KPMG Cyber Threat Intelligence Platform

BPFDoor Malware - Covert Linux Backdoor Exploiting BPF for Stealth

TLP : Clear

KPMG. Make the Difference.

BPFDoor is a highly stealthy and persistent Linux backdoor, believed to be linked to the threat group tracked as Earth Bluecrow, aka Red Menshen. First identified in July 2021, the malware leverages the Berkeley Packet Filter (BPF) to perform covert kernel-level network monitoring and command execution, allowing it to effectively evade conventional detection methods. BPFDoor targets critical sectors such as government, telecommunications, education, and defense, with activity observed across Asia, the Middle East, and Africa, including South Korea, Hong Kong, Myanmar, Malaysia, and Egypt.

Initial access is gained by exploiting vulnerable Linux systems, often through compromised services or misconfigured servers. BPFDoor uses the Berkeley Packet Filter (BPF) to monitor network traffic directly from the kernel, filtering for specific "magic" packets that trigger its backdoor functionality. Operating without open ports, the malware remains invisible to traditional port scans and firewall detection. It responds only to specially crafted packets authenticated via a hardcoded key, supporting multiple protocols (TCP, UDP, ICMP) for flexible C2. Upon activation, a reverse shell is provided for interactive control, with commands executed directly in memory to avoid disk writes and minimize forensic evidence. Persistence is achieved through the manipulation of system services or startup scripts, allowing the backdoor to survive reboots. Detection is evaded by bypassing standard logging mechanisms and system utilities, and the malware can exfiltrate sensitive data such as credentials and system information through covert channels established via BPF. Additional stealth is achieved through process masquerading & memory-only execution, hindering detection by EDR solutions.

BPFDoor's kernel-level stealth and covert communication capabilities underscore the importance of proactive monitoring, timely patching, and robust incident response.

What should you do?

- Monitor Indicators of Compromise (IoCs) in your environment to identify anomalies.
- Ensure your Windows environment is patched to the brim and is protected with multi-factor authentication.
- Conduct a comprehensive, full spectrum, threat assessment exercise to uncover blind spots and improvement areas.

KPMG Cyber Threat Intelligence Platform is an industry defining, research-based capability for enhanced visibility into cyber threats.

Our machine ingestible feeds and analysis are the result of automated, sensor-based intelligence metrics with dedicated, expert insights of each threat to provide you the appropriate context on a timely basis in industry standard formats such as STIX/ TAXII/ MISP.

These feeds are additionally co-related with our industry partners and independent research for additional context. The intelligence obtained is then curated from strategic, tactical and operational perspective to give you a wide-ranging view of cyber threats.

We also assist you with our renowned cyber incident response and threat hunting services in case you identify an active threat in your environment.

We offer a wide-range of services, including:
Strategic threat intelligence report
Machine ingestible threat intelligence feeds
Threat intelligence driven pre-emptive threat hunting exercise
Cyber Incident Response Services

KPMG in India Cyber Response Hotline: 1800 2020 502

KPMG in India contacts:

Atul Gupta
Partner
Head of Cyber Security
T: +91 98100 81050
E: atulgupta@kpmg.com

B V, Raghavendra
Partner
T: +91 98455 45202
E: raghavendrabv@kpmg.com

Sony Anthony
Partner
T: +91 98455 65222
E: santhony@kpmg.com

Manish Tembhurkar
Partner
T: +91 98181 99432
E: mtembhurkar@kpmg.com

Rishabh Dangwal
Director
T: +91 99994 30277
E: rishabhd@kpmg.com

kpmg.com/in

Follow us on:
kpmg.com/in/socialmedia

KPMG

KPMG Cyber Threat Intelligence Platform

BPFDoor Malware - Covert Linux Backdoor Exploiting BPF for Stealth

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes
e086fabda4078355c40543d6eafeec91
e0eb814b8b712573f8378574c2ec9104
f9a2fa83b78edbb23aec4b819fdcd45d
97603540ca33abac4ed81e705b50eb66
0cb92ea9c8cbfc5670cd60f4983968b6
462b1f3e78ff332ad0d565e53261ae20
d95f02ac786f587a734bf14bcec472df
1a3bcff5d7ff9ec9b4ff30a414485f85
770231fbf23b3923826f0ffa3cedb1c5
6aa8b196572ac773c5a5e3777979b23d
6dd745bb19c6deb3af86e06ba4bb3fe3
76eee7b520f98d9990bd3f09dd3e6a1e
317f579e32f9adda62277e9b7c36d4b9
712823df0696ae694cd690b767fad955
83023ecfc4836df0a25eec8826cbb80c
1c5892cbf7a5f9df9f01305dcccc522a
f6c72b40eb76b7389a2bbae80355f7d1
86279d833afe38baa4036cc5a20583cd
81cef3f9209dff2a9754466581a0a7ff
d5fb6d880ac18de3494d7cbb943935b9
9dc3fd2a0768db599503a1a19e02e18b
8ba84f5b91e9b53584526af479a4030e
7616b2b80c23f911a0a9b84621466a7e
821e33c0aea4f5a056540254e622a9951c0ddff2
2bc4dfec30893df28357e8affae068b32f0796d8
ca73295816ca7b693471803274115457a156ecb2

