Attack Playbook 2

[{  
 "type": "playbook",  
 "spec\_version": "cacao-2.0",  
 "id": "playbook--fefb9f12-d308-461c-8aa7-a5d6279ab468",  
 "name": "LockyBart ransomware",  
 "description": "This playbook captures the sequence of steps of how encrypts files to obtain a ransom using the LockyBart ransomware.",  
 "playbook\_types": ["attack"],  
 "playbook\_activities": ["step-sequence"],  
 "created\_by": "identity--c59f3ff7-2f24-5bd4-a0ed-2fd36ec04b06",  
 "created": "2023-05-01T12:08:00.000Z",  
 "modified": "2023-05-01T12:08:00.000Z",  
 "labels": [  
 "ransonware",  
 "LockyBart"  
 ],  
 "external\_references": [{  
 "name": "Locky Bart ransomware and backend server analysis",  
 "url": "https://www.malwarebytes.com/blog/news/2017/01/locky-bart-ransomware-and-backend-server-analysis"  
 }],  
 "workflow\_start": "start--507aadb2-9f8f-4937-8643-5f50cd358906",  
 "workflow": {

**------------------------------------0---------------------------------**  
 "start--507aadb2-9f8f-4937-8643-5f50cd358906": {  
 "type": "start",  
 "name": "Start LockyBart ransomware attack",  
 "on\_completion": "action--cdc2f237-8823-413b-8beb-84a612be0ae8"  
 },

**------------------------------------1---------------------------------**  
 "action--cdc2f237-8823-413b-8beb-84a612be0ae8": {  
 "type": "action",  
 "name": "Use a software protection technique",  
 "description": "Code virtualization is added to the Locky Bart binary using WPProtect.",  
 "external\_references": [{  
 "name": "Anti-Static Analysis::Executable Code Virtualization",  
 "source": "mbc",  
 "external\_id": "B0008",  
 "reference\_id": "malware-behavior--2cfd6d52-467d-4d05-9091-b31916218bc2"  
 }],  
 "commands": [{  
 "type": "bash",  
 "command": "WPProtect",  
 "playbook\_activity": "step-sequence"  
 }],  
 "agent": "group--a757ce82-b838-4c68-9e41-74b0e94211a5",  
 "targets": ["software--5e1cadae-7532-45d8-89f8-fe051a1e7df8"],  
 "on\_completion": "action--3fdb51db-2548-4beb-ab7d-f52b3ab1e5ed"  
 },

**------------------------------------2---------------------------------**  
 "action--3fdb51db-2548-4beb-ab7d-f52b3ab1e5ed": {  
 "type": "action",  
 "name": " Install LockyBart on victim's endpoint",  
 "description": "ftp LockyBart to victim",  
 "external\_references": [{  
 "name": "Command and Control::Ingress Tool Transfer",  
 "source": "mitre-attack",  
 "external\_id": "T1105",  
 "reference\_id": "attack-pattern--e6919abc-99f9-4c6c-95a5-14761e7b2add"  
 }],  
 "commands": [{  
 "type": "ftp",  
 "command": "ftp malware.victim.com lockybart.exe",  
 "playbook\_activity": "step-sequence"  
 }],  
 "agent": "group--a757ce82-b838-4c68-9e41-74b0e94211a5",  
 "targets": ["security-category--324ccb41-3306-4876-b017-1e07a81e16de"],  
 "on\_completion": "action--7953f6e2-5f09-4fe3-8ffd-476ec5dabe3c"  
 },

**------------------------------------3---------------------------------**  
 "action--7953f6e2-5f09-4fe3-8ffd-476ec5dabe3c": {  
 "type": "action",  
 "name": "Wipe System Restore Points with VSSadmin",  
 "description": "The ransomware deletes any backed-up files",  
 "external\_references": [{  
 "name": "Impact:: Inhibit System Recovery",  
 "source": "mitre-attack",  
 "external\_id": "T1490",  
 "reference\_id": "attack-pattern--f5d8eed6-48a9-4cdf-a3d7-d1ffa99c3d2a"  
 }],  
 "commands": [{  
 "type": "bash",  
 "command": "vssadmin.exe delete shadows /all /quiet",  
 "playbook\_activity": "step-sequence"  
 }],  
 "agent": "software--5e1cadae-7532-45d8-89f8-fe051a1e7df8",  
 "on\_completion": "action--d31e28d1-3584-4f59-a139-6764c6509c6e"  
 },

