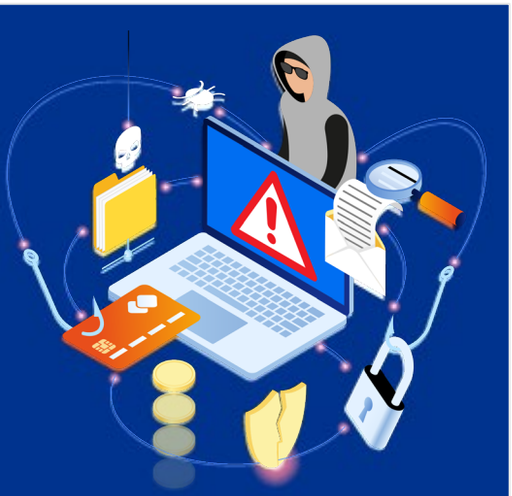
KPMG Cyber Threat Intelligence Platform

Aurora Stealer – Botnet turned MaaS turned Stealer



Thriving in Russian-speaking underground forums, Aurora Stealer in its nascent stages in April 2022 was marketed as a botnet bundled with stealing and remote access capabilities. Within the period of July, it was further sold as Malware-as-a-Service & got rebranded as stealer in August. This Go-lang based stealer is well-equipped to steal browser data, telegram, and a range of crypto wallet apps. Aurora is known to be spread via multiple infection chains, owing to the growing adoption by various traffers – cybercriminal groups that lure victims and redirect legitimate to malicious content operated by others.

Aurora infection chains includes fake cryptocurrency sites whose links are sent via phishing emails & use of stolen YouTube accounts to direct users to fake 'free software catalogue' websites to lure victims into downloading the malware disguised as other software. Once executed, it fingerprints the host via a Windows API wrapper package for Go, takes a screenshot of the Desktop and leverages built-in 'walk' function in Go library to traverse directories to find matching target extensions. It matches the filename with pre-defined stealer logic and follows up with compiling the stolen data into a specific format and base-64 encodes it for exfiltration. C2 comms takes place via non-standard TCP ports 8081 & 9865. If configured to deliver a second stage remote payload, Aurora uses the built-in 'net_http_Get' function in Go to download it which gets saved with random name under temporary folder. Further, a PowerShell 'start-process' command is used to execute it.

It is imperative for organizations to avoid downloading software from third-party websites and deploy spam protection solutions. A sound awareness program and routine phishing simulations aid in overall training and protection from 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

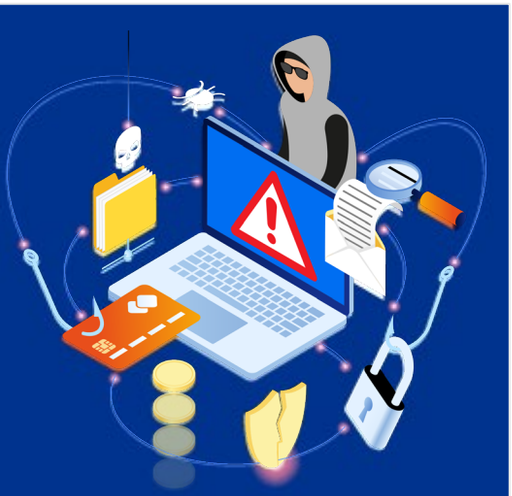
Chandra Prakash
Partner, KPMG in India
T: +91 99000 20190
E: chandraprakash@kpmg.com

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

KPMG

KPMG Cyber Threat Intelligence Platform

Aurora Stealer – Botnet turned MaaS turned Stealer



Indicators of Compromise: IP Addresses	
5.9.85[.]111	45.144.30[.]146
37.220.87[.]2	45.15.156[.]115
49.12.97[.]28	45.15.157[.]137
45.15.156[.]22	49.12.222[.]119
45.15.156[.]33	65.108.253[.]85
45.15.156[.]80	65.109.25[.]109
45.15.156[.]97	78.153.144[.]31
81.19.140[.]21	85.192.63[.]114
138.201.92[.]44	95.214.55[.]225
146.19.24[.]118	167.235.233[.]95
185.173.36[.]94	79.137.195[.]171
185.209.22[.]98	82.115.223[.]218
193.233.48[.]15	89.208.104[.]160
45.137.65[.]190	

