ADVISORY FOR IM SECTORS

Earth Lusca uses novel backdoor for cyber espionage operation

Original report published on: Sep 04 , 2024 [1]

Executive Summary

Trend Micro researchers have identified Earth Lusca, a Chinese-nexus threat actor using KTLVdoor, a new highly obfuscated multiplatform backdoor as part of a large-scale attack campaign. The backdoor was written in Golang which impersonates legitimate system utility names or tools such as sshd, java, sqlite, bash, edr-agent and more in both Windows and Linux OSes. The backdoor is usually distributed as a dynamic-link library (DLL) and allows attackers to carry out various tasks including file manipulation, command execution, remote port scanning and more. The backdoor's configuration and communication involve sophisticated encryption and obfuscation techniques to hinder malware analysis.

Background

Earth Lusca, also known as AQUATIC PANDA, Charcoal Typhoon, TAG-22 and RedHotel, has been active since at least April 2019. The China-based threat actor primarily focuses on targeting entities in telecommunications, technology, and government sectors across Asia.

They are known to rely heavily on Cobalt Strike, ShadowPad, Winnti and Spyder malware families. KTLVdoor, the latest addition to the group's malware arsenal, is observed to have more than 50 command and control (C2) servers, all hosted by Chinese ISP Alibaba. With embedded strings that are not directly readable, symbols stripped, and most functions and packages renamed to random Base64-like looking strings, the malware becomes difficult to analyse and slows down malware analysis.

Detection and Mitigation Techniques

IMDA recommends organisations to perform continual testing and validating of existing security controls to ensure detection and prevention against the MITRE ATT&CK techniques identified in this advisory:

- Monitor networks within your environment for any suspicious reconnaissance tactics such as port scanning activities.
- Deploy data loss prevention (DLP) solutions to ensure that data remains within the enterprise or approved networks.
- Scan for Indicators of Compromise (IOCs) on your network. Validate before adding malicious file hashes to blocklist in anti-virus and/or Endpoint Detection & Response (EDR) and eXtended Detection and Response (XDR) including servers.

IMDA encourages organisations to conduct thorough analysis to identify potential risks and assess their potential impact prior to deploying defensive measures.

Indicators of Compromise [4]

Indicator	Type	Description
39.105.121.123	IP	Command & Control

39.107.101.26	IP	Command & Control
47.94.223.124	IP	Command & Control
47.94.166.190	IP	Command & Control
59.110.136.109	IP	Command & Control
123.56.45.175	IP	Command & Control
123.57.223.22	IP	Command & Control
39.107.75.91	IP	Command & Control
182.92.101.4	IP	Command & Control
123.56.45.175	IP	Command & Control
123.57.223.22	IP	Command & Control
39.107.75.91	IP	Command & Control
182.92.101.4	IP	Command & Control
123.57.6.3	IP	Command & Control
39.107.67.131	IP	Command & Control
101.200.156.217	IP	Command & Control
182.92.155.149	IP	Command & Control
123.57.218.176	IP	Command & Control
47.99.78.41	IP	Command & Control
47.96.97.77	IP	Command & Control
47.96.5.136	IP	Command & Control
47.96.135.49	IP	Command & Control
116.62.120.97	IP	Command & Control
123.57.60.94	IP	Command & Control
39.105.107.130	IP	Command & Control
182.92.233.242	IP	Command & Control
47.94.229.250	IP	Command & Control
182.92.169.60	IP	Command & Control
47.96.160.242	IP	Command & Control
116.62.231.152	IP	Command & Control
47.96.13.99	IP	Command & Control
47.98.173.175	IP	Command & Control
47.97.109.62	IP	Command & Control
139.224.254.181	IP	Command & Control
139.224.45.232	IP	Command & Control
47.102.36.88	IP	Command & Control
47.101.43.111	IP	Command & Control
139.196.196.178	IP	Command & Control
123.57.60.94	IP	Command & Control
39.105.107.130	IP	Command & Control
182.92.233.242	IP	Command & Control
47.94.229.250	IP	Command & Control
182.92.169.60	IP	Command & Control
47.100.98.234	IP	Command & Control
106.14.175.235	IP	Command & Control
106.15.193.24	IP	Command & Control
47.100.121.195	IP	Command & Control

