MINNESOTA IT SERVICES

Legislative Commission on Cybersecurity
MNIT Update

June 14, 2022

Agenda

- Opening Remarks
- National Cybersecurity Prioritization
- Cybersecurity Threats Update
  - Ransomware attacks
  - Supply chain attacks
  - Cyber espionage activity
  - Denial of Service activity
- Closing Remarks

National Cybersecurity Prioritization

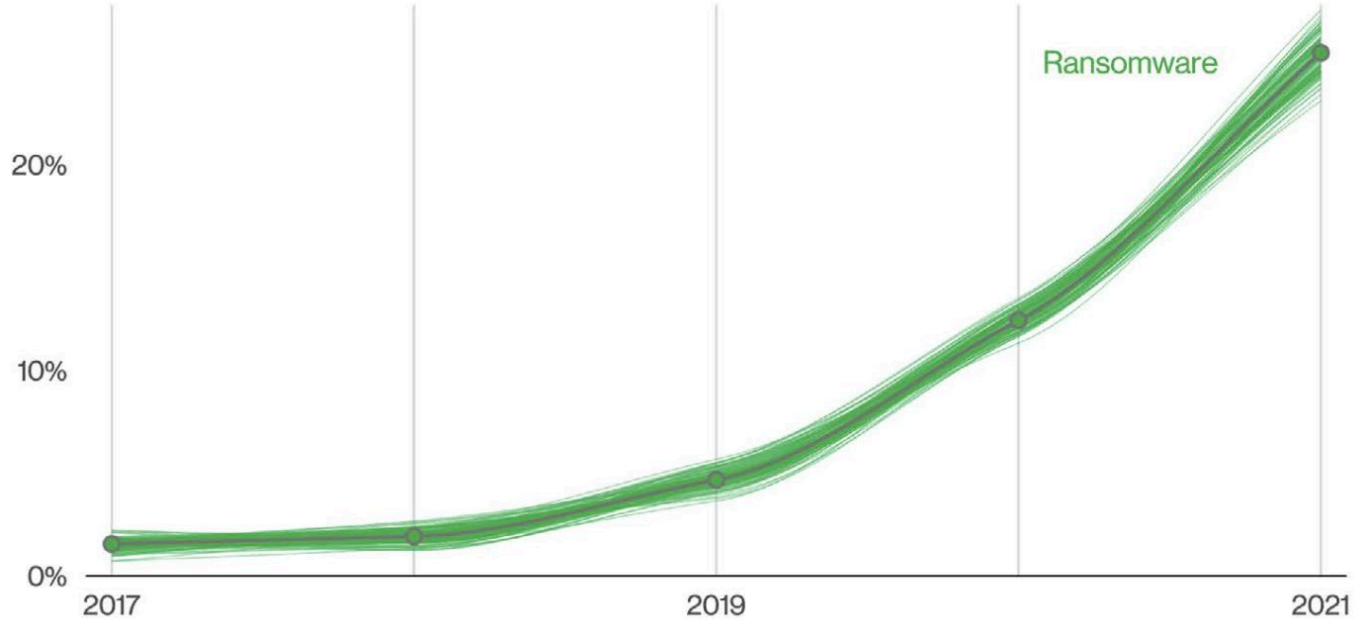
- White House issued Executive Order on Improving the Nation's Cybersecurity
- U.S. Securities and Exchange Commission (SEC) Proposed Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies
- Cybersecurity & Infrastructure Security Agency (CISA) issued alert – Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure
- Gartner Inc. estimates that cybersecurity spending up more than 12% in 2021 and is expected to grow in 2022

Ransomware Attacks

How prevalent is ransomware?

