool since as early as 2015. The group has also used creative persistence mechanisms, such as application shimming, to spawn a Carbanak backdoor and seprately to install a payment card harvesting utility. It has also been reported that the group has developed defense evasion techniques rapidly, such as we creating novel obfuscation methods that in some cases were modified on a daily basis while launching attacks targeting multiple victims. FireEye dubbed their development of a payload obfuscation style using the Windows command interpreter's native string substitution as "FINcoding."

FIN7 has also used point-of-sale malware, such as Pillowmint, to scrape track 1 and track 2 payment card data from memory.

*LLaMa 2 (no fine-tuning):*

1. Technique ID: T1059 - Limited Use of Exploits: FIN7 has been observed to use a limited number of exploits, blending publicly available and unique or altered tools.
2. Technique ID: T1083 - Hidden Shortcut Files (LNK Files): FIN7 has been reported to use LNK files to initiate infection.
3. Technique ID: T1087 - VBScript: FIN7 has been observed to use VBScript functionality launched by mshta.exe to infect the victim.
4. Technique ID: T1160 - Carbanak Backdoor: FIN7 has been reported to use the Carbanak backdoor as a post-exploitation tool since as early as 2015.
5. Technique ID: T1165 - Persistence Mechanisms: FIN7 has been observed to use creative persistence mechanisms, such as application shimming, to spawn a Carbanak backdoor and separately to install a payment card harvesting utility.
6. Technique ID: T1180 - Payload Obfuscation: FIN7 has been reported to develop and use novel obfuscation methods for their payloads, which were sometimes modified on a daily basis while launching attacks targeting multiple victims. MITRE dubbed this technique "FINcoding."
7. Technique ID: T1190 - Point-of-Sale Malware: FIN7 has been observed to use point-of-sale malware, such as Pillowmint, to scrape track 1 and track 2 payment card data from memory.

*LLaMa 2-13B:*

1. Technique: Code Obfuscation (T1490) - FIN7 uses code obfuscation to evade detection and analysis.

ID: T1490

1. Technique: Data Encoding (T1480) - FIN7 uses data encoding to conceal malicious data in network traffic.

ID: T1480

1. Technique: File and Directory Discovery (T1083) - FIN7 uses file and directory discovery to locate and access sensitive information.

ID: T1083

1. Technique: File and Execution Control (T1059) - FIN7 uses file and execution control to execute malicious files and gain control of the system.

ID: T1059

1. Technique: Command and Scripting Interpreter (T1063) - FIN7 uses command and scripting interpreters to execute malicious commands and scripts.

ID: T1063

1. Technique: PowerShell (T1059.003) - FIN7 uses PowerShell to execute malicious commands and scripts.

ID: T1059.003

1. Technique: Windows Command Shell (T1063.001) - FIN7 uses the Windows command shell to execute malicious commands and scripts.

ID: T1063.001

1. Technique: System Configuration Modification (T1082) - FIN7 modifies system configuration to maintain persistence and evade detection.

ID: T1082

1. Technique: Data Tampering (T1080) - FIN7 tampers with data to conceal malicious activity and evade detection.

ID: T1080

1. Technique: Network Protocols (T1041) - FIN7 uses network protocols to communicate with its command and control (C2) servers.

ID: T1041

1. Technique: Malware Reporting (T1087) - FIN7 uses malware reporting to send information about the compromised system to its C2 servers.

ID: T1087

1. Technique: Defense Evasion (T1083) - FIN7 uses defense evasion techniques to evade detection and analysis.

ID: T1083

1. Technique: Credential Access (T1003) - FIN7 uses credential access to steal sensitive information such as login credentials.

ID: T1003

1. Technique: Lateral Movement (T1085) - FIN7 uses lateral movement to spread laterally within the compromised network.

ID: T1085

1. Technique: Persistence (T1086) - FIN7 uses persistence techniques to maintain access to the compromised system over time.

ID: T1086

*LLaMa2-70B:*

1. TA0004 - Privilege Escalation: FIN7 has been reported to use application shimming to spawn a Carbanak backdoor, which suggests they are attempting to escalate privileges.
2. T1083 - File and Directory Discovery: FIN7 has been reported to use hidden shortcut files (LNK files) to initiate infection, which involves discovering files and directories on the victim's system.
3. T1080 - Taint Shared Content: FIN7 has been reported to use VBScript functionality launched by mshta.exe to infect the victim, which involves tainting shared content.
4. T1140 - Deobfuscate/Decode Files or Information: FIN7 has been reported to develop defense evasion techniques rapidly, including creating novel obfuscation methods that were modified on a daily basis while launching attacks targeting multiple victims. This suggests they are attempting to deobfuscate or decode files or information to evade detection.
5. T1059.003 - Command and Scripting Interpreter: Windows Command Shell: FIN7 has been reported to use the Windows command interpreter's native string substitution to develop a payload obfuscation style, which is a technique identified in the MITRE ATT&CK framework.
6. T1085 - User Account Credentials: FIN7 has been reported to use the Carbanak backdoor as a post-exploitation tool, which can be used to steal user account credentials.
7. T1046 - Network Service Scanning: FIN7 has been reported to use the Carbanak backdoor to scrape track 1 and track 2 payment card data from memory, which involves scanning network services.
8. T1086 - Data Encryption: FIN7 has been reported to use encryption to evade detection, which is a common technique used by attackers to protect their tools and communication.
9. T1030 - Malicious Software: FIN7 has been reported to use point-of-sale malware, such as Pillowmint, to scrape track 1 and track 2 payment card data from memory, which involves using malicious software.

