KPMG Cyber Threat Intelligence Platform

CR4T Malware - Targeting Government Entities in the Middle East

CR4T, a versatile malware strain, has emerged, targeting government entities in the Middle East through the DuneQuixote campaign. This campaign, discovered in February 2024, distributes new variants of the CR4T malware implant across various organizations in the region. CR4T exists in two strains, coded in C/C++ and Golang, respectively. The malware's main functions include granting attacker's access to infected devices and allowing remote command execution and file transfers.

CR4T uses Windows x64 executable with DLL versions, all in C/C++, as an initial dropper, incorporating Assembler segments, featuring invalid digital signatures. Upon execution, it initiates decoy API calls with Spanish poem snippets, constructs API call structures, and dynamically resolves API calls. The dropper decrypts C2 address using a unique technique involving filename concatenation and hashing for decryption key. After downloading payload, dropper verifies its validity with a "M" magic byte check, masquerading as a legitimate Total Commander installer. Installer dropper includes anti-analysis measures, checking for debugger presence, known research tools, system resources, cursor movement, and disk capacity. CR4T implant aims to grant attackers command line console access, utilizing named pipes for inter-process communication, configuring user agent as "TroubleShooter", and connecting to C2 server. The Golang variant of CR4T shares similar capabilities with the original version, including a command execution and file manipulation, along with persistence via scheduled tasks using the Go-ole library, while adopting Telegram API for C2 communication.

The "DuneQuixote" campaign, exemplified by the CR4T malware strain, showcases versatility, sophisticated tactics, and evasion techniques. Security experts must remain vigilant and adaptable to counter these threats effectively.

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

Indicators of Compromise: Domains	
commonline[.]space	userfeedsync[.]com

Indicators of Compromise: Hashes
3aaf7f7f0a42a1cf0a0f6c61511978d7
5759acc816274d38407038c091e56a5c
606fdee74ad70f76618007d299adb0a4
5a04d9067b8cb6bcb916b59dcf53bed3
48c8e8cc189eef04a55ecb021f9e6111
7b9e85afa89670f46f884bb3bce262b0
4f29f977e786b2f7f483b47840b9c19d
9d20cc7a02121b515fd8f16b576624ef
4324cb72875d8a62a210690221cdc3f9
3cc77c18b4d1629b7658afbf4175222c
6cfec4bdcbcf7f99535ee61a0ebae5dc
c70763510953149fb33d06bef160821c
f3988b8aaaa8c6a9ec407cf5854b0e3b
cf4bef8537c6397ba07de7629735eb4e
1bba771b9a32f0aada6eaee64643673a
72c4d9bc1b59da634949c555b2a594b1
cc05c7bef5cff67bc74fda2fc96ddf7b
0fdbe82d2c8d52ac912d698bb8b25abc
9b991229fe1f5d8ec6543b1e5ae9beb4
5e85dc7c6969ce2270a06184a8c8e1da
71a8b4b8d9861bf9ac6bd4b0a60c3366
828335d067b27444198365fac30aa6be
84ae9222c86290bf585851191007ba23
450e589680e812ffb732f7e889676385
56d5589e0d6413575381b1f3c96aa245
a5574951b352f8ea77a2abea67b96cca92dd7ff0
77efd0a85eb90a616e9823570d22b2b712660721
c0407f6884111dfda621390810860 2ed1760bf30
848559e05fb7f7220763546ce2ae96603880d76f
187c3fc869aff8f89d35a0d04c24976bcbfd439f

KPMG

KPMG Cyber Threat Intelligence Platform

CR4T Malware - Targeting Government Entities in the Middle East

Indicators of Compromise: Hashes
e91e5ac5583526599294780acb1cba9909ab54d8
17ffa01187ce7eef1a2e9a989d21e7b744714064
5aaf9ce8d14811a1aff66fe393c0ba3f99a19c44
44a8c0a99c7c33202501519dea17e94e9416abae
c6d3af73d561dae7713b8f81cf2f03ddcf68d98b
21e15f422ae5fbdbed17161c6ac2bf1718afe13f
eae6debecea22b29251e77386d0dbb50eb18fb07
d91ab96c6a5963962f64d0af3a7fddf7229bbd57
358f8757418c28e9e2a3c17dda180ace60aaa905
dd1f3df3d07754843a58ce9613669fb8a57d83cb
32539b7ade2830b7bf404e1cb85318cd9b81fb66
6312568efa6cc02004acbc77bda6a2ec83e7b945
068e76cb548019d8c9dade1493fdf9343d86d8b9
db7ab88046f162ad5f2ab713dfbbdb23c7c9a8d1
a42a255e1c3d79c317180e2603eb5487c5afc303
d6c77554b9821c6405fe386bd04a799426c8c118
98671bd063cef4d6f3e17c58652c4a88c57701b8
d7cf715b9596abe119e3e6f64026ee05efcd539c
f34b71af24fd1982d0899283c8bfb7b0f1392434
bbea7b0b57b2eb72e0f373f914143a62851ffe65
74db9683f7f0ea511dc37435851b6d77cc4781e4
e3783a51b31b891b2a9720c3cda3f8cd6e7dbe76
b0995830516b85596aee105168f89cde0d1b044f
348bdafa72afdbc1d37ddc4007a964efa953df49
2b69929e1bda591e8178134e92f3e4df5dd13330
0e6072efb087ef19318a03a0509758fe9543222a
bbea7b0b57b2eb72e0f373f914143a62851ffe65
74db9683f7f0ea511dc37435851b6d77cc4781e4
2ee6ef73396acc305a7b7e1765bf147afa68e26e8c9912c7c224b41dbc9eb7b6
63c3ec84fde25125b2dbbba7b8e7bc7367b72f00a947941338724e4b1a68df57
fc96c64173c2df82c2923036e850c0e78e076fb83796871f82037826869715 71
6d7b64f8ea9d7f5c7f89eebe0136bedaa454061a2c1a479398cff55252b4d05e
c3424df8827187cd425335de1038b7ac4e75897c306df9061190af9a89649a4f
4e769cb1ca6f54fc08e84972a64a0889eb7743151372755e9fa6fc614e686f55

KPMG Cyber Threat Intelligence Platform

CR4T Malware - Targeting Government Entities in the Middle East

Indicators of Compromise: Hashes
24d1987571c493e55d8427ffbb77be3c5685dc5a395c58f57455b8d23029d0a8
cdddd4dd5a05a90e709943cc1c1ebbd08e92f75fb0cf643464c4f5292c0137a7
016265214722a400afcddaaaf8b6c71a02dda3de045f9ca595a7eefd579b1e15
30cd168a58c3a6ab2c077a6bf0e9b7ab37077c7f44210224154acdc571900ebb
a2c33c597ecd4a402e3a8ef8e623a7fbb3fd8ae78d34a1e2b6110b8bef0a6b2b
c466b9b6ae1de1666d3047ea2a47497941e3e38cf04d28175901de2ea2ba4fa6
e9f17dcc4537f6812404b32e9e99772ba679948a312c8e9fdf71a0981556e0d6
c2b3f88649148b6ff1770352a9717690d91cddb18195ebaf4a29560843b9e31f
f6e90769296b70c7b925337dc9de43f5c3af5004dd3b6c3aede9ee91de8b4233
54a1b46f4cefe5fa5ac0b9a538da27cdd9dca6e3b6cd512e3c07b3ebd67148d3
b31df45851a4046e51663de55cb1b82efe77e86d67869d92889dd1fde982d3d1
75c9685d1792d949374eceaacdee95235aa86bc55c8dffec150bee768e4e60e3
ec14b9ba9b291f3151a3c0b45304c09b4bcc4576854e9df9ae6208e920e74d75
7d8bec8c8132108dd7c53c341830adb1ce372dc108fabcbdefc5cc42274fb12a
d2c0969437ced872ab124e5ceb0a7f1524063849e4ea6dceb740951c7014cd2c
918f22452999a65b9fdb7ef45906f9a971311fbebe3dc1953aea48a57d4d2816
64b7cfa58b4fb54c984300ffe6c91d93898cd32bea692cadedb5d5f333b91040
2fbe796bacccb20ed30262d0f4428e8e75968d6ff45dc9baf357712231ba7546
8330369176eafb7d636897c427c8357e47bfadcce2acb54001cbd1d7567f55b6
47e7fd9135c7b908711dfc9fe52a667573ab0f342797098cc3bdf88a24c66e7d
6ccfdf185e0812583171f1239bc1cdf1bb48e4e57a1e99518c47804340fe5e76
073bef4b8edc37bb1e7291f79f8deb186c1727c1aaa5205286ca959def4b0136
ec3cc983c91a9acefd707c0d43c144d188ba9e120dc87bcc2649ae7d47557cd0
873f2d7a4ea7c92d637f310cbbbac454f798b6df667996cabe444accbf793a96
64da1f321a6f338dbd753b0ca0a33bab7a1501b38ff7131faa27bf85805655f1
446c20567ef09819ad160537f49efe9f242d8eacde86eb662571c0be56f0a00d
17119d30e63243 4e04d2106cf3d0b361d5c69180550e3db8ef07aa76c5e586dc
72c0b1193e076c682359b3412f2ef124e88c2082c60d58ee939152b0da6742eb
4ed7f0ef2942f48aa3b4a69523506aef2fb74e412a382c3bf4c6f7769bf53da1
da8e8df35bc9eeee004f9fb377996e6f1a6b2ac4309b5a2748ea7c227ef24cfa
f01f9de94f4aa56e5ae6ecde5a7ef97f4e181aac412bb44791ae094d776f1dd1
cc3a7442e1025bca67e12326860c398e7055e89904f211c3324d2b055cf2547d
c21f2a00c33897cc4b06128b90bfbd662eb9763196152bbb2d98ac657e9537c0
8dade177642a50ff101519b159d38a41aedf157df44f0a875310f7f21c2e9808