- Increased by 13% to a total of 25% of all security breach investigations in 2021
- Interrupt critical functions. Not targeting specific data value (e.g. credit cards, banking information, PII)
- Dwell time is only 5 days (one-seventh of non-ransomware)

Ransomware over time



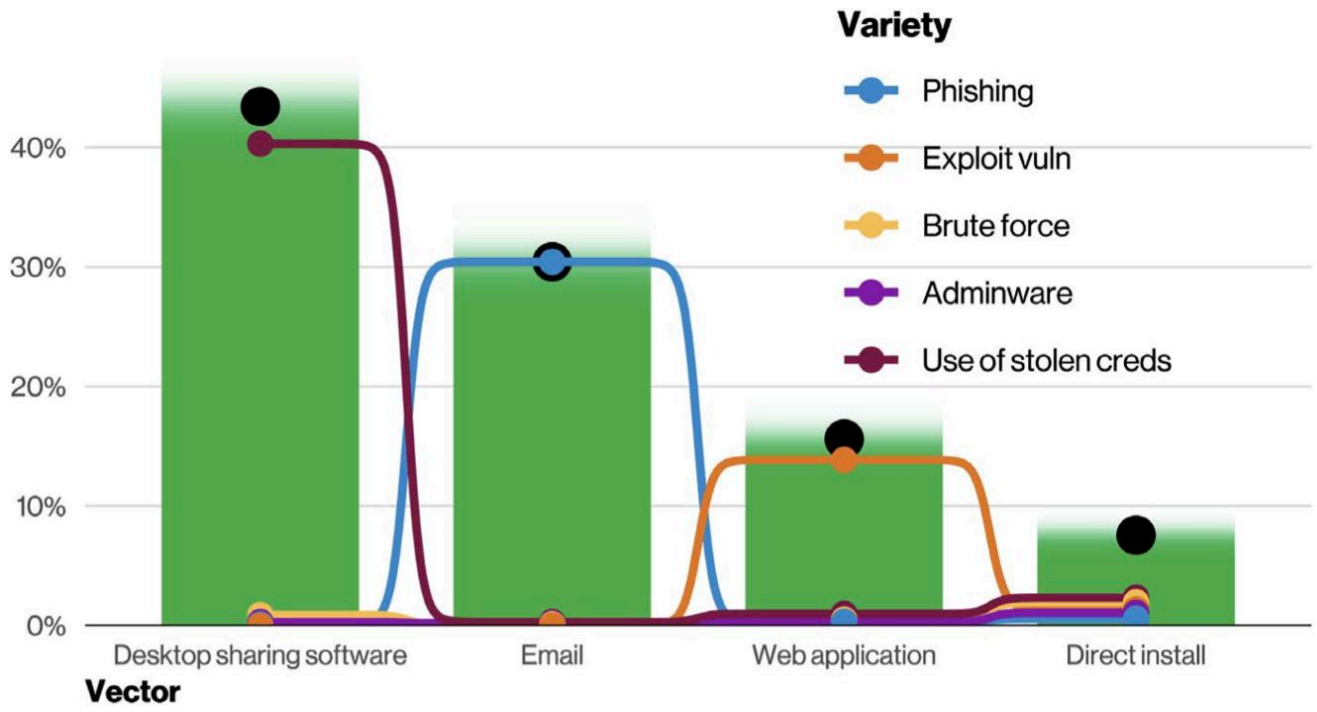
Source: Verizon Data Breach Investigation Report (DBIR) 2022 and M-Trends 2022

Ransomware Attacks

Ransomware points of entry

- 40% Stolen remote access credentials
- 35% Phishing through email
- 15% Brute force of web applications

Ransomware Intrusion Vector



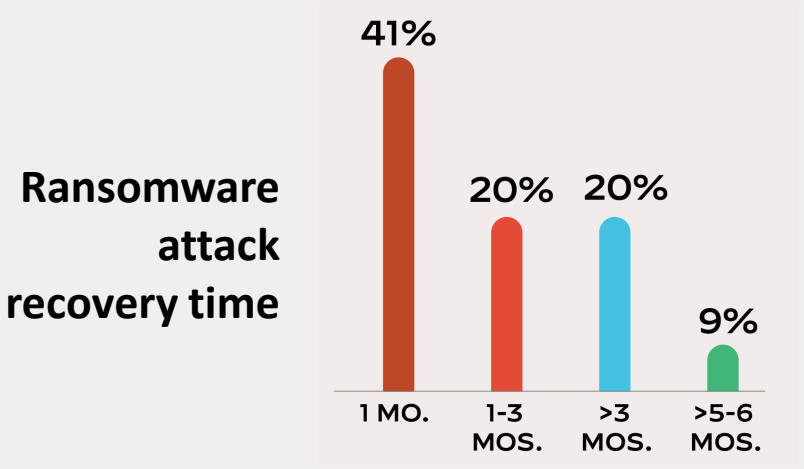
Source: Verizon Data Breach Investigation Report (DBIR) 2022