*Falcon-40B:*

* Exploit Public-Facing Application (T1199)
* Execute Command (T1078)
* Spearphishing Link (T1192)
* Lateral Movement (T1565)
* Persistence (T1053)
* Defense Evasion (T1027)
* Obfuscation (T1028)
* Custom C2 Channel (T1079)
* Custom Backdoor (T1060)
* Point-of-Sale Malware (T1194)

*Falcon-7B:* Cannot detect techniques from MITRE ATT&CK.

*GPT-3.5:*

1. Technique: Exploitation for Client Execution
   * ID: T1203
2. Technique: Scripting
   * ID: T1064
3. Technique: Shortcut Modification
   * ID: T1023
4. Technique: User Execution
   * ID: T1204
5. Technique: Hidden Files and Directories
   * ID: T1158
6. Technique: Spearphishing Attachment
   * ID: T1193
7. Technique: Registry Run Keys / Startup Folder
   * ID: T1060
8. Technique: Obfuscated Files or Information
   * ID: T1027
9. Technique: Process Injection
   * ID: T1055
10. Technique: Application Shimming
    * ID: T1138
11. Technique: Input Capture
    * ID: T1056
12. Technique: Data from Local System
    * ID: T1005
13. Technique: Data from Network Shared Drive
    * ID: T1039
14. Technique: Remote File Copy
    * ID: T1105
15. Technique: Data Staged
    * ID: T1074
16. Technique: Data Encrypted
    * ID: T1022
17. Technique: Data Obfuscation
    * ID: T1001
18. Technique: Credential Dumping
    * ID: T1003
19. Technique: Data from Removable Media
    * ID: T1025
20. Technique: Exfiltration Over Command and Control Channel
    * ID: T1041
21. Technique: Data Compressed
    * ID: T1002
22. Technique: Data Transfer Size Limits
    * ID: T1030
23. Technique: Input Capture
    * ID: T1056
24. Technique: Data from Local System
    * ID: T1005
25. Technique: Data from Network Shared Drive
    * ID: T1039
26. Technique: Remote File Copy
    * ID: T1105
27. Technique: Data Staged
    * ID: T1074
28. Technique: Data Encrypted
    * ID: T1022
29. Technique: Data Obfuscation
    * ID: T1001
30. Technique: Credential Dumping
    * ID: T1003
31. Technique: Data from Removable Media
    * ID: T1025
32. Technique: Exfiltration Over Command and Control Channel
    * ID: T1041
33. Technique: Data Compressed
    * ID: T1002
34. Technique: Data Transfer Size Limits
    * ID: T1030

*AttackG:*

T1003 Technique matching score: 1.9351145038167938

{0: None, 1: ('pillowmint#file#223', 1.0), 2: ('fireeye#executable#186', 1.0), 3: None, 4: ('utility#network#145', 1.0), 5: None}

T1070 Technique matching score: 2.1776767821357

{0: ('fireeye#executable#186', 1.0), 1: None, 2: None, 3: ('utility#network#145', 1.0), 4: None, 5: ('pillowmint#file#223', 1.0), 6: None, 7: None, 8: None, 9: None}

T1071 Technique matching score: 2.998561151079137

{0: ('fireeye#executable#186', 1.0), 1: ('utility#network#145', 1.0), 2: ('utility#network#145', 1.0), 3: None, 4: ('pillowmint#file#223', 1.0), 5: None, 6: None}

T1083 Technique matching score: 2.761687614960147

{0: ('fireeye#executable#186', 1.0), 1: ('pillowmint#file#223', 1.0), 2: None, 3: ('utility#network#145', 1.0), 4: None, 5: None, 6: ('utility#network#145', 1.0), 7: None, 8: None}

T1105 Technique matching score: 2.092976909234624

{0: None, 1: ('pillowmint#file#223', 1.0), 2: ('utility#network#145', 1.0), 3: None, 4: None, 5: None, 6: ('fireeye#executable#186', 1.0), 7: None, 8: None, 9: ('fireeye#executable#186', 1.0), 10: None}

T1571 Technique matching score: 2.034375

{0: ('fireeye#executable#186', 1.0), 1: ('utility#network#145', 1.0), 2: ('pillowmint#file#223', 1.0), 3: None}

T1573 Technique matching score: 1.9488955119214588

{0: ('fireeye#executable#186', 1.0), 1: ('utility#network#145', 1.0), 2: None, 3: ('pillowmint#file#223', 1.0), 4: None, 5: None, 6: None, 7: None}

*Summarized version with AttackG:*

FIN7 is a highly sophisticated cybercrime group known for their technical innovation and adaptability. They use a mix of publicly available and custom tools, including LNK files and VBScript, to infect victims. They have also been observed using the Carbanak backdoor and developing their own payment card harvesting utility. FIN7's tactics are constantly evolving, with new obfuscation methods and defense evasion techniques being developed rapidly. They have also been known to use point-of-sale malware to scrape payment card data from memory.

