Hitting the Jackpot

How Ransomware targeting VMware ESXi servers is used in Big Game Hunting to increase the speed and scope of the attacks
## Versions

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>02.06.2021</td>
<td>BSI</td>
<td>Initial Version</td>
</tr>
</tbody>
</table>

Federal Office for Information Security  
Postfach 20 03 63  
53133 Bonn  
Tel.: +49 22899 9582-5110  
E-Mail: certbund@bsi.bund.de  
Web: https://www.bsi.bund.de  
© Federal Office for Information Security 2021
Contents

1 Introduction ......................................................................................................................................................................................................... 4
2 Defray777 and its copycats ............................................................................................................................................................................ 4
3 Initial Access and Lateral Movement ....................................................................................................................................................... 5
4 Ransomware and Extortion .......................................................................................................................................................................... 5
5 Prevention and Countermeasures ............................................................................................................................................................. 6
Abbreviations .................................................................................................................................................................................................................. 7
References ........................................................................................................................................................................................................................ 8
1 Introduction

Throughout the last months, the Federal Office for Information Security (BSI) continued to observe large-scale ransomware campaigns targeted at financially strong victims – a strategy commonly referred to as "Big Game Hunting (BGH)". Thereby, the threat actors typically do not plan to target a certain company or institution beforehand, but rather choose their victims opportunistically after gaining an initial foothold (e.g., after a successful phishing attack). Benefiting from tools and methods offered as "Cybercrime-as-a-Service (CCaaS)" and different blackmailing methods (e.g., data encryption, data deletion, data leakage, DDoS-attacks during the negotiation phase, parallel blackmailing and harassment of the victim’s customers, etc.), this modus operandi has proven to be highly effective for the threat actors.

While most of these attacks are targeted at systems running a version of the Microsoft Windows operating system, a small yet growing number of threat actors has begun to deploy Linux versions of their ransomware, specifically tailored to compromise VMware ESXi servers. Since it is common practice to host numerous corporate systems on just a few ESXi servers, a ransomware deployed on these hosts has the potential to significantly increase the speed of the attack as well as the scope of the affected systems and therefore also the potential damage. The Cybersecurity Company CrowdStrike has therefore named this new technique "Hypervisor Jackpotting" ([LF2021], [All2021]).

2 Defray777 and its copycats

The first known ransomware of this kind was Defray777 (aka RansomExx or Ransom X) associated with the threat actor SPRITE SPIDER (aka GOLD DUPONT). However, driven by the extremely high damaging effect, also other threat actors have started to deploy ESXi-targeting Linux-Versions of their ransomware and more are expected to follow. Currently, there are known or announced Linux versions of at least Darkside, REvil/Sodinokibi, and Babuk Locker.3

The remainder of this document, however, will focus mainly on Defray777, as the BSI has already observed several successful attacks with this ransomware against ESXi servers of German companies since the beginning of these attacks in the second half of 2020. Thereby, the attackers have made forensic investigations almost impossible by demonstrating high operational security (OPSEC), using sophisticated attack methods (e.g., by staging payloads on internal servers or deploying tools in-memory-only), and often encrypting log files, which were stored on the same ESXi servers.

---

1 A very detailed description of CCaaS can be found in the 2019 “Bundeslagebild Cybercrime” of The Federal Criminal Police Office (BKA) [BKA2019]. However, please note that the publication is available in German only.

2 VMware ESXi is a Type-1 hypervisor (aka "bare-metal hypervisor") and part of VMware's virtualization platform vSphere. ESXi hypervisors are often centrally managed through the Server-Management-Software VMware vCenter ([VMw2021]).

3 In May 2021, the Ransomware-as-a-Service Darkside as well as Babuk Locker ended their service. However, their former operators could still use Darkside and Babuk Locker in the future or sell the source code to other threat actors.
3 Initial Access and Lateral Movement

As mentioned above, BGH threat actors mostly choose their victims opportunistically. Accordingly, various attack vectors are used (either by the attackers themselves or by so-called Access Brokers) to gain an initial foothold.

The most common ones are:

- Phishing mail / Social Engineering methods.
- Abusing stolen credentials for Remote Access Services such as RDP, VPN, or VDI.
- Abusing vulnerabilities in internet facing services/products such as Citrix Application Delivery Controller.
- Using the BokBot (aka IcedID) Trojan [FKI2021a].

