coordinates

cor. Security Operations Center

CYBERSECURITY ACTIVITY REPORTING

Prepared for: ATOMZ
Recurrence: Monthly
Version: Sample Report
Date: 31-DEC-2018

coordinates

cor. Reporting

REPORT INFORMATION

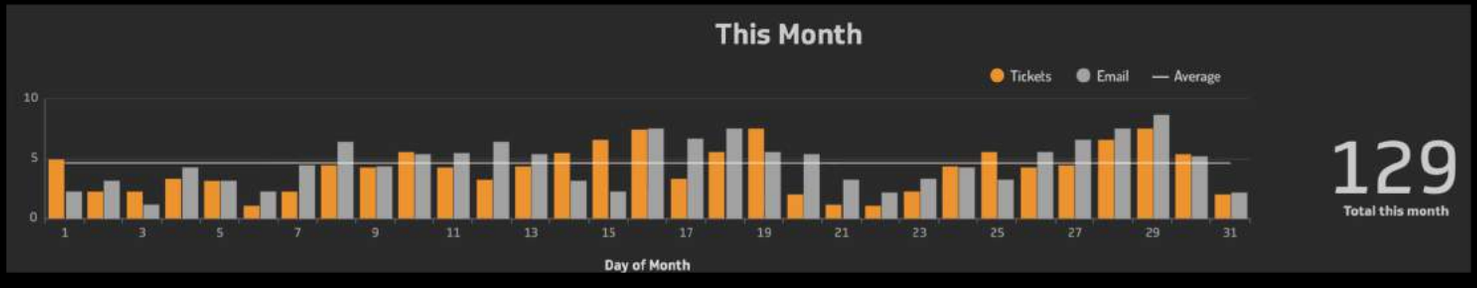
Report #	COR-M-1957
Time period	01 DEC 2018 – 31 DEC 2018
Prepared for	ATOMZ

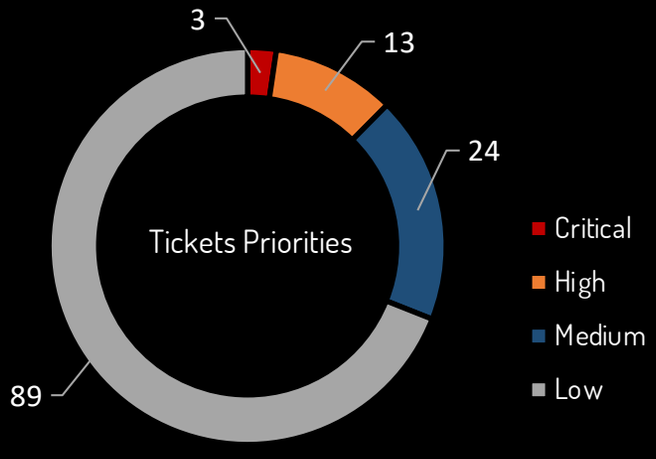
Threat Level

04 / 10

TICKETING INFORMATION

129	4	10	115
Total # of ticket(s) within the period	Open ticket(s)	Pending ticket(s)	Closed ticket(s)





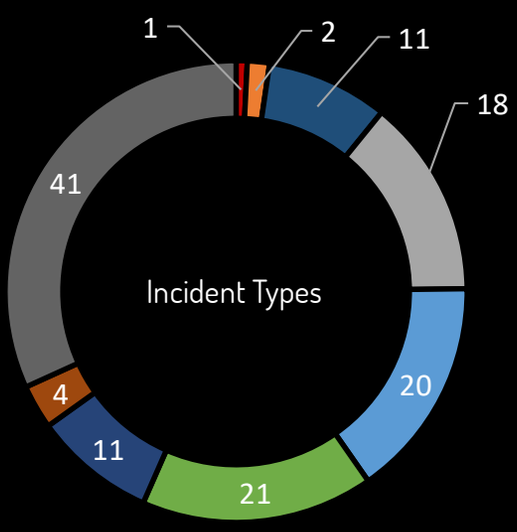
Severity

	Open	Pending	Closed
Critical	0	0	3
High	0	1	12
Medium	1	3	20
Low	3	6	80

coordinates

cor. Reporting

INCIDENTS INFORMATION



- Credential Theft
- Malware Post Compromise
- Inbound Exploit
- Policy Violation
- Brute Force Attack
- Pre-Compromise Malware
- Inboud Web Attack
- Adware
- Phishing

