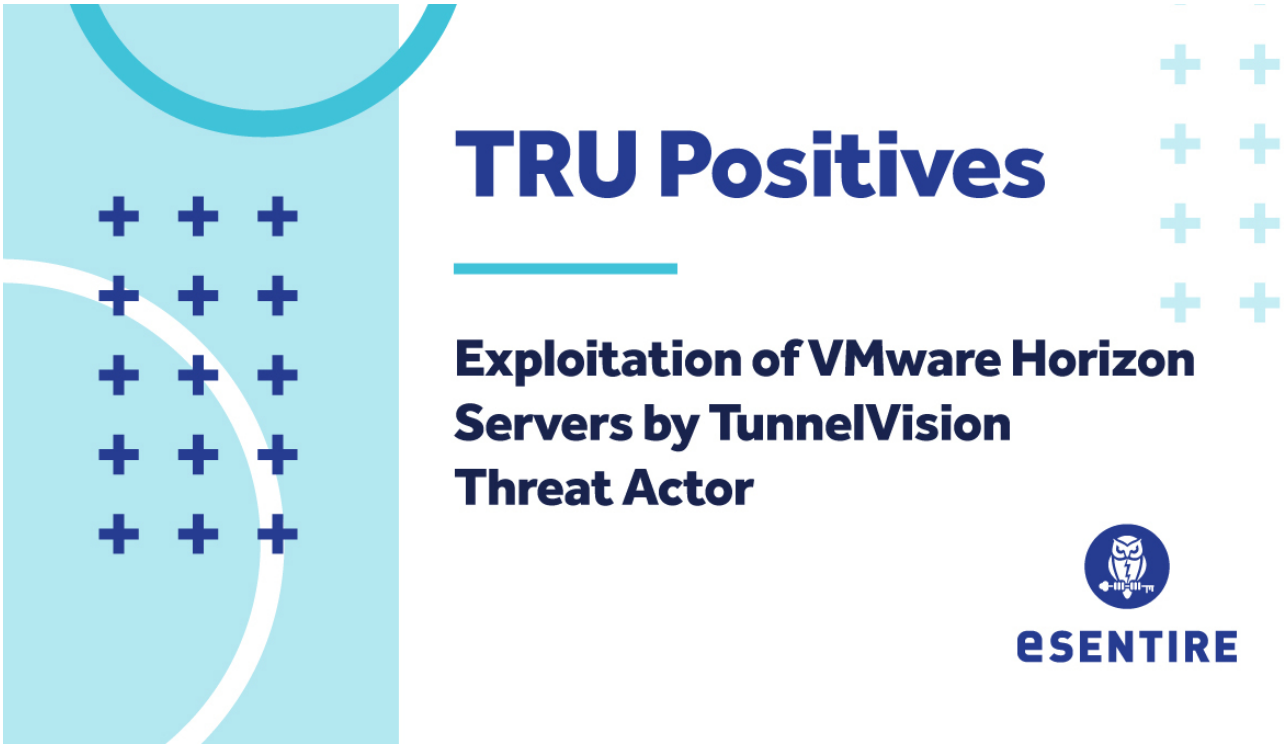
Exploitation of VMware Horizon Servers by TunnelVision Threat Actor

esentire.com/blog/exploitation-of-vmware-horizon-servers-by-tunnelvision-threat-actor



Adversaries don't work 9-5 and neither do we. At eSentire, our 24/7 SOCs are staffed with Elite Threat Hunters and Cyber Analysts who hunt, investigate, contain and respond to threats within minutes.

We have discovered some of the most dangerous threats and nation state attacks in our space – including the Kaseya MSP breach and the more_eggs malware.

Our Security Operations Centers are supported with Threat Intelligence, Tactical Threat Response and Advanced Threat Analytics driven by our Threat Response Unit – the TRU team.

In TRU Positives, eSentire's Threat Response Unit (TRU) provides a summary of a recent threat investigation. We outline how we responded to the confirmed threat and what recommendations we have going forward.

Here's the latest from our TRU Team…

What did we find?

- In early February 2022, we identified suspicious account creation and credential harvesting attempts on a customer's endpoint. The activity was escalated and traced to a VMware Horizon server.
- This server was operating an out-of-date version known to be vulnerable to Log4Shell (CVE-2021-44228). The server itself was not publicly accessible but believed to be exposed to untrusted input routed from an Internet-facing system.
- Analysis by our Threat Intelligence team indicates a strong link to TunnelVision, an activity cluster operated by an Iranian-aligned threat actor(s).
- Attribution to the TunnelVision activity cluster is supported by the following artifacts and observed Tactics, Techniques and Procedures (TTPs):
    - Common use of tunnel server 142.44.135[.]86
    - Observed C2 domain **activate-microsoft[.]cf** utilizes a similar naming convention to known TunnelVision server **microsoft-updateserver[.]cf** and shares similar registration characteristics.
    - TTPs (summarized below) observed in this case align with known TunnelVision behavior.
- The summary of intrusion activity for TunnelVision is as follows:
    - The initial pivot from compromised Horizon server occurred using NTLM authentication for a generic administrator account.
    - A backdoor account "DomainAdmin" is created on secondary systems using net command and then added to local administrators' group.
    - The adversary then performs lateral movement using PSexec and RDP.
    - Credentials are then harvested using Procdump.
    - Malware is written to C:\Users\DomainAdmin\Desktop\Drokbk.exe which creates service name, "SessionManagerService".
    - The malware written to c:\programdata\SoftwareDistribution\SessionService.exe communicates with activate-microsoft[.]cf and GitHub.
    - Sysinternals and SSH tools are downloaded by the backdoor account using a web browser on compromised systems.
    - Lastly, RDP tunneling is done using Ngrok to IP 142.44.135[.]86.

