The Rise of Ransomware and Steps to Mitigate its Risk

New technology developments always come with new threats. Industries and infrastructures all over the world depend on digital systems to operate—and while these systems enable increased efficiency and profitability, they open the door for cybercriminals to take advantage of their weaknesses.

Over the past several years, ransomware has evolved in sophistication and increased in frequency. In 2020, the United States alone experienced 65,000 ransomware attacks—an average of just over seven attacks every hour.[1] Hackers are getting smarter, and the consequences are getting steeper.

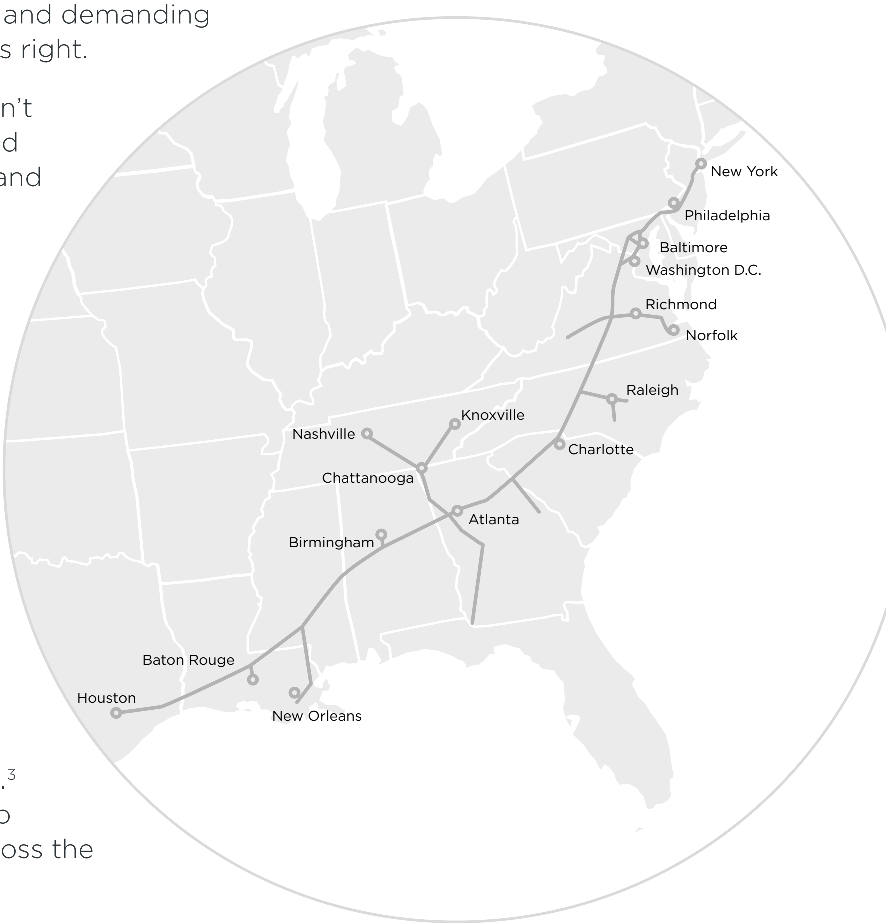
RANSOMWARE IN ACTION

Before May of 2021, no one had heard of DarkSide, a little-known group of cyberattackers based in eastern Europe. They gained instant notoriety when their ransomware attack shut down the Colonial Pipeline, one of the United States' biggest fuel pipeline operators. Gangs like DarkSide specialize in hacking IT systems, stealing sensitive organizational data, and demanding exorbitant ransom payments before setting things right.

The long-term effects of a ransomware attack don't just involve money—although lost productivity and ransom costs can be debilitating. Data breaches and frozen systems can also impact national security, as evidenced by the Colonial Pipeline shutdown. The 5,500-mile pipeline's downtime caused a fuel shortage across the southeastern United States and threatened economic stability.

The ransom attack resulted in a payment of $4.4 million. Additionally, the disruption to the payment collection system led to shutdowns, and the perceived gas shortage triggered stockpiling and public panic.[2]

"This [attack] underscores the threat that ransomware poses to organizations regardless of size or sector," said Eric Goldstein, executive assistant director of the cybersecurity division at the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency.[3] Without a 360-degree security solution in place to analyze all vulnerabilities and risks, companies across the globe are susceptible to hackers' creativity.

