KPMG Cyber Threat Intelligence Platform

Akira Ransomware – Targeting Global Enterprises

TLP : Clear

KPMG. Make the Difference.

Akira ransomware, identified in March 2023, is a sophisticated cyber threat known for its double-extortion tactics and evolving attack methods. Initially developed in C++, newer versions are written in Rust, appending extensions like .akira or .powerranges to the encrypted files. This ransomware group primarily targets sectors such as business services, critical infrastructure, construction, manufacturing, education, retail, and technology, with a geographical focus on North America, Europe, and Australia.

Initial access is obtained by exploiting VPN services without MFA and using valid accounts from initial access brokers. Threat actors also target external-facing services and conduct spear phishing campaigns to infiltrate organizations. Persistence is maintained by creating new domain accounts, allowing the attackers to establish a strong foothold within the compromised system. Discovery is performed using techniques like Kerberoasting and tools like Mimikatz and LaZagne to extract credentials stored in LSASS memory. The Zemana antimalware driver is employed to terminate antimalware-related processes, and Windows Defender is disabled through PowerShell to evade defenses. Tools like NetScan and Advanced IP Scanner are used for gathering network information, while PowerShell and Windows Net Commands are used to query the Active Directory. Remote services like RDP and SMB are used to move laterally within the network. Data is exfiltrated using tools like FileZilla, WinRAR, WinSCP, and RClone, and command and control is established using MobaXterm, Ngrok, AnyDesk, RustDesk, and Cloudflare Tunnel. They utilize a sophisticated hybrid encryption scheme, combining ChaCha20 and RSA, and use PowerShell commands to delete volume shadow copies to prevent recovery.

Akira's misuse of misconfigured VPNs and open-source tools underscores the necessity for advanced detection systems and proactive threat mitigation to counter sophisticated cyber threats.

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

Chandra Prakash
Partner
T: +91 99000 20190
E: chandraprakash@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

Akira Ransomware – Targeting Global Enterprises

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: IPs	
45.11.59[.]16	77.247.126[.]158
184.107.5[.]46	79.141.173[.]238
66.181.33[.]32	185.235.137[.]150
194.33.45[.]167	208.115.232[.]194
23.227.162[.]18	192.229.211[.]108
45.86.208[.]146	185.181.230[.]108
57.128.101[.]78	

Indicators of Compromise: Hashes
503f112e243519a1b9e0344499561908
777ee1bd450cece70663df8ba8155bcf
68729b85aa01cd8c9f4ccd137ddde137
d724d178eb09cd8ce2af8b088117b332
66c0423f3d8ad3abb14a21be90bf7bc5
aee6801792d67607f228be8cec8291f9
fe1897800d8fca8579ccabc83a0ca181
6615ea2fa3b879d27687a7ce917e93b0
0a6757bea01c2c48b50b7ec2bc39e31c
b87639f9a6cf5ba8c9e1f297c5745a67
77a243cb73f6bdd610eeb10786b752fb
ad739c2e9985161bc2ff9ed3a9a393ca
397550d976529add28274ef3adcff132
481a2965635bffdccf82bbb1f3e4b630
66ee3157cb461c50d0614620347d655f
0d76233931dfa993fd9b546bd5229976
e95e38c00b5a74f5fd31cd743d2449ce

Follow us on:
kpmg.com/in/socialmedia

KPMG Cyber Threat Intelligence Platform

Akira Ransomware – Targeting Global Enterprises

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes
748b043f1602547196fbbada0536a7c3
a74812faa9245f21516393218545387c
de8f808ba308e34097afa5c3136a0640
262e3fe7631204be404bdbdc2633282072461a61
c28ac747eedad47c36e93960dfa19e87e38b6803
48a07edd0af819e110173a8d0ee0c401b4defa98
5e4a8066b7a71b06fcaffd8ee50176c858721fb1
3f87d550f0b7c4f2ec8e60e8eed4214d49ddee61
b2643228c07d29f7ee1ead76bb4363351216fd17
ae6d6beeb79106464978608d0da56a3ec3a501e5
651c70f9d995c52fa48493b2e60904d15cad8821
edc878475896f13d14af40ecb0837a6f913c24fa
1cce67a2b76d3bcd85f158f533e55296b8aea592
93a202bdc9782283612fa1ee9b4f060ac01739e3
31af7f96a9df14900089a528dd9a3b9ce3549ace
7901d79f118cc659b7b6c09ce77d578de43bcc02
941d001e2974c9762249b93496b96250211f6e0f
b70b0784e43404f66a282231c65723aa66c63891
d7e073f9355723e2e731ee8b46ecb67863d9b81b
db9ba4f42942b27e1690c6d8a1bbd5b9d188fe49
923161f345ed3566707f9f878cc311bc6a0c5268
f070a115100559dcaf31ce34d9e809a3134b2511
104db47b553f6d06fd0d2353f806d0706e11cecb
0ceb5e99b2e1b2dd04cc07d1301c9649ce4cb458
2cde82cf7a1bc88c8fc5865cb57f31f6437f74fc
1d345799307c9436698245e7383914b3a187f1ec

