KPMG Cyber Threat Intelligence Platform

Andariel Group - North Korea's Advanced Cyber Warfare Tactics

Andariel (aka Onyx Sleet, APT45, DarkSeoul, Silent Chollima, and Stonefly/Clasiopa) is a North Korean state-sponsored cyber group under the RGB 3rd Bureau. Evolving from destructive attacks to focus on cyber espionage and ransomware, the group targets defense, aerospace, nuclear, and engineering sectors, along with medical and energy industries. Their operations affect entities in the U.S., Japan, India, and globally, with funding from ransomware attacks on U.S. healthcare.

Initial access is gained by exploiting web server vulnerabilities to deploy web shells and access sensitive data, leading to breaches via public-facing devices. Once inside, actors use native tools like Windows command line, PowerShell, WMIC, and Linux bash for system and network enumeration, favoring netstat. They evade detection by packing tools with VMProtect and Themida, resulting in large files with unusual section names. For privilege escalation, they use Mimikatz, ProcDump, and Dumpert to dump credentials, target NTDS.dit, and leverage vssadmin or registry data for offline extraction. Custom .NET tools are employed to enumerate directories, gather file details, and use SMB for file enumeration. They collect system logging data, including active window changes and clipboard data, and use RDP for network traversal. Malware is disguised in HTTP packets, with traffic routed through tunneling tools (3Proxy, PLINK, Stunnel) and custom proxies to C2 servers. Data is archived in RAR files (sometimes with malicious WinRAR), exfiltrated to cloud storage or secondary servers, and transferred to North Korean servers using PuTTY, WinSCP, and FTP, with RDP connections or HTTP GET requests for data retrieval.

Andariel's sophisticated toolset, advanced evasion techniques, and complex exfiltration methods underscore the need for stringent patching, and advanced threat detection to mitigate the risk.

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
Partner. KPMG in India
T: +91 98181 99432
E: mtembhurkar@kpmg.com

KPMG

KPMG Cyber Threat Intelligence Platform

Andariel Group - North Korea's Advanced Cyber Warfare Tactics

Indicators of Compromise: Domains
beebeep[.]info

Indicators of Compromise: Hashes
c8346b39418f92725719f364068a218d
ecb4a09618e2aba77ea37bd011d7d7f7
977d30b261f64cc582b48960909d0a89
730bff14e80ffd7737a97cdf11362ab5
c7b09f1dd0a5694de677f3ecceda41b7
e53ca714787a86c13f07942a56d64efa
f8aef59d0c5afe8df31e11a1984fbc0a
7aa132c0cc63a38fb4d1789553266fc7
4156a7283284ece739e1bae05f99e17c
3026d419ee140f3c6acd5bff54132795
1a0811472fad0ff507a92c957542fffd
0984954526232f7d05910aa5b07c5893
eb7ba9f7424dffdb7d695b00007a3c6d
e7fd7f48fbf5635a04e302af50dfb651
a2aefb7ab6c644aa8eeb482e27b2dbc4
33b2b5b7c830c34c688cf6ced287e5be
073e3170a8e7537ff985ec8316319351
13b4ce1fc26d400d34ede460a8530d93
fe25c192875ec1914b8880ea3896cda2
dc70dc9845aa747001ebf2a02467c203
ca564428a29faf1a613f35d9fa36313f
c2f8c9bb7df688d0a7030a96314bb493
c1f266f7ec886278f030e7d7cd4e9131
ad6d4eb34d29e350f96dc8df6d8a092e
49bb2ad67a8c5dfbfe8db2169e6fa46e
bda0686d02a8b7685adf937cbcd35f46
bbaee4fe73ccff1097d635422fdc0483
95c276215dcc1bd7606c0cb2be06bf70
8c2b77c32b334164532571d80284037a92556524
1df16f8bb6068e5f65f0a9a3613cc31fe5321a8d

