KPMG Cyber Threat Intelligence Platform

Akira Ransomware – Wrecking Damage in Retro-Style

Akira ransomware campaign was launched in March 2023 and has attracted attention for its distinctive retro-themed data leak site. Despite sharing a name with a 2017 ransomware strain, this new Akira variant shows no code similarity, suggesting that it has different origin and objectives. This group uses a multi-extortion strategy, threatening victims with data leaks on their TOR site unless a ransom is paid. They have over 15 publicly disclosed victims, mostly located in the US, focusing on sectors like education, finance, manufacturing, real estate, and healthcare.

Initial access is achieved by exploiting user accounts with Multi-Factor Authentication (MFA) bypass or by targeting known vulnerabilities in VPN software. The attackers perform network discovery by creating scheduled tasks named "Windows Update" & employ Living Off The Land Binaries (LOLBins) to move laterally within the network. Further, they extract credentials through LSASS memory dumping via “comsvcs.dll” with proxy execution by “rundll32.exe”. To evade detection, windows defender and other security solutions are disabled. Upon gaining a stronger foothold, the ransomware payload is executed. PowerShell commands are used to disable volume shadow copies (VSS) to inhibit system restoration. The ransomware scans through the file structure, matching files to predefined list of extensions to be encrypted & encrypts them using the Windows Restart Manager (WRM) API, utilizing RSA and AES encryption algorithms. WinRAR is used to compress the collected data, while remote management tools like Radmin, AnyDesk are used to establish persistent access & to exfiltrate data from the compromised machines.

With Akira attacks on the rise, it is important to mitigate against it to avoid imminent damage. Thorough patch management and regular security audits are key components in defending against such 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.

The 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

Contact us:

KPMG in India Cyber Response Hotline : +91 9176 471 471

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

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

Sony Anthony
Partner, KPMG in India
T: +91 98455 65222
E: santhony@kpmg.com

Chandra Prakash
Partner, KPMG in India
T: +91 99000 20190
E: chandraprakash@kpmg.com

Manish Tembhurkar
Associate Partner,
KPMG in India
T: +91 98181 99432
E: mtembhurkar@kpmg.com

KPMG

KPMG Cyber Threat Intelligence Platform

Akira Ransomware – Wrecking Damage in Retro-Style

Indicators of Compromise: IP Addresses	
209.197.3[.]8	23.216.147[.]64
23.216.147[.]76	208.111.186[.]128

Indicators of Compromise: Domains
akiral2iz6a7qgd3ayp3l6yub7xx2uep76idk3u2kollpj5z3z636bad[.]onion

Indicators of Compromise: Hashes
c7ae7f5becb7cf94aa107ddc1caf4b03
af95fbcf9da33352655f3c2bab3397e2
d25890a2e967a17ff3dad8a70bfdd832
e44eb48c7f72ffac5af3c7a37bf80587
503f112e243519a1b9e0344499561908
68729b85aa01cd8c9f4ccd137ddde137
0885b3153e61caa56117770247be0444
e148dee0132f5d20c01fbb4a3fc87b47
302f76897e4e5c8c98a52a38c4c98443
ddec50fc00e3be31cedb24bc7bfa9fb8
431d61e95586c03461552d134ca54d16
9f1c1e45b292299818c7fe64c865e67a
16b9b5e0f9f1747350ad37eff94bb82f
66004c532d292572494de9934fe3910b
77958f66ade19ace783617531f0d82ac
d724d178eb09cd8ce2af8b088117b332
de8f808ba308e34097afa5c3136a0640
923161f345ed3566707f9f878cc311bc6a0c5268
f070a115100559dcaf31ce34d9e809a3134b2511
2cde82cf7a1bc88c8fc5865cb57f31f6437f74fc
db9ba4f42942b27e1690c6d8a1bbd5b9d188fe49
8d635ca131d8aa20971744dcb30a9e2e1f8cd1be
960b01ab967e96fd6d875eb157667e8ef7ff1c4a
941d001e2974c9762249b93496b96250211f6e0f
b70b0784e43404f66a282231c65723aa66c63891

