

ONE OF THE MOST DANGEROUS ATTACKS

MY-NGOC NGUYEN, SANS PRINCIPAL INSTRUCTOR AND CEO OF SECURED IT SOLUTIONS

PHD - KEY ACTIONS

- Persist
- Harvest
- Decrypt



PERSISTENCE PERSISTS

Hiding in plain sight

- Motives tend to be other than ransom
- Attackers can operate undetected for extended periods, carrying out malicious activities on a larger scale.
- Harvesting data as well as capabilities and paths to further permeating into the environment
- For example, the advisories seek to "own" the environment so at their time of choosing, they can disrupt operations such as those utilities and critical infrastructure.

What's old is really what's new

- Continuum of sophistication and evolution of old techniques

HOW THEY HIDE IN PLAIN SIGHT

- Weaponizing legitimate tools like remote monitoring and management tools and employing "living off the land" techniques like:
  - Using PowerShell
  - Leveraging dedicated connections, shared services, authorized network ports or protocols over trusted pathways, migrating into processes
  - Using valid credentials
- Gaining access through VPNs via valid accounts with weak credentials
- Further exploiting Third Party Services like MSPs and Cloud Providers
- Impersonating legitimate tools; mimicking trusted applications

HARVEST EVERYTHING

- Credentials and access
  - Further permeate
- Beware even with implementation of Zero Trust Architecture.

Harvest Now, Decrypt Later

  - Leveraging the advancement of Quantum Computing, attackers are obtaining and gathering all the data even if they are encrypted.



DECRYPT LATER

- While a typical computer would take few hundred trillion years or more to decrypt an RSA 2,048-bit encryption, a quantum computer could crack it in hours.
- NIST estimates there is a "materially high" likelihood that a quantum computer capable of breaking RSA-2048 within 24 hours will emerge within the next 10 years.
- Attackers will wait for the advancement of quantum

MITIGATION

- Work factor of encryption needs to be considered and realistic
- Start transitioning to the new NIST standards as soon as possible.
  - Mid- Aug of 2024, NIST Releases First 3 Finalized Post-Quantum Encryption Standards, FIPS 203, FIPS 204, FIPS 205
- Use AES 256-bit or higher
- Conduct basic security hygiene like patching, logging, and detecting
- Implement MFA for all remote connections, at minimum
- Continue the Zero Trust journey
- Mature business and operations resiliency program



THANK YOU

MYNGOCN@SECITSOL.COM