Upon initial infection, SPRITE SPIDER uses different tools/malware to move laterally in the network, collect valid credentials, escalate privileges, compromise the domain controllers (DC), and exfiltrate sensitive data. In this context, SPRITE SPIDER has been observed to use the following tools:

- Cobalt Strike Beacons
- Mimikatz
- Vatet Loader
- PyXie [FKI2021b]

Vatet Loader is allegedly developed and maintained by the group itself (see [RS2020]) and is used to load the Remote Access Trojan (RAT) PyXie, with which the attackers try to steal valid credentials within the compromised network (e.g., by using the PyXie LaZagne module to recover VMware vCenter credentials stored in web browsers) and to collect sensitive data for exfiltration. If the attackers were able to gain access to the domain controllers, they might use this access to exfiltrate the data to a Cloud-Storage-Service like MEGA.

4 Ransomware and Extortion

In general, SPRITE SPIDER has been observed to use two different methods to roll out the ransomware Defray777 ([FKI2021c], [Cyb2021], [SK2020], [TAU2021]) on VMware ESXi servers:

1. They use stolen credentials to login to the VMware vCenter Server-Management-Software (e.g., after stealing the credentials with PyXie (see above)) and centrally deploy the ransomware.
2. They use two known vulnerabilities in unpatched VMware ESXi instances (i.e., CVE-2019-5544 and CVE-2020-3992, see, e.g., [Cim2021]) to gain access and deploy the ransomware by sending malicious SLP requests to the servers.

The attackers usually write the ransomware to /tmp/, thereby using a seemingly legitimate tool name to hide from detection. Before deploying the ransomware, the attackers usually terminate all running Virtual Machines (VM) in order to encrypt also all files associated with the VMs (see, e.g., [LF2021]).
Deploying the ransomware on the ESXi servers allows the attackers to significantly increase the speed of the attack as well as the number of affected systems. Moreover, in all cases observed by the BSI, the attackers managed to encrypt also all associated log files, which made forensic analysis practically impossible.

In addition to encrypting the files and demanding a ransom for the decryption, SPRITE SPIDER also threatens the victims to leak the previously exfiltrated data on a dedicated leak site on the Darknet\(^6\) - a method that has become increasingly common in BGH and is also known as double extortion.

5 Prevention and Countermeasures

Besides the commonly known prevention and countermeasures against ransomware attacks (see, e.g. [BSI2021]), companies and institutions that use VMware ESXi servers should consider the following suggestions:

- Keep all VMware instances at the latest patch level.
- Safe the associated log files on a separate server that cannot be reached via the network (similarly to offline backups).
- Disable SSH on ESXi servers or filter SSH access (on the switch/firewall) to ESXi servers.
- Separate authentication in VMWare from Microsoft Windows Domain authentication.
- Apply network segmentation with restrictive packet filters (e.g., administration network, normal employee-network, server-network, etc.).
- Prohibit direct internet access from administration workstations.
- Use different machines and accounts for administration and normal office-work for IT staff.

\(^6\) SPRITE SPIDER dedicated leak site: http://rnsm777cdsjsdls4v5qoeppu3px6sb2igmh53jzr7ipcrbje5b2ad7.onion/
# Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGH</td>
<td>Big Game Hunting</td>
</tr>
<tr>
<td>BKA</td>
<td>Bundeskriminalamt / Federal Criminal Police Office</td>
</tr>
<tr>
<td>BSI</td>
<td>Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security</td>
</tr>
<tr>
<td>CCaaS</td>
<td>Cybercrime-as-a-Service</td>
</tr>
<tr>
<td>DC</td>
<td>Domain Controller</td>
</tr>
<tr>
<td>OPSEC</td>
<td>Operational Security</td>
</tr>
<tr>
<td>RAT</td>
<td>Remote Access Trojan</td>
</tr>
<tr>
<td>RDP</td>
<td>Remote Desktop Protocol</td>
</tr>
<tr>
<td>SLP</td>
<td>Service Location Protocol</td>
</tr>
<tr>
<td>SSH</td>
<td>Secure Shell</td>
</tr>
<tr>
<td>VDI</td>
<td>Virtual Desktop Infrastructure</td>
</tr>
<tr>
<td>VM</td>
<td>Virtual Machine</td>
</tr>
<tr>
<td>VPN</td>
<td>Virtual Private Network</td>
</tr>
</tbody>
</table>
References