T1070 Technique matching score: 2.153628685943315

{0: ('fincoding#executable#65', 1.0), 1: None, 2: None, 3: None, 4: None, 5: ('lnk#file#35', 1.0), 6: None, 7: None, 8: None, 9: None}

T1071 Technique matching score: 2.6345323741007194

{0: ('fincoding#executable#65', 1.0), 1: None, 2: None, 3: None, 4: ('lnk#file#35', 1.0), 5: None, 6: None}

T1083 Technique matching score: 2.725206928264868

{0: ('fincoding#executable#65', 1.0), 1: ('lnk#file#35', 1.0), 2: None, 3: None, 4: None, 5: None, 6: None, 7: None, 8: None}

T1105 Technique matching score: 1.9543145927582786

{0: None, 1: ('lnk#file#35', 1.0), 2: None, 3: None, 4: None, 5: None, 6: ('fincoding#executable#65', 1.0), 7: None, 8: None, 9: ('fincoding#executable#65', 1.0), 10: None}

**menuPass:**

menuPass actors are reported to have pursued initial access by spearphishing to achieve user execution. menuPass spearphishing attempts generally assume a pretext that would be of interest to the intended target and are reported to have featured password protected Microsoft Word documents embedded with VBA macros, an executable attachment that exploits a vulnerability, or a link that points to a payload server. Once inside the target organization, menuPass actors have used a variety of open-source, modified open-source, and custom tools to perform discovery, escalate privileges, access credentials, move laterally, and exfiltrate data.

"Operation Cloud Hopper," was a long-term persistent effort to compromise MSPs with the intent of abusing trust relationships in order to pivot into customer networks. menuPass actors are thought to have achieved initial access to MSP networks by spearphishing. From the MSP networks, menuPass actors are reported to have used legitimate but compromised local accounts coupled with legitimate remote access applications to access customer environments. From this initial point of presence, menuPass actors are reported to have used administrative tools native to the Windows environment to download an operational toolkit from an attacker controlled server. This toolkit enabled the pursuit of tactical objectives with the operational intent of exfiltrating intellectual property. This activity will serve as the basis for Scenario 1.

menuPass is also reported to have engaged in phishing campaigns, the most prolific of which were directed against Japanese institutions. Successful compromise resulted in the deployment of menuPass malware to the victim network and the establishment of command and control. menuPass malware has been categorized by the manner in which it was employed by menuPass actors and not necessarily by the malware's inherent functionality. PWC categorized menuPass malware as tactical or sustained. Tactical malware is usually deployed during delivery, or upon initial access, and is intended to perform lightweight tasks, such as discovery and execution. Sustained malware is often modular and has an enhanced set of features. Sustained malware is deployed to specific systems to facilitate a long-term point of presence. menuPass is reported to have leveraged the access facilitated by its malware to pursue operational objectives. This activity will serve as the basis for Scenario 2.

*LLaMa 2 (no fine-tuning):*

* Initial Access: Spearphishing (ID: Technique T1059) - menuPass actors are reported to have pursued initial access by spearphishing to achieve user execution.
* Discovery: Using legitimate but compromised local accounts (ID: Technique T1083) - menuPass actors are reported to have used legitimate but compromised local accounts coupled with legitimate remote access applications to access customer environments.
* Escalate Privileges: Using administrative tools native to the Windows environment (ID: Technique T1056) - menuPass actors are reported to have used administrative tools native to the Windows environment to download an operational toolkit from an attacker-controlled server.
* Credentials: Accessing credentials (ID: Technique T1078) - menuPass actors are reported to have used legitimate remote access applications to access customer environments.
* Lateral Movement: Using legitimate remote access applications (ID: Technique T1082) - menuPass actors are reported to have used legitimate remote access applications to access customer environments.
* Exfiltration: Using operational toolkit to exfiltrate data (ID: Technique T1087) - menuPass actors are reported to have used an operational toolkit from an attacker-controlled server to download and exfiltrate data.

*LLaMa2-13B:*

Scenario 1: Operation Cloud Hopper

1. Technique: Spear Phishing (T1566.001) - menuPass actors are reported to have pursued initial access by spearphishing to achieve user execution.

ID: T1566.001

1. Technique: Phishing (T1566) - menuPass actors are reported to have used phishing campaigns to trick victims into opening malicious attachments or clicking on links to malicious websites.

ID: T1566

1. Technique: Password Protected Documents (T1490) - menuPass actors are reported to have used password-protected Microsoft Word documents embedded with VBA macros to deliver malware.

ID: T1490

1. Technique: Executable Attachments (T1498) - menuPass actors are reported to have used executable attachments to exploit vulnerabilities and gain initial access.

ID: T1498

1. Technique: Links to Payload Servers (T1499) - menuPass actors are reported to have used links to payload servers to deliver malware and conduct further attacks.

ID: T1499

1. Technique: Privilege Escalation (T1059) - menuPass actors are reported to have used legitimate but compromised local accounts coupled with legitimate remote access applications to access customer environments.

ID: T1059

1. Technique: Administrative Tools (T1083) - menuPass actors are reported to have used administrative tools native to the Windows environment to download an operational toolkit from an attacker-controlled server.

ID: T1083

1. Technique: Exfiltration (T1089) - menuPass actors are reported to have used the operational toolkit to exfiltrate intellectual property.

ID: T1089

Scenario 2: Phishing Campaigns

1. Technique: Phishing (T1566) - menuPass actors are reported to have engaged in phishing campaigns, the most prolific of which were directed against Japanese institutions.

ID: T1566

1. Technique: Malware Deployment (T1086) - menuPass actors are reported to have deployed malware to the victim network and established command and control.

ID: T1086

1. Technique: Malware Management (T1087) - menuPass actors are reported to have leveraged the access facilitated by their malware to pursue operational objectives.

ID: T1087

1. Technique: Sustained Malware (T1088) - menuPass actors are reported to have used sustained malware to facilitate a long-term point of presence.

