Associated Group Descriptions

| **Name** | **Description** |
| --- | --- |
| T-APT-17 | [[1]](https://blog.talosintelligence.com/2022/05/bitter-apt-adds-bangladesh-to-their.html) |

**ATT&CK® Navigator Layers**

Techniques Used

| **Domain** | **ID** | | **Name** | **Use** |
| --- | --- | --- | --- | --- |
| Enterprise | [T1583](https://attack.mitre.org/techniques/T1583) | [.001](https://attack.mitre.org/techniques/T1583/001) | [Acquire Infrastructure](https://attack.mitre.org/techniques/T1583): [Domains](https://attack.mitre.org/techniques/T1583/001) | [BITTER](https://attack.mitre.org/groups/G1002) has registered a variety of domains to host malicious payloads and for C2.[[2]](https://www.forcepoint.com/blog/x-labs/bitter-targeted-attack-against-pakistan) |
| Enterprise | [T1071](https://attack.mitre.org/techniques/T1071) | [.001](https://attack.mitre.org/techniques/T1071/001) | [Application Layer Protocol](https://attack.mitre.org/techniques/T1071): [Web Protocols](https://attack.mitre.org/techniques/T1071/001) | [BITTER](https://attack.mitre.org/groups/G1002) has used HTTP POST requests for C2.[[1]](https://blog.talosintelligence.com/2022/05/bitter-apt-adds-bangladesh-to-their.html)[[2]](https://www.forcepoint.com/blog/x-labs/bitter-targeted-attack-against-pakistan) |
| Enterprise | [T1568](https://attack.mitre.org/techniques/T1568) | | [Dynamic Resolution](https://attack.mitre.org/techniques/T1568) | [BITTER](https://attack.mitre.org/groups/G1002) has used DDNS for C2 communications.[[2]](https://www.forcepoint.com/blog/x-labs/bitter-targeted-attack-against-pakistan) |
| Enterprise | [T1573](https://attack.mitre.org/techniques/T1573) | | [Encrypted Channel](https://attack.mitre.org/techniques/T1573) | [BITTER](https://attack.mitre.org/groups/G1002) has encrypted their C2 communications.[[2]](https://www.forcepoint.com/blog/x-labs/bitter-targeted-attack-against-pakistan) |
| Enterprise | [T1203](https://attack.mitre.org/techniques/T1203) | | [Exploitation for Client Execution](https://attack.mitre.org/techniques/T1203) | [BITTER](https://attack.mitre.org/groups/G1002) has exploited Microsoft Office vulnerabilities CVE-2012-0158, CVE-2017-11882, CVE-2018-0798, and CVE-2018-0802.[[1]](https://blog.talosintelligence.com/2022/05/bitter-apt-adds-bangladesh-to-their.html)[[2]](https://www.forcepoint.com/blog/x-labs/bitter-targeted-attack-against-pakistan) |
| Enterprise | [T1068](https://attack.mitre.org/techniques/T1068) | | [Exploitation for Privilege Escalation](https://attack.mitre.org/techniques/T1068) | [BITTER](https://attack.mitre.org/groups/G1002) has exploited CVE-2021-1732 for privilege escalation.[[3]](https://ti.dbappsecurity.com.cn/blog/articles/2021/02/10/windows-kernel-zero-day-exploit-is-used-by-bitter-apt-in-targeted-attack/)[[4]](https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-1732) |
| Enterprise | [T1105](https://attack.mitre.org/techniques/T1105) | | [Ingress Tool Transfer](https://attack.mitre.org/techniques/T1105) | [BITTER](https://attack.mitre.org/groups/G1002) has downloaded additional malware and tools onto a compromised host.[[1]](https://blog.talosintelligence.com/2022/05/bitter-apt-adds-bangladesh-to-their.html)[[2]](https://www.forcepoint.com/blog/x-labs/bitter-targeted-attack-against-pakistan) |
| Enterprise | [T1559](https://attack.mitre.org/techniques/T1559) | [.002](https://attack.mitre.org/techniques/T1559/002) | [Inter-Process Communication](https://attack.mitre.org/techniques/T1559): [Dynamic Data Exchange](https://attack.mitre.org/techniques/T1559/002) | [BITTER](https://attack.mitre.org/groups/G1002) has executed OLE objects using Microsoft Equation Editor to download and run malicious payloads.[[1]](https://blog.talosintelligence.com/2022/05/bitter-apt-adds-bangladesh-to-their.html) |
| Enterprise | [T1036](https://attack.mitre.org/techniques/T1036) | [.004](https://attack.mitre.org/techniques/T1036/004) | [Masquerading](https://attack.mitre.org/techniques/T1036): [Masquerade Task or Service](https://attack.mitre.org/techniques/T1036/004) | [BITTER](https://attack.mitre.org/groups/G1002) has disguised malware as a Windows Security update service.[[1]](https://blog.talosintelligence.com/2022/05/bitter-apt-adds-bangladesh-to-their.html) |
| Enterprise | [T1095](https://attack.mitre.org/techniques/T1095) | | [Non-Application Layer Protocol](https://attack.mitre.org/techniques/T1095) | [BITTER](https://attack.mitre.org/groups/G1002) has used TCP for C2 communications.[[2]](https://www.forcepoint.com/blog/x-labs/bitter-targeted-attack-against-pakistan) |
| Enterprise | [T1027](https://attack.mitre.org/techniques/T1027) | | [Obfuscated Files or Information](https://attack.mitre.org/techniques/T1027) | [BITTER](https://attack.mitre.org/groups/G1002) has used a RAR SFX dropper to deliver malware.[[2]](https://www.forcepoint.com/blog/x-labs/bitter-targeted-attack-against-pakistan) |
| Enterprise | [T1588](https://attack.mitre.org/techniques/T1588) | [.002](https://attack.mitre.org/techniques/T1588/002) | [Obtain Capabilities](https://attack.mitre.org/techniques/T1588): [Tool](https://attack.mitre.org/techniques/T1588/002) | [BITTER](https://attack.mitre.org/groups/G1002) has obtained tools such as PuTTY for use in their operations.[[2]](https://www.forcepoint.com/blog/x-labs/bitter-targeted-attack-against-pakistan) |
| Enterprise | [T1566](https://attack.mitre.org/techniques/T1566) | [.001](https://attack.mitre.org/techniques/T1566/001) | [Phishing](https://attack.mitre.org/techniques/T1566): [Spearphishing Attachment](https://attack.mitre.org/techniques/T1566/001) | [BITTER](https://attack.mitre.org/groups/G1002) has sent spearphishing emails with a malicious RTF document or Excel spreadsheet.[[1]](https://blog.talosintelligence.com/2022/05/bitter-apt-adds-bangladesh-to-their.html)[[2]](https://www.forcepoint.com/blog/x-labs/bitter-targeted-attack-against-pakistan) |
| Enterprise | [T1053](https://attack.mitre.org/techniques/T1053) | [.005](https://attack.mitre.org/techniques/T1053/005) | [Scheduled Task/Job](https://attack.mitre.org/techniques/T1053): [Scheduled Task](https://attack.mitre.org/techniques/T1053/005) | [BITTER](https://attack.mitre.org/groups/G1002) has used scheduled tasks for persistence and execution.[[1]](https://blog.talosintelligence.com/2022/05/bitter-apt-adds-bangladesh-to-their.html) |
| Enterprise | [T1608](https://attack.mitre.org/techniques/T1608) | [.001](https://attack.mitre.org/techniques/T1608/001) | [Stage Capabilities](https://attack.mitre.org/techniques/T1608): [Upload Malware](https://attack.mitre.org/techniques/T1608/001) | [BITTER](https://attack.mitre.org/groups/G1002) has registered domains to stage payloads.[[2]](https://www.forcepoint.com/blog/x-labs/bitter-targeted-attack-against-pakistan) |
| Enterprise | [T1204](https://attack.mitre.org/techniques/T1204) | [.002](https://attack.mitre.org/techniques/T1204/002) | [User Execution](https://attack.mitre.org/techniques/T1204): [Malicious File](https://attack.mitre.org/techniques/T1204/002) | [BITTER](https://attack.mitre.org/groups/G1002) has attempted to lure victims into opening malicious attachments delivered via spearphishing.[[1]](https://blog.talosintelligence.com/2022/05/bitter-apt-adds-bangladesh-to-their.html)[[2]](https://www.forcepoint.com/blog/x-labs/bitter-targeted-attack-against-pakistan) |

