KPMG Cyber Threat Intelligence Platform

Daxin Backdoor – Over-engineered for Stealth

Daxin, a backdoor malware whose origin dates back to 2013, exhibits a level of technical expertise never witnessed in most cases. Known to be used by Chinese intelligence organizations, it targets companies of strategic importance in manufacturing, transportation and telecommunications sectors of Asia, Africa, etc. With the capability to hijack genuine TCP/IP connections & implement its own communication components, Daxin appears to have been tailor-made for deep infiltration into highly secure networks to be managed from anywhere in the world.

Disguised as a Windows kernel driver, Daxin primarily snatches TCP/IP connections by closely inspecting the system traffic, searching for specific patterns and then cutting off the original process. With the ability to be function as both the initiator and target of a key exchange, it performs a key exchange after capturing the traffic. This enables Daxin to set up an encrypted channel with C2 & exfiltrate data. By impersonating legitimate traffic patters, it gets beyond stringent firewall rules while lowering the likelihood of generating network anomalies. Post establishing comms, Daxin is well equipped with features like persistence, execution of arbitrary DLLs & EXEs and spawning of an interactive shell. Daxin further adopts a radical approach to route traffic between multiple custom selected infected nodes, configurable via a single command. This enables the attacker to craft intricate ways to quickly establish and re-establish connections and access to tightly-controlled networks.

Daxin throws light on the level of sophistication cyber threat groups are moving towards in order to compromise their targets. While attackers gear themselves with special capabilities to even target well-protected networks, organizations must proactively guard themselves by staying up-to-date & following security best practices.

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

Daxin Backdoor – Over-engineered for Stealth

Indicators of Compromise: Hashes
f242cffd9926c0ccf94af3bf16b6e527
bf14555b3a8378ab1276642160b52ffe
79df0eabbf2895e4e2dae15a4772868c
6d131a7462e568213b44ef69156f10a5
4b058945c9f2b8d8ebc485add1101ba5
47e6ac52431ca47da17248d80bf71389
fb7c61ef427f9b2fdff3574ee6b1819b
f242cffd9926c0ccf94af3bf16b6e527
bd5b0514f3b40f139d8079138d01b5f6
b0770094c3c64250167b55e4db850c04
a6e9d6505f6d2326a8a9214667c61c67
8636fe3724f2bcba9399daffd6ef3c7e
79df0eabbf2895e4e2dae15a4772868c
e5f4ec79c3d4cb85732265ff668f852afff5143f
d417c0be261b0c6f44afdec3d5432100e420c3ed
d02403f85be6f243054395a873b41ef8a17ea279
53f776d9a183c42b93960b270dddeafba74eb3fb
37e6450c7cd6999d080da94b867ba23faa8c32fe
25bf4e30a94df9b8f8ab900d1a43fd056d285c9d
1f25f54e9b289f76604e81e98483309612c5a471
064de88dbbea67c149e779aac05228e5405985c7
8302802b709ad242a81b939b6c90b3230e1a1f1e
80a7066e76801dc46bddf637dc558bff3ab37384
73bac306292b4e9107147db94d0d836fdb071e33
731b37eb5154f082911707eab85e69029c590c8d
71469dce9c2f38d0e0243a289f915131bf6dd2a8
6abbc3003c7aa69ce79cbbcd2e3210b07f21d202
53f776d9a183c42b93960b270dddeafba74eb3fb
3b6b35bca1b05fafbfc883a844df6d52af44ccdc
25bf4e30a94df9b8f8ab900d1a43fd056d285c9d
e5f4ec79c3d4cb85732265ff668f852afff5143f
dd6fcbe0e3c6997e3358788c156dc937c72af8a0
cb3f30809b05cf02bc29d4a7796fb0650271e542
c257aa4094539719a3c7b7950598ef872dbf9518