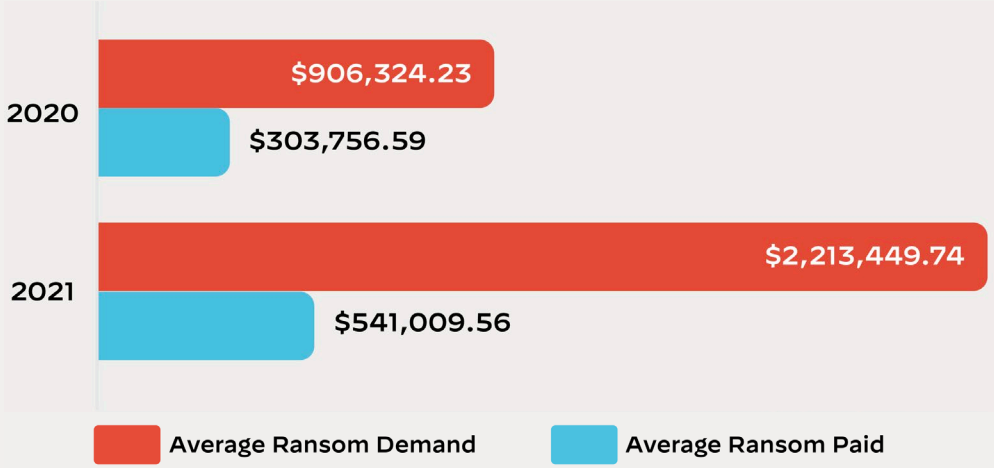
Ransomware Attacks

Impacts of ransomware

- Downtime and business disruption
  - 59% more than a month for recovery
- Payment extortion
  - 144% increase in average demand
  - 78% increase in average payments

Source: Palo Alto Unit 42 Ransomware Threat Report 2022





Supply Chain Attacks

- 2021 saw a significant increase in third-party and partner attacks
- SolarWinds attack primary contributor to the 2021 increase
  - 18,000 private and public organizations impacted
- NotPetya attack in 2017 is the most expensive

Firms Directly Affected by NotPetya Cyber Attack

Organization	Total Assets	Total Cost
Beiersdorf	$7.69B	$43M
Fedex	$33.07B	$400M
Maersk	$68.84B	$300M
Merck	$98.17B	$670M
Mondelez	$66.82B	$180M
Nuance	$5.82B	$92M
Reckitt Benkiser	$24.19B	117M
WPP	$41.55B	$15M

Source: Pirates without Borders: The Propagation of Cyberattacks through Firms' Supply Chains, Federal Reserve Bank of New Yor, July 2020

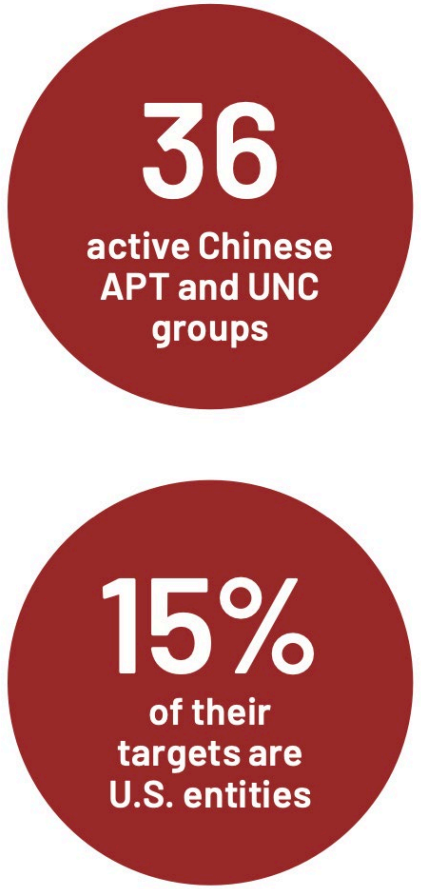
Cyber Espionage Activity

Trends in cyber espionage activity

- 244 total Chinese cyber espionage active groups observed from 2016 to 2021
  - 36 active in 2021
  - Geographic focus on U.S. and Asia
  - Government organizations interest is steady since 2018
- Organizations targeted align with strategic interest to national economic outcomes

