Chinese Espionage Group UNC3886 Found Exploiting CVE-2023-34048 Since Late 2021

cloud.google.com/blog/topics/threat-intelligence/chinese-vmware-exploitation-since-2021/

Mandiant

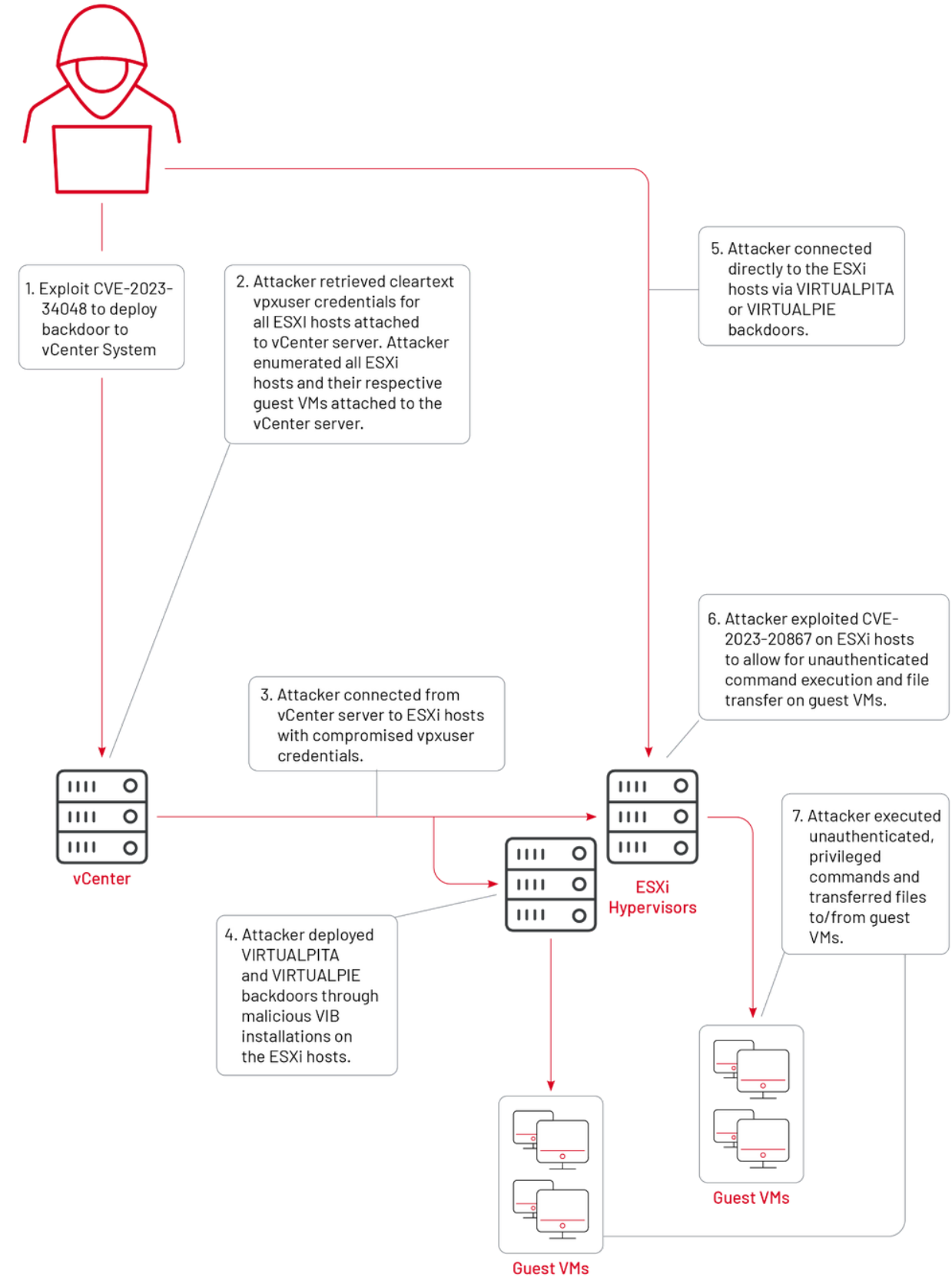
Written by: Alexander Marvi, Shawn Chew, Punsaen Boonyakarn

While publicly reported and patched in October 2023, Mandiant and VMware Product Security have found UNC3886, a highly advanced China-nexus espionage group, has been exploiting CVE-2023-34048 as far back as late 2021.

