

## C RTA Unique Techniques

Table 11 and Table 12 provide a list of the unique TTPs extracted from the company and CISA reports, respectively.

Table 11: RTA unique techniques obtained from the company reports. Format: *Tactic: Technique – Sub-technique (if exists)*;

RTA	#	Unique Techniques
<b>Blackcat</b>	2	Defense Evasion: Hide Artifacts – Hidden Files and Directories; Discovery: Domain Trust Discovery
<b>Lockbit</b>	3	Impact: Account Access Removal; Lateral Movement: Use Alternate Authentication Material – Pass the Hash; Discovery: Account Discovery – Local Account
<b>Carver Phobos</b>	15	Persistence: Boot or Logon Autostart Execution – Shortcut Modification; Persistence: Boot or Logon Autostart Execution – Kernel Modules and Extensions; Persistence: Boot or Logon Autostart Execution – Re-opened Applications; Persistence: Boot or Logon Autostart Execution – Winlogon Helper DLL; Persistence: Boot or Logon Autostart Execution – Security Support Provider; Persistence: Boot or Logon Autostart Execution – Registry Run Keys / Startup Folder; Persistence: Boot or Logon Autostart Execution – LSASS Driver; Persistence: Boot or Logon Autostart Execution – Print Processors; Persistence: Boot or Logon Autostart Execution – Active Setup; Persistence: Boot or Logon Autostart Execution – Login Items; Persistence: Boot or Logon Autostart Execution – XDG Autostart Entries; Persistence: Boot or Logon Autostart Execution – Time Providers; Persistence: Boot or Logon Autostart Execution – Authentication Package; Persistence: Boot or Logon Autostart Execution – Port Monitors; Discovery: Network Sniffing
<b>Play</b>	3	Persistence: Valid Accounts – Cloud Accounts; Persistence: Valid Accounts – Local Accounts; Persistence: Valid Accounts – Default Accounts
<b>Blackbasta</b>	12	Execution: User Execution – Malicious File; Defense Evasion: Obfuscated Files or Information – Indicator Removal from Tools; Defense Evasion: Obfuscated Files or Information – Embedded Payloads; Defense Evasion: Obfuscated Files or Information – LNK Icon Smuggling; Defense Evasion: Obfuscated Files or Information – HTML Smuggling; Defense Evasion: Obfuscated Files or Information – Command Obfuscation; Defense Evasion: Obfuscated Files or Information – Compile After Delivery; Defense Evasion: Obfuscated Files or Information – Dynamic API Resolution; Defense Evasion: Obfuscated Files or Information – Steganography; Defense Evasion: Obfuscated Files or Information – Stripped Payloads; Defense Evasion: Obfuscated Files or Information – Software Packing; Defense Evasion: Obfuscated Files or Information – Binary Padding
<b>Royal</b>	3	Persistence: Create or Modify System Process – Windows Service; Defense Evasion: Indicator Removal – Clear Windows Event Logs; Resource Development: Acquire Infrastructure – Botnet
<b>Mallox</b>	3	Persistence: Server Software Component – SQL Stored Procedures; Discovery: System Network Configuration Discovery – Wi-Fi Discovery; Discovery: System Network Configuration Discovery – Internet Connection Discovery
<b>Ransomhouse</b>	4	Persistence: Scheduled Task/Job – Scheduled Task; Persistence: Event Triggered Execution – Windows Management Instrumentation Event Subscription; Discovery: Network Share Discovery; Command and Control: Ingress Tool Transfer
<b>INC</b>	5	Credential Access: Credentials from Password Stores – Windows Credential Manager; Credential Access: Credentials from Password Stores – Keychain; Credential Access: Credentials from Password Stores – Password Managers; Credential Access: Credentials from Password Stores – Cloud Secrets Management Stores; Credential Access: Credentials from Password Stores – Securityd Memory
<b>Monti</b>	2	Privilege Escalation: Valid Accounts – Cloud Accounts; Privilege Escalation: Valid Accounts – Default Accounts
<b>Ragnar</b>	2	Defense Evasion: Use Alternate Authentication Material – Pass the Hash; Command and Control: Application Layer Protocol – File Transfer Protocols
<b>Blacksuit</b>	1	Initial Access: Drive-by Compromise
<b>8base</b>	0	
<b>Hellokittykat</b>	2	Lateral Movement: Remote Service Session Hijacking – SSH Hijacking; Resource Development: Acquire Infrastructure – Server
<b>C3RB3R</b>	1	Persistence: Server Software Component – Web Shell
<b>ESXIArgs</b>	0	