ID: T1088

1. Technique: Tactical Malware (T1089) - menuPass actors are reported to have used tactical malware to perform lightweight tasks such as discovery and execution.

ID: T1089

*LLaMa 2-70B:*

1. TA0004 - Privilege Escalation: MenuPass actors are reported to have used legitimate but compromised local accounts coupled with legitimate remote access applications to access customer environments, which suggests they are attempting to escalate privileges.
2. T1083 - File and Directory Discovery: MenuPass actors are reported to have used discovery tools to perform discovery, which involves discovering files and directories on the victim's system.
3. T1080 - Taint Shared Content: MenuPass actors are reported to have used spearphishing attempts that feature password-protected Microsoft Word documents embedded with VBA macros, which involves tainting shared content.
4. T1140 - Deobfuscate/Decode Files or Information: MenuPass actors are reported to have used custom tools to perform discovery, escalate privileges, access credentials, move laterally, and exfiltrate data, which suggests they are attempting to deobfuscate or decode files or information to evade detection.
5. T1059.003 - Command and Scripting Interpreter: Windows Command Shell: MenuPass actors are reported to have used legitimate remote access applications, which could involve using the Windows command shell to execute commands and scripts.
6. T1085 - User Account Credentials: MenuPass actors are reported to have used spearphishing attempts that feature password-protected Microsoft Word documents embedded with VBA macros, which can be used to steal user account credentials.
7. T1046 - Network Service Scanning: MenuPass actors are reported to have used legitimate remote access applications, which could involve scanning network services to identify vulnerabilities and potential entry points.
8. T1086 - Data Encryption: MenuPass actors are reported to have used custom tools to exfiltrate data, which could involve encrypting data to evade detection.
9. T1030 - Malicious Software: MenuPass actors are reported to have used malware to facilitate their operations, which involves using malicious software.
10. T1087 - Account Manipulation: MenuPass actors are reported to have used legitimate but compromised local accounts coupled with legitimate remote access applications to access customer environments, which involves manipulating accounts to maintain persistence.
11. T1130 - Internal Spearphishing: MenuPass actors are reported to have used spearphishing attempts that feature password-protected Microsoft Word documents embedded with VBA macros, which involves using internal spearphishing to target specific individuals or groups within an organization.
12. T1142 - Ingress Tool Transfer: MenuPass actors are reported to have used legitimate remote access applications, which could involve transferring tools into the victim's environment to facilitate further exploitation.

*Falcon-40B:*

* Spearphishing (T1192)
* Password Protected Microsoft Word Document (T1199)
* VBA Macros (T1204)
* Exploit Public-Facing Application (T1199)
* Executable Attachment (T1200)
* Lateral Movement (T1565)
* Credential Access (T1110)
* Privilege Escalation (T1112)
* Discovery (T1012)
* Exfiltration (T1025)
* Persistence (T1053)
* Abusing Trust Relationships (T1117)
* Remote Access (T1078)
* Administrative Tools (T1079)
* Operational Toolkit (T1079)
* Phishing Campaigns (T1194)
* Malware Delivery (T1047)
* Modular Malware (T1059)
* Point of Presence (T1065)

*Falcon-7B:* Cannot detect techniques from MITRE ATT&CK.

*GPT-3.5:*

1. Technique: Spearphishing Attachment
   * ID: T1193
2. Technique: Exploitation for Client Execution
   * ID: T1203
3. Technique: User Execution
   * ID: T1204
4. Technique: Command-Line Interface
   * ID: T1059
5. Technique: PowerShell
   * ID: T1086
6. Technique: Remote Services
   * ID: T1021
7. Technique: Valid Accounts
   * ID: T1078
8. Technique: Remote File Copy
   * ID: T1105
9. Technique: Data Staged
   * ID: T1074
10. Technique: Exfiltration Over Command and Control Channel
    * ID: T1041
11. Technique: Scheduled Task
    * ID: T1053
12. Technique: Windows Management Instrumentation
    * ID: T1047
13. Technique: File and Directory Discovery
    * ID: T1083
14. Technique: System Information Discovery
    * ID: T1082
15. Technique: Credential Dumping
    * ID: T1003
16. Technique: Lateral Movement
    * ID: T1071
17. Technique: Remote Desktop Protocol
    * ID: T1076
18. Technique: Data Encrypted
    * ID: T1022
19. Technique: Data Obfuscation
    * ID: T1001
20. Technique: Phishing
    * ID: T1566
21. Technique: Command and Scripting Interpreter
    * ID: T1059
22. Technique: Remote Services
    * ID: T1021
23. Technique: Valid Accounts
    * ID: T1078
24. Technique: Remote File Copy
    * ID: T1105
25. Technique: Data Staged
    * ID: T1074
26. Technique: Exfiltration Over Command and Control Channel
    * ID: T1041
27. Technique: Scheduled Task
    * ID: T1053
28. Technique: Windows Management Instrumentation
    * ID: T1047
29. Technique: File and Directory Discovery
    * ID: T1083
30. Technique: System Information Discovery
    * ID: T1082
31. Technique: Credential Dumping
    * ID: T1003
32. Technique: Lateral Movement
    * ID: T1071
33. Technique: Remote Desktop Protocol
    * ID: T1076
34. Technique: Data Encrypted
    * ID: T1022
35. Technique: Data Obfuscation
    * ID: T1001

*AttackG:*

T1003 Technique matching score: 3.2362351794705213

{0: None, 1: ('menupass#file#274', 1.0), 2: ('attacker#executable#212', 1.0), 3: ('tasks#system#342', 1.0), 4: ('server#network#214', 1.0), 5: None}

