2-2-2019

Cyber Threat Report 02 February 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/37
**Threat Actor Update**

**Russians accused of hacking DNC after 2018 midterms**
Attack attempt apparently unsuccessful, but bears similarities to APT29, the Russian hacking group "Cozy Bear."

**FireEye links DNS hijacking campaign to Iran**
The campaign has targeted dozens of government, telecom, and Internet infrastructure entities across the Middle East, North Africa, Europe, and North America.

**Lazarus-affiliated tools used against Chilean interbank network**
The malware toolkit, linked to the North Korean Advanced Persistent Threat group, continues targeting Latin American financial institutions.

**DarkHydrus APT utilizes Google Drive in malware attack campaign**
The APT group is utilizing Google Drive as its command-and-control server against targets in the Middle East according to 360TIC and Palo Alto Networks.

**Threat Target Update**

**Ukrainians hacked SEC for insider trading**
New Jersey prosecutors allege two Ukrainians committed securities fraud conspiracy, wire fraud conspiracy, computer fraud conspiracy, wire fraud, and computer fraud.

**German man releases private data of politicians and celebrities**
The 20-year-old confessed to the biggest data hack in German history and claimed to have acted out of anger at his targets. No foreign intelligence involvement is suspected.

"Cyber incident" compromises Airbus personal data
Hackers acquired professional contact and IT identification details of Europe-based employees, but may have been targeting the firm’s intellectual property.

**Malware disrupts Tribune Publishing and Los Angeles Times**
The attack, which debilitated printing operations, is believed to have originated outside of the US and can reportedly be traced to the Ryuk ransomware that took down a NC water utility in October.

**Shipping industry targeted in "whaling" attacks**
Pen Test Partners identifies business email compromise attacks are rampant against the shipping industry, which is known for its lax security standards.

---

**ACI Update**

- A Fifth Domain article quotes an ACI researcher on preventing cyber attacks through the use of Artificial Intelligence.
- The United States Military Academy’s Cyber Policy Team wins inaugural Cyber 9/12 Strategy Challenge in Lille, France.
- The Army Cyber Institute welcomed Soldiers from the 335th Signal Command (Theater) Army Reserve Cyber Operations Group, formally beginning a mutually beneficial partnership.