5-6-2019

Cyber Threat Report May 06, 2019

Patrick Bell
Army Cyber Institute

Follow this and additional works at: https://digitalcommons.usmalibrary.org/aci_rp

Recommended Citation
https://digitalcommons.usmalibrary.org/aci_rp/40
 Threat Actor Update

Iranian Hackers Target UK Organizations in Ongoing Attack
State-sponsored Iranian hackers have been blamed for a cyber-attack campaign that has compromised employees working in banks, local government, and the Post Office.

Amnesty International Hit By China-linked Cyber Attack
The human rights NGO claims its Hong Kong office has been hit by a years-long cyberattack from hackers with known links to the Chinese government.

Hamas shifts tactics in bitcoin fundraising
The armed wing of Hamas now generates a new digital wallet with every donation transaction, complicating outsiders’ efforts to flag or even monitor transactions.

State-Sponsored DNS Hijacking Infiltrates 40 Firms Globally
A newly discovered campaign targets national security organizations primarily across the Middle East and North Africa with DNS hijacking attacks to scoop up credentials.

North Korean-linked Lazarus Group releases Hoplight malware
DHS and FBI have identified a new Trojan malware variant that functions as spyware capable of securely connecting to a control server and uploading pilfered files.

Threat Target Update

Microsoft Hacked: Attackers Actually Able to Read User Emails
Cybercriminals compromised a Microsoft support agent’s account and could potentially have accessed any user’s email account as long as it wasn’t a corporate level account.

2 Million Credit Cards Exposed in Earl Enterprises Hack
Malware installed in point-of-sale systems has compromised credit cards used at restaurant chains Buca di Beppo, Planet Hollywood, and Earl of Sandwich, among others.

Bayer Contains Cyber Attack that Bore Chinese Hallmarks
The German drugmaker has contained a cyber-attack that utilized WINNTI malware and believes no data theft occurred or third party data was compromised.

Notable Ransomware Attacks in April
Link: Cleveland Airport: email services crippled and information screens disabled for days
Link: Arizona Beverages struggled for nearly five days to restore systems and retrieve data.

Cyberattack at med-tech conglomerate Hoya slowed production 60%
Japanese manufacturer Hoya temporarily shut down production at a factory in Thailand following a cyberattack that infected roughly 100 computers with cryptojacking malware.

ACI Update

- The Spring 2019 edition of The Cyber Defense Review is now available for digital download!
- Dr. David Gioe authored “Make America Strategic Again” in The National Interest.
- Listen to him discuss the article in this Blog Talk Radio podcast.
- Dr. Erica Borghard co-authored "The Overlooked Military Implications of the 5G Debate" for the Council of Foreign Relations.
- The West Point Cyber Policy Team repeated as champions of the European Cyber 9/12 Strategy Challenge, besting 21 other teams from 13 countries.

This report is comprised of a compilation of links to cyber-related media reports for the purpose of promoting situational awareness in the United States Government. The report is a work of the United States Government and is not subject to copyright protection in the United States. The linked articles may be subject to copyright protection. This report is not vetted intelligence and does not represent the official position of the United States Government or the Department of Defense.

UNCLASSIFIED