

RANSOMWARE

What It Is and What To Do About It



WHAT IS RANSOMWARE?

Ransomware is a type of malicious software cyber actors use to deny access to systems or data. The malicious cyber actor holds systems or data hostage until the ransom is paid. After the initial infection, the ransomware attempts to spread to shared storage drives and other accessible systems. If the demands are not met, the system or encrypted data remains unavailable, or data may be deleted.

HOW DO I PROTECT MY NETWORKS?

A commitment to cyber hygiene and best practices is critical to protecting your networks. Here are some questions you may want to ask of your organization to help prevent ransomware attacks:

1. **Backups:** Do we backup all critical information? Are the backups stored offline? Have we tested our ability to revert to backups during an incident?
2. **Risk Analysis:** Have we conducted a cybersecurity risk analysis of the organization?
3. **Staff Training:** Have we trained staff on cybersecurity best practices?
4. **Vulnerability Patching:** Have we implemented appropriate patching of known system vulnerabilities?
5. **Application Whitelisting:** Do we allow only approved programs to run on our networks?
6. **Incident Response:** Do we have an incident response plan and have we exercised it?
7. **Business Continuity:** Are we able to sustain business operations without access to certain systems? For how long? Have we tested this?
8. **Penetration Testing:** Have we attempted to hack into our own systems to test the security of our systems and our ability to defend against attacks?

HOW DO I RESPOND TO RANSOMWARE?

Implement your security incident response and business continuity plan. It may take time for your organization's IT professionals to isolate and remove the ransomware threat to your systems and restore data and normal operations. In the meantime, you should take steps to maintain your organization's essential functions according to your business continuity plan. Organizations should maintain and regularly test backup plans, disaster recovery plans, and business continuity procedures.

Contact law enforcement immediately. We encourage you to contact a local **FBI**¹ or **USSS**² field office immediately to report a ransomware event and request assistance.

There are serious risks to consider before paying the ransom. We do not encourage paying a ransom. We understand that when businesses are faced with an inability to function, executives will evaluate all options to protect their shareholders, employees, and customers. As you contemplate this choice, consider the following risks:

- Paying a ransom does not guarantee an organization will regain access to their data; in fact, some individuals or organizations were never provided with decryption keys after having paid a ransom.
- Some victims who paid the demand have reported being targeted again by cyber actors.
- After paying the originally demanded ransom, some victims have been asked to pay more to get the promised decryption key.
- Paying could inadvertently encourage this criminal business model.

¹ https://www.fbi.gov/contact-us/field/listing_by_state

² <http://www.secretservice.gov/contact/>



United States Secret Service & Homeland Security Investigations



RANSOMWARE PREVENTION & MITIGATION ARE ESSENTIAL

Prevention and mitigation are the key to limiting the risk posed by ransomware. Response and recovery options are extremely limited if an enterprise does not have back-ups in place. Companies should ensure their Continuity of Operations Plan (COOP) includes having appropriate back-ups in place to avoid being in a circumstance where payment of the ransom may be the only option to recover the data.

Questions to Assess Preparedness

- Have we identified our most valuable data? Is it backed up or protected through extra measures, including isolating your critical data from other networks and encryption?
- Does my organization have, and regularly, test a cyber incident response plan?
- How do we coordinate and implement cyber incident response planning across the enterprise?
- Does my organization have a cybersecurity policy in place?
- What are the risks to the critical functions of our organization if data was compromised or withheld? How would it affect our bottom line?
- How have we linked our physical security team with our cybersecurity team?
- Do we know when we will call law enforcement or DHS for assistance, and who we will call?

LAW ENFORCEMENT

The U.S. Secret Service and U.S. Immigration and Customs Enforcement/Homeland Security Investigations (ICE/HSI) discourages the paying of extortion demands. Unfortunately, we are currently not aware of any particular means to recover the data encrypted by current versions of major ransomware families, without access to the private key, or restoring the withheld data from an available back-up. Accordingly, companies should ensure they have appropriate backups in place to avoid being placed in this dilemma. Whatever a business's decision, it should report the crime and coordinate its approach with an appropriate law enforcement agency. Paying the ransom may recover the data in some cases, but it also has risks, including:

- It may encourage criminals to re-target the victim with higher ransom demands,
- In some cases it does not recover the data,
- It may contribute to increasing the prevalence of this criminal scheme, and
- Paying the ransom may result in further legal or reputation risks to the business.

In all cases of extortion immediately contact an appropriate law enforcement agency, whether Federal, State, or Local, to report a ransomware event and request assistance. The United States Secret Service's Electronic Crimes Task Forces and ICE/HSI field offices are available to respond and investigate significant ransomware cases.

FEDERAL LAW ENFORCEMENT CONTACT INFORMATION

United States Secret Service
Electronic Crimes Task Forces
www.secretservice.gov/investigation/#field

USSS Field Offices
www.secretservice.gov/contact/

U.S. Immigration and Customs Enforcement
Homeland Security Investigations (ICE/HSI)
HSI Tip Line: Call 866-DHS-2-ICE (866-347-2423)
<https://www.ice.gov/webform/hsi-tip-form>
HSI Field Offices
<https://www.ice.gov/contact/hsi>