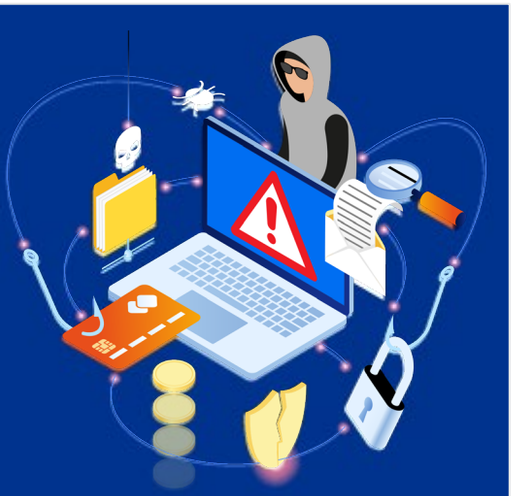
Indicators of Compromise: Domains	
alls0ft[.]cloud	winsofts[.]cloud
unisoft[.]store	cheatcloud[.]info
allsofts[.]cloud	mividajugosa[.]com
winsoft[.]cloud	freesoft[.]digital

Indicators of Compromise: Hashes
028127380d80a772b49b51e429b0f2df
238a69aa001a8f4801f018863fa06a7c
dfc4a031492642766e68c03f4d8ec744
f1827fa50344a56e1e96cc6908987edc
f1bd13f3967109836a4f8257e5d97979
18e5bbab98dfe3754ccffb2ed245a5ff708c2975
999fbb849ef6643c5dda377f96f08c3125e456c0
b86b1bcdca1e6e9a9486bed90d2133742f9cb4bb
d70b62de10f3ab0d51bd462127637afdb0430085
04b2edcc9d62923a37ef620f622528d70edab52ccd340981490046ad3aa255e5
131c895c99072d35444d5f02b7cd655d896f6e46b4797a411e67fbeec67d2b25

KPMG

KPMG Cyber Threat Intelligence Platform

Aurora Stealer – Botnet turned MaaS turned Stealer



Indicators of Compromise: Hashes
2bdba09d02482f3016df62a205a456fc5e253f5911543bf40da14a59ad2bc566
2e9dbda19d9c75a82dabac8ffba5ea76689ada81639867c41c395a29aeaba788
459a8faa7924a25a15f64c34910324baed5c24d2fe68badd9a4a320628c08cb8
47332ce5b904b959aa814ddfde8662931fdfb5233422dc45053ad04cffc44fb4
4b5450b61a1be5531d43fe36f731c78a28447b85f2466b4389ea7bbb09ecec9c
51a2fe0ea58a7a656bc817e91913f6d6c50e947823b96a3565e7593eea2fd785
5eebb883b26f3fa90720e3a03ce506304e55e16466fd17fb826fe7bd6e7b067b
665ea7e8d46a70f45072482085ffb24983c17c29d996c1ee0ea0108c124a48ff
6ddc2187ee3ee580224cccd0af87200548f200a71c1cc2b68f21674d4aba358f
719e7cc10663b3eaaeec42a6404d6be6c934e40ad6bd986dea5e5a1da69cb416
7450681968a1358f286f20cf90a805d69efde674dfa31daa74a72b8f9de50d71
88e02def17fda0021d4dba5ea812772c542b0fa6ca8930bcf06c42375c00bd29
8e24e96e1e87cf00e27c3a3745414636fbf6e148077c0f6815a2b87bacf85c8d
9742a534e644c151da070dabdbc27a121ae9f12ccb8e05a558378263f761e569
9db1744112aea85c625cd046fc737bf28bef254bebfbf7123df6844f62167759
a485913f71bbd74bb8a1bdce2e2c5d80c107da7d6c08bf088599c1ee62ccb109
a4a3a66aee74f3442961a860b8376d2a2dc2cf3783b0829f6973e63d6d839e5b
aa3766a3a70aab357e3a7f29965e7690caad40bbdbeb32560d0be9f254b59455
aa504264669e5bdbda0aac3ada1cd16964499c92d2b48d036a16ba22d79f44f6
de8d16087160bda144055c99d266c98bb4b2ac38a8745acc6b79ae61e061ee19
e58107788c19c30811c6225ea2803952303c99aa67fd8d6edffa056140e84afc
f6b17c5c0271074fc27c849f46b70e25deafa267a060c35f1636ab08dda237d6