**------------------------------------4---------------------------------**  
 "action--d31e28d1-3584-4f59-a139-6764c6509c6e": {  
 "type": "action",  
 "name": "Generate a seed to create a key to encrypt user’s files.",  
 "description": "Execute the function used to generate a seed, which is used to create a key to encrypt the files with. It uses variables like system time, process ID, thread ID, Process Alive Time, and CPU ticks to generate a random number",  
 "external\_references": [{  
 "name": "Cryptography::Generate Pseudo-random Sequence::Use",  
 "source": "mbc",  
 "external\_id": "C0021.003",  
 "reference\_id": "malware-method--82332a69-b4e9-4ce1-a3df-8d846a5b568e"  
 }],  
 "commands": [{  
 "type": "subroutine",  
 "command": "GenerateSeed()",  
 "playbook\_activity": "step-sequence"  
 }],  
 "agent": "software--5e1cadae-7532-45d8-89f8-fe051a1e7df8",  
 "on\_completion": "action--191bce6e-2fea-4a7e-b4a5-c0d96f129a8d"  
 },

**------------------------------------5---------------------------------**  
 "action--191bce6e-2fea-4a7e-b4a5-c0d96f129a8d": {  
 "type": "action",  
 "name": "Enumerate the files it wants to encrypt, skipping certain folders to speed it up",  
 "description": "Scan filesystem for user files",  
 "external\_references": [{  
 "name": "Discovery::File and Directory Discovery",  
 "source": "mbc",  
 "external\_id": "E1083",  
 "reference\_id": "malware-behavior--bd42af9f-9cb2-43c2-948d-da271591f890"  
 }],  
 "commands": [{  
 "type": "subroutine",  
 "command": "Enumerate()",  
 "playbook\_activity": "step-sequence"  
 }],  
 "agent": "software--5e1cadae-7532-45d8-89f8-fe051a1e7df8",  
 "targets": ["security-category--acc1cff5-af87-4caa-8529-84b08c187653"],  
 "on\_completion": "action--edd41723-869d-5a07-9971-55876c706533"  
 },

**------------------------------------6---------------------------------**  
 "action--edd41723-869d-5a07-9971-55876c706533": {  
 "type": "action",  
 "name": "Generate Key using data on victim's endpoint",  
 "description": "Locky Bart gathers information on the victim’s machine to create an encryption key.",  
 "external\_references": [  
 {  
 "name": "Discovery::Process Discovery",  
 "source": "mitre-attack",  
 "url": "https://attack.mitre.org/techniques/T1057/",  
 "external\_id": "T1057",  
 "reference\_id": "attack-pattern--8f4a33ec-8b1f-4b80-a2f6-642b2e479580"  
 },  
 {  
 "name": "Cryptography::Encryption Key",  
 "source": "mbc",   
 "external\_id": "C0028",  
 "reference\_id": "malware-behavior--99267783-7a99-4ab7-881f-0dbf52c5bfba"  
 }  
 ],  
 "commands": [{  
 "type": "subroutine",  
 "command": "Run function to perform action",  
 "playbook\_activity": "step-sequence"  
 }],  
 "agent": "software--5e1cadae-7532-45d8-89f8-fe051a1e7df8",  
 "targets": ["security-category--324ccb41-3306-4876-b017-1e07a81e16de "],  
 "on\_completion": "action--3f0dc5a7-ffd8-57e1-8b0b-2181638f5c95"  
 },