47.100.59.42	IP	Command & Control
47.100.160.164	IP	Command & Control
47.101.48.168	IP	Command & Control
47.101.137.187	IP	Command & Control
139.196.89.210	IP	Command & Control
106.15.90.75	IP	Command & Control
47.93.38.26	IP	Command & Control
39.106.135.228	IP	Command & Control
47.95.198.228	IP	Command & Control
101.201.68.58	IP	Command & Control
47.94.194.248	IP	Command & Control
182.92.243.166	IP	Command & Control
47.95.168.191	IP	Command & Control
47.98.121.179	IP	Command & Control
47.96.106.167	IP	Command & Control
116.62.142.53	IP	Command & Control
121.40.70.23	IP	Command & Control
118.31.53.137	IP	Command & Control
47.98.50.198	IP	Command & Control
39.106.40.121	IP	Command & Control
101.200.63.187	IP	Command & Control
101.201.35.96	IP	Command & Control
39.107.231.100	IP	Command & Control
47.95.12.152	IP	Command & Control
47.94.20.102	IP	Command & Control
101.201.69.42	IP	Command & Control
47.94.202.137	IP	Command & Control
47.94.193.44	IP	Command & Control
47.94.227.15	IP	Command & Control
47.94.143.163	IP	Command & Control
39.106.13.202	IP	Command & Control
47.93.47.186	IP	Command & Control
59.110.226.246	IP	Command & Control
47.94.200.23	IP	Command & Control
9ceb37c55a1e55afe50e2b892d3756e5c89ee71131245f5da72c1b8dd0005b99	SHA256	KTLV Backdoor
6eec892054e6cb1addbde2fa92d3ccb5d56d37aa992f81f9106aaf124b9d3525	SHA256	KTLV Backdoor
20f09959706797b81b2a4de627c01d0c0d890d142954d455a0e50f7811bdc951	SHA256	KTLV Backdoor
7ff329e0a20a96dd4d0e8b42a216ade348161566250b7e39e166031c881f34d0	SHA256	KTLV Backdoor
12435ae8d190c4a0cae64009416f17195dbb7f7ca732b69e6178e9dd4c66fcb2	SHA256	KTLV Backdoor
19f94c523d4488a50584dd3d96500820e4f479cadcef4d14a1dd7cf939cd3154	SHA256	KTLV Backdoor

dc4277e5f6e76ef3f5c0da8a6703acd69a017747aac0413f7248911e51214641	SHA256	KTLV Backdoor
b66dab4fbdae54eea59313fd218abc96a54c0bbf0ab774dbe8776de9322510b2	SHA256	KTLV Backdoor
d095e636400ee633ae22488bba77d53f584f1ff279fd604bb6e60c0211d1957e	SHA256	KTLV Backdoor
99027cf9f6fcce91d1d08a8cc15043912e51aff82804d4678c7b453e55899404	SHA256	KTLV Backdoor
3d753a9e8e6ab22a498f7c6702910ea3e77ca8ef524f8435ac4614a9d4cbf345	SHA256	KTLV Backdoor
c75c5d7b4bdedcf5c6e78305d62f6830f4766c4517cf650a36493e19574c507d	SHA256	KTLV Backdoor
a133b1839bad5616b51915f2dfe420be36e05ee5c5f1c8e81220177b14c12848	SHA256	KTLV Backdoor
01ef286f55d1a15f308f2bed102bec0916d799d8e883a48117cecfe713a74267	SHA256	KTLV Backdoor
1887185af63849aea9cdd7855b638110447842f178fca9cd81b76c72acd16e68	SHA256	KTLV Backdoor
3dcad2fdebd68390ea4a80398593cfc3360ef51291b853cb3e9a607915ec74cb	SHA256	KTLV Backdoor
aa7bc130c5340364f61074f7c98651e80db3b08396a4fb449f614e0889acfdd3	SHA256	KTLV Backdoor
c0b1deaa2598936c284684b50a652f98771a129e882f382ac011d5ab984fd132	SHA256	KTLV Backdoor
1185fa967aa989d5e072577e493d2b307c48181480129d4c45337da64d5bfd25	SHA256	KTLV Backdoor
d18019064e5903dcf7c29921c10a7a90176cccd55d9cf3ba1e3e9805c1364df1	SHA256	KTLV Backdoor
644b88ce37d8ccb9258df6fcd74c6b485323dcfd9feb0f961252e6c311241703	SHA256	KTLV Backdoor
0b2e9328d82a045ce00f6b1b449ae32d8997f631f691350ea39d85c78eb66216	SHA256	KTLV Backdoor
18e2b7df374a838a57ebf3186b13a26e523cf964afde50b7ba765ed4d5509670	SHA256	KTLV Backdoor
d72ea22e6f35e848a2e5870863e410f0434013ad43c3f5b6935168fc07c7d7b0	SHA256	KTLV Backdoor
aa5ff64cadabd2d8aba7963c2372270bbfdafa155f85a9a9ec2b57674cf8173e	SHA256	Earth Lusca’s archive
fcf0cf8a19fa16792771310462d36f3c059ed7d36ef90899316313f4626d24d7	SHA256	Earth Lusca’s LNK file
fd3205edef38248c059898274f5818abbcb757adb707ca47580d4b16772a38d1	SHA256	Earth Lusca’s DLL decryptor

MITRE ATT&CK Tactics and Techniques

Tactic	**Technique ID**	**Technique Name**
Execution	T1059	Command and Scripting Interpreter

Defense Evasion	T1620	Reflective Code Loading
	T1027.013	Encrypted/Encoded File
	T1140	Deobfuscate/Decode Files or Information
	T1036.005	Masquerading: Match Legitimate Name or Location
Discovery	T1083	File and Directory Discovery
	T1046	Network Service Discovery
Command and Control	T1001	Data Obfuscation
	T1573	Encrypted Channel

References

1. https://www.trendmicro.com/en_sg/research/24/i/earth-lusca-ktlvdoor.html