Source: M-Trends 2022

2021 Snapshot of Size and Focus

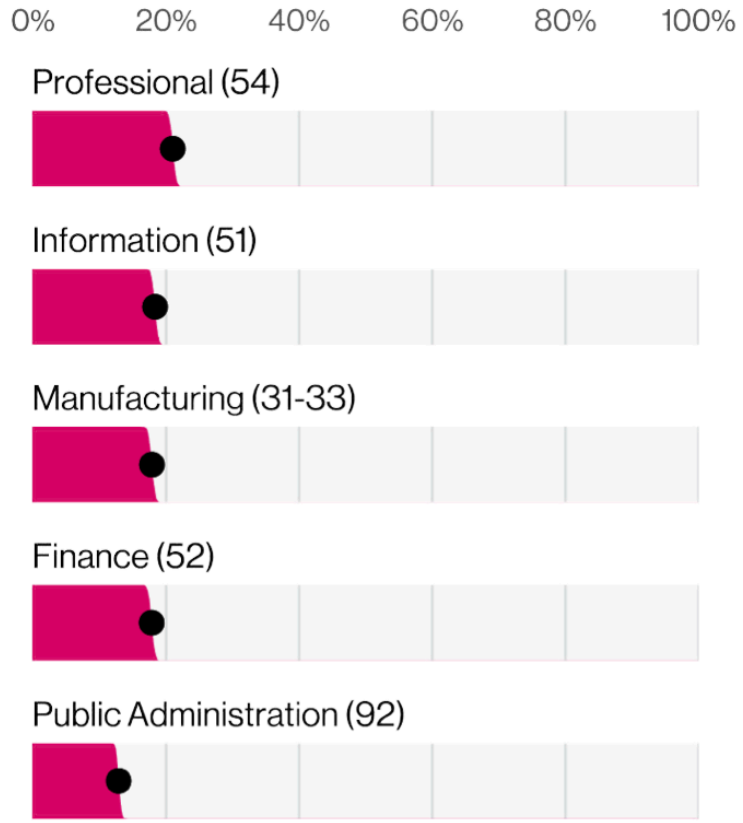


Denial of Service Attacks

How prevalent are Denial of Service attacks?

- On average, entities in the top targeted industries experience 10 attacks per year
- Median attack today is around 1.3 Gbps
- Median attacks last for four hours

2021 Top 5 Targeted Industries



Source: Verizon Data Breach Investigation Report (DBIR) 2022

Cyber Attacks Affecting Minnesota

Cybersecurity & Infrastructure Security Agency (CISA) issued a warning about ransomware targeting food and agriculture companies

- Ransomware attack compromised a farm co-op and food processor

Civil and social unrest targeted Minnesota government resources with DDoS

- Distributed Denial of Service attacks targeted state resources for fourteen consecutive days at unprecedented levels

Federal Cybersecurity Grants

- Infrastructure Investment and Jobs Act provided $1B nationwide for FY22-25
  - Minnesota:
    - $18M in federal funds after $5.7M state match
- 80% of funding for programs that benefit local, tribal and territorial governments (25% to rural areas based on census data)
- Funding use determined by the planning committee
- Further guidance expected in summer 2022

Federal Cybersecurity Grants, cont...

- Planning Committee Composition requires representation from:
  - State
  - Counties
  - Cities
  - Towns
  - Public education
  - Public health
  - Tribal nations
- Members from suburban, rural, and high-population jurisdictions
- No less than half of members have professional experience related to cybersecurity or IT

MINNESOTA IT SERVICES

Thank You

Tarek Tomes

tarek.tomes@state.mn.us

Rohit Tandon

rohit.tandon@state.mn.us