KPMG Cyber Threat Intelligence Platform

Grandoreiro Trojan – Unveiling the Banking Sector's Nemesis

Grandoreiro, a sophisticated banking trojan, was first observed in 2016, primarily operating as a Malware-as-a-Service (MaaS). Its latest variant boasts significant updates, including enhanced string decryption and Domain Generation Algorithm (DGAs). This trojan targets over 1,500 global banking applications and websites across 60 countries, enabling attackers to perform banking fraud in countries spanning regions such as Central and South America, Africa, Europe, and the Indo-Pacific.

The attack commences with phishing emails impersonating official entities, urging recipients to click malicious links. These links redirected the users to a large ZIP archive, disguised in an image of a PDF icon, containing the Grandoreiro loader executable. The custom loader is deliberately enlarged to over 100 MB to evade automatic anti-malware scans, presenting a CAPTCHA pop-up for manual execution. It utilizes AES string encryption to obfuscate detection while collecting essential system data to assess sandboxing and establish communication with the C2 server. Upon successful communication, the loader retrieves and decrypts the final payload, the Grandoreiro banking trojan, which establishes persistence on the victim's system by creating registry entries and configuration files. The trojan employs a sophisticated DGA to dynamically calculate its C2 server's domain based on the current date, to evade takedown efforts. Once installed, the trojan supports a range of commands for remote control, including mouse manipulation, and browser behavior influence. It also can harvests Outlook emails for spam propagation, covering its tracks by deleting sent messages and using DGA seeds for harvesting.

Grandoreiro's enhancements in string decryption and DGA calculation algorithms have enhanced its evasion capabilities, highlighting the need for robust defense mechanisms against evolving 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

Grandoreiro Trojan – Unveiling the Banking Sector's Nemesis

Indicators of Compromise: IP Addresses	
66.70.160[.]251	185.228.72[.]38
167.114.4[.]175	167.114.138[.]249
77.246.96[.]204	167.114.137[.]244
62.84.100[.]225	

Indicators of Compromise: Domains	
rufnag[.]com	pjohconstruccionescpaz[.]com

Indicators of Compromise: Hashes
af7b60fed4e328f28ea58608768b51f3
5d5a63bb52a4ddbd9d3e031704245397
0a0b01ed0e0a756041c4696c0ffe4110
8d2ab8795ce1172503535464c5d4fb7a
f199aa84eb2b80e7a5a9f21e5a2307dc
a6445cbe3235b32217f751e8e471994f
7466f951c79dd5d92add631e9f503a81
09b3686d233d69ae96d460428c61b17d
c7e0b4ca6fe0ae4688db2e5f123a1ebf
970f00d7383e44538cac7f6d38c23530
724f26179624dbb9918609476ec0fce4
2ec2d539acfe23107a19d731a330f61c
6433f9af678fcd387983d7afafae2af2
56416fa0e5137d71af7524cf4e7f878d
7ea19ad38940ddb3e47c50e622de2aae
e02c77ecaf1ec058d23d2a9805931bf8
6ab9b317178e4b2b20710de96e8b36a0
5b7cbc023390547cd4e38a6ecff5d735
531ac581ae74c0d2d59c22252aaac499
6b659741bf29921d1a4db838f8b81ce27be660b8
3294c12bfca2c398f4ece3160ead58ab9d52a2ca
394627ae720e00ad1d926fabbed2ee43b38f522a