KPMG

KPMG Cyber Threat Intelligence Platform

Akira Ransomware – Targeting Global Enterprises

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes
67396e1aacacb6efbca51f4c03d2017af78c9842
806a232379ad0af437d4bc5b87fb42065dbf82d4
648a5d7064cdf2a86f465ea6b318d0b1ceac905f77c438dac2778a001b50647c
b5268f32fb72dfcfc1109c4a305d3a4bac11a5815123659cd345b24dee0854eb
dbde2858580ec4f3484e91a42483cccdee2d243a5bb66a190f7363b129c02751
64c154ab8d7962fc7beeb2eb8b3893bbfb0badefc96eaafcfd0a9adc17720bff
48087149b5404e8b3945f8b4b0d581390c19cad10624bf9bad754fec82f69f28
18b967bd7a44f60521dd123dea0daf278572089b558b2e5632a6c06d9aad4529
3805f299d33ef43d17a5a1040149f0e5e2d5db57ec6f03c5687ac23db1f77a30
566ef5484da0a93c87dd0cb0a950a7cff4ab013175289cd5fccf9dd7ea430739
68d5944d0419bd123add4e628c985f9cbe5362ee19597773baea565bff1a6f1a
78d75669390e4177597faf9271ce3ad3a16a3652e145913dbfa9a5951972fcb0
8816caf03438cd45d7559961bf36a26f26464bab7a6339ce655b7fbad68bb439
88da2b1cee373d5f11949c1ade22af0badf16591a871978a9e02f70480e547b2
0ee1d284ed663073872012c7bde7fac5ca1121403f1a5d2d5411317df282796c
2b28270c1675990a2c78b31faab547fb75948dd1c2b22e892377ee5e40abebc2
1d3b5c650533d13c81e325972a912e3ff8776e36e18bca966dae50735f8ab296
25a6758df930b32eed548fca56735f0ddde442b5662e51c625eadbbaf09c9e96
27009c0abd2709cd5cac4c0135b8f3bed3229b0921601638ba9e90713ede91ea
379ef7c4f6dfae8cc0c8556861ff41930b88c7d9b107a5de10ccd194e1bda0cb
67afa125bf8812cd943abed2ed56ed6e07853600ad609b40bdf9ad4141e612b4
82e25f32e01f1898ccce2b6d5292245759733c22a104443a8a9c7db1ebf05c57
8738ba49fcd520789569aea7bf7af890741a745c79ae2bef49b93fb46c076c2b
89f5f29cf6b5bcfc85b506fb916da66cb7fd398cf6011d58e9409c7813e1a6f3
8bfa4c2c1065b105ec80a86f460e0e0221b39610109cc6cd4b441dd86e6b4aef
d0c1662ce239e4d288048c0e3324ec52962f6ddda77da0cb7af9c1d9c2f1e2eb

KPMG

KPMG Cyber Threat Intelligence Platform

Akira Ransomware – Targeting Global Enterprises

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes
0c0e0f9b09b80d87ebc88e2870907b6cacb4cd7703584baf8f2be1fd9438696d
131da83b521f610819141d5c740313ce46578374abb22ef504a7593955a65f07
28cea00267fa30fb63e80a3c3b193bd9cd2a3d46dd9ae6cede5f932ac15c7e2e
2c7aeac07ce7f03b74952e0e243bd52f2bfa60fadc92dd71a6a1fee2d14cdd77
2f629395fdfa11e713ea8bf11d40f6f240acf2f5fcf9a2ac50b6f7fbc7521c83
3298d203c2acb68c474e5fdad8379181890b4403d6491c523c13730129be3f75
43c5a487329f5d6b4a6d02e2f8ef62744b850312c5cb87c0a414f3830767be72
5c62626731856fb5e669473b39ac3deb0052b32981863f8cf697ae01c80512e5
6005dcbe15d60293c556f05e98ed9a46d398a82e5ca4d00c91ebec68a209ea84
7f731cc11f8e4d249142e99a44b9da7a48505ce32c4ee4881041beeddb3760be
87b4020bcd3fad1f5711e6801ca269ef5852256eeaf350f4dde2dc46c576262d
8e9a33809b9062c5033928f82e8adacbef6cd7b40e73da9fcf13ec2493b4544c
95477703e789e6182096a09bc98853e0a70b680a4f19fa2bf86cbb9280e8ec5a
9585af44c3ff8fd921c713680b0c2b3bbc9d56add848ed62164f7c9b9f23d065
988776358d0e45a4907dc1f4906a916f1b3595a31fa44d8e04e563a32557eb42
bcae978c17bcddc0bf6419ae978e3471197801c36f73cff2fc88cecbe3d88d1a
c9c94ac5e1991a7db42c7973e328fceeb6f163d9f644031bdfd4123c7b3898b0
9f393516edf6b8e011df6ee991758480c5b99a0efbfd68347786061f0e04426c
a546ef13e8a71a8b5f0803075382eb0311d0d8dbae3f08bac0b2f4250af8add0
a6b0847cf31ccc3f76538333498f8fef79d444a9d4ecfca0592861cf731ae6cb
abba655df92e99a15ddcde1d196ff4393a13dbff293e45f5375a2f61c84a2c7b
b55fbe9358dd4b5825ce459e84cd0823ecdf7b64550fe1af968306047b7de5c9
c0c0b2306d31e8962973a22e50b18dfde852c6ddf99baf849e3384ed9f07a0d6
ccda8247360a85b6c076527e438a995757b6cdf5530f38e125915d31291c00d5
dfe6fddc67bdc93b9947430b966da2877fda094edf3e21e6f0ba98a84bc53198
e3fa93dad8fb8c3a6d9b35d02ce97c22035b409e0efc9f04372f4c1d6280a481