KPMG Cyber Threat Intelligence Platform

PureCrypter – Proliferating Multiple Malware Families

Popularly rented as a malware distributer, PureCrypter is a .NET-based malware downloader leveraged to deliver an array of info-stealers and RATs since its debut in March 2021. Besides its similarity to the features of most Malware-as-a-Service offerings, it provides persistence, infection status updates, multiple payload injection types, etc. It has been observed to deploy malware families such as AgentTesla, Redline Stealer, Arkei, AsyncRAT, and many more. PureCrypter has been actively used to target government entities in Asia-Pacific and North American regions, with the infection rate constantly growing.

The attack vector uses a 2 stage-package mechanism which involves a lightweight downloader and a more sophisticated injector to bypass security controls. The initial downloader is hosted on Discord app as a password protected ZIP archive & is delivered via email with the URL for the same. Upon execution, it secretly downloads the second-stage injector which is a .NET assembly heavily obfuscated via SmartAssembly tool. The injector, further executes a series of reversing, decompression, deserialization & checks the runtime environment for anti-sandboxing before loading the final payload. PureCrypter includes a new feature to send infection status update to the attacker via Discord or Telegram APIs. The malware sets up persistence by renaming and copying itself to the startup folder or by modifying 'Run' registry keys. PureCrypter boasts multiple injection methods such as process hollowing, creating shellcode for embedded resources and loading payloads as assembly. Before injecting final payload, it also performs anti-virtualization check using WMI queries.

Being feature rich and highly sophisticated in its operation, PureCrypter is spreading almost 10 malware families indicating that the operators have a mature infrastructure to keep growing.

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

PureCrypter – Proliferating Multiple Malware Families

Indicators of Compromise: IP
89.34.27[.]167
79.110.62[.]23

Indicators of Compromise: Domains
gbtak[.]ir
letmaker[.]top
taskmgrdev[.]com
oracleservice[.]top
cents-ability[.]org
amcomri.upro[.]site
sub.areal-parfumi[.]si

Indicators of Compromise: Hashes
5e0c7ed04b645309256d4cbb4bcb0ada
0180decb30ec5d3934893c90995b2aca
8d816bd3b14271a3bd2953970d1cbc6f
eff7ae696a293b48cc7932e6304bcaa5
d6f8fe93185b1f97a8ded2e50f4affb6
009ed09f1bc8b4c9dbbf40d74f60c61e
e6ee01eefc03e56e385cb620990516d8
14e4bfe2b41a8cf4b3ab724400629214
f1c29ba01377c35e6f920f0aa626eaf5
5420dcbae4f1fba8afe85cb03dcd9bfc
18e9cd6b282d626e47c2074783a2fa78
2499343e00b0855882284e37bf0fa327
0d8b1ad53fddacf2221409c1c1f3fd70
17f512e1a9f5e35ce5761dba6ccb09cb
b5c60625612fe650be3dcbe558db1bbc
a478540cda34b75688c4c6da4babf973
765f09987f0ea9a3797c82a1c3fced46
bbd003bc5c9d50211645b028833bbeb2
71b4db69df677a2acd60896e11237146
f4eebe921b734d563e539752be05931d

KPMG

KPMG Cyber Threat Intelligence Platform

PureCrypter – Proliferating Multiple Malware Families

Indicators of Compromise: Hashes
fdd4cd11d278dab26c2c8551e006c4ed
dbcaa05d5ca47ff8c893f47ad9131b29
c9ca95c2a07339edb13784c72f876a60
c3b90a10922eef6d635c6c786f29a5d0
8ef7d7ec24fb7f6b994006e9f339d9af
fa4ffa1f263f5fc67309569975611640
754920678bc60dabeb7c96bfb88273de
2964ce62d3c776ba7cb68a48d6afb06e
8503b56d9585b8c9e6333bb22c610b54
eaaf20fdc4a07418b0c8e85a2e3c9b27
b6c849fcdcda6c6d8367f159047d26c4
7d53cba56ef089dd5530135766f652be5e9240b3
181cf9bd4aaa5e0fc3e329f72a32e5fdb5af2e67
2cedfdc8fe097481618267837bf56d94871a2a97
5c81b45d6d9c53e4e481bbac8e4edb6930f0121a
c2af7cff7678443b4a8aad601e8af7c9965bce20
781171f5738f6b84191def495704ca0d532e2a21
f64b4f867b05ed4ac03bfa4c61cad6cd7f51a248
c582964b54cf705ac12adec72740737b245b491d
7b2c191bc2d5d549c5e65613f93d59ece1842f02
db19ee960f0b21125f5483fbd9b88bf067d6ce7d
29fbc33455a7d0e34b4fdaef0ef05d88736ee3d0
c2a0423639ed2031855848b975b8d72fc280d3c4
942933b7a1dc5a460cad61cd76d2cad275ddfb4c
6c4314eba14a0b89426c11926405294653dcd53f
86d8e308e646b8e58b0e1c4feaa9f66b756b58e2
4f279b9b7dfbbcd71080c70eec73ad57cf3bdc15
e092ae101d611b45da02b84a5b083a3f1927fe3f
77a484bca5ab057c03c1484f72e279b8098a1e46
762ec7932b53e879e00a35abfae3843f9ca4d537
facdebf8ae77289bbe5f07092cda5e1725659be7
99803aab3de2340359ca7e30667ebdbb268d4c28
d25d94e9fa1b95023ccd3ba06241135495b9f99f
297cc6a96b3778ad3eeea64e335ff9b390071427