T1005 Technique matching score: 2.2541310541310544

{0: ('attacker#executable#212', 1.0), 1: ('menupass#file#274', 1.0), 2: None, 3: None, 4: ('tasks#system#342', 1.0), 5: ('server#network#214', 1.0), 6: None, 7: ('server#network#214', 1.0)}

T1018 Technique matching score: 1.9484788359788359

{0: None, 1: ('menupass#file#274', 1.0), 2: ('attacker#executable#212', 1.0), 3: ('tasks#system#342', 1.0), 4: None, 5: None, 6: None, 7: ('server#network#214', 1.0)}

T1021 Technique matching score: 2.5541147741147743

{0: ('attacker#executable#212', 1.0), 1: ('menupass#file#274', 1.0), 2: ('tasks#system#342', 1.0), 3: None, 4: None, 5: None, 6: ('server#network#214', 1.0)}

T1036 Technique matching score: 3.2249458372021045

{0: ('attacker#executable#212', 1.0), 1: None, 2: None, 3: ('tasks#system#342', 1.0), 4: None, 5: ('menupass#file#274', 1.0), 6: None, 7: ('server#network#214', 1.0)}

T1041 Technique matching score: 2.7218518518518517

{0: ('attacker#executable#212', 1.0), 1: ('server#network#214', 1.0), 2: None, 3: ('menupass#file#274', 1.0), 4: None, 5: ('menupass#file#274', 1.0), 6: ('tasks#system#342', 1.0)}

T1049 Technique matching score: 2.0834464043419265

{0: ('attacker#executable#212', 1.0), 1: None, 2: ('server#network#214', 1.0), 3: ('menupass#file#274', 1.0), 4: None, 5: None, 6: ('tasks#system#342', 1.0), 7: None, 8: None}

T1053 Technique matching score: 2.483569378876238

{0: ('attacker#executable#212', 1.0), 1: None, 2: ('tasks#system#342', 1.0), 3: ('server#network#214', 1.0), 4: None, 5: None, 6: None, 7: None, 8: None, 9: None, 10: ('menupass#file#274', 1.0), 11: None, 12: None}

T1059 Technique matching score: 3.2319415120614527

{0: ('attacker#executable#212', 1.0), 1: ('attacker#executable#212', 1.0), 2: ('tasks#system#342', 1.0), 3: None, 4: ('tasks#system#342', 1.0), 5: None, 6: ('menupass#file#274', 1.0), 7: ('server#network#214', 1.0), 8: ('menupass#file#274', 1.0), 9: None}

T1070 Technique matching score: 3.15067436460222

{0: ('attacker#executable#212', 1.0), 1: ('tasks#system#342', 1.0), 2: None, 3: ('server#network#214', 1.0), 4: None, 5: ('menupass#file#274', 1.0), 6: None, 7: None, 8: None, 9: None}

T1071 Technique matching score: 11.898561151079138

{0: ('attacker#executable#212', 1.0), 1: ('server#network#214', 1.0), 2: ('server#network#214', 1.0), 3: None, 4: ('menupass#file#274', 1.0), 5: None, 6: None}

T1082 Technique matching score: 4.097274281580851

{0: None, 1: ('attacker#executable#212', 1.0), 2: None, 3: ('tasks#system#342', 1.0), 4: ('menupass#file#274', 1.0), 5: ('server#network#214', 1.0), 6: None, 7: None, 8: None, 9: None}

T1083 Technique matching score: 4.221068362967505

{0: ('attacker#executable#212', 1.0), 1: ('menupass#file#274', 1.0), 2: None, 3: ('server#network#214', 1.0), 4: ('tasks#system#342', 1.0), 5: None, 6: ('server#network#214', 1.0), 7: None, 8: None}

T1105 Technique matching score: 3.243214039454432

{0: None, 1: ('menupass#file#274', 1.0), 2: ('server#network#214', 1.0), 3: None, 4: None, 5: None, 6: ('attacker#executable#212', 1.0), 7: ('tasks#system#342', 1.0), 8: None, 9: ('attacker#executable#212', 1.0), 10: None}

T1132 Technique matching score: 2.111024542267238

{0: ('server#network#214', 1.0), 1: None, 2: None, 3: None, 4: None, 5: ('menupass#file#274', 1.0), 6: ('attacker#executable#212', 1.0), 7: None, 8: None}

T1140 Technique matching score: 2.2951741041244085

{0: ('attacker#executable#212', 1.0), 1: None, 2: None, 3: None, 4: ('menupass#file#274', 1.0), 5: ('server#network#214', 1.0), 6: ('attacker#executable#212', 1.0), 7: None, 8: ('tasks#system#342', 1.0), 9: None, 10: None}

T1204 Technique matching score: 3.076652040952001

{0: None, 1: None, 2: ('attacker#executable#212', 1.0), 3: ('server#network#214', 1.0), 4: ('server#network#214', 1.0), 5: None, 6: ('menupass#file#274', 1.0), 7: None}

T1555 Technique matching score: 2.3141293013555786

{0: None, 1: ('menupass#file#274', 1.0), 2: ('attacker#executable#212', 1.0), 3: ('tasks#system#342', 1.0), 4: None, 5: None, 6: None, 7: None, 8: None, 9: None}

