





# Emerging IT Security Risks

## Who is behind the breaches?

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

	 <b>HACK AS A SERVICE</b>	 <b>ORGANIZED CRIME</b>	 <b>STATE-SPONSORED</b>	 <b>HACKTIVISTS</b>
Risk & Trend	↔ Steady-state threat	↑ Increasing threat	↑ Increasing threat	↔ Steady-state threat
Motive	Financially motivated, paid % of profit	Financially motivated (Ransomware to collect easy cash, volume based; data exfiltration for higher payoffs)	Research, espionage and sensitive proprietary information	Motivated by social justice causes to seek confidential information to defame or damage an enterprise
Characteristics	<ul style="list-style-type: none"> <li>Cyber crime as a service (CAAS)</li> <li>Allows others to rent infrastructure for attacks: botnets, phishing tools, and vulnerability scanning of targets</li> </ul>	<ul style="list-style-type: none"> <li>Aim to collect ransom, personal data, including medical records, credit cards and social security numbers</li> <li>Structured and operated similar to start-up companies, typically have an industry focus</li> <li>Efficient and profit focused</li> <li>Increasingly are focusing on cash-rich (US, EU, etc) citizens or companies</li> <li>Increasing level of sophistication - using denial of service ransomware</li> </ul>	<ul style="list-style-type: none"> <li>Highly-skilled and highly-persistent groups with unlimited resources</li> <li>Employ sophisticated and previously unknown methods (e.g., custom malware)</li> <li>Pursue and achieve specific objectives</li> <li>Maintain a low profile to cover their tracks and remain in the network for months, if not years</li> </ul>	<ul style="list-style-type: none"> <li>Unstructured coalitions of individuals that come together based on common cause</li> <li>Rely on social engineering techniques</li> <li>Employ less sophisticated attack methods due to resource limitations</li> <li>Engage armies of infected computers available in the dark web</li> </ul>

## 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 11<sup>th</sup>, 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

- 1 Credential theft/loss and unauthorized access** into cloud services
- 2 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