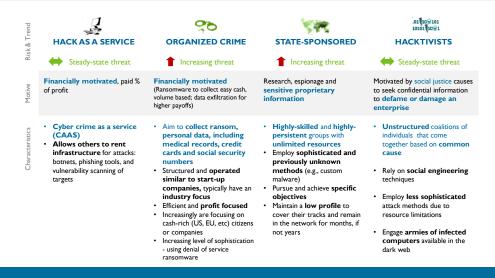
Emerging IT Security Risks

Who is behind the breaches?

Cyber criminal organizations and attackers threatening U.S. corporations are often categorized into four profiles



2

Latest examples

HEALTHCARE ORGS TARGETED BY APT

APT29 is targeting healthcare and other industries with spear phishing messages

- Threat intelligence indicates that APT29, the Russian state-sponsored hacker group, has re-emerged to target multiple US sectors including healthcare with crafted spear phishing messages
- The phishing emails were made to look like secure communication from the U.S. Department of State, hosted on a page made to look like a Department of State official's personal drive
- FireEye has detected intrusion attempts against more than 20 of its customers across multiple industries including: law enforcement, media, U.S. military, imagery, transportation, pharmaceutical, government, and defense contracting
- APT29 has compromised the email server of a hospital and the corporate website of a consulting company to use their infrastructure to send phishing emails

MALICIOUS RANSOMWARE EMAILS

Compromised healthcare email accounts targeted healthcare sector via malicious attachments

- Reports received about 12 compromised O365 email accounts at a medical device company replying to existing email threads with infected word documents containing GandCrab ransomware
- About 400 to 500 companies were targeted and impacted across various industries. KP is aware of one California health care provider that was severely impacted
- At this time it is unclear who the threat actor is; the threat vector for the compromised O365 email accounts was phishing

HACKER AUCTIONS MEDICAL ACCESS

Threat actor auctioning on the dark web "medical access" from a competitor healthcare organization

- On Aug 11th, intelligence sources discovered on the dark web that a threat actor was offering "control panel access" to medical centers in Miami, Florida
- The threat vector was detailed through screenshots, indicating a vulnerable machine was infected by a botnet
- According to the threat actor, access to the control panel allows users to communicate with employees, write prescriptions, prescribe treatment, and access 26k records of patient information. Thus, enabling the possibility of Medicare fraud and the monetization of medical records
- The access to the panels and datasets were later sold for \$1500 US Dollars
- The H-ISAC worked with payers and located the compromised clinics based on claims information and this information was given to law enforcement for victim notification purposes

3

What does the community need to be concerned about?

TOP THREATS

- Credential theft/loss and unauthorized access into cloud services
- Worms delivering Ransomware/wiperware, through either direct network access or through a vendor interconnection with an infected system
- 3 Phishing attacks delivering malware or stealing credentials
- 4 Compromise of clinical and physical IoT devices with malware, ransomware, or denial of service
- 5 Data loss or malware compromise Through unsanctioned cloud services



- 6 Credential theft and access into internal systems and applications
- 7 Compromised commercial or open source software updates being downloaded onto KP assets
- 8 Personal or unsanctioned devices downloading sensitive data into unprotected containers
- 9 Exploitation of vulnerabilities in the browser and associated desktop applications via malicious sites
- 10 Exploitation of internet-facing server-side vulnerabilities at the application layer including denial of service

4