KPMG

KPMG Cyber Threat Intelligence Platform

Andariel Group - North Korea's Advanced Cyber Warfare Tactics

Indicators of Compromise: Hashes
10408e6cf829699f0eb4c5199575261db14fee66
6ff55c00a1c09ccd6af7727d526e21ca969e0af0
232106cbc0feb6aeab2816a6535e81a0fa16243b
74b37080adf8482d25917f1823eb02aa04a2659c
3173031bf8b3ed00863aa5a4fdb6e21ef8089b22
d27f94701c8f588748ee9115b194e4664990969c
393ec0051c457f199c406d5771d276754fa29e3b
dfe5d75ed31b6cfc2cceebb1404d3eabc02f0021
a100daa33d7db6d2424ac1a8c9ec4b3ae8a3105c
4a0507273603c8dfcfaa44724cd348179b90e02e
0f3b24e4e3e44bf60c5aad5b457fd8e0f6836c29
baa104cb2c73289ab890a94d54c39de7710ea1aa
b1c0b42a6b64536dfb825a7a7b029a1c72060167
0a00a6711b190bc7e3a0f2fdfa2351271ba53252
97e9c7091a7275655d0e44559a3df6d5a0cf21d9
eab52df44d91dfc53163c176c1e3722c73f3b4f7
ee11f6ecfd03105e79b4ac44ca8583c71842b1cf
926bfb37f292c1f4e37b1ad00b9edd7d4ee557d9
3b49d20f726a8b4209827f3fc8dbf6b971297c90
b365bed712582b3792096ff389e1755ff99a1f7e
46a06581c2751a423568e308d19188de7185ce16
c054cf1e19526fcbf228ba0c12a176632ee36a52
87cf92b22593d21434530449d1b08367e98a077b
01ba053236c0d9a78e4ec9f09a0ae5b16459a239
fb70e2fd6dc61b5681d8de373b98ac534d8ec41b
cf8d86010759c618757fecfb9854b1e20d31bd86
343ba35278079832b940b825bc029e92bef14c04
38c293caea82d25dbf7eb898dba0fc44ee32c32d
3b665481a57096c026c5dcb62be17eb1714dc4c0
e1ff89f8b2830778ee9bdae64ab94fc64d16af5a
8bab70bdfb7f8df0356727d9cb3c6024acb383a2
9a5504dcfb7e664259bfa58c46cfd33e554225daf1cedea2ec2a9d83bbbfe238
aa29bf4292b68d197f4d8ca026b97ec7785796edcb644db625a8f8b66733ab54
2a1b556770982acd711188821bfd90bb7a3eb2a977232303d7e64ba0b8682934

KPMG

KPMG Cyber Threat Intelligence Platform

Andariel Group - North Korea's Advanced Cyber Warfare Tactics

Indicators of Compromise: Hashes
51deba8b044183574fe7e381f194a8c9d6ececcb1a1730f5dcd63252c5b07939
4df7b87bd5fa5994b9e42981ea16afd0219a745205c8f8dec593725f9d5e3e92
7df30215533194a5003bbd3cb2dce23c524a6f8d4d20ae01d6b9ad32484c6d96
4aadf767491077ab83c6436cf108b014fc0bf8c3bd01cc6087a0f2b80564bc08
772b06f34facf6a2ce351b8679ff957cf601ef3ad29645935cb050b4184c8d51
34d5a5d8bec893519f204b573c33d54537b093c52df01b3d8c518af08ee94947
0996a8e5ec1a41645309e2ca395d3a6b766a7c52784c974c776f258c1b25a76c
588cdbd3ee3594525eb62fa7bab148f6d7ab000737fc0c311a5588dc96794acc
664f8d19af3400a325998b332343a9304f03bab9738ddab1530869eff13dae54
2c077e619e42318b22a1835cc625eb4389245786aacf584303d3184f234dfea2
069989db9d006c09d735c702a552a26456e6c77d023cea1ff94259df1923496f
175fad19a29374f183ddc1938787255c59a34512c29fa198267421bd76112e29
5f71d7511bdd0b236d05b35396eddc20eae57ab2561f09ff62f212f32ef310cc
eb0855e107dd516366bd23c685d78360d0a52a18fe18d029093bb2a93c0234b0
0400905f1024823618712b920b5f0fbb0b024a768690e6345104e2a0cca39612
490f1934035671fce949f631e08a8ef1153eb485a5b73545f3aac63ea62880a3
0c5e0a81efc0ccc406e5e6eaa222a79b491f4aa2938cf7cc72d0d027b53a9d99
0e416e3cc1673d8fc3e7b2469e491c005152b9328515ea9bbd7cf96f1d23a99f
1177105e51fa02f9977bd435f9066123ace32b991ed54912ece8f3d4fbeeade4
152743ffa9df246e5f8c5687381121d8a66dfc05ca2ec2e58000caf964abafc2
16db0063e4aa666d94752414549fa09fb33142481d894b01a0fae45b339a09fb
2e500b2f160f927b1140fb105b83300ca21762c21bb6195c44e8dc613f7d7b12
2eb16dbc1097a590f07787ab285a013f5fe235287cb4fb948d4f9cce9efa5dbc
3cf63d516c580d8f988aa4f9b7d482bbdf3901dce435356dbca83eb311c32382
42daf0f3080b50a0a1f14291f5ae3fa8fa400d838a915618f68a8f059777bcd4
4e5e42b1acb0c683963caf321167f6985e553af2c70f5b87ec07cc4a8c09b4d8
58fef66f346fe3ed320e22640ab997055e54c8704fc272392d71e367e2d1c2bb
60425a4d5ee04c8ae09bfe28ca33bf9e76a43f69548b2704956d0875a0f25145
6319102bac226dfc117c3c9e620cd99c7eafbf3874832f2ce085850aa042f19c
655aa64860f1655081489cf85b77f72a49de846a99dd122093db4018434b83ae
6ca3c2a6001f1149ff75ab46402dee40d97602bab0b43ac144ca70fbd2101404
782791c9ec3550cd522fd27b992e75381d5c5bc4d95b2f3934f9af6b6d5a57f4
789c3aeb31700b078f6449cb310b4a2b7d8c03aefeed46a69b1dcb40a18001a7
846c2a02505dc1463019cabc021969f7f6095215efb63ec374da1d055e778390