**-----------------------------------6b---------------------------------**  
 "action--3f0dc5a7-ffd8-57e1-8b0b-2181638f5c95": {  
 "type": "action",  
 "name": "Encrypt Files",  
 "description": "Encrypt files gathered during a previous step with the key generated in the previous step",  
 "external\_references": [{  
 "name": " Impact::Data Encrypted for Impact",  
 "source": "mbc",  
 "external\_id": "E1486",  
 "reference\_id": "malware-behavior--d2b9f551-8477-424b-8042-9c4289cb3cfe"  
 }],  
 "commands": [{  
 "type": "subroutine",  
 "command": "Run function to perform action",  
 "playbook\_activity": "step-sequence"  
 }],  
 "agent": "software--5e1cadae-7532-45d8-89f8-fe051a1e7df8",  
 "targets": ["security-category--191bce6e-2fea-4a7e-b4a5-c0d96f129a8d "],  
 "on\_completion": "action--a7fca25a-2ee2-59c0-8df6-9f6ade83e286"  
 },

**------------------------------------7---------------------------------**  
 "action--a7fca25a-2ee2-59c0-8df6-9f6ade83e286": {  
 "type": "action",  
 "name": "Encrypt key",  
 "description": "Encrypt the key used to encrypt the files with a master key, which now becomes the victim\u2019s UID used to identify them",  
 "external\_references": [{  
 "name": "Cryptography::Encrypt Data::RC4 (C0027.009)",  
 "source": "mbc",  
 "external\_id": "C0027.009",  
 "reference\_id": "malware-method--77c46dd0-28a7-4b9b-9c62-849e91f6306a"  
 }],  
 "commands": [{  
 "type": "subroutine",  
 "command": "Encrypt key using a public key and RC4 PRGA",  
 "playbook\_activity": "step-sequence"  
 }],  
 "agent": "software--5e1cadae-7532-45d8-89f8-fe051a1e7df8",  
 "on\_completion": "action--e742fc09-743d-4174-9edb-1b4bcccd03bb"  
 },

**------------------------------------8---------------------------------**  
 "action--e742fc09-743d-4174-9edb-1b4bcccd03bb": {  
 "type": "action",  
 "name": "Create and display ransom note",  
 "description": "Locky Bart then generates a URL on the victim\u2019s machine. It contains the link to a TOR cloaked .onion address where the malicious backend website is hosted. This URL has a user ID within it. This UID is the original decryption key, in encrypted form. Display the ransom note on the desktop with the URL to a payment page.",  
 "commands": [{  
 "type": "subroutine",  
 "command": "Create note with URL that contains the encrypted decryption key",  
 "playbook\_activity": "step-sequence"  
 }],  
 "agent": "software--5e1cadae-7532-45d8-89f8-fe051a1e7df8",  
 "on\_completion": " end--0176c66e-9dad-4008-8b4c-bc2d52264557"  
 },  
 "end--0176c66e-9dad-4008-8b4c-bc2d52264557": {  
 "type": "end",  
 "name": "Ransomware attack initiated"  
 }  
 },  
 "agents": {  
 "software--5e1cadae-7532-45d8-89f8-fe051a1e7df8": {  
 "type": "software",  
 "name": "LockyBart",  
 "description": "ransomware"  
 },  
 "group--a757ce82-b838-4c68-9e41-74b0e94211a5": {  
 "type": "group",  
 "name": "Adversary Group",  
 "description": "The threat actor group that runs the LockyBart malicious website"  
 }  
 },  
 "targets": {  
 "software--5e1cadae-7532-45d8-89f8-fe051a1e7df8": {  
 "type": "software",  
 "name": "LockyBart",  
 "description": "ransomware"  
 },  
 "security-category--191bce6e-2fea-4a7e-b4a5-c0d96f129a8d": {  
 "type": "security-category",  
 "category": ["filesystem"],  
 "name": "Files on endpoint",  
 "description": "File system on the victim's endpoint for which to select files that will be encrypted."  
 },  
 "security-category--324ccb41-3306-4876-b017-1e07a81e16de": {  
 "type": "security-category",  
 "category": ["endpoint"],  
 "name": "Endpoint with ransomware",  
 "description": "Endpoint where the ransomware attack takes place"  
 }  
 }  
}]