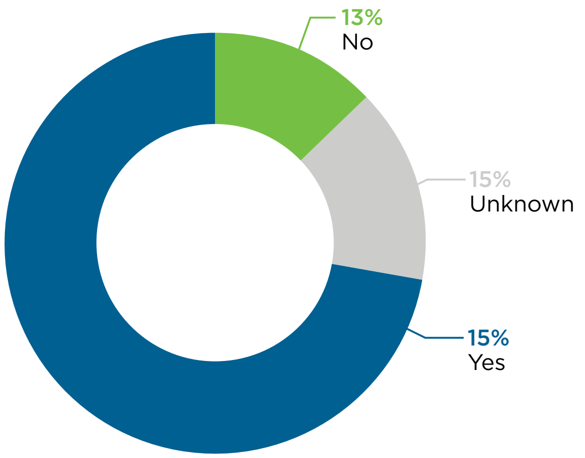


RANSOMWARE AS A COMMODITY

Today's cybercriminals don't just attack their own targets—they offer their services for hire. Ransomware as a service (RaaS) enables almost anyone to wreak havoc, as long as they sign up for the service. RaaS kits give bad actors a quick, affordable avenue to attack by offering a ready-made ransomware package to whomever is willing to pay. Much like software as a service (SaaS) features, RaaS kits can provide 24/7 support, bundle offers, user reviews, forums, and other features—with monthly costs ranging from $40 to several thousand dollars.[4] Anyone from disgruntled employees to international gangs can pose a threat, and no company is immune.

The average cost of the ransom payments increased more than 80% over the first five months of 2021. As in the case of the Colonial Pipeline attack, the actual ransom payments made by organizations are likely to be eclipsed by the combined costs of lost business, damage done to consumer trust, expenses of emergency remediation actions, and business disruption created by the ransom incident. Add to this the possible litigation fees for lost consumer data, and the impact of ransomware takes on a whole new dimension. In the 48 ransomware incidents in the United States healthcare sector tracked by HC3 in 2021, at least 72% included leaked victim data, whether from full file dumps, screenshots, or samples. HC3 estimated that data leaks ranged from just a few screenshots to as large as terabytes of data from the victims.[5]

U.S. HPH RANSOMWARE INCIDENTS 2021:
WAS DATA LEAKED?



FACT:
RANSOMWARE ATTACKS

The average ransom payment has increased by almost

50%

in 2021.

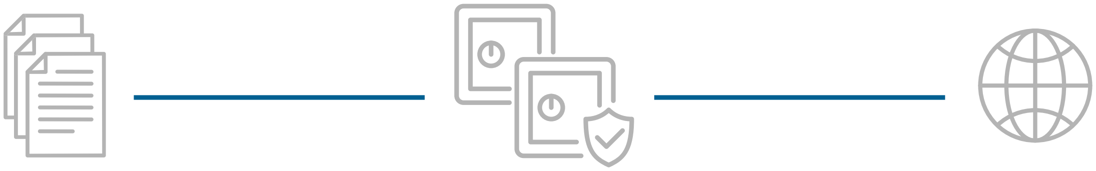
Payouts averaged $155k at the end of 2020, but rose to almost $280k as of May 2021.

2021 LEADING SUCCESSFUL RANSOMWARE ATTACKS BY INDUSTRY

Data from January 2021-April 2021**

Government	19+
Services	19+
Education	17+
Manufacturing	10+
Technology	9+
Healthcare	7+
Retail	7+
Utilities	3+
Finance	3+
Other	5+

3-2-1 Backup Rule



Maintain at least **3 copies** of your data

Keep **2 copies** stored at separate locations

Store at least **1 copy** at an off-site location

PROTECTING AGAINST RANSOMWARE

As cybercriminals get smarter, organizations must achieve a 360-degree view of risk to prevent a ransomware attack. Today's CISOs cannot expect to eliminate the threat of ransomware entirely, which means establishing both prevention and recovery plans is critical.

Consider these recommendations from CISA's Alert (AA21-131A) *DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks*:

1. **Require multi-factor authentication** for remote access to OT and IT networks.

2. **Enable strong spam filters** to prevent phishing emails from reaching end users. Filter emails containing executable files from reaching end users.