T1566 Technique matching score: 3.2948955824878605

{0: None, 1: ('server#network#214', 1.0), 2: ('menupass#file#274', 1.0), 3: None, 4: ('menupass#file#274', 1.0), 5: ('attacker#executable#212', 1.0), 6: ('attacker#executable#212', 1.0), 7: None}

T1571 Technique matching score: 4.034375

{0: ('attacker#executable#212', 1.0), 1: ('server#network#214', 1.0), 2: ('menupass#file#274', 1.0), 3: None}

T1573 Technique matching score: 6.577927769985975

{0: ('attacker#executable#212', 1.0), 1: ('server#network#214', 1.0), 2: None, 3: ('menupass#file#274', 1.0), 4: None, 5: None, 6: None, 7: None}

*Summarized version of AttackG:*

MenuPass actors use spearphishing to gain initial access to targets, followed by the use of legitimate local accounts and remote access apps to access customer environments. Once inside, they use native Windows administrative tools to download an operational toolkit for exfiltrating intellectual property. MenuPass also engages in phishing campaigns, with successful compromise resulting in the deployment of malware to the victim network. The malware is categorized as either tactical or sustained, depending on its purpose and functionality.

T1003 Technique matching score: 2.8287315250933895

{0: None, 1: ('tools#file#37', 1.0), 2: ('menupass#executable#0', 1.0), 3: None, 4: ('network#network#68', 1.0), 5: None}

T1005 Technique matching score: 1.907977207977208

{0: ('menupass#executable#0', 1.0), 1: ('tools#file#37', 1.0), 2: None, 3: None, 4: None, 5: ('network#network#68', 1.0), 6: None, 7: ('network#network#68', 1.0)}

T1021 Technique matching score: 2.1123076923076924

{0: ('menupass#executable#0', 1.0), 1: ('tools#file#37', 1.0), 2: None, 3: None, 4: None, 5: None, 6: ('network#network#68', 1.0)}

T1036 Technique matching score: 2.3980315691736305

{0: ('menupass#executable#0', 1.0), 1: None, 2: None, 3: None, 4: None, 5: ('tools#file#37', 1.0), 6: None, 7: ('network#network#68', 1.0)}

T1059 Technique matching score: 2.4997978527469567

{0: ('menupass#executable#0', 1.0), 1: ('menupass#executable#0', 1.0), 2: None, 3: None, 4: None, 5: None, 6: ('tools#file#37', 1.0), 7: ('network#network#68', 1.0), 8: ('tools#file#37', 1.0), 9: None}

T1070 Technique matching score: 3.189581544040462

{0: ('menupass#executable#0', 1.0), 1: None, 2: None, 3: ('network#network#68', 1.0), 4: None, 5: ('tools#file#37', 1.0), 6: None, 7: None, 8: None, 9: None}

T1071 Technique matching score: 7.48189448441247

{0: ('menupass#executable#0', 1.0), 1: ('network#network#68', 1.0), 2: ('network#network#68', 1.0), 3: None, 4: ('tools#file#37', 1.0), 5: None, 6: None}

T1083 Technique matching score: 4.359901900674433

{0: ('menupass#executable#0', 1.0), 1: ('tools#file#37', 1.0), 2: None, 3: ('network#network#68', 1.0), 4: None, 5: None, 6: ('network#network#68', 1.0), 7: None, 8: None}

T1105 Technique matching score: 3.2424614453170983

{0: None, 1: ('tools#file#37', 1.0), 2: ('network#network#68', 1.0), 3: None, 4: None, 5: None, 6: ('menupass#executable#0', 1.0), 7: None, 8: None, 9: ('menupass#executable#0', 1.0), 10: None}

T1140 Technique matching score: 2.1675963488843815

{0: ('menupass#executable#0', 1.0), 1: None, 2: None, 3: None, 4: ('tools#file#37', 1.0), 5: ('network#network#68', 1.0), 6: ('menupass#executable#0', 1.0), 7: None, 8: None, 9: None, 10: None}

T1204 Technique matching score: 2.6925940699375084

{0: None, 1: None, 2: ('menupass#executable#0', 1.0), 3: ('network#network#68', 1.0), 4: ('network#network#68', 1.0), 5: None, 6: ('tools#file#37', 1.0), 7: None}

T1555 Technique matching score: 2.280326729231839

{0: None, 1: ('tools#file#37', 1.0), 2: ('menupass#executable#0', 1.0), 3: None, 4: None, 5: None, 6: None, 7: None, 8: None, 9: None}

T1566 Technique matching score: 2.041470924953614

{0: None, 1: ('network#network#68', 1.0), 2: ('tools#file#37', 1.0), 3: None, 4: ('tools#file#37', 1.0), 5: ('menupass#executable#0', 1.0), 6: ('menupass#executable#0', 1.0), 7: None}

T1571 Technique matching score: 3.184375

{0: ('menupass#executable#0', 1.0), 1: ('network#network#68', 1.0), 2: ('tools#file#37', 1.0), 3: None}

T1573 Technique matching score: 3.91663744740533

{0: ('menupass#executable#0', 1.0), 1: ('network#network#68', 1.0), 2: None, 3: ('tools#file#37', 1.0), 4: None, 5: None, 6: None, 7: None}

**oilRig:**

 OilRig’s tradecraft is notable for their commitment to stealth and persistence in the pursuit of their mission objective. OilRig has demonstrated adeptness in a broad range of attack vectors and a willingness to deviate from their existing arsenal to use novel techniques to accomplish their objectives. OilRig predominantly leverages social engineering as an initial attack vector but has also exploited patched vulnerabilities. Following the 2019 leak of OilRig’s tools and victim data, the group actively evolved their payload arsenal and retooling to avoid detection, creating multiple different malware variants with the same purpose as always: to gain an initial foothold on targeted devices.