KPMG

KPMG Cyber Threat Intelligence Platform

Grandoreiro Trojan – Unveiling the Banking Sector's Nemesis

Indicators of Compromise: Hashes
03048f3b29f4a2eadd1612b50b40427017c4a548
3ff50510a1d0d9782d8b2032d21f5a8d79aa6ede
6f8fb8cc3f8b75927f3158ae19c12f12a7ac8c87
4ed6e543479f9dbdce8a087e4d445dfebeea103b
fb32344292ab36080f2d040294f17d39f8b4f3a8
08c7453bd36de1b9e0d921d45aef6d393659fdf5
a99a72d323ab5911ada7762fbc725665ae01fdf9
4cdf7883c8a0a83eb381e935cd95a288505aa8b8
f00f72183cc957ad051121eda04656d5a079917f
74cc8f29e9e219ee788685437aa3287236fa44e9
77590e32bd7df8266667853ede94c2a9485f373b
8555af4421fd963e005d1c9bb2deb41a8e7a4792
3b5a146a68bcf19367c599dc902dfd15e9f646bd
16185a41cabc4faddfb0e171a6dcb1bb900ad8de
930bf7e87dc8da35157e51113c77d30cc1041554
7da32f17e5fdea124ffd8a0f3281aee76df13a4a
a18e0a6d74a0c7a01786baaba98c2b4c92de3333
9f3cbe6bac6c21e60ce82365b0f19c375b578c73
84572c0de71bce332eb9fa03fd342433263ad0c4f95dd3acd86d1207fa7d23f0
70f22917ec1fa3a764e21f16d68af80b697fb9d0eb4f9cd6537393b622906908
d005abe0a29b53c5995a10ce540cc2ffbe96e7f80bf43206d4db7921b6d6aa10
fb3d843d35c66f76b1b1b88260ad20096e118ef44fd94137dbe394f53c1b8a46
6772d2425b5a169aca824de3ff2aac400fa64c3edd93faaabd17d9c721d996c1
f8f2c7020b2d38c806b5911acb373578cbd69612cbe7f21f172550f4b5d02fdb
55426bb348977496189cc6a61b711a3aadde155772a650ef17fba1f653431965
97f3c0beef87b993be321b5af3bf748cc8e003e6e90cf5febf69dfd81e85f581
afd53240a591daf50f556ca952278cf098dbc5b6c2b16c3e46ab5a0b167afb40
10b498562aef754156e2b540754bf1ccf9a9cb62c732bf9b661746dd08c67bd1
2ab8c3a1a7fe14a49084fbf42bbdd04d6379e6ae2c74d801616e2b9cf8c8519c
29f19d9cd8fe38081a2fde66fb2e1eff33c4d4b5714ef5cada5cc76ec09bf2fa
bfcd71a4095c2e81e2681aaf0239436368bc2ebddae7fdc8bb486ffc1040602c
3f920619470488b8c1fda4bb82803f72205b18b1ea31402b461a0b8fe737d6bd
305e220e1f1cb506c32bb509f246515e3cba7ec1dabae95298f358d26654bfa6
2c01734ff63d041a91d10acdb302ef4ffc400396e34140335e4faa2e3f002dbe

KPMG

KPMG Cyber Threat Intelligence Platform

Grandoreiro Trojan – Unveiling the Banking Sector's Nemesis

Indicators of Compromise: Hashes
db883e29daa7a6bfd2b93578ff25546124732c0b3d82b76fe241b07a338bc91a
1bdf381e7080d9bed3f52f4b3db1991a80d3e58120a5790c3d1609617d1f439e
800c1831533a241de65d74040e392d32751e4ab83e98100620b4d6db12aa30c2
91158471341b3dd28b5e77baae17c760b1a7bbb83ba1952624f6f63a4dd3f07e
c65bd36a8c9cbdf57fd3b0f8cec21954b33171c389b8448e9a47043da2b17912
fa4ee29065ca13f70603095ed2bce63362ece4452af31efb1e354b0c928169e7
70430bd264c23fd9b1959b9dd86629534a8c432046d50b7b5d2ff93a3fe33fe1
8d2c34be21c015790dd8be90432f4ae4b5c2611629b3d9ea28fb0934c20c4e83
fb3fafe0620142c8eeffefbfdf88a66d5eddfea05d90d0e55ec9517d9c0c3dda
d17f046256a9996fc3d1596c9f3d84b512d3c3e2bd10d120e18bf82f2f2599f5