Trends

Incidents
Up **20.56%** from last month

Phishing attempts
Up **32.12%** from last month

Critical incidents
Down **37.14%** from last month

High Severity incidents
Down **53.00%** from last month

Top incidents

Incident	Severity	Date	Ticket ID	Status
High Severity Non Cisco IPS Exploit	High	03-12-2018	#11001957	Resolved
Exfiltration Large Outbound Transfer (cor. v1.0)	High	05-12-2018	#11001997	Resolved
Inbound Brute Force Attempt SSH Protocol (cor. v1.0)	High	12-12-2018	#11002218	Resolved
Internal Excessive Denied DNS Queries (cor. v1.0)	Medium	11-12-2018	#11002057	Resolved
Multiple Logon Failures Misc. App (cor. v1.0)	Medium	08-12-2018	#11002001	Pending
DNS Unauthorized Server Detected (cor. v1.0)	Medium	14-12-2018	#11002332	Resolved
MCASB Failed Login (cor. v1.0)	Medium	18-12-2018	#11002401	Resolved
Excessive Repeated DNS Queries To Same Domain (cor. v1.0)	Medium	12-12-2018	#11002119	Resolved
Outbound Unsecure Protocol Usage From Non Guest Network	Medium	03-12-2018	#11001956	Resolved
Excessive End User Mail (cor. v1.0)	Medium	22-12-208	#11002589	Resolved
Internal Sudden Increase in ICMP Requests	Medium	24-12-2018	#11002592	Resolved
Unauthorized SSH Attempt Detected On FW (cor. v1.0)	Medium	02-12-2018	#11001923	Open
CASB Log ON Detected from unusual country (cor. v1.0)	Medium	28-12-2018	#11002601	Pending
DHCP Unauthorized Server Detected (cor. v1.0)	Medium	30-12-208	#110026032	Resolved
Rogue or Unsecure AP Detected	Medium	11-12-2018	#11002033	Resolved

For More information, Kindly access your cor. live Dashboard

Automatically generated by cor.

MALWARE DATA

Top Infected devices

Computer Name	User Name	Malware Name	Malware Type	Filename
ASI004	orlando.marizo	Android/Hiddad.HI!tr	Virus	Oka Saraina Niku Status.apk
ASI007	ASI	Android/DrdDream.BI!exploit	Virus	360.zip
ASI034	vakumar.thushi	Adware/Hiddad!Android	Virus	video_player_3gp.apk
ASI036	alice.johnny	Adware/Mocean!Android	Virus	Seethamma Chettu Bgms Hd P.apk
ASI036	jinth.pankaj	Android/Hiddad.HI!tr	Virus	76f356-4ab2-8100-29dc63174f42.apk
ASI053	pradeep.prabata	Android/Piom.WYC!tr	Virus	IDM.P1.ArabLionZ..BY.ELOSTOORA.rar
ASI060	bishoy.george	Riskware/Patcher	Virus	vcds_12.exe.rename
ASI061	satheesh.swamy	W32/Kryptik.GKZJ!tr	Virus	indian_wife_college.apk
ASI063	vineesh.vishwa	Android/Generic.Z.8ADBDF!tr	Virus	Oka Saraina Niku Gurthosthana.apk
ASI069	jennifer.luctu	Adware/Hiddad!Android	Virus	Chettu Bgms Micky J Meyer.apk
ASI101	prancis.antoine	Adware/Hiddad!Android	Virus	video_player_3gp16.apk
ASI115	jithin.pankaj	Adware/Hiddad!Android	Virus	816ea92a1-b2cf-9021c4e73606.apk
ASI122	michael.markez	Android/Generic.Z.91C090!tr	Virus	Na Manasuni Status Song.apk
DESKTOP-06AIE50	hany.bassoul	Android/Hiddad.HI!tr	Virus	new_song.mp3.apk
DESKTOP-0D5N9BK	mohammed.fahmy	Android/Hiddad.HI!tr	Virus	Yoanime__Nichijou__7.exe.rename
DESKTOP-3BVFRFK	bhupinder.singh	W32/Kryptik.GKZJ!tr	Virus	YourTemplate.2b981aee30e22f817.exe
DESKTOP-4B5H1VA	alex.kallivalappil	FSA/RISK_MALICIOUS	Virus	FromDocToPDF.593aca1a012ef701.exe
DESKTOP-7ATAUES	michael.milad	Adware/Agent	Virus	YourTemplateFinder.210d90ee0c.exe
DESKTOP-9900FLG	david.zakit	Adware/Agent	Virus	f818c22b828273a010eef16260fac9f2

For More information, Kindly access your cor. live Dashboard

* * * * *

coordinates

CLOSING THE GAP IN THE FIGHT AGAINT CYBER THREATS