KPMG

KPMG Cyber Threat Intelligence Platform

PureCrypter – Proliferating Multiple Malware Families

Indicators of Compromise: Hashes
4b36745a28fbb8a64eed742a1851d378d31eac51
e43d2beb514e71cfce596a7c7481b55eeabb9077
bffba8a4cc2ba225b51d1650c3db80198175f842
9cda8af1c9ed103c4fba9eb8997a4aa6ba903c0000d1b231b38923bf64ca7d85
9ebaa5be5c27c9bce67ab15bd06f02c2f9fcf5e15f3e1f1136223fa8d1e0f3ad
a142668e7eacf65fb0e493da9881cff7d9f074cb0414a5824a63a8a2704d2d67
ceff897df7716a8b4dfb91c0c40ff22958e23479b5ae96163f20bef42ebb58ce
db6888d6c351e7a0df0fc86d900499dd9584a6d93e8eb7a39a77e4d143438cf6
e97f6e8e367e2ccaff9912703665530a5c6cec0a962ba07fa09e3302b57b26a2
ef0fdc710efe73584e0e6a0a16840fb3863ac5c27d73148463242f53b003991c
f5062c918df69fbe64a8999744a5f0345a6b3cdb34471a826f0caf5e4f28c38f
fa423ae9c8044f369df9fc62048653a3971fe43c8016aeb4846abc4c8cfff3f1
0868b330a014bd3a723f3af33eef76fca94a61049b1d7836226b16a0ad96ce1c
c8f27a841f726761652f562c1e2c61b1eb4490c8b7bdd264f6fd08b8e5d92e4b
132b33d15b8a8c2031df9b7e50e0fde9ba6a0aa4a10b29ece281457f6d777997
14df7a24c57be46551df4ce6fe2cba8bc32965d48216819d6c6a277f90b2fee4
1c35533679377e4109f5e79004ab6e92c45c0c65c2c5e779bf2be1315f271ee3
2209a22038dbf801f853caea4ed26258cf75ff463d343af24e81afa62a7314bd
22d12e21cdf1faf0b0296a49962f1f948bb5277128b4b57c1f9b856296e0da60
2a73f9630efba72072a6ab746a2edb54fae3d17784f225e0b6aa5c3bc3112d20
2a73f9630efba72072a6ab746a2edb54fae3d17784f225e0b6aa5c3bc3112d20
2cf3025121889c2d16b2f03facb5b1b0bdfe0a0a374a1439de85e720b597ef1b
32f8199d8289b3cf11abee24f6ca75d434e1c7f2b7410c256b9576d9729ea62e
0706791a5a4e03269d368cf03ee0647ba89d637d149a6fe3d8d7045a55fa7fac
3ad5383d0dbf16164fe43fde5c4d3d28e7fb2d555c6088942ab2c196551a50ec
3eb2ff798dd0355a0586a1f69c22fae3633b496366f92a0706f7206ec2e9c265
50a087604400b8f52ee602b5ef789d1a8af6995768e13d54bc5979bb787889c2
575dc19ebedafd5e9ae703469770f54cd454b156534263fda77f5f0b7b41243f
5873ee190579a89e39f8dc0979f4bbfd7faa26244eb2457c62b236c0ebd687f4
58a9f1fc454bea4dcbc81ab4585bec797cd02933018ba80e6e2d824d1fe9f820
72af49a238243953363be4ab915d943f9f38c31f0a8ec77397477340c2a389d9
78ee0644bbe5776bbf4474fa112e69da56a250d40357f7b09ddf09e0de117ea1
80d4414ca76e050007cb39c7fb598e1828ad168bea5725fb5466ee9388d6fa05
8a9a16c96fb72aaee2e108dea290e1767bbc854eccafd0cffadc6f2bf1f27b00