Software

| **ID** | **Name** | **References** | **Techniques** |
| --- | --- | --- | --- |
| [S1013](https://attack.mitre.org/software/S1013) | [ZxxZ](https://attack.mitre.org/software/S1013) | [[1]](https://blog.talosintelligence.com/2022/05/bitter-apt-adds-bangladesh-to-their.html) | [Data from Local System](https://attack.mitre.org/techniques/T1005), [Deobfuscate/Decode Files or Information](https://attack.mitre.org/techniques/T1140), [Ingress Tool Transfer](https://attack.mitre.org/techniques/T1105), [Masquerading](https://attack.mitre.org/techniques/T1036): [Masquerade Task or Service](https://attack.mitre.org/techniques/T1036/004), [Native API](https://attack.mitre.org/techniques/T1106), [Obfuscated Files or Information](https://attack.mitre.org/techniques/T1027), [Phishing](https://attack.mitre.org/techniques/T1566): [Spearphishing Attachment](https://attack.mitre.org/techniques/T1566/001), [Process Discovery](https://attack.mitre.org/techniques/T1057), [Query Registry](https://attack.mitre.org/techniques/T1012), [Scheduled Task/Job](https://attack.mitre.org/techniques/T1053): [Scheduled Task](https://attack.mitre.org/techniques/T1053/005), [Software Discovery](https://attack.mitre.org/techniques/T1518): [Security Software Discovery](https://attack.mitre.org/techniques/T1518/001), [System Information Discovery](https://attack.mitre.org/techniques/T1082), [System Owner/User Discovery](https://attack.mitre.org/techniques/T1033), [User Execution](https://attack.mitre.org/techniques/T1204): [Malicious File](https://attack.mitre.org/techniques/T1204/002) |