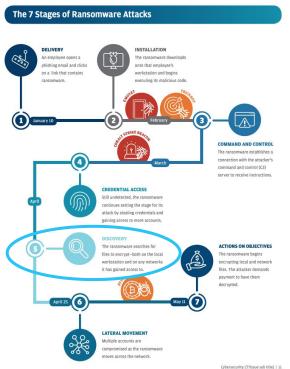
Lockheed Martin Intelligence Driven Defense® Model



JP Morgan: The Anatomy of a Ransomware Attack

5



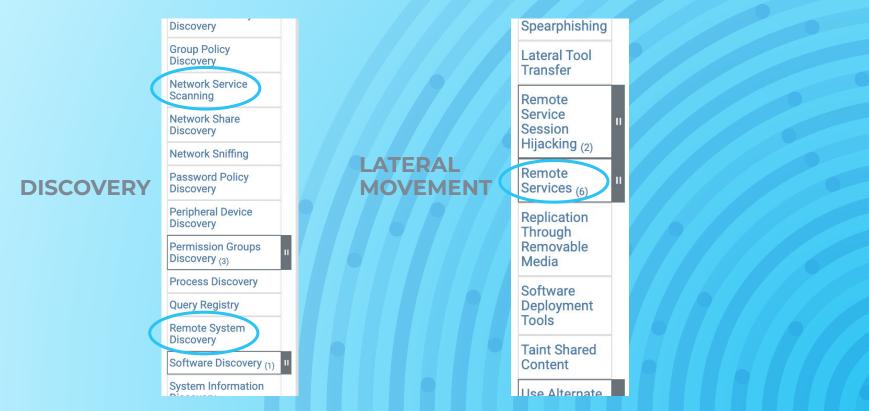
DISCOVERY

The ransomware searches for files to encrypt-both on the local workstation and on any networks it has gained access to.

MITRE ATT&CK® Techniques

efense Evasion 40 techniques	Credential Access 15 techniques	Discovery 29 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Commanc Contro 16 techniq
e Elevation rol Mechanism ₍₄₎	Adversary-in- the-Middle (2) Brute Force (4) Credentials from Password Stores (5) Exploitation for Credential Access Forced	Account Discovery (4)	Exploitation of Remote Services Internal Spearphishing Lateral Tool Transfer Remote Service Session Hijacking (2)	Adversary-in- the-Middle (2)	Application Layer Protocol (4) Communica Through Removable Media
ss Token		Application Window Discovery		Archive Collected Data (3) Audio Capture Automated Collection	
pulation ₍₅₎		Browser Bookmark Discovery			
Image on Host		Cloud Infrastructure Discovery			
fuscate/Decode					Data Encoding (2)
or Information		Cloud Service Dashboard		Browser Session Hijacking	Data
by Container		Cloud Service Discovery			Obfuscation
t Volume Access	Authentication		Remote II		Dynamic

MITRE ATT&CK® Techniques



MITRE ATT&CK® Data Sources

DS0004	Maiware Repository	Information optained (via snared or submitted samples) regarding malicious software (droppers, backdoors, etc.) used by adversaries
DS0011	Module	Executable files consisting of one or more shared classes and interfaces, such as portable executable (PE) format binaries/dynamic link libraries (DLL), executable and linkable format (ELF) binaries/shared libraries, and Mach-O format binaries/shared libraries
DS0023	Named Pipe	Mechanisms that allow inter-process communication locally or over the network. A named pipe is usually found as a file and processes attach to it
DS0033	Network Share	A storage resource (typically a folder or drive) made available from one host to others using network protocols, such as Server Message Block (SMB) or Network File System (NFS)
DS0029	Network Traffic	Data transmitted across a network (ex: Web, DNS, Mail, File, etc.), that is either summarized (ex: Netflow) and/or captured as raw data in an analyzable format (ex: PCAP)
DS0021	Persona	A malicious online profile representing a user commonly used by adversaries to social engineer or otherwise target victims
DS0014	Pod	A single unit of shared resources within a cluster, comprised of one or more containers