From: 08-Feb-2023 18:00 IST

To: 09-Feb-2023 18:00 IST Monitored by: SOC Team

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Sl. No. | Risk | Alert Category | Description | Tool | Action taken | Status |
| 1 | Medium | **Network | Suspicious Network Activity** | Observed inbound traffic from malicious source IP **88.214.26.9** from untrusted location – **Seychelles**, towards 182.66.250.38 over port 443 and we noticed that **Bangalore-Firewall** is allowing the traffic where the action is **start, client-rst** | LogRhythm | Raised Support Ticket to block the IP.  Request# 156802 | Closed |
| 2 | Medium | **O365 | Phish/Spam Email** | Found an email send from **sharandaow@taksheelimpex.com** to **admin.backoffice@qualitestgroup.com** contains malicious URL’s. the mail is from external domain(“**taksheelimpex.com**”).  **Sender**: sharandaow@taksheelimpex.com  **Recipient**: admin.backoffice@qualitestgroup.com  **Subject**: horst froehlich trump hat keinen sex? | LogRhythm | SOC team have validated the email and found it as malicious, requested O365 team to not to release. | Closed |
| 3 | Medium | **O365 | Phish/Spam Email** | Found an email send from **email\_accountsever@proton.me** to[**jonathan.berger@qualitestgroup.com**](mailto:jonathan.berger@qualitestgroup.com) **,**the mail is from an external domain and the link it is redirecting to a fake Qualitest page asking for credentials.  **Sender**: email\_accountsever@proton.me  **Recipient**: jonathan.berger@qualitestgroup.com  **Subject**: account expiration notification qualitestgroup.com | LogRhythm | SOC team have validated the email and found it as malicious, requested O365 team to not to release. | Closed |
| 4 | Medium | **O365 | Phish/Spam Email** | Found an email send from **ak@kpg99.in** to **chris.wilmot@qualitestgroup.com** contains a malicious URL and attachment, the mail is from an external domain(“kpg99.in”).  **Sender**: ak@kpg99.in  **Recipient**: chris.wilmot@qualitestgroup.com  **Subject**: january salary statement | LogRhythm | SOC team have validated the email and found it as malicious, requested O365 team to not to release. | Closed |
| 5 | Medium | **O365 | Phish/Spam Email** | Found an email send from **bounces+srs=oc9qn=6e@olenick.com** to **cameron.leblanc@qualitestgroup.com**, the mail is from an external domain which is suspected of email spoofing via **selvesgame.com**.  **Sender**: bounces+srs=oc9qn=6e@olenick.com  **Recipient**: cameron.leblanc@qualitestgroup.com  Subject: bill reminder #72216 | LogRhythm | SOC team have validated the email and found it as malicious, requested O365 team to not to release. | Closed |
| 6 | Medium | **O365 | Phish/Spam Email** | Found an email send from **andromedauk@pocoshocktradecenter.com** to **joshua.bell@qualitestgroup.com** the mail is from an external domain pocoshocktradecenter.com.  **Sender**: andromedauk@pocoshocktradecenter.com  **Recipient**: joshua.bell@qualitestgroup.com  **Subject**: joshua bell, hat messi erektionsschwierigkeiten? | LogRhythm | SOC team have validated the email and found it as malicious, requested O365 team to not to release. | Closed |
| 7 | Medium | **O365 | Phish/Spam Email** | Found an email send from **Lauraannx@bdro.org** to **soudabeh.ajiri@qualitestgroup.com** the mail is from an external domain bdro.org and  **Sender**: Lauraannx@bdro.org  **Recipient**: soudabeh.ajiri@qualitestgroup.com  **Subject**: soudabeh ajiri bestellen sie per diskreten Bank- berweisung | LogRhythm | SOC team have validated the email and found it as malicious, requested O365 team to not to release. | Closed |
| 8 | Medium | **O365 | Phish/Spam Email** | Found an email sent from **bounce+53a3e2.ec86b-tali=qualitest.co.il@mg.wuthqa.net** to **shail@qualitestgroup.com**. The mail is from an external domain (mg.wuthqa.net) .  **Sender**: bounce+53a3e2.ec86b-tali=qualitest.co.il@mg.wuthqa.net  **Recipient**: shail@qualitestgroup.com. And erez.cohen@qualitestgroup.com  **Subject**: message from caller | LogRhythm | SOC team have validated the email and found it as malicious, requested O365 team to not to release. | Closed |
| 9 | Medium | **O365 | Phish/Spam Email** | Found an email sent from [info@khalaf.com.jo](mailto:info@khalaf.com.jo) to [gianna.martyna@qualitestgroup.com](mailto:gianna.martyna@qualitestgroup.com). The mail is from an external domain which is suspected of email spoofing which can be either a phishing email or a malware email. Requested to block the sender domain. | LogRhythm | SOC team have validated the email and requested to block the domain. | Closed |
| 10 | Medium | **O365 | Phish/Spam Email** | Found an email sent from [karisasu@ensafecolombia.com](karisasu@ensafecolombia.com%20 ) to [markus.sell@qualitestgroup.com](markus.sell@qualitestgroup.com%20 )The mail is from an external domain (**ensafecolombia.com**) which is malicious.  **Sender**: karisasu@ensafecolombia.com  **Recipient**: markus.sell@qualitestgroup.com.  **Subject**: markus sell sofort erektionstabs kaufen  **URL**: http://www.spontan-lust.nl/ | LogRhythm | SOC team have validated the email and found it as malicious, requested O365 team to not to release. | Closed |
| 11 | Medium | **O365 | Phish/Spam Email** | Found an email send from [ladawnawe@iaeti.org](mailto:ladawnawe@iaeti.org)  to [denis.pramme@qualitestgroup.com](mailto:denis.pramme@qualitestgroup.com)  the mail is from an external domain iaeti.org  **Sender**: ladawnawe@iaeti.org  **Recipient**: denis.pramme@qualitestgroup.com  **Subject**: denis pramme, im bett nichts los? | LogRhythm | SOC team have validated the email and found it as malicious, requested O365 team to not to release. | Closed |
| 12 | Medium | **O365 | Phish/Spam Email** | Found an email send from [silvija.tasevska@higinagyker.hu](mailto:silvija.tasevska@higinagyker.hu) to multiple users in a single mailcontains **malicious attachments**, the mail is from external domain.  **Sender**: silvija.tasevska@higinagyker.hu  **Recipients**: amitabh@qualitestgroup.com , ashish.s@qualitestgroup.com , siddharth.anand@qualitestgroup.com , rajesh.sharma@qualitestgroup.com , kunal.chauhan@qualitestgroup.com ,  ashwin.arora@qualitestgroup.com , sanjay.krishnamurthy@qualitestgroup.com  **File Name**: "Rechnung.pdf.gz" and "BESTELLUNG 02881701.vbs"  **Malware Family**: "O97M/Tisifi.RQ!MTB" and "Malicious Payload" | LogRhythm | SOC team have validated the email and found it as malicious, requested O365 team to not to release. | Closed |

|  |  |  |
| --- | --- | --- |
| **UPDATES** | | |
| **Opened Case books** | 12 | 12-Closed |
| 0-Open |

|  |  |  |
| --- | --- | --- |
| **IOC Updates** | | |
| **IOCs** | **Today** | **Total (This Month)** |
| **No. Of Hash are reported** | 0 | 34 |
| **No. Of IP’s Blocked** | 1 | 71 |
| **No. Of URL/Domain Blocked** | 0 | 27 |