How did we find it?

We used eSentire MDR for Endpoint to identify post-exploitation TTPs.

What did we do?

- Our 24/7 SOC alerted the customer and responded to isolate the host on the client's behalf. We automatically blocked certain actions such as credential harvesting.
- Our Incident Handler team was engaged for further identification and containment actions.

What can you learn from this TRU positive?

- In a recent blog post, SentinelOne researchers linked TunnelVision's activity to the deployment of ransomware using n-day vulnerabilities including Log4Shell to access and compromise targets
- While overall exploitation of Log4Shell has diminished since peaking in December 2021 (see figure 1), opportunistic exploitation of VMware Horizon servers continues.
- We responded to several cases of Horizon Log4Shell exploitation throughout January and February 2022 (including this one).
- Network visibility determines the level of response effort required with regards to the exploitation of Horizon servers. It means the difference between identifying direct exploitation vs. just the ripple effects of a threat actor with a network foothold.
    - Where we had network and endpoint telemetry on Horizon servers, we were able to react and contain successful exploitation prior to lateral spread.
    - Where visibility was adjacent to these servers, we identified post-exploitation activity such as lateral movement using compromised credentials.
- In certain cases, vulnerable Horizon servers were not Internet-facing, but ultimately had exploit requests routed to them from external gateways.

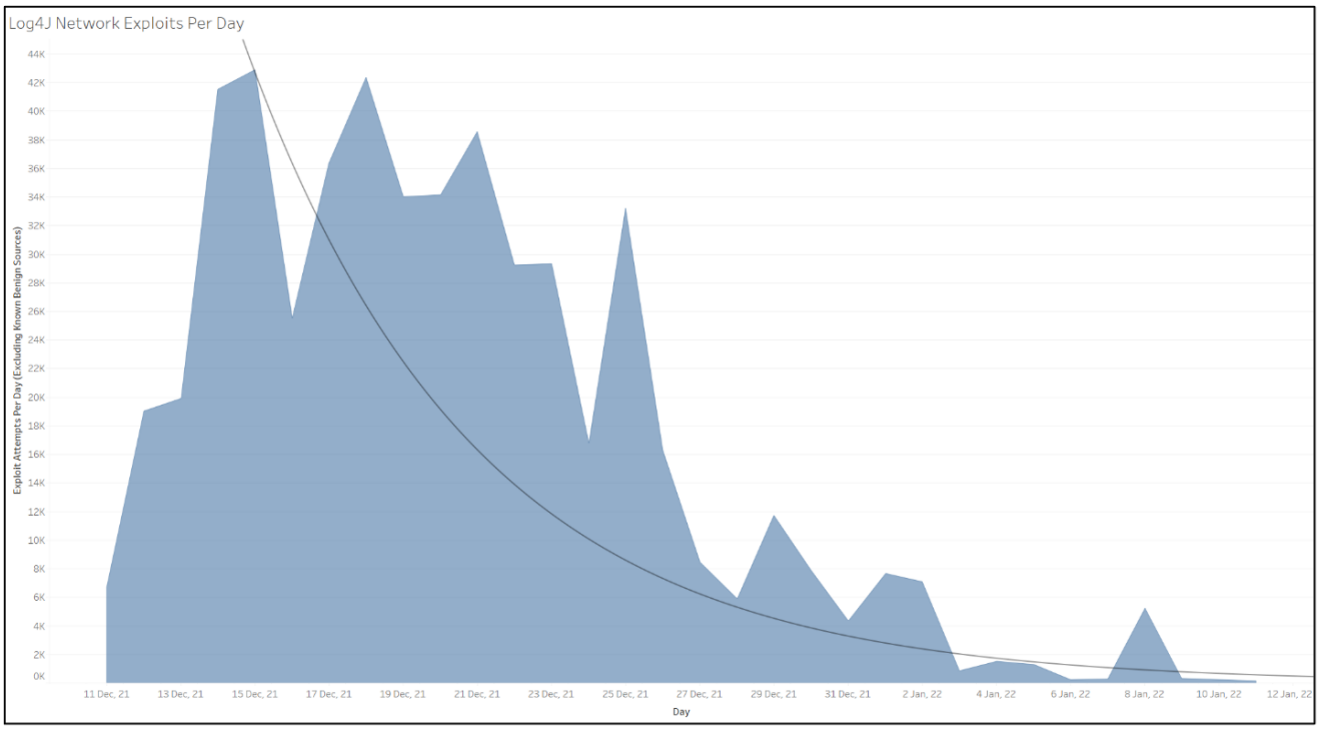


Figure 1 Log4J exploit events observed by MDR for Network, December 2021 to January 2022

Recommendations from our Threat Response Unit (TRU) Team:

Loader malware attempts to install other malware, so the priority should be to identify and investigate the presence of follow-on malware on systems. In addition, we recommend:

- Ensure any system which is directly exposed to the Internet or that handles untrusted data routed from Internet-facing systems is patched for Log4Shell (CVE-2021-44228).
- Ensure your security tools are monitoring critical servers such as VMware Horizon.
    This should include network, endpoint, and log visibility to aid with detection, response, and containment activities.

Ask Yourself…

- Are you monitoring for compromise of critical systems and follow-on actions?
- Are patches in place for actively exploited vulnerabilities?

If you're not currently engaged with a Managed Detection and Response provider, we highly recommend you partner with us for security services in order to disrupt threats before they impact your business.

Want to learn more? Connect with an eSentire Security Specialist.