OilRig is reported to have attained initial access via phishing, and credential abuse. After achieving an initial foothold, OilRig actors are reported to use credential dumping tools, such as Mimikatz, to gather legitimate account credentials then move laterally to other systems on the network. OilRig is also known for installing webshells to transfer tools and maintain persistent access to the network.

1. Initial Access:

* Technique: Phishing (T1089)  
  ID: ATT&CK-1089

1. Credential Access:

* Technique: Credential Abuse (T1059)  
  ID: ATT&CK-1059

1. Credential Dumping:

* Technique: Credential Dumping (T1087)  
  ID: ATT&CK-1087

1. Lateral Movement:

* Technique: Web Shell (T1083)  
  ID: ATT&CK-1083

1. Persistence:

* Technique: Installation of Web Shell (T1083)  
  ID: ATT&CK-1083

1. Command and Control:

* Technique: Transferring Tools (T1081)  
  ID: ATT&CK-1081

1. Avoidance of Detection:

* Technique: Evolving Payload Arsenal (T1085)  
  ID: ATT&CK-1085

1. Avoidance of Detection:

* Technique: Avoiding Detection (T1086)  
  ID: ATT&CK-1086

*LLaMa2-13B:*

* TA00-100: Phishing
* T1059.003: Credential Abuse
* T1083: Credential Dumping
* T1490: Web Shell
* T1140: Lateral Movement
* T1086: Persistence
* T1087: Defense Evasion

*LLaMA2-70B:*

1. Initial Access:  
   \* Phishing (MITRE ATT&CK ID: TA0004)  
   \* Credential Abuse (MITRE ATT&CK ID: TA0006)
2. Lateral Movement:  
   \* Credential Dumping (MITRE ATT&CK ID: TA0007)  
   \* Webshell (MITRE ATT&CK ID: TA0010)
3. Persistence:  
   \* Webshell (MITRE ATT&CK ID: TA0010)
4. Defense Evasion:  
   \* OilRig has demonstrated a willingness to deviate from their existing arsenal to use novel techniques to accomplish their objectives, which can be seen as a form of defense evasion.
5. Credential Access:  
   \* Credential Dumping (MITRE ATT&CK ID: TA0007)
6. Discovery:  
   \* OilRig actors are reported to use credential dumping tools, such as Mimikatz, to gather legitimate account credentials, which can be used for discovery.
7. Command and Scripting Interpreter:  
   \* OilRig is known for installing webshells to transfer tools and maintain persistent access to the network, which can be used as a command and scripting interpreter.
8. File and Directory Discovery:  
   \* OilRig actors are reported to use credential dumping tools, such as Mimikatz, to gather legitimate account credentials, which can be used for file and directory discovery.
9. Data Encoding:  
   \* OilRig is known for using encryption to evade detection, which can be seen as a form of data encoding.

*Falcon-40B:*

* Initial Access (T1219) - OilRig is reported to have attained initial access via phishing and credential abuse.
* Execution (T1035) - OilRig actors are reported to use credential dumping tools, such as Mimikatz, to gather legitimate account credentials.
* Defense Evasion (T1062) - OilRig is known for installing webshells to transfer tools and maintain persistent access to the network, which could be considered defense evasion.
* Social Engineering (T1566) - OilRig predominantly leverages social engineering as an initial attack vector.
* Exploitation of Patched Vulnerabilities (T1190) - OilRig has also exploited patched vulnerabilities.
* Lateral Movement (T1078) - OilRig actors are reported to use credential dumping tools, such as Mimikatz, to gather legitimate account credentials and move laterally to other systems on the network.
* Web Shells (T1079) - OilRig is also known for installing webshells to transfer tools and maintain persistent access to the network.

*Falcon-7B:* Cannot detect techniques from MITRE ATT&CK.

*GPT-3.5:*

1. Initial Access:
   * Phishing: OilRig is reported to have attained initial access via phishing.
2. Execution:
   * Credential Dumping: OilRig actors are reported to use credential dumping tools, such as Mimikatz, to gather legitimate account credentials.
3. Lateral Movement:
   * Credential Access: After achieving an initial foothold, OilRig actors move laterally to other systems on the network using the gathered credentials.
   * Web Shell: OilRig is known for installing webshells to transfer tools and maintain persistent access to the network.

*AttackG:*

T1003 Technique matching score: 2.1805614206052732

{0: None, 1: ('stealth#file#10', 1.0), 2: ('malware#executable#95', 1.0), 3: ('systems#system#159', 1.0), 4: ('network#network#180', 1.0), 5: None}

T1036 Technique matching score: 2.13850139275766

{0: ('malware#executable#95', 1.0), 1: None, 2: None, 3: ('systems#system#159', 1.0), 4: None, 5: ('stealth#file#10', 1.0), 6: None, 7: ('network#network#180', 1.0)}

T1059 Technique matching score: 2.205982809996556

{0: ('malware#executable#95', 1.0), 1: ('malware#executable#95', 1.0), 2: ('systems#system#159', 1.0), 3: None, 4: ('systems#system#159', 1.0), 5: None, 6: ('stealth#file#10', 1.0), 7: ('network#network#180', 1.0), 8: ('stealth#file#10', 1.0), 9: None}