These findings stem from Mandiant's continued research of the novel attack paths used by UNC3886, which historically focuses on technologies that are unable to have EDR deployed to them. UNC3886 has a track record of utilizing zero-day vulnerabilities to complete their mission without being detected, and this latest example further demonstrates their capabilities.

When covering the discovery of CVE-2023-20867 in VMware's tools, the attack path in Figure 1 was presented describing the flow of attacker activity within the VMware ecosystem (i.e. vCenter, ESXi Hypervisors, Virtualized Guest Machines). At the time, with the evidence available, Mandiant continued researching how backdoors were being deployed to vCenter systems.

ATTACK PATH


1. Exploit CVE-2023-34048 to deploy backdoor to vCenter System
2. Attacker retrieved cleartext vpxuser credentials for all ESXI hosts attached to vCenter server. Attacker enumerated all ESXi hosts and their respective guest VMs attached to the vCenter server.
3. Attacker connected from vCenter server to ESXi hosts with compromised vpxuser credentials.
4. Attacker deployed VIRTUALPITA and VIRTUALPIE backdoors through malicious VIB installations on the ESXi hosts.
5. Attacker connected directly to the ESXi hosts via VIRTUALPITA or VIRTUALPIE backdoors.
6. Attacker exploited CVE-2023-20867 on ESXi hosts to allow for unauthenticated command execution and file transfer on guest VMs.
7. Attacker executed unauthenticated, privileged commands and transferred files to/from guest VMs.
vCenter
ESXi Hypervisors
Guest VMs
Guest VMs
MANDIANT