3. **Implement a user training program** and simulated attacks for spear phishing to discourage users from visiting malicious websites or opening malicious attachments, and reinforce the appropriate user responses to spear phishing emails.

4. **Filter network traffic** to prohibit ingress and egress communications with known malicious IP addresses. Prevent users from accessing malicious websites by implementing URL block lists and/or allow lists.

5. **Update software**, including operating systems, applications, and firmware on IT network assets, in a timely manner. Consider using a centralized patch management system; use a risk-based assessment strategy to determine which OT network assets and zones should participate in the patch management program.

6. **Limit access to resources over networks**, especially by restricting RDP. After assessing risks, if RDP is deemed operationally necessary, restrict the originating sources, and require multi-factor authentication.

7. **Set anti-virus/anti-malware programs to conduct regular scans** of IT network assets using up-to-date signatures. Use a risk-based asset inventory strategy to determine how OT network assets are identified and evaluated for the presence of malware.

8. **Implement unauthorized execution prevention by:**
   - Disabling macro scripts from Microsoft Office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full Microsoft Office suite applications.
   - Implementing application allow-listing, which only allows systems to execute programs known and permitted by security policy.
   - Monitoring and/or blocking inbound connections from Tor exit nodes and other anonymization services.
   - Deploying signatures to detect and/or block inbound connection from Cobalt Strike servers and other post exploitation tools.

SDG | TRUOPS: END-TO-END CYBER RISK MANAGEMENT SOLUTIONS

To maintain cyber risk awareness and cyber resilience, your organization needs up-to-the-minute insights into your risk posture.

SDG is a global cybersecurity and governance and regulatory compliance (GRC) services and software firm that enables clients to mitigate and manage cyber risk more effectively.

For nearly 30 years, SDG security professionals and support teams have helped clients architect and implement effective information security, cyber defense, and risk management solutions that address:

- **Identity access governance (IAM, SSO, MFA)**
- **Cyber security managed services (vulnerability management, patch & configuration management, continuous security & risk monitoring)**
- **Cloud strategy, security, & migration**
- **Governance, risk, and compliance (GRC) SaaS software**
- **GRC as-a-service solutions:**
  - Compliance as a service (CaaS)
  - Third-party vendor risk management as a service (3PRMaaS)
  - Vulnerability management as a service (VMaaS)

SDG's cyber risk management platform, TruOps™ **www.truops.com**, is a SaaS solution that enables a modular, integrated approach to managing GRC and cybersecurity automation while seamlessly supporting organization-wide IT risk management program initiatives. TruOps modules address a comprehensive range of capabilities:

- **Policy management**
- **IT risk management**
- **Compliance management**
- **Issues and exception management**
- **Cyber threat and vulnerability management**
- **Vendor and third-party risk management**
- **Identity risk management**

Reach out to us today to set up a demo.

WHAT TO DO IF YOUR ORGANIZATION IS IMPACTED BY A RANSOMWARE INCIDENT

1

Isolate the infected system.

2

Turn off other computers and devices.

3

Power-off and segregate any other computers or devices that shared a network with the infected computer(s) that have not been fully encrypted by ransomware.

4

Secure your backups.

5

Ensure that your backup data is offline, secure, and free of malware.

ABOUT SDG

With more than 30 years of experience partnering with global enterprises on complex business and IT initiatives, SDG is a trusted provider of advisory, transformation, and managed services. The firm empowers organizations to strengthen cyber resilience by integrating AI into identity, threat, and risk management solutions that protect digital assets and deliver measurable business value. Learn more at www.sdgc.com.

RESOURCES

1. https://www.npr.org/2021/06/09/1004684788/u-s-suffers-over-7-ransomware-attacks-an-hour-its-now-a-national-security-risk
2. https://www.hhs.gov/sites/default/files/ransomware-trends-2021.pdf
3. https://www.washingtonpost.com/business/2021/05/08/cyber-attack-colonial-pipeline/
4. https://www.crowdstrike.com/cybersecurity-101/ransomware/ransomware-as-a-service-raas/
5. https://www.hhs.gov/sites/default/files/ransomware-trends-2021.pdf

SDG

Contact Us: solutions@sdgc.com

55 North Water Street
Norwalk, CT 06854

203.866.8886

sdgc.com