KPMG

KPMG Cyber Threat Intelligence Platform

Bitter APT : An Intelligence Accumulator!

T-APT-17 (a.k.a Bitter APT or APT-C-08) is suspected to be a South Asian espionage-focused threat group. Active since 2013, the threat actor has been primarily targeting energy, engineering and government sectors in China, Pakistan and Saudi Arabia in the past few years. Known for targeting both mobile and desktop platforms, Bitter APT effectively exploits known vulnerabilities in victim's environments leveraging RCE for lateral movement. In their latest operation, the threat actor has drawn out its target to Bangladeshi government entities.

In a recent attack, the threat actor targeted the Rapid Action Battalion (RAB), a unit of the Bangladesh police force, via spear phishing emails. The spoofed email addresses were used to impersonate Pakistani government organizations, containing either a malicious RTF document or an MS Excel spreadsheet. Once the weaponized document is opened, the "Equation Editor" application gets launched, which then runs the embedded objects containing the shellcode to exploit MS Office vulnerabilities (CVE-2017-11882, CVE-2018-0798 and CVE-2018-0802). This downloads and executes the trojan from Command & Control servers into the victim's machine. The trojan "ZxxZ" used by the group is deployed in the affected systems which masquerades itself as a windows security update service, subsequently allowing remote code execution by the threat actors alongside the installation of other custom malware tools.

Provided the advanced techniques, tactics and procedures with which Bitter APT emerged again, organizations should adapt a layered defense strategy and robust endpoint defense plan inclusive of matured incident response plans in order to sustain and survive the ever-growing complexities of these threat actors.

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

Sony Anthony
Partner, KPMG in India
T: +91 98455 65222
E: santhony@kpmg.com

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

B V, Raghavendra
Partner, KPMG in India
T: +91 98455 45202
E: raghavendrabv@kpmg.com

Chandra Prakash
Partner, KPMG in India
T: +91 99000 20190
E: chandraprakash@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 endeavour 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

KPMG

KPMG Cyber Threat Intelligence Platform

Bitter APT : An Intelligence Accumulator!

Indicators of Compromise: IP Addresses	
82.221.136[.]27	27.136.221[.]82

Indicators of Compromise: Domains	
urocakpmpanel[.]com	tomcruefrshsvc[.]com
autodefragapp[.]com	levarisnetqlsvc[.]net
mswsceventlog[.]net	helpdesk.autodefragapp[.]com
olmajhnservice[.]com	

Indicators of Compromise: Hashes
5e5201514800509b2e75a3fcffad7405
527dc131149644af439e0e8f96a2c4eb
2c8ed4045b76a1eca8c8d0161a4b65ec
2a340b72e16fb1ece13d7f553ec3c266
2454a5b5f7793d372c96fd572c1de2cc
bdbbd70229591fb1102365f4bb22196b
b9025eca96614a473e204e9e8a873e1d
3f45d49bdb6afceb670978cf98f5c2be
25a16b0fca9acd71450e02a341064c8d
72a7130e98119ecd70c4e0f6ce9c0030
bf51119c8b0673a9cfee1c384d1e236a
59b043a913014a1f03258c695b9333af
5e5201514800509b2e75a3fcffad7405
527dc131149644af439e0e8f96a2c4eb
2c8ed4045b76a1eca8c8d0161a4b65ec
2a340b72e16fb1ece13d7f553ec3c266
0cbf8c7ff9faf01a9b5c3874e9a9d49cbbf5037b
25092b60d972e574ed593a468564de2394fa008b
4fbde39a0735d1ad757038072cf541dfdc65faa3
5a972665b590cc77dcdfb4500c04acda5dc1cc4e
530f597666afc147886f5ad651b5071d0cc894ba
04a75df9b60290efb1a2d934570ad203a23f4e9c
aeb02ac0c0f0793651f32a3c0f594ce79ba99e82
b12e459dd3857f5379ac99e48def4ad2b8a3aa16

