Changes in the Cyber Insurance Landscape & Continued Russian Threats

Russian Cyber Threat Roundup

INSURER DROPPING COVERAGE FOR STATE-BACKED HACKS

*What's New:* Lloyd's of London will require underwriters to exclude coverage for state-backed cyberattacks linked to war or catastrophic damages.

*Go Deeper:* Lloyd’s is mandating its insurance groups, at minimum, must specifically exempt coverage for losses “arising from a war,” and state-backed cyberattacks that “significantly impair the ability of a state to function,” or which impact a state’s security capabilities. They also mandate that syndicates have a clear system for how to attribute an attack to a state-based actor.

*Why it Matters:* Lloyd’s mandates coincide with concerns about the growing cost of cyberattacks and who is ultimately liable.

RUSSIAN STATE-SPONSORED CYBER THREATS

*What's New:* CISA continually updates resources on active threats and resources on Russian state-sponsored cyber activity:

- Shields Up
- Shields Up Technical Guidance
- CISA's Russia Cyber Threat Overview and Advisories webpage

Malicious IPs and Domains

*The Bottom Line:* Malicious IP addresses and domains downloadable file can be used to protect your network.

*Go Deeper:* The Multi-State Information Sharing and Analysis Center (MS-ISAC) recommends reviewing and removing old indicators from previous lists as they may no longer be malicious. MS-ISAC creates this list based on observed and recorded malicious IP addresses and domains and shares this list.

*Note:* Recipients may only share this information with peers and partner organizations but not via publicly accessible channels.

Data Leak Sites Report
SECURITY ROUNDUP

WHITE HOUSE'S THREE-HEADED CYBERSECURITY TEAM

**What's New:** The Biden administration has three key leaders for the country to turn to during a major cyberattack — but until last year, two of the three positions they hold didn't exist.

Biden's "big three" are national cyber director Chris Inglis; CISA director Jen Easterly; and Anne Neuberger, deputy national security adviser for cyber and emerging tech at the White House's National Security Council.

**Go Deeper:** Easterly broke down their respective turfs in an interview with Axios:

- Neuberger handles the White House's cyber policy agenda.
- Inglis develops strategies to strengthen the larger U.S. cyber ecosystem, including the private and public sectors.
- Easterly concentrates on defending the federal government and private sector from attacks.

DROP IN RANSOMWARE NUMBERS IS AN ILLUSION

**What's New:** Tallies of ransomware attacks have declined, but changes in ransomware tactics, and less reliance on leak sites, may be skewing these numbers.

**Go Deeper:** Those tallying ransomware attacks have less information than before. Tallying figures depend on ransomware gangs' leak sites - where groups post alleged victims' identities and data in an attempt to compel them to pay. Ransomware gangs are relying less on those sites and directly contacting victims as a means of pressuring them to pay the ransom. Gangs are also using ransomware-like tactics without using the actual malicious software, stealing data and threatening to release it without necessarily locking up victim networks.

SECURING THE CLOUD BY DESIGN AND DEFAULT

**What's New:** To reduce data breaches from cloud services, seek out providers who ensure functionality is 'secure by default.'

**Go Deeper:** The U.K.'s National Cyber Security Centre stresses a new security model that assigns as much security responsibility to your cloud provider instead of your internal IT team. Organizations should choose a provider that is secure in its own right and helps you meet your security responsibilities.

CYBER INSURERS WEIGH IN ON TRENDS AND THREATS

**What's New:** The cyber insurance industry has observed remote desktop threats, ransomware, business email compromise, phishing, Microsoft Exchange exploitation, and Log4j as the top cyber trends and threats.

**The Bigger Picture:** The rate of American businesses purchasing cyber insurance has doubled since 2016. This increase has given insurance firms unique insight into cybersecurity trends and the vulnerabilities that are plaguing businesses the most.

**PwC SURVEY:** CYBER IS NO.1 BUSINESS RISK
What's New: In PricewaterhouseCooper’s recent Pulse Survey, business leaders said cyber was the number 1 business risk.

Go Deeper: In the survey, 40% of all respondents listed more frequent and/or broader cyber attacks as a serious risk (and another 38% called it a moderate risk).

The Bigger Picture: This signals a shift in cybersecurity’s perception - cyber threats are no longer solely the domain of a business’s CISO.

PROXIES AND CONFIGURATIONS USED FOR CREDENTIAL STUFFING
What’s New: Proxies and configurations are being used by cyber criminals to mask and automate credential attacks on US companies.

Action Step: The FBI recommends several mitigation steps to defend against credential cracking, including enabling multi-factor authentication, not relying solely on CAPTCHA, and using Secure Socket Layer (SSL) pinning.

BLACKBYTE 2.0 UTILIZES NEW EXTORTION TECHNIQUES
What’s New: BlackByte ransomware’s version 2.0 includes a new data leak site utilizing new extortion techniques borrowed from LockBit.

Go Deeper: After a brief disappearance, BlackByte is now promoting a new data leak site on hacker forums and through Twitter accounts. The data leak site has new extortion strategies that allow victims to pay to extend the publishing of their data by 24 hours ($5,000), download the data ($200,000), or destroy all the data ($300,000).

US-CERT BULLETIN VULNERABILITY SUMMARY

RE-ISAC

This information comes from the Real Estate Information Sharing and Analysis Center. NMHC welcomes feedback on these alerts and how the content can helpful for NMHC members. Please send any questions or comments to jgoodfellow@nmhc.org or ddudzinski@nmhc.org.

Should others in your organization also be interested in receiving NMHC Cyber Alerts, they can sign up here.