KPMG

KPMG Cyber Threat Intelligence Platform

Akira Ransomware – Wrecking Damage in Retro-Style

Indicators of Compromise: Hashes
9180ea8ba0cdfe0a769089977ed8396a68761b40
76beb70b06cfe714c4fa250b6b2d1e5025fe3c50
c4d6c1fd4c1a702a2302cc62bce7d770e5b7369c
24e7848dab0b82b200781630e617d6ed7e6016e7
30d49ced95cb9a0fb6526b30131501b28cbbc388
5e6d77960065df450e0533f9a8409c7463292243
688d67eb4ff993963c86297ab8345962334ead27
843f3ad221a9da48d82df672bd8806cc090430b5
9a14a69eb279513cde2de0be538cc8d275fd34e9
bdb3fa0c50db18f7ada02b2060b4c5110016e859
f2e6853050f76517a9a7d472f3a994d0ae8411cf
1cce67a2b76d3bcd85f158f533e55296b8aea592
5e4a8066b7a71b06fcaffd8ee50176c858721fb1
3f87d550f0b7c4f2ec8e60e8eed4214d49ddee61
b2643228c07d29f7ee1ead76bb4363351216fd17
c5b39dec7922bbfd6f7e0d067eaa7339dab6479b
5961a99181df157b81d35a50eeb27f96577a2fa2
4cb8365b18b1c319d374be0b9d219144c20fb8714e9cf346e655f854d2c60170
3c92bfc71004340ebc00146ced294bc94f49f6a5e212016ac05e7d10fcb3312c
5c62626731856fb5e669473b39ac3deb0052b32981863f8cf697ae01c80512e5
7b295a10d54c870d59fab3a83a8b983282f6250a0be9df581334eb93d53f3488
678ec8734367c7547794a604cc65e74a0f42320d85a6dce20c214e3b4536bb33
8631ac37f605daacf47095955837ec5abbd5e98c540ffd58bb9bf873b1685a50
1b6af2fbbc636180dd7bae825486ccc45e42aefbb304d5f83fafca4d637c13cc
d0510e1d89640c9650782e882fe3b9afba00303b126ec38fdc5f1c1484341959
6cadab96185dbe6f3a7b95cf2f97d6ac395785607baa6ed7bf363deeb59cc360
9ca333b2e88ab35f608e447b0e3b821a6e04c4b0c76545177890fb16adcab163
1d3b5c650533d13c81e325972a912e3ff8776e36e18bca966dae50735f8ab296
c417a89cdc86ea6d674d2dc629ae1872b4054ac43e948e8ed60d3f3f47178598
67afa125bf8812cd943abed2ed56ed6e07853600ad609b40bdf9ad4141e612b4
d793aaaba1b4b34a20432b86505b851d838def0cd722b8cbdd1d08e19a08b6ee
b44b4e162de1decc9a5d3c61a045eb4776c55fccd33c9eced5b9f622faee19fa
a6cd727a18e5e2a80fbd8a51c299a2030bd5e68e4bbf136e07eb9d0b3f3bb8ce
99331170be7aa48d572728f68e52ac8d3eb3c8307cb8050ce504ef9f4624a4ba

KPMG

KPMG Cyber Threat Intelligence Platform

Akira Ransomware – Wrecking Damage in Retro-Style

Indicators of Compromise: Hashes
619614cda94a4b6b185c0c122d11ef2b8b0b3e7fc94a1a5c2ff1ac49233df54b
4222681314f5ffd69fe17ab2ae4b9aaa60866571fe2b53afc10f87e3738cedda
367e13f234a46822aa9655690f18000319123ad07a62e56bcf8bebbfbb0de7b9
637e28b38086ff9efd1606805ff57aaf6cdec4537378f019d6070a5efdc9c983
2a9257c6c74e37d051f78ed5abaa620b71b27fa3604798af077256a128d911bb
3f4ceeada7ff021c30df1646437d2ab0e55997bbb281444501f6d1f4ea8fa209
fb2433beb961839b36198e242d0dedb7fa85ab3e08a1141d02874aa4235ac776
c239dadd55b55b817fda5b0c2bb062adf399a5b78a8b3280a473d3ae66f81777