KPMG

KPMG Cyber Threat Intelligence Platform

BPFDoor Malware - Covert Linux Backdoor Exploiting BPF for Stealth

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes
213dbb5862a19a423e5b10789a07ee163ab71969
7e7234c5e94a92dd8f43632aca1ac60db7d96d56
c2717777ba2cb9a698889fca884eb7650144f32e
a778d7ad5a23a177f2d348a0ae4099772c09671e
b631d5ed10d0b2c7d9c39f43402cccde7f3cb5ea
5ddcbe4b591293f7b34fc0ef65db6248bcc67eb6
e6ccf59c2b7f6bd0f143cde356f60d2217120ad2
466527d15744cdbb6e1d71129e1798acbe95764d
e3399ea3ebbbd47c588ae807c4bd429f6eef8deb
2ca9a29b139b7b2993cabf025b34ead957dee08b
67a3a1f8338262cd9c948c6e55a22e7d9070ca6c
0f12ab32bac3f4db543f702d58368f20b6f5d324
28765121730d419e8656fb8d618b2068408fe5ae
e16b9469f265eba6548fb611df157b7eaa073666
92439c3c736a0554883118ecfe082b27aa6c9143
ed0cd45c3bb95ef8da214048799395e247040d17
27fc5359c0200cb33b328048d317605c255db6ea
8535c3b18a10649b94531c6d9f79750324498e5c
e935bbdc493017ff6b427d194c81063125705259
851d9a438b9bf3e9b0dc65fb2d18d6f3636ad71c
057b1783e8829e34e0c544c770360215fb60b7bb
5c2aa2735f5c925fd309b41d02f29473448aea68
0e214a3bb9955b9b792d0ef785beee212a26c7fd
07a0006381758443a91daa210bf6707ab1f0232284ccc712e247dc8d350a52e4
e764842d309d9465b8b27ad60fa4037708a06709205076124719d7dcfbbcc433
591198c234416c6ccbcea6967963ca2ca0f17050be7eed1602198308d9127c78

Follow us on:
kpmg.com/in/socialmedia

KPMG

KPMG Cyber Threat Intelligence Platform

BPFDoor Malware - Covert Linux Backdoor Exploiting BPF for Stealth

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes
63d5390d4cd15fa700595b7273e2a834f11588f94066b71d9062212e97543b48
b83127fbde5074247b81012553de69604365f7c4c378d8bcb54552c81ea85414
d2604c1aac79371108af426aa426e975cea582eb7e9a1d6890ae8a8896cf0cc5
9ea0645d862bc0604b47e9424bd27419f648ebc28ed6cd180b63fece7f3f4511
fa0defdabd9fd43fe2ef1ec33574ea1af1290bd3d763fdb2bed443f2bd996d73
3a1b174f0c19c28f71e1babde01982c56d38d3672ea14d47c35ae3062e49b155
bd353a28886815f43fe71c561a027fdeff5cd83e17e2055c0e52bea344ae51d3
fe9f3b7451913f184e1f53b52a03a981dcea5564633cfcb70d01bd0aec8f30a7
a002f27f1abb599f24e727c811efa36d2d523e586a82134e9b3e8454dde6a089
144526d30ae747982079d5d340d1ff116a7963aba2e3ed589e7ebc297ba0c1b3
14b1dea80394fb413fff084b0becd1904fd6077189d1ff73208d8d749529e00b
39d8d80a727ffab6e08ae2b9551f7251a652f4d4edfe5df21d0e2684d042268f
7c7db2ff3f428167aa8b59917fb1cde7e9244cb2240c0e24bddea5e0f0a26ff4
93f4262fce8c6b4f8e239c35a0679fbbbb722141b95a5f2af53a2bcafe4edd1c
af1911d5ad4653e5c972dcfe912fe2e2c928dc16d306609ffbb446ee11fca174
23320f05f929f6d587d86454c70f34c9ed3df38d32ae246a7636e6b6dc14a0c7
34dbc85ed0386e024c724c7969e8d0ff0ff0b1882508ea259c458d59657a1971
b8d775e2c9a18504aff01d8464fab1c470a8a37b501451fd9af6b4a848b42051
1925e3cd8a1b0bba0d297830636cdb9ebf002698c8fa71e0063581204f4e8345
cc61091ac6c8a8219b54f8f07976a2ab915e7675f715a00b8488ba180a5b3a07
e09efb3fb74728011ee52ec83b7f9764c899761432ba3e6b576b1b74605209bc
4713ac314e0fc64df3599b79331e867e1d3742e21cc4ca563e374868967efca5
a0a3a45adf5258414344214c3d2c661a570f54609b7d87d5ac24eb37fd30c3e6