ATTACK PATH

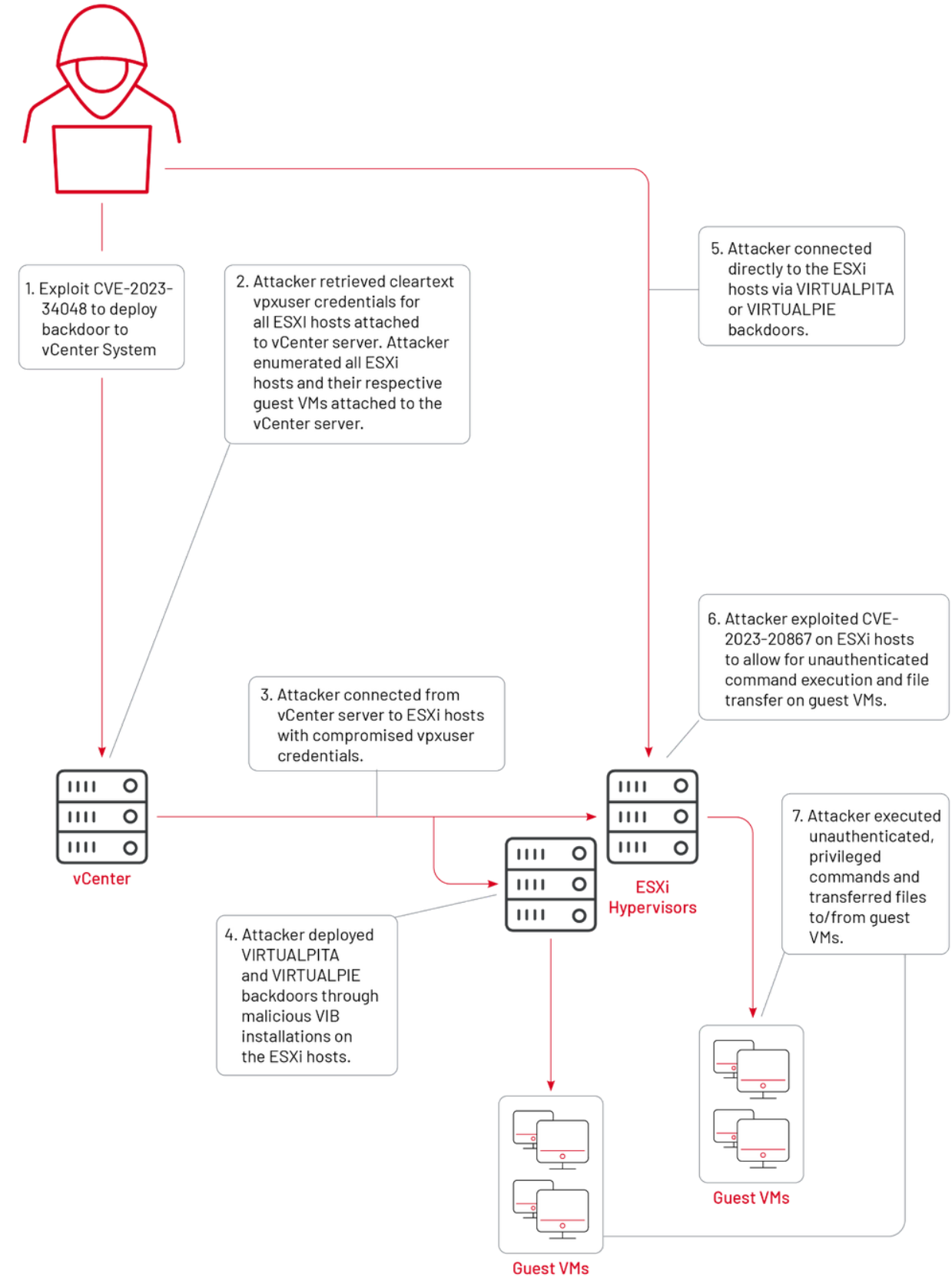

1. Exploit CVE-2023-34048 to deploy backdoor to vCenter System
2. Attacker retrieved cleartext vpxuser credentials for all ESXI hosts attached to vCenter server. Attacker enumerated all ESXi hosts and their respective guest VMs attached to the vCenter server.
3. Attacker connected from vCenter server to ESXi hosts with compromised vpxuser credentials.
4. Attacker deployed VIRTUALPITA and VIRTUALPIE backdoors through malicious VIB installations on the ESXi hosts.
5. Attacker connected directly to the ESXi hosts via VIRTUALPITA or VIRTUALPIE backdoors.
6. Attacker exploited CVE-2023-20867 on ESXi hosts to allow for unauthenticated command execution and file transfer on guest VMs.
7. Attacker executed unauthenticated, privileged commands and transferred files to/from guest VMs.
vCenter
ESXi Hypervisors
Guest VMs
Guest VMs
MANDIANT

Figure 1: Attack path

In late 2023, a similarity was observed across impacted vCenter systems that explained how the attacker was gaining initial access to the vCenter systems. Located in the VMware service crash logs, /var/log/vMonCoredumper.log, the following entries (Figure 2) show the "vmdird" service crashing minutes prior to attacker backdoors being deployed.

```
2022-01-01T01:31:55.361+00:00| <REDACTED>| I125: FILE: FileCreateDirectoryEx: Failed
to create /tmp. Error = 17
2022-01-01T01:31:55.362+00:00| <REDACTED>| I125: FILE: FileCreateDirectoryEx: Failed
to create /tmp/vmware-root. Error = 17
2022-01-01T01:31:55.419+00:00| <REDACTED>| I125: Notify vMon about vmdird dumping
core. Pid : 1558
2022-01-01T01:31:55.421+00:00| <REDACTED>| I125: Successfully notified vMon.
2022-01-01T01:31:55.927+00:00| <REDACTED>| I125: Successfully generated core file.
```

Figure 2: vMonCorDumper.log (Timestamps revised for client confidentiality)

Analysis of the core dump of "vmdird" by both Mandiant and VMware Product Security showed that the process crashing is closely aligned with the exploitation of CVE-2023-34048, the out-of-bounds write vCenter vulnerability in the implementation of the DCE/RPC protocol patched in October 2023, which enables unauthenticated remote command execution on vulnerable systems.

While publicly reported and patched in October 2023, Mandiant has observed these crashes across multiple UNC3886 cases between late 2021 and early 2022, leaving a window of roughly a year and a half that this attacker had access to this vulnerability. Most environments where these crashes were observed had log entries preserved, but the "vmdird" core dumps themselves were removed. VMware's default configurations keep core dumps for an indefinite amount of time on the system, suggesting the core dumps were purposely removed by the attacker in an attempt to cover their tracks.

As mentioned in the VMware advisory, this vulnerability has since been patched in vCenter 8.0U2 and Mandiant recommends VMware users updating to the latest version of vCenter to account for this vulnerability seeing exploitation in the wild.