KPMG Cyber Threat Intelligence Platform

PicassoLoader Malware – Concealed Threats In Image Files

PicassoLoader malware surfaced in April 2022, utilizing phishing lures and decoy documents for deployment. This malware serves as a conduit for launching other advance malware like Cobalt Strike Beacon and njRAT. It was observed in recent activities that cyber espionage threat actors, such as Ghost Writer and APT 28, employ this malware. The malware aims to illicitly obtain sensitive data , establish persistent remote access and execute nefarious payloads over targeted systems. Government entities, military organizations, and civilian users in Ukraine and Poland have been targeted as part of a series of campaigns.

The PicassoLoader malware employs sophisticated techniques, initiating its intrusion through phishing emails with misleading attachments posing as familiar file types like Excel or PowerPoint documents. Once opened, these attachments trigger hidden code, setting off a complex chain of actions. This includes the deployment of a ".LNK" file via an embedded VBA macro or by leveraging regsvr32.exe to fetch a DLL downloader from an encrypted JPG image. This downloader ultimately fetches and runs the PicassoLoader payload. To maintain persistence, the malware creates autostart entries, concealing itself within image files to evade detection and verify endpoint security before launching. PicassoLoader serves as the gateway for more harmful malware like AgentTesla RAT, Cobalt Strike Beacon, and njRAT, creating a multi-layered threat that significantly jeopardizes sensitive data security.

The PicassoLoader malware, camouflaging malicious payloads with image files, highlights the need for regular security updates, cautious downloads and robust endpoint protection to counter evolving 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.

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

PicassoLoader Malware – Concealed Threats In Image Files

Indicators of Compromise: IP Addresses
112.78.109[.]74

Indicators of Compromise: Domains	
carpetmarker[.]pw	everything-everywhere.at.ply[.]gg

Indicators of Compromise: Hashes
36703e31039e026976a6762c4cbe14f7
552d020c3c090c7b297a8f23f7c48648
e8a3a4367ac7ac4b838d1bbb75b3b4b8
f75df4d551f84f12531908a81b776d8d
8568d46ff95b41d9c6f98343394ac322
fbb5c2f2f8c4eb6e719831010e724893
88c2f95bb1e008e2952799a427ab8492
fd50e12495d42282362f348428d132d9
6857da89a25728b066dcf7f47d25455b
adf00c9e47cc724dd4ff1f9af14401b5
6e6c39f498d0231417f6fa75e27b3008
4e23e56fb247e92980331ca23a1b7300
c0dc96834b07ec32bc67d3bce7b60a28
5bf951438305f16e42f6a85b81d6c5d7
192e12e92dd0fe7a838e104eb65665ef
552d020c3c090c7b297a8f23f7c48648
6857da89a25728b066dcf7f47d25455b
f09420169a24a54eff0fc35cd15d68bc
a85c94825f1420dd15cd80851e89efb1
4d8bc51e52067f4b983e4f60d5618a15
1d3f26e8b8f0a145d752bc089e5904e5
d43e0c177c7de3d311706609fecdabb8
6ca2fd21f500ec2dd5ae6bceaa5a72c019a6ee19
7add9ddca40c6557092b65ede6f457c05687c552
5c991f0e6201f0a47750f4ff5d0fa0f5cb435e79
953b3a6f7012ef73b613631752306026e6a9d189
310d58a1b2b8258ca635b25820b221787aa379e9

KPMG

KPMG Cyber Threat Intelligence Platform

PicassoLoader Malware – Concealed Threats In Image Files

Indicators of Compromise: Hashes
01b37a3c0a7861fc9681a44fb49a722a85c53f97
f17036d5c24e099ac3ee877163347cbb7a8909e7
e43e6c3d61aa6507b23aecca2dc5347a241c694f
33d671d18013d30be36be01f5f58f9c62e03f61c
30c986ae5db230b142a1a87f37c2493be4fe4f06
20d11c2e518d4041fd470141d5910445f8733636
e6e2ea1f742b93db6110dc86e21941e4c3001841
c7efa71b25fb0ffe00d4d0ef07b6294660f2e2c4
67fecd37e6c4ac2282fa8e6f8ab7d4cb6bfe44e4
4785b730ed724c742e2914ca07cce054f0da948f
61154ddda3692ef0e7fc324528d51badad7fdfba
F00939201f7e77221e94e917a8e34c3d2143324e02fdf35058526d870a0023a0
4d9cca1d75d4691e794dfe9efb9eef6e9e64b4e978ad17831b459d4bb6722829
2c5ba56a41f40bac2f21065fb9883545ef8d359883cb7bc351c481cb9542e104
44fd895174a7c1c0019fc95bb04201106dc165704c70e902e3de58db98f03c7e
30d46a740e2677c8fee383c2a4762561a10c66c5b99215262e42bfabf6bfb1aa
924d3589d642e8fd65746dc156ff9f104d43114a04ea9509f51ee6a439d1915b
Bc92a5b1c4205ea1fbfec9144b8aab485e095142c7105c9d616b089ec668f198
Ad8e3ebd496fb4d97e5075adb4f2f1b91195cca059800d0acd182a07698c13b6
0f3bdbc64446555c6ff611b02f2e64250fcaf39b78237ae4cca7c74d94731b32
35d1e819d2ac2535f0aa9e2294570135f37519386872c415e326146e931b8fb9
4da99f963c26bcc4537ba0437c9cc1445be8bea64067d34308dda6c2e49c8c65
0f3bdbc64446555c6ff611b02f2e64250fcaf39b78237ae4cca7c74d94731b32
7893965d1861c712b751bc2d5fb53a34ec0d276bcf389b7fc574728940575152
6dd40ea5e53754a7160801aa5e378089c7dcd9b76429c2536d115c022e3484e8
3b7702a3c2434f8677dddcd44b8ab09bd23129df98ce76929d5731d156398c32
b27ec1a0d4e122765abbecc5e66742f4ed546adfda208b4320fbf277d37a38f5
97894351c3c0728f3c2c740b0ea60af7bd9db955f2d3dc1a97668227956c89f3
4d9cca1d75d4691e794dfe9efb9eef6e9e64b4e978ad17831b459d4bb6722829
5061bf0d671aacb5fc8e89918c6e5dc5e0b8cb14020422ca73ca5941a7f34b98
7f89ec40687564ad7bae34c3f9cddcea28624b3ecf4807e3cef9911d850aecf8
32cf2acd3300d5c0cf7aadc70f07d137d705f379e35510e25018578e3ee40f42
1de7d03db87618e20b85c4e30e040168f26e4a0bdc98943736ef9a2c5f648e23
52fe07167694935a5a6441c1e6de73b08f786f736057034de766a7fa3866e576