T1070 Technique matching score: 2.2453172217450774

{0: ('malware#executable#95', 1.0), 1: ('systems#system#159', 1.0), 2: None, 3: ('network#network#180', 1.0), 4: None, 5: ('stealth#file#10', 1.0), 6: None, 7: None, 8: None, 9: None}

T1071 Technique matching score: 6.190227817745803

{0: ('malware#executable#95', 1.0), 1: ('network#network#180', 1.0), 2: ('network#network#180', 1.0), 3: None, 4: ('stealth#file#10', 1.0), 5: None, 6: None}

T1082 Technique matching score: 2.4148418491484183

{0: None, 1: ('malware#executable#95', 1.0), 2: None, 3: ('systems#system#159', 1.0), 4: ('stealth#file#10', 1.0), 5: ('network#network#180', 1.0), 6: None, 7: None, 8: None, 9: None}

T1083 Technique matching score: 2.859163601062743

{0: ('malware#executable#95', 1.0), 1: ('stealth#file#10', 1.0), 2: None, 3: ('network#network#180', 1.0), 4: ('systems#system#159', 1.0), 5: None, 6: ('network#network#180', 1.0), 7: None, 8: None}

T1105 Technique matching score: 2.3378875789733327

{0: None, 1: ('stealth#file#10', 1.0), 2: ('network#network#180', 1.0), 3: None, 4: None, 5: None, 6: ('malware#executable#95', 1.0), 7: ('systems#system#159', 1.0), 8: None, 9: ('malware#executable#95', 1.0), 10: None}

T1204 Technique matching score: 2.050081992642822

{0: None, 1: None, 2: ('malware#executable#95', 1.0), 3: ('network#network#180', 1.0), 4: ('network#network#180', 1.0), 5: None, 6: ('stealth#file#10', 1.0), 7: None}

T1571 Technique matching score: 2.5510416666666664

{0: ('malware#executable#95', 1.0), 1: ('network#network#180', 1.0), 2: ('stealth#file#10', 1.0), 3: None}

T1573 Technique matching score: 3.639755726975222

{0: ('malware#executable#95', 1.0), 1: ('network#network#180', 1.0), 2: None, 3: ('stealth#file#10', 1.0), 4: None, 5: None, 6: None, 7: None}

*Summarized version for AttackG:*

OilRig is a highly skilled and adaptive threat actor known for their stealth and persistence in achieving their objectives. They primarily use social engineering as an initial attack vector, but also exploit patched vulnerabilities. After gaining an initial foothold, OilRig actors use credential dumping tools like Mimikatz to gather legitimate account credentials and move laterally across the network. They also install webshells for persistent access and to transfer additional tools. Despite being exposed in 2019, OilRig continues to evolve and adapt their tactics to evade detection.

T1003 Technique matching score: 2.0521357804125384

{0: None, 1: ('stealth#file#12', 1.0), 2: ('oilrig#executable#0', 1.0), 3: None, 4: ('engineering#network#25', 1.0), 5: None}

T1059 Technique matching score: 2.136965994339877

{0: ('oilrig#executable#0', 1.0), 1: ('oilrig#executable#0', 1.0), 2: None, 3: None, 4: None, 5: None, 6: ('stealth#file#12', 1.0), 7: ('engineering#network#25', 1.0), 8: ('stealth#file#12', 1.0), 9: None}

T1070 Technique matching score: 2.2252958297547476

{0: ('oilrig#executable#0', 1.0), 1: None, 2: None, 3: ('engineering#network#25', 1.0), 4: None, 5: ('stealth#file#12', 1.0), 6: None, 7: None, 8: None, 9: None}

T1071 Technique matching score: 7.048561151079136

{0: ('oilrig#executable#0', 1.0), 1: ('engineering#network#25', 1.0), 2: ('engineering#network#25', 1.0), 3: None, 4: ('stealth#file#12', 1.0), 5: None, 6: None}

T1083 Technique matching score: 2.895616186388718

{0: ('oilrig#executable#0', 1.0), 1: ('stealth#file#12', 1.0), 2: None, 3: ('engineering#network#25', 1.0), 4: None, 5: None, 6: ('engineering#network#25', 1.0), 7: None, 8: None}

T1105 Technique matching score: 2.5156573216057585

{0: None, 1: ('stealth#file#12', 1.0), 2: ('engineering#network#25', 1.0), 3: None, 4: None, 5: None, 6: ('oilrig#executable#0', 1.0), 7: None, 8: None, 9: ('oilrig#executable#0', 1.0), 10: None}

T1204 Technique matching score: 2.1346230554447545

{0: None, 1: None, 2: ('oilrig#executable#0', 1.0), 3: ('engineering#network#25', 1.0), 4: ('engineering#network#25', 1.0), 5: None, 6: ('stealth#file#12', 1.0), 7: None}

T1566 Technique matching score: 1.9387311989262168

{0: None, 1: ('engineering#network#25', 1.0), 2: ('stealth#file#12', 1.0), 3: None, 4: ('stealth#file#12', 1.0), 5: ('oilrig#executable#0', 1.0), 6: ('oilrig#executable#0', 1.0), 7: None}

T1571 Technique matching score: 2.734375

{0: ('oilrig#executable#0', 1.0), 1: ('engineering#network#25', 1.0), 2: ('stealth#file#12', 1.0), 3: None}

T1573 Technique matching score: 3.7230890603085554

{0: ('oilrig#executable#0', 1.0), 1: ('engineering#network#25', 1.0), 2: None, 3: ('stealth#file#12', 1.0), 4: None, 5: None, 6: None, 7: None}