Indicators of Compromise: Hashes
bcd7a2191af9ddb1bd627e36a55fc55680e36f51
b17f0381fc7e4c4c6bb15dfcc0c37d2945266c6e
7a94a3dcd68792877a4ca8747e23ec084b12da16
3ba50221785aa8d1f2dea2894fc9a9449e826724
33f7efb563052da4d25405dd7f0366bb3bff5b26
81f6de303c0e9279744bb1a00e70ea62428bf28e
826334eb7990950f7e154d2494cc12437723aad2
d297031f13599df567b3b8c1ed1cb7cd32bf758d
3d540373b74ed12df6b21e1ea21566907fba04a1
2af2dcd9482a281228d987723640203e08ff93c9
33f7efb563052da4d25405dd7f0366bb3bff5b26
3ba50221785aa8d1f2dea2894fc9a9449e826724
b17f0381fc7e4c4c6bb15dfcc0c37d2945266c6e
7a94a3dcd68792877a4ca8747e23ec084b12da16
b0b687977eee41ee7c3ed0d9d179e8c00181f0c0db64eebc0005a5c6325e8a82
f7ed5eec6d1869498f2fca8f989125326b2d8cee8dcacf3bc9315ae7566963db
490e9582b00e2622e56447f76de4c038ae0b658a022e6bc44f9eb0ddf0720de6
b7765ff16309baacff3b19d1a1a5dd7850a1640392f64f19353e8a608b5a28c5
ce922a20a73182c18101dae7e5acfc240deb43c1007709c20ea74c1dd35d2b12
e4545764e0c54ed1e1321a038fa2c1921b5b70a591c95b24127f1b9de7212af8
fa0ed2faa3da831976fee90860ac39d50484b20bee692ce7f0ec35a15670fa92
3fdf291e39e93305ebc9df19ba480ebd60845053b0b606a620bf482d0f09f4d3
69b397400043ec7036e23c225d8d562fdcd3be887f0d076b93f6fcaae8f3dd61
90fd32f8f7b494331ab1429712b1735c3d864c8c8a2461a5ab67b05023821787
7b64a739836c6b436c179eac37c446fee5ba5abc6c96206cf8e454744a0cd5f2
26b3c9a5077232c1bbb5c5b4fc5513e3e0b54a735c32ae90a6d6c1e1d7e4cc0f
1a749857e726960a8d36df68a459f973dffdc8ed2ac9f38d097154ab7ab462bc
522e4d8a0006b6c4c97c2933d139fd4a76179b4956673796336cff1a2eb8e615
8baeed906fa01b6724a436b521f756c2970615817a8cbf7d747fb7ca9aaae7a6
dcf5ea6163e7508c44756b6727061743db1ee778692f1532bb53ea8cd1d15666
ce439ac52c5c69769ea087f6b601099fc8105ca9feb8615283ade76d46457742
37df0b604e142565cdf64304655c13b53474cf8240abd2de9a6efc37660acf4d
c2f962ded401fe1d00a71a8c4363129f7ffd4f184d997c6daa36d66560ddedf9
7d1cd9303a5db4827d3a4de272d7a7b44ab34a2417e04f77c40682f28b086575

Indicators of Compromise: Hashes
ceb2fad16f86f8d9dd968e74240a0efefe004b5a7e3f9402ca76eb378e1dda24
73e5a29f48d5ab979eeda062493bc7e679265c1344ef936978b8becec5549497
0bfb6916497e74aeb944005bd7924f9b56f0e487cf5a8be6a13b1bfc0eb2aa2c
e1a9434ff6776798131d886c89777b32c0e1d084500034a36b917b8d565907b1
aa1153624625a359e5598e2669574a47d43dac2ef4a0238508937c29a7d50c9e
c486aa375053cb9d51d128584441ec32e57d61d4393e0844aa7b5f66c7d30415
d138b1df68a86bbe22d1e86ccbcf4ae23a18910e6e62b3387268bcefde078036
425fc8da0481281a7bea2ab1fba434cdc861cdc4e89e47aee03bc1a0fb43f440
681d3ba69e09bcd91f7b05b317a29b1d817f2aeedf99ea7ccd30b2400d33af98
6a050cfc05f09f34e8f7d50d4d2c49eb894379029d4d23f108ba0ef263ce511c
08e69c236af9e5029205ab97f9749d4b68fe2ec80440faab84749b0dd1cdd003
cb22f2f6de284d8c92aeb828e718c0308db6bb0700208689c49189c166554339
3992d5a725126952f61b27d43bd4e03afa5fa4a694dca7cf8bbf555448795cd6
bd0d25194634b2c74188cfa3be6668590e564e6fe26a6fe3335f95cbc943ce1d
156137ac2d7fae74e0286df47c4d1c75e65d5ef1455ff74c4d46176aef06fe56
02f94213b97792c83aff874ce2c60ac1f1663f4922ed1ac4e31584e8fff265c1
2de1fc9c48c4b0190361c49cdb053fd39cf81e32f12c82d08f88aec34358257f
0f367fabd244a7863e3e7d3e23e42980fb04b6c7f0a82356a8c7b015bb76f8d3
995593528c135f50aaf7450a5c6f29612db0f3dfa7b289b066ea8635168b5502
45668e0f6f64f860a161c0989b31c194067f3ea50a4bdd75153e3fa464b33f69
c2bc809c0ea0c282996b77dd06441372b88b233420918f0fbf85ce13ba97bcd3
d865dd12c7536090f02f683aba5de590827881f272794433354da9c6c4df5512
419a292da3fd4fbee0e073c39d6cc37b7e4fa030ef486490f6ad8237519eded8
01124b062f2174e956273ad51b00ac4b6fc27c3b11cefdd57ccc5a3819003bce
60ca1ffcf67457bab82b81f21ee94ca947dc99c8a077df1398db489a7cee22b5
03e10918feef8b8dea594d26451aad7d595cd3f79fc6c8b25339e8fce2ddaee7
530ffd2f48256dd3dfc5fa7506d687e472caae34c268947db76bd9d808bfb9f3
9002ee844223b30a88e26d7a1a4223656cbe002537596b111cee0ea760557e42
c828c759bc826c5f510052d632027c4c9979e45c2be00e42b9d9b2f1bb7fd579
de9555dbe0b9b1459ef4daddc4f60b73d68685185caf51fa91ceaf4483e239a6
e88cd35f0fb89d4d03534de7b4f82786ef0f0a2ea4b611f2801beac6ff852362
6fc6460dd3f1852fce3aa213ee7850193d3e8829ab76729df5d3f461f85ac671
5aa0d7817105bea29bf56ccf62db63e2217719d192e1f7f66ae55922fb4c3725
255a65d30841ab4082bd9d0eea79d49c5ee88f56136157d8d6156aef11c12309