What We Can Learn From the Bangladesh Central Bank Cyber Heist

Posted on: March 15, 2016 at 8:30 pm **Posted in:** Malware, Targeted Attacks
Author: Martin Roesler (Director, Threat Research)

The reported hacking of Bangladesh's central bank accounts with the U.S. Federal Reserve once again shows how bad the impact of cyber attacks to organizations, enterprises or even nation-states can be. Peel off all the other layers in this narrative for a moment—the amount of money stolen, the alleged players, the politics—and at its core, we have the same tactics and procedures any enterprising criminal will carry out against his or her intended target.

The hacking incident is one of the most ambitious thefts committed via cybercrime to date. Were it not for a small typo, more than a billion US dollars would have been stolen. As it stands, more than $80 million was still wired and laundered via several casinos in the Philippines. Investigations of the attack are looking at the possibility of malware being installed on the central bank's computer systems as the primary tool used to help facilitate the heist.

If malware was involved:

- How did the attackers gain authorization to do the transaction? Did they get control of an account that has the power to do so, and if so, how (phishing, keylogging, others)?
- Are there security measures or controls in place that would have triggered anomalies (e.g., high amount of transaction, high volume of transactions, etc.)?

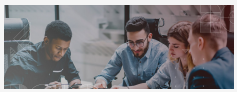
If malware was used, this incident may not be entirely different from other cases of cybercrime and targeted attacks that happen every day. There's a wide variety of tools like cheap keyloggers sold in the cybercriminal underground and the Deep Web which criminals can use, along with enhanced social engineering tactics like those employed in Business Email Compromise (BEC) attacks.

So what can organizations learn from this? For starters, try answering the questions above in the context of your *own* network, your policies–your solutions. Who, in your organization, has access to the most important data? How do you ensure that these data are protected? Do your processes, policies, and your infrastructure empower your employees to see "trigger warnings" and perform appropriate action at the right time?

Security should not be a simple item on a checklist. It should be a process, an attitude, and a mindset. This incident adds to the growing list of proof points that support this statement, especially now that cyber attacks are getting bigger and definitely more "real" in terms of impact.

Tags: cybercrime cybercrime underground

Security Predictions for 2020



Cybersecurity in 2020 will be viewed through many lenses — from differing attacker motivations and cybercriminal arsenal to technological developments and global threat intelligence — only so defenders can keep up with the broad range of threats.
Read our security predictions for 2020.

Business Process Compromise

Attackers are starting to invest in long-term operations that target specific processes enterprises rely on. They scout for vulnerable practices, susceptible systems and operational loopholes that they can leverage or abuse. To learn more, read our Security 101: Business Process Compromise.

Recent Posts

OpenSMTPD Vulnerability (CVE-2020-8794) Can Lead to Root Privilege Escalation and Remote Code Execution

Operation Overtrap Targets Japanese Online Banking Users Via Bottle Exploit Kit and Brand-New Cinobi Banking Trojan

March Patch Tuesday: LNK, Microsoft Word Vulnerabilities Get Fixes, SMBv3 Patch Follows

Busting Ghostcat: An Analysis of the Apache Tomcat Vulnerability (CVE-2020-1938 and CNVD-2020-10487)

Dissecting Geost: Exposing the Anatomy of the Android Trojan Targeting Russian Banks

Popular Posts

LokiBot Impersonates Popular Game Launcher and Drops Compiled C# Code File

Misconfigured Container Abused to Deliver Cryptocurrency-mining Malware

Dissecting Geost: Exposing the Anatomy of the Android Trojan Targeting Russian Banks

Outlaw Updates Kit to Kill Older Miner Versions, Targets More Systems

February Patch Tuesday: Fixes for Critical LNK, RDP, Trident Vulnerabilities

Stay Updated

Email Subscription
Your email here
Subscribe

HOME AND HOME OFFICE | FOR BUSINESS | SECURITY INTELLIGENCE | ABOUT TREND MICRO

Asia Pacific Region (APAC): Australia / New Zealand, 中国, 日本, 대한민국, 台灣 Latin America Region (LAR): Brasil, México North America Region (NABU): United States, Canada
Europe, Middle East, & Africa Region (EMEA): France, Deutschland / Österreich / Schweiz, Italia, Россия, España, United Kingdom / Ireland

Privacy Statement Legal Policies