Report Analyzed: Cisco Talos Intelligence Group - Comprehensive Threat Intelligence Bitter APT adds Bangladesh to their targets

1 Finished Reporting to ATT&CK

The finished report with tactics and techniques highlighted is enclosed with this report. The process involved reading the executive summary to get the gist of the entire event. We searched for similar procedural examples (by MITRE) using keywords. Then by deconstructing the events into different Tactics (by MITRE), we were able to find the corresponding techniques suited to our scenario. Other reports may differ in some cases and we will be happy to integrate other techniques on discussion with analysts.

2 Defensive Recommendations

The defensive recommendations for each technique have been documented and their corresponding trade-offs have been listed keeping in mind the nature of the organisation. Remedies involve around installing basic security software and developing user habits to prevent an attack in the future. Along with each recommendation, the detection/mitigation ID provided by MITRE is listed (if applicable). After thorough analysis, we came up with the following recommendations:

2.1 Technical

1. Installation and upgradation of anti-virus software on all endpoints
2. Conduct cost-based analysis for implementation of NIPS/NIDS on internet-facing network
3. Logging should be done for each user-called API and system call. The stream should be searched for specific keywords (for eg. schtask) in an online manner and should immediately alert the responsible department. File downloads should be treated with suspicion.
4. Network Segmentation should be properly done in consultation with executives and IT Department. This should be done to ensure that sensitive information is isolated in case of an event.
5. Avoid giving sudo access to non-critical machines. The list of sudoers should be kept and carefully scrutinized. Setup execution controls for employees other than developers.
6. Backups should be made on external disks and carefully stored in a vault. In case of a ransomware attack, to prevent sensitive information loss, make sure that the sensitive files are encrypted.
7. The system configuration settings should be made according to STIG benchmarks. Automated checking by open-source tools (for eg. osscap) should be encouraged.

2.2 Policy

1. Backup and Restore SOP should be defined. The exact period of backup (hourly/daily/weekly) should be decided by the executives. Regular drills need to be conducted to ensure the smooth functioning and validity of the SOP and also to inculcate this habit into the workforce.
2. Yearly audit of cybersecurity practices should be performed by an external agency. All files shared with the auditor should be marked confidential and should be encrypted.
3. Users should be trained on healthy cyber practices with hands-on training on encryption, anti-phishing campaigns, email-sandboxing, malicious indicators etc.
4. The organisation should establish an IT security department responsible for maintaining cyber-resiliency of systems and to implement all the technical recommendations.
5. Personal device should not be plugged to the organisation network. New endpoints should be detected at the SOC.
6. The IT security department in consultation with the executives should assign specific roles and responsibilities to each individual and RBAC should be maintained with utmost priority.

2.3 Risk Management

1. As the organisation is not involved in critical infrastructures, some downtime of machines is tolerable.
2. Sensitive documents (for eg. case files, threat intelligence, employee records etc.) must remain classified and should be isolated in case of compromise.
3. Loss of non-critical information as an anomaly is tolerable but future preparation including both technical, policy recommendations must be adhered to prevent future attacks

3 References

1. MITRE ATT&CK™
2. Cyber Analytics Repository, MITRE
3. The Windows ATT&CK Logging Cheat Sheet
4. MITRE D3FEND™
5. Microsoft Security Response Center
6. Google

4 Assumptions

Rapid Action Battalion Unit of the Bangladesh police (RAB) is an anti-crime and anti-terrorism unit of the Bangladesh Police. Being at the forefront of national crime detection including both cyber and physical crime, we expect the organisation to be well-equipped in terms of cybersecurity tools and hygiene. We also expect the existence of a Security Operations Center. However with the report of the persistent attack by the Bitter APT group, we can still see a scope for improvement. We notice the absence of email-spoof detection software, email detonation software. Although the data exfiltration was successful, no sensitive information was lost indicating that either the sensitive documents are stored with additional protection measures or network is segmented to ensure isolation.
Reference: `https://en.wikipedia.org/wiki/Rapid_Action_Battalion`