Table 12: RTA unique techniques obtained from the CISA reports. Format: *Tactic: Technique – Sub-technique (if exists)*;

RTA	#	Unique Techniques
<b>Snatch</b>	9	Execution: System Services – Service Execution; Execution: System Services – Launchctl; Reconnaissance: Gather Victim Network Information – Domain Properties; Reconnaissance: Gather Victim Network Information – DNS; Reconnaissance: Gather Victim Network Information – IP Addresses; Reconnaissance: Gather Victim Network Information – Network Trust Dependencies; Reconnaissance: Gather Victim Network Information – Network Topology; Reconnaissance: Gather Victim Network Information – Network Security Appliances; Command and Control: Application Layer Protocol – Web Protocols
<b>Lockbit</b>	0	
<b>CI0p</b>	18	Execution: Shared Modules; Execution: Exploitation for Client Execution; Persistence: Event Triggered Execution – Application Shimming; Lateral Movement: Remote Service Session Hijacking – RDP Hijacking; Defense Evasion: Process Injection – Process Doppelgänger; Defense Evasion: Process Injection – Process Hollowing; Defense Evasion: Process Injection – Proc Memory; Defense Evasion: Process Injection – ListPlanting; Defense Evasion: Process Injection – VDSO Hijacking; Defense Evasion: Process Injection – Thread Local Storage; Defense Evasion: Process Injection – Extra Window Memory Injection; Defense Evasion: Process Injection – Dynamic-link Library Injection; Defense Evasion: Process Injection – Thread Execution Hijacking; Defense Evasion: Process Injection – Ptrace System Calls; Defense Evasion: Process Injection – Asynchronous Procedure Call; Defense Evasion: Process Injection – Portable Executable Injection; Defense Evasion: Hijack Execution Flow – DLL Side-Loading; Collection: Screen Capture
<b>Phobos</b>	15	Execution: Native API; Execution: User Execution – Malicious File; Privilege Escalation: Process Injection – Asynchronous Procedure Call; Privilege Escalation: Access Token Manipulation – Token Impersonation/Theft; Privilege Escalation: Access Token Manipulation – Create Process with Token; Defense Evasion: Deobfuscate/Decode Files or Information; Defense Evasion: System Binary Proxy Execution – Mshta; Resource Development: Establish Accounts – Cloud Accounts; Resource Development: Establish Accounts – Email Accounts; Resource Development: Establish Accounts – Social Media Accounts; Reconnaissance: Active Scanning – Scanning IP Blocks; Reconnaissance: Search Open Websites/Domains – Search Engines; Reconnaissance: Search Open Websites/Domains – Code Repositories; Reconnaissance: Search Open Websites/Domains – Social Media; Command and Control: Data Obfuscation – Protocol Impersonation
<b>Royal</b>	3	Privilege Escalation: Domain Policy Modification – Group Policy Modification; Collection: Automated Collection; Command and Control: Ingress Tool Transfer
<b>Bian Lian</b>	0	
<b>Rhysida</b>	1	Defense Evasion: Hide Artifacts – Hidden Window
<b>Akira</b>	1	Persistence: Create Account – Domain Account
<b>AvosLocker</b>	0	
<b>Black Basta</b>	0	
<b>DPRK</b>	3	Initial Access: Supply Chain Compromise – Compromise Software Dependencies and Development Tools; Initial Access: Supply Chain Compromise – Compromise Software Supply Chain; Initial Access: Supply Chain Compromise – Compromise Hardware Supply Chain
<b>Play</b>	0	
<b>ALPHV</b>	4	Credential Access: Steal or Forge Kerberos Tickets – Kerberoasting; Credential Access: Steal or Forge Kerberos Tickets – Silver Ticket; Credential Access: Steal or Forge Kerberos Tickets – AS-REP Roasting; Credential Access: Steal or Forge Kerberos Tickets – Golden Ticket