KPMG

KPMG Cyber Threat Intelligence Platform

Andariel Group - North Korea's Advanced Cyber Warfare Tactics

Indicators of Compromise: Hashes
8aa6612c95c7cef49709596da43a0f8354f14d8c08128c4cb9b1f37e548f083b
8bc74559c3678d299826755f29d5ba75b1148b0f8d1fa71a120b2f879f85f08b
90fb0cd574155fd8667d20f97ac464eca67bdb6a8ee64184159362d45d79b6a4
a0a0b0dd33b5b685317f6abe7b4caf0610938f548f6d178919bf43c24e1a3a4b
a1990d863e0b5c7661358dab72ce9223e2d54570915105707374ea8cf68828bd
ac5e0ec03658a281bb57e8b1b17f1fa1da2c819a373524577459c63b0b9d9a75
afb2d4d88f59e528f0e388705113ae54b7b97db4f03a35ae43cc386a48f263a0
b7435d23769e79fcbe69b28df4aef062685d1a631892c2354f96d833eae467be
c28bb61de4a6ad1c5e225ad9ec2eaf4a6c8ccfff40cf45a640499c0adb0d8740
c8fb5988ad3f71412cb5b4f1248df7ddf82c8c5f3dce60c73c4787b6e443b7b0
c9724eecab6cfb1c312d4538630fdac0d30434c0cffa131f9190e5a76bef6304
cb4d45338798b97177d8d96eea82dae22481dada40174dda0386026d11136209
d30abdf9db88da8a23dccb8188cd4caff48bc437bb3eb3ad576a013ff675161a
e263aa0e7e6a6a1d59677eaf2d4ccb848fe65a84035ab4f24c4e26a1ab089c79
e8e61112e8b896ad00ddefb42feb33e5d0fc38d2fb462b9f980606fe79d42571
ed8ec7a8dd089019cfd29143f008fa0951c56a35d73b2e1b274315152d0c0ee6
f5f6e538001803b0aa008422caf2c3c2a79b2eeee9ddc7feda710e4aba96fea4
f67ee77d6129bd1bcd5d856c0fc5314169b946d32b8abaa4e680bb98130b38e7
f93ddb2377e02b0673aac6d540a558f9e47e611ab6e345a39fd9b1ba9f37cd22
66415464a0795d0569efa5cb5664785f74ed0b92a593280d689f3a2ac68dca66
1962ebb7bf8d2b306c6f3b55c3dcd69a755eeff1a17577b7606894b781841c3a
f226086b5959eb96bd30dec0ffcbf0f09186cd11721507f416f1c39901addafb
6db57bbc2d07343dd6ceba0f53c73756af78f09fe1cb5ce8e8008e5e7242eae1
830207029d83fd46a4a89cd623103ba2321b866428aa04360376e6a390063570
45d8ac1ac692d6bb0fe776620371fca02b60cac8db23c4cc7ab5df262da42b78
5b7ecf7e9d0715f1122baf4ce745c5fcd769dee48150616753fec4d6da16e99e
199ba618efc6af9280c5abd86c09cdf2d475c09c8c7ffc393a35c3d70277aed1
fc36ef795b06bfa82620095be881d1d5c56709155e447f62baee60c189cb2b09
d68036a30b99e8beba1c3aa52b6c5986eee823c21699a24d9af7022eaa9190ac
18b75949e03f8dcad513426f1f9f3ca209d779c24cd4e941d935633b1bec00cb
8ce219552e235dcaf1c694be122d6339ed4ff8df70bf358cd165e6eb487ccfc5
dda53eee2c5cb0abdbf5242f5e82f4de83898b6a9dd8aa935c2be29bafc9a469
c2904dc8bbb569536c742fca0c51a766e836d0da8fac1c1abd99744e9b50164f
b9af4660da00c7fa975910d0a19fda072031c15fad1eef935a609842c51b7f7d