KPMG Cyber Threat Intelligence Platform

Amadey – Return of the Malware Distributor

Amadey Malware, a botnet of Russian origin was first observed in the late 2018. Capable of performing recon, info stealing & loading payload, it has been used by the operators of GandCrab, Clop, Fallout & Rig exploit kits in the past. After phasing out in 2020, it has resurfaced now, and is being used to spread LockBit 3.0. With Amadey being sold on underground forums, its being used to target countries such as US, Japan, Mexico and Brazil.

Amadey has been observed to be circulated via SmokeLoader which is concealed as malicious e-mail attachments, maldocs, internet adverts or disguised as software crack or keygen and relies on victims to download & execute. On execution, the loader Injects "Main Bot" into the active “explorer.exe” process to evade detection and downloads & runs Amadey. Upon downloading, it copies itself to a TEMP folder, registers itself in startup folder and sets up a scheduled process via cmd.exe to preserve persistence. Basic system info along with architecture, OS & AV versions, availability of admin privilege, etc., are collected and communicated to the C2 as a plaintext HTTP POST request. Further, it receives C2 commands to download & execute additional malware such as RedLine stealer or LockBit 3.0 from various remote sources. Powershell commands are then used to add Defender exclusions and to abuse 'FXSUNATD.exe’ to elevate privileges & execute the downloaded payloads using DLL hijacking. Once the main payload is executed, the scope of impact is further widened depending on the environment & group operating it.

Despite being simple, Amadey has been quite effective in achieving its goal of delivering various malwares. Also, with Lockbit 3.0 being aggressively distributed via multiple channels, it is of vital importance to tighten security across the organization at every level.

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

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai - 400 011 Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.

This document is for e-communication only.

#KPMG josh

home.kpmg/in

Follow us on home.kpmg/in/socialmedia

KPMG

KPMG Cyber Threat Intelligence Platform

Amadey – Return of the Malware Distributor

Indicators of Compromise: IP	
45.9.74[.]80	185.17.0[.]52
62.204.41[.]5	62.204.41[.]6
31.41.244[.]200	62.204.41[.]4
188.34.187[.]110	179.43.154[.]147
190.123.44[.]138	94.142.138[.]182
185.246.221[.]126	

Indicators of Compromise: Domains	
specialblue[.]in	hellomr[.]observer
authymysexy[.]info	valorantcheatsboss[.]com
nftmatrixed[.]info	teamfighttacticstools[.]info

Indicators of Compromise: Hashes
c115b34186a6f8add04cb29504cc0950
1adc717687e60609ba37cbf2416cd2d8
033ed2bd3f101882ec5bd9fc7456d6a9
63f3f9d6ff6e490bbbe0831a228e59b1
bb3f19b64b51827da5d35063397151bd
a6db57a937be8608709cc35dc05abf74
d6e084a3fef5620bfe521266c2d67373
7b7cffc0ef24c8ef230122cec85bcc78
a0758e715229f401905361dd814281a5
826afff15284905486ee20d583f1ed1e
afffe3e41d9b499d3c023e8835dcde5e
339518b4f23d147c26108b11907d3d78
e6dece6adbc32f446c3963d895317294
f4e2491dc8b01a83cfc02d0f935de57d
af34a25bef0d100c93a1def910601110
a359f00c1f48a7d4bb1eb05ad9a2fe3f
bf331800dbb46bb32a8ac89e4543cafa
56c9c8f181803ece490087ebe053ef72
5e7b31ef4be668d9d7586d5d0e75a49b
2067fca42df57e725aa6e0d4fd851533

KPMG Cyber Threat Intelligence Platform

Amadey – Return of the Malware Distributor

Indicators of Compromise: Hashes
34b872f8b83951cfdf37748e6df4c0bb3c103dcb
891a07ddaf9b723696a841088874ffb1ca2a6590
a5137ebb95345be050162dc5dce5a89e6397ac7b
587e94fc99ca0d0c1dbc452c98ccb838ea26b5ba
5caab983639cd958bc68091326677652e85d6db1
049bfd790fd4d7f333429c312d3417d237f88bdb
d8cb927a060cd5fd1c24db37b5cf3344b91e8b30
57e5156d60eb69ea5ffc94d75548fd00eaf7df4a
23cccac06462988b2355e22a36974edf3f2a9e71
833ac348fb902dfc8aa24c841810581c0ac7bf35
356543cd6fb4b2c7ca956e1977682dd094bb654c
b286353ebbc7e68fd198472f561c63ec24380bdc
3455d3db4516f5ed3017fe783c36677b47e4d619
fd7cf4a90bb5fd0e9bff41ffca04db80229e05ec
6c90db3de600923f76d5c1c5a8837506a5e6a52ff2883bb8d4c332cbcf8e6126
90cc787870f37ff7bd617976d253b613eab4fcbe65fb31cf3890efeb6636d9d3
7970613a8bdc95bb97d4996d9302153feef816b64a6b1861045a2aec85dcdb8d
8fb3b241a2578c6fbaf43a7c4d1481dc5083d62601edece49d1ce68b0b600197
ca02d7d9ded6d35965b5eae79da178fbb884c9002ae33b342a689ee8842990dc
06c034757f977337ebfd88435f03a269565aa91bcd0c12e3b65fa67be93a08b5
0463d0233cd7c8f52eef695455104382b26a9e271295434cbadc922b9aefd53b
0a072e13fdda89ff7ab9321e391808ef874fbf43a2fd8eb8e467bed2356786e8
0a8b40ab270592c164cf20e7c4bce25c463cad38921cad5c38011ce0e92c62bb
0e75d7203122528f762c3e7deea3909a9edc15dd7f1a60501c06e29a9078342b
144bc0eaf4de9456739293f88ebb89d2b86854f94bc5b68fd4a22e11040acd09
150a035a466943bc6a45350e5356fe175b7cf5838741f690dac38153ceecc838
23c13654e8b97d771c48deb3f2152c16cfa9e42ef16106c4fe1fb9893ec0ba60
2250359f6596055abd142e60de17b3a70444af528aea344dde3770404e2d23c3
21f0eeeb708c08d4dd1407ee543e264be08c9569ecb1ef865b492bb39c094e67
2152e1f3040073ddc4e34e84a067743fda7b16e10a2dba24306709443e78849d
212ad5ff5dfa070c2a796171152fa6283ffb0518a992c8bcb06cc7b909156e22
1eca7d0651b6abece4f654b4f9415c16304b4df4b0eddb0dc429eb70cf9f2b9a
1a25c881cb175dadf627d38b4c45dd0529bc890689df7b11e809205299a1d96c
37f92634e86fb911d9310cdf7d70a8db8f6b59441fe7ebfa271dee4116f99ac2