KPMG

KPMG Cyber Threat Intelligence Platform

Daxin Backdoor – Over-engineered for Stealth

Indicators of Compromise: Hashes
a53e46a5d401e8a87fe1520e75ebcbe69ea6e6d1
08dc602721c17d58a4bc0c74f64a7920086f776965e7866f68d1676eb5e7951f
53d23faf8da5791578c2f5e236e79969289a7bba04eee2db25f9791b33209631
7a7e8df7173387aec593e4fe2b45520ea3156c5f810d2bb1b2784efd1c922376
8dafe5f3d0527b66f6857559e3c81872699003e0f2ffda9202a1b5e29db2002e
96bf3ee7c6673b69c6aa173bb44e21fa636b1c2c73f4356a7599c121284a51cc
9c2f3e9811f7d0c7463eaa1ee6f39c23f902f3797b80891590b43bbe0fdf0e51
c0d88db11d0f529754d290ed5f4c34b4dba8c4f2e5c4148866daabeab0d25f9c
e6a7b0bc01a627a7d0ffb07faddb3a4dd96b6f5208ac26107bdaeb3ab1ec8217
5c1585b1a1c956c7755429544f3596515dfdf928373620c51b0606a520c6245a
8d9a2363b757d3f127b9c6ed8f7b8b018e652369bc070aa3500b3a978feaa6ce
b9dad0131c51e2645e761b74a71ebad2bf175645fa9f42a4ab0e6921b83306e3
e7af7bcb86bd6bab1835f610671c3921441965a839673ac34444cf0ce7b2164e
5bc3994612624da168750455b363f2964e1861dba4f1c305df01b970ac02a7ae
b0eb4d999e4e0e7c2e33ff081e847c87b49940eb24a9e0794c6aa9516832c427
06a0ec9a316eb89cb041b1907918e3ad3b03842ec65f004f6fa74d57955573a4
a0ac5f7d41e9801b531f8ca333c31021c5e064f13699dbd72f3dfd429f19bb26
c791c007c8c97196c657ac8ba25651e7be607565ae0946742a533af697a61878
b0eb4d999e4e0e7c2e33ff081e847c87b49940eb24a9e0794c6aa9516832c427
aa7047a3017190c66568814eb70483bf74c1163fb4ec1c515c1de29df18e26d7
8dafe5f3d0527b66f6857559e3c81872699003e0f2ffda9202a1b5e29db2002e
8d9a2363b757d3f127b9c6ed8f7b8b018e652369bc070aa3500b3a978feaa6ce
81c7bb39100d358f8286da5e9aa838606c98dfcc263e9a82ed91cd438cb130d1
7a08d1417ca056da3a656f0b7c9cf6cd863f9b1005996d083a0fc38d292b52e9
7867ba973234b99875a9f5138a074798b8d5c65290e365e09981cceb06385c54
705be833bd1880924c99ec9cf1bd0fcf9714ae0cec7fd184db051d49824cbbf4
6908ebf52eb19c6719a0b508d1e2128f198d10441551cbfb9f4031d382f5229f
53d23faf8da5791578c2f5e236e79969289a7bba04eee2db25f9791b33209631
514d389ce87481fe1fc6549a090acf0da013b897e282ff2ef26f783bd5355a01
49c827cf48efb122a9d6fd87b426482b7496ccd4a2dbca31ebbf6b2b80c98530
447c3c5ac9679be0a85b3df46ec5ee924f4fbd8d53093125fd21de0bff1d2aad
3e7724cb963ad5872af9cfb93d01abf7cd9b07f47773360ad0501592848992f4
1a5c23a7736b60c14dc50bf9e802db3fcd5b6c93682bc40141d6794ae96138d3
0f82947b2429063734c46c34fb03b4fa31050e49c27af15283d335ea22fe0555

KPMG

KPMG Cyber Threat Intelligence Platform

Daxin Backdoor – Over-engineered for Stealth

Indicators of Compromise: Hashes
06a0ec9a316eb89cb041b1907918e3ad3b03842ec65f004f6fa74d57955573a4
0f82947b2429063734c46c34fb03b4fa31050e49c27af15283d335ea22fe0555
3e7724cb963ad5872af9cfb93d01abf7cd9b07f47773360ad0501592848992f4
447c3c5ac9679be0a85b3df46ec5ee924f4fbd8d53093125fd21de0bff1d2aad
49c827cf48efb122a9d6fd87b426482b7496ccd4a2dbca31ebbf6b2b80c98530
5bc3994612624da168750455b363f2964e1861dba4f1c305df01b970ac02a7ae
5c1585b1a1c956c7755429544f3596515dfdf928373620c51b0606a520c6245a
6908ebf52eb19c6719a0b508d1e2128f198d10441551cbfb9f4031d382f5229f
7867ba973234b99875a9f5138a074798b8d5c65290e365e09981cceb06385c54
7a08d1417ca056da3a656f0b7c9cf6cd863f9b1005996d083a0fc38d292b52e9
8d9a2363b757d3f127b9c6ed8f7b8b018e652369bc070aa3500b3a978feaa6ce
b0eb4d999e4e0e7c2e33ff081e847c87b49940eb24a9e0794c6aa9516832c427
b9dad0131c51e2645e761b74a71ebad2bf175645fa9f42a4ab0e6921b83306e3
cf00e7cc04af3f7c95f2b35a6f3432bef990238e1fa6f312faf64a50d495630a
e7af7bcb86bd6bab1835f610671c3921441965a839673ac34444cf0ce7b2164e
ea3d773438c04274545d26cc19a33f9f1dbbff2a518e4302addc1279f9950cef
81c7bb39100d358f8286da5e9aa838606c98dfcc263e9a82ed91cd438cb130d1
06a0ec9a316eb89cb041b1907918e3ad